XenApp y XenDesktop 7.15 LTSR

Apr 18, 2018

El programa Long Term Service Release (LTSR o Servicio a largo plazo) de XenApp y XenDesktop ofrece estabilidad y respaldo a largo plazo para XenApp y XenDesktop.

Los programas LTSR de XenApp y XenDesktop actualmente disponibles corresponden a las versiones 7.6 y 7.15. Cumulative Update 2 (CU2) es la actualización más reciente de la versión 7.15 LTSR. Si no conoce el programa LTSR y no ha implementado las versiones 7.6 o 7.15 LTSR, no es necesario instalarlas ahora. En vez de ello, Citrix recomienda empezar directamente con la actualización CU2 de 7.15 LTSR.

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

Para obtener información general sobre las funciones de 7.15 LTSR que se han agregado desde la versión 7.6 LTSR, consulte la tabla XenApp and XenDesktop Feature Summary Comparison.

Descargas

7.15 LTSR XenApp y XenDesktop Cumulative Update 2

7.15 LTSR XenApp y XenDesktop

Enlaces útiles

- Citrix Supportability Pack

  Citrix Supportability Pack (paquete de compatibilidad) es un conjunto de herramientas comunes escritas por ingenieros de Citrix para ayudar a diagnosticar y solucionar problemas de productos XenDesktop o XenApp. Las herramientas se organizan en características y componentes para encontrarlos y utilizarlos más fácilmente. Las primeras versiones del Pack sirvieron de trampolín para trabajo posterior...

- Preguntas frecuentes de LTSR (FAQ)

  El equipo Citrix Windows App Delivery ha estado publicando innovaciones y mejoras de funcionalidades para las líneas de producto de XenApp y XenDesktop a un ritmo rápido; en el año 2015, se publicaron nuevas versiones de producto cada trimestre. Este ritmo acelerado de innovaciones mejora los casos de uso de XenApp y...

- Opciones de servicio de XenApp y XenDesktop

  Unas opciones flexibles de servicio permiten una asistencia previsible. Citrix ofrece periódicamente características y funcionalidades nuevas de XenApp y XenDesktop para que su negocio siga siendo competitivo, para optimizar sus operaciones de TI, mejorar la seguridad de sus datos y garantizar que sus empleados tengan acceso a sus recursos empresariales desde cualquier lugar.

- Fechas de la vida útil del producto

  Consulte esta tabla para ver las fechas de vida útil de los productos. En la siguiente tabla matriz de productos, se

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ofrece información acerca de los productos Citrix cuyos ciclos de vida útil se rigen por fases de ciclo de vida. Los hitos de ciclo de vida de los productos son: Notice of Status Change (NSC o Aviso de cambio de estado), End of Sales (EOS o Fin de ventas), End of Maintenance (EOM o Fin de mantenimiento) y End of Life (EOL o Fin de vida).

- Programa LTSR para Receiver para Windows

  Para cada versión principal (p. ej., v3.0) de Citrix Receiver para Windows, Mac, Linux, HTML5, Java, o WinCE, los usuarios recibirán un ciclo de vida de un mínimo de 4 años. El ciclo de vida consiste en una fase de mantenimiento principal (Mainstream Maintenance Phase) de, al menos, los tres primeros años, seguida de una fase de mantenimiento ampliado (Extended Maintenance Phase) para...

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Novedades

Apr 18, 2018

Acerca de esta versión

Acerca de Cumulative Update 2 (CU2)

Acerca de Cumulative Update 1 (CU1)

Acerca de 7.15 LTSR (versión inicial)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cumulative Update 2 (CU2)

Apr 18, 2018

Acerca de esta versión

En XenApp y XenDesktop 7.15 LTSR Cumulative Update 2 (CU2), se han solucionado más de 150 problemas notificados desde la publicación de 7.15 LTSR CU1.

7.15 LTSR (información general)

Problemas resueltos desde XenApp y XenDesktop 7.15 LTSR CU1

Problemas conocidos en esta versión

Descargas

Descargar 7.15 LTSR CU2

Nuevas implementaciones

¿Cómo implemento la actualización CU2 desde cero?

Puede configurar un entorno nuevo de XenApp o XenDesktop basado en CU2 mediante el metainstalador de CU2. Antes de hacerlo, se recomienda familiarizarse con el producto:

Consulte la sección XenApp y XenDesktop 7.15 LTSR (versión inicial) y lea atentamente las secciones Información técnica general, Instalación y configuración y Seguridad antes de planificar la implementación. Compruebe que la configuración de todos los componentes cumple los requisitos del sistema.

Implementaciones existentes

¿Qué actualizo?

CU2 ofrece actualizaciones para componentes base de 7.15 LTSR.Recuerde: Citrix recomienda actualizar a CU2 todos los componentes de LTSR de la implementación. Por ejemplo: Si Provisioning Services forma parte de su implementación LTSR, actualice los componentes de Provisioning Services a CU2. Si Provisioning Services no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

Componentes base de XenApp y XenDesktop 7.15 LTSR CU2

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Baseline Component	Version	Notes
VDA para SO de escritorio	7.15.2000	
VDA para SO de servidor	7.15.2000	
Delivery Controller	7.15.2000	
Citrix Studio	7.15.2000	
Citrix Director	7.15.2000	
Experiencia de administración de Directivas de grupo	3.1.2000	
StoreFront	3.12.2000	
Provisioning Services	7.15.3	
Universal Print Server	7.15.2000	
Grabación de sesiones	7.15.2000	Solo edición Platinum
Linux VDA	7.15.2000	Consulte la documentación de Linux VDA para ver las plataformas respaldadas.
Profile Management	7.15.2000	
Servicio de autenticación federada	7.15.2000	

Componentes compatibles con XenApp y XenDesktop 7.15 LTSR CU2

Se recomienda usar los siguientes componentes en entornos 7.15 LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 7.15 LTSR.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR CU2 Compatible Components and Platforms	Version
App Layering	4.10.0
Citrix SCOM Management Pack para License Server	1.2
Citrix SCOM Management Pack para Provisioning Services	1.19
Citrix SCOM Management Pack para StoreFront	1.13
Citrix SCOM Management Pack para XenApp y XenDesktop	3.14
HDX RealTime Optimization Pack	2.4
License Server	11.14.0.1 compilación 23101
Autoservicio de restablecimiento de contraseñas	1.1.10.0
Workspace Environment Management	4.6

Versiones compatibles de Citrix Receiver

Para facilitar el mantenimiento y para garantizar un rendimiento óptimo, Citrix recomienda actualizar a la versión más reciente de Citrix Receiver que esté disponible. Las versiones más recientes pueden descargarse desde https://www.citrix.com/downloads/citrix-receiver.html. Para mayor comodidad, considere la posibilidad de suscribirse al Feed RSS de Citrix Receiver para recibir una notificación cuando una nueva versión de Citrix Receiver esté disponible.

Tenga en cuenta que Citrix Receiver no da derecho a ventajas de XenApp y XenDesktop LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice a una versión más reciente de Citrix Receiver en sus entornos 7.15 LTSR. En el caso de Citrix Receiver para Windows, Citrix ha anunciado un programa LTSR especial. Encontrará más información acerca de este programa en la página Lifecycle Milestones for Citrix Receiver.

Específicamente, 7.15 LTSR CU2 admite las siguientes versiones de Citrix Receiver y todas las versiones posteriores.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR CU2 Compatible Version of Citrix Receiver	Version
Citrix Receiver para Android	3.13.5 o posterior
Citrix Receiver para Chrome	2.6.5 o posterior
Citrix Receiver para HTML5	2.6.5 o posterior
Citrix Receiver para iOS	7.5.3 o posterior
Citrix Receiver para Linux	13.9.1 o posterior
Citrix Receiver para Mac	12.9 o posterior
Citrix Receiver para UWP (Plataforma universal de Windows)	1.0.5 o posterior
Citrix Receiver para Windows	4.9 o posterior

Exclusiones notables de XenApp y XenDesktop 7.15 LTSR

Las siguientes características, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 7.15 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y características excluidos están disponibles a través de las versiones publicadas regularmente.

Excluded Features
Framehawk
Integración de StoreFront con Citrix Online

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Excluded Components
Personal vDisk: • Excluido para máquinas Windows 10. • Para máquinas con Windows 7, hay respaldo limitado de LTSR hasta el 14 de enero de 2020 (requisitos de CU aplicables)
AppDisks

Excluded Windows Platforms *
Windows 2008 de 32 bits (para Universal Print Server)

* Citrix se reserva el derecho a actualizar el respaldo para plataformas basándose en los hitos de ciclo de vida de proveedores externos.

Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes. Para obtener más información, consulte http://more.citrix.com/XD-INSTALLER.

Migración de XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficiente y rápida desde una comunidad XenApp 6.5 a un sitio que ejecuta XenApp 7.15 LTSR CU2. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de XenApp 7.15 LTSR CU2 y crear un sitio, siga estos pasos para el proceso de migración:

- Ejecute el instalador de XenApp 7.15 CU2 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5. Estos cmdlets exportan las configuraciones de aplicaciones y directivas Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de XenApp 7.15 LTSR CU2 por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de XenApp 7.15 CU2. Estos cmdlets importan las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para obtener más información, consulte Migración de XenApp 6.x.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resueltos

Apr 18, 2018

Citrix Director

- Cuando filtra las máquinas por nombre DNS, es posible que Citrix Director no muestre ninguna máquina o bien muestre entradas duplicadas de máquinas. El problema ocurre la primera vez que la máquina se agrega a la base de datos de supervisión, pero se agrega simultáneamente desde dos Delivery Controllers diferentes. Por eso, se crean dos entradas de la máquina. [#LC4905]
- Puede ocurrir una excepción cuando no se puede recuperar la configuración de Remote PC desde el catálogo de máquinas con el rol de administrador personalizado. El problema ocurre cuando se tiene permiso para administrar el catálogo de máquinas, pero el ámbito no contiene ese catálogo concreto. [#LC8170]
- Si va a **Filtros** > **Sesiones** en Citrix Director e intenta cambiar el tamaño del explorador Web, toda la tabla se ajusta incorrectamente. [#LC8624]
- El archivo CSV queda inutilizable cuando exporta datos desde Citrix Director. Este problema se produce cuando configura versiones de Microsoft Windows que no son en inglés como idioma de visualización de Director, ya que las comas se entienden como separadores de valores y decimales. [#LC8625]
- Cuando inicia Citrix Director, aparece el siguiente mensaje de error en la ficha **Infraestructura**:

  "No se puede obtener los datos. Se ha perdido la conexión con el servidor Web. Compruebe la conexión de red y vuelva a intentarlo". [#LC8752]
- Los nombres de sitios de Director aparecen truncados cuando hay varios sitios configurados. [#LC9258]

Directiva de Citrix

- Cuando abre una segunda instancia del Editor de directivas de grupo (gpedit.msc), el nodo de directivas de Citrix no se abre y aparece este mensaje de error:

  "Unhandled exception in managed code snap-in" (Excepción no controlada en el complemento de código administrado). [#LC7600]
- Cuando se aplican directivas Citrix a través de la Consola de administración de directivas de grupo (GPMC), es posible que las directivas no aparezcan en las configuraciones de directivas de GPMC. Sin embargo, al editar el objeto de directiva de grupo (GPO), las directivas aparecen y las configuraciones se habilitan. [#LC8282]
- Usar la Administración de Directivas de grupo Citrix 3.1 para agregar la configuración **Asignaciones de impresora** a una **Directiva de usuario** en Active Directory puede causar un problema de cambio de tamaño de la ventana. La ventana puede comenzar a cambiar automáticamente de tamaño horizontal después de abrirla, hasta extenderse a la esquina de la pantalla. Por eso, modificar la directiva puede ser difícil porque no puede llegar a todas las columnas. [#LC8684]
- Cuando los archivos ubicados en la carpeta de caché de las directivas locales (%ProgramData%/CitrixCseCache) se

© 1999-2017 Citrix Systems, Inc. All rights reserved.

definen como "Solo lectura", es posible que la configuración de las directivas no se aplique correctamente. [#LC8750]

- 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 los detalles de la aplicación. [#LC8798]
- Puede que no se agreguen máquinas a un grupo de entrega cuando se usa el nombre NETBIOS para las asociaciones de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC9393]

Citrix Studio

- Cuando intenta agregar manualmente una aplicación desde Linux VDA, puede aparecer el mensaje de error:

  "El valor no puede ser nulo mientras se publica la aplicación".

  No obstante, la aplicación se agrega correctamente cuando hace clic en "Aceptar" en el mensaje de error que aparece. [#LC7910]
- Los intentos de eliminar aplicaciones de un grupo de entrega pueden fallar cuando las aplicaciones se encuentran en la subcarpeta del nodo **Aplicación** en Citrix Studio. [#LC8705]
- Puede que no se agreguen máquinas a un grupo de entrega cuando se usa el nombre NETBIOS para las asociaciones de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC9393]

Controller

- Pueden aparecer caracteres extraños al final de "Nombre simplificado del servicio" y "Descripción del servicio" de determinados servicios de Citrix instalados en sistemas operativos en japonés. [#LC5208]
- Cuando intenta recuperar datos de sesiones desde Citrix Director, aparecen entradas nulas en la base de datos de Monitor. En consecuencia, algunos datos no aparecen en Citrix Director, mientras que aparece el siguiente mensaje de error:

  "No se pudo obtener datos". [#LC6273]
- Cuando intenta agregar manualmente una aplicación desde Linux VDA, puede aparecer el mensaje de error:

  "El valor no puede ser nulo mientras se publica la aplicación".

  No obstante, la aplicación se agrega correctamente cuando hace clic en "Aceptar" en el mensaje de error que aparece. [#LC7910]
- Citrix Broker Service (Brokerservice.exe) puede cerrarse inesperadamente. El problema ocurre por un error en el módulo LicPolEng.dll. [#LC8638]
- Cuando aprovisiona las máquinas virtuales (VM) con los privilegios mínimos necesarios de VMware a través de Machine Creation Services, los intentos de eliminar las máquinas virtuales pueden fallar. Este error puede ocurrir incluso con los

© 1999-2017 Citrix Systems, Inc. All rights reserved.

permisos mínimos concedidos para VMware. [#LC8868]

- Cuando se elimina un usuario de Active Directory que está asignado con preferencia de zona, pueden fallar los intentos de importar la configuración del broker al broker secundario. La operación de importación también puede fallar después de actualizar XenDesktop a la versión más reciente. [#LC9269]
- Puede que no se agreguen máquinas a un grupo de entrega cuando se usa el nombre NETBIOS para las asociaciones de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC9393]

Redirección de Flash de HDX MediaStream

- Con la redirección de Flash de HDX MediaStream habilitada, cuando vuelve a conectar una sesión de VDA a Qumu.com, puede que el contenido Flash no se cargue en Microsoft Internet Explorer. [#LC9193]

Instalador

- Los intentos de cambiar la ruta del directorio de instalación en Delivery Controller podrían no funcionar para **XaXdProxy.msi**. [#LC8691]

Linux VDA

- La operación de registrar un Linux VDA utilizando el Delivery Controller podría fallar intermitentemente. [#LC7982]
- Un Citrix Director 7.13 que se ejecuta en Red Hat Enterprise Linux Server 7.3 podría no mostrar los detalles de la sesión de la máquina. Aparece el siguiente mensaje de error:

  "No se puede obtener los datos". [#LC8204]
- Un Linux VDA puede registrarse en el Delivery Controller y cancelar el registro más adelante. [#LC8205]
- Algunas aplicaciones de terceros que se utilizan para consultar la pantalla de una sesión en Linux VDA no muestran todos los píxeles. [#LC8419]
- Cuando hay varios servidores LDAP, pueden fallar los intentos de iniciar una aplicación en un Linux VDA después de que se actualicen las directivas y se agote el tiempo de espera de la sesión. [#LC8444]
- El proceso ctxhdx puede cerrarse inesperadamente con un fallo de segmentación (segfault) cuando la sesión está conectada a un Linux VDA. [#LC8611]
- Al utilizar la versión Linux VDA 7.16 Early Access Release, es posible que el agente del broker no obtenga el nombre de la aplicación. Este error hace que Director muestre el error **Agente solicitado**, después de lo cual se inicia de nuevo el proceso de registro. [#LC9243]

Profile Management

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Después de reiniciar el servicio Profile Management Service, puede que Citrix Director no muestre la información de inicio de sesión y personalización de usuario. [#LC6942]

Provisioning Services

StoreFront

- Con la opción de "Inicio automático del escritorio" habilitada, la opción para impedir inicios múltiples puede no funcionar. En consecuencia, fallan las solicitudes subsiguientes para iniciar la misma instancia del escritorio. [#LC7430]
- Después de actualizar StoreFront 2.6 instalado en una unidad no predeterminada, es posible que no se conserven los datos de suscripción de aplicaciones de los usuarios. [#LC8046]
- Después de reiniciar la consola MMC de StoreFront, el valor de la casilla **Mostrar Desktop Viewer** puede aparecer incorrectamente. [#LC8520]
- Si ejecuta un comando **Set-STFWebReceiverSiteStyle** con un archivo PNG (que respalda la transparencia) para personalizar StoreFront, el archivo PNG se convierte en un archivo JPEG. El formato de archivo JPEG puede perder el respaldo para transparencia. [#LC8677]
- Si se ejecuta un comando **Set-STFWebReceiverApplicationShortcuts** para configurar las URL de confianza para accesos directos a aplicaciones en sitios de Citrix Receiver para Web, puede agregarse una barra ("/") al final de la URL. [#LC8761]
- Cuando se utiliza el comando **Set-STFWebReceiverSiteStyle** para personalizar StoreFront, style.css puede modificarse incorrectamente en la carpeta Custom. Como resultado, la consola de StoreFront no puede leer la personalización. [#LC8776]
- Se puede producir un error de autenticación en los servidores de StoreFront. El problema ocurre debido al agotamiento del puerto dinámico TCP. [#LC8795]
- Pueden fallar los intentos de cambiar el logotipo de StoreFront mediante el comando **Set-STFWebReceiverSiteStyle**. [#LC8994]
- Pueden fallar los intentos de actualizar StoreFront cuando hay archivos de solo lectura presentes en el directorio de archivos personalizados en cualquier instancia de sitio de Citrix Receiver para Web. [#LC9252]

VDA para SO de escritorio

HDX 3D Pro

- Con HDX 3D Pro habilitado y una resolución personalizada habilitada en un VDA que se ejecuta en Microsoft Windows 10, aparece intermitentemente una pantalla gris al iniciar sesión. [#LC8417]

Redirección de Flash de HDX MediaStream

- Con la redirección de Flash de HDX MediaStream habilitada, cuando vuelve a conectar una sesión de VDA a Qumu.com,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

puede que el contenido Flash no se cargue en Microsoft Internet Explorer. [#LC9193]

Redirección de Windows Media de HDX MediaStream

- Con la Redirección de Windows Media de HDX MediaStream inhabilitada, los intentos de abrir ciertos formatos de archivos de vídeo desde el Reproductor de Windows Media pueden hacer que el vídeo que se está reproduciendo gire verticalmente. [#LC9194]

HDX RealTime

- Se instala RealTime Connector. Al usar aplicaciones con cámara Web redirigida (como Skype Empresarial), la cámara Web que se instala en un VDA de SO de escritorio puede redirigirse y detectarse durante el primer inicio de sesión. No obstante, cuando se reconecta a la sesión del usuario, la cámara Web ya no se detecta. El problema ocurre cuando RealTime Media Engine no está instalado en el dispositivo del usuario. [#LC8793]

Teclado

- Cuando inicia una aplicación en un dispositivo Android y se encuentra en un campo de texto, es posible que el teclado no aparezca automáticamente. Además, siempre tiene que tocar en el botón del teclado para abrir o cerrar. [#LC8936]

Impresión

- No se puede imprimir en ambas caras del papel cuando la impresora está configurada con Microsoft Word. [#LC7501]
- No se puede imprimir un documento desde una instancia publicada de Microsoft Internet Explorer. [#LC8093]
- Con el idioma francés como idioma de visualización instalado en un VDA, no se imprimen los documentos. [#LC8209]
- Una impresora redirigida desde un dispositivo de usuario puede no redirigirse tras volver a conectarse a la sesión. [#LC8762]
- El reinicio del servicio Citrix Print Manager Service (cpsvc.exe) puede fallar cuando detiene el servicio Print Spooler Service durante el inicio de la primera sesión. [#LC9192]

Sesión/Conexión

- Cuando se lee un archivo procedente de una unidad de cliente asignada, es posible que se devuelva el tamaño anterior del archivo que se haya guardado en la memoria caché si ese tamaño de archivo se ha modificado fuera de la sesión de cliente. Además, se insertan caracteres de valor nulo para los caracteres eliminados.

  Para habilitar la corrección, establezca el siguiente valor del Registro en "0":

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  Nombre: CacheTimeout
  Tipo: REG_DWORD
  Valor: El valor predeterminado es 60 segundos. Si CacheTimeOut se establece en 0, el tamaño del archivo se vuelve a cargar inmediatamente. Si no, se carga una vez superado el tiempo de espera definido. [#LC6314]

- Una sesión que se ejecuta en un VDA para SO de escritorio puede dejar de responder cuando se usa el modo de gráficos antiguo. Cuando se produce el problema, no puede actualizar nada en el Desktop Viewer, aunque éste no haya dejado de responder. Además, pasados entre 30 a 60 minutos, la sesión que antes no respondía se recupera. [#LC7777]
- Cuando inicia una aplicación con la persistencia de sesiones habilitada, la sesión puede cerrarse después de que aparezca

© 1999-2017 Citrix Systems, Inc. All rights reserved.

la aplicación. [#LC8245]

- Cuando intente iniciar un VDA para SO de escritorio, es posible que el escritorio se inicie y desaparezca pasados unos segundos. [#LC8373]
- Es posible que el Explorador de Windows se cierre de forma inesperada en los siguientes casos:
  - Al seleccionar una gran cantidad de archivos cuyos nombres contengan más de 260 caracteres y, a continuación, seleccionar la opción "Enviar a > Destinatario de fax".
  - Al intentar abrir aplicaciones de terceros.
  - Al intentar combinar archivos mediante Nitro PDF. [#LC8423]
- Los cambios que realice en Configuración avanzada del sistema, en la sección Efectos visuales, se aplican a la sesión actual del VDA para SO de escritorio, pero es posible que no se conserven para las sesiones subsiguientes. Para que estos cambios sean permanentes, debe establecer la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nombre: EnableVisualEffect
  Tipo: DWORD
  Valor: 1 [#LC8049, #LC8658]

- Después de desconectar una sesión, monitor1 podría aparecer incorrectamente como el monitor principal en el próximo inicio de sesión local. Este comportamiento puede ocurrir cuando inicia sesión localmente en un VDA con Acceso con Remote PC en un entorno de varios monitores y configura el monitor2 como el monitor principal, se conecta a través de un dispositivo de usuario y luego desconecta una sesión usando Desktop Viewer. [#LC8675]
- Cuando intenta iniciar una aplicación publicada que se ejecuta en Microsoft Windows Server 2012 o 2016, es posible que su acceso se bloquee. [#LC8681]
- Cuando inicia una aplicación en un entorno de varios monitores, puede aparecer una pancarta de inicio de sesión que abarque ambos monitores. Cuando utiliza un solo monitor, la ventana de la pancarta de inicio de sesión aparece en pantalla completa. [#LC8741]
- Con el acceso a aplicaciones locales habilitado, cuando intenta abrir aplicaciones en los escritorios publicados que se ejecutan en Microsoft Windows 10, las aplicaciones no se pueden minimizar. [#LC8813]
- El software DLP podría no examinar los archivos que contengan el enlace UNC. [#LC8893]
- Después de iniciar una aplicación publicada, la tecla Bloq Num no funciona. El problema ocurre cuando el indicador LED de la tecla Bloq Num se ve en el dispositivo del usuario, pero los números no funcionan en la sesión del usuario. El problema se produce a veces cuando la actualización de LED que solicitó el cliente ocurre antes de que el escritorio remoto recién creado inicialice su estado de LED. Cuando eso sucede, WinsStation puede no actualizar su estado de LED y el estado de LED entre el VDA y el dispositivo de punto final deja de estar sincronizado. [#LC8921]
- Puede que las aplicaciones y los escritorios no se inicien. El problema se da cuando el VDA para SO de servidor deja de responder.

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
  Nombre: EnableSCardHookVcResponseTimeout

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tipo: DWORD
Valor: 1 [#LC8969]

- Puede que las aplicaciones alojadas en la máquina virtual no se inicien. [#LC9001]
- Los intentos de volver a conectarse a una sesión pueden fallar. [#LC9040]
- Cuando utiliza el comando **WFQuerySessionInformation** del WFAPI SDK en una sesión para recuperar la información de la versión del VDA instalado, el comando no funciona. [#LC9041]
- Después de actualizar XenApp y XenDesktop de la versión 7.14 a la versión 7.15, si intenta cambiar entre las fichas de una aplicación publicada, la aplicación puede dejar de responder. Además, si disminuye el tamaño de la ventana integrada y luego la expande, lleva tiempo pintar todos los elementos incluidos en ella. [#LC9078]
- Una aplicación publicada puede cerrarse de forma intermitente inmediatamente después de iniciarla. [#LC9167]
- En un conjunto de aplicaciones Millennium con una resolución de pantalla diferente de la existente en la conexión inicial, una aplicación integrada podría cambiar incorrectamente de tamaño si vuelve a conectarse a ella. Por eso, es posible que la ventana esté truncada. [#LC9214]
- Intentar conectarse a un escritorio publicado en Windows 10 versión 1709 a través de un dispositivo de usuario puede resultar en una pantalla gris. Cuando intenta conectarse a través de la consola del hipervisor a un escritorio publicado, aparece una pantalla en negro con una rueda giratoria. Sin embargo, la conexión a través de un RDP a un escritorio publicado funciona correctamente. [#LC9215]
- Los intentos de iniciar aplicaciones desde Citrix Receiver para Mac pueden fallar. El problema ocurre cuando no se puede obtener la licencia del cliente (LicenseRequestClientLicense). [#LC9286]
- Con HDX 3D Pro habilitado, los intentos de iniciar un XenDesktop pueden fallar intermitentemente. El problema ocurre cuando hay un fallo de GPU. [#LC9343]
- Cuando se usa un perfil móvil, la visualización de la sesión desde una sesión de usuario a una sesión de escritorio remoto no administrada puede ser incorrecta. [#LC9471]

Tarjetas inteligentes

- Al usar una tarjeta inteligente, ciertas aplicaciones de terceros pueden dejar de responder en lugar de mostrar una solicitud de PIN. [#LC8805]

Excepciones del sistema

- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [#LC6177]
- Los servidores pueden sufrir una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA). [#LC6985]
- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [#LC7574]
- Los servidores pueden experimentar una excepción fatal en vdtw30.dll y mostrar una pantalla azul con el código de detención SYSTEM_SERVICE_EXCEPTION (3b). [#LC8087]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en pdcrypt2.sys con el código de comprobación de errores 0x3B. El problema ocurre cuando se inicia un VDA. [#LC8328]
- Con HDX 3D Pro y la codificación por hardware de GPU habilitados, cuando se usan las GPU de NVIDIA, el proceso de gráficos del software de Citrix (Ctxgfx.exe) puede cerrarse inesperadamente. El problema ocurre cuando se usan pantallas de alta resolución. [#LC8435]
- Los agentes VDA para SO de servidor pueden sufrir una excepción irrecuperable en picadm.sys y mostrar una pantalla azul. [#LC8708]
- Los VDA pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [#LC8749]
- Cuando inicia sesión por primera vez después de reiniciar el VDA, se produce una excepción inesperada de infracción del acceso. El proceso de gráficos del software de Citrix (Ctxgfx.exe) se cierra inesperadamente. En consecuencia, la imagen y el texto que aparecen en el VDA son borrosos. [#LC9005]
- Es posible que el Explorador de Windows se cierre de forma inesperada en los siguientes casos:
  - Al seleccionar una gran cantidad de archivos cuyos nombres contengan más de 260 caracteres y, a continuación, seleccionar la opción **Enviar a** > **Destinatario de fax**.
  - Al intentar abrir aplicaciones de terceros.
  - Al intentar combinar archivos mediante Nitro PDF. [#LC9076]

Experiencia de usuario

- Cuando copia contenido de cualquier aplicación que se ejecuta en un cliente y lo pega en una aplicación en una sesión de usuario, el contenido no se pega. Además, el botón **Pegar** no está habilitado. [#LC8516]
- Puede que la pantalla no se actualice con la solicitud de inicio de sesión tras intentar iniciar sesión en una sesión que se bloqueó. [#LC8774]

Interfaz de usuario

- Aparece un fondo de pantalla incluso después de haber establecido la directiva de fondos de pantalla en "Prohibida". [#LC8398]
- Algunas aplicaciones de terceros que se utilizan para consultar la pantalla de una sesión en Linux VDA no muestran todos los píxeles. [#LC8419]

Otros problemas

- Esta corrección soluciona problemas de rendimiento y ofrece mejoras de calidad para Enlightened Data Transport (EDT). [#LC9278]

VDA para SO de servidor

Redirección de Windows Media de HDX MediaStream

- Con la Redirección de Windows Media de HDX MediaStream inhabilitada, los intentos de abrir ciertos formatos de archivos de vídeo desde el Reproductor de Windows Media pueden hacer que el vídeo que se está reproduciendo gire

© 1999-2017 Citrix Systems, Inc. All rights reserved.

verticalmente. [#LC9194]

HDX RealTime

- Se instala RealTime Connector. Al usar aplicaciones con cámara Web redirigida (como Skype Empresarial), la cámara Web que se instala en un VDA de SO de escritorio puede redirigirse y detectarse durante el primer inicio de sesión. No obstante, cuando se reconecta a la sesión del usuario, la cámara Web ya no se detecta. El problema ocurre cuando RealTime Media Engine no está instalado en el dispositivo del usuario. [#LC8793]

Teclado

- Cuando inicia una aplicación en un dispositivo Android y se encuentra en un campo de texto, es posible que el teclado no aparezca automáticamente. Además, siempre tiene que tocar en el botón del teclado para abrir o cerrar. [#LC8936]

Impresión

- No se puede imprimir en ambas caras del papel cuando la impresora está configurada con Microsoft Word. [#LC7501]
- No se puede imprimir un documento desde una instancia publicada de Microsoft Internet Explorer. [#LC8093]
- Con el idioma francés como idioma de visualización instalado en un VDA, no se imprimen los documentos. [#LC8209]
- El reinicio del servicio Citrix Print Manager Service (cpsvc.exe) puede fallar cuando detiene el servicio Print Spooler Service durante el inicio de la primera sesión. [#LC9192]

Administración de servidores/sitios

- El servicio Citrix Stack Control Service (SCService64.exe) puede cerrarse inesperadamente cuando el VDA comprueba la pertenencia a grupos del usuario si hay dos o más grupos con el mismo nombre en varios dominios. El problema ocurre cuando la cadena "DnsDomainName" está vacía en la estructura de DS_DOMAIN_TRUSTSW. [#LC8484]

Sesión/Conexión

- Cuando se inicia un VDA de SO de servidor de Long Term Service Release Cumulative Update 2 o de versiones anteriores, puede aparecer el siguiente mensaje de advertencia en el registro de eventos de sistema:

  "Falló un intento de conexión con SemsService, con el código de error 0x2". [#LC6311]

- Cuando se lee un archivo procedente de una unidad de cliente asignada, es posible que se devuelva el tamaño anterior del archivo que se haya guardado en la memoria caché si ese tamaño de archivo se ha modificado fuera de la sesión de cliente. Además, se insertan caracteres de valor nulo para los caracteres eliminados.

  Para habilitar la corrección, establezca el siguiente valor del Registro en "0":

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  Nombre: CacheTimeout
  Tipo: REG_DWORD
  Valor: El valor predeterminado es 60 segundos. Si CacheTimeOut se establece en 0, el tamaño del archivo se vuelve a cargar inmediatamente. Si no, se carga una vez superado el tiempo de espera definido. [#LC6314]

- Después de desacoplar un equipo portátil, se dejan de compartir sesiones. El problema ocurre cuando el VDA se vuelve a registrar en el Delivery Controller mientras se activa una notificación "sin servicio" durante la reconexión automática del cliente. [#LC7450]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Una sesión que se ejecuta en un VDA para SO de escritorio puede dejar de responder cuando se usa el modo de gráficos antiguo. Cuando se produce el problema, no puede actualizar nada en el Desktop Viewer, aunque éste no haya dejado de responder. Además, pasados entre 30 a 60 minutos, la sesión que antes no respondía se recupera. [#LC7777]
- En un dispositivo iOS, después de cerrar una aplicación publicada con un cliente App-V instalado en el VDA y las configuraciones "EnablePubilishingRefreshUI" y "Session Lingering" habilitadas en la sesión, podría abrirse y permanecer abierta una ventana en negro. El problema ocurre cuando la sesión está en un estado persistente activo. [#LC8080]
- Cuando inicia una aplicación con la persistencia de sesiones habilitada, la sesión puede cerrarse después de que aparezca la aplicación. [#LC8245]
- Los servidores dejan de responder en RPM.dll y aparece el siguiente mensaje de error:

  "ID de evento 1009, picadm: Se superó el tiempo de espera para el mensaje de respuesta del cliente". [#LC8339]
- Es posible que el Explorador de Windows se cierre de forma inesperada en los siguientes casos:
  - Al seleccionar una gran cantidad de archivos cuyos nombres contengan más de 260 caracteres y, a continuación, seleccionar la opción "Enviar a > Destinatario de fax".
  - Al intentar abrir aplicaciones de terceros.
  - Al intentar combinar archivos mediante Nitro PDF. [#LC8423]
- Citrix Director podría informar de varios fallos de conexión. El problema ocurre cuando la expansión de grupos asignados para controlar la visibilidad limitada de una aplicación se usa para cada usuario. Este proceso de expansión tarda mucho tiempo en completarse y se da en redes grandes que tienen muchos grupos que abarcan varios dominios. [#LC8652]
- Es posible que los puertos COM no se asignen en la versión 7.15 de los VDA. [#LC8656]
- Cuando intenta iniciar una aplicación publicada que se ejecuta en Microsoft Windows Server 2012 o 2016, es posible que su acceso se bloquee. [#LC8681]
- Cuando inicia una aplicación en un entorno de varios monitores, puede aparecer una pancarta de inicio de sesión que abarque ambos monitores. Cuando utiliza un solo monitor, la ventana de la pancarta de inicio de sesión aparece en pantalla completa. [#LC8741]
- Con el acceso a aplicaciones locales habilitado, cuando intenta abrir aplicaciones en los escritorios publicados que se ejecutan en Microsoft Windows 10, las aplicaciones no se pueden minimizar. [#LC8813]
- Cuando conecta un dispositivo de usuario a un VDA, es posible que no se muestre el escritorio. En cambio, aparece una pantalla gris en el escritorio. [#LC8821]
- El software DLP podría no examinar los archivos que contengan el enlace UNC. [#LC8893]
- Después de iniciar una aplicación publicada, la tecla Bloq Num no funciona. El problema ocurre cuando el indicador LED de la tecla Bloq Num se ve en el dispositivo del usuario, pero los números no funcionan en la sesión del usuario. El problema se produce a veces cuando la actualización de LED que solicitó el cliente ocurre antes de que el escritorio remoto recién creado inicialice su estado de LED. Cuando eso sucede, WinsStation puede no actualizar su estado de LED y el estado de LED entre el VDA y el dispositivo de punto final deja de estar sincronizado. [#LC8921]
- Puede que las aplicaciones y los escritorios no se inicien. El problema se da cuando el VDA para SO de servidor deja de responder.

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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartCard
Nombre: EnableSCardHookVcResponseTimeout
Tipo: DWORD
Valor: 1 [#LC8969]

- Puede que las aplicaciones alojadas en la máquina virtual no se inicien. [#LC9001]
- Cuando utiliza el comando **WFQuerySessionInformation** del WFAPI SDK en una sesión para recuperar la información de la versión del VDA instalado, el comando no funciona. [#LC9041]
- Después de actualizar XenApp y XenDesktop de la versión 7.14 a la versión 7.15, si intenta cambiar entre las fichas de una aplicación publicada, la aplicación puede dejar de responder. Además, si disminuye el tamaño de la ventana integrada y luego la expande, lleva tiempo pintar todos los elementos incluidos en ella. [#LC9078]
- Una aplicación publicada puede cerrarse de forma intermitente inmediatamente después de iniciarla. [#LC9167]
- En un conjunto de aplicaciones Millennium con una resolución de pantalla diferente de la existente en la conexión inicial, una aplicación integrada podría cambiar incorrectamente de tamaño si vuelve a conectarse a ella. Por eso, es posible que la ventana esté truncada. [#LC9214]
- Los intentos de iniciar aplicaciones desde Citrix Receiver para Mac pueden fallar. El problema ocurre cuando no se puede obtener la licencia del cliente (LicenseRequestClientLicense). [#LC9286]

Tarjetas inteligentes

- Al usar una tarjeta inteligente, ciertas aplicaciones de terceros pueden dejar de responder en lugar de mostrar una solicitud de PIN. [#LC8805]

Excepciones del sistema

- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [#LC6177]
- Los servidores pueden sufrir una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA). [#LC6985]
- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [#LC7574]
- Es posible que el proceso Service Host (svchost.exe) sufra una infracción de acceso y se cierre de forma inesperada. El problema ocurre por un error en el módulo icaendpoint.dll. [#LC7694]
- Los servidores pueden experimentar una excepción fatal en vdtw30.dll y mostrar una pantalla azul con el código de detención SYSTEM_SERVICE_EXCEPTION (3b). [#LC8087]
- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en pdcrypt2.sys con el código de comprobación de errores 0x3B. El problema ocurre cuando se inicia un VDA. [#LC8328]
- Con HDX 3D Pro y la codificación por hardware de GPU habilitados, cuando se usan las GPU de NVIDIA, el proceso de gráficos del software de Citrix (Ctxgfx.exe) puede cerrarse inesperadamente. El problema ocurre cuando se usan pantallas de alta resolución. [#LC8435]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en icardd.dll con el código de comprobación de errores 0x0000003B. [#LC8492]
- Los agentes VDA para SO de servidor pueden sufrir una excepción irrecuperable en picadm.sys y mostrar una pantalla azul. [#LC8708]
- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en icardd.dll con el código de comprobación de errores 0x0000003B. [#LC8732]
- Los VDA pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picadm.sys con el código de comprobación de errores 0x22. [#LC8749]
- Cuando inicia sesión por primera vez después de reiniciar el VDA, se produce una excepción inesperada de infracción del acceso. El proceso de gráficos del software de Citrix (Ctxgfx.exe) se cierra inesperadamente. En consecuencia, la imagen y el texto que aparecen en el VDA son borrosos. [#LC9005]
- Es posible que el Explorador de Windows se cierre de forma inesperada en los siguientes casos:
  - Al seleccionar una gran cantidad de archivos cuyos nombres contengan más de 260 caracteres y, a continuación, seleccionar la opción **Enviar a** > **Destinatario de fax**.
  - Al intentar abrir aplicaciones de terceros.
  - Al intentar combinar archivos mediante Nitro PDF. [#LC9076]

Experiencia de usuario

- Cuando copia contenido de cualquier aplicación que se ejecuta en un cliente y lo pega en una aplicación en una sesión de usuario, el contenido no se pega. Además, el botón **Pegar** no está habilitado. [#LC8516]
- En el VDA para SO de servidor, el cursor del mouse podría desaparecer de la sesión. Este problema se da cuando el cursor cambia al cursor **Text Select** y el color de fondo es el mismo que el color del cursor **Text Select**. En Microsoft Windows, el color de fondo predeterminado para las áreas editables es blanco; el color predeterminado del cursor **Text Select** también es blanco. Por eso, puede que el cursor no se vea. [#LC8807]
- Es posible que Microsoft Windows siga conservando el campo de contraseña editable durante el inicio de sesión incluso después de enviar las credenciales correctas. [#LC9407]

Interfaz de usuario

- Aparece un fondo de pantalla incluso después de haber establecido la directiva de fondos de pantalla en "Prohibida". [#LC8398]
- Algunas aplicaciones de terceros que se utilizan para consultar la pantalla de una sesión en Linux VDA no muestran todos los píxeles. [#LC8419]

Otros problemas

- Esta corrección soluciona problemas de rendimiento y ofrece mejoras de calidad para Enlightened Data Transport (EDT). [#LC9278]

Otros problemas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cuando Citrix Telemetry Service está inhabilitado o detenido, y se utiliza un metainstalador para actualizar XenApp y XenDesktop 7.15 LTSR a Cumulative Update 1 (CU1), puede aparecer este mensaje de advertencia:

"No podemos iniciar el servicio de Citrix que habilita la inscripción en Call Home. Consulte el artículo CTX218094 para obtener más información". [#LCM-3642]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cumulative Update 1 (CU1)

Apr 18, 2018
Fecha de publicación: 5 de diciembre de 2017

Acerca de esta versión

XenApp y XenDesktop 7.15 LTSR Cumulative Update 1 (CU1) soluciona más de 80 problemas notificados desde la publicación inicial de la versión 7.15 LTSR.

7.15 LTSR (información general)

Problemas resueltos desde XenApp y XenDesktop 7.15 LTSR (versión inicial)

Problemas conocidos en esta versión

Antes de actualizar desde 7.6 LTSR CU5...

La ventaja principal de actualizar 7.6 LTSR CU5 a 7.15 LTSR CU1 es que la versión base de 7.15 LTSR contiene muchas más características que la versión base de 7.6 LTSR. Sin embargo, si está considerando la posibilidad de actualizar, tenga en cuenta que hay un pequeño subconjunto de correcciones que se incluyen en 7.6 LTSR CU5 pero no están incluidas en 7.15 LTSR CU1. Esto es porque la versión 7.15 LTSR CU1 se lanzó antes que la versión 7.6 LTSR CU5. Para obtener una lista de correcciones que son aplicables a la versión 7.15 pero no están incluidas en la versión 7.15 LTSR CU1, consulte la Lista de correcciones existentes en 7.6 LTSR CU5 que no están incluidas en 7.15 LTSR CU1. Si su implementación tiene dependencias en correcciones específicas incluidas en 7.6 LTSR CU5, Citrix recomienda que revise esta lista antes de realizar la actualización.

Nuevas implementaciones

¿Cómo implemento la actualización CU1 desde cero?

Puede configurar un entorno nuevo de XenApp o XenDesktop basado en CU1 mediante el metainstalador de CU1. Antes de hacerlo, se recomienda familiarizarse con el producto:

Consulte la sección XenApp y XenDesktop 7.15 LTSR (versión inicial) y lea atentamente las secciones Información técnica general, Instalación y configuración y Seguridad antes de planificar la implementación. Compruebe que la configuración de todos los componentes cumple los requisitos del sistema.

Implementaciones existentes

¿Qué actualizo?

CU1 ofrece actualizaciones de 13 componentes base de 7.15 LTSR.Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a CU1. Por ejemplo: Si Provisioning Services forma parte de su implementación LTSR, actualice los componentes de Provisioning Services a CU1. Si Provisioning Services no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

Componentes base de XenApp y XenDesktop 7.15 LTSR CU1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR CU1 Baseline Component	Version	Notes
VDA para SO de escritorio	7.15.1000	
VDA para SO de servidor	7.15.1000	
Delivery Controller	7.15.1000	
Citrix Studio	7.15.1000	
Citrix Director	7.15.1000	
Experiencia de administración de Directivas de grupo	3.1.1000	
StoreFront	3.12.1000	
Provisioning Services	7.15.1	
Universal Print Server	7.15.1000	
Grabación de sesiones	7.15.1000	Solo edición Platinum
VDA Linux	7.15.1000	Consulte la documentación de Linux VDA para ver las plataformas respaldadas.
Profile Management	7.15.1000	
Servicio de autenticación federada	7.15.1000	

Componentes compatibles con XenApp y XenDesktop 7.15 LTSR CU1

Se recomienda usar los siguientes componentes en entornos 7.15 LTSR CU1. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos 7.15 LTSR CU1.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Compatible Components and Platforms	Version
AppDNA	7.16
Citrix SCOM Management Pack para License Server	1.2
Citrix SCOM Management Pack para Provisioning Services	1.19
Citrix SCOM Management Pack para StoreFront	1.13
Citrix SCOM Management Pack para XenApp y XenDesktop	3.14
HDX RealTime Optimization Pack	2.2.100
Servidor de licencias	11.14.0.1 compilación 22103
Administración del entorno de espacio de trabajo	4.4
App Layering	4.6
Autoservicio de restablecimiento de contraseñas	1.1

Versiones compatibles de Citrix Receiver

Para facilitar el mantenimiento y para garantizar un rendimiento óptimo, Citrix recomienda actualizar a la versión más reciente de Citrix Receiver que esté disponible. Las versiones más recientes pueden descargarse desde https://www.citrix.com/downloads/citrix-receiver.html. Para mayor comodidad, considere la posibilidad de suscribirse al Feed RSS de Citrix Receiver para recibir una notificación cuando una nueva versión de Citrix Receiver esté disponible.

Tenga en cuenta que Citrix Receiver no da derecho a ventajas de XenApp y XenDesktop LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice a una versión más reciente de Citrix Receiver en sus entornos 7.15 LTSR CU1. En el caso de Citrix Receiver para Windows, Citrix ha anunciado un programa LTSR especial. Encontrará más información acerca de este programa en la página Lifecycle Milestones for Citrix Receiver.

Específicamente, 7.15 LTSR CU1 admite las siguientes versiones de Citrix Receiver y todas las versiones posteriores.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LTSR Compatible Version of Citrix Receiver	Version
Citrix Receiver para Android	3.12.3 o versiones posteriores
Citrix Receiver para Chrome	2.5.2 o versiones posteriores
Citrix Receiver para HTML5	2.5.2 o versiones posteriores
Citrix Receiver para iOS	7.3.1 o versiones posteriores
Citrix Receiver para Linux	13.7 o versiones posteriores
Citrix Receiver para Mac	12.7 o versiones posteriores
Citrix Receiver para UWP (Plataforma universal de Windows)	1.0.5 o versiones posteriores
Citrix Receiver para Windows	4.9 o una versión posterior

Exclusiones notables de XenApp y XenDesktop 7.15 LTSR

Las siguientes características, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 7.15 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y características excluidos estarán disponibles a través de las versiones publicadas regularmente.

Excluded Features
Framehawk
Integración de StoreFront con Citrix Online

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Excluded Components
Personal vDisk: • Excluido para máquinas Windows 10. • Para máquinas con Windows 7, hay respaldo limitado de LTSR hasta el 14 de enero de 2020 (requisitos de CU aplicables)
AppDisks

Excluded Windows Platforms *
Windows 2008 de 32 bits (para Universal Print Server)

* Citrix se reserva el derecho a actualizar el respaldo para plataformas basándose en los hitos de ciclo de vida de proveedores externos.

Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes. Para obtener más información, consulte http://more.citrix.com/XD-INSTALLER.

Migración de XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficiente y rápida desde una comunidad XenApp 6.5 a un sitio que ejecuta XenApp 7.15 LTSR CU1. Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de XenApp 7.15 LTSR CU1 y crear un sitio, siga estos pasos para el proceso de migración:

- Ejecute el instalador de XenApp 7.15 CU1 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de XenApp 7.15 LTSR CU1 por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell al nuevo Controller de XenApp 7.15 CU1, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para obtener más información, consulte Migración de XenApp 6.x.

Lista de correcciones presentes en 7.6 LTSR CU5 pero no incluidas en 7.15 LTSR CU1

Si está considerando la posibilidad de llevar a cabo esta actualización desde 7.6 LTSR CU5 a 7.15 LTSR CU1, tenga en cuenta que hay un pequeño subconjunto de correcciones que se incluyen en 7.6 LTSR CU5 pero no están presentes en 7.15 LTSR CU1. Si su implementación tiene dependencias en correcciones específicas incluidas en 7.6 LTSR CU5, Citrix recomienda que revise esta lista antes de realizar la actualización.

LC6311
LC6985
LC7430
LC7450
LC7574
LC7600
LC7777
LC7911
LC8046
LC8080
LC8130
LC8170
LC8281
LC8339
LC8492
LC8732
LC8750
LC8774

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resueltos

Apr 18, 2018

XenApp y XenDesktop 7.15 LTSR Cumulative Update 1 (CU1) soluciona más de 80 problemas notificados desde la publicación inicial de la versión 7.15 LTSR:

Citrix Director

- Cuando abre la consola de Director y busca usuarios por primera vez, la barra de carga no aparece. En las búsquedas siguientes, la barra aparece según lo previsto. [#LC8190]

Directiva de Citrix

- Pueden fallar los intentos de agregar una nueva regla de redirección de USB a una directiva de usuario en Active Directory. El problema ocurre cuando la barra de desplazamiento no está disponible. [#LC8112]
- Si intenta administrar la directiva "Asignaciones de impresoras", pueden darse los siguientes problemas:
  - Se produce la excepción "InvalidCastException" al agregar o modificar la directiva "Asignaciones de impresoras".
  - Se produce la excepción "InvalidOperationException" al agregar una nueva impresora de sesión.
  - Se produce un error cuando intenta eliminar una impresora de sesión que hubiera en la directiva "Asignaciones de impresoras". Este problema ocurre cuando la opción "Quitar" está inhabilitada.
  - Cuando deja de teclear en el cuadro de búsqueda de la directiva "Asignaciones de impresoras", no se inicia la acción de búsqueda.
  - Las casillas para anular las opciones de la impresora de sesión (PrintQuality, PaperSize, Scale y TrueTypeOption) siempre se marcan, incluso aunque las haya desmarcado antes. [#LC8146]

Citrix Studio

- Cuando intenta agregar máquinas asignadas a un grupo de entrega, pueden aparecer máquinas sin asignar en la página "Asignación de máquinas". [#LC6755]
- Si intenta acceder a catálogos de máquinas en Citrix Studio, puede que Citrix Studio se cierre inesperadamente y aparezca la siguiente excepción:

  "ID de error: XDDS:ABB14FD9". [#LC7961]
- El texto de la opción "Almacenamiento local en el hipervisor" en el asistente "Agregar conexión y recursos" que se ejecuta en una versión no inglesa del sistema operativo Windows puede verse truncado. [#LC8041]
- Después de actualizar Citrix Studio a la versión 7.14.1, la columna "Utilizado por" (que hace referencia al grupo de entrega que utiliza la aplicación) para los paquetes de App-V existentes pueden aparecer en blanco. [#LC8075]
- Si hace clic en el hipervínculo del grupo de entrega en Citrix Studio, puede que no se le redirija al nodo "Grupos de entrega" seleccionado. [#LC8095]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si intenta administrar la directiva "Asignaciones de impresoras", pueden darse los siguientes problemas:
  - Se produce la excepción "InvalidCastException" al agregar o modificar la directiva "Asignaciones de impresoras".
  - Se produce la excepción "InvalidOperationException" al agregar una nueva impresora de sesión.
  - Se produce un error cuando intenta eliminar una impresora de sesión que hubiera en la directiva "Asignaciones de impresoras". Este problema ocurre cuando la opción "Quitar" está inhabilitada.
  - Cuando deja de teclear en el cuadro de búsqueda de la directiva "Asignaciones de impresoras", no se inicia la acción de búsqueda.
  - Las casillas para anular las opciones de la impresora de sesión (PrintQuality, PaperSize, Scale y TrueTypeOption) siempre se marcan, incluso aunque las haya desmarcado antes. [#LC8146]
- Después de actualizar el Delivery Controller a la versión 7.15, Citrix Studio no se puede iniciar en el Delivery Controller y aparece el siguiente mensaje de error:

  "MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand"
  [#LC8396]

- Cuando selecciona el nodo "Grupos de entrega" en Citrix Studio y luego selecciona la ficha "Aplicación", el hipervínculo de la ficha "Aplicación" no funciona. [#LC8555]

Controller

- Si un grupo de entrega contiene uno o varios VDA en modo de mantenimiento, es posible que no pueda seleccionar el grupo de entrega para iniciar aplicaciones publicadas. [#LC6943]
- Después de actualizar un catálogo de máquinas creado con Machine Creation Services (MCS), las máquinas virtuales alojadas en vSAN 6 o versiones posteriores pueden no iniciarse. Aparece un mensaje de error de este tipo en la consola de VMware:

  "Se ha producido un error general del sistema: Se ha producido el error PBM durante PreProcessReconfigureSpec: pbm.fault.PBMFault; Error al intentar ejecutar la validación del aprovisionamiento previo; Entidad no válida". [#LC7860]

- Si intenta acceder a catálogos de máquinas en Citrix Studio, puede que Citrix Studio se cierre inesperadamente y aparezca la siguiente excepción:

  "ID de error: XDDS:ABB14FD9". [#LC7961]

- Citrix Director puede mostrar una cantidad incorrecta de sesiones desconectadas al principio de cada hora. [#LC8006]
- La directiva "AllowRestart" para las sesiones en SO de servidor no permite cerrar la sesión en las sesiones desconectadas. Cuando reinicia una sesión desconectada, la sesión se reconecta a la sesión previa, en lugar de iniciar una nueva. [#LC8090]
- Si intenta administrar la directiva "Asignaciones de impresoras", pueden darse los siguientes problemas:
  - Se produce la excepción "InvalidCastException" al agregar o modificar la directiva "Asignaciones de impresoras".
  - Se produce la excepción "InvalidOperationException" al agregar una nueva impresora de sesión.
  - Se produce un error cuando intenta eliminar una impresora de sesión que hubiera en la directiva "Asignaciones de impresoras". Este problema ocurre cuando la opción "Quitar" está inhabilitada.
  - Cuando deja de teclear en el cuadro de búsqueda de la directiva "Asignaciones de impresoras", no se inicia la acción de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

búsqueda.
  - Las casillas para anular las opciones de la impresora de sesión (PrintQuality, PaperSize, Scale y TrueTypeOption) siempre se marcan, incluso aunque las haya desmarcado antes. [#LC8146]
- El servicio de supervisión (Monitoring Service) no puede insertar los datos de sesiones nuevas en la base de datos de supervisión. [#LC8191]
- El panel "Duración de inicio de sesión por sesión de usuario" en **Director** > **Tendencias** > **Rendimiento de inicio de sesión** puede mostrar solo registros parciales de inicios de sesión. [#LC8265]
- Después de actualizar el Delivery Controller a la versión 7.15, Citrix Studio no se puede iniciar en el Delivery Controller y aparece el siguiente mensaje de error:

  "MissingMandatoryParameter,Citrix.Licensing.Admin.SDK.Commands.GetLicAlertsCommand"
  [#LC8396]
- En un entorno grande de XenApp y XenDesktop, el procedimiento guardado para limpiar la base de datos de supervisión no funcionan correctamente si el tamaño de esa base de datos es grande. [#LC8770]

Redirección de Flash de HDX MediaStream

- Con la Redirección de Flash de HDX MediaStream habilitada, los vídeos de Flash no se reproducen en MSN.com ni News.com. [#LC6823]

Linux VDA

- Un Linux VDA puede registrarse en el Delivery Controller y cancelar el registro más adelante. [#LC8205]
- Algunas aplicaciones de terceros que se utilizan para consultar la pantalla de una sesión en Linux VDA no muestran todos los píxeles. [#LC8419]
- Cuando hay varios servidores LDAP, pueden fallar los intentos de iniciar una aplicación en un Linux VDA después de que se actualicen las directivas y se agote el tiempo de espera de la sesión. [#LC8444]

Profile Management

- Profile Management puede provocar que aparezca una pantalla en negro cuando intenta iniciar una sesión de Microsoft Windows 10. Con esta corrección, debe configurar la directiva "Directorios para sincronizar" y agregar la carpeta "*AppData\Local\Microsoft\Windows\Caches*". [#LC7596]
- Cuando se cierra la sesión de un VDA que se ejecuta en Microsoft Windows 10, el archivo ntuser.dat puede estar en uso y no copiarse al almacén de Profile Management. Como resultado, los cambios realizados en la clave de Registro "HKEY_CURRENT_USER" se pierden. [#LC8068]
- Con la directiva "Eliminar perfiles guardados en caché local al cerrar la sesión" habilitada y la "Demora antes de eliminar perfiles en caché" establecida en dos minutos, cuando se intenta cerrar la sesión e iniciarla en el periodo de dos minutos utilizando la misma cuenta de usuario, se podría crear un nuevo perfil local. [#LC8388]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Provisioning Services

StoreFront

- Con "TWIMode" establecido en "Desactivado" solo para algunas aplicaciones, todas las aplicaciones se inician en modo de ventana cuando se usa Citrix Receiver para Chrome. [#LC7558]
- Cuando hay dos o más tiendas en StoreFront, al hacer clic en "Configurar parámetros de acceso remoto" en la primera o segunda tienda, puede duplicarse el nombre de esa tienda en la tienda agregada más recientemente. [#LC8089]
- Al configurar tiendas con la autenticación compartida en StoreFront, los intentos de vincular un nuevo dispositivo de NetScaler Gateway a una tienda pueden hacer que se quiten los dispositivos existentes de NetScaler Gateway que ya estaban vinculados. Cuando se intenta iniciar sesión en las tiendas, aparece un mensaje de error similar al siguiente:

  "Su inicio de sesión ha caducado. Inicie una sesión de nuevo para continuar.

  Además, la consola de StoreFront muestra nombres de tiendas duplicados. [#LC8219]
- Al importar una tienda con configuración HTML5 utilizando el comando de PowerShell "Import-STFConfiguration", la importación puede completarse correctamente. Sin embargo, a veces no se puede lanzar una aplicación con Citrix Receiver para HTML5. [#LC8290]
- El servidor StoreFront puede mostrar entradas nulas para los sitios de Receiver para Web en la consola. El problema ocurre cuando el nombre de la tienda empieza con el texto "discovery" en la dirección URL. [#LC8320]
- Con el servicio de captura de registros de W3C habilitado, pueden fallar los intentos de hacer cambios en la configuración de StoreFront y aparece este mensaje de error:

  "Ocurrió un error al guardar los cambios". [#LC8370]
- Con la agrupación de sockets habilitada y la conectividad de la base de datos del sitio en estado inconsistente, los sockets de StoreFront pueden agotarse cuando se inicia y se cierra sesión continuamente. [#LC8514]

VDA para SO de escritorio

Redirección de Flash de HDX MediaStream

- Con la Redirección de Flash de HDX MediaStream habilitada, los vídeos de Flash no se reproducen en MSN.com ni News.com. [#LC6823]
- Si intenta guardar archivos de Microsoft Office (como hojas de cálculo de Microsoft Excel que se ejecutan en una sesión con las aplicaciones HDX integradas habilitadas), puede que los archivos se cierren inesperadamente. [#LC8572]

HDX Plug and Play

- Los dispositivos USB que indican el mismo número de serie para más de un dispositivo (como Syn-Tech ProKee V2) no se redirigen a una sesión de VDA. Aparece el siguiente rastreo CDF:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

"No se pudo asignar el ID de la instancia, error 0xc000000d". [#LC8264]

Impresión

- No se puede iniciar una aplicación publicada cuando esa aplicación espera un objeto mutex en el servicio Citrix Print Manager (cpsvc.exe). [#LC6829]
- El servicio Citrix Print Manager (cpsvc.exe) puede cerrarse de forma intermitente. [#LC7535]
- Cuando una sesión se mueve entre varios clientes, no se pueden eliminar las impresoras de sesión. Por ejemplo, si configura la impresora A para el cliente A y la impresora B para el cliente B en la directiva "Asignaciones de impresoras", la impresora A no se elimina cuando la sesión pasa del cliente A al cliente B. [#LC8077]

Administración de servidores/sitios

- En un VDA 7.12 o posterior, cuando intenta evitar que aparezca la barra de idiomas en una sesión integrada y, para ello, establece el marcador integrado en "0x00040000" (inhabilita al agente de la barra de idiomas) en la clave de Registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI, el idioma ya no se oculta. [#LC8349]

Sesión/Conexión

- Con el "Acceso a aplicaciones locales" habilitado, cuando se usa la directiva interactiva de renuncia de responsabilidad de inicio de sesión, puede aparecer una pantalla gris o negra durante 45 segundos. [#LC6518]
- El usuario no puede volver a conectarse a una aplicación. El problema ocurre cuando una de las aplicaciones desconectadas dejó de responder cuando la sesión se desconectó en su momento. [#LC6550]
- Cuando una sesión de varios monitores se bloquea mediante HDX 3D Pro, solo se bloquea el monitor principal. [#LC7767]
- Al establecer una videollamada de Skype Empresarial, puede aparecer un borde de ventana azul después de que la ventana se cruce con la ventana de una aplicación de terceros. [#LC7773]
- Con el "Acceso a aplicaciones locales" habilitado, cuando se usa la directiva interactiva de renuncia de responsabilidad de inicio de sesión, puede aparecer una pantalla gris o negra. [#LC7798]
- Algunas aplicaciones publicadas no cubren toda la pantalla cuando se maximizan. [#LC7854]
- Cuando se realiza una operación de inserción entre dos hojas de cálculo de Microsoft Excel 2010 que se ejecutan en un VDA 7.9, la ventana de Excel puede dejar de responder. [#LC7912]
- En algunos casos, las aplicaciones integradas no aparecen en el modo integrado o algunas funciones no funcionan. [#LC8030]
- En un VDA, con HDX 3D Pro habilitado y la directiva "Message text for users attempting to log on" (Texto del mensaje para usuarios que intentan iniciar sesión) habilitada cuando aparece la pantalla de inicio de sesión, el escritorio publicado no se inicia y aparece una pantalla gris.

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\BitmapRemotingConfig
  Nombre: HKLM_DisableMontereyFBCOnInit
  Valor: DWORD
  Tipo: 1 para habilitar. [#LC8082]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Con el "Acceso a aplicaciones locales" habilitado, cuando se usa la directiva interactiva de renuncia de responsabilidad de inicio de sesión, el visor de escritorio muestra una pantalla gris al conectarse a un VDA. [#LC8136]
- Al usar aplicaciones que usan una cámara Web redirigida (como Skype Empresarial o el reproductor multimedia VLC), la cámara Web puede redirigirse y detectarse durante el primer inicio de sesión. No obstante, cuando se reconecta a la sesión del usuario, la cámara Web ya no se detecta. Aparece una pantalla gris en lugar de la vista previa del vídeo. [#LC8588]

Tarjetas inteligentes

- Cuando inicia una sesión utilizando una tarjeta inteligente, la sesión puede dejar de responder hasta que se desconecte de ella y vuelva a conectarse a ella. [#LC8036]

Excepciones del sistema

- El proceso wfshell.exe puede cerrarse inesperadamente mientras apunta al módulo de agrupación de la barra de tareas. [#LC6968]
- Con la directiva de redirección de USB habilitada, los agentes VDA pueden sufrir una excepción irrecuperable y mostrar una pantalla azul con el código de comprobación de errores SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [#LC7999]
- Los VDA pueden experimentar una excepción irrecuperable con el código de comprobación de errores 0x7E y mostrar una pantalla azul. El problema ocurre cuando se deja la sesión de VDA inactiva durante algún tiempo. [#LC8045]
- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picavc.sys con el código de comprobación de errores SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [#LC8063]

Experiencia de usuario

- Al volver a conectarse a una sesión de aplicaciones integradas, las ventanas de las aplicaciones no aparecen correctamente en el lado del cliente. En vez de ello, los gráficos de la sesión se generan dentro de un rectángulo pequeño en el lado del cliente. [#LC7857]
- El Reproductor de Windows Media muestra verticalmente los archivos AVI de Microsoft. [#LC8308]
- Cuando una aplicación publicada se maximiza en la pantalla de un tercer monitor, es posible que la aplicación no cubra toda la pantalla. En vez de ello, aparece un borde negro. [#LC8472]
- Las aplicaciones integradas que se alojan en el VDA 7.15 pueden mostrar un marco gris o negro cuando estén en segundo plano y se mueva la ventana de la aplicación. [#LC8551]

Interfaz de usuario

- En Excel 2010, si abre una hoja de cálculo que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC7557]

VDA para SO de servidor

Redirección de Flash de HDX MediaStream

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si intenta guardar archivos de Microsoft Office (como hojas de cálculo de Microsoft Excel que se ejecutan en una sesión con las aplicaciones HDX integradas habilitadas), puede que los archivos se cierren inesperadamente. [#LC8572]

HDX Plug and Play

- Los dispositivos USB que indican el mismo número de serie para más de un dispositivo (como Syn-Tech ProKee V2) no se redirigen a una sesión de VDA. Aparece el siguiente rastreo CDF:

  "No se pudo asignar el ID de la instancia, error 0xc000000d". [#LC8264]

Impresión

- No se puede iniciar una aplicación publicada cuando esa aplicación espera un objeto mutex en el servicio Citrix Print Manager (cpsvc.exe). [#LC6829]
- El servicio Citrix Print Manager (cpsvc.exe) puede cerrarse de forma intermitente. [#LC7535]
- Cuando una sesión se mueve entre varios clientes, no se pueden eliminar las impresoras de sesión. Por ejemplo, si configura la impresora A para el cliente A y la impresora B para el cliente B en la directiva "Asignaciones de impresoras", la impresora A no se elimina cuando la sesión pasa del cliente A al cliente B. [#LC8077]

Administración de servidores/sitios

- En un VDA 7.12 o posterior, cuando intenta evitar que aparezca la barra de idiomas en una sesión integrada y, para ello, establece el marcador integrado en "0x00040000" (inhabilita al agente de la barra de idiomas) en la clave de Registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI, el idioma ya no se oculta. [#LC8349]

Sesión/Conexión

- El usuario no puede volver a conectarse a una aplicación. El problema ocurre cuando una de las aplicaciones desconectadas dejó de responder cuando la sesión se desconectó en su momento. [#LC6550]
- Si hace clic en "Cancelar" en la barra de progreso de un inicio de sesión, se conserva una información incorrecta de la sesión en el Delivery Controller. En consecuencia, no se crea la sesión real en el VDA y puede que no pueda iniciar una nueva sesión más adelante. [#LC6779]
- En una sesión de usuario, el micrófono se redirige de forma intermitente incluso después de establecer en "Prohibida" la directiva "Redirección de micrófonos del cliente".

  Esta solución se ocupa de este problema. Sin embargo, si el problema persiste, aplique la siguiente clave del Registro en el dispositivo que tiene el micrófono:

  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    Nombre: MaxPolicyAge
    Tipo: DWORD
    Valor: Tiempo máximo permitido (en segundos) entre la última evaluación de la directiva y la hora de activación del punto final. De forma predeterminada, es de 30 segundos.
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig
    Nombre: PolicyTimeout
    Tipo: DWORD
    Valor: Tiempo máximo (en milisegundos) que el sistema espera a las directivas después de determinar que las directivas no están actualizadas. De forma predeterminada, es de 4000 milisegundos. Cuando se agota el tiempo de espera, el

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

sistema lee las directivas y continúa con la inicialización. Establecer este valor en 0 omite la comprobación de las directivas de Active Directory y procesa las directivas de inmediato. [#LC7495]

- Al establecer una videollamada de Skype Empresarial, puede aparecer un borde de ventana azul después de que la ventana se cruce con la ventana de una aplicación de terceros. [#LC7773]
- Algunas aplicaciones publicadas no cubren toda la pantalla cuando se maximizan. [#LC7854]
- Cuando se usa una vGPU, después de actualizar a las versiones 7.13, 7.14 o 7.15 de VDA, aparece una zona en negro en las aplicaciones o los escritorios publicados que se ejecutan en el sistema operativo Microsoft Windows Server. [#LC7875]
- Cuando se realiza una operación de inserción entre dos hojas de cálculo de Microsoft Excel 2010 que se ejecutan en un VDA 7.9, la ventana de Excel puede dejar de responder. [#LC7912]
- En algunos casos, las aplicaciones integradas no aparecen en el modo integrado o algunas funciones no funcionan. [#LC8030]
- Con el "Acceso a aplicaciones locales" habilitado, cuando se usa la directiva interactiva de renuncia de responsabilidad de inicio de sesión, el visor de escritorio muestra una pantalla gris al conectarse a un VDA. [#LC8136]
- Los VDA para SO de servidor pueden registrarse de forma intermitente cuando se envía una notificación "sin servicio" a los Delivery Controllers. [#LC8228]
- Al usar aplicaciones que usan una cámara Web redirigida (como Skype Empresarial o el reproductor multimedia VLC), la cámara Web puede redirigirse y detectarse durante el primer inicio de sesión. No obstante, cuando se reconecta a la sesión del usuario, la cámara Web ya no se detecta. Aparece una pantalla gris en lugar de la vista previa del vídeo. [#LC8588]

Tarjetas inteligentes

- Cuando inicia una sesión utilizando una tarjeta inteligente, la sesión puede dejar de responder hasta que se desconecte de ella y vuelva a conectarse a ella. [#LC8036]

Excepciones del sistema

- El proceso wfshell.exe puede cerrarse inesperadamente mientras apunta al módulo de agrupación de la barra de tareas. [#LC6968]
- Windows Shell Experience Host puede cerrarse inesperadamente al hacer clic en el control de volumen en la barra de tareas. [#LC7000]
- Es posible que el proceso Service Host (svchost.exe) sufra una infracción de acceso y se cierre de forma inesperada. El problema ocurre por un error en el módulo icaendpoint.dll. [#LC7900]
- Con la directiva de redirección de USB habilitada, los agentes VDA pueden sufrir una excepción irrecuperable y mostrar una pantalla azul con el código de comprobación de errores SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [#LC7999]
- Los servidores pueden experimentar una excepción irrecuperable y mostrar una pantalla azul en picavc.sys con el código de comprobación de errores SYSTEM_THREAD_EXCEPTION_NOT_HANDLED (7e). [#LC8063]

Experiencia de usuario

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Al volver a conectarse a una sesión de aplicaciones integradas, las ventanas de las aplicaciones no aparecen correctamente en el lado del cliente. En vez de ello, los gráficos de la sesión se generan dentro de un rectángulo pequeño en el lado del cliente. [#LC7857]
- El Reproductor de Windows Media muestra verticalmente los archivos AVI de Microsoft. [#LC8308]
- Cuando una aplicación publicada se maximiza en la pantalla de un tercer monitor, es posible que la aplicación no cubra toda la pantalla. En vez de ello, aparece un borde negro. [#LC8472]
- Las aplicaciones integradas que se alojan en el VDA 7.15 pueden mostrar un marco gris o negro cuando estén en segundo plano y se mueva la ventana de la aplicación. [#LC8551]

Interfaz de usuario

- Al usar la Central de conexiones para cerrar una sesión integrada con datos sin guardar, aparece una ventana en negro con el siguiente mensaje:

  "Todavía deben cerrarse programas" con estas dos opciones: "Forzar cierre de sesión" y "Cancelar". La opción "Cancelar" no funciona.

  Después de instalar esta corrección, la opción "Cancelar" funciona como es debido. [#LC6075]
- En Excel 2010, si abre una hoja de cálculo que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC7557]
- La pantalla de cierre de sesión puede no aparecer cuando intenta cerrar la sesión en un escritorio Microsoft Windows Server 2008 R2. Podrá cerrar la sesión, pero ésta aparecerá como si se hubiera desconectado inesperadamente. [#LC8016]

Componentes de escritorio virtual: Otros

- Citrix Director puede mostrar una cantidad incorrecta de sesiones desconectadas al principio de cada hora. [#LC8006]
- El servicio de supervisión (Monitoring Service) no puede insertar los datos de sesiones nuevas en la base de datos de supervisión. [#LC8191]
- El panel "Duración de inicio de sesión por sesión de usuario" en **Director** > **Tendencias** > **Rendimiento de inicio de sesión** puede mostrar solo registros parciales de inicios de sesión. [#LC8265]
- El cliente System Center Configuration Manager (SCCM) puede cerrarse inesperadamente después de actualizar Microsoft Windows 10 de la compilación 1511 a la compilación 1703 con un VDA instalado en él. [#LC8632]
- En Microsoft Windows 10, el rearme de Microsoft Office 2016 podría fallar si usa Machine Creation Services (MCS). [#LC8680]
- En un entorno grande de XenApp y XenDesktop, el procedimiento guardado para limpiar la base de datos de supervisión no funcionan correctamente si el tamaño de esa base de datos es grande. [#LC8770]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR (versión inicial)

Apr 18, 2018

Acerca de esta versión

XenApp y XenDesktop 7.15 Long Term Service Release (LTSR) incluye nuevas versiones de los agentes VDA para Windows y nuevas versiones de varios componentes principales de XenApp y XenDesktop. Puede:

- **Instalar o actualizar un sitio de XenApp o XenDesktop**

  Use el archivo ISO de esta versión para instalar o actualizar todos los VDA y los componentes principales. Instalar o actualizar a la última versión le permite utilizar todas las características más recientes.

- **Instalar o actualizar los VDA de un sitio existente**

  Si tiene una implementación de XenApp o XenDesktop pero aún no está listo para actualizar los componentes principales, sí que puede usar varias de las funciones de HDX más recientes actualizando los VDA con la versión nueva. A menudo, puede interesarle actualizar solo los agentes VDA para probar mejoras en un entorno independiente del entorno de producción.

Para obtener instrucciones, consulte el artículo Antes de la instalación o Actualización de una implementación.

En las páginas de descarga de XenApp y XenDesktop de esta versión, también se incluyen las versiones actualizadas del siguiente software. Para obtener más información sobre las funciones y las instrucciones de instalación, consulte la documentación del componente.

StoreFront

AppDNA

Citrix SCOM Management Pack para XenApp y XenDesktop

Para obtener información general sobre las funciones que se han agregado desde XenApp y XenDesktop 7.6 LTSR, consulte https://www.citrix.com/content/dam/citrix/en_us/documents/data-sheet/xenapp-xendesktop-715-ltsr-feature-summary-comparison-to-76-ltsr.pdf.

La versión del producto también incluye las siguientes características nuevas, modificadas y mejoradas desde XenApp y XenDesktop 7.14.1.

Instalación de VDA en las máquinas sin Microsoft Media Foundation

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

Actualización de un servidor de trabajo XenApp 6.5 a un nuevo VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Después de migrar una comunidad de XenApp 6.5, puede actualizar un servidor de trabajo XenApp 6.5 a un nuevo VDA. Antes, ejecutar el programa de instalación de XenApp y XenDesktop en el servidor de trabajo quitaba automáticamente el software de XenApp 6.5 e instalaba el nuevo VDA. Ahora, primero debe quitar HRP7 y el software de XenApp 6.5 del servidor, siguiendo procesos independientes. A continuación, debe instalar el nuevo VDA. Para obtener información, consulte Actualización de un servidor de trabajo XenApp 6.5 a un nuevo VDA.

Respaldo de Machine Creation Services para las VM de 2ª generación

Cuando use Microsoft System Center Virtual Machine Manager para proporcionar máquinas virtuales, ahora puede usar Machine Creation Services (MCS) para aprovisionar máquinas virtuales de 2ª generación.

Caché de host local

Durante una nueva instalación de XenApp y XenDesktop, la caché de host local está habilitada de forma predeterminada. En cambio, la función de concesión de conexiones está inhabilitada de forma predeterminada.

Después de una actualización, no se modifica la configuración de la caché de host local. Por ejemplo, si la caché de host local estaba habilitada en la versión anterior, permanece habilitada en la versión actualizada. En cambio, si la caché de host local estaba inhabilitada (o no se admitía) en la versión anterior, permanece inhabilitada en la versión actualizada.

Director

Supervisión de fallos de aplicaciones. Director amplía la vista Tendencias porque incluye la ficha **Fallos y errores de aplicación**. En esta ficha, puede ver fallos históricos asociados a las aplicaciones publicadas. Puede ver los fallos y los errores que se han producido al iniciar o ejecutar una aplicación o un proceso seleccionados durante el período de tiempo que haya elegido. Esta información permite entender y solucionar problemas específicos de la aplicación.Para obtener más información, consulte Supervisión de fallos históricos de aplicaciones en "Solución de problemas de aplicaciones".

De forma predeterminada, se supervisan 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 la supervisión de fallos de aplicación en "Configuraciones de directiva de Supervisión".

Esta función requiere agentes VDA y Delivery Controller 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.

Agentes Virtual Delivery Agent (VDA) 7.15

Después de actualizar los agentes VDA desde 7.9, 7.11, 7.12, 7.13 o 7.14, no es necesario actualizar el nivel funcional del catálogo de máquinas. El nivel funcional predeterminado, es decir "7.9 o posterior (...)", sigue siendo el nivel funcional más reciente. Para obtener más información, consulte Niveles funcionales y versiones de VDA.

Grabación de sesiones 7.15

Equilibrio de carga para la Grabación de sesiones. Esta función experimental, presente en XenApp y XenDesktop 7.14, no se incluye en esta versión.

Nuevas implementaciones

© 1999-2017 Citrix Systems, Inc. All rights reserved.

¿Cómo implemento 7.15 LTSR desde cero?

Puede configurar un entorno totalmente nuevo de XenApp o XenDesktop mediante el instalador Metainstaller de 7.15 LTSR. * Antes de hacerlo, le recomendamos que se familiarice con el producto:

Consulte la documentación de XenApp y XenDesktop 7.15 Long Term Service Release y lea atentamente las secciones Información técnica general, Instalación y configuración y Seguridad antes de planificar la implementación. Compruebe que la configuración de todos los componentes cumple los requisitos del sistema. Para la implementación, siga las instrucciones indicadas en Instalación y configuración.

* Nota: Provisioning Services y la Grabación de sesiones están disponibles como descargas y archivos de instalación independientes.

Implementaciones existentes

¿Qué actualizo?

XenApp y XenDesktop 7.15 LTSR ofrece actualizaciones de todos los componentes base de 7.6 LTSR. Recuerde: Citrix recomienda actualizar todos los componentes de LTSR de la implementación a 7.15 LTSR. Por ejemplo: Si Provisioning Services forma parte de su implementación LTSR, actualice el componente Provisioning Services. Si Provisioning Services no forma parte de la implementación, no necesita instalarlo ni actualizarlo.

Desde la versión 7.6 LTSR, se ha agregado un metainstalador que permite actualizar los componentes de su entorno LTSR desde una interfaz unificada. Siguiendo las Instrucciones de actualización, use el metainstalador para actualizar los componentes LTSR de la implementación.

Componentes base de XenApp y XenDesktop 7.15 LTSR

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Baseline Component	Version	Notes
VDA para SO de escritorio	7.15	
VDA para SO de servidor	7.15	
Delivery Controller	7.15	
Citrix Studio	7.15	
Citrix Director	7.15	
Experiencia de administración de Directivas de grupo	3.1	
StoreFront	3.12	
Provisioning Services	7.15	
Universal Print Server	7.15	
Grabación de sesiones	7.15	Solo edición Platinum
VDA Linux	7.15	Consulte la documentación de Linux VDA para ver las plataformas respaldadas.
Profile Management	7.15	
Servicio de autenticación federada	7.15	

Componentes compatibles con XenApp y XenDesktop 7.15 LTSR

Se recomienda usar los siguientes componentes en entornos 7.15 LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice estos componentes a una versión más reciente dentro de sus entornos LTSR 7.15:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.15 LTSR Compatible Components and Platforms	Version
AppDNA	7.15
Citrix SCOM Management Pack para License Server	1.2
Citrix SCOM Management Pack para Provisioning Services	1.19
Citrix SCOM Management Pack para StoreFront	1.12
Citrix SCOM Management Pack para XenApp y XenDesktop	3.13
HDX RealTime Optimization Pack	2.3
Servidor de licencias	11.14.0 compilación 21103
Administración del entorno de espacio de trabajo	4.4
App Layering	4.3
Autoservicio de restablecimiento de contraseñas	1.1

Versiones compatibles de Citrix Receiver

Para facilitar el mantenimiento y para garantizar un rendimiento óptimo, Citrix recomienda actualizar a la versión más reciente de Citrix Receiver que esté disponible. Las versiones más recientes pueden descargarse desde https://www.citrix.com/downloads/citrix-receiver.html. Para mayor comodidad, considere la posibilidad de suscribirse al Feed RSS de Citrix Receiver para recibir una notificación cuando una nueva versión de Citrix Receiver esté disponible.

Tenga en cuenta que Citrix Receiver no da derecho a ventajas de XenApp y XenDesktop LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente). Citrix puede pedirle que actualice a una versión más reciente de Citrix Receiver en sus entornos 7.15 LTSR. En el caso de Citrix Receiver para Windows, Citrix ha anunciado un programa LTSR especial. Encontrará más información acerca de este programa en la página Lifecycle Milestones for Citrix Receiver.

Específicamente, 7.15 LTSR admite las siguientes versiones de Citrix Receiver y todas las versiones posteriores.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LTSR Compatible Version of Citrix Receiver	Version
Citrix Receiver para Android	3.11.1 o una versión posterior
Citrix Receiver para Chrome	2.4 o una versión posterior
Citrix Receiver para HTML5	2.4 o una versión posterior
Citrix Receiver para iOS	7.2 o una versión posterior
Citrix Receiver para Linux	13.5 o una versión posterior
Citrix Receiver para Mac	12.5 o una versión posterior
Citrix Receiver para UWP (Plataforma universal de Windows)	1.0.5 o versiones posteriores
Citrix Receiver para Windows	4.9 o una versión posterior

Exclusiones notables de XenApp y XenDesktop 7.15 LTSR

Las siguientes características, componentes y plataformas no dan derecho a las ventajas y prestaciones del ciclo de vida de 7.15 LTSR. Específicamente, se excluyen las ventajas de actualizaciones acumulativas y el ciclo de vida ampliado. Las actualizaciones de los componentes y características excluidos estarán disponibles a través de las versiones publicadas regularmente.

Excluded Features
Framehawk
Integración de StoreFront con Citrix Online

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Excluded Components
Personal vDisk: • Excluido para máquinas Windows 10. • Para máquinas con Windows 7, hay respaldo limitado de LTSR hasta el 14 de enero de 2020 (requisitos de CU aplicables)
AppDisks

Excluded Windows Platforms *
Windows 2008 de 32 bits (para Universal Print Server)

* Citrix se reserva el derecho a actualizar el respaldo para plataformas basándose en los hitos de ciclo de vida de proveedores externos.

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes. Para obtener más información, consulte http://more.citrix.com/XD-INSTALLER.

Migración de XenApp 6.5

El proceso de migración de XenApp 6.5 permite realizar una transición eficiente y rápida desde una comunidad XenApp 6.5 a un sitio que ejecuta XenApp 7.15 LTSR (u otra versión compatible que sea más reciente). Esta transición puede resultarle útil en caso de implementaciones que contienen una gran cantidad de aplicaciones y directivas de grupo Citrix, porque reduce el riesgo de que se produzcan errores accidentales al mover manualmente las aplicaciones y las directivas de grupo Citrix al nuevo sitio de XenApp.

Después de instalar los componentes principales de XenApp 7.15 LTSR y crear un sitio, el proceso de migración sigue estos pasos:

- Ejecute el instalador de XenApp 7.15 en cada servidor de trabajo de XenApp 6.5. Este instalador actualiza automáticamente el servidor a un nuevo Virtual Delivery Agent para SO de servidor listo para usar en el nuevo sitio.
- Ejecute los cmdlets de exportación de PowerShell en un Controller de XenApp 6.5, que exporta las configuraciones de aplicaciones y directivas Citrix a archivos XML.
- Si fuera necesario, modifique los archivos XML para seleccionar con exactitud lo que quiere importar al sitio nuevo. Al adaptar los archivos, puede importar las configuraciones de directivas y aplicaciones al sitio de XenApp 7.15 LTSR por fases: algunas configuraciones ahora y otras más tarde.
- Ejecute los cmdlets de importación de PowerShell en el nuevo Controller de XenApp 7.15, el cual importa las configuraciones contenidas en los archivos XML al nuevo sitio de XenApp.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para obtener más información, consulte Migración de XenApp 6.x.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resueltos

Apr 18, 2018

Se han solucionado los problemas siguientes desde la versión 7.14.1:

Problemas resueltos en comparación con 7.14.1

Problemas resueltos en comparación con 7.6 LTSR CU4

Problemas resueltos en comparación con 7.14.1

AppDNA

Citrix Director

- Al ir a la ficha **Tendencias** > **Fallos** > **Conexión** en Citrix Director, puede que aparezca este mensaje de error:

  "Error inesperado. Compruebe la conexión de red o consulte los registros de eventos del servidor de Director para obtener más información". [#LC7755]

- No se puede ver información sobre directivas para ciertas sesiones en Citrix Director y aparece el siguiente mensaje de error:

  "No se puede obtener los datos". [#LC8207]

Directiva de Citrix

- Puede que no se apliquen los objetos de directiva de grupo que contienen parámetros de Citrix y Microsoft. Este problema ocurre cuando la unidad de extensión que hay en la lista contiene más de dos GUID. [#LC7533]

Citrix Studio

- Puede que no se agreguen las cuentas de equipo a máquinas de catálogos nuevas o existentes cuando se usa el modo de interfaz gráfica de usuario en lugar de usar los comandos de PowerShell. El problema ocurre cuando la herramienta de búsqueda de directorios no vincula el objeto correcto mientras busca el nombre NetBIOS.

  Por ejemplo, si el nombre de dominio es "xyz.ad.airxyz.aa" y el nombre de NetBIOS es "xyz-Ad", el nombre de NetBIOS se acepta como "xyz" en lugar de "xyz-Ad" cuando se usa el modo de interfaz gráfica de usuario. En consecuencia, la cuenta de máquina no se puede agregar en caso de cuentas de equipo existentes ni nuevas. [#LC6679]

- Después de actualizar Citrix Delivery Controller a la versión 7.12, puede que no se agreguen máquinas de Citrix Provisioning Services (PVS) a un catálogo de máquinas en un entorno con varios dominios. El problema ocurre cuando PVS

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

no devuelve el nombre de dominio junto con el nombre del dispositivo. Cuando Citrix Studio busca el nombre de cuenta en el dominio local, no se encuentra la cuenta. [#LC6818]

- Puede fallar la publicación de aplicaciones App-V. [#LC7421]
- Cuando un administrador intenta agregar una aplicación App-V desde un grupo de aislamiento al grupo de entrega o intenta crear un grupo de aislamiento, es posible que aparezca el siguiente mensaje de error en Citrix Studio:

  "Ocurrió un error desconocido". [#LC7594]
- Puede que no se agreguen máquinas a un grupo de entrega mediante el nombre "NETBIOS" para la asociación de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC7830]

Controller

- Después de actualizar Citrix Delivery Controller a la versión 7.12, puede que no se agreguen máquinas de Citrix Provisioning Services (PVS) a un catálogo de máquinas en un entorno con varios dominios. El problema ocurre cuando PVS no devuelve el nombre de dominio junto con el nombre del dispositivo. Cuando Citrix Studio busca el nombre de cuenta en el dominio local, no se encuentra la cuenta. [#LC6818]
- Cuando se intenta agregar máquinas a un catálogo existente de Machine Creation Services, es posible que el procedimiento no siga el método round robin para almacenamientos múltiples que pueden seleccionarse para aceptar las nuevas máquinas. [#LC7456]
- Es posible que los administradores personalizados no puedan crear un grupo de aislamiento y aparezca el siguiente mensaje de error:

  "No tiene los permisos necesarios para completar esta solicitud. Para obtener más información, póngase en contacto con el administrador del sitio de XenDesktop". [#LC7563]
- Cuando un administrador intenta agregar una aplicación App-V desde un grupo de aislamiento al grupo de entrega o intenta crear un grupo de aislamiento, es posible que aparezca el siguiente mensaje de error en Citrix Studio:

  "Ocurrió un error desconocido". [#LC7594]
- En Citrix Delivery Controller, intentar inhabilitar TLSv1.0 puede provocar pérdida de comunicación con el hipervisor de VMware vCenter. [#LC7686]
- Puede que no se agreguen máquinas a un grupo de entrega mediante el nombre "NETBIOS" para la asociación de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC7830]

HDX RealTime Optimization Pack

Profile Management

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Cuando abre archivos en un perfil con streaming de perfiles habilitado, el archivo puede aparecer vacío después de iniciar sesión. [#LC6996]
- Los servidores pueden experimentar una excepción irrecuperable en upmjit.sys con el código de comprobación de errores 0x135 y mostrar una pantalla azul. [#LC7841]
- UserProfileManager.exe puede cerrarse inesperadamente cuando se inicia sesión en un VDA. [#LC7952]

StoreFront

- Es posible que no pueda volver a conectarse a sesiones desconectadas en una implementación de agrupación multisitio. Por eso, puede recibir una segunda instancia del mismo recurso. [#LC7453]
- Cuando se inhabilita una parte de la fuente de una aplicación agregada, la aplicación puede ocultarse inesperadamente al usuario final. [#LC7675]
- En StoreFront, puede que no se inhabilite la opción de autoservicio de cuentas, incluso aunque la opción aparezca inhabilitada. [#LC7744]
- En StoreFront, si intenta quitar la autenticación compartida de tiendas, puede aparecer el siguiente mensaje de error al guardar los cambios:

  "Ocurrió un error al guardar los cambios.". [#LC8370]

Universal Print Server

Cliente

- El servicio de cola de impresión puede dejar de responder y, como resultado, la impresión universal puede dejar de funcionar. El problema ocurre cuando se agota el tiempo de espera de una respuesta de transacción desde el servicio de cola. [#LC5209]
- Cuando se usa Profile Management, los cambios en las impresoras de Citrix Universal Print Server (agregar, quitar o cambiarles el nombre) realizados en la sesión de un servidor pueden no verse correctamente reflejados en sesiones posteriores en otros servidores. [#LC7645]

Servidor

- Los intentos de imprimir un documento pueden fallar y aparece el siguiente mensaje de error:

  "No se puede imprimir debido a un problema con la impresora seleccionada". [#LC6825]
- Cuando se usan determinadas impresoras, Microsoft Notepad puede mostrar el mensaje "El identificador no es válido" y no imprimir. El problema se da si está configurada la opción "Usar solo los controladores específicos de la impresora" en la directiva de Citrix "Uso de controladores de impresión universal" y si está configurada la opción "Habilitado, sin respaldo de la impresión remota nativa de Windows" en la directiva de Citrix "Habilitar Universal Print Server". [#LC7623]

VDA para SO de escritorio

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación, desinstalación y actualización

- Después de actualizar el VDA desde la versión 5.6.400 a la versión 7.9, reiniciar el VDA puede provocar que los controladores de reflejo instalados por la versión anterior no se desinstalen. [#LC6295]
- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7555]
- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7587]

Impresión

- El servicio Citrix Print Manager (cpsvc.exe) puede dejar de responder y cerrarse de forma inesperada cuando los nuevos usuarios inicien sesión. [#LC6933]
- Después de actualizar el VDA desde la versión 7.9 a la versión 7.12 o posterior, puede que las impresiones desde Microsoft Internet Explorer mediante el controlador de impresora universal de Citrix se dirijan solo a la bandeja 1, en lugar de dirigirse a la bandeja seleccionada. [#LC7463]

Sesión/Conexión

- Cuando se instalan varias cámaras Web del mismo modelo en el VDA para SO de escritorio, puede que la sesión solo reconozca y asigne la cámara Web más reciente. [#LC5008]
- En el VDA para SO de escritorio, puede que el WFAPI SDK no devuelva unidades extraíbles del cliente. [#LC6877]
- No se conserva la posición de las ventanas al reconectarse a una sesión de escritorio publicado cuando se usan varios monitores. [#LC7644]
- Cuando se cambia entre sesiones con varios monitores en modo de pantalla completa con el modo de gráficos antiguo habilitado y sin Desktop Viewer configurado, parece que solo se ejecuta un monitor en la sesión. [#LC7907]

Tarjetas inteligentes

- En ocasiones, quitar una tarjeta inteligente puede no bloquear la sesión del usuario, aunque se haya configurado el bloqueo de la sesión del usuario cuando éste quita la tarjeta inteligente. [#LC7411]

Excepciones del sistema

- Los VDA pueden experimentar una excepción irrecuperable en vd3dk.sys con el código de comprobación de errores 0X00000050 y mostrar una pantalla azul. [#LC6833]
- Los VDA pueden experimentar una excepción irrecuperable en picadm.sys con el código de comprobación de errores 0x7F y mostrar una pantalla azul al apagar una sesión. [#LC7545]
- Es posible que el proceso Service Host (svchost.exe) sufra una infracción de acceso y se cierre de forma inesperada. El problema ocurre por un error en el módulo scardhook64.dll. [#LC7580]
- Los servidores pueden sufrir una excepción irrecuperable en vdtw30.dll con el código de detención 0xc0000006 y mostrar una pantalla azul. [#LC7608]
- Los VDA pueden experimentar una excepción irrecuperable en tdica.sys con un código de comprobación de errores y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

mostrar una pantalla azul. [#LC7632]

- Esta corrección soluciona un problema de memoria con el archivo wdica.sys que puede provocar que los servidores se cierren inesperadamente. [#LC7666]

Experiencia de usuario

- Esta solución mejora el respaldo para los sonidos que se reproducen durante un espacio corto de tiempo al usar sonido de alta calidad.

  Nota:

  - Esta corrección no tiene efecto en las sesiones que se ejecuta en Windows Server 2008 R2.
  - Para que esta corrección funcione, debe usar Citrix Receiver para Windows 4.4 Long Term Service Release (LTSR) CU5 o versiones posteriores y la versión de VDA de XenApp y XenDesktop 7.6 LTSR CU4 o una versión posterior.

  [#LC5842]

- Cuando se realiza una operación de inserción entre dos hojas de cálculo de Microsoft Excel 2010 que se ejecutan en un VDA 7.9, la ventana de Excel puede dejar de responder. [#LC7481]

- En un entorno de varios monitores, defina el monitor externo como "Pantalla principal" de Windows y colóquelo a la derecha del monitor del portátil o tableta secundarios en los parámetros de configuración de pantalla del Panel de Control. Cuando se inicia una aplicación publicada que aparece en el monitor externo y se mueve esta aplicación al monitor de tableta o a un portátil que está conectado al monitor externo, al abrir o cerrar la tapa de la tableta o del portátil la aplicación publicada puede aparecer en negro.

  Para habilitar la corrección, debe establecer la siguiente clave de Registro en el VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire
  Nombre: EnableDrvTw2NotifyMonitorOrigin
  Tipo: REG_DWORD
  Valor: 1 (habilitar) y 0 (inhabilitar; 0 es el valor predeterminado). De forma predeterminada, falta este valor de Registro.

  [#LC7760]

Interfaz de usuario

- Los iconos de accesos directos de URL pueden aparecer vacíos cuando se usa un escritorio con optimización táctil. [#LC6663]

- En Excel 2010, si abre una hoja de cálculo que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC7557]

VDA para SO de servidor

Instalación, desinstalación y actualización

- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7555]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7587]

Impresión

- El servicio Citrix Print Manager (cpsvc.exe) puede dejar de responder y cerrarse de forma inesperada cuando los nuevos usuarios inicien sesión. [#LC6933]
- Después de actualizar el VDA desde la versión 7.9 a la versión 7.12 o posterior, puede que las impresiones desde Microsoft Internet Explorer mediante el controlador de impresora universal de Citrix se dirijan solo a la bandeja 1, en lugar de dirigirse a la bandeja seleccionada. [#LC7463]

Administración de servidores/sitios

- Los usuarios de dominios secundarios pueden ver el siguiente mensaje de error cuando inicien una aplicación a través de la interfaz Web o StoreFront:

  "No tiene permisos para acceder a esta aplicación publicada". [#LC7566]

Sesión/Conexión

- Cuando se instalan varias cámaras Web del mismo modelo en el VDA para SO de escritorio, puede que la sesión solo reconozca y asigne la cámara Web más reciente. [#LC5008]
- Los intentos de volver a conectarse a una sesión pueden fallar de forma intermitente y provocar que los VDA de SO de servidor vayan al estado "Inicializando". El problema ocurre cuando el VDA se registra nuevamente en un Delivery Controller.

  [#LC6647]
- Es posible que se desconecten las sesiones activas en los servidores XenApp cuando el Delivery Controller pierde la conexión. El problema ocurre cuando los VDA no puede realizar un seguimiento correcto del estado de las sesiones que se mueven desde un estado de "preinicio" a un estado "activo". Como resultado, cuando se reinicia el Delivery Controller, éste intenta borrar los recursos de los VDA, y las sesiones en estado de preinicio se desconectan o se cierran mientras las aplicaciones se está utilizando activamente. [#LC6819]
- Cuando se inicia una aplicación publicada en Microsoft Windows Server 2016, aparece una pantalla en negro durante varios segundos antes de que la aplicación se vuelva visible. [#LC7947]

Excepciones del sistema

- Los VDA pueden experimentar una excepción irrecuperable en picadm.sys con el código de comprobación de errores 0x7F y mostrar una pantalla azul al apagar una sesión. [#LC7545]
- Es posible que el proceso Service Host (svchost.exe) sufra una infracción de acceso y se cierre de forma inesperada. El problema ocurre por un error en el módulo scardhook64.dll. [#LC7580]
- Los servidores pueden sufrir una excepción irrecuperable en vdtw30.dll con el código de detención 0xc0000006 y mostrar una pantalla azul. [#LC7608]
- Los VDA pueden experimentar una excepción irrecuperable en tdica.sys con un código de comprobación de errores y mostrar una pantalla azul. [#LC7632]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Esta corrección soluciona un problema de memoria con el archivo wdica.sys que puede provocar que los servidores se cierren inesperadamente. [#LC7666]

Experiencia de usuario

- Esta solución mejora el respaldo para los sonidos que se reproducen durante un espacio corto de tiempo al usar sonido de alta calidad.

  Nota:

  - Esta corrección no tiene efecto en las sesiones que se ejecuta en Windows Server 2008 R2.
  - Para que esta corrección funcione, debe usar Citrix Receiver para Windows 4.4 Long Term Service Release (LTSR) CU5 o versiones posteriores y la versión de VDA de XenApp y XenDesktop 7.6 LTSR CU4 o una versión posterior.

  [#LC5842]

- Cuando se realiza una operación de inserción entre dos hojas de cálculo de Microsoft Excel 2010 que se ejecutan en un VDA 7.9, la ventana de Excel puede dejar de responder. [#LC7481]

- En un entorno de varios monitores, defina el monitor externo como "Pantalla principal" de Windows y colóquelo a la derecha del monitor del portátil o tableta secundarios en los parámetros de configuración de pantalla del Panel de Control. Cuando se inicia una aplicación publicada que aparece en el monitor externo y se mueve esta aplicación al monitor de tableta o a un portátil que está conectado al monitor externo, al abrir o cerrar la tapa de la tableta o del portátil la aplicación publicada puede aparecer en negro.

  Para habilitar la corrección, debe establecer la siguiente clave de Registro en el VDA:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Ica\Thinwire
  Nombre: EnableDrvTw2NotifyMonitorOrigin
  Tipo: REG_DWORD
  Valor: 1 (habilitar) y 0 (inhabilitar; 0 es el valor predeterminado). De forma predeterminada, falta este valor de Registro.

  [#LC7760]

Interfaz de usuario

- Los iconos de accesos directos de URL pueden aparecer vacíos cuando se usa un escritorio con optimización táctil. [#LC6663]

- En Excel 2010, si abre una hoja de cálculo que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC7557]

Componentes de escritorio virtual: Otros

- Puede fallar la publicación de aplicaciones App-V. [#LC7421]

- No se pueden iniciar aplicaciones App-V en el modo Administración única. El problema ocurre cuando el nombre de la aplicación contiene caracteres especiales. [#LC7897]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resueltos en comparación con 7.6 LTSR CU4

Citrix Director

- Citrix Director y la autenticación integrada de Windows (WIA) pueden no funcionar con una configuración de delegación Kerberos limitada. [#LC5196]
- Se produce un error "Sistema no disponible" después de intentar iniciar sesión en Citrix Director. [#LC5385]
- Citrix Director puede no mostrar los detalles de la sesión. El problema ocurre cuando se usa "Contenido publicado" como tipo de aplicación. [#LC6577]

Directiva de Citrix

- El procesamiento de directivas de Citrix puede dejar de responder, lo que hace que las sesiones de usuario dejen de responder. Cuando esto ocurre, no se pueden establecer conexiones con Citrix Receiver ni con Escritorio remoto (RDP). [#LA4969]
- En sistemas que tienen instalada la corrección #LC1987 (GPCSExt170W2K8R2X64006 o su sustituto), puede que no se apliquen las directivas de Active Directory (AD) que contienen parámetros de Citrix y Microsoft a la vez.

  Nota: Esta corrección soluciona el problema para las directivas de Active Directory que se creen después de instalar esta actualización. También lo soluciona para las directivas *existentes* donde los parámetros de Citrix se hayan configurado antes de los parámetros de Microsoft. No soluciona el problema para las directivas existentes de AD donde los parámetros de Microsoft se hayan configurado *antes* de los parámetros de Citrix. Debe abrir esas directivas de AD y guardar los parámetros de Citrix. [#LC2121]
- Con esta mejora de la funcionalidad, el motor de directivas de grupo Citrix genera más mensajes del registro de eventos cuando procesa las directivas de Citrix. [#LC3664]
- Cuando se actualiza desde la versión 7.6 a la versión 7.8 o 7.9, ciertas combinaciones de colores en Citrix Studio pueden aparecer demasiado oscuras para que el texto aparezca correctamente. [#LC5690]
- Después de instalar el Servicio de autenticación federada de Citrix, intentar configurar las **listas de control de acceso de seguridad** en el servidor StoreFront (en **Reglas de usuario**) puede provocar que la ventana de configuración deje de responder. [#LC5788]
- Cuando se abre un archivo con la extensión XLSM que contiene macros, Microsoft Excel puede provocar un pico en el consumo de memoria y CPU. Por eso, no se puede abrir el archivo. [#LC6142]
- Puede que no se apliquen los objetos de directiva de grupo que contienen parámetros de Citrix y Microsoft. Este

© 1999-2017 Citrix Systems, Inc. All rights reserved.

problema ocurre cuando la unidad de extensión que hay en la lista contiene más de dos GUID. [#LC7533]

Citrix Studio

- Si varios usuarios crean directivas en varias sesiones de Studio, la última directiva creada sobrescribe la anterior cuando se actualiza Citrix Studio. [#LA5533]
- Es posible que Citrix Studio no reconozca la licencia de XenDesktop App Edition. En ese caso, aparecerá el siguiente mensaje de error:

  "No se encuentra una licencia válida
  . No hay licencias adecuadas disponibles. Compruebe si la dirección del servidor de licencias, la edición y el modelo del producto son correctos". [#LC0822]
- Al intentar agregar usuarios de varios dominios a un grupo de entrega, Citrix Studio resuelve su dominio real como la cuenta de dominio local. [#LC1886]
- Intentar publicar una aplicación en Citrix Studio 7.7 con argumentos de línea de comandos que contienen comillas (") puede resultar en un mensaje de error. [#LC4525]
- Citrix Studio puede ofrecer la opción de revertir el catálogo aunque no se haya actualizado el catálogo. Revertir provoca una excepción. [#LC4791]
- No se pueden agregar máquinas a un catálogo desde Citrix Studio y aparece un mensaje de error. El problema no ocurre cuando se agregan máquinas mediante el asistente XenDesktop Setup Wizard. [#LC5030]
- Si dos aplicaciones tienen el mismo ApplicationID, actualizar las aplicaciones de App-V puede provocar que Citrix Studio establezca incorrectamente el nombre del paquete de App-V. [#LC5261]
- Cuando un Delivery Controller se desconecta o deja de estar disponible por algún otro motivo, puede que Citrix Studio funcione con lentitud. [#LC5335]
- Después de actualizar XenApp o XenDesktop de 7.6 a 7.7, puede aparecer ocasionalmente una solicitud de actualización en Citrix Studio. [#LC5478]
- Al cerrar y, a continuación, intentar volver a abrir una instancia de la versión 7.9 de Citrix Studio que está configurada con varios servidores App-V que contienen varios paquetes, Studio permanece en un estado de expansión y no se abre. [#LC5643]
- Desde Citrix Studio, solo puede agregar un servidor App-V a un sitio. Para agregar servidores App-V adicionales al sitio, debe utilizar PowerShell. [#LC5767]
- Después de actualizar Citrix Studio de 7.8 a 7.9, las aplicaciones que agregue aparecen sin versión ni nombre de paquete. [#LC5958]
- En Citrix Studio, agregar una aplicación mediante el nodo Aplicaciones puede provocar un error y la aplicación no se agrega. Como solución temporal, use el nodo Grupo de entrega para agregar aplicaciones. [#LC5975]
- Cuando se crea un nuevo sitio de XenDesktop a través de Citrix Studio y se apunta al agente de escucha de AlwaysOn de SQL, puede aparecer el siguiente error: "No se pudo contactar con el servidor réplica .

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Compruebe el estado de la base de datos en el servidor SQL Server. Asegúrese de que el servidor de base de datos permite conexiones remotas y el firewall no está bloqueando las conexiones". [#LC6010]

- En Citrix Studio, si quita un paquete publicado existente de App-V e intenta agregar otra versión del mismo paquete de App-V con el mismo nombre y la misma ubicación de publicación al grupo de entrega, es posible que el paquete aparezca con un signo de exclamación rojo y el siguiente mensaje de error:

  "No se pudo cargar los datos de aplicación para la aplicación 'NOMBRE DE LA APLICACIÓN'". [#LC6254]

- No se puede agregar un Delivery Controller a una configuración de base de datos reflejada mediante la opción para agregar un controlador adicional desde Citrix Studio y el comando de PowerShell "Add-XDController". [#LC6563]

- Puede que no se agreguen las cuentas de equipo a máquinas de catálogos nuevas o existentes cuando se usa el modo de interfaz gráfica de usuario en lugar de usar los comandos de PowerShell. El problema ocurre cuando la herramienta de búsqueda de directorios no vincula el objeto correcto mientras busca el nombre NetBIOS.

  Por ejemplo, si el nombre de dominio es "xyz.ad.airxyz.aa" y el nombre de NetBIOS es "xyz-Ad", el nombre de NetBIOS se acepta como "xyz" en lugar de "xyz-Ad" cuando se usa el modo de interfaz gráfica de usuario. En consecuencia, la cuenta de máquina no se puede agregar en caso de cuentas de equipo existentes ni nuevas. [#LC6679]

- Después de actualizar Citrix Delivery Controller a la versión 7.12, puede que no se agreguen máquinas de Citrix Provisioning Services (PVS) a un catálogo de máquinas en un entorno con varios dominios. El problema ocurre cuando PVS no devuelve el nombre de dominio junto con el nombre del dispositivo. Cuando Citrix Studio busca el nombre de cuenta en el dominio local, no se encuentra la cuenta. [#LC6818]

- Cuando se actualiza un sitio de XenApp, el modelo de licencia podría cambiar inesperadamente de XenApp a XenDesktop. [#LC6981]

- El comando "Start-Transcript" falla para "Get-XDSite" y otros comandos PoSH de alto nivel administrativo de XenDesktop cuando se ejecutan en PowerShell 5. [#LC7006]

- Cuando un administrador intenta agregar una aplicación App-V desde un grupo de aislamiento al grupo de entrega o intenta crear un grupo de aislamiento, es posible que aparezca el siguiente mensaje de error en Citrix Studio:

  "Ocurrió un error desconocido". [#LC7594]

- Puede que no se agreguen máquinas a un grupo de entrega mediante el nombre "NETBIOS" para la asociación de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC7830]

Controller

- Falla la implementación de máquinas virtuales con Machine Creation Services en Citrix Studio. Aparece el mensaje de error:

  "ID de error: XDDS:0F7CB924". [#LC4930]

- Cuando los usuarios intentan eliminar un catálogo de escritorios agrupados creado en XenServer y, a continuación, ejecutan la actualización del catálogo, los discos base no se eliminan del almacenamiento y la cantidad de discos base puede aumentar. [#LC0577]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- La fiabilidad de la sesión no se puede inhabilitar mediante el objeto de directiva de grupo (GPO) de Active Directory o mediante Citrix Studio en sesiones de VDA 7.x que se inician por medio de XenDesktop 5.6 Desktop Delivery Controller (DDC). [#LC0878]
- Al crear una nueva máquina agrupada mediante Machine Creation Services a partir de una imagen maestra con la configuración personalizada VMX y nvram, esa configuración no se copia a las nuevas máquinas virtuales. [#LC0967]
- Puede agotarse el tiempo de espera de la tarea PrepareSession que ejecuta el servicio Broker cuando se usa en entornos de XenDesktop 5.6, lo que hace que StoreFront falle. [#LC1055]
- Esta corrección soluciona un problema de tiempo que puede darse cuando el hipervisor está congestionado mientras da formato a un volumen de disco PvD durante la creación inicial de las máquinas. [#LC3275]
- Puede que falle la creación de máquinas virtuales con Machine Creation Services si usa VMware vSphere 6.0 y el almacenamiento vSAN 6. [#LC4563]
- La respuesta de WaitForTask provoca la excepción VimApi.MissingProperty, que no permite actualizar catálogos de máquinas. [#LC4573]
- No se pueden agregar máquinas a un catálogo desde Citrix Studio y aparece un mensaje de error. El problema no ocurre cuando se agregan máquinas mediante el asistente XenDesktop Setup Wizard. [#LC5030]
- Después de actualizar el VDA a la versión 7.8, no se puede realizar la operación de actualizar inventario y aparece el siguiente mensaje de error:

  "La actualización del inventario falló con un error interno de código 0x2". [#LC5051]
- Pueden aparecer caracteres extraños al final de "Nombre simplificado del servicio" y "Descripción del servicio" de determinados servicios de Citrix instalados en sistemas operativos en japonés. [#LC5208]
- Si dos aplicaciones tienen el mismo ApplicationID, actualizar las aplicaciones de App-V puede provocar que Citrix Studio establezca incorrectamente el nombre del paquete de App-V. [#LC5261]
- Después de actualizar XenApp o XenDesktop de 7.6 a 7.7, puede aparecer ocasionalmente una solicitud de actualización en Citrix Studio. [#LC5478]
- Una y comercial (&) en el título de una aplicación provoca daños en el XML de StoreFront y este deja de mostrar aplicaciones o iconos. [#LC5505]
- Al cerrar y, a continuación, intentar volver a abrir una instancia de la versión 7.9 de Citrix Studio que está configurada con varios servidores App-V que contienen varios paquetes, Studio permanece en un estado de expansión y no se abre. [#LC5643]
- Después de actualizar a XenDesktop 7.9, es posible que el inicio de sesión falle ocasionalmente debido a que el broker de NetScaler no envía correctamente las credenciales. [#LC5753]
- Desde Citrix Studio, solo puede agregar un servidor App-V a un sitio. Para agregar servidores App-V adicionales al sitio, debe utilizar PowerShell. [#LC5767]
- Después de instalar el Servicio de autenticación federada de Citrix, intentar configurar las **listas de control de acceso de seguridad** en el servidor StoreFront (en **Reglas de usuario**) puede provocar que la ventana de configuración deje de responder. [#LC5788]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Cambiar el puerto SDK de los servicios Flexcast Management Architecture (como Analytics, Broker, Log, etc.) hace que Citrix Studio no se conecte correctamente. [#LC6005]
- Cuando se crea un nuevo sitio de XenDesktop a través de Citrix Studio y se apunta al agente de escucha de AlwaysOn de SQL, puede aparecer el siguiente error: "No se pudo contactar con el servidor réplica .

  Compruebe el estado de la base de datos en el servidor SQL Server. Asegúrese de que el servidor de base de datos permite conexiones remotas y el firewall no está bloqueando las conexiones". [#LC6010]
- Citrix Director muestra una cantidad de máquinas no registradas en el panel de mandos que no coincide con los datos del informe de la página Tendencias. [#LC6184]
- El servicio de supervisión (Monitoring Service) no puede insertar los datos de sesiones nuevas en la base de datos de supervisión cuando está habilitada la directiva "Índice de patrón de carga". Esto puede hacer que Citrix Director no muestre información actualizada para sesiones, tales como Duración del inicio de sesión, Número de sesiones activas, etc. A pesar de que el problema aparezca en Citrix Director, se debe a un problema en el Delivery Controller. En la versión actual del Controller se ha solucionado el problema. [#LC6241]
- Quitar una unidad de alojamiento puede provocar que falle la replicación de AppDisks en cualquier otra unidad de alojamiento. En consecuencia, las máquinas del grupo de entrega con AppDisks no pueden iniciarse. [#LC6433]
- Después de reiniciar el servicio de supervisión de Citrix o el Delivery Controller de Citrix, puede aparecer el suceso de ID 1013:

  "Error del mantenimiento inicial de la base de datos con: System.NullReferenceException: Referencia a objeto no establecida como instancia de un objeto".

  El problema se produce cuando se detiene el servicio Monitoring Service de Citrix. [#LC6438]
- Pueden fallar los intentos de utilizar determinadas aplicaciones de terceros, como RayStation, en un Delivery Controller de Citrix; aparece un mensaje de error similar a:

  "El objeto de comunicación System.ServiceModel.Channels.ServiceChannel no se puede utilizar para la comunicación porque se encuentra en un estado de fallo".[#LC6552]
- No se puede agregar un Delivery Controller a una configuración de base de datos reflejada mediante la opción para agregar un controlador adicional desde Citrix Studio y el comando de PowerShell "Add-XDController". [#LC6563]
- No se pueden eliminar catálogos MCS en VMware VSAN.
- El consumo de memoria de Monitoring Service puede dispararse y causar que los servidores dejen de responder. [#LC6705]
- Después de actualizar Citrix Studio desde versiones anteriores o cuando se realiza una instalación de cero de la versión 7.12 de Citrix Studio, el Delivery Controller puede provocar que Citrix Studio entre en un bucle de actualización obligatoria. [#LC6737]
- Cuando se usa la versión 7.12 de Machine Creation Services para crear máquinas virtuales, XenTools no se instala, lo que impide un apagado ordenado de las máquinas virtuales. [#LC6769]
- Después de actualizar Citrix Delivery Controller a la versión 7.12, puede que no se agreguen máquinas de Citrix

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Provisioning Services (PVS) a un catálogo de máquinas en un entorno con varios dominios. El problema ocurre cuando PVS no devuelve el nombre de dominio junto con el nombre del dispositivo. Cuando Citrix Studio busca el nombre de cuenta en el dominio local, no se encuentra la cuenta. [#LC6818]

- Los permisos para publicar paquetes de App-V podrían denegarse a los administradores que no tengan permisos de administrador total. Aparece la siguiente excepción:

  "Citrix.Console.Models.Exceptions.PermissionDeniedException: No tiene los permisos necesarios para realizar esta operación".[#LC6897]

- El proceso HighAvailabilityService.exe puede llegar a consumir altos niveles de memoria. [#LC6918]
- Cuando se actualiza un sitio de XenApp, el modelo de licencia podría cambiar inesperadamente de XenApp a XenDesktop. [#LC6981]
- El comando "Start-Transcript" falla para "Get-XDSite" y otros comandos PoSH de alto nivel administrativo de XenDesktop cuando se ejecutan en PowerShell 5. [#LC7006]
- Esta revisión soluciona un problema de memoria en el servicio Host de Citrix. [#LC7516]
- Es posible que los administradores personalizados no puedan crear un grupo de aislamiento y aparezca el siguiente mensaje de error:

  "No tiene los permisos necesarios para completar esta solicitud. Para obtener más información, póngase en contacto con el administrador del sitio de XenDesktop".[#LC7563]

- Cuando un administrador intenta agregar una aplicación App-V desde un grupo de aislamiento al grupo de entrega o intenta crear un grupo de aislamiento, es posible que aparezca el siguiente mensaje de error en Citrix Studio:

  "Ocurrió un error desconocido". [#LC7594]

- No se puede instalar el VDA en Microsoft Windows Server cuando ya está instalado el servicio de rol Host de sesión de Escritorio remoto de Microsoft. [#LC7680]
- En Citrix Delivery Controller, intentar inhabilitar TLSv1.0 puede provocar pérdida de comunicación con el hipervisor de VMware vCenter. [#LC7686]
- Puede que no se agreguen máquinas a un grupo de entrega mediante el nombre "NETBIOS" para la asociación de usuario. En su lugar, es posible que aparezca el nombre de dominio. El problema ocurre cuando el nombre NETBIOS usa la URL incorrecta. [#LC7830]

Licencias

- Si no se define el tipo de encabezado "X-Frame-Options", el servidor de licencias puede dar error en el escáner de cumplimiento con la PCI (Industria de tarjetas de pago) que se realiza para evitar el secuestro de clic. [#LC1983]
- Agregar un grupo de dominio cuyo nombre contenga más de 32 caracteres podría fallar. [#LC1986]
- Si el nombre de dominio NetBIOS contiene el carácter &, no puede abrir la ficha Licencias en Studio y aparece este mensaje de error:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

"Servidor de licencias de Citrix no disponible". [#LC2728]

Profile Management

- Cuando ciertas aplicaciones de terceros intentan cambiar el nombre o mover archivos durante el inicio o cierre de sesiones, el intento puede fallar. Por ejemplo, si en el perfil local existen los archivos archivo0, archivo1 y archivo2, no se puede cambiar el nombre de archivo2 por archivo3, archivo1 por archivo2 ni archivo0 por archivo1 durante el proceso de cierre de sesión si ya existe un archivo2 en el área de archivos pendientes o en el almacén de usuarios. [#LC0465]

- Cuando los usuarios cierran sesión, el servicio Profile Management (UserProfileManager.exe) falla algunas veces. [#LC0625]

- El panel "Duración de inicio de sesión" (LOGON DURATION) en el contador del Monitor de rendimiento (Perfmon) puede registrar datos de inicios de sesión de usuarios que no están administrados por Profile Manager. [#LC0779]

- Profile Manager puede no sincronizar los archivos con la tienda de usuarios después de un determinado periodo de tiempo. [#LC1338]

- Después de habilitar las siguientes opciones de captura de registros, no se registra ninguna información de depuración en el archivo de registros:
  - Directiva: Acciones de Active Directory
  - Directiva: Valores de directivas al iniciar y cerrar la sesión
  - Directiva: Diferencias en el Registro del sistema al cerrar sesión

[#LC2003]

- Si un usuario habilita la captura de versiones de perfiles como se describe en https://support.microsoft.com/en-us/kb/2890783, User Profile Manager puede no migrar por los motivos siguientes:

  - El perfil móvil de Microsoft se creó con la extensión "V4"
  - El perfil de UPM no se migró y creó a partir de la plantilla de "Usuario predeterminado".

[#LC2427]

- Después de restablecer el perfil del usuario en Desktop Director, la redirección de carpetas no funciona cuando los usuarios inician sesión por primera vez. La redirección de carpetas sí que funciona cuando los usuarios inician sesión después. [#LC2602]

- El servicio Profile Management (UserProfileManager.exe) puede cerrarse inesperadamente. [#LC2979]

- Después de aplicar la corrección #LC0625, el servicio Profile Management (UserProfileManager.exe) puede cerrarse inesperadamente. [#LC3058]

- En Windows 8.1, fallan las descargas de archivos mediante Internet Explorer 11 si el Modo protegido mejorado (EPM) está habilitado. [#LC3464]

- Pueden producirse bloqueos de archivos en Profile Management durante el proceso de cierre de sesión con el siguiente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

mensaje de error:

"El proceso no puede acceder al archivo porque está bloqueado por otro proceso".

No se puede eliminar los archivos bloqueados por Profile Management hasta que el bloqueo se levanta. [#LC3532]

- Profile Management puede cerrarse inesperadamente mientras el dispositivo del usuario está apagándose. [#LC3626]
- Los servidores XenApp pueden dejar de responder en la comunidad de servidores hasta que se reinician. [#LC4318]
- Al intentar iniciar sesión en un servidor XenApp 7.7 usando RDP, el servidor puede dejar de responder en la pantalla de bienvenida. [#LC5169]
- Después de actualizar un VDA desde la versión 7.6.1000 (o versiones anteriores) a la versión 7.7 (o versiones posteriores), pueden fallar las operaciones de eliminar, reparar o reinstalar el VDA o Profile Management. [#LC5207]
- Al cerrar sesión, Profile Management puede bloquear archivos o carpetas en el servidor, lo que hace que no se puedan iniciar las aplicaciones. Los perfiles guardados en caché local tampoco se eliminan. [#LC5266]
- En ocasiones, Profile Management bloquea archivos en los perfiles de usuario. Cuando eso sucede, los usuarios reciben un perfil temporal mientras intentan reconectar hasta que se levanta el bloqueo de su perfil. [#LC5278]
- Los perfiles guardados en caché local pueden no eliminarse cuando los usuarios cierran la sesión. [#LC5470]
- Cuando el servidor de licencias no está en línea, los archivos que usan la carpeta de redirección de usuarios en el servidor se pierden. [#LC5595]
- Los archivos de los usuarios se pierden cuando finaliza el periodo de licencias de evaluación sin renovarlo. [#LC5775]
- Profile Management puede marcar "NetworkDetection" incorrectamente para indicar que se ha perdido la red. Esta corrección presenta una comprobación adicional para asegurarse de que la red no está disponible, en lugar de haberse perdido temporalmente. [#LC5943]
- En ocasiones, la pantalla de inicio de sesión del usuario deja de responder en Windows Server 2012 R2. [#LC6149]
- Puede que no se migren los perfiles móviles a Profile Management. El problema ocurre cuando se agrega un número incorrecto de versión al perfil. [#LC6150]
- Los iconos de aplicaciones pueden aparecer atenuados al intentar copiarlos desde el almacén de perfiles de usuario en Profile Management a través de una conexión WAN. [#LC6152]
- Puede que las asociaciones de tipos de archivo no pasen de una sesión a otra cuando se trata de sesiones con Profile Management en máquinas Microsoft Windows 10 y Windows Server 2016. [#LC6736]
- Cuando la directiva "Eliminar perfiles guardados en caché local al cerrar la sesión" está habilitada en Windows 10 o Windows 2016, el archivo NTUSER.DAT puede no eliminarse al cerrar la sesión, lo que hace que se cree otro perfil local la

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

próxima vez que se inicia una sesión. [#LC6765]

- Cuando se usa Profile Management en Microsoft Windows Server 2016 y usrclass.dat está incluido, el menú Inicio no funciona. [#LC6914]
- Cuando abre archivos en un perfil con streaming de perfiles habilitado, el archivo puede aparecer vacío después de iniciar sesión. [#LC6996]
- Profile Management puede provocar que aparezca una pantalla en negro cuando intenta iniciar una sesión de Microsoft Windows 10. Con esta corrección, debe configurar la directiva "Directorios para sincronizar" y agregar la carpeta "*AppData\Local\Microsoft\Windows\Caches*". [#LC7596]

Provisioning Services

Problemas de consola

- Con esta corrección, las opciones "Schedule the next vDisk update to occur on" y "Apply vDisk updates as soon as they are directed by the server" ya no están disponibles para Provisioning Services. [#LA4166]
- La creación de máquinas virtuales mediante el asistente XenDesktop Setup Wizard puede fallar en entornos de Microsoft System Center Virtual Machine Manager (SCVMM) cuyo idioma no sea el inglés. [#LC5451]
- La imagen ISO no se crea con el script New-BootDeviceManager de PowerShell y aparece este mensaje de error: "ISOFileName must be called with the name of the new ISO file to create". [#LC5559]
- Cuando se usa el almacenamiento de volúmenes en clúster, el asistente Streamed VM Setup Wizard no cumple la selección de volúmenes y puede crear dispositivos de destino en volúmenes aleatorios. [#LC5890]
- Cerrar la consola Provisioning Services Console después de ejecutar el asistente XenDesktop Setup Wizard o el asistente Streamed VM Setup Wizard provoca una excepción. [#LC6048]
- Después de actualizar a PVS 7.11 desde la versión 7.6, los usuarios de otros dominios pueden tener problemas al iniciar sesión en la consola. [#LC6216]
- Se agota el tiempo de espera en la comunicación con el servidor. En algunos casos, el tiempo de inicio de sesión es demasiado largo (por ejemplo, más de 2 minutos). Eso puede ocasionar problemas de tiempo de espera agotado entre la consola de PVS y el servidor SOAP. De forma predeterminada, el tiempo de espera para estas conexiones es de 2 minutos. Sin embargo, puede aumentar este valor. Para ello, modifique el valor del Registro HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout = . Si el tiempo de inicio de sesión es superior a aproximadamente 4 minutos, los usuarios también tendrán problemas de tiempos de espera agotados en la consola MMC de Microsoft que contiene la consola de PVS (estos tiempos de espera se pueden descartar).

  Uno de los motivos de este problema son dominios no accesibles en Active Directory: se aplica un tiempo de espera de 30 segundos en cada intento de conexión a un dominio no accesible. Lo que puede convertirse rápidamente en varios minutos si hay varios dominios no accesibles. En general, se crean dominios no accesibles cuando se agrega un dominio experimental o de prueba a Active Directory para quitarlo más tarde. A pesar de que el dominio ya no exista, Active

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Directory sigue notificándolo como existente cuando enumera los dominios o los grupos de autorización.

Los dominios no accesibles también pueden deberse a un controlador de dominio que se apaga y se desconecta temporalmente de la red. Por eso, no se puede incluir a todos los dominios no accesibles en la lista negra.

La mejor forma de determinar si hay dominios no accesibles es consultar el rastro CDF del módulo PVS_DLL_ADSUPPORT y buscar en él si hay errores "Unreachable Domain" (Dominio no accesible) y "ServerReferral" (Referencia de servidor). Si encuentra algunos, consulte sus dominios para comprobar que ya no se usan. Si es así, agregue el nombre de esos dominios a la lista negra.

Esa lista negra es un archivo en formato JSON llamado "%ProgramData\Citrix\Provisioning Services\blacklist.json". Por ejemplo:
{

"Domains":

[

"sub.xs.local",

"sb.xs.local"

]

}

donde ambos dominios, **sub.xs.local** y **sb.xs.local**, se excluirán de la enumeración de grupos y dominios. Después de actualizar el archivo, debe reiniciar el servidor SOAP y las consolas en ejecución para que se carguen los valores actualizados. [#LC6249]

- Después de configurar la consola Provisioning Services Console, puede que falten los nombres de etiqueta en las propiedades del dispositivo de destino. [#LC6864]

Problemas de servidor

- En implementaciones de VMware ESX, es posible que el asistente XenDesktop Setup Wizard indique una excepción, lo que impide a los usuarios configurar debidamente plantillas y máquinas. [#LA2499]

- Es posible que dos servidores PVS no puedan ver el estado de replicación de un vDisk en el servidor opuesto, pero cada servidor muestra correctamente el estado de sus propios discos vDisk. [#LC4317]

- El servicio Citrix PXE puede omitir las entradas del archivo BOOTPTAB. [#LC4600]

- Cuando se usa una partición BDM, los dispositivos de destino que ejecutan VMware no intentan iniciar sesión en todos los servidores de la lista, si el servidor que está en el primer lugar de la misma no es contactable. [#LC4736]

- La creación de máquinas virtuales mediante el asistente XenDesktop Setup Wizard puede fallar en entornos de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Microsoft System Center Virtual Machine Manager (SCVMM) cuyo idioma no sea el inglés. [#LC5451]

- Si no se clonan todas las particiones en un disco duro, pueden fallar las particiones finales que se clonan. [#LC5452]
- Al ejecutar el estado de la replicación para dos servidores PVS desde la consola PVS, el estado en ambos servidores aparece como incompleto. [#LC5700]
- Cuando se usa el almacenamiento de volúmenes en clúster, el asistente Streamed VM Setup Wizard no cumple la selección de volúmenes y puede crear dispositivos de destino en volúmenes aleatorios. [#LC5890]
- Después de actualizar a PVS 7.11 desde la versión 7.6, los usuarios de otros dominios pueden tener problemas al iniciar sesión en la consola. [#LC6216]
- Se agota el tiempo de espera en la comunicación con el servidor. En algunos casos, el tiempo de inicio de sesión es demasiado largo (por ejemplo, más de 2 minutos). Eso puede ocasionar problemas de tiempo de espera agotado entre la consola de PVS y el servidor SOAP. De forma predeterminada, el tiempo de espera para estas conexiones es de 2 minutos. Sin embargo, puede aumentar este valor. Para ello, modifique el valor del Registro HOTKEY_LOCAL_MACHINE\Software\Citrix\ProvisioningServices ConnectionTimeout = . Si el tiempo de inicio de sesión es superior a aproximadamente 4 minutos, los usuarios también tendrán problemas de tiempos de espera agotados en la consola MMC de Microsoft que contiene la consola de PVS (estos tiempos de espera se pueden descartar).

  Uno de los motivos de este problema son dominios no accesibles en Active Directory: se aplica un tiempo de espera de 30 segundos en cada intento de conexión a un dominio no accesible. Lo que puede convertirse rápidamente en varios minutos si hay varios dominios no accesibles. En general, se crean dominios no accesibles cuando se agrega un dominio experimental o de prueba a Active Directory para quitarlo más tarde. A pesar de que el dominio ya no exista, Active Directory sigue notificándolo como existente cuando enumera los dominios o los grupos de autorización.

  Los dominios no accesibles también pueden deberse a un controlador de dominio que se apaga y se desconecta temporalmente de la red. Por eso, no se puede incluir a todos los dominios no accesibles en la lista negra.

  La mejor forma de determinar si hay dominios no accesibles es consultar el rastro CDF del módulo PVS_DLL_ADSUPPORT y buscar en él si hay errores "Unreachable Domain" (Dominio no accesible) y "ServerReferral" (Referencia de servidor). Si encuentra algunos, consulte sus dominios para comprobar que ya no se usan. Si es así, agregue el nombre de esos dominios a la lista negra.

  Esa lista negra es un archivo en formato JSON llamado "%ProgramData\Citrix\Provisioning Services\blacklist.json". Por ejemplo:

  {

  "Domains":

  [

  "sub.xs.local",

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

"sb.xs.local"

]

}

donde ambos dominios, **sub.xs.local** y **sb.xs.local**, se excluirán de la enumeración de grupos y dominios. Después de actualizar el archivo, debe reiniciar el servidor SOAP y las consolas en ejecución para que se carguen los valores actualizados. [#LC6249]

Problemas de dispositivos de destino

- La función de actualización automática del dispositivo de destino de Provisioning Services genera el siguiente mensaje de error de la aplicación (Id. de evento: 0) en el Visor de eventos del destino si la actualización no está disponible. "No se encontró ningún servidor de actualización. Deteniendo el servicio de cliente". [#LC0450]

- El software del dispositivo de destino no reconoce la unidad del AppDisk y la usa como caché de escritura, lo que puede provocar conflictos. [#LC5409]

- Cuando se configura un disco vDisk para usar la opción de escritura en caché de RAM (Write Cache on RAM) y se establece el tamaño de caché de RAM en 4096 MB o 4097 MB, arrancar desde una máquina virtual de Hyper-V GEN 2 puede provocar que los dispositivos de destino sufran una excepción grave y muestren una pantalla azul. [#LC6707]

StoreFront

- El servicio de dominio predeterminado de StoreFront no vuelve a cargar el nuevo valor aunque el administrador modifique la directiva de grupo llamada MaxPasswordAge. En StoreFront, el usuario puede ver "una cantidad incorrecta de días restantes hasta la caducidad de la contraseña".

  Nota: Este problema está resuelto. Sin embargo, el nuevo valor puede llegar a tardar una hora en cargarse. [#DNA-41380]

- Con StoreFront 3.5 instalado, el color de las carpetas en la vista de categorías ya no usa el color personalizado definido en la consola de administración de StoreFront. Vuelve al color predeterminado. [#LC5001]

- StoreFront puede cerrarse inesperadamente al administrar sitios de Citrix Receiver para Web. El problema ocurre cuando se personaliza la hoja de estilo style.css para Citrix Receiver para Web. [#LC5589]

- Habilitar el Servicio de autenticación federada en StoreFront puede provocar errores de inicio de sesión. [#LC5708]

- Incluso cuando Citrix Receiver para HTML5 está habilitado en Citrix StoreFront, la consola de StoreFront puede mostrar "No se utiliza" en lugar de mostrar la versión de HTML. [#LC6626]

- Cuando se selecciona un sitio configurado durante la instalación de XenDesktop, puede crearse una tienda predeterminada en StoreFront que usa el Servicio de autenticación predeterminado. Si se quita esta tienda, los usuarios de Citrix Receiver para Windows no pueden agregar otras tiendas y aparece un mensaje de error como este:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

"Se ha producido un error de protocolo al comunicarse con el servicio de autenticación". [#LC6664]

- Si se configura el Autoservicio de restablecimiento de contraseña (SSPR) para una tienda específica en la consola de StoreFront, la configuración se aplica a todas las tiendas, no sólo a la tienda específica que haya seleccionado. [#LC6987]

- Es posible que no pueda volver a conectarse a sesiones desconectadas en una implementación de agrupación multisitio. Por eso, puede recibir una segunda instancia del mismo recurso. [#LC7453]

- Cuando se inhabilita una fuente de una aplicación agregada, la aplicación puede ocultarse inesperadamente al usuario final. [#LC7675]

- En StoreFront, puede que la opción de autoservicio de cuentas no se inhabilite, incluso aunque aparezca inhabilitada. [#LC7744]

- En StoreFront, si intenta quitar la autenticación compartida de tiendas, aparece este mensaje de error al guardar los cambios:

  "Se ha producido un error al guardar los cambios". [#LC7781]

Universal Print Server

Cliente

- Cuando se usa Profile Management, los cambios en las impresoras de Citrix Universal Print Server (agregar, quitar o cambiarles el nombre) realizados en la sesión de un servidor pueden no verse correctamente reflejados en sesiones posteriores en otros servidores. [#LC7645]

Servidor

- No se puede imprimir desde Microsoft Internet Explorer, y aparece este mensaje cuando se usa el controlador de impresora universal de Citrix:

  "Hubo un error interno e Internet Explorer no puede imprimir este documento". [#LC4735]

- No se puede imprimir documentos y aparece este mensaje de error:

  "No se puede imprimir debido a un problema con la impresora seleccionada". [#LC6825]

- Cuando se usan determinadas impresoras, Microsoft Notepad puede mostrar el mensaje "El identificador no es válido" y no imprimir. El problema se da si está configurada la opción "Usar solo los controladores específicos de la impresora" en la directiva de Citrix "Uso de controladores de impresión universal" y si está configurada la opción "Habilitado, sin respaldo de la impresión remota nativa de Windows" en la directiva de Citrix "Habilitar Universal Print Server". [#LC7623]

VDA para SO de escritorio

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección de contenido

- Cuando intenta capturar imágenes con DirectShow, la operación falla y la aplicación se cierra inesperadamente. [#LC6667]

HDX Broadcast

- Es posible que los dispositivos de sonido HDX se inhabiliten de forma aleatoria al iniciar sesión. [#LC5281]

Instalación, desinstalación y actualización

- Después de actualizar el VDA desde la versión 5.6.400 a la versión 7.9, reiniciar el VDA puede provocar que los controladores de reflejo instalados por la versión anterior no se desinstalen. [#LC6295]
- Al actualizar desde la versión 5.6 de VDA a 7.x, puede que se instale un controlador de vídeo antiguo incorrecto. [#LC6363]
- Cuando se usa la versión 7.12 de Machine Creation Services para crear máquinas virtuales, XenTools no se instala, lo que impide un apagado ordenado de las máquinas virtuales. [#LC6769]
- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7555]
- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7587]

Teclado

- Citrix Receiver para Linux podría no admitir tarjetas de DNI electrónico español. [#LC6547]
- Con HDX 3D Pro habilitado en un VDA, las combinaciones de teclas "Alt + p" y "Alt + s" podrían no funcionar. [#LC6826]

Impresión

- Cuando intente imprimir dos o más copias de un documento, puede que solo se imprima una copia. El problema se da si está configurada la opción "Usar solo los controladores específicos de la impresora" en la directiva de Citrix "Uso de controladores de impresión universal" y si está configurada la opción "Habilitado, sin respaldo de la impresión remota nativa de Windows" en la directiva de Citrix "Habilitar Universal Print Server". [#LC6023]
- El servicio Citrix Print Manager (cpsvc.exe) puede dejar de responder y cerrarse de forma inesperada cuando los nuevos usuarios inicien sesión. [#LC6933]
- Después de actualizar el VDA desde la versión 7.9 a la versión 7.12 o posterior, puede que las impresiones desde Microsoft Internet Explorer mediante el controlador de impresora universal de Citrix se dirijan solo a la bandeja 1, en lugar de dirigirse a la bandeja seleccionada. [#LC7463]

Administración de servidores/sitios

- Los cambios que realice en "Configuración avanzada del sistema" en "Efectos visuales" se aplican a la sesión actual del VDA para SO de escritorio, pero es posible que no se conserven para las sesiones subsiguientes. Para que estos cambios sean permanentes, debe establecer la siguiente clave de Registro:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
Nombre: EnableVisualEffect
Tipo: DWORD
Valor: 1

[#LC8049]

Sesión/Conexión

- Puede que no se aplique la directiva Reglas de redirección de dispositivos USB del cliente. El problema ocurre cuando, en la directiva, la cantidad de caracteres que introduce el usuario supera los 1002.[#LC1144]
- Es posible que no pueda volver a conectarse a una sesión de VDA después de una interrupción de red. El problema se produce tras actualizar el agente VDA a la versión 7.8. [#LC5040]
- Con Framehawk habilitado, el botón de desplazamiento del mouse puede no realizar ninguna acción en una sesión de VDA de XenDesktop 7.8. La solución correspondiente al VDA está disponible en XenDesktop 7.9. [#LC5302]
- Un VDA podría experimentar una excepción irrecuperable del tipo 0x50 (Page_Fault_In_NonPaged_Area) en el controlador de pantalla vdodk.sys de Citrix. [#LC5074]
- Cuando AppDisk está conectado a una máquina virtual que ejecuta un sistema operativo Windows cuyo idioma no es el inglés, puede aparecer la solicitud "Reiniciar ahora" o "Reiniciar más tarde". Con esta solución, la solicitud desaparece. [#LC5403]
- Tras volver a conectarse a una sesión desconectada de varios monitores, las pantallas aparecen en negro y las configuraciones personalizadas vuelven a los valores predeterminados. [#LC5556]
- Después de actualizar un VDA de la versión 7.6.300 a la versión 7.8, la sincronización del portapapeles podría dejar de funcionar. [#LC5699]
- Con Framehawk habilitado, el botón de desplazamiento del mouse puede no realizar ninguna acción en una sesión de VDA de XenDesktop 7.9. [#LC5779]
- Cuando un VDA se configura para el Servicio de autenticación federada, ese VDA podría dejar de aceptar conexiones y dejar de responder en la pantalla de bienvenida hasta que se reinicie. [#LC5978]
- Citrix Receiver no puede pasar de "Conexión establecida. Negociando capacidades..." cuando se inicia una aplicación. [#LC6021]
- Los cambios que realice en "Configuración avanzada del sistema" en "Efectos visuales" se aplican a la sesión actual del VDA, pero es posible que no se conserven para las sesiones subsiguientes. Para que estos cambios sean permanentes, debe establecer la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nombre: EnableVisualEffect
  Tipo: DWORD
  Valor: 0

  [#LC6163]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si intenta desconectarse de una sesión de RemotePC que se ejecuta en un dispositivo táctil, puede aparecer una pantalla vacía que no se puede recuperar. [#LC6384]
- Citrix Receiver para Linux podría no admitir tarjetas de DNI electrónico español. [#LC6547]
- Cuando se bloquea una sesión de Remote PC con SecureDoc instalado en Windows 10, la pantalla de bloqueo aparece un máximo de dos minutos. Durante ese tiempo, no se puede interactuar con dicha sesión. [#LC6668]
- Al desconectar y volver a conectarse a una sesión de Citrix Receiver para Mac varias veces durante la reproducción de un vídeo, el sonido podría no funcionar. [#LC6678]
- En el VDA para SO de escritorio, puede que el WFAPI SDK no devuelva unidades extraíbles del cliente. [#LC6877]
- Cuando se usa el modo de gráficos antiguo en un VDA de XenDesktop 7.13 que ejecuta Windows 7, puede aparecer una pantalla en gris. [#LC7477]
- Cuando se cambia entre sesiones con varios monitores en modo de pantalla completa con el modo de gráficos antiguo habilitado y sin Desktop Viewer configurado, parece que solo se ejecuta un monitor en la sesión. [#LC7907]

Excepciones del sistema

- Los agentes VDA para SO de servidor podrían sufrir una excepción irrecuperable en TDICA.sys y mostrar una pantalla azul. [#LC6898]
- Los servidores pueden sufrir una excepción irrecuperable en vdtw30.dll con el código de detención 0xc0000006 y mostrar una pantalla azul. [#LC7608]
- Los VDA pueden experimentar una excepción irrecuperable en tdica.sys con un código de comprobación de errores y mostrar una pantalla azul. [#LC7632]
- Esta corrección soluciona un problema de memoria con el archivo wdica.sys que puede provocar que los servidores se cierren inesperadamente. [#LC7666]

Tarjetas inteligentes

- Al cambiar entre las sesiones de usuario y las sesiones de Escritorio remoto de Microsoft, las aplicaciones compatibles con tarjetas inteligentes de la sesión (como Microsoft Outlook y Microsoft Word) dejan de poder usar tarjetas inteligentes. Por eso, es posible que aparezcan varios mensajes de error. Además, probar el respaldo a las tarjetas inteligentes en la sesión con "CertUtil /scinfo" en una ventana de comandos puede resultar en este mensaje de error:

  "El administrador de recursos de tarjetas inteligentes de Microsoft no se está ejecutando". [#LC5839]
- La autenticación PassThrough con tarjeta inteligente puede fallar de forma intermitente. [#LC6147]

Experiencia de usuario

- Si abre una hoja de cálculo de Excel 2010 que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC5370]
- Solo aparece el ángulo superior izquierdo de la pantalla cuando se usa el modo de gráficos antiguo en un VDA de XenDesktop 7.11 que ejecuta Windows 7. [#LC6532]
- Cuando se realiza una operación de inserción entre dos hojas de cálculo de Microsoft Excel 2010 que se ejecutan en un

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDA 7.9, la ventana de Excel puede dejar de responder. [#LC7912]

Interfaz de usuario

- Al usar la Central de conexiones para cerrar una sesión integrada con datos sin guardar, aparece una ventana en negro con el siguiente mensaje:

  "Todavía deben cerrarse programas" con dos opciones: "Forzar cierre de sesión" o "Cancelar". La opción "Cancelar" no funciona.

  Después de instalar esta corrección, la opción "Cancelar" funciona como es debido. [#LC6075]

- Con la directiva "Presentación automática del teclado" configurada como habilitada y la directiva "Iniciar escritorio con optimización táctil" establecida en prohibida, iniciar un escritorio publicado desde un iPad puede provocar que el visor de documentos aparezca al 80 %. Cuando cierre algunas aplicaciones en el escritorio, el visor de documentos puede aparecer al 100 %. [#LC6460]

- En Excel 2010, si abre una hoja de cálculo que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC7557]

VDA para SO de servidor

Redirección de contenido

- Cuando intenta capturar imágenes con DirectShow, la operación falla y la aplicación se cierra inesperadamente. [#LC6667]

Instalación, desinstalación y actualización

- Después de actualizar un VDA para SO de escritorio de 7.11 a 7.12, aparece el siguiente mensaje de error al iniciar una determinada aplicación:

  "Falta wfapi.dll". [#LC6874]

- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7555]

- Algunas clases de WMI pueden cambiar de nombre después de instalar la versión 7.12 o 7.13 de VDA en una versión de sistema operativo Microsoft Windows cuyo idioma no sea el inglés. [#LC7587]

Impresión

- Citrix Print Manager se cierra de forma inesperada al intentar asignar una impresora de red mediante el comando CreateClientPrinter. [#LC4685]

- Cuando intente imprimir dos o más copias de un documento, puede que solo se imprima una copia. El problema se da si está configurada la opción "Usar solo los controladores específicos de la impresora" en la directiva de Citrix "Uso de controladores de impresión universal" y si está configurada la opción "Habilitado, sin respaldo de la impresión remota

© 1999-2017 Citrix Systems, Inc. All rights reserved.

nativa de Windows" en la directiva de Citrix "Habilitar Universal Print Server". [#LC6023]

- El servicio Citrix Print Manager (cpsvc.exe) puede dejar de responder y cerrarse de forma inesperada cuando los nuevos usuarios inicien sesión. [#LC6933]
- Después de actualizar el VDA desde la versión 7.9 a la versión 7.12 o posterior, puede que las impresiones desde Microsoft Internet Explorer mediante el controlador de impresora universal de Citrix se dirijan solo a la bandeja 1, en lugar de dirigirse a la bandeja seleccionada. [#LC7463]

Administración de servidores/sitios

- Si el usuario se mueve entre sesiones que se encuentran en varias subredes distintas de la red, la lista de impresoras contendrá las impresoras de todas las subredes, en lugar de las pertenecientes a la subred de la sesión actual en que haya iniciado la sesión. [#LC2308]
- Los usuarios de dominios secundarios pueden ver el siguiente mensaje de error cuando inicien una aplicación a través de la Interfaz Web:

  "No tiene permisos para acceder a esta aplicación publicada". [#LC7566]
- Los cambios que realice en "Configuración avanzada del sistema" en "Efectos visuales" se aplican a la sesión actual del VDA para SO de escritorio, pero es posible que no se conserven para las sesiones subsiguientes. Para que estos cambios sean permanentes, debe establecer la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nombre: EnableVisualEffect
  Tipo: DWORD
  Valor: 1

  [#LC8049]

Sesión/Conexión

- En sistemas que dispongan de la corrección #LC2702 (incluido en Hotfix Rollup Pack 6), las aplicaciones no guardan el trabajo en las unidades de cliente asignadas y se generen archivos dañados. [#LC3976]

- Con Streaming Profiler u Offline Plug-in instalado, puede fallar la operación de iniciar un proceso con WinDbg.exe. El problema se produce porque RadeAPHook vincula el parámetro de HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*nombre del proceso*> y HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<*nombre del proceso*>.

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

- *En Windows de 32 bits:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\StreamingHook
  Nombre: EnableReadImageFileExecOptionsExclusionList
  Tipo: Reg_SZ
  Valor: < *Lista de los archivos ejecutables que no se vincularán a la configuración "Image File Execution Options", sin espacios y separados por comas. Por ejemplo, windbg.exe,application_1.exe.*>

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

- *En Windows de 64 bits para aplicaciones de 32 bits:*
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\StreamingHook
  Nombre: EnableReadImageFileExecOptionsExclusionList
  Tipo: Reg_SZ
  Valor: < *Lista de los archivos ejecutables que no se vincularán a la configuración "Image File Execution Options", sin espacios y separados por comas. Por ejemplo, windbg.exe,application_1.exe.* >

  [#LC4750]

- Cuando se inicia una nueva sesión, es posible que el servicio Citrix Audio Redirection Service no consiga conectarse a una sesión de canal virtual que contiene información no válida. [#LC5024]

- Con Framehawk habilitado, el botón de desplazamiento del mouse puede no realizar ninguna acción en una sesión de VDA de XenDesktop 7.8. La solución correspondiente al VDA está disponible en XenDesktop 7.9. [#LC5302]

- Después de actualizar un VDA de la versión 7.6.300 a la versión 7.8, la sincronización del portapapeles podría dejar de funcionar. [#LC5699]

- Con Framehawk habilitado, el botón de desplazamiento del mouse puede no realizar ninguna acción en una sesión de VDA de XenDesktop 7.9. [#LC5779]

- Cuando un VDA se configura para el Servicio de autenticación federada, ese VDA podría dejar de aceptar conexiones y dejar de responder en la pantalla de bienvenida hasta que se reinicie. [#LC5978]

- Los cambios que realice en "Configuración avanzada del sistema" en "Efectos visuales" se aplican a la sesión actual del VDA, pero es posible que no se conserven para las sesiones subsiguientes. Para que estos cambios sean permanentes, debe establecer la siguiente clave de Registro:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix
  Nombre: EnableVisualEffect
  Tipo: DWORD
  Valor: 0

  [#LC6163]

- Cuando se inicia un VDA de SO de servidor de Long Term Service Release Cumulative Update 2 o de versiones anteriores, puede aparecer el siguiente mensaje de advertencia en el registro de eventos de sistema:

  "Falló un intento de conexión con SemsService, con el código de error 0x2." [#LC6311]

- Puede crearse una sesión no operativa de XenApp cuando una sesión de escritorio remoto toma el control de una sesión de consola en un VDA para SO de servidor. [#LC6617]

- Los intentos de volver a conectarse a una sesión pueden fallar de forma intermitente y provocar que los VDA de SO de servidor vayan al estado "Inicializando". El problema ocurre cuando el VDA se registra nuevamente en un Delivery Controller. [#LC6647]

- Cuando se bloquea una sesión de Remote PC con SecureDoc instalado en Windows 10, la pantalla de bloqueo aparece un máximo de dos minutos. Durante ese tiempo, no se puede interactuar con dicha sesión. [#LC6668]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Al desconectar y volver a conectarse a una sesión de Citrix Receiver para Mac varias veces durante la reproducción de un vídeo, el sonido podría no funcionar. [#LC6678]
- Cuando se inicia una aplicación publicada en Microsoft Windows Server 2016, aparece una pantalla en negro durante varios segundos antes de que la aplicación se vuelva visible. [#LC7947]

Tarjetas inteligentes

- Al cambiar entre las sesiones de usuario y las sesiones de Escritorio remoto de Microsoft, las aplicaciones compatibles con tarjetas inteligentes de la sesión (como Microsoft Outlook y Microsoft Word) dejan de poder usar tarjetas inteligentes. Por eso, es posible que aparezcan varios mensajes de error. Además, probar el respaldo a las tarjetas inteligentes en la sesión con "CertUtil /scinfo" en una ventana de comandos puede resultar en este mensaje de error:

  "El administrador de recursos de tarjetas inteligentes de Microsoft no se está ejecutando". [#LC5839]

Excepciones del sistema

- Los agentes VDA para SO de servidor podrían sufrir una excepción irrecuperable en TDICA.sys y mostrar una pantalla azul. [#LC6898]
- Los servidores pueden sufrir una excepción irrecuperable en vdtw30.dll con el código de detención 0xc0000006 y mostrar una pantalla azul. [#LC7608]
- Los VDA pueden experimentar una excepción irrecuperable en tdica.sys con un código de comprobación de errores y mostrar una pantalla azul. [#LC7632]
- Esta corrección soluciona un problema de memoria con el archivo wdica.sys que puede provocar que los servidores se cierren inesperadamente. [#LC7666]

Experiencia de usuario

- Si abre una hoja de cálculo de Excel 2010 que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC5370]
- Cuando se realiza una operación de inserción entre dos hojas de cálculo de Microsoft Excel 2010 que se ejecutan en un VDA 7.9, la ventana de Excel puede dejar de responder. [#LC7912]

Interfaz de usuario

- Al usar la Central de conexiones para cerrar una sesión integrada con datos sin guardar, aparece una ventana en negro con el siguiente mensaje:

  "Todavía deben cerrarse programas" con dos opciones: "Forzar cierre de sesión" o "Cancelar". La opción "Cancelar" no funciona.

  Después de instalar esta corrección, la opción "Cancelar" funciona como es debido. [#LC6075]
- Con la directiva "Presentación automática del teclado" configurada como habilitada y la directiva "Iniciar escritorio con optimización táctil" establecida en prohibida, iniciar un escritorio publicado desde un iPad puede provocar que el visor de documentos aparezca al 80 %. Cuando cierre algunas aplicaciones en el escritorio, el visor de documentos puede aparecer al 100 %. [#LC6460]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- En Excel 2010, si abre una hoja de cálculo que tiene más de un libro, la barra de tareas muestra solo el libro de versión más reciente. [#LC7557]

Componentes de escritorio virtual: Otros

- El tipo de sesión de una aplicación alojada en una máquina virtual puede cambiar inesperadamente de "Aplicación" a "Escritorio". Por eso, el usuario no puede volver a conectarse a la aplicación. [#LC5461]
- Cuando se inicia un paquete de App-V con la infraestructura de Microsoft App-V 5.0 integrada en XenDesktop, el paquete de App-V no se sincroniza y aparece esta excepción:

  "No se puede iniciar ". [#LC5483]
- Si intenta cargar una aplicación App-V a través de la red, aparece el siguiente mensaje de error:

  "El índice estaba fuera del intervalo. No puede ser negativo y debe ser inferior al tamaño de la colección". [#LC5828]
- Después de actualizar de la versión 7.7 a la versión 7.8 de XenApp, podrían fallar los inicios de aplicaciones App-V. El problema ocurre cuando el valor de la opción booleana "TargetIn" se establece en "0" en lugar de "1". Además, establecer el valor de forma manual puede no tener ningún efecto. Puede revertirse cuando se actualice la aplicación. [#LC5861]
- Al agregar un paquete de App-V que contiene varias aplicaciones a Citrix Studio y publicar todas las aplicaciones del paquete, es posible que solo se inicie la primera aplicación en la sesión de usuario. [#LC5863]
- Un solo usuario puede iniciar la aplicación de App-V. Si otro usuario intenta iniciar la misma aplicación en el mismo servidor, la operación puede fallar. [#LC6414]
- Las aplicaciones secuenciadas de App-V podrían no incluirse en el paquete real de App-V, incluso aunque el paquete haga referencia a ellas (InTarget = False). En consecuencia, el inicio de la aplicación no se aplica a ningún grupo de conexión relacionado que sea necesario para que esa aplicación funcione correctamente. [#LC6534]
- Después de actualizar desde XenApp/XenDesktop 7.11 a 7.12, no se respetan las programaciones de reinicios de los grupos de entrega existentes. [#LC6766]
- Las aplicaciones de App-V pueden no iniciarse desde una unidad asignada. [#LC6961]
- Puede fallar la publicación de aplicaciones App-V.

  [#LC7421]
- Si está instalado Microsoft Message Queuing en la imagen maestra del VDA, los catálogos de máquinas no se crean y aparece el siguiente mensaje de error en Citrix Studio:

  "Image Preparation did not complete. Status 'NotSet". [#LC7528]
- No se pueden iniciar aplicaciones App-V en el modo Administración única. El problema ocurre cuando el nombre de la aplicación contiene caracteres especiales. [#LC7897]

Otros problemas resueltos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- En Citrix Studio, desaparecen las directivas de grupo si la directiva UPM - Software\Microsoft\Speech_OneCore en Profile Management > Registro > Exclusiones predeterminadas se configuró antes de actualizar Delivery Controller de 7.11 a 7.14, de 7.12 a 7.14 o de 7.13 a 7.14. [#UPM-538]
- No se puede instalar ni actualizar Grabación de sesiones 7.14 con el programa de instalación de producto completo de XenApp y XenDesktop en Windows Server 2008; aparece un mensaje de error similar a: "Fallo de Microsoft Message Queuing". [#SRT-1782]
- Después de actualizar los Controllers, el estado de energía de un VDA podría indicar "Desconocido". [#DNA-37756]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas conocidos

Apr 18, 2018

Los problemas conocidos que se describen en las secciones de 7.15 base y CU1 de este artículo siguen estando presentes en CU2 a menos que estén incluidos en la lista de problemas resueltos.

Problemas conocidos en Cumulative Update 2

- En W2k16 VDA, puede que los usuarios que inician sesión con tarjetas inteligentes no vean a todos los usuarios disponibles al iniciar sesión. El problema es el resultado del tamaño predeterminado de la ventana de inicio de sesión, que es 600 x 520. Para obtener más información sobre este problema y su solución temporal, consulte el artículo CTX204070 en Knowledge Center. [LCM-3951]

- Para obtener una lista de los problemas conocidos con Windows 10 Redstone 4 (compilaciones Insider Preview), consulte el artículo CTX231942 de Knowledge Center.

Problemas conocidos en Cumulative Update 1

- La consola de administración de StoreFront no se abre después de una actualización a StoreFront 3.12.1000 (XenApp y XenDesktop 7.15 LTSR CU1) desde StoreFront 3.12 (XenApp y XenDesktop 7.15 LTSR) o después de una instalación de StoreFront 3.12.1000. La consola de administración de StoreFront muestra el error "MMC no puede crear el complemento. Es posible que el complemento no se haya instalado correctamente". Para solucionar este problema, siga los pasos que se describen en CTX233206. [#LC8935]

- Cuando se instala un controlador firmado con un certificado SHA-256 en una máquina con Windows 7 o Windows Server 2008 R2, aparece un mensaje de Microsoft WHQL (Windows Hardware Quality Labs). Para resolver el problema, instale estas revisiones hotfix de Microsoft en la máquina:
  - Windows 7 (una revisión hotfix): https://support.microsoft.com/es-es/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i
  - Windows Server 2008 R2 (dos revisiones hotfix): https://support.microsoft.com/en-us/help/2921916/the-untrusted-publisher-dialog-box-appears-when-you-install-a-driver-i y https://support.microsoft.com/en-us/help/2837108/you-cannot-import-a-windows-8-signed-driver-on-a-windows-server-2008-r [#LCM-2836]
- Cuando Citrix Telemetry Service está inhabilitado o detenido, y se utiliza un metainstalador para actualizar XenApp y XenDesktop 7.15 LTSR a Cumulative Update 1 (CU1), puede aparecer este mensaje de advertencia:
  "No podemos iniciar el servicio de Citrix que habilita la inscripción en Call Home. Consulte el artículo CTX218094 para obtener más información". [#LCM-3642]

Problemas conocidos en 7.15 LTSR (versión inicial)

La versión XenApp y XenDesktop 7.15 LTSR presenta los siguientes problemas:

App-V

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- En Studio, al eliminar una o varias aplicaciones de App-V que haya en el nodo Aplicaciones o en un grupo de entrega seleccionado, aparece el mensaje "Ocurrió un error desconocido". Puede ignorar el mensaje; las aplicaciones se eliminan correctamente. [#DNA-29702]

- No se puede quitar una aplicación App-V de un grupo de entrega si un proceso secundario de esa aplicación se inició, pero no pudo cerrarse cuando se cerró la aplicación. El mensaje de error indica que la aplicación está en uso. Para determinar el nombre del proceso, ejecute Get-AppVVirtualProcess. A continuación, finalice ese proceso con el Administrador de tareas o Stop-AppVClientPackage. [#DNA-23624]

- Cuando se quita un paquete App-V de la biblioteca de aplicaciones, este se elimina de la pantalla de Studio, pero no del VDA. Como solución temporal, ejecute los siguientes cmdlets desde el VDA con privilegios elevados de administrador:

  ```
  Import-Module AppvClient
  Get-AppVClientPackage -all
  #Identify the PackageId and VersionId of the package to be removed
  Remove-AppVClientPackage -PackageId <packageid> -VersionId <versionid>
  ```

  [#DNA-47379]

- Debido al comportamiento de Microsoft App-V, cuando publica varias versiones secuenciadas de la misma aplicación usando el método de administración única o dual, solo puede ejecutarse una versión de la aplicación a la vez por usuario en el VDA. La primera versión que inicie el usuario determina la versión que se ejecutará posteriormente para él. 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. Hasta la fecha, en Citrix hemos visto este problema en versiones diferentes de navegadores Mozilla Firefox y Google Chrome. [#APPV-60]

Instalar y actualizar

- Al actualizar un VDA 7.14 a VDA 7.15, las claves creadas en la clave de Registro HKEY_LOCAL_MACHINE\Software\Policies\Citrix para las configuraciones de directivas Citrix que se aplican con la **Plantilla administrativa** pueden eliminarse del VDA. [#LCM-3876]

- Al instalar componentes con la aplicación AutoSelect desde los medios de instalación, el archivo autorun.log puede contener errores y excepciones acerca de derechos insuficientes. Siempre que la instalación se complete correctamente, puede ignorar estos errores. No obstante, para evitarlos, inicie AutoSelect con la opción **Ejecutar como administrador**. [#DNA-45937]

- Al actualizar una implementación de XenDesktop 5.6 a XenDesktop 7.15 LTSR, falta la directiva de grupo. Como solución temporal, actualice de XenDesktop 5.6 a XenDesktop 7.13. A continuación, actualice de 7.13 a 7.15 LTSR. [#DNA-44818]

- 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]

- Al instalar un Delivery Controller en Windows Server 2012 R2 o Windows Server 2016, si decide conectar con Smart Tools y tiene varias organizaciones vinculadas a su cuenta de Citrix Cloud, el proceso de inicio de sesión puede no completarse después de introducir sus credenciales de Citrix Cloud. Como solución temporal, complete uno de los pasos siguientes:
  - Compruebe que el servidor de Windows e Internet Explorer tienen las actualizaciones más recientes.
  - Desactive la opción del navegador de Internet Explorer: Opciones de Internet > Seguridad > Intranet local > Sitios > Incluir todos los sitios que no usen un servidor proxy.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[#CAM-9816]

- Si StoreFront se instaló en su momento desde el archivo ejecutable presente en los medios de instalación, no aparece como apto para la actualización cuando se usa el programa de instalación de producto completo para una versión posterior. Como solución temporal, actualice StoreFront con el archivo ejecutable desde los medios de instalación. [#DNA-47816]
- Cuando el Delivery Controller se actualiza desde una versión anterior a 7.13 a la versión 7.13 y versiones posteriores, 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 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 CTX22947. [#DNA-52476]
- Cuando seleccione máquinas y las agregue a grupos de entrega existentes, Studio permite agregar máquinas provenientes de catálogos incompatibles con el mismo grupo de entrega. (Si selecciona primero un grupo de entrega y luego le agrega máquinas, Studio impide correctamente que se agreguen máquinas provenientes de catálogos incompatibles.) [#DNA-39589]

General

- Cuando se usa un certificado de sesión del Servicio de autenticación federada para autenticar una conexión TLS 1.1 (o una versión anterior), puede fallar la conexión. Se registra un ID de evento 305, que indica un ID hash no respaldado. El Servicio de autenticación federada no respalda el hash SHAMD5. Para solucionar temporalmente este problema, use las conexiones TLS 1.2. Este problema afecta a XenApp y XenDesktop desde 7.9 hasta esta versión. [#DNA-47628]
- No se guardan los parámetros de la directiva "Asignación y compatibilidad de controladores de impresora". Como solución temporal, use Citrix Group Policy PowerShell Provider para modificar este parámetro. Para obtener más información sobre la solución temporal, consulte CTX226589. [#DNA-47423]
- Error de registro de eventos de Windows: "Windows no puede comprobar la integridad de imagen del archivo MfApHook64.dll". Para obtener más información, consulte CTX226397. [HDX-9063]
- 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]
- El contenido publicado no se inicia correctamente al iniciarlo desde Citrix Receiver. El contenido que se abre mediante el cliente Web de StoreFront (o la interfaz Web) se inicia como era de esperar. [#LC6316, #RFWIN-4957]
- El proceso de actualización de la imagen de Machine Creation Services (MCS) puede fallar con VMware VSAN 6.x porque no se puede garantizar que el disco de identidad se pueda desconectar y volver a conectar a la máquina virtual. Si esto sucede, elimine y vuelva a crear la máquina virtual manualmente o cree un nuevo catálogo para la actualización de la imagen. Para obtener más información, consulte CTX219670.
- 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. [#DNA-37964]
- 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. Como solución temporal, agregue esta clave de registro en el punto final:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream\
Nombre: DisableVMRSupport
Tipo: DWORD
Valor: 4

[#HDX-10055]

Impresión

- El proceso CpSvc.exe deja de responder cuando se detiene o se reinicia el servicio Citrix Print Manager Service. Como solución temporal, detenga el proceso CpsSvc.exe antes de detener o reiniciar el servicio en el complemento Servicios, o bien, reinicie el VDA para evitar este problema. [#HDX-10071]

- 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 de Knowledge Center. [#335153]

Profile Management

Profile Management puede provocar que aparezca una pantalla en negro cuando intenta iniciar una sesión de Microsoft Windows 10. Con esta corrección, debe configurar la directiva "Directorios para sincronizar" y agregar la carpeta "*AppData\Local\Microsoft\Windows\Caches*". Para obtener más información y una solución temporal, consulte el artículo CTX234144 de Knowledge Center. [#LC-9030]

Grabación de sesiones

- Cuando Machine Creation Services (MCS) o Provisioning Services (PVS) crean varios agentes VDA con una imagen maestra configurada y Microsoft Message Queuing (MSMQ) instalado, esos VDA pueden tener el mismo QMId en ciertos casos. Esto puede causar diversos problemas, como:
  - Las sesiones pueden no grabarse aunque el acuerdo de grabación se acepte.
  - El Servidor de grabación de sesiones puede no recibir la señal del cierre de sesión, lo que hace que la sesión se quede en estado "Activo" permanentemente.

  Consulte los artículos de instalación de la Grabación de sesiones para obtener una solución temporal. [#528678]

Problemas de terceros

- Citrix y Microsoft han identificado un problema que se daba al iniciar las aplicaciones integradas desde un VDA de servidor que ejecuta Windows Server 2016. Cuando un usuario inicia una aplicación publicada desde este VDA, Citrix Receiver muestra una pantalla en negro que cubre el área de trabajo del monitor durante varios segundos antes de iniciar la aplicación. Para obtener más información, consulte https://support.citrix.com/article/CTX225819.

  Advertencia: Si utiliza Azure Active Directory (AAD), no haga el cambio en el Registro que se indica en CTX225819. Si hace ese cambio, pueden producirse fallos al lanzar sesiones para los usuarios de AAD. [HDX-5000]

- En un entorno de pruebas de estrés, de 20 000 inicios de sesión, Microsoft Windows WinLogon.exe puede dejar de funcionar de manera intermitente con una frecuencia de < 0,001 %. [#HDX-9938]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avisos de terceros

Apr 18, 2018

Esta versión de XenApp y XenDesktop puede incluir software de terceros con licencias definidas en los términos de los siguientes documentos:

PDF Avisos legales de terceros para XenApp y XenDesktop

PDF Aviso de software para uso no comercial de FlexNet Publisher 2016 R1 (11.14.0.0)

PDF Documentación complementaria de FlexNet Publisher: licencias de software de código abierto que se aplican a FlexNet Publisher 11.14.0

PDF Avisos de terceros para la grabación de sesiones

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Obsolescencia

Apr 18, 2018

Los siguientes anuncios tienen por objeto avisarle por adelantado acerca de las plataformas, los productos y las funcionalidades 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 funcionalidad que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Esta lista está sujeta a cambios en las versiones posteriores y puede no contener todas las funciones o características obsoletas.

Las siguientes plataformas, las características y los productos Citrix están *obsoletos*. Esto no significa que se quitan inmediatamente. Citrix sigue admitiéndolos en esta versión de XenApp y XenDesktop 7.15 Long Term Service Release (LTSR). Sin embargo, esos elementos obsoletos se quitarán de la versión posterior a esta LTSR.Siempre que sea posible, se sugerirán soluciones alternativas a los elementos obsoletos.

Para obtener información detallada acerca del respaldo al ciclo de vida útil del producto, consulte el artículo Product Lifecycle Support Policy.

Elemento	Obsolescencia anunciada 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.
Agentes VDA en Windows 10 versión 1511 (Threshold 2) y versiones anteriores de SO de escritorio Windows, incluido Windows 8.x y Windows 7.	7.15 LTSR (y 7.12)	Instale agentes VDA de SO de escritorio en Windows 10 versión 1607 (Redstone 1) o una versión más reciente de Canal semianual. Si utiliza LTSB 1607, se recomienda un VDA 7.15.
Agentes VDA en Windows Server 2008 R2 y Windows Server 2012 (incluidos los Service Packs).	7.15 LTSR (y 7.12)	Instale agentes VDA de SO de servidor en las versiones admitidas (como Windows Server 2012 R2 o Windows Server 2016).
Delivery Controllers en Windows Server 2012 y 2008 R2 (incluidos los Service Packs).	7.15 LTSR	Instale Delivery Controllers en otro sistema operativo respaldado.
Studio en Windows 7 (incluidos los Service Packs).	7.15 LTSR	Instalar Studio en otro sistema operativo respaldado.
Redirección de Flash.	7.15 LTSR	Use el vídeo HTML5. Para obtener más información, consulte Fin de vida para la redirección de Flash.
Comunicación remota de comandos de	7.15 LTSR	Use Thinwire.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

DirectX (DCR).		
Integración de Citrix Online (producto de la familia GoTo) con StoreFront.	7.14 (y StoreFront 3.11)	Desde StoreFront 3.12, esta función no puede configurarse en la consola de administración de StoreFront. Si actualiza a StoreFront 3.12, puede seguir utilizando esta función. Para cambiar la configuración, use el cmdlet de PowerShell llamado Update-DSGenericApplications. Para obtener más información, consulte Integración de las aplicaciones de Citrix Online en las tiendas
Actualizaciones locales desde StoreFront 2.0, 2.1, 2.5 y 2.5.2.	7.13	Debe actualizar desde una de estas versiones a una versión posterior respaldada y, a continuación, actualizar a XenApp y XenDesktop 7.13.
Actualizaciones locales desde XenDesktop 5.6 o 5.6 FP1.	7.12	Debe migrar su implementación de XenDesktop 5.6 o 5.6 FP1 a la versión actual de XenDesktop.
Agentes VDA en Windows 8.1 y versiones anteriores de escritorios Windows.	7.12	Instale agentes VDA de SO de escritorio en Windows 10.
Agentes VDA en Windows Server 2008 R2.	7.12	Instale agentes VDA de SO de servidor en las versiones admitidas (como Windows Server 2012 R2 o Windows Server 2016).
XenDesktop 5.6 en Windows XP. No se admitirán instalaciones de VDA en Windows XP.	7.12	Instale los VDA en una versión compatible de Windows.
Conexiones a CloudPlatform.	7.12	Use un hipervisor o servicio de nube respaldados.
Conexiones Azure Classic (también conocido como Administración de servicios de Azure).	7.12	Use el Administrador de recursos de Azure.
Instalación de componentes principales (aparte de Studio) en máquinas de 32 bits: Delivery Controller, Director, StoreFront y el servidor de licencias.	7.12	Use máquinas de 64 bits.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Concesión de conexiones.	7.12	Use Caché de host local.
Modo antiguo de Thinwire	7.12	Use Thinwire.
Redirección HDX de composición del escritorio (DCR)	7.12	

AppDisk y Personal vDisk

La funcionalidad de AppDisks y Personal vDisk, suministrada por XenApp y XenDesktop, ha quedado obsoleta para las versiones actuales*. Citrix está reemplazando esta funcionalidad por una tecnología recientemente adquirida de Unidesk (Citrix App Layering).Durante este período de transición, Citrix seguirá manteniendo los niveles actuales de respaldo, como se describe en Opciones de servicio de XenApp y XenDesktop.

* La opción de servicio Long Term Service Release (LTSR) no cubre AppDisks ni Personal vDisk.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sección 508: Plantilla voluntaria de accesibilidad del producto (VPAT)

Apr 18, 2018

PDF Citrix XenApp and XenDesktop 7.15 Director VPAT

PDF Citrix XenApp and XenDesktop 7.15 Installer VPAT

PDF Citrix XenApp and XenDesktop 7.15 Licensing Administration Console VPAT

PDF Citrix XenApp and XenDesktop 7.15 Licensing Manager VPAT

PDF Citrix XenApp and XenDesktop 7.15 Receiver for Web Classic Experience VPAT

PDF Citrix XenApp and XenDesktop 7.15 Receiver for Web Unified Experience VPAT

PDF Citrix XenApp and XenDesktop 7.15 StoreFront VPAT

PDF Citrix XenApp and XenDesktop 7.15 Studio VPAT

PDF Citrix Provisioning Services Boot Device Manager VPAT

PDF Citrix Provisioning Services BOOTPTAB Editor VPAT

PDF Citrix Provisioning Services Client Side Imaging Wizard VPAT

PDF Citrix Provisioning Services Configuration Wizard VPAT

PDF Citrix Provisioning Services Console VPAT

PDF Linux VDA VPAT

PDF Citrix Scout VPAT

PDF Citrix Session Recording Player VPAT

PDF Citrix Session Recording Authorization Console VPAT

PDF Citrix Workspace Environment Management Administration Console VPAT

PDF Citrix Workspace Environment Management Infrastructure Service Configuration VPAT

PDF Citrix Workspace Environment Management Agent Log Parser VPAT

PDF Citrix Workspace Environment Management Installer VPAT

PDF Citrix Workspace Environment Management Profile Cleanser VPAT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PDF Citrix Workspace Environment Management Integrity Condition List Manager VPAT

PDF Citrix Workspace Environment Management Database Management Utility VPAT

PDF Citrix Self-Service Password Reset VPAT

PDF Citrix SCOM Management Pack VPAT

PDF Citrix Receiver for macOS VPAT

PDF Citrix Management Pack Configuration VPAT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Requisitos del sistema

Apr 18, 2018

En este artículo:

- Introducción
- Delivery Controller
- Bases de datos
- Citrix Studio
- Citrix Director
- Virtual Delivery Agent (VDA) para sistemas operativos de escritorio
- Virtual Delivery Agent (VDA) para sistemas operativos de servidor
- Hosts o recursos de virtualización
- Niveles funcionales de Active Directory
- HDX
- Grabación de sesiones
- Universal Print Server
- Otros

Introducción

Los requisitos del sistema descritos en este documento eran válidos en el momento de la publicación de la presente versión de producto. Sin embargo, se realizan actualizaciones de forma periódica. Aquellos componentes de los requisitos del sistema que no se incluyen aquí (como, por ejemplo, StoreFront, sistemas host, Citrix Receivers y Plug-ins, y Provisioning Services) se describen en su documentación respectiva.

Importante: Revise el artículo Antes de la instalación antes de comenzar la instalación.

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

Los medios de instalación contienen varios componentes de terceros. Antes de usar el software de Citrix, busque actualizaciones para los componentes de terceros e instálelas.

Para obtener información acerca de la globalización, consulte CTX119253.

Para las funcionalidades y los componentes de XenApp y XenDesktop que se pueden instalar en servidores Windows, no se respaldan las instalaciones Core Server y Nano Server a menos que se indique específicamente.

Para conocer los componentes y las características que se pueden usar en máquinas Windows 10, se admiten las siguientes ediciones y opciones de prestación de servicios de Windows 10:

- Semi-annual Channel: Pro, Enterprise, Education, Mobile Enterprise (IoT Core Pro Edition solo se admite para Citrix Receiver)
- Long-term Servicing Channel (LTSC): Enterprise LTSB Edition

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para obtener más información, consulte CTX224843.

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 características que utilice y la cantidad de usuarios, entre otros factores. Utilizar solo lo mínimo puede derivar en un rendimiento lento.

Por ejemplo, la cantidad de espacio en disco necesario en el Controller para la concesión de conexiones (habilitada de forma predeterminada) depende de la cantidad de los usuarios, las aplicaciones y del modo. Así, 100 000 usuarios RDS con 100 aplicaciones usadas recientemente requieren aproximadamente 3 GB para concesiones de conexiones; es posible que las implementaciones con más aplicaciones necesiten más espacio. Para los escritorios VDI dedicados, 40 000 escritorios requieren al menos 400-500 MB. En cualquier caso, Citrix sugiere proporcionar varios GB de espacio adicional.

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

Componente	**Mínimo**
Todos los componentes principales en un servidor, solo para una evaluación, no para 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 requiere más espacio en disco si se habilita una funcionalidad Alta disponibilidad como la Concesión de conexiones.)	5 GB de RAM 800 MB de disco duro Base de datos: consulte el artículo Guía de tamaños
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Consulte la documentación sobre licencias para conocer las recomendaciones de disco.

Tamaño de las máquinas virtuales que entregan escritorios y aplicaciones

No se pueden ofrecer recomendaciones concretas debido a la naturaleza dinámica y compleja del hardware existente en el mercado, además de que cada implementación de XenApp o XenDesktop tiene necesidades únicas. Por lo general, el tamaño de una máquina virtual de XenApp se calcula en función del hardware y no se tienen en cuenta las cargas de trabajo del usuario (excepto para la memoria RAM, porque necesitará más memoria RAM para aplicaciones que consuman más).El Manual y prácticas recomendadas para Citrix VDI contiene la guía más reciente sobre el tamaño del VDA.

Delivery Controller

Sistemas operativos respaldados:

- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows Server 2012, Standard y Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise y Datacenter Edition

Requisitos:

- Microsoft .NET Framework 3.5.1 (solo Windows Server 2008 R2).
- Microsoft .NET Framework 4.5.2 (de 4.6 a 4.7 también se respaldan).
- Windows PowerShell 3.0 o una versión posterior.
- 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 hasta SP1, ediciones Express, Standard y Enterprise.
- SQL Server 2014 hasta SP2, 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 respaldan 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Grupos de disponibilidad AlwaysOn de SQL Server (incluidos los grupos de disponibilidad básica)
- Creación de 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 funcionalidad Memoria caché del 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
- CTX114501
- Guía para tamaños de base de datos
- Memoria caché del host local

Citrix Studio

Sistemas operativos respaldados:

- Windows 10 (consulte el respaldo a las ediciones en la sección *Introducción*)
- Windows 8.1, Professional y Enterprise Edition
- Windows 7, Professional, Enterprise y Ultimate Edition
- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows Server 2012, Standard y Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise y Datacenter Edition

Requisitos:

- Microsoft .NET Framework 4.5.2 (de 4.6 a 4.7 también se respaldan).
- Microsoft .NET Framework 3.5 SP1 (solo Windows Server 2008 R2 y Windows 7)
- Microsoft Management Console 3.0 (se incluye con todos los sistemas operativos compatibles)
- Windows PowerShell 2.0

Citrix Director

Sistemas operativos respaldados:

- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows Server 2012, Standard y Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise y Datacenter Edition

Requisitos:

- Microsoft .NET Framework 4.5.2 (de 4.6 a 4.7 también se respaldan).
- Microsoft .NET Framework 3.5 SP1 (solo Windows Server 2008 R2)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

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. Debe usar 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.
- 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 respaldados:

- Windows 10 (consulte la información sobre ediciones respaldadas, en la sección *Introducción*). Las siguientes funcionalidades no se admiten en Windows 10: la redirección de composición del escritorio ni el modo de gráficos antiguo.
- Windows 8.1, Professional y Enterprise Edition
- Windows 7 SP1, Professional, Enterprise y Ultimate Edition

Requisitos:

- Microsoft .NET Framework 4.5.2 (de 4.6 a 4.7 también se respaldan).
- Microsoft .NET Framework 3.5.1 (solo Windows 7)
- 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. El agente Virtual Delivery Agent (VDA) da respaldo al arranque seguro (Secure Boot) para el acceso con Remote PC de XenDesktop 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

multimedia, pero se puede obtener el software de Microsoft o de un tercero. Para obtener más información, consulte Antes de la instalación.

Durante la instalación de VDA, puede elegir el modo HDX 3D Pro de VDA para SO de escritorio Windows. Ese modo es idóneo sobre todo cuando se usan también aplicaciones basadas en DirectX y OpenGL, y con contenido multimedia enriquecido (como vídeos). Consulte la sección HDX 3D Pro para obtener más información acerca de la compatibilidad.

Para obtener más información acerca de Linux VDA, consulte los artículos de Linux Virtual Delivery Agent.

Para usar la característica VDI de servidor, puede usar la interfaz de línea de comandos para instalar un VDA para SO de escritorio Windows en un sistema operativo de servidor compatible. Consulte VDI de servidor para obtener instrucciones.

Virtual Delivery Agent (VDA) para sistemas operativos de servidor

Sistemas operativos respaldados:

- Windows Server 2016, Standard y Datacenter Edition
- Windows Server 2012 R2, Standard y Datacenter Edition
- Windows Server 2012, Standard y Datacenter Edition
- Windows Server 2008 R2 SP1, Standard, Enterprise 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 4.5.2 (de 4.6 a 4.7 también se respaldan).
- Microsoft .NET Framework 3.5.1 (solo Windows Server 2008 R2)
- 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, por ejemplo, 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 ediciones de Windows Server, la funcionalidad de Media Foundation se instala mediante el Administrador del servidor (para Windows Server 2012 y versiones posteriores: ServerMediaFoundation; para Windows Server 2008 R2: DesktopExperience). 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 la instalación.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para obtener más información acerca de Linux VDA, consulte los artículos de Linux Virtual Delivery Agent.

Hosts o recursos de virtualización

Es posible que algunas funcionalidades de XenApp y XenDesktop no reciban respaldo en todas las plataformas de host ni todas las versiones de plataforma. Por ejemplo, los AppDisks se respaldan en XenServer, VMware y los hosts de System Center Virtual Machine Manager. Consulte la documentación sobre funcionalidades para obtener más información.

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

Plataformas de host y entornos de virtualización respaldados

IMPORTANTE: Se respaldan 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 7.4
- XenServer 7.3
- XenServer 7.2
- XenServer 7.1 LTSR
- XenServer 7.0
- XenServer 6.5 y SP1
- XenServer 6.2 SP1 y revisiones hotfix (debe aplicar SP1 para habilitar la aplicación de revisiones hotfix futuras)
- XenServer 6.1

VMware vSphere (vCenter + ESXi) No se ofrece respaldo para la operación "Linked Mode" de vSphere vCenter.

- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- VMware vSphere 5.1
- VMware vSphere 5.0
- Dispositivo VMware vCenter 5.5, 6 y 6.5

System Center Virtual Machine ManagerIncluye 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 4.5

Amazon Web Services (AWS)

- Puede aprovisionar aplicaciones y escritorios en sistemas operativos Windows Server compatibles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- No se admite Amazon Relational Database Service (Amazon RDS).
- Consulte Citrix XenDesktop en Amazon Web Services para obtener información adicional.

CloudPlatform

- La versión mínima respaldada es 4.2.1 con las revisiones hotfix 4.2.1-4.
- Las implementaciones se han probado usando XenServer 6.2 (con Service Pack 1 y revisión hotfix XS62ESP1003) e hipervisores vSphere 5.1.
- CloudPlatform no respalda el uso de hipervisores Hyper-V.
- CloudPlatform 4.3.0.1 respalda VMware vSphere 5.5.
- Para obtener más información, consulte la documentación de CloudPlatform (incluidas las notas de la versión para su versión de CloudPlatform).

Microsoft Azure

Administrador de recursos de Azure de Microsoft

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
- Windows Server 2003
- Windows 2000 nativo (no se admite para controladores de dominio)

HDX

El sonido UDP para ICA de multisecuencia está respaldado en Receiver para Windows y Receiver para Linux 13.

La cancelación del eco está respaldada en Citrix Receiver para Windows.

Consulte a continuación el respaldo y los requisitos necesarios para la función HDX.

HDX y la redirección de composición del escritorio

El cliente ligero o dispositivo de usuario Windows debe admitir o contener:

- DirectX 9
- Pixel Shader 2.0 (admitido en hardware)
- 32 bits por píxel
- Procesador de 1,5 GHz de 32 bits ó 64 bits
- 1 GB de RAM
- 128 MB de memoria de vídeo en la tarjeta gráfica o un procesador de gráficos integrado

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX consulta al dispositivo Windows para comprobar que tiene la capacidad de GPU necesaria y, si no es el caso, revierte automáticamente a la composición de escritorio en el lado del servidor. Los dispositivos que cuentan con la capacidad de GPU necesaria, pero no cumplen las especificaciones de RAM o de velocidad del procesador, deben incluirse en el grupo del objeto de directiva de grupo (GPO) como dispositivos excluidos de la redirección de composición del escritorio.

El ancho de banda mínimo disponible es de 1,5 Mbps; el ancho de banda recomendado es de 5 Mbps. Estos valores incorporan la latencia de extremo a extremo.

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: Citrix Receiver para Windows, Citrix Receiver para iOS y Citrix Receiver 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 http://developer.nvidia.com/cuda/cuda-gpus.

Redirección de Flash de HDX

Se admiten los siguientes clientes y reproductores de Adobe Flash:

- Citrix Receiver para Windows (para las funcionalidades de redirección de Flash de segunda generación). Las funcionalidades de redirección de Flash de segunda generación requieren Adobe Flash Player for Other Browsers, también conocido como NPAPI (Netscape Plugin Application Programming Interface) Flash Player.
- Citrix Receiver para Linux (para las funciones de redirección de Flash de segunda generación). Las funciones de redirección de Flash de segunda generación requieren Adobe Flash Player para otros sistemas Linux o Adobe Flash Player para Ubuntu.
- Citrix Online Plug-in 12.1 (para las funciones antiguas de redirección de Flash). Las funciones antiguas de redirección de Flash requieren Adobe Flash Player para Windows Internet Explorer (a veces considerado un reproductor ActiveX).

El número de versión principal del reproductor de Flash en el dispositivo de usuario debe ser mayor o igual que el número de versión principal del reproductor de Flash en el servidor. Si se ha instalado una versión más antigua del reproductor de Flash en el dispositivo de usuario, o si no es posible instalar el reproductor de Flash en el dispositivo del usuario, el contenido Flash se genera en el servidor.

Las máquinas que ejecutan agentes VDA requieren:

- Adobe Flash Player para Windows Internet Explorer (el reproductor ActiveX)
- Internet Explorer 11 (no en el modo de interfaz Modern UI). Puede usar las versiones de 7 a 10 de Internet Explorer, pero Microsoft respalda (y Citrix recomienda usar) la versión 11. La redirección de Flash requiere Internet Explorer en el servidor; con otros exploradores, el contenido Flash se genera en el servidor.
- El modo protegido inhabilitado en Internet Explorer (Herramientas > Opciones de Internet > ficha Seguridad > casilla "Habilitar Modo protegido" no marcada). Reinicie Internet Explorer para realizar el cambio.

HDX 3D Pro

Cuando instala un VDA para SO de escritorio Windows, puede elegir instalar la versión HDX 3D Pro.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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 respaldadas (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 http://www.citrix.com/intel y http://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.
- Citrix Receiver debe estar instalado.

Para obtener más información, consulte 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 respaldados: Citrix Receiver para Windows, Citrix Receiver para Mac y Citrix Receiver para Linux.

Aplicaciones de conferencias de vídeo respaldadas:

- Adobe Connect
- Cisco WebEx

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrix GoToMeeting HDFaces
- Google+ Hangouts
- IBM Sametime
- Aplicaciones de vídeo basadas en Media Foundation en Windows 8.x, Windows Server 2012 y Windows Server 2012 R2
- Microsoft Lync 2010 y 2013
- Microsoft Office Communicator
- Microsoft Skype 6.7

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.
- Controladores de cámara Web, obtenidos del fabricante de la cámara, cuando sea posible.

Grabación de sesiones

Componentes de Administración de grabación de sesiones

Los componentes de Administración de grabación de sesiones (Base de datos de grabación de sesiones, Servidor de grabación de sesiones y Consola de directivas de grabación de sesiones) se pueden instalar en un mismo servidor o en servidores diferentes.

Base de datos de grabación de sesiones

Sistemas operativos respaldados:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Versiones compatibles de Microsoft SQL Server:

- Microsoft SQL Server 2016 SP1, ediciones Enterprise, Express y Standard
- Microsoft SQL Server 2014 SP2, ediciones Enterprise, Express y Standard
- Microsoft SQL Server 2012 SP3, ediciones Enterprise, Express y Standard
- Microsoft SQL Server 2008 R2 SP3, ediciones Enterprise, Express y Standard

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Requisito: .NET Framework 4.7, 4.6.2 o 4.5.2

Servidor de grabación de sesiones

Sistemas operativos respaldados:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Otros requisitos:

- Internet Information Services (IIS) 10, 8.5, 8.0 o 7.5
- .NET Framework 4.7, 4.6.2 o 4.5.2
- Si el servidor de Grabación de sesiones usa HTTPS como protocolo de comunicaciones, agregue un certificado válido. La grabación de sesiones utiliza HTTPS de manera predeterminada (recomendado por Citrix).
- Microsoft Message Queuing (MSMQ), con la integración en Active Directory inhabilitada y el respaldo para MSMQ HTTP habilitado
- Para la captura de registros de administrador: Última versión de Chrome, Firefox o Internet Explorer 11

Consola de directivas de grabación de sesiones

Sistemas operativos respaldados:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1

Requisito: .NET Framework 4.7, 4.6.2 o 4.5.2

Agente de grabación de sesiones

Instale el Agente de grabación de sesiones en cada uno de los servidores XenApp y XenDesktop donde desee grabar sesiones.

Sistemas operativos respaldados:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows 10
- Windows 8.1
- Windows 7 SP1

Requisitos:

- XenApp 7.15 o XenDesktop 7.15 con licencia Platinum
- XenApp 7.6.4000 o XenDesktop 7.6.4000 con licencia Platinum (solo VDA para SO de servidor Windows; VDA para SO de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

escritorio Windows no respaldados)
- .NET Framework 4.7, 4.6.2 o 4.5.2
- Microsoft Message Queuing (MSMQ), con la integración en Active Directory inhabilitada y el respaldo para MSMQ HTTP habilitado

Reproductor de grabación de sesiones

Sistemas operativos respaldados:

- Windows 10
- Windows 8.1
- Windows 7 SP1

Requisito: .NET Framework 4.7, 4.6.2 o 4.5.2

Para obtener los mejores resultados, instale el Reproductor de grabación de sesiones en una estación de trabajo con:

- Resolución de pantalla de 1024 x 768
- Profundidad de color de al menos 32 bits
- 2 GB de RAM mínimo. Disponer de más RAM y recursos de CPU/GPU puede mejorar el rendimiento cuando se reproducen grabaciones de uso intensivo de gráficos, especialmente cuando contienen muchas animaciones.

El tiempo de respuesta de la búsqueda depende del tamaño de la grabación y de las especificaciones de hardware de su máquina.

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 y 2012
- Windows Server 2008 R2 SP1

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 Aprovisionamiento de impresoras.

Otros

StoreFront 3.12.2000 es la versión mínima admitida en esta versión.Para usar la funcionalidad Preferencia de zonas, debe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

utilizar como mínimo StoreFront 3.12.2000 o posterior y NetScaler Gateway 11.0-65.x.

Al usar Provisioning Services con esta versión, la versión mínima compatible de Provisioning Services es la versión 7.15.3.

Solo se admite el servidor de licencias de Citrix 11.14.

La Consola de administración de directivas de grupo (GPMC) de Microsoft es necesaria si desea almacenar la información sobre directivas de Citrix en Active Directory en lugar de la base de datos de configuración de sitios. Si instala CitrixGroupPolicyManagement_x64.msi por separado (por ejemplo, en una máquina que no tiene instalado un componente principal de XenApp o XenDesktop), esa máquina debe tener instalada la biblioteca de tiempo de ejecución de Visual Studio 2015. Para más información, consulte la documentación de Microsoft.

Se admiten varias tarjetas de interfaz de red.

De forma predeterminada, se instala Citrix Receiver para Windows al instalar un VDA. Para obtener más información, consulte la documentación de Receiver para Windows.

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

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

Consulte la documentación de Autoservicio de restablecimiento de contraseñas para ver información de respaldo y requisitos.

Sistemas operativos que admiten la redirección de carpetas de cliente:

- Server: Windows Server 2008 R2 SP1, Windows Server 2012 y Windows Server 2012 R2
- Cliente (con la versión más reciente de Citrix Receiver 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 XenDesktop y XenApp. 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, 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 XenApp y XenDesktop no es compatible con AppDNA 7.8 ni AppDNA 7.9. Citrix recomienda usar la versión actual de AppDNA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Visión técnica general

Dec 05, 2017

En este artículo:

- Componentes clave de XenApp y XenDesktop
- ¿Cómo funciona una implementación típica?
- ¿Cómo se gestionan las conexiones de usuario?
- ¿Cómo funciona el acceso a los datos?
- Entrega de aplicaciones y escritorios: catálogos de máquinas, grupos de entrega y grupos de aplicaciones

XenApp y XenDesktop son soluciones de virtualización que proporcionan a los equipos de TI el control de máquinas virtuales, aplicaciones, licencias y seguridad, al tiempo que permiten un acceso desde cualquier lugar y cualquier dispositivo.

Con XenApp y XenDesktop:

- 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.

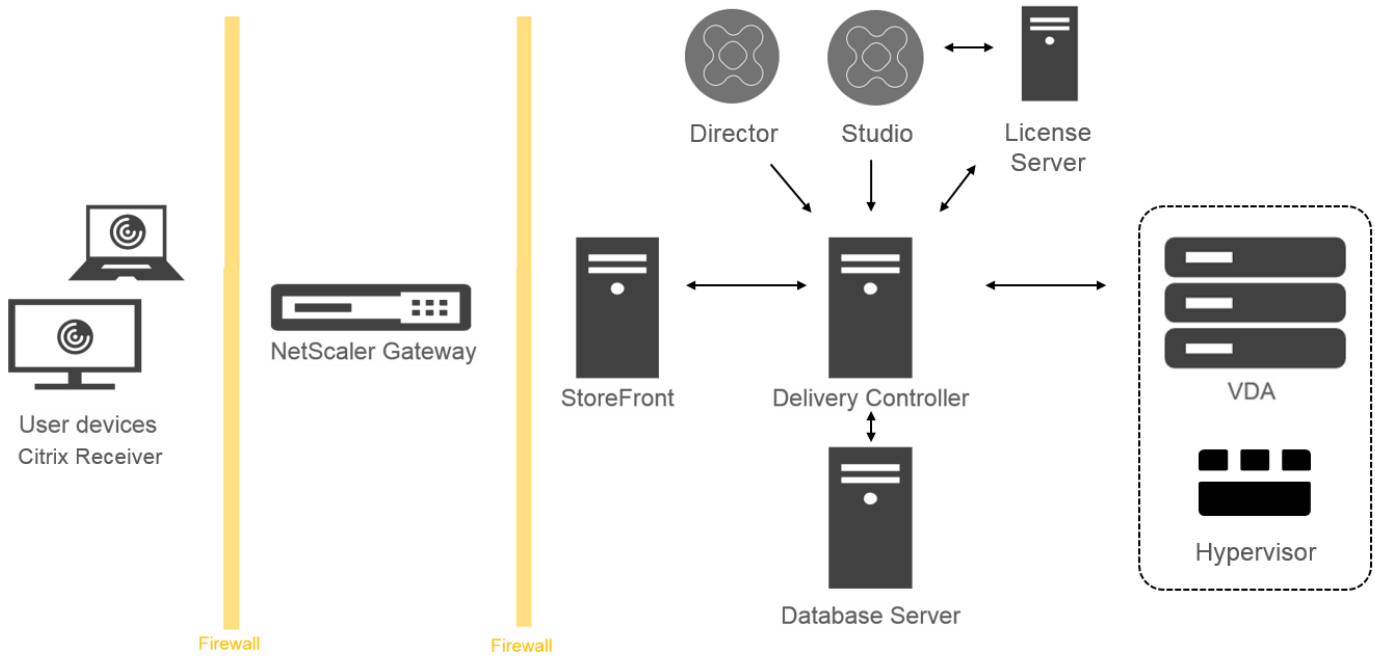
XenApp y XenDesktop comparten una arquitectura unificada llamada FlexCast Management Architecture (FMA). Las funciones principales de la arquitectura FMA son el aprovisionamiento integrado y la capacidad de ejecutar distintas versiones de XenApp o XenDesktop desde un único sitio.

Componentes clave de XenApp y XenDesktop

Sugerencia: Este artículo es muy útil si acaba de empezar a utilizar XenApp o XenDesktop. Si tiene una comunidad de XenApp 6.x o una versión anterior, o bien un sitio de XenDesktop 5.6 o una versión anterior, también debería consultar el artículo Cambios en 7.x.

En esta imagen, se muestran los componentes clave de una implementación típica de XenApp o XenDesktop, que se denomina "sitio".

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Delivery Controller

El Delivery Controller es el componente de administración central de los sitios de XenApp o XenDesktop. 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 máquinas virtuales alojadas en un hipervisor o un servicio de nube, los servicios de Controller se comunican con el hipervisor para distribuir aplicaciones y escritorios, autenticar y administrar el acceso de los usuarios, actuar como intermediarios en las conexiones entre los usuarios y sus aplicaciones y escritorios virtuales, optimizar y equilibrar las conexiones de los usuarios.

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 para que cada sitio de XenApp o XenDesktop almacene 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de configuración y una base de datos de supervisión. De forma predeterminada, se instalan en la misma ubicación que la base de datos del sitio; este aspecto no 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 podrán entregar 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, verifican que haya una licencia de Citrix disponible para el usuario o para 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 servidor al mismo tiempo. Los VDA para SO de escritorio Windows permiten la conexión de un solo usuario al escritorio en un momento dado. Un VDA de Linux también está disponible.

Citrix StoreFront

StoreFront autentica a los usuarios en los sitios que alojan los recursos, 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 hace un seguimiento de las suscripciones a aplicaciones de los usuarios, los nombres de los accesos directos y otros datos, para garantizar una coherencia de uso entre los distintos dispositivos.

Citrix Receiver

Se instala en los dispositivos de usuario y otros dispositivos de punto final (por ejemplo, escritorios virtuales). Citrix Receiver da a los usuarios un acceso rápido, seguro y de autoservicio a los documentos, las aplicaciones y los escritorios, desde cualquier dispositivo del usuario, incluidos smartphones, tabletas y PC. Citrix Receiver también ofrece acceso a petición a aplicaciones Windows, Web y de Software como servicio (SaaS). Para los dispositivos donde no se puede instalar el software de Citrix Receiver, Citrix Receiver para HTML5 ofrece una conexión a través de un explorador Web compatible con HTML5.

Citrix Studio

Studio es la consola de administración que permite configurar y administrar la implementación de XenApp y XenDesktop, lo que elimina la necesidad de consolas de administración separadas para gestionar la entrega de aplicaciones y escritorios. Studio incluye varios asistentes que funcionan como guía 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.

© 1999-2017 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 XenApp o XenDesktop.

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.
- Datos sobre el tráfico HDX (también conocido como tráfico ICA) capturados por HDX Insight desde NetScaler, si el entorno incluye un dispositivo NetScaler y la edición de XenApp o XenDesktop incluye HDX Insight.

También puede ver sesiones de usuario e interactuar con ellas mediante Director utilizando la Asistencia remota de Windows.

Citrix License Server

El servidor de licencias administra las licencias de los productos Citrix. Se comunica con el Controller para administrar las licencias para cada sesión de usuario, y con Studio, para asignar los archivos de licencias. Debe crear 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 XenApp y XenDesktop. Un hipervisor se instala en un host dedicado enteramente a ejecutar el hipervisor y alojar máquinas virtuales.

XenApp y XenDesktop respaldan una serie de servicios de nube o de hipervisor.

Aunque la mayoría de las implementaciones de XenApp y XenDesktop requieren un hipervisor, este no se necesita para ofrecer acceso con Remote PC ni cuando usa Provisioning Services (incluido con algunas ediciones de XenApp y XenDesktop) en lugar de Machine Creation Services (MCS) para aprovisionar las máquinas virtuales.

Para obtener más información sobre:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Puertos, consulte Puertos de red.
- Bases de datos, consulte Bases de datos.
- Servicios Windows en los componentes de XenApp y XenDesktop, consulte Configurar derechos de usuario.
- Hipervisores y servicios de nube respaldados, consulte Requisitos del sistema.

Componentes adicionales

Los siguientes componentes adicionales, no incluidos en la imagen anterior, también pueden incluirse en las implementaciones de XenApp o XenDesktop. Para obtener más información, consulte la documentación correspondiente.

Provisioning Services (PVS)

Provisioning Services es un componente optativo de XenApp y XenDesktop, 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 al dispositivo de usuario. Provisioning Services no requiere un hipervisor para hacerlo, por lo tanto, se puede usar para alojar máquinas físicas. Si el sitio tiene Provisioning Services, este se comunica con el Controller para proporcionar recursos a los usuarios.

NetScaler Gateway

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

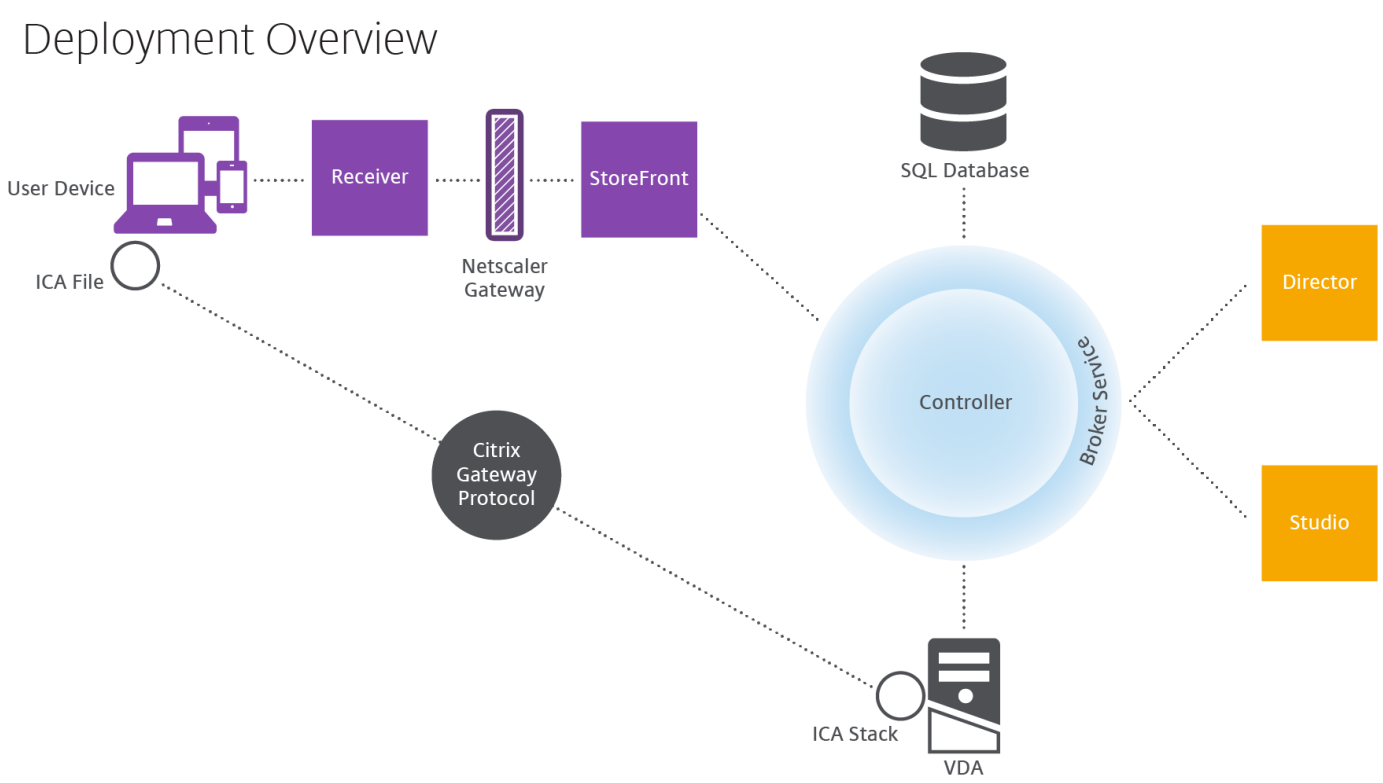
NetScaler SD-WAN

En las implementaciones donde se entregan escritorios virtuales a usuarios de ubicaciones remotas, como sucursales de oficina, se puede emplear la tecnología de Citrix NetScaler SD-WAN (antes llamado Citrix CloudBridge, Branch Repeater o WANScaler) para optimizar el rendimiento. Repeater acelera el rendimiento de las redes de área extensa (WAN), de modo que, al incluirlos en la red, los usuarios de las sucursales pueden experimentar un rendimiento similar al de una red local (LAN) en la red WAN. NetScaler SD-WAN puede dar prioridad a diferentes partes de la experiencia de usuario de modo que, por ejemplo, no se empeore la misma en la sucursal donde se envía 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 de XenApp y XenDesktop 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 de XenApp o de XenDesktop se compone de máquinas de servidor y escritorio con VDA instalado, y Delivery Controller, que se encarga de administrar el acceso.

© 1999-2017 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 más Controllers y, puesto que 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 en el sitio mediante StoreFront, sus credenciales se transfieren al Broker Service ubicado en el Controller, el cual obtiene sus perfiles y los recursos que estén disponibles a partir de las directivas configuradas para ellos.

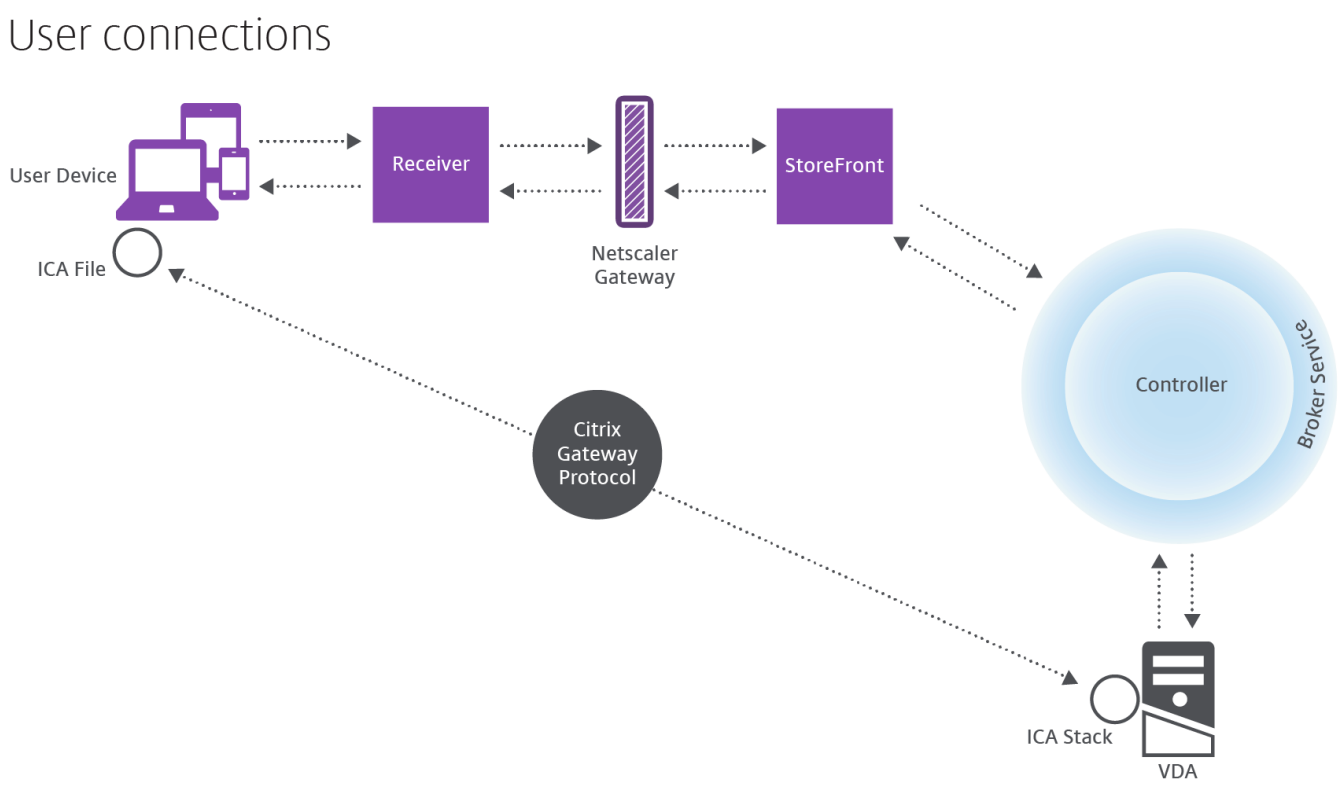
¿Cómo se gestionan las conexiones de usuario?

Para iniciar una sesión de XenApp o XenDesktop, el usuario se conecta a través de Citrix Receiver, instalado en el dispositivo del usuario, o bien a través de un sitio de Citrix Receiver para 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 Citrix Receiver.

© 1999-2017 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 escritorios disponibles se envía de vuelta al usuario a través de la ruta StoreFront-Citrix Receiver. Cuando el usuario selecciona las aplicaciones o los escritorios en esta lista, esa información vuelve por la misma ruta al Controller, que 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 Citrix Receiver. En StoreFront, se recopila un conjunto de parámetros requeridos. A continuación, estos parámetros se envían a Citrix Receiver, ya sea como parte de la conversación del protocolo de Receiver-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: Citrix Receiver, StoreFront y Controller.

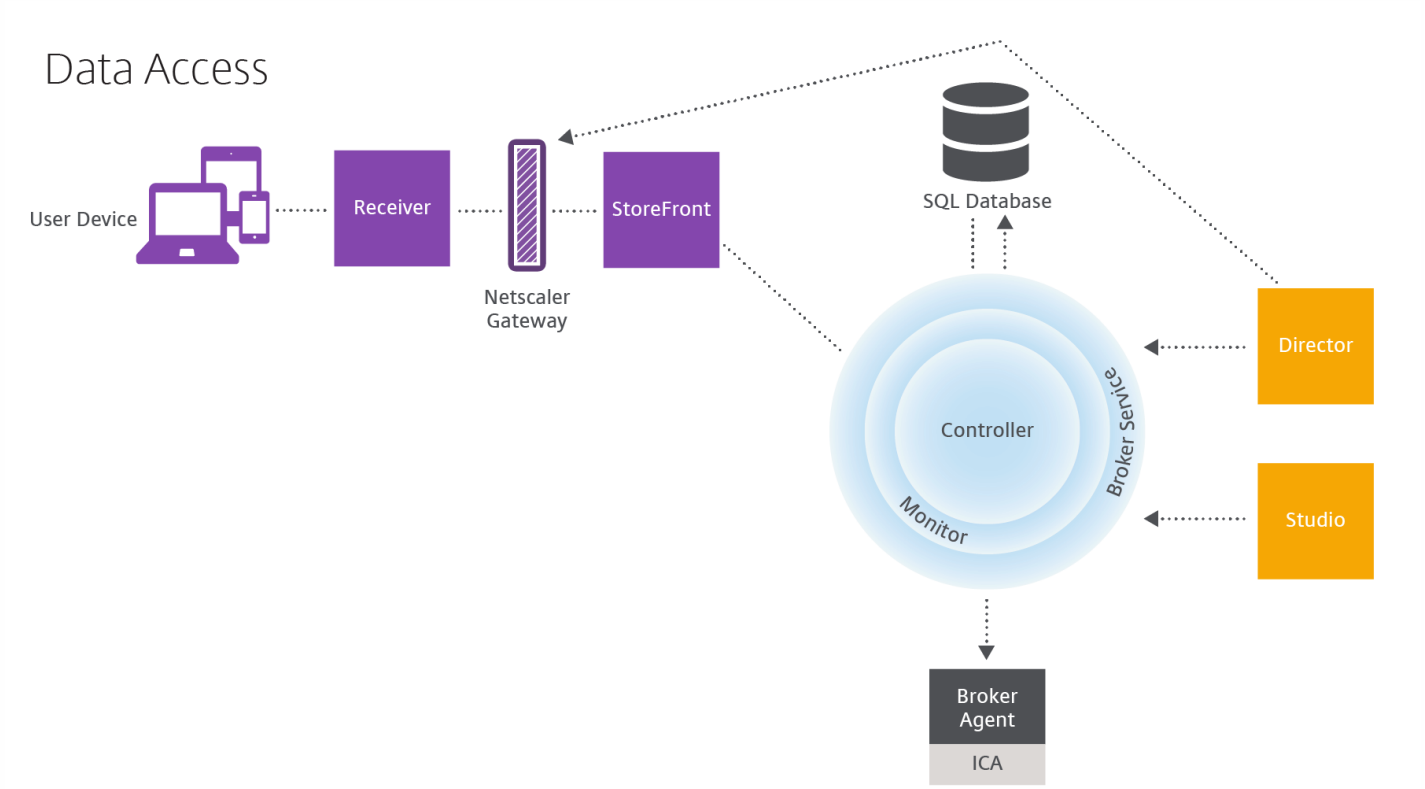
La conexión entre Citrix Receiver y el VDA usa el protocolo CGP (Citrix Gateway Protocol). Si la conexión se pierde, la funcionalidad de fiabilidad de la sesión habilita al usuario para reconectar con el VDA en lugar de tener que reiniciarse a través de toda la infraestructura de administración. La fiabilidad de la sesión se puede habilitar o inhabilitar en las directivas de Citrix.

Cuando el cliente se ha conectado al VDA, el VDA notifica al Controller que el usuario ha iniciado una sesión, y el Controller envía esta información a la base de datos del sitio y empieza a registrar datos en la base de datos de supervisión.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

¿Cómo funciona el acceso a los datos?

Cada sesión de XenApp o XenDesktop 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 mejor los sitios. Director accede a los mismos datos en tiempo real, además de acceder a datos históricos almacenados en la base de datos de supervisión y datos de HDX procedentes de NetScaler Gateway para facilitar la solución de problemas y la 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 NetScaler Gateway para obtener información sobre los datos de HDX.

Entrega de aplicaciones y escritorios: catálogos de máquinas, grupos de entrega y grupos de aplicaciones

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

catálogos) y qué usuarios pueden acceder a ellos.

Catálogos de máquinas

Los catálogos de máquinas son colecciones de máquinas virtuales o físicas 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 (PVS o MCS) 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 de SO de servidor**. Máquinas físicas o virtuales basadas en un sistema operativo de servidor, que se utilizan para entregar aplicaciones publicadas de XenApp, también conocidas como aplicaciones alojadas en servidores, y escritorios publicados de XenApp, también conocidos como escritorios alojados en servidores. Estas máquinas permiten que varios usuarios se conecten a ellas simultáneamente.
- **Máquinas de SO de escritorio**. Máquinas físicas o virtuales basadas en un sistema operativo de escritorio, que se utilizan para entregar escritorios VDI (escritorios que ejecutan sistemas operativos de escritorio que pueden personalizarse totalmente con ayuda de opciones), aplicaciones alojadas en VM (aplicaciones de sistemas operativos de escritorio) y escritorios físicos alojados. Solo un usuario a la vez puede conectar con cada uno de estos escritorios.
- **Acceso con Remote PC**. Permite a usuarios remotos acceder a sus equipos físicos de oficina desde cualquier dispositivo que ejecute Citrix Receiver. Los equipos de oficina se administran a través de la implementación de XenDesktop, y requieren que los dispositivos de usuario se incluyan en una lista blanca.

Para obtener más información, consulte el artículo Crear catálogos de máquinas.

Grupos de entrega

Los grupos de entrega especifican los usuarios que pueden acceder a las aplicaciones y/o los escritorios y las máquinas que se pueden utilizar para ello. Los grupos de entrega contienen máquinas del catálogo de máquinas y usuarios de Active Directory que tienen acceso al sitio. A menudo, tiene sentido asignar usuarios a los grupos de entrega según su grupo de Active Directory, 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 de máquinas y cada catálogo de máquinas puede suministrar sus máquinas a más de un grupo de entrega, pero 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, una manera de hacerlo consiste en instalar todas las aplicaciones que se quieren entregar 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, se configura cada grupo de entrega para que entreguen distintos subconjuntos de esas aplicaciones instaladas en las máquinas.

Para obtener más información, consulte el artículo Crear grupos de entrega.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 el artículo Crear grupos de aplicaciones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Active Directory

Dec 05, 2017

Para la autenticación y la autorización es necesario usar Active Directory. La infraestructura de Kerberos en Active Directory se usa para garantizar la autenticidad y confidencialidad de las comunicaciones con los Delivery Controllers. Para obtener más información sobre Kerberos, consulte la documentación de Microsoft.

En el artículo Requisitos del sistema, se ofrece una lista de los niveles funcionales admitidos para el dominio y el bosque. Para usar el modelado de directivas, el controlador de dominio 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 Agents (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 más información acerca de este método de detección, consulte el artículo Delivery Controllers y CTX118976.

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

Implementación en un entorno de Active Directory de varios bosques

Nota: Esta información es aplicable a XenDesktop 7.1 y XenDesktop 7.5, como 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. Para obtener más información acerca de este asistente, consulte la documentación de Microsoft.

No se necesitan zonas DNS inversas en la infraestructura DNS si se incluyen los reenviadores DNS adecuados entre los bosques.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

- 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 de 32 bits o 64 bits, localice la clave del Registro HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs
  - Nombre: ListOfSIDs
  - Tipo: REG_SZ
  - Datos: identificador de seguridad (SID) de los Controllers

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

1. Localice el archivo \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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tipo de confianza	Transitividad	Dirección	Se admite en esta versión
Acceso directo	Transitiva	Unidireccional o bidireccional	SI
Dominio	Transitiva o no transitiva	Unidireccional o bidireccional	NO

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Bases de datos

Dec 05, 2017

Un sitio de XenApp o XenDesktop utiliza 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 del 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; es necesaria 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 base de datos del sitio debe estar siempre en la zona principal. 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**. 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 http://msdn.microsoft.com/en-us/library/hh510230.
- **Imagen reflejo de la base de datos de SQL Server**. Reflejar la base de datos garantiza que, si se pierde la conexión con el servidor de base de datos activo, el proceso automático de conmutación por error se produzca rápidamente (en cuestión de segundos) para que los usuarios en general no resulten afectados. No obstante, este método es más costoso que las soluciones alternativas, ya que se requieren licencias de SQL Server completas en cada servidor de base de datos; tenga en cuenta que no se puede usar SQL Server Express en un entorno reflejado.
- **Agrupación en clústeres de SQL**. La tecnología de agrupación en clústeres de SQL de Microsoft se puede usar para permitir automáticamente que un servidor tome el control de las tareas y las responsabilidades de otro servidor que ha fallado. No obstante, la instalación de esta solución es más complicada y el proceso automático de conmutación por error generalmente es más lento que con las soluciones alternativas como la creación de reflejo de SQL.
- **Con las funciones de alta disponibilidad del hipervisor**. Con este método, usted implementa la base de datos como

© 1999-2017 Citrix Systems, Inc. All rights reserved.

una máquina virtual y utiliza 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.

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

La función de 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 el artículo 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). Esta función solo debe utilizarse 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.

Instalación del 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 regla general, esa acción predeterminada es suficiente para implementaciones piloto o de prueba de concepto. Sin embargo, SQL Server Express no admite las funciones de alta disponibilidad de Microsoft.

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

Si es necesario, puede seleccionar**Ocultar instancia** para la instancia de la base de datos. Al configurar la dirección de la base de datos en Studio, introduzca el número de puerto estático de la instancia, en lugar de su nombre. Consulte la documentación de Microsoft para obtener información más detallada sobre cómo ocultar una instancia del motor de base de datos de SQL Server.

Por lo tanto, la mayoría de las implementaciones de producción y cualquier implementación que use funciones de alta disponibilidad de Microsoft, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 más adelante los *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, se puede usar la opción automática si usted (como usuario de Studio y administrador Citrix) tiene los privilegios de base de datos pertinentes; consulte más adelante el apartado Permisos necesarios para configurar bases de datos.

Después de crear el sitio, puede cambiar la ubicación de una base de datos. Para ello, consulte el apartado *Cambiar ubicaciones de bases de datos* que se muestra más adelante.

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.

Sugerencia: Para verificar la creación de la base de datos reflejada después de crear el sitio, ejecute el cmdlet de PowerShell **get-configdbconnection** para comprobar que el asociado de conmutación por error se ha definido en la cadena de conexión a 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 el artículo de Delivery Controllers.

Configuración automática

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

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

Configuración por script

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

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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.
- Si quiere usar las funciones de alta disponibilidad, deberá configurarlas.
- Para configurar la creación de reflejo, primero debe configurar la base de datos para que use el modelo de recuperación completa (a diferencia del modelo simple, que es el valor predeterminado). Haga una copia de seguridad de la base de datos principal en un archivo y cópielo al servidor reflejado. En la base de datos reflejada, restaure el archivo de copia de seguridad para el servidor reflejado. A continuación, inicie la creación de reflejo en el servidor principal.

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

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

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

Permisos necesarios para configurar bases de datos

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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Actualizar un esquema	Aplica revisiones o actualizaciones a los esquemas		db_owner

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

Cuando se 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:

- NombreServidor
- NombreServidor\NombreInstancia
- NombreServidor,NúmeroPuerto

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

Cambio de ubicaciones de bases de datos

Después de crear un sitio, se puede cambiar la ubicación de las bases de datos. Cuando se cambia 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 la base de datos automáticamente. Studio intenta acceder a la base de datos usando sus credenciales; si eso falla, se le pedirán las credenciales del usuario de la base de datos. Studio carga el esquema de base de datos en la base de datos. Las credenciales se conservan solo durante el 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Para obtener más información

Los artículos de la sección Conceptos avanzados contienen artículos de mayor profundidad y contenido técnico provenientes de los distintos equipos de Citrix. Por ejemplo:

- La colección Diseño contiene un artículo referente a una herramienta para calcular el tamaño de las bases de datos.
- Las colecciones Implementación y Configuración contienen una guía para establecer el tamaño de la base de datos del sitio y configurar las cadenas de conexión cuando se utilizan soluciones de alta disponibilidad de SQL Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Métodos de entrega

Dec 05, 2017

Puede resultar complicado satisfacer las necesidades de cada usuario de la organización a partir de una única implementación de virtualización. XenApp y XenDesktop permiten a los administradores personalizar la experiencia del usuario con una variedad de métodos también conocidos como modelos FlexCast.

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

Adaptación de las aplicaciones Windows en dispositivos móviles

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

XenApp con Citrix Receiver 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 de aplicaciones publicadas de XenApp 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, las funciones de GPS y la cámara. Muchas funciones táctiles están disponibles de forma nativa en XenApp y XenDesktop, 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

Reducción del coste de actualización de los PC

La actualización de equipos físicos es una tarea complicada que muchos negocios afrontan cada período de 3 a 5 años, especialmente si el negocio necesita mantener sus sistemas operativos y aplicaciones al día. Los negocios en crecimiento también se enfrentan a 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, al mismo tiempo que se usan 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenDesktop y XenApp, 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 puntero, sonido y actualizaciones de pantalla. Al mantener estos recursos en un centro de datos, XenDesktop y XenApp 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 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.

Aceleración de 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 Citrix Receiver en la máquina virtual actualizada, sin encontrar 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 servicio de asistencia.

Otras ventajas adicionales de usar XenDesktop durante la migración son:

- 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 de XenDesktop 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, compartir 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.

Transformación de los centros de llamadas

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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

coste mínimo, cuando se quiere aprovisionar escritorios a una gran cantidad de 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 en XenApp 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 de XenApp, los usuarios no pueden instalar aplicaciones, ni cambiar los parámetros del sistema, ni reiniciar el servidor.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aplicaciones y escritorios publicados de XenApp

Mar 21, 2018

Use máquinas de SO de servidor para entregar aplicaciones publicadas de XenApp y escritorios publicados de XenApp.

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.
- 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.

Procesamiento, alojamiento y entrega de aplicaciones

- El procesamiento de las aplicaciones tiene lugar en las máquinas que las alojan (hosts), en lugar de procesarse en los dispositivos de usuario. Estas máquinas host pueden ser físicas o virtuales.
- Las aplicaciones y los escritorios residen en una máquina de SO de servidor.
- Las máquinas están disponibles a través de los catálogos de máquinas.
- Las máquinas incluidas en catálogos de máquinas 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.

Administración de sesiones y asignación

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Para entregar aplicaciones y escritorios publicados de XenApp:

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aplicaciones alojadas en VM (VM Hosted Apps)

Dec 05, 2017

Uso de 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.
- 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.

Administración de sesiones y asignación

- 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de máquinas, decida si desea que los usuarios se conecten a una nueva VM cada vez que inicien una sesión o que se conecten a la misma máquina 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Escritorios VDI

Dec 05, 2017

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 XenApp, 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, debe 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 única imagen maestra. Todos los cambios realizados en el escritorio se pierden cuando la máquina se reinicia.
- Escritorio estático no persistente. La primera vez que un usuario inicia una sesión para usar uno de estos escritorios, el usuario recibe un escritorio de un grupo de escritorios basados en una única 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 cuando la máquina se reinicia.
- 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 única 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Puertos de red

Mar 21, 2018

La tabla siguiente enumera los puertos de red predeterminados utilizados por los Delivery Controllers de XenApp y XenDesktop, 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 obtener 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 Provisioning Services, consulte el artículo actual "Requisitos del sistema" del componente en cuestión.

La tabla solo enumera 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). Para ver información sobre estas asignaciones, consulte http://www.iana.org/assignments/port-numbers; no obstante, la información descriptiva que guarda IANA no siempre refleja el uso que se les da hoy en día.

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

Componente	Uso	Protocolo	Puertos de entrada predeterminados	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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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	Todos los Citrix Receivers
VDA	ICA/HDX sobre WebSocket	TCP	8008	Citrix Receiver para HTML5 y Citrix Receiver para Chrome 1.6 y versiones anteriores solamente
VDA	Transporte de audio en tiempo real ICA/HDX sobre UDP	UDP	16500...16509	
VDA	ICA/HDX Framehawk	UDP	3224-3324	
VDA	ICA/Universal Print Server	TCP	7229	Utilizado por el agente de escucha del protocolo CGP para el flujo de datos de impresión proveniente de Universal Print Server.
VDA	ICA/Universal Print Server	TCP	8080	Utilizado por el agente de escucha de Universal Print Server para solicitudes HTTP/SOAP entrantes.
VDA	Wake On LAN	UDP	9	Administración de energía de Acceso con Remote PC
VDA	Proxy de reactivación	TCP	135	Administración de energía de Acceso con Remote PC
VDA	Delivery Controller	TCP	80	
Delivery	VDA, StoreFront, Director,	TCP	80	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Controller	Studio			
Delivery Controller	StoreFront, Director, Studio sobre TLS	TCP	443	
Delivery Controller	Delivery Controller, VDA	TCP	89	Memoria caché del host local (Este uso del puerto 89 podría cambiar en versiones futuras.)
Delivery Controller	Orchestration	TCP	9095	Orchestration
Director	Delivery Controller	TCP	80, 443	

Para Citrix Licensing:

Componente	**Uso**	**Protocolo**	**Puertos de entrada predeterminados**	Notas
License Server	License Server	TCP	27 000	
License Server	License Server para Citrix (demonio de proveedor)	TCP	7279	
License Server	License Administration Console	TCP	8082	
License Server	Web Services for Licensing	TCP	8083	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX

Dec 05, 2017

> ## 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Citrix HDX incluye una gran gama de tecnologías que ofrecen una experiencia de usuario de alta definición.

En el dispositivo

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

En la red

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

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

En el centro de datos

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

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

HDX Insight 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.

Para experimentar con las capacidades HDX en su escritorio virtual:

- Para ver cómo la redirección de Flash, una de las tres tecnologías HDX de redirección multimedia, acelera la entrega de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

contenido multimedia Flash:

1. Descargue Adobe Flash Player (http://get.adobe.com/flashplayer/) e instálelo tanto en el escritorio virtual como en el dispositivo del usuario.
2. En la barra de herramientas de Desktop Viewer, seleccione **Preferencias**. En el cuadro de diálogo Preferencias de Desktop Viewer, seleccione la ficha **Flash** y seleccione **Optimizar el contenido**.
3. Para ver cómo la redirección de Flash acelera la entrega de contenido multimedia Flash a los escritorios virtuales, vea un vídeo en su escritorio desde un sitio Web que contenga vídeos Flash, como YouTube. La redirección de Flash se ejecuta de forma silenciosa, de modo que los usuarios no notan cuándo está teniendo lugar. Puede comprobar si se usa la redirección de Flash. Si es así, verá un bloque de color que aparecerá momentáneamente antes de que se inicie Flash Player, o bien, haga clic con el botón secundario en el vídeo y busque "Redirección de Flash" en el menú.

- Vea cómo HDX entrega sonido de alta definición:
  1. Configure el cliente Citrix con la máxima calidad de sonido; consulte la documentación de Citrix Receiver para obtener más información.
  2. Reproduzca archivos de música con 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 por el servidor cuando la redirección multimedia no está disponible: vea un vídeo de un sitio Web que contiene vídeos de alta definición, como http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/.

Tenga en cuenta:

- 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 aún 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 y las configuraciones de directivas Citrix, consulte la documentación de las directivas de 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Limitación

Cuando usa Windows Media Player con Remote Audio & Video Extensions (RAVE) habilitado dentro de una sesión, si hace

© 1999-2017 Citrix Systems, Inc. All rights reserved.

clic con el botón secundario en el vídeo y selecciona **Reproducción en curso siempre visible**, aparece una pantalla en negro.

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 producen las reconexiones.
- **Aplicaciones.** La ventana de sesión se cierra y aparece un diálogo que contiene 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:

- **Escritorios.** La ventana de sesión se vuelve transparente y aparece un temporizador de cuenta atrás que muestra el tiempo hasta que se producen 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 transparencia 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.

Modo tableta para dispositivos de pantalla táctil

De forma predeterminada, cualquier dispositivo táctil que se conecte o se mueva por roaming a un VDA de Windows 10 se inicia en modo tableta.

El modo tableta requiere al menos la versión 7.2 de XenServer. XenServer 7.2 se integra con el VDA de XenDesktop, 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 más información, consulte http://docs.citrix.com/content/dam/docs/en-us/xenserver/current-release/downloads/xenserver-release-notes.pdf.

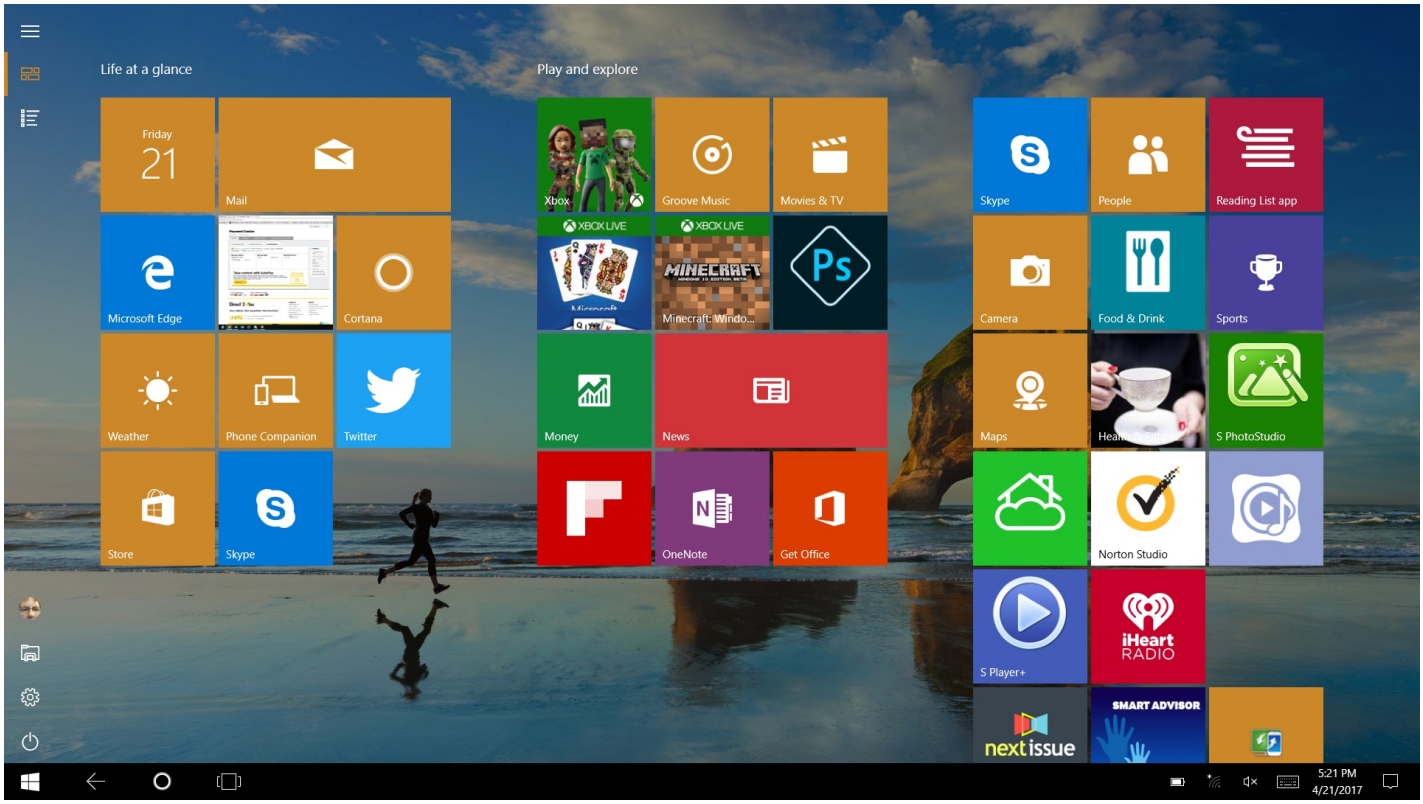
El modo tableta ofrece una interfaz de usuario que se adapta mejor a las pantallas táctiles:

- 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.

Receiver para Web no admite el modo tableta.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Ejecute el comando CLI de XenServer para permitir el cambio entre equipo portátil y tableta:

xe vm-param-set uuid= platform:acpi_laptop_slate=1

Para habilitar o inhabilitar el modo tableta, configure este parámetro del Registro en XenApp y XenDesktop:

HKEY_LOCAL_MACHINE\Software\Citrix\Sessions

Nombre: CitrixEnhancedUserExperience
Type: REG_DWORD

Valor:
0 (Inhabilitar)
1 (Habilitar)

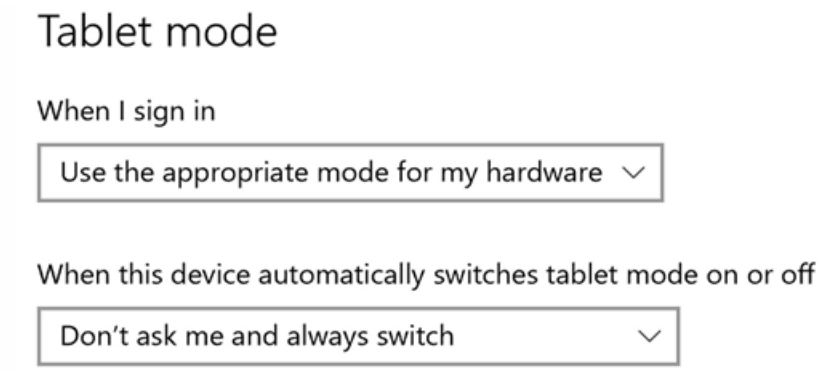
Antes de iniciar una sesión

Antes de iniciar sesión, se recomienda que vaya a **Configuración > Sistema > Modo tableta** en el VDA y establezca las siguientes opciones en los menús de lista desplegable:

- Usar el modo adecuado para mi hardware
- No preguntarme y cambiar siempre

Si no configura estas opciones antes de iniciar la sesión, configúrelas después de iniciar la sesión y reinicie el VDA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Mejora de la calidad de imagen enviada a los dispositivos de usuario

Las siguientes configuraciones de directiva de presentación visual controlan la calidad de las imágenes que se envían desde los escritorios virtuales a los dispositivos de los usuarios.

- Calidad visual. Controla la calidad visual de las imágenes que se muestran en el dispositivo de usuario: media, alta, siempre sin pérdida, gradual sin pérdida (la opción predeterminada es media). La calidad real del vídeo con la configuración predeterminada media depende del ancho de banda disponible.
- Velocidad de fotogramas de destino. Especifica la cantidad máxima de fotogramas por segundo que se envían desde el escritorio virtual al dispositivo de usuario (la opción predeterminada es 30). Para dispositivos que tienen unidades CPU lentas, especifique un valor bajo para mejorar la experiencia de usuario. La velocidad máxima permitida es de 60 fotogramas por segundo.
- Límite de memoria de presentación. Especifica el tamaño máximo de búfer para vídeos de la sesión en kilobytes (la opción predeterminada es 65536 KB). Para las conexiones que requieran mayor profundidad de color y mayor resolución, aumente el límite. Puede calcular la memoria máxima necesaria.

Mejora del rendimiento de videoconferencia

Se han optimizado varias aplicaciones conocidas de videoconferencia para la entrega de XenApp y XenDesktop 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 Citrix Receiver pueden anular este comportamiento predeterminado. Para ello, deben seleccionar la configuración **No usar mi micrófono ni mi cámara Web** de Micro y cámara Web en 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si una cámara Web es compatible con la codificación por hardware H.264, 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 (en tiempo real, interactivo, de fondo y en masa) y dos secuencias UDP (para voz y para las pantallas remotas de Framehawk) que están disponibles para transportar el tráfico ICA entre el dispositivo de usuario y el servidor. 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.

Precaución: 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 sobre 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 configurar este parámetro. 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) deseado.
- Configuración de usuario para multisecuencia. Esta configuración está inhabilitada de forma predeterminada.

Para que las directivas que contienen estas configuraciones tengan efecto, los usuarios deben cerrar la sesión y después volver a iniciar una sesión en la red.

Información relacionada

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Graphics
- Multimedia
- General content redirection
- Adaptive transport

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Transporte adaptable

Apr 12, 2018

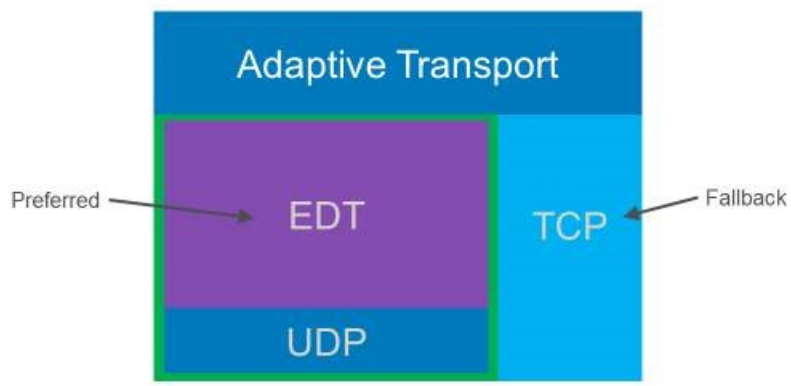
Introducción

El transporte adaptable es un nuevo mecanismo de transporte de datos para XenApp y XenDesktop. Es más rápido, más 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 nuevo 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. El mismo parámetro se aplica 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).

De forma predeterminada, la funcionalidad Enlightened Data Transport está **desactivada** y se usa siempre TCP.

Para realizar pruebas, se puede establecer **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 XenApp y XenDesktop.

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. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Requisitos y consideraciones

- XenApp y XenDesktop: como mínimo la versión 7.13
- VDA para SO de escritorio: como mínimo la versión 7.13
- VDA para SO de servidor: versión mínima 7.13
- StoreFront: como mínimo la versión 3.9
- Citrix Receiver para Windows: como mínimo la versión 4.7
- Citrix Receiver para Mac: como mínimo la versión 12.5
- Citrix Receiver para iOS: como mínimo la versión 7.2
- Citrix Receiver para Linux: versión 13.6 para solamente conexiones directas de VDA, y versión 13.7 para el respaldo DTLS cuando se usa NetScaler Gateway (o DTLS para conexiones directas de VDA)
- Citrix Receiver para Android: versión 3.12.3 solamente para conexiones directas de VDA, y versión 3.13 para el respaldo DTLS cuando se usa NetScaler Gateway (o DTLS para conexiones directas de VDA)
- Solo agentes VDA IPv4. No se admiten configuraciones de IPv6 ni mixtas (de IPv4 e IPv6).
- NetScaler: como mínimo la versión 11.1-51.21 Para obtener más información sobre la configuración de NetScaler, consulte Configuración de NetScaler Gateway para admitir el transporte avanzado.

Configuración

1. Instalar XenApp y XenDesktop.
2. Instalar StoreFront.
3. Instale el VDA (para SO de escritorio o SO de servidor).
4. Instale Citrix Receiver para Windows (Citrix Receiver para Mac o Citrix Receiver para iOS).
5. En Studio, habilite la configuración de directiva de transporte adaptable HDX (inhabilitada de forma predeterminada). Asimismo, se recomienda no habilitar esta funcionalidad como una directiva universal para todos los objetos del sitio.
   - Para habilitar este parámetro 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.
     - **Desactivado.** Se obliga el uso de TCP y EDT está inhabilitado.
6. Haga clic en Siguiente y siga los pasos indicados en el asistente.
7. 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 el parámetro de directiva al servidor, pero el usuario seguirá teniendo que reconectarse a la sesión ICA.
8. Inicie sesión desde un Citrix Receiver compatible para establecer conexión mediante el transporte adaptable.
9. Para un acceso externo seguro, configure el cifrado de DTLS en NetScaler Unified Gateway. Para obtener más información, consulte Configuración de NetScaler Gateway para admitir el transporte avanzado.

Para confirmar que el parámetro de directiva ha surtido efecto:

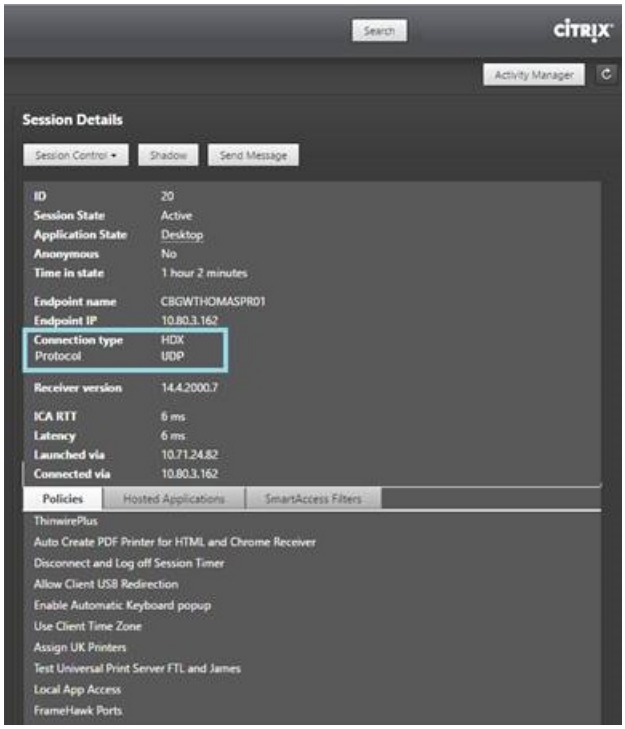
- Compruebe que los servicios User Datagram Protocol (UDP) de ICA están habilitados en un agente VDA mediante **netstat -a**.
- Compruebe que los canales virtuales se están ejecutando en EDT: use **Director** o la utilidad de línea de comandos **CtxSession.exe** disponible en el VDA.

Ejemplo con Director

En Director, **Detalles de la sesión > Tipo de conexión** muestra los parámetros 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 respaldo o

© 1999-2017 Citrix Systems, Inc. All rights reserved.

predeterminado. Si el tipo de conexión es **RDP**, no se usa ICA y el protocolo es **n/d**. Para obtener más información, consulte Supervisión de sesiones.



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
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación y configuración

Dec 05, 2017

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 el siguiente orden para implementar XenApp o XenDesktop.

Preparación

Consulte el artículo Antes de la instalación, 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 programas de instalación, las herramientas y las interfaces disponibles.

Instalación de 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.

Creación de un sitio

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

Instalación de 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 Instalación de agentes VDA o Instalación mediante línea de comandos.Se ofrecen scripts de ejemplo si quiere instalar agentes VDA a través de Active Directory.

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

Para implementaciones de acceso con Remote PC, instale un VDA para SO de escritorio en cada PC de la oficina. Si necesita solamente los servicios principales del agente VDA, utilice el programa de instalación independiente VDAWorkstationCoreSetup.exe y sus métodos existentes de distribución electrónica de software (ESD). (Antes de la instalación contiene información completa sobre los programas de instalación de VDA disponibles.)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de componentes opcionales

Si va a usar el servidor Citrix Universal Print Server, instale su componente de servidor correspondiente en los servidores de impresión. Consulte Instalación de componentes principales o Instalación 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. Consulte la documentación del Autoservicio de restablecimiento de contraseñas para obtener más información.

Si lo prefiere, puede integrar otros componentes de Citrix en la implementación de XenApp o XenDesktop.

- Provisioning Services es un componente optativo de XenApp y XenDesktop que aprovisiona máquinas mediante la transmisión por streaming de una imagen maestra a dispositivos de destino.
- Citrix NetScaler 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 NetScaler SD-WAN es un conjunto de dispositivos que optimizan el rendimiento en WAN.

Para obtener instrucciones para la instalación, consulte la documentación para estos componentes, funciones y tecnologías.

Creación de un catálogo de máquinas

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

Un catálogo puede contener máquinas físicas o virtuales (VM). Las máquinas virtuales se pueden crear a partir de una imagen maestra. Si usa un hipervisor 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.

Creación de 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.

Creación de grupos 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Antes de la instalación

Mar 01, 2018

La implementación de XenApp y XenDesktop comienza con la instalación de los siguientes componentes. Este proceso prepara para 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, NetScaler. Para una introducción al uso de NetScaler con StoreFront, consulte Integrar XenApp y XenDesktop con NetScaler Gateway.

¿Cómo instalar los componentes?

Puede usar el instalador de producto completo de XenApp y XenDesktop, 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 y Provisioning Services. Para obtener más información, consulte Instalar agentes VDA mediante scripts.

Como una alternativa automatizada frente a los instaladores, Citrix Smart Tools utiliza modelos ("blueprints") para crear una implementación de XenApp y XenDesktop. Para obtener más información, consulte la documentación de producto de Smart Tools.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 compatibles. 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.

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 en Windows Server 2012 R2 o un VDA en Windows 8.1 o 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.

La guía de optimización para máquinas con Windows 10 está disponible 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.

Permisos y requisitos de Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

- En el artículo Requisitos del sistema, se ofrece una lista de los niveles funcionales que admite 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 componentes de XenApp o XenDesktop en un controlador de dominio.
- No use barras diagonales (/) cuando indique nombres de unidades organizativas en Studio.

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

Para obtener más información:

- Recomendaciones referentes a la seguridad
- Administración delegada
- Documentación de Microsoft con instrucciones de 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 programa de instalación 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 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 más información acerca de estos programas, consulte Citrix Insight Services.

Durante la instalación de VDA:

Citrix Receiver para Windows se incluye de forma predeterminada cuando se instala un VDA (excepto cuando se usa el instalador VDAWorkstationCoreSetup.exe). Citrix Receiver se puede excluir de la instalación. Usted o sus usuarios pueden descargarse e instalar (y actualizar) Citrix Receiver y otros Citrix Receivers desde el sitio Web de Citrix. También puede poner esos Citrix Receivers a disposición de los usuarios desde el servidor StoreFront. Consulte Cómo ofrecer archivos de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instalación de Citrix Receiver en el servidor o el contenido equivalente en la versión de StoreFront que utilice.

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.

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.

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, ejecute el instalador o el comando de nuevo para continuar con la instalación del VDA.

Instaladores

Instalador de producto completo

Con el instalador de producto completo, incluido en la imagen ISO de XenApp o XenDesktop, puede:

- Instalar, actualizar o quitar los componentes principales de XenApp y XenDesktop: Delivery Controller, Studio, Director, StoreFront, el servidor de licencias
- Instalar o actualizar agentes VDA para Windows en sistemas operativos de servidor o de escritorio
- Instalar el componente de Universal Print Server en los servidores de impresión
- Instalar el Servicio de autenticación federada

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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:

- 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.

El instalador VDAWorkstationCoreSetup.exe no instala ni contiene Citrix Receiver para Windows.

Utilizar VDAWorkstationCoreSetup.exe equivale a usar VDAWorkstationSetup o el instalador de producto completo para

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instalar un VDA de SO de escritorio y:

- En la interfaz gráfica: Marcar la opción de acceso con Remote PC en la página **Entorno** y desmarcar la casilla Citrix Receiver en la página **Componentes**.
- En la interfaz de línea de comandos: Especificar las opciones /remotepc y components /vda.
- 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".

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización para el Administrador de recursos de Azure

Dec 05, 2017

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

Puede configurar XenApp o XenDesktop para aprovisionar recursos en Azure Resource Manager cuando cree el sitio de XenApp o XenDesktop (lo que incluye crear una conexión), o bien cuando cree una conexión de host posterior (después de crear el sitio).

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/es-es/documentation/articles/active-directory-integrating-applications/
- Entidad de servicio: https://azure.microsoft.com/es-es/documentation/articles/active-directory-application-objects/

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

Creación de una conexión al Administrador de recursos de Azure

Consulte los artículos Creación de un sitio y Conexiones y recursos para obtener información completa sobre todas las páginas de los asistentes para la creación de un sitio o una conexión. En los siguientes artículos, se describen solamente datos específicos de las conexiones al Administrador de recursos de Azure.

Existen dos métodos para establecer una conexión de host al Administrador de recursos de Azure:

- 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** 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 o los caracteres: \/;:#.*?= <>|[]{}"'()'). Después de introducir el ID de suscripción y el nombre de la conexión, se habilita el botón **Crear nueva**.

© 1999-2017 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 XenApp o XenDesktop los permisos de la lista. XenApp o XenDesktop 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.

Los recursos constituyen la región y la red.

- En la página **Región**, seleccione una región.
- En la página **Red**:
  - Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red en Studio. Un nombre de recurso no puede contener solo espacios en blanco ni los caracteres \/;:#.*?=<>|[]{}"'()'.
  - 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.

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 va a crear en Azure Active Directory.
- $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:

Paso 1: Conéctese a su suscripción de Azure Resource Manager.

```
Login-AzureRmAccount.
```

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

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

Paso 3: Cree la aplicación en su inquilino de AD.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Paso 4: Cree una entidad de servicio.

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

Paso 5: Asigne un rol a la entidad de servicio.

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

Paso 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 o los caracteres: \/;:#.*?= <>|[]{}'"()'.
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.)

Los recursos constituyen la región y la red.

- En la página **Región**, seleccione una región.
- En la página **Red**:
  - Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red en Studio. Un nombre de recurso no puede contener solo espacios en blanco ni los caracteres \/;:#.*?=<>|[]{}'"()'.
  - 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.

Complete el asistente.

Crear un catálogo de máquinas con una imagen maestra de Azure Resource Manager

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

Una imagen maestra es la plantilla que se usará para crear las máquinas virtuales en un catálogo de máquinas. Antes de crear

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Creación de 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/es-es/documentation/articles/storage-introduction/

  https://azure.microsoft.com/es-es/documentation/articles/storage-premium-storage/

  https://azure.microsoft.com/es-es/documentation/articles/storage-redundancy/

  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). Información más detallada disponible 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 ("on-premises") de Windows Server a Azure para usar HUB. No se respaldan las imágenes de la galería de Azure. Las licencias locales ("on-premises") de cliente 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/%23comment-145

  Para comprobar que las máquinas virtuales aprovisionadas utilizan HUB, ejecute el comando de PowerShell:

  ```
  Get-AzureRmVM -ResourceGroup MyResourceGroup -Name MyVM
  ```

  y verifique que el tipo de licencia es Windows_Server. Instrucciones adicionales disponibles 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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Complete el asistente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización de Microsoft Azure

Dec 05, 2017

Configuración de 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):

```
ServiceManagementUrl="https://management.core.windows.net"
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, 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 Modificación de una conexión.

Máquinas virtuales

En Studio, al crear un catálogo de máquinas, la selección del tamaño de cada máquina virtual depende de las opciones que presente Studio, el coste y el rendimiento del tipo seleccionado de instancia de VM, además de la escalabilidad.

Studio presenta todas las opciones de instancia de máquina virtual que Microsoft Azure ofrece en una región seleccionada; Citrix no puede modificar esta presentación. Por lo tanto, debe conocer sus aplicaciones y sus CPU, su memoria y sus requisitos de E/S. Dispone de varias opciones de rendimiento a precios diferentes; consulte los siguientes artículos de Microsoft para entenderlas mejor.

- MSDN. Tamaños de máquinas virtuales y servicios en la nube de Azure: https://msdn.microsoft.com/es-es/library/azure/dn197896.aspx.
- Precios de máquinas virtuales: https://azure.microsoft.com/es-es/pricing/details/virtual-machines/.

Nivel Básico. Las máquinas virtuales que tengan como prefijo "Básico" representan el disco básico. Están limitadas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 máquinas virtuales de nivel Estándar se dividen 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 EUA, el coste de cada tipo de instancia de máquina virtual por hora está disponible en http://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

Cuando se trabaja con entornos de nube, es importante entender los requisitos informáticos reales. En pruebas de concepto u otras actividades de prueba, puede ser tentador aprovechar los tipos de instancias de máquinas virtuales de alto rendimiento. También puede resultar tentador utilizar las máquinas virtuales de menor rendimiento para ahorrar costes. Sin embargo, el objetivo es usar una máquina virtual apropiada para la tarea en cuestión. Empezar por las de mayor rendimiento puede no darle los resultados que necesita y será muy caro con el tiempo (en algunos casos, en solo siete días). En caso de tipos de instancias de máquinas virtuales de bajo rendimiento con un coste menor, el rendimiento y la usabilidad pueden no ser adecuados para la tarea.

Para cargas de trabajo de SO de escritorio (VDI) o SO de servidor (RDSH), los resultados de las pruebas con LoginVSI y su carga media de trabajo muestran que los tipos de instancia Mediana (A2) y Grande (A3) ofrecen la mejor relación entre precio y rendimiento.

Los tipos de instancia Mediana (A2) y Grande (A3 o A5) representan la mejor relación entre coste y rendimiento para evaluar cargas de trabajo. No se recomienda nada menor. Una serie de máquinas virtuales con mayores capacidades pueden ofrecer a aplicaciones o usuarios el rendimiento y la usabilidad que estos necesiten. Sin embargo, es mejor usar los tres tipos de instancia mencionados como referencia para determinar si el coste más elevado que implica un tipo de instancia de VM con mayores capacidades se traduce en un valor real.

Escalabilidad

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 cierta cantidad de máquinas virtuales; no obstante, este límite cambia con frecuencia. Puede comprobar la información más reciente en: https://azure.microsoft.com/es-es/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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización Microsoft System Center Virtual Machine Manager

Dec 05, 2017

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 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

Actualización de VMM

- Actualización de VMM 2012 a VMM 2012 SP1 o VMM 2012 R2
  Para obtener más información acerca de los requisitos de hosts Hyper-V y VMM, consulte http://technet.microsoft.com/en-us/library/gg610649.aspx. Para ver los requisitos de la consola de VMM, consulte http://technet.microsoft.com/en-us/library/gg610640.aspx.

  No se da respaldo a clústeres mixtos de Hyper-V. Un ejemplo de clúster mixto es aquel en el que la mitad del clúster ejecuta Hyper-V 2008 y la otra mitad ejecuta Hyper-V 2012.

- Actualización de VMM 2008 R2 a VMM 2012 SP1
  Si va a actualizar desde XenDesktop 5.6 en VMM 2008 R2, siga estos pasos para evitar momentos de inactividad de XenDesktop.
  1. Actualice VMM a 2012 (ahora con XenDesktop 5.6 y VMM 2012)
  2. Actualice XenDesktop a la versión más reciente (ahora con la versión más reciente de XenDesktop y VMM 2012)
  3. Actualice VMM de 2012 a 2012 SP1 (ahora con la versión más reciente de XenDesktop y VMM 2012 SP1)
- Actualización de VMM 2012 SP1 a VMM 2012 R2
  Si empieza desde XenDesktop o XenApp 7.x en VMM 2012 SP1, siga estos pasos para evitar momentos de inactividad de XenDesktop.
  1. Actualice XenDesktop o XenApp a la versión más reciente (ahora con la versión más reciente de XenDesktop o XenApp y VMM 2012 SP1)
  2. Actualice VMM de 2012 SP1 a 2012 R2 (ahora con la versión más reciente de XenDesktop o XenApp y VMM 2012 R2)

Resumen de instalación y configuración

1. 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.
   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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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).

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

2. Crear una VM maestra.
   1. Instale un agente Virtual Desktop Agent en la VM maestra y seleccione la opción de optimizar el escritorio. Esto mejora el rendimiento.
   2. Tome una instantánea de la VM maestra para usarla como copia de seguridad.
3. 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 el cuadro de diálogo Detalles del host, seleccione el clúster o el host independiente que desea utilizar para crear las nuevas VM.
      Importante: 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 correctamente 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.

- **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
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 HCL no puede cargar directamente el disco de identidad en el almacenamiento de SMB. Por lo tanto, la máquina Hyper-V debe cargar y copiar el disco de identidad en el almacenamiento. Debido a que la máquina Hyper-V no puede leer el disco del Controller, la HCL debe copiar primero el disco de identidad mediante la máquina Hyper-V tal y como se indica.
  1. La HCL carga la identidad en la máquina Hyper-V mediante el recurso compartido de administrador.
  2. La máquina Hyper-V copia el disco en el almacenamiento de SMB a través de un script de PowerShell que se ejecuta en la sesión remota de PowerShell. Se crea una carpeta en la máquina Hyper-V y los permisos de la carpeta están bloqueados únicamente para el usuario de VMM (a través de la conexión remota de PowerShell).
  3. La biblioteca HCL elimina el archivo del recurso compartido de administrador.
  4. Cuando la biblioteca HCL completa la carga del disco de identidad en la máquina Hyper-V, la sesión remota de PowerShell copia los discos de identidad al almacenamiento de SMB y, después, los elimina de la máquina Hyper-V. La carpeta del disco de identidad se vuelve a crear si se elimina para que esté disponible para volver a usarse.

- **Descargar discos de identidad**. Al igual que con las cargas, los discos de identidad pasan a través de la máquina Hyper-V hasta la HCL. El siguiente proceso crea una carpeta que solo tiene permisos de usuario de VMM en el servidor Hyper-V si no existe.
  1. 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.
  2. La HCL lee el disco desde el recurso compartido de administrador de la máquina Hyper-V y lo copia en memoria.
  3. La HCL elimina el archivo del recurso compartido de administrador.
- **Crear 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización VMware

Dec 05, 2017

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 MCS, no inhabilite la característica de explorador del almacén de datos 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.

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 XenApp o XenDesktop 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 XenApp y XenDesktop y los privilegios mínimos requeridos de VMware.

Agregar conexión 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Create snapshot vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

Si desea que las VM creadas se etiqueten, agregue los siguientes permisos para la cuenta de usuario:

SDK	**Interfaz de usuario**
Global.ManageCustomFields	Global > Administrar atributos personalizados
Global.SetCustomField	Global > Definir atributo personalizado

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.

Aprovisionar máquinas (Provisioning Services)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Todos los privilegios de "**Aprovisionar máquinas (Machine Creation Services)**" y:

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
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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	Virtual machine > Provisioning > Clone virtual machine

Eliminar máquinas aprovisionadas

SDK	**Interfaz de usuario**
Datastore.Browse	Almacén de datos > Examinar almacén de datos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Obtención e importación de 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 VMware. Agregue el certificado de VMware vCenter a cada Controller. Siga el siguiente procedimiento:

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 usando alguno de los métodos siguientes:
   - Desde el servidor vCenter:
     1. Copie el archivo rui.crt desde el servidor vCenter a una ubicación accesible en los Delivery Controllers.
     2. 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 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.
     1. Abra el explorador Web y establezca una conexión Web segura con el servidor vCenter; por ejemplo https://servidor1.dominio1.com
     2. Acepte las advertencias de seguridad.
     3. Haga clic en la barra de dirección donde aparece el error de certificado.
     4. Vea el certificado y haga clic en la ficha Detalles.
     5. Seleccione Copiar a archivo y exporte en formato .CER; escriba un nombre cuando lo pida el procedimiento.
     6. Guarde el certificado exportado.
     7. Vaya a la ubicación del certificado exportado y abra el archivo . CER.
   - Impórtelo directamente desde Internet Explorer ejecutado como administrador:
     1. Abra el explorador Web y establezca una conexión Web segura con el servidor vCenter; por ejemplo https://servidor1.dominio1.com.
     2. Acepte las advertencias de seguridad.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Haga clic en la barra de dirección donde aparece el error de certificado.
4. Vea el certificado.

- Importe el certificado en el almacén de certificados de cada uno de los Controllers:
  1. Haga clic en Instalar certificado, seleccione Máquina local y, a continuación, haga clic en Siguiente.
  2. Seleccione Colocar todos los certificados en el siguiente almacén y, a continuación, haga clic en Examinar.
  3. Si está usando Windows Server 2008 R2:
     1. Marque la casilla Mostrar almacenes físicos.
     2. Expanda Personas de confianza.
     3. Seleccione Equipo local.
     4. Haga clic en Siguiente y, a continuación, en Finalizar.

     Si usa Windows Server 2012, Windows Server 2012 R2 o Windows Server 2016:

     1. Seleccione Personas de confianza, y haga clic en Aceptar.
     2. Haga clic en Siguiente y, a continuación, en Finalizar.

Importante: Si cambia el nombre del servidor de vSphere después de la instalación, debe generar un certificado autofirmado nuevo en ese servidor antes de importar el certificado nuevo.

Creación de una VM maestra

Use una VM maestra para proporcionar las aplicaciones y los escritorios de los usuarios. 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.

Creación de escritorios virtuales

Si utiliza Studio para crear las VM, en lugar de seleccionar un catálogo de máquinas existente, especifique la siguiente información cuando configure la infraestructura de alojamiento para crear escritorios virtuales.

1. Seleccione el tipo de host de VMware vSphere.
2. Escriba la dirección del punto de acceso para el SDK de vCenter.
3. Introduzca las credenciales de la cuenta de usuario de VMware que configuró anteriormente y que incluye permisos para crear nuevas VM. Especifique el nombre de usuario en el formato domain/username.

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 funcionalidad 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 en XenApp o XenDesktop o, incluso si no es en ellos, en 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entornos de Microsoft System Center Configuration Manager

Dec 05, 2017

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 7.5 para Configuration Manager 2012**: Citrix Connector es un puente entre Configuration Manager y XenApp o XenDesktop. 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 XenApp o XenDesktop. Para obtener más información acerca de Connector, consulte Citrix Connector 7.5 para System Center Configuration Manager 2012.
- **Proxy Wake On LAN de Configuration Manager**. La función Wake on LAN del Acceso con Remote PC requiere Configuration Manager. Para obtener más información, consulte los apartados siguientes.
- **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. Estas propiedades son utilizadas automáticamente por Citrix Connector, 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.

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

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

Propiedad	Descripción
AssignmentType	Establece el valor de IsAssigned. Los valores válidos son: • ClientIP • ClientName • Ninguno • Usuario: 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propiedad	Descripción
HostIdentifier	Es un GUID que 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 en una máquina virtual que se usa como una imagen maestra (este valor se establece durante la instalación basada en una selección). • Cleared en una máquina virtual que esté 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.
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 más información, consulte la documentación de Microsoft.

Configuration Manager y Wake on LAN para 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 y usar Studio para crear o actualizar la implementación de acceso con Remote PC:

- Configure Configuration Manager 2012, 2012 R2 o 2016 dentro de la organización. A continuación, implemente el cliente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
  - 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 dar respaldo al proxy de reactivación, habilite la opción en ConfigMgr. 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 implementación de acceso con Remote PC en Studio.

- Si habilita la administración de energía, especifique los datos de conexión: un 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 el uso de Magic Packets y proxy de reactivación de ConfigMgr; también puede cambiar el método de transmisión de paquetes.

Consulte Acceso con Remote PC para obtener más información.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entornos de virtualización de Nutanix

Mar 01, 2018

Siga estas instrucciones si usa Nutanix Acropolis para proporcionar máquinas virtuales en su entorno de XenApp o XenDesktop. El proceso de configuración incluye las siguientes tareas:

- Instalar y registrar el plugin de Nutanix en el entorno de XenApp o XenDesktop.
- 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 con 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 https://portal.nutanix.com.

Para obtener información de asistencia relacionada con Nutanix y Provisioning Services, consulte el artículo CTX131239 de Knowledge Center.

Instalar y registrar el plugin de Nutanix

Después de instalar los componentes de XenDesktop o XenApp, complete el siguiente procedimiento para instalar y registrar el plugin de Nutanix en los Delivery Controllers. A continuación, 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 plugin 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:\Archivos de programa\Common Files\Citrix\HCLPlugins\RegisterPlugins.exe –PluginsRoot "C:\Archivos de programa\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 plugin de Nutanix Acropolis se ha registrado:

    Add-PSSnapin Citrix*
    Get-HypHypervisorPlugin

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, y un nombre para la conexión. En la página **Red**, seleccione una red para la unidad de alojamiento.

Crear catálogo de máquinas usando una instantánea

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de Nutanix

Esta información complementa a 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 de máquinas. 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 XenApp y XenDesktop. 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".

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de componentes principales

Dec 05, 2017

Los componentes principales son el Delivery Controller, Studio, Director, StoreFront y el servidor de licencias.

Importante: Antes de comenzar una instalación, consulte Antes de la instalación. 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 Instalación mediante 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 XenApp y XenDesktop. Descargue el archivo ISO del producto.

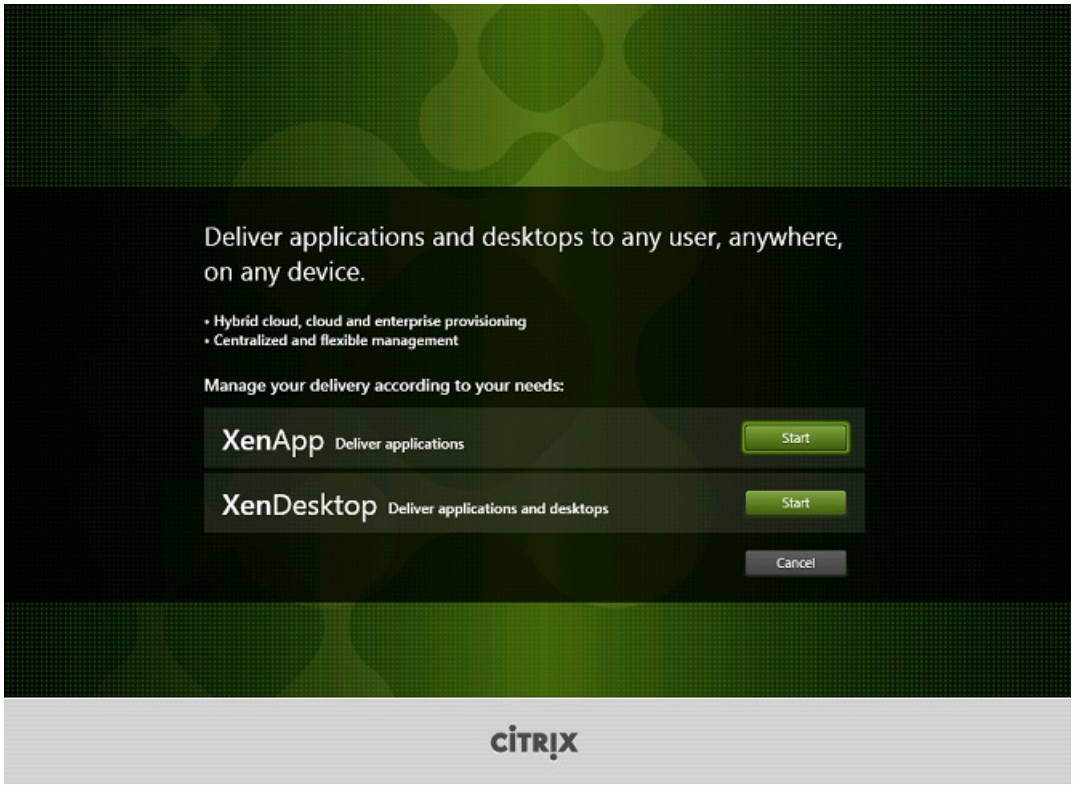
Descomprima el archivo. Si lo desea, puede grabar un DVD del archivo ISO.

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 programa de instalación no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

Paso 2. Elija el producto a instalar

© 1999-2017 Citrix Systems, Inc. All rights reserved.



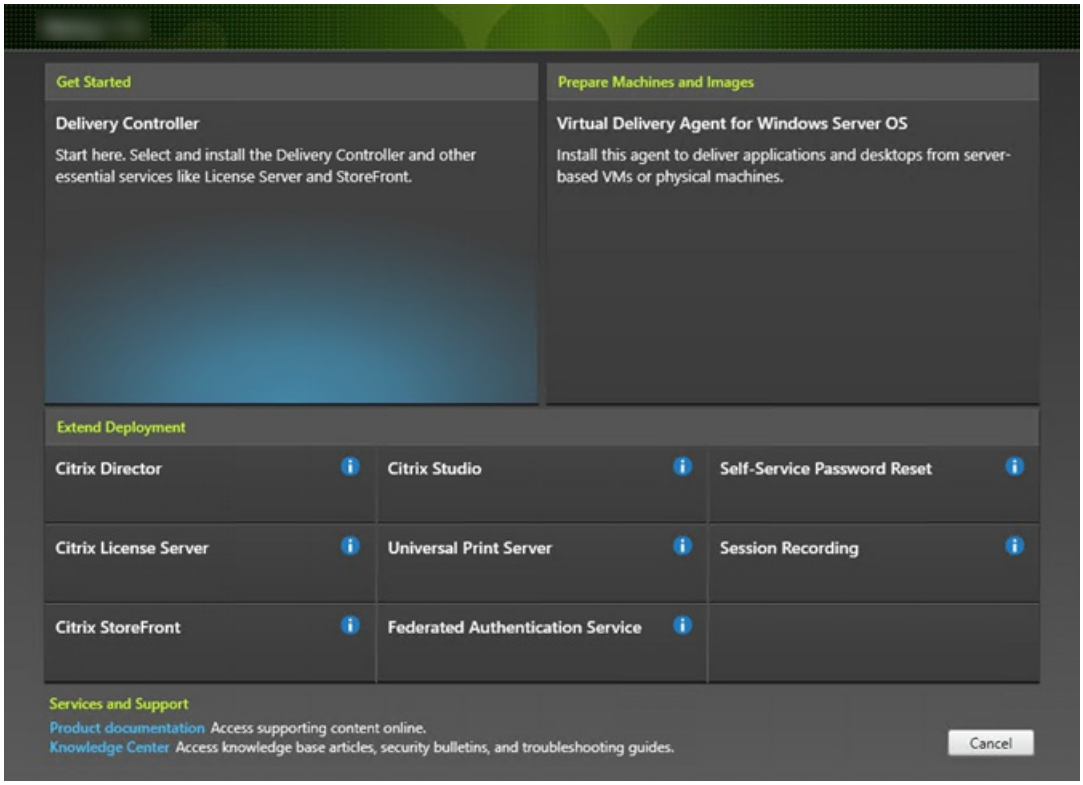
Haga clic en **Iniciar** junto al producto que quiera instalar: XenApp o XenDesktop.

(Si la máquina ya tiene instalados componentes de XenApp o XenDesktop, esta página no aparecerá.)

Opción de la línea de comandos: /xenapp para instalar XenApp; se instala XenDesktop si se omite la opción

Paso 3. Elija qué instalar

© 1999-2017 Citrix Systems, Inc. All rights reserved.



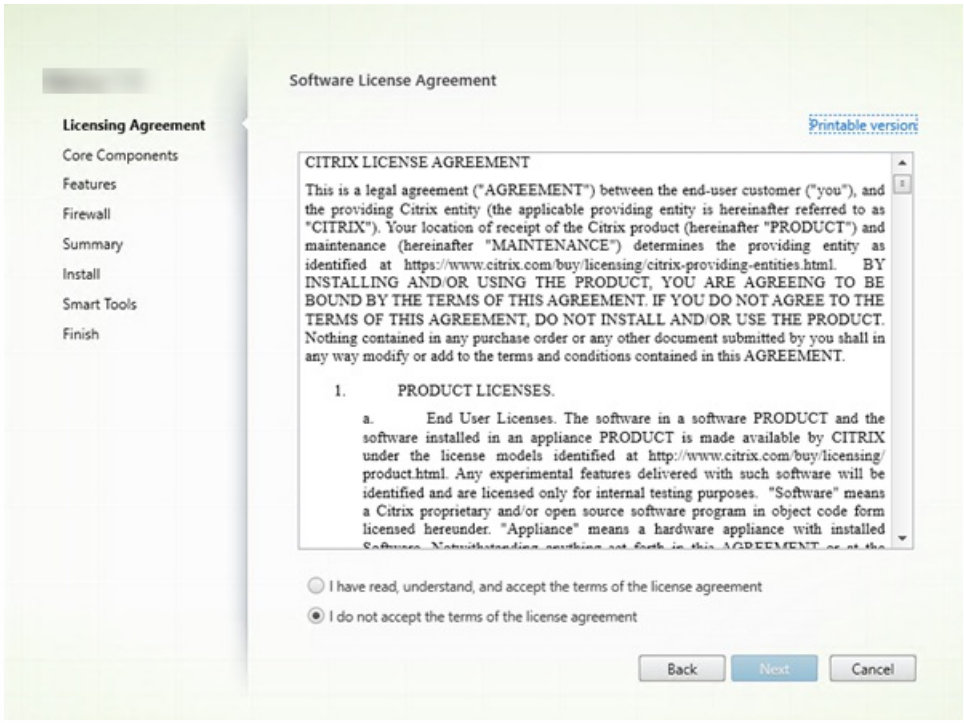
Si acaba de empezar, seleccione **Delivery Controller**. (En una página posterior, seleccionará los componentes concretos que se instalarán en esta máquina.)

Si ya ha instalado un Controller (en esta máquina o en otra) y quiere instalar otro componente, selecciónelo en la sección Ampliar implementación.

Opción de línea de comandos: /components

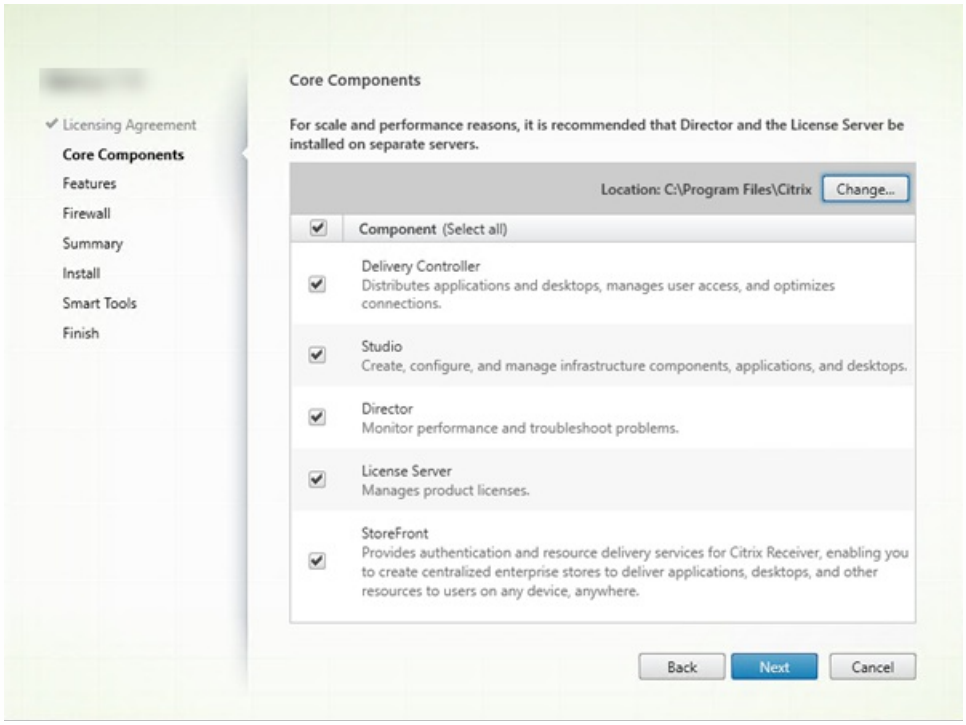
Paso 4. Lea y acepte el contrato de licencia

© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Contrato de licencia**, después de leer el contrato de licencia, indique que lo ha leído y lo acepta. A continuación, haga clic en **Siguiente**.

Paso 5. Seleccione los componentes a instalar y la ubicación de la instalación



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, las casillas de todos los componentes principales están marcadas. 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.

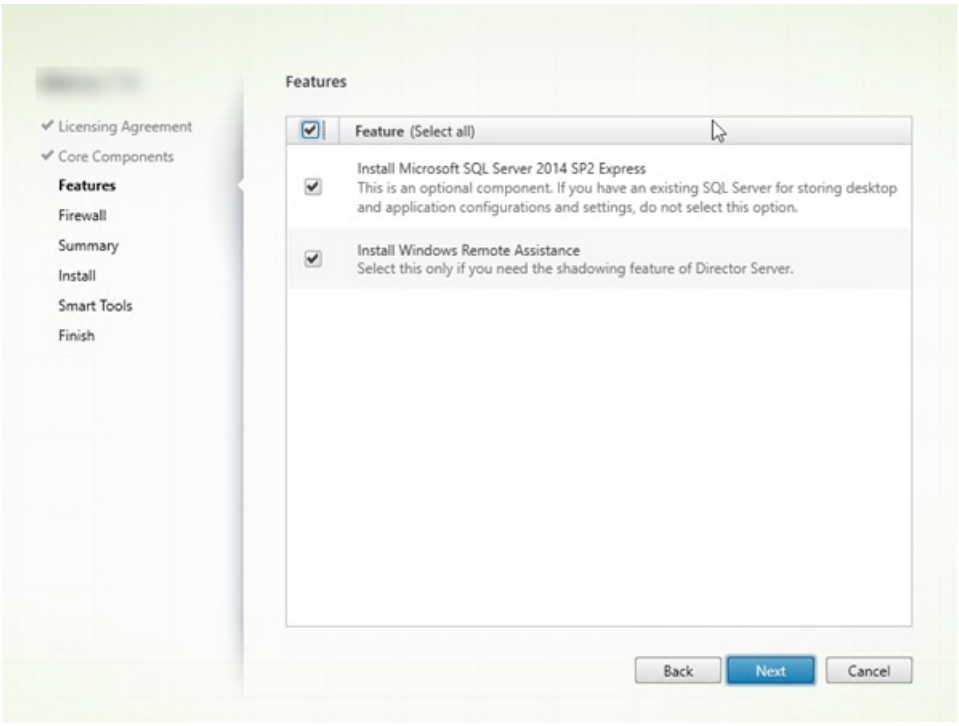
  Indique solo los componentes que quiera instalar en esta máquina. Después de instalar los componentes en esta máquina, podrá ejecutar de nuevo el programa de instalación en otras máquinas para instalar otros componentes.

  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 necesariamente 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 XenApp y XenDesktop, consulte Bases de datos.
- Al instalar Director, la Asistencia remota de Windows se instala automáticamente. Puede elegir si quiere habilitar el

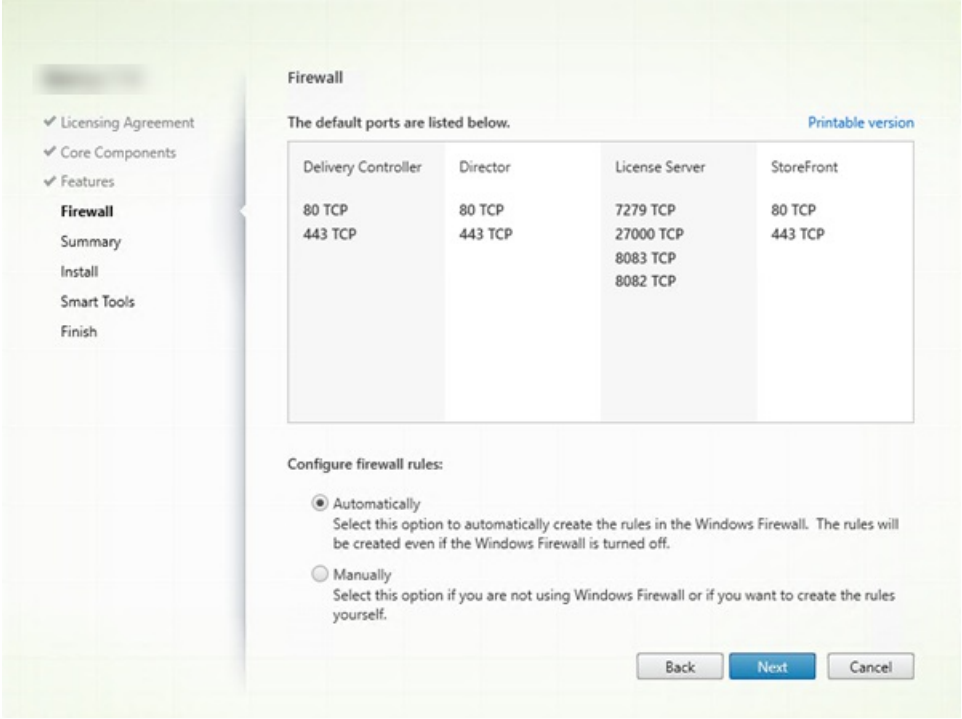
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 funcionalidad está habilitada. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Esta funcionalidad aparece solamente cuando se instala Director.

Haga clic en **Siguiente**.

Opciones de línea de comandos: /nosql (para impedir la instalación), /no_remote_assistance (para impedir que se habilite)

Paso 7. Abra automáticamente los puertos del Firewall de Windows



De forma predeterminada, los puertos que aparecen en la página **Firewall** se abren automáticamente si el servicio Firewall de Windows se está ejecutando, incluso aunque el firewall no esté habilitado. La opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte Puertos de red.

Haga clic en **Siguiente**.

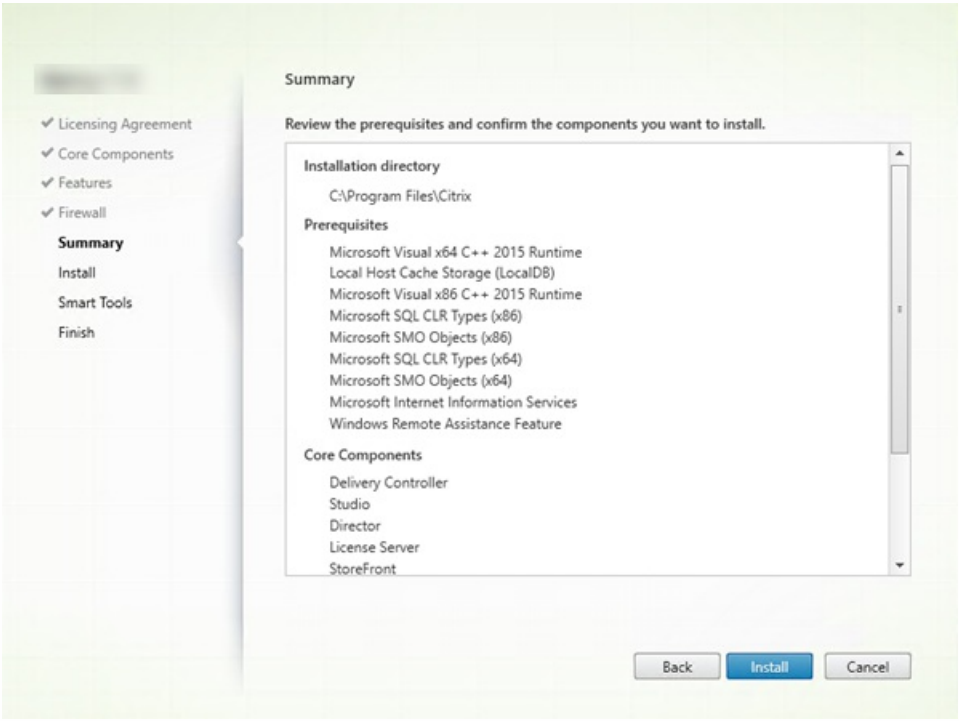
(En el gráfico, se muestran las listas de los puertos que aparecen si se elige instalar todos los componentes principales en esta máquina. Por regla general, este tipo de instalación solo se realiza para las implementaciones de prueba.)

Opción de línea de comandos: /configure_firewall

Paso 8. Revise los requisitos previos y confirme la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instalación

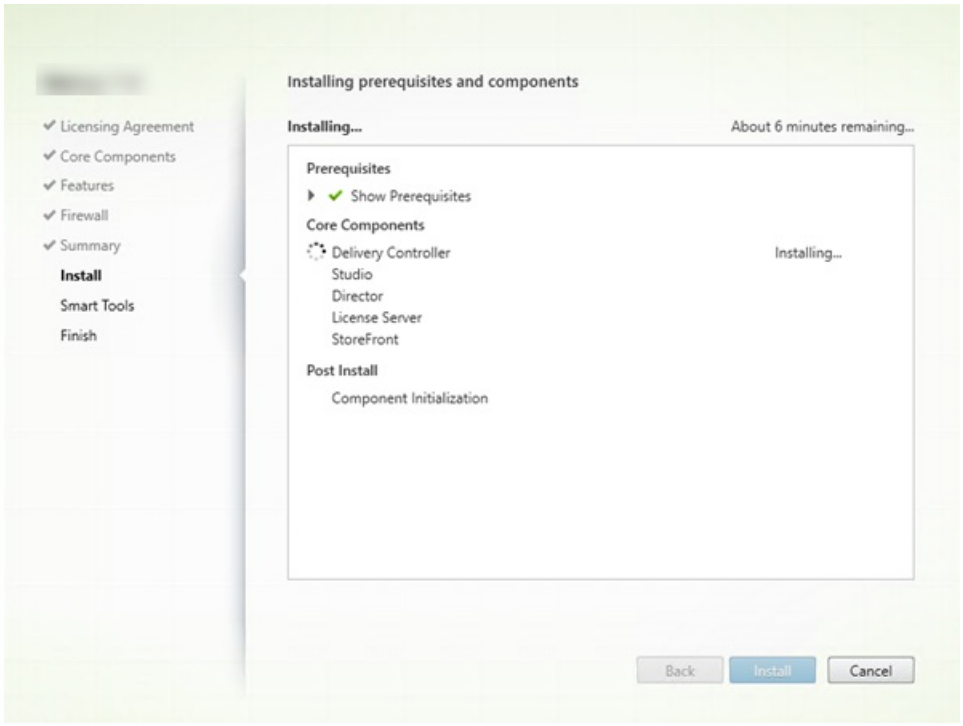


La página **Resumen** muestra lo que se instalará. Si fuera necesario, puede usar el botón Atrás para volver a las páginas anteriores del asistente y cambiar las opciones.

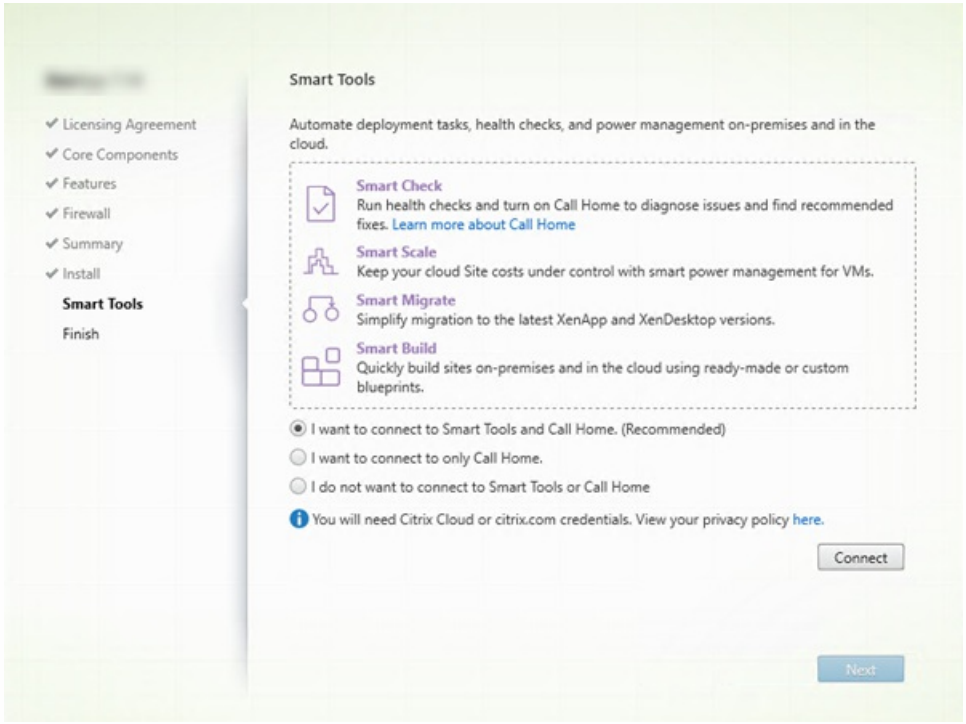
Cuando haya terminado, haga clic en **Instalar**.

La pantalla muestra el progreso de la instalación.

© 1999-2017 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

si se produce un error en el programa de instalación relacionado con el servicio de telemetría de Citrix.
- No habilitar conexiones con Smart Tools o Call Home.

Si instala StoreFront (pero no instala ningún Controller), el asistente muestra la página **Smart Tools**. Si instala otros componentes principales (pero no un Controller ni StoreFront), el asistente no mostrará ni la página **Smart Tools** ni **Call Home**.

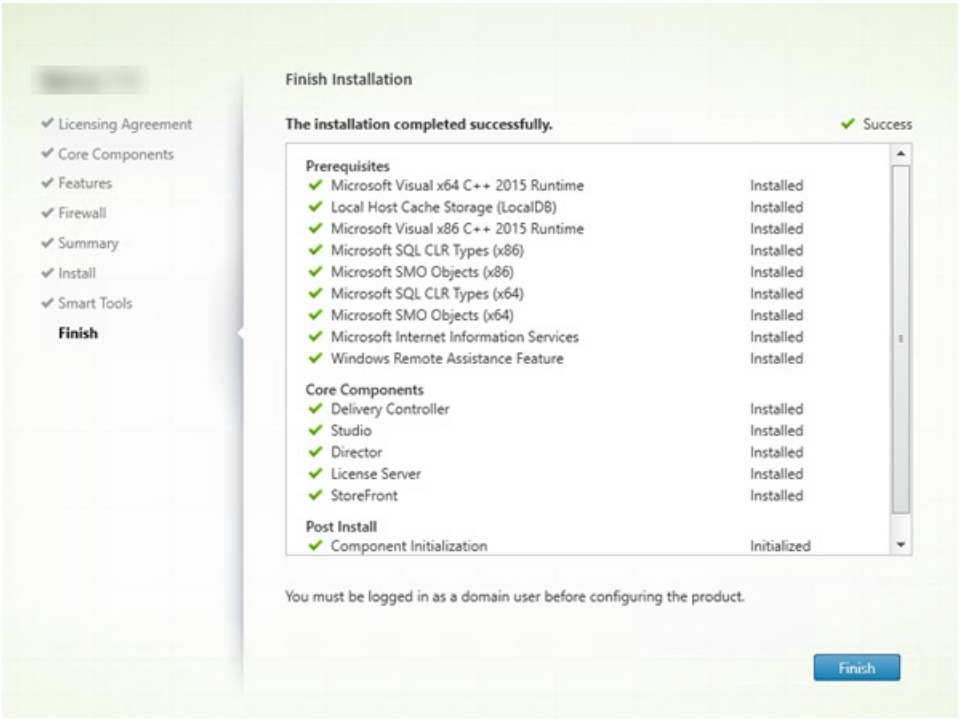
Si elige una de las opciones que habilitan las conexiones con Smart Tools y/o Call Home:

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 botón **Conectar**. Si se produce 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 **Finalizar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 programa de instalación en las demás máquinas para instalar otros componentes principales. También puede instalar más Controllers en otros servidores.

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 programa de instalación de producto completo en cualquier momento para ampliar la implementación con los siguientes componentes:

- Componente de servidor Universal Print Server: Inicie el programa de instalación 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 Instalación mediante línea de comandos.
- Servicio de autenticación federada: Consulte Servicio de autenticación federada
- Autoservicio de restablecimiento de contraseñas: Consulte la documentación referente al Autoservicio de restablecimiento de contraseñas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de agentes VDA

Dec 05, 2017

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 la instalación. 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 Instalación mediante línea de comandos.

Paso 1. Descargue el software del producto e inicie el asistente

Si usa el instalador de producto completo:

- Si aún no ha descargado el archivo ISO de XenApp y XenDesktop:
  - Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de XenApp y XenDesktop. Descargue el archivo ISO del producto.
  - Descomprima el archivo. Si lo desea, puede grabar un DVD del archivo ISO.
- 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:

- Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de XenApp y XenDesktop. Descargue el paquete correspondiente:

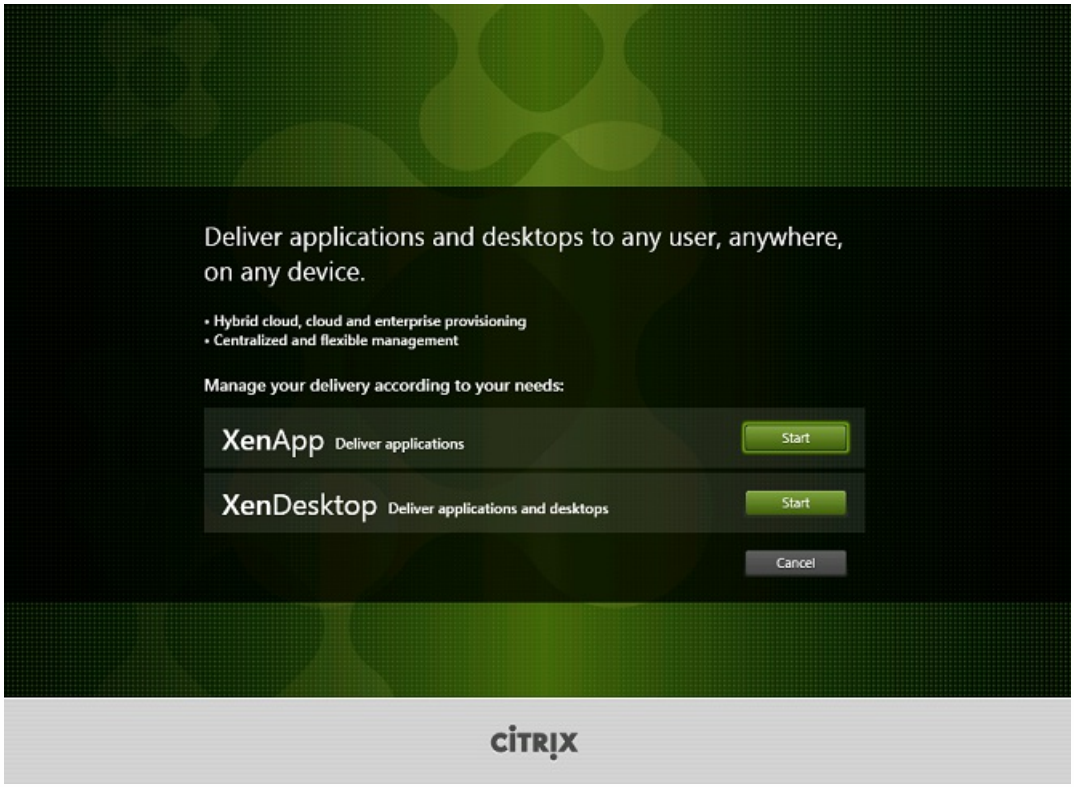
Nombre del componente en la página de descarga	**Nombre del archivo del instalador**
Virtual Delivery Agent de SO de servidor <*versión*>	VDAServerSetup.exe
Virtual Delivery Agent de SO de escritorio <*versión*>	VDAWorkstationSetup.exe
Virtual Delivery Agent de SO de escritorio con los servicios principales	VDAWorkstationCoreSetup.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

<versión>	

- Haga clic con el botón secundario en el paquete que ha descargado y seleccione **Ejecutar como administrador.**
- Se iniciará el asistente de instalación.

Paso 2. Elija el producto a instalar

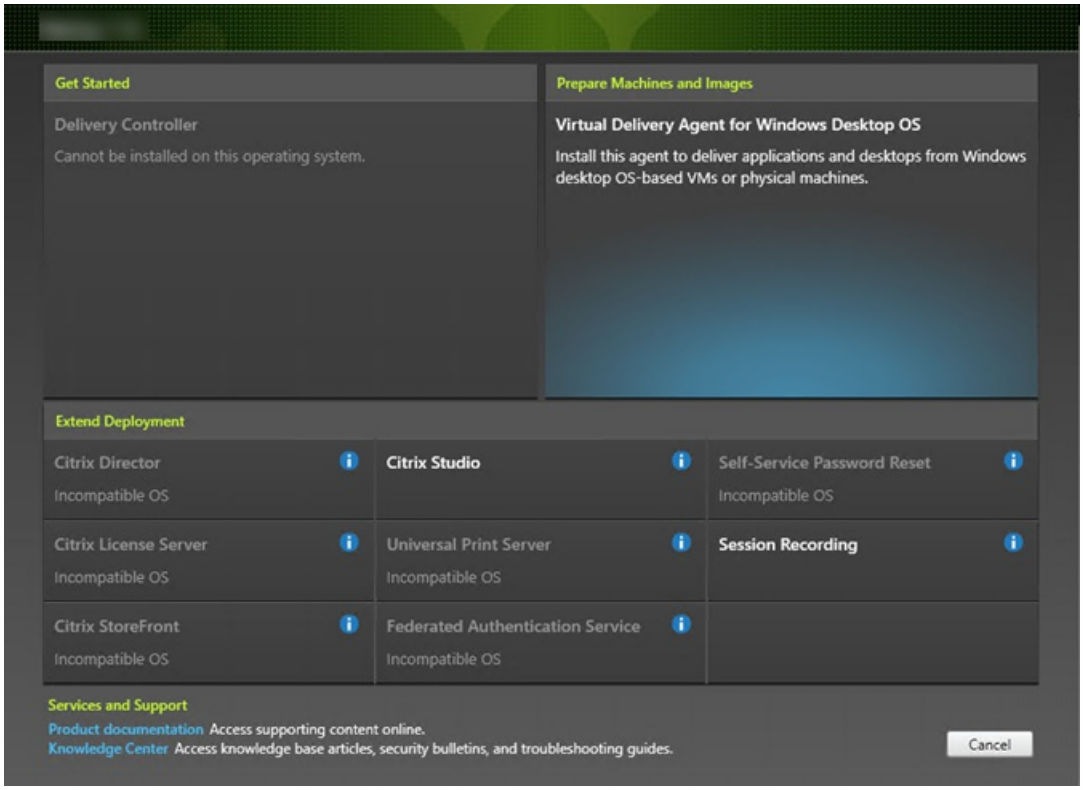


Haga clic en **Iniciar** junto al producto que quiera instalar: XenApp o XenDesktop. (Si la máquina ya tiene instalado un componente de XenApp o XenDesktop, esta página no aparecerá.)

Opción de la línea de comandos: /xenapp para instalar XenApp; se instala XenDesktop si se omite la opción

Paso 3. Seleccione el VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

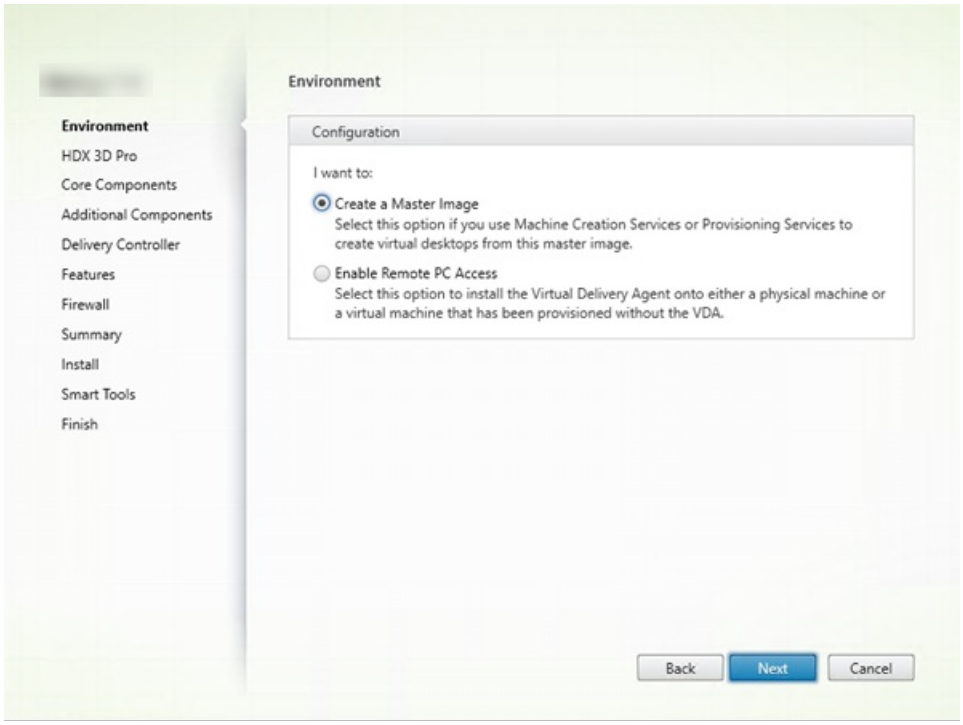


Seleccione la entrada de Virtual Delivery Agent. El instalador detecta si se ejecuta en un SO de escritorio o de servidor, de modo que solo ofrece el tipo de VDA apropiado.

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.

Paso 4. Especifique cómo se usará el VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Entorno**, especifique cómo se usará el VDA. Elija una de las siguientes opciones:

- **Imagen maestra**. Opción predeterminada. El VDA se va a instalar en una imagen de máquina. Tiene pensado usar las herramientas de Citrix (Machine Creation Services o Provisioning Services) para crear máquinas virtuales a partir de esa imagen maestra.
- **Habilitar conexiones con una máquina de servidor** (si instala en un servidor) o **Acceso con Remote PC** (si instala en una máquina de escritorio). Va a instalar el VDA en una máquina física o en una VM que se aprovisionó sin agente VDA. Si selecciona la opción Acceso con Remote PC, no se instalarán o no se habilitarán los siguientes componentes:
  - App-V
  - Profile Management
  - Machine Identity Service
  - Personal vDisk

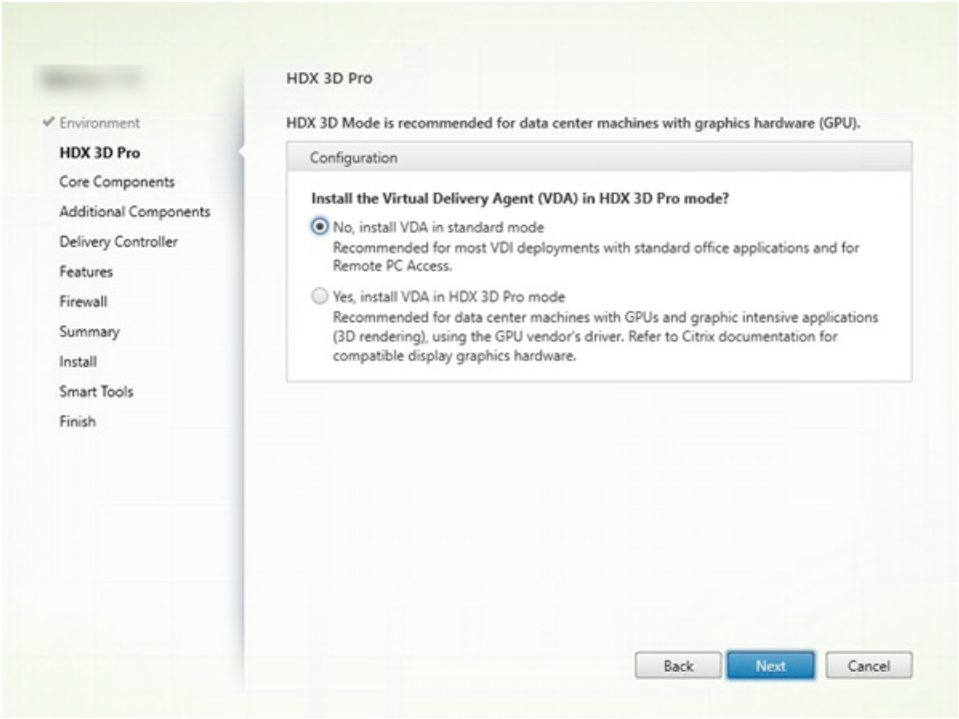
Haga clic en **Siguiente**.

Opciones de la línea de comandos: /masterimage, /remotepc

Si utiliza el instalador "VDAWorkstationCoreSetup.exe", esta página no aparece en el asistente y las opciones de la línea de comandos no son válidas.

Paso 5. Elija si habilitar el modo de HDX 3D Pro

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **HDX 3D Pro** aparecerá solamente si se instala un VDA para SO de escritorio.

- El modo de VDA estándar se recomienda para la mayoría de los escritorios, incluidos aquellos habilitados con Microsoft RemoteFX. El modo de VDA estándar es la opción predeterminada.
- El VDA en el modo HDX 3D Pro optimiza el rendimiento de los programas que hacen un uso intensivo de gráficos y de las aplicaciones ricas en medios. El modo de VDA para HDX 3D Pro se recomienda si la máquina va a acceder a un procesador de gráficos para generación 3D.
- Para el acceso con Remote PC, el VDA suele configurarse con el modo de VDA estándar. Para el acceso con Remote PC configurado con HDX 3D Pro, se admite mostrar una pantalla vacía con
  - Gráficos Intel Iris Pro y gráficos Intel HD 5300 y posteriores (procesadores Intel Core de 5ª generación y procesadores Intel Core i5 de 6ª generación)
  - GPU de NVIDIA Quadro y NVIDIA GRID
  - AMD RapidFire

Modo estándar	**Modo de HDX 3D Pro**
Por lo general, es la mejor opción para escritorios virtuales sin aceleración de hardware de gráficos y para el acceso con Remote PC.	Por lo general, es la mejor opción para escritorios de centros de datos con aceleración del hardware de gráficos, a menos que se necesiten más de cuatro monitores.
Se puede usar cualquier GPU para el acceso con Remote PC, con algunas limitaciones de compatibilidad de las aplicaciones: • En Windows 7, 8 y 8.1, la aceleración de GPU para la funcionalidad DirectX iguala a 9.3. Algunas aplicaciones	Admite la aceleración de GPU con cualquier GPU. sin embargo, la consola con pantalla vacía, las resoluciones personalizadas y varios monitores requieren gráficos NVIDIA GRID, Intel Iris Pro o AMD RapidFire. Utiliza el controlador de gráficos del distribuidor para

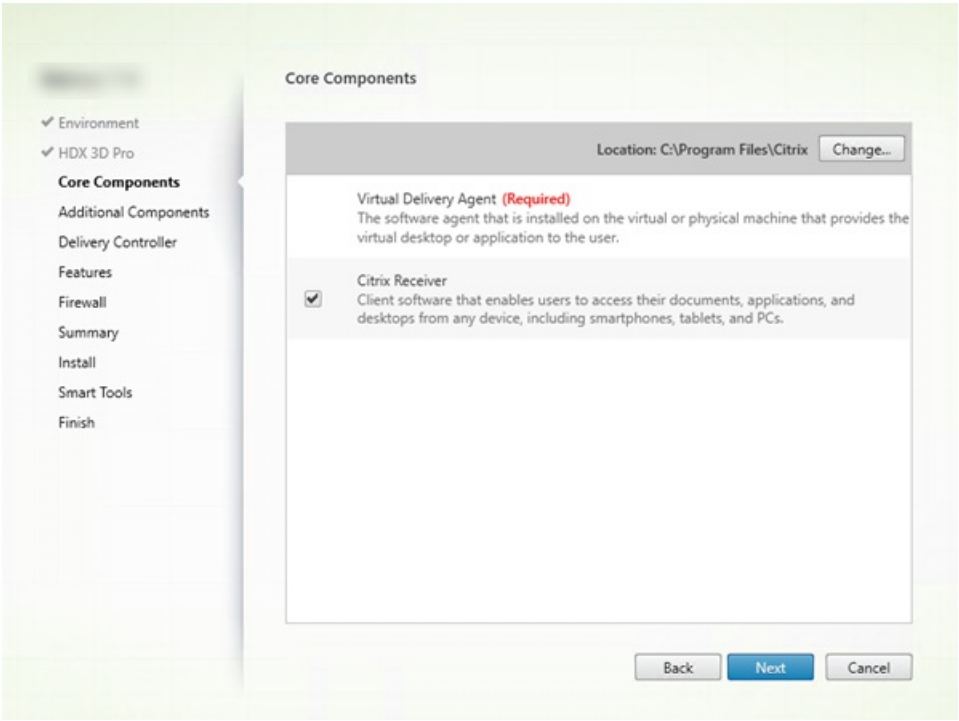
© 1999-2017 Citrix Systems, Inc. All rights reserved.

DirectX 10, 11 y 12 pueden no ejecutarse si no admiten el respaldo a DirectX 9. • En Windows 10, la aceleración de GPU se ofrece para aplicaciones de ventana (no en pantalla completa) DirectX 10, 11 y 12. Las aplicaciones DX 9 se representan con WARP. Las aplicaciones DX no se pueden usar en el modo de pantalla completa. • La aceleración de aplicaciones OpenGL en sesiones remotas, si la admite el distribuidor de la GPU (en la actualidad, solo NVIDIA).	obtener la mayor compatibilidad con las aplicaciones: • Todas las API de 3D (DirectX u OpenGL) que admite la GPU. • Respaldo para aplicaciones 3D de pantalla completa con Intel Iris Pro (solo para Win10), NVIDIA GRID y AMD RapidFire. • Respaldo para las API y las extensiones de controlador personalizadas. Por ejemplo, OpenCL o CUDA.
Las resoluciones arbitrarias de monitor (límite determinado por el rendimiento y el sistema operativo de Windows) y hasta ocho monitores.	Admite hasta cuatro monitores.
La codificación por hardware H.264 está disponible con procesadores de gráficos Intel Iris Pro.	La codificación por hardware H.264 está disponible con tarjetas de NVIDIA y procesadores de gráficos Intel Iris Pro.

Haga clic en **Siguiente.**

Opción de línea de comandos: /enable_hdx_3d_pro

Paso 6. Seleccione los componentes a instalar y la ubicación de la instalación



© 1999-2017 Citrix Systems, Inc. All rights reserved.

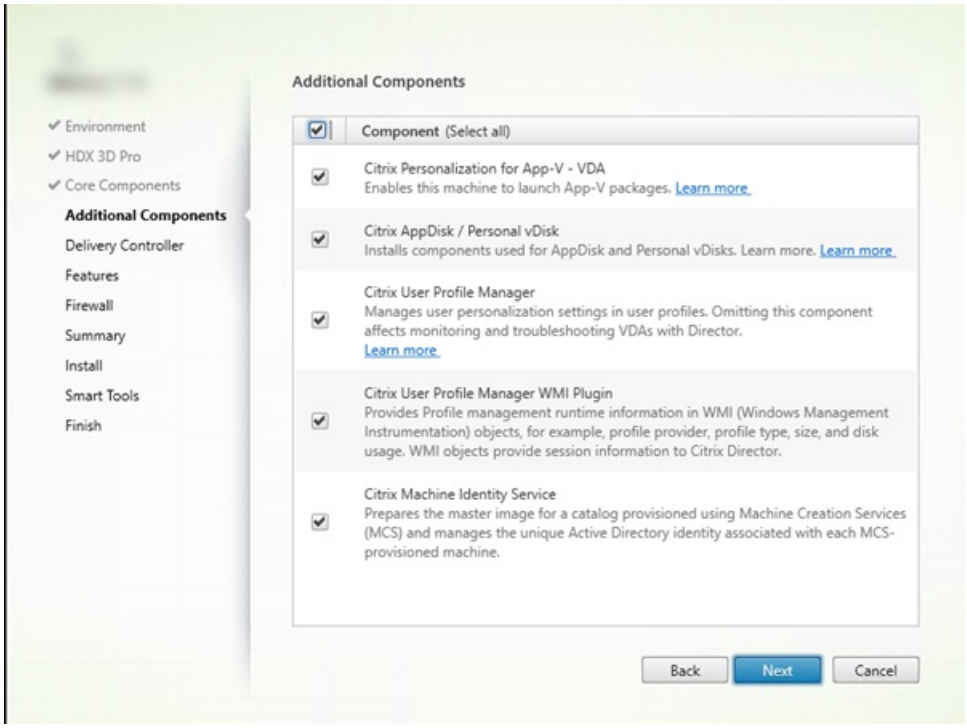
En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en C:\Archivos de programa\Citrix. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de ejecución para el servicio de red.
- **Componentes:** De forma predeterminada, se instala Citrix Receiver para Windows con el VDA (a menos que esté usando el instalador VDAWorkstationCoreSetup.exe). Desmarque la casilla de verificación si no quiere que se instale ese Citrix Receiver. Si utiliza el instalador VDAWorkstationCoreSetup.exe, Citrix Receiver para Windows no se instala nunca, así que esta casilla no aparece.

Haga clic en **Siguiente**.

Opciones de la línea de comandos: /installdir, "/components vda" para impedir la instalación de Citrix Receiver para Windows

Paso 7. 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. 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.)

Citrix Personalization for App-V

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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: /exclude "Citrix Personalization for App-V – VDA" para impedir la instalación de este componente

Citrix AppDisk o Personal vDisk

Válido solamente cuando se instala un VDA para SO de escritorio en una VM. Instala los componentes utilizados para Personal vDisk y AppDisk. Para obtener más información, consulte AppDisks y Personal vDisk.

Opción de línea de comandos: /exclude "Personal vDisk" para impedir la instalación de los componentes AppDisk y Personal vDisk

Citrix Profile Management:

Este componente administra los parámetros de personalización de usuario en los perfiles de usuario. Para obtener más detalles, consulte Profile Management.

Excluir Citrix Profile Manager de la instalación afecta a la supervisión y la solución de problemas de los agentes VDA con Citrix Director. En las páginas Detalles del usuario y Punto final, el panel de 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.

Opción de línea de comandos: /exclude "Citrix User Profile Manager" para impedir la instalación de este componente

Citrix Profile Management WMI Plugin:

Este plugin 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: /exclude "Citrix User Profile Manager WMI Plugin" para impedir la instalación de este componente

Citrix Machine Identity Service

Este servicio prepara la imagen maestra para un catálogo aprovisionado por MCS. El servicio también administra la identidad de Active Directory única de cada máquina aprovisionada.

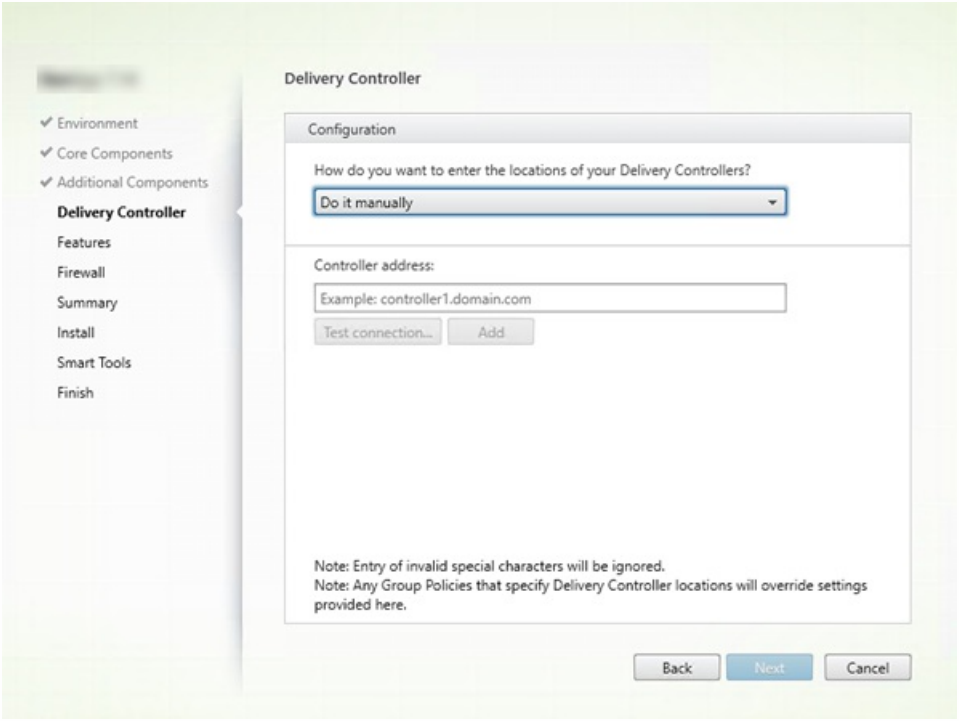
Opción de línea de comandos: /exclude "Machine Identity Service" para impedir la instalación de este componente

Valores predeterminados en la interfaz gráfica

- Si ha seleccionado "Crear una imagen maestra" en la página **Entorno** (Paso 4), los elementos de la página **Componentes adicionales** se habilitan de forma predeterminada.
- Si ha seleccionado "Habilitar el acceso con Remote PC" o "Habilitar conexiones con una máquina de servidor" en la página **Entorno**, los elementos de la página **Componentes adicionales** se inhabilitan de forma predeterminada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paso 8. Direcciones de Delivery Controller



En la página **Delivery Controller**, elija cómo quiere especificar las direcciones de los Controllers instalados. Citrix recomienda especificar las direcciones de los Controllers ahora ("Hacerlo manualmente"), mientras instala el VDA. El VDA no puede registrarse en el Controller sin esta información. Si un VDA no puede registrarse, los usuarios no podrán acceder a las aplicaciones ni a los escritorios que contenga ese VDA.

- **Hacerlo manualmente**. (Opción predeterminada.) Introduzca el nombre de dominio completo (FQDN) de un Controller instalado y, a continuación, haga clic en **Agregar**. Si ha instalado Controllers adicionales, agregue sus direcciones respectivas.
- **Hacerlo más tarde (Avanzado)**. Si elige esta opción, el asistente le solicitará confirmación antes de continuar. Para especificar más adelante esas direcciones, puede volver a ejecutar el instalador más adelante o usar una directiva de grupo de Citrix. El asistente también se lo recordará en la página **Resumen**.
- **Elegir ubicaciones desde Active Directory**. Esta opción es válida solamente cuando la máquina está unida a un dominio y el usuario es un usuario de dominio.
- **Dejar que Machine Creation Services lo haga automáticamente**. Esta opción es válida solamente si utiliza Machine Creation Services (MCS) para aprovisionar máquinas.

Haga clic en **Siguiente**. Si ha seleccionado la opción "Hacerlo más tarde (avanzado)", se le pedirá que confirme que especificará las direcciones de Controller más adelante.

Otras consideraciones

- La dirección no puede contener los caracteres { | } ~ [\ ] ^ ' : ; < = > ? & @ ! " # $ % ( ) + / ,
- 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

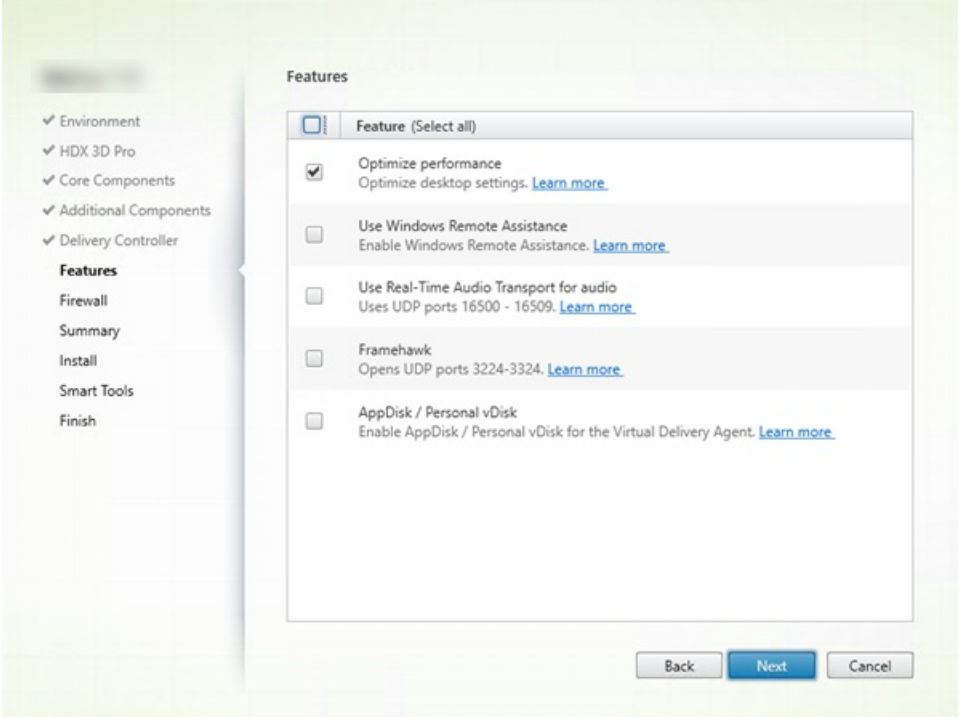
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Delivery Controllers.

Opción de línea de comandos: /controllers

Paso 9. Habilite o inhabilite las características



En la página **Características**, marque o desmarque las casillas de verificación para habilitar o inhabilitar respectivamente las funcionalidades que quiera utilizar.

Optimizar el 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si esta opción está habilitada, la Asistencia remota de Windows se usa con la función de remedo de usuarios de 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 Citrix Receiver o de VDA a NetScaler Gateway) y externos (de NetScaler Gateway a Citrix Receiver). Si se implementa NetScaler 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

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. Para obtener más información, consulte AppDisks y Personal vDisks.

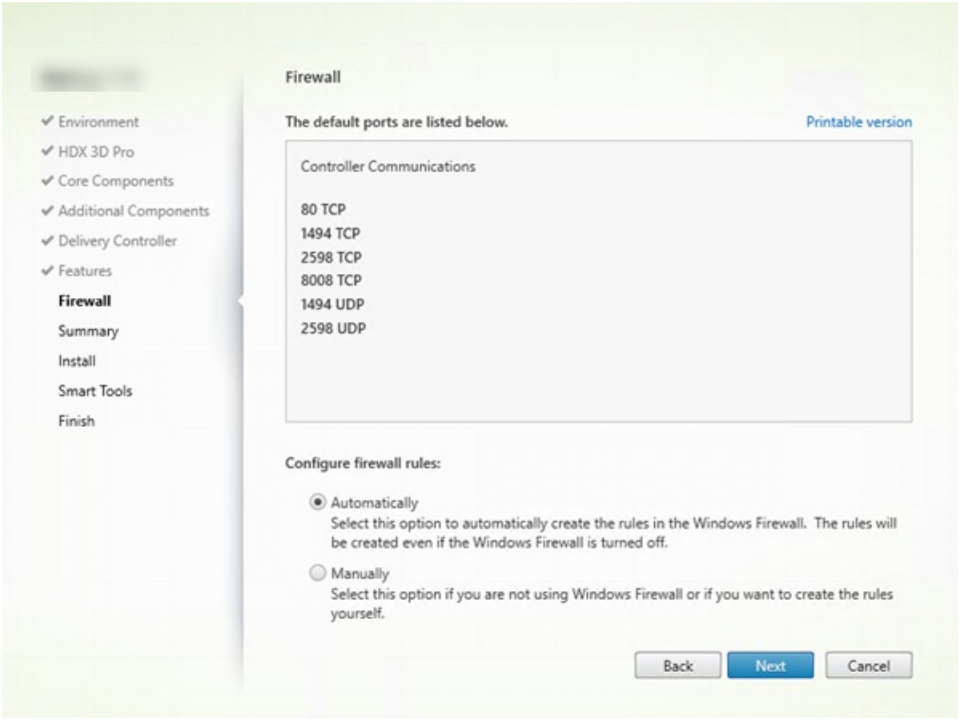
Opción de la línea de comandos: /baseimage

Si utiliza el instalador VDAWorkstationCoreSetup.exe, esta característica no aparecerá en el asistente y la opción de línea de comandos no será válida.

Haga clic en **Siguiente**.

Paso 10. Puertos de firewall

© 1999-2017 Citrix Systems, Inc. All rights reserved.



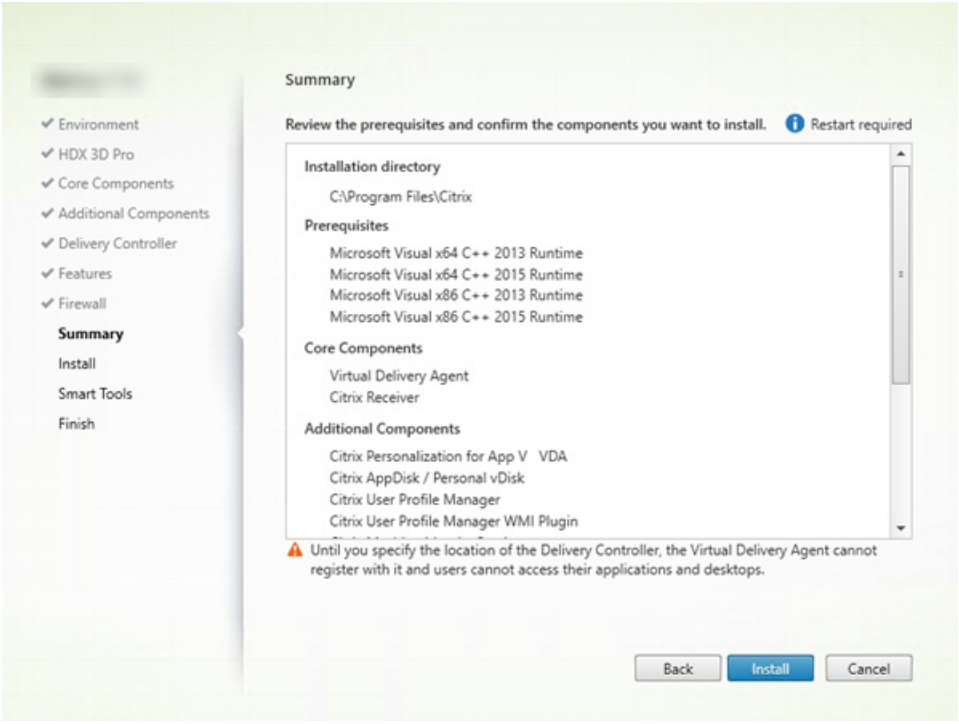
De forma predeterminada, los siguientes puertos se abren automáticamente en la página **Firewall** si el servicio Firewall de Windows se está ejecutando, incluso aunque el firewall no esté habilitado. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Para obtener información acerca de los puertos, consulte Puertos de red.

Haga clic en **Siguiente**.

Opción de la línea de comandos: /enable_hdx_ports

Paso 11. Revise los requisitos previos y confirme la instalación

© 1999-2017 Citrix Systems, Inc. All rights reserved.



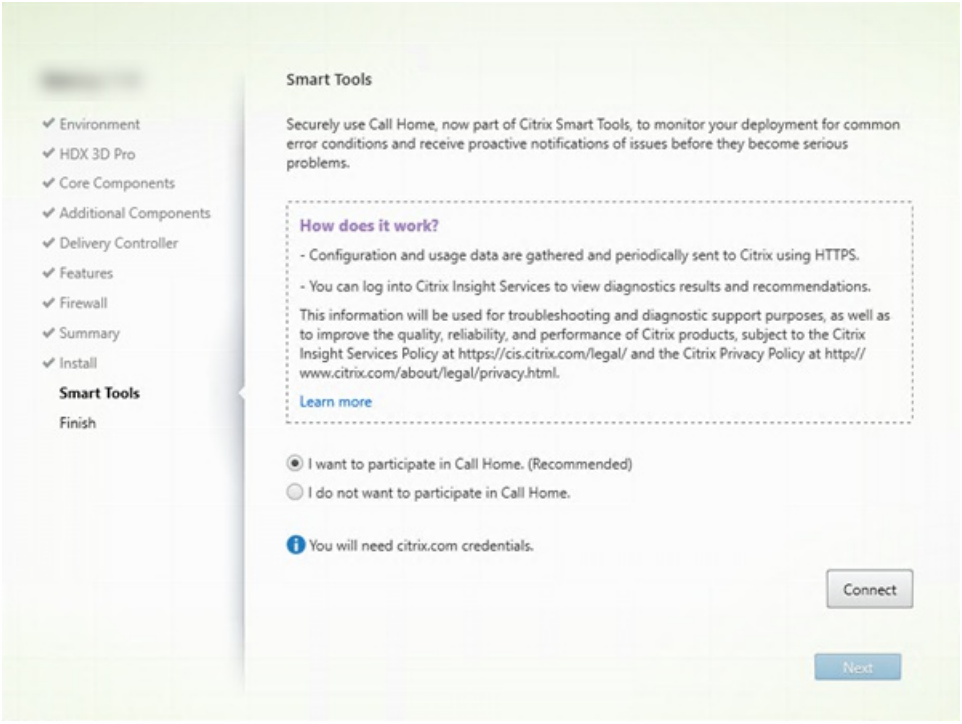
La página **Resumen** muestra lo que se instalará. Puede usar el botón Atrás para volver a las páginas anteriores del asistente y cambiar las opciones.

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 la instalación.

Paso 12. Participar en Smart Tools

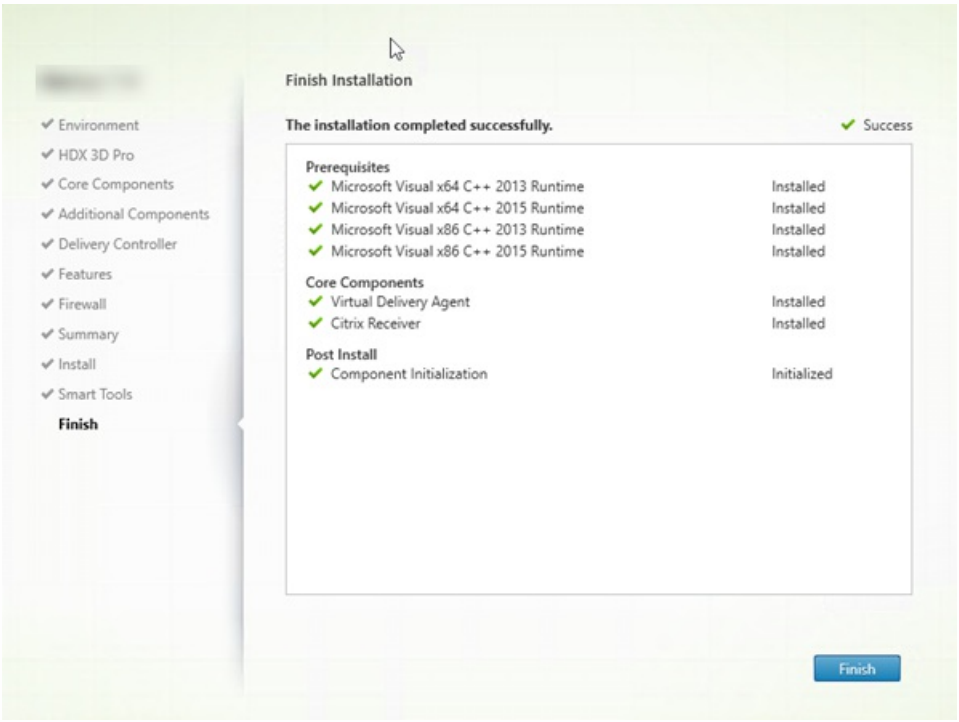
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.

Paso 13. Finalice la instalación



 © 1999-2017 Citrix Systems, Inc. All rights reserved.

La página **Finalizar** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar**. De forma predeterminada, la máquina se reinicia automáticamente. (Aunque puede inhabilitar este reinicio automático, el VDA no se podrá utilizar hasta que se reinicie la máquina.)

Siguiente: Instale los demás VDA y continúe la configuración

Repita los pasos anteriores para instalar agentes VDA en otras máquinas o imágenes si fuera necesario.

Después de instalar todos los VDA, inicie Studio. Si aún no ha creado ningún sitio, Studio le guiará automáticamente cuando lo haga. Una vez que haya terminado, Studio le guiará para crear un catálogo de máquinas y un grupo de entrega. Consulte:

- Crear un sitio
- Crear catálogos de máquinas
- Crear grupos de entrega

Posteriormente, 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 con servicios principales de VDI**. A continuación, haga clic en el botón secundario y seleccione **Cambiar**.
2. Seleccione **Personalizar configuración de Virtual Delivery Agent**. Cuando se inicie el instalador, puede cambiar:

- Direcciones de Controller
- El puerto TCP/IP utilizado para registrarse en el Controller (predeterminado = 80)
- Si abrir automáticamente los puertos del Firewall de Windows

Solución de problemas

Si su implementación usa Microsoft System Center Configuration Manager, la instalación de un VDA puede notificar un error con el código de salida 3, aunque el VDA se haya instalado correctamente. Para evitar este mensaje que da lugar a confusión, puede empaquetar la instalación en un script CMD o cambiar los códigos de éxito en el paquete de Configuration Manager. Para obtener más información, consulte los foros de debate en http://discussions.citrix.com/topic/350000-sccm-install-of-vda-71-fails-with-exit-code-3/.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación mediante línea de comandos

Jan 24, 2018

Lo descrito en este artículo se aplica en caso de instalar componentes en máquinas con sistemas operativos Windows. Para obtener más información acerca de los agentes VDA para sistemas operativos Linux, consulte la documentación de Linux Virtual Delivery Agent.

En este artículo:

- Usar el instalador de producto completo
- Usar el instalador independiente de VDA
- Opciones de línea de comandos para instalar componentes principales
- Ejemplos: Instalar componentes principales
- Opciones de línea de comandos para instalar un VDA
- Ejemplos: Instalar un VDA
- Personalizar un agente VDA mediante línea de comandos
- Instalar Universal Print Server mediante línea de comandos

Importante: En este artículo, se describe cómo emitir comandos de instalación del producto. Antes de comenzar cualquier instalación, consulte el artículo Antes de la instalación. Este artículo contiene las descripciones de los instaladores disponibles.

Para ver el progreso de ejecución del comando y devolver valores, debe ser el administrador original o debe utilizar la opción **Ejecutar como administrador**. Para obtener más información, consulte la documentación de comandos de Microsoft.

Para complementar el uso de los comandos de instalación directamente, se proporcionan scripts de ejemplo en la imagen ISO del producto. Puede usarlos para instalar, actualizar o quitar máquinas VDA de Active Directory. Para obtener más información, consulte Instalación de agentes VDA mediante scripts.

Uso del programa de instalación 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 el comando **XenDesktopServerSetup.exe** con las opciones que aparecen en Opciones de línea de comandos para instalar componentes principales.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para instalar un VDA:

Ejecute el comando **XenDesktopVDASetup.exe** con las opciones que aparecen en Opciones de línea de comandos para instalar un VDA.

Para instalar Universal Print Server:

Siga las instrucciones indicadas en Instalar Universal Print Server mediante línea de comandos.

Para instalar el servicio de autenticación federada:

Citrix recomienda usar la interfaz gráfica.

Para instalar el Autoservicio de restablecimiento de contraseñas:

Siga las instrucciones indicadas en la documentación del Autoservicio de restablecimiento de contraseñas.

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 bien debe usar la opción **Ejecutar como administrador**.

- Descargue el paquete correspondiente de Citrix:

Nombre del componente en la página de descarga	**Nombre del archivo del instalador**
Virtual Delivery Agent de SO de servidor <*versión*>	VDAServerSetup.exe
Virtual Delivery Agent de SO de escritorio <*versión*>	VDAWorkstationSetup.exe
Virtual Delivery Agent de SO de escritorio con los servicios principales <*versión*>	VDAWorkstationCoreSetup.exe

- 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 la opción **/extract** con la ruta absoluta, por ejemplo: .\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia. (El directorio debe existir. De lo contrario, falla la extracción.) 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 <*component*> [,<*component*>] ...

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

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

Impide la instalación de una o varias funciones o tecnologías, separadas por comas y escritas entre comillas. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/help o /h

Muestra la ayuda del comando.

/installdir <*directorio*>

Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

/logpath <*ruta*>

Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. Predeterminado = "%TEMP%\Citrix\XenDesktop Installer"

/no_remote_assistance

Válido solamente cuando se instala Director. Inhabilita la funcionalidad de remedo de usuarios que utiliza la Asistencia remota de Windows.

/noreboot

Impide que se reinicie el sistema después de la instalación. (Para la mayoría de los componentes principales, el reinicio no está habilitado de forma predeterminada.)

/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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/xenapp

Instala el componente XenApp. Si se omite esta opción, se instala XenDesktop.

Ejemplos: Instalar componentes principales

El siguiente comando instala el controlador de XenDesktop, Studio, Citrix Licensing y SQL Server Express en un servidor. Los puertos de firewall necesarios para la comunicación entre componentes se abrirán automáticamente.

\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall

El siguiente comando instala el Controller de XenApp, 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 siguientes comandos: **XenDesktopVDASetup.exe**, **VDAServerSetup.exe**, **VDAWorkstationSetup.exe** o **VDAWorkstationCoreSetup.exe**.

/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. Para obtener más información, consulte Personal vDisk.

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: Citrix Receiver para Windows (CitrixReceiver.exe)

Por ejemplo, para instalar el VDA y no Citrix Receiver, especifique /components vda.

Si se omite esta opción, se instalan todos los componentes.

Esta opción no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe. Ese instalador no puede instalar Citrix Receiver.

/controllers "<*controller*> [<*controller*>] [...]"

Lista de nombres de dominio completos (FQDN) de Controllers, separados por espacios y entre comillas, con los que se puede comunicar el VDA. No especifique las opciones /site_guid y /controllers a la vez.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

/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.

/enable_hdx_3d_pro

Instala el VDA en el modo HDX 3D Pro.

/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.

Sugerencia: 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.

Sugerencia: 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, escritos entre comillas. Por ejemplo, instalar o actualizar un VDA en una imagen que no se administrará mediante Machine Creation Services no requiere los componentes Personal vDisk ni Machine Identity Service. Los valores válidos son:

Personal vDisk

Machine Identity Service

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix User Profile Manager

Citrix User Profile Manager WMI Plugin

Citrix Universal Print Client

Citrix Telemetry Service

Personalización de Citrix para App-V - VDA

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.

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.

/installdir <*directorio*>

Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

/logpath <*ruta*>

Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. Predeterminado = "%TEMP%\Citrix\XenDesktop Installer"

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 no es válida cuando se usa el instalador VDAWorkstationCoreSetup.exe.

/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.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

La mayoría de las ediciones Windows admitidas vienen con Microsoft Media Foundation ya instalado, a excepción de las ediciones N.

/nocitrixwddm

Válido solamente en máquinas Windows 7 que no incluyen un controlador WDDM. Inhabilita la instalación del controlador WDDM de Citrix.

Esta opción no está disponible en la interfaz gráfica.

/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.

/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.

/reconfig

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 solamente para implementaciones de acceso con Remote PC. Excluye la instalación de los componentes

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Esta opción no está disponible en la interfaz gráfica.

Ejemplos: Instalar un VDA

Instalar un VDA con el instalador de producto completo:

El siguiente comando instala un VDA para SO de escritorio y Citrix Receiver en la ubicación predeterminada en una VM. Este VDA se usará como una imagen maestra. El VDA se registrará inicialmente en el Controller en el servidor denominado "Contr-Main" en el dominio "mydomain". Asimismo, el VDA usará discos Personal vDisk, la función de optimización y la Asistencia remota de Windows.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /quiet /components vda,plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /optimize /masterimage /baseimage /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. Citrix Receiver 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 mediante línea de comandos

Después de instalar un VDA, puede personalizar varios parámetros. Desde el directorio \x64\XenDesktop Setup de los medios del producto, ejecute el comando XenDesktopVdaSetup.exe, mediante una o varias de las siguientes opciones, descritas en Opciones de línea de comandos para instalar un VDA.

- /reconfigure (opción necesaria para personalizar un VDA)
- /h o /help
- /quiet
- /noreboot
- /controllers
- /portnumber port
- /enable_hdx_ports

Instalar Universal Print Server mediante línea de comandos

Ejecute alguno de los siguientes comandos en cada servidor de impresión:

- En un sistema operativo de 32 bits compatible: desde el directorio \x86\Universal Print Server\ de los medios de instalación de Citrix, ejecute **UpsServer_x86.msi**.
- En sistemas operativos de 64 bits compatibles: desde el directorio \x64\Universal Print Server\ de los medios de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instalación de Citrix, ejecute **UpsServer_x64.msi**.

Después de instalar el componente Universal Print Server en los servidores de impresión, configúrelo siguiendo las instrucciones de Aprovisionar impresoras.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de agentes VDA mediante scripts

Dec 05, 2017

Este artículo se aplica en caso de instalar agentes VDA en máquinas con sistemas operativos Windows. Para obtener más 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 usan Machine Creation Services y 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 desde la imagen ISO completa del producto es XenDesktopVdaSetup.exe, o bien VDAWorkstationSetup.exe, o bien VDAServerSetup.exe desde el programa de instalación independiente.
- Los detalles de registros se almacenan localmente en cada máquina. Si quiere registrar los resultados en una ubicación centralizada, para poder consultarlos y analizarlos, los scripts necesitan acceso de Lectura y Escritura para Todos en el recurso compartido de red correspondiente.

Para comprobar los resultados de la ejecución de un script, consulte el recurso compartido de registros centralizados. Los registros capturados incluyen el registro del script, el registro del instalador y los registros de instalación de MSI. Cada intento de instalación o eliminación se registra en una carpeta con su fecha y hora. El nombre de la carpeta indica si la operación se realizó o no correctamente, con el prefijo PASS o FAIL, respectivamente. Puede usar herramientas estándar de búsqueda de directorios para buscar una instalación o eliminación fallidas en el recurso compartido de registros centralizados. Esas herramientas ofrecen una alternativa a la búsqueda local en las máquinas de destino.

Importante: Antes de comenzar cualquier instalación, consulte y complete las tareas de Antes de la instalación.

Instalación o actualización de agentes VDA mediante el script

1. Obtenga el script de ejemplo InstallVDA.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 instalar: SET DESIREDVERSION. 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.
   - 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=\\ServidorArchivos1\PuntoCompartido1.
   - Si lo desea, puede especificar también una ubicación en el recurso compartido de red para guardar los registros centralizados. Por ejemplo: SET LOGSHARE=\\ServidorArchivos1\Logs1.
   - Especifique las opciones de configuración del agente VDA como se describe en Instalación mediante línea de comandos. Las opciones /quiet y /noreboot se incluyen de manera predeterminada en el script y son necesarias: SET

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Eliminación de agentes VDA mediante el script

1. Obtenga el script de ejemplo UninstallVDA.bat en el directorio \Support\AdDeploy\ de los medios de instalación. Citrix recomienda realizar una copia de 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.

Solución de problemas

El script genera archivos de registros internos que describen el progreso de la ejecución del script. El script copia un registro llamado Kickoff_VDA_Startup_Script en el recurso compartido de registros centralizados a los pocos segundos de iniciarse la implementación. Eso permite comprobar que el proceso global está funcionando. Si este registro no se copia al recurso compartido de registros centralizados como es de esperar, puede inspeccionar la máquina local para buscar a qué se debe. El script coloca dos archivos de registro de depuración en la carpeta %temp% de cada máquina:

- Kickoff_VDA_Startup_Script_.log
- VDA_Install_ProcessLog_.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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación de un sitio

Dec 05, 2017

Un *sitio* es el nombre que se da a una implementación de XenApp o XenDesktop. 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.

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 ese artículo antes de iniciar el Asistente para la creación de sitios.

Para crear un sitio:

Abra Studio, si aún no está abierto. Se le guiará automáticamente a la acción que inicia el asistente para la creación de sitios. En las páginas del asistente, se cubren las siguientes áreas de configuración:

Nombre y tipo de sitio

Existen dos tipos de sitio. Elija uno:

- **Sitio de entrega de aplicaciones y escritorios**. Cuando crea un sitio de entrega de aplicaciones y escritorios, también puede decidir si crear un sitio de implementación completa (recomendado) o un sitio vacío. Un sitio vacío solo está configurado parcialmente y son los usuarios avanzados los que suelen crearlo.
- **Sitio de acceso con Remote PC**. Un sitio de acceso con Remote PC permite a usuarios designados acceder a sus equipos de oficina de forma remota a través de una conexión segura.

Si crea ahora una implementación de entrega de aplicaciones y escritorios, puede agregar más adelante una implementación de acceso con Remote PC. De igual manera, si ahora crea una implementación de acceso con Remote PC, puede agregar más adelante una implementación completa.

Escriba un nombre para el sitio. Después de crear el sitio, su nombre aparece en la parte superior del panel de navegación de Studio: **Citrix Studio** (*nombre-de-sitio*).

Bases de datos

La página **Bases de datos** contiene opciones para configurar las bases de datos del sitio, de supervisión y 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Controllers al sitio y ya ha instalado el software de Controller en otros servidores, puede agregar esos Controllers desde esta página. Si va a generar scripts para configurar las bases de datos, agregue los Controllers antes de generarlos.

Licencia

Considere la posibilidad de usar las licencias existentes o la prueba gratuita de 30 días que le permite agregar archivos de licencia más tarde. También 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 del asistente hasta que se establezca una conexión con el servidor de licencias.

Administración de energía (solo para acceso con Remote PC)

Consulte Acceso con Remote PC.

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.

Página Conexión: Consulte Fuentes de información sobre tipos de conexión.

> 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.

Páginas Almacenamiento y Red: Consulte Almacenamiento del host, Administración del almacenamiento y Selección de almacenamiento para obtener más información sobre los tipos de almacenamiento y los métodos de administración.

Funcionalidades adicionales

Puede seleccionar funcionalidades 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

> Válido si utiliza AppDisks y ha 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

resolverlos. Para obtener más información, consulte AppDisks.

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.

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 System Center Configuration Manager de Microsoft.

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 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 la información de usuario, haga clic en **Agregar usuarios**. Seleccione los usuarios y los grupos de usuarios y, a continuación, haga clic en **Agregar usuarios**.

  Para agregar datos 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**.

Al crear un sitio de acceso con Remote PC, se crea automáticamente un catálogo de máquinas llamado Cuentas de máquinas de usuario 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.

Resumen

La última página del asistente para la creación de sitios es un resumen de la información especificada. Utilice el botón **Atrás** si quiere cambiar algo. Cuando haya terminado, haga clic en **Crear** y comenzará la creación del sitio.

Pruebe la configuración del sitio

Para ejecutar pruebas después de crear un sitio, seleccione **Citrix Studio (Sitio** *nombre-de-sitio***)** en la parte superior del

© 1999-2017 Citrix Systems, Inc. All rights reserved.

panel de navegación. A continuación, haga clic en **Probar sitio** en el panel central. Puede ver un informe HTML de los resultados de la prueba del sitio.

La prueba de funcionamiento del sitio puede fallar si hay un Controller instalado en Windows Server 2016. El error se produce cuando una base de datos local SQL Server Express se utiliza como la base de datos del sitio y no se ha iniciado el servicio SQL Server Browser. Para evitar este fallo, complete las tareas siguientes.

1. Habilite el servicio SQL Server Browser (si fuera necesario) e inícielo.
2. Reinicie el servicio SQL Server (SQLEXPRESS).

Solución de problemas

Después de configurar el sitio, puede instalar Studio y agregarlo a través de la consola MMC como un complemento en una máquina remota. Si intenta quitar ese complemento más adelante, la consola MMC puede dejar de responder. Como solución temporal, reinicie MMC.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación de catálogos de máquinas

Apr 16, 2018

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 Provisioning Services (PVS). O bien, puede utilizar sus propias herramientas para aprovisionar máquinas.

- Si utiliza Provisioning Services para crear las máquinas, consulte la documentación de Provisioning Services para obtener instrucciones.
- Si elige Machine Creation Services para aprovisionar las máquinas, debe proporcionar una imagen maestra (o instantánea) para crear máquinas virtuales idénticas en el catálogo. Antes de crear el catálogo, primero debe usar las herramientas en el hipervisor o servicio de nube para crear y configurar la imagen maestra. Este proceso incluye instalar un Virtual Delivery Agent (VDA) en la imagen. Después, crea un catálogo de máquinas en Studio. Debe seleccionar esa imagen (o una instantánea de ella), 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 utiliza Machine Creation Services o Provisioning Services 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. Posteriormente, puede ejecutar pruebas en cualquier momento desde Studio.

Solo para implementaciones locales: Si utiliza Machine Creation Services o Provisioning Services 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.

Sugerencia: 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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

registrados pueden derivar en una infrautilización de los recursos disponibles. Existen diversos motivos por los que un VDA puede no estar registrado, 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), puede optar por agregarla de todos modos.

Para ver los mensajes sobre el nivel funcional, consulte Niveles funcionales y versiones de VDA.

Para obtener más información sobre cómo solucionar problemas de registro de VDA, consulte CTX136668.

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 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.

Preparar una imagen maestra en el hipervisor o servicio de nube

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sugerencia: Para obtener más información sobre cómo crear las 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.

Tenga en cuenta:

- 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 pueden usar otros nombres.
- Al usar Provisioning Services, se puede usar una imagen maestra o un equipo físico como dispositivo de destino maestro. Provisioning Services usa una terminología diferente de Machine Creation Services para hacer referencia a las imágenes; consulte la documentación de Provisioning Services para obtener más información.
- Compruebe que el hipervisor o el servicio de nube tienen procesadores, memoria y capacidad de almacenamiento suficientes para admitir la cantidad de máquinas creadas.
- Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo de la máquina.
- Los catálogos de máquinas 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. Si la implementación incluye un VDA de la versión 5.x con un host de XenServer 6.0.2, consulte CTX128580.
- 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 Provisioning Services o Machine Creation Services, no debe ejecutar Sysprep en imágenes maestras.

Para preparar una imagen maestra:

1. Mediante la herramienta de administración del hipervisor, cree una imagen maestra y, a continuación, instale el sistema operativo, además de todos los Service Pack y las actualizaciones. Especifique la cantidad de CPU virtuales. También puede especificar el valor de la CPU virtual si crea el catálogo de máquinas mediante PowerShell. No se puede especificar la cantidad de CPU virtuales si crea el catálogo con Studio. Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Provisioning Services, 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 Provisioning Services.
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.

Preparar una imagen maestra para máquinas que pueden usar GPU en XenServer

Cuando se utiliza XenServer para la infraestructura de alojamiento, las máquinas que pueden utilizar 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. In XenCenter, cree una VM con VGA estándar, redes y vCPU.
2. Actualice la configuración de la máquina virtual para habilitar el uso de GPU (PassThrough o vGPU).
3. Instale un sistema operativo compatible y habilite el protocolo RDP.
4. Instale 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.

Crear un catálogo de máquinas mediante Studio

Antes de iniciar el Asistente para la creación de catálogos de máquinas, consulte esta sección para obtener más información acerca de las decisiones que deberá tomar y la información que deberá facilitar.

Importante: 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

El asistente le guiará a través de los elementos que se describen a continuación. Las páginas del asistente pueden variar según las opciones que escoja.

Sistema operativo

Cada catálogo contiene máquinas de un solo tipo:

- **SO de servidor.** Un catálogo con SO de servidor proporciona 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 con SO de escritorio proporciona aplicaciones y escritorios VDI que se pueden asignar a una variedad de usuarios diferentes.
- **Máquinas de acceso con Remote PC**. Un catálogo de acceso con Remote PC ofrece a los usuarios acceso remoto a sus escritorios físicos de oficina. El acceso con Remote PC no requiere una VPN para proporcionar seguridad.

Administración de máquinas

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

La página **Administración de máquinas** indica cómo se administran las máquinas y con qué herramienta se implementan.

Elija si la administración de energía de las máquinas del catálogo se llevará a cabo a través de Studio.

- Las opciones de energía de las máquinas se administran a través de Studio o se aprovisionan mediante un entorno de nube (por ejemplo, máquinas virtuales o equipos Blade). Esta opción solo está disponible si ya dispone de una conexión configurada a un hipervisor o servicio de nube.
- Las opciones de energía de las máquinas no se administran a través de Studio (por ejemplo, máquinas físicas).

Si ha indicado que las opciones de energía de las máquinas se administran a través de Studio o se aprovisionan mediante un entorno de nube, elija la herramienta que se va a utilizar para crear las máquinas virtuales.

- **Citrix Machine Creation Services (MCS)**. Utiliza una imagen maestra para crear y administrar máquinas virtuales. Los catálogos de máquinas en entornos de nube usan MCS. MCS no está disponible para máquinas físicas.
- **Citrix Provisioning Services (PVS)**. Administra los dispositivos de destino como una colección de dispositivos. Un disco vDisk de Provisioning Services creado a partir de un dispositivo de destino maestro entrega escritorios y aplicaciones. Esta opción no está disponible para los entornos de nube.
- **Otros**. Una herramienta que administra máquinas que ya se encuentran en el centro de datos. Citrix recomienda usar Microsoft System Center Configuration Manager u otra aplicación de terceros para una mayor uniformidad entre las máquinas del catálogo.

Tipos de escritorio (experiencia de escritorio)

Esta página solo aparece cuando se crea un catálogo que contiene máquinas de SO de escritorio.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si elige la segunda opción y usa PVS 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.
- 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.

Imagen maestra

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

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:

- Si utiliza Machine Creation Services o Provisioning Services, no debe ejecutar Sysprep en las imágenes maestras.
- Si especifica una imagen maestra en lugar de una instantánea, Studio creará una instantánea pero usted no le podrá asignar ningún nombre.

Para que pueda utilizar las funciones más recientes del producto, compruebe que la imagen maestra tiene instalada la versión más reciente de VDA. No cambie la selección predeterminada de VDA mínimo. No obstante, si debe usar una versión anterior de VDA, consulte Niveles funcionales y versiones de VDA.

Aparecerá un mensaje de error si selecciona una instantánea o máquina virtual que no sea compatible con la tecnología de administración de la máquina que haya seleccionado antes en el asistente.

Entornos de servicios y plataformas de nube

Si utiliza un servicio o una plataforma de nube (como Azure Resource Manager, Nutanix o Amazon Web Services) para alojar máquinas virtuales, el Asistente para la creación de catálogos de máquinas puede contener páginas específicas para ese host.

Para obtener más información, consulte Dónde encontrar información acerca de los tipos de conexión.

Colección de dispositivos

Esta página solo aparece cuando se utiliza Provisioning Services para crear máquinas virtuales. Muestra los conjuntos de dispositivos y aquellos dispositivos que aún no se han agregado a los catálogos.

Seleccione los conjuntos de dispositivos que va a usar. Para obtener información más detallada, consulte la documentación de Provisioning Services.

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 para crear máquinas:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Especifique la cantidad de máquinas virtuales que se van a crear.
- Seleccione la cantidad de memoria (en MB) que tendrá cada máquina virtual.
- **Importante:** Cada máquina virtual creada tendrá un disco duro. El tamaño está establecido en la imagen maestra y 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.

Si utiliza PVS para crear máquinas:

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 para proporcionar las máquinas:

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 ha indicado máquinas estáticas en la página **Experiencia de escritorio** del asistente, 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 esa página del asistente.

Si utiliza Provisioning Services (PVS) 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 PVS) 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 registrarse correctamente; esta opción 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 XenApp y XenDesktop 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 XenApp y XenDesktop 7.15 LTSR contiene un VDA 7.15, el nivel funcional predeterminado ("7.9 y versiones posteriores") sigue siendo el más actual. Por lo tanto, después de instalar o actualizar los componentes de 7.9-7.14 a 7.15 LTSR, no es necesario cambiar el nivel funcional predeterminado.
>
> En las implementaciones de Citrix Cloud, Studio usa un nivel funcional predeterminado que puede ser anterior a la versión más reciente.

El nivel funcional seleccionado determina la lista anterior de máquinas. En la lista, un cuadro de información situado junto a cada entrada indica si el VDA de la máquina es compatible con el catálogo en ese nivel funcional.

Aparecen mensajes en la página si el VDA de las máquinas no cumple o excede el nivel funcional mínimo seleccionado. Puede continuar con el asistente, pero tenga en cuenta que las máquinas seguramente 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.
- Elegir 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.

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.

Puede especificar si los datos temporales utilizarán un almacenamiento local o compartido al crear la conexión que el catálogo utiliza; para obtener más información, consulte Conexiones y recursos. La habilitación y configuración de 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). Los valores predeterminados difieren en función del tipo de conexión. Por lo general, los valores

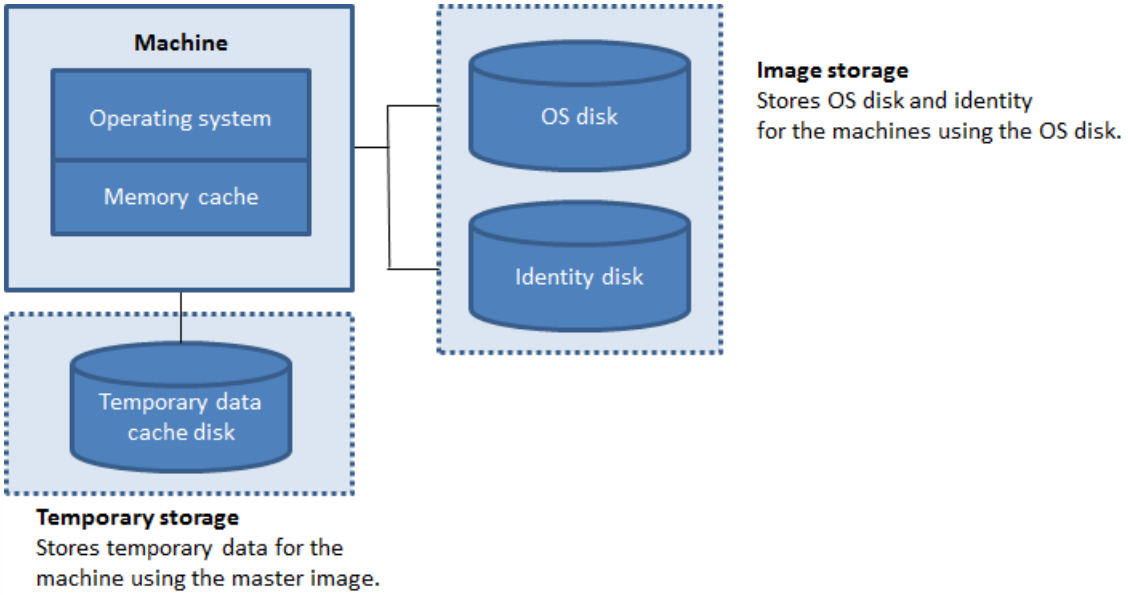
 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 significativamente 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.



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, se debe especificar un valor para **Memoria asignada para caché** que sea lo suficientemente grande para alojar todos los datos temporales; esto es posible solo si hay una gran cantidad de RAM disponible para asignar a cada VM.

Si deja sin marcar ambas casillas, los datos temporales no se guardan en caché. Se escriben en el disco diferencial (ubicado

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Tarjetas de interfaz de red (NIC)

Esta página no aparece cuando se crean catálogos de acceso con Remote PC.

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.

Cuentas de máquina

Esta página solo aparece cuando se crean catálogos de acceso con Remote PC.

Especifique las cuentas de máquina de Active Directory o unidades organizativas (OU) para agregarlas a usuarios o grupos de usuarios. No use barras diagonales (/) en el nombre de una unidad organizativa.

Puede elegir una conexión de administración de energía que haya configurado previamente o puede optar por no usar la administración de energía. Si quiere usar la administración de energía, pero aún no se ha configurado la conexión correspondiente, puede crear dicha conexión más tarde y posteriormente modificar el catálogo de máquinas para actualizar la configuración de la administración de energía.

Cuentas de equipo

Esta página solo aparece cuando se utiliza Machine Creation Services para crear máquinas virtuales.

Cada máquina del catálogo debe tener una cuenta de equipo de Active Directory correspondiente. Indique si se van a crear cuentas nuevas o si se van a utilizar cuentas existentes, además de la ubicación de estas.

- Si opta por crear nuevas 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:

  [ADComputerAccount]
  ADcomputeraccountname.domain

  ...

  Compruebe que hay cuentas suficientes para las máquinas que está agregando. Como Studio es el responsable de

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Provisioning Services, las cuentas de equipo de los dispositivos de destino se administran de forma diferente. Para obtener más información al respecto, consulte la documentación de Provisioning Services.

Resumen, nombre y descripción

En la página **Resumen** del asistente, revise la configuración especificada. Escriba un nombre y una descripción para el catálogo. Esta información se mostrará en Studio.

Después de revisar la información especificada, haga clic en **Finalizar** para iniciar la creación de catálogos.

Solución de problemas

Use la información de esta sección para solucionar los problemas que puedan surgir al trabajar con catálogos de máquinas.

Citrix recomienda recopilar registros para ayudar al equipo de asistencia a ofrecer soluciones; use 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 nueva instantánea.

3. En el DDC, inicie PowerShell con los complementos de Citrix PowerShell cargados y ejecute el siguiente comando:

```
Set-ProvServiceConfigurationData -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 siguientes archivos de la raíz C:\.

- Image-prep.log

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- PvsVmAgentLog.txt

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:

Code COPIAR

```
Remove-ProvServiceConfigurationData -Name ImageManagementPrep_NoAutoShutdown
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administración de catálogos de máquinas

Dec 05, 2017

En este artículo:

- Introducción
- Agregar máquinas a un catálogo de máquinas
- Eliminar máquinas de catálogos de máquinas
- Cambiar la descripción de un catálogo de máquinas o cambiar la configuración de acceso con Remote PC
- Cambiar el nombre catálogos de máquinas
- Transferir un catálogo de máquinas a otra zona
- Eliminar catálogos de máquinas
- Administrar cuentas de equipo de Active Directory en un catálogo de máquinas
- Actualizar un catálogo de máquinas
- Actualizar un catálogo de máquinas

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), puede mantener las máquinas actualizando primero la imagen maestra utilizada en el catálogo y luego las máquinas en sí. Esto permite actualizar de forma eficiente una gran cantidad de máquinas de usuario. Para máquinas creadas con Provisioning Services, las actualizaciones de las máquinas se propagan mediante discos Personal vDisk. Para obtener información más detallada, consulte la documentación de Provisioning Services.
- Para catálogos que contienen máquinas estáticas asignadas de forma permanente y catálogos de máquinas de acceso con Remote PC, puede administrar las actualizaciones de las máquinas de usuarios fuera de Studio, ya sea de forma individual o colectiva mediante herramientas de distribución de software de terceros.

Para obtener más información sobre la creación y la administración de conexiones con hosts de hipervisores y servicios de nube, consulte Conexiones y recursos.

Sugerencia: Para las máquinas que presentan un "Estado de energía desconocido", consulte CTX131267 para obtener instrucciones.

Agregar máquinas a un catálogo de máquinas

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Compruebe que tiene suficientes cuentas de equipo de Active Directory sin usar. Si utiliza cuentas existentes, tenga en cuenta que la cantidad de máquinas que puede agregar se limita a la cantidad de cuentas disponibles.
- Si usa Studio con el fin de crear cuentas de equipo de Active Directory para las máquinas adicionales, debe tener los permisos de administrador de dominio apropiados.

Para agregar máquinas a un catálogo:

1. Seleccione **Catálogos de máquinas** en el panel de navegación de Studio.
2. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en el panel Acciones.
3. Seleccione la cantidad de máquinas virtuales que se van a agregar.
4. Si no hay suficientes cuentas existentes de Active Directory para la cantidad de máquinas virtuales que quiere agregar, seleccione el dominio y la ubicación donde se crearán las cuentas. Especifique un esquema de nombres de cuenta con marcas hash para indicar dónde aparecerán los números o las letras secuenciales. No use barras diagonales (/) en el nombre de una unidad organizativa. Un nombre no puede empezar con un número. Por ejemplo, un esquema de nombres de PC-Ventas-## (con números del 0 al 9 seleccionados) tiene como resultado cuentas de equipo llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.
5. Si usa cuentas existentes de Active Directory, vaya a esas cuentas o haga clic en **Importar** y especifique un archivo CSV que contenga los nombres de cuenta. Compruebe que hay cuentas suficientes para las máquinas que está agregando. 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 catálogos de máquinas

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 impedirá 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.

Cambiar la descripción de un catálogo de máquinas o cambiar la configuración de acceso con Remote PC

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Nota: Para conocer los catálogos para el acceso con Remote PC en un entorno XenApp and XenDesktop Service de Citrix Cloud, siga las instrucciones de CTX220737.

Cambiar el nombre catálogos de máquinas

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.

Transferir un catálogo de máquinas a otra zona

Si la implementación tiene más de una zona, puede mover un catálogo de una zona a otra.

Precaución: 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 catálogos de máquinas

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrar cuentas de equipo de Active Directory en un catálogo de máquinas

Para administrar cuentas de Active Directory en un catálogo de máquinas, puede:

- Liberar cuentas de máquina sin utilizar eliminando cuentas de equipo de Active Directory que haya en catálogos de máquinas de SO de 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.

Nota: 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 de máquinas

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 Provisioning Services, debe publicar un disco Personal vDisk nuevo para aplicar los cambios al catálogo. Para obtener más información, consulte la documentación de Provisioning Services.

Una vez actualizada la máquina, se reinicia automáticamente.

Actualizar o crear una nueva imagen maestra

Sugerencia: Para obtener información acerca de la administración de conexiones, consulte Conexiones y recursos.

Antes de actualizar un catálogo de máquinas, actualice la imagen maestra existente o cree una nueva 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Para máquinas Windows 10, consulte los recursos de optimización cuyos enlaces se ofrecen en *Antes de instalar*.
6. Apague la máquina virtual.
7. Tome una instantánea de la VM y dele un nombre significativo que se reconocerá 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 aplicar.
4. En la página **Estrategia de implantación**, elija cuándo se actualizarán las máquinas del catálogo con la nueva imagen maestra (en el siguiente apagado o inmediatamente). Consulte los siguientes apartados para obtener información más detallada.
5. Compruebe la información de la página de **Resumen** y, a continuación, haga clic en **Finalizar**. Cada máquina se reiniciará automáticamente después de actualizarse.

Sugerencia: 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.

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 a la vez o puede especificar la duración total de tiempo que debería llevar iniciar la actualización de todas las máquinas en el catálogo. Un algoritmo interno determina cuándo se actualiza y se reinicia cada máquina durante ese intervalo.
- **Notificación**. En la lista desplegable de notificaciones, 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.

Reversión de una actualización

Después de aplicar una imagen maestra nueva o actualizada, puede revertirla. Esto puede ser necesario si surgen problemas con las máquinas recién actualizadas. Cuando revierte una actualización, las máquinas del catálogo vuelven a la última imagen funcional. Las nuevas funciones que requieran la nueva imagen ya no estarán disponibles. Al igual que en la implantación, la reversión de una máquina implica un reinicio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Seleccione **Catálogos de máquinas** en el panel de navegación de Studio.
2. Seleccione el catálogo 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.

Actualización o reversión de la versión de un catálogo de máquinas

Actualice el catálogo de máquinas después de actualizar los VDA de las máquinas a una versión más reciente. Citrix recomienda actualizar todos los VDA a la versión más reciente para permitir el acceso a todas las funciones nuevas.

Antes de actualizar un catálogo de máquinas:

- Si utiliza Provisioning Services, debe actualizar la versión de VDA en la consola de Provisioning Services.
- 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. La ficha Detalles en el panel inferior 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación de grupos de entrega

Dec 05, 2017

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. El grupo de entrega especifica los usuarios que pueden usar esas máquinas y las aplicaciones y/o escritorios disponibles para esos usuarios.

Crear un grupo de entrega es el siguiente paso de la configuración de la implementación después de crear un sitio y de crear un catálogo de máquinas. Posteriormente, puede cambiar los parámetros iniciales del primer grupo de entrega y crear otros. Sin embargo, existen funciones y configuraciones que se pueden definir solo cuando se modifica un grupo de entrega, no cuando se crea.

Para el acceso con Remote PC, cuando se crea un sitio, se crea automáticamente un grupo de entrega llamado **Escritorios de acceso con Remote PC**.

Para crear un grupo de entrega:

1. Si ha creado un sitio y un catálogo de máquinas, pero aún no ha creado ningún grupo de entrega, Studio le dirigirá al punto de partida idóneo para crear uno. 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 quitar 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.

Máquinas

Seleccione un catálogo de máquinas y especifique la cantidad de máquinas que quiere usar de ese catálogo.

Tenga en cuenta:

- Al menos una máquina debe permanecer sin uso en el catálogo de máquinas seleccionado.
- Se puede especificar un 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 se denomina 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 las funcionalidades 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

Tipo de entrega

Esta página solo aparece si ha seleccionado un catálogo de máquinas que contiene máquinas estáticas (asignados) de SO de escritorio. Elija **Aplicaciones** o **Escritorios** en la página Tipo de entrega; no se pueden activar 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.

AppDisks

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. (Si selecciona la ficha **Aplicaciones**, ubicada sobre la columna derecha, aparecerán las aplicaciones en un formato similar a un menú Inicio. En cambio, si selecciona la ficha **Paquetes instalados**, aparecerán las aplicaciones en un formato similar a la lista Programas y características.)

Marque una o varias casillas de verificación.

Para obtener más información, consulte el artículo AppDisks.

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. De forma predeterminada, la regla de directiva de derechos de aplicaciones incluye a todos los usuarios; consulte el cmdlet del SDK de PowerShell BrokerAppEntitlementPolicyRule para obtener más detalles.
- Grupos de aplicaciones (si se han configurado).
- Grupos de entrega.
- Aplicaciones.

La lista de usuarios que pueden acceder a una aplicación a través de StoreFront está formada por la intersección de las listas de usuarios indicadas arriba. Por ejemplo, para configurar el uso de una aplicación A para un departamento específico, sin restringir innecesariamente el acceso por parte de otros grupos:

- Use la regla predeterminada de directiva de derechos de aplicaciones que incluye a todos los usuarios.
- Configure la lista de usuarios del grupo de entrega para permitir que todos los usuarios de las oficinas centrales usen cualquiera de las aplicaciones especificadas en el grupo de entrega.
- (Si hay grupos de aplicaciones configurados) Configure la lista de usuarios del grupo de aplicaciones para permitir que los miembros de la unidad de negocio de Administración y Finanzas accedan a las aplicaciones con nombres desde la A a la L.
- Configure las propiedades de la aplicación A para restringir su visibilidad únicamente al personal de Cuentas por cobrar en el departamento de Administración y Finanzas.

Usuarios autenticados y no autenticados

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Autenticados

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 Citrix Receiver. Para grupos de entrega que contengan máquinas de SO de escritorio, puede importar los datos de usuario (una lista de usuarios) después, al modificar el grupo de entrega.

No autenticados (anónimos)

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 Citrix Receiver. Por ejemplo, en máquinas de pantalla completa, 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 AnonXYZ, donde XYZ es un valor único de tres dígitos.

Las sesiones de usuarios no autenticados tienen un valor predeterminado de tiempo de inactividad de 10 minutos, y se cierran automáticamente cuando el cliente se desconecta. No se admiten funciones como la reconexión, la movilidad entre clientes y el control del espacio de trabajo.

En la siguiente tabla, se describen las opciones de la página Usuarios:

Habilitar acceso para	**¿Agregar o asignar usuarios y grupos de usuarios?**	**¿Marcar la casilla "Dar acceso a usuarios no autenticados"?**
Solo usuarios autenticados	Sí	NO
Solo usuarios no autenticados	NO	Sí
Usuarios autenticados y no autenticados	Sí	Sí

Aplicaciones

Tenga en cuenta:

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 Receiver.

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 creada a partir de la imagen maestra en un catálogo de máquinas seleccionado. Cuando se selecciona este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, haga clic en **Aceptar**.
- **Definidas manualmente**. Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Después de introducir la información, haga clic en **Aceptar**.
- **Existentes**. Se trata de aplicaciones agregadas anteriormente al sitio, existentes posiblemente en otro grupo de entrega. Cuando se selecciona este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, haga clic en **Aceptar**.
- **App-V**. Se trata de las aplicaciones presentes en paquetes de App-V. Cuando se selecciona este origen, se abre una nueva página donde se puede seleccionar el servidor 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 el artículo 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.

Escritorios (o reglas de asignación de escritorios)

El título de esta página depende del catálogo de máquinas que haya elegido anteriormente en el asistente:

- Si eligió un catálogo con máquinas agrupadas, esta página se llamará Escritorios.
- Si eligió un catálogo con máquinas asignadas y especificó "Escritorios" en la página Tipo de entrega, esta página se llamará Asignaciones de usuarios de escritorios.
- Si eligió un catálogo con máquinas asignadas y especificó "Aplicaciones" en la página Tipo de entrega, esta página se llamará Asignaciones de usuarios de máquinas de aplicación.

Haga clic en **Add**. En el cuadro de diálogo:

- En los campos Nombre simplificado y Descripción, escriba la información que se verá en Receiver.
- 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. (Consulte el artículo Etiquetas para obtener más información.)
- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

los usuarios que puedan acceder a ese grupo de entrega, o bien, grupos de usuarios y usuarios específicos.

- Si el grupo contiene máquinas asignadas, especifique la cantidad máxima de escritorios por usuario. Este debe ser un valor de uno o más.
- Habilite o inhabilite el escritorio (para máquinas agrupadas) o la regla de asignación de escritorios (para máquinas asignadas). Si inhabilita un escritorio, este deja de entregar escritorios; inhabilitar una regla de asignación de escritorios detiene la asignación automática de escritorios a los usuarios.
- Cuando haya finalizado con el cuadro de diálogo, haga clic en **Aceptar**.

Resumen

Escriba un nombre para el grupo de entrega. También puede especificar una descripción (opcional), que aparecerá en Receiver y en Studio.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administración de grupos de entrega

Dec 05, 2017
En este artículo:

- Introducción
- Cambiar la configuración de usuario en un grupo de entrega
- Agregar o eliminar usuarios de un grupo de entrega
- Cambiar el tipo de entrega de un grupo de entrega
- Cambiar direcciones de StoreFront
- Agregar, modificar o eliminar una restricción de etiqueta para un escritorio
- Actualizar o revertir la versión de un grupo de entrega
- Administrar grupos de entrega de acceso con Remote PC
- Apagar y reiniciar máquinas en un grupo de entrega
- Administrar la energía de las máquinas de un grupo de entrega
- Crear una programación de reinicios para las máquinas de un grupo de entrega
- Crear varias programaciones de reinicios para las máquinas de un grupo de entrega
- Impedir que los usuarios se conecten a una máquina (modo de mantenimiento) en un grupo de entrega
- Cambiar asignaciones de máquinas a usuarios en un grupo de entrega
- Cambiar la cantidad máxima de máquinas por usuario en un grupo de entrega
- Administrar la carga de las máquinas de un grupo de entrega
- Quitar una máquina de un grupo de entrega
- Restringir el acceso a máquinas en un grupo de entrega
- Actualizar una máquina en un grupo de entrega
- Cerrar o desconectar una sesión, o enviar un mensaje a los usuarios de un grupo de entrega
- Configurar el preinicio y la persistencia de sesiones

Introducción

Este artículo describe los procedimientos para la administración de 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.

Consulte Aplicaciones para obtener información sobre cómo administrar aplicaciones en los grupos de entrega, incluido cómo agregar y quitar aplicaciones de un grupo de entrega, y cambiar las propiedades de las aplicaciones.

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.

Sugerencias:

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Registro de VDA en un Delivery Controller

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. En otras palabras, una o varias máquinas que están activadas y no están en modo de mantenimiento, pero no están actualmente registradas en el Controller. Al ver una máquina que "no está registrada pero debería estarlo", consulte la ficha Solución de problemas del panel 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 más información sobre cómo solucionar problemas de registro de VDA, consulte CTX136668.

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 de entrega y, a continuación, seleccione **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, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Parámetro	**Descripción**
Descripción	El texto que utiliza 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	Protege las comunicaciones desde y hacia las máquinas del grupo de entrega mediante SecureICA, que cifra el protocolo ICA (el valor predeterminado es 128 bits; el nivel se puede cambiar con 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Agregar o eliminar usuarios de un grupo de entrega

Para obtener información detallada acerca de los usuarios, consulte la sección Usuarios en el artículo "Crear grupos de entrega".

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Usuarios**, para agregar usuarios, haga clic en **Agregar** y, a continuación, especifique los usuarios que quiere agregar. Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, haga clic en **Quitar**. También puede marcar o desmarcar la casilla de verificación que permite o deniega el acceso a usuarios no autenticados.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o haga 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, seleccione **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Asignación de máquinas**, seleccione **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, o haga 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 del grupo.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Tipo de entrega**, seleccione el tipo de entrega que quiera.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cambiar direcciones de StoreFront

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en el panel Acciones.
3. En la página **StoreFront**, seleccione o agregue direcciones URL de StoreFront que utilizará el Citrix Receiver instalado en cada máquina del grupo de entrega.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

También puede especificar la dirección de servidor StoreFront. Para ello, deberá seleccionar **Configuración > StoreFront** en el panel de navegación de Studio.

Agregar, modificar o eliminar una restricción de etiqueta para un escritorio

Importante: Agregar, modificar o eliminar restricciones de etiqueta puede tener efectos no esperados en los escritorios que se tengan en cuenta para el inicio. No olvide consultar las precauciones y los aspectos a tener en cuenta en el artículo Etiquetas.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **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 quitar una restricción de etiqueta, seleccione otra etiqueta 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.

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 Provisioning Services, debe actualizar la versión de VDA en la consola de Provisioning Services.
- 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y seleccione **Actualizar grupo de entrega** en el panel Acciones. La acción **Actualizar grupo de entrega** solo aparece si Studio detecta agentes VDA actualizados.

Antes de iniciar el proceso de actualización, Studio le indica cuál de las máquinas no se puede actualizar y por qué (si las hubiera). 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, seleccione **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 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):

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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, 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.
- **Apague.** Solicita al sistema operativo que se apague.

Para acciones no forzadas, si la máquina no se apaga en un plazo de 10 minutos, se le obliga a apagarse. Si Windows intenta instalar actualizaciones durante el cierre, 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 el artículo Conexiones y recursos.

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 físicas (incluidas las máquinas de acceso con Remote PC). Las máquinas con 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 reinicio, que también se describe en este artículo.

En grupos de entrega que contengan máquinas agrupadas, las máquinas de SO de escritorio virtual 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 de SO de escritorio virtual 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. Gracias a eso, 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 según el momento del día. En caso de grupos de entrega estáticos, utilice el SDK para configurar la agrupación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (un porcentaje del tamaño del grupo de entrega). En el caso de grupos de entrega grandes, se puede activar una cantidad considerable de máquinas cuando se supera el umbral. Por eso, debería planificar a conciencia los tamaños de los grupos de entrega o utilizar el SDK para ajustar el tamaño predeterminado del búfer.

Temporizadores de estado de energía. Puede usar temporizadores de estado de energía para suspender máquinas después de que los usuarios se hayan desconectado durante un período de tiempo especificado. Por ejemplo, las máquinas se suspenderán automáticamente fuera del horario de oficina si los usuarios han estado desconectados durante, al menos, 10 minutos. Las máquinas aleatorias o las máquinas con discos Personal vDisk se apagan automáticamente cuando los usuarios cierran sesión, a menos que se configure la propiedad de grupo de entrega ShutdownDesktopsAfterUse en el SDK.

Se pueden configurar temporizadores para los días de la semana y para los fines de semana, para intervalos de horas punta y viceversa.

Administración parcial de energía en máquinas de asignación permanente. En el 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 de entrega y, a continuación, seleccione **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 días de la semana a los días de lunes a viernes.
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: En **Durante horas punta - Cuando está desconectado**, especifique la demora (en minutos) antes de suspender una máquina desconectada del grupo de entrega y seleccione Suspender. En **Durante horas normales - Cuando está desconectado**, especifique la demora 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, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Use el SDK para:

- Apagar (en lugar de suspender) las máquinas en respuesta a los temporizadores de estado de energía, o si prefiere que los temporizadores se basen en los cierres de sesión en lugar de basarse en las desconexiones.
- Cambiar las definiciones predeterminadas de días de la semana y días de fin de semana.
- Inhabilite la administración de energía; consulte CTX217289.

Crear una programación de reinicios para las máquinas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de un grupo de entrega

Nota: En esta sección, se describe cómo configurar una programación de reinicios en Studio. De forma alternativa, puede utilizar PowerShell para configurar varias programaciones de reinicios dirigidos a subconjuntos distintos de máquinas en un grupo de entrega. Consulte la sección siguiente para obtener más información.

Una programación de reinicios especifica cuándo reiniciar periódicamente todas las máquinas de un grupo de entrega.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Programación de reinicios**, si no quiere reiniciar automáticamente las máquinas del grupo de entrega, seleccione el botón de radio **No** y vaya al último paso de este procedimiento. No se definirá ninguna programación de reinicios ni estrategia de implantación. Si ya se había definido una programación, esta selección la cancelará.
4. En cambio, si quiere reiniciar automáticamente las máquinas del grupo de entrega, seleccione el botón de radio **Sí**.
5. Para la frecuencia de reinicio, en **Reiniciar**, elija **Cada día** o el día de la semana en que se llevará a cabo el reinicio.
6. En **Empezar el reinicio a**, con la ayuda del reloj de 24 horas, especifique la hora del día en que se comenzará el proceso de reinicio.
7. Para la **Duración de reinicio**, elija si todas las máquinas deben iniciarse al mismo tiempo, o bien elija la longitud total de tiempo para empezar a reiniciar todas las máquinas del grupo de entrega. Un algoritmo interno determina cuándo se reinicia cada máquina durante ese intervalo.
8. En la lista desplegable **Notificación**, situada a la izquierda, 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 la lista desplegable **Repetir notificación**) si repetir el mensaje cada cinco minutos después del primer mensaje. De forma predeterminada, el mensaje no se repite.
9. Escriba el texto de notificación en el cuadro **Mensaje de notificación**; no hay texto predeterminado. Si quiere que el mensaje contenga el número de minutos que quedan antes del reinicio, incluya la variable **%m%** (por ejemplo, Advertencia: El equipo se reiniciará automáticamente en %m% minutos). Si selecciona un intervalo de repetición de notificaciones y su mensaje contiene el marcador de posición %m%, 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 del grupo de entrega en el momento correspondiente antes de que empiece el reinicio, calculado por un algoritmo interno.
10. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Desde Studio, no se puede llevar a cabo el encendido o apagado automatizado, sino solo un reinicio.

Crear varias programaciones de reinicios para las máquinas de un grupo de entrega

Puede usar los cmdlets de PowerShell para crear varias programaciones de reinicios de las máquinas que haya en un grupo de entrega. Todas las programaciones se pueden configurar para que solo afecten a las máquinas del grupo que tengan una etiqueta concreta. Esta funcionalidad de restricciones de etiqueta permite crear fácilmente programaciones de reinicios diferentes para subconjuntos distintos de máquinas en un grupo de entrega.

Por ejemplo, supongamos que utiliza un grupo de entrega para todas las máquinas de la empresa. Quiere reiniciar todas las

© 1999-2017 Citrix Systems, Inc. All rights reserved.

máquinas al menos una vez por semana (el domingo por la noche), pero las máquinas que utiliza el departamento de contabilidad deben reiniciarse todos los días. Puede configurar una programación semanal para todas las máquinas y una programación diaria solo para las máquinas que utilice el departamento de contabilidad.

Superposición de programaciones

Es posible que las programaciones se solapen. En el ejemplo anterior, las máquinas que use el departamento de contabilidad se verán afectadas por ambos reinicios programados, por lo que es posible que se reinicien 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 ambas 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/o la duración, más probable será que haya dos reinicios. Además, 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 reinicia todas las máquinas puede iniciar los reinicios mucho más rápidamente que el reinicio diario programado (según la duración configurada para cada uno).

Requisitos

Actualmente, la creación de varias programaciones de reinicios y el uso de restricciones de etiqueta en una programación de reinicios solo se admite y está disponible con la línea de comandos de PowerShell, mediante los cmdlets RebootScheduleV2 de PowerShell que se han introducido recientemente en XenApp y XenDesktop 7.12. (Se conocen como cmdlets "V2" en este artículo.)

Requisitos para utilizar los cmdlets V2:

- Delivery Controller 7.12 (mínimo).
  - Si utiliza la versión más reciente del plugin de SDK con un Controller anterior a 7.12, las programaciones nuevas que cree no funcionarán según lo esperado.
  - En un sitio mixto (donde se hayan actualizado algunos Controllers pero no todos), los cmdlets V2 no funcionarán hasta que se actualice la base de datos y al menos un Controller se haya actualizado y se esté utilizando (al especificar la opción – adminaddress con los cmdlets V2).
  - Se recomienda no crear programaciones nuevas hasta que todos los Controllers del sitio se hayan actualizado.
- El complemento del SDK de PowerShell que se proporciona con XenDesktop y XenApp 7.12 (mínimo). Después de instalar o actualizar los componentes y el sitio, ejecute el complemento Add-PSSnapin Citrix.* para cargar los cmdlets de la versión más reciente.

Studio utiliza los cmdlets RebootSchedule V1 de PowerShell, por lo que no mostrará las programaciones que se creen con cmdlets V2.

Después de crear una programación de reinicios que use una restricción de etiqueta y luego usar Studio para quitar la etiqueta de una máquina afectada durante un intervalo de reinicios (ciclo) o agregar la etiqueta a otras máquinas durante un ciclo de reinicios, estos cambios no surtirán efecto hasta que comience el siguiente ciclo de reinicios. (Los cambios no afectarán al ciclo actual de reinicios.)

Cmdlets de PowerShell

Utilice los siguientes cmdlets RebootSchedule V2 desde la línea de comandos para crear varias programaciones y usar restricciones de etiqueta en ellas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cmdlet nuevo (V2)	Reemplaza el cmdlet anterior (V1)
New-BrokerRebootScheduleV2	New-BrokerRebootSchedule
Get-BrokerRebootScheduleV2	Get-BrokerRebootSchedule
Set- BrokerRebootScheduleV2	Set-BrokerRebootSchedule
Remove-BrokerRebootScheduleV2	Remove-BrokerRebootSchedule
Rename-BrokerRebootScheduleV2	-

Para conocer la sintaxis completa de los cmdlets y ver las descripciones de los parámetros, introduzca **Get-Help –full** <*nombre-de-cmdlet*>.

Aviso de terminología: En el SDK de PowerShell, el parámetro DesktopGroup identifica al grupo de entrega.

Si conoce la interfaz de Studio para crear una programación de reinicios, conocerá todos los parámetros disponibles cuando use el cmdlet V2 para crear o actualizar una programación. Además, puede:

- Restringir la programación a las máquinas que tengan una etiqueta especificada.
- Especificar un intervalo antes de enviar el primer mensaje de advertencia, durante el que no se intermediará ninguna sesión nueva a las máquinas afectadas.

Configuración

Si configura una programación de reinicios que usa una restricción de etiqueta, también deberá agregar (aplicar) esa etiqueta a las máquinas a las que esa programación debería afectar. (Para obtener más información, consulte Etiquetas.)

1. Desde Studio, seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione el grupo de entrega que contiene las máquinas a las que afectará la programación.
3. Seleccione "Ver máquinas" y, a continuación, seleccione las máquinas a las que agregará la etiqueta.
4. Seleccione **Administrar etiquetas** en el panel Acciones.
5. Si la etiqueta ya existe, marque la casilla de verificación situada junto al nombre de la etiqueta. En cambio, si la etiqueta no existe, haga clic en **Crear** y, a continuación, especifique un nombre para la etiqueta. Una vez creada, marque la casilla de verificación situada junto al nombre de la etiqueta recién creada.
6. Haga clic en **Guardar** en el cuadro de diálogo Administrar etiquetas.

Después de crear y agregar (aplicar) etiquetas, use el parámetro –RestrictToTag para especificar el nombre de la etiqueta al crear o modificar la programación con el cmdlet V2.

Si había creado una programación de reinicios con una versión anterior de XenApp o XenDesktop

Actualmente, Studio utiliza los cmdlets RebootSchedule V1. Si tiene una programación de reinicios creada antes de actualizarse a 7.12 (versión mínima), puede seguir administrándola desde Studio con cmdlets V1, pero no podrá usar Studio para agregar una restricción de etiqueta a esa programación ni para crear programaciones adicionales (porque Studio no admite los cmdlets V2). Mientras use los cmdlets V1, Studio mostrará la información correcta acerca de la programación de

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

reinicios.

De forma alternativa, puede modificar su programación desde la línea de comandos, con los nuevos cmdlets RebootSchedule V2. Con los cmdlets V2, podrá usar la restricción de etiqueta en las programaciones, así como crear programaciones de reinicios adicionales. Sin embargo, después de usar cmdlets V2 para cambiar su programación, Studio no mostrará la información completa de esa programación (porque solo reconocerá la información V1). No podrá verificar si se usa una restricción de etiqueta ni tampoco verá el nombre y la descripción de la programación.

Impedir que los usuarios se conecten a una máquina (modo de mantenimiento) en un grupo de entrega

Cuando tenga que detener temporalmente las conexiones nuevas a las máquinas, puede activar el modo de mantenimiento para una o todas las máquinas de un grupo de entrega. Puede hacerlo antes de aplicar revisiones o mediante herramientas de administración.

- Cuando una máquina con SO de servidor está en modo de mantenimiento, los usuarios pueden conectarse a las sesiones existentes, pero no pueden iniciar sesiones nuevas.
- Cuando una máquina con SO de escritorio (o un PC de acceso con Remote PC) está en modo de mantenimiento, los usuarios no pueden conectarse o volver a conectarse. Las conexiones actuales permanecen conectadas hasta que se desconectan o cierran sesión.

Para activar o desactivar el modo de mantenimiento:

1. Seleccione **Grupos de entrega** en el panel de navegación 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 con 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.
- 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 (lo que afecta a las máquinas que usan dicha conexión) o de un catálogo de máquinas (lo que afecta a las máquinas de ese catálogo).

Cambiar asignaciones de máquinas a usuarios en un

© 1999-2017 Citrix Systems, Inc. All rights reserved.

grupo de entrega

Solo es posible cambiar las asignaciones de máquinas de SO de escritorio, no máquinas de SO de servidor ni máquinas creadas con Provisioning Services.

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** (solo una de ambas páginas estará disponible, en función 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, o haga 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 de entrega y, a continuación, seleccione **Modificar grupo de entrega** en el panel Acciones.
3. En la página **Reglas de asignación de escritorio**, establezca el valor de cantidad máxima de escritorios por usuario.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o haga 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 con 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:

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 Máquina, seleccione Índice de carga.

En el SDK, use el cmdlet Get-BrokerMachine. Para obtener más información, consulte CTX202150.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Cómo quitar una máquina de un grupo de entrega

Al quitar una máquina, se elimina de un grupo de entrega, pero no 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.

Tenga en cuenta que las máquinas pueden contener datos personales, así que actúe con precaución a la hora de asignar una máquina a otro usuario. Es posible que quiera volver a crear una imagen de la máquina.

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. Asegúrese de que la máquina se apaga.
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 proporcione acceso solamente a ciertas aplicaciones. Para obtener información más detallada, consulte el artículo Administración delegada.

Restringir el acceso a usuarios a través de las expresiones de directiva de SmartAccess para filtrar las conexiones de usuario realizadas a través de NetScaler Gateway.

1. Seleccione **Grupos de entrega** en el panel de navegación de Studio.
2. Seleccione un grupo de entrega y seleccione **Modificar grupo de entrega** en el panel Acciones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 NetScaler Gateway y agregue, modifique o quite las expresiones de directiva de SmartAccess para las situaciones de acceso autorizado de los usuarios. Para obtener información más detallada, consulte la documentación de NetScaler Gateway.
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.

Restringir el acceso de los usuarios a través de los filtros de exclusión en las directivas de acceso que usted estableció en el SDK. Las directivas de acceso se aplican a grupos de entrega para limitar las conexiones. Por ejemplo, puede restringir el acceso a las máquinas por parte de un subconjunto de usuarios. También puede especificar los dispositivos de usuario permitidos. El uso de filtros de exclusión permite definir más detalladamente las directivas de acceso. Por ejemplo, por razones de seguridad, puede negar el acceso a un subconjunto de usuarios o dispositivos. De forma predeterminada, los filtros de exclusión están inhabilitados.

Por ejemplo: en el caso de un laboratorio escolar ubicado en una subred dentro de la red corporativa, para impedir el acceso desde ese laboratorio a un determinado grupo de entrega, independientemente del usuario que utilice las máquinas del laboratorio, use el comando 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 está conectado mediante un explorador web o con la funcionalidad de experiencia de usuario unificada de Citrix Receiver 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: cuándo actualizar la imagen maestra (ahora o en el siguiente reinicio), la hora de distribución de reinicios (el total de tiempo para iniciar la actualización de todas las máquinas de un grupo) y si se notificará a los usuarios del reinicio, además del mensaje que recibirán.

Cerrar o desconectar una sesión, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
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.

Es posible configurar temporizadores de estado de energía de las máquinas con SO de escritorio para gestionar automáticamente las sesiones que no se estén utilizando. Consulte la sección Administración de energía de las máquinas para obtener más información.

Configuración del preinicio de sesiones y la persistencia de sesiones en un grupo de entrega

Estas funciones 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, como mínimo, un VDA 7.6 para SO de servidor Windows.
- Estas funciones se admiten solamente cuando se usa Citrix Receiver para Windows, y también necesitan una configuración adicional de Citrix Receiver. Para obtener instrucciones, busque preinicio de sesiones en la documentación de producto correspondiente a la versión de Citrix Receiver para Windows de que dispone.
- Tenga en cuenta que no se admite Citrix Receiver 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 o sesiones, pero, si un usuario cierra la sesión de Citrix Receiver, 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).
- 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 Citrix Receiver.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Los puede configurar 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 aparecerá en la pantalla de Studio de ese grupo de entrega o en el asistente 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 provocarán conexiones denegadas porque estas finalizarán de forma automática cuando los recursos sean necesarios para sesiones de usuario nuevas.

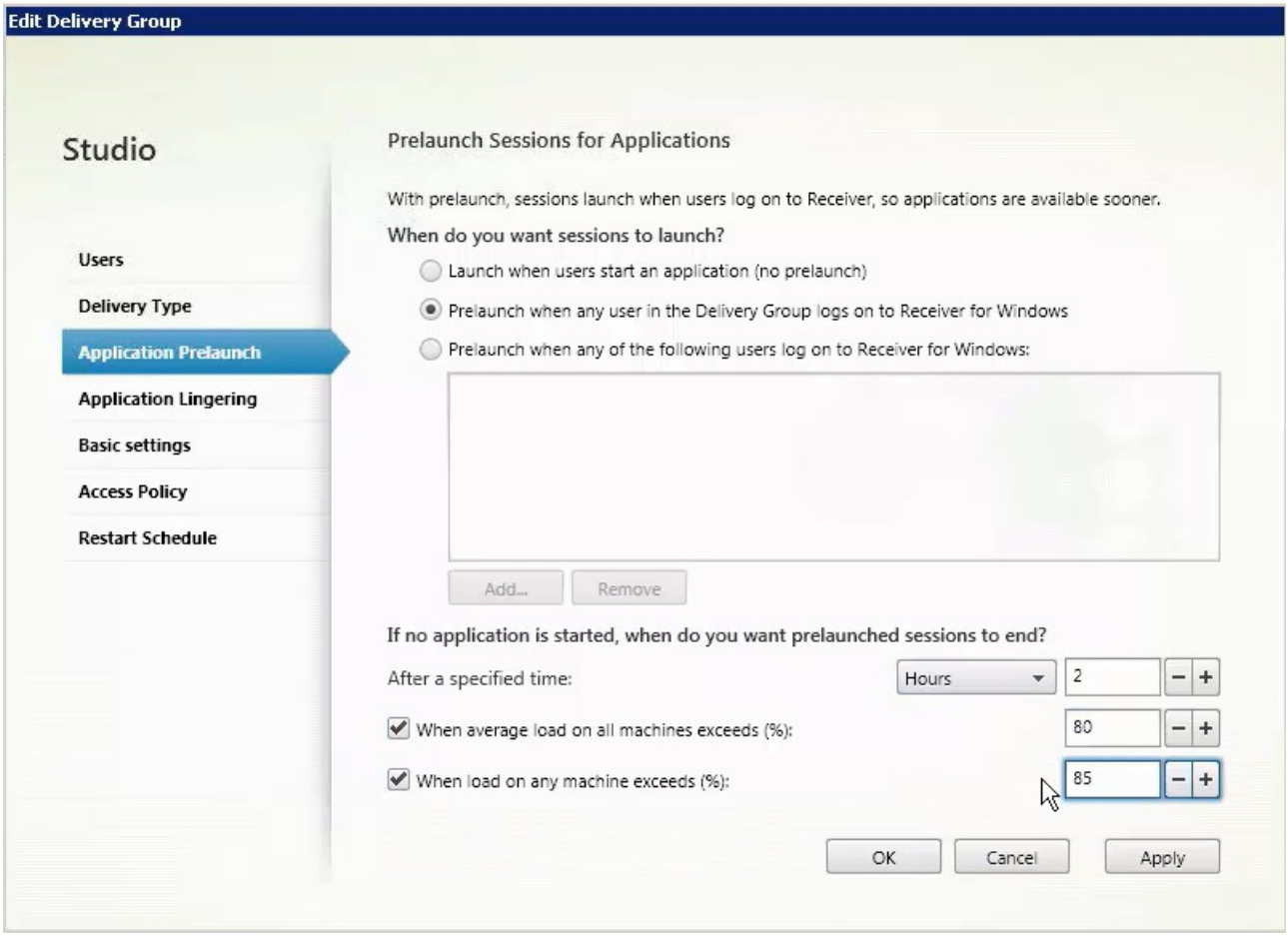
  Puede configurar dos umbrales: el porcentaje medio de carga de todos los servidores del grupo de entrega y el porcentaje máximo de carga de un servidor único del grupo de entrega. Cuando se supera un umbral, se finalizan aquellas sesiones que hayan tenido el estado de preinicio o persistente durante más tiempo. Las sesiones se finalizan una a una con intervalos de minutos entre cada cierre hasta que la carga baja por debajo del umbral. (Mientras el umbral permanezca rebasado, no se iniciará ninguna sesión de preinicio.)

Los servidores con VDA que no se hayan registrado con el Controller y los servidores en el modo de mantenimiento se consideran servidores con carga completa. Una interrupción no planificada tendrá como consecuencia la finalización automática de sesiones de preinicio y sesiones persistentes para liberar capacidad.

Para habilitar la función de preinicio de sesiones

1. Seleccione **Grupos de entrega** en el panel de navegación 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 **Preinicio de aplicaciones**, habilite el preinicio de sesiones. Para ello, elija cuándo deben iniciarse estas:
   - Cuando un usuario inicia una aplicación. Este es el parámetro predeterminado; el preinicio de sesiones está inhabilitado.
   - Cuando un usuario del grupo de entrega inicia sesión en Citrix Receiver para Windows.
   - Cuando alguien de una lista de usuarios y grupos de usuarios inicia sesión en Citrix Receiver para Windows. Si elige esta opción, compruebe que ha especificado también los usuarios o los grupos de usuarios.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



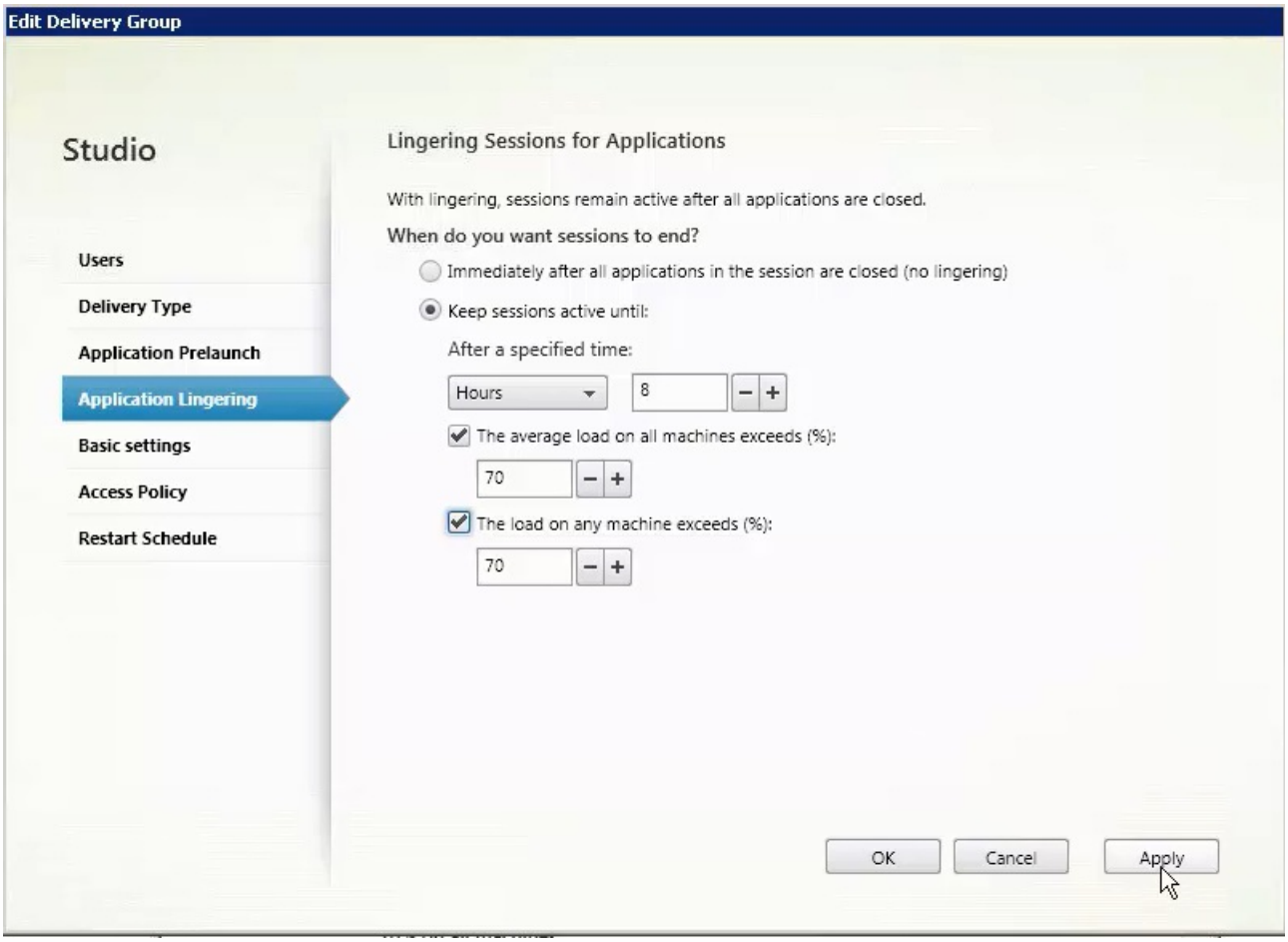
4. Una sesión preiniciada se reemplaza por una sesión habitual cuando el usuario inicia una aplicación. Si el usuario no inicia una aplicación (es decir, la sesión preiniciada no se llega a utilizar), la siguiente configuración afecta a la cantidad de tiempo que esta sesión permanece activa.
   - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo (de 1 a 99 días, de 1 a 2376 horas, o de 1 a 142560 minutos).
   - Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado (del 1 al 99 %).
   - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado (del 1 al 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 de entrega 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Algunos parámetros influyen en la cantidad de tiempo que las sesiones persistentes pueden permanecer activas si el usuario no inicia otra aplicación.
   - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo (de 1 a 99 días, de 1 a 2376 horas, o de 1 a 142560 minutos).
   - Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado (del 1 al 99 %).
   - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado (del 1 al 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación de grupos de aplicaciones

Dec 05, 2017

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:

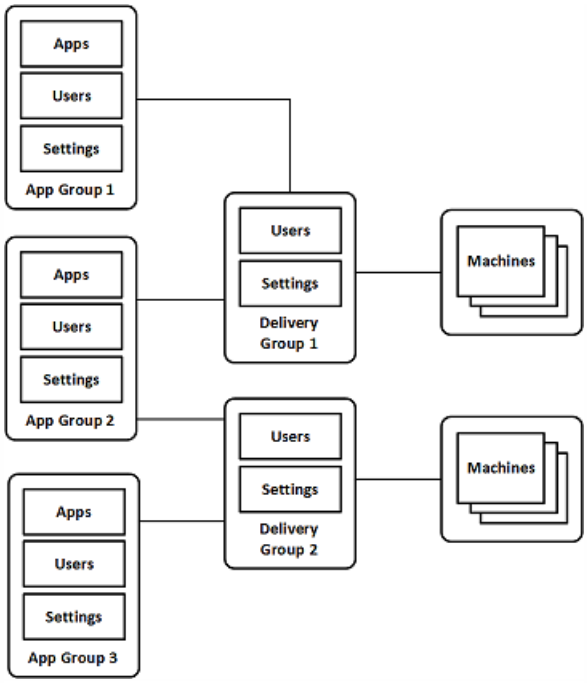
- La agrupación lógica de las aplicaciones y sus parámetros permite administrar esas aplicaciones como una sola unidad. Por ejemplo, no tiene que agregar (publicar) la misma aplicación en grupos de entrega individuales de uno en uno.
- El uso compartido de sesiones entre grupos de aplicaciones puede limitar 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 funcionalidad *restricción de etiqueta* para publicar aplicaciones desde un grupo de aplicaciones teniendo en cuenta para ello solo un subconjunto de las máquinas en 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 XenApp o XenDesktop que incluye grupos de aplicaciones:

© 1999-2017 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.)

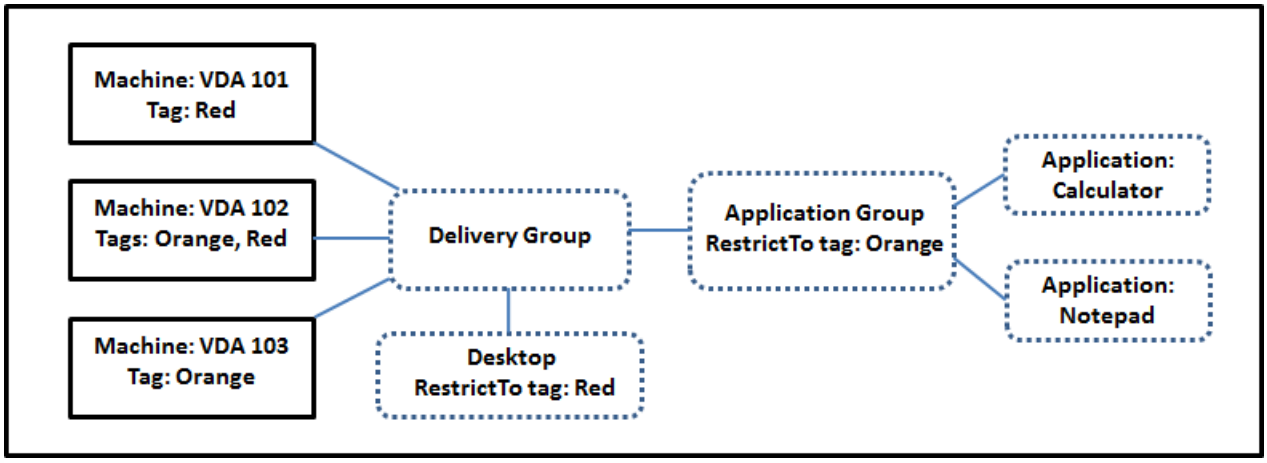
El grupo de aplicaciones 1 está asociado al grupo de entrega 1. A las aplicaciones del Grupo de aplicaciones 1 tienen acceso los usuarios especificados en el Grupo de aplicaciones 1, siempre y cuando también estén en la lista de usuarios del Grupo de entrega 1. Esto es conforme a la recomendación de 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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 el artículo 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 el artículo Administración de grupos de aplicaciones.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones; consulte Uso compartido de sesiones entre grupos de aplicaciones.

Citrix recomienda que los grupos de entrega se actualicen a la versión actual. Esto requiere (1) actualizar los VDA de las máquinas utilizadas en el grupo de entrega; a continuación, (2) actualizar los catálogos de máquinas que contienen esas máquinas, y después (3) actualizar el grupo de entrega. Para obtener más información, consulte Administración de 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 el artículo 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.

Uso compartido de sesiones entre grupos de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Uso compartido de sesiones entre grupos de aplicaciones

Puede permitir que las sesiones de aplicaciones se compartan entre los grupos de aplicaciones, o bien, puede inhabilitarlo para limitar la capacidad de compartir sesiones solo a las aplicaciones que se encuentren en el mismo grupo de aplicaciones.

Este es un ejemplo de cuándo puede ser útil habilitar el uso compartido de sesiones entre los grupos de aplicaciones:

> El grupo de aplicaciones 1 contiene aplicaciones de Microsoft Office como Word y Excel. El grupo de aplicaciones 2 contiene otras aplicaciones (como el Bloc de notas y la Calculadora), y ambos grupos de aplicaciones están conectados al mismo grupo de entrega. Un usuario que tiene acceso a ambos grupos de aplicaciones inicia una sesión de aplicación 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:

> Suponga que 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.

IMPORTANTE: El uso compartido de 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, el uso compartido de sesiones de aplicaciones entre grupos de aplicaciones se habilita cuando se crea un grupo de aplicaciones; esto no se puede cambiar cuando se crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro; consulte el artículo Administración de grupos de aplicaciones.

Cómo 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, las aplicaciones pueden compartir sesiones cuando se crea un grupo de aplicaciones; este comportamiento no se puede cambiar cuando se crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro; consulte el artículo Administración de grupos de aplicaciones.

Creación de grupos 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 Resumen.

Grupos de entrega

Se muestran todos los grupos de entrega, junto con la cantidad de máquinas que contiene cada uno.

- La lista **Grupos de entrega compatibles** contiene los grupos de entrega que se pueden 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 se pueden seleccionar. Cada entrada

© 1999-2017 Citrix Systems, Inc. All rights reserved.

explica por qué no es compatible, como, por ejemplo, porque contienen máquinas asignadas estáticas.

Un grupo de aplicaciones se puede asociar con grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También se pueden seleccionar grupos de entrega que contengan máquinas compartidas que entreguen escritorios, si (1) el grupo de entrega contiene máquinas compartidas y se creó con una versión anterior de XenDesktop 7.x, y (2) usted tiene el permiso de 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 se 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. Consulte el artículo Etiquetas para obtener información detallada.

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.

Dónde se especifican las listas de usuarios

Las listas de usuarios de Active Directory se especifican al crear o modificar lo siguiente:

- La lista de usuarios con derechos del grupo de entrega, que no se configura a través de Studio. De forma predeterminada, la regla de directiva de derechos de aplicaciones incluye a todos los usuarios; consulte el cmdlet del SDK de PowerShell BrokerAppEntitlementPolicyRule para obtener más detalles.
- La lista de usuarios del grupo de aplicaciones.
- La lista de usuarios del grupo de entrega.
- La propiedad de visibilidad de la aplicación.

La lista de usuarios que pueden acceder a una aplicación a través de StoreFront está formada por la intersección de las listas de usuarios indicadas arriba. Por ejemplo, para configurar el uso de una aplicación A para un departamento concreto, sin restringir el acceso a otros grupos:

- Use la regla predeterminada de directiva de derechos de aplicaciones que incluye a todos los usuarios.
- Configure la lista de usuarios del grupo de entrega para permitir que todos los usuarios de las oficinas centrales usen

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

cualquiera de las aplicaciones especificadas en el grupo de entrega.

- 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.

Aplicaciones

Tenga en cuenta:

- 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 el nombre nuevo; de lo contrario, cambie el nombre antes de agregarla. Para obtener más información, consulte Administración de 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 Citrix Receiver.
- 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.

Origen	Descripción
Desde el menú Inicio	Las aplicaciones que se han detectado 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 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 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	Las aplicaciones que fueron previamente agregadas 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 contiene ninguna aplicación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V	Aplicaciones de paquetes 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 (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).

Ámbitos

Esta página aparecerá sólo si ya se ha creado un ámbito. De forma predeterminada, está seleccionado el ámbito **Todo**. Para obtener más información, consulte el artículo Administración delegada.

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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administración de grupos de aplicaciones

Dec 05, 2017

En este artículo:

- Introducción
- Habilitación o inhabilitación de un grupo de aplicaciones
- Habilitación o inhabilitación del uso compartido de sesiones de aplicación entre grupos de aplicaciones
- Inhabilitación del uso compartido de sesiones de aplicación en un grupos de aplicaciones
- Cambio de nombre de un grupo de aplicaciones
- Agregar, quitar o cambiar la prioridad de las asociaciones de grupos de entrega con grupos de aplicaciones
- Agregar, modificar o eliminar una restricción de etiqueta en un grupo de aplicaciones
- Cómo agregar o eliminar usuarios en un grupo de aplicaciones
- Cambio de los ámbitos en un grupo de aplicaciones
- Eliminación de un grupo de aplicaciones

Introducción

En este artículo, se describe el procedimiento necesario para administrar grupos de aplicaciones después de crearlos.

Consulte el artículo Aplicaciones para obtener información acerca de cómo administrar aplicaciones en los grupos de entrega y los grupos de aplicaciones, incluido cómo:

- Agregar o quitar aplicaciones en un grupo de aplicaciones.
- Cambiar asociaciones de grupos de aplicaciones.

La administración de grupos de aplicaciones requiere los permisos de administración delegada correspondientes al rol integrado de Administrador de grupo de entrega. Para obtener información más detallada, consulte el artículo Administración delegada.

Habilitación o inhabilitación de 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.

Los grupos de aplicaciones se habilitan en el momento de crearlos y esto no se puede cambiar al crearlos.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Habilitación o inhabilitación del uso compartido de sesiones de aplicación entre grupos de aplicaciones

El uso compartido de sesiones de aplicaciones entre grupos de aplicaciones se habilita cuando se crea un grupo de aplicaciones; esto no se puede cambiar cuando se crea el grupo. Para obtener más información sobre el uso compartido de sesiones, consulte Uso compartido de sesiones entre 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.

Inhabilitación del uso compartido de sesiones de aplicación en un grupos 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 Broker 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. Para obtener más información sobre el uso compartido de sesiones, consulte Uso compartido de sesiones con grupos de aplicaciones.

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 (es decir, 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 Broker 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
```

Notas

- 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 al uso compartido de 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, uno tiene la opción establecida en True, mientras que el otro en False), lo que resulta en un comportamiento inesperado.

Cambio de nombre de un grupo de aplicaciones

1. Seleccione **Aplicaciones** en el panel de navegación de Studio.
2. Seleccione el grupo de aplicaciones en el panel central y, a continuación, seleccione **Cambiar nombre de grupo de aplicaciones** en el panel Acciones.
3. Especifique un nuevo nombre único y, a continuación, haga clic en **Aceptar**.

Agregar, quitar o cambiar la prioridad de las asociaciones de grupos de entrega con grupos de aplicaciones

Un grupo de aplicaciones se puede asociar con grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También se pueden seleccionar grupos de entrega que contengan máquinas compartidas que entreguen escritorios, si (1) el grupo de entrega contiene máquinas compartidas y se creó con una versión anterior de XenDesktop 7.x, y (2) usted tiene el permiso de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 casillas de verificación de grupos de entrega disponibles. (Los grupos de entrega incompatibles no se pueden seleccionar.) Cuando termine de seleccionarlos, haga clic en **Aceptar**.
5. Para quitar grupos de entrega, marque las casillas correspondientes a los grupos que quiere quitar y haga clic en **Quitar**. Confirme la eliminación cuando se le solicite.
6. Para cambiar la prioridad de un grupo de entrega, marque su casilla 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.

Cómo agregar, modificar o eliminar una restricción de etiqueta en un grupo de aplicaciones

Importante: Agregar, modificar o eliminar restricciones de etiqueta puede tener efectos no esperados en las máquinas que se tengan en cuenta para el inicio de aplicaciones. No olvide consultar las precauciones y los aspectos a tener en cuenta en el artículo 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.

Cómo agregar o eliminar usuarios en un grupo de aplicaciones

Para obtener información detallada acerca de los usuarios, consulte la sección Usuarios en el artículo Creación de 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 desea 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, a continuación, especifique los usuarios que quiere agregar. Para quitar usuarios,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Cambio de los 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 el artículo 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.

Eliminación de un grupo de aplicaciones

La aplicación debe estar asociada con, al menos, un grupo de entrega o un grupo de aplicaciones. Si intenta eliminar un grupo de aplicaciones, hará que una o varias aplicaciones dejen de pertenecer a un grupo y se le advertirá que al eliminar el grupo también se eliminarán esas aplicaciones. A continuación, puede confirmar o cancelar la eliminación.

Cuando se elimina una aplicación esto no la elimina en su lugar de origen, pero si quiere que la aplicación vuelva a estar disponible, tendrá que volver a agregarla desde el origen.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Acceso con Remote PC

Dec 05, 2017

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. Citrix Receiver, ejecutado en el dispositivo cliente, ofrece acceso a las aplicaciones y los datos almacenados en el equipo de la oficina desde la sesión de escritorio de acceso con Remote PC.

Un usuario puede tener varios escritorios, incluidos varios equipos físicos o una combinación de equipos físicos y escritorios virtuales.

Nota: No se admiten los modos Suspensión e Hibernación para el acceso con Remote PC. (Para implementaciones locales de XenApp y XenDesktop: El acceso con Remote PC solo es válido para las licencias de XenDesktop; las sesiones de acceso con Remote PC consumen las licencias de la misma forma que otras sesiones de XenDesktop.)

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 acerca del 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Aspectos a tener en cuenta acerca de 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 técnica 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.

Se admite Aero de Windows 7 en el equipo de la oficina, pero no es un requisito.

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.
- Inhabilite las funciones de ahorro de energía de la tarjeta de interfaz de red.
- Inhabilite las tecnologías de ahorro de batería.

Para dispositivos de acceso con Remote PC, no se admiten:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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
- Inhabilite las tecnologías de ahorro de batería

Instale Citrix Receiver 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 Citrix Receiver. Cuando un usuario inicia una sesión en el PC de forma remota, ese recurso aparece como no disponible para otros usuarios.

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.

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. Debe hacer una copia de seguridad del Registro antes de editarlo.

HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001

Puede personalizar más el comportamiento de esta función en:
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC

RpcaMode (con dword):

> Indicar 1 significa que el usuario remoto siempre ganará si no responde a los mensajes de la interfaz de usuario en el período de tiempo de espera especificado.
>
> Indicar 2 significa que siempre ganará 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 se da al 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 aquí debe ser de 30 segundos. El usuario debe reiniciar la máquina para que estos cambios surtan efecto.
>
> 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 desea permitir o denegar la conexión del usuario local. Si permite la conexión, la sesión del usuario remoto se desconecta.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Acceso con Remote PC y modo de HDX 3D Pro

Para el acceso con Remote PC, el VDA suele configurarse mediante la opción de VDA estándar. Para el acceso con Remote PC configurado con HDX 3D Pro, se admite la pantalla vacía en monitores con gráficos Intel Iris Pro, Intel HD 5300 y versiones posteriores (procesadores Intel Core de 5ª generación y procesadores Intel Core i5 de 6ª generación) y NVIDIA Quadro y GPU de NVIDIA GRID.

Para obtener más información, consulte Aceleración de GPU para sistemas operativos de escritorio Windows.

Wake on LAN

Nota: 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 recibe respaldo 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 Receiver está disponible la acción de reinicio.**Importante**: 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.

Para obtener más información sobre la configuración, consulte Configuration Manager y Wake on LAN para Acceso con Remote PC.

Configuration Manager y Wake on LAN para 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

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

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. Para obtener más información, consulte Configuration Manager y Wake on LAN para Acceso con Remote PC.

En el asistente para la creación de sitios:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.
- En las páginas **Usuarios y Cuentas de máquina**, especifique las cuentas de máquinas y de usuarios.

La creación de una implementación de acceso con Remote PC crea 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.

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) y, a continuación, modificar 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.

Instale el VDA en los PC de oficina utilizados para el acceso local y remoto. Por lo general, el VDA se implementa automáticamente desde el 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.

Utilizar el programa de instalación 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 los siguientes componentes (que son equivalentes a los elementos de la página **Componentes adicionales** del asistente):

    App-V
    Citrix User Profile Manager
    Citrix User Profile Manager WMI Plugin
    Machine Identity Service
    Personal vDisk

  De forma alternativa, puede usar la opción /exclude para excluir cada uno de estos componentes.

Utilizar el programa de instalación VDAWorkstationSetup.exe. Con este programa de instalación, no se pueden instalar ni Citrix Receiver 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 XenApp o XenDesktop, debe agregar usuarios o grupos al grupo de usuarios de acceso directo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Indique a los usuarios que descarguen e instalen Citrix Receiver en cada dispositivo que usarán para acceder al equipo de oficina de forma remota.Citrix Receiver está disponible en http://www.citrix.com o en los sistemas de distribución de aplicaciones para los dispositivos móviles compatibles.

Solución de 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

Solo para implementaciones locales: Cuando se habilita la administración de energía para el acceso con Remote PC, puede que las difusiones dirigidas a subredes no inicien las máquinas que se encuentren 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V

Dec 18, 2017

Uso de App-V con XenApp y XenDesktop

Microsoft Application Virtualization (App-V) le permite implementar, actualizar y respaldar 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 respaldadas.

App-V	**Versiones de XenDesktop y XenApp**	
	Delivery Controller	**VDA**
5.0 y 5.0 SP1	Desde XenDesktop 7 hasta la actual Desde XenApp 7.5 hasta la actual	7.0 hasta la versión actual
5.0 SP2	Desde XenDesktop 7 hasta la actual Desde XenApp 7.5 hasta la actual	7.1 hasta la actual
5.0 SP3 y 5.1	Desde XenDesktop 7.6 hasta la actual Desde XenApp 7.6 hasta la actual	Desde 7.6.300 hasta la actual
App-V en Windows Server 2016	Desde XenDesktop 7.12 hasta la actual Desde XenApp 7.12 hasta la actual	Desde 7.12 hasta la actual

El cliente de App-V no admite el acceso sin conexión a las aplicaciones. El respaldo para la integración de App-V incluye el uso de recursos compartidos SMB para aplicaciones. El protocolo HTTP no recibe respaldo.

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, la medición, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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 Citrix Receiver
- Desde el menú Inicio
- A través del cliente de App-V y Citrix Receiver
- Simultáneamente por varios usuarios 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.

Métodos de administración

Puede usar los paquetes de App-V que se crearon con el secuenciador de App-V y se encuentran en servidores App-V o recursos compartidos de red.

- **Servidores App-V**. Utilizar aplicaciones provenientes de paquetes presentes en servidores App-V requiere una comunicación constante entre Studio y los servidores App-V para la detección, la configuración y la descarga en los agentes 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 denomina método de *administración dual*, porque el acceso a aplicaciones y paquetes de App-V requiere tanto la consola de servidor App-V como la consola de Studio. Este método funciona mejor en implementaciones de App-V y Citrix estrechamente ligadas.

- **Recurso compartido de red**. Los paquetes 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. (Aun así, necesita instalar el cliente de App-V de Microsoft en cada VDA.)

  Esto se denomina el método de *administración única*, porque el uso de aplicaciones y paquetes de App-V requiere solamente 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.

  La 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.

Puede usar uno o ambos métodos de administración de forma simultánea. En otras palabras, al agregar aplicaciones a grupos de entrega, esas aplicaciones pueden proceder de paquetes de App-V ubicados en servidores App-V y/o en un recurso compartido de red.

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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

la memoria caché de la biblioteca de aplicaciones. Al seleccionar un paquete, el panel de detalles muestra las aplicaciones que contiene ese paquete.

Grupos de aislamiento

Cuando se usa el método de administración única de App-V, crear grupos de aislamiento permite especificar grupos interdependientes de aplicaciones que deben ejecutarse en el sandbox. Esta funcionalidad es similar (pero no idéntica) a los grupos de conexión de App-V. En lugar de la terminología "paquetes obligatorios" y "paquetes optativos" que utiliza el servidor de administración de App-V, Citrix utiliza los términos "automática" y "explícita" cuando se refiere a las opciones de implementación de paquetes.

- Así, cuando un usuario inicia una aplicación 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.

Configuración

En la siguiente tabla, se resume la secuencia de las tareas de configuración a realizar para utilizar App-V en XenApp y XenDesktop.

Método de administración		Tarea
Administración única	Administración dual	
X	X	Implementación de App-V
X	X	Empaquetado y selección de ubicación
	X	Configuración de direcciones de servidor App-V en Studio

© 1999-2017 Citrix Systems, Inc. All rights reserved.

X	X	Instalación de software en máquinas VDA
X		Incorporación de paquetes de App-V a la biblioteca de aplicaciones
X		Incorporación de grupos de aislamiento de App-V (opcional)
X	X	Incorporación de aplicaciones App-V a grupos de entrega

Implementación de Microsoft App-V

Para obtener 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 que las aplicaciones App-V se inicien correctamente, escriba **Set-CtxAppvServerSetting –UserRefreshonLogon 0**.

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.

Empaquetado y selección de 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 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.

Configuración de direcciones de servidor App-V en Studio

> **Important**
>
> 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

restablecerse a los valores predeterminados. Estas propiedades se utilizan en los VDA para conectarse a los servidores de publicación de App-V. Si eso ocurriera, vuelva a configurar en los servidores los valores no predeterminados de las propiedades restablecidas.

Este procedimiento solo es válido para la administración dual.

Puede especificar las direcciones de los servidores de administración y publicación de App-V para la administración dual durante o después de la creación de sitios. Puede hacerlo durante o después de crear el sitio.

Durante la creación de sitio:

En la página **App-V** del asistente, escriba la URL del servidor de administración de App-V, así como la URL y el número de puerto del servidor de publicación de App-V. Pruebe la conexión antes de continuar con el asistente. Si se produce un error en la prueba, consulte la sección de solución de problemas que se presenta a continuación.

Después de la creación de sitio:

1. Seleccione **Configuración > Publicación App-V** en el panel de navegación de Studio.
2. Si no ha indicado antes direcciones de servidor App-V, seleccione **Agregar servidor de Microsoft** en el panel Acciones.
3. Para cambiar direcciones de servidores 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 de solución de problemas que se presenta a continuación.

Posteriormente, si quiere quitar todos los enlaces a los servidores de administración y publicación de App-V y quiere que Studio deje de detectar paquetes de App-V desde 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.

Instalación de 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 App-V de Microsoft

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 mediante la ejecución del cmdlet de PowerShell **Enable-AppV** (sin parámetros). El cmdlet **Get-AppVStatus** obtiene el estado actual (habilitado/no habilitado).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sugerencia: Después de instalar el cliente de App-V, con permisos de administrador, ejecute el cmdlet de PowerShell **Get-AppvClientConfiguration** y verifique que EnablePackageScripts esté establecido en 1. Si no tiene el valor 1, ejecute **Set-AppvClientConfiguration -EnablePackageScripts $true**.

Componentes App-V de Citrix

El componente de software de App-V desarrollado por Citrix se instala y habilita de forma predeterminada cuando se instala un VDA.

Puede controlar esta acción predeterminada durante la instalación del VDA. En la interfaz gráfica, deje sin marcar la casilla **Citrix Personalization para App-V - VDA** en la página **Componentes adicionales**. En la interfaz de línea de comandos, incluya la opción **/exclude "Citrix Personalization for App-V - VDA"**.

Si inhabilita expresamente la instalación de 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.

Incorporación o eliminación de 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.

Incorporación de 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**.

Eliminación de 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 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.

Incorporación, modificación o eliminación de grupos de aislamiento de App-V

Incorporación de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

Modificación de 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 **Modificar parámetros de paquete del grupo de aislamiento**, cambie el nombre o la descripción del grupo de aislamiento, agregue o quite aplicaciones, cambie el tipo de implementación o el orden de las aplicaciones.
5. Cuando haya terminado, haga clic en **Aceptar**.

Eliminación de 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.
4. Confirme la eliminación.

Incorporación de 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 más detallada sobre cómo crear un grupo de entrega, consulte Creación de grupos de entrega.

Paso 1. Seleccione si quiere crear un nuevo grupo de entrega o agregar aplicaciones App-V a un grupo de entrega ya 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 aplicación. Seleccione **App-V**.

Paso 3. En la página **Agregar aplicaciones App-V**, elija el origen 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

situadas junto a las aplicaciones que quiera agregar. A continuación, haga clic en **Aceptar**.

Paso 4. Complete el asistente.

Tenga en cuenta:

- 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, 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".

Solución de problemas

Los problemas que solo pueden ocurrir cuando se utiliza el método de administración dual están marcados con "(DUAL)".

(DUAL) Se produce un error de conexión de PowerShell cuando selecciona **Configuración > Publicación de App-V** en el panel de navegación de Studio.

- ¿El administrador de Studio es también un administrador del servidor 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 **\\<*FQDN del servidor App-V*>** 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 \\<*FQDN del servidor App-V*> 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), aparecerá 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".

© 1999-2017 Citrix Systems, Inc. All rights reserved.

En este caso, agregue una entrada para el nombre del servidor App-V a la directiva de grupo Hosts de confianza en GPO (Plantillas administrativas > Componentes de Windows > Administración remota de Windows (WinRM) > Cliente WinRM).

(DUAL) Falla la detección cuando se agrega una aplicación 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 no se inician.

- (DUAL) ¿Se está ejecutando el servidor de publicación?
- (DUAL) ¿Los paquetes de App-V tienen los permisos de seguridad adecuados para que los usuarios puedan acceder a ellos?
- (DUAL) En el agente VDA, compruebe que Temp hace referencia a la ubicación correcta y que hay espacio suficiente disponible en el directorio Temp.
- (DUAL) En el servidor de publicación de App-V, ejecute **Get-AppvPublishingServer *** para ver 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, como 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. Use uno de los siguientes dos métodos para configurar ExecutionPolicy: (1) como administrador, escriba el cmdlet **Set-ExecutionPolicy RemoteSigned**, o bien (2) desde Configuración de directiva de grupo, vaya a Configuración del equipo > Directivas > Plantillas administrativas > Componentes > 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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:
3. Reinicie el servicio de Broker para comenzar la captura de registros.

Para habilitar los registros del VDA:

1. Cree la carpeta C:\CtxAppvLogs.
2. Vaya a C:\Archivos de programa\Citrix\Virtual Desktop Agent. Abra CtxAppvCommon.dll.config en un editor de texto y quite la marca de comentario de la línea siguiente:
3. Quite la marca de comentario de la línea y establezca el valor en 1:
4. Reinicie la máquina para comenzar a capturar registros.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

AppDisks

Dec 05, 2017

Información general

Administrar las aplicaciones y, a su vez, las imágenes en que esas aplicaciones están instaladas puede ser complejo. En estos casos, la funcionalidad 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 funcionalidad Citrix AppDNA, puede integrar la funcionalidad AppDisks con ella, ya que AppDNA permite que XenApp y XenDesktop analicen automáticamente aplicaciones en cada AppDisk. Usar AppDNA ayuda a sacar el máximo provecho de la funcionalidad AppDisks. Sin ella, la compatibilidad de las aplicaciones no se prueba ni 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 funcionalidad AppDisks no aísla las aplicaciones. Las separa (a ellas y a sus archivos auxiliares y claves del Registro) del sistema operativo. Para el sistema operativo y el usuario, los AppDisks aparecen y se comportan como si estuvieran instalados directamente en la imagen maestra.
- La administración de cambios (actualizar las imágenes maestras y probar la compatibilidad de las actualizaciones con las aplicaciones instaladas) puede redundar en un gasto considerable. Con los informes de AppDNA, puede identificar problemas y sugerir correcciones. Por ejemplo, AppDNA puede identificar las aplicaciones que tienen dependencias comunes (como .NET) para, así, instalarlas en una sola imagen base común. Asimismo, AppDNA puede identificar las aplicaciones que se cargan pronto en la secuencia de inicio del SO, por lo que puede comprobar si se comportan de la manera esperada.

Tenga en cuenta:

- 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 no se cerrará".

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 funcionalidad 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 que solo use AppDisks con escritorios alojados agrupados y compartidos.
- Puede usar AppDisks con escritorios compartidos alojados.
- Puede compartir AppDisks entre las imágenes maestras y las plataformas de SO (por cada aplicación); sin embargo, esto no funcionará para todas las aplicaciones. Si dispone de aplicaciones con scripts de instalación para SO de escritorio que les impiden funcionar en un SO de servidor, Citrix recomienda empaquetar las aplicaciones por separado para cada sistema operativo.
- En muchos casos, AppDisks funciona en diferentes sistemas operativos. Por ejemplo, puede agregar un AppDisk, creado en una VM de Windows 7, a un grupo de entrega que contenga máquinas con Windows 2008 R2, siempre que ambos sistemas operativos tengan el mismo valor de bits (32 bits o 64 bits) y admitan la aplicación. Sin embargo, Citrix recomienda no agregar AppDisks creados en una versión posterior de sistema operativo (como Windows 10) a grupos de entrega que contengan máquinas con una versión anterior de sistema operativo (por ejemplo, Windows 7), porque es posible que no funcionen correctamente.
- Aun así, si debe conceder acceso a las aplicaciones de un AppDisk a solo un subconjunto de usuarios pertenecientes a un grupo de entrega, Citrix recomienda utilizar una directiva de grupo para ocultar a algunos usuarios las aplicaciones pertinentes 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, un archivo de registro (DaFsFilter) podría suprimirse, 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.

© 1999-2017 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 XenApp y XenDesktop 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, XenApp y XenDesktop se coordinarán con la librería AppLibrary, interactuarán con Machine Creation Services (MCS) o Provisioning Services (PVS) 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 el artículo Requisitos del sistema.

La funcionalidad AppDisks solo se admite en implementaciones que contienen (como mínimo) las versiones de Delivery Controller y Studio suministradas en la descarga de XenApp y XenDesktop 7.8, incluidos los requisitos previos que el programa de instalación instala automáticamente (como .NET 4.5.2).

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 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 se denomina *nivel funcional*.) Para obtener más información acerca de los niveles funcionales, consulte el artículo Creación de grupos de entrega.

Si quiere aprovisionar las máquinas virtuales que se usarán para crear AppDisks, puede usar:

- La versión de Machine Creation Services proporcionada con la versión 7.8 (mínima) de Controller.
- La versión de Provisioning Services que se ofrece en la página de descarga para su versión de XenApp y XenDesktop.
- 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 XenApp y XenDesktop.

La creación de AppDisks no recibe respaldo en las máquinas de catálogos de MCS que usan caché de datos temporales.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **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 respaldan 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:

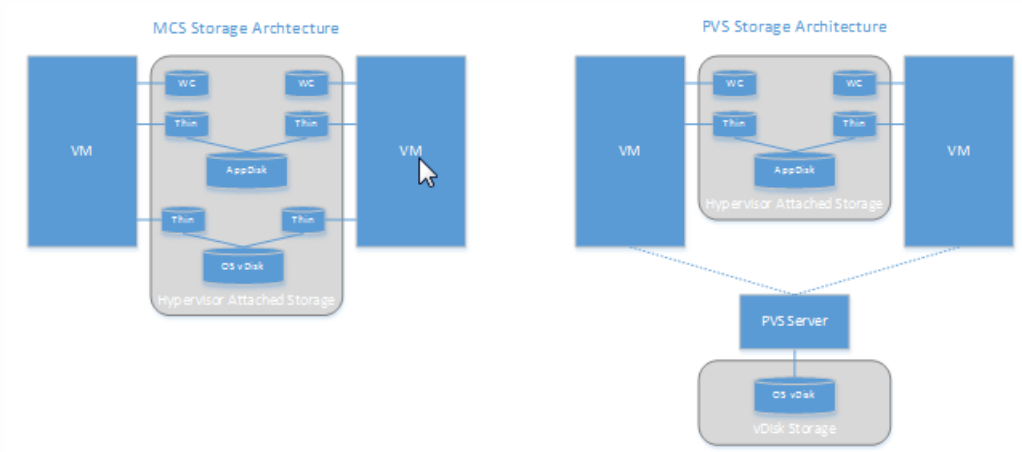
- Consulte la documentación de AppDNA y las preguntas frecuentes de AppDisk.
- El software de AppDNA y Controller no deben estar instalados en el mismo servidor. Utilice la versión de AppDNA proporcionada con esta versión de XenApp y XenDesktop. Para conocer otros requisitos de AppDNA, consulte la documentación referente a esa funcionalidad.
- 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 XenApp o XenDesktop, puede habilitar el análisis de compatibilidad con AppDNA en la página **Características adicionales** del asistente para la creación de sitios. También puede habilitar o inhabilitarlo más adelante. Para ello, deberá seleccionar **Configuración > AppDNA** en el panel de navegación de Studio.
- En Studio, al hacer clic en el enlace "Ver informe de problemas", aparece el informe de AppDNA. Sin embargo, las combinaciones de sistema operativo que utiliza AppDNA de forma predeterminada son Windows 7 de 64 bits para grupos de entrega de escritorios y Windows Server 2012 R2 para grupos de entrega de servidores. Si los grupos de entrega cuentan con versiones diferentes de Windows, las combinaciones predeterminadas de imagen en los informes que muestra Studio serán incorrectas. Para solucionar este problema, 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):

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Product Version	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 MCS y PVS. "WC" indica la memoria caché de escritura, mientras que "Thin" indica el disco ligero usado para almacenar las diferencias entre los discos virtuales de sistema operativo y el AppDisk de una máquina virtual.



En entornos de MCS:

- Puede seguir equilibrando el tamaño de los discos virtuales (vDisk) del sistema operativo y de los AppDisks con las directrices de tamaño de datos existentes en la empresa. Si los AppDisks se comparten entre varios grupos de entrega, se puede reducir la capacidad total de almacenamiento.
- Los AppDisks y los discos virtuales de SO se encuentran en las mismas áreas de almacenamiento, por lo que debe planificar con cuidado sus requisitos de capacidad de almacenamiento con el fin de evitar cualquier efecto negativo en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 PVS:

Debe permitir IOPS y la capacidad aumentada porque las aplicaciones se moverán desde el almacenamiento de AppDisk al almacenamiento correspondiente al hipervisor.

Con Provisioning Services, los AppDisks y los discos virtuales (vDisk) del SO no comparten los 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 PVS el tamaño adecuado para dar cabida a esos cambios.

Los AppDisks del almacenamiento correspondiente al hipervisor requieren más IOPS, mientras que los discos virtuales del sistema operativo requieren menos.

Memoria caché de escritura: PVS 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 PVS, 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 PVS, las aplicaciones no se encuentran en el disco virtual (vDisk) del SO, por lo que se realizan menos solicitudes al servidor de PVS. Con la menor carga resultante en cada dispositivo de destino, el servidor de PVS 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.

Creación de un AppDisk

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.
- Si usa AppDNA, siga las instrucciones proporcionadas en la sección anterior Requisitos. 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

usen la activación de Key Management Server (KMS). Para obtener más información, consulte la documentación de la aplicación.

- No se conservan los archivos, las carpetas ni las entradas de Registro que se hayan creado en ubicaciones específicas del usuario durante la creación de AppDisk. Además, algunas aplicaciones ejecutan un asistente de primer uso para crear datos de usuario durante la instalación. Use una solución de administración de perfiles para conservar esos datos y evitar que el asistente aparezca cada vez que se inicie el AppDisk.
- Si usa AppDNA, el análisis comienza automáticamente después de que se complete el proceso de creación. Durante este intervalo, el estado del AppDisk en Studio es "analizando".

Consideraciones acerca de PVS

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.

Creación de 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.

Creación de 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, a continuación, 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 el catálogo de máquinas agrupadas aleatorias que se usará como imagen maestra en 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 contenga máquinas virtuales agrupadas aleatorias, se producirá un error en la creación del AppDisk. Después de seleccionar una máquina virtual de un catálogo de máquinas agrupadas aleatorias, haga clic en **Siguiente**.
5. En la página **Resumen**, escriba un nombre y una descripción para el AppDisk. Revise la información especificada en las páginas anteriores del asistente. Haga clic en **Finalizar**.

Recuerde: Si utiliza Provisioning Services, siga las instrucciones de la sección Consideraciones acerca de PVS indicadas arriba.

Una vez cerrado el asistente, la pantalla de Studio referente al nuevo AppDisk indicará "Creando". Después de crea el AppDisk, la pantalla cambia a "Listo para instalar aplicaciones".

Instalación de aplicaciones en el AppDisk:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 en el hipervisor.) 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 de instalación de aplicaciones en el panel Acciones de Studio.)

Sellado del AppDisk:

1. Seleccione **AppDisks** en el panel de navegación de Studio.
2. Seleccione el AppDisk que ha creado y, a continuación, seleccione **Sellar AppDisk** en el panel Acciones.

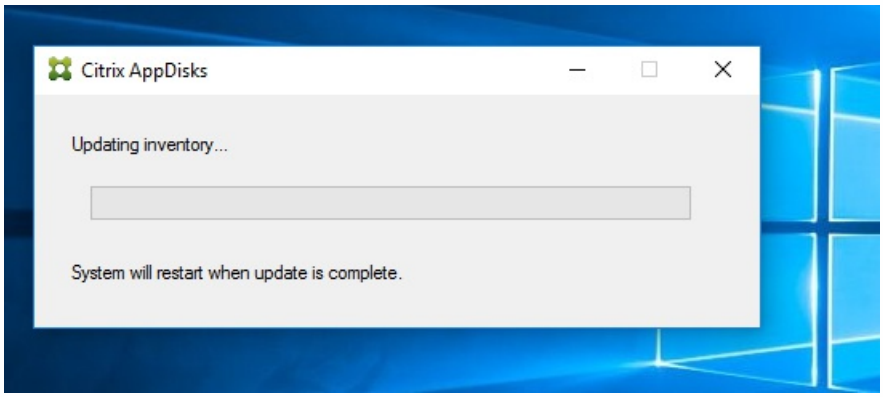
Después de crear el AppDisk, instale aplicaciones en él, séllelo y asígnelo a un grupo de entrega.

Cómo cancelar la preparación y el sellado de AppDisk

En algunos casos, es posible un administrador necesite cancelar la creación o el sellado de AppDisk:

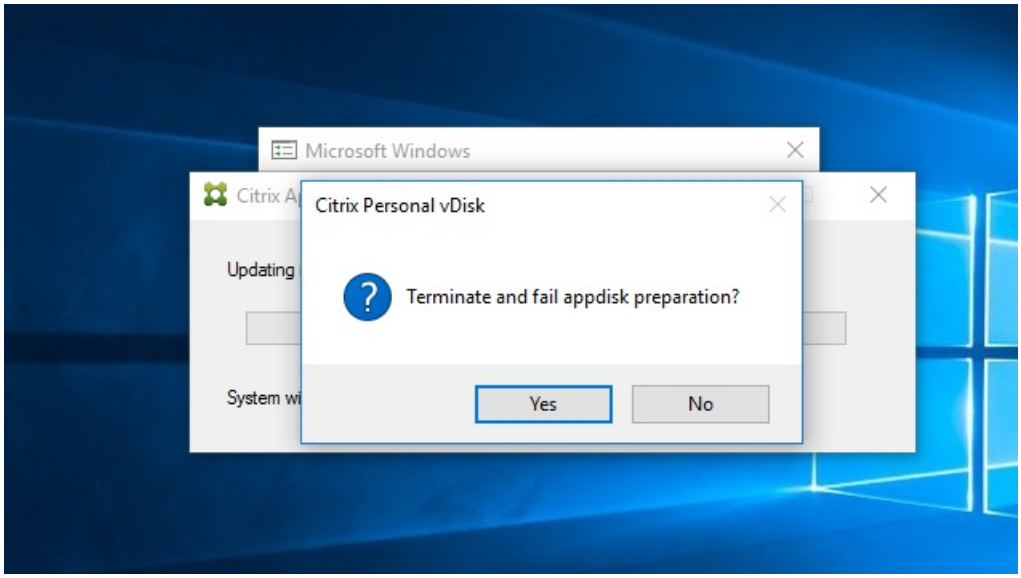
1. Acceda a la máquina virtual.

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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nota

Si cancela la preparación de AppDisk, reiniciar la máquina la devuelve a su estado inicial; lo contrario, debe crear una VM limpia.

Creación de un AppDisk en el hipervisor y su importación 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.

Preparación, instalación de aplicaciones y sellado de 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 **Empaquetar AppDisk** ubicado 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. En la página **Introducción**, revise la información y, a continuación, haga clic en **Siguiente**.
3. En la página **Crear AppDisk**, seleccione el botón de radio **Importar AppDisk existente**. Seleccione el recurso (red y almacenamiento) donde reside el AppDisk que ha creado en el hipervisor. Haga clic en **Siguiente**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. En la página **Máquina de preparación**, vaya a la máquina, seleccione el disco y, a continuación, haga clic en **Siguiente**.
5. En la página **Resumen**, escriba un nombre y una descripción para el AppDisk. Revise la información especificada en las páginas anteriores del asistente. Haga clic en **Finalizar**. Studio importa el AppDisk.

Después de importar el AppDisk en Studio, asígnelo a un grupo de entrega.

Asignación de 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 quiere agregar AppDisks a un grupo de entrega que está creando, siga las siguientes instrucciones para la página **AppDisks** del asistente Crear grupo de entrega (para obtener información acerca de otras páginas de ese asistente, consulte el artículo Creación de 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, a continuación, 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. En la página **Estrategia de implantación**, siga las instrucciones de Creación de una programación de reinicios.

Página de AppDisks:

En la página **AppDisks** (en el asistente Crear grupo de entrega o en el flujo Administrar AppDisks), se muestran los AppDisks ya implementados en el grupo de entrega y su prioridad. (Si está creando el grupo de entrega, la lista estará vacía.) Para obtener más información, consulte la sección Prioridad de AppDisk en un grupo de entrega.

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. (Si selecciona la ficha **Aplicaciones**, ubicada sobre la columna derecha, aparecerán las aplicaciones en un formato similar a un menú Inicio. En cambio, si selecciona la ficha **Paquetes instalados**, aparecerán las aplicaciones en un formato similar a 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 AppDisks.

Prioridad de AppDisk en un grupo de entrega

Cuando un grupo de entrega tiene más de un AppDisk asignado, la página **AppDisks** (en las pantallas Crear grupo de entrega, Modificar grupo de entrega y Administrar AppDisks) muestra los AppDisks con las prioridades clasificadas por orden 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 automáticamente las aplicaciones y establece la prioridad cuando los AppDisks se asignan al grupo de entrega. Posteriormente, si agrega o quita AppDisks del grupo, hacer

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Administración de 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.

> ### Important
>
> Puede usar el servicio Windows Update para actualizar aplicaciones (como, 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 revisiones 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 de 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 al antivirus marca ciertos procesos como peligrosos. Estos procesos, **CtxPvD.exe** y **CtxPvDSrv.exe**, deben agregarse a la lista de excepciones del antivirus que utilice la VM base.

En esta sección, se ofrece información sobre cómo agregar excepciones en las siguientes aplicaciones de antivirus:

- Windows Defender (para Windows 10)
- OfficeScan (versión 11.0)
- Symantec (versión 12.1.16)
- McAfee (versión 4.8)

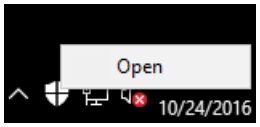
Windows Defender

Si la VM base usa Windows Defender (versión 10):

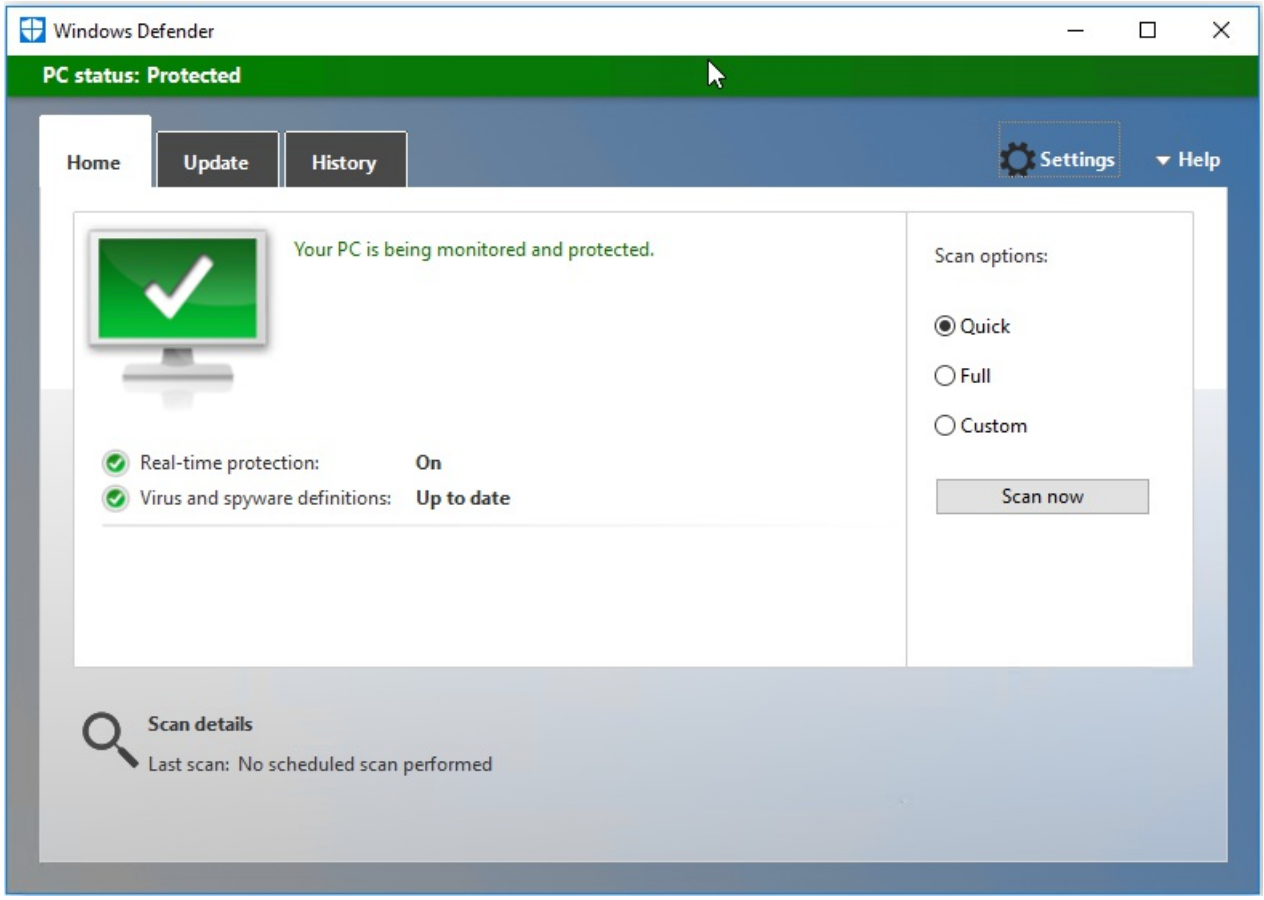
1.Inicie sesión en el equipo con privilegios de administrador local.

2.Seleccione el icono de Windows Defender y haga clic con el botón secundario para ver el botón **Abrir**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

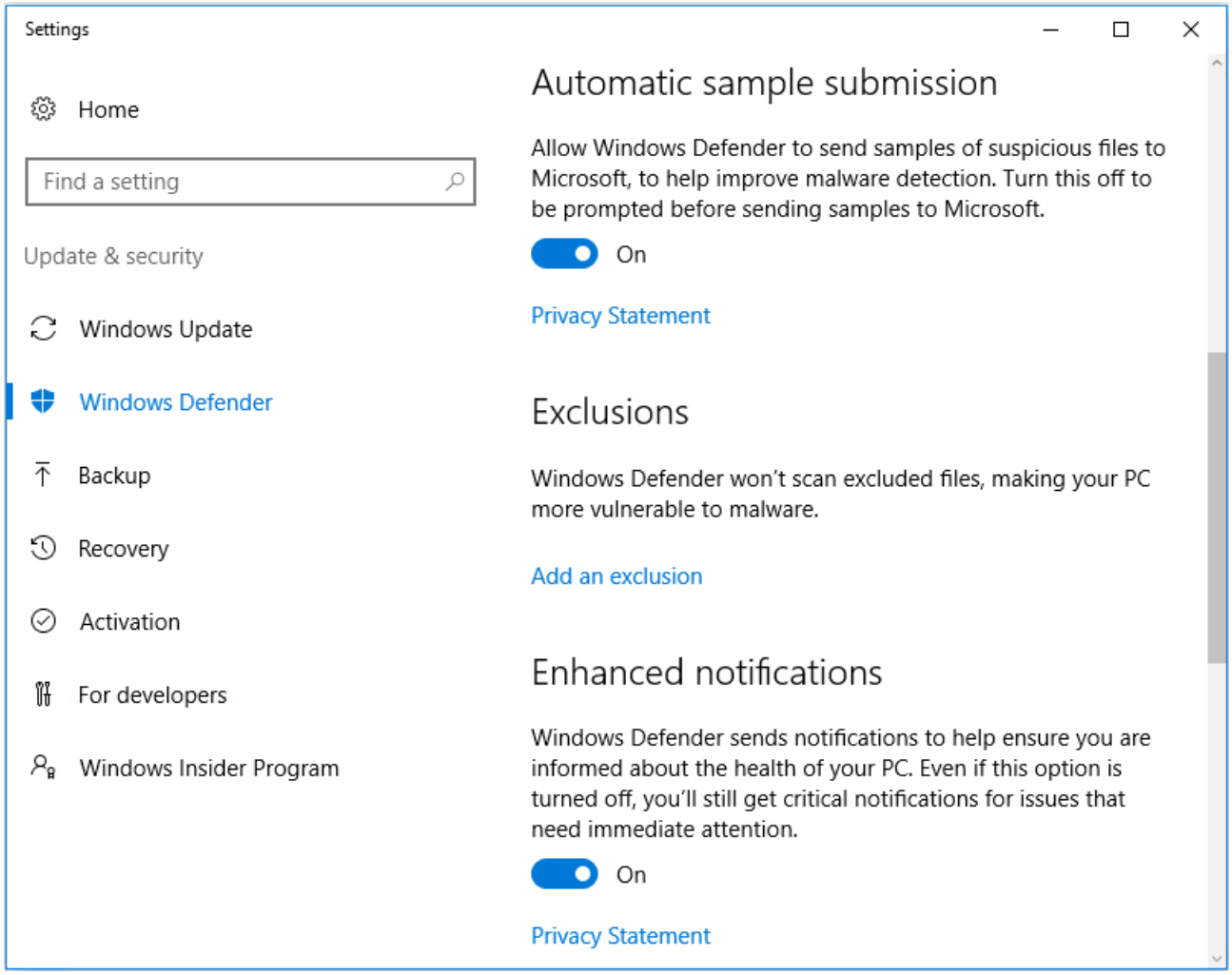


3. En la consola de Windows Defender, seleccione **Configuración** en la parte superior derecha de la interfaz:



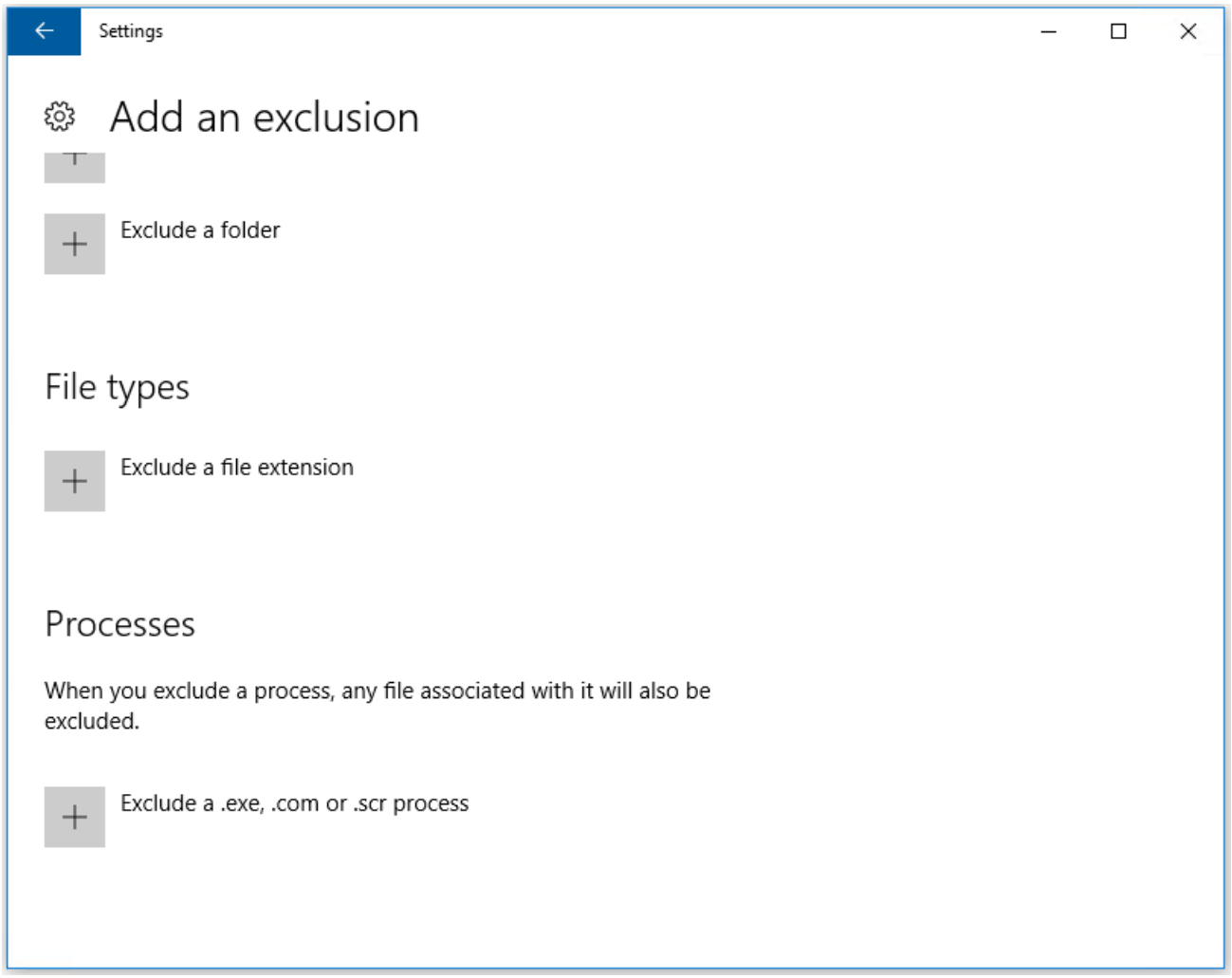
4. En la sección **Exclusiones** de la pantalla Configuración, haga clic en **Agregar exclusión**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

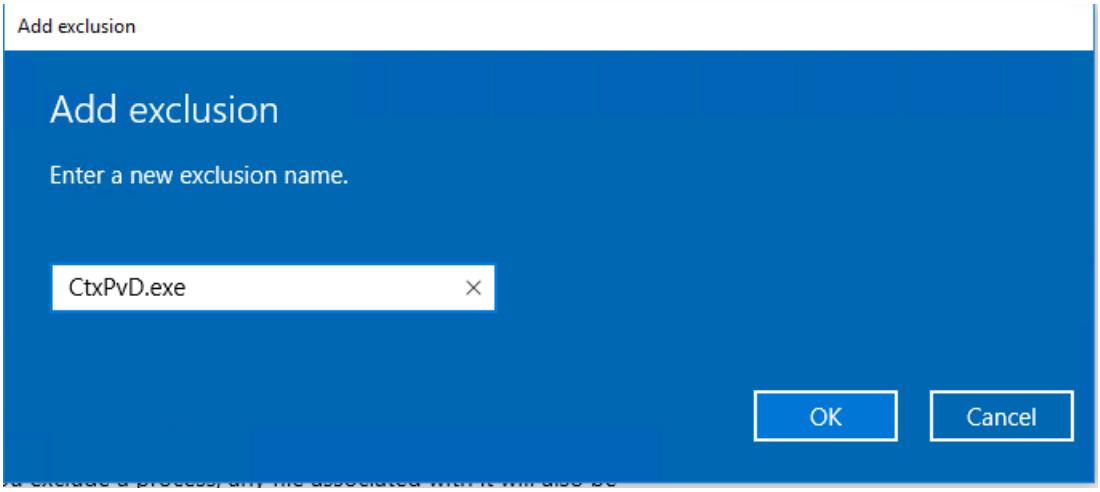


5. En la pantalla **Agregar exclusión**, seleccione **Excluir un proceso .exe, .com o .scr**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

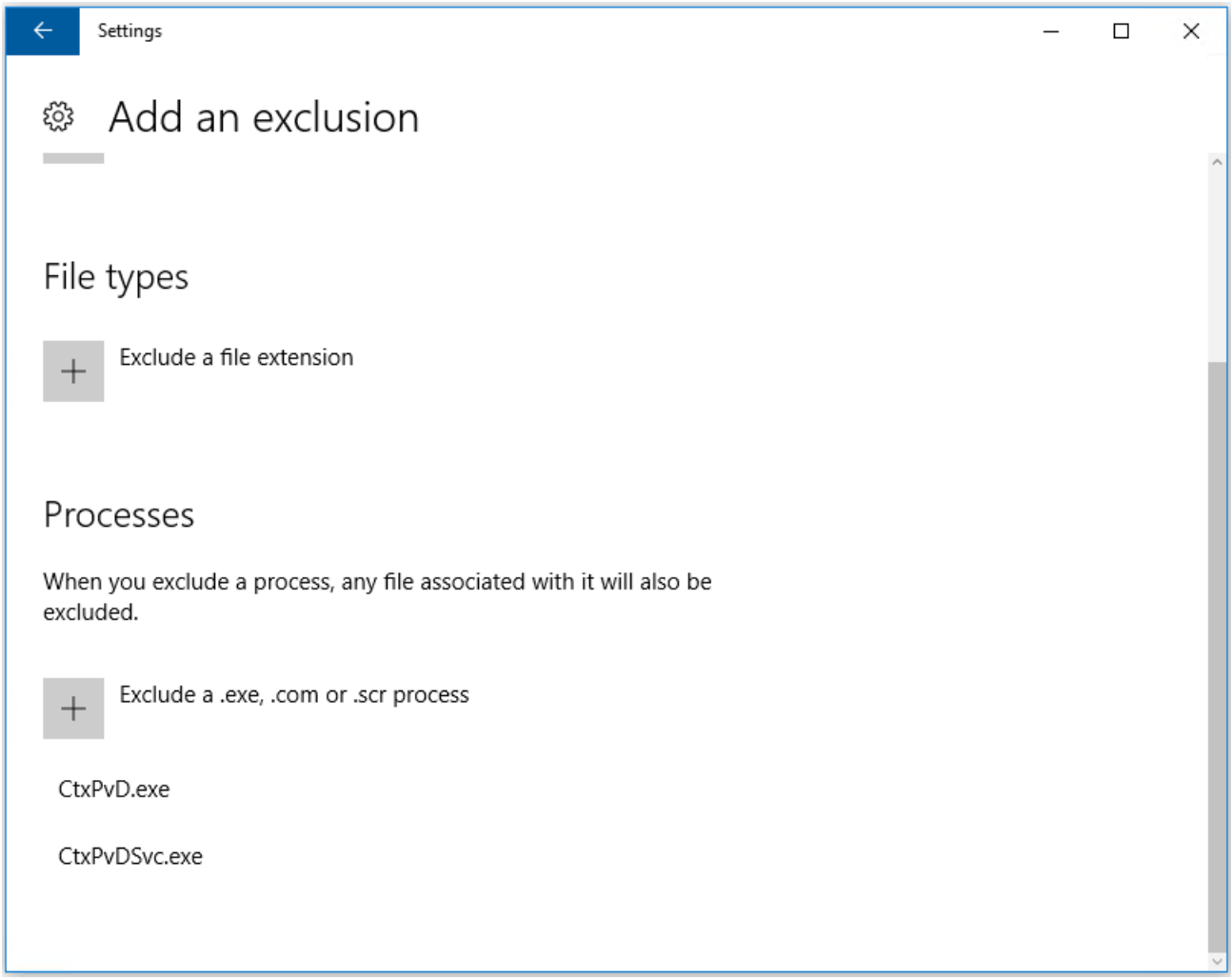


6. En la pantalla **Agregar exclusión**, introduzca el nombre de la exclusión; deben agregarse **CtxPvD.exe** y **CtxPvDSvc.exe** a fin de evitar conflictos en el momento de crear un AppDisk. Después de introducir el nombre de exclusión, haga clic en **Aceptar**:



Después de agregar las exclusiones, estas aparecen en la lista de procesos excluidos en la pantalla **Configuración**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

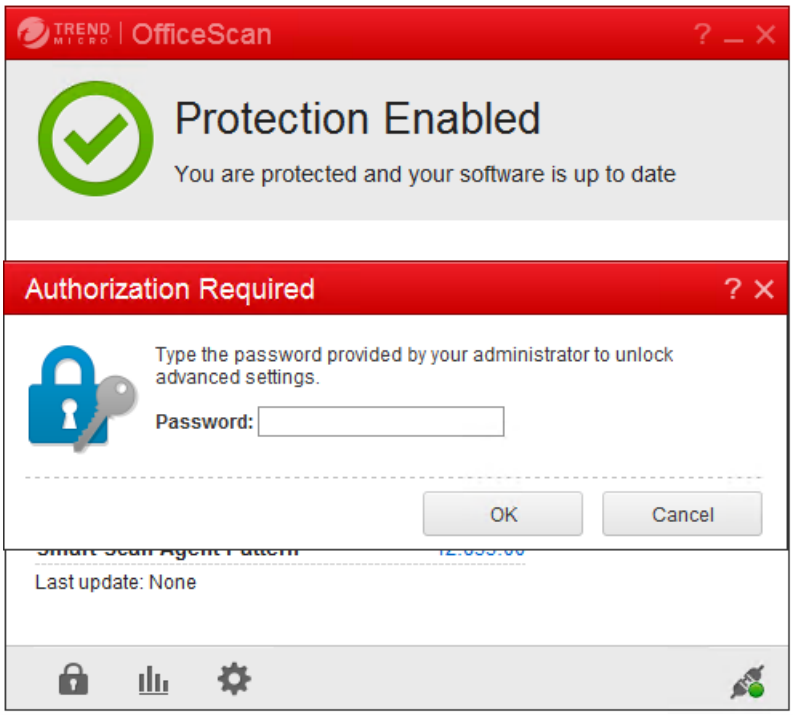


OfficeScan

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:

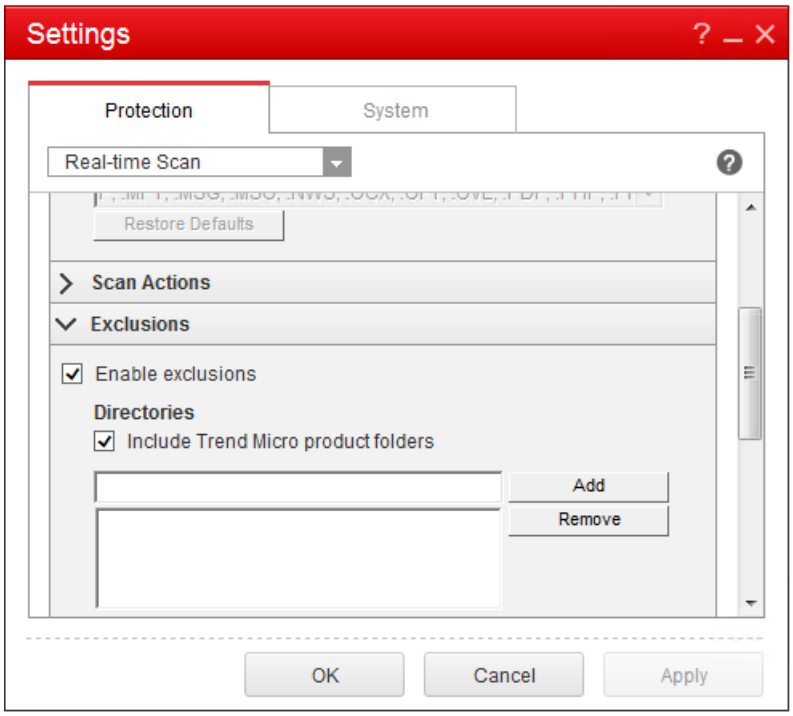
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.



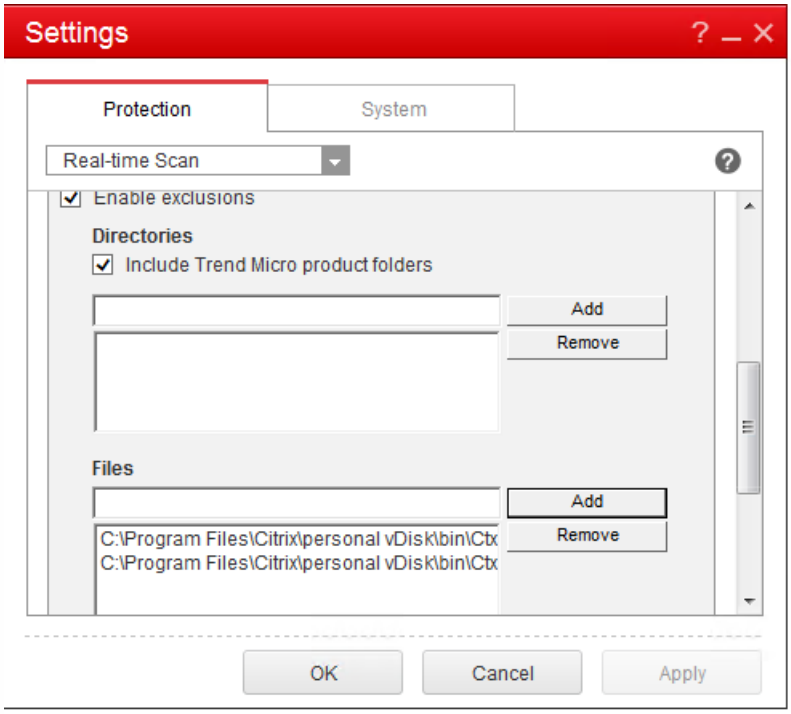
6. En la sección **Files**, haga clic en **Add** y, a continuación, introduzca los siguientes procesos de AppDisk a la lista de excepciones:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

comando COPIAR

```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```



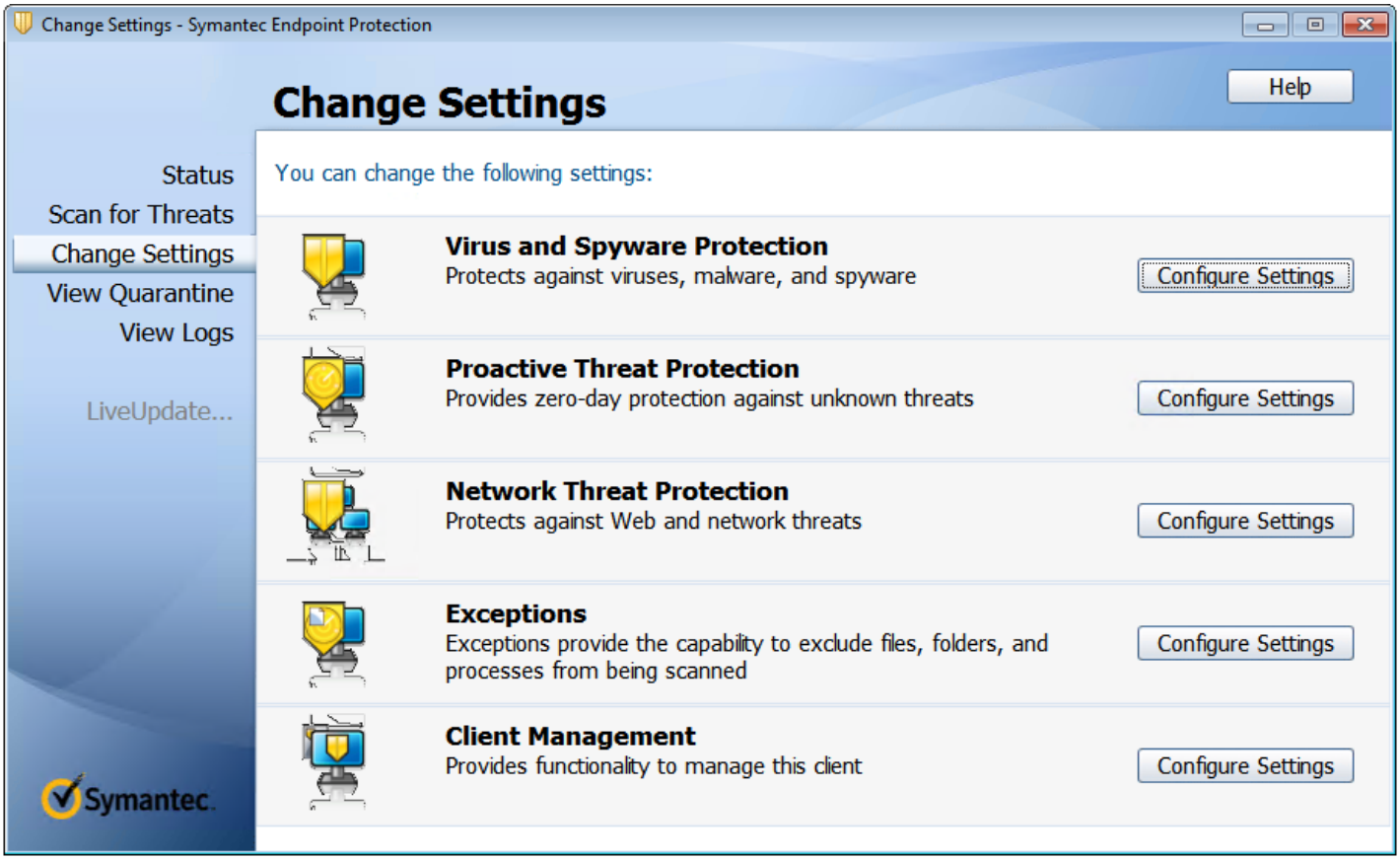
7. Haga clic en **Apply** y, a continuación, en **OK** para agregar las exclusiones.

Symantec

Si la VM base usa Symantec (versión 12.1.16):

1. Inicie la consola de Symantec.
2. Haga clic en **Change Settings**.
3. En la sección **Exceptions**, haga clic en la opción **Configure settings**:

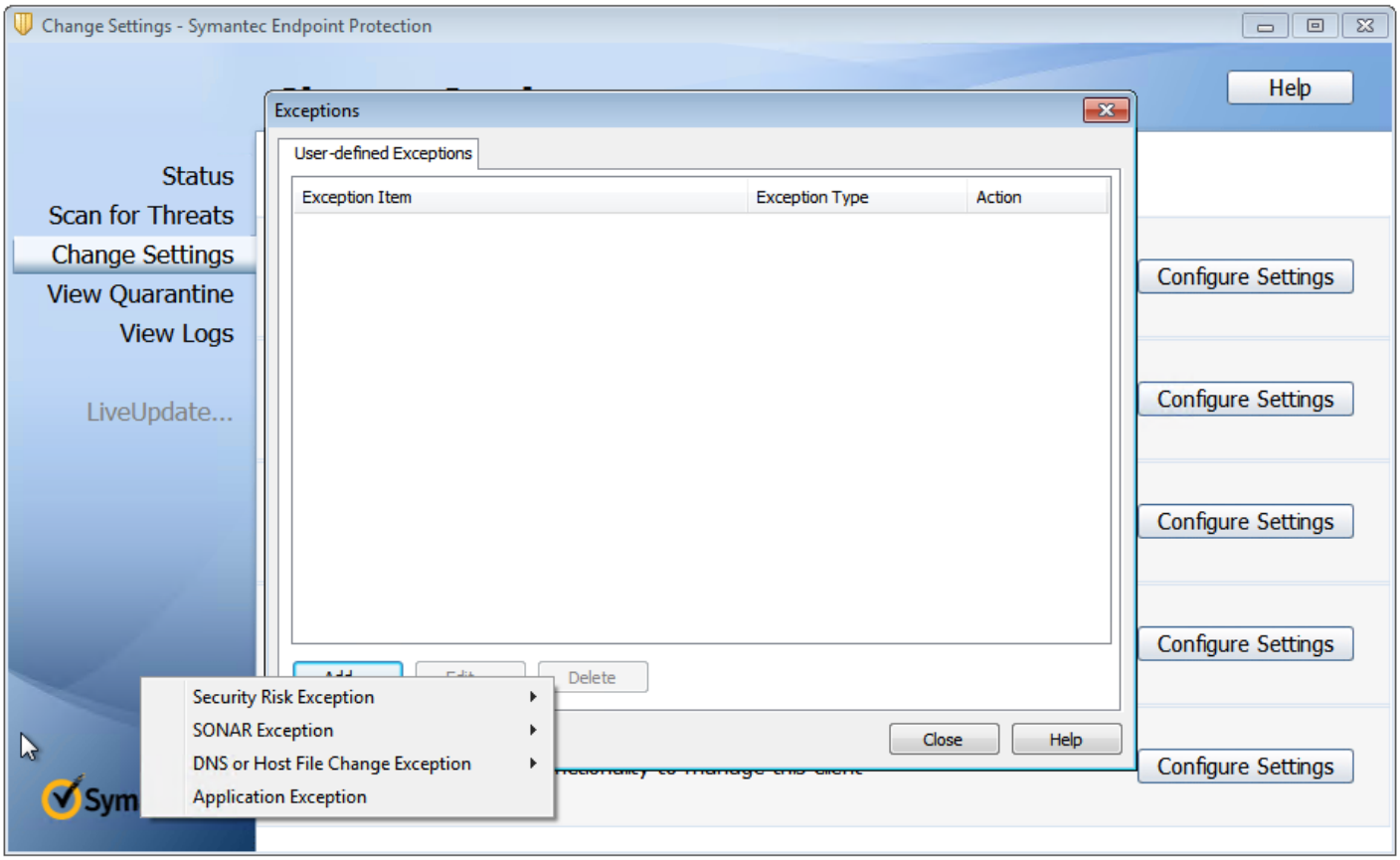
© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. En la pantalla de configuración detallada, 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**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



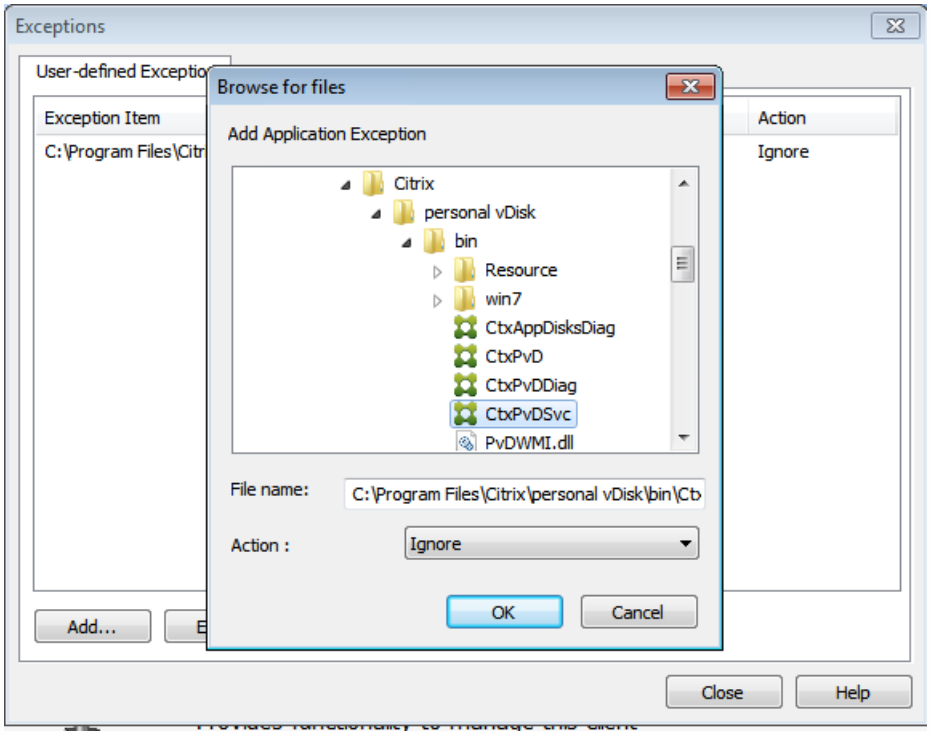
6. En la pantalla de excepciones, introduzca las siguientes rutas de archivo de AppDisk y establezca la acción **Ignore**:

comando COPIAR

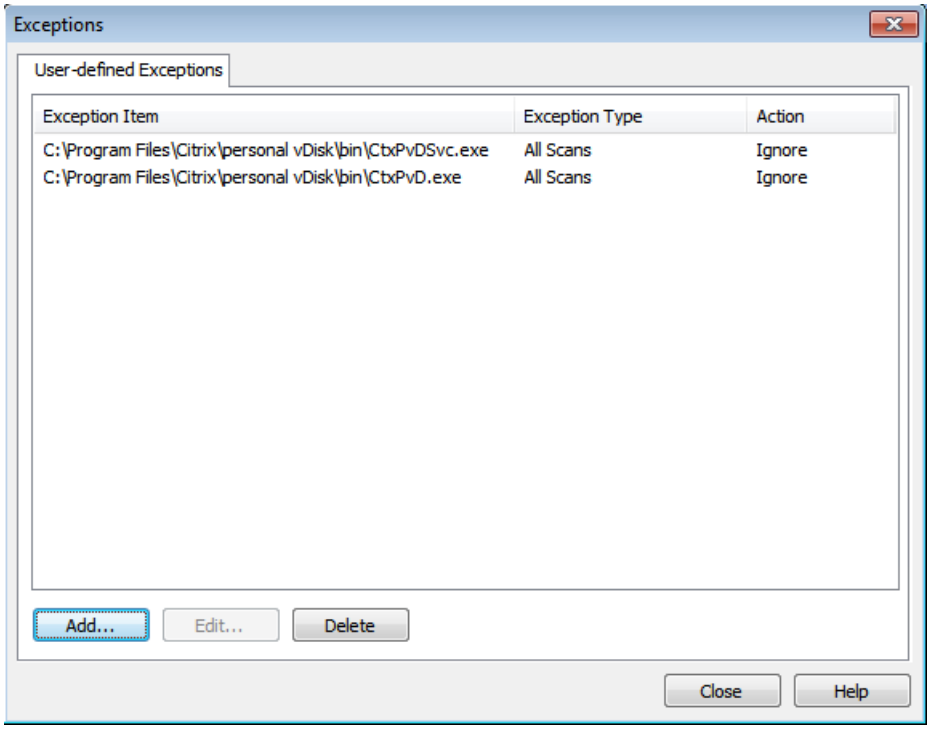
```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.



Las excepciones indicadas se agregan a la lista. Cierre la ventana para aplicar los cambios:

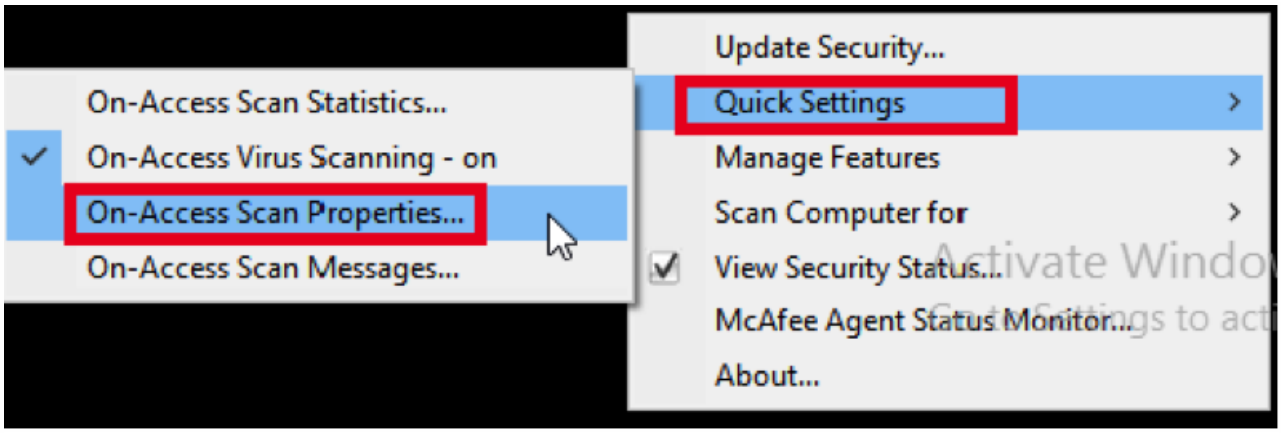


McAfee

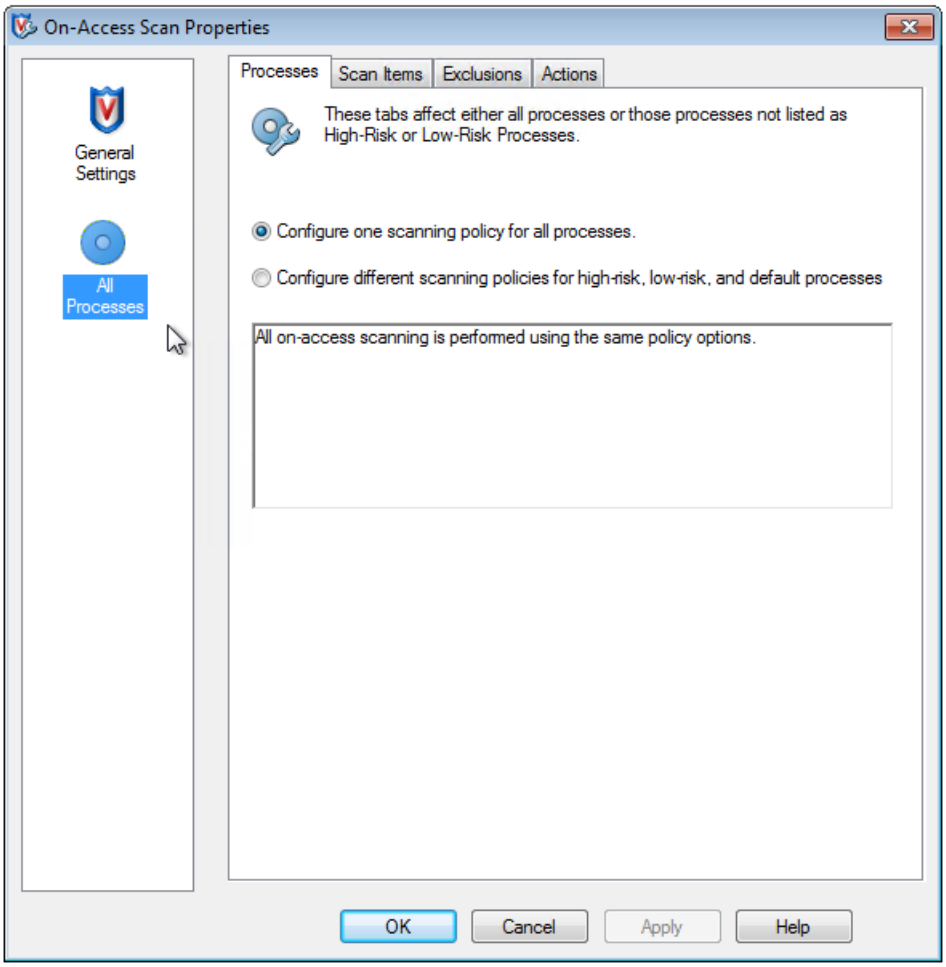
Si la VM base usa McAfee (versión 4.8):

1. Haga clic con el botón secundario en el icono de McAfee y expanda la opción de **configuración rápida**.
2. En el menú expandido, seleccione **On-Access Scan Properties**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. En la pantalla **On-Access Scan Properties**, haga clic en **All Processes**:

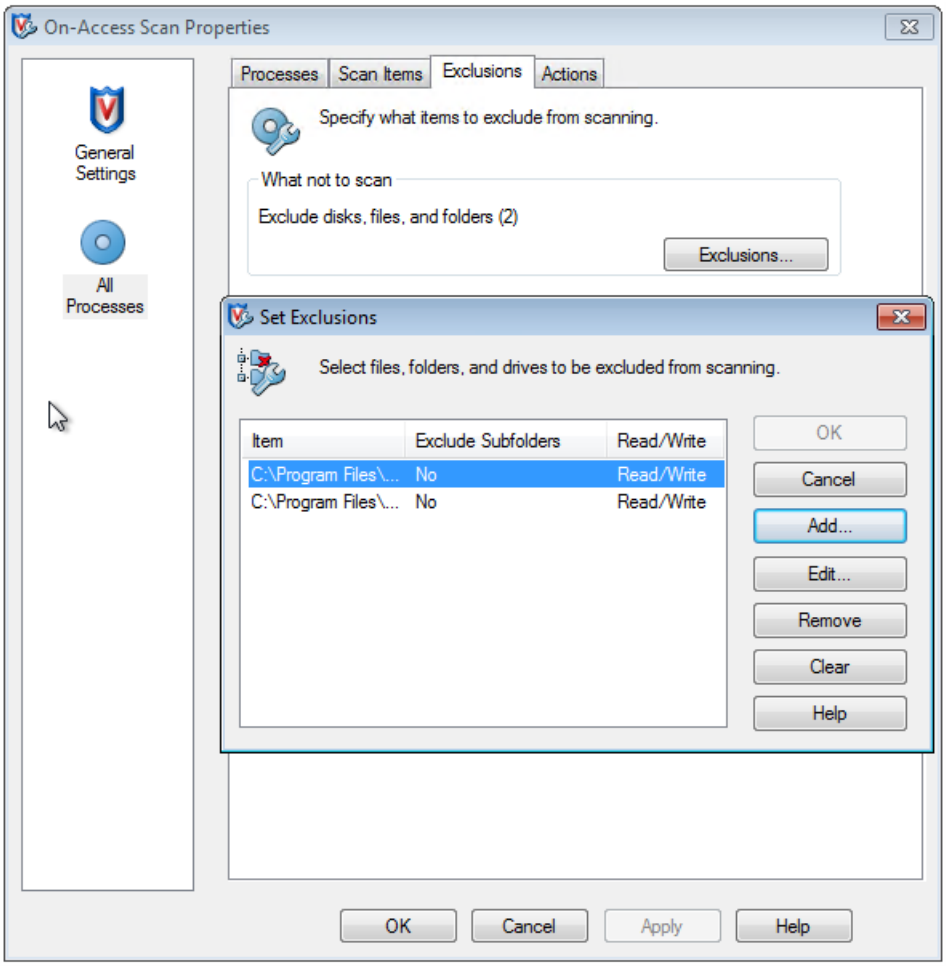


4. Seleccione la ficha **Exclusions**.

5. Haga clic en el botón **Exclusions**.

6. En la pantalla **Set exclusions**, haga clic en **Add**:

© 1999-2017 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:

comando COPIAR

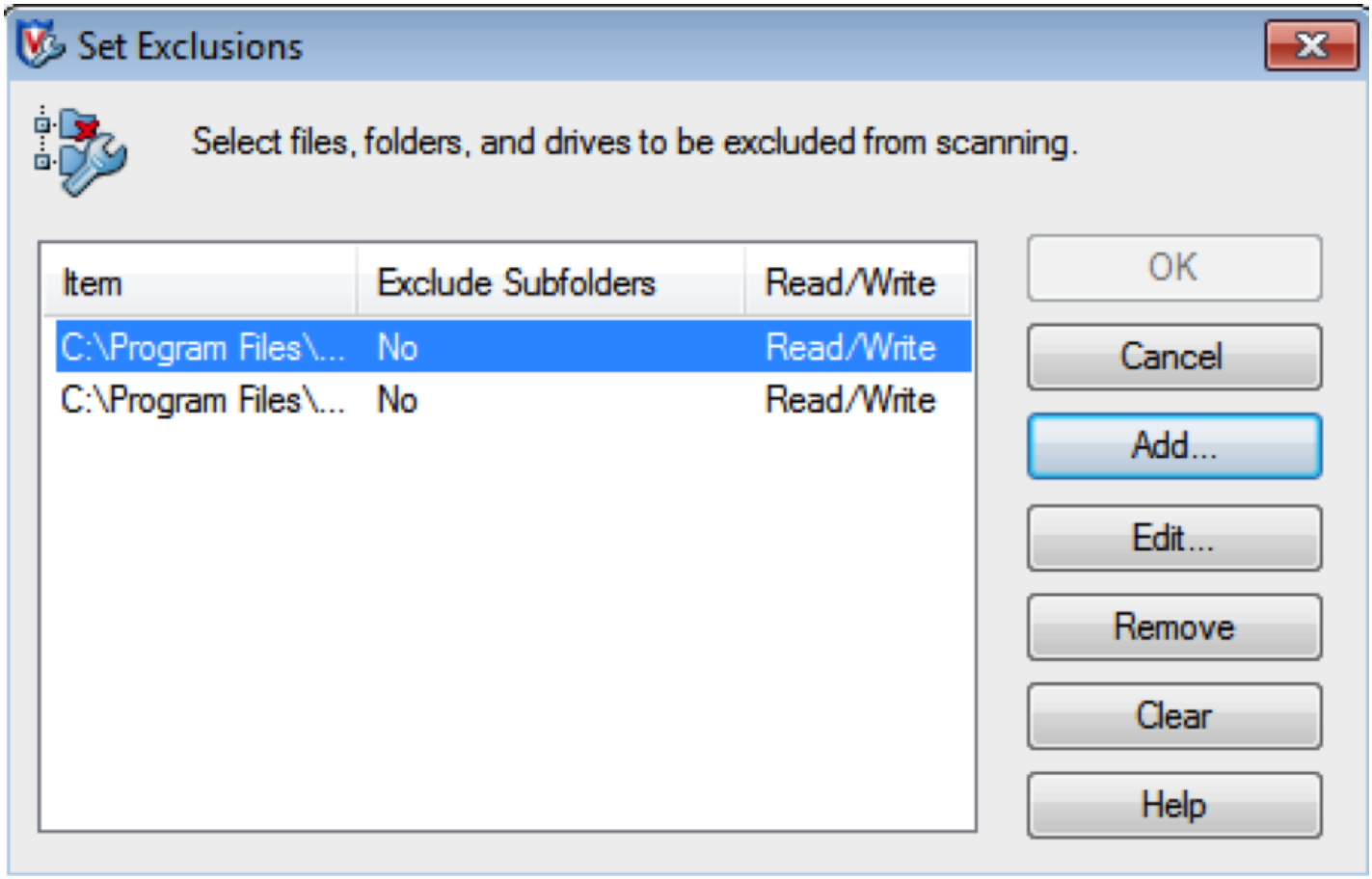
```
C:\Program Files\Citrix\personal vDisk\bin\CtxPvD.exe

C:\Program Files\Citrix\personal vDisk\bin\CtxPvDSvc.exe
```

8.Haga clic en **OK**.

9Ahora, la pantalla **Set Exclusions** muestra las exclusiones agregadas. Haga clic en **OK** para aplicar los cambios:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



> **Nota**
>
> Después de la configuración de estas exclusiones, cree el AppDisk.

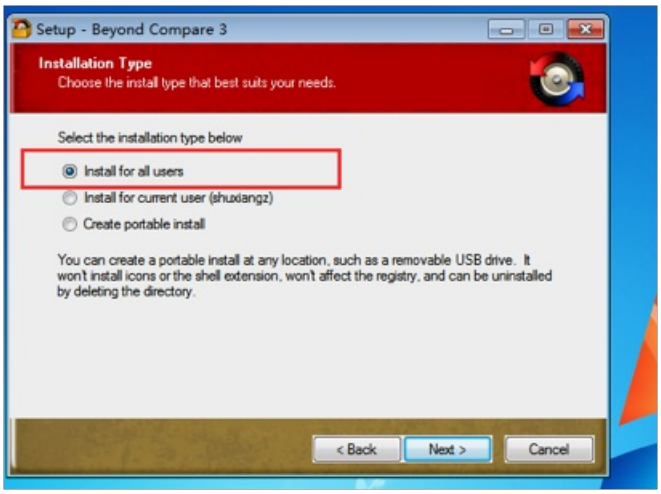
Cómo aparecen las aplicaciones en el menú Inicio

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.

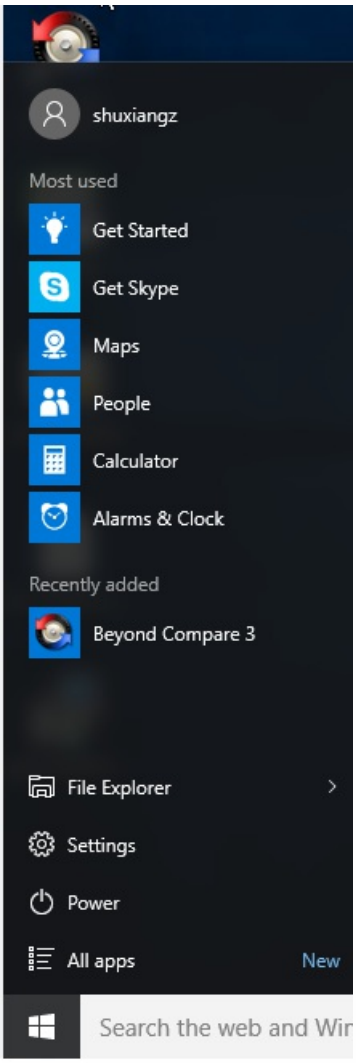
Por ejemplo, cree una nueva aplicación y póngala a disposición de todos los usuarios:

1. Instale una aplicación en el AppDisk (por ejemplo, *Beyond Compare*):

© 1999-2017 Citrix Systems, Inc. All rights reserved.



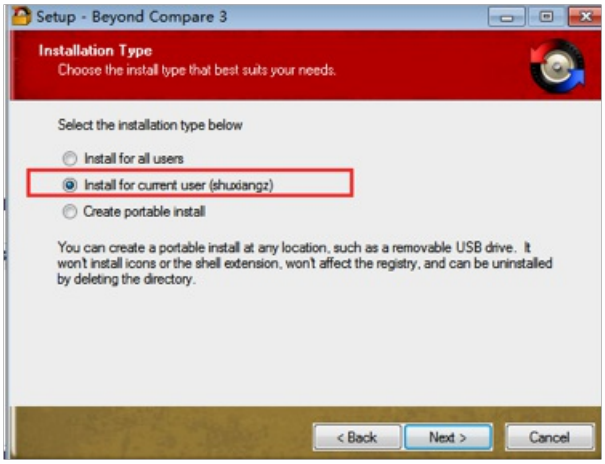
2. Conecte el disco al escritorio y el acceso directo de la aplicación recién instalada (*Beyond Compare*) aparecerá en el menú Inicio:



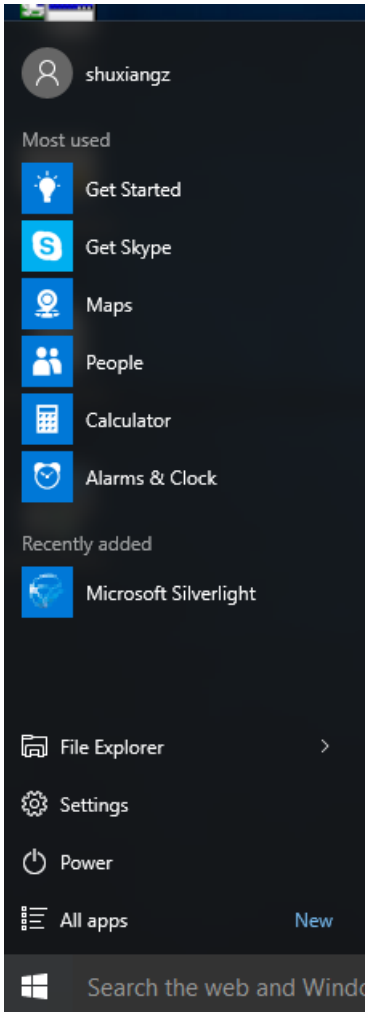
Para instalar una aplicación solo para el usuario actual:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Instale una aplicación en el AppDisk y póngala a disposición del usuario actual:



2. Conecte el disco al escritorio; tenga en cuenta que el acceso directo no aparecerá en el menú Inicio:



Actualizaciones en la captura de registros de AppDisk

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Esta versión ofrece una mejora al paradigma de asistencia y captura de registros de AppDisk. Con esta actualización, los usuarios de AppDisk pueden obtener información de diagnóstico y cargarla en el sitio Web de Citrix Insight Services (CIS).

¿Cómo funciona?

En esta nueva 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 PowerShell 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.

Uso de scripts de PowerShell para recopilar archivos de registro de AppDisk o PVD

El programa de instalación de AppDisk o PVD agrega dos scripts nuevos 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.

> **Nota**
>
> 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, si quiere, cargar manualmente los datos en el sitio Web de CIS.

```
comando                                                    COPIAR
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
SYNTAX

    Upload-AppDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]

        -OutputFile

            Local path for zip file instead of uploading to CIS

 EXAMPLES

    Upload-AppDDiags

        Upload diagnostic data to Citrix CIS website using credentials entered by interactive user.

    Upload-AppDDiags -OutputFile C:\MyDiags.zip

        Save AppDisk diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.
```

Sugerencia

Si no hay ningún argumento **–OutputFile**, la carga tiene lugar. Si se especifica **–OutputFile**, el script crea un archivo ZIP que se puede cargar manualmente más tarde.

Upload-PvDDiags.ps1

Use este script para iniciar la recopilación de datos de diagnóstico de PvD y, si quiere, cargar manualmente los datos en el sitio Web de CIS.

comando COPIAR

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
SYNTAX

 Upload-PvDDiags [[-OutputFile] <string>] [-help] [<CommonParameters>]

    -OutputFile

        Local path for zip file instead of uploading to CIS

 EXAMPLES

    Upload-PvDDiags

        Upload PvD diagnostic data to Citrix CIS website using credentials entered by interactive user.

    Upload-PvDDiags -OutputFile C:\MyDiags.zip

        Save PvD diagnostic data to the specified zip file. You can access https://cis.citrix.com/ to upload it later.
```

Sugerencia

Si no hay ningún argumento **–OutputFile**, la carga tiene lugar. Si se especifica **–OutputFile**, el script crea un archivo ZIP que se puede cargar manualmente más tarde.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp Secure Browser

Dec 05, 2017

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 XenApp 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. XenApp Secure Browser mostrará la aplicación compatible con Internet Explorer como una pestaña en el explorador Firefox.

Implementación de XenApp Secure Browser Edition

Citrix recomienda utilizar el plan de acción (blueprint) Citrix Smart Tools para XenApp Secure Browser con el fin de simplificar la implementación.

El plan de acción de XenApp Secure Browser contiene scripts para automatizar las siguientes tareas:

- Instalar XenApp, incluido Citrix License Server y StoreFront
- Crear un sitio de entrega de XenApp
- Unir las máquinas aprovisionadas al dominio existente

Uso del plan de Citrix Smart Tools

Para usar el plan de Citrix Smart Tools:

1. Desde la página principal de Citrix Cloud, vaya a Services; haga clic en Request Trial for Citrix Smart Tools. Tras solicitar la versión de prueba, recibirá un correo electrónico que le notificará cuándo estará disponible el servicio de prueba. Esto suele tardar de 5 a 10 minutos.
2. Haga clic en Manage en el correo que haya recibido cuando solicitó la versión de prueba para ver la página principal de Citrix Smart Tools.
3. Descargue la imagen ISO de Citrix XenApp Secure Browser Edition desde el sitio de descargas de Citrix.

Tenga en cuenta lo siguiente después de descargar la ISO de Secure Browser Edition:

- Empiece a usar el plan de XenApp Secure Browser siguiendo las instrucciones indicadas en XenApp Secure Installation with a Citrix Smart Tools Blueprint.
- Después de completar la instalación, puede optimizar aún más el entorno para la entrega de aplicaciones Web siguiendo los pasos de configuración especificados en la Guía de implementación de XenApp Secure Browser.

Instalación manual de XenApp Secure Browser

Para instalar XenApp Secure Browser manualmente:

1. Descargue la imagen ISO de Citrix XenApp Secure Browser Edition desde el sitio de descargas de Citrix.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Siga las instrucciones para instalar los diferentes componentes de XenApp.
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.

    Nota: 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.

    Nota: "Asnp" representa Add-PSSnapin.

    c. Compruebe el modo de licencia y la configuración del sitio actuales ejecutando el cmdlet Get-ConfigSite.

    d. Establezca el modo de licencia en XenApp Secure Browser Edition ejecutando Set-ConfigSite -ProductCode XDT -ProductEdition BAS.

    e. Confirme que el modo de licencia y XenApp Secure Browser Edition están configurados correctamente ejecutando el cmdlet Get-BrokerSite.

> ## Nota
>
> Después de completar la instalación, puede optimizar aún más el entorno para la entrega de aplicaciones Web siguiendo los pasos de configuración especificados en la Guía de implementación de XenApp Secure Browser.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Publicación de contenido

Dec 05, 2017

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 igual que las demás aplicaciones de StoreFront y Citrix Receiver. Los usuarios acceden a ese contenido 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 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 del directorio UNC (por ejemplo, file://myServer/myShare o \\myServer\myShare)
- Ruta del archivo UNC (por ejemplo, file://myServer/myShare/myFile.asf o \\myServer\myShare\myFile.asf)

Compruebe que cuenta con el SDK correcto.

- Para implementaciones de XenApp and XenDesktop Service, descargue e instale el SDK de XenApp y XenDesktop de PowerShell remoto.
- Para implementaciones locales de XenApp y XenDesktop, 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Se ha creado un catálogo de máquinas.
- Se ha creado un grupo de entrega llamado PublishedContentApps. El grupo utiliza una máquina de SO de servidor proveniente del catálogo. Se ha agregado la aplicación WordPad al grupo.
- Se han hecho asignaciones para el nombre del grupo de entrega, la ubicación CommandLineExecutable y el nombre de la aplicación.

Introducción

En la máquina que contiene el SDK de PowerShell, abra PowerShell.

El cmdlet siguiente agrega el complemento adecuado del SDK de PowerShell y asigna el registro devuelto del grupo de entrega.

```
Add-PsSnapin Citrix*
$dg = Get-BrokerDesktopGroup –Name PublishedContentApps
```

Si utiliza XenApp and XenDesktop Service, debe autenticarse con sus credenciales de Citrix Cloud. Si hay más de un cliente, elija uno.

Publicación de 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.

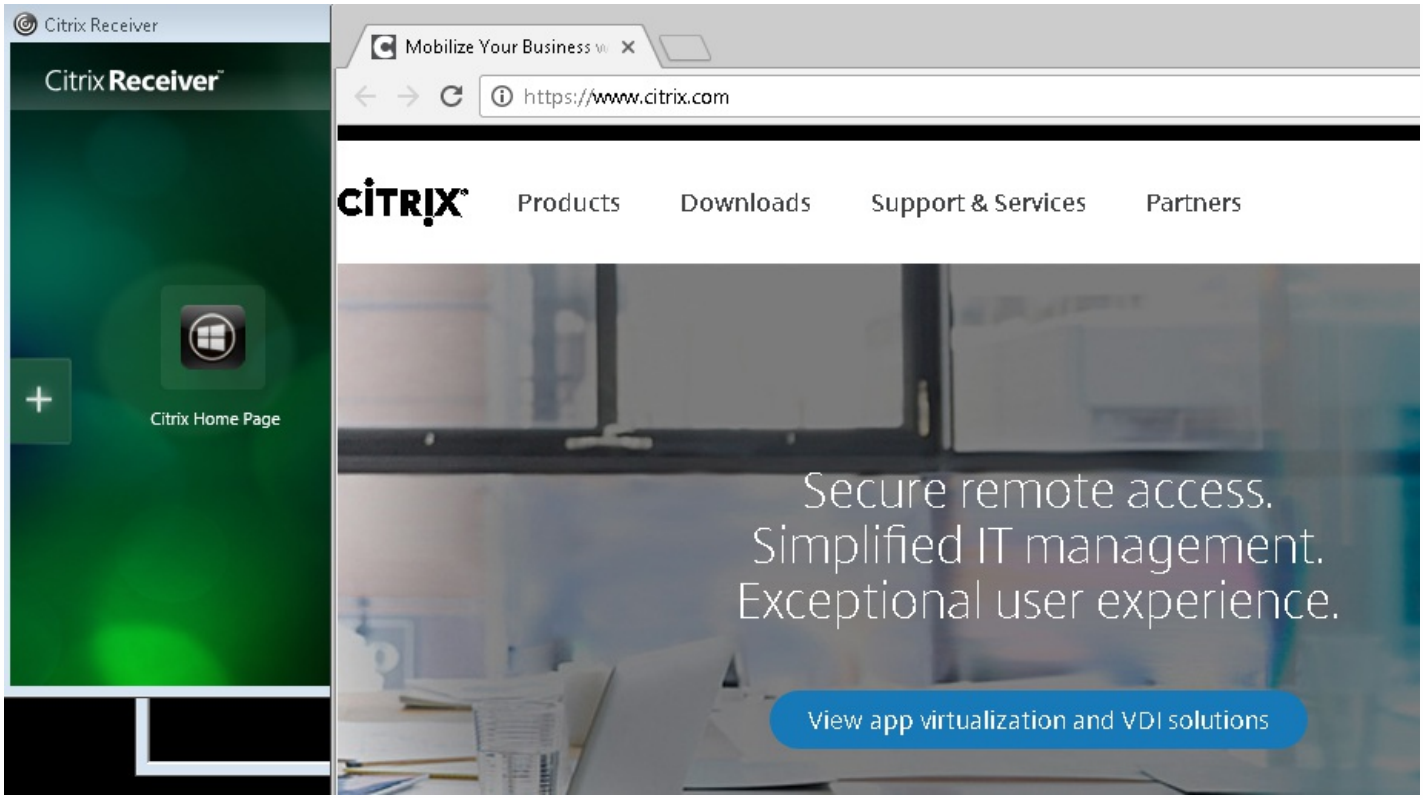
```
$citrixUrl = "https://www.citrix.com/"
$appName = "Citrix Home Page"

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Publicación de recursos ubicados en rutas UNC

En este ejemplo, el administrador ya ha creado un recurso compartido llamado PublishedResources. Después de asignar las ubicaciones y los nombres de las aplicaciones, los siguientes cmdlets publican un archivo RTF y un archivo DOCX en ese recurso compartido.

```
$rtfUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedRTF.rtf"
$rtfAppName = "PublishedRTF"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $rtfUNC -Name $rtfAppName
-DesktopGroup $dg.Uid

$docxUNC = "\\GMSXJ-EDGE0.xd.local\PublishedResources\PublishedDOCX.docx"
$docxAppName = "PublishedDOCX"

New-BrokerApplication –ApplicationType PublishedContent
–CommandLineExecutable $docxUNC -Name $docxAppName
-DesktopGroup $dg.Uid
```

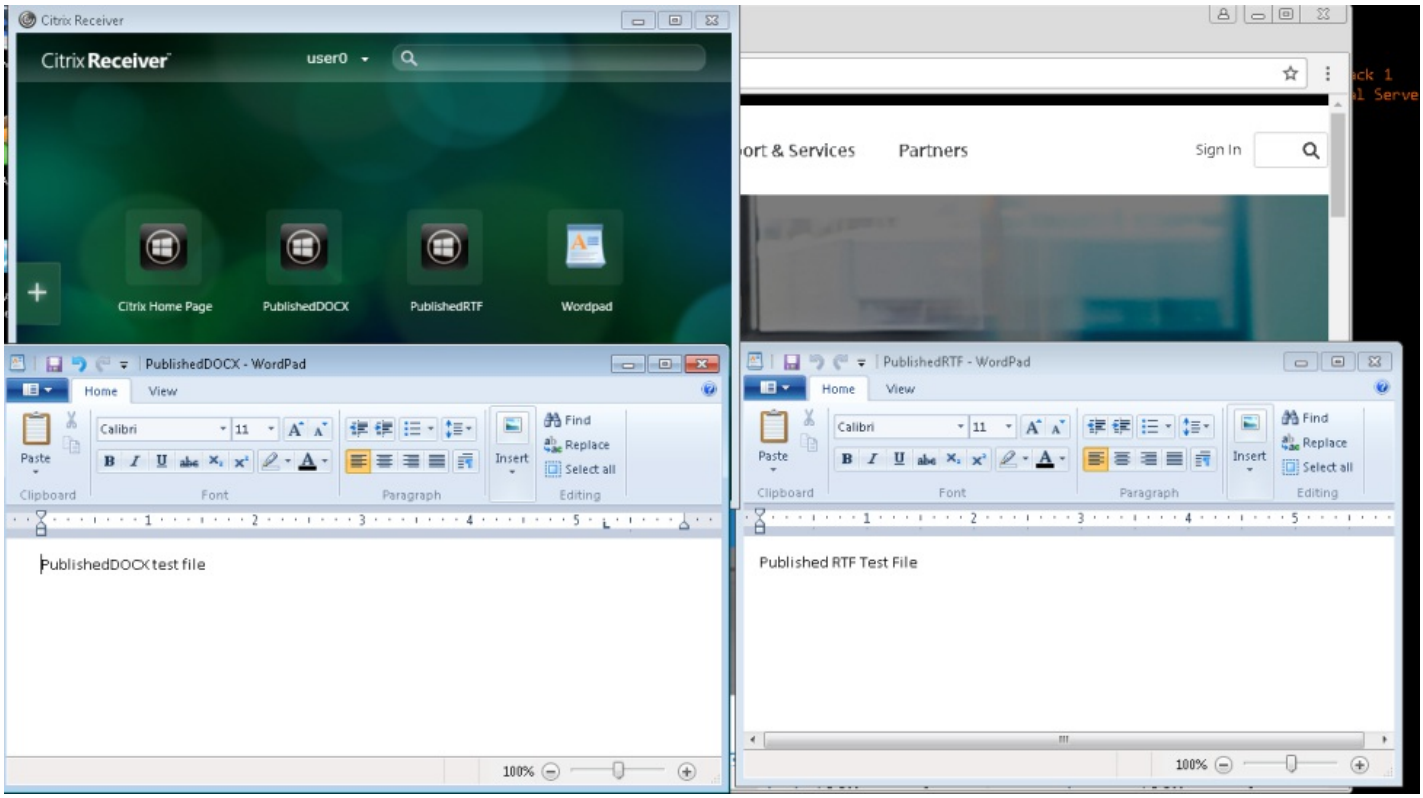
Compruebe el resultado:

- Actualice la ventana de StoreFront para ver los documentos recién publicados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



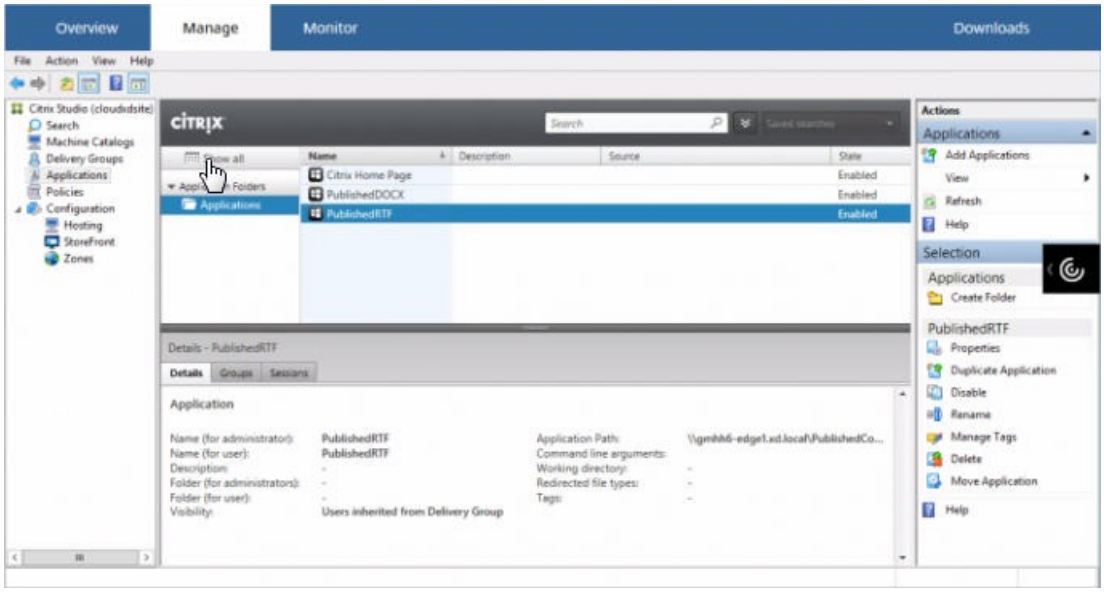
- Haga clic en las aplicaciones PublishedRTF y PublishedDOCX. Cada documento se abre en un WordPad ejecutado localmente.



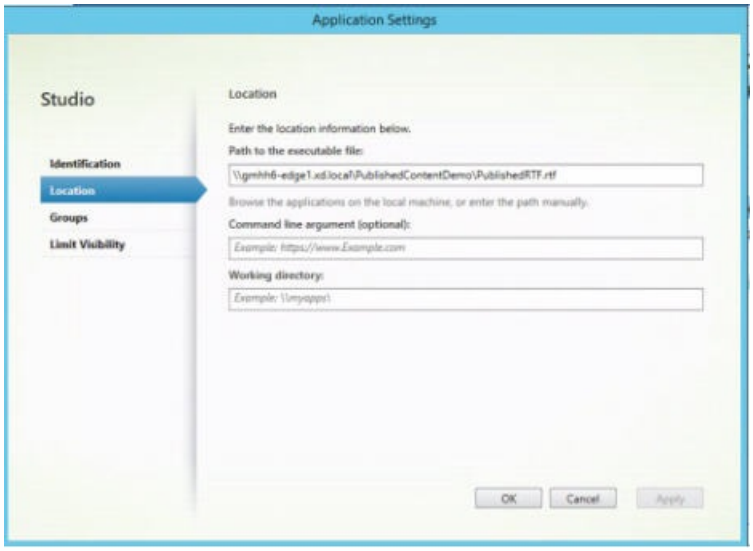
Cómo ver y editar aplicaciones PublishedContent

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



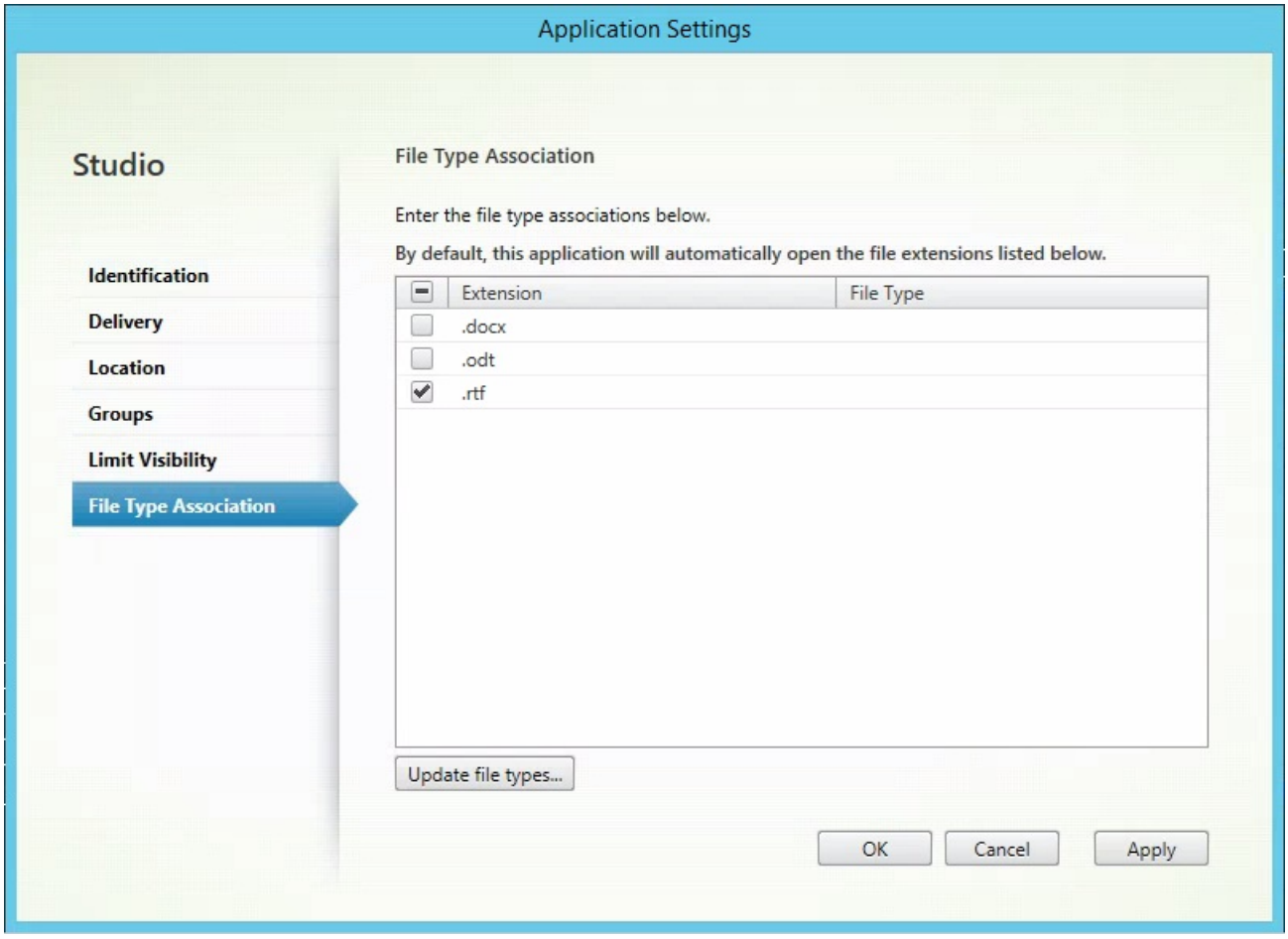
Las propiedades de aplicación (por ejemplo, la visibilidad a los usuarios, la asociación de grupo y el acceso directo) se aplican al contenido publicado. Sin embargo, no puede cambiar el argumento de la línea de comandos ni las propiedades del directorio de trabajo que se ven en la página **Ubicación**. Para cambiar el recurso, modifique el campo "Ruta del archivo ejecutable" en dicha página.



Si quiere usar una aplicación publicada para abrir una aplicación PublishedContent (en lugar de una aplicación local), modifique la propiedad de 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.

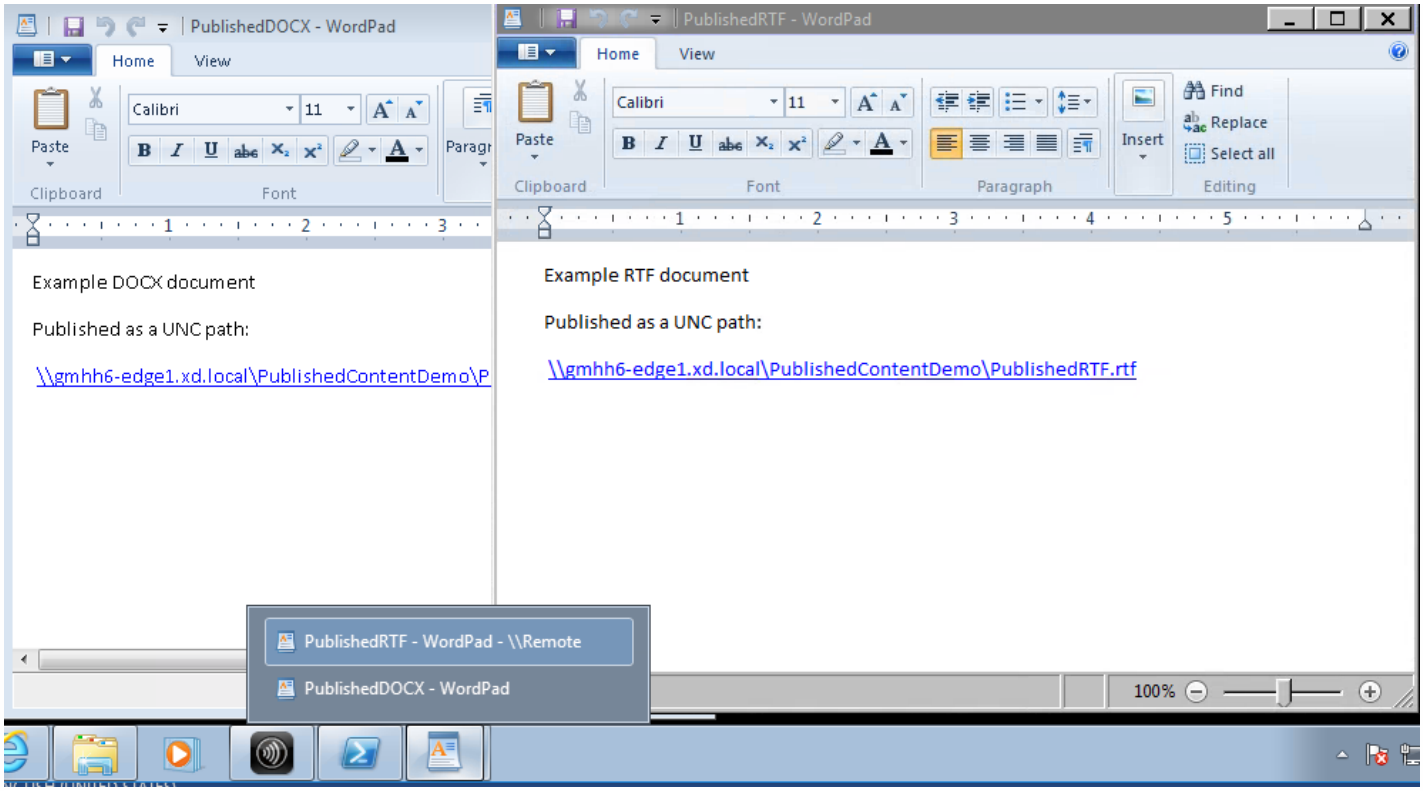
Importante: Active el modo de mantenimiento para el grupo de entrega antes de modificar la asociación de tipos de archivo. Recuerde que debe desactivar el modo de mantenimiento cuando haya terminado.

© 1999-2017 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para obtener más información

- Creación de catálogos de máquinas
- Creación de grupos de entrega
- Cómo cambiar las propiedades de la aplicación

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDI de servidor

Dec 05, 2017

Use la función VDI (infraestructura de escritorios virtuales) de servidor para entregar escritorios desde un sistema operativo de servidor a un solo usuario.

- Los administradores de empresa pueden entregar sistemas operativos de servidor como escritorios VDI, lo cual puede ser útil para usuarios como ingenieros y diseñadores.
- Los proveedores de servicios pueden ofrecer escritorios desde la nube; esos escritorios cumplen con el Contrato de licencia de proveedor de servicios (SPLA) de Microsoft.

Puede usar la configuración de directiva "Enhanced Desktop Experience" de Citrix para que el sistema operativo del servidor parezca un sistema operativo de escritorio.

Las siguientes funciones no se pueden usar con VDI de servidor:

- Discos Personal vDisk
- Aplicaciones alojadas
- Acceso a aplicaciones locales
- Conexiones de escritorio directas (sin broker)
- Acceso con Remote PC

Para que los servidores VDI funcionen con los dispositivos TWAIN (por ejemplo, escáneres), debe instalarse la característica Experiencia de escritorio de servidor Windows. En Windows Server 2012, esta es una característica opcional que se instala desde Herramientas administrativas > Administrador del servidor > Características > Agregar características > Experiencia de escritorio.

El VDI de servidor se admite en los mismos sistemas operativos de servidor que el VDA con SO de servidor Windows.

Para instalar el VDI de servidor:

Paso 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.)
- Asegúrese de que la propiedad 'Restringir cada usuario a una sola sesión' está habilitada.

    En Windows Server 2008 R2, acceda a esta propiedad desde Herramientas administrativas > Servicios de Escritorio remoto > Configuración de host de sesión de Escritorio remoto. En la sección Editar configuración > General, el parámetro Restringir cada usuario a una sola sesión debe indicar Sí.

    En Windows Server 2012 R2 o Windows Server 2016, modifique el Registro y establezca el parámetro de Terminal Server. En la clave de Registro HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer, establezca DWORD fSingleSessionPerUser en 1.

Paso 2. Para Windows Server 2008 R2, instale Microsoft .NET Framework 3.5 SP1 en el servidor antes de instalar el VDA.

Paso 3. Use la interfaz de línea de comandos correspondiente al programa de instalación para instalar un VDA en un servidor compatible o en la imagen maestra de un servidor compatible. Debe especificar las opciones /quiet y /servervdi. (De forma

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.)

Implementaciones locales de XenApp y XenDesktop: XenDesktopVdaSetup.exe /quiet /servervdi

Implementaciones locales de XenApp y XenDesktop o implementaciones de XenDesktop Service: VDAWorkstationSetup.exe /quiet /servervdi

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 /masterimage si está instalando el VDA en una imagen y va a usar MCS para crear máquinas VM de servidor a partir de esa imagen.

No incluya opciones para funciones que no son compatibles con VDI de servidor, como, por ejemplo, /baseimage.

Paso 4. Cree un catálogo de máquinas para VDI de servidor.

- 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 Server VDI; 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 que creó aparece en la ficha Máquinas con SO de escritorio, aunque el VDA se instalara en un servidor.

Paso 5. Cree un grupo de entrega y asigne el catálogo de Server VDI que creó en el paso anterior.

Si no ha especificado los Delivery Controllers o Cloud Connector durante la instalación del VDA, especifíquelos posteriormente con la configuración de directivas de Citrix, con Active Directory o con la modificación de los valores del Registro en la máquina del agente VDA. Consulte Registro de VDA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personal vDisk

Dec 05, 2017

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 si el administrador modifica la imagen maestra, las implementaciones con discos Personal vDisk conservan dichos cambios. Esto significa que los administradores pueden administrar de manera centralizada y sencilla las imágenes maestras, al mismo tiempo que proporcionan a los usuarios una experiencia de escritorio personalizada.

Los discos Personal vDisk permiten esta separación al redirigir todos los cambios que efectúa el usuario en la máquina virtual a un disco aparte (el disco Personal vDisk) asociado a la máquina virtual del usuario. El contenido del disco Personal vDisk se fusiona en tiempo de ejecución con el contenido de la imagen publicada para proporcionar una experiencia unificada. De este modo, los usuarios pueden seguir accediendo a las aplicaciones aprovisionadas por el administrador en la imagen maestra.

Los discos virtuales personales constan de dos partes, que utilizan letras de unidad distintas y tienen el mismo tamaño de manera predeterminada:

- Perfil de usuario. Contiene los datos, los documentos y el perfil del usuario. De manera predeterminada, esta parte usa la unidad P: pero se puede seleccionar otra letra de unidad cuando se crea un catálogo de máquinas con discos Personal vDisk. La unidad usada también depende del parámetro EnableUserProfileRedirection.
- Archivo de 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 conflictos.

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 Personal vDisk garantizan que todos los cambios hechos y todas las aplicaciones instaladas se guardan en el disco virtual personal. Cuando una aplicación de un disco Personal vDisk coincide exactamente con una aplicación existente en la imagen maestra, la copia de Personal vDisk se descarta para ahorrar espacio, sin que el usuario pierda acceso a ella.

Físicamente, los discos Personal vDisk se almacenan en el hipervisor, pero no es necesario que residan en la misma ubicación que los demás 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Personal vDisk 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.

> ## Nota
>
> Consulte el artículo Solución de problemas para obtener información sobre informes, mensajes y problemas conocidos de PvD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación y actualización

Dec 05, 2017

Personal vDisk 7.x se respalda desde XenDesktop 5.6 hasta la versión actual. La documentación referente a los requisitos del sistema para cada versión de XenDesktop ofrece una lista de los sistemas operativos compatibles con los agentes Virtual Delivery Agent (VDA), las versiones compatibles de hosts (recursos de virtualización) y Provisioning Services. Para obtener más información acerca de las tareas de Provisioning Services, consulte la documentación actualizada de Provisioning Services.

Instalación y habilitación de 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 Instalación de 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 XenApp o XenDesktop.

Cómo 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 Provisioning Services (PVS), Personal vDisk se habilita automáticamente o bien cuando ejecuta el inventario durante el proceso de creación de imagen maestra (base), o bien cuando la actualización automática ejecuta el inventario por usted.

Por lo tanto, si instala los componentes de PvD, pero no los habilita durante la instalación del VDA, puede utilizar la misma imagen para crear escritorios con o sin PvD, debido a que PvD se habilita durante el proceso de creación del catálogo.

Cómo agregar discos Personal vDisk

Los discos Personal vDisk se agregan a hosts cuando se 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.

Actualización de 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 XenDesktop. A continuación, se puede ejecutar el inventario de PvD.

Desinstalación de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si ha actualizado Personal vDisk mediante el archivo MSI de PvD, puede desinstalarlo desde la lista de programas.

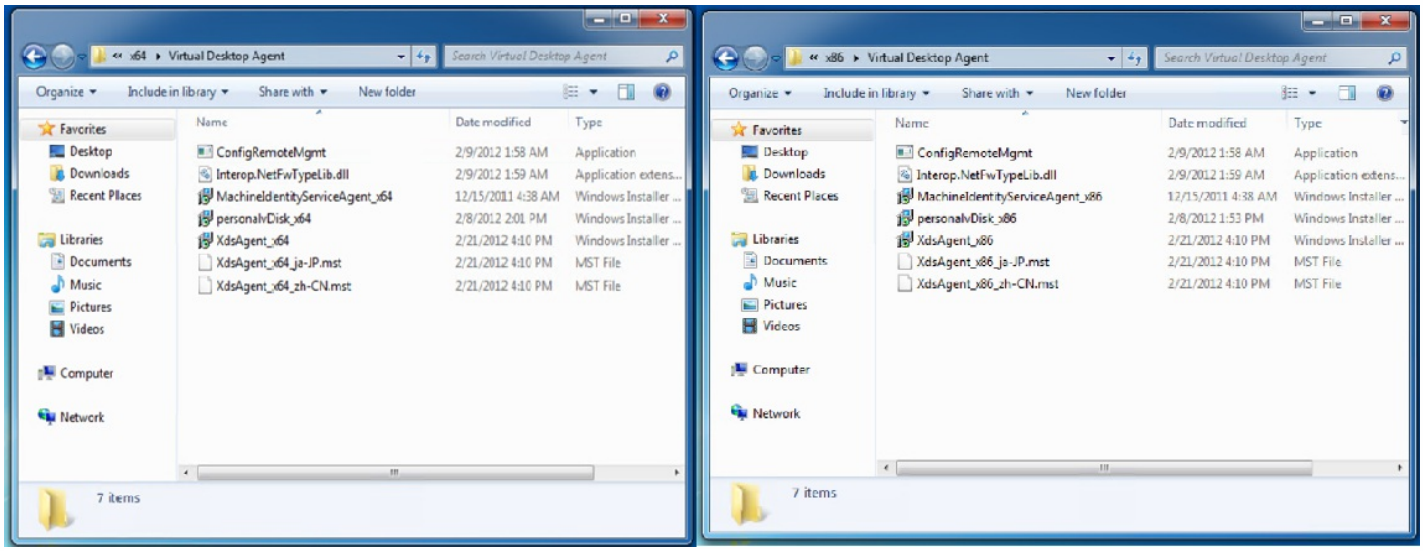
Si desinstala PvD y quiere volver a instalar la misma versión o una versión más reciente, primero haga una copia de seguridad de la clave de Registro HKLM\Software\Citrix\personal vDisk\config, que contiene los parámetros de configuración del entorno que pueden haber cambiado. Después de instalar PvD, restablezca los valores del Registro que puedan haber cambiado. Para ello, compárelos con la versión de la copia de seguridad.

Consideraciones importantes al desinstalar Personal vDisk

La desinstalación puede fallar si se ha instalado un disco Personal vDisk con Windows 7 (64 bits) en la imagen base. Para evitar este problema, Citrix recomienda que quite el disco Personal vDisk antes de actualizar:

1. Seleccione la copia correspondiente del instalador vDisk en los medios de XenApp o XenDesktop. Busque el instalador MSI más reciente de Personal vDisk en la imagen ISO de XenApp o XenDesktop 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

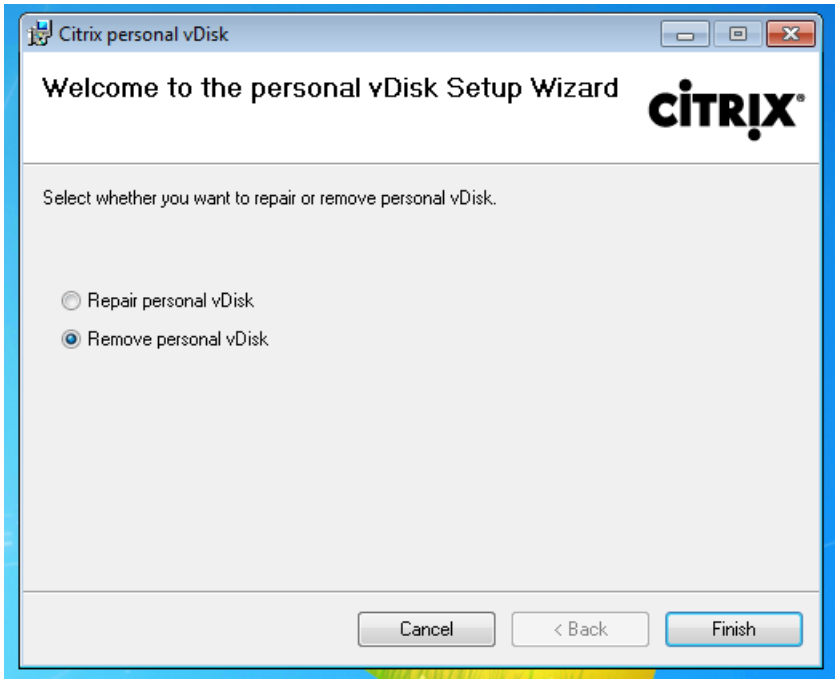


2. Quite la instalación de Personal vDisk. Seleccione el paquete de instalador MSI de Personal vDisk que ha localizado en el paso 1. Aparecerá la pantalla de configuración de Personal vDisk.

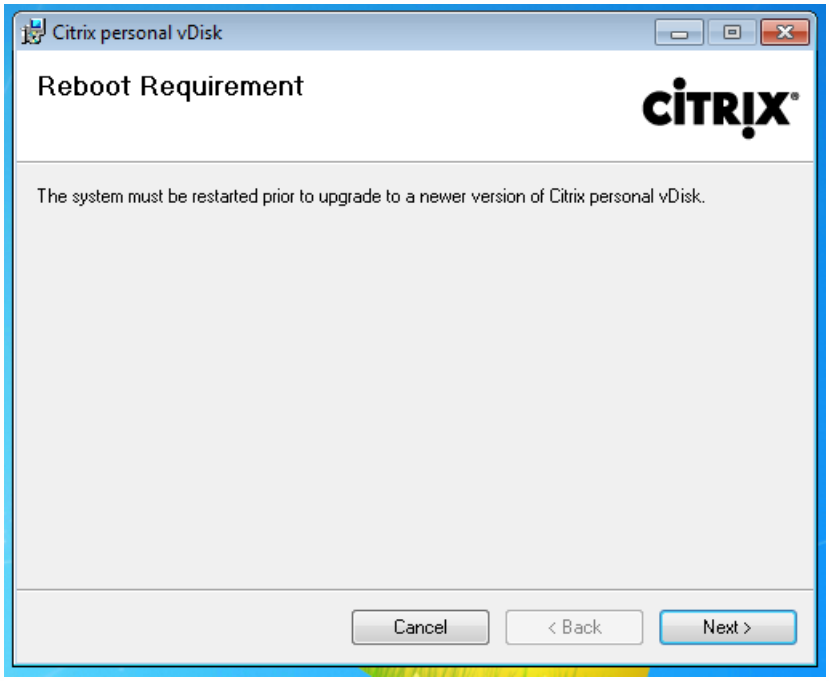
3. Seleccione "Quitar personal vDisk".

4. Haga clic en **Finalizar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

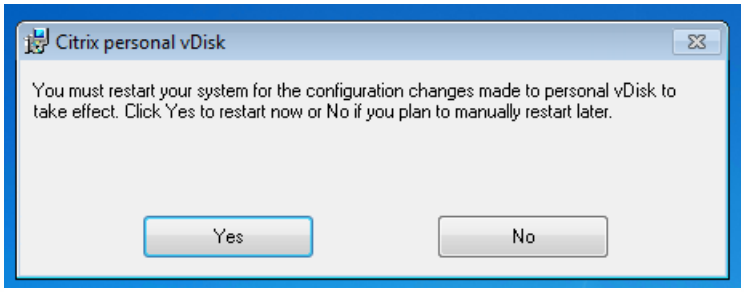


5. Aparecerá una página con el requisito de reiniciar la máquina. Haga clic en **Siguiente**:



6. Haga clic en **Sí** para reiniciar el sistema y aplicar los cambios de configuración:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración y administración

Dec 05, 2017

En este apartado se describen los elementos que se deben tener en cuenta a la hora de configurar y administrar un entorno de Personal vDisk (PvD). También se incluyen las prácticas recomendadas y las descripciones de las tareas pertinentes.

En el caso de tareas que implican trabajar con el Registro de Windows:
Precaución: Si 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenDesktop) o la herramienta Personal vDisk Image Update Monitoring Tool (en la carpeta Support/Tools/Scripts\PvdTool) pueden ayudar a identificar los discos PvD de un catálogo que se estén actualizando y que están casi llenos.

  La presencia de productos antivirus puede afectar el tiempo necesario para ejecutar el inventario o realizar una actualización. El rendimiento se puede mejorar si agrega CtxPvD.exe y CtxPvDSvc.exe a la lista de exclusión del producto antivirus. Estos archivos se encuentran en C:\Archivos de programa\Citrix\Personal vDisk\bin. La exclusión de esos ejecutables para que no sean analizados por el antivirus puede mejorar el rendimiento del inventario y de las actualizaciones de imagen y mejorar su velocidad hasta diez veces.

- **Los recursos por crecimiento inesperado (instalación inesperada de aplicaciones, entre otros)**
  Tenga en cuenta la conveniencia de agregar una cantidad de espacio extra (ya sea una cantidad fija o un porcentaje del total del disco PvD) al tamaño total para que, de ese modo, quepan instalaciones no previstas de aplicaciones que el usuario realice durante la implementación.

Cómo configurar el tamaño y la asignación del disco Personal vDisk

Es posible ajustar de forma manual el algoritmo de cambio automático de tamaño que determina el tamaño del disco VHD en relación a la unidad P:. Para ello, establezca el tamaño inicial del disco VHD. Esto puede resultar útil si, por ejemplo, se sabe que los usuarios instalarán varias aplicaciones que son demasiado grandes para la capacidad del VHD incluso 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.

Compruebe 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

(No modifique ningún otro parámetro de esta clave de 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 de perfil 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, automáticamente cambia el tamaño del área de las aplicaciones (C:) cuando el espacio disponible en C: baja del 10 %. Los valores permitidos son 1 y 0. Para que el cambio de tamaño tenga efecto, es necesario un reinicio.
  - Cuando se establece en 0, el tamaño del disco VHD se determina según el método usado en las versiones anteriores a XenDesktop 7.x

  Valor predeterminado = 1

- **EnableUserProfileRedirection**
  Habilita o inhabilita la redirección del perfil del usuario al disco virtual.
  - 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:\Users 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: se asigne a las aplicaciones.

    Se asume que, si este valor se establece 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 Personal vDisk a C: y oculta el disco PvD.

  Configure este valor antes de implementar un catálogo. Este valor 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **PercentOfPvDForApps**
  Define la división entre la parte de las aplicaciones (C:) y la parte del perfil del disco virtual. Este valor se usa al crear nuevas máquinas virtuales y durante las actualizaciones de imagen cuando EnableDynamicResizeOfAppContainer tiene el valor 0.

  Cambiar PercentOfPvDForApps solo es efectivo cuando EnableDynamicResizeOfAppContainer tiene el valor 0. De forma predeterminada, EnableDynamicResizeOfAppContainer está establecido en 1 (habilitado), lo que significa que AppContainer (que aparece como la unidad C:) es dinámico, por lo que solo se expande cuando queda menos del 10 % del espacio disponible.

  Cuando se aumenta PercentOfPvDForApps solo se aumenta el espacio máximo para el que se permite expandir la parte de Aplicaciones. El espacio no se aprovisiona inmediatamente. También debe configurar la división de espacio en la imagen maestra donde se aplicará durante la próxima actualización de imagen.

  Si ya ha generado un catálogo de máquinas con el parámetro EnableDynamicResizeOfAppContainer establecido en 1, cambie ese parámetro a 0 en la imagen maestra para la siguiente actualización y configure una división de espacio apropiada. El tamaño de división solicitado se aplicará siempre que sea mayor que el tamaño actualmente asignado para la unidad C:.

  Si quiere conservar el control total sobre la división de espacio, este valor debe establecerse en 0. Esto permite el control total sobre el tamaño de la unidad C:, en lugar de depender de que un usuario consuma espacio por debajo del umbral para expandir la unidad.

  Valor predeterminado = 50 % (se asigna un espacio de igual tamaño a ambas partes)

- **PvDReservedSpaceMB**
  Define el tamaño del espacio reservado (en MB) en el disco virtual para almacenar los registros de Personal vDisk y otros datos.

  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 de XenDesktop, se utiliza 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. Si Windows Update Service tiene que ejecutarse en el disco Personal vDisk (PvD), puede optar por la opción No buscar actualizaciones para ayudar a evitar que se instalen actualizaciones en las máquinas asociadas.
  La Tienda de Windows 8 necesita ejecutar este servicio para instalar cualquier aplicación de estilo Moderno.

- **Actualizaciones de Windows**. Se incluyen las actualizaciones de Internet Explorer y se debe aplicar en la imagen maestra.
- **Actualizaciones que requieren reinicios**: Las actualizaciones de Windows aplicadas en la imagen maestra pueden requerir varios reinicios para instalarse completamente, según el tipo de revisión que se entregue con ellas. Debe reiniciar correctamente la imagen maestra para completar la instalación de las actualizaciones de Windows aplicadas a ella antes de seleccionar el inventario de PvD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Actualizaciones de aplicaciones**. Actualice las aplicaciones instaladas en la imagen maestra para conservar espacio en los discos Personal vDisk de los usuarios. Así 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, Citrix Receiver)
- 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 una gran cantidad 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 e instalar esa misma aplicación en su disco Personal vDisk.
- Actualice o desinstale aplicaciones con cuidado en la imagen maestra. Después de instalar la 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 actualización posterior de Office en la imagen maestra podría hacer que la versión local instalada de Visio pasara a ser inutilizable.
- No se admite el software que usa licencias dependientes del hardware (ya sea mediante llaves o hardware basado en firma).

Consideraciones: Provisioning Services

Al usar Provisioning Services 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. Esto garantiza que los escritorios PvD se colocan en el estado de preparación (Preparing) cuando el vDisk de Provisioning Services (PVS) pasa a la fase de producción.
- Debe usarse la función de control de versiones de Provisioning Services 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 Provisioning

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Services (de lo contrario, Provisioning Services 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. Esto implica que se puede reducir el tamaño del disco de memoria caché de escritura de Provisioning Services. No obstante, cuando PvD no está activo (como, por ejemplo, durante las operaciones de actualización de la imagen), un disco pequeño de memoria caché de escritura de Provisioning Services podría llegar a llenarse, lo que provocaría un bloqueo de la máquina.

Citrix recomienda asignar un tamaño a los discos de memoria caché de escritura de Provisioning Services según las prácticas recomendadas de Provisioning Services. Asimismo, se recomienda agregar un espacio que doble el tamaño del disco VHD de plantilla en la imagen maestra (para que se cumplan los requisitos de fusión). Es muy poco probable que una operación de fusión requiera todo este espacio, pero podría darse el caso.

Al usar Provisioning Services para implementar un catálogo de máquinas con Personal vDisk habilitado:
- Siga las instrucciones indicadas en la documentación de Provisioning Services.
- 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 Provisioning Services 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 Provisioning Services 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 de XenDesktop.
- 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 especificada durante la actualización de la máquina.
- Use la herramienta Personal vDisk Image Update Monitoring Tool o el script personal-vdisk-poolstats.ps1 para supervisar

© 1999-2017 Citrix Systems, Inc. All rights reserved.

el disco Personal vDisk en el estado de preparación (Preparing).

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 hacerlo cuando los discos Personal vDisk están en fase de implementación. Los archivos de reglas tienen el nombre custom_*_rules.template.txt y se encuentran en la carpeta \config. Los comentarios de cada archivo ofrecen documentación adicional.

Cómo ejecutar el inventario al actualizar una imagen maestra

Con Personal vDisk habilitado, después de realizar actualizaciones en la imagen maestra posteriores a la instalación, es importante actualizar el inventario del disco ("ejecutar el inventario") y tomar una nueva instantánea.

Puesto que son los administradores y no los usuarios quienes administran las imágenes maestras, si instala una aplicación que coloca archivos binarios en el perfil de usuario del administrador, dicha aplicación no está disponible para los usuarios de los escritorios virtuales compartidos (incluidos aquellos basados en catálogos agrupados de máquinas y catálogos agrupados de máquinas con Personal vDisk). Son los propios usuarios quienes tienen que instalar las aplicaciones.

Se recomienda tomar una instantánea de la imagen después de realizar cada paso de este procedimiento.

1. Actualice la imagen maestra instalando aplicaciones y actualizaciones del sistema operativo y configurando el sistema en la máquina como desee.
   Para las imágenes maestras basadas en Windows XP que desee implementar con discos Personal vDisk, compruebe que no haya ningún cuadro de diálogo abierto (por ejemplo, mensajes que confirman la instalación de un programa o mensajes que piden autorización para usar controladores sin firma). Cuando quedan cuadros de diálogo abiertos en imágenes maestras en este entorno, se impide que VDA pueda registrarse con el Delivery Controller. Para impedir la aparición de mensajes que piden autorización para usar controladores sin firma, use el Panel de control. Por ejemplo, vaya a Sistema > Hardware > Firma de controladores, y seleccione la opción pertinente para omitir advertencias.
2. Apague la máquina. Para máquinas con Windows 7, haga clic en Cancelar cuando el disco Personal vDisk de Citrix bloquee el apagado de la máquina.
3. En el cuadro de diálogo del disco Citrix Personal vDisk, haga clic en Actualizar inventario. Este paso puede tardar varios minutos en completarse.
   Importante: Si interrumpe el siguiente apagado (aunque sea para realizar una pequeña actualización en la imagen), el inventario del disco Personal vDisk ya no coincidirá con la imagen maestra. Esto hace que la función Personal vDisk deje de funcionar. Si interrumpe el apagado del sistema, debe reiniciar la máquina, apagarla y, cuando lo pida el sistema, hacer clic de nuevo en Actualizar inventario.
4. Cuando la operación de inventario haya apagado la máquina, tome una instantánea de la imagen maestra.

Puede exportar un inventario a un punto compartido de red y, a continuación, importar ese inventario en una imagen maestra. Para obtener más información, consulte Exportación e importación de un inventario de PvD.

Cómo configurar parámetros de 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 valores de limitación de conexiones:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 la cantidad de máquinas virtuales que deben estar activas en un momento dado en el almacenamiento. Calcule este valor dividiendo el total de IOPS entre IOPS/VM.

     Por ejemplo, si el almacenamiento del usuario final es de 14 000 IPS, la cantidad de máquinas virtuales es: 14 000 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 en 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 en 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).
   1. 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.
   2. 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

instalar igual que otra aplicación de imagen maestra. La siguiente información se aplica solo a System Center Configuration Manager 2007. No se admiten las versiones de Configuration Manager anteriores a Configuration Manager 2007.

Complete los siguientes pasos para utilizar el software del agente Configuration Manager 2007 en un entorno de Personal vDisk.

1. Instale el agente cliente en la imagen maestra.
    1. Instale el cliente de Configuration Manager en la imagen maestra.
    2. Detenga el servicio ccmexec (SMS Agent) e inhabilítelo.
    3. 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)
    4. Elimine o cambie de nombre el archivo C:\Windows\smscfg.ini.
2. Quite la información que identifique de manera exclusiva al cliente.
    1. (Opcional) Elimine o mueva archivos de registros de C:\Windows\System32\CCM\Logs.
    2. Instale Virtual Delivery Agent (si no estaba ya instalado) y seleccione el inventario de PvD.
    3. 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. Puede hacerlo mediante un objeto de directiva de grupo (GPO) de dominio, por ejemplo.
    - Confirme que PvD está activo comprobando la presencia de la clave de Registro HKLM\Software\Citrix\personal vDisk\config\virtual.
    - Configure el servicio ccmexec (agente SMS) en Automático e inicie el servicio. El cliente de Configuration Manager contacta con el servidor de Configuration Manager, y obtiene certificados y GUID nuevos y exclusivos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Herramientas

Dec 05, 2017

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:

- Cómo se ven 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 XenDesktop. 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.

Restablecimiento del área de aplicaciones

Si un escritorio queda dañado (después de instalar una aplicación defectuosa o por algún otro motivo), puede revertir el área de aplicaciones del disco PvD a su estado predeterminado de fábrica (vacío). La operación de restablecimiento deja intacta el área de datos de perfil de usuario.

Para restablecer el área de aplicaciones del disco PvD, use uno de estos métodos:

- Inicie 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exportación e importación de 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 “<path-to-export-location>”

  El software detecta la ubicación del inventario actual y lo exporta a una carpeta denominada “ExportedPvdInventory” en la ubicación especificada. Este es un fragmento del resultado devuelto por el comando:
  C:\Archivos de programa\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 \\ …. Código de error = OPS
- Para importar un inventario ya exportado, ejecute el comando de importación como administrador en la imagen maestra:

Cómo 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 <network location\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. Un fragmento del resultado devuelto por el comando:
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory
\\share location\ExportedInventory\ExportedPvdInventory
Importing inventory \\share location\ExportedInventory\ExportedPvdInventory
…
Successfully added inventory \\share location\ExportedInventory\ExportedPvdInventory to the
store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
Después de la exportación, el recurso 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pantallas, mensajes y solución de problemas

Dec 05, 2017

Supervisión de 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. Ejecute **C:\Archivos de programa\Citrix\personal vDisk\bin\CtxPvdDiag.exe** en la máquina que quiera supervisar.
2. Vaya a la ubicación donde quiere 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 del 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 generan en P:\Usuarios\\AppData\Local\Temp\PVDLOGS, aunque se transfieren a la ubicación seleccionada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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-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)**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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\Settings\Inventory\VER-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.

- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Se ha producido un error interno durante el inicio de Personal vDisk. Revise los registros de Personal vDisk para obtener más información.**
  Código de error 10. Esto puede deberse a que el controlador de PvD no haya podido iniciar una sesión de virtualización a raíz de un error interno o a que Personal vDisk está dañado. Intente reiniciar el escritorio a través del Controller. Si el problema persiste, recopile los registros y póngase en contacto con la asistencia técnica de Citrix.

- **Se ha agotado el tiempo de espera de Personal vDisk cuando intentaba encontrar un disco para almacenar los parámetros de personalización de los usuarios.**
  Código de error 11. Este error se produce cuando el controlador de PvD no puede encontrar el disco PvD en 30 segundos después del reinicio. Esto suele deberse a un tipo de controlador SCSI incompatible o a una latencia de almacenamiento. Si esto ocurre con todos los escritorios del catálogo, cambie el tipo de controlador SCSI asociado a la "VM de plantilla" o a la "VM maestra" por un tipo compatible con la tecnología de Personal vDisk. Si esto ocurre con solo algunos escritorios del catálogo, es posible que se deba a picos de latencia de almacenamiento causados por una gran cantidad de escritorios que se inician al mismo tiempo. Intente limitar el parámetro de número máximo de acciones de energía activo asociado a la conexión de host.

- **Personal vDisk se ha desactivado porque se ha detectado un apagado no seguro del sistema. Reinicie la máquina.**
  Código de error 12. Esto puede deberse a un escritorio que no haya podido completar el proceso de arranque con PvD habilitado. Intente reiniciar el escritorio. Si el problema persiste, vea el inicio del escritorio por medio de la consola del hipervisor y, allí, compruebe si el escritorio se bloquea. Si el escritorio se bloquea durante el inicio, restaure PvD a partir de la copia de seguridad (si dispone de una copia) o bien restablezca PvD.

- **La letra de unidad especificada para montar Personal vDisk no está disponible.**
  Código de error 13. Esto puede deberse a que Personal vDisk no puede montar el disco PvD en el punto de montaje especificado por el administrador. El disco PvD no se podrá montar si otro hardware ya utiliza la letra de unidad. Seleccione otra letra como punto de montaje para Personal vDisk.

- **Los controladores de modo kernel de Personal vDisk no se han podido instalar.**
  Código de error 14. Personal vDisk instala controladores durante la primera actualización de inventario que se realiza después de la instalación. Algunos productos antivirus impiden la instalación del controlador cuando esta instalación tiene lugar fuera del contexto de un instalador. Inhabilite temporalmente el análisis en tiempo real del antivirus o bien agregue excepciones al antivirus para los controladores de PvD durante la creación del primer inventario.

- **No se puede crear una instantánea del volumen del sistema. Compruebe que el Servicio de instantáneas de volumen esté habilitado.**
  Código de error 15. Esto puede suceder porque el Servicio de instantáneas de volumen está inhabilitado. Habilite el Servicio de instantáneas de volumen e intente seleccionar un inventario de nuevo.

- **El diario de cambios no se ha podido activar. Inténtelo de nuevo después de esperar unos minutos.**
  Código de error 16. Personal vDisk utiliza el diario de cambios para realizar un 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.**
  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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **No hay suficiente espacio disponible en el almacenamiento de Personal vDisk. Expanda el almacenamiento de Personal vDisk para proporcionar más espacio.**
  Código de error 18. No hay suficiente espacio disponible en la unidad de Personal vDisk cuando se realiza una actualización de imagen. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk. La actualización de imagen debería volver a iniciarse tras el próximo reinicio.

- **La unidad de almacenamiento de Personal vDisk tiene demasiadas confirmaciones. Expanda el almacenamiento de Personal vDisk para proporcionar más espacio.**
  Código de error 19. No hay suficiente espacio disponible en la unidad de Personal vDisk para que quepa el disco de aprovisionamiento pesado "UserData.V2.vhd". Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk.

- **Registro del sistema dañado.**
  Código de error 20. El Registro del sistema está dañado, es ilegible o no se puede encontrar. Restablezca Personal vDisk o restáurelo a partir de una copia de seguridad anterior.

- **Se ha producido un error interno durante el restablecimiento de Personal vDisk. Revise los registros de Personal vDisk para obtener más información.**
  Código de error 21. Este es un comodín para todos los errores detectados durante un restablecimiento de Personal vDisk. Recopile los registros y póngase en contacto con la asistencia técnica de Citrix.

- **No se ha podido restablecer Personal vDisk porque no hay suficiente espacio libre en el disco de almacenamiento de Personal vDisk.**
  Código de error 22. No hay suficiente espacio disponible en la unidad de Personal vDisk al realizar una operación de restablecimiento. Expanda el almacenamiento de Personal vDisk o elimine archivos no utilizados para liberar espacio en el disco de almacenamiento de Personal vDisk.

Mensajes de error: versiones anteriores a 7.6

Los siguientes errores son válidos para versiones de PvD 7.x anteriores a 7.6:

- **No se pudo iniciar. Personal vDisk no ha podido encontrar el disco para almacenar los parámetros de personalización de usuario.**
  El software de PvD no pudo encontrar el disco Personal vDisk (de manera predeterminada, la unidad P:) o no pudo montarlo como el punto de montaje seleccionado por el administrador cuando se creó el catálogo.
  - Compruebe los registros del servicio de PvD para ver si contienen la entrada: "PvD 1 status --> 18:183".
  - Si está usando una versión de PvD anterior a 5.6.12, resolverá el problema actualizando a la versión más reciente.
  - En cambio, 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 mediante chkdsk.
- **No se pudo iniciar. Citrix Personal vDisk no se ha podido iniciar. Para obtener ayuda... Código de estado: 7, código de error: 0x70**
  El código de estado 7 implica que se encontró un error al intentar actualizar el disco PvD. El error puede ser uno de los siguientes:

Código de error	Descripción
0x20000001	No se pudo guardar el paquete de diferenciación (diff), seguramente debido a que no hay suficiente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Código de error	Descripción
	espacio libre en el disco VHD.
0x20000004	No se pudo obtener los privilegios requeridos para actualizar el PvD.
0x20000006	No se pudo cargar una sección de la imagen del PvD o del inventario de PvD, seguramente debido a que la imagen o el inventario están dañados.
0x20000007	No se pudo cargar el inventario de sistema de archivos, seguramente debido a que la imagen o el inventario de PvD están dañados.
0x20000009	No se pudo abrir el archivo que contiene el inventario de sistema de archivos, seguramente debido a que la imagen o el inventario de PvD están dañados.
0x2000000B	No se pudo guardar el paquete de diferenciación (diff), seguramente debido a que no hay suficiente espacio libre en el disco 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 el disco Personal vDisk, pero no se ha podido crear una sesión de PvD.

  Recopile los registros y compruebe SysVol-IvmSupervisor.log para ver errores de creación de sesiones:
  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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de una actualización de inventario.

3. Reinicie el escritorio virtual afectado. Si el problema continúa, póngase en contacto con la asistencia técnica de Citrix.

- **No se pudo iniciar. Citrix Personal vDisk se ha desactivado porque se ha detectado un apagado no seguro del sistema. Para volver a intentarlo, seleccione Reintentar. Si el problema continúa, póngase en contacto con el administrador del sistema.**

  La VM agrupada no puede iniciarse completamente con el disco 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).

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 aparece ninguno de estos eventos.

El ID de evento 1 indica un mensaje informativo, un ID de evento 2 indica un error. Es posible que no se usen todos los eventos en cada versión de Personal vDisk.

ID de suceso	Descripción
1	Estado de Personal vDisk: Se ha iniciado la actualización del inventario.
1	Estado de Personal vDisk: Se ha completado la actualización del inventario. GUID: %s.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ID de suceso	Descripción
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 cierre incorrecto del sistema.
2	La actualización de la imagen falló. Código de error %d.
2	Personal vDisk encontró un error interno. Código de estado[%d], código de error[0x%X].
2	El restablecimiento de Personal vDisk falló.
2	No se encuentra el disco para almacenar los parámetros de personalización de usuario.
2	No hay suficiente espacio disponible en el disco de almacenamiento para crear un contenedor de Personal vDisk.

Problemas conocidos no relacionados con la versión

Se han identificado estos problemas en 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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. Para solucionarlo, restablezca Personal vDisk. [#474071]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Eliminación de componentes

Dec 05, 2017

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. Al quitar un Controller, el software y las bases de datos de SQL Server no se eliminan.

Antes de quitar un Controller, quítelo del sitio. Antes de quitar Studio o Director, Citrix recomienda cerrarlos.

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 programa de instalación para quitar la Interfaz Web.

Al quitar un VDA, la máquina se reinicia automáticamente después de la eliminación de forma predeterminada.

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, seleccione Citrix XenApp <*versión*> o Citrix XenDesktop *ersión*>. A continuación, haga clic con el botón secundario y seleccione **Desinstalar**. Se inicia el programa de instalación y puede seleccionar los componentes que quiere quitar. También puede quitar StoreFront si hace clic con el botón secundario en **Citrix StoreFront** y selecciona **Desinstalar**.
- Para quitar un VDA, seleccione **Citrix Virtual Delivery Agent** <*versión*>, haga clic con el botón secundario y seleccione **Desinstalar**. Se inicia el instalador y puede seleccionar los componentes que quiere quitar.
- Para quitar Universal Print Server, seleccione **Citrix Universal Print Server** y, a continuación, haga clic con el botón secundario y seleccione **Desinstalar**.

Eliminación de componentes principales mediante línea de comandos

Desde el directorio \x64\XenDesktop Setup en los medios de instalación, ejecute el comando **XenDesktopServerSetup.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 Instalación mediante línea de comandos.

Por ejemplo, el siguiente comando elimina Studio.

```
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Eliminación de un VDA mediante 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 Instalación mediante línea de comandos.

Por ejemplo, el siguiente comando elimina el VDA y Citrix Receiver.

```
\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall
```

En Active Directory, para quitar agentes VDA mediante un script, consulte Instalación o eliminación de agentes Virtual Desktop Agent mediante scripts.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Actualización y migración

Dec 05, 2017

Actualizar

Las actualizaciones cambian las implementaciones aplicando las versiones más actualizadas de los componentes, sin necesidad de instalar nuevas máquinas o nuevos sitios; este proceso se conoce como actualización en contexto. Puede actualizar a la versión actual desde:

- XenDesktop 5.6*
- XenDesktop 7.0
- XenDesktop 7.1
- XenApp/XenDesktop 7.5
- XenApp/XenDesktop 7.6
- XenApp/XenDesktop 7.6 LTSR
- XenApp/XenDesktop 7.7
- XenApp/XenDesktop 7.8
- XenApp/XenDesktop 7.9
- XenApp/XenDesktop 7.11
- XenApp/XenDesktop 7.12
- XenApp/XenDesktop 7.13
- XenApp/XenDesktop 7.14
- XenApp/XenDesktop 7.15 LTSR

También puede actualizar un servidor de trabajo de XenApp 6.5 a un VDA actual para SO de servidor Windows. Esta es una actividad complementaria a la migración de XenApp 6.5. Consulte Actualización de un servidor de trabajo de XenApp 6.5 a un nuevo VDA para SO de servidor Windows
.

Para actualizar:

1. Ejecute el instalador en las máquinas donde están instalados los componentes principales y los VDA. 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.

* Para actualizar desde XenDesktop 5.6, actualice a la versión 7.6 LTSR (con la Cumulative Update más reciente) y, a continuación, actualice a 7.15 LTSR (con la Cumulative Update más reciente).

Para obtener más información, consulte Actualizar una implementación.

Para obtener información acerca de la instalación de revisiones hotfix de Controller, consulte CTX201988.

Migrar

La migración mueve los datos de una implementación a la versión más reciente. Puede migrar una implementación de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Sugerencia: Para obtener información sobre los cambios de arquitectura, componentes y características que se han introducido en las versiones 7.x, consulte el artículo Cambios en 7.x.

Para migrar desde XenApp 6.5:

1. Instale los componentes principales y cree un nuevo sitio de XenApp.
2. Desde el Controller de XenApp 6.5, use los cmdlets de PowerShell para exportar los datos de la comunidad y las directivas a archivos XML. Puede editar el contenido del archivo XML para ajustar la información que se va a importar.
3. Desde el nuevo sitio, use los cmdlets de PowerShell y los archivos XML para importar datos de directivas y aplicaciones en el sitio nuevo.
4. Realice las tareas posteriores a la migración en el nuevo sitio.

Para obtener más información, consulte Migrar XenApp 6.x.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cambios en 7.x

Jan 03, 2018

La arquitectura, la terminología y las características de XenApp y XenDesktop han cambiado a partir de las versiones 7.x. Si solo conoce las versiones anteriores (a 7.x), en este artículo se le explicarán los cambios.

> **Sugerencia:** Una vez haya cambiado a la versión 7.x, los cambios en las versiones posteriores se enumerarán en Novedades.

A menos que se indique específicamente, *7.x* hace referencia a la versión 7.5 o posterior de XenApp, así como a la versión 7 o posterior de XenDesktop.

En este artículo, se ofrece una visión general.Para obtener información detallada sobre cómo cambiar desde versiones anteriores a 7.x a la versión más reciente, consulte Actualización a XenApp 7.

Diferencias de elementos entre XenApp 6 y la versión actual de XenApp

Aunque no son equivalentes exactos, la siguiente tabla ayuda a hacer una correspondencia entre los elementos funcionales de XenApp 6.5 (con sus versiones anteriores) y los elementos funcionales de XenApp y XenDesktop a partir de 7.x. A continuación, dispone de descripciones de las diferencias que existen entre cada arquitectura.

En vez de esto en XenApp ≤ 6.5:	Piense en esto en XenApp y XenDesktop ≥ 7.x:
Arquitectura IMA (Independent Management Architecture)	Arquitectura FMA (FlexCast Management Architecture)
Comunidad	Sitio
Grupo de trabajo	Catálogo de máquinas Grupo de entrega
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, 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 XenApp 7.x y XenDesktop 7.x, el sitio es el elemento de nivel superior. Los sitios ofrecen aplicaciones y escritorios a grupos de usuarios. FMA requiere que usted se encuentre en un dominio para implementar un sitio. Por ejemplo, para instalar los servidores, su cuenta debe tener privilegios de administrador local y ser un usuario de dominio de Active Directory.
- **Catálogos de máquinas y grupos de entrega**. Las máquinas que alojaban aplicaciones en XenApp 6.5 y versiones anteriores pertenecían a grupos de trabajo para una administración eficaz de las aplicaciones y del software de servidor. Los administradores podían administrar todas las máquinas de un grupo de trabajo como una sola unidad con el objetivo de mejorar la administración de la aplicación y el equilibrio de carga. Las carpetas se utilizaban para organizar aplicaciones y máquinas. En XenApp 7.x y XenDesktop 7.x, 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 XenApp 7.x y XenDesktop 7.x, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

solicitudes de conexión de los usuarios y de la comunicación con los hipervisores. En XenApp 7.x y XenDesktop 7.x, 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 XenApp 7.x y XenDesktop 7.x, la función de zonas de 7.x permite ayudar 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 XenApp 7.x y XenDesktop 7.x, 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**. XenApp 7.x y XenDesktop 7.x no usan 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 mediciones predeterminadas para determinar la carga de una máquina. Las conexiones de usuarios se podían asociar a máquinas con menos carga. En XenApp 7.x y XenDesktop 7.x, se utilizan directivas de administración de carga para equilibrar la carga entre las máquinas.
- **Administración delegada**. En XenApp 6.5 y versiones anteriores, se creaban administradores personalizados y se les asignaban permisos basados en carpetas y objetos. En XenApp 7.x y XenDesktop 7.x, 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 anteriores:	**Use esto a partir de XenApp y XenDesktop 7.x:**
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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 XenApp y XenDesktop 7.x, 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.
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". Como alternativa a la Caché de host local, la característica Concesión de conexiones permite a los usuarios conectarse varias veces a los últimos escritorios y aplicaciones que hayan utilizado, incluso cuando la base de datos del sitio no esté disponible. Consulte Concesión de conexiones.
Distribución de aplicaciones por streaming	App-V de Citrix ofrece aplicaciones distribuidas por streaming que se administran mediante Studio.
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 de características y respaldo a ellas

Las siguientes características ya no se ofrecen, ya no se respaldan o han cambiado significativamente a partir de XenApp o XenDesktop 7.x.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cifrado Secure ICA por debajo de 128 bits. En versiones anteriores a 7.x, Secure ICA podía cifrar conexiones de cliente para el cifrado básico de 40, 56 y 128 bits. Con las versiones 7.x, el cifrado Secure ICA solo está disponible para el cifrado de 128 bits.

Impresión antigua. Las funciones de impresión siguientes ya no se admiten en las versiones 7.x:

- Compatibilidad con versiones anteriores de los clientes de DOS e impresoras de 16 bits.
- Compatibilidad para impresoras conectadas a los sistemas operativos de Windows 95 y Windows NT, incluidas las propiedades de impresora extendidas y mejoradas y Win32FavorRetainedSetting.
- Capacidad para habilitar o inhabilitar impresoras conservadas y restauradas automáticamente.
- DefaultPrnFlag, un parámetro de Registro para servidores que se utiliza para habilitar o inhabilitar impresoras conservadas y restauradas automáticamente, almacenadas en perfiles de usuario del servidor.

NOTA: Se admiten los nombres de las impresoras del cliente heredadas.

Secure Gateway. En versiones anteriores a 7.x, Secure Gateway era una opción para proteger las conexiones entre el servidor y los dispositivos de usuario. NetScaler 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 v1. 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 del 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. Puede encontrarla en el sitio Web de descargas de Citrix: http://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 habilitar la conexión directa desde dispositivos de usuario (con el archivo ICA) a una máquina específica. En las versiones 7.x, esta función está inhabilitada de forma predeterminada, pero puede habilitarse para su uso normal mediante un grupo local, o se puede usar en el modo de alta disponibilidad si el Controller deja de estar disponible.

Módulo de administración para System Center Operations Manager (SCOM) 2007. El módulo de administración, que

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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. El nuevo flujo de trabajo simplificado de instalación y configuración en las versiones 7.x, 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 7.x.

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 profundidad de color para el grupo de entrega se puede configurar mediante los cmdlets de PowerShell Set-BrokerDesktopGroup o New-BrokerDesktopGroup.

Iniciar escritorio con optimización táctil. Este parámetro se ha inhabilitado y no está disponible para máquinas Windows 10 y Windows Server 2016. Para obtener más información, consulte Configuración de directiva de Experiencia móvil.

Funciones no incluidas en Citrix Receiver o que tienen diferentes valores predeterminados

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 de XenDesktop y XenApp, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 admiten el códec de audio PCM.

Respaldo para Microsoft ActiveSync.

Respaldo de proxy para versiones anteriores. Esto 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 Citrix Receiver correspondiente a su versión.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Actualización de una implementación

Feb 22, 2018

En este artículo:

- Introducción
- Secuencia de actualización
- Las versiones de componentes de producto que se pueden actualizar
- Preparación y limitaciones
- Consideraciones sobre entornos mixtos
- Agentes VDA en máquinas con Windows XP o Windows Vista
- Agentes VDA en máquinas con Windows 8.x o Windows 7
- Asistencia para los VDA mixtos
- Procedimiento de actualización
- Actualizar las bases de datos y el sitio

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 Actualización para ver una lista de las versiones que se pueden actualizar.

También puede usar el programa de instalación actual de XenApp para actualizar un servidor de trabajo de XenApp 6.5 al VDA actual para SO de servidor Windows. Esta es una actividad complementaria a la migración de XenApp 6.5. Consulte Actualización de un servidor de trabajo de XenApp 6.5 a un nuevo VDA para SO de servidor Windows.

Para iniciar una actualización, ejecute el programa de instalación desde la nueva versión para actualizar los VDA y los componentes principales previamente instalados (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server). A continuación, actualice las bases de datos y el sitio.

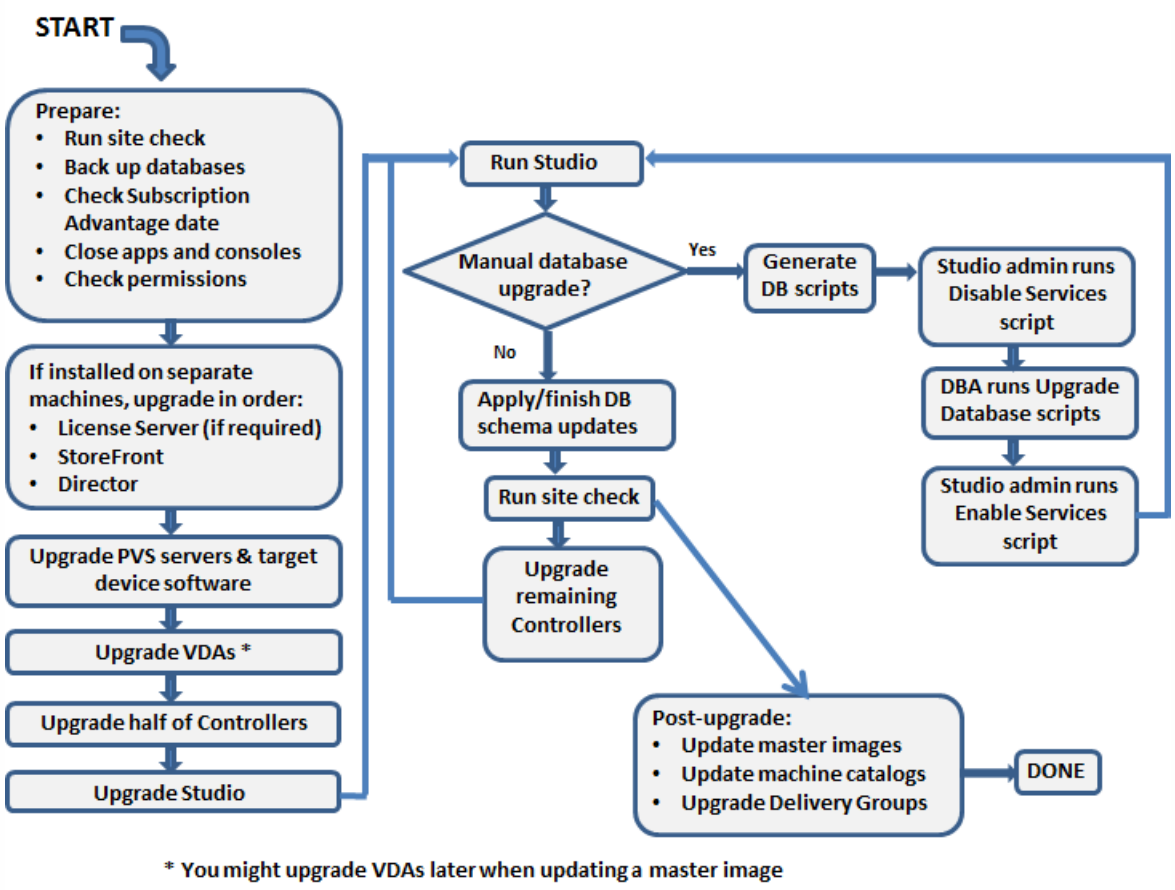
Consulte toda la información contenida en este artículo antes de comenzar la actualización.

(Si actualiza a 7.16 o una versión posterior, consulte las instrucciones indicadas en Actualizar una implementación.)

Secuencia de actualización

El diagrama siguiente resume la secuencia de actualización. Se ofrece información detallada más adelante, en la sección Procedimiento de actualización. Por ejemplo, si tiene más de un componente principal instalado en un servidor, ejecutar el instalador en esa máquina actualizará 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Las versiones de componentes de producto que se pueden actualizar

Con el instalador de producto, puede actualizar:

- StoreFront, Studio y Citrix License Server
- Delivery Controller 5.6 o versiones posteriores
- VDA 5.6 o versiones posteriores
  - A diferencia de las versiones anteriores de VDA, debe usar el programa de instalación para actualizar los VDA; no puede usar archivos MSI.
  - Si el programa de instalación detecta Receiver para Windows (Receiver.exe) en la máquina, se actualiza a la versión de Receiver que se incluye en los medios de instalación del producto.
  - De VDA 5.6 a VDA 7.8: Si el instalador detecta Receiver para Windows Enterprise (CitrixReceiverEnterprise.exe) en la máquina, se actualiza a Receiver para Windows Enterprise 3.4.
- Director 1 o versiones posteriores
- Base de datos. Esta acción de Studio actualiza el esquema y migra los datos de la base de datos del sitio (además de las bases de datos de registros de configuración y de supervisión, si se está llevando a cabo una actualización desde una versión anterior a 7.x).
- Personal vDisk

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: Para actualizar desde XenDesktop 5.6, actualice a la versión 7.6 LTSR (con la Cumulative Update más reciente) y, a continuación, actualice a esta versión.

Con la ayuda de instrucciones procedentes de la documentación del producto o de la función, actualice lo siguiente, si fuera necesario:

- Provisioning Services (para XenApp 7.x y XenDesktop 7.x, Citrix recomienda usar la última versión publicada; la versión mínima respaldada es Provisioning Services 7.0).
  - Actualice el servidor de Provisioning Services mediante la actualización gradual del servidor, y los clientes mediante el sistema de versiones de disco virtual (vDisk).
  - Provisioning Services 7.x no admite la creación de nuevos escritorios con versiones de XenDesktop 5. Por lo tanto, aunque los escritorios existentes seguirán funcionando, no podrá utilizar Provisioning Services 7.x para crear nuevos escritorios hasta que actualice XenDesktop. Por lo tanto, si quiere un entorno mixto de sitios de XenDesktop 5.6 y 7.x, no actualice Provisioning Services a la versión 7.
- Versión del hipervisor del host.
- StoreFront.
- Profile Management.

Limitaciones

Las actualizaciones tienen los límites siguientes:

Instalación selectiva de componentes

Si instala o actualiza 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 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.

Versión de XenApp anterior a 7.5

No puede actualizar desde una versión de XenApp anterior a 7.5. Puede migrar desde XenApp 6.x; consulte Migración de XenApp 6.x.

Aunque no pueda actualizar una comunidad de XenApp 6.5, puede reemplazar el software de XenApp 6.5 en un servidor Windows Server 2008 R2 por un VDA actualizado para SO de servidor. Consulte Actualización de un servidor de trabajo XenApp 6.5 a un nuevo VDA.

Versión de XenDesktop anterior a 5.6

No puede actualizar desde una versión de XenDesktop anterior a 5.6.

XenDesktop Express Edition

No puede actualizar XenDesktop Express Edition. Obtenga e instale una licencia para una edición respaldada actualmente y, a continuación, realice la actualización.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Versiones Technology Preview o Early Release

No puede actualizar desde una versión Technology Preview o Early Release de XenApp o XenDesktop.

Windows XP o Vista

Si tiene agentes VDA instalados en máquinas con Windows XP o Windows Vista, consulte Agentes VDA en máquinas con Windows XP o Windows Vista.

Selección del producto

Cuando actualice desde una versión anterior a 7.x, no seleccione ni especifique el producto (XenApp o XenDesktop), 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.

Preparación

Antes de comenzar una actualización:

Decida qué interfaz e instalador utilizará

Puede usar el instalador de producto completo que se proporciona en el archivo ISO de XenApp o XenDesktop para actualizar los componentes principales. 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. (Nota: 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 programa de instalación de VDA de producto completo o el programa de instalación VDAWorkstationSetup.exe para actualizar el VDA, los componentes que se hayan excluido en su momento pueden instalarse esta vez, a menos que los vuelva a omitir o excluir expresamente de la actualización.

Por ejemplo, si ha instalado VDA 7.13 mediante VDAWorkstationCoreSetup.exe y, a continuación, ha usado el programa de instalación de producto completo para actualizar ese VDA a la versión 7.14, los componentes que se excluyeron de la instalación original (por ejemplo, Profile Management o Personal vDisk) pueden instalarse durante la actualización, si acepta la configuración predeterminada o no usa la opción /exclude en la línea de comandos.

Compruebe el estado del sitio

Antes de iniciar la actualización, compruebe que el sitio es estable y está operativo. Si un sitio tiene problemas, la actualización no los solucionará, y puede dejar el sitio en un estado muy complejo del que puede ser difícil recuperarlo. Para probar el sitio, seleccione la entrada del **sitio** en el panel de navegación de Studio. En la parte de la configuración del sitio en el panel central, haga clic en **Probar sitio**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Realice una copia de seguridad de las 3 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.

Si lo prefiere, 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.

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 01.08.2017. (Esta fecha se aplica a la versión 7.15 LTSR, no a las actualizaciones acumulativas (CU) siguientes.)

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.)

Importante: Antes de comenzar una actualización, detenga e inhabilite los servicios de agentes de supervisión externos que haya.

Compruebe que dispone de los permisos correctos

Además de ser un usuario del dominio, usted debe ser un administrador local en las máquinas donde quiere actualizar los componentes de producto.

La base de datos del sitio y el sitio pueden actualizarse automáticamente 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 el artículo Bases de datos. Si el usuario de Studio no tiene los permisos necesarios, se generarán scripts al iniciar una actualización manual de la base de datos. El usuario de Studio ejecuta algunos scripts desde Studio, mientras que el administrador de la base de datos ejecuta otros scripts mediante una herramienta como SQL Server Management Studio.

Consideraciones sobre entornos mixtos

Si el entorno contiene sitios o comunidades con diferentes versiones de producto (un entorno mixto), Citrix recomienda usar StoreFront para agrupar escritorios y aplicaciones de diferentes versiones de producto (por ejemplo, si tiene un sitio de XenDesktop 7.13 y un sitio de XenDesktop 7.14). 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 Provisioning Services para ambos, instale una nueva implementación de Provisioning Services para usarla con el sitio 7.x, o actualice la implementación actual de Provisioning Services, aunque entonces ya no podrá aprovisionar nuevas cargas de trabajo en el sitio de XenDesktop 5.6.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

- Los sitios con Controllers en la versión 5.x y con VDA en la versión 7.x deben permanecer en ese estado solo temporalmente. Preferiblemente, debe completar la actualización de todos los componentes tan pronto como sea posible.
- No actualice una versión autónoma de Studio hasta que esté listo para usar la nueva versión.

Agentes VDA en máquinas con Windows XP o Windows Vista

No se pueden actualizar los VDA instalados en máquinas con Windows XP o Windows Vista a una versión 7.x. Debe usar VDA 5.6 FP1 con algunas revisiones; consulte CTX140941 para obtener instrucciones. Aunque los VDA de versiones anteriores se pueden ejecutar en un sitio 7.x, no pueden utilizar muchas de sus funciones, incluidas:

- Funciones descritas en Studio que requieren una versión más reciente de VDA.
- Configuración de aplicaciones App-V desde Studio.
- Configuración de direcciones de StoreFront desde Studio.
- Respaldo automático para licencias KMS de Microsoft Windows al utilizar Machine Creation Services. Consulte CTX128580.
- Información en Director:
  - Duración de los inicios de sesión y eventos al finalizar la sesión que afectan la duración del inicio de sesión en las vistas Panel de mandos, Tendencias y Detalles del usuario.
  - Detalles desglosados sobre la duración de los inicios de sesión durante autenticaciones y conexiones HDX, además de detalles sobre la duración de la carga de perfil, la carga de directiva de grupo, el script de inicio de sesión y el establecimiento de inicios de sesión interactivos.
  - Varias categorías de porcentaje de errores de conexión y de máquina.
  - Administrador de actividades en las vistas Asistencia técnica y Detalles del usuario.

Citrix recomienda cambiar la imagen de máquinas con Windows XP y Windows Vista a una versión respaldada de SO y, a continuación, instalar en ellas la versión más reciente de VDA.

Agentes VDA en máquinas con Windows 8.x o Windows 7

Para actualizar agentes VDA instalados en máquinas con Windows 7 o Windows 8.x a Windows 10, Citrix recomienda primero cambiar la imagen de las máquinas Windows 7 o Windows 8.x a Windows 10 y, después, instalar el agente VDA para Windows 10 admitido. Si no se puede cambiar la imagen, desinstale el agente VDA antes de actualizar el sistema operativo; de lo contrario, el VDA entrará en un estado no compatible.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 indica la versión más reciente recomendada de VDA. Tenga en cuenta que deberá plantearse cambiarlo solamente si el catálogo de máquinas contiene máquinas con versiones anteriores de VDA. Sin embargo, no se recomienda mezclar versiones de VDA en un catálogo de máquinas.

Si se crea un catálogo de máquinas con el parámetro predeterminado recomendado de la versión de VDA, y alguna de las máquinas del catálogo tiene una versión anterior de VDA instalada, esas máquinas no podrán registrarse con 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, consulte Instalar mediante línea de comandos.

Paso 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 en ese servidor.

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.

Paso 2. Si utiliza Provisioning Services, actualice los servidores y los dispositivos de destino de Provisioning Services con la ayuda de las instrucciones proporcionadas en la documentación de Provisioning Services.

Paso 3. Ejecute el instalador de producto en las máquinas con agentes VDA. (Consulte el paso 12 si utiliza imágenes maestras y Machine Creation Services.)

Paso 4. Ejecute el instalador de producto en la mitad de los Controllers. (Esta acción 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 con 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.

Paso 5. Si Studio está instalado en otra máquina que no sea una de las actualizadas en el paso anterior, ejecute el

© 1999-2017 Citrix Systems, Inc. All rights reserved.

instalador en la máquina donde está instalado Studio.

Paso 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.

Paso 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**.

Paso 8. Una vez completada la actualización y la confirmación en los Controllers restantes, 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.

Paso 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.

Paso 10. Una vez que seleccione **Finalizar** una vez completado 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.

Paso 11. Después de actualizar los componentes, la base de datos y el sitio, pruebe 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 ejecutaron automáticamente después de actualizar la base de datos, pero no 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.
>
> 1. Habilite el servicio SQL Server Browser (si fuera necesario) e inícielo.
> 2. Reinicie el servicio SQL Server (SQLEXPRESS).

Paso 12. Si utiliza Machine Creation Services y quiere actualizar los VDA: después de actualizar y probar la implementación, actualice los VDA que se usan 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.A continuación, actualice los catálogos de máquinas que usan esas imágenes maestras, y actualice los grupos de entrega que usan esos catálogos.

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: Compruebe la sección Preparación indicada 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.

Importante: Citrix recomienda encarecidamente que realice una copia de seguridad de la base de datos antes de actualizarla. Consulte CTX135207.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 completada la actualización de la base de datos y los productos y los servicios están habilitados, 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.

Actualización automática de la base de datos y del 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.

Actualización manual de la base de datos y del sitio:

Paso 1. Inicie el recién actualizado Studio. Después de optar por la actualización manual del sitio, 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.

Paso 2. Ejecute los siguientes scripts en el orden indicado.

Script	Descripción
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.
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.

Paso 3. Después de completar las tareas de la lista de verificación, haga clic en **Finalizar actualización**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Actualización de un servidor de trabajo XenApp 6.5 a un nuevo VDA

Dec 05, 2017

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 y, a continuación, instale un nuevo VDA para SO de servidor.

NOTA: 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 Eliminación de funciones 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. Instale un VDA para SO de servidor mediante un instalador suministrado con esta versión. Consulte Instalación de agentes VDA o Instalación mediante línea de comandos.

Después de instalar el nuevo VDA, desde Studio en el nuevo sitio de XenApp, cree catálogos de máquinas (o modifique los existentes) para los servidores de trabajo actualizados.

Solución de problemas

Síntomas: 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 Windows.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Migración de XenApp 6.x

Dec 05, 2017

Nota: No se puede utilizar el producto de migración Citrix Smart Migrate con esta versión de XenApp y XenDesktop. Sin embargo, la herramienta de migración está disponible.

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.

Aquí tiene un vídeo resumen de la herramienta de migración.

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:
    1. Importe los módulos de exportación de PowerShell.
    2. 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:
    1. Importe los módulos de importación de PowerShell.
    2. 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 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.

Novedades de esta versión

Esta versión publicada en diciembre de 2014 (versión 20141125) contiene las actualizaciones siguientes:

- Si encuentra problemas al usar la herramienta de migración en una comunidad de XenApp 6.x, notifíquelos en el foro de asistencia http://discussions.citrix.com/forum/1411-xenapp-7x/, de forma que Citrix pueda investigarlos y mejorar la herramienta.
- Nuevo paquete. El archivo XAMigration.zip contiene ahora dos paquetes separados independientes: ReadIMA.zip e ImportFMA.zip. Para exportar desde un servidor XenApp 6.x, solo necesita ReadIMA.zip. Para importar a un servidor XenApp 7.6, solo necesita ImportFMA.zip.
- El cmdlet Export-XAFarm admite un nuevo parámetro (EmbedIconData), que elimina la necesidad de copiar los datos de iconos en archivos separados.
- El cmdlet Import-XAFarm admite tres nuevos parámetros:
    - MatchServer. Importa aplicaciones desde servidores cuyos nombres coinciden con una determinada expresión
    - NotMatchServer. Importa aplicaciones desde servidores cuyos nombres no coinciden con una determinada expresión
    - IncludeDisabledApps: importa aplicaciones inhabilitadas
- Las aplicaciones de preinicio no se importan.
- El cmdlet Export-Policy funciona con XenDesktop 7.x.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paquete de herramienta de migración

La herramienta de migración está disponible en el sitio de descargas de Citrix 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.
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Se crea un grupo de entrega durante la importación. Consulte Uso avanzado para obtener más información sobre cómo usar los parámetros para filtrar lo que se importa.
- Solo se importan las configuraciones de directiva de Citrix creadas con la consola de administración de AppCenter; las configuraciones de directiva de Citrix creadas con objetos de directiva de grupo (GPO) de Windows no se importan.
- Los scripts de migración están diseñados para las migraciones desde XenApp 6.x a XenApp 7.6 únicamente.
- Studio no 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.

Captura de registros y control de 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; de lo contrario, se coloca en la carpeta de ejecución del script actual. El nombre predeterminado de los registros es "XFarmYYYYMMDDHHmmSS-xxxxxx"; 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.

Importante: No olvide consultar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (Administración > Creación de almacenes).
- 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 <string> 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 mediante la herramienta Citrix IMA Helper (CTX133983): en la ficha IMA Datastore, ejecute Master Check (y, 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 scripts falla.
- Puede ejecutar los cmdlets de exportación en una comunidad de servidores en ejecución, con conexiones de usuario activas, ya que los scripts de exportación solo leen los datos estáticos de directivas y configuración de la comunidad.

Para importar en el servidor XenApp 7.6:

- Puede importar datos a las implementaciones de XenApp 7.6 (y versiones posteriores admitidas). Debe instalar un Controller de XenApp 7.6 y Studio, y crear un sitio, antes de importar los datos exportados desde la comunidad XenApp 6.x. Aunque los VDA no son necesarios para importar configuraciones, permiten que los tipos de archivo de las aplicaciones estén disponibles.
- Para ejecutar los cmdlets de importación de XenApp, debe ser un administrador XenApp con permisos para leer y crear objetos. Un administrador total tiene estos permisos. También hay que tener suficientes permisos de Windows para ejecutar scripts de PowerShell; los procedimientos paso a paso siguientes contienen instrucciones.
- No debe haber otras conexiones de usuario activas durante una importación. Los scripts de importación crean muchos objetos nuevos y pueden producirse interrupciones si hay otros usuarios cambiando la configuración al mismo tiempo.

Recuerde que puede exportar datos y, a continuación, usar el parámetro -Preview con los cmdlets de importación para tener una vista previa de lo que sucedería durante una importación real, sin importar nada todavía. Los registros indicarán exactamente lo que sucedería durante la importación; si se producen errores, resuélvalos antes de iniciar la importación real.

Exportar datos, paso a paso

Aquí hay un vídeo donde puede ver un proceso de exportación paso a paso.

Complete los siguientes pasos para exportar datos desde un Controller de XenApp 6.x a archivos XML.

1. Descargue el paquete de la herramienta de migración XAMigration.zip desde el sitio de descargas de Citrix. Para mayor comodidad, colóquelo en un recurso compartido de archivos en la red, al que tengan acceso tanto la comunidad XenApp 6.x como el sitio XenApp 7.6. Descomprima XAMigration.zip en el recurso compartido de archivos en la red. Se descomprimirá en otros dos archivos zip: ReadIMA.zip e ImportFMA.zip.
2. Inicie la sesión en el Controller de XenApp 6.x como un administrador de XenApp con, al menos, permiso de solo lectura y permisos de Windows para ejecutar scripts de PowerShell.
3. Copie ReadIMA.zip desde el recurso compartido de archivos de la red al Controller de XenApp 6.x. Descomprima y extraiga el contenido de ReadIMA.zip en el Controller en una carpeta (por ejemplo: C:\XAMigration).
4. Abra una consola de PowerShell y establezca como directorio actual el directorio donde se encuentran los scripts. Por ejemplo:
   cd C:\XAMigration
5. Ejecute Get-ExecutionPolicy para consultar la directiva de ejecución de scripts.
6. Establezca la directiva de ejecución de scripts como, al menos, RemoteSigned para permitir que los scripts se ejecuten. Por ejemplo:
   Set-ExecutionPolicy RemoteSigned
7. Importe los archivos de definición de módulos ExportPolicy.psd1 y ExportXAFarm.psd1:
   Import-Module .\ExportPolicy.psd1

   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 directivas, ejecute el cmdlet Export-Policy.

Parámetro	Descripción

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
XmlOutputFile "<string>.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 "<string>"	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 Captura de registros y control de 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 #yyyyMMdd-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"
```

9. Para exportar los datos de la comunidad, ejecute el cmdlet Export-XAFarm; deberá especificar un archivo de registros y un archivo XML.

Parámetro	Descripción
-XmlOutputFile "<string>.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 "<string>"	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 Captura de registros y control de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
	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 #yyyyMMdd-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 para obtener información acerca del uso. Valor predeterminado: False; se exporta la información sobre administradores
-IgnoreApps	No exportar información de aplicaciones. Consulte Uso avanzado para obtener información acerca del uso. 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 Nota: La finalidad del conmutador -IgnoreOthers es permitir continuar una exportación aunque haya un error, si el error no afecta a los datos en sí utilizados para el proceso de importación o exportación.
-AppLimit <integer>	Cantidad de aplicaciones para exportar. Consulte Uso avanzado para obtener información acerca del uso. 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. Para obtener información más detallada, consulte Requisitos, preparación y procedimientos recomendados.
-SkipApps <integer>	Cantidad de aplicaciones para omitir. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: No se omite ninguna aplicación

Ejemplo: El cmdlet siguiente exporta la información sobre la comunidad al archivo XML denominado MyFarm.xml. La operación genera registros que se guardan en el archivo MyFarm.log. Se crea una carpeta denominada "MyFarm-icons" para almacenar los archivos de datos de iconos de las aplicaciones; esta carpeta está en la misma ubicación que MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML" -LogFile ".\MyFarm.Log"
```

Una vez ejecutados los scripts de exportación, los archivos XML especificados en las líneas de comandos contienen los datos de la comunidad XenApp y las directivas. Los archivos de iconos de aplicaciones contienen archivos de datos de icono, y el archivo de registros indica qué ocurrió durante la exportación.

Importar datos, paso a paso

Aquí hay un vídeo donde puede ver un proceso de importación paso a paso.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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

   Import-Module .\ImportXAFarm.psd1

   Tenga en cuenta:
   - 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 directivas, ejecute el cmdlet Import-Policy; deberá especificar el archivo XML que contiene los datos exportados de las directivas.

Parámetro	Descripción
-XmlInputFile "<string>.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 "<string>"	Nombre del archivo XSD. Los scripts de importación usan este archivo para validar la sintaxis del archivo XML de entrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: PolicyData.XSD
-LogFile "<string>"	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 Captura de registros y control de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-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 #yyyyMMdd-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"
```

9. Para importar aplicaciones, ejecute el cmdlet 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 "<string>.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 "<string>"	Nombre del archivo XSD. Los scripts de importación usan este archivo para validar la sintaxis del archivo XML de entrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: XAFarmData.XSD
-LogFile "<string>"	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 Captura de registros y control de 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 #yyyyMMdd-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

© 1999-2017 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 "<string>"	Nombre del grupo de entrega para todas las aplicaciones importadas. Consulte Uso avanzado para obtener información acerca del uso. Default: "<xenapp-farm-name> - Delivery Group"
-MatchFolder "<string>"	Importar solo las aplicaciones que se encuentran en carpetas cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-NotMatchFolder "<string>"	Importar solo las aplicaciones que se encuentran en carpetas cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-MatchServer "<string>"	Importar solo las aplicaciones que se encuentran en servidores cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso.
-NotMatchServer "<string>"	Importar solo las aplicaciones que se encuentran en servidores cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-MatchWorkerGroup "<string>"	Importar solo las aplicaciones publicadas para grupos de trabajo cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-NotMatchWorkerGroup "<string>"	Importar solo las aplicaciones publicadas para grupos de trabajo cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-MatchAccount "<string>"	Importar solo las aplicaciones publicadas para cuentas de usuarios cuyos nombres coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-NotMatchAccount "<string>"	Importar solo las aplicaciones publicadas para cuentas de usuarios cuyos nombres no coinciden con la cadena suministrada. Consulte Uso avanzado para obtener información acerca del uso. Valor predeterminado: no se realiza una coincidencia
-IncludeStreamedApps	Importar aplicaciones del tipo: "StreamedToClientOrServerInstalled". (No se importa ninguna otra aplicación distribuida por streaming.) Valor predeterminado: las aplicaciones distribuidas por streaming no se importan

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-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"
```

10. Una vez completada correctamente la migración, hay que realizar las tareas posteriores a la migración.

Tareas posteriores a la migración

Una vez importadas las directivas y la configuración de la comunidad de XenApp 6.x en un sitio de XenApp 7.6, siga las siguientes instrucciones para asegurarse de que los datos se han importado correctamente.

- **Directivas y configuraciones de directivas**
  La importación de directivas es fundamentalmente una operación de copia, con la excepción de las directivas y configuraciones que 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 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.

© 1999-2017 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.
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:
     - Compruebe visualmente que se conservaron sus propiedades básicas durante la importación. Use la información de la sección 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 la sección “Registro y control de errores”, si se quiere usar una cobertura 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

una referencia completa de toda la actividad de importación y exportación.

Gracias a las marcas de hora incluidas en los archivos de registros se pueden diagnosticar ciertos problemas. Por ejemplo, si una exportación o importación tardó mucho tiempo en ejecutarse, se puede averiguar si la causa fue una conexión de base de datos defectuosa o algún problema al resolver las cuentas de usuario.

Los comandos grabados en los archivos de registros también indican cómo se leen o se crean algunos objetos. Por ejemplo, para crear un grupo de entrega, se ejecutan varios comandos no solo para crear el grupo de entrega propiamente dicho, sino también otros objetos tales como reglas de directivas de acceso que permiten asignar objetos de aplicación al grupo de entrega.

El archivo de registros se puede usar también para diagnosticar un fallo de importación o exportación. Por lo general, las últimas línea 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 Agents) 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 directivas a un archivo XML. Del mismo modo, Export-XAFarm exporta todos los datos de la 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 para exportar.
  - SkipApps: Especifica la cantidad de aplicaciones para 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 desea exportar solo las primeras 200 aplicaciones; para ello, especifica ese valor en el parámetro AppLimit.
  Export-XAFarm -XmlOutputFile "Apps1-200.xml"
  -AppLimit "200"
  La siguiente vez que ejecuta Export-XAFarm, desea exportar las 100 aplicaciones siguientes; para ello, hay que usar 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 ciertos 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; esto 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

1. Use el parámetro DeliveryGroupName con el cmdlet Import-XAFarm. El script crea el grupo de entrega especificado si éste no existe.
2. Utilice los siguientes parámetros con expresiones regulares para filtrar las aplicaciones que se importan en el grupo de entrega, en función de carpetas, grupos de trabajo, cuentas de usuario y/o nombres de servidores. Se recomienda poner la expresión regular entre comillas simples o dobles. Para obtener más información acerca de las expresiones regulares, consulte http://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" en 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" en 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" en 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" en 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 el los archivos XSD (o crear sus propios archivos XSD) para almacenar datos adicionales o datos en diferentes formatos en los archivos XML. Puede especificar un archivo XSD no predeterminado con cada uno de los cmdlets de importación.
  Nota: 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.

Solución de problemas

- Si usa PowerShell 2.0 y agregó el complemento Citrix Group Policy PowerShell Provider o el complemento Citrix Common Commands mediante el cmdlet Add-PSSnapIn, es posible 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 directamente el nombre completo del módulo de scripts de PowerShell en la ventana de la consola de PowerShell (por ejemplo, Import-Module.\ExportPolicy.psd1).
- Si recibe un error de permisos al ejecutar una exportación o importación, asegúrese de que usted es un administrador de XenApp con permisos para leer objetos (para poder exportar), o para leer y crear objetos (para poder importar). También debe tener suficientes permisos de Windows para ejecutar scripts de PowerShell.
- Si la exportación falla, compruebe si la comunidad de XenApp 6.x se encuentra en un estado correcto, ejecutando las utilidades DSMAINT y DSCHECK en el servidor de Controller de XenApp 6.x.
- Si ejecuta una vista previa de la importación y luego ejecuta los cmdlets de importación de nuevo para una migración real, pero descubre que no se ha importado nada, compruebe si quitó el parámetro Preview de los cmdlets de importación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 admiten estas configuraciones han sido reemplazadas por otras tecnologías y componentes nuevos, o bien 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)
- Filtrado de direcciones de adaptador de IP virtual, Lista de programas para compatibilidad con IP virtual, Compatibilidad mejorada de IP virtual, Lista de programas para filtrado de direcciones de adaptador de IP virtual
- Nombre de la carga de trabajo
- Edición del producto XenApp, Modelo del producto XenApp
- Puerto de XML Service

* Reemplazada por Asistencia remota de Windows

Configuraciones de directiva de usuario que no se importan

- Conectar automáticamente puertos COM del cliente, Conectar automáticamente puertos LPT del cliente
- Redirección de puertos COM del cliente, Redirección de puertos LPT del cliente
- Nombres de impresora del cliente
- Límite de sesiones simultáneas
- Entradas de conexiones de remedo*
- Intervalo de temporizador de desconexión de sesión persistente, Intervalo de temporizador de fin de sesión persistente
- Registrar intentos de remedo*
- Notificar al usuario sobre conexiones de remedo pendientes*
- Intervalo de temporizador de desconexión de sesión de preinicio, Intervalo de temporizador de fin de sesión de preinicio
- Importancia de la sesión
- Single Sign-On, Almacén central de Single Sign-On
- Usuarios que pueden remedar a otros usuarios, Usuarios que no pueden remedar a otros usuarios*

* Reemplazada por Asistencia remota de Windows

Tipos de aplicaciones que no se importan

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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Asignación de propiedades de aplicaciones

El script de importación de datos de la comunidad solo importa aplicaciones. Las siguientes propiedades de aplicación se importan sin cambios.

Propiedad de IMA	Propiedad de FMA
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel
Descripción	Descripción
DisplayName	PublishedName
Habilitado	Habilitado
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Nota: IMA y FMA tienen restricciones diferentes en cuanto a 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\"
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propiedad de FMA	Valor
UserFilterEnabled	No inicializada; el valor predeterminado es false
UUID	Solo lectura, asignado por el Controller
Visible	No inicializada; el valor predeterminado es true

Las siguientes propiedades de aplicación se migran parcialmente:

Propiedad de IMA	Comentarios
FileTypes	Solo se migran los tipos de archivos que ya existen en el nuevo sitio de XenApp. Aquellos tipos de archivo que no existan en el sitio nuevo se omiten. Los tipos de archivo se importan solo después de que se actualicen los tipos de archivo del sitio nuevo.
IconData	Se crean nuevos objetos de icono si los datos de icono se han proporcionado para las aplicaciones exportadas.
Cuentas	Las cuentas de usuario de una aplicación se dividen entre la lista de usuarios para el grupo de entrega y la aplicación. Los usuarios explícitos se usan para inicializar la lista de usuarios para la aplicación. Además, la cuenta "Usuarios de dominio" del dominio de las cuentas de usuario se agrega a la lista de usuarios para el grupo de entrega.

Las siguientes propiedades de XenApp 6.x no se importan:

Propiedad de IMA	Comentarios
ApplicationType	Omitido.
HideWhenDisabled	Omitido.
AccessSessionConditions	Reemplazada por las directivas de acceso de grupos de entrega.
AccessSessionConditionsEnabled	Reemplazada por las directivas de acceso de grupos de entrega.
ConnectionsThroughAccessGatewayAllowed	Reemplazada por las directivas de acceso de grupos de entrega.
OtherConnectionsAllowed	Reemplazada por las directivas de acceso de grupos de entrega.
AlternateProfiles	FMA no 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propiedad de IMA	Comentarios
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.
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Seguridad

Dec 05, 2017

XenApp y XenDesktop ofrecen una solución, de diseño seguro, que permite ajustar el entorno a las necesidades de seguridad del mismo.

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, XenApp y XenDesktop gestiona de manera segura los datos confidenciales y de propiedad intelectual, porque los separa de los dispositivos de punto final y los guarda 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 XenDesktop y XenApp 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.

XenApp y XenDesktop también simplifican las auditorías y el cumplimiento de la normativa porque los investigadores pueden usar una traza de auditoría centralizada para determinar quién tuvo acceso 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 el acceso a XenDesktop y XenApp con detalle. Lo que da flexibilidad a la organización para conceder a ciertos administradores un acceso completo a ciertas tareas, operaciones y ámbitos, mientras que otros administradores tienen acceso limitado.

Con XenApp y XenDesktop, 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 XenApp o XenDesktop 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.

XenApp y XenDesktop también admiten la autenticación de varios factores para Windows o para una aplicación específica. La autenticación de varios factores también se puede usar para administrar todos los recursos entregados por XenApp y XenDesktop. Estos métodos incluyen:

- Tokens
- Tarjetas inteligentes
- RADIUS
- Kerberos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Biometría

XenDesktop puede 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.

Ciertas versiones de XenApp y XenDesktop están certificadas para el estándar de Common Criteria. Para obtener una lista de los estándares, vaya a http://www.commoncriteriaportal.org/cc/.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recomendaciones y consideraciones de seguridad

Apr 10, 2018

En este documento, se describen:

- Recomendaciones de seguridad general para el uso de esta versión y todas las diferencias relacionadas con la seguridad que existen entre esta versión y un entorno informático convencional
- Administrar cuentas de usuario
- Administrar privilegios de usuario
- Administrar derechos de inicio de sesión
- Configurar derechos de usuario
- Configurar parámetros de servicios
- Casos de implementación y sus implicaciones de seguridad
- Consideraciones de seguridad respecto a acceso con Remote PC

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. XenApp y XenDesktop 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 y 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 se han registrado oficialmente ante la Agencia de asignación de números de Internet (consulte 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.

Al planificar los privilegios de escritorio, tenga en cuenta que:

- 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 la hora local al utilizar los escritorios, consulte Cambiar parámetros básicos.
- 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.

Algunas aplicaciones requieren privilegios de escritorio, aunque estén destinadas a usuarios en lugar de administradores. Es posible que estos usuarios no sean tan conscientes de los riesgos de seguridad.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Trate estas aplicaciones como confidenciales, incluso aunque sus datos no sean confidenciales. Considere estos enfoques para reducir el riesgo de seguridad:

- Aplicar la autenticación de dos factores y desactivar cualquier mecanismo de inicio de sesión único (Single Sign-On) para la aplicación
- Aplicar directivas de acceso contextual
- Publicar la aplicación en un escritorio dedicado. Si la aplicación debe publicarse en un escritorio alojado compartido, no publique ninguna otra aplicación en ese escritorio alojado compartido
- Comprobar que los privilegios de escritorio solo se apliquen a ese escritorio, no a otros equipos
- Habilitar la Grabación de sesiones para la aplicación. También puede habilitar otras capacidades de captura de registros de seguridad en la aplicación y dentro de Windows en sí.
- Configurar XenApp y XenDesktop para limitar las funciones utilizadas con la aplicación (por ejemplo, portapapeles, impresora, unidad de cliente y redirección USB)
- Habilitar las funciones de seguridad de la aplicación. Puede limitarlas para que coincidan estrictamente con los requisitos de los usuarios, y nada más
- Configurar las características de seguridad de Windows para que coincidan estrictamente con los requisitos de los usuarios. Esta configuración será más sencilla si solamente se publica esa aplicación en el escritorio y ninguna otra; por ejemplo, se puede usar una configuración restrictiva de AppLocker. Controlar el acceso al sistema de archivos.
- Tener planeados los procedimientos en caso de tener que volver a configurar, actualizar o reemplazar la aplicación para que los privilegios de escritorio no sean necesarios en el futuro

Estos enfoques no eliminarán todos los riesgos de seguridad de las aplicaciones que requieren privilegios de 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 la 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).

Las directivas de seguridad de su organización pueden establecer explícitamente que se quite este derecho de inicio de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenApp y XenDesktop, 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.
- 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 XenApp o XenDesktop, 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 mediciones de XenApp o XenDesktop, almacena información histórica y proporciona una interfaz de consultas para la solución de problemas y herramientas para la generación de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Memoria caché del 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 proceso, Generar auditorías de seguridad y Reemplazar un símbolo (token) de nivel de proceso. No es necesario que cambie estos derechos de usuario. Delivery Controller no utiliza estos privilegios y están inhabilitados automáticamente.

Configurar parámetros de servicios

Excepto Citrix StoreFront Privileged Administration Service y Citrix Telemetry Service, los servicios Windows de Delivery Controller enumerados arriba en la sección Configurar derechos de usuario están configurados para iniciar sesión como la identidad NETWORK SERVICE. No modifique estos parámetros de servicio.

Citrix Storefront Privileged Administration está configurado para iniciar la sesión de sistema local (NT AUTHORITY\SYSTEM). Esto es necesario para las operaciones de StoreFront con Delivery Controller que no están normalmente disponibles 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de los casos de implementación

El entorno de usuario puede contener dispositivos de usuario que la empresa no administra y, por tanto, están bajo el control total del usuario, o bien, dispositivos de usuario que administra totalmente la empresa. En general, las consideraciones de seguridad para estos dos entornos son diferentes.

Dispositivos del usuario administrados

Los dispositivos de usuario administrados permanecen bajo un control administrativo; se encuentran bajo el control del usuario o de otra organización de su confianza. Es posible configurar y suministrar dispositivos del usuario directamente a usuarios. También es posible proporcionar terminales en los que se ejecute un solo escritorio en modo solo de pantalla completa. Es necesario respetar las recomendaciones de seguridad descritas anteriormente para todos los dispositivos de usuario administrados. La ventaja de esta versión es que presenta requisitos mínimos de software para un dispositivo del usuario.

Un dispositivo de usuario administrado puede configurarse para su uso solo en el modo de pantalla completa o en el modo de ventana:

- Modo solo de pantalla completa. Los usuarios inician sesión en la pantalla habitual de Iniciar sesión en Windows. A continuación, se utilizan las mismas credenciales de usuario para iniciar sesión automáticamente en esta versión.
- Los usuarios ven su escritorio en una ventana. Primero deben iniciar sesión en el dispositivo del usuario y luego en esta versión a través del sitio Web proporcionado con ella.

Dispositivos del usuario no administrados

Los dispositivos de usuario que no se encuentran bajo la administración de una organización fiable no pueden considerarse parte de un control administrativo. Por ejemplo, se puede permitir que los usuarios obtengan y configuren sus propios dispositivos, pero es posible que los usuarios no respeten las prácticas recomendadas de seguridad general descritas anteriormente. Esta versión presenta la ventaja de permitir la entrega de escritorios de forma segura a dispositivos del usuario no administrados. Aun así, estos dispositivos deben contar con una protección antivirus básica que anule los registradores de pulsaciones de teclas y los ataques de entrada similares.

Aspectos a tener en cuenta sobre el almacenamiento de datos

Al utilizar esta versión, es posible evitar que los usuarios almacenen datos en los dispositivos del usuario que se encuentren bajo su control físico. No obstante, es necesario tener en cuenta las implicaciones del almacenamiento de datos en los escritorios por parte de los usuarios. Almacenar datos en los escritorios no es una práctica recomendada para los usuarios; los datos deben conservarse en servidores de archivos, servidores de base de datos u otros repositorios donde se encuentren debidamente protegidos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

El entorno de escritorio puede estar compuesto por varios tipos de escritorios, como escritorios agrupados y dedicados. Los usuarios no deben almacenar nunca sus datos en escritorios compartidos entre los usuarios, como es el caso de los escritorios agrupados. Cuando los usuarios almacenan datos en escritorios dedicados, esos datos deben eliminarse si el escritorio posteriormente pasa a estar disponible para otros usuarios.

Entornos de versiones mixtas

En algunas actualizaciones, los entornos que contienen varias versiones son inevitables. Siga las prácticas recomendadas y minimice el tiempo de coexistencia para los componentes de Citrix de versiones distintas. En entornos de varias versiones, es posible que las directivas de seguridad, por ejemplo, no se cumplan uniformemente.

Nota: Esta es una situación habitual en caso de otros productos de software. Una versión anterior de Active Directory solo aplica parcialmente la directiva de grupo con 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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, 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. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

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.

- Eliminar a todos los usuarios asignados del VDA: $machine.AssociatedUserNames | %{ Remove-BrokerUser-Name $_ -Machine $machine
- Eliminar el VDA del grupo de entrega: $machine | Remove-BrokerMachine -DesktopGroup $desktopGroup

Reinicie el PC físico de la oficina.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

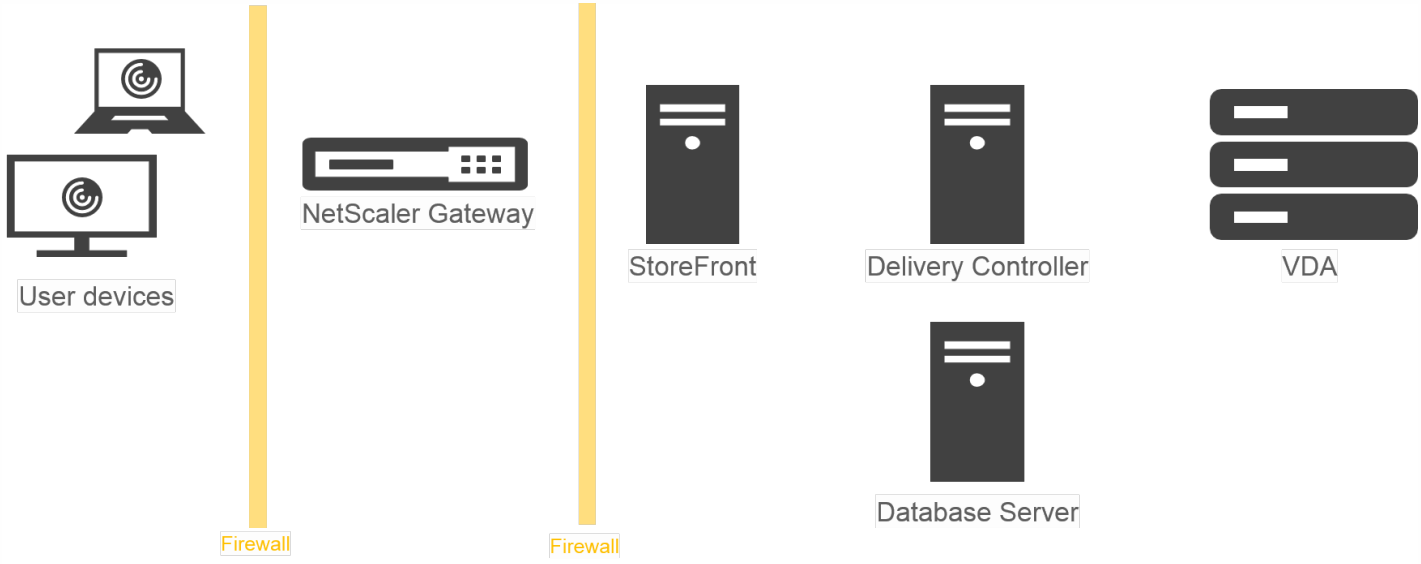
Integración de XenApp y XenDesktop con NetScaler Gateway

Dec 05, 2017

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 NetScaler Gateway y colocarlo delante de StoreFront.

> ## Nota
>
> Para conocer los pasos detallados de configuración para integrar XenApp y XenDesktop con NetScaler Gateway, consulte la documentación de StoreFront.

En el siguiente diagrama, se ofrece un ejemplo de una implementación simplificada de Citrix que incluye NetScaler Gateway. NetScaler Gateway se comunica con StoreFront para proteger las aplicaciones y los datos que entrega XenApp y XenDesktop. Los dispositivos de usuario ejecutan Citrix Receiver para crear una conexión segura y acceder a sus aplicaciones, escritorios y archivos.



Los usuarios inician sesiones y se autentican usando NetScaler Gateway. NetScaler Gateway está implementado y protegido en la zona desmilitarizada (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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administración delegada

Dec 05, 2017

El modelo de administración delegada ofrece flexibilidad para adaptarse al modo en que la organización desee delegar actividades de administración. Para ello, utiliza el control basado en los roles y los objetos. La administración delegada se adapta a implementaciones de todos los tamaños y permite configurar permisos con mucho más detalle a medida que la implementación adquiere complejidad. La administración delegada utiliza tres conceptos: los administradores, los roles y los ámbitos.

- **Administradores**. Un administrador representa una persona o un grupo de usuarios identificados por su cuenta de Active Directory. Cada administrador está asociado a uno o más roles y pares de 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.
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 del 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

La compañía XYZ ha decidido administrar aplicaciones y escritorios por departamento (Cuentas, Ventas, y Almacén) y el sistema operativo de escritorio (Windows 7 o Windows 8). El administrador creó cinco ámbitos. Luego, etiquetó cada grupo de entrega con dos ámbitos: una para el departamento en el que se utilizan y otra para el sistema operativo.

Se crearon los siguientes administradores:

Administrador	Roles	Ámbitos
dominio/Fred	Administrador total	Todo (el rol de administrador total siempre tiene el ámbito Todo)
dominio/Rob	Administrador de solo lectura	Todas
dominio/Heidi	Administrador de solo lectura Administrador de asistencia técnica	Todas Ventas
dominio/adminalmacén	Administrador de asistencia técnica	Almacén de datos
dominio/Peter	Administrador del grupo de entrega Administrador de catálogo de máquinas	Win7

- Daniel es un administrador total y puede ver, modificar y eliminar todos los objetos del sistema.
- Marcos puede ver todos los objetos del sitio, pero no los puede modificar ni eliminar.
- Olivia 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, 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 de datos.
- Pablo 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 Windows 7, independientemente de si se encuentran dentro del ámbito del departamento o no. El administrador se planteó si convertir a Pablo en administrador total del ámbito Win7; sin embargo, descartó esa opción porque un administrador total también tiene derechos totales sobre todos los objetos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

no incluidos en ningún ámbito, como "sitio" y "administrador".

Por lo general, la cantidad 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 una cantidad reducida de ellos; no se delega nada. En este caso, cree a cada administrador con el rol integrado de administrador total, cuyo ámbito es Todo.
- Las implementaciones grandes con más máquinas, aplicaciones y escritorios implican mayor delegación. Varios administradores pueden tener responsabilidades funcionales más específicas (roles). Por ejemplo, dos son administradores totales y los demás son administradores de asistencia. 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 cada administrador a un rol personalizado o integrado, además de 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.

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 total si se trata del único administrador total habilitado en ese momento. La casilla de verificación para habilitar o inhabilitar está activa al crear, copiar o modificar un administrador.

Cuando se elimina una pareja de rol y ámbito 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 total si se trata del único administrador total habilitado en ese momento.

Los nombres de rol pueden contener un máximo de 64 caracteres Unicode; no pueden incluir los siguientes caracteres: \ (barra diagonal inversa), / (barra diagonal), ; (punto y coma), : (dos puntos), # (almohadilla) , (coma), * (asterisco), ? (signo de interrogación), = (signo igual), < (flecha izquierda), > (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 admiten los roles personalizados. Las ediciones donde no se admiten 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 al rol. Haga clic en la ficha Administradores en el panel inferior para ver 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 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.

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 al menos a una pareja de rol y 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 incluir los siguientes 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), ()

© 1999-2017 Citrix Systems, Inc. All rights reserved.

(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).
- 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.

Puede generar dos tipos de informes de administración delegada:

- Un informe HTML que ofrece una lista de las parejas de rol y ámbito asociadas a un administrador, además de los permisos individuales de cada tipo de objeto (por ejemplo, grupos de entrega y catálogos de máquinas). Este informe se genera desde Studio.
  Para crear este informe, haga clic en Configuración > Administradores en el panel de navegación. 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	Destino de escritura de los resultados. Valor predeterminado = stdout

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetro	Descripción
-AdminAddress <string>	La dirección IP o el nombre de host del Delivery Controller con el que hay que establecer conexión. Predeterminado = localhost
-Show	(Válido solamente cuando el parámetro -Path también se especifica.) Cuando se escribe el resultado en un archivo, -Show hace que dicho archivo se abra con el programa adecuado como, por ejemplo, un explorador Web.
	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer y OutVariable. Para obtener más información, consulte la documentación de Microsoft.

En el siguiente ejemplo, se escribe una tabla HTML en un archivo denominado Roles.html y se abre la tabla en un explorador Web.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
-Path Roles.html –Show
```

En el siguiente ejemplo, se escribe una tabla CSV en un archivo denominado Roles.csv. La tabla no se muestra.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"
–CSV -Path Roles.csv
```

Desde el símbolo del sistema Windows, el comando del ejemplo anterior es:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'
-CSV -Path Roles.csv"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tarjetas inteligentes

Dec 05, 2017

Las tarjetas inteligentes y otras tecnologías equivalentes se admiten si se ajustan a las directrices descritas en este artículo.Para usar tarjetas inteligentes con XenApp o XenDesktop:

- 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 XenApp o XenDesktop.
- 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.XenApp y XenDesktop admiten esos 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 XenApp o XenDesktop.

Para tarjetas inteligentes de empresa, existen opciones equivalentes que son compatibles y se pueden utilizar de una forma similar.

- Un token USB equivalente a una tarjeta inteligente se conecta directamente a un puerto USB. Esos tokens USB tienen normalmente el tamaño de una unidad flash USB, pero pueden ser tan pequeños como la tarjeta SIM de un teléfono móvil. Aparecen como la combinación de una tarjeta inteligente y un lector USB de tarjetas inteligentes.
- Una tarjeta inteligente virtual que utiliza el módulo de plataforma segura (Trusted Platform Module) de Windows aparece como una tarjeta inteligente. Esas tarjetas inteligentes virtuales se admiten en Windows 8 y Windows 10 con Citrix Receiver 4.3 como versión mínima.
  - Las versiones de XenApp y XenDesktop que sean anteriores a 7.6 FP3 no admiten 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

inteligentes.

El respaldo para tarjeta inteligente de XenApp y XenDesktop 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 en http://www.citrix.com/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
Minicontrolador GemAlto para tarjeta .NET	GemAlto .NET v2+
Controlador nativo de Microsoft	Tarjetas inteligentes virtuales (TPM)

Para obtener más información sobre el uso de tarjetas inteligentes con otros tipos de dispositivo, consulte la documentación de Citrix Receiver referente al dispositivo concreto. Para obtener más información acerca del uso de PIV con XenDesktop, consulte Configuring Citrix XenDesktop 7.6 and NetScaler Gateway 10.5 with PIV Smart Card Authentication.

Para obtener más información sobre el uso de tarjetas inteligentes con otros tipos de dispositivo, consulte la documentación de Citrix Receiver referente al dispositivo concreto.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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 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 tarjeta 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 tarjeta inteligente de clase 2 pueden estar integrados en un teclado que contenga a su vez un teclado numérico seguro. Para lectores de tarjeta inteligente de clase 2, póngase en contacto con su representante de Citrix. Puede ser necesario un controlador de dispositivo específico del lector para habilitar la función de teclado numérico seguro.
- Los lectores de tarjetas inteligentes de clase 3 contienen, además, una pantalla segura.Los lectores de tarjetas inteligentes de clase 3 no se admiten.
- Los lectores de tarjetas inteligentes de clase 4 contienen, además, un módulo de transacción segura. Los lectores de tarjetas inteligentes de clase 4 no se respaldan.

Nota: La clase que tenga el lector de tarjetas inteligentes no tiene que ver con la clase de dispositivo USB.

Los lectores de tarjeta inteligente 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 versión de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Receiver que utiliza. En la documentación de Citrix Receiver, las versiones admitidas se incluyen normalmente 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 XenApp y XenDesktop mediante un canal virtual ICA/HDX determinado para tarjetas inteligentes que está habilitado de forma predeterminada.

Importante: No utilice la redirección de USB genérico para lectores de tarjetas inteligentes.Esta funcionalidad está inhabilitada de forma predeterminada para lectores de tarjeta inteligente 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.

Si está utilizando aplicaciones alojadas ejecutadas en Windows Server 2008 o 2008 R2 y con tarjetas inteligentes que requieren el Proveedor base de servicios de cifrado para tarjetas inteligentes de Microsoft, es posible que, si un usuario ejecuta una transacción de tarjeta inteligente, se bloqueen los demás usuarios que utilizan una tarjeta inteligente en el proceso de inicio de sesión. Para obtener más información y una revisión hotfix para este tema, consulte http://support.microsoft.com/kb/949538.

Puede restablecer los PIN con un sistema de administración de tarjetas o alguna herramienta del proveedor.

> **Important**
>
> En una sesión de XenApp o XenDesktop, no se admite el uso de una tarjeta inteligente con la aplicación Conexión a Escritorio remoto de Microsoft. Esto a veces se describe como un uso de "doble salto".

Antes de implementar tarjetas inteligentes

- Obtenga un controlador de dispositivo para el lector de tarjetas inteligentes e instálelo en el dispositivo de usuario. Muchos lectores de tarjetas inteligentes pueden usar el controlador de dispositivo CCID que proporciona Microsoft.
- Obtenga un controlador de dispositivo y el software de proveedor de servicios de cifrado (CSP) del proveedor de la tarjeta inteligente e instálelos en los dispositivos de usuario y escritorios virtuales. El controlador y el software CSP deben ser compatibles con XenApp y XenDesktop; consulte la documentación del proveedor para comprobarlo. Para los escritorios virtuales con tarjetas inteligentes que admiten y usan el modelo de minicontroladores, los minicontroladores de tarjeta inteligente deberían descargarse automáticamente, pero pueden obtenerse en http://catalog.update.microsoft.com o del proveedor. Además, si se necesita middleware de PKCS #11, puede obtenerlo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Citrix Receiver 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 NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optativo para acceso con Remote PC): Microsoft Exchange Server

Habilitación del uso de tarjetas inteligentes

Paso 1. Proporcione tarjetas inteligentes a los usuarios de acuerdo con su directiva de emisión de tarjetas.

Paso 2.(Opcional) Configure las tarjetas inteligentes para permitir a los usuarios el acceso con Remote PC.

Paso 3. Instale y configure el Delivery Controller y StoreFront (si no están ya instalados) para la comunicación remota con tarjetas inteligentes.

Paso 4. Habilite StoreFront para usar tarjetas inteligentes. Para obtener más información, consulte "Configurar la autenticación con tarjeta inteligente" en la documentación de StoreFront.

Paso 5. Habilite NetScaler 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 de la tarjeta inteligente, habilite la comunicación de datos de la tarjeta inteligente entre Citrix Receiver 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 "Configurar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Instale el middleware del proveedor de la tarjeta inteligente.
- Instale y configure Citrix Receiver 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 Citrix Receiver).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Implementaciones de tarjeta inteligente

Dec 05, 2017

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 NetScaler Gateway
Equipos no unidos a dominio	Conectados directamente
Acceso remoto desde equipos no unidos a un dominio	Conectados a través de NetScaler 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.

Cuando es posible en cada una de estas implementaciones, Receiver respalda 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 ha caducado).

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, se solicita a los usuarios 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 NetScaler Gateway, los usuarios inician sesión en sus dispositivos y Receiver para Windows les pedirá

© 1999-2017 Citrix Systems, Inc. All rights reserved.

autenticarse en NetScaler 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 NetScaler Gateway con su tarjeta inteligente y su PIN o con credenciales explícitas. Esto permite ofrecer a los usuarios la autenticación bimodal para los inicios de sesión de NetScaler Gateway. Configure la autenticación PassThrough de NetScaler Gateway a StoreFront y delegue la validación de las credenciales a NetScaler Gateway para los usuarios de tarjeta inteligente, de modo que los usuarios se autentiquen silenciosamente en StoreFront.

En un entorno Citrix, se respalda el uso de tarjetas inteligentes dentro de un único bosque. Los inicios de sesión con tarjeta inteligente en varios bosques requieren una relación de confianza bidireccional entre los bosques y 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).

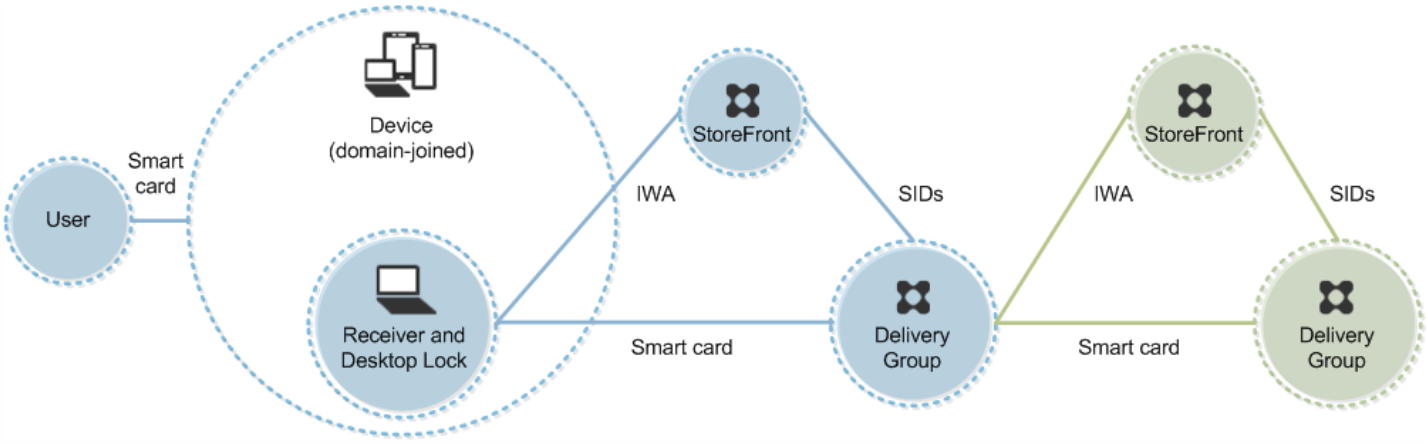
La directiva de extracción de tarjetas inteligentes definida en el producto determina el comportamiento al extraer la tarjeta inteligente del lector durante una sesión. El sistema operativo Windows configura y controla esta directiva de extracción.

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 datos.
Desconectar si es una sesión remota de Terminal Services	La sesión se desconecta y el escritorio virtual queda bloqueado.

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.

Esta implementación contiene dispositivos de usuario que están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan directamente a StoreFront.

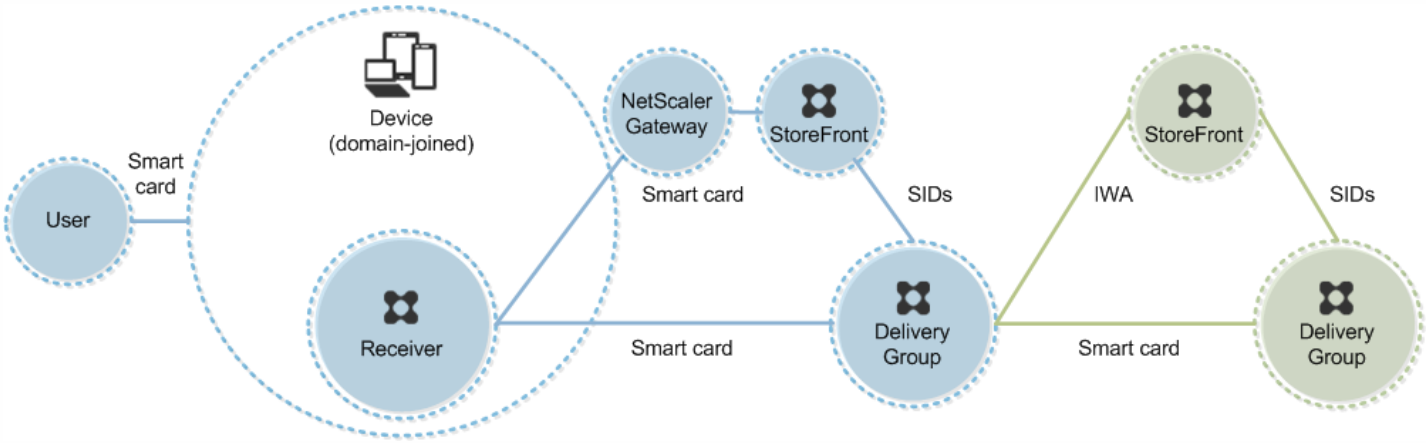
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 XenApp o XenDesktop. Cuando el usuario inicia una aplicación o un escritorio virtual, no se vuelve a solicitar el PIN al usuario porque la función 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 presente en el escritorio virtual se autentica en el segundo servidor StoreFront. En esta segunda conexión, se puede usar cualquier método de autenticación. La configuración mostrada para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

Esta implementación contiene dispositivos de usuario que están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan a StoreFront a través de NetScaler Gateway/Access Gateway.



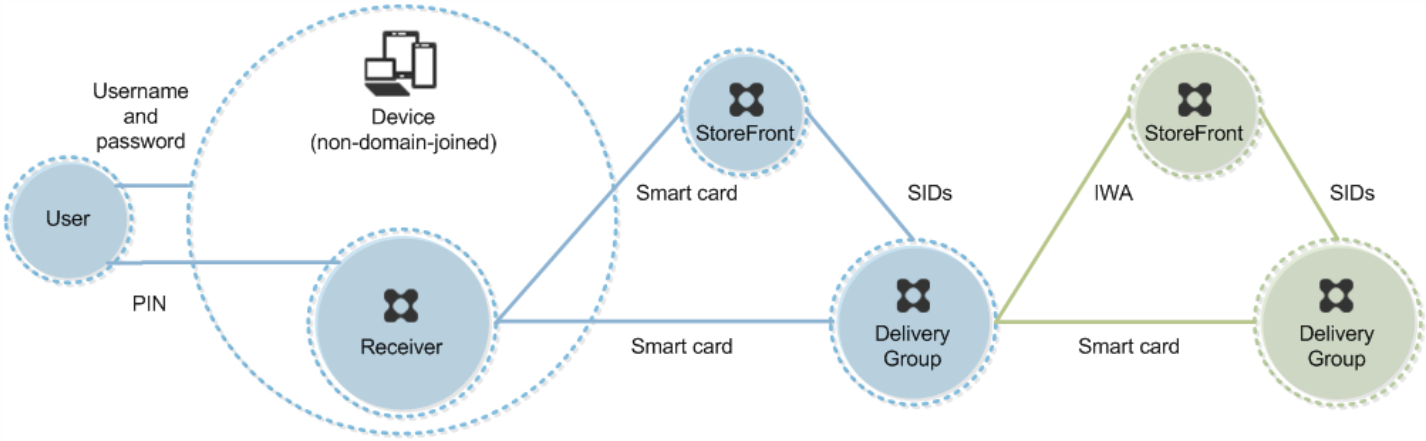
El usuario inicia sesión en un dispositivo con una tarjeta inteligente y un PIN y, a continuación, inicia otra sesión en NetScaler Gateway/Access Gateway. Este segundo inicio de sesión puede realizarse con la tarjeta inteligente y el PIN, o bien, con un nombre de usuario y una contraseña, porque Receiver 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 XenApp o XenDesktop. Cuando el usuario inicia una aplicación o un escritorio virtual, no se le vuelve a solicitar el PIN porque la función Single Sign-On está configurada en Receiver.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 presente en el escritorio virtual se autentica en el segundo servidor StoreFront. En esta segunda conexión, se puede usar cualquier método de autenticación. La configuración mostrada para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

Esta implementación contiene dispositivos de usuario que no están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan directamente a StoreFront.



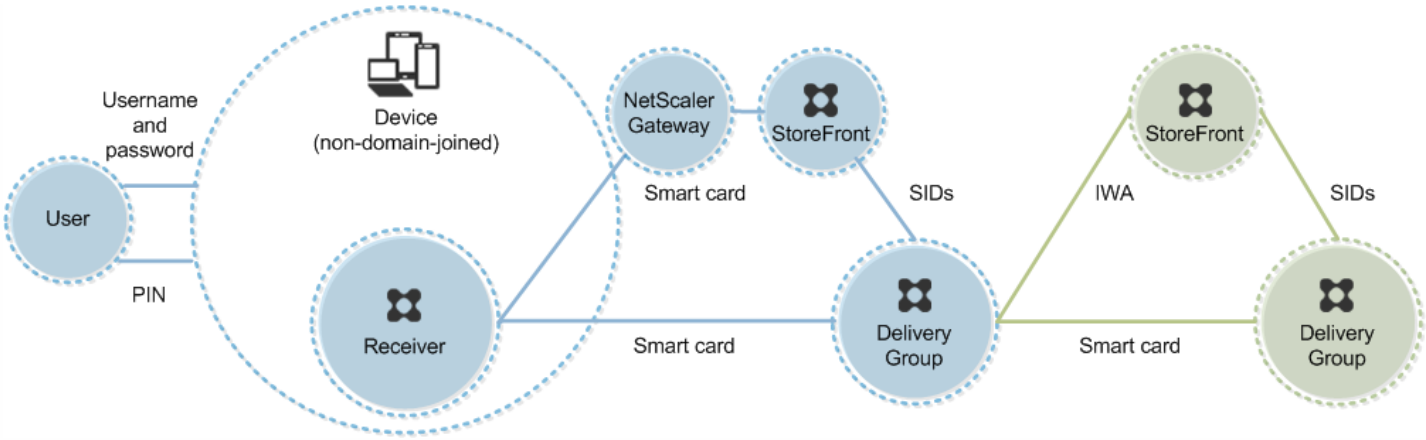
El usuario inicia la sesión en un dispositivo. Por lo general, el usuario introduce un nombre de usuario y una contraseña pero, como el dispositivo no está unido a un dominio, las credenciales de inicio de sesión son optativas. Como la autenticación bimodal es posible en esta implementación, Receiver pide al usuario una tarjeta inteligente y un PIN, o bien, un nombre de usuario y una contraseña. A continuación, Receiver se autentica en Storefront.

StoreFront pasa los identificadores de seguridad del usuario (SID) a XenApp o XenDesktop. Cuando el usuario inicia una aplicación o un escritorio virtual, se le solicita un PIN de nuevo porque la función 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 presente en el escritorio virtual se autentica en el segundo servidor StoreFront. En esta segunda conexión, se puede usar cualquier método de autenticación. La configuración mostrada para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

Esta implementación contiene dispositivos de usuario que no están unidos a un dominio, y que ejecutan Desktop Viewer y se conectan directamente a StoreFront.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 bien, un nombre de usuario y una contraseña. A continuación, Receiver se autentica en Storefront.

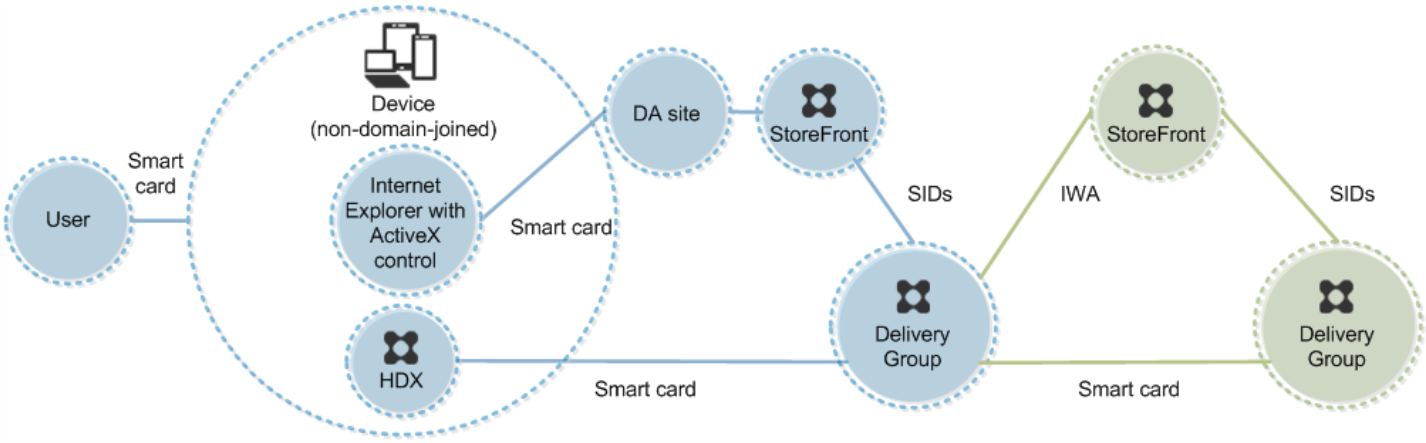
StoreFront pasa los identificadores de seguridad del usuario (SID) a XenApp o XenDesktop. Cuando el usuario inicia una aplicación o un escritorio virtual, se le solicita un PIN de nuevo porque la función Single Sign-On no está disponible en esta implementación.

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 presente en el escritorio virtual se autentica en el segundo servidor StoreFront. En esta segunda conexión, se puede usar cualquier método de autenticación. La configuración mostrada para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

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 XenApp, XenDesktop 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 a los dispositivos subyacentes. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

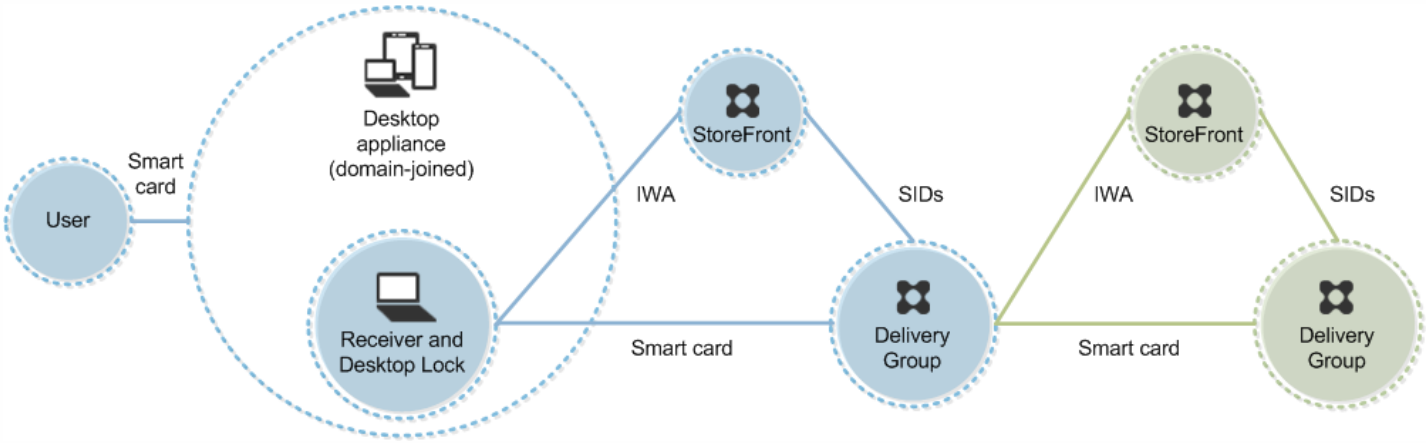


El usuario inicia una sesión en un dispositivo usando una tarjeta inteligente. Si Desktop Lock se está ejecutando en el dispositivo, el dispositivo se configura para iniciar el sitio de Desktop Appliance a través de Internet Explorer ejecutado en modo quiosco (pantalla completa). Un control ActiveX en el sitio solicita el PIN al usuario y lo envía a StoreFront. StoreFront pasa los identificadores de seguridad del usuario (SID) a XenApp o XenDesktop. Se iniciará el primer escritorio que esté disponible en la lista alfabética del grupo de escritorios asignados.

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 presente en el escritorio virtual se autentica en el segundo servidor StoreFront. En esta segunda conexión, se puede usar cualquier método de autenticación. La configuración mostrada para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

Esta implementación contiene dispositivos de usuario que están unidos a un dominio, 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 XenApp, XenDesktop 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 a los dispositivos subyacentes. 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenApp o XenDesktop. Cuando el usuario inicia un escritorio virtual, no se le vuelve a solicitar el PIN porque la función 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 presente en el escritorio virtual se autentica en el segundo servidor StoreFront. En esta segunda conexión, se puede usar cualquier método de autenticación. La configuración mostrada para el primer salto se puede volver a utilizar en el segundo salto o usarse en el segundo salto solamente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autenticación PassThrough y Single Sign-On con tarjetas inteligentes

Dec 05, 2017

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 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 autenticación directa a 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 tarjeta inteligente unidas a dominio, directas a StoreFront: Defina DisableCtrlAltDel como Off
- Implementaciones de tarjeta inteligente unidas a dominio, desde NetScaler a StoreFront: Defina UseLocalUserAndPassword como On

Para obtener instrucciones sobre cómo configurar estos parámetros, consulte la documentación de StoreFront o NetScaler Gateway.

La disponibilidad de la funcionalidad Single Sign-On depende de varios factores, incluidos, entre otros:

- Las directivas de seguridad de la organización respecto al inicio de sesión único.
- 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 Virtual Delivery Agent (VDA) en una máquina que tiene un lector de tarjeta inteligente conectado, puede aparecer un icono de Windows que representa el anterior método de autenticación utilizado

© 1999-2017 Citrix Systems, Inc. All rights reserved.

correctamente (como una tarjeta inteligente o contraseña). Por eso, si 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Transport Layer Security (TLS)

Jan 05, 2018

La configuración de un sitio de XenApp o XenDesktop para que use el protocolo Transport Layer Security (TLS) incluye los siguientes procedimientos:

- 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 los usuarios y los agentes VDA (Virtual Delivery Agent) completando las siguientes tareas:
  - Configure TLS en las máquinas donde los VDA están instalados. (Para mayor comodidad, las siguientes referencias a máquinas donde haya agentes VDA instalados se denominarán simplemente "agentes VDA".) Puede usar un script de PowerShell suministrado por Citrix o configurarlo manualmente. Para obtener más información, consulte Acerca de los parámetros de TLS en los VDA. Para obtener más información, consulte Configuración de TLS en un agente VDA mediante el script de PowerShell y Configuración manual de TLS en un agente VDA.
  - Configure TLS en los grupos de entrega que contienen los VDA mediante la ejecución de un conjunto de cmdlets de PowerShell en Studio. Para obtener más información, consulte Configurar TLS en 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 de Controllers; los administradores totales tienen este permiso.
  - Para configurar TLS en los VDA, debe ser un administrador Windows en la máquina donde está instalado el VDA.
  - Si tiene pensado configurar TLS en los VDA que se han actualizado desde versiones más antiguas, desinstale cualquier software de traspaso SSL que haya en esas máquinas antes de actualizarlas.
  - El script de PowerShell configura el protocolo TLS en agentes VDA estáticos, no lo configura en VDA agrupados y aprovisionados por Machine Creation Services o Provisioning Services, en los que la imagen de las máquinas se restablece con cada reinicio.

> ## 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Para obtener información acerca de la habilitación de TLS para la base de datos del sitio, consulte CTX137556.

> ## Nota
>
> Si TLS y UDT están habilitados en el VDA:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Para el acceso directo al VDA, Citrix Receiver utiliza siempre TLS sobre TCP (no UDP y UDT).
- Para acceder indirectamente al VDA mediante NetScaler Gateway, Citrix Receiver usa el protocolo DTLS sobre UDP para la comunicación con NetScaler Gateway. Para la comunicación entre NetScaler Gateway y el VDA, se utiliza UDP sin DTLS. Se utiliza UDT.

Instale certificados de servidor TLS en los Controllers

Para HTTPS, XML Service respalda las funciones de TLS mediante el uso de certificados de servidor, pero no de certificados de cliente. Para obtener, instalar y registrar un certificado en un Controller y para configurar un puerto con el certificado TLS:

Si IIS está instalado en el Controller, siga los pasos descritos en https://technet.microsoft.com/es-es/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 como se describe en http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx. Para obtener información sobre la herramienta certreq, consulte http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx.
   Si quiere utilizar el script de PowerShell para configurar TLS en los VDA y, a menos que vaya a especificar la huella digital del certificado de SSL, compruebe que el certificado se encuentra en la sección Equipo local > Personal > Certificados, en el almacén de certificados. Si hay más de un certificado en esa ubicación, se usa el primero que se encuentra.
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.

El orden en la lista 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_SHA384 o TLS_ECDHE_RSA_WITH_AES_128_GCM _SHA256.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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”. Establezca esta directiva como Habilitada.
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 el artículo 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 <*http-port*> -WISSLPORT <*https-port*>

donde <*http-port*> es el número de puerto para el tráfico HTTP y <*https-port*> es el número de puerto para el tráfico HTTPS.

> ## Nota
>
> Después de cambiar de un puerto, Studio puede mostrar un mensaje acerca de la actualización y la compatibilidad de licencias. Para resolver el problema, vuelva a registrar las instancias de servicio mediante esta secuencia de cmdlet de PowerShell:
>
> Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding XML_HTTPS |
>
> Unregister-ConfigRegisteredServiceInstance
>
> Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |
> Register-ConfigServiceInstance

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Un grupo de entrega no puede incluir una mezcla de VDA con TLS configurado y VDA sin TLS configurado. Al 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, cambiarán los permisos del certificado TLS instalado, lo que da al servicio ICA acceso de lectura a la clave privada del certificado e informa a 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.

> ## Important
>
> 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.

- ¿Qué conjuntos de cifrado TLS permitir?

  El conjunto de cifrado selecciona el cifrado que se usará para una conexión. Los clientes y los agentes VDA pueden admitir varios grupos diferentes de conjuntos de cifrado. Cuando un cliente (Citrix Receiver 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 más información sobre el modo FIPS de Windows. La tabla siguiente muestra los conjuntos de cifrado en cada grupo:

Conjunto de cifrado TLS	GOV	COM	Todo	GOV	COM	Todo
Modo FIPS	Apagado	No	No	Sí	Sí	Iniciado
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	x		x	x		x

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TLS_RSA_WITH_AES_256_GCM_SHA384	x		x	x		x
TLS_RSA_WITH_AES_128_GCM_SHA256	x	x	x	x	x	x
TLS_RSA_WITH_AES_256_CBC_SHA256	x		x	x		x
TLS_RSA_WITH_AES_256_CBC_SHA	x		x	x		x
TLS_RSA_WITH_AES_128_CBC_SHA		x	x		x	x
TLS_RSA_WITH_RC4_128_SHA		x	x			
TLS_RSA_WITH_RC4_128_MD5		x	x			
TLS_RSA_WITH_3DES_EDE_CBC_SHA	x		x	x		x

Important

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), Citrix Receiver para HTML5 y Citrix Receiver para Chrome. También se incluyen las conexiones a través de NetScaler Gateway.

Este paso también es necesario para todas las conexiones que pasan por NetScaler Gateway, para todas las versiones de VDA, si TLS entre NetScaler Gateway y el VDA está configurado. Eso afecta a todas las versiones de Citrix Receiver.

En el VDA (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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TLS_RSA_WITH_3DES_EDE_CBC_SHA

> **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 (Citrix Receiver 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.

> **Important**
>
> 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.

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.

Al habilitar TLS, el script inhabilita todas las reglas de Firewall de Windows para el puerto TCP especificado antes de agregar una nueva regla que permite que el servicio ICA acepte conexiones entrantes en el puerto TCP 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 por TLS; no pueden usar ICA/HDX, ICA/HDX con Fiabilidad de la sesión o HDX por WebSocket, sin TLS.

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.

> **Important**
>
> Debe indicar el parámetro Enable o Disable, así como el parámetro CertificateThumbPrint. Los demás parámetros son opcionales.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sintaxis

Enable-VdaSSL {-Enable | -Disable} -CertificateThumbPrint ""
[–SSLPort] [-SSLMinVersion ""] [-SSLCipherSuite""]

Parameter	Description
Habilitar	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.
CertificateThumbPrint ""	Huella digital del certificado TLS en el almacén de certificados, entre comillas. El script utiliza la huella digital especificada para seleccionar el certificado a utilizar. Este parámetro es obligatorio; si no lo indica, se selecciona un certificado incorrecto.
–SSLPort	Puerto TLS. Valor predeterminado: 443
SSLMinVersion ""	Versión mínima del protocolo TLS, entre comillas. Valores válidos: • "SSL_3.0" • "TLS_1.0" • "TLS_1.1" • "TLS_1.2" Valor predeterminado: "TLS_1.0" **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 TLS, entre comillas. Valores válidos: • "GOV" • "COM" • "ALL" Valor predeterminado: "ALL"

Ejemplos

El siguiente script instala y habilita el valor de versión del protocolo 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"
```

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
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

-CertificateThumbPrint "12345678987654321"
–SSLPort 400 'SSLMinVersion "TLS_1.2"
–SSLCipherSuite "GOV"

El siguiente script inhabilita la escucha de TLS en el VDA.

Enable-VdaSSL –Disable

Al configurar TLS en un VDA manualmente, 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 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. Edite 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.

   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 el puerto TCP de TLS está abierto en el Firewall de Windows, si no es el predeterminado 443. (Cuando cree la regla de entrada en el Firewall de Windows, compruebe que tenga las entradas "Permitir la conexión" y

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

"Habilitada" están seleccionadas 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.)

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 '<*delivery-group-name*>' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true**.
4. Ejecute **Set-BrokerSite -DnsResolutionEnabled $true**.

Si se produce un error de conexión, compruebe el registro de eventos del sistema en el VDA.

Cuando se usa Citrix Receiver para Windows, si recibe un error de conexión (por ejemplo, 1030) que indica un error TLS, inhabilite Desktop Viewer y, a continuación, intente conectarse de nuevo. Aunque la conexión fallará, 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.)

Comunicación entre Controller y VDA

La comunicación entre el Controller y el VDA está protegida con la protección de mensajes Windows Communication Framework (WCF). No se necesita la protección adicional de transporte mediante el protocolo TLS. La configuración de WCF usa Kerberos para la autenticación mutua entre el Controller y el VDA. Para el cifrado, se usa AES en el modo CBC con una clave de 256 bits. Para la integridad de los mensajes, se usa SHA-1.

Según Microsoft, los Protocolos de seguridad que utiliza WCF cumplen los estándares de OASIS (Organization for the Advancement of Structured Information Standards), incluidos los WS-SecurityPolicy 1.2.Además, Microsoft afirma que WCF admite todos los conjuntos de algoritmos que constan en Security Policy 1.2.

La comunicación entre el Controller y el VDA usa el conjunto de algoritmos basic256, cuyos algoritmos son como se ha señalado anteriormente.

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 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.

Para obtener más información sobre la redirección de vídeo HTML5, consulte Configuraciones de directiva de Multimedia.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota

Si no tiene intención de utilizar la redirección de vídeo HTML5, le recomendamos eliminar los dos certificados del 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.

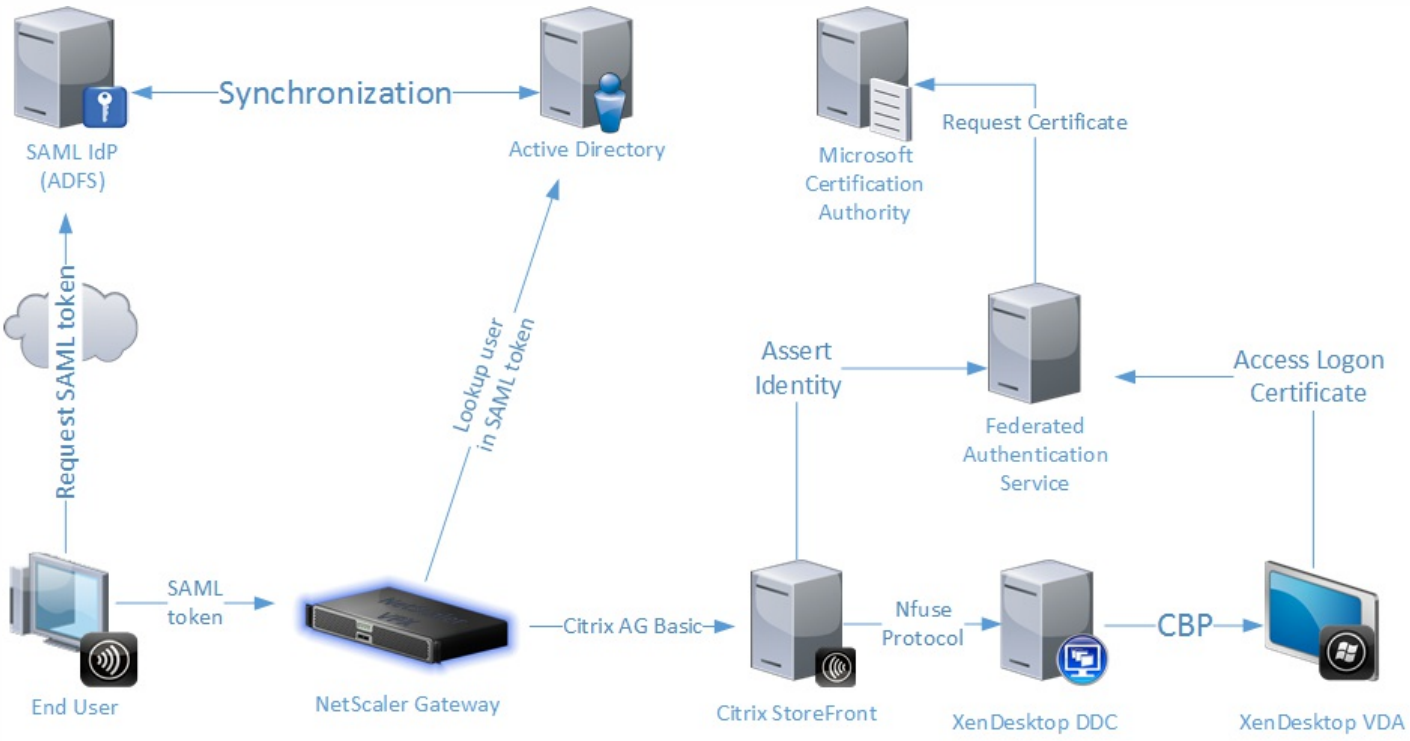
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Servicio de autenticación federada

Dec 05, 2017

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 XenApp y XenDesktop.



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 sesión de XenApp o XenDesktop 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 cada operación de firma y descifrado que necesita llevar a cabo con el certificado al servicio FAS.

Requisitos

El servicio de autenticación federada se admite en servidores Windows (Windows Server 2008 R2 o una versión posterior).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrix recomienda la instalación del servicio FAS en un servidor que no contenga ningún otro 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 XenApp o XenDesktop:

- 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. Instalación del Servicio de autenticación federada
2. Habilitación del plug-in del Servicio de autenticación federada en los servidores StoreFront
3. Configuración de 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 para usar su entidad de certificación
5. Configuración de reglas de usuario

Instalación del 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:

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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

Habilitación del plug-in del Servicio de autenticación federada en una tienda de StoreFront

Para habilitar la integración del Servicio de autenticación federada en una tienda de StoreFront, ejecute los siguientes cmdlets de PowerShell con una cuenta de administrador. Si tiene más de una tienda, o si la tienda tiene otro nombre, la ruta indicada aquí puede ser distinta de la suya.

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "FASClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "FASLogonDataProvider"
```

Para dejar de usar el servicio FAS, use el siguiente script de PowerShell:

```
Get-Module "Citrix.StoreFront.*" -ListAvailable | Import-Module

$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName "standardClaimsFactory"

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de Delivery Controller

Para usar el Servicio de autenticación federada, configure el Delivery Controller de XenApp o XenDesktop para que confíe en los servidores StoreFront que pueden conectarse a él: ejecute el cmdlet de PowerShell **Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true**.

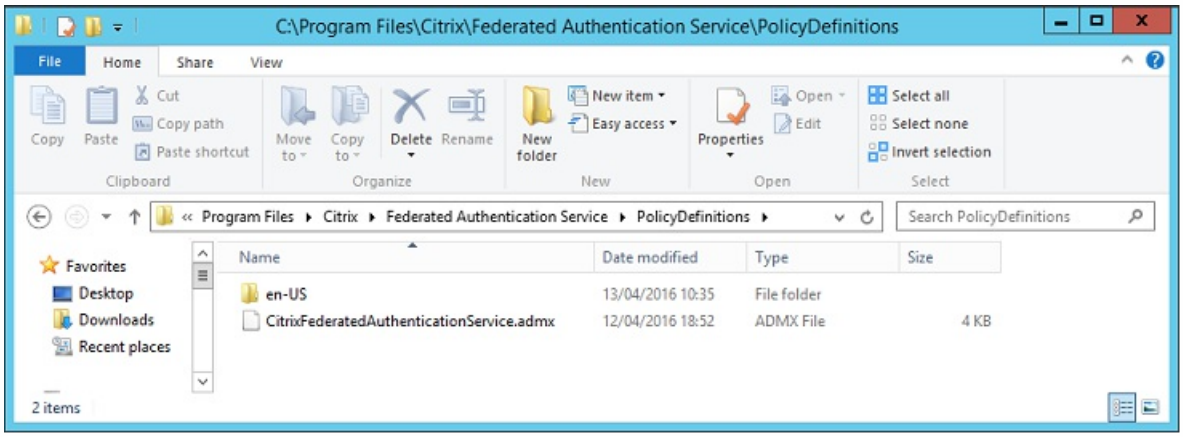
Configuración de la directiva de grupo

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.

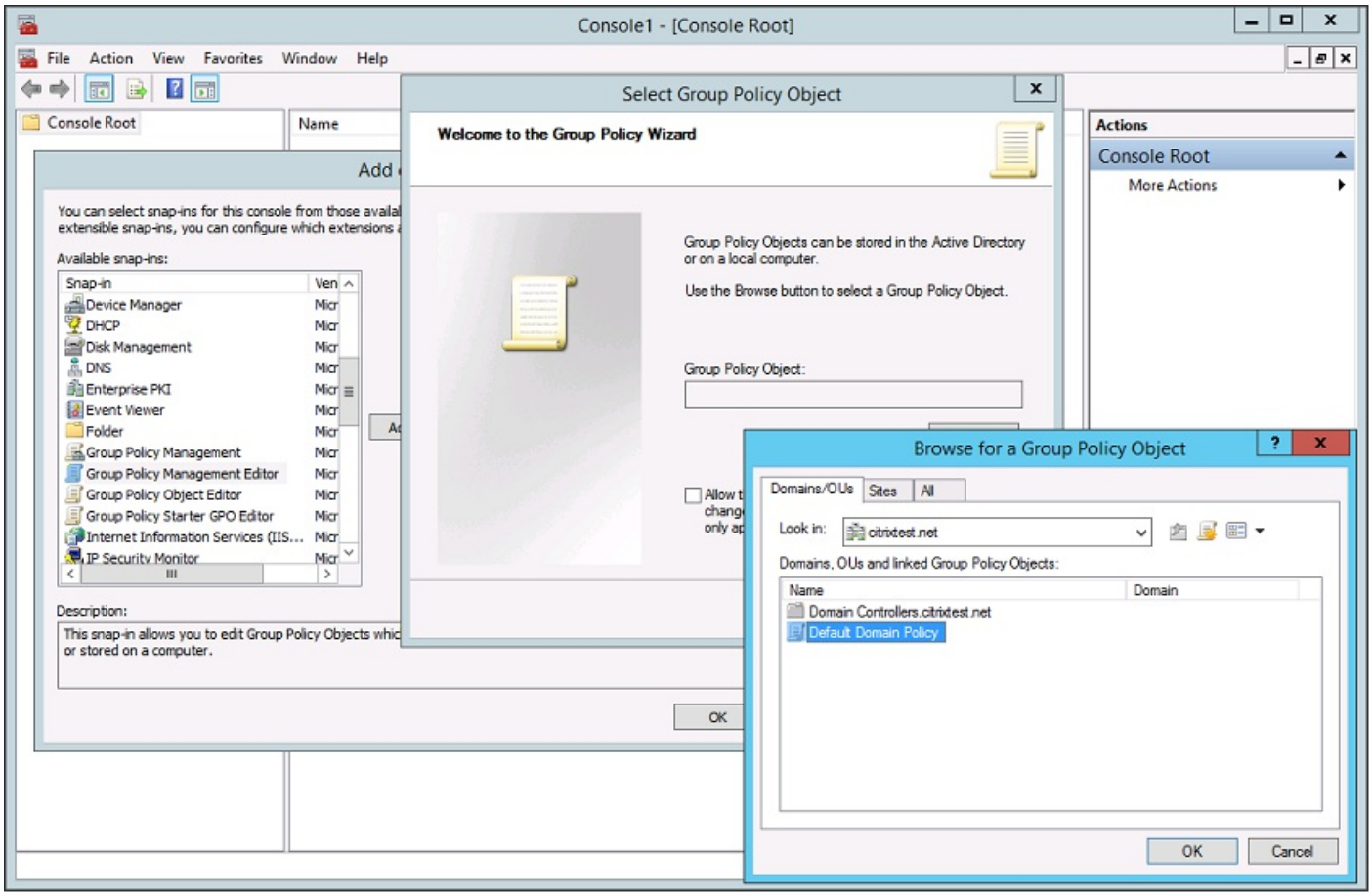


Paso 2. Cópielos en el controlador de dominio y colóquelos en la unidad C:\Windows\PolicyDefinitions y en la subcarpeta en-US.

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**.

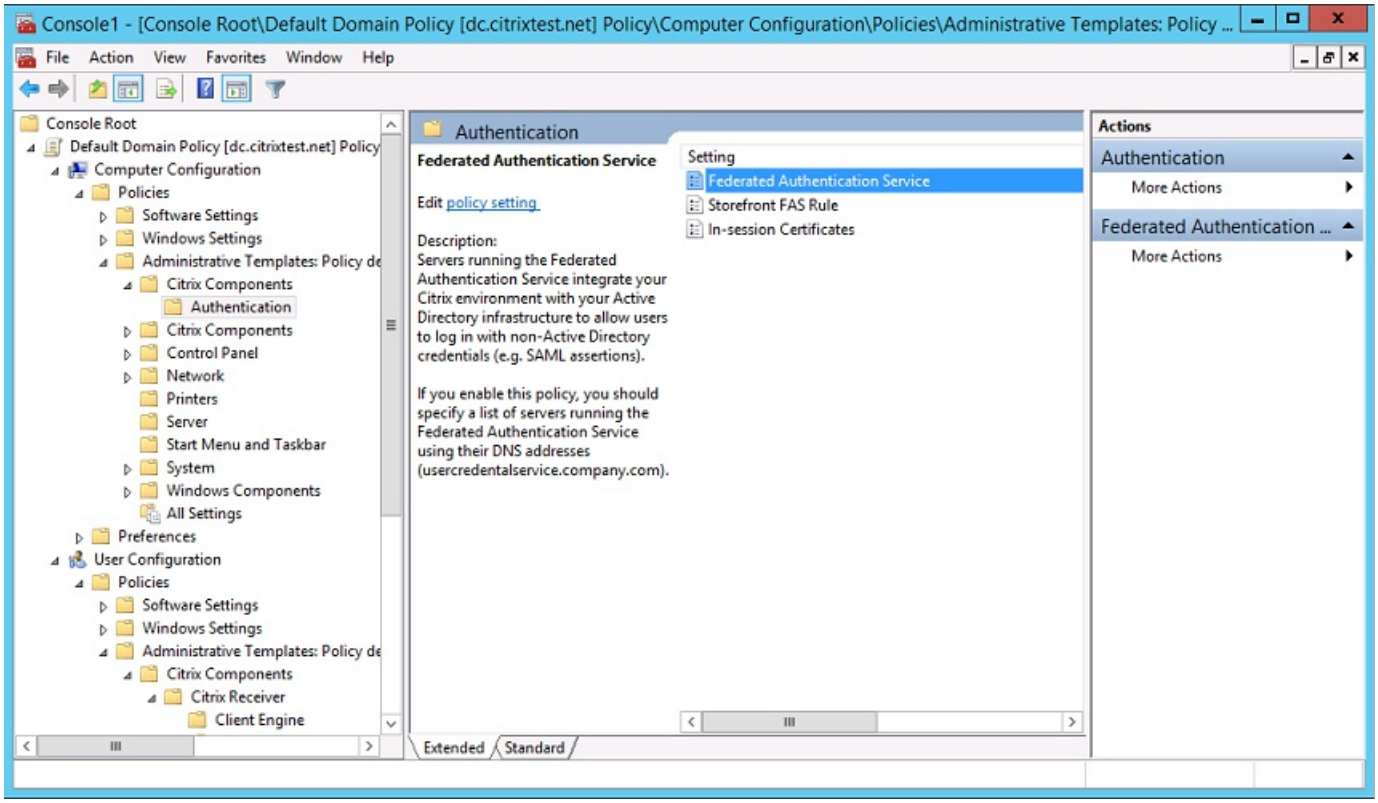
Cuando se le solicite un objeto de directiva de grupo, seleccione **Examinar** y, a continuación, seleccione **Directiva predeterminada de dominio**. De forma alternativa, puede crear y seleccionar un objeto de directiva adecuado para el entorno, mediante las herramientas de su elección. La directiva debe aplicarse a todas las máquinas que ejecutan el software de Citrix afectado (VDA, servidores StoreFront, herramientas de administración).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

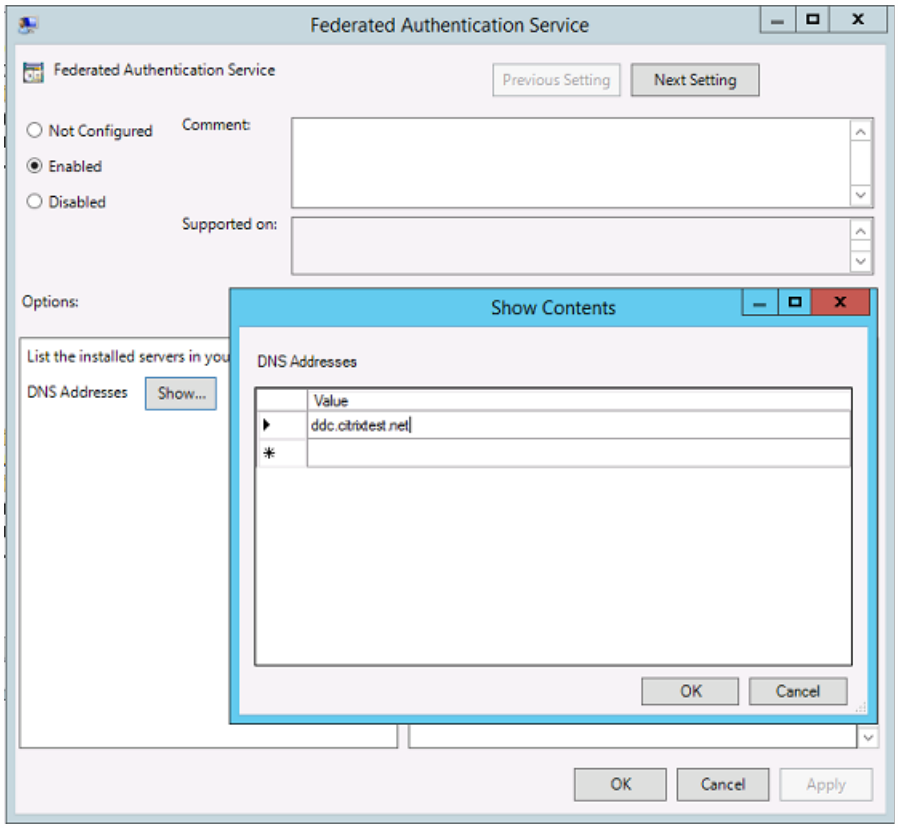


Paso 4. Vaya a la directiva de Servicio de autenticación federada (Federated Authentication Service) en Configuración del equipo/Directivas/Plantillas administrativas/Citrix Components/Authentication.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



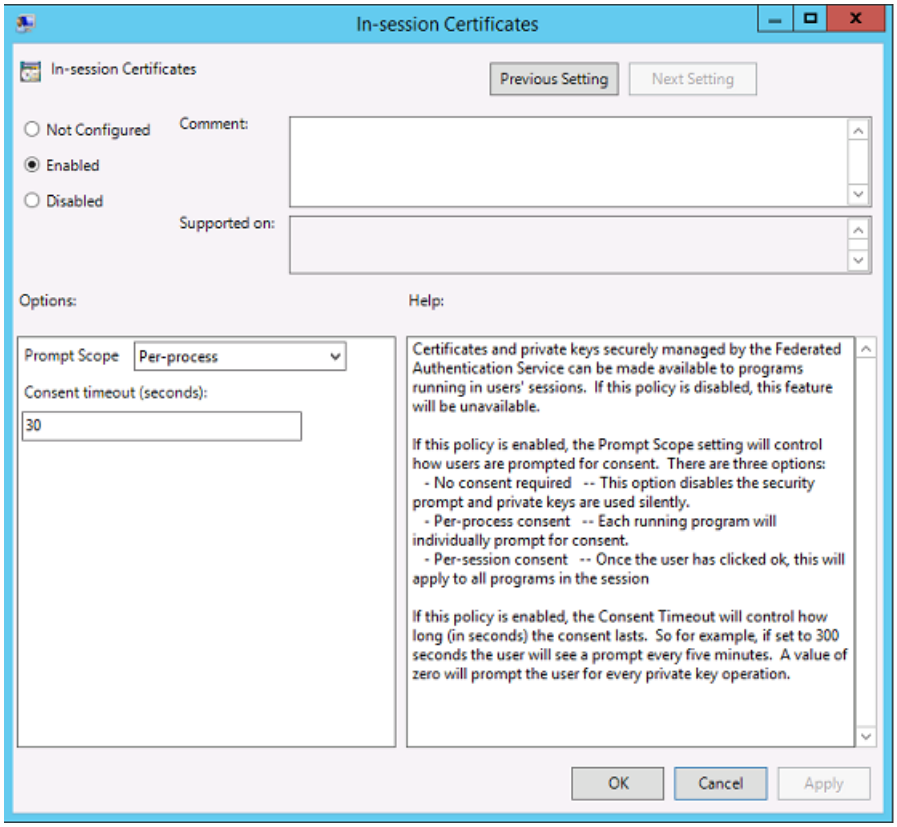
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 las direcciones 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.

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.

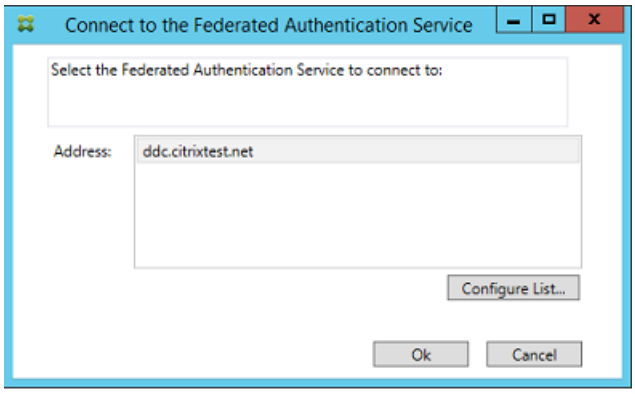


Uso de la consola de administración de los Servicios de autenticación federada

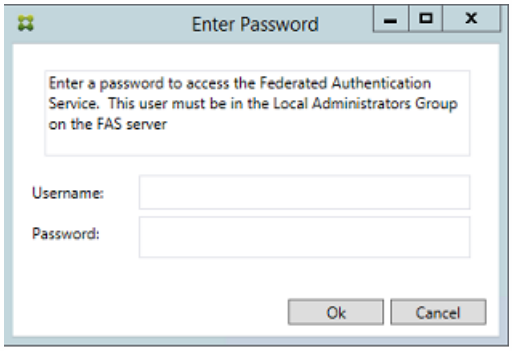
La consola de administración del Servicio de autenticación federada se instala como parte del servicio de autenticación federada. Se coloca el icono Citrix Federated Authentication Service en el menú Inicio.

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 Configuración de la directiva de grupo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

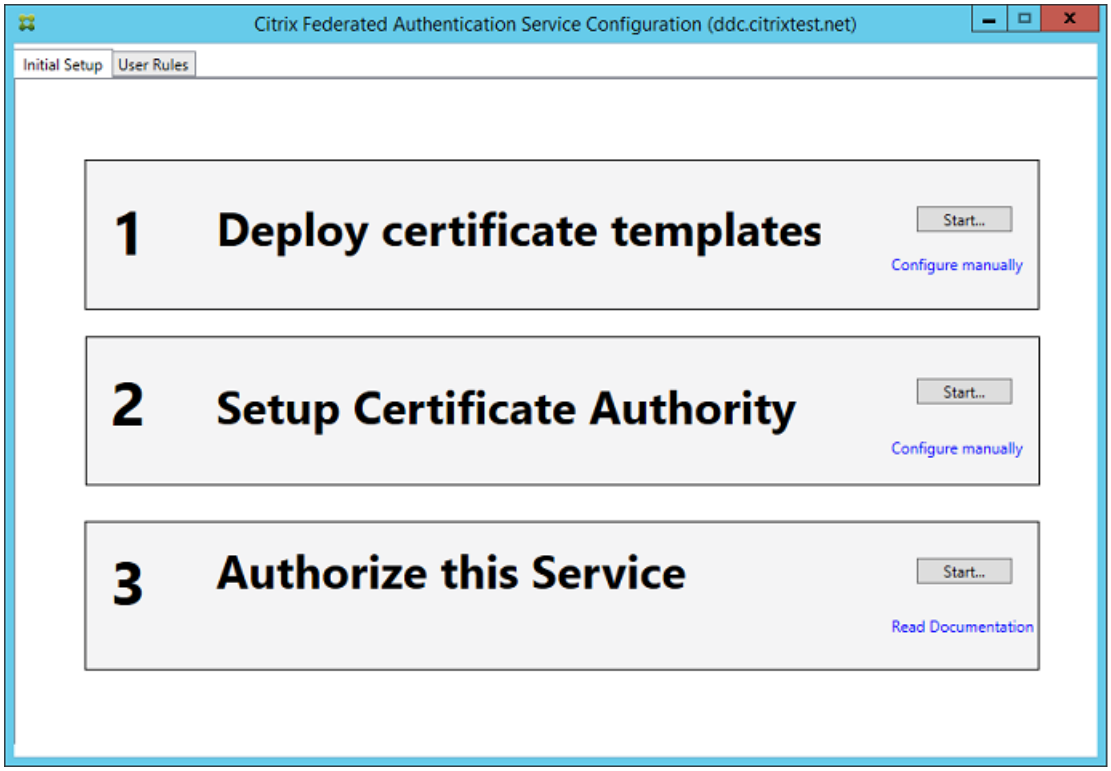


Si la cuenta de usuario no es miembro del grupo Administradores en el equipo que ejecuta el Servicio de autenticación federada, se le solicitará que introduzca las credenciales.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

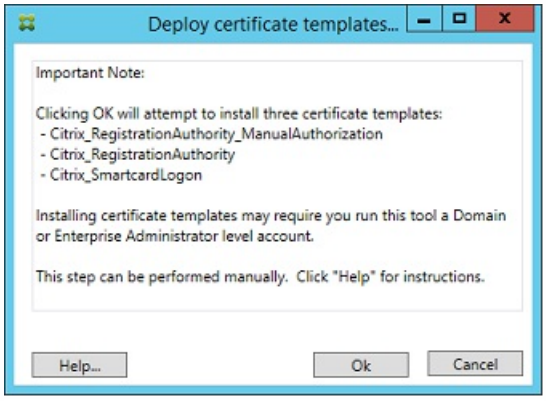


Implementación de plantillas de certificado

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 **Implementación de plantillas de certificado**. Esta herramienta debe ejecutarse con una cuenta que tenga permisos para administrar el bosque de su empresa.



La configuración de las plantillas se encuentra en los archivos XML con la extensión .certificatetemplate que se instalan con

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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)
```

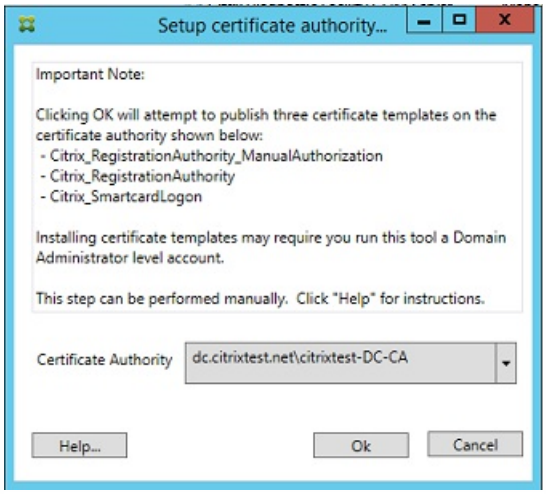
Configuración de los Servicios de certificados de Active Directory

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.

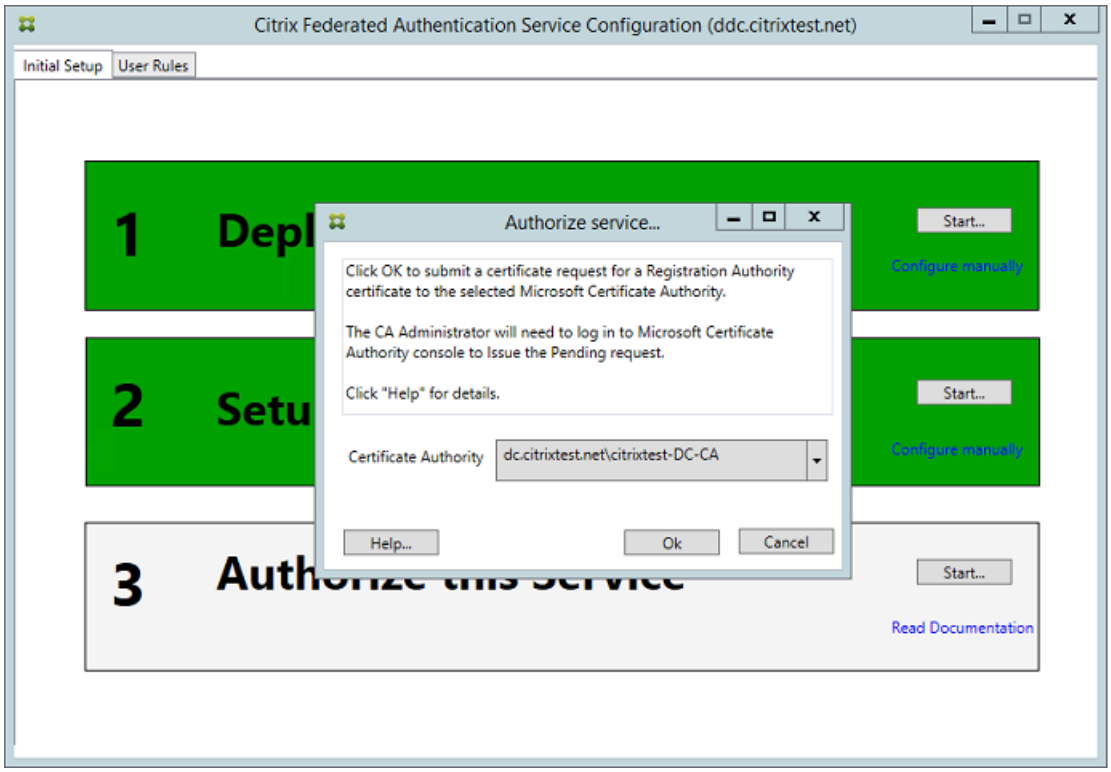
(También se pueden publicar plantillas de certificado mediante la consola de Entidad de certificación de Microsoft.)

© 1999-2017 Citrix Systems, Inc. All rights reserved.



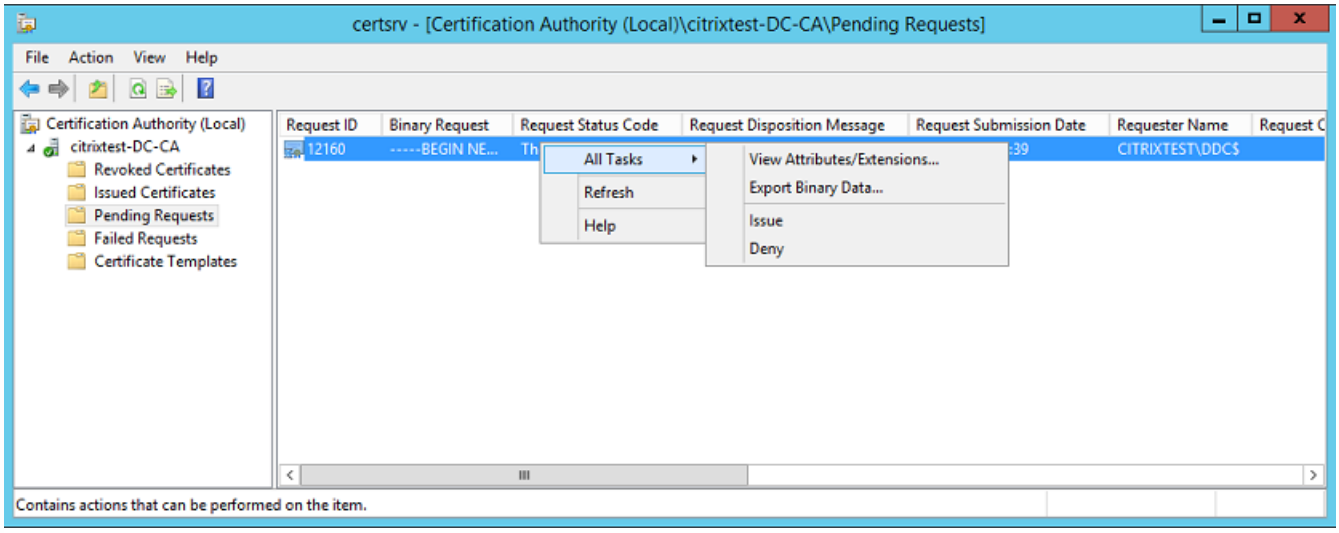
Autorización del Servicio de autenticación federada

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.

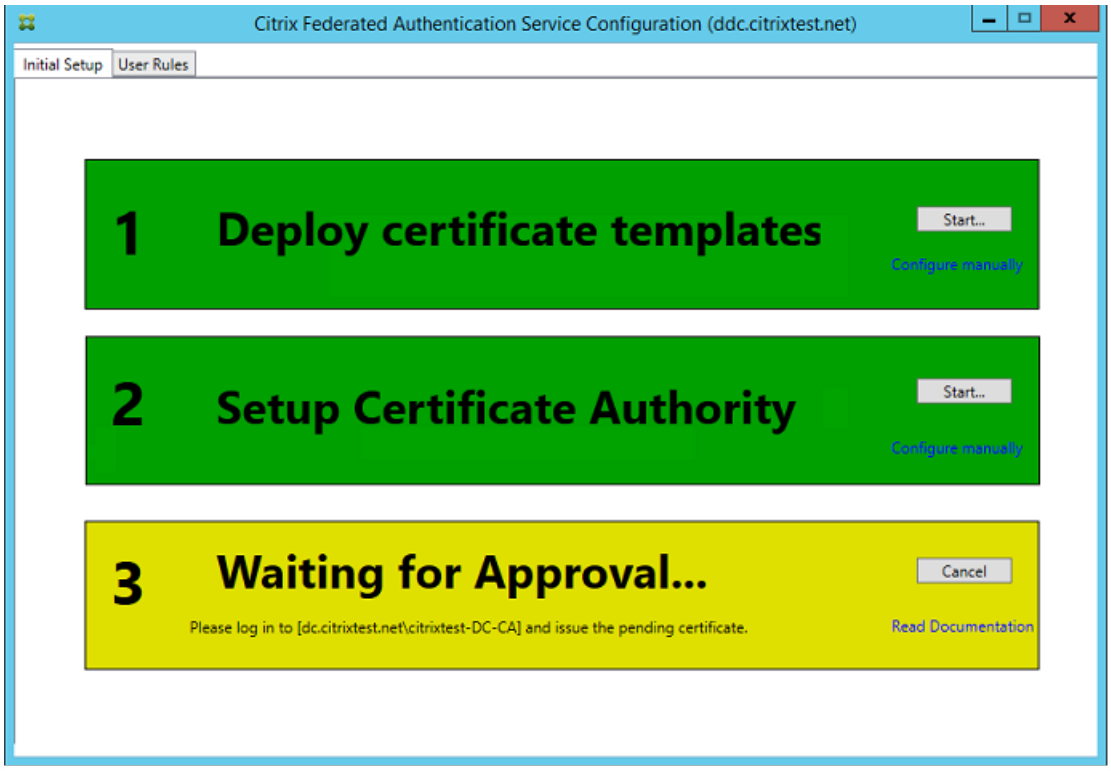


Después de enviarse la solicitud, aparecerá en la lista **Solicitudes pendientes** de la consola de la entidad de certificación de Microsoft. El administrador de la entidad de certificación debe elegir entre **Emitir** o **Rechazar** la solicitud para que la configuración del Servicio de autenticación federada pueda continuar. Tenga en cuenta que la solicitud de autorización aparece como una **Solicitud pendiente** desde la cuenta de máquina de FAS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

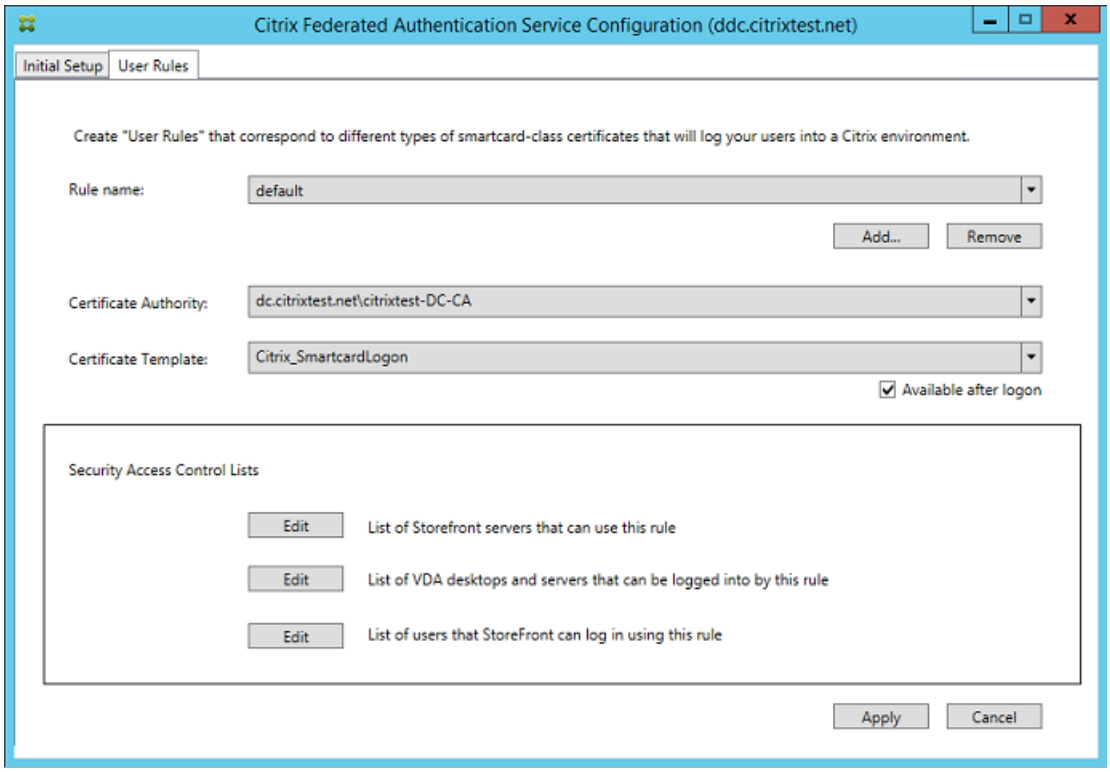


Configuración de reglas de usuario

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



Campos:

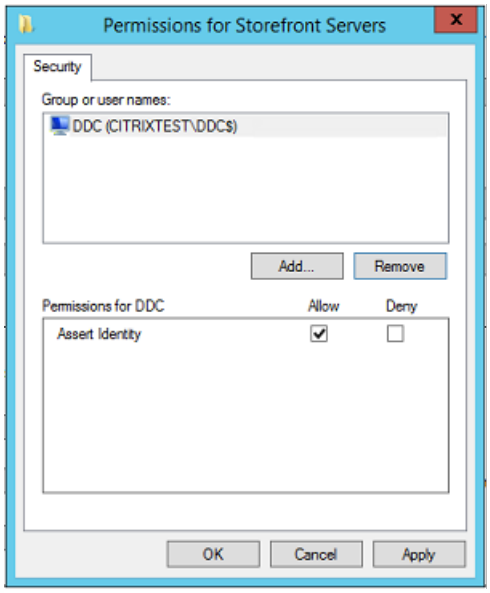
Certificate Authority and Certificate Template. La plantilla de certificado y la entidad de certificación que se van a usar para emitir certificados de usuario. Esta debe ser la plantilla Citrix_SmartcardLogon, o una copia modificada de ella, en una de las entidades de certificación donde esté publicada 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.

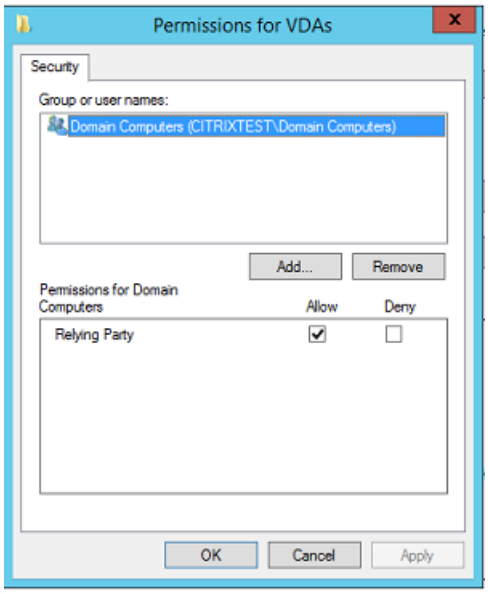
In-Session Certificates. La casilla **Available after logon** controla si un certificado puede usarse también como certificado de la sesión. Si no se marca la casilla, el certificado se usará solo para el inicio o la reconexión de la sesión, y el usuario no tendrá acceso al certificado después de autenticarse.

List of StoreFront servers that can use this rule. La lista de máquinas de servidor StoreFront de confianza que están autorizadas a solicitar certificados para el inicio o la reconexión de sesiones de usuarios. Tenga en cuenta que este parámetro es fundamental para la seguridad y es necesario configurarlo muy cuidadosamente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

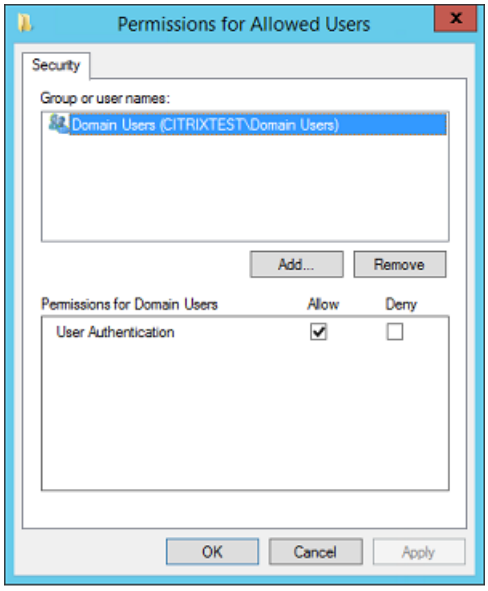


List of VDA desktops and servers that can be logged into by this rule. La lista de las máquinas VDA donde los usuarios pueden iniciar sesiones mediante el sistema del Servicio de autenticación federada.



List of users that StoreFront can log in using this rule. Lista de los usuarios para los que se pueden emitir certificados a través del Servicio de autenticación federada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. Para ello, haga clic en **Agregar** para que haga referencia a la nueva plantilla de certificado.

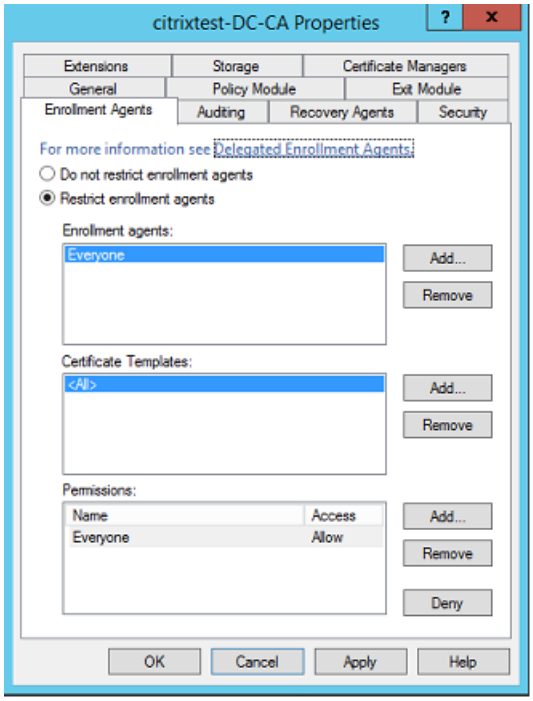
Consideraciones sobre seguridad

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.

© 1999-2017 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, se recomienda impedir que el Servicio de autenticación federada emita certificados para los usuarios incluidos en un grupo de Administración o de Usuarios protegidos.

Configuración de una lista de control de acceso

Como se describe en la sección de Configuración de 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 estos usuarios. Esto es adicional a las funciones de seguridad estándar de la entidad de certificación o de Active Directory que configure.

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.

Supervisión del registro de eventos

El Servicio de autenticación federada y el VDA escriben información en el registro de eventos de Windows. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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).

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:

```
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

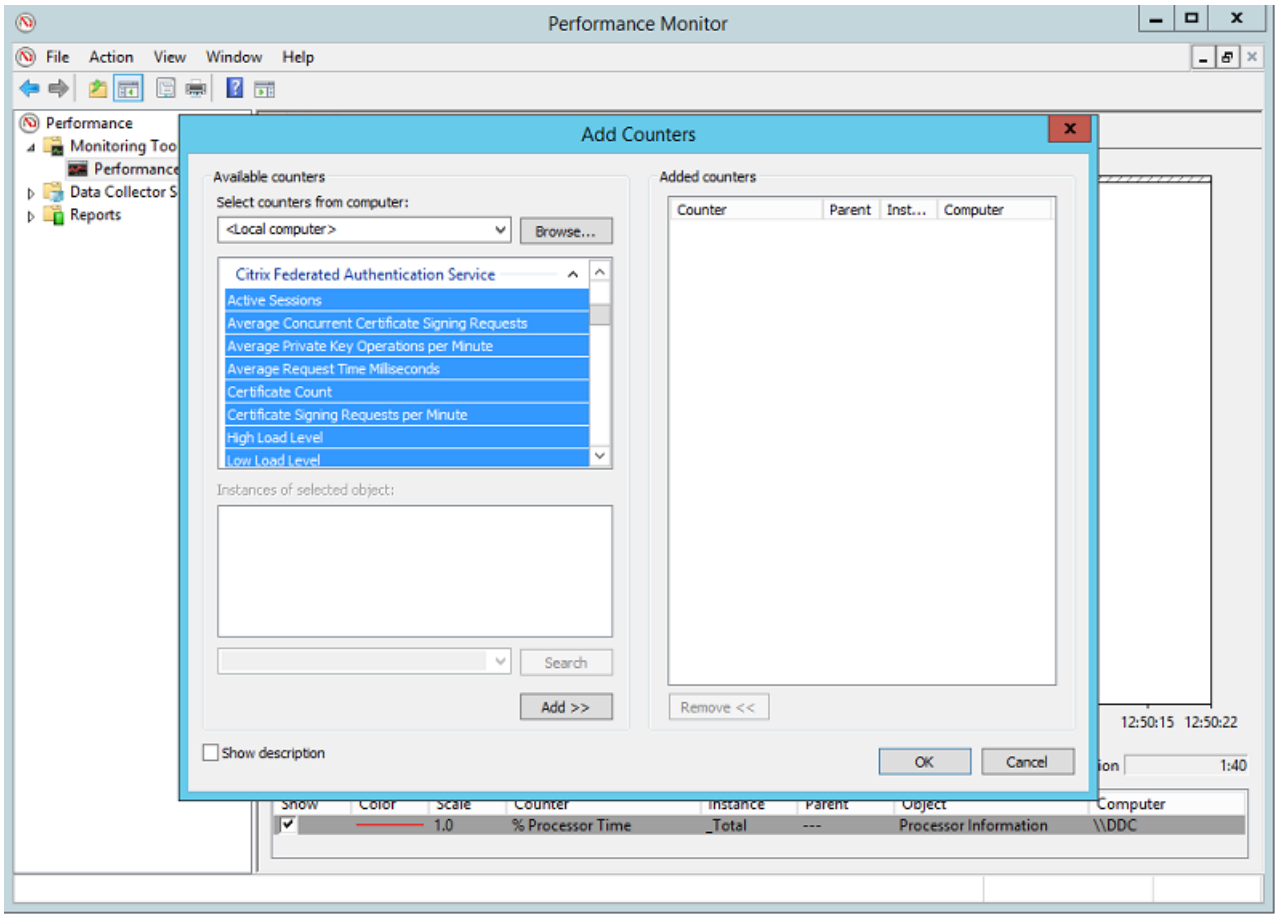
*-FasRule	Administra las reglas de usuario configuradas en el Servicio de autenticación federada.
*-FasUserCertificate	Muestra y administra certificados almacenados en caché por el Servicio de autenticación federada.

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.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
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 de "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.

Administration events (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}]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[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}]

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}]

Creación de 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})

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[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}].

Actuando 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.
[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}].

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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}].

Inicio de 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}]
[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}]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[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.

Códigos de solicitud y generación de certificados [Servicio de autenticación federada]

[Origen del evento: Citrix.TrustFabric]

Estos eventos de bajo nivel se registran cuando el Servicio de autenticación federada realiza operaciones criptográficas de bajo nivel.

Códigos de registro
[S0001]TrustArea::TrustArea: Installed certificate chain
[S0002]TrustArea::Join: Callback has authorized an untrusted certificate
[S0003]TrustArea::Join: Joining to a trusted server
[S0004]TrustArea::Maintain: Renewed certificate
[S0005]TrustArea::Maintain: Retrieved new certificate chain

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[S0006]TrustArea::Export: Exporting private key
[S0007]TrustArea::Import: Importing Trust Area
[S0008]TrustArea::Leave: Leaving Trust Area
[S0009]TrustArea::SecurityDescriptor: Setting Security Descriptor
[S0010]CertificateVerification: Installing new trusted certificate
[S0011]CertificateVerification: Uninstalling expired trusted certificate
[S0012]TrustFabricHttpClient: Attempting single sign-on to {0}
[S0013]TrustFabricHttpClient: Explicit credentials entered for {0}
[S0014]Pkcs10Request::Create: Created PKCS10 request
[S0015]Pkcs10Request::Renew: Created PKCS10 request
[S0016]PrivateKey::Create
[S0017]PrivateKey::Delete
[S0018]TrustArea::TrustArea: Waiting for Approval
[S0019]TrustArea::Join: Delayed Join
[S0020]TrustArea::Join: Delayed Join
[S0021]TrustArea::Maintain: Installed certificate chain

Códigos de registro
[S0101]TrustAreaServer::Create root certificate

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[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
[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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Información relacionada

- Las implementaciones más comunes del servicio FAS se resumen en el artículo Vista general de las arquitecturas del Servicio de autenticación federada.
- En el artículo Administración y configuración del Servicio de autenticación federada, se indican otros artículos de procedimientos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vista general de las arquitecturas de Servicios de autenticación federada

Dec 05, 2017

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.En este documento, se describen 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 XenApp o XenDesktop.

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 de Windows 10 a Azure AD

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.

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.Para ello, se usan 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 Citrix XenApp o un Virtual Delivery Agent (VDA) de XenDesktop, 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.

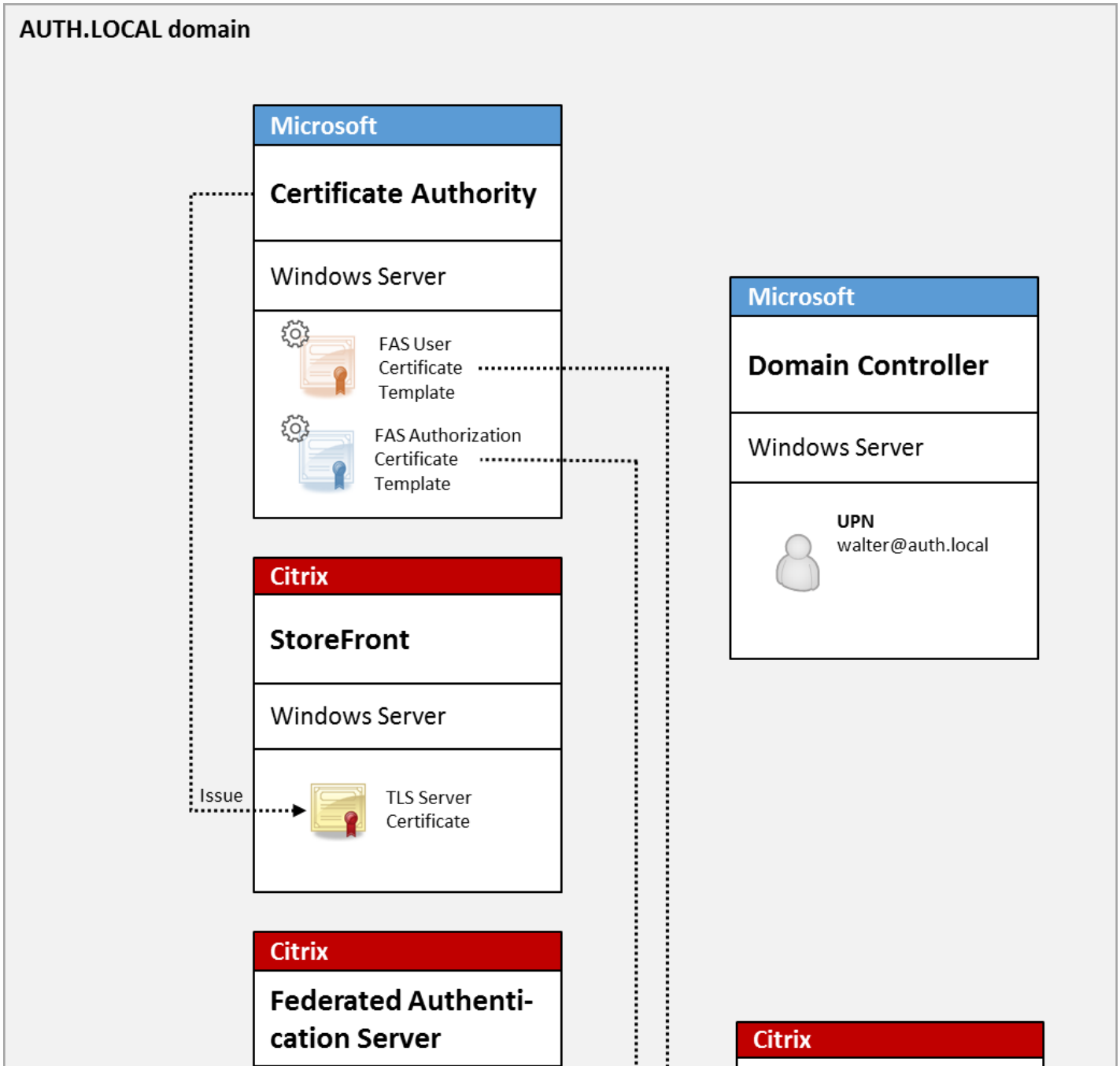
Esto permite la autenticación de Windows sin diálogos para introducir las credenciales de usuario o el PIN de tarjeta

© 1999-2017 Citrix Systems, Inc. All rights reserved.

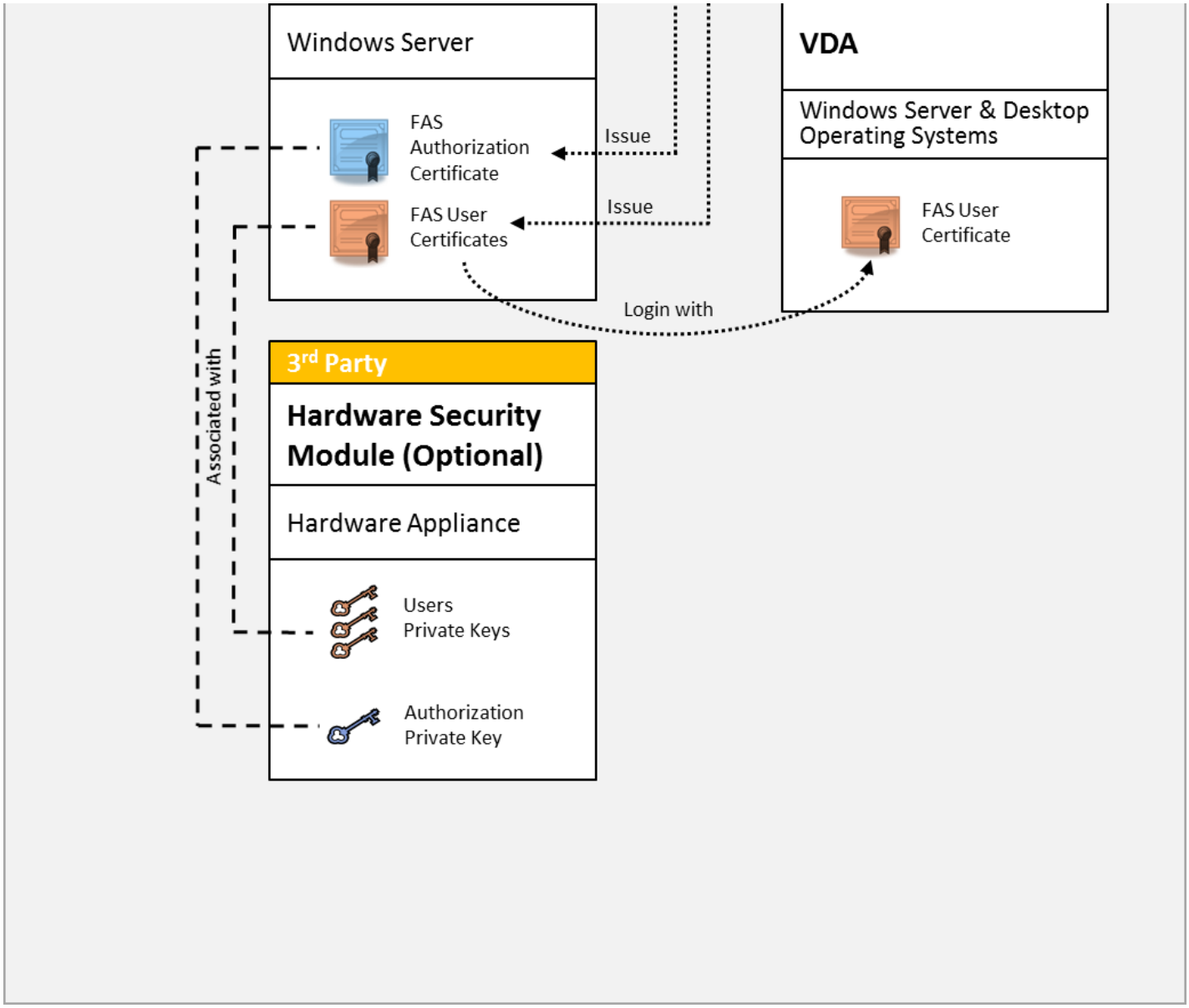
inteligente, y sin tener que usar la funcionalidad de "administración de contraseñas guardadas", tales como el servicio Single Sign-on Service.Puede utilizarse para reemplazar las funciones de inicio de sesión que ofrezca la Delegación limitada de Kerberos, disponible en versiones anteriores de XenApp.

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 certificados 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



El entorno de XenApp o XenDesktop 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:

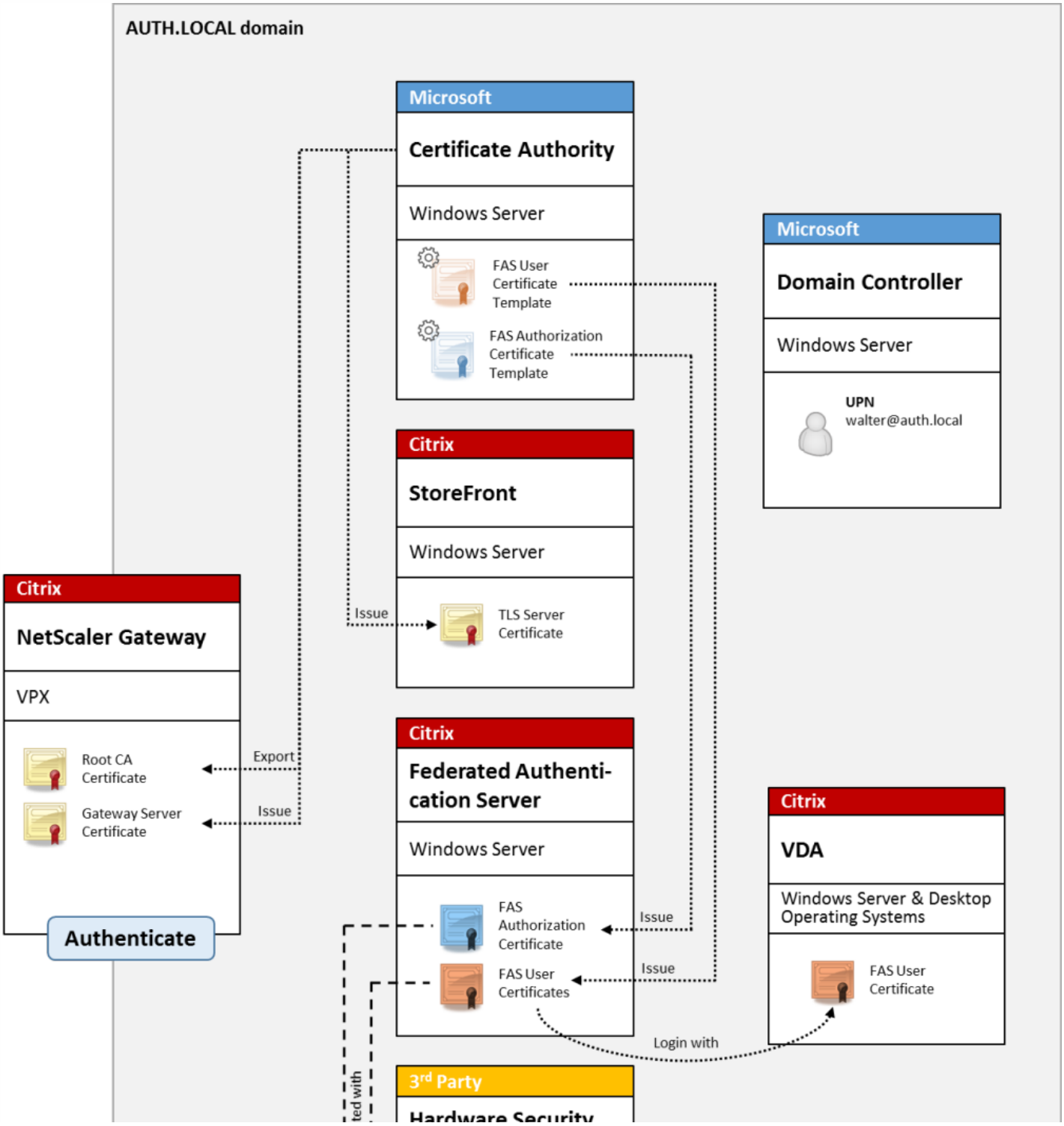
- Las claves se pueden almacenar en un módulo de seguridad de hardware (HSM) o en un módulo de plataforma de confianza (TPM) integrado.Para obtener más información, consulte el artículo Protección de claves privadas para el Servicio de autenticación federada.
- El artículo de Servicio de autenticación federada describe cómo instalar y configurar el FAS.

Implementación de NetScaler Gateway

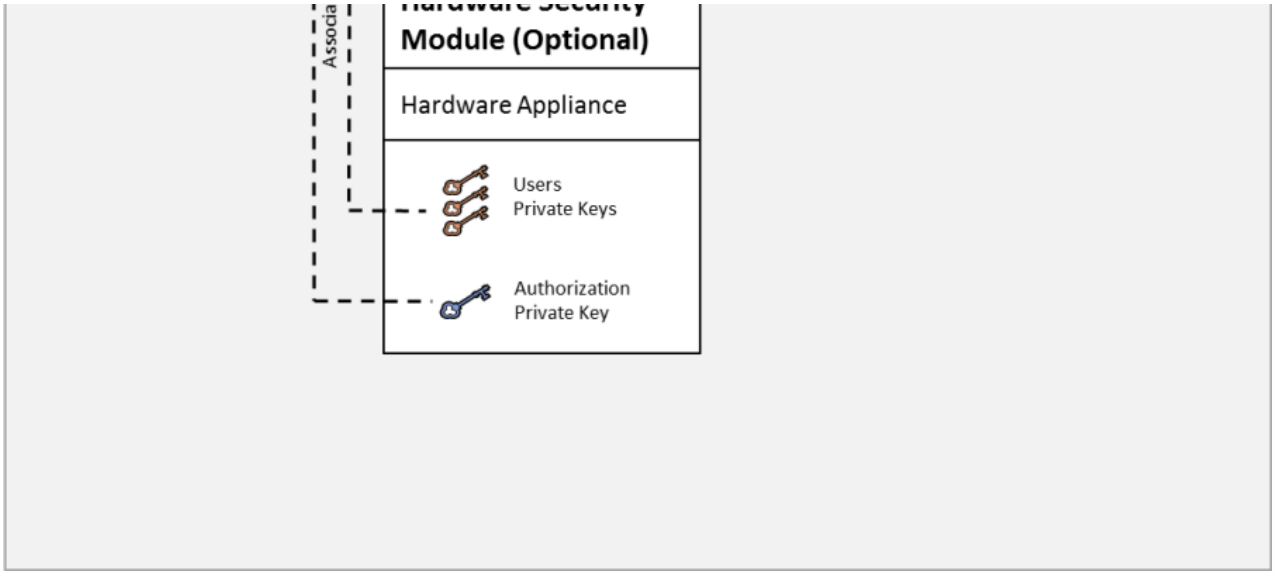
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



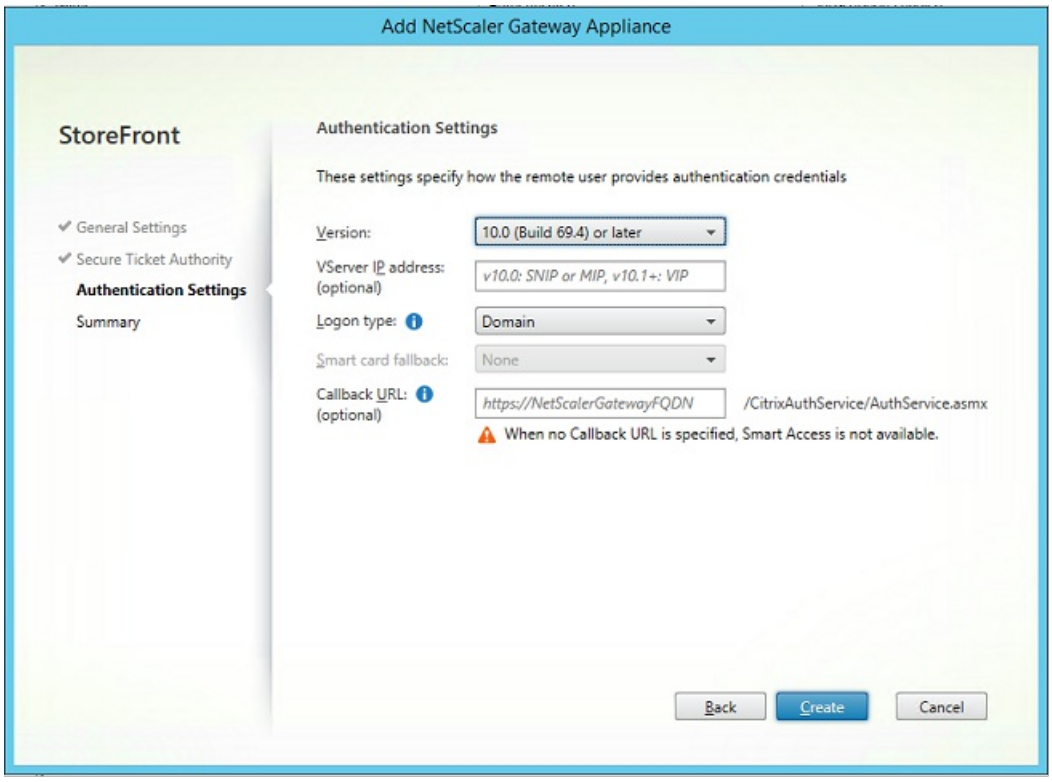
© 1999-2017 Citrix Systems, Inc. All rights reserved.



El entorno de XenApp o XenDesktop 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 esto puede usarse para autenticar el servidor NetScaler en esta implementación.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

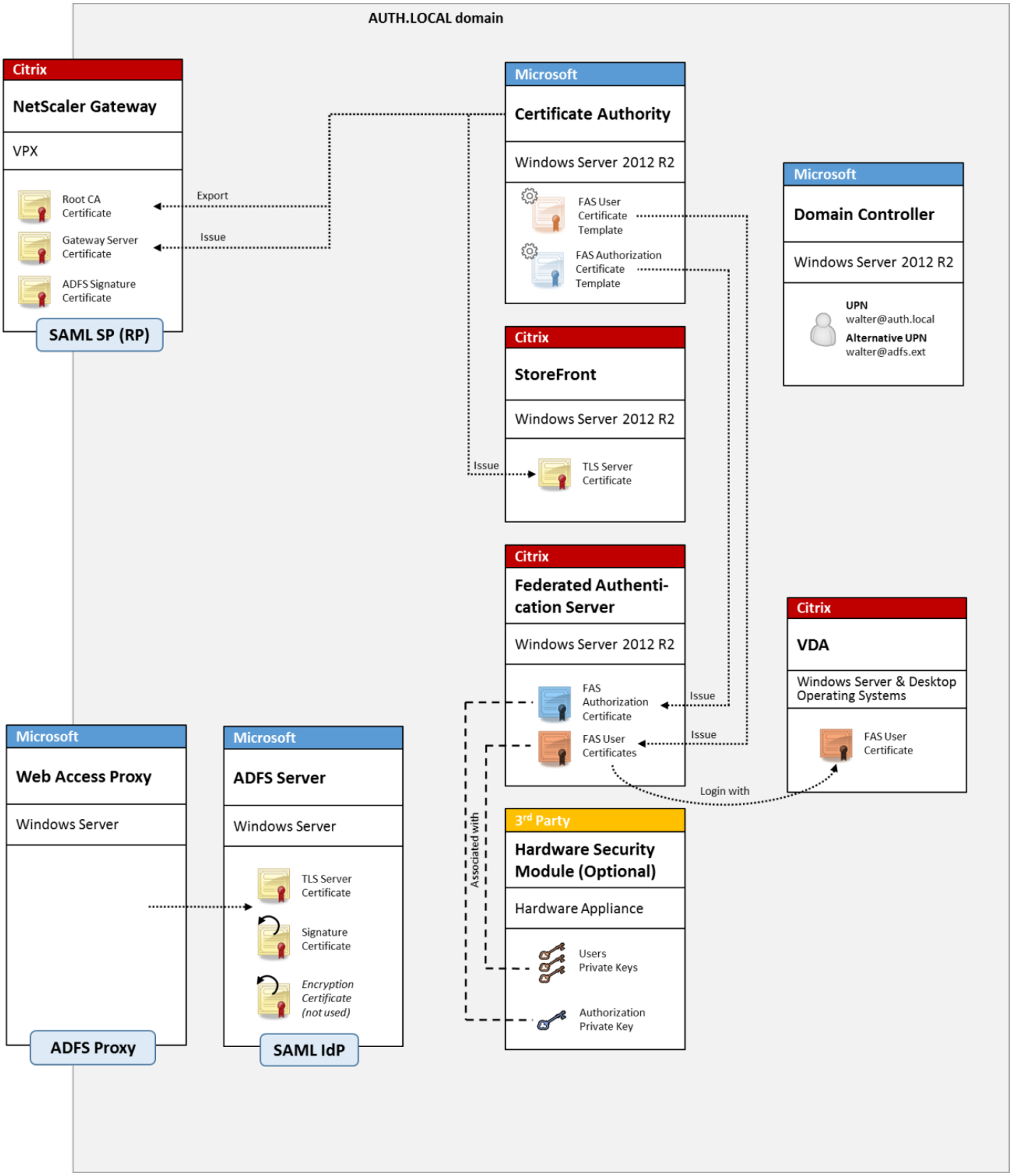
Información relacionada:

- Para configurar NetScaler Gateway, consulte “Cómo configurar NetScaler Gateway 10.5 para usarlo con StoreFront 3.6 y XenDesktop 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.Esto 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).

© 1999-2017 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:

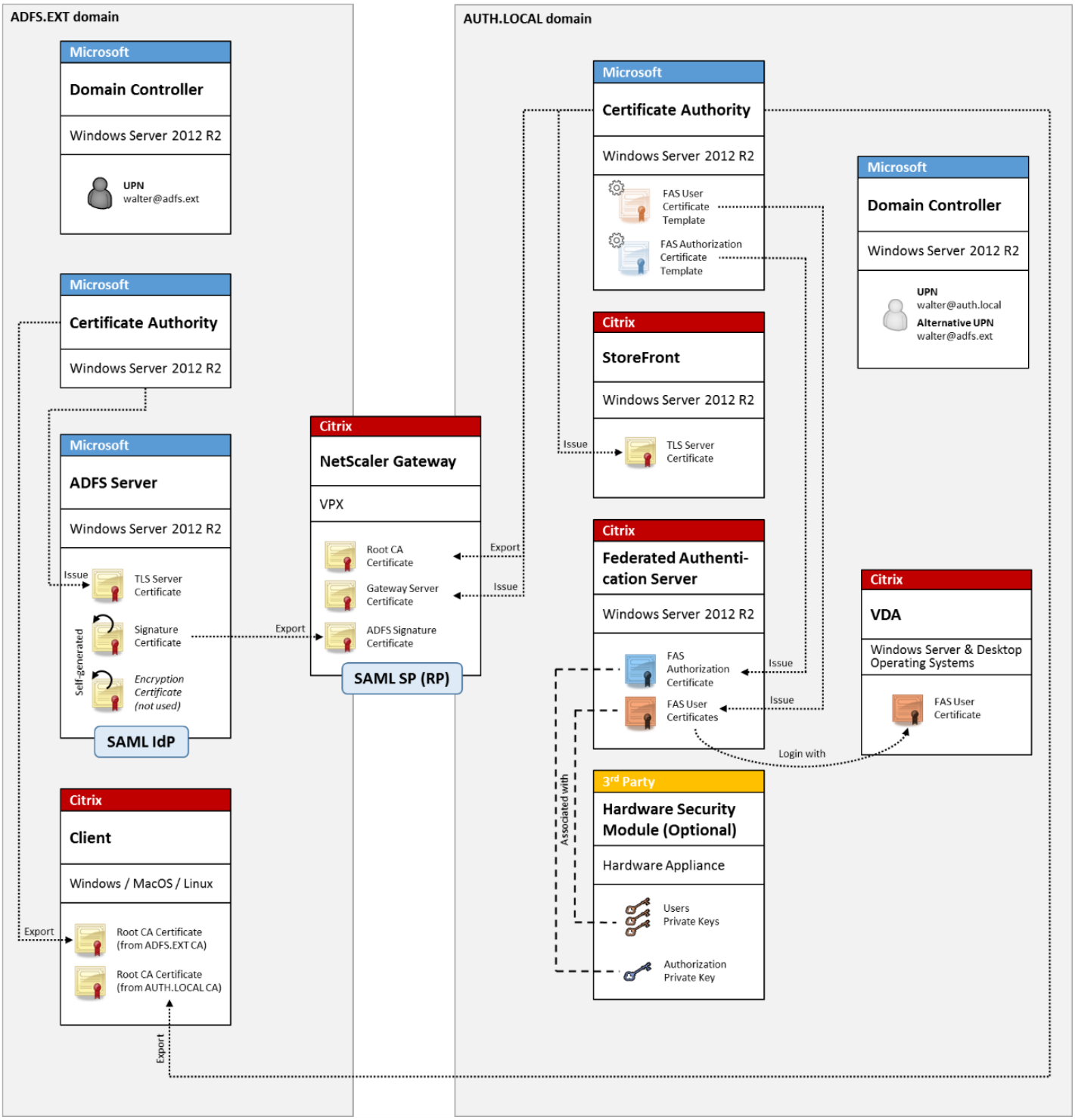
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- El artículo Implementación ADFS del servicio de autenticación federada contiene información al respecto.
- El artículo Servicio de autenticación federada describe cómo instalar y configurar el FAS.
- La sección Implementación de NetScaler Gateway en este artículo contiene información acerca de la configuración.

Asignación de cuentas B2B

Si dos empresas desean usar los sistemas informáticos de la otra, una opción común es configurar un servidor ADFS (Servicio de federación de Active Directory) con una relación de confianza. Esto 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 asigna automáticamente esto a una "cuenta sombra" en el entorno de AD de la otra empresa.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Información relacionada:

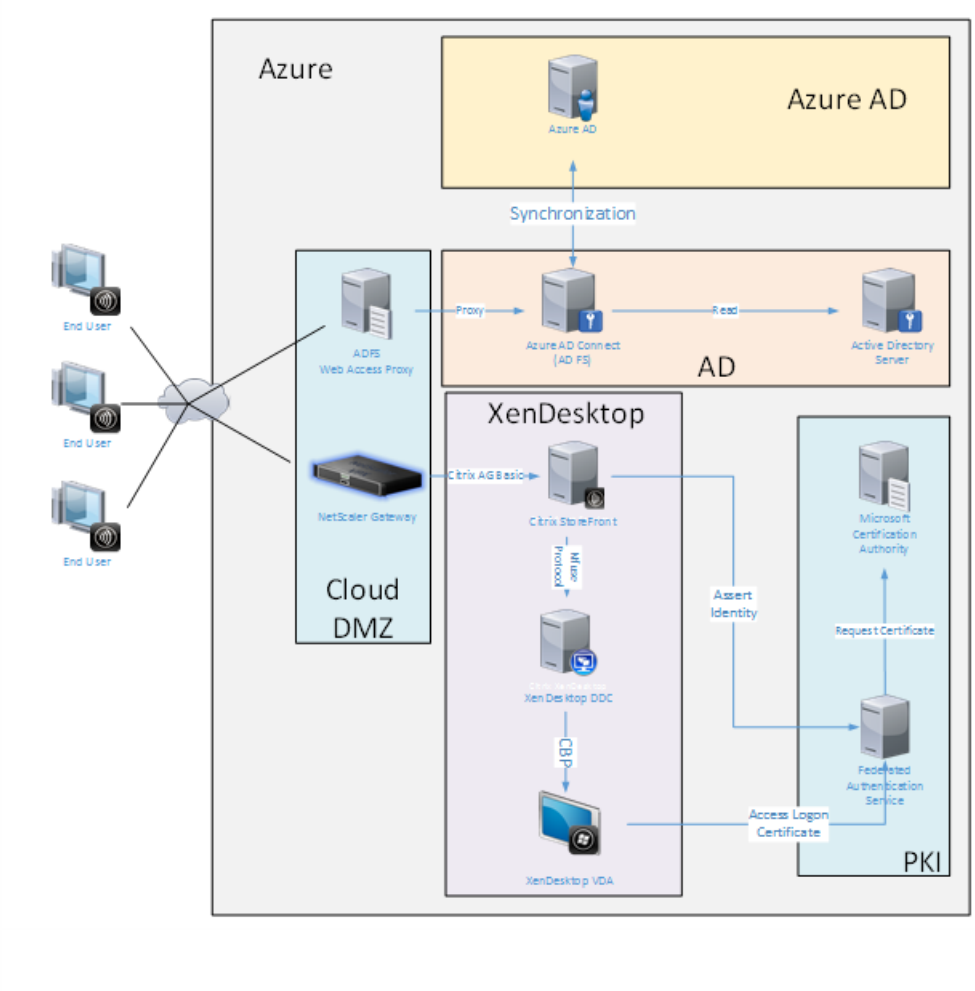
- El artículo Servicio de autenticación federada describe cómo instalar y configurar el FAS.

Unión de Windows 10 a Azure AD

Windows 10 introdujo el concepto de "Unión a Azure AD", que es conceptualmente similar a la unión a un dominio Windows

© 1999-2017 Citrix Systems, Inc. All rights reserved.

tradicional, solo que destinado a escenarios 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 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:

- El artículo Servicio de autenticación federada describe cómo instalar y configurar el FAS.
- El artículo Integración de Azure AD y el servicio FAS de autenticación federada contiene información al respecto.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Implementación ADFS del servicio de autenticación federada

Dec 05, 2017

Introducción

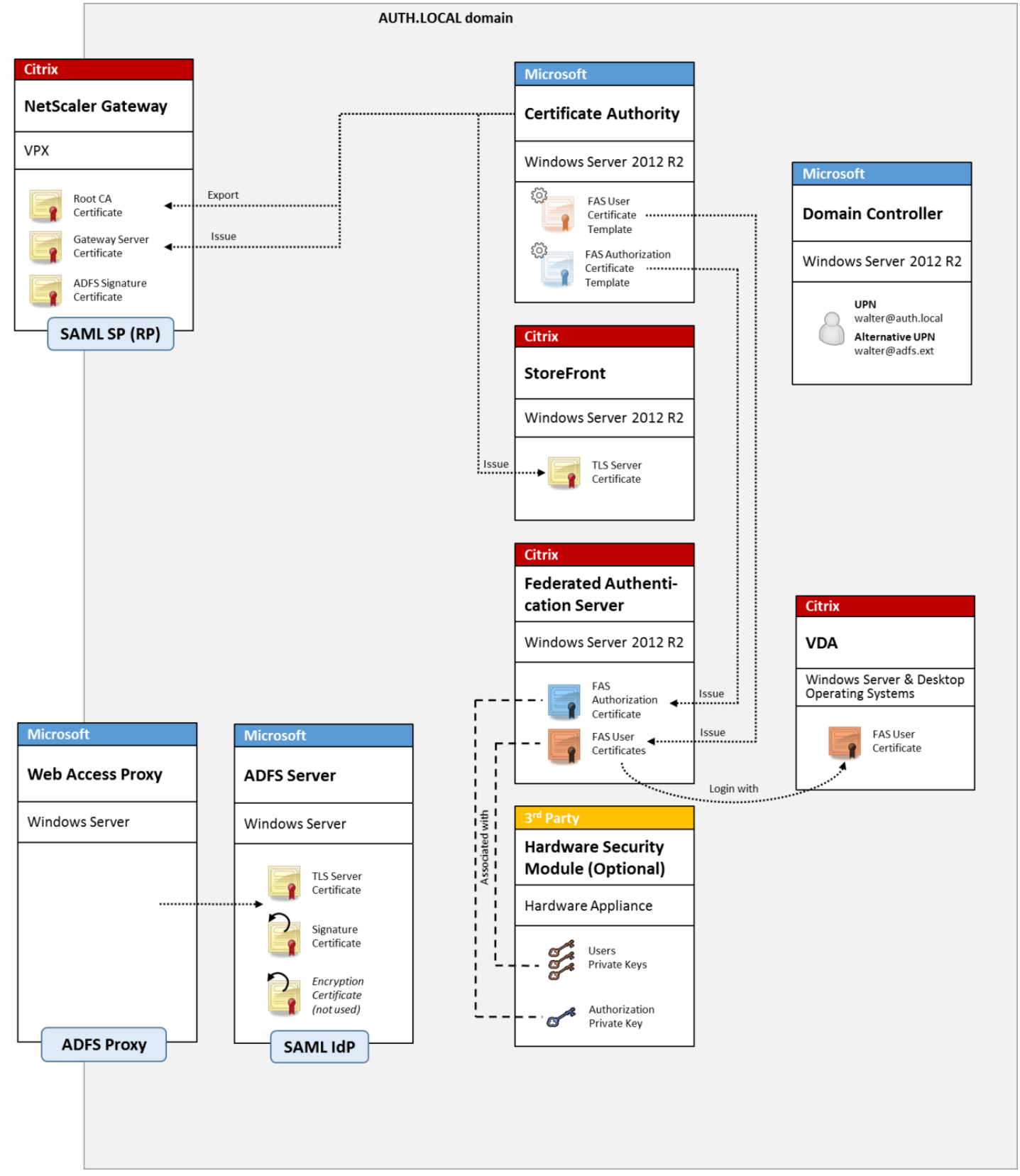
Este documento describe cómo integrar un entorno de Citrix con Microsoft ADFS.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Descripción general de SAML

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 consta de los siguientes elementos:

Dirección URL de redireccionamiento [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:// con el formato: https://adfs.miEmpresa.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]

El ID de entidad (EntityID) es un identificador único que NetScaler incluye en los datos de POST enviados a ADFS.Esto 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 [dirección 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 el EntityID.Esto es normalmente una dirección https:// en el servidor NetScaler original con el formato: https://ns.miEmpresa.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 SAM usando su clave privada.Para validar la firma, NetScaler debe estar configurado para comprobar esas firmas con la ayuda de una clave pública incluida 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 representa una sesión conectada.

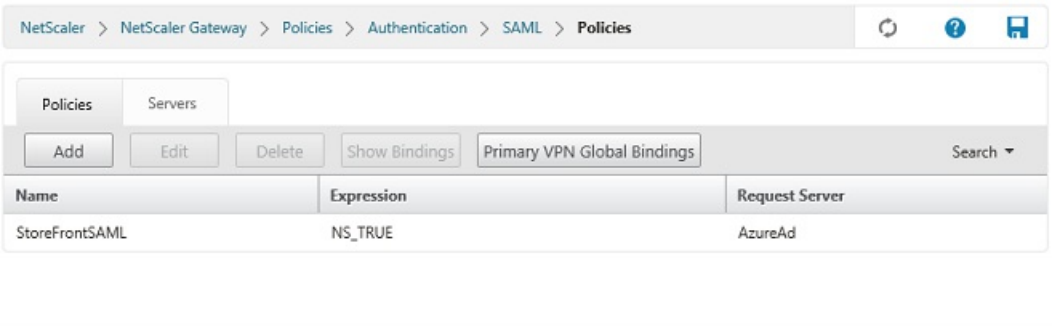
Esta es una característica optativa, no es necesario que esté configurada. Suele ser una dirección https:// con el formato https://adfs.mycompany.com/adfs/logout. (Tenga en cuenta que puede ser la misma que la dirección URL de inicio de sesión único.)

Configuración

La sección Implementación de NetScaler Gateway en el artículo Vista general de las arquitecturas de Servicios de autenticación federada describe cómo configurar NetScaler Gateway para gestionar opciones de autenticación LDAP

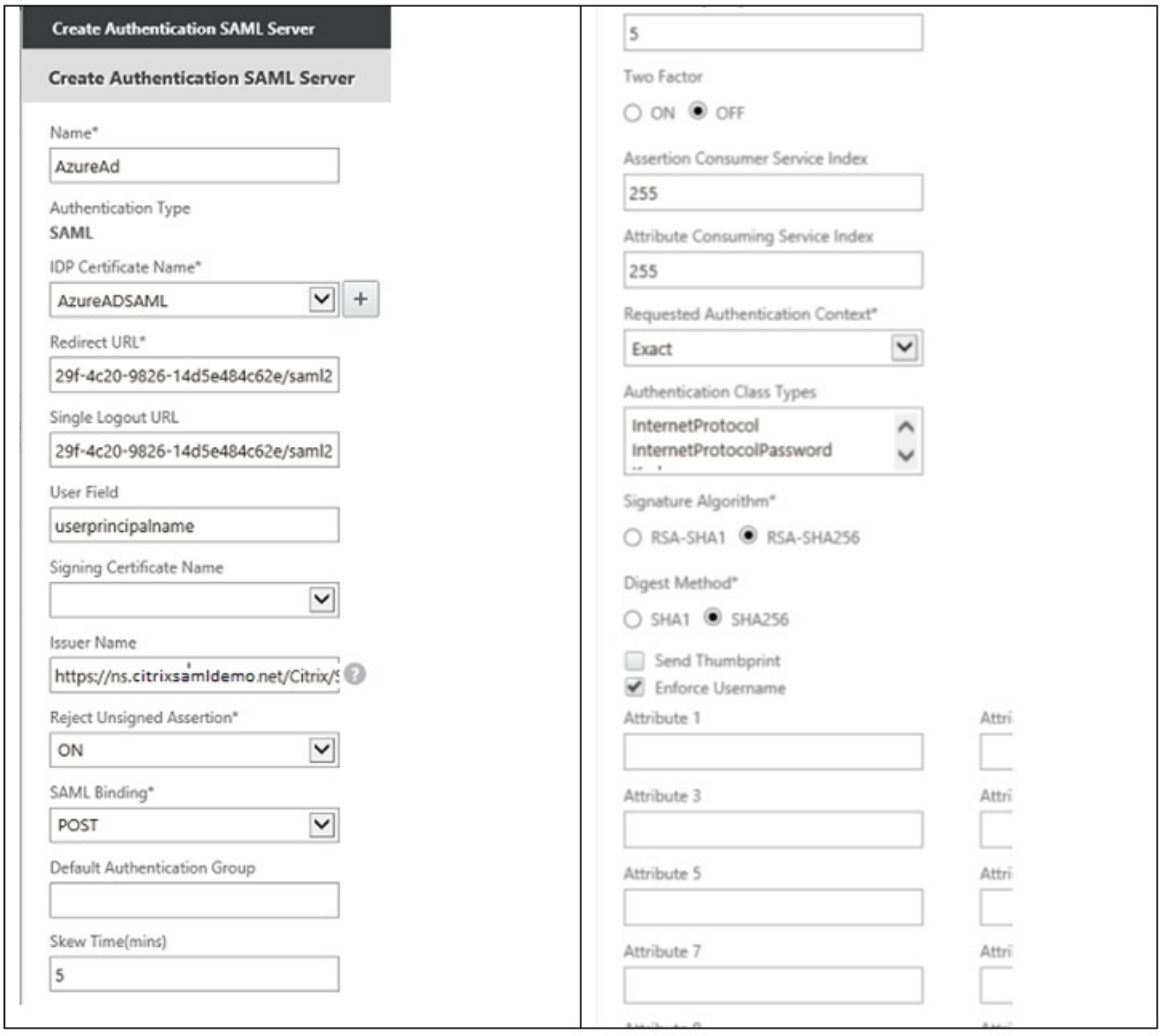
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, 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.



© 1999-2017 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 Vista general de las arquitecturas del Servicio de autenticación federada.
- En el artículo Administración y configuración del Servicio de autenticación federada, se indican otros artículos de procedimientos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Integración de Azure AD y el servicio FAS de autenticación federada

Dec 05, 2017

En este artículo:

- Introducción
- Arquitectura
- Crear una zona DNS
- Crear un servicio de nube
- Crear máquinas virtuales de Windows
- Configurar un DNS interno
- Configurar una dirección DNS externa
- Configurar grupos de seguridad
- Crear un certificado ADFS
- Configurar Azure AD
- Habilitar la función Unirse a Azure a AD
- Instalar XenApp o XenDesktop
- Configurar una nueva aplicación de Azure AD para inicios de sesión Single Sign-on en StoreFront
- Instalar y configurar NetScaler Gateway
- Configurar la dirección de StoreFront
- Habilitar el respaldo para la autenticación SAML
- Verificar el sistema de extremo a extremo
- Apéndice

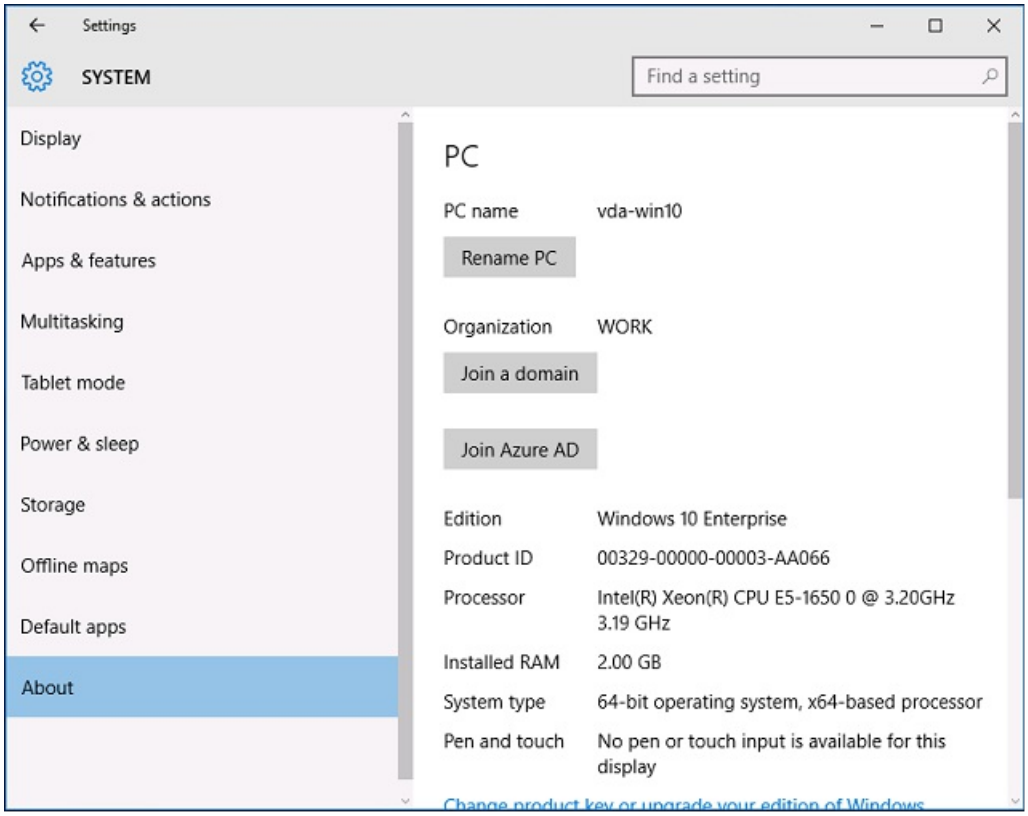
Introducción

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.

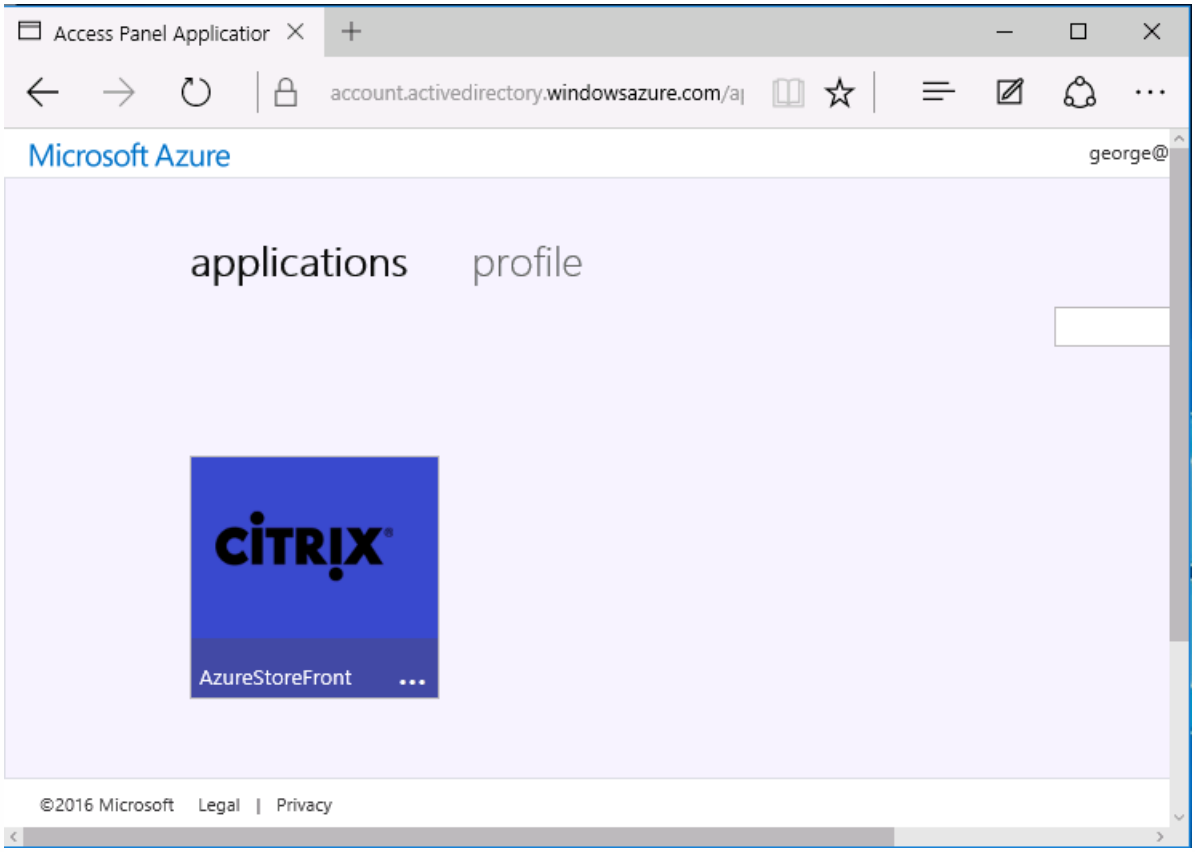
El ejemplo de implementación en este documento describe un sistema donde TI proporciona a los nuevos usuarios una dirección de correo electrónico de la empresa y un código de inscripción para sus portátiles Windows 10 personales.Los usuarios acceden a este código mediante la opción Sistema > Acerca de > Unirse a Azure AD en el panel **Configuración**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

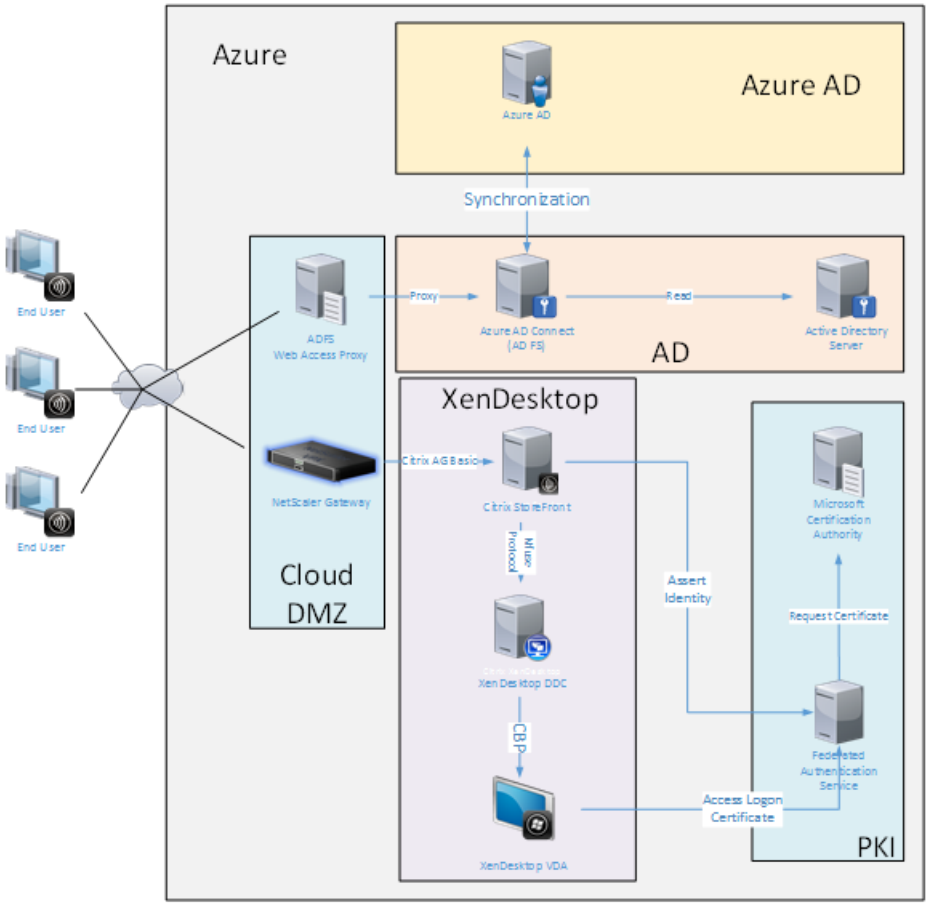


Arquitectura

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 razón para 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.

© 1999-2017 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.

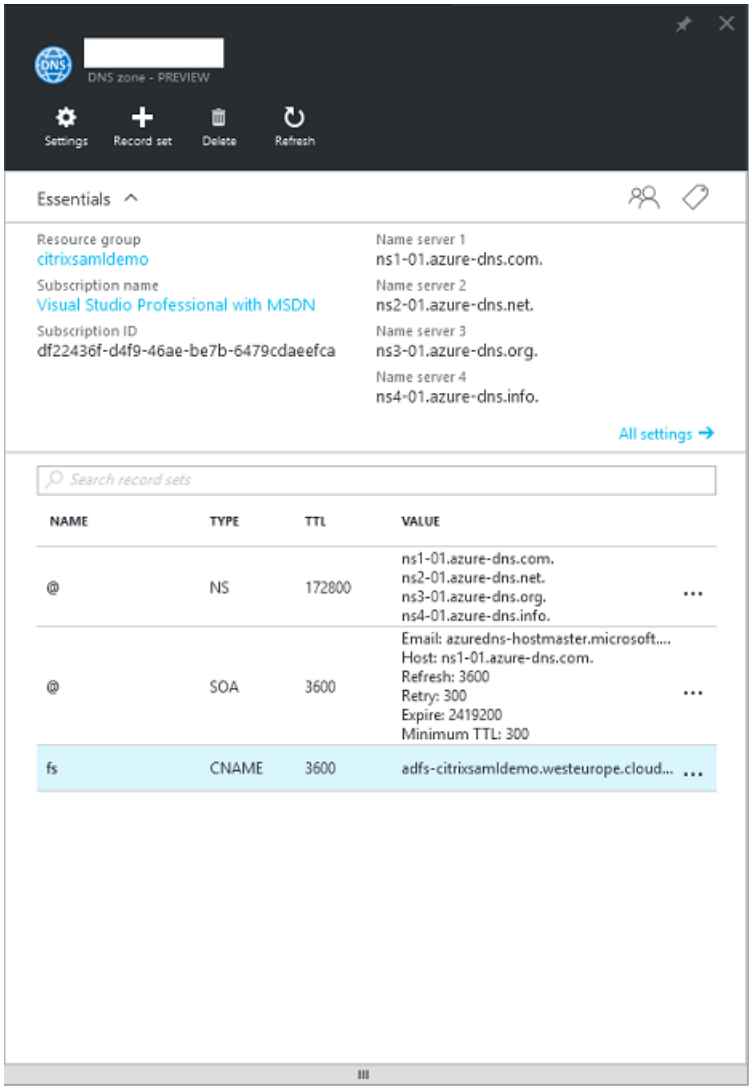
Cuando un usuario inicia una aplicación tradicional, el acceso tiene lugar usando aplicaciones publicadas de XenApp y XenDesktop.Los diferentes tipos de aplicaciones se intercalan a través de la página **Aplicaciones de Azure** del usuario con la ayuda de las funciones Single Sign-On de Microsoft Edge.Microsoft también proporciona aplicaciones de iOS y Android que pueden enumerar e iniciar aplicaciones de Azure.

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".

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La consola muestra los nombres de los servidores DNS de Azure.Estos deben constar en las entradas 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.

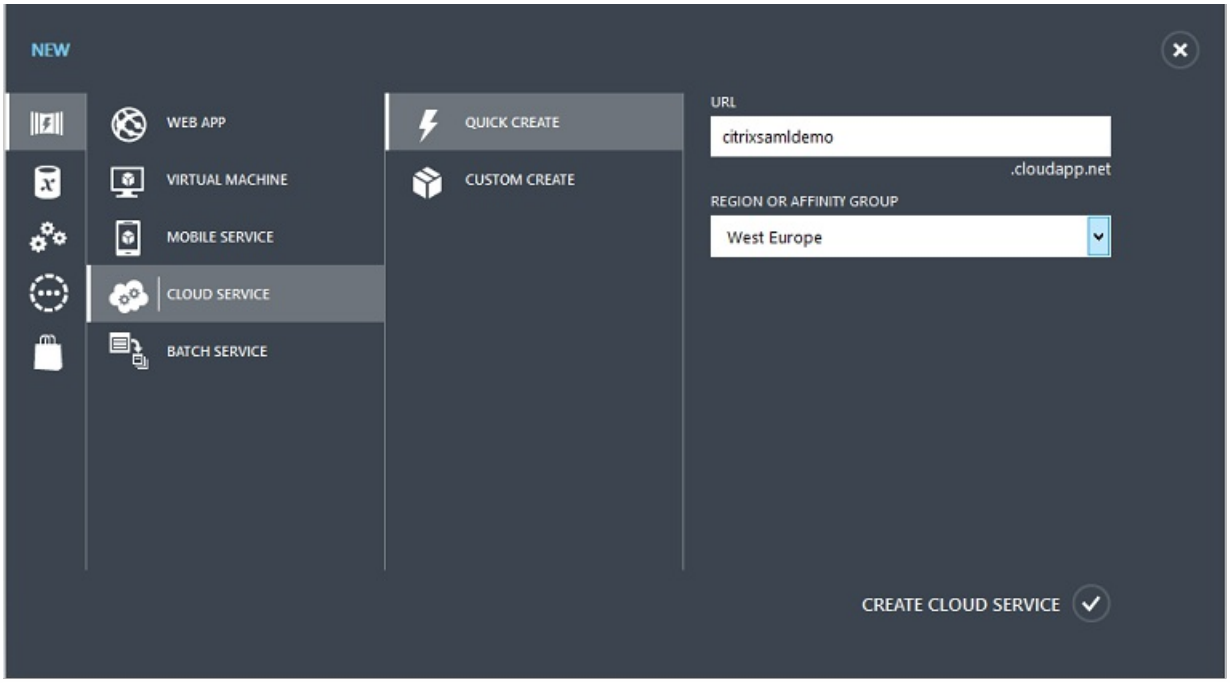
Los sufijos de ambas direcciones DNS interna y externa coincidirán en esta implementación.El dominio es citrixsamldemo.net y se usa DNS dividido (10.0.0.* internamente).

Agregue una entrada “fs.citrixsamldemo.net” que haga referencia al servidor Proxy de aplicación Web.Este es el Servicio de federación de 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".

© 1999-2017 Citrix Systems, Inc. All rights reserved.

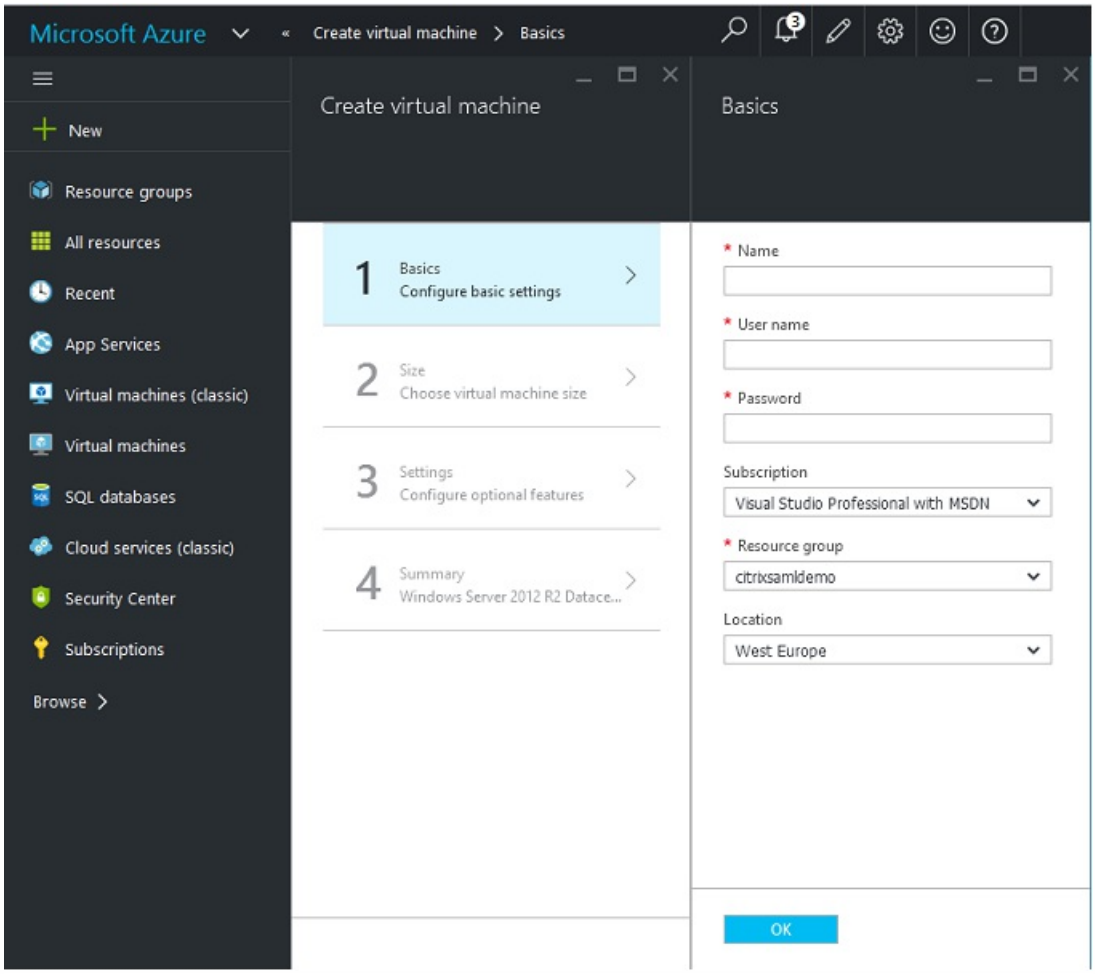


Crear máquinas virtuales de Windows

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)
- Citrix XenDesktop Delivery Controller (ddc)
- Citrix XenDesktop Virtual Delivery Agent (vda)

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Controlador de dominio

- Agregue los roles de **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 **Azure DNS settings**. (Para obtener más información, consulte el Apéndice en este documento.)

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.

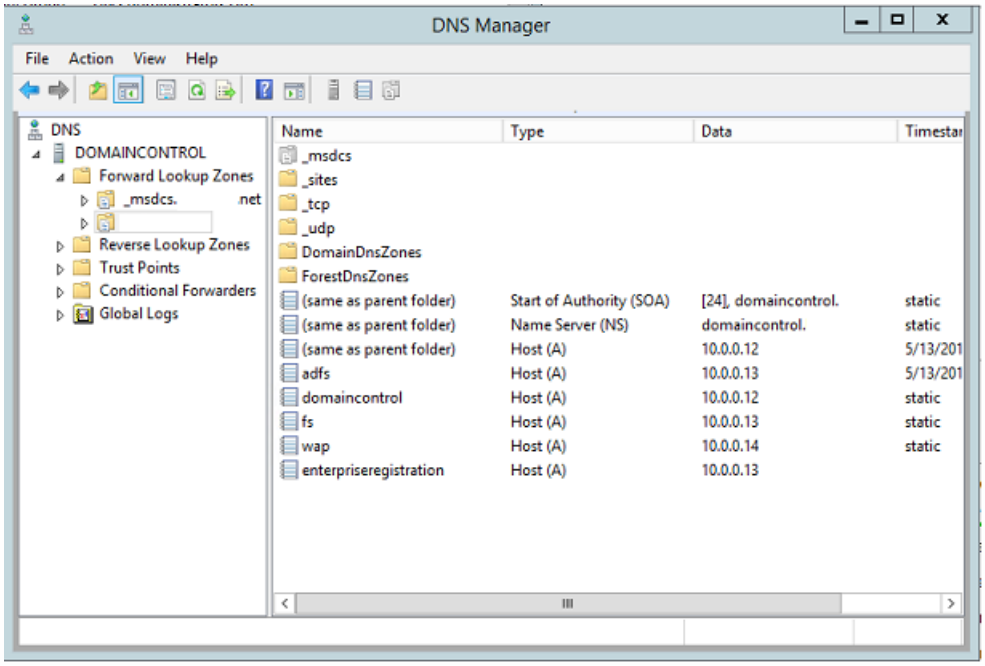
Delivery Controller de XenDesktop y VDA

- Instale XenApp o XenDesktop Delivery Controller y VDA en los otros dos servidores Windows unidos a citrixsamldemo.

Configurar un DNS interno

© 1999-2017 Citrix Systems, Inc. All rights reserved.

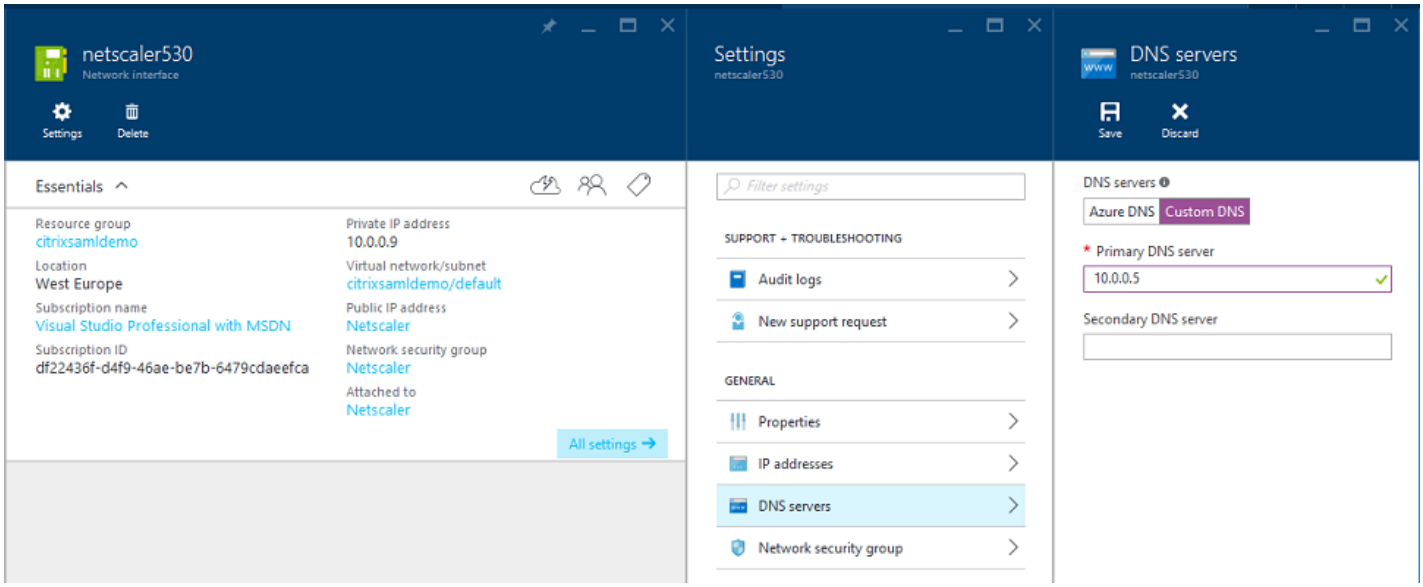
Después de que el controlador de dominio está instalado, configure el servidor DNS para controlar la vista de citrixsamldemo.net y actuar como un reenviador a un servidor DNS externo (por ejemplo: 8.8.8.8).



Agregue un registro estático para:

- wap.citrixsamldemo.net [la VM de proxy de aplicaciones Web no estará unidad a un dominio]
- fs.citrixsamldemo.net [dirección de servidor de federación interno]
- enterpriseregistration.citrixsaml.net [lo mismo 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.

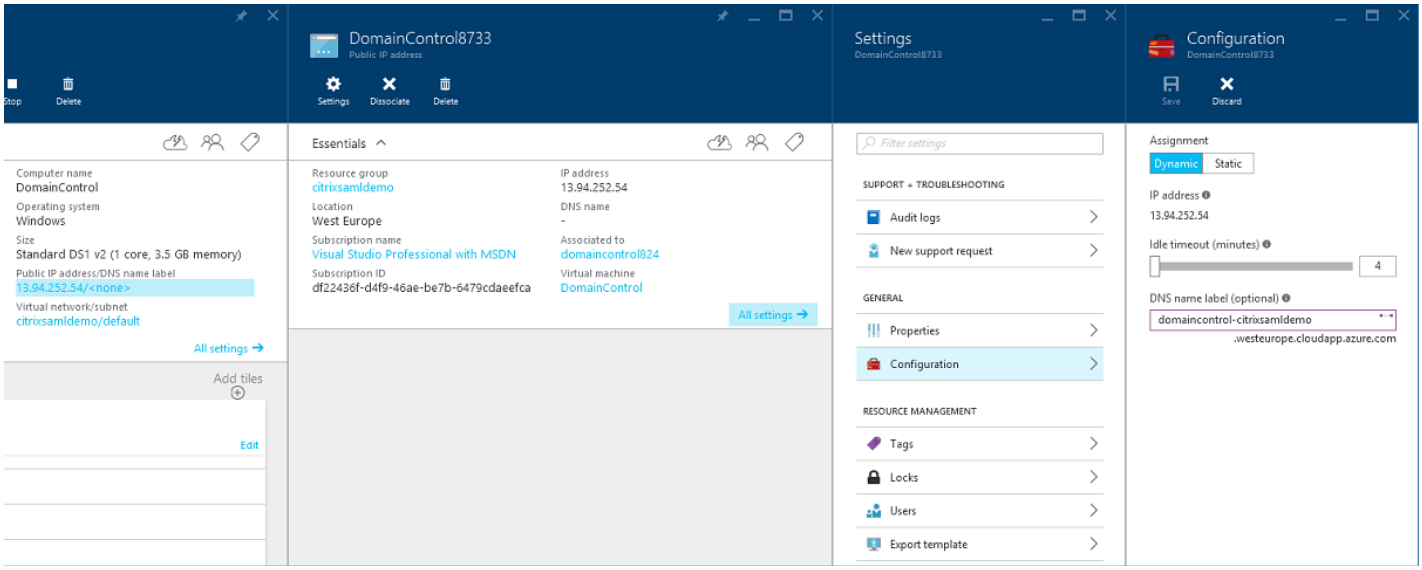


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 se inicia cada VM de manera predeterminada.



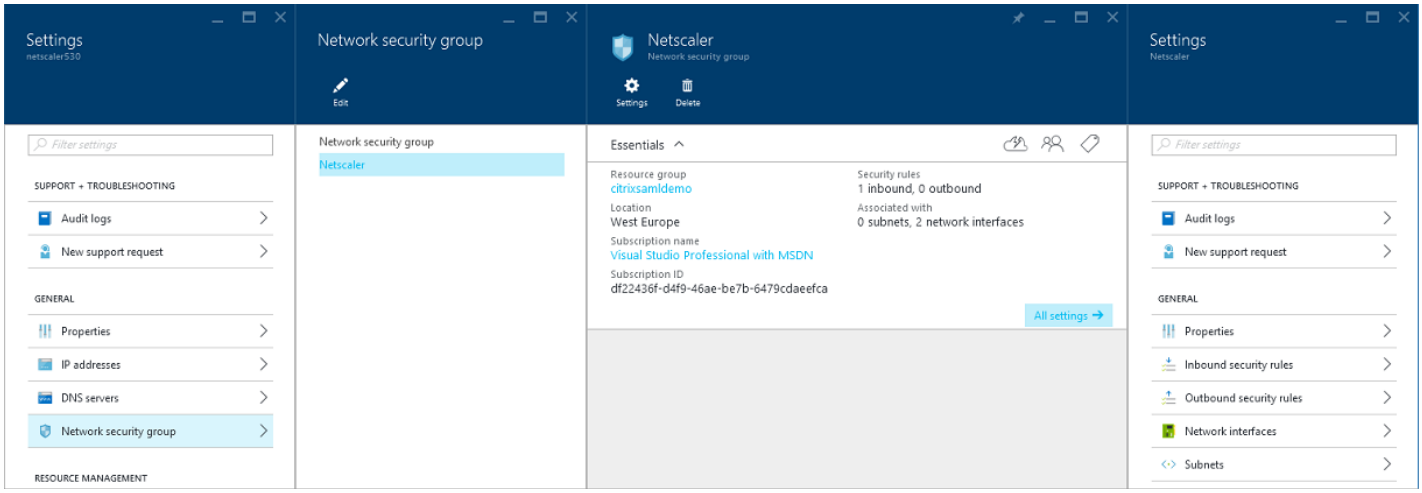
Este ejemplo asigna una dirección DNS de domaincontrol-citrixsamldemo.westeurope.cloudapp.azure.com al controlador de dominio.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



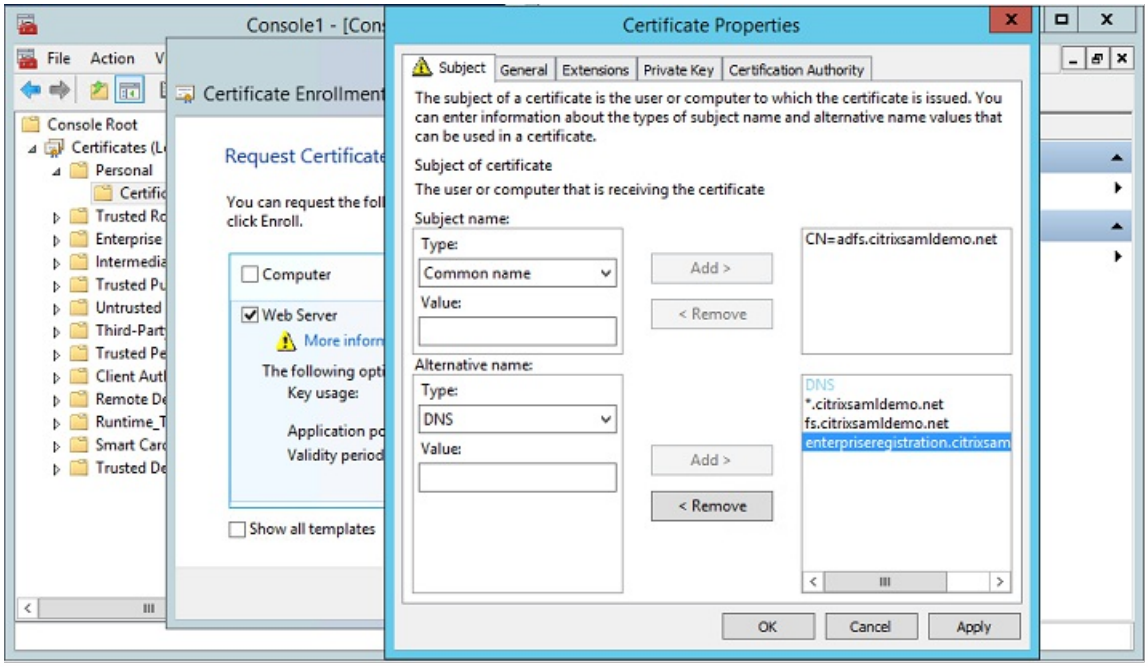
Crear un certificado ADFS

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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



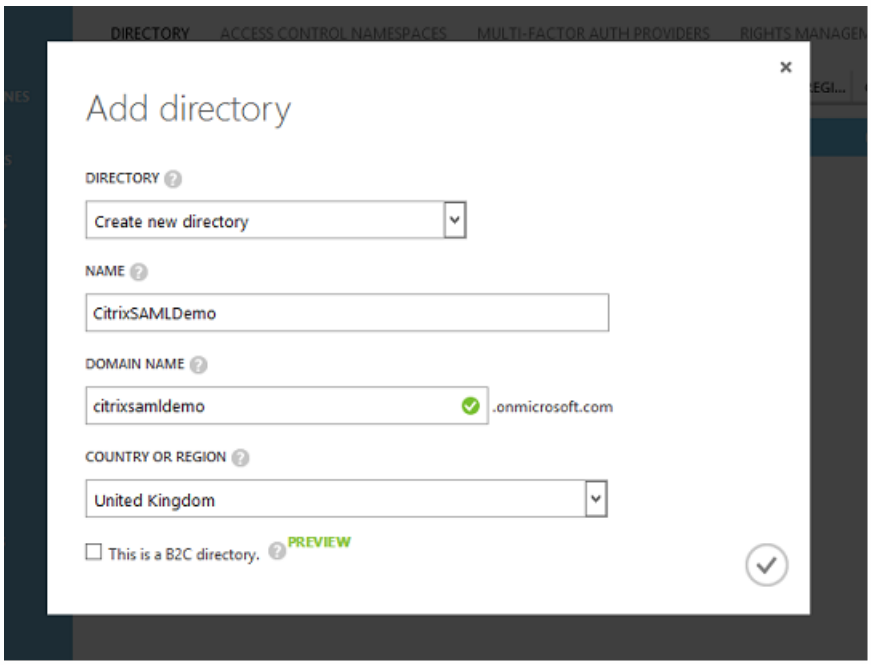
Exporte el certificado a un archivo PFX, incluida una clave privada protegida por contraseña.

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.

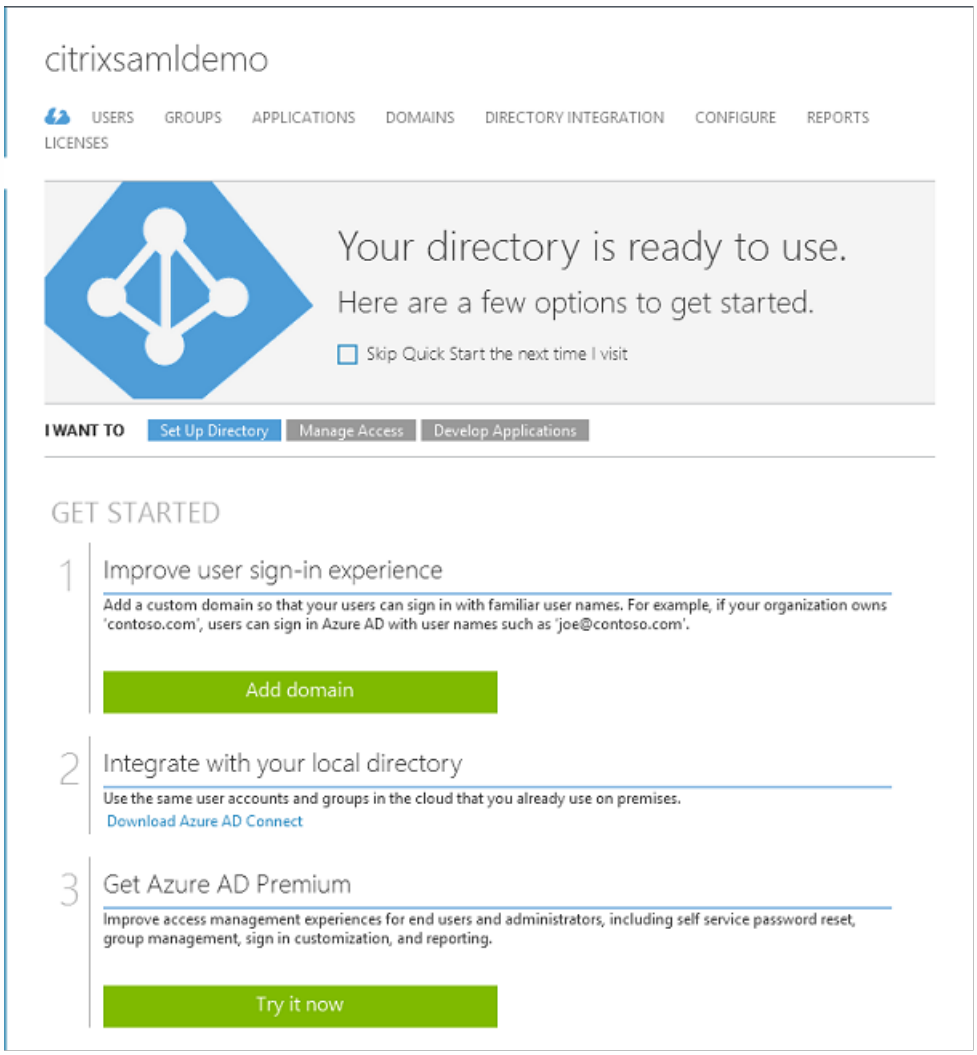
Crear un directorio nuevo

Inicie sesión en el portal Azure clásico y cree un directorio nuevo.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

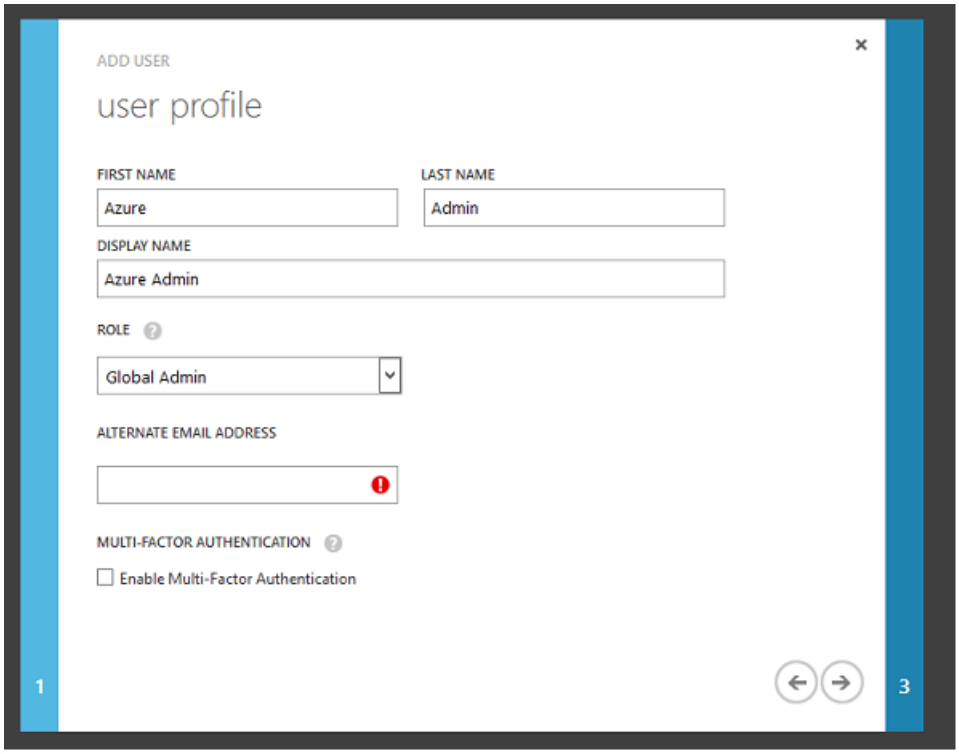
Una vez completado, aparece una página de resumen.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Registrar su dominio con Azure AD

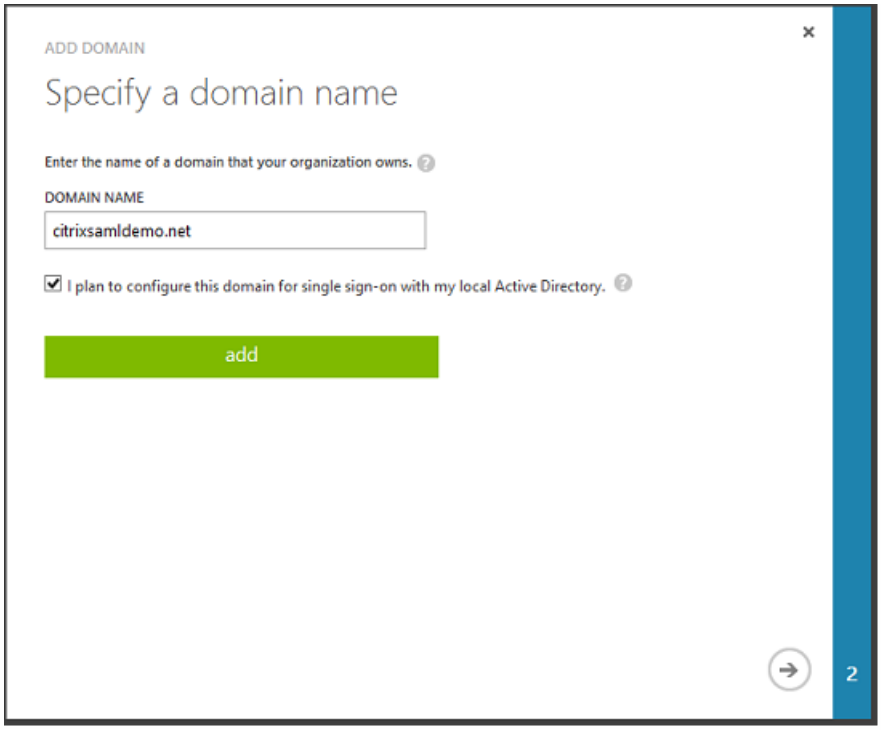
De forma predeterminada, los usuarios se identifican mediante una dirección de correo electrónico en el formato: *<nombre.usuario>@<empresa>.onmicrosoft.com*.

Aunque esto funciona sin más 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: @.com

La acción **Add domain** configura una redirección desde el dominio real de su empresa.En el ejemplo, se utiliza citrixsamldemo.net.

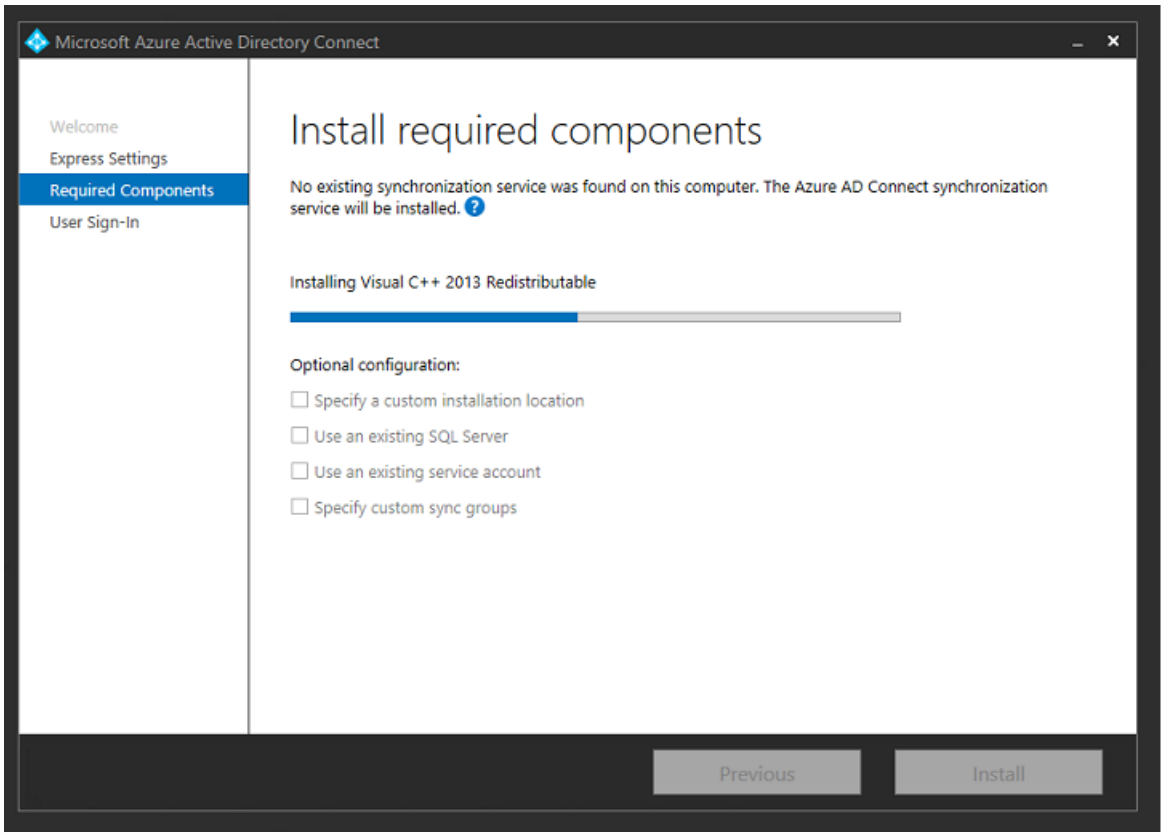
Si quiere configurar ADFS para el inicio de sesión único Single Sign-on, marque la casilla correspondiente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



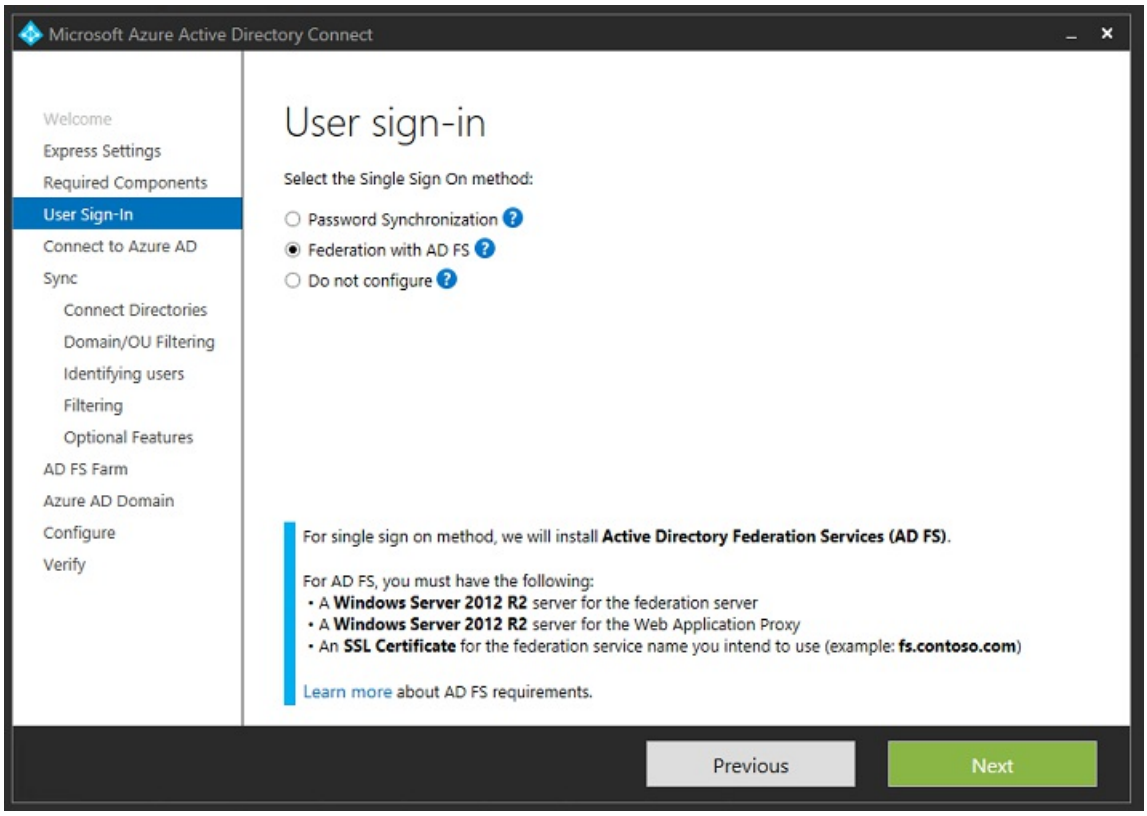
Instalar Azure AD Connect

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 **Custom install**, en lugar de **Express Settings**, para poder acceder a las opciones de ADFS.

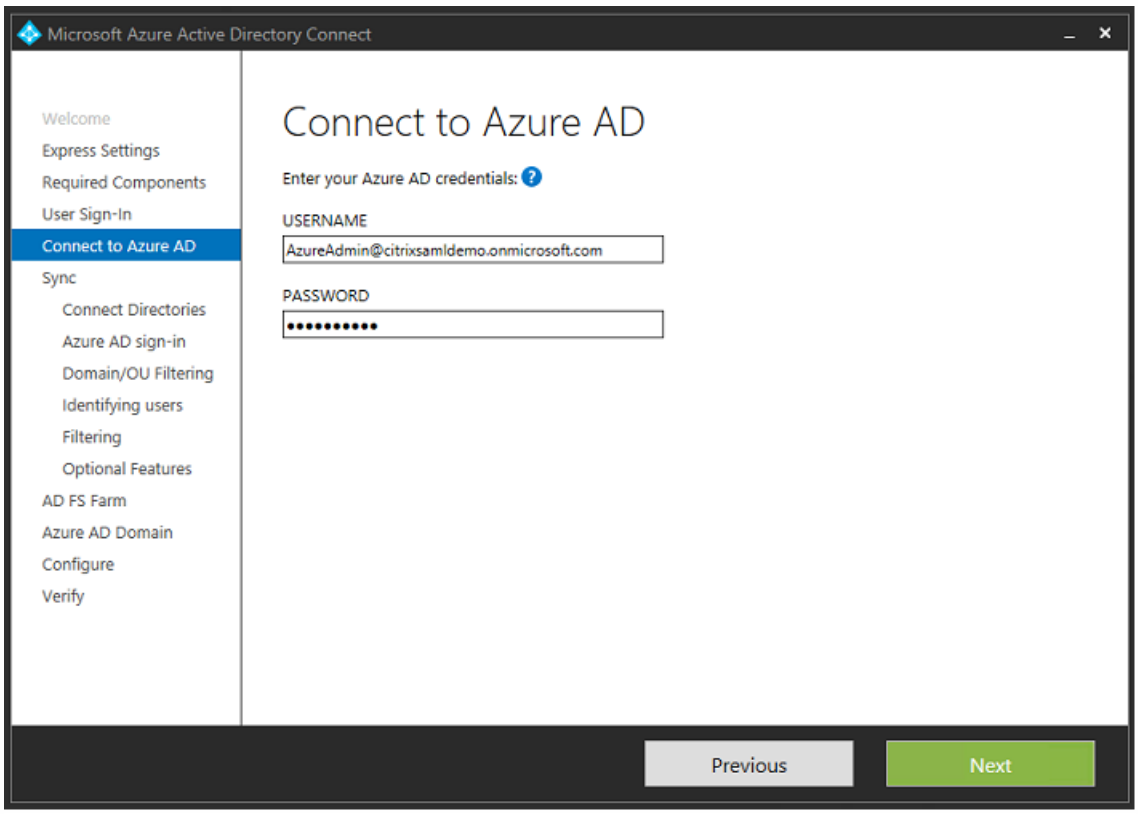


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Seleccione la opción Single Sign-on de **Federation with AD FS**.

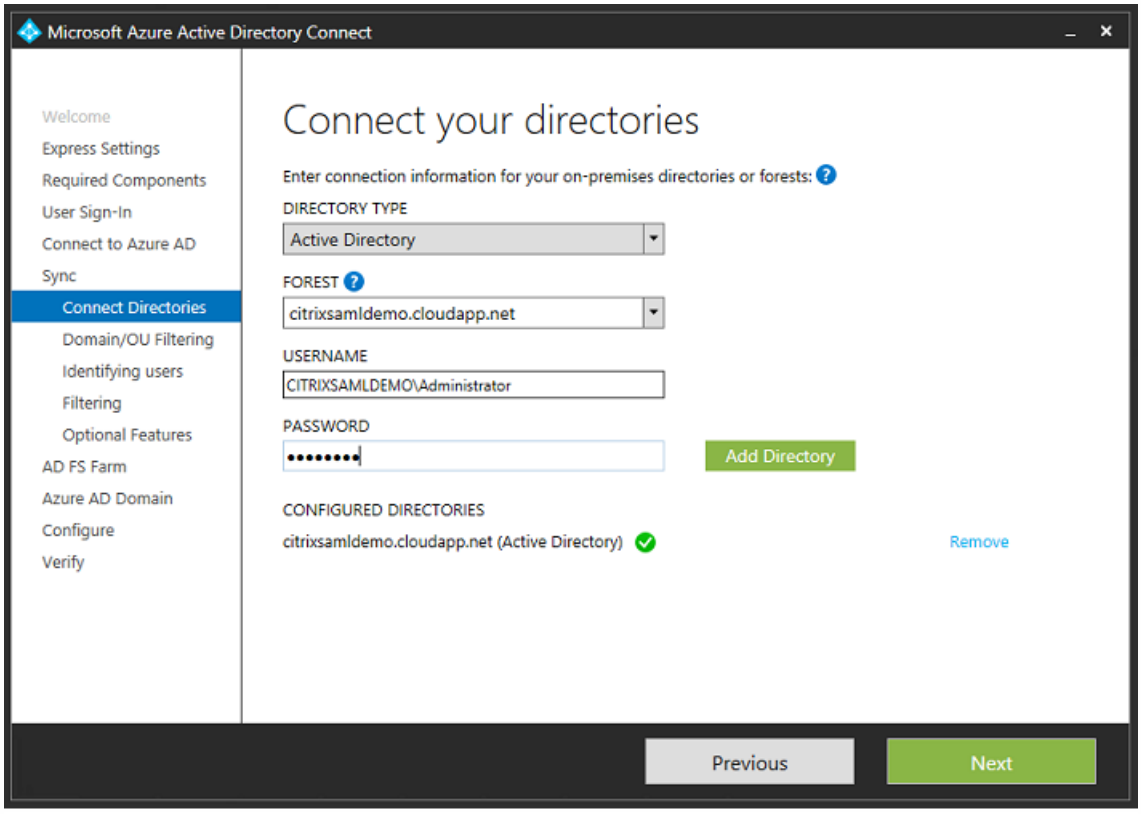


Conéctese a Azure con la cuenta de administrador que ha creado anteriormente.



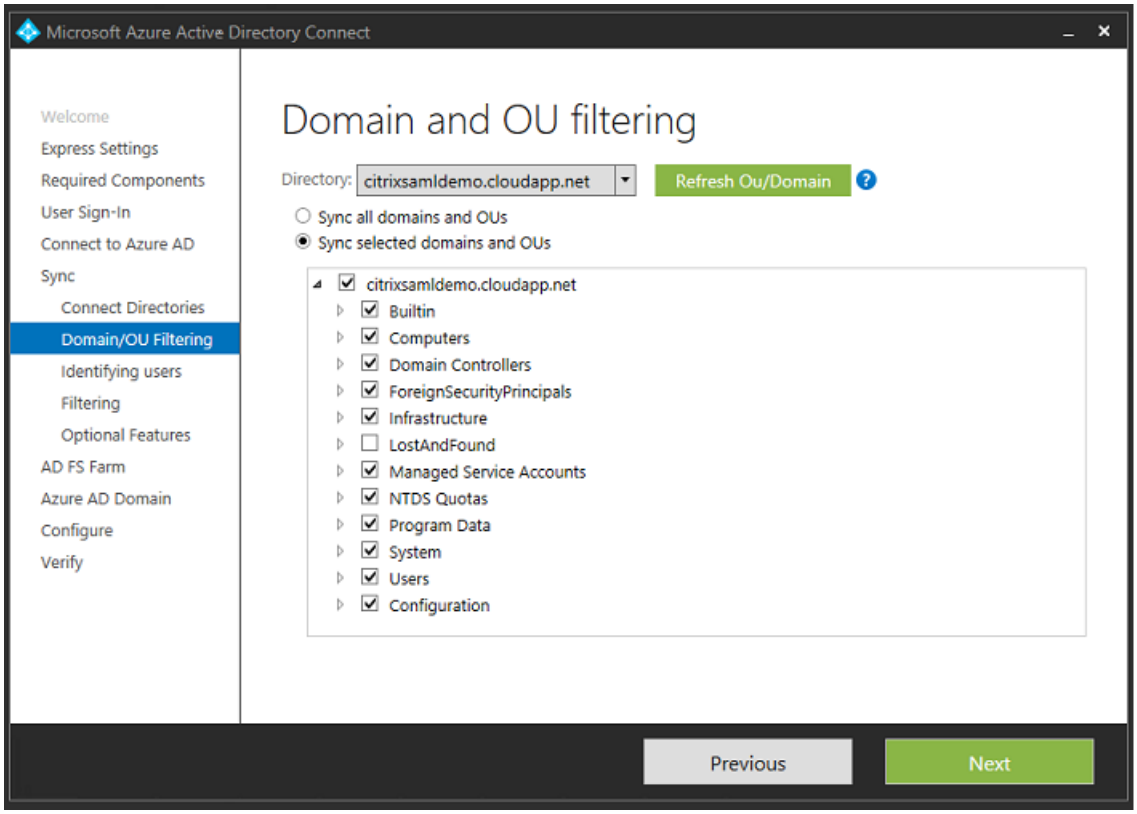
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Seleccione el bosque de AD interno.

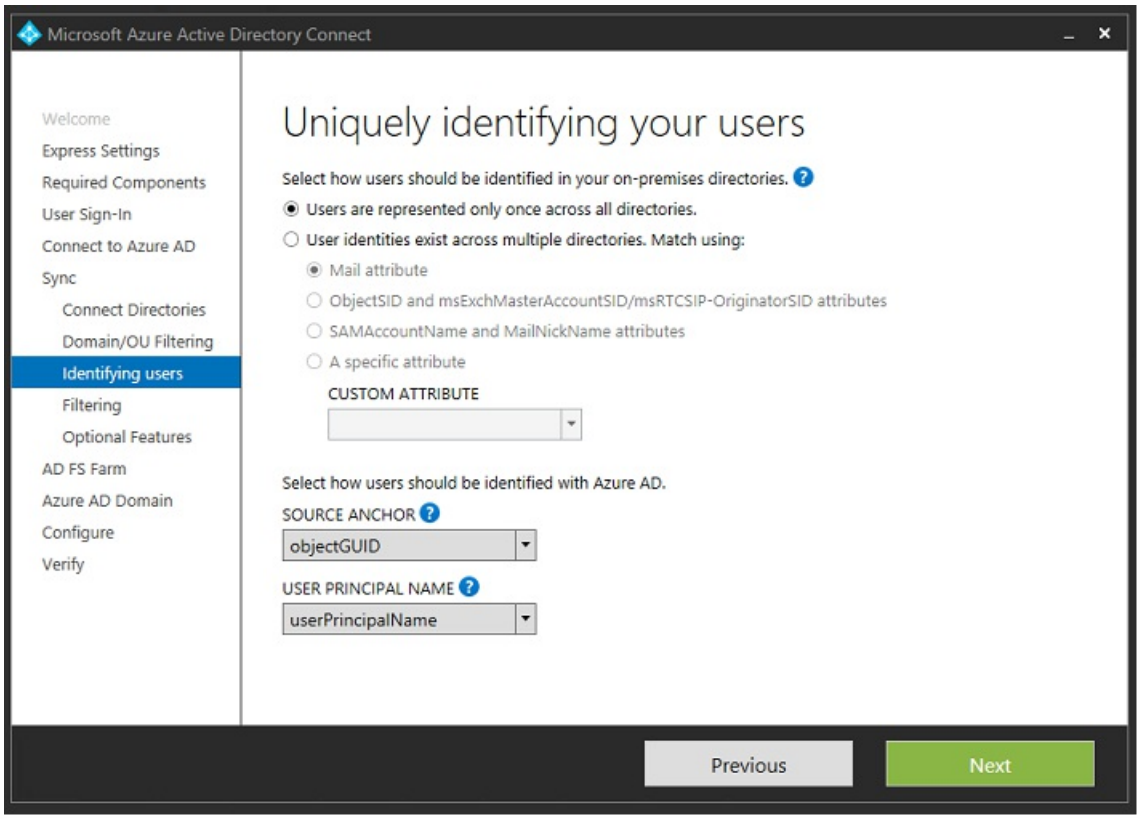


Sincronice todos los objetos de Active Directory antiguos con Azure AD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

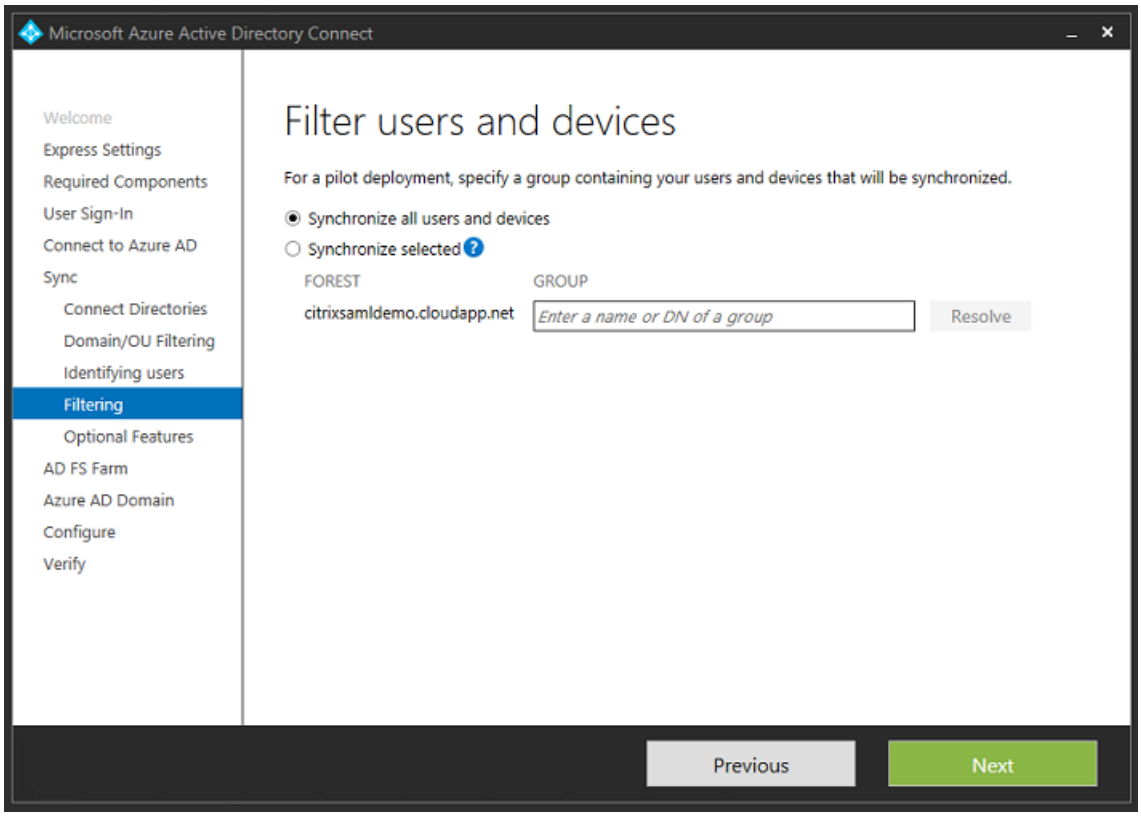


Si la estructura de directorio es sencilla, puede asumir que los nombres de usuario serán lo suficientemente únicos para identificar al usuario que inicia una sesión.

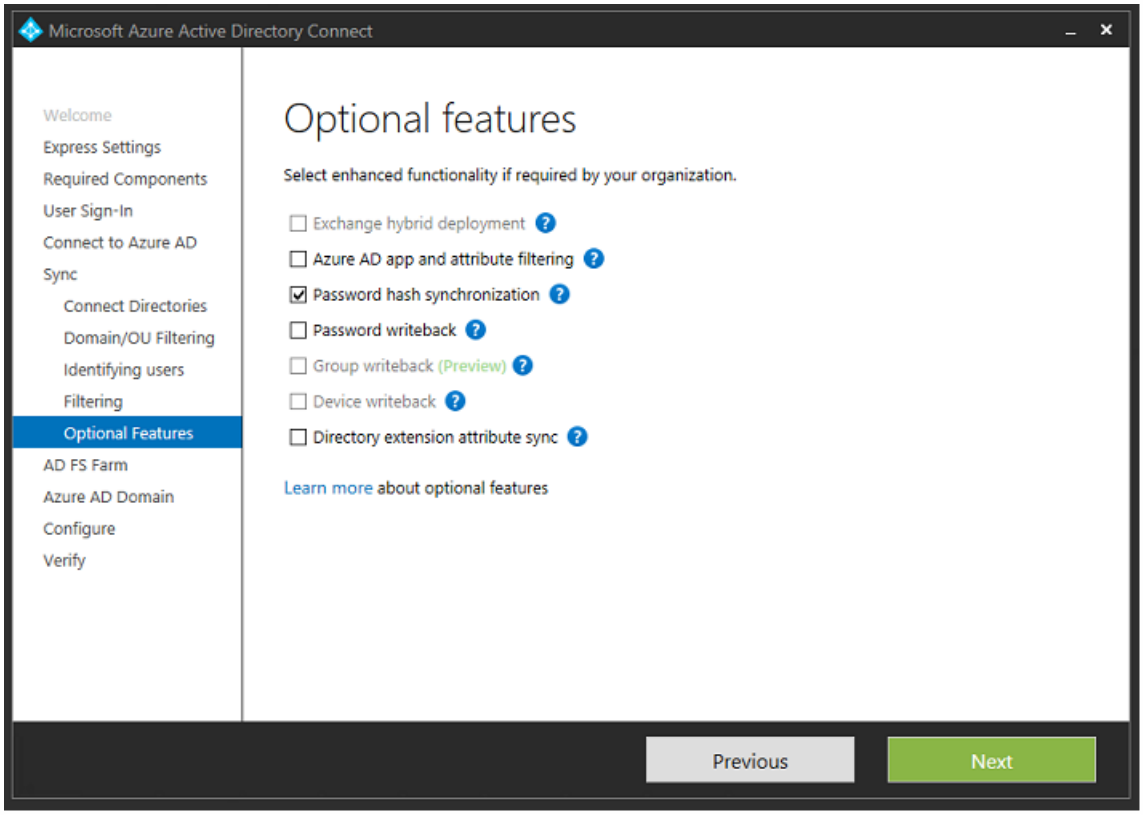


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Acepte las opciones de filtrado predeterminadas, o restrinja usuarios y dispositivos a un conjunto de grupos determinado.

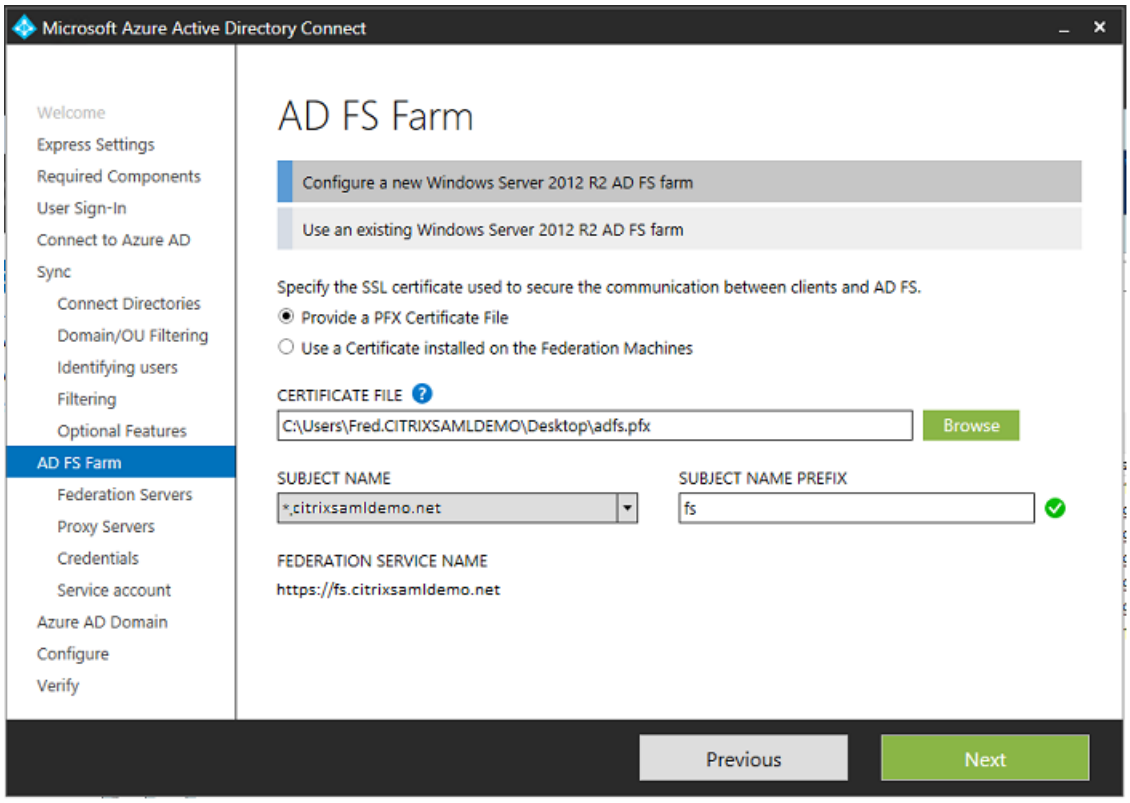


Si lo desea, puede sincronizar las contraseñas de Azure AD con Active Directory. Esto normalmente no es necesario para la autenticación basada en ADFS.



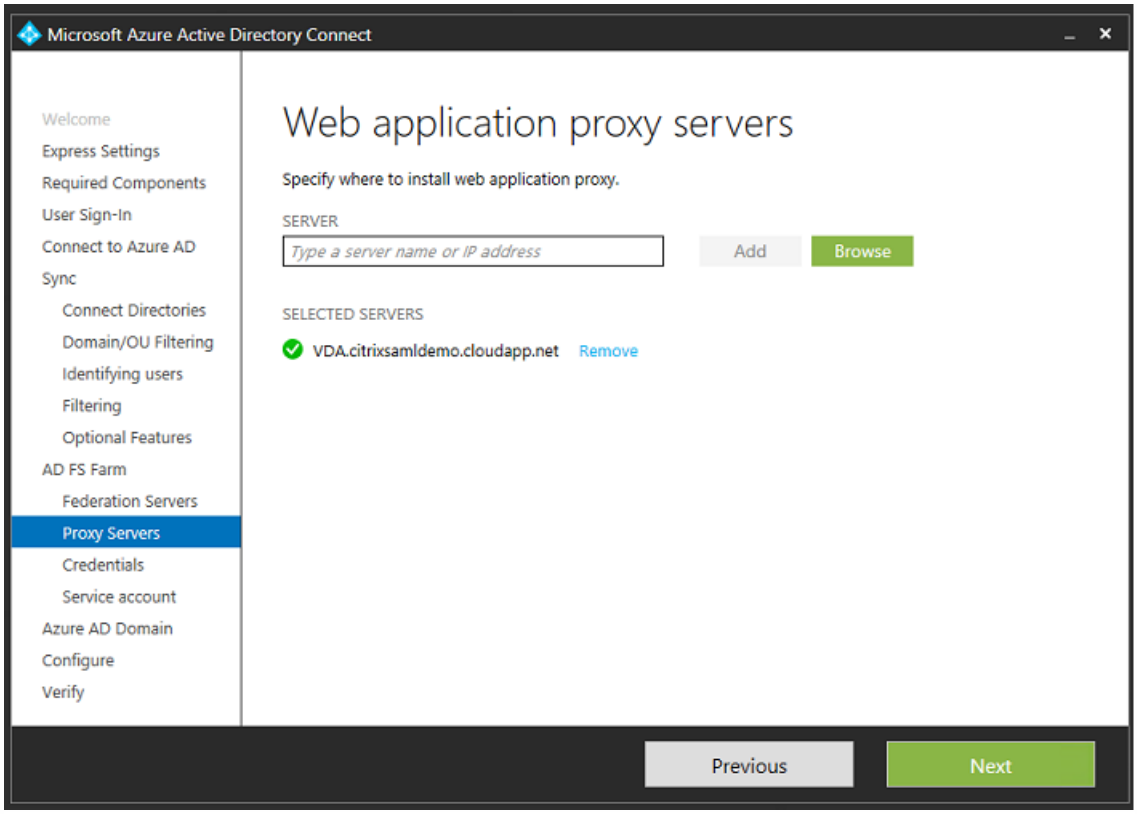
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Seleccione el archivo de certificado PFX que se va a usar en ADFS, especificando fs.citrixsamldemo.net como nombre DNS.



Cuando se le pida seleccionar un servidor proxy, escriba la dirección del servidor wap.citrixsamldemo.net.Es posible que deba ejecutar el cmdlet **Enable-PSRemoting – Force** como administrador en el servidor proxy de aplicaciones Web, para que Azure AD Connect pueda configurarlo.

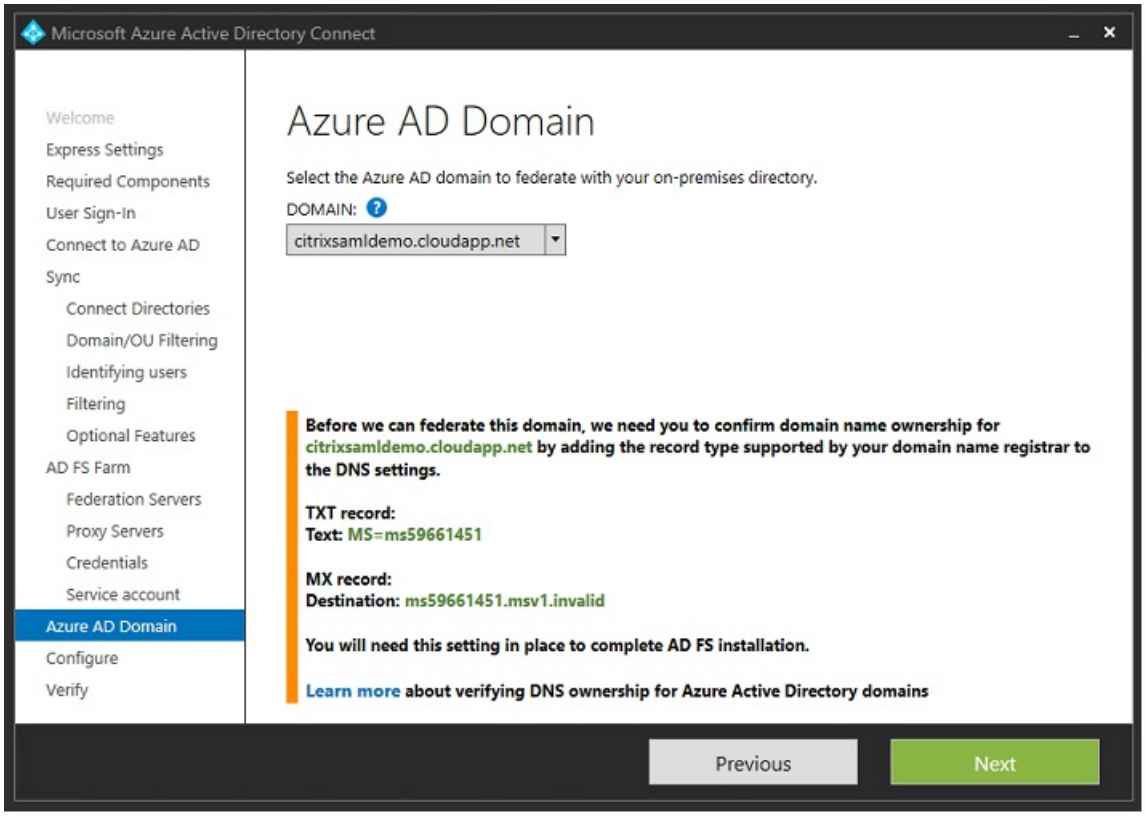
© 1999-2017 Citrix Systems, Inc. All rights reserved.



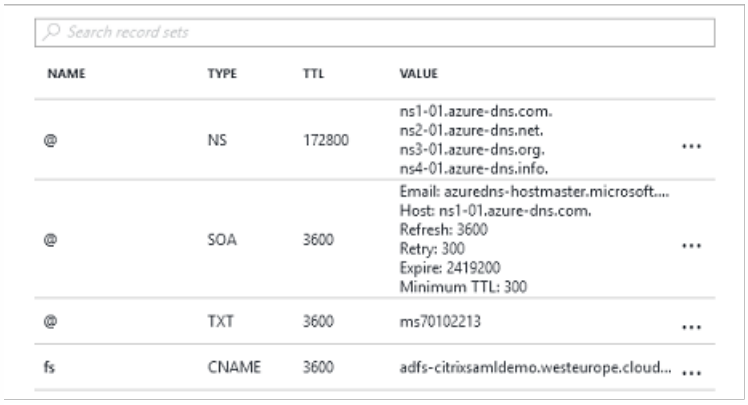
Nota: Si este paso falla debido a problemas de confianza con el PowerShell remoto, una el servidor proxy de aplicaciones Web al dominio.

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.

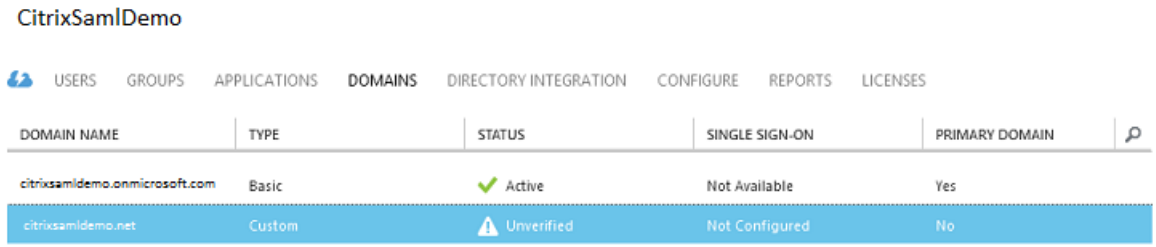
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Agregue los registros TXT y MX a los registros de direcciones DNS en Azure.



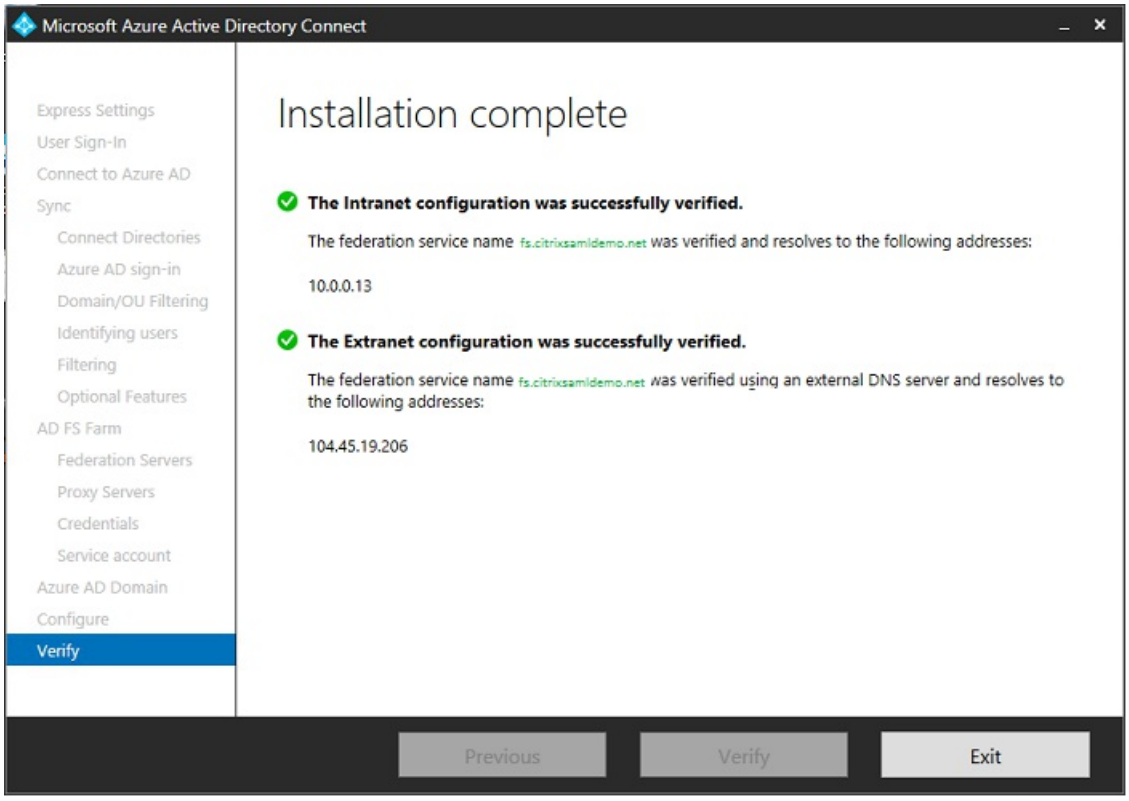
Haga clic en **Verify** en Azure Management Console.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: Si este paso falla, puede verificar el dominio antes de ejecutar Azure AD Connect.

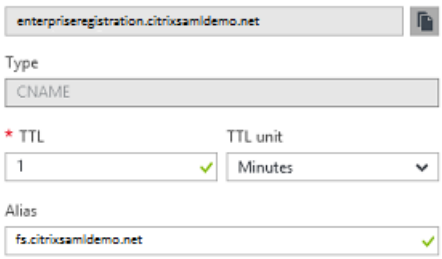
Una vez completado, se contacta con la dirección externa fs.citrixsamldemo.net a través del puerto 443.



Habilitar la función Unirse a Azure a AD

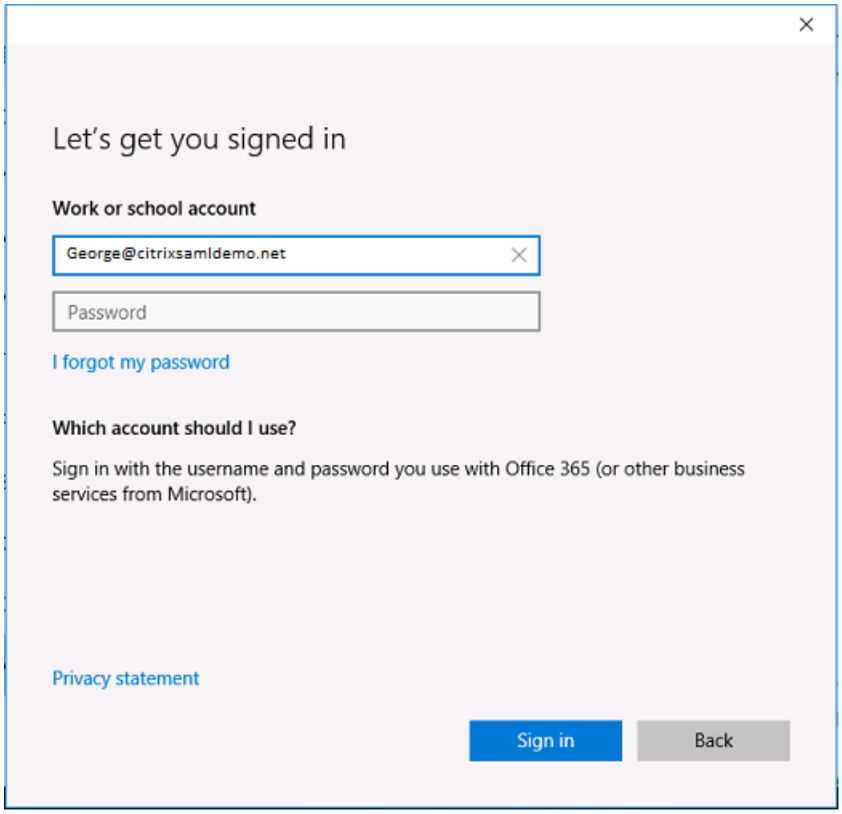
Cuando un usuario introduce una dirección de correo electrónico para que Windows 10 pueda unirse a Azure AD, el sufijo DNS se usa para crear un registro DNS CNAME que debe apuntar a ADFS: enterpriseregistration..

En este ejemplo, esto es fs.citrixsamldemo.net.

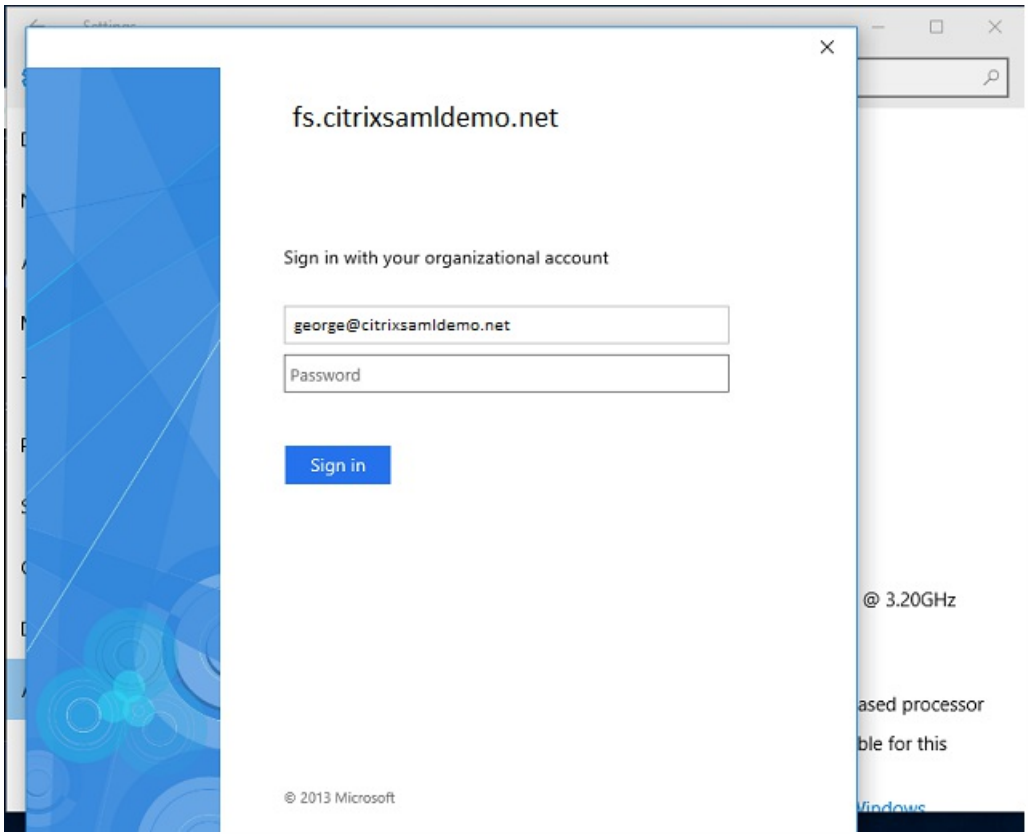


Si no está usando una entidad de certificación CA pública, asegúrese de que el certificado raíz de ADFS está instalado en el equipo con Windows 10 de modo que Windows confié en el servidor ADFS.Realice la unión con el dominio de Azure AD utilizando la cuenta de usuario estándar generada anteriormente.

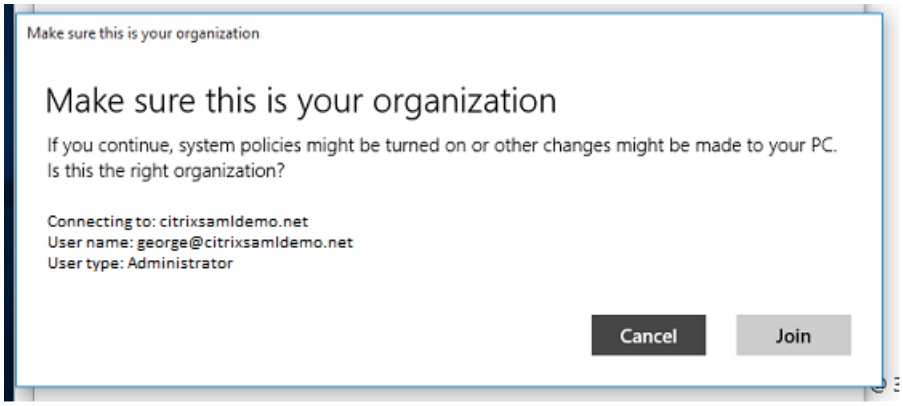
© 1999-2017 Citrix Systems, Inc. All rights reserved.

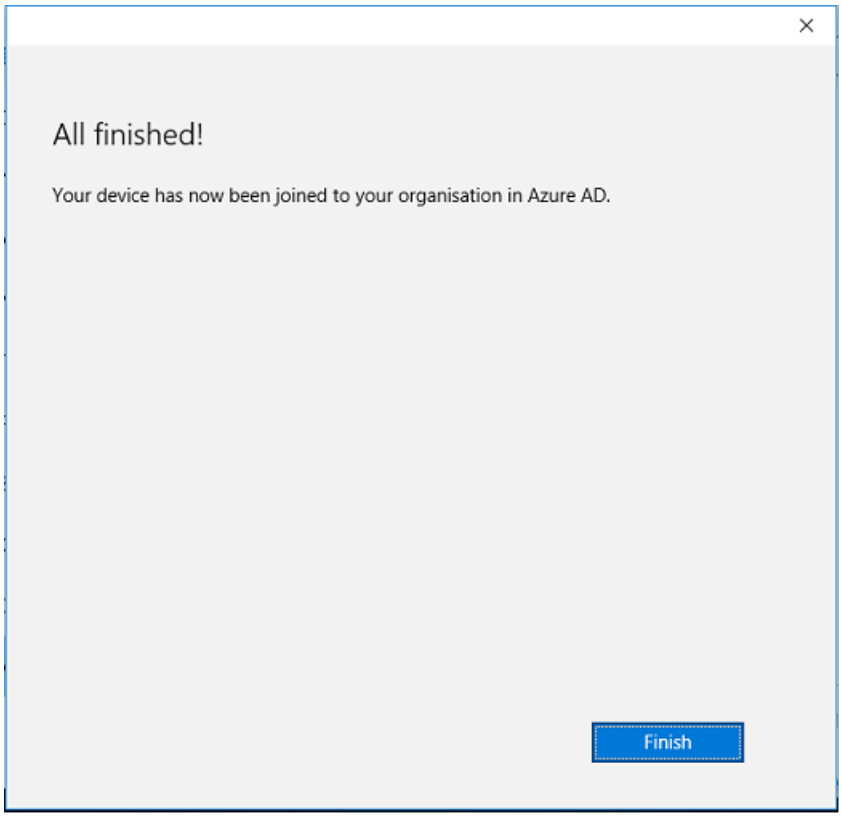


Tenga en cuenta que el nombre UPN debe coincidir con el nombre UPN reconocido por el controlador de dominio de ADFS.



 © 1999-2017 Citrix Systems, Inc. All rights reserved.





Verifique si la unión al dominio de Azure AD tuvo éxito reiniciando la máquina e iniciando la 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.

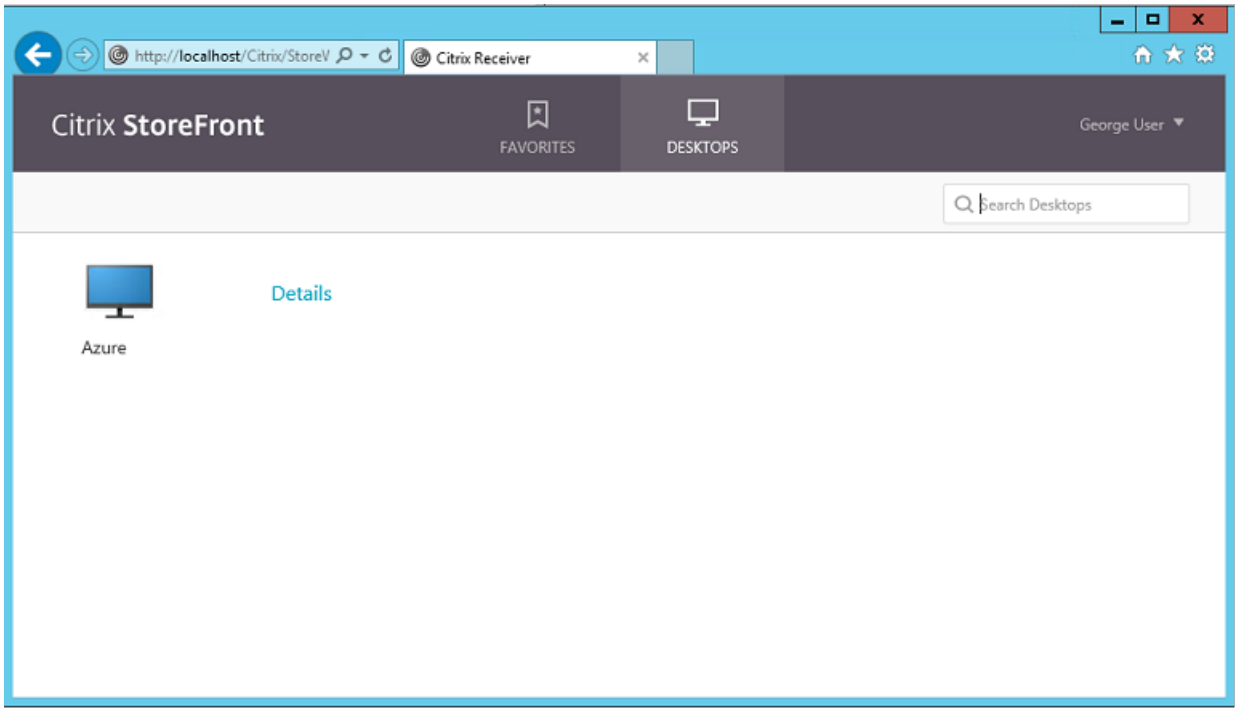
Instalar XenApp o XenDesktop

Puede instalar las máquinas virtuales del Delivery Controller y los VDA directamente en Azure desde la imagen ISO de XenDesktop o XenApp 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).Antes de continuar, compruebe que el usuario Jorge@citrixsamldemo.net se puede autenticar con

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

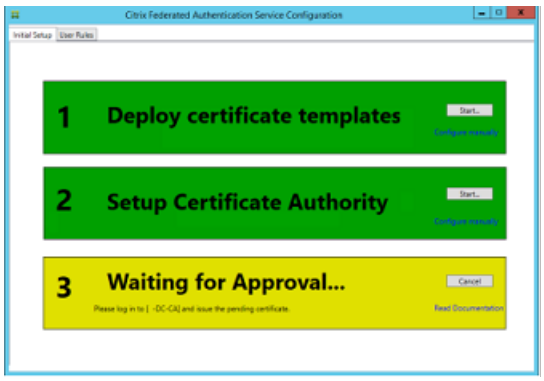
una contraseña.



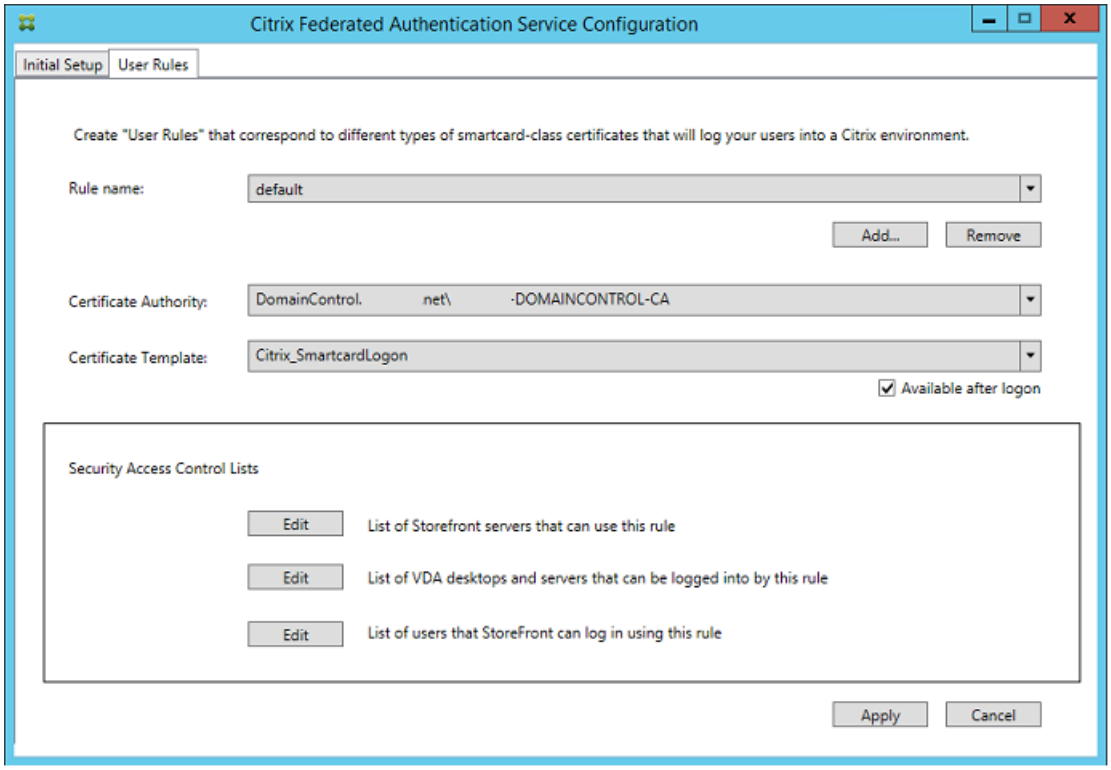
Ejecute el cmdlet **Set-BrokerSite –TrustRequestsSentToTheXmlServicePort $true** de PowerShell en el Controller para permitir que StoreFront se autentique sin las credenciales de los usuarios.

Instalación del 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.

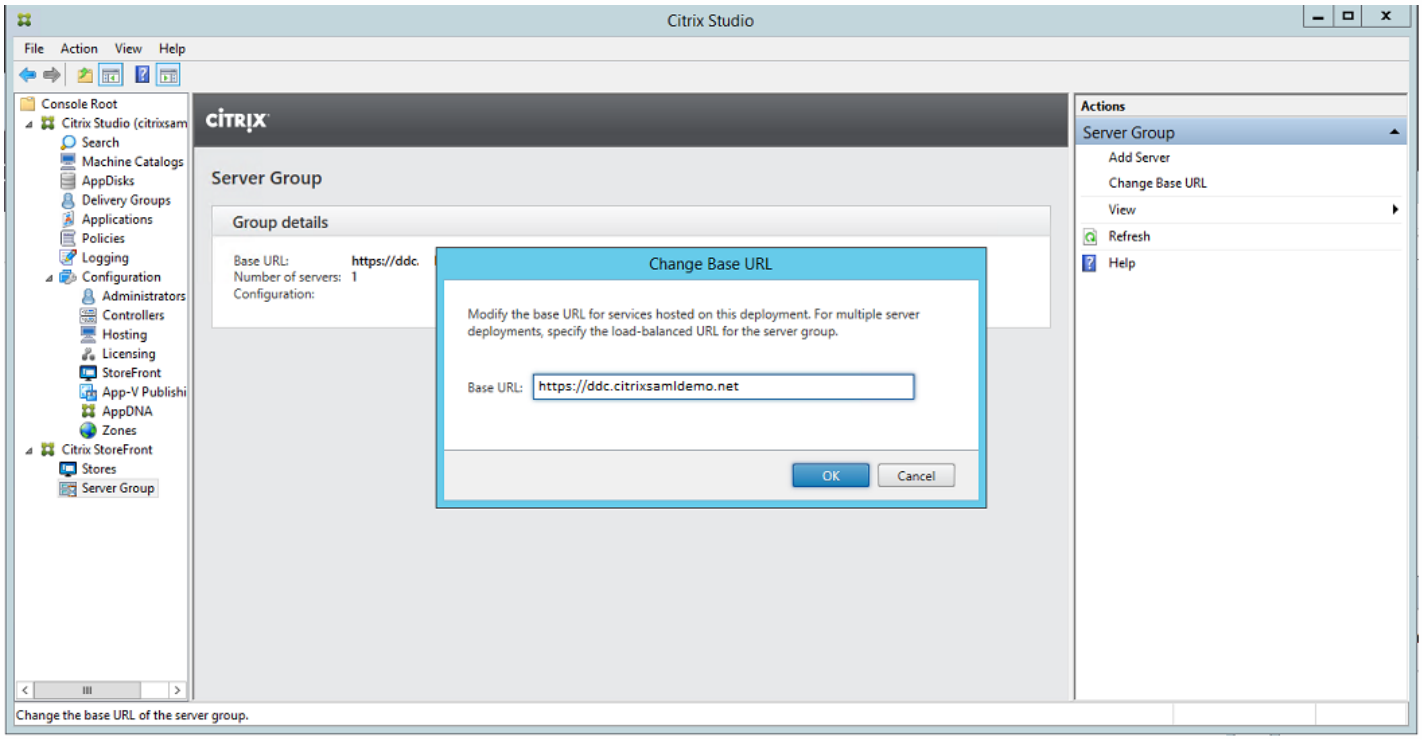


© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configuración de StoreFront

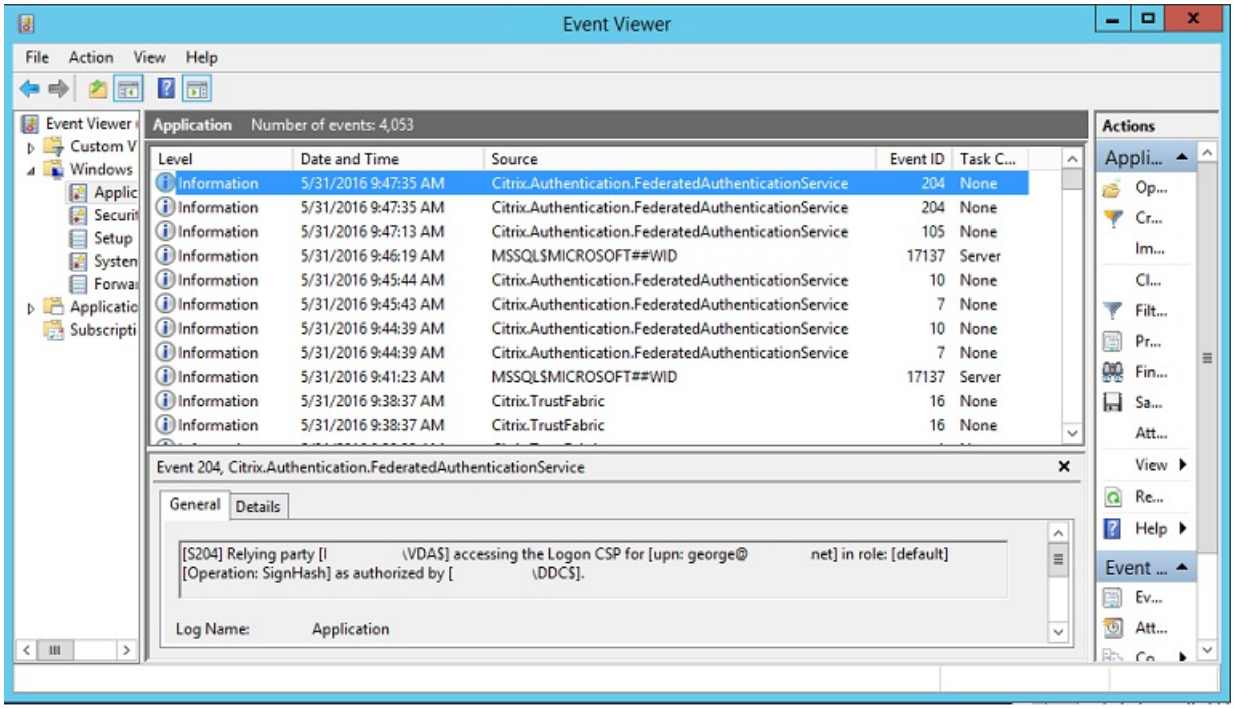
Solicite un certificado de equipo para el Delivery Controller y configure IIS y StoreFront para usar HTTPS estableciendo un enlace de IIS para el puerto 443 y cambiando la dirección de base de datos de StoreFront a https:.



Configure StoreFront para usar el servidor de FAS (use el script de PowerShell en el artículo Servicio de autenticación

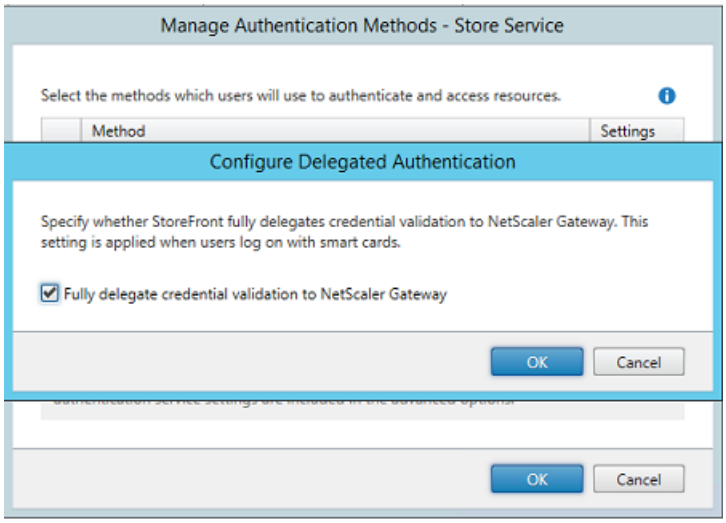
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



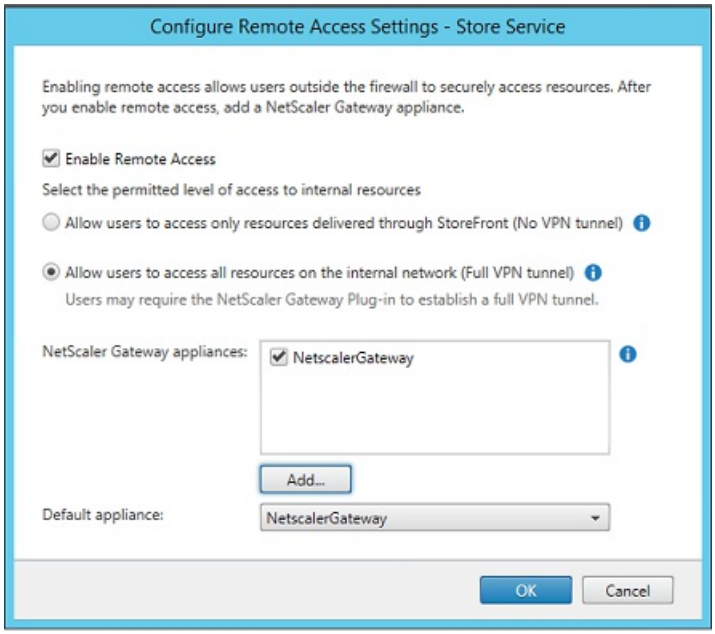
Configuración de StoreFront para usar NetScaler

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.



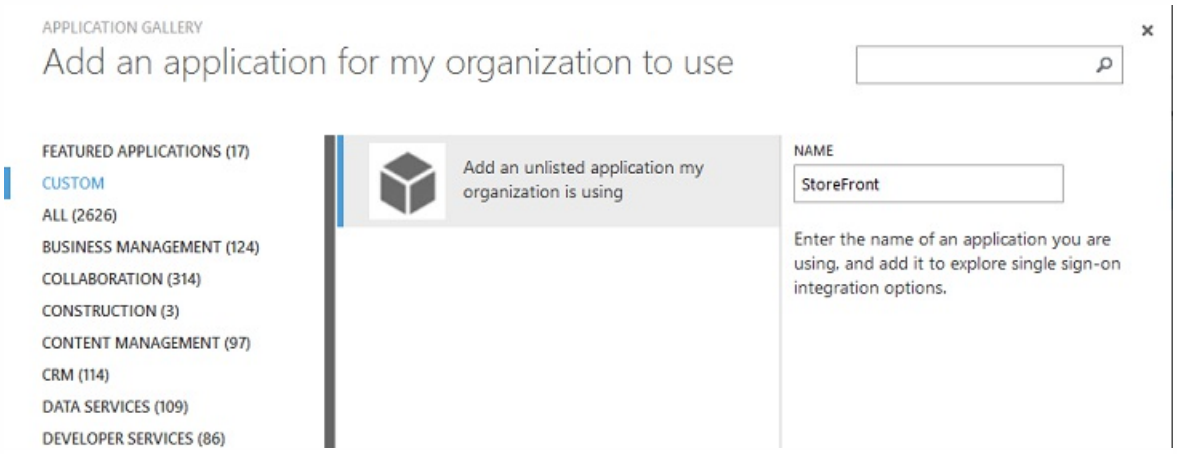
Para integrar las opciones de autenticación de NetScaler, configure Secure Ticket Authority (STA) y configure la dirección de NetScaler Gateway.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurar una nueva aplicación de Azure AD para inicios de sesión 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 **Aplicación nueva**, y elija **Agregar una aplicación de la galería**.



Seleccione **Personalizado > Agregar una aplicación que no figura en la lista de mi organización está usando** para crear una nueva aplicación personalizada para sus usuarios.

Configurar un icono

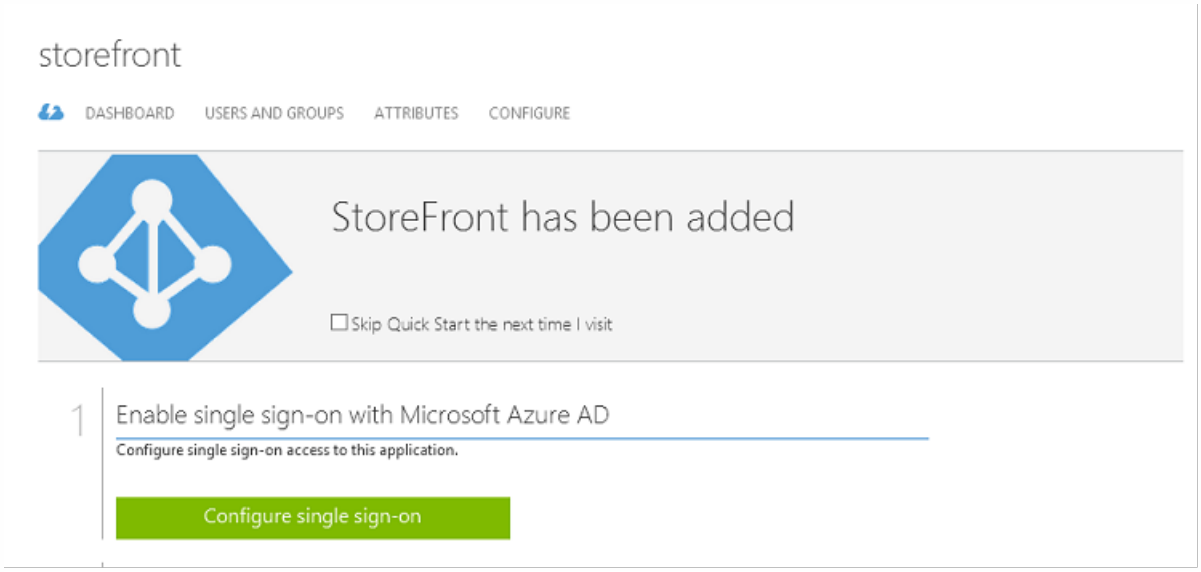
Cree una imagen de 215 x 215 píxeles de tamaño y cárguela en la página CONFIGURE para usarla como icono de la aplicación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

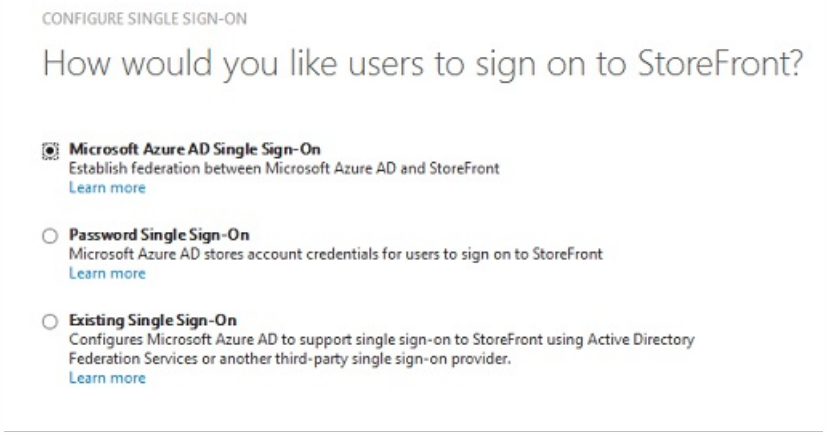


Configuración de la autenticación SAML

Vuelva a la página Application dashboard overview y seleccione **Configure Single Sign-on**.

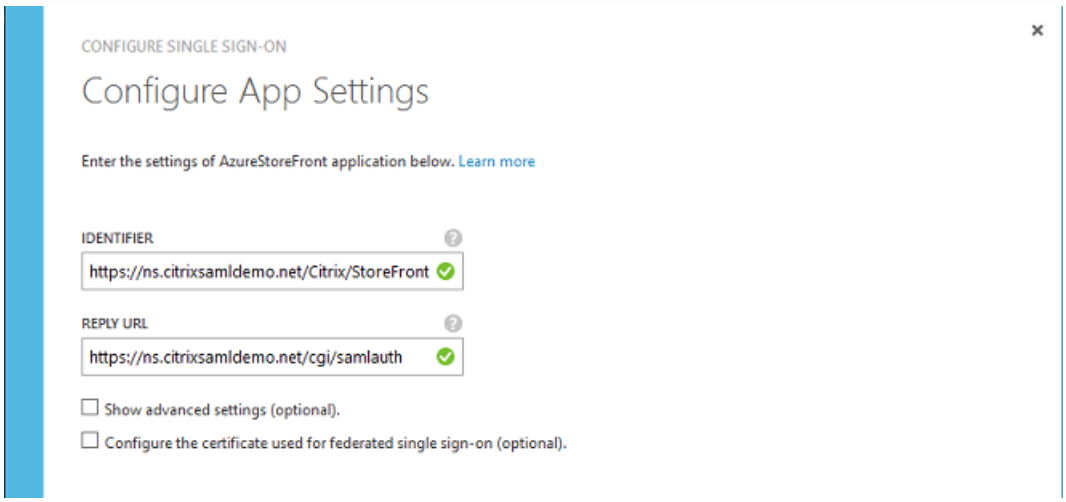


Esta implementación utilizará la autenticación SAML 2.0, que corresponde a **Microsoft Azure AD Single Sign-On**.

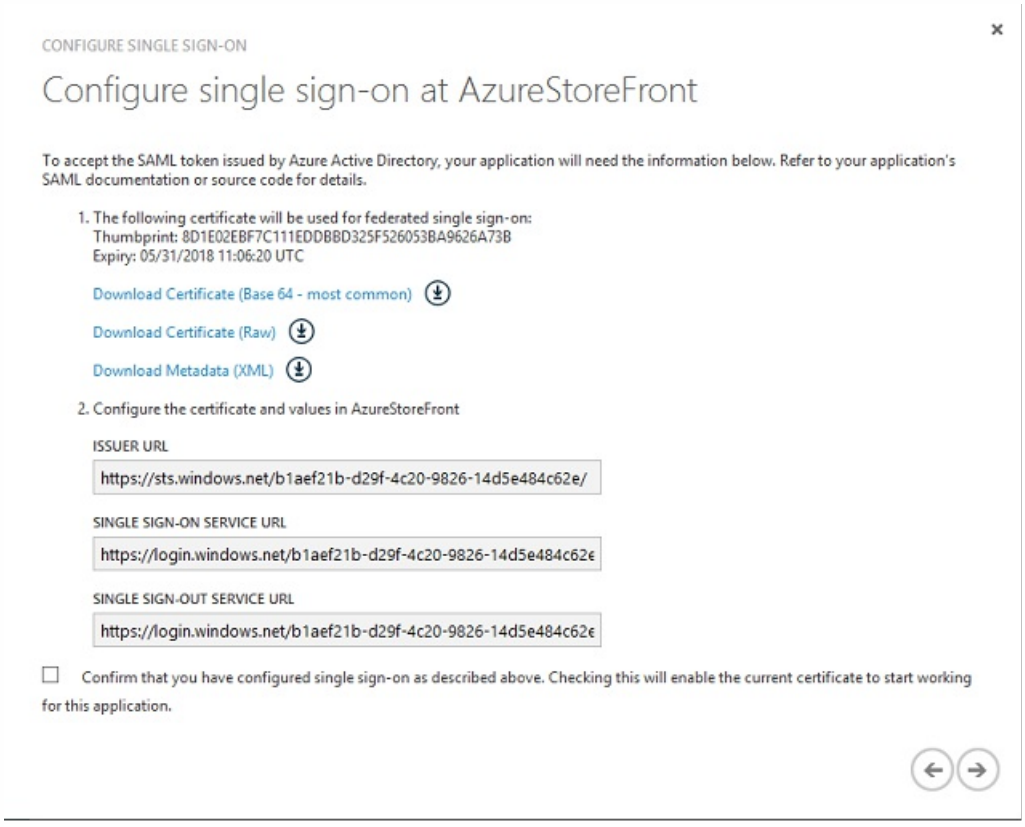


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



La siguiente página contiene información que se usa para configurar NetScaler como una parte de confianza para Azure AD.

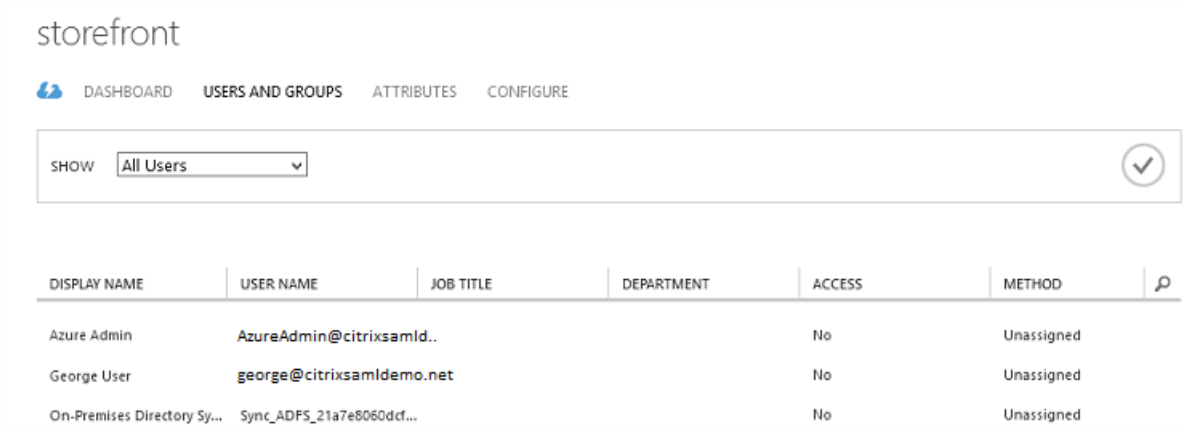


Descargue el certificado de firma de confianza de base 64 y copie las URL de inicio y cierre de sesión.Pegará estas URL en al configuración de NetScaler más adelante.

Asignar la aplicación a los usuarios

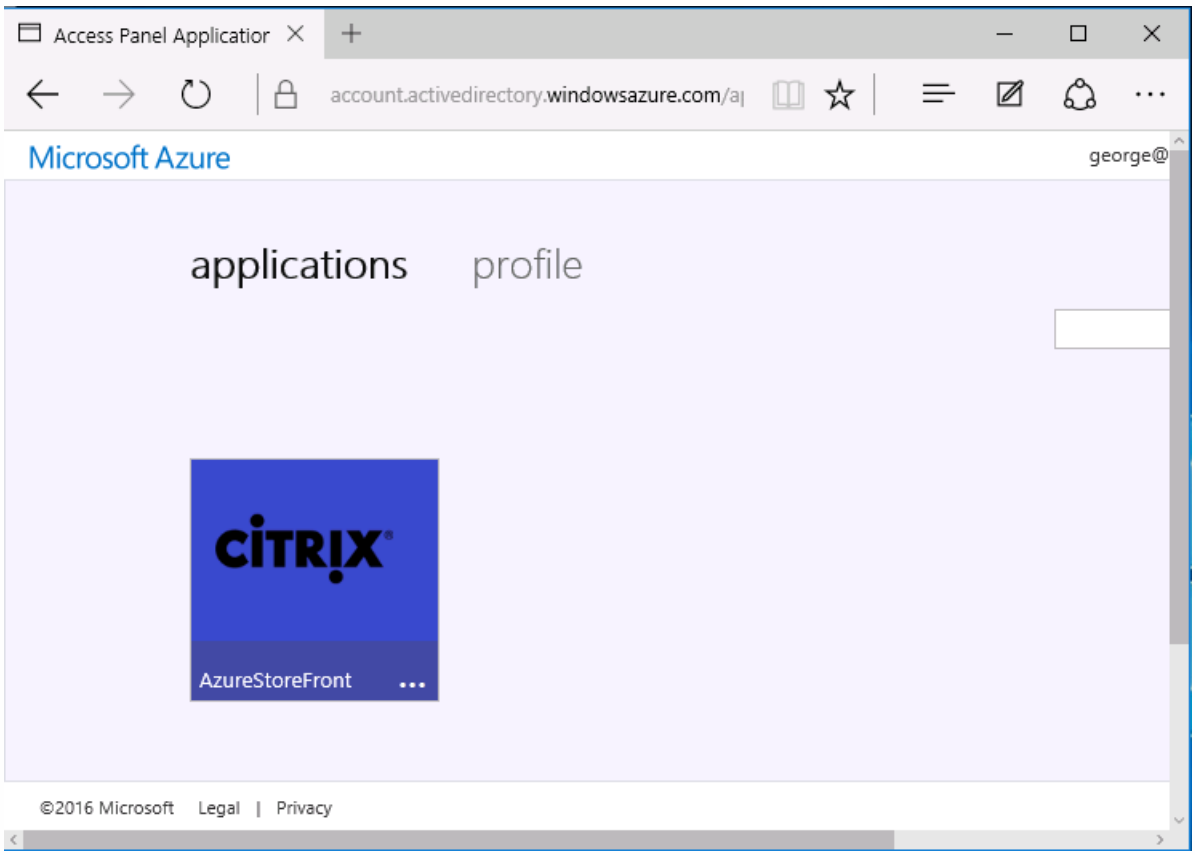
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 que sincroniza Azure AD Connect.También puede usar otras cuentas, pero deben estar explícitamente asignadas, porque no cumplen el formato @.



Página de MyApps

Cuando la aplicación se ha configurado, aparece en las listas de los usuarios de las aplicaciones de Azure cuando estos visitan https://myapps.microsoft.com.



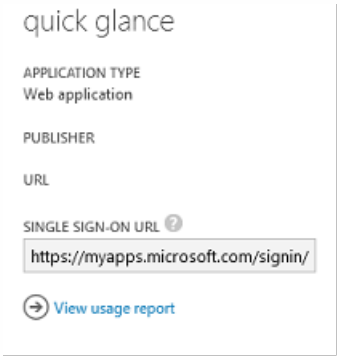
Cuando está unido a Azure AD, Windows 10 admite el inicio de sesión único Single Sign-on en las aplicaciones de Azure para el usuario que inicie sesión.Al hacer clic en el icono, el explorador va a la página de SAML cgi/samlauth que se configuró

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

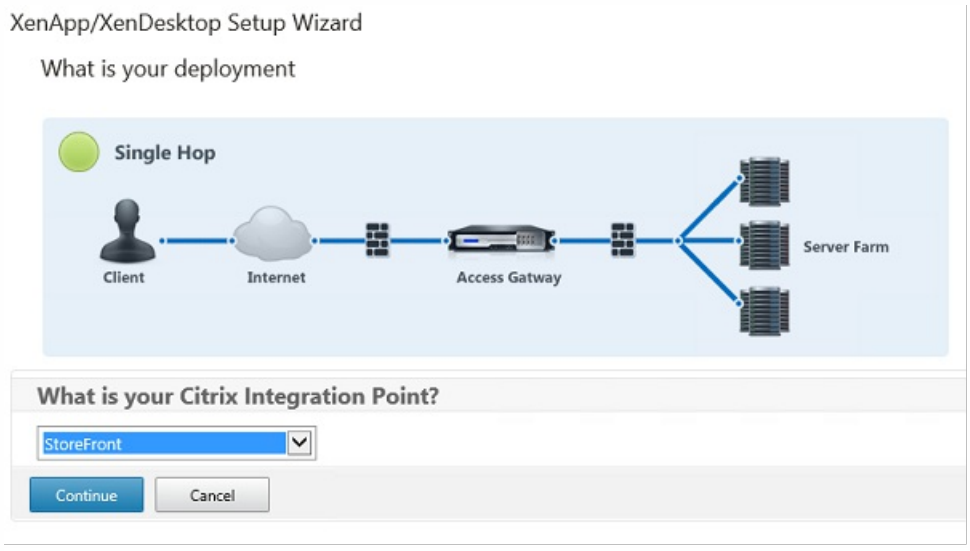


Inicie sesión en la VM de NetScaler, apuntando el explorador Web a la dirección IP interna, usando las credenciales especificadas cuando el usuario se autenticó.Tenga en cuenta que debe cambiar la contraseña del usuario nsroot en una VM de Azure AD.

Agregue licencias, seleccionando **reboot** después de agregar cada una de ellas, y apunte la resolución DNS al controlador de dominio de Microsoft.

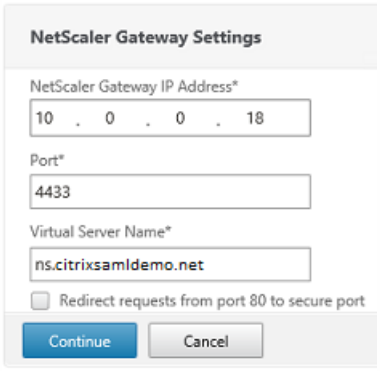
Ejecute el asistente de instalación de XenApp y XenDesktop

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.

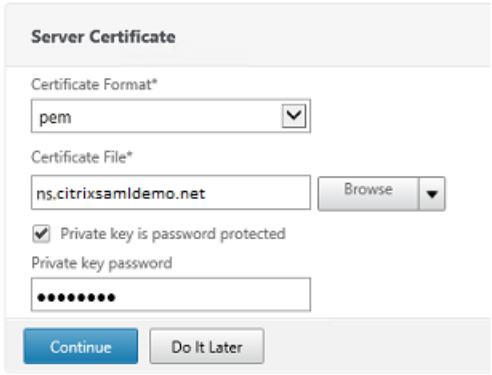


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



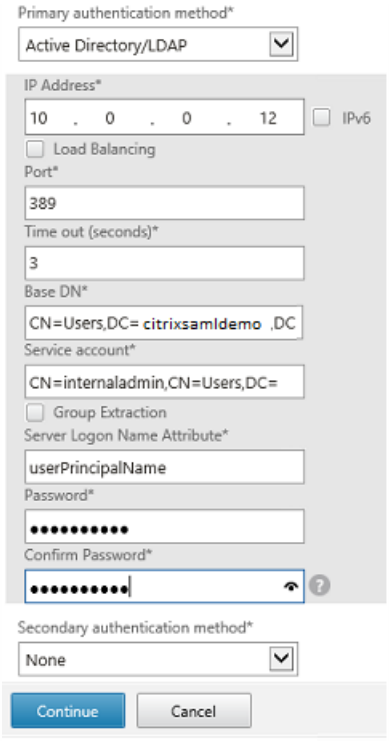
Para simplificar las tareas, el ejemplo carga un certificado de servidor existente y una clave privada guardada en un archivo.



Configurar el controlador de dominio para la administración de cuentas de AD

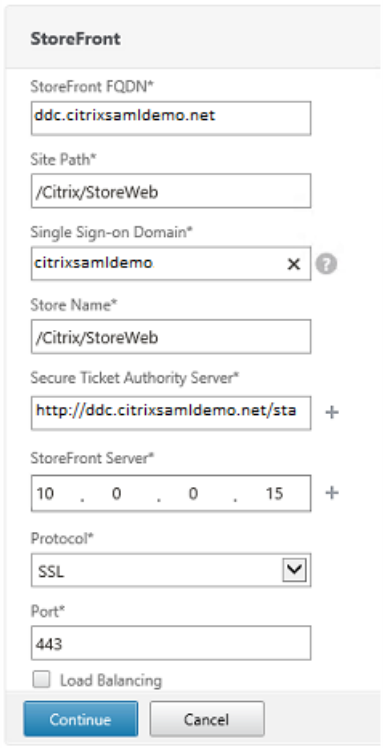
El controlador de dominio se usará para la resolución de cuentas, por lo que hay que agregar su dirección IP en el método de autenticación principal.Tenga en cuenta el formato esperado en cada campo del cuadro de diálogo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurar la dirección de StoreFront

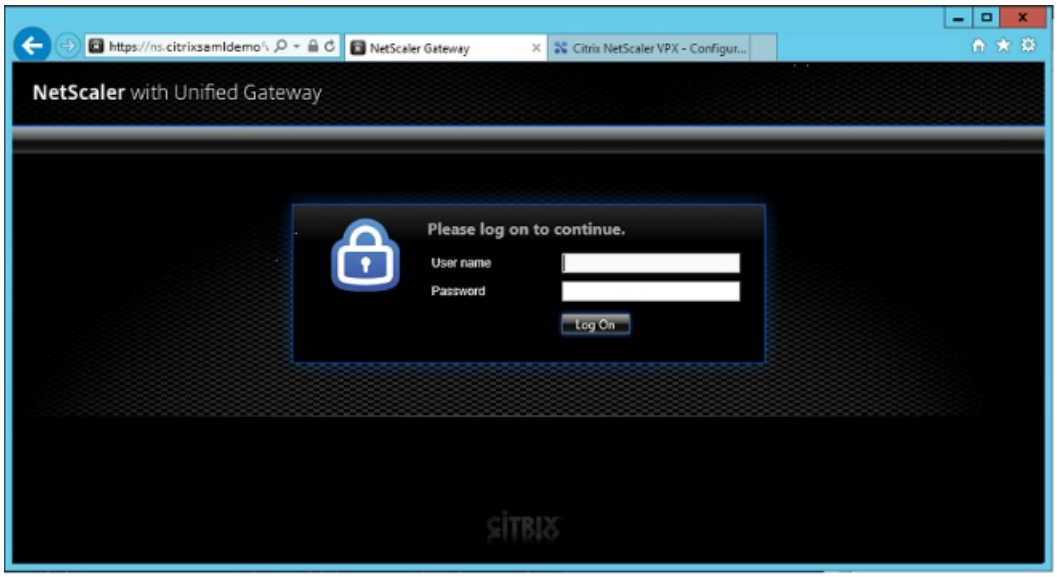
En este ejemplo, StoreFront se ha configurado usando HTTPS, por lo tanto, seleccione las opciones de protocolo SSL.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

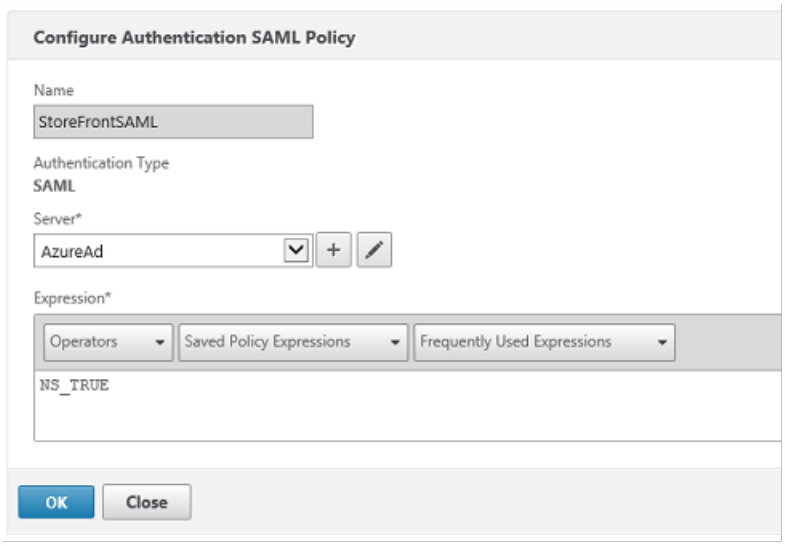
Verificar la implementación de NetScaler

Conéctese a NetScaler y compruebe que la autenticación y el inicio se realizan correctamente con el nombre de usuario y la contraseña.



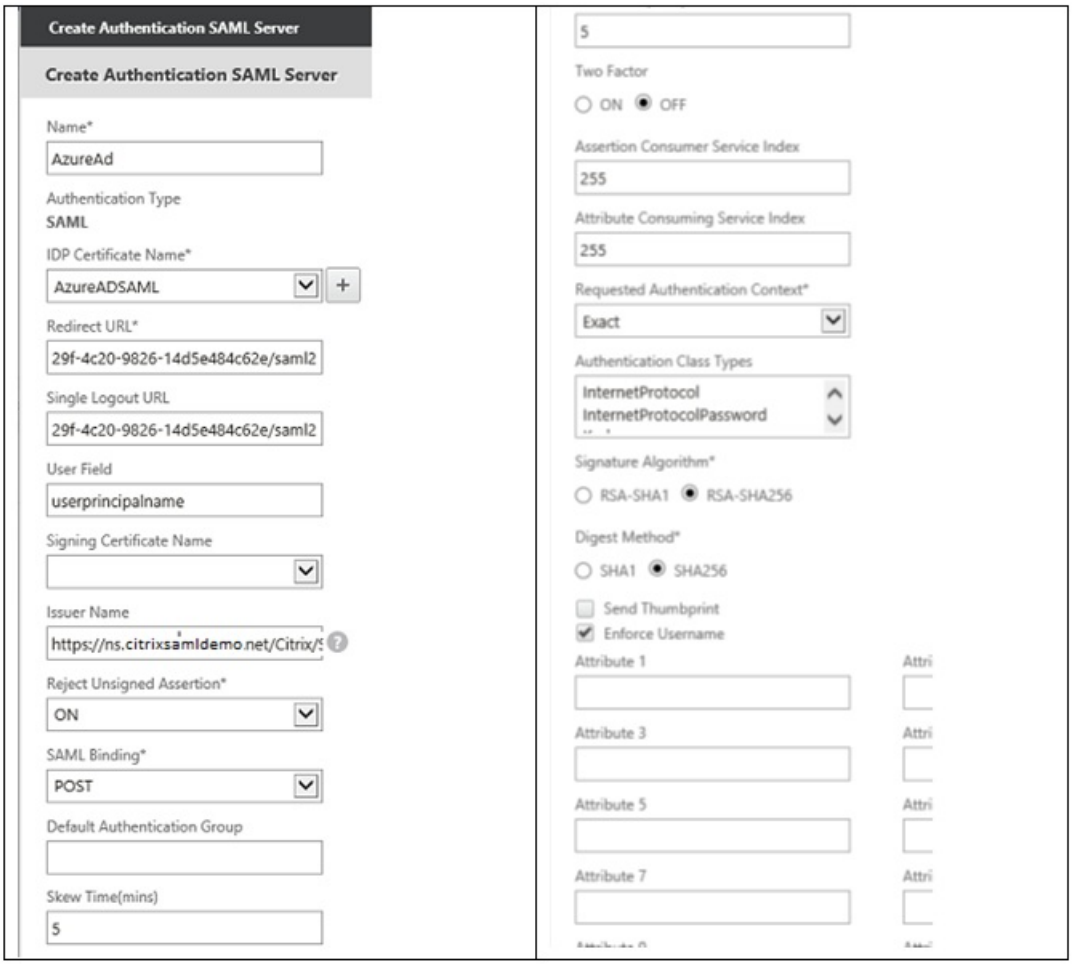
Habilitar el respaldo para la autenticación SAML

El uso de SAML con StoreFront es similar al uso de SAMl 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

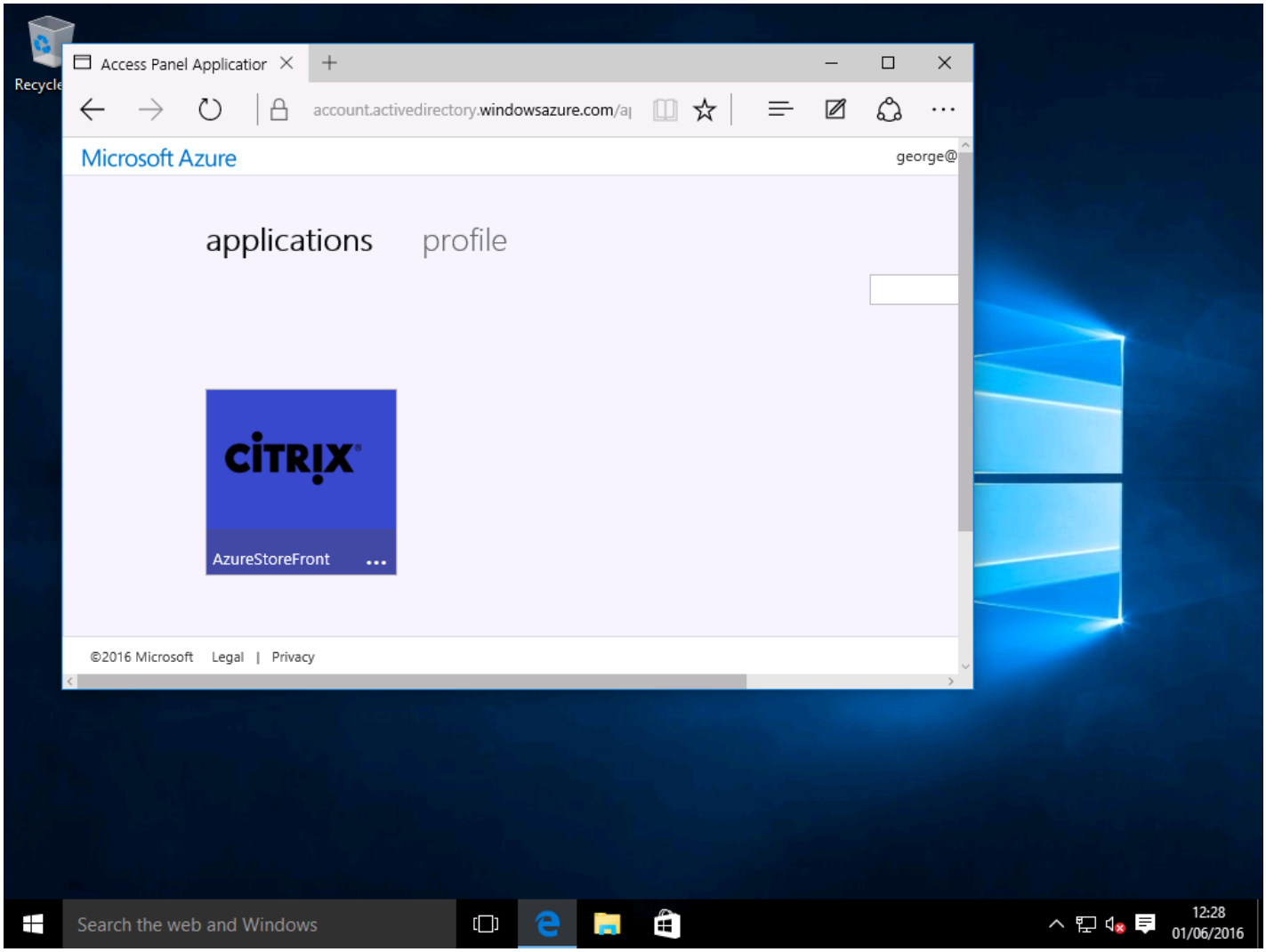


Verificar el sistema de extremo a extremo

Inicie sesión en un escritorio de Windows 10 unido a Azure AD, usando una cuenta registrada en Azure AD.Abra Microsoft Edge y conéctese a https://myapps.microsoft.com.

El explorador Web debe mostrar las aplicaciones de Azure AD para el usuario.

© 1999-2017 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).

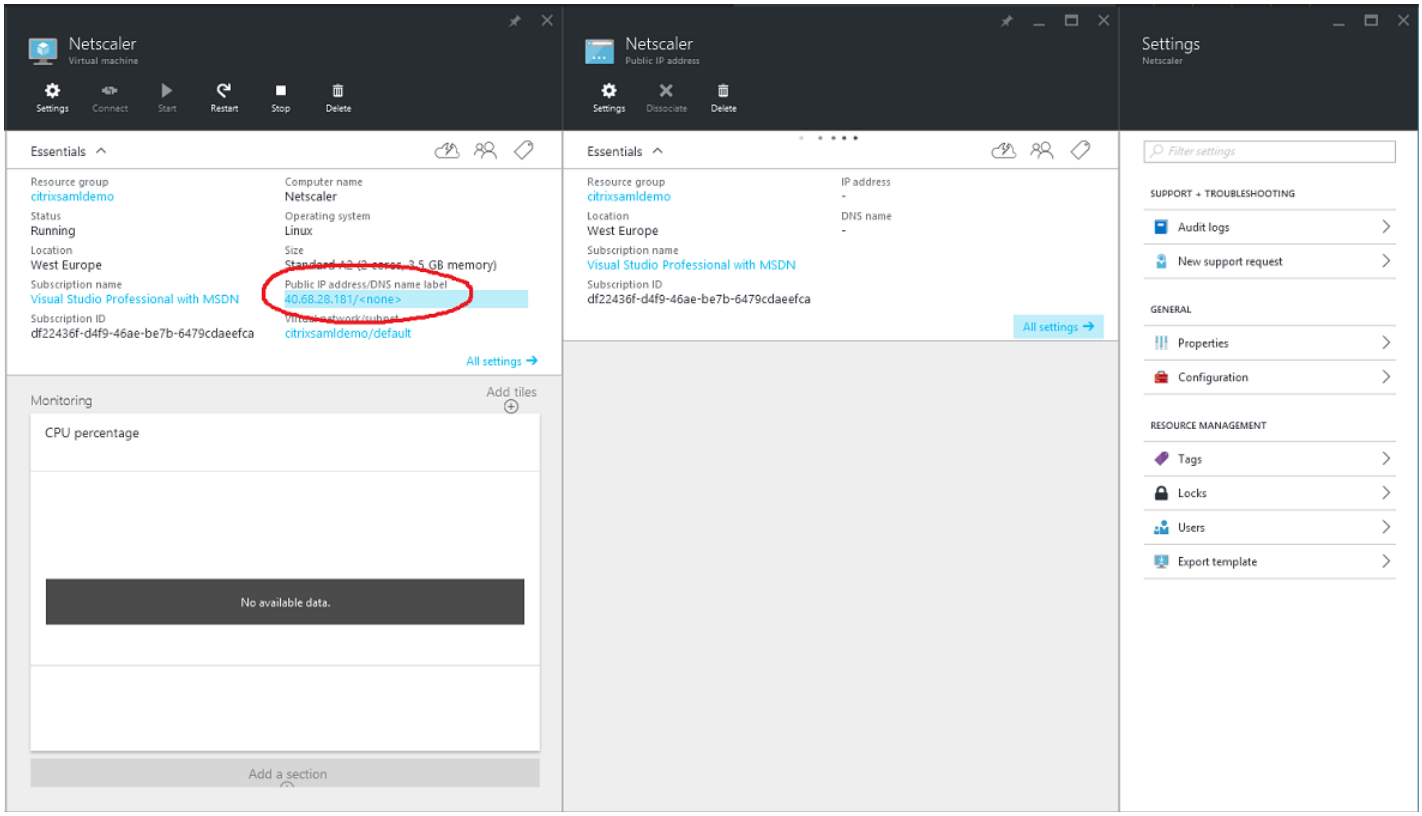
Apéndice

Deben configurarse algunas opciones estándar al configurar una VM en Azure.

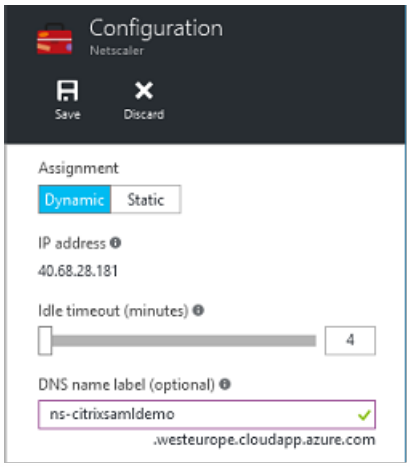
Proporcione una dirección IP pública y una dirección DNS

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.

© 1999-2017 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, con lo que todos los registros DNS apuntan correctamente a la VM incluso aunque la dirección IP se reasigne.



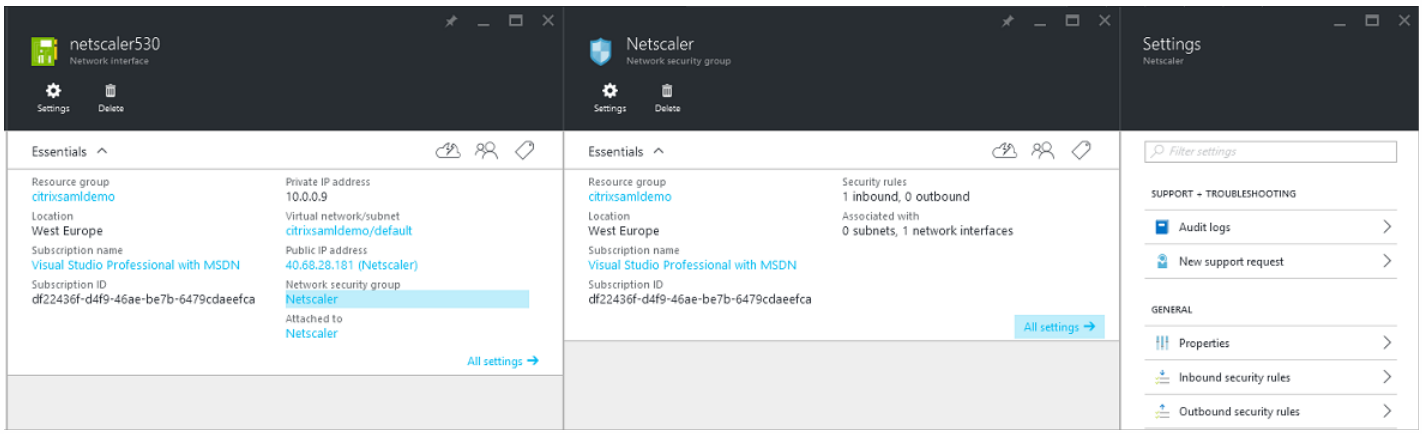
Configurar las reglas de firewall (grupo de seguridad)

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 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**

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Vista general de las arquitecturas del Servicio de autenticación federada.
- En el artículo Administración y configuración del Servicio de autenticación federada, se indican otros artículos de procedimientos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Procedimientos del sistema de autenticación federada: configuración y administración

Dec 05, 2017

Los siguientes artículos de procedimientos ofrecen instrucciones para la configuración y administración avanzadas del sistema de autenticación federada (FAS):

- Protección de la clave privada
- Configuración de la entidad de certificación (CA)
- Seguridad y administración de red
- Solución a 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 - Federated Authentication Service) es la referencia principal para la instalación y la configuración de este servicio.
- El artículo Vista general de las arquitecturas de Servicios de autenticación federada ofrece un resumen de las principales arquitecturas de FAS, además de enlaces con otros artículos sobre arquitecturas más complejas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración del servicio de autenticación federada para la entidad de certificación

Dec 05, 2017

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.

Configuración de 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.

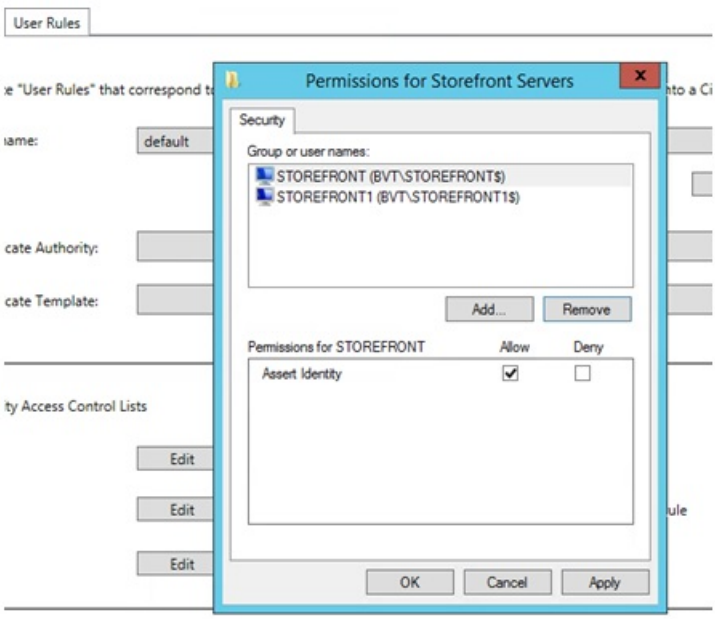
```
PS > Add-PSSnapin Citrix*
PS > Get-FASMsCertificateAuthority

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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

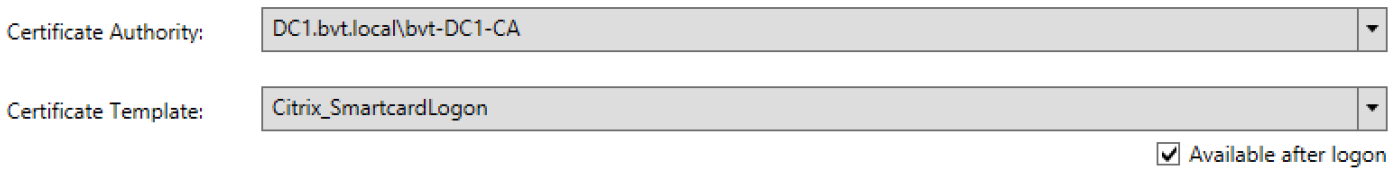


Para agregar varias entidades de certificación al campo de la entidad de certificación (característica que no se admite en la consola de administración de esta versión), debe configurar la definición de certificado. En primer lugar, necesita el nombre de la definición de certificado. Este nombre no se 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:

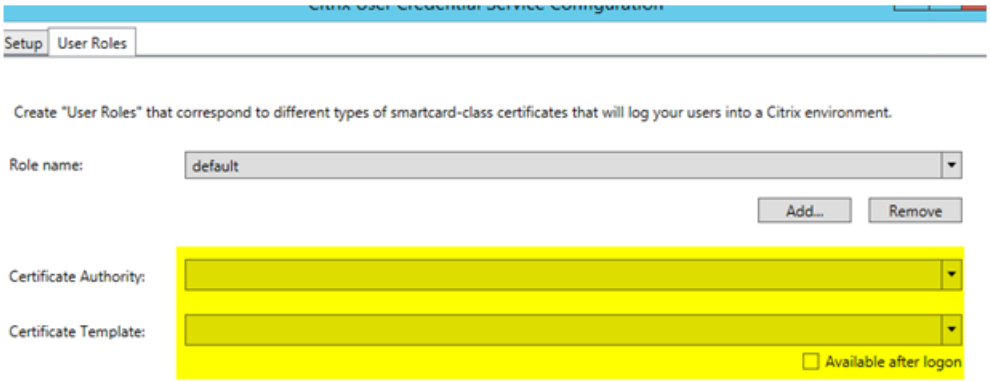
```
PS > Set-FASCertificateDefinition -Name default_Definition -CertificateAuthorities @("DC1.bvt.
local\bvt-DC1-CA", "ca1.bvt.local\CA1.bvt.local", "ca2.bvt.local\ca2.bvt.local")
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

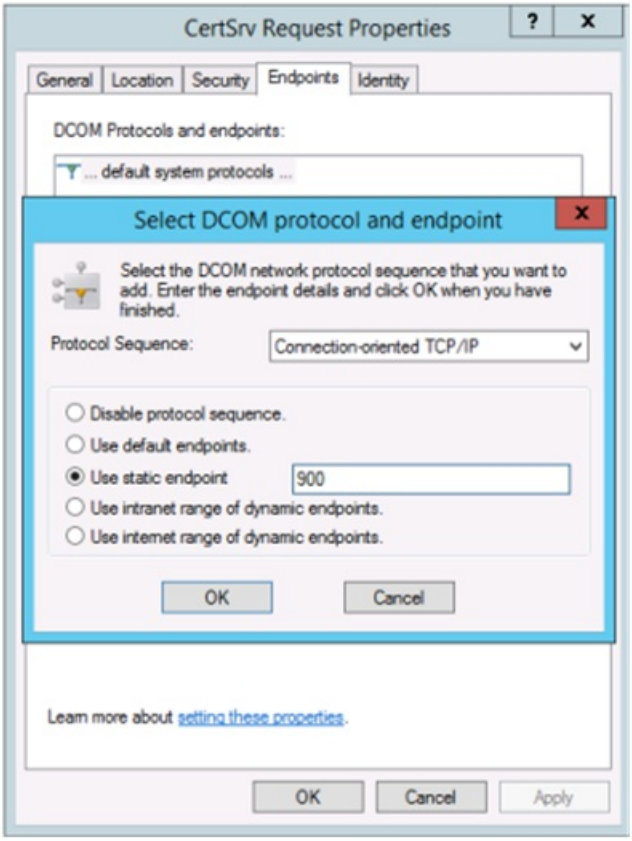
Cambios de comportamiento previstos

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.

Configuración de CA de Microsoft para el acceso por TCP

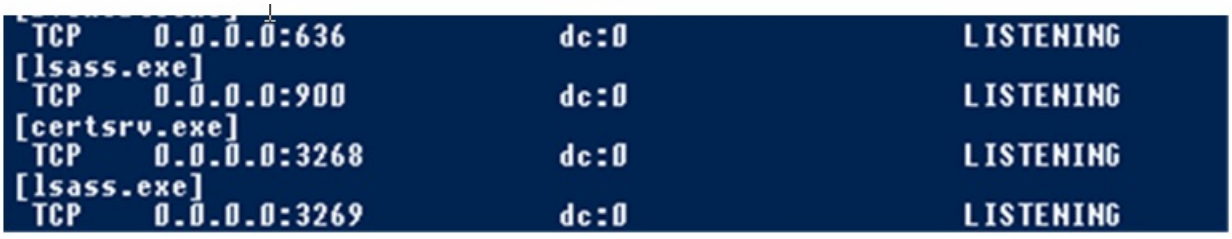
De forma predeterminada, la entidad de certificación de Microsoft utiliza DCOM para el acceso. Esto puede provocar complicaciones cuando se implemente la seguridad del firewall, por lo que Microsoft puede cambiar a un puerto TCP estático. En la entidad de certificación de Microsoft, abra el panel de configuración de DCOM y modifique las propiedades de “CertSrv Request”:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cambie los “extremos” para seleccionar un extremo 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 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.

Generación previa de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

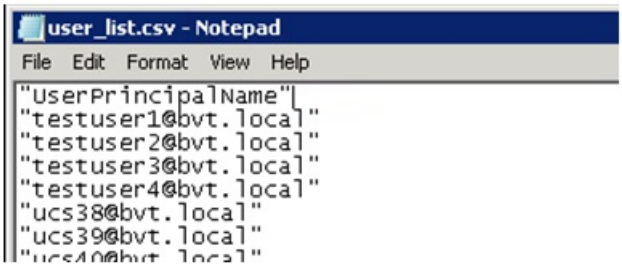
$searchbase = "cn=users,dc=bvt,dc=local" # AD User Base to Look for Users, leave it blank to search all
$filename = “user_list.csv” # Filename to save

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 "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:



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

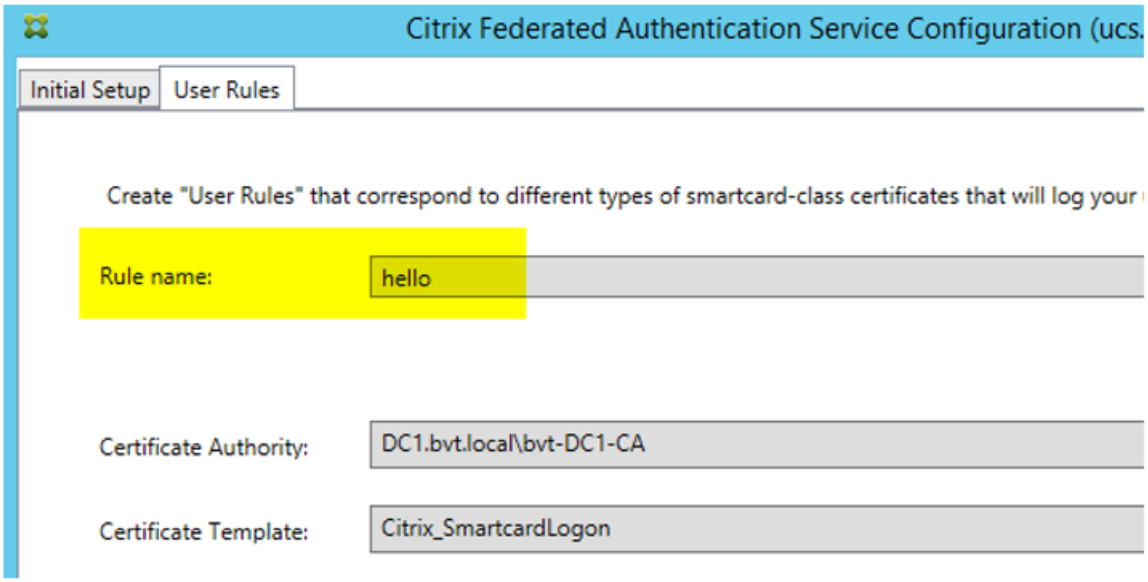
```
Add-PSSnapin Citrix.A*

$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.



Renovación de 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 volver a autorizar FAS,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 -MaintenanceMode $true

4. Cambie el nuevo certificado de autorización:

    Set-FasCertificateDefinition –AuthorizationCertificate

5. Desactive el modo de mantenimiento del servidor FAS:

    Set-FasServer –Address -MaintenanceMode $false

6. Elimine el certificado anterior de autorización:

    Remove-FasAuthorizationCertificate

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 Vista general de las arquitecturas de Servicios de autenticación federada.
- En el artículo Administración y configuración del servicio de autenticación federada se indican otros artículos de procedimientos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Protección de claves privadas para el servicio de autenticación federada

Dec 05, 2017

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 instalación 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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Establezca los valores correspondientes en el archivo Citrix.Authentication.FederatedAuthenticationService.exe.config como se muestra a continuación:

Citrix.TrustFabric.ClientSDK.TrustAreaJoinParameters.**ProviderLegacyCsp** (cambie entre CAPI y las API de CNG)

Valor	Comentario
Verdadero	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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/Key Storage Provider	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)

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.

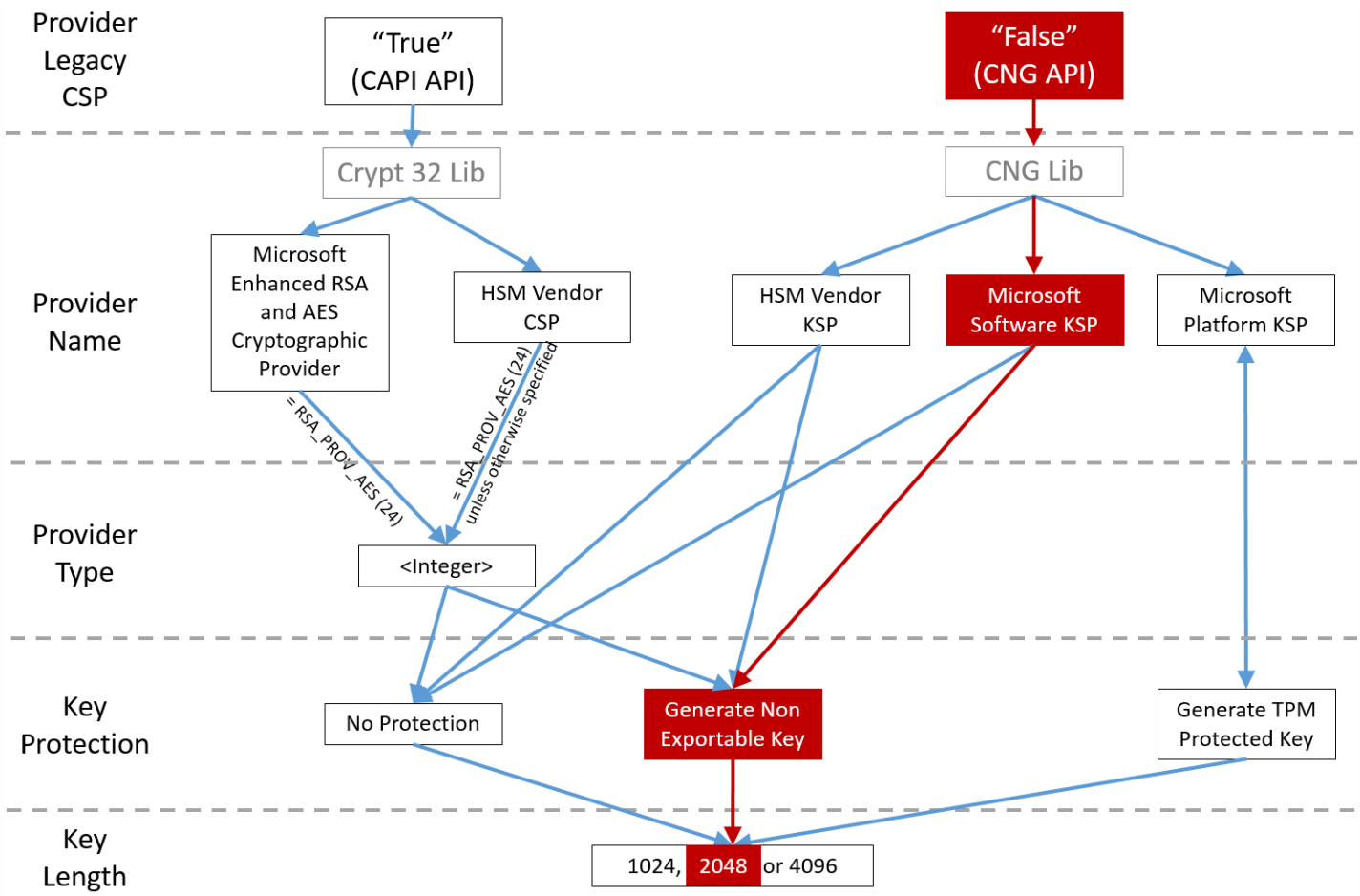
Valor	Comentario
NoProtection	Se puede exportar la clave privada.
GenerateNonExportableKey	Predeterminado. No se puede exportar la clave privada.
GenerateTPMProtectedKey	La clave privada se administrará mediante TPM. La clave privada se almacena mediante el nombre de proveedor que especifique en ProviderName (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):

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Ejemplos de configuración

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.

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.

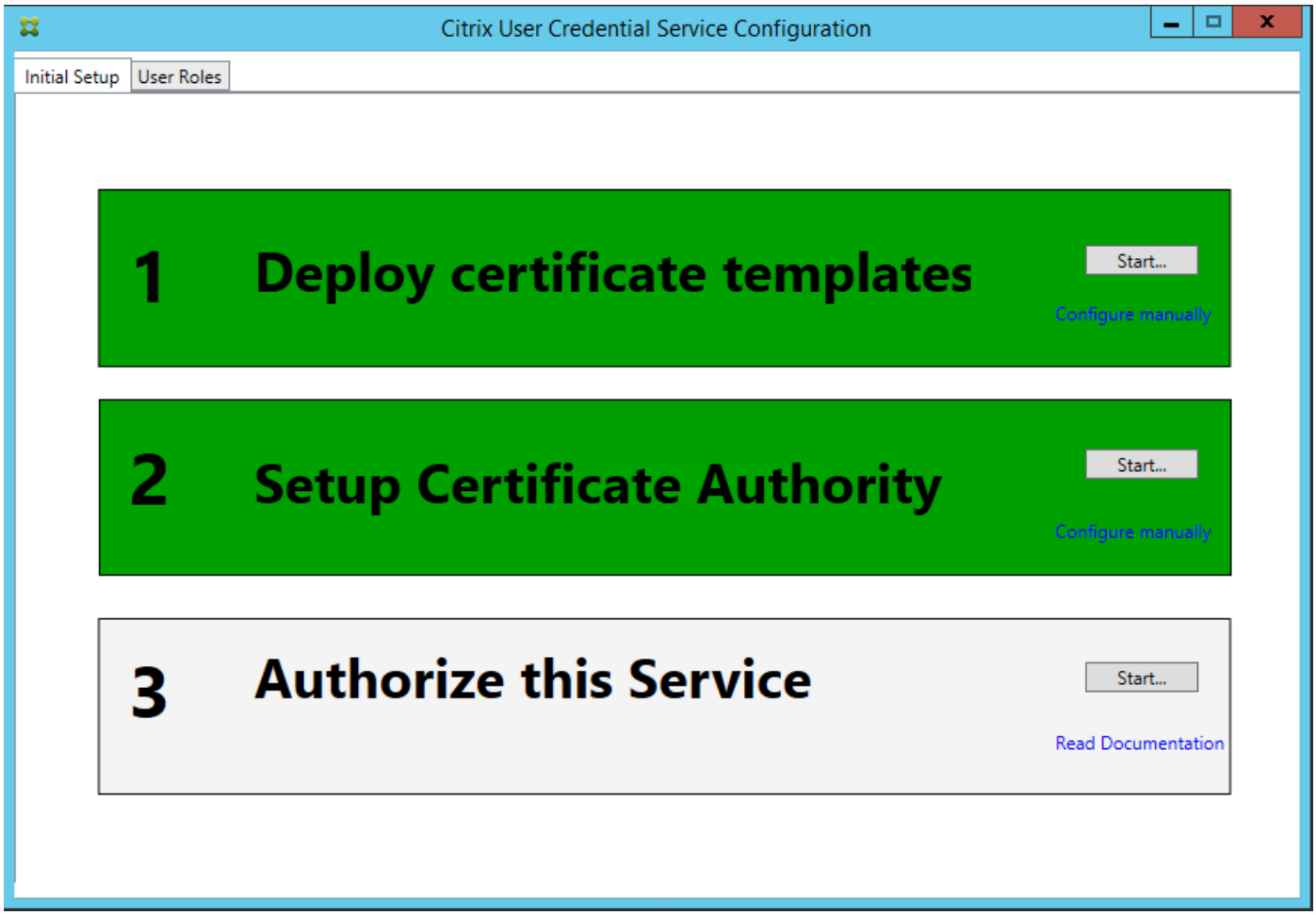
Uso de PowerShell (recomendado)

El certificado de RA se puede solicitar sin conexión mediante PowerShell. Se recomienda en empresas que no quieran que su

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

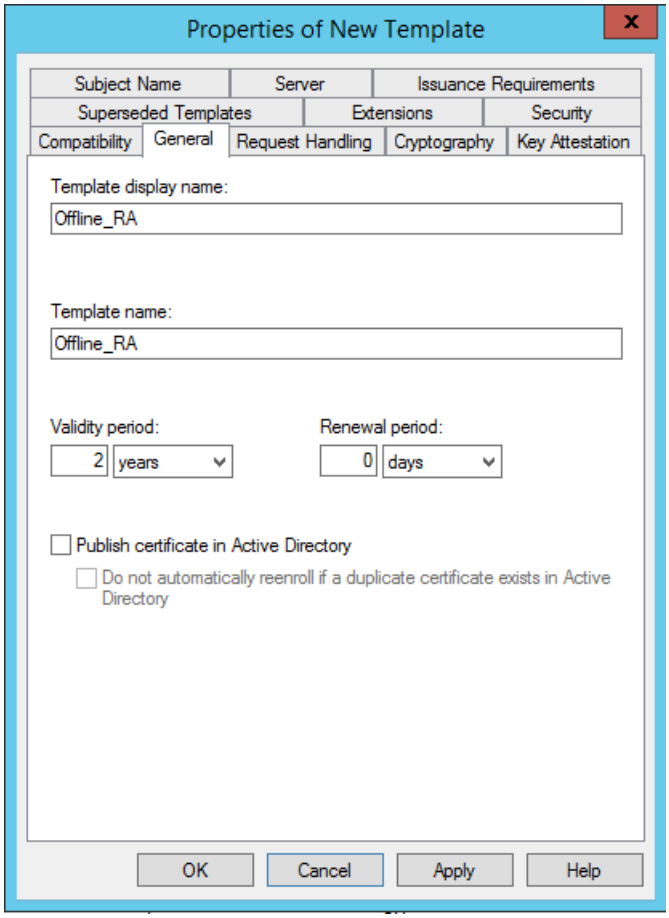
Paso 1: Durante la configuración inicial de FAS con la consola de administración, complete solo los primeros dos pasos, es decir, implemente las plantillas de certificado y configure la entidad de certificación.



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_ManualAuthorization** 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Paso 3: En el servidor de la entidad de certificación, agregue el complemento MMC de ésta. 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:

```
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 los siguientes cmdlets 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
```

Por ejemplo:

```
New-FasAuthorizationCertificateRequest -UseTPM $true -address fashsm.auth.net
```

Aparecerá lo siguiente:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
PS C:\Users\Administrator.AUTH> New-UcsAuthorizationCertificateRequest -UseTPM $true -address ucshsm.auth.local

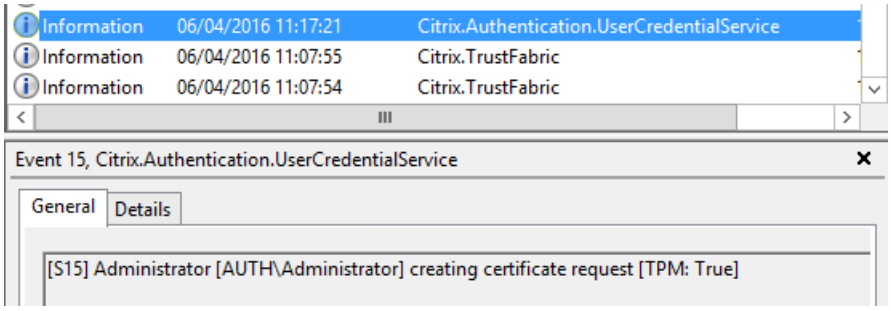
Id                  : 5ac3d8bd-b484-4ebe-abf8-4b2cfd62ca39
Address             : [Offline CSR]
TrustArea           :
CertificateRequest  : -----BEGIN CERTIFICATE REQUEST-----
                      MIICaDCCAVACAQIwIzEhMB8GCgmSJomT8ixkARkWEUNpdHJpeFRydXNORmFicmljMIIBIjANBgkq
                      hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwAtwoCLXJuJ3yIscT8Y5v/7zuYqBhbHkhZV3wTNfROXW
                      lhCMwi7X4YpTE7CbJtgiFY/9SEBa9StGeTVpeJi66gKoZCdxydc2BwX6JNZrLi9hAflbInFPgrz+
                      vbG3YjKuKtK35JpGqYWjUEDzKiQFaob3Dkh/pwP3V7DcEYthxB8CfbaN9MHOEFbepoSYOCAfunXW
                      snwIbXD9lc/fGyN/3f94P4fbNrjEIOHc+4Oy/WsPgPBgcq9XBwRjzpGjOgOWRoJS9g22OY5PwD77
                      7f7vZvoQkRy5N%%%ATJ+xxYEPLp9JuJaE1W%rTJG+%P3SnG/oCCPit7iUIIc9FjGa3qTUQIDAQAB
                      oAAwDQYJKoZIhvcNAQENBQADggEBAIJV8jR9%WHIvztpjxPeJzAVDsrLpOsCfNdvYn9u+I7J8Gsr
                      4tuLjuQ+An4Y2Rw7b6pZxEICU8rqd5Gy+wtPnUZoAf6eLg1Vht2RVfb6d7Ns6+Mc+F5bFegLHs8c
                      YlITNOtmcHFKt4Loz5D5E+tQw39MProEj3p7GwF7HrGY+QSbFD38rbL19Z5cfNYYqMbsgyMgdR8F
                      3SmagQjN3C8lyqT8z1iF4l32xlmQrP/4%Qvr1F+TD15PM5Fxjj6PEKWopWTYZ%GzSC1ufxevcO1K
                      +tTH9tQYJM6xw3+6TIcfuWDjrd8KJjTdC5SMu7LJuIajTNZ5Z+1eM61TAT03%G/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.
- 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.

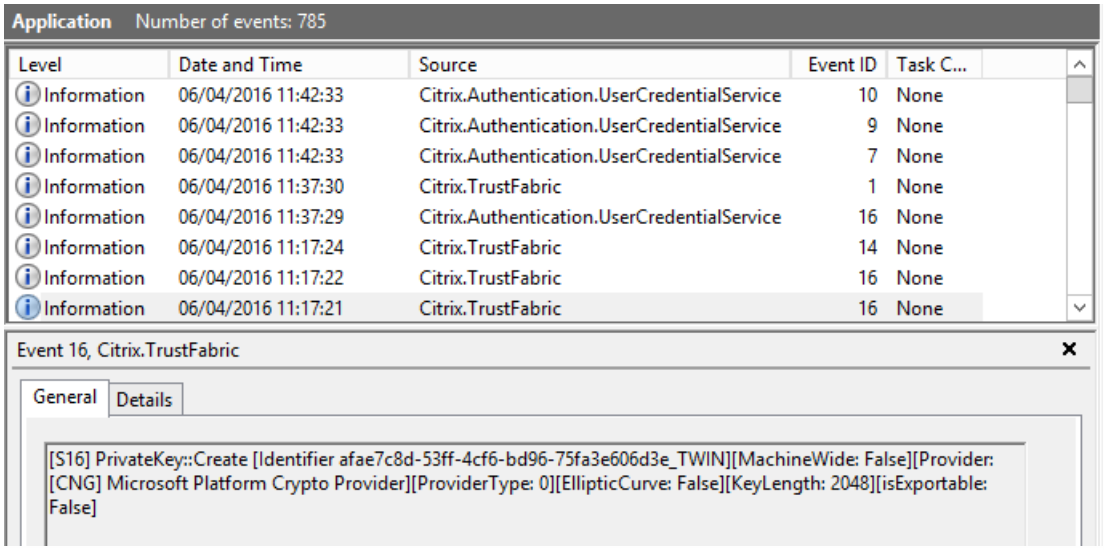
Para verificar que se haya utilizado el TPM para generar el par de claves, abra el registro de la aplicación en el visor de eventos de Windows que está presente en el servidor FAS y consulte el momento en que se generó el par de claves.



Nota: “[TPM: True]”

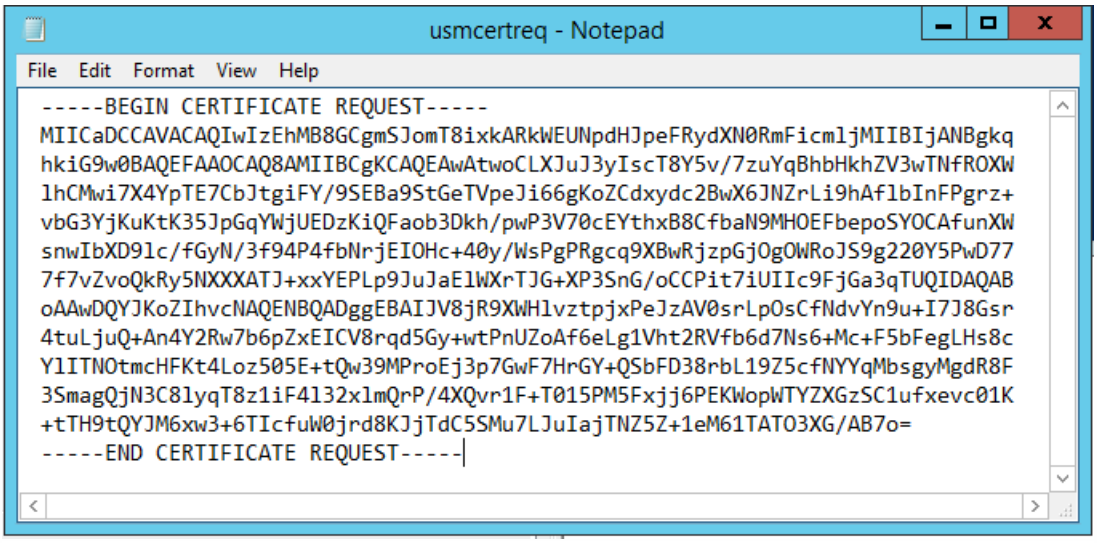
Seguido de:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



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:"

Por ejemplo:

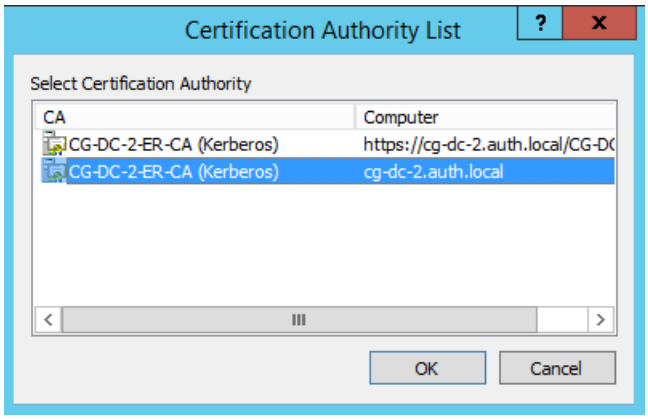
certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt

Aparecerá lo siguiente:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Desktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-DB0C-4D21-A4FD-2E29502177C2}
  ldap:
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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:



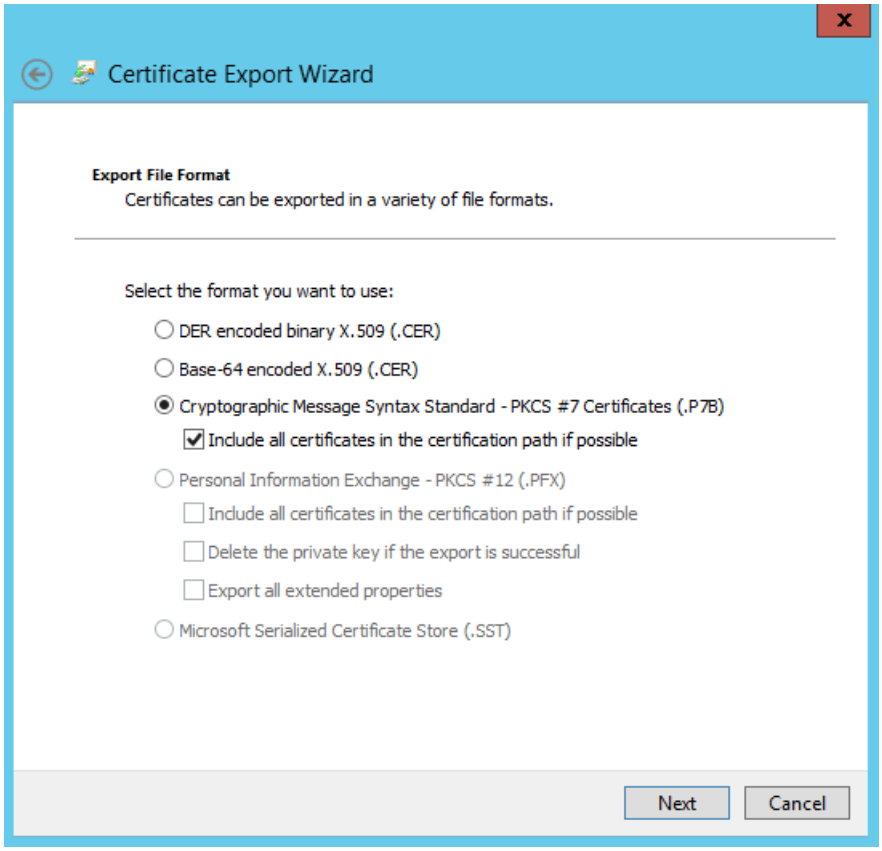
Tras especificar la entidad de certificación (CA), PowerShell pide el ID de la solicitud mediante RequestID:

```
PS C:\Users\Administrator.AUTH> certreq -submit -attrib "certificatetemplate:Offline_RA" C:\Users\Administrator.AUTH\Des
ktop\usmcertreq.txt
Active Directory Enrollment Policy
  {4F7616DE-0B0C-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 estas opciones para el formato de archivo:

© 1999-2017 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 Registro del servidor FAS. Para ello, introduzca los siguientes cmdlets 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
```

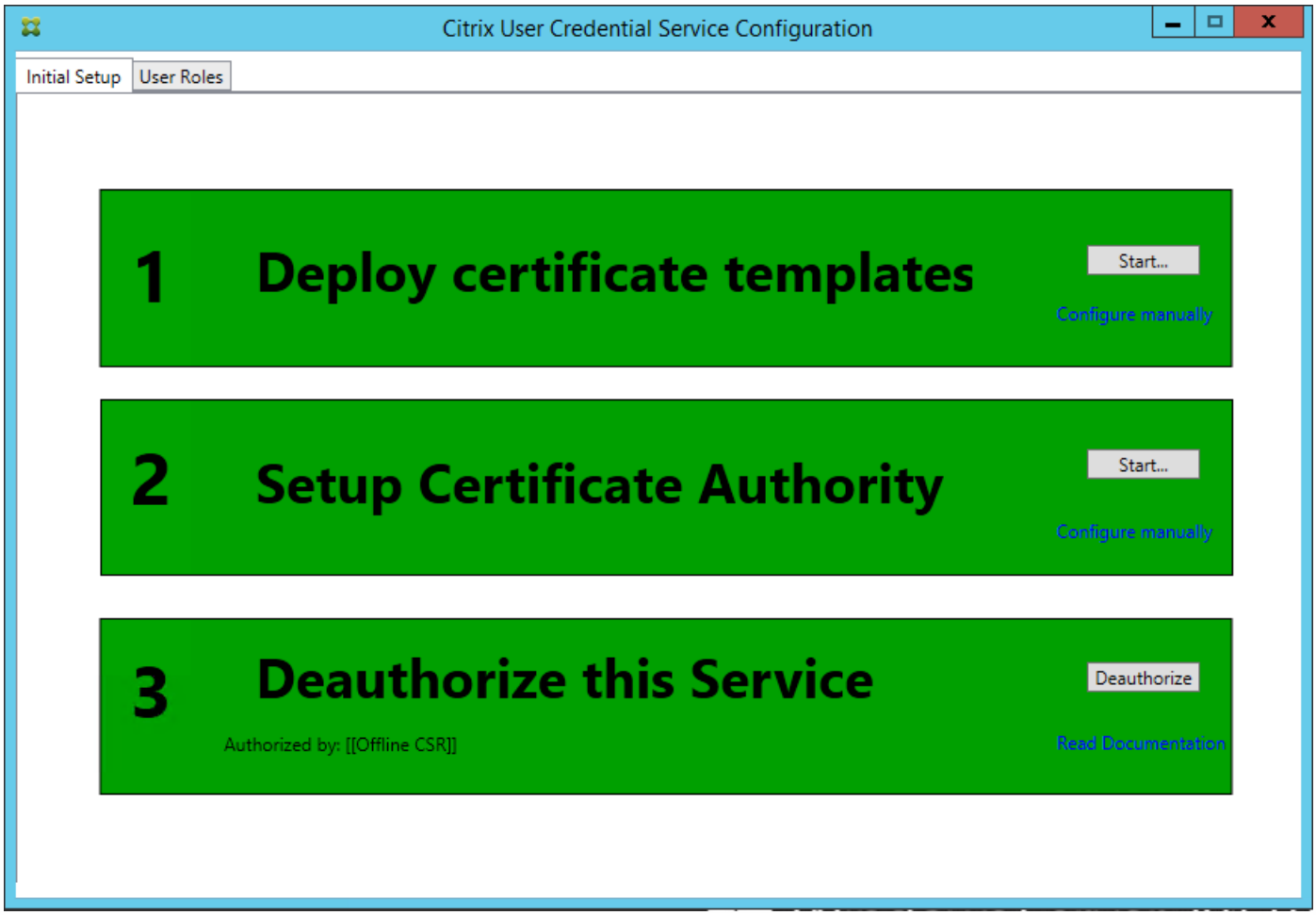
Aparecerá lo siguiente:

```
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-8963-16ec311020fc
CertificateRequest  :
Status              : Ok
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paso 12: Cierre la consola de administración FAS y reiníciela.



Verá que el paso “Authorize this Service” pasa a ser verde y ahora aparece “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

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"/>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Especifique una longitud de clave que su hardware admita.

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 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

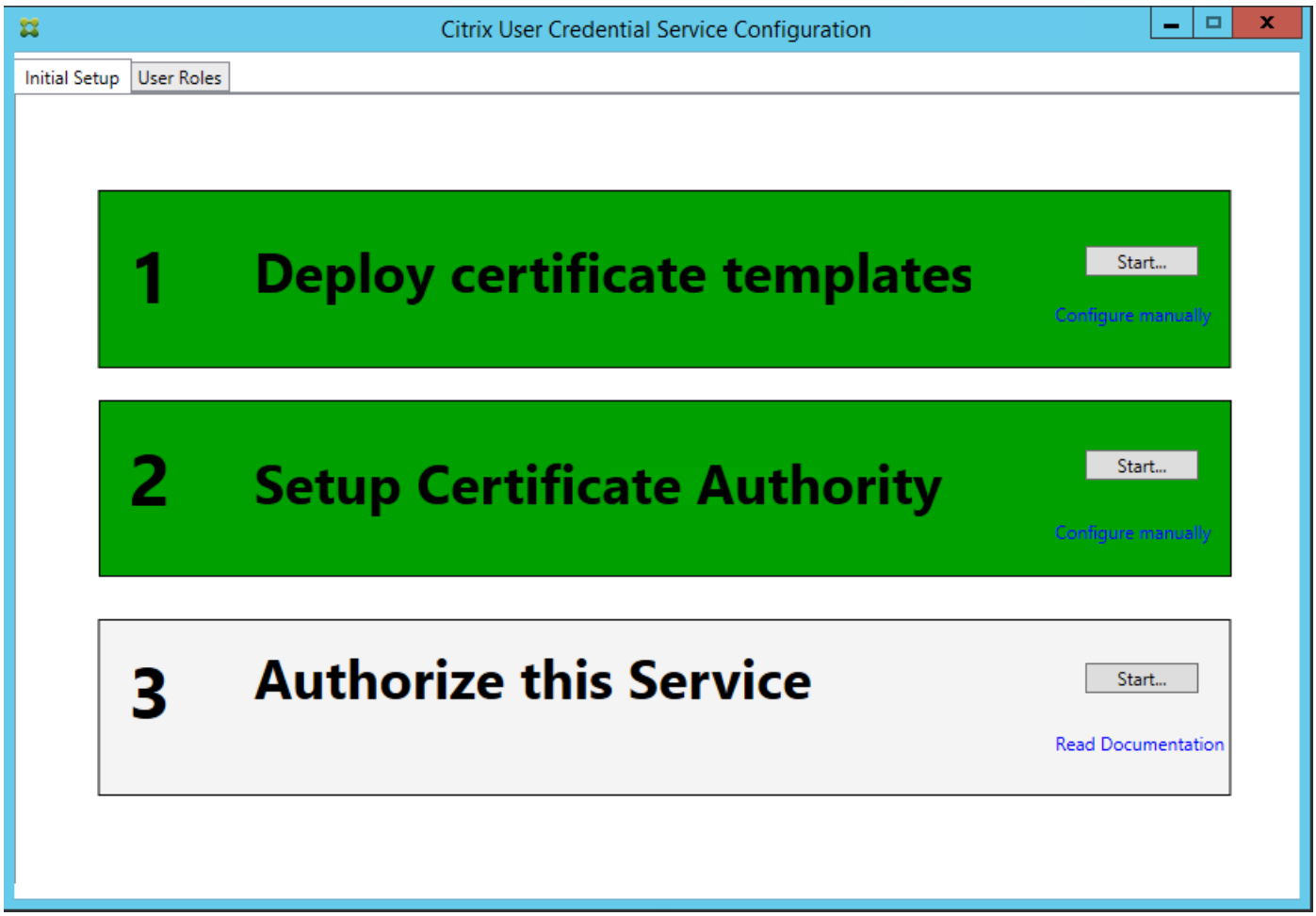
© 1999-2017 Citrix Systems, Inc. All rights reserved.

usuario.

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.



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"/>
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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="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]

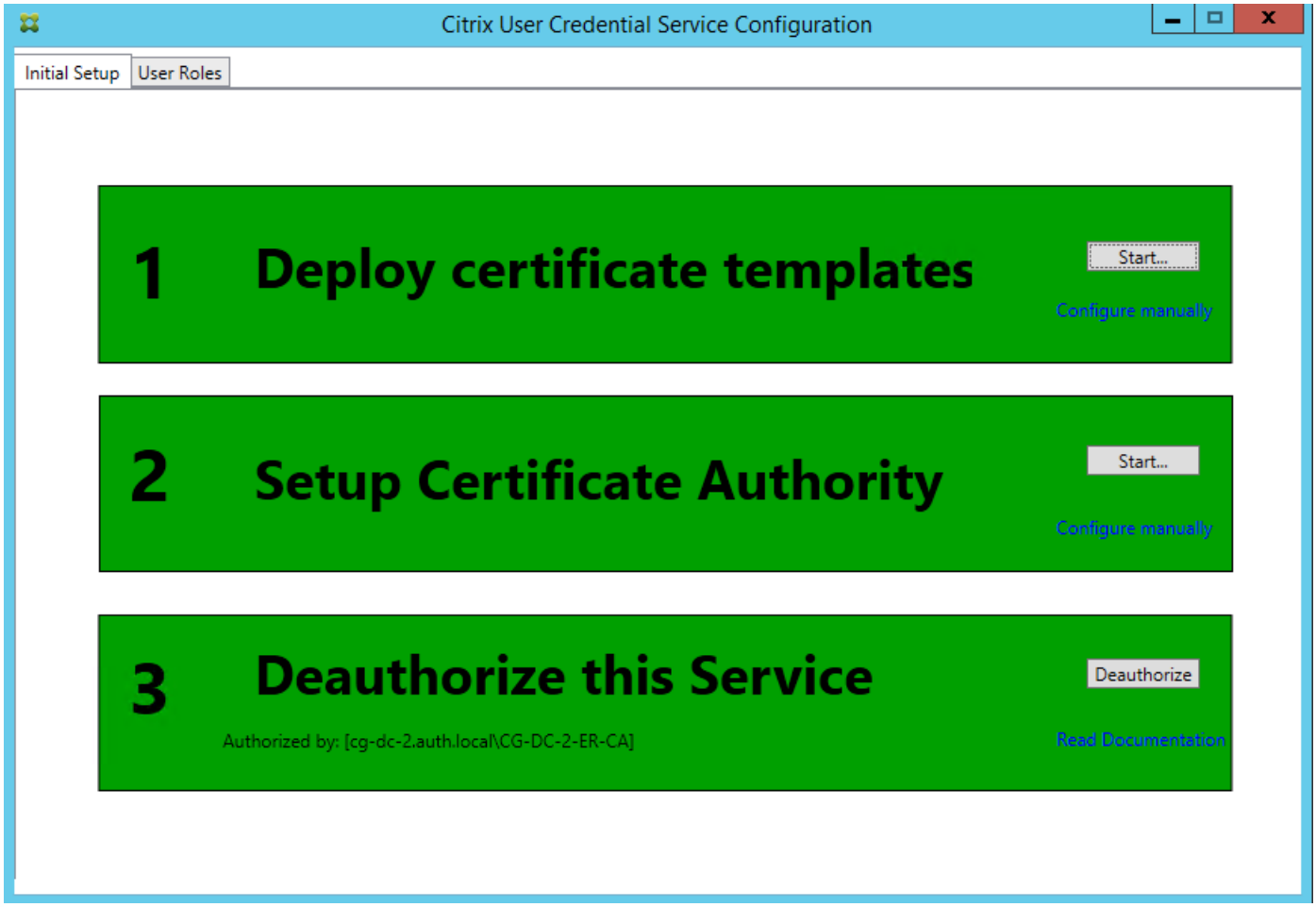
Paso 7: En el servidor de la entidad de certificación, en el complemento MMC de esta, seleccione el nodo **Solicitudes pendientes**:

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$	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Haga clic con el botón secundario en la solicitud y seleccione **Emitir**.

Verá que el paso “Authorize this Service” pasa a ser verde y ahora aparece “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. En su lugar, utiliza el Registro para ello.

Nota: Al usar un HSM para almacenar las claves privadas, los contenedores de HSM se identifican con un GUID. El GUID de la clave privada en el HSM coincide con el GUID del certificado equivalente en el Registro.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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/lBb3elZKA4OOoi9Ou64Q916
                     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

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
```

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 Vista general de las arquitecturas de Servicios de autenticación federada.
- En el artículo Administración y configuración del servicio de autenticación federada se indican otros artículos de procedimientos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Seguridad y configuración de red del Servicio de autenticación federada

Dec 05, 2017

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.

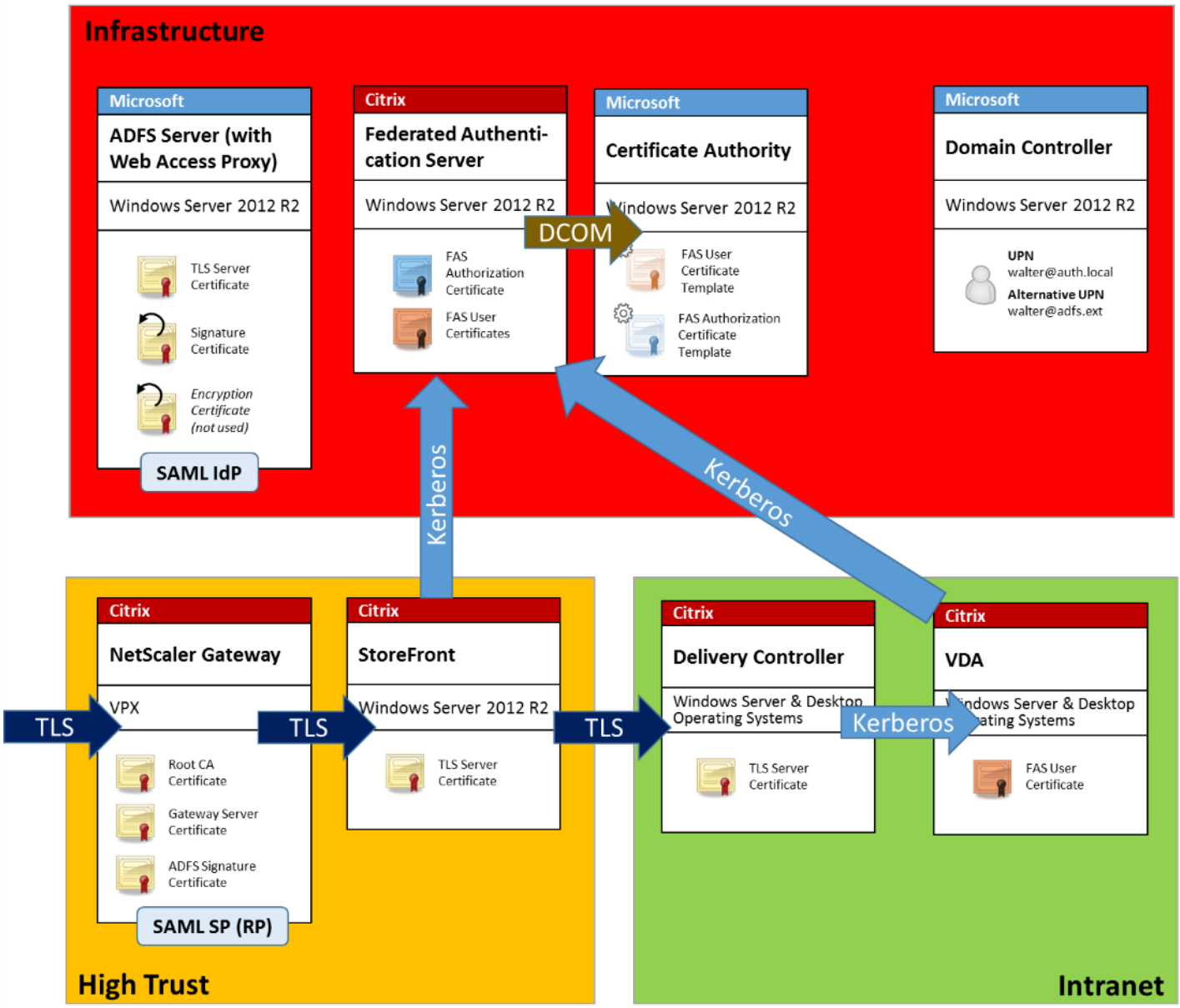
Este documento presenta un resume de las cuestiones de seguridad que se deben tener en cuenta al implementar los servicios FAS. También proporciona una visión general de las características disponibles que pueden ayudarle a proteger su infraestructura.

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 XenApp y XenDesktop no se ven afectados por la introducción de FAS.

© 1999-2017 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 NetScaler 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.La autenticación utiliza la identidad Kerberos HOST/FQDN del servidor FAS y la identidad Kerberos de la cuenta de máquina del servidor StoreFront.Esto 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Servidor	Puertos de firewall
Servicio de autenticación federada	[entrada] Kerberos sobre HTTP desde StoreFront y VDA [salida] DCOM hacia la entidad de certificación (CA) de Microsoft
NetScaler	[entrada] HTTPS desde máquinas cliente [entrada/salida] HTTPS desde y hacia los servidores StoreFront [salida] HDX hacia VDA
StoreFront	[entrada] HTTPS desde NetScaler [salida] HTTPS hacia Delivery Controller [salida] Kerberos HTTP hacia FAS
Delivery Controller	[entrada] HTTPS desde servidores StoreFront [entrada/salida] Kerberos sobre HTTP desde VDA
VDA	[entrada/salida] Kerberos sobre HTTP desde Delivery Controller [entrada] HDX desde NetScaler 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenDesktop	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.

Configuración de directivas de grupo

Las máquinas FAS de confianza se identifican en una tabla de búsqueda de "número de índice -> FQDN" configurada mediante Directiva de grupo. Al contactar con un servidor FAS, los clientes verifican la identidad Kerberos HOST\ 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. Modifique la lista de servidores de FAS con cuidado, 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. No reutilice 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.

Cambio del 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

publicar la plantilla, y

- Utilice el comando New-FasCertificateDefinition para configurar FAS con el nombre de su plantilla.

Modificación de 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.

Modificación de 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**.

Modificación de 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.

Modificación de propiedades de atestación de clave

No modifique estas propiedades. FAS no admite la atestación de la clave.

Modificación de propiedades de plantillas reemplazadas

No modifique estas propiedades. FAS no admite la sustitución de plantillas.

Modificación de propiedades de extensiones

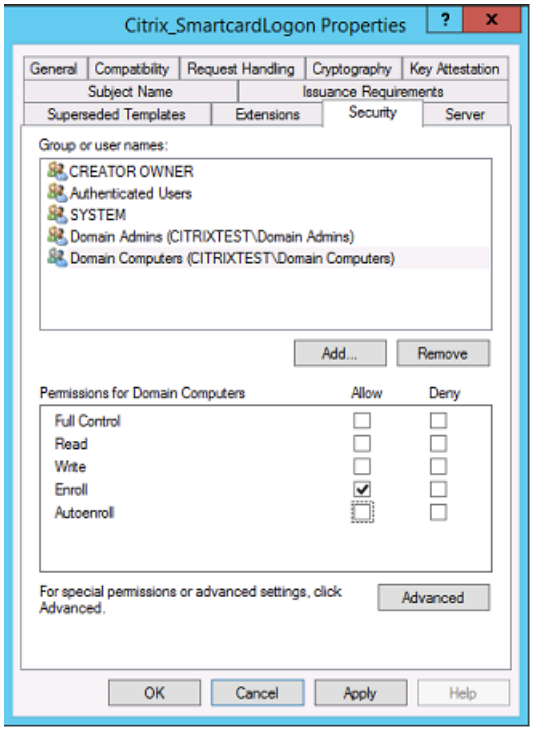
Puede modificar estas opciones de configuración para que coincidan con la directiva de la organización.

Nota: Una configuración inadecuada de las extensiones puede causar problemas de seguridad o resultar en certificados inutilizables.

Modificación de 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. Es posible que le interese conceder otros permisos; por ejemplo, para permitir que los administradores de FAS vean una plantilla modificada para solucionar problemas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Modificación de propiedades de nombre del sujeto

Si fuera necesario, puede modificar estas opciones de configuración para que coincidan con la directiva de la organización.

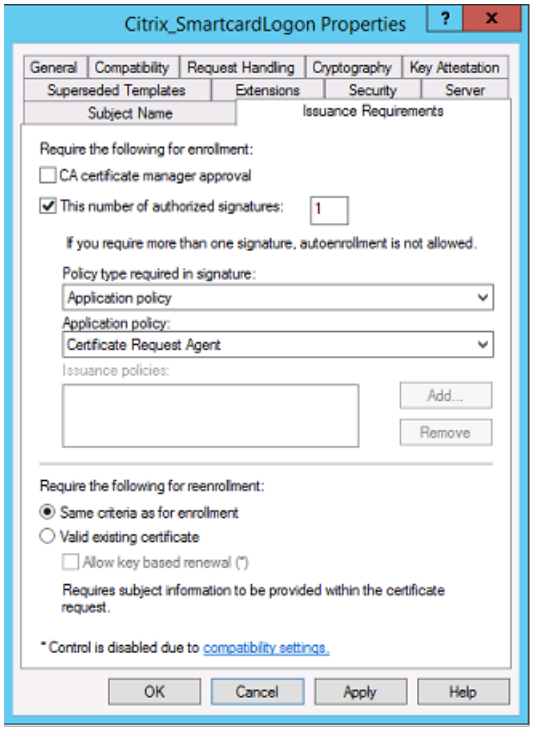
Modificación de propiedades de servidor

Aunque Citrix no lo recomienda, puede modificar estas opciones de configuración para que coincidan con la directiva de la organización si fuera necesario.

Modificación de propiedades de requisitos de emisión

No modifique estos parámetros. Estos parámetros deben ser como se muestra a continuación:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Modificación de 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).

Administración de 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.

Publicación de 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.

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.

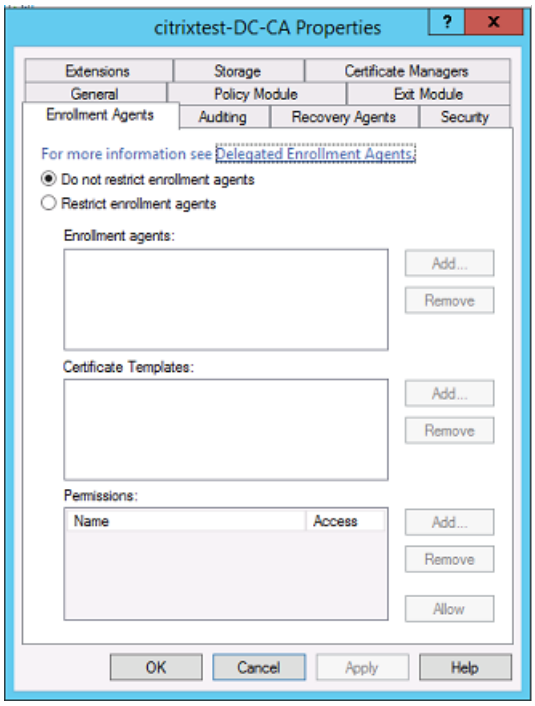
Parámetros de firewall

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.Esto debe restringirse a un grupo de usuarios sin privilegios con la ayuda de la propiedad “Restringir agentes de inscripción” de la CA.



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.

Administración de 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
StoreFront [IdP]	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.
VDA [entidad de confianza]	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	que una cuenta de VDA de este grupo que esté en situación de riesgo tendrá un ámbito muy limitado para atacar el sistema.
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 XenApp o XenDesktop 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.

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, por lo menos, la clave privada del certificado de RA esté protegida almacenándola en un módulo TPM; esta opción se suministra 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 de "Administradores locales” tienen control total sobre la configuración de FAS. Esta lista se debe mantener con cuidado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administradores XenApp, XenDesktop y VDA

En general, el uso de FAS no cambia el modelo de seguridad de Delivery Controller y los administradores de VDA, 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. Aquellos servidores de la infraestructura que sean vitales 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.

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 Vista general de las arquitecturas de Servicios de autenticación federada.
- En el artículo Administración y configuración del servicio de autenticación federada se indican otros artículos de procedimientos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Dec 05, 2017

En este artículo:

- Certificados e infraestructura de clave pública
- Nombre UPN y asignación de certificados
- Control en la selección del controlador de dominio para iniciar sesión
- Habilitación de eventos de auditoría de cuentas
- Registros de validación de certificados
- Registros Kerberos
- Mensajes del registro de sucesos
- Mensajes de error del usuario final
- Información relacionada

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 @ y @, es decir, @ y @.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 del 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Control en 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.

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

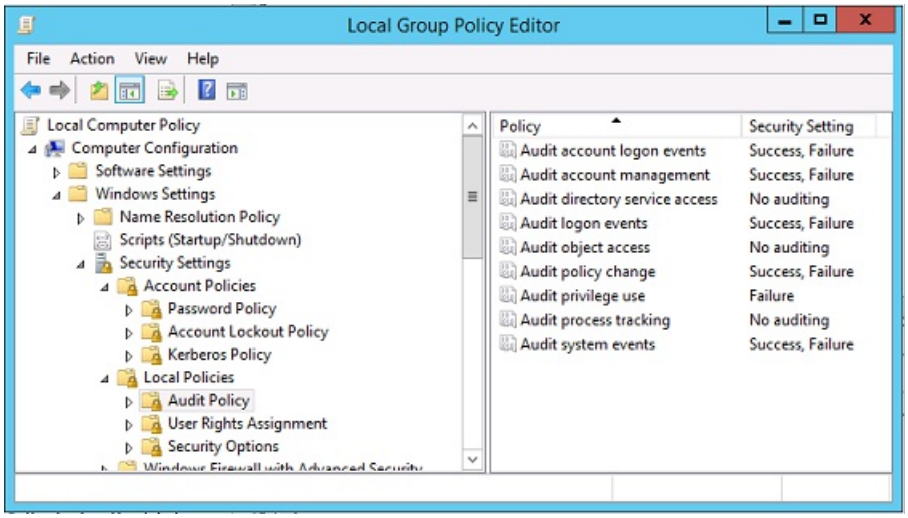
Durante el inicio de sesión, Windows aplica una variable de entorno MSDOS con el controlador de dominio que inició la sesión del usuario.Para verlo, inicie el símbolo del sistema con el comando: **echo %LOGONSERVER%**.

Los registros relacionados con la autenticación se almacenan en el equipo que devuelva este comando.

Habilitación de 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.

© 1999-2017 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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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\Kerberos\Parameters	LogLevel	0x1
CurrentControlSet\Control\Lsa\Kerberos\Parameters	KerbDebuglevel	0xffffffff
CurrentControlSet\Services\Kdc	KdcDebugLevel	0x1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

CurrentControlSet\Services\Kdc	KdcExtraLogLevel	0x1f

El registro Kerberos se guarda en el registro de eventos del sistema.

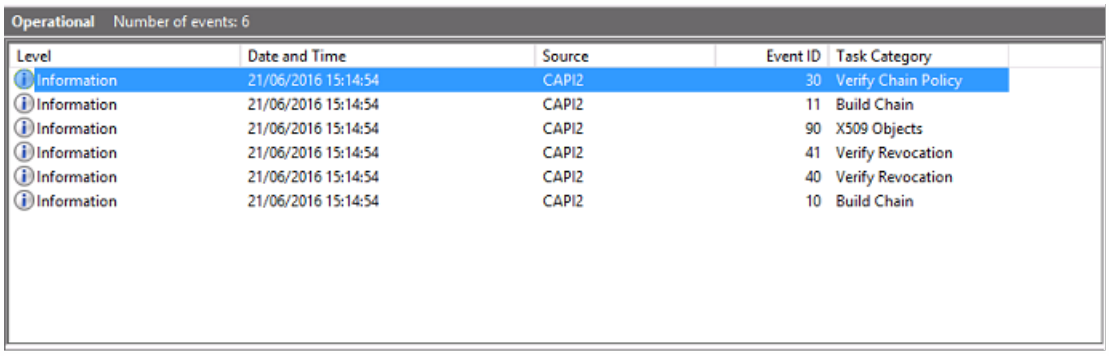
- Los mensajes del tipo "El certificado no es de confianza" deberían ser fáciles de diagnosticar.
- Hay dos códigos de error que son informativos y se pueden ignorar sin consecuencias negativas:
  - KDC_ERR_PREAUTH_REQUIRED (utilizado para la compatibilidad con versiones anteriores de controladores de dominio)
  - 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
- Registro de seguridad del controlador de dominio
- Registro de seguridad del VDA
- Registro de CAPI del VDA
- Registro del sistema del VDA

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 lsass.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".

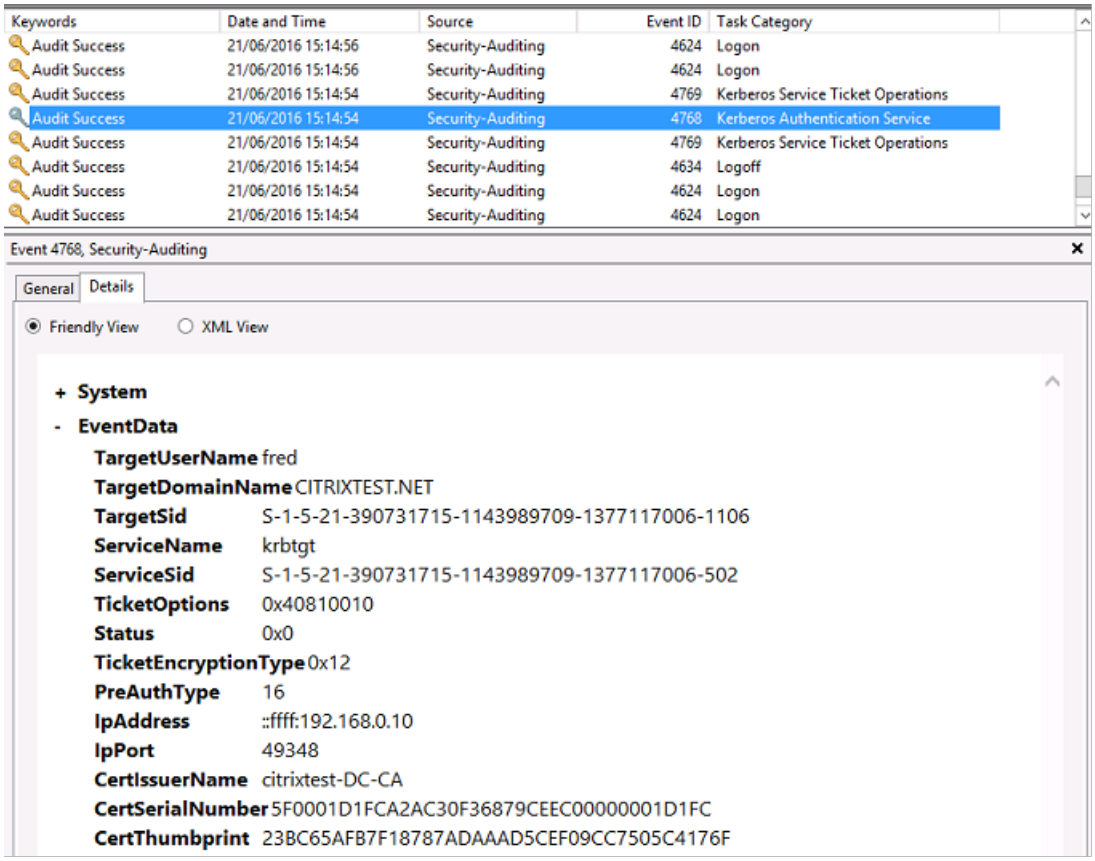
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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

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).

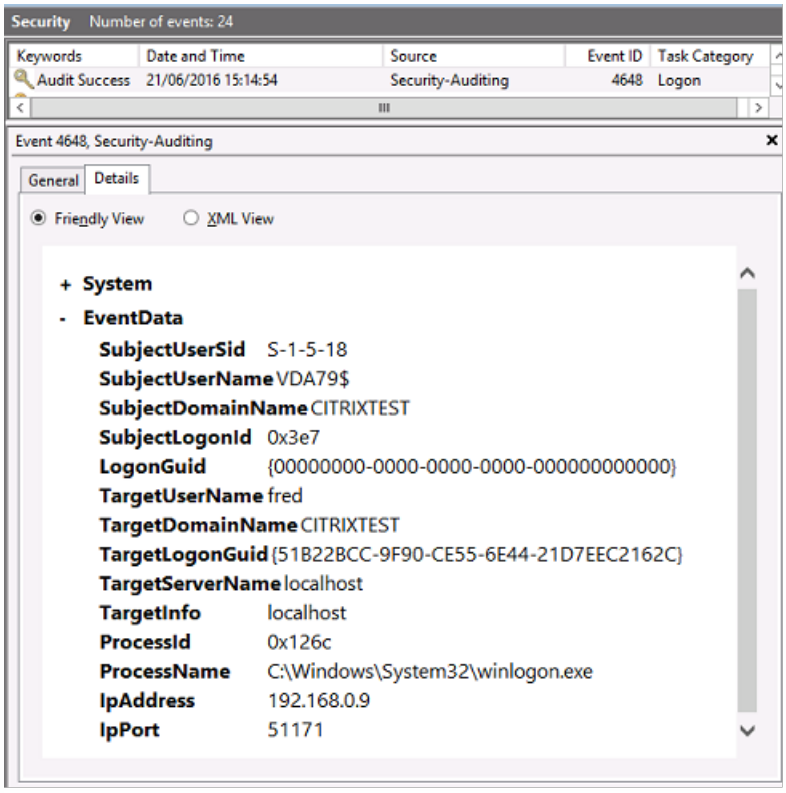
Los mensajes anteriores a este muestran la cuenta de máquina del servidor que se autentica en el controlador de dominio.Los mensajes siguientes muestran la cuenta de usuario que pertenece al nuevo vale krbtgt que se usa para autenticarse en el controlador de dominio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

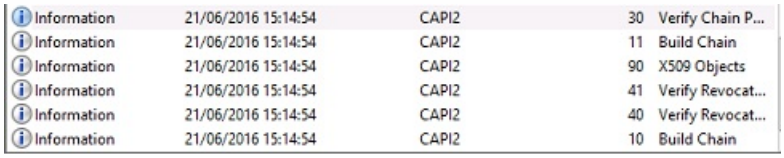


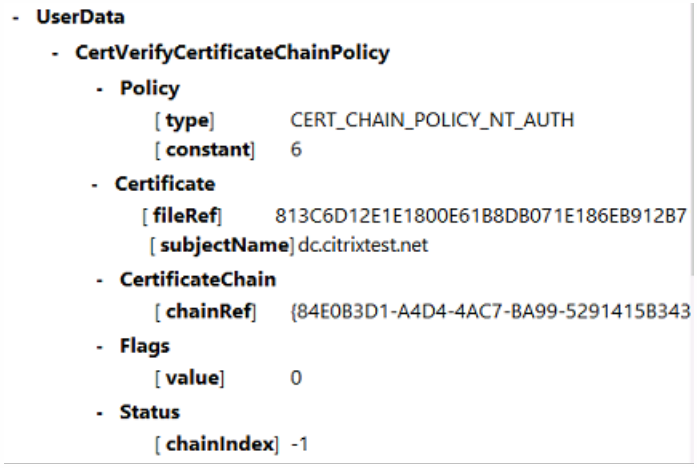
El registro de auditoría de seguridad del VDA que corresponde al evento de inicio de sesión es la entrada cuyo ID de evento es 4648, originado de winlogon.exe.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



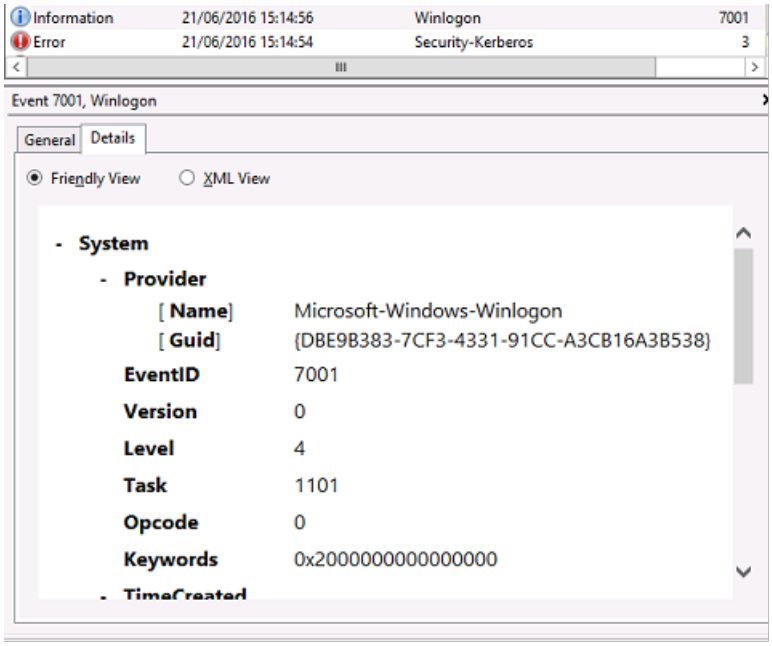
En este ejemplo, el registro de CAPI del VDA muestra una sola secuencia de compilación de cadena y comprobación desde lsass.exe, que valida el certificado del controlador de dominio (dc.citrixtest.net).





 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



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	Los certificados intermedios y de raíz no están instalados

© 1999-2017 Citrix Systems, Inc. All rights reserved.

el estado de revocación del certificado de la tarjeta inteligente usado para la autenticación.	en el equipo local. Consulte CTX206156 para obtener instrucciones sobre la instalación de certificados de tarjeta inteligente en equipos sin dominio. Además, consulte la sección Certificados e infraestructura de clave pública en este artículo.
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.
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	tarjeta inteligente debe restablecerse a los parámetros de fábrica.
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

- Configuración de un dominio para el inicio de sesión con tarjeta inteligente: http://support.citrix.com/article/CTX206156
- Directivas de inicios de sesión con tarjeta inteligente: https://technet.microsoft.com/en-us/library/ff404287%28v=ws.10%29.aspx
- Habilitación de captura de registros de CAPI: http://social.technet.microsoft.com/wiki/contents/articles/242.troubleshooting-pki-problems-on-windows.aspx
- Habilitación de 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 externas de certificación: https://support.microsoft.com/es-es/kb/281245

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cmdlets de PowerShell del Servicio de autenticación federada (FAS)

Dec 05, 2017

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:

```
Add-PSSnapin Citrix.Authentication.FederatedAuthenticationService.V1
```

En una ventana de PowerShell, use Get-Help <*nombre del cmdlet*> para ver la ayuda del cmdlet.

El archivo zip del enlace siguiente contiene archivos de ayuda para todos los cmdlets de PowerShell para FAS. Para usarlo, haga clic en el enlace, lo que descargará el archivo zip. A continuación, extraiga su contenido en una carpeta local. El archivo index.html enumera todos los cmdlets, con enlaces a cada uno de sus archivos de ayuda.

Archivos de ayuda para los cmdlets de PowerShell del Servicio de autenticación federada (FAS)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gráficos

Dec 05, 2017

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 XenApp y XenDesktop. 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 (por ejemplo, OpenGL Software Accelerator). La generación 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 XenApp y XenDesktop.

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 XenApp y XenDesktop 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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

OpenGL Software Accelerator

OpenGL Software Accelerator es un rasterizador de software para aplicaciones OpenGL como ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD y CAM. En algunos casos, OpenGL Software Accelerator puede eliminar la necesidad de usar tarjetas gráficas para ofrecer una experiencia de usuario satisfactoria con aplicaciones OpenGL.

Información relacionada

> Thinwire
> HDX 3D Pro
> GPU acceleration for Windows Desktop OS
> GPU acceleration for Windows Server OS
> Framehawk
> OpenGL Software Accelerator

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Framehawk

Dec 05, 2017

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. Asimismo, Framehawk puede ser una opción adecuada para los usuarios que se conectan a redes de banda ancha "de largo recorrido" (con alta latencia), donde incluso una pérdida pequeña de paquetes puede afectar la experiencia de usuario. Se recomienda usar el transporte adaptable para este caso; para obtener más información, consulte Transporte adaptable.

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.

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 porque hay datos nuevos que los reemplazan rápidamente.

Sin embargo, cuando se trata de zonas estáticas de la pantalla (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), nos volvemos muy exigentes; 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 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 Citrix Receiver 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Mientras que Thinwire ha sido la mejor opción en cuanto a la eficiencia del ancho de banda y conviene a una amplia gama de situaciones de acceso y condiciones de red, utiliza el protocolo TCP para establecer comunicaciones fiables de datos. En consecuencia, cuando se trata de una red congestionada o con pérdidas, debe retransmitir paquetes, y esta retransmisión provoca retrasos en la experiencia de usuario. Dispone de Thinwire en una nueva capa de transporte de datos "más ligera", con lo que mejoran las limitaciones de TCP en conexiones de red de alta latencia.

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.

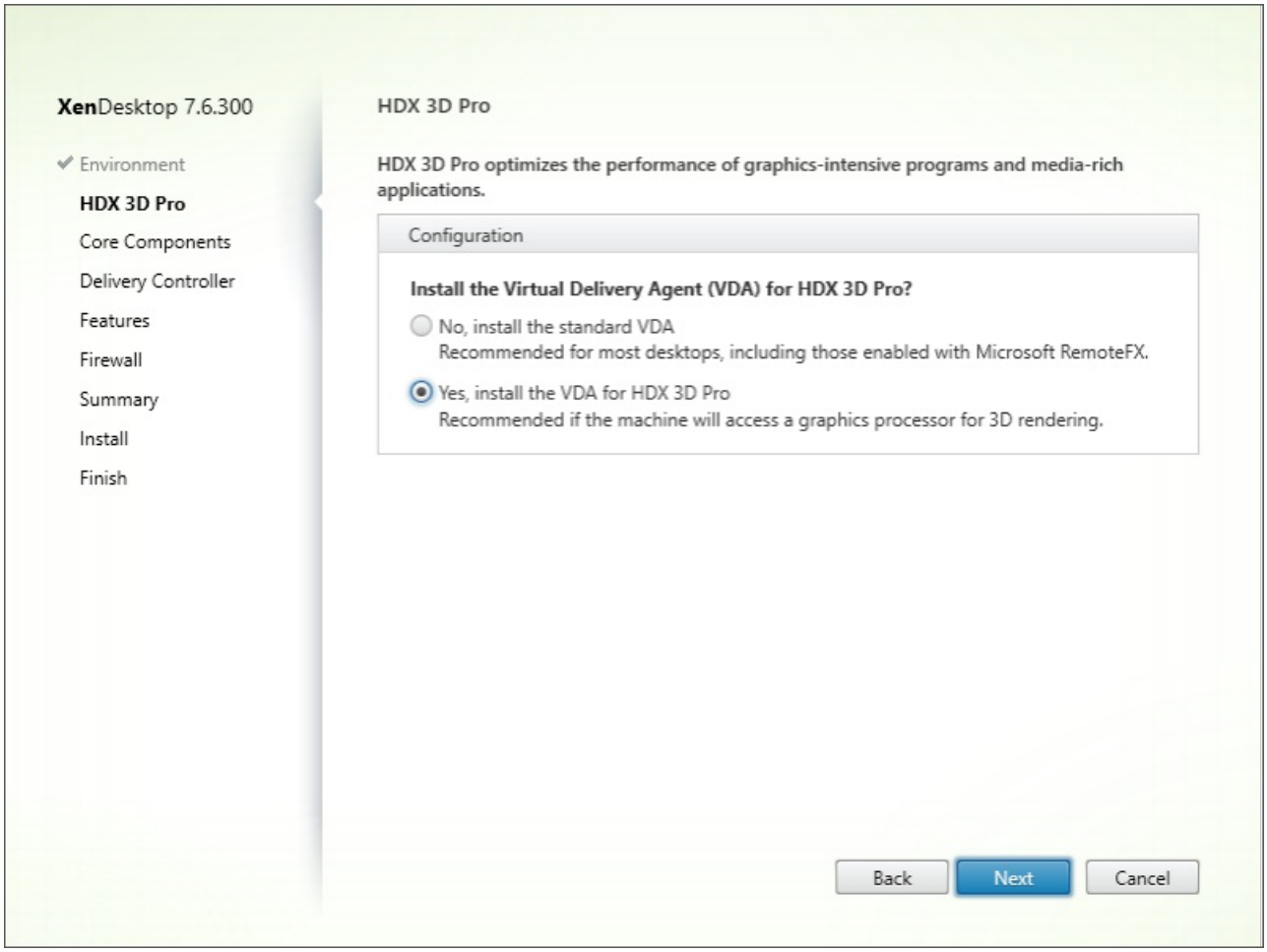
Generalmente, recomendamos un ancho de banda formado por una base de 1,5 Mbps y 150 Kbps por usuario para Thinwire. Para obtener información más detallada, consulte el blog sobre ancho de banda de XenApp y XenDesktop. Sin embargo, verá que, con una pérdida de paquetes del 3 %, Thinwire por TCP necesita 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.

Framehawk admite todos los casos de uso de HDX 3D Pro, tanto para aplicaciones XenApp (SO de servidor) como XenDesktop (SO de escritorio). Se ha validado en entornos de cliente con latencias de 400 a 500 ms y pérdidas de paquetes de 1 % a 2 % Por lo tanto, ofrece una buena interactividad cuando se usan aplicaciones de modelo 3D típicas, como AutoCAD y Siemens NX, entre otros. Este respaldo amplía la capacidad de ver y manipular grandes modelos de CAD cuando se trabaja fuera de la oficina habitual o en condiciones de red deficientes.(Se recomienda a las entidades que necesiten entregar aplicaciones 3D a través de conexiones de red de largo recorrido que utilicen el transporte adaptable. Para obtener más información, consulte Transporte adaptable.)

Habilitar esta funcionalidad no requiere tareas de configuración adicionales. Cuando instale el VDA, seleccione la opción 3DPro al principio de la instalación:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Con esta opción, HDX utiliza el controlador de vídeo GPU del fabricante, en lugar del controlador de vídeo de Citrix. De manera predeterminada, muestra la codificación H.264 en pantalla completa con Thinwire, en lugar de la pantalla adaptable habitualmente predeterminada para la codificación selectiva H.264.

Framehawk requiere, como mínimo, VDA 7.6.300 y Administración de directivas de grupo 7.6.300.

El punto final debe tener, como mínimo, Citrix Receiver para Windows 4.3.100 o Citrix Receiver para iOS 6.0.1.

Framehawk usa un intervalo de puertos UDP bidireccionales (el intervalo predeterminado es del 3224 al 3324) para intercambiar datos del canal de presentación Framehawk con Citrix Receiver. 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 XenApp), 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. Esto se aplica en conexiones que pasan por NetScaler Gateway y conexiones internas directamente al servidor StoreFront.

Para obtener acceso remoto, se debe implementar un NetScaler Gateway. De forma predeterminada, NetScaler utiliza el puerto UDP 443 para cifrar la comunicación entre los Citrix Receiver del cliente y Gateway. Este puerto debe estar abierto en los firewall externos para permitir la comunicación segura en ambas direcciones. Este protocolo se denomina Datagram

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (HA) de NetScaler desde XenApp y XenDesktop 7.12.

Tenga en cuenta los siguientes procedimientos recomendados 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, NetScaler Gateway se instala en la zona desmilitarizada, rodeada 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.

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:

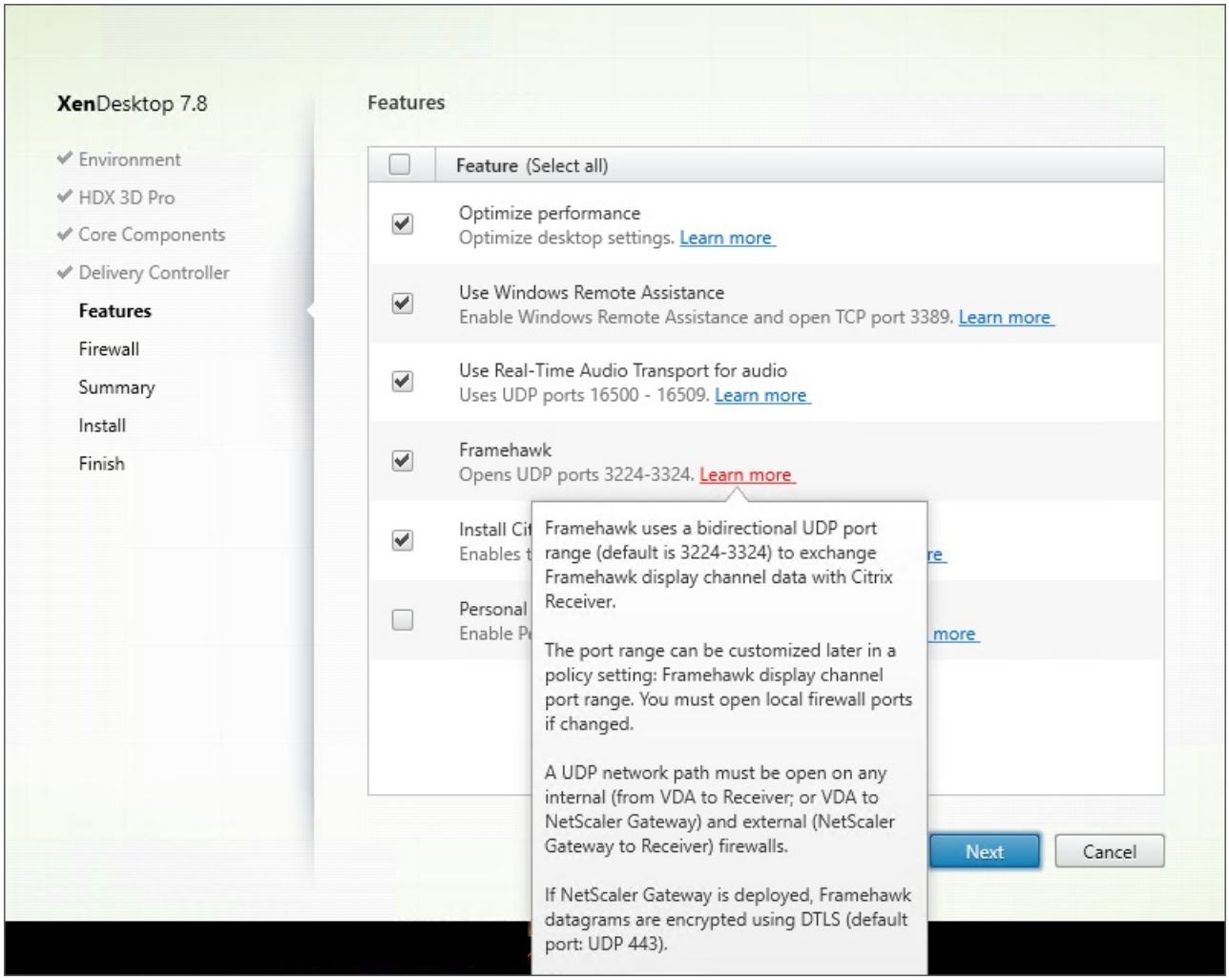
- Canal de presentación Framehawk. Habilita o inhabilita la funcionalidad.
- Intervalo de puertos del canal de presentación Framehawk. Especifica el intervalo de puertos UDP (del número de puerto más bajo al más alto) que el VDA utiliza para intercambiar datos del canal de presentación Framehawk con 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.

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:

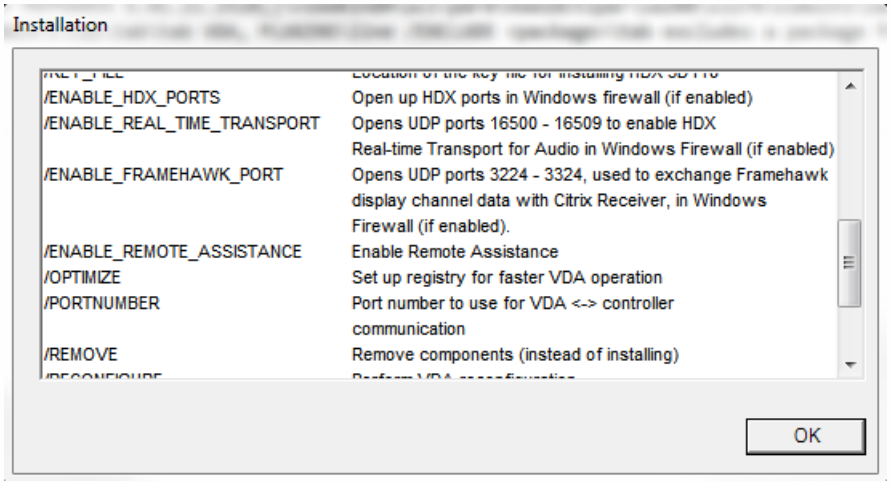
- Para los firewalls de red.
  O bien:
- Si se personaliza el intervalo predeterminado de puertos.

Para abrir esos puertos UDP, marque la casilla **Framehawk**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



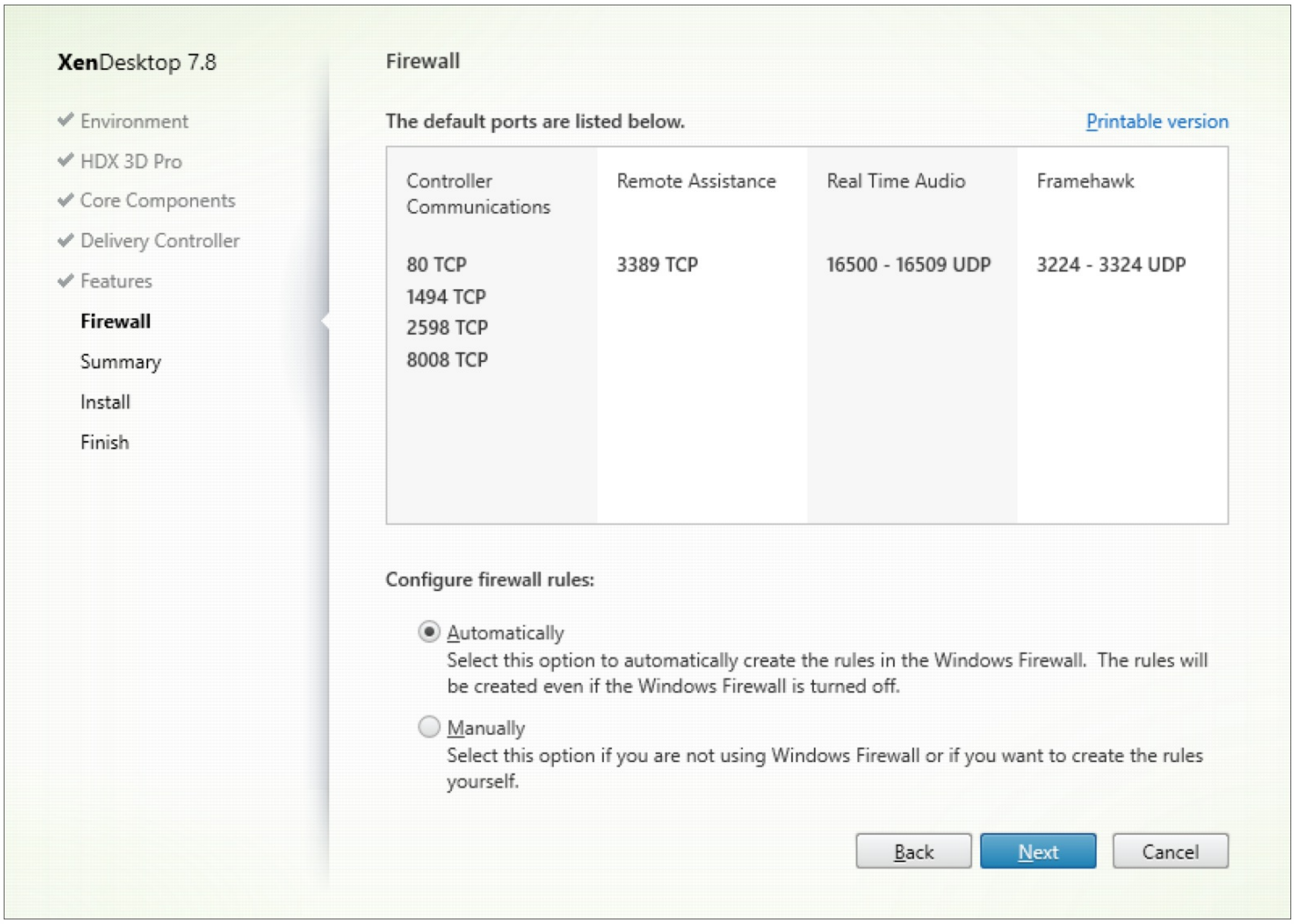
También puede utilizar la línea de comandos para abrir los puertos UDP para Framehawk mediante **/ENABLE_FRAMEHAWK_PORT**:



Comprobación de las asignaciones de puertos UDP a Framehawk

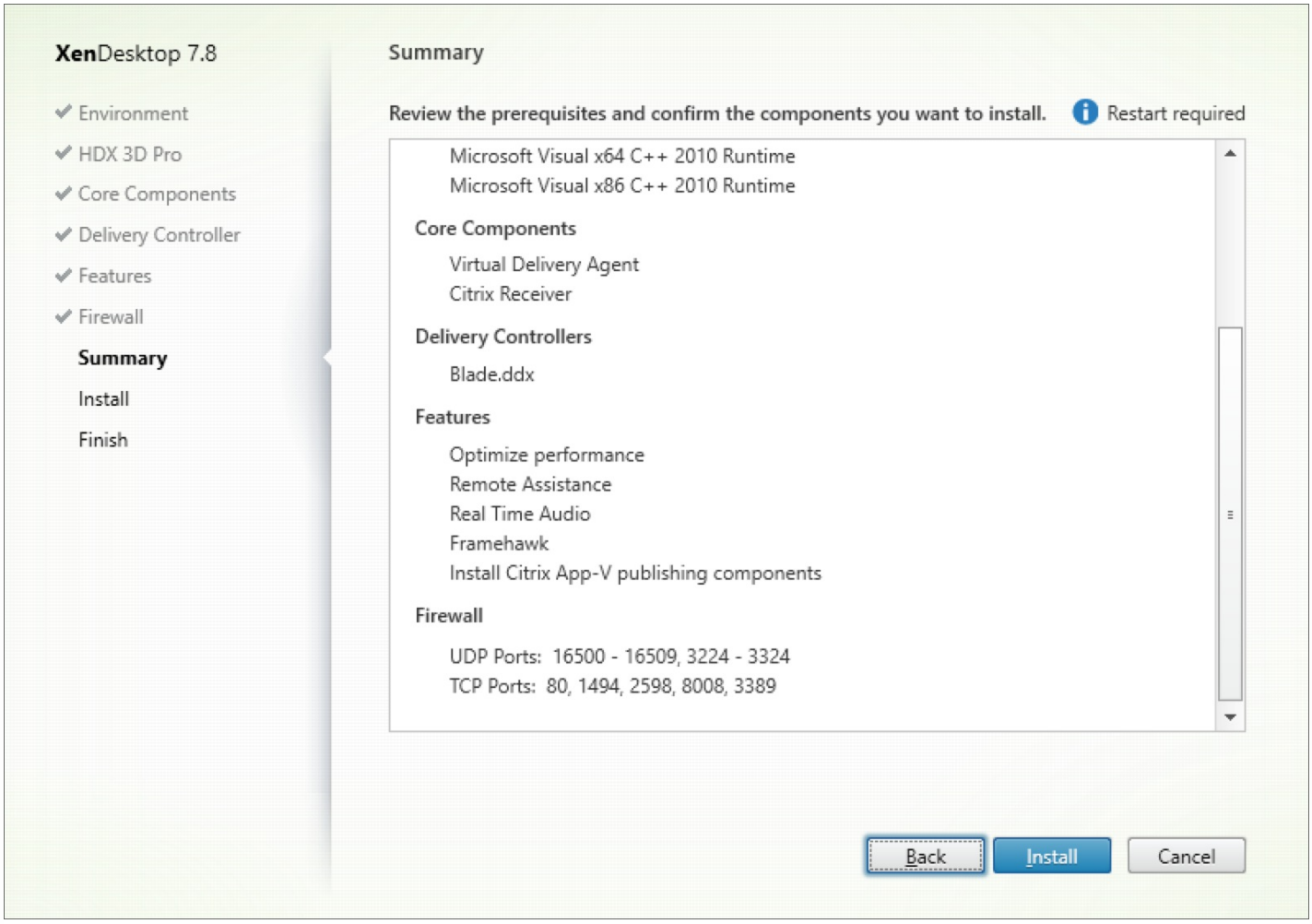
Durante la instalación, puede comprobar los puertos UDP asignados Framehawk en la pantalla **Firewall**:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la pantalla **Resumen**, se indica si está habilitada la funcionalidad Framehawk:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



El tráfico cifrado de Framehawk se admite en NetScaler Gateway a partir de la versión 11.0.62.10 y en NetScaler Unified Gateway a partir de la versión 11.0.64.34.

- NetScaler 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. Es decir, el servidor de la red privada virtual tiene una dirección IP pública asignada y el usuario se conecta directamente a esa dirección IP.
- NetScaler con Unified Gateway hace referencia a la implementación en que el servidor de VPN de la puerta de enlace 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 de Framehawk en NetScaler Gateway, el parámetro del protocolo DTLS debe estar habilitado en el servidor virtual de VPN de la puerta de enlace. Una vez habilitado el parámetro y actualizados los componentes de XenApp o XenDesktop, el audio, el vídeo y el tráfico interactivo de Framehawk se cifran entre el servidor virtual de VPN de la puerta de enlace y el dispositivo del usuario.

NetScaler Gateway, Unified Gateway y NetScaler Gateway con Global Server Load Balancing (Equilibrio de carga del servidor global) son compatibles con Framehawk.

Los siguientes casos no son compatibles con Framehawk:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- HDX Insight
- NetScaler Gateway en el modo de IPv6
- NetScaler Gateway de doble salto
- NetScaler Gateway con la configuración en clústeres

Caso	Respaldo para Framehawk
NetScaler Gateway	Sí
NetScaler Gateway + Equilibrio de carga del servidor global	Sí
NetScaler con Unified Gateway	Sí Nota: Se da respaldo a Unified Gateway 11.0.64.34 y versiones posteriores.
HDX Insight	NO
NetScaler Gateway en el modo de IPv6	NO
NetScaler Gateway de doble salto	NO
Varios Secure Ticket Authority (STA) en NetScaler Gateway	Sí
NetScaler Gateway con alta disponibilidad (HA)	Sí
NetScaler Gateway con la configuración en clústeres	NO

Para habilitar el respaldo de Framehawk en NetScaler Gateway, habilite el parámetro del protocolo DTLS en el *servidor virtual* de VPN de Gateway. Una vez habilitado el parámetro y actualizados los componentes de XenApp o XenDesktop, el audio, el vídeo y el tráfico interactivo de Framehawk se cifran entre el servidor virtual de VPN de la puerta de enlace y el dispositivo del usuario.

Se necesita esta configuración para habilitar el cifrado de UDP en NetScaler Gateway para el acceso remoto.

Al configurar NetScaler para que admita 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
- Desenlace y vuelva a enlazar el par de claves de certificado SSL. Este paso no es necesario si se usa NetScaler 11.0.64.34

© 1999-2017 Citrix Systems, Inc. All rights reserved.

o versiones posteriores.

Si quiere configurar NetScaler Gateway para que admita Framehawk:

1. Implemente y configure NetScaler Gateway para comunicarse con StoreFront y autenticar a los usuarios de XenApp y XenDesktop.
2. En la ficha de configuración de NetScaler, expanda NetScaler Gateway, y seleccione **Virtual Servers**.
3. Haga clic en **Edit** para ver los parámetros básicos del servidor virtual de la red VPN. Compruebe el estado del parámetro de DTLS.
4. Haga clic en **More** para ver más opciones de configuración:
5. Seleccione **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.
2. Habilite el parámetro DTLS en el *servidor virtual* de la VPN que está vinculado al *servidor virtual* de CS como *servidor virtual de destino*.

Si hay entradas DNS obsoletas del servidor virtual NetScaler 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.

NetScaler Gateway es el único producto SSL VPN que respalda el cifrado de UDP que requiere Framehawk. La directiva de Framehawk puede fallar si se usa otro SSL VPN o una versión incorrecta de NetScaler Gateway. Los productos tradicionales

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

IPSec VPN respaldarán Framehawk sin modificaciones.

Si quiere configurar versiones antiguas de Citrix Receiver para iOS con el objetivo de que admitan Framehawk, debe editar manualmente el archivo default.ica.

1. En el servidor StoreFront, acceda al directorio App_Data de su tienda en c:\inetpub\wwwroot\.
2. Abra el archivo default.ica y agregue la línea Framehawk=On a la sección WFClient.
3. Guarde los cambios.

Este procedimiento permite que se establezcan sesiones de Framehawk desde un Citrix Receiver compatible presente en dispositivos iOS. Este paso no es necesario si usa Citrix Receiver para Windows.

> ## Nota
>
> Con Citrix Receiver para iOS 7.0 y versiones posteriores, no tiene que agregar explícitamente el parámetro **Framehawk=On** en el archivo default.ica.

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 **Proveedor = VD3D** y **Conectado = 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 la solución de problemas de Framehawk.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HDX 3D Pro

Dec 05, 2017

Las capacidades HDX 3D Pro de XenApp y XenDesktop permiten entregar escritorios y aplicaciones que rinden más gracias a una unidad de procesamiento de gráficos (GPU) para la aceleración de hardware. Estas aplicaciones incluyen gráficos 3D profesionales basados en OpenGL y DirectX. El VDA estándar solo admite la aceleración GPU de DirectX. Para obtener más información sobre cómo elegir el VDA estándar o HDX 3D Pro, consulte "Paso 5. Elija si habilitar el modo de HDX 3D Pro", en el artículo Instalar los VDA.

Todos los Citrix Receiver respaldados 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 Citrix Receiver para Windows y Citrix Receiver para Linux. Para obtener más información sobre las versiones respaldadas de Citrix Receiver, consulte Lifecycle Milestones for Citrix Receiver.

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:

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para 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/.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aceleración de GPU para sistemas operativos de escritorio Windows

Dec 05, 2017

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. 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 5ª y 6ª 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.

HDX 3D Pro ofrece las siguientes características:

- Compresión intensa y adaptable basada en H.264 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 se puede usar con tarjetas de NVIDIA que admiten NVENC.
- La opción de compresión sin pérdida para casos de uso especiales. HDX 3D Pro también ofrece un códec sin pérdida basado en CPU para 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".

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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. Para obtener más información acerca de los códigos de tecla virtual, consulte Virtual-Key Codes en MSDN.
  - 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 edita 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

- 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 doble monitor 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.
- 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

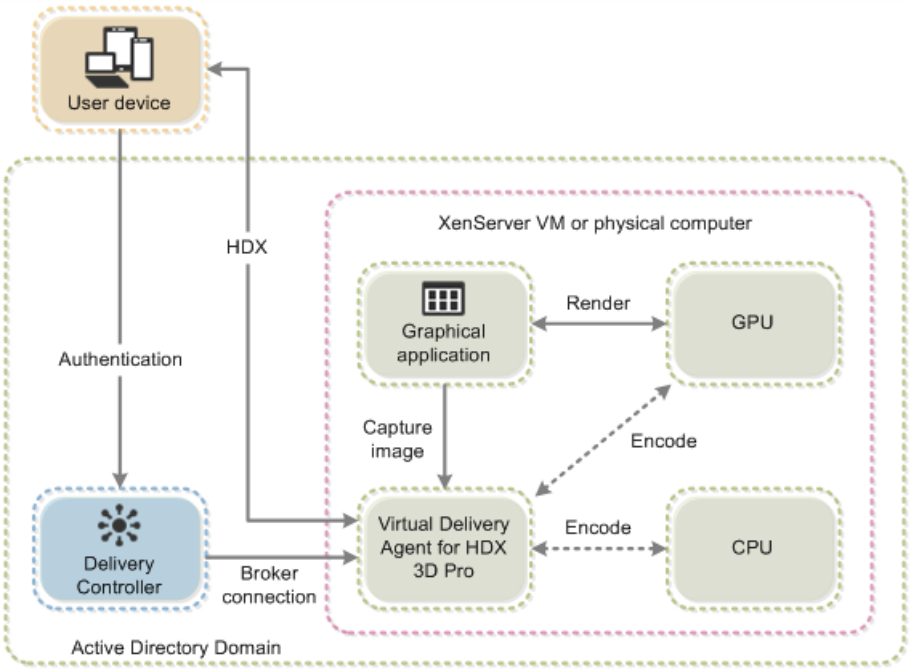
- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA y los procesadores gráficos de Intel Iris Pro. Esta funcionalidad se controla mediante una configuración de directiva (habilitada de forma predeterminada) y permite el uso de codificación por hardware para la codificación H.264 (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 Citrix Receiver 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 Citrix Receiver y el VDA para HDX 3D Pro.



Cuando use la interfaz gráfica del programa de instalación para instalar un VDA para SO de escritorio Windows, seleccione Sí en la página HDX 3D Pro. Cuando utilice la interfaz de línea de comandos, incluya la opción /enable_hdx_3d_pro con el comando XenDesktop VdaSetup.exe.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para realizar una actualización de HDX 3D Pro, desinstale el componente individual HDX 3D para gráficos profesionales y el VDA antes de instalar el VDA en el modo de HDX 3D Pro. Del mismo modo, para pasar del modo estándar de VDA para SO de escritorio Windows al modo de 3D Pro, desinstale el VDA estándar primero, y luego instale el VDA en el modo de HDX 3D Pro.

Modo estándar	Modo de HDX 3D Pro
Por lo general, es la mejor opción para escritorios virtuales sin aceleración de hardware de gráficos y para el acceso con Remote PC.	Por lo general, es la mejor opción para escritorios de centros de datos con aceleración del hardware de gráficos, a menos que se necesiten más de cuatro monitores.
Se puede usar cualquier GPU para el acceso con Remote PC, con algunas limitaciones de compatibilidad de las aplicaciones: • En Windows 7, 8 y 8.1, la aceleración de GPU para la funcionalidad DirectX iguala a 9.3. Algunas aplicaciones DirectX 10, 11 y 12 pueden no ejecutarse si no admiten el respaldo a DirectX 9. • En Windows 10, la aceleración de GPU se ofrece para aplicaciones de ventana (no en pantalla completa) DirectX 10, 11 y 12. Las aplicaciones DX 9 se representan con WARP. Las aplicaciones DX no se pueden usar en el modo de pantalla completa. • La aceleración de aplicaciones OpenGL en sesiones remotas, si la admite el distribuidor de la GPU (en la actualidad, solo NVIDIA).	Admite la aceleración de GPU con cualquier GPU, aunque la consola con pantalla vacía, las resoluciones personalizadas y varios monitores requieren gráficos NVIDIA GRID, Intel Iris Pro o AMD RapidFire. Utiliza el controlador de gráficos del distribuidor para obtener la mayor compatibilidad con las aplicaciones: • Todas las API de 3D (DirectX u OpenGL) que admite la GPU. • Respaldo para aplicaciones 3D de pantalla completa con Intel Iris Pro (solo para Win10), NVIDIA GRID y AMD RapidFire. • Respaldo para las API y las extensiones de controlador personalizadas. Por ejemplo, OpenCL o CUDA.
Las resoluciones arbitrarias de monitor (límite determinado por el rendimiento y el sistema operativo de Windows) y hasta ocho monitores.	Admite hasta cuatro monitores.
La codificación por hardware H.264 está disponible con procesadores de gráficos Intel Iris Pro.	La codificación por hardware H.264 está disponible con procesadores de gráficos Intel Iris Pro y tarjetas 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**

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 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.

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 Citrix Receiver: 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aceleración de GPU para sistemas operativos de servidor Windows

Dec 05, 2017

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 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 XenApp 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. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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/.

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

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:00000001
- [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:00000001
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit_Dlls\Graphics Helper] "OpenCL"=dword:00000001

© 1999-2017 Citrix Systems, Inc. All rights reserved.

OpenGL Software Accelerator

Dec 05, 2017

OpenGL Software Accelerator es un rasterizador de software para aplicaciones OpenGL como ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD y CAM. En algunos casos, OpenGL Software Accelerator puede eliminar la necesidad de usar tarjetas gráficas para ofrecer una experiencia del usuario satisfactoria con aplicaciones OpenGL.

> ## Important
>
> OpenGL Software Accelerator se ofrece *tal cual*, y se debe probar con todas las aplicaciones porque es posible que no admita algunas de ellas. Está diseñado como una solución en caso de que el rasterizador de Windows OpenGL no ofrezca el rendimiento adecuado. Si OpenGL Software Accelerator funciona con sus aplicaciones, se puede utilizar para evitar el coste de hardware de GPU.

OpenGL Software Accelerator se suministra en la carpeta Support de los medios de instalación y se respalda en todas las plataformas de VDA válidas.

¿Cuándo se debe probar OpenGL Software Accelerator?

- En servidores sin hardware para procesar gráficos, si el rendimiento de las aplicaciones OpenGL ejecutadas en máquinas virtuales de XenServer u otros hipervisores es problemático. Con algunas aplicaciones, OpenGL Accelerator presenta un mejor rendimiento que el rasterizador de software OpenGL de Microsoft que viene incluido en Windows, porque OpenGL Accelerator usa SSE4.1 y AVX. OpenGL Accelerator también respalda aplicaciones que usan versiones de OpenGL hasta la versión 2.1.
- Para las aplicaciones que se ejecutan en una estación de trabajo, primero pruebe con la versión predeterminada de respaldo para OpenGL suministrada por el adaptador de gráficos de la propia estación de trabajo. Si la tarjeta gráfica es de la versión más reciente, en la mayoría de los casos ofrecerá el mejor rendimiento. Si la tarjeta gráfica es de una versión antigua o no ofrece un rendimiento satisfactorio, pruebe con OpenGL Software Accelerator.
- Las aplicaciones OpenGL de 3D que no se entregan correctamente cuando se utiliza una rasterización de software basada en CPU pueden beneficiarse de la aceleración de hardware por GPU de OpenGL. Esta función se puede usar en máquinas físicas o virtuales.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Thinwire

Dec 05, 2017

Thinwire es la tecnología predeterminada de Citrix para pantallas remotas que se utiliza en XenApp y XenDesktop.

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 XenApp y XenDesktop.

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.

En su configuración predeterminada, Thinwire puede entregar gráficos 3D o muy interactivos, pero habilitar el modo de HDX 3D Pro durante la instalación del VDA para SO de escritorio es una buena opción para esos casos. El modo 3D Pro configura Thinwire con la codificación H.264 de pantalla completa para la transmisión de 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.

- Thinwire se ha optimizado para sistemas operativos modernos, como Windows Server 2012 R2, Windows Server 2016, Windows 7 y Windows 10. Para Windows Server 2008 R2, se recomienda el modo de gráficos antiguo. Utilice las plantillas de directivas de Citrix integradas, así como las plantillas "Alta escalabilidad de servidores para sistemas operativos antiguos" y "Optimización de redes WAN para sistemas operativos antiguos" para entregar las combinaciones de configuraciones de directiva que Citrix recomienda para estos casos de uso.
- El parámetro de directiva que controla el comportamiento de Thinwire, **Usar códec de vídeo para compresión**, está disponible en las versiones de VDA de 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 XenApp y XenDesktop 7.9 o posterior.
- Todos los Citrix Receiver admiten Thinwire. Sin embargo, algunos Citrix Receiver pueden admitir funcionalidades de Thinwire que otros no admiten (por ejemplo, gráficos de 8 o 16 bits para reducir el uso del ancho de banda). Citrix Receiver negocia automáticamente si admitir o no esas funcionalidades.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

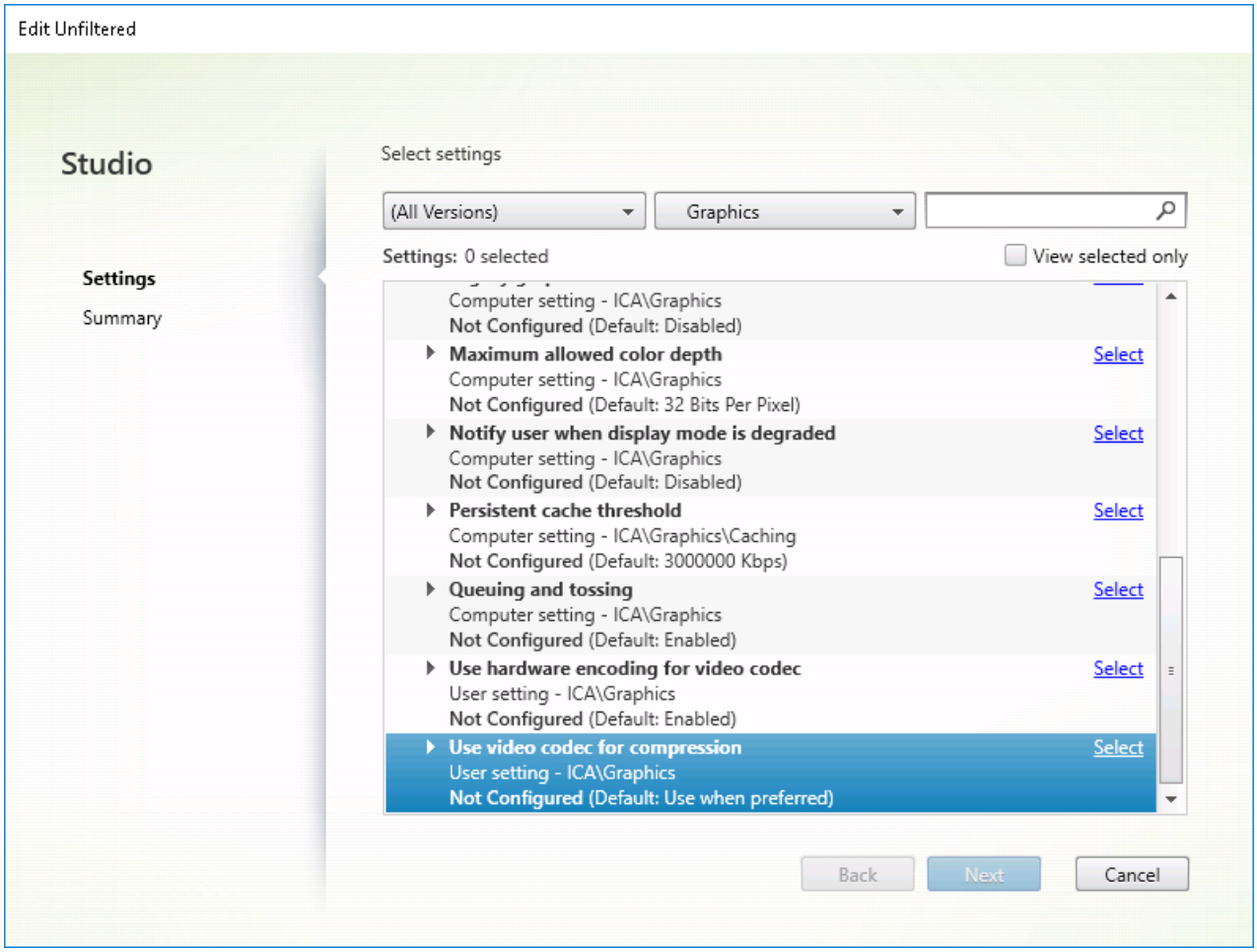
- Thinwire usará más recursos de servidor (CPU, memoria) cuando haya varios monitores y una alta resolución de pantalla. Es posible ajustar la cantidad de recursos que utiliza Thinwire. Sin embargo, puede que eso provoque un aumento del uso de ancho de banda.
- En situaciones de poco ancho de banda y 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.

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:
  - **Para áreas en cambio constante**. En Thinwire, la tecnología de pantalla adaptable identifica imágenes en movimiento (vídeo, 3D en movimiento) y usa H.264 solo en aquella parte de la pantalla donde se mueva la imagen.
  - **Para la pantalla entera**. Entrega Thinwire con H.264 de pantalla completa para mejorar la experiencia del usuario y optimizar el ancho de banda, sobre todo cuando haya un uso intensivo de gráficos 3D.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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:

- Preferencia de profundidad de color para gráficos sencillos
- Velocidad de fotogramas de destino
- Calidad visual

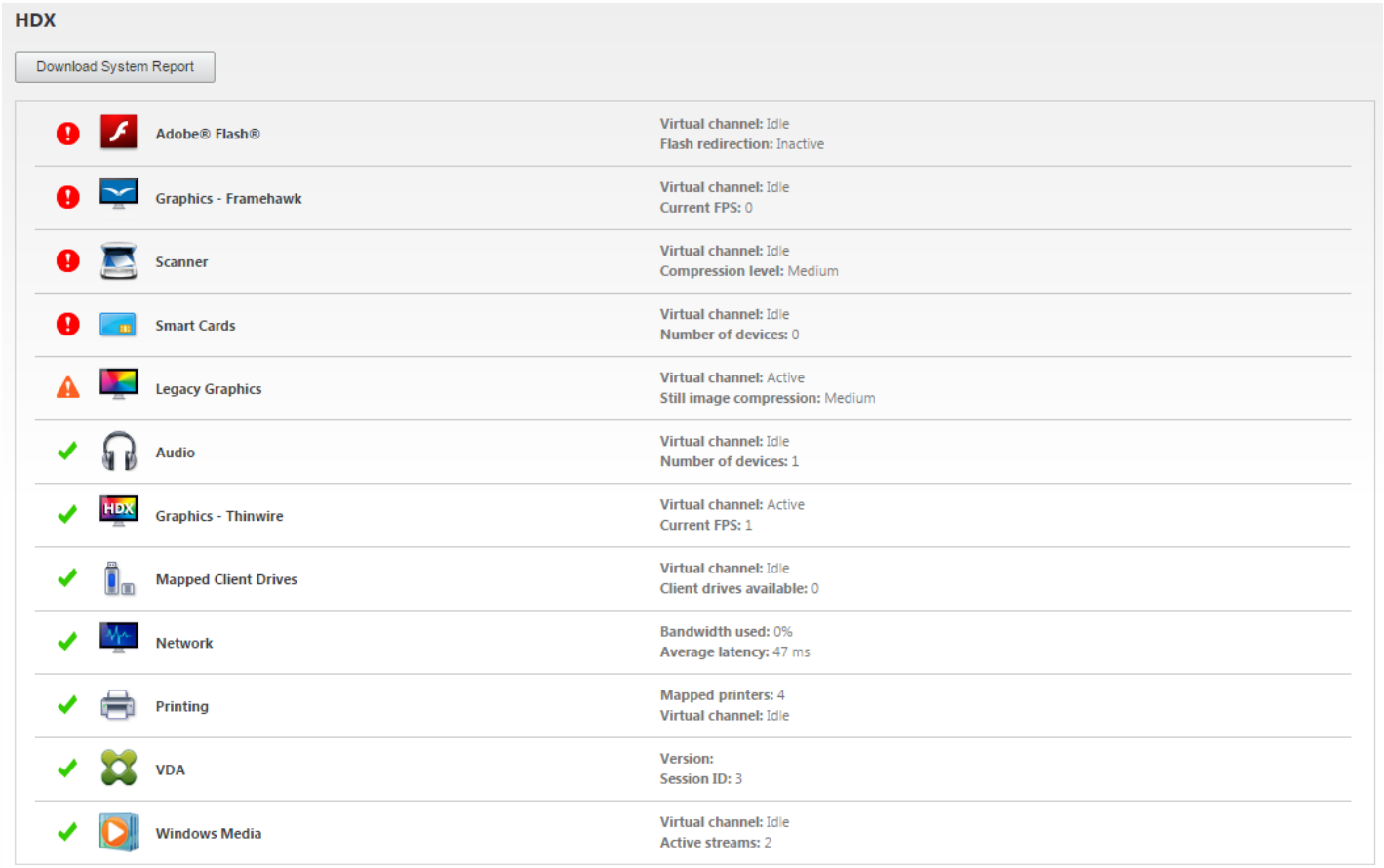
Para conocer las combinaciones de configuraciones de directiva que Citrix recomienda para diferentes casos de uso en empresas, use las plantillas de directivas de Citrix integradas. Las plantillas **Alta escalabilidad de servidores** y **Experiencia de usuario de muy alta definición** usan Thinwire con las mejores combinaciones de configuraciones de directiva para las prioridades de la empresa y las expectativas de los usuarios.

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:

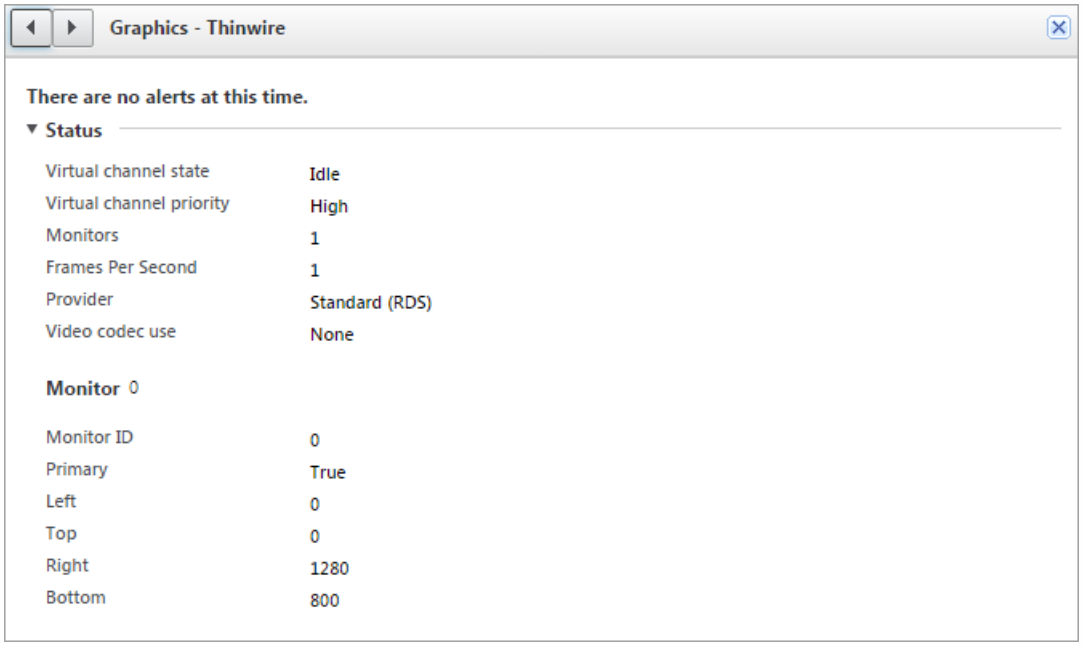
1. En Director, busque un usuario, una máquina o un dispositivo de punto final, abra una sesión activa y haga clic en **Detalles**. O bien, puede seleccionar **Filtros** > **Sesiones** > **Todas las sesiones**, abrir una sesión activa y hacer clic en **Detalles**.

2. Desplácese hacia abajo hasta el panel **HDX**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Seleccione **Gráficos: Thinwire**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Contenido multimedia

Dec 05, 2017

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 sonido y vídeo en el servidor XenApp o XenDesktop. Una vez recibido, el contenido se comprime y se entrega por protocolo ICA al Citrix Receiver 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.

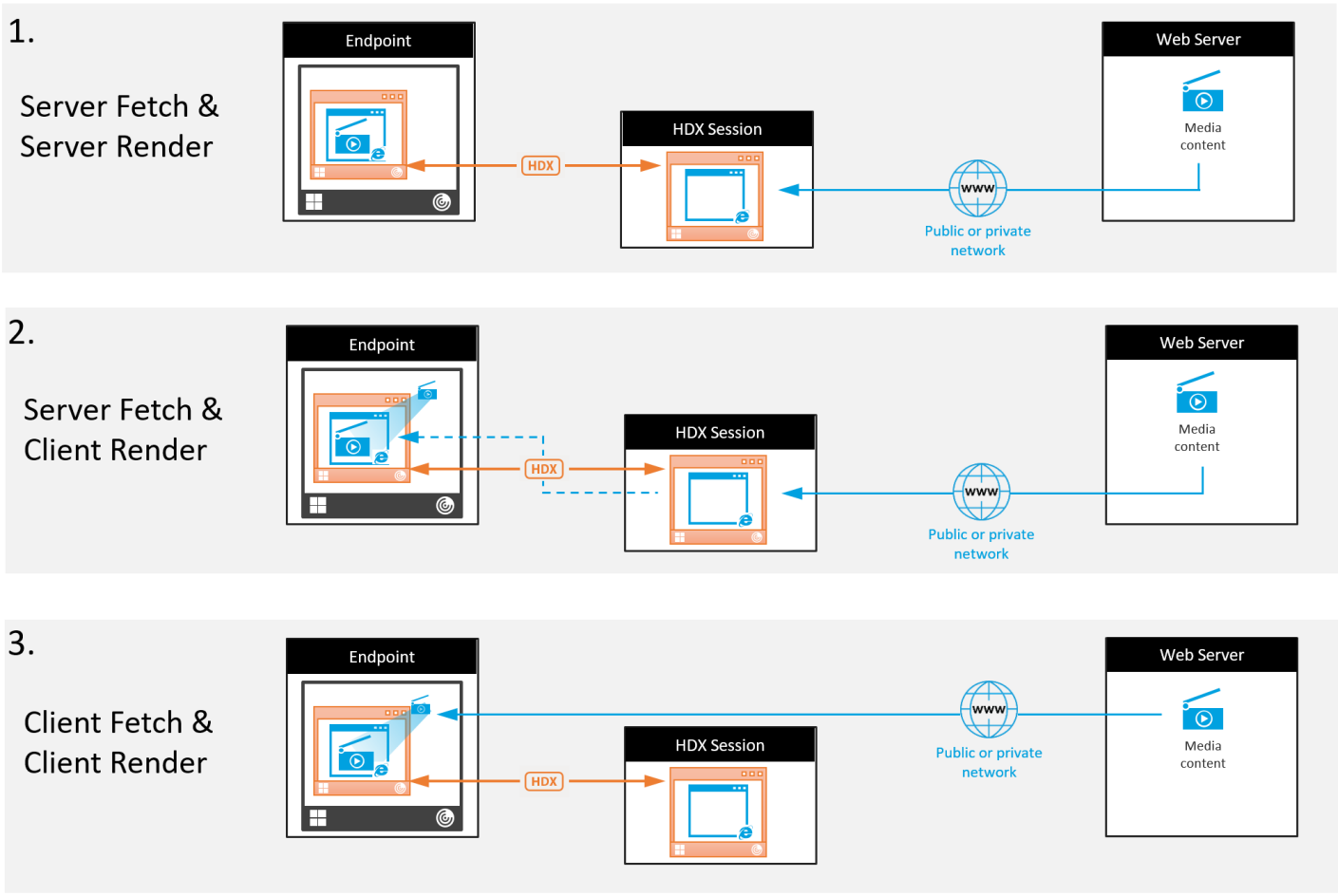
Puesto que la mayoría de los servidores no ofrecen la aceleración de hardware para la compresión de vídeo, la escalabilidad de servidor se ve afectada negativamente si todo el procesamiento de vídeo se realiza en el servidor de la CPU. Para mantener una alta escalabilidad de servidor, muchos formatos 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.

Casos de ejemplo

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Supuesto 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.

Supuesto 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.

Sin embargo, conlleva algunos requisitos de hardware y software adicionales para el cliente. El cliente debe poder

© 1999-2017 Citrix Systems, Inc. All rights reserved.

decodificar todos los formatos que pueda recibir.

Supuesto 3. (Obtener en cliente y generar en cliente)

Este enfoque necesita poder 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 solo se envían comandos de control desde el servidor. 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 y más fácil de aplicaciones multimedia. En esta tabla se muestran algunos de los entornos multimedia más comunes. En cada entorno se divide el procesamiento multimedia en varias etapas y se usa una arquitectura adaptada.

Framework	Platform
DirectShow	Windows (98 y versiones posteriores)
Media Foundation	Windows (Vista y versiones posteriores)
Gstreamer	Linux
QuickTime	Mac OS X

Redirección de Flash de HDX	No
Redirección de Windows Media	Sí
Redirección de vídeos HTML5	Sí
Redirección de sonido	No

Información relacionada

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Audio features
- Flash redirection
- HTML5 multimedia redirection
- Windows Media redirection
- General content redirection

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Características de sonido

Dec 05, 2017

Puede configurar y agregar las siguientes configuraciones de directiva de Citrix a una directiva que optimice las características de sonido 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.

> ## Important
>
> Aunque es mejor entregar sonido por el protocolo UDP (User Datagram Protocol) en lugar de TCP, el cifrado de sonido por UDP mediante DTLS solo está disponible entre NetScaler Gateway y Citrix Receiver. Por lo tanto, a veces puede ser preferible usar el transporte TCP. TCP respalda el cifrado TLS de extremo a extremo desde el VDA a Citrix Receiver.

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 configuración de directiva Calidad de sonido está establecida en "Alta: sonido de alta definición" cuando se utiliza el transporte TCP y "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 vídeochat o chat de voz no optimizadas (por ejemplo, programas de softphone), ya que puede provocar unos niveles de latencia en la ruta de sonido que no son adecuados para las comunicaciones en tiempo real. La configuración de directiva "Medio: optimizado para voz" se recomienda 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; consulte Configuraciones de directiva de sonido para dispositivos de usuario.

Para permitir que los usuarios reciban sonido desde una aplicación en un servidor mediante los altavoces u otros dispositivos de sonido (como auriculares) en sus dispositivos de usuario, deje la configuración Redirección de sonido del cliente en su opción predeterminada (Permitida).

La asignación de sonido del cliente supone una carga adicional en los servidores y en la red; sin embargo, si se prohíbe la redirección de sonido del cliente, se inhabilita toda la funcionalidad de sonido de HDX.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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; consulte Configuraciones de directiva de sonido para dispositivos de usuario.

Para permitir que los usuarios graben sonidos por medio de dispositivos de entrada (por ejemplo, micrófonos) en sus dispositivos de usuario, deje 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 Citrix Receiver.

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; consulte Configuraciones de directiva de sonido para dispositivos de usuario.

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 establecido.

Esta configuración sólo se aplica a máquinas con SO de servidor Windows.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva 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. 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; consulte Configuraciones de directiva de sonido para dispositivos de usuario.

De manera predeterminada, la opción Transporte de sonido en tiempo real por UDP está Permitida (si se selecciona en el momento de la instalación), lo que abre un puerto UDP en el servidor para las conexiones que usan el transporte de sonido en tiempo real por UDP. Citrix recomienda configurar UDP/RTP para sonido, para garantizar la mejor experiencia de usuario en el caso de producirse una congestión de la red o pérdida de paquetes.Para el sonido en tiempo real típico de aplicaciones softphone, ahora 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: Los datos de sonido transmitidos con UDP no se cifran si no se usa NetScaler Access Gateway. Si NetScaler

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Access Gateway está configurado para obtener acceso a los recursos de XenApp y XenDesktop, el tráfico del sonido entre el dispositivo de punto final y NetScaler Access Gateway está protegido 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 sonido con el dispositivo de usuario.
De forma predeterminada, el intervalo es 16500 - 16509.

Para obtener detalles sobre la configuración del Transporte de sonido en tiempo real sobre UDP, consulte Configuraciones de directiva de Sonido; para ver más detalles 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; consulte Configuraciones de directiva de sonido para dispositivos de usuario.

1. Cargue las plantillas de directiva de grupo siguiendo las instrucciones de Configuración de Receiver con la plantilla de objeto de directiva de grupo.
2. En el Editor de directivas de grupo, expanda Plantillas administrativas > Citrix Components > Citrix Receiver > User Experience.
3. En **Parámetros de sonido del cliente**, seleccione **No configurada**, **Habilitada** o **Inhabilitada**.
   - **Sin configurar**. De forma predeterminada, la redirección de sonido está habilitada con alta calidad de sonido, o con los parámetros de sonido personalizados configurados previamente.
   - **Habilitada**. La redirección de sonido se habilita con las opciones seleccionadas.
   - **Inhabilitada**. La redirección de sonido está inhabilitada.
4. Si ha seleccionado **Habilitada**, elija una calidad de sonido. Para el sonido UDP, use solo la calidad de sonido **Media** (la opción predeterminada).
5. Para el sonido UDP solamente, seleccione **Habilitar el transporte en tiempo real** y configure el intervalo de puertos de entrada que se abrirán en el Firewall de Windows local.
6. Para utilizar el sonido UDP con NetScaler Access Gateway, seleccione **Allow Real-Time Transport Through gateway**. NetScaler Access Gateway debe estar configurado con DTLS. Para obtener más información, consulte UDP Audio Through a Netscaler Gateway.

Como administrador, si no tiene control sobre los dispositivos de punto final para hacer estos cambios, por ejemplo, en el caso de equipos que son propiedad de los usuarios (Bring Your Own Device) o equipos domésticos, use los atributos del archivo default.ica de StoreFront para habilitar el sonido UDP.

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].



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
; This is to enable Real-Time Transport

EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway

EnableUDPThroughGateway=true

; This is to set 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.

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 proporciona una opción de eliminación del eco (habilitada de forma predeterminada, que permite minimizarlo. La eficacia de la cancelación del eco depende de la distancia entre los altavoces y el micrófono. Los dispositivos no deben estar ni demasiado cerca ni demasiado lejos el uno del otro.

La eliminación de eco se puede inhabilitar mediante un parámetro de Registro.

> ## Advertencia
>
> Si se usa el Editor del 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. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

1. En el Editor del Registro, vaya a una de estas ubicaciones:
   - Equipos de 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
- 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.

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.

XenApp y XenDesktop admiten varias alternativas para la entrega de aplicaciones softphone.

- **Modo de control**. En términos simples, la aplicación softphone alojada controla un teléfono físico configurado. En este modo, no hay tráfico de sonido que pase por el servidor XenApp o XenDesktop.
- **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.
  - Avaya Communicator para entornos VDI para one-X Communicator y one-X Agent.
- **Acceso a aplicaciones locales**. Una función de XenApp y XenDesktop que permite que una aplicación softphone se ejecute localmente en el dispositivo Windows del usuario final al mismo tiempo que aparece perfectamente integrada en el escritorio virtual o publicado. 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 sobre 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 sonido se dirige mediante el protocolo ICA de Citrix (preferentemente por UDP/RTP) al dispositivo de usuario que ejecuta Citrix Receiver.

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 XenApp y XenDesktop:

- ¿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 final?

XenApp y XenDesktop contiene 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 Citrix Receiver para Mac, Windows, Linux y Chrome también admiten VoIP. Citrix Receiver para Windows ofrece las siguientes funciones:

- Búfer de vibración en el cliente. Suaviza el sonido incluso cuando fluctúa la latencia de red.
- Eliminación de eco. Permite mayor variación en la distancia entre el micrófono y los altavoces para usuarios que no disponen de auriculares con micrófono.
- 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 funcionalidades de Citrix Receiver, consulte Matriz de características de Citrix Receiver.

Recomendaciones de configuración del sistema

Hardware y software del cliente
. Para una calidad óptima del sonido, le recomendamos la versión más reciente de Citrix Receiver y unos auriculares de buena calidad con eliminación de eco acústico (AEC). Las versiones de Citrix Receiver para Windows, Linux y Mac admiten VoIP. Además, Dell Wyse ofrece respaldo para VoIP en ThinOS (WTOS).

Consideraciones de 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 XenDesktop.

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. Configure esta funcionalidad para admitir la calidad de servicio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 para mantener una alta calidad de servicio. 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
. NetScaler Gateway 11 admite DTLS para entregar el tráfico UDP/RTP de forma nativa (sin encapsulación en TCP). Debe abrir 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).

Entrega de 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.

Entrega de sonido desde y hacia el dispositivo de usuario

HDX RealTime genérico admite dos métodos para entregar sonido desde y hacia el dispositivo de usuario:

- **Citrix Audio Virtual Channel**.Por lo general, se recomienda Citrix Audio Virtual Channel porque se ha diseñado específicamente para el transporte de sonido.
- **Redirección de USB genérico**.Útil para admitir dispositivos de sonido 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 XenApp o XenDesktop.

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, lo comprime y 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

optimizado para voz (calidad media). Sus características son ideales para la voz por IP (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. Esta 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 usuarios conectados por LAN porque 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, pero 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 (como 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección de Flash

Dec 05, 2017

Important

El 25 de julio de 2017, Adobe anunció el ciclo de 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 HDX hasta el final del año 2020. No hemos decidimos aún de qué versiones de XenApp y XenDesktop 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 multimedia HTML5.

La redirección de Flash descarga el procesamiento de la mayoría del contenido Adobe Flash (incluidas animaciones, vídeos y aplicaciones) en los dispositivos de los usuarios conectados por LAN o WAN y los dispositivos Linux x86 de 32 bits, lo que reduce la carga en el servidor y en la red. Esto resulta en una mayor escalabilidad, al tiempo que garantiza una experiencia de usuario de alta definición. La configuración de la redirección de Flash requiere la configuración de parámetros tanto en el lado del cliente como en el lado del servidor.
Precaución: La redirección de Flash requiere una interacción importante 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 funcionalidades 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 sucesos de Windows en el servidor para registrar sucesos de Flash. El registro de sucesos indicará si se está usando la redirección de Flash y proporcionará información sobre los problemas que se produzcan. A continuación se enumeran las acciones más comunes a todos los sucesos registrados por la redirección de Flash:

- Redirección de Flash registra sucesos en el registro de Aplicación.
- En los sistemas con Windows 10, Windows 8 o Windows 7, aparece un registro específico de 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 las actualizaciones más recientes de la compatibilidad de HDX Flash, consulte CTX136588.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

- 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. Tenga en cuenta que algunos contenidos Flash pueden no redirigirse correctamente.
- La configuración de directiva Lista de URL para obtener contenido Flash del lado del servidor le permite especificar sitios Web cuyo contenido Flash se debería descargar en el servidor y luego transferirse al dispositivo de usuario para su generación. (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) el parámetro Habilitar obtención de contenido del lado del servidor en el dispositivo de usuario, y está diseñada básicamente para sitios de la intranet y aplicaciones Flash internas; consulte los siguientes apartados para obtener más información. 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 XenApp o XenDesktop proporciona dicha conexión).
  Nota: La obtención de contenido del lado del servidor no admite aplicaciones Flash que usan protocolos de mensajería en tiempo real (RTMP); en su lugar, se usa la generación en el 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, es decir, si se genera en el dispositivo del usuario, se genera 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.

Instale Citrix Receiver 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 de cliente HDX MediaStream Flash Redirection (HdxFlashClient.adm), que está disponible en las siguientes carpetas:

- En equipos de 32 bits: %Archivos de programa%\Citrix\ICA Client\Configuration\language
- En equipos de 64 bits: %Archivos de programa (x86)%\Citrix\ICA Client\Configuration\language

La configuración de directiva aparece bajo 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.

Cómo 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 generar el contenido Flash en el dispositivo del usuario.

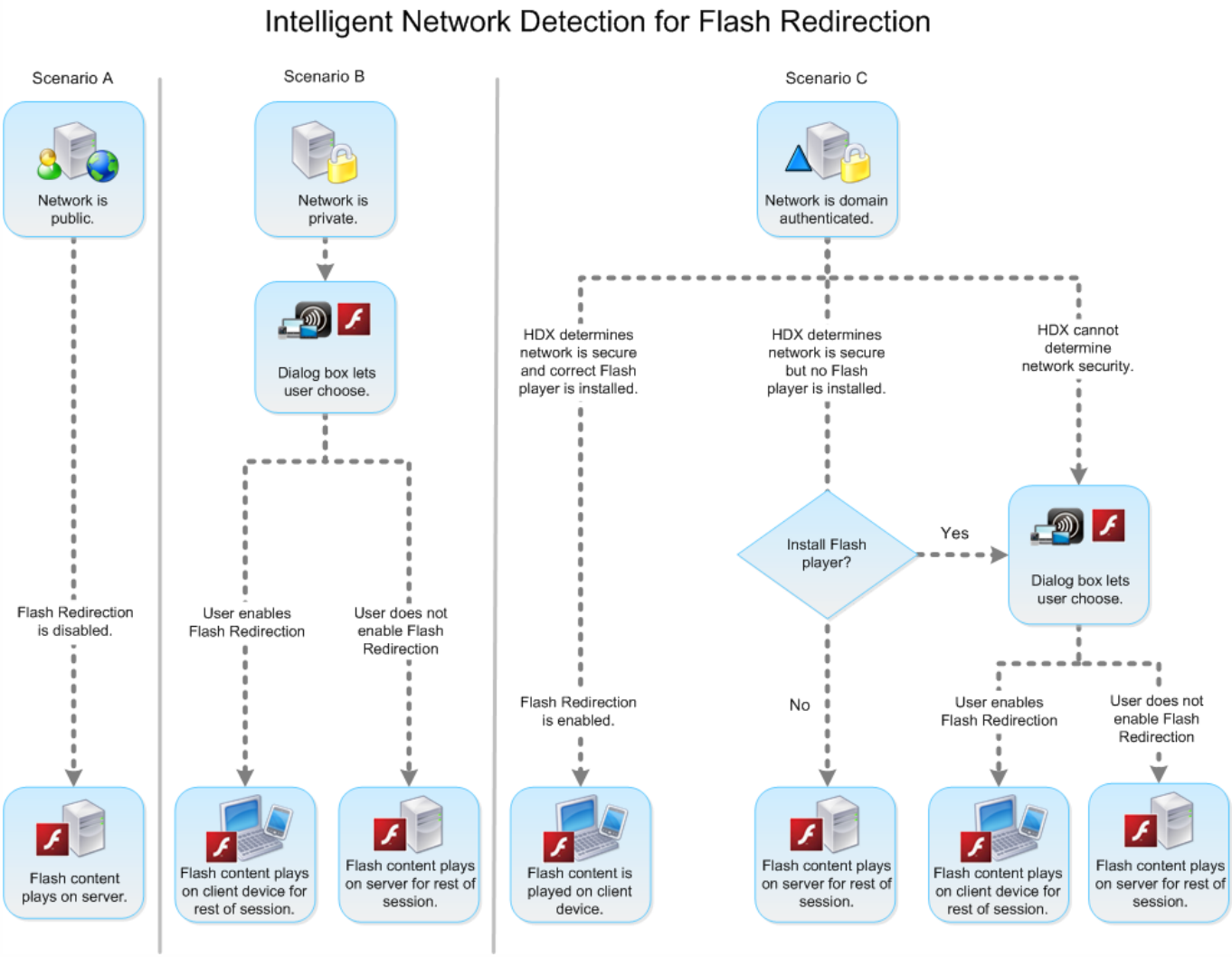
Si no hay ninguna configuración definida y se usa Desktop Lock, la redirección de Flash está habilitada en el dispositivo de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

usuario de manera predeterminada.

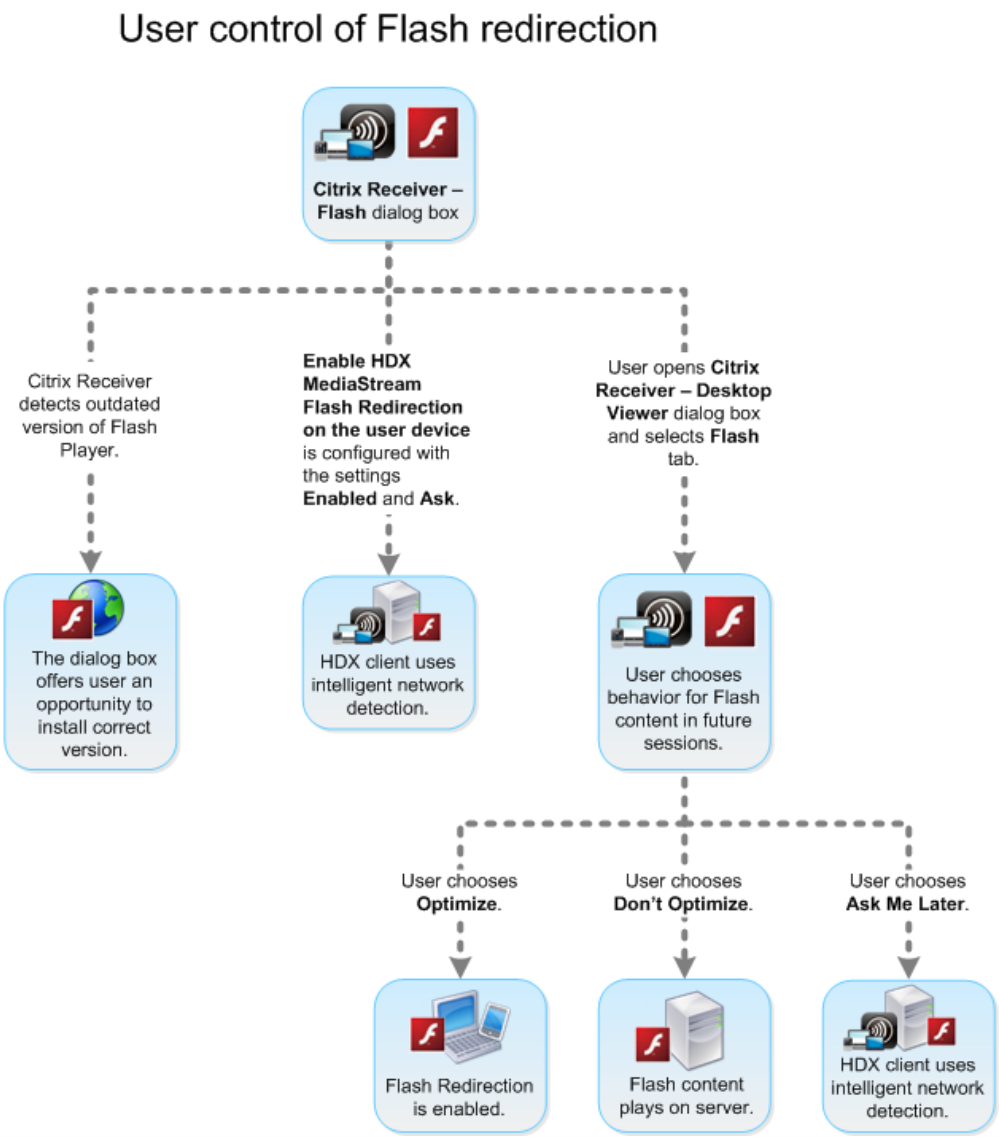
Para cambiar cuándo se usa la redirección de Flash o para inhabilitar la redirección de Flash en el dispositivo del usuario:

1. En la lista Configuración, seleccione Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario y después haga clic en configuración de directiva.
2. Seleccione No configurada, Habilitada (opción predeterminada) o Inhabilitada.
3. Si ha seleccionado Habilitada, elija una opción en lista Usar la redirección de HDX MediaStream para Flash:
   - Seleccione Con segunda generación solamente para usar la funcionalidad de 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 para 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 desea usar la redirección de Flash. Si el nivel de seguridad de la red no se puede determinar, se pregunta al usuario si desea usar la redirección de Flash.
     La siguiente ilustración muestra cómo se controla la redirección de Flash en diversos tipos de red.



Los usuarios pueden anular la detección de red inteligente desde el cuadro de diálogo Citrix Receiver - Preferencias de Desktop Viewer, seleccionando 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 ilustración.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Sincronización de 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; posteriormente, estas cookies HTTP se usarán para la obtención de contenido en el cliente, y estarán disponibles según sea necesario para los sitios con contenido Flash.
Nota: Las cookies del lado del cliente no se sustituyen durante la sincronización; permanecen disponibles incluso aunque la directiva de sincronización se inhabilite 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).

Habilitación de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Nota: 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 el contenido del lado del servidor en la caché del dispositivo de usuario; esto mejora el rendimiento, dado que el contenido reutilizado está ya disponible en el dispositivo de 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 haga clic en 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
Inhabilitado	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.
Habilitado	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.
Habilitado (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.
Habilitado (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.

Redirección de los dispositivos de usuario a otros servidores para la obtención de contenido en el lado del cliente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Cuando se configura esta función, se proporcionan dos patrones de URL; cuando el dispositivo de usuario intenta obtener contenido de 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 para compensar por redes de entrega de contenido (CDN). Algunos sitios Web que entregan contenido Flash usan la redirección CDN para permitir al usuario obtener el contenido a partir del grupo más cercano de servidores que entregan el mismo contenido. Cuando se usa la función de obtención de contenido en el lado del cliente de la redirección de Flash, el contenido Flash se solicita desde el dispositivo de usuario, mientras que el resto de la página Web donde reside el contenido Flash es solicitada por el servidor. Si se usa CDN, la solicitud del servidor se redirige al servidor más cercano y la solicitud del dispositivo de usuario se redirige a la misma ubicación. Tenga en cuenta que es posible que esta no sea la ubicación más cercana al dispositivo de usuario; dependiendo de la distancia entre ellos, es posible que exista cierta demora entre la carga de la página Web y la reproducción del contenido Flash.

1. En la lista de 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 configurado, Habilitado o Inhabilitado. No configurada es la opción predeterminada; si se elige Inhabilitada se ignorarán las reglas de reescritura de URL configuradas en el paso siguiente.
3. Si habilita la configuración, haga clic en 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.

Advertencia

Si se usa el Editor del 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Puede agregar parámetros de Registro que especifiquen la versión mínima necesaria para la redirección de Flash de dispositivos cliente que acceden a agentes VDA mediante Citrix Receiver para Windows o Citrix Receiver 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 (Citrix Receiver).

Estas cadenas de 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 estos no se pueden usar porque el significado de una máscara que no sea cero puede cambiar. Se

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 requerirá 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, comparará 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 Citrix Receiver para Linux. La subclave ClientID0x1 especifica Citrix Receiver 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 "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\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Configuración del cliente ICA de Windows

"ClientFlashPlayerVersionMinimum"="16.0.0" Indica la versión mínima de Flash Player necesaria para el cliente Windows
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Configuración del cliente ICA de Linux

"FlashPlayerVersionComparisonMask"=dword:00000000 Esto 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" Esto 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]

"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]

"ClientFlashPlayerVersionMinimum"="16.0.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]

"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección multimedia HTML5

Jan 05, 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.

Los medios basados en HTML5 presentan muchas ventajas frente los complementos de 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 duro tal cual se recibe, y se reproduce desde ese disco duro. 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 el elemento de vídeo en la página Web y buscar el origen (un formato de contenedor mp4) en la etiqueta de vídeo HTML5:

Comparación entre HTML5 y Flash

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Feature	HTML5	Flash
Requiere un reproductor propietario	No	Sí
Se ejecuta en dispositivos móviles	Sí	Algunos
Velocidad de ejecución en distintas plataformas	Alta	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:

- Generación en el lado del servidor
- Obtención en servidor, generación en cliente
- Obtención del lado del cliente

Estas opciones se controlan mediante directivas. Para obtener más información, consulte Configuraciones de directiva Multimedia.

Versiones mínimas de Citrix Receiver:

- Citrix Receiver para Windows 4.5
- Citrix Receiver para Linux 13.5

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Minimum VDA browser version	Windows OS version/build/SP
Internet Explorer 11.0	Windows 10 x86 (1607 RS1) y x64 (1607 RS1) Windows 7 x86 y x64 Windows Server 2016 RTM 14393 (1607) Windows Server 2012 R2
Firefox 47 Debe agregar manualmente los certificados al almacén de certificados de Firefox o configurar Firefox para buscar certificados provenientes de un almacén de certificados de confianza de Windows. Para obtener más información, consulte 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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?

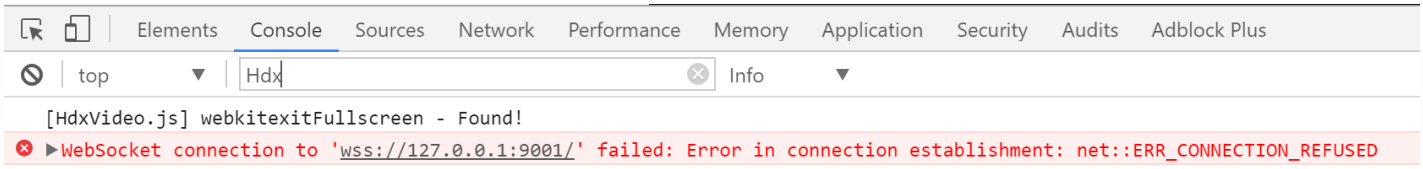
En esta versión, esta funcionalidad está disponible solo para las páginas Web controladas. Requiere que se añada HdxVideo.js de JavaScript (incluido en los medios de instalación de XenApp y XenDesktop) a las páginas Web donde está disponible el contenido multimedia de HTML5. Por ejemplo, vídeos en un 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:



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección de Windows Media

Dec 05, 2017

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 el XenDesktop Collector para rastrear el método utilizado con Citrix Diagnosis Facility (CDF) desde HostMMTransport.dll.

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 de directiva **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 el parámetro **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección de contenido general

Dec 05, 2017

La redirección de contenido permite controlar si los usuarios acceden a la información mediante aplicaciones publicadas en servidores o mediante aplicaciones que se ejecutan localmente en dispositivos de usuario.

Redirección de carpetas del cliente

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Cuando se habilita solo la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention). Cuando se habilita la redirección de carpetas del cliente en el servidor y, a continuación, el usuario lo configura en el dispositivo de escritorio Windows, solo se redirige la parte del volumen local que especifique el usuario.

Redirección del host al cliente

La redirección del host al cliente resulta útil para casos concretos y poco frecuentes. 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.

Consideraciones sobre unidades del cliente y USB

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin respaldo optimizado o cuando ese respaldo no es adecuado.

Información relacionada

- Client folder redirection
- Host to client redirection
- Local App Access and URL redirection
- USB and client drive considerations
- Multimedia

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección de carpetas del cliente

Dec 05, 2017

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. A continuación, en el dispositivo cliente, especifique las carpetas que quiere redirigir (la aplicación que usted utiliza para especificar las opciones de carpeta del cliente está incluida en el software de Citrix Receiver proporcionado con esta versión).

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. Debe hacer una copia de seguridad del Registro antes de editarlo.

1. En el servidor:
    1. Cree una clave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
    2. Cree un valor REG_DWORD.
        - Nombre: CFROnlyModeAvailable
        - Tipo: REG_DWORD
        - Datos: Establézcalo en 1.
2. En el dispositivo de usuario:
    1. Compruebe que está instalada la versión más reciente de Citrix Receiver.
    2. En el directorio de instalación de Citrix Receiver, inicie CtxCFRUI.exe.
    3. Seleccione el botón de opción Personalizada y agregue, modifique o quite carpetas.
    4. Desconecte y vuelva a conectar sus sesiones para que la configuración tenga efecto.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Redirección del host al cliente

Dec 05, 2017

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 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, de forma que siempre se use la aplicación que se instale 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).

Cumplimiento de normativas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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 y/o redirección de Flash
Desktop Appliance	El proveedor admite la redirección multimedia y/o la redirección de Flash	Redirección multimedia y/o 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 con requisitos mínimos (o cliente Zero)	El proveedor admite la redirección multimedia y/o la redirección de Flash	Redirección multimedia y/o redirección de Flash

A continuación, dispone de ejemplos para guiarle a la hora de escoger el método adecuado para la redirección de contenido.

© 1999-2017 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

La redirección del host al cliente se admite en Citrix Receiver para Windows, Citrix Receiver para Mac, Citrix Receiver para Linux, Citrix Receiver para HTML5 y Citrix Receiver 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 dispositivo del usuario es un dispositivo de escritorio, cliente ligero o cliente con requisitos mínimos, compruebe que dispone de las aplicaciones adecuadas y es lo suficientemente potente.

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (en una página Web o en la barra de direcciones del explorador Web).

> **Nota**
>
> Si los usuarios cambian su explorador Web predeterminado en el VDA (por ejemplo, con "Establecer programas predeterminados"), ese cambio puede interferir con la redirección del host al cliente de las aplicaciones.

Cuando la redirección de contenido del host al cliente está habilitada, la aplicación que se utiliza para abrir la URL depende de 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 (protocolo de transferencia de hipertexto)
- HTTPS (protocolo de transferencia de hipertexto seguro)
- RTSP (Real Player y QuickTime)
- RTSPU (Real Player y QuickTime)
- PNM (Real Player de versiones anteriores)
- MMS (formato multimedia de Microsoft)

Puede cambiar la lista de tipos de URL para la redirección del host al cliente eliminando y agregando tipos de URL (incluidos los tipos de URL personalizada).

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Debe hacer una copia de seguridad del Registro antes de editarlo.

1. Copie el texto ubicado entre "**Reg file start**" y "**Reg file end**", 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
- Reg file start --

Windows Registry Editor Version 5.00



[HKEY_CLASSES_ROOT\ServerFTAHTML\shell\open\command]

@="\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0"

"ApplicationName"="ServerFTA"



[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]

"http"="ServerFTAHTML"

"https"="ServerFTAHTML"



[HKEY_LOCAL_MACHINE\SOFTWARE\RegisteredApplications]

"Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"

-- Reg file end --
```

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**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
-- xml file start --
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />
</DefaultAssociations>
-- 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.

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:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

customtype1://;customtype2://

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.

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. Eso coincide con un único nivel de dominio, lo que es coherente con las reglas de RFC 6125.Por ejemplo:

www.ejemplo.com

*.ejemplo.com

Para usar Internet Explorer 9 y versiones posteriores como un explorador publicado, cambie los siguientes valores de claves del Registro en el VDA de servidor:

Teclas:

HKLM\Software\Classes\htmlfile\shell\opennew

HKLM\Software\Classes\http\shell\open

HKLM\Software\Classes\https\shell\open

HKCR\http\shell\open

HKCR\https\shell\open

HKCR\htmlfile\shell\opennew

Cambiar de:

Nombre: CommandID

Tipo: REG_SZ

Datos: IE.Protocol

A:

Nombre: CommandID

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Tipo: REG_SZ

Datos: IE.ProtocolX

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Acceso a aplicaciones locales y redirección de URL

Dec 05, 2017

En este artículo:

- Introducción
- Requisitos, consideraciones y limitaciones
- Interacción con Windows
- Configuración del acceso a aplicaciones locales y la redirección de URL

Introducción

La función de 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 de 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 XenApp y XenDesktop, las sesiones de escritorio alojado usan la redirección de URL para iniciar aplicaciones de acceso local. La función de redirección de URL permite que la aplicación esté 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 de 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 alguna de las siguientes maneras:

- Desde el equipo del usuario al escritorio alojado
- Desde el servidor XenApp o XenDesktop 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

negra de URL en el Virtual Delivery Agent. Estas listas contienen claves de Registro de cadena múltiple que especifican la configuración de directiva de redirección de URL; para obtener más información, consulte la configuración de directiva de Acceso a aplicaciones locales.

Las direcciones URL pueden generarse en el VDA, con las siguientes excepciones:

- Configuración regional y geográfica. Sitios web que requieren configuración regional, como msn.com o news.google.com (abre la página de un país concreto; esa página se basa 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 a los usuarios finales una experiencia nativa y ahorran ancho de banda incluso en redes de latencia alta. Aunque existe una función para redirección de Flash, esto se complementa redirigiendo sitios que contienen otros tipos de contenido multimedia, tales como Silverlight. Esto se aplica en un entorno muy 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 inicia aplicaciones locales cuando se encuentra un archivo en la sesión. Si se inicia una aplicación local, esta debe tener acceso al archivo para abrirlo. Por lo tanto, solo puede abrir archivos que residen en recursos compartidos de red o en las unidades del cliente (mediante la asignación de unidades del cliente) con aplicaciones locales. Por ejemplo, cuando se abre un archivo PDF, si un lector de PDF es una aplicación local, el archivo se abre con ese lector de PDF. Debido a que la aplicación local puede acceder al archivo directamente, este no se transfiere por la red a través de ICA para abrirse.

Requisitos, consideraciones y limitaciones

La función de acceso a aplicaciones locales recibe respaldo en los sistemas operativos válidos para los VDA para SO de servidor Windows y VDA para SO de escritorio Windows, y requiere como mínimo Citrix Receiver para Windows, versión 4.1. 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 la función de acceso a aplicaciones locales y la redirección de URL.

- La función de acceso a aplicaciones locales está diseñada para escritorios virtuales en pantalla completa expandida a todos los monitores:
  - Si la función de 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 respalda 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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. Esto incluye las aplicaciones que se abren en el modo de pantalla completa, como las presentaciones con diapositivas de PowerPoint o los visores de fotos que ocupan todo el escritorio.
- La función de acceso a aplicaciones locales copia las propiedades de la aplicación local (como los accesos directos en el escritorio del cliente y del menú Inicio) en el VDA; 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.
- No se pueden iniciar aplicaciones mediante 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 de 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).
- La función de redirección de URL solo funciona con sesiones de escritorio, no con las sesiones de aplicación.
- La carpeta de escritorio local en una sesión de VDA no permite que los usuarios creen archivos nuevos.
- 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 de acceso a aplicaciones locales con Windows incluye los siguientes comportamientos.

- Comportamiento de los accesos directos en Windows 8 y Windows Server 2012
  - Las aplicaciones de la Tienda Windows instaladas en el cliente no se enumeran en la lista de accesos directos de la función de 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 de acceso a aplicaciones locales enumera las aplicaciones de la Tienda Windows y abre los accesos directos con aplicaciones de escritorio.
- Programas locales

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

Configuración del acceso a aplicaciones locales y la redirección de URL

Para usar la función de acceso a aplicaciones locales y la redirección de URL con Citrix Receiver:

- Instale Citrix Receiver en la máquina cliente local. Puede habilitar ambas funciones durante la instalación de Citrix Receiver, 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 de Acceso a aplicaciones locales.

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 agente VDA ni los accesos directos de acceso a aplicaciones locales ni las aplicaciones publicadas de administrador.) Esta configuración de directiva se aplica a toda la máquina y a la directiva de redirección de URL.
2. Habilite el acceso a aplicaciones locales y la redirección de URL durante la instalación de Citrix Receiver para 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 Receiver con la opción siguiente:

   CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

   CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1

1. Ejecute **gpedit.msc**.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 icaclient.adm ubicada en la carpeta Configuration de Citrix Receiver (por regla general, en c:\Archivos de programa (x86)\Citrix\Online Plugin\Configuration). (Una vez agregada la plantilla icaclient.adm en Configuración del equipo, también estará disponible en Configuración de usuario.)
4. Expanda **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Citrix Components > Citrix Receiver > User Experience**.
5. Seleccione **Local App Access settings**.
6. Seleccione **Habilitada** y, a continuación, seleccione **Allow URL Redirection**. Para la redirección de URL, registre los complementos de explorador Web mediante la línea de comandos, como se describe a continuación.

Para proporcionar acceso solo a las aplicaciones publicadas:

1. En el servidor donde está instalado Delivery Controller, ejecute **regedit.msc**.
    1. Vaya a HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
    2. 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.
    1. Seleccione **Grupos de entrega** en el panel de navegación de Studio y, a continuación, seleccione la ficha Aplicaciones.
    2. Seleccione **Crear aplicación de acceso local** en el panel Acciones.
    3. Seleccione el Grupo de entrega de escritorios.
    4. Escriba la ruta completa del archivo ejecutable de la aplicación en la máquina local del usuario.
    5. 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.
    6. 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 Citrix Receiver para 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 Citrix Receiver 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.)

Nota: Los complementos del explorador Web necesarios para la redirección de URL se registran automáticamente al instalar Citrix Receiver 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*>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Para cancelar el registro de complementos en un dispositivo cliente: <*carpeta de instalación del cliente*>\redirector.exe /unreg<*explorador*>
- Para registrar complementos en un VDA: <*carpeta de instalación del VDA*>\VDARedirector.exe /reg<*explorador*>
- Para cancelar el registro de complementos en un VDA: <*carpeta de instalación del VDA*>\VDARedirector.exe /unreg<*explorador*>

donde <*explorador*> puede ser IE, FF, Chrome o All.

Por ejemplo, el siguiente comando registra los complementos de Internet Explorer en un dispositivo que ejecuta Citrix Receiver.

```
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
```

- De manera predeterminada, Internet Explorer redirige la dirección URL que se haya introducido. Si la URL no está en la lista negra pero es redirigida a otra URL por el explorador o el sitio Web, la URL final no se redirige aunque estuviera presente 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. Se debe permitir 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 de 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.

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 REG_DWORD Terminate con 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Consideraciones sobre unidades del cliente y USB

Dec 05, 2017

La tecnología HDX ofrece **respaldo optimizado** a los dispositivos USB más comunes. Esto incluye:

- Monitores
- Punteros (ratones)
- 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 ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión sobre una 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 respaldo optimizado o cuando ese respaldo no es adecuado, 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 Citrix Receiver para Android.
- La versión de Citrix Receiver 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 USB genérico puede utilizarse junto con el respaldo optimizado. Si habilita la redirección de USB genérico, configure las directivas de dispositivos USB de Citrix tanto para la redirección de USB genérico como para el respaldo optimizado si quiere evitar comportamientos inesperados e incoherentes.
> - La configuración de directiva Reglas de optimización de dispositivos USB del cliente de Citrix es una configuración específica para la redirección de USB genérico, para un determinado de dispositivo USB. No es el respaldo optimizado que se describe aquí.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Redirección de dispositivos USB Plug and Play del cliente es una característica relacionada que ofrece respaldo optimizado para dispositivos tales como cámaras y reproductores de medios que usan el protocolo de transferencia de imágenes (PTP) o el protocolo de transferencia multimedia (MTP). La redirección de USB Plug and Play del cliente no forma parte de la redirección de USB genérico. La redirección de USB Plug and Play del cliente solo está disponible en SO de servidor.

Con la redirección de USB genérico, para algunos tipos de dispositivos USB, la latencia de red y el ancho de banda pueden afectar a la experiencia de usuario y al funcionamiento del dispositivo USB. Por ejemplo, es posible que los dispositivos que tengan en cuenta el tiempo no funcionen correctamente en conexiones con enlaces de alta latencia y poco ancho de banda. En su lugar, use el respaldo optimizado, si es posible.

Algunos dispositivos USB requieren mucho ancho de banda para poderse usar como, por ejemplo, un mouse 3D (se usa con aplicaciones 3D que también suelen requerir una gran cantidad de ancho de banda). Puede evitar problemas de rendimiento con directivas de Citrix. 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.

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 que pueden ser confidenciales.

Los dispositivos USB se utilizan con frecuencia para distribuir software malicioso (malware). Configurar Citrix Receiver, XenApp y XenDesktop 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.

Important

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 el respaldo optimizado para ello.

Ofrezca instrucciones a los usuarios para un uso seguro de los dispositivos USB: usar solo los dispositivos USB que se hayan obtenido de una fuente de confianza; no perder de vista los dispositivos USB en entornos de libre acceso (por ejemplo, una unidad flash en una cafetería con WiFi). Asimismo, explique los riesgos de utilizar un dispositivo USB en más de un equipo.

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.

Estos Citrix Receiver admiten la redirección de USB genérico:

- Citrix Receiver para Windows. Consulte Configuración del entorno de XenDesktop.
- Citrix Receiver para Mac. Consulte Configuración de Citrix Receiver para Mac.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Citrix Receiver para Linux. Consulte Optimización.
- Citrix Receiver para Chrome OS. Consulte Acerca de Citrix Receiver para Chrome 2.1.

Para ver las versiones de Citrix Receiver, consulte Matriz de características de Citrix Receiver.

Si usa versiones anteriores de Citrix Receiver, consulte la documentación de Citrix Receiver para ver si se admite la redirección de USB genérico. Consulte la documentación de Citrix Receiver 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 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 genérico, consulte CTX123569. Algunos dispositivos USB no funcionan correctamente con la redirección de USB genérico.

Puede decidir los tipos de dispositivos USB que usarán la redirección de USB genérico. Se puede configurar de forma independiente:

- 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 Citrix Receiver, mediante los mecanismos que dependen de Citrix Receiver. Por ejemplo, Citrix Receiver para Windows se configura con parámetros de Registro que pueden gestionarse desde una plantilla administrativa. De forma predeterminada, la redirección de USB se permite para ciertas clases de dispositivos USB y se rechaza para otras; para obtener más información, consulte Configuración del entorno de XenDesktop en la documentación de Citrix Receiver para Windows para obtener más información.

Esta configuración independiente tiene la ventaja de ofrecer flexibilidad. Por ejemplo:

- Si dos departamentos o empresas diferentes se encargan de Citrix Receiver y del VDA, pueden aplicar medidas de control por separado. Estas se aplicarían cuando un usuario, ubicado en una empresa, accediera a una aplicación ubicada en otra empresa.

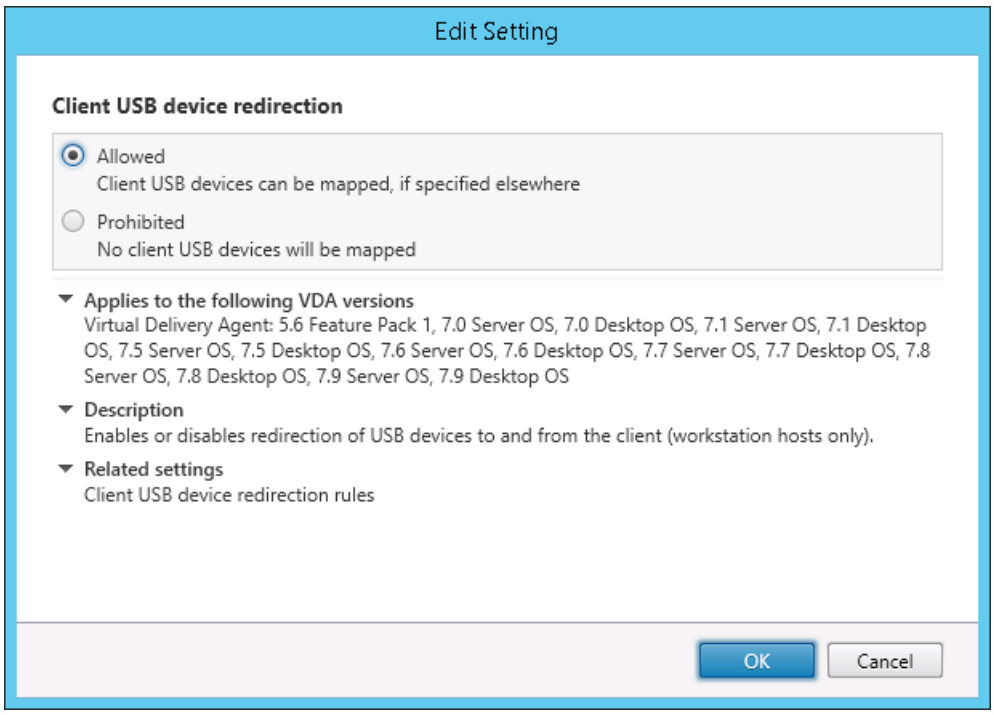
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Si solo 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 NetScaler Gateway), se puede controlar con las configuraciones de directivas de Citrix.

Para habilitar la redirección de USB genérico, configure Citrix Receiver y las configuraciones de directiva de Citrix.

En configuraciones de directiva de Citrix:

1. Agregue Redirección de dispositivos USB del cliente a una directiva y establezca su valor en **Permitida**.

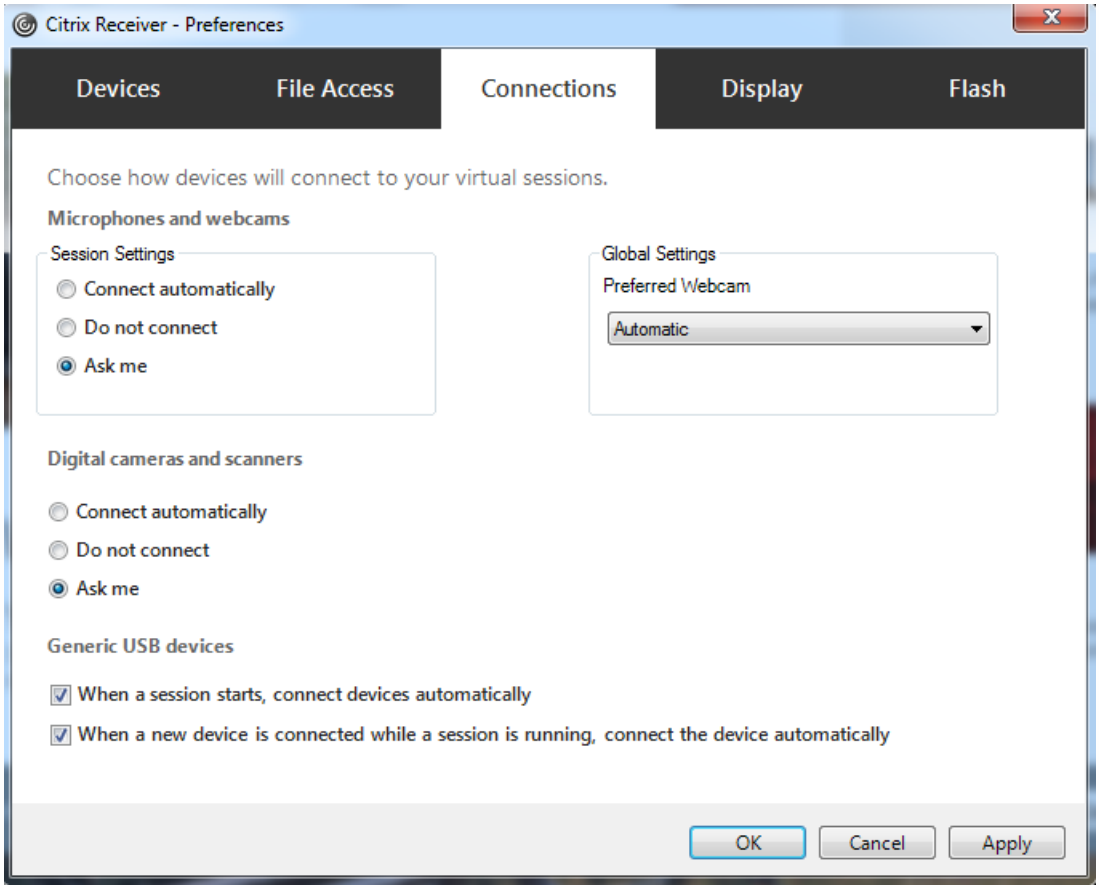


2. (Optativo.) Para actualizar la lista de dispositivos USB disponibles para la redirección, agregue la configuración Reglas de redirección de dispositivos USB del cliente a una directiva y especifique las reglas de la directiva de USB.

En Citrix Receiver:

3. Habilite el respaldo de USB cuando instale Citrix Receiver en los dispositivos de usuario. Puede hacerlo mediante una plantilla administrativa, o bien en Citrix Receiver para Windows > Preferencias > Conexiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



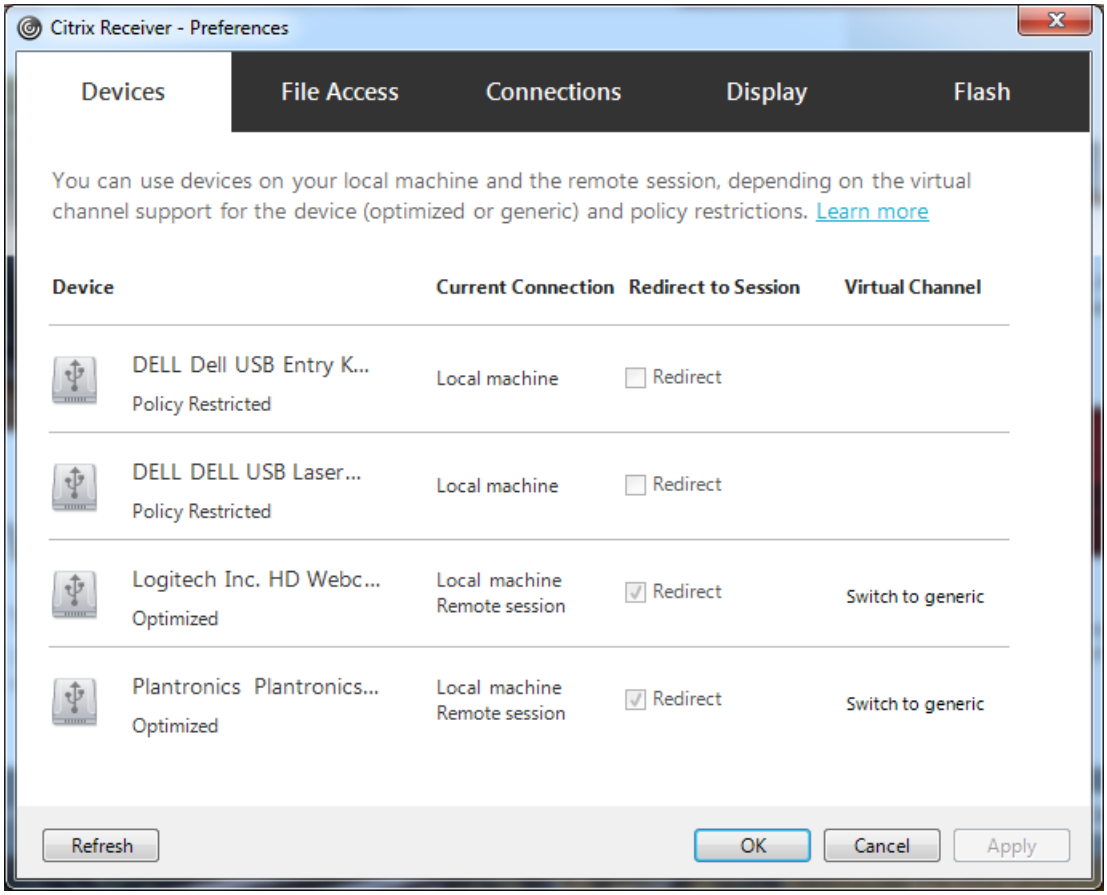
Si especificó reglas de directiva de USB para el agente VDA en el paso anterior, especifique las mismas reglas de directiva para Citrix Receiver.

Para los clientes ligeros, consulte al fabricante para obtener detalles sobre el respaldo de USB y cualquier configuración requerida.

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 de Citrix Receiver para Windows Cómo mostrar los dispositivos en Desktop Viewer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para usar la redirección de USB genérico en lugar del respaldo optimizado, puede:

- En Citrix Receiver, seleccione manualmente el dispositivo USB con que se va a usar la redirección de USB genérico, elija **Cambiar a genérico** en la ficha Dispositivos del cuadro de diálogo Preferencias.
- Seleccionar 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 CTX123015.

Nota: Configure la redirección de USB genérico para cámara Web solo si esta no resulta compatible con la redirección multimedia HDX.

Para evitar que los dispositivos USB se redirijan o se enumeren, puede especificar reglas de dispositivo para Citrix Receiver y el VDA.

Para la redirección de USB genérico, debe conocer al menos la clase y la subclase del dispositivo USB. No todos los dispositivos USB utilizan una clase y una subclase obvias. Por ejemplo:

- Las llaves de memoria o datos utilizan la clase de dispositivo del mouse.
- Los lectores de tarjeta inteligente pueden usar la clase de dispositivo HID o la que defina el proveedor.

Para un control más preciso, también necesitará saber el ID de proveedor, el ID de producto y el ID de versión. Puede obtener esa información del proveedor del dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important

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 de USB genérico especificando reglas de redirección de dispositivos USB tanto para VDA como para Citrix Receiver. De esta manera, se anularán las reglas predeterminadas de directiva de 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 Citrix Receiver 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 edita 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Las reglas predeterminadas del producto se almacenan en HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. 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. Las suplantaciones del objeto de directiva de grupo (GPO) se evalúan antes que las reglas predeterminadas del producto.

Las reglas de suplantación del administrador se almacenan en HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

REL	Identificador de la versión tomado del descriptor del dispositivo
Clase	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 nuevas 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 con el signo #. 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:

- En el siguiente ejemplo, se muestra una regla de directiva de USB definida por el administrador para identificadores de producto y proveedor:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
        Deny: VID=046D # Deny all Logitech products
```

- En el siguiente ejemplo, se muestra una regla de directiva de USB definida por el 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
```

Los usuarios pueden conectar un dispositivo USB antes o después de iniciar una sesión virtual.

Cuando se usa Citrix Receiver para Windows, ocurre lo siguiente:

- Los dispositivos conectados 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Se ofrece respaldo optimizado para dispositivos de almacenamiento USB, que forma parte la asignación de unidades del cliente de XenApp y XenDesktop. 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 con letras de unidades asignadas. Para configurar la asignación de unidades del cliente, utilice la configuración **Unidades extraíbles del cliente** en la sección Configuraciones de directiva de Redirección de archivos de las configuraciones de directivas ICA.

Con dispositivos de almacenamiento 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:

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	NO
Dispositivo para quitar 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 USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se inserta un dispositivo de almacenamiento antes o después de iniciar una sesión, el dispositivo se redirigirá mediante la asignación de unidades del cliente. Cuando la directiva de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se configura un dispositivo para la redirección automática (consulte http://support.citrix.com/article/CTX123015), y se inserta un dispositivo de almacenamiento antes o después de iniciar una sesión, el dispositivo se redirigirá mediante la redirección de USB genérico.

> ## Nota
>
> Se respalda la redirección USB en conexiones de poco ancho de banda: por ejemplo, conexiones de 50 kbps. Sin embargo, no funcionará copiar archivos de gran tamaño.

Puede controlar si los usuarios pueden copiar archivos desde sus entornos virtuales a sus dispositivos de usuario. De manera

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Impresión

Dec 05, 2017

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.

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.

En este entorno, toda impresión se inicia (por un usuario) en las máquinas que alojan las aplicaciones. Los trabajos de impresión se redirigen a través del servidor de impresión de red o un dispositivo del usuario hacia el dispositivo de impresión.

No hay ningún espacio de trabajo persistente para los usuarios de aplicaciones y escritorios virtuales. Cuando una sesión finaliza, se elimina el área de trabajo del usuario, por lo que todos los parámetros se deben volver a generar al comienzo de cada sesión. Por lo tanto, cada vez que un usuario inicia sesión, el sistema debe volver a generar el área de trabajo del usuario.

Cuando un usuario imprime:

- Determina las impresoras que se proporcionarán al usuario. Esto es lo que se conoce como aprovisionamiento de impresoras.
- Restaura las preferencias de impresión del usuario.
- Determina la impresora predeterminada de la sesión.

Puede personalizar el modo en que se realizan estas tareas si configura las opciones de aprovisionamiento de impresoras, enrutamiento de trabajos de impresión, retención de propiedades de impresora y administración de controladores. Asegúrese de conocer el modo en que los cambios en los diferentes parámetros de las opciones pueden afectar la experiencia de usuario y el rendimiento de la impresión en el entorno.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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:

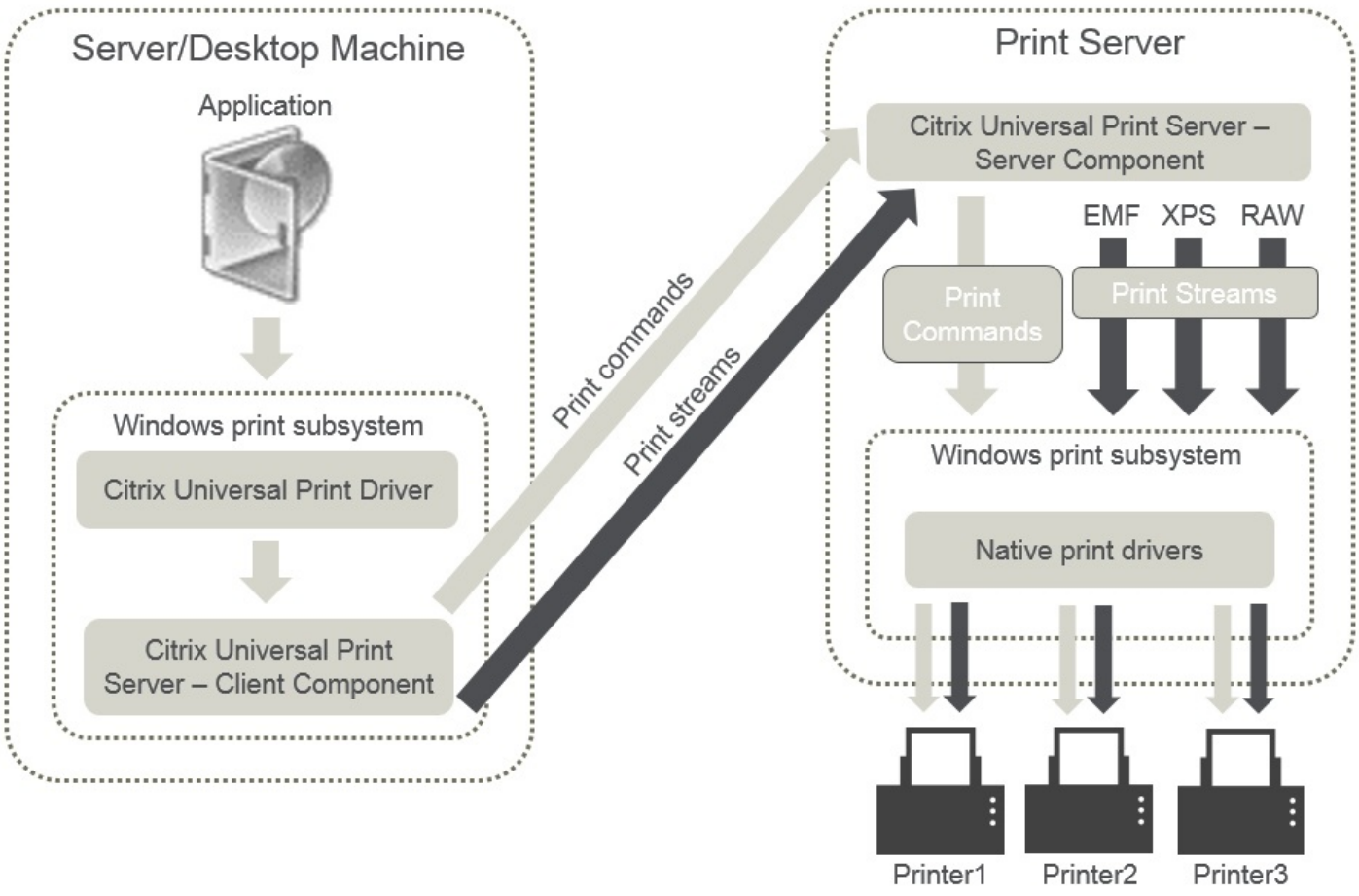
  Un componente de cliente, **UPClient**. Habilite UPClient en todas las máquinas con sistema operativo de servidor que aprovisionen impresoras de red para sesiones y usen el controlador de impresión universal.

  Un componente de servidor, **UPServer**. Instale UPServer en todos los servidores de impresión que aprovisionen impresoras de red para sesiones y usen el controlador de impresión universal para las impresoras de las sesiones (tanto si las impresoras de las sesiones se aprovisionan de manera centralizada como si no).

Para obtener información acerca de la instalación y los requisitos de Universal Print Server, consulte los artículos Requisitos del sistema e Instalación.

La siguiente ilustración muestra el flujo de trabajo típico que tiene una impresora de red en un entorno con Universal Print Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Al habilitar Citrix Universal Print Server, se aprovechan automáticamente todas las impresoras de red que están conectadas gracias a la detección automática.

Nota: Universal Print Server también se admite en VDI-in-a-Box 5.3. Para obtener más información acerca de la instalación de Universal Print Server con VDI-in-a-Box, consulte la documentación de VDI-in-a-Box.

- **Creación automática**. La *Creación automática* hace referencia a las impresoras que se crean automáticamente al comienzo de cada sesión. Se pueden actualizar automáticamente tanto las impresoras de red remotas como las impresoras de cliente conectadas localmente. Considere la posibilidad de crear automáticamente solo la impresora predeterminada del cliente para entornos con un gran número de impresoras por usuario. La creación automática de un número menor de impresoras produce una sobrecarga menor (consume menos memoria y CPU) en máquinas con sistema operativo 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La creación automática de impresoras del cliente y de red va asociada a un mantenimiento. Por ejemplo, agregar una impresora requiere:

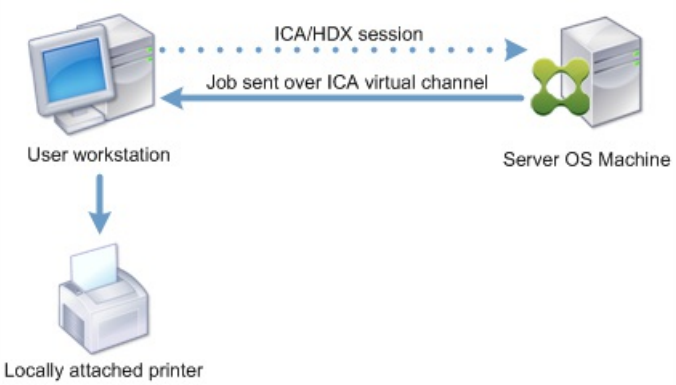
- Actualizar la configuración de directiva Impresoras de la sesión.
- Agregar el controlador a todas las máquinas con sistema operativo de servidor mediante la configuración de directiva Asignación y compatibilidad de controladores de impresora.

El término ruta de impresión incluye la ruta por la que se enrutan los trabajos de impresión y la ubicación donde se administran dichos trabajos en cola. Ambos aspectos de este concepto son importantes. El enrutamiento afecta al tráfico de red. La administración de la cola de impresión afecta a la utilización de recursos locales del dispositivo que procesa el trabajo de impresión.

En este entorno, los trabajos de impresión pueden tomar dos rutas para llegar a un dispositivo de impresión: a través del cliente o a través de un servidor de impresión de red. Estas rutas se conocen como la ruta de impresión de cliente y la ruta de impresión de red. La ruta de acceso seleccionada de forma predeterminada depende del tipo de impresora utilizada.

Impresoras conectadas localmente

El sistema 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 basadas en 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:

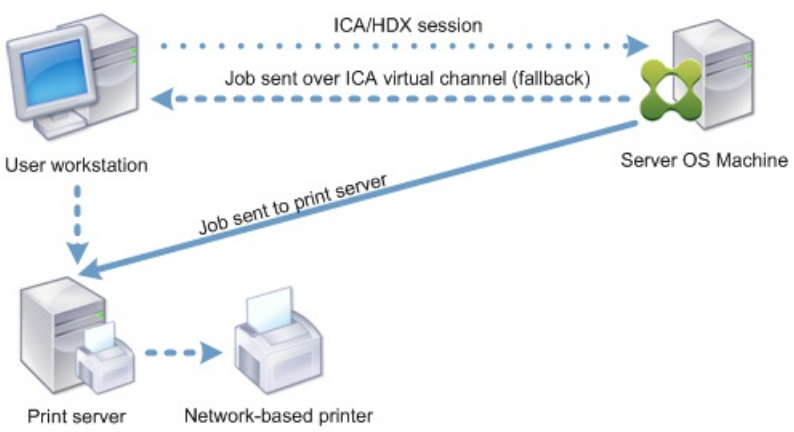
- Si el escritorio virtual o la aplicación no pueden establecer contacto con el servidor de impresión.
- Si el controlador nativo de impresora no está disponible en la máquina con sistema operativo de servidor.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



El controlador de impresora universal de Citrix (UPD) 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 del VDA de XenApp o XenDesktop. 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

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 Citrix Receiver. Obtiene el flujo de impresión entrante de la sesión de XenApp o XenDesktop. A continuación, lo reenvía al subsistema de impresión local, donde el trabajo de impresión se genera con los controladores específicos de impresora. Además del controlador de impresora universal de Citrix, el controlador PDF de impresora universal de Citrix se puede instalar por separado con Citrix Receiver para HTML5 y Citrix Receiver para Chrome.

El controlador de impresora universal de Citrix respalda los siguientes formatos de impresión:

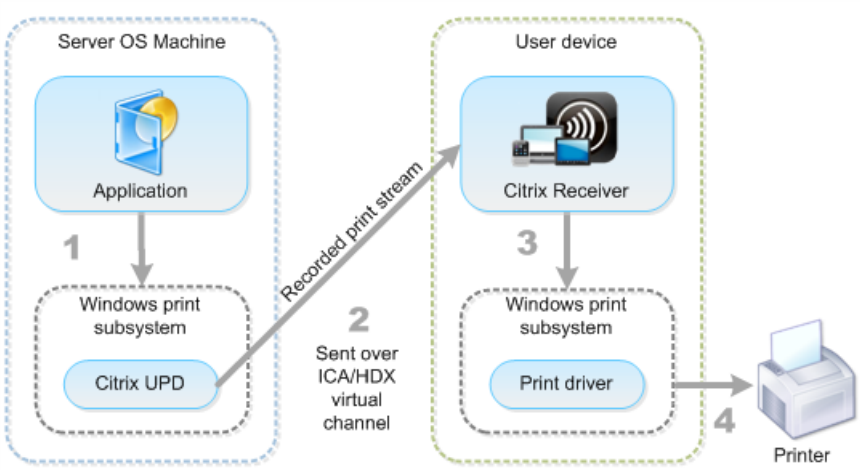
- Formato de metarchivo mejorado (**EMF**); opción predeterminada. EMF es la versión de 32 bits de Windows Metafile (WMF). Solo los clientes Windows pueden usar el controlador de EMF.
- XML Paper Specification (**XPS**). El controlador XPS utiliza XML para crear un "documento electrónico" independiente 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

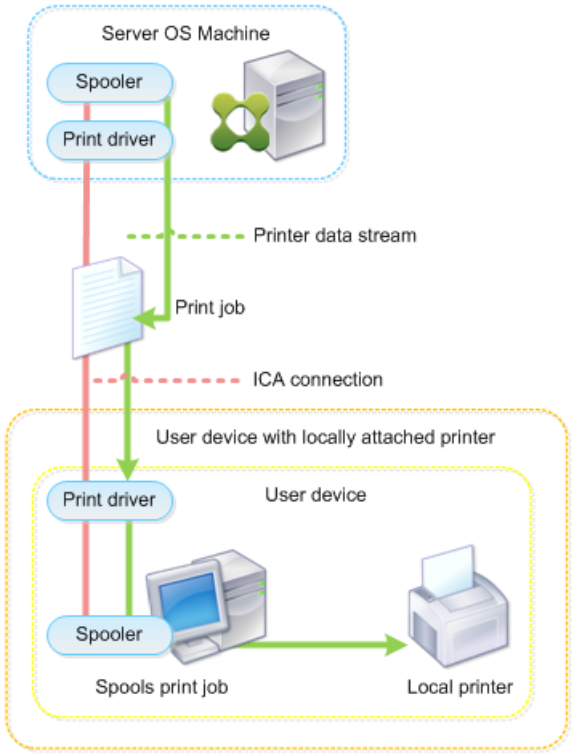


A la hora de planificar su estrategia de administración de controladores, decida si va a admitir controladores específicos del dispositivo, el controlador de impresión universal o ambos. Si decide admitir controladores estándar, también debe decidir:

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 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.

- Ejemplo de configuración de impresión
- Procedimientos recomendados, aspectos a tener en cuenta sobre la seguridad y operaciones predeterminadas
- Directivas y preferencias de impresión
- Aprovisionar impresoras
- Mantener el entorno de impresión

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ejemplo de configuración de impresión

Mar 26, 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:

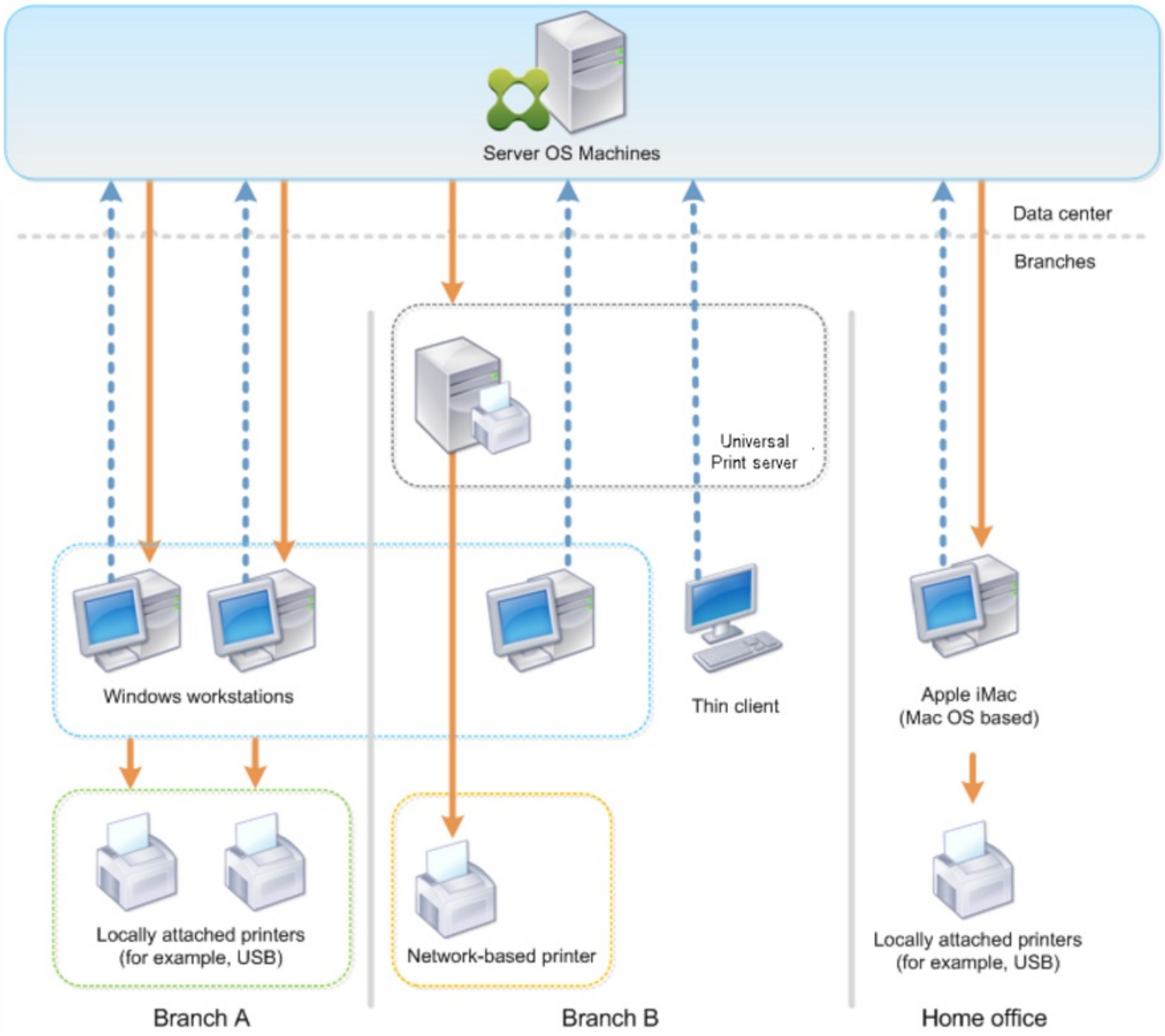
- Las necesidades de su negocio y la infraestructura de impresión existente.
  Diseñe la configuración de impresión teniendo en cuenta las necesidades de su organización. Estudie la implementación actual (capacidad de los usuarios para agregar impresoras, qué usuarios tienen acceso a qué impresora, etcétera) 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.

La siguiente ilustración muestra la implementación de impresión para estos casos de uso:

- **Oficina A**. Una pequeña sucursal exterior con algunas estaciones de trabajo Windows. La estación de trabajo de cada usuario tiene una impresora conectada localmente, privada.
- **Oficina B**. Una gran sucursal con clientes ligeros y estaciones de trabajo Windows. Para una mayor eficiencia, los usuarios de esta oficina comparten impresoras de red (una por planta). Unos servidores de impresión Windows ubicados dentro de la oficina se encargan de administrar las colas de impresión.
- **Oficina en casa**. Una oficina en el domicilio de un usuario, con un dispositivo de usuario Mac OS, que accede a la infraestructura Citrix de la empresa. El dispositivo del usuario tiene una impresora conectada localmente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Las secciones siguientes describen las configuraciones que minimizan la complejidad del entorno y simplifican la administración.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

En la Oficina B, todas las impresoras están en red y sus colas de impresión se administran en un servidor de impresión Windows, por lo que Citrix Universal Print Server es la configuración más eficaz.

Los administradores locales instalan y administran todos los controladores de impresora obligatorios en el servidor de impresión. La asignación de impresoras en la sesión del escritorio virtual o de la aplicación funciona del siguiente modo:

- Para estaciones de trabajo Windows. El equipo de TI local ayuda a los usuarios a conectarse a la impresora de red correspondiente a sus estaciones de trabajo Windows. Esto permite a los usuarios imprimir desde las aplicaciones instaladas localmente.
  Durante la sesión de una aplicación o un escritorio virtual, las impresoras configuradas de forma local se enumeran a través de la creación automática. A continuación, el escritorio virtual o la aplicación se conectan al servidor de impresión como una conexión de red directa, si es posible.

  Los componentes de Citrix Universal Print Server están instalados y habilitados, por lo que no se requieren los controladores nativos de impresora. La actualización de un controlador o la modificación de una cola de impresión no requieren configuración adicional en el centro de datos.

- Para clientes ligeros. En caso de usuarios de clientes ligeros, las impresoras deben estar conectadas en la sesión del escritorio virtual o de la aplicación. Con el fin de proporcionar a los usuarios la experiencia de impresión más sencilla posible, los administradores configuran una sola directiva de Impresoras de la sesión de Citrix por planta para establecer la impresora de la planta como impresora predeterminada.
  Para asegurarse de que esté conectada la impresora correcta incluso si los usuarios se desplazan entre las distintas plantas, las directivas se filtran según la subred o el nombre del cliente ligero. Esa configuración, conocida como impresión de proximidad, permite el mantenimiento del controlador de impresora local (de acuerdo con el modelo de administración delegada).

  En caso de agregar o modificar una cola de impresión, los administradores Citrix deben modificar la correspondiente directiva de Impresoras de la sesión en el entorno.

Debido a que el tráfico de impresión de red se envía fuera del canal virtual ICA, se implementa QoS. El tráfico de red entrante y saliente de los puertos usados para el tráfico de ICA/HDX tiene prioridad sobre el tráfico de red restante. Esta configuración garantiza que las sesiones de usuario no se vean afectadas por trabajos de impresión de gran envergadura.

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Procedimientos recomendados, aspectos a tener en cuenta sobre la seguridad y operaciones predeterminadas

Dec 05, 2017

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.

Las soluciones de impresión de Citrix se han diseñado para ofrecer seguridad.

- El servicio Citrix Print Manager Service lleva a cabo una supervisión constante y responde a sucesos de sesión tales como el inicio y cierre de sesión, la desconexión y reconexión, y la terminación de la sesión. Se encarga de las solicitudes de servicio mediante la suplantación de la sesión real del usuario.
- La impresión de Citrix asigna a cada impresora un único espacio de nombres en una sesión.
- La impresión de Citrix establece el descriptor de seguridad predeterminado para impresoras de creación automática para asegurarse de que las impresoras del cliente creadas automáticamente en una sesión no sean accesibles para usuarios de otras sesiones. De forma predeterminada, los usuarios administrativos no pueden imprimir por error en la impresora del cliente de otra sesión, aunque sí pueden ver y ajustar manualmente los permisos de cualquier impresora del cliente.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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, 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 está seguro de cuáles son los parámetros de impresión de fábrica, puede verlos creando una nueva directiva y definiendo todas las reglas de directiva de impresión con la opción Habilitada. La opción que aparece es la opción predeterminada.

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 de PowerShell **Start-TelemetryUpload**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Directivas y preferencias de impresión

Dec 05, 2017

Cuando los usuarios acceden a impresoras desde las aplicaciones publicadas, puede configurar directivas de XenApp para especificar:

- Cómo se aprovisionan las impresoras (cómo se agregan a las sesiones)
- Cómo se enrutan los trabajos de impresión
- Cómo se administran los controladores de impresora

Puede tener configuraciones de impresión diferentes para distintos dispositivos del usuario, usuarios o cualquier otro objeto sobre los que se puedan aplicar filtros de directiva.

La mayoría de las funcionalidades de impresión se configuran mediante las directivas de impresión de Citrix.Las configuraciones de impresión siguen el comportamiento de las directivas estándar de Citrix.

El sistema puede escribir las configuraciones de impresora en el objeto de impresora al final de la sesión o en un dispositivo de impresión del cliente, con tal de que la cuenta de red del usuario tenga los permisos necesarios. De forma predeterminada, Citrix Receiver 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.

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 mismo dispositivo del usuario.** 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 como, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

cambios. Esto también significa que la configuración de impresión que aparece en un lugar como, por ejemplo, un programa de hojas de cálculo, puede ser distinta a la que aparece en otro (por ejemplo, en documentos). Como resultado, la configuración de impresión aplicada a una impresora específica puede cambiar durante la misma sesión.

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 de sistema operativo de servidor con cualquier otra configuración de impresora conservada o del cliente.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aprovisionamiento de impresoras

Dec 05, 2017

Existen tres métodos de aprovisionamiento de impresoras:

- Citrix Universal Print Server
- Impresoras del cliente creadas automáticamente
- Impresoras de sesión asignadas por los administradores

A la hora de determinar la mejor solución de impresión para el entorno, tenga en cuenta lo siguiente:

- Universal Print Server ofrece funciones no disponibles para el proveedor de impresión de Windows: almacenamiento en caché de imágenes y fuentes, compresión avanzada, optimización y 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.

Instalación de 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 Instalación de componentes principales e Instalación mediante 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 XenApp y XenDesktop para SO de escritorio Windows o SO de servidor Windows.
2. Extraiga el VDA siguiendo las instrucciones de línea de comandos descritas en Instalación de VDA 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
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

Cómo 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 no quiere 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 edita 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. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

Para obtener más información, consulte Citrix Insight Services.

Configuración de Universal Print Server

Utilice las siguientes configuraciones de directiva de Citrix para definir Universal Print Server. Para obtener más información, consulte la ayuda en pantalla de las configuraciones de directiva.

- **Habilitar Universal Print Server**.De forma predeterminada, Universal Print Server está inhabilitado. Al habilitar Universal Print Server, puede elegir si desea usar el proveedor de impresión de Windows en caso de que Universal Print Server no esté disponible. Después de habilitar Universal Print Server, los usuarios pueden agregar y enumerar las impresoras de red a través de las interfaces del proveedor de impresión de Windows y del proveedor de Citrix.
- **Puerto del flujo de datos de impresión de Universal Print Server (CGP)**.Especifica el número de puerto TCP utilizado por el proceso de escucha del protocolo CGP del flujo de datos de impresión de Universal Print Server. El valor predeterminado es **7229**.
- **Puerto del servicio Web de Universal Print Server (HTTP/SOAP)**.Especifica el número de puerto TCP utilizado por el proceso de escucha de Universal Print Server para solicitudes HTTP/SOAP entrantes. El valor predeterminado es **8080**.

Para cambiar el puerto predeterminado de HTTP 8080 para la comunicación entre Universal Print Server y los agentes VDA de XenApp y XenDesktop, también debe crearse el siguiente 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:

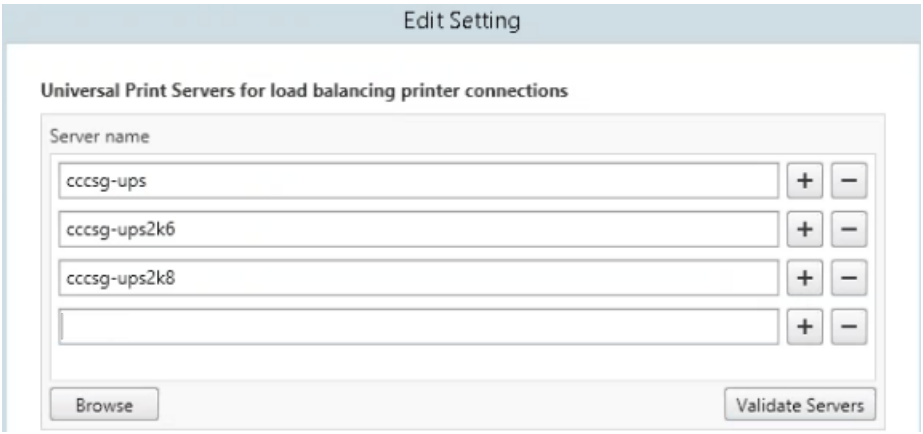
Este número de puerto debe coincidir con el puerto del servicio Web de Universal Print Server (HTTP/SOAP) de la directiva HDX, en Studio.

- **Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (kpbs)**.Especifica el límite

© 1999-2017 Citrix Systems, Inc. All rights reserved.

superior (en kilobits por segundo) de la velocidad de transferencia de datos de impresión entregada desde cada trabajo de impresión a Universal Print Server mediante CGP. El valor predeterminado es 0 (no hay límite).

- **Universal Print Servers para equilibrio de carga**. Esta configuración enumera los servidores de impresión universal que se usarán para equilibrar la carga de las conexiones de impresora establecidas al comienzo de las sesiones, después de evaluar otras configuraciones de impresión de Citrix. Para optimizar la creación de impresoras, Citrix recomienda que todos los servidores de impresión tengan el mismo conjunto de impresoras compartidas.



- **Umbral para servidores Universal Print Server fuera de servicio**. Especifica cuánto tiempo debe esperar el equilibrador de carga a que se recupere un servidor de impresión no disponible antes de determinar que ese servidor está fuera de línea permanentemente y redistribuir su carga en otros servidores de impresión disponibles. El valor predeterminado es 180 segundos.

Una vez que las directivas de impresión se modifican en el Delivery Controller, los cambios de la directiva pueden tardar unos minutos en aplicarse en los VDA.

Interacciones con otras configuraciones de directiva. Universal Print Server acepta otras configuraciones de directiva de impresión Citrix e interactúa con ellas como se indica en la siguiente tabla. En la tabla siguiente se presupone que la directiva de Universal Print Server está habilitada, que sus componentes están instalados y que se están aplicando las configuraciones de la directiva.

Configuración de directiva	Interacción
Redirección de impresoras del cliente, Crear automáticamente las impresoras del cliente	Después de habilitar Universal Print Server, las impresoras de red del cliente se crean mediante el controlador de impresión universal en lugar de los controladores nativos. Los usuarios verán el mismo nombre de impresora que antes.
Impresoras de la sesión	Cuando se utiliza la solución Citrix Universal Print Server, se respetan las configuraciones de directiva del controlador de impresión universal.
Conexiones directas con servidores de impresión	Cuando Universal Print Server está habilitado y la configuración de directiva sobre el uso del controlador de impresión universal está configurada para usar solo la impresión universal, se puede crear una conexión directa entre la impresora de red y el servidor de impresión

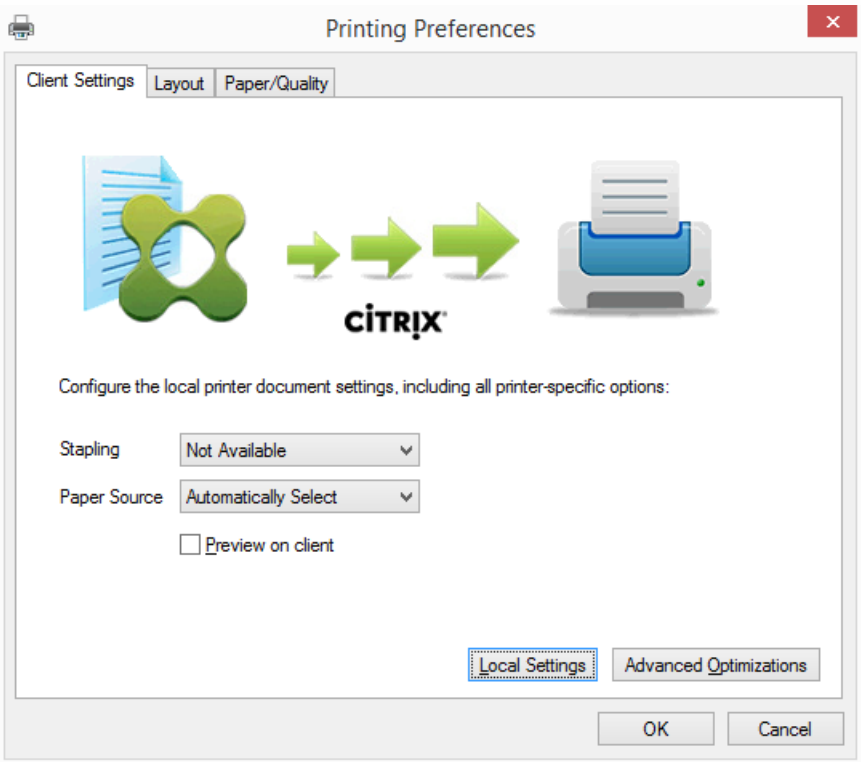
© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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.



Diálogo de impresión personalizado del controlador UPD

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

estarán disponibles cuando se use el controlador de impresora universal de Citrix.

Cuando se usa Universal Print Server, el asistente Agregar impresora para el proveedor de impresión de Citrix es el mismo que el asistente Agregar impresora del proveedor de impresión de Windows, con las siguientes excepciones:

- Cuando se agrega una impresora por su nombre o su dirección, puede proporcionar un número de puerto HTTP/SOAP para el servidor de impresión. Ese número de puerto formará parte del nombre de la impresora y es el que se muestra en pantalla.
- Si en la configuración de directiva sobre el uso del controlador de impresión universal de Citrix se especifica que se debe usar la impresión universal, cuando se seleccione una impresora aparecerá el nombre del controlador de impresión universal. El proveedor de impresión de Windows no puede usar el controlador de impresión universal.

El proveedor de impresión de Citrix no respalda la generación en el lado del cliente.

Para obtener más información acerca de Universal Print Server, consulte CTX200328.

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 o Citrix Receivers 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 Citrix Receivers que no sean de Windows, use uno de los otros controladores de impresión universal que están basados en PostScript/PCL y se instalan automáticamente.

- **Controladores de impresora universal de Citrix**: Un controlador de impresora universal que es independiente del dispositivo. Si configura el controlador de impresión universal de Citrix, el sistema usa el controlador de impresión universal EMF de forma predeterminada.
  El controlador de impresión universal de Citrix también puede crear trabajos de impresión más pequeños que controladores de impresora anteriores o menos avanzados. No obstante, puede que sea necesario usar el controlador específico del dispositivo para optimizar los trabajos de impresión para la impresora especializada.

Configurar la impresión universal Utilice las siguientes configuraciones de directiva Citrix para configurar la impresión universal. Para obtener más información, consulte la ayuda en pantalla de las configuraciones de directiva.

- Uso de controladores de impresión universal. Especifica cuándo se usa la impresión universal.
- Crear automáticamente una impresora universal genérica. Habilita o inhabilita la creación automática del objeto genérico de Citrix Universal Printer para las sesiones en las que se utiliza un dispositivo de usuario compatible con la impresión universal. De forma predeterminada, el objeto genérico de impresora universal no se crea automáticamente.
- Preferencia de controlador universal. Especifica el orden en que el sistema intenta usar los controladores de impresión universal, a partir del primer elemento de la lista. Es posible agregar, modificar o eliminar controladores, y cambiar el orden de los controladores en la lista.
- Preferencia de vista previa en impresión universal. Especifica si se usará la función de vista previa de impresión para las impresoras universales genéricas o creadas automáticamente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 obtener más información, consulte Optimización del 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. Puede controlar el tipo de impresoras que se aprovisionan 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).

De forma predeterminada, las impresoras de red del dispositivo del usuario se crean automáticamente al comienzo de las sesiones. El sistema permite reducir el número de impresoras de red que se enumeran y se asignan al especificar las impresoras de red que se crearán en cada sesión. Estas impresoras se denominan impresoras de sesión.

Puede filtrar las directivas de impresora de sesión por dirección IP para proporcionar la impresión de proximidad. Con la impresión de proximidad los usuarios que se encuentran dentro de un intervalo de direcciones IP especificado acceden automáticamente a los dispositivos de impresión en red que existen dentro de ese intervalo. Citrix Universal Print Server ofrece la impresión de proximidad, que no requiere la configuración que se describe en esta sección.

La impresión de proximidad puede utilizarse en estas circunstancias:
- La red interna de la empresa opera con un servidor DHCP que designa automáticamente direcciones IP a los usuarios.
- Todos los departamentos de la organización tienen intervalos de direcciones IP designados de manera exclusiva.
- Existen impresoras de red para cada uno de los intervalos de direcciones IP de departamento.

Cuando se configura la impresión de proximidad y un empleado se desplaza de un departamento a otro, no se requiere la configuración adicional de un dispositivo de impresión. Después de reconocer el dispositivo del usuario en el nuevo intervalo de direcciones IP del departamento, este dispositivo tendrá acceso a todas las impresoras de red pertenecientes a ese intervalo.

Configurar impresoras específicas para redirigirlas durante las sesiones Para crear impresoras asignadas por un administrador, configure el parámetro de directiva 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 en el formato \\servername\printername.
- Busque una ubicación para la impresora en la red.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Busque impresoras en un servidor específico. Introduzca el nombre del servidor en el formato \\servername y haga clic en Examinar.

Importante: El servidor combina todas las configuraciones de parámetros de impresoras de sesión que estén habilitadas en todas las directivas aplicadas, empezando por las de mayor prioridad. Cuando una impresora está configurada en varios objetos de directiva, se toman los parámetros predeterminados únicamente del objeto de directiva de mayor prioridad en el cual se haya configurado la impresora.
Las impresoras de red creadas con la configuración Impresoras de la sesión pueden variar según las condiciones en donde se inició la sesión al aplicar un filtro en objetos, como, por ejemplo, las subredes.

Especificar una impresora de red predeterminada para una sesión De manera predeterminada, se usa la impresora principal del usuario como la impresora predeterminada de la sesión. Use la configuración de directiva de Citrix Impresora predeterminada para cambiar la forma en que la impresora predeterminada del dispositivo del usuario se establece en una sesión.

1. En la página de configuración Impresora predeterminada, seleccione un parámetro para Elegir impresora predeterminada del cliente:
   - Network printer name. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mantenimiento del entorno de impresión

Dec 05, 2017

Mantener el entorno de impresión implica:

- Administrar controladores de impresora
- Optimizar el rendimiento de la impresión
- Visualizar la impresora y administrar las colas de impresión

Para minimizar la carga de administración y los problemas potenciales de los controladores de impresión, Citrix recomienda el uso del controlador de impresión universal de Citrix.

Si se produce un error en el proceso de creación automática, de forma predeterminada, el sistema instala un controlador de impresora nativo de Windows, proporcionado con Windows. Si el controlador no está disponible, el sistema recurre al controlador de impresión universal. Para obtener más información acerca de los valores predeterminados del controlador de impresora, consulte Procedimientos recomendados, aspectos a tener en cuenta sobre la seguridad y operaciones predeterminadas.

Si el controlador de impresión universal de Citrix no es una opción válida en todas las situaciones, asigne controladores de impresora para reducir la cantidad de controladores instalados en las máquinas con sistema operativo 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Para prohibir un controlador de impresora, seleccione el nombre del controlador y elija el parámetro No crear.
3. Si fuera necesario, modifique una asignación existente de controladores, elimínela o cambie el orden de los controladores en la lista.
4. Si quiere modificar los parámetros de impresión para los controladores de impresoras del cliente asignadas, seleccione el controlador de impresora, haga clic en Configuración y especifique parámetros tales como la calidad de impresión, la orientación y el color. Si especifica una opción de impresión que no 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.

Para optimizar el rendimiento de la impresión, use Universal Print Server y el controlador de impresión universal. Las siguientes directivas rigen la optimización y la compresión de la impresión:

- Valores predeterminados de optimización de la impresión universal. Especifica los parámetros predeterminados al crear una impresora universal para la sesión:
  - Calidad de imagen deseada especifica el límite predeterminado de compresión de imagen aplicable a la impresión universal. De forma predeterminada, la Calidad estándar está habilitada, de manera que los usuarios solo pueden imprimir imágenes con la compresión de calidad estándar o reducida.
  - Habilitar la compresión intensa habilita o inhabilita la reducción de ancho de banda más allá del nivel de compresión definido por Calidad de imagen deseada, sin pérdida de calidad de imagen. La compresión intensa está inhabilitada de forma predeterminada.
  - La configuración de Almacenamiento en caché de imágenes y fuentes especifica si las imágenes y fuentes que aparecen varias veces en el flujo de impresión se almacenan en caché, para que cada imagen individual se envíe solo una vez a la impresora. De forma predeterminada, las fuentes e imágenes incrustadas se almacenan en caché.
  - Permitir a los no administradores modificar estos parámetros especifica si los usuarios pueden cambiar los parámetros predeterminados de optimización de la impresión en una sesión. De forma predeterminada, los usuarios no pueden cambiar los parámetros predeterminados de la optimización de impresión.
- Límite de compresión de imagen para la impresión universal. Define la calidad máxima y el nivel de compresión mínimo disponibles para las imágenes impresas con el controlador de impresión universal. De forma predeterminada, el límite de compresión de imagen está definido en Mejor calidad (compresión sin pérdida).
- Límite de calidad de la impresión universal. Especifica la cantidad máxima de puntos por pulgada (ppp) disponibles para generar una salida impresa en la sesión. De forma predeterminada, no existe ningún límite.

De forma predeterminada, todos los trabajos de impresión destinados a impresoras de red se enrutan desde la máquina con sistema operativo 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)

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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

La siguiente tabla resume los sitios donde se pueden administrar colas de impresión y mostrar las impresoras existentes en el entorno.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Ruta de impresión	¿Control de cuentas de usuario habilitado?	Ubicación
Impresoras del cliente (Impresoras conectadas al dispositivo del usuario)	Ruta de impresión de cliente	Iniciado	Complemento Administración de impresión de la consola Microsoft Management Console
		Apagado	Versiones anteriores a 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	Iniciado	Servidor de impresión > Complemento Administración de impresión de la consola Microsoft Management Console
		Apagado	Servidor de impresión > Panel de control
Impresoras de red (Impresoras de un servidor de impresión en red)	Ruta de impresión de cliente	Iniciado	Servidor de impresión > Complemento Administración de impresión de la consola Microsoft Management Console
		Apagado	Versiones anteriores a 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	Iniciado	Servidor de impresión > Panel de control
		Apagado	Servidor de impresión > Panel de control

Nota: Las colas de impresión de las impresoras de red que usan la ruta de impresión en red son privadas y no se pueden administrar en el sistema.

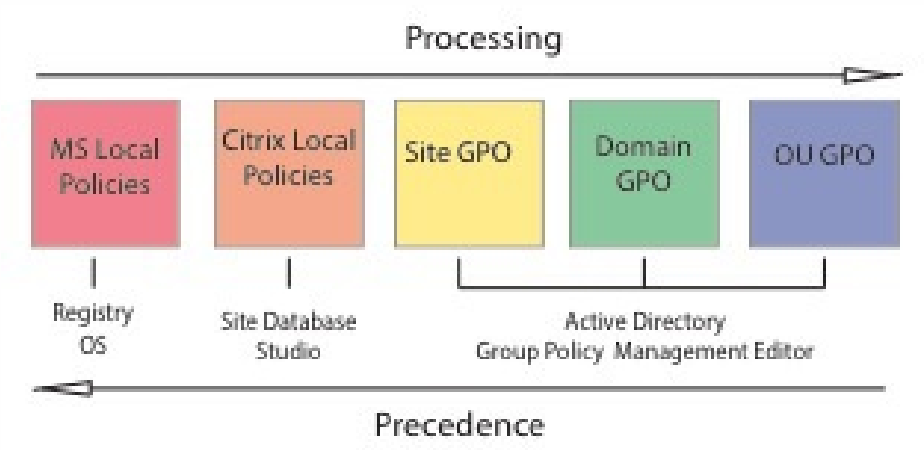
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Policies (Directivas)

Dec 05, 2017

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 reglas y criterios 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 del objeto de directiva de grupo (GPO) de la unidad organizativa (OU) tienen la precedencia más alta en la red. Las directivas a nivel de grupo GPO del dominio anulan las directivas de GPO del sitio que, a su vez, anulan las directivas en conflicto que haya en los niveles de directivas locales de Citrix y de Microsoft.

Todas las Directivas locales de Citrix se crean y se administran en la consola de Citrix Studio y se guardan en la base de datos del sitio, mientras que las Directivas de grupo se crean y se administran con la Consola de administración de directivas de grupo (GPMC) de Microsoft 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) desde la Consola de administración de directivas de grupo GPMC 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. Los parámetros de directiva sin configurar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Receiver 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 directiva y las aplica a los Registros del dispositivo de punto final y la máquina que aloja el recurso.
7. El usuario cierra la sesión en el recurso. Las directivas de Citrix para el usuario final y el dispositivo de punto final ya no están activas.
8. El usuario cierra la sesión en el dispositivo de usuario, lo que libera las directivas del GPO de usuario.
9. El usuario final apaga el dispositivo, lo que libera las directivas del GPO de máquina.

Al crear directivas para grupos de usuarios, dispositivos y máquinas, algunos miembros pueden tener diferentes requisitos y necesitan excepciones en algunas configuraciones de directiva. Las excepciones se realizan mediante filtros en Studio y la consola GPMC, que determinan a quién o a qué afecta la directiva.

Nota: No se admite la combinación de directivas de Windows y Citrix en el mismo objeto de directiva de grupo.

Contenido relacionado

- Trabajar con directivas
- Plantillas de directiva
- Crear directivas
- Comparar, priorizar, modelar y solucionar problemas de directivas
- Parámetros predeterminados de directivas
- Referencia para configuraciones de directivas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Trabajar con directivas

Dec 05, 2017

Configure directivas de Citrix para controlar el acceso de los usuarios y los entornos de sesión. Las directivas de Citrix son el método más eficaz para controlar los parámetros de conexión, seguridad y ancho de banda. Puede crear directivas para grupos de usuarios, dispositivos o tipos de conexión específicos. Cada directiva puede contener varias configuraciones.

Herramientas para trabajar con las directivas de Citrix

Puede utilizar las siguientes herramientas para trabajar con directivas de Citrix.

- **Studio**: Si usted es un administrador Citrix y no tiene permisos para administrar directivas de grupo, utilice Studio para crear directivas para su sitio. Las directivas creadas con Studio se almacenan en la base de datos del sitio y las actualizaciones se envían al escritorio virtual cuando el escritorio virtual se registra con el broker o cuando un usuario se conecta a ese escritorio virtual.
- **Editor de directivas de grupo local** (complemento de Microsoft Management Console): Si su entorno de red utiliza Active Directory y usted tiene permisos para administrar las directivas de grupo, puede usar el Editor de directivas de grupo local para crear directivas para un sitio. Las configuraciones que defina afectarán a los objetos de directiva de grupo (GPO) que especifique en la Consola de administración de directivas de grupo.
  Importante: Debe usar el Editor de directivas de grupo local para definir algunas configuraciones de directiva, incluidas las relacionadas con el registro de los VDA en el Controller, y las relacionadas con servidores de Microsoft App-V.

Procesamiento de directivas y precedencia

Las configuraciones de directiva de grupo se procesan en el orden siguiente:

1. GPO locales
2. GPO del sitio de XenDesktop o XenApp (almacenados en la base de datos del sitio)
3. GPO de sitio
4. GPO de dominio
5. Unidades organizativas

No obstante, en caso de un conflicto, las últimas configuraciones de directiva que se procesan 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 permite 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 impide 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 a nivel de objeto de directiva de grupo del 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Comparación, prioridad, modelado y solución de 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.

Exploración de las directivas y las configuraciones de Citrix

En el Editor de directivas de grupo local, las directivas y las configuraciones aparecen en dos categorías: Configuración de equipo y Configuración de usuario. Cada categoría tiene un nodo de Directivas de Citrix. Consulte la documentación de Microsoft para obtener más detalles sobre cómo explorar y usar este complemento.

En Studio, las configuraciones de directiva se ordenan en categorías según la funcionalidad o la característica a la que afectan. Por ejemplo, la sección Profile Management contiene las configuraciones de directiva de Profile Management.

- Las configuraciones de equipo (configuraciones de directiva que se aplican a las máquinas) definen el comportamiento de los escritorios virtuales y se aplican cuando se inicia un escritorio virtual. Estas configuraciones se aplican incluso cuando no hay sesiones de usuario activas en el escritorio virtual. Las configuraciones de usuario definen la experiencia del usuario al conectarse mediante ICA. Las directivas de usuario se aplican cada vez que un usuario se conecta o reconecta mediante ICA. Las directivas de usuario no se aplican cuando un usuario se conecta a través de RDP o inicia sesión directamente en la consola.

  Para acceder a las directivas, sus configuraciones y plantillas, seleccione Directivas en el panel de navegación de Studio.

  - La ficha **Directivas** muestra todas las directivas. Cuando se selecciona una directiva, las etiquetas a la derecha muestran: Información general (el nombre, la prioridad, su estado habilitado o inhabilitado y una descripción), Configuraciones (lista de configuraciones definidas) y Asignada a (objetos de usuario y máquina a los que la directiva esté asignada en ese momento). Para obtener más información, consulte Creación de directivas.
  - La ficha **Plantillas** enumera las plantillas suministradas por Citrix y las plantillas que usted haya creado. Cuando se selecciona una plantilla, las fichas a la derecha muestran: Descripción (para qué se puede usar la plantilla) y Configuraciones (lista de configuraciones definidas). Para obtener más información, consulte Plantillas de directiva.
  - La ficha **Comparación** permite comparar las configuraciones de una directiva o de una plantilla con las de otras directivas o plantillas. Por ejemplo, puede que quiera verificar los valores de configuración para asegurar que se cumplen las directrices recomendadas. Para obtener más información, consulte Comparación, prioridad, modelado y solución de problemas de directivas.
  - En la ficha **Modelado**, puede simular escenarios de conexión con directivas de Citrix. Para obtener más información, consulte Comparación, prioridad, modelado y solución de problemas de directivas.

  Para buscar una configuración dentro de una directiva o una plantilla:

  1. Seleccione la directiva o la plantilla.
  2. Seleccione Modificar directiva o Modificar plantilla en el panel Acciones.
  3. En la página Configuraciones, comience a escribir el nombre de la configuración.

  Puede limitar la búsqueda si selecciona una versión específica del producto, seleccionando una categoría (por ejemplo, el Ancho de banda) o marcando la casilla Ver solo seleccionadas o eligiendo buscar solo entre las configuraciones que se han agregado a la directiva seleccionada. Para realizar una búsqueda sin filtro, seleccione Todas las configuraciones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

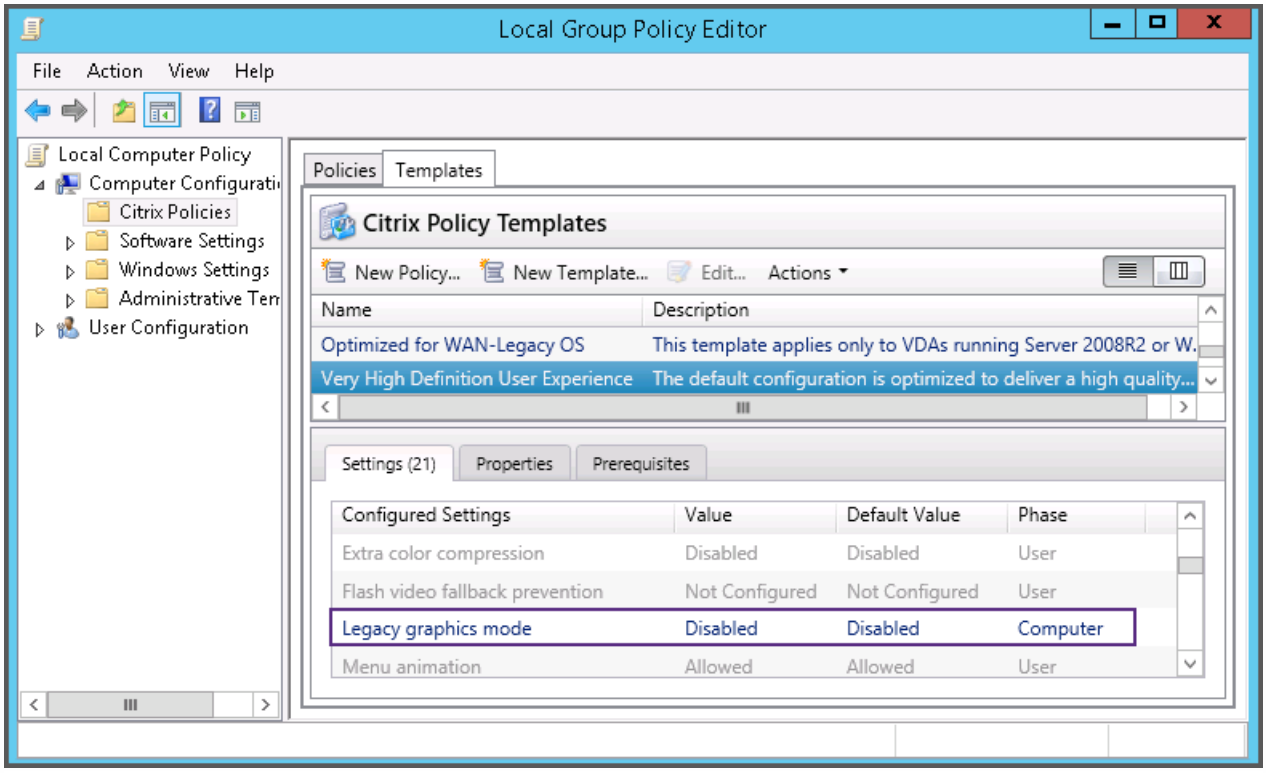
Puede limitar la búsqueda mediante la selección de una versión específica del producto o seleccionando una categoría. Para realizar una búsqueda sin filtro, seleccione Todas las configuraciones.

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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Plantillas de directiva

Dec 05, 2017

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.

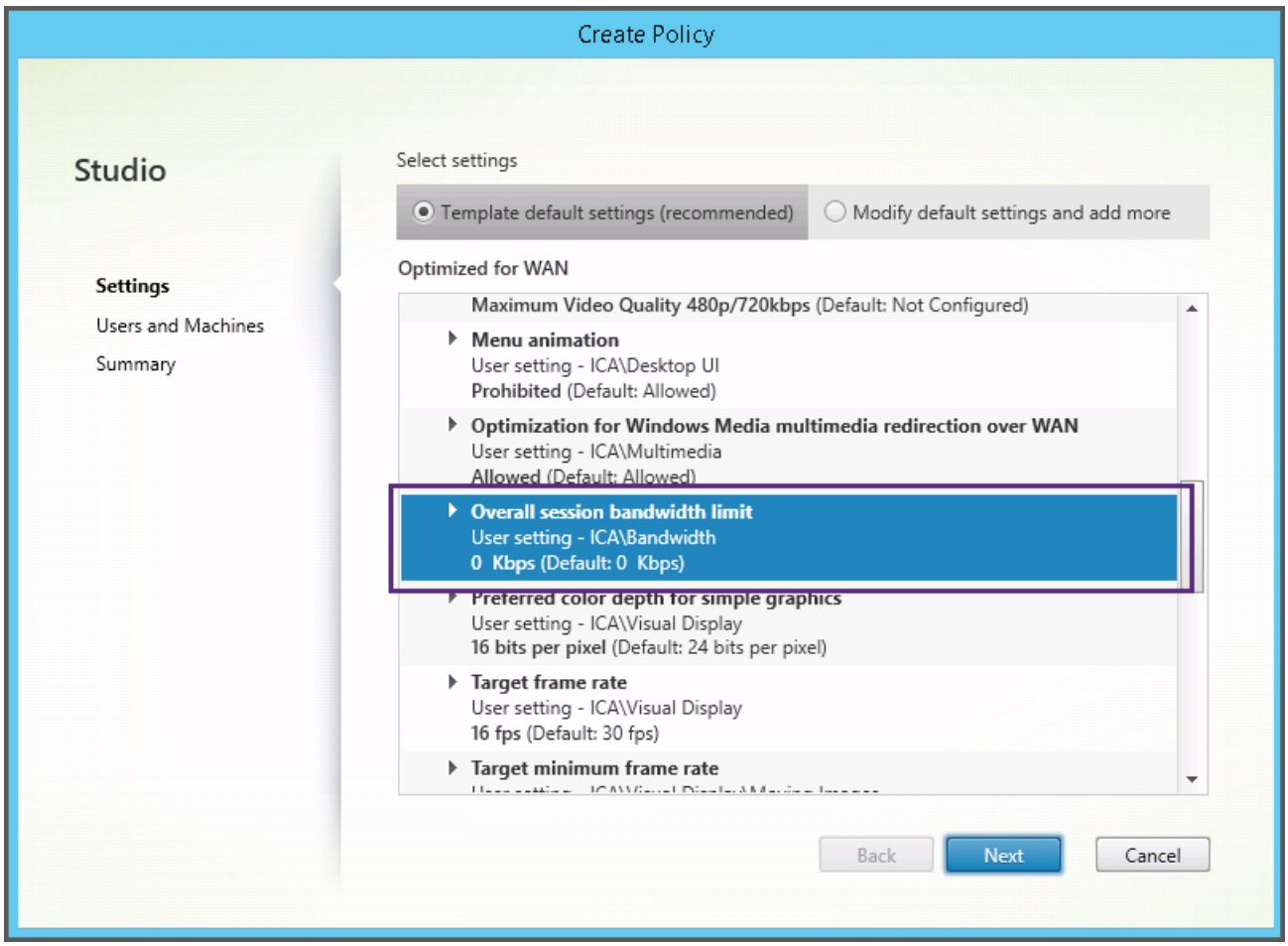
Plantillas integradas de Citrix

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 remotas 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



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.

Cómo 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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:

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.

Creación y administración de 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 nueva 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.
Ver la configuración de la plantilla	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en la ficha Configuraciones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tarea	Instrucción
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación de directivas

Dec 05, 2017

Antes de crear una directiva, decida a qué grupo de usuarios o dispositivos debe afectar. Puede crear una directiva según las funciones laborales del usuario, el tipo de conexión, el dispositivo de usuario o la ubicación geográfica. De forma alternativa, puede utilizar los mismos criterios que utiliza para las directivas de grupo de Active Directory de Windows.

Si ya creó una directiva aplicable a un grupo, considere la posibilidad de modificar dicha directiva para agregarle las configuraciones apropiadas, en lugar de crear otra directiva nueva. Evite la creación de una directiva nueva exclusivamente para habilitar una configuración específica o para excluir la aplicación de la directiva a determinados usuarios.

Al crear una nueva directiva, puede basarla en las configuraciones de una plantilla de directiva y personalizarlas según sea necesario, o puede crearla sin usar plantilla y agregar las configuraciones que necesite.

En Citrix Studio, las nuevas directivas creadas se establecen como inhabilitadas a menos que se marque explícitamente la casilla Habilitar directiva.

Configuraciones de directivas

Las configuraciones de directiva pueden habilitarse, inhabilitarse o se pueden dejar 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 sesión. Los cambios de configuraciones de directiva que afectan a usuarios surten efecto la próxima vez que el usuario inicia sesión. Si 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 las agrega a una directiva. Puede limitar la configuración de un determinado parámetro si selecciona Usar el valor predeterminado; esta opción impide configurar el parámetro y permite usar solo el valor predeterminado al aplicar la configuración de directiva, independientemente del valor que se hubiera introducido antes de seleccionar Usar el valor predeterminado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recomendaciones:

- Asigne las directivas a grupos, no a usuarios individuales. Si asigna directivas a grupos, 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 de seguridad de punto final o de la directiva de sesión que se va a usar.
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.
Dirección IP del cliente	Dirección IP del dispositivo de 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	Unidad organizativa.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre de asignación	Aplica una directiva según
organizativa (UO)	
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, 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- La asignación C es una asignación de usuario que especifica el grupo Ventas con el modo Permitir
- La asignación D es una asignación de dirección IP del cliente que especifica 10.8.169.* (la red de la empresa) con el modo Permitir

Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, se aplica la directiva, ya que la conexión satisface ambas asignaciones.

La directiva 3 incluye las siguientes asignaciones:

- La asignación E es una asignación de usuario que especifica el grupo Ventas con el modo Permitir
- La asignación F es una asignación de control de acceso que especifica condiciones de conexión de NetScaler Gateway con el modo Permitir

Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, no se aplica la directiva, ya que la conexión no satisface la asignación F.

Creación de una nueva 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. Para ello, dispone 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, pero 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.

Creación de una nueva 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, pero 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

Creación y administración de directivas con el Editor de directivas de grupo

En el Editor de directivas de grupo, expanda Configuración del equipo o Configuración de usuario. Expanda el nodo Directivas y seleccione Directivas de Citrix. Elija la acción adecuada.

Tarea	Instrucción
Crear una nueva 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 nueva directiva a partir de una plantilla existente	En la ficha Plantillas, seleccione la plantilla y, a continuación, haga clic en Nueva directiva.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Comparación, prioridad, modelado y solución de problemas de directivas

Dec 05, 2017

Puede utilizar varias directivas para personalizar el entorno y responder a las necesidades de los usuarios según su función laboral, su ubicación geográfica o su tipo de conexión. Por ejemplo, es posible que, por motivos de seguridad, deba establecer restricciones en los grupos de usuarios que trabajan regularmente con datos confidenciales. Puede crear una directiva para evitar que los usuarios guarden archivos con información confidencial en sus unidades de cliente locales. No obstante, si algunos de los miembros del grupo de usuarios necesitan acceder a las unidades locales, puede crear otra directiva para permitirles el acceso a esos usuarios en particular. A continuación, puede clasificar y dar prioridad a las dos directivas para establecer cuál de ellas tiene preferencia.

Cuando se utilizan varias directivas, debe determinar cuál es su prioridad, cómo crear las excepciones y cómo ver la directiva vigente cuando hay un conflicto de directivas.

En general, las directivas anulan configuraciones similares definidas para todo el sitio, para Delivery Controllers específicos o en el dispositivo del usuario. La excepción a este principio es la seguridad. La configuración de cifrado más exigente en su entorno, incluidos el sistema operativo y la configuración de remedo más restrictiva, siempre anulan otras configuraciones y directivas.

Las directivas de Citrix interactúan con directivas configuradas en su sistema operativo. En un entorno de Citrix, los parámetros de Citrix sobrescriben los parámetros similares configurados en una directiva de Active Directory o mediante Configuración de host de sesión de Escritorio remoto. Esto incluye las configuraciones relacionadas con la configuración típica de conexión del cliente del Protocolo de escritorio remoto (RDP), como Tapiz del escritorio, Animación de 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.

Comparación de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Para ver todas las configuraciones, seleccione Mostrar todas las configuraciones. Para volver a la vista predeterminada, seleccione Mostrar configuraciones en común.

Prioridad de las directivas

La asignación de prioridades en las directivas permite definir la prioridad de las directivas cuando contienen configuraciones conflictivas. Cuando un usuario inicia sesión, se identifican todas las directivas que coinciden con las asignaciones para la conexión. Las directivas se ordenan por prioridad y se comparan varias instancias de cualquier configuración. Cada configuración se aplica según la clasificación de prioridades de la directiva.

Usted asigna la prioridad de las directivas asignándoles diferentes números de prioridad en Studio. De forma predeterminada, las nuevas directivas tienen la prioridad más baja. Si hay conflictos en la configuración de las directivas, las directivas de mayor prioridad (el número de prioridad 1 es el máximo) anulan las de menor prioridad. Las configuraciones se combinan según su prioridad y su condición (por ejemplo, si la configuración está habilitada o inhabilitada). Una configuración inhabilitada anula otra configuración de menor prioridad que esté habilitada. Las configuraciones de directiva que no estén configuradas se omiten y no anulan ninguna configuración de menor prioridad.

1. Seleccione Directivas en el panel de navegación de Studio. Compruebe 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.

Determinación de las directivas que se aplican a una conexión

En ocasiones, una conexión no responde según lo previsto debido a que se aplican varias directivas. Si se aplica una directiva de mayor prioridad a una conexión, esta puede anular la configuración definida en la directiva original. Es posible determinar cómo se combinan las configuraciones de directiva finales para una conexión mediante el cálculo del Conjunto resultante de directivas o RSOP (Resultant Set of Policies).

El Conjunto resultante de directivas se puede calcular de diversas maneras:

- Con la ayuda del 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

calcula el conjunto resultante de directivas utilizando 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 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.

Uso del Asistente de modelado de directivas de grupo Citrix

Abra el Asistente de modelado de directivas de grupo Citrix mediante uno de los procedimientos siguientes:
- Seleccione Directivas en el panel de navegación de Studio, seleccione la ficha Modelado y, a continuación, seleccione Iniciar asistente de modelado en el panel Acciones.
- Abra la Consola de administración de directivas de grupo (gpmc.msc), haga clic con el botón secundario en el nodo Modelado de Directivas de grupo Citrix del panel del árbol y seleccione Asistente de modelado de Directivas de grupo Citrix.

Siga las instrucciones del asistente para seleccionar el controlador de dominio, los usuarios, los equipos, los parámetros del entorno y los criterios de asignación de Citrix que quiera 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.

Solución de 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 según lo previsto. 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 aplica ninguna directiva 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 quiere aplicar configuraciones de directiva a las conexiones que cumplen un criterio determinado, debe comprobar lo siguiente:
- Las directivas que quiere aplicar a esas conexiones están habilitadas.
- Las directivas que quiere aplicar tienen definidas las configuraciones adecuadas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetros predeterminados de directivas

Dec 05, 2017

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
Redirección del portapapeles del cliente	Permitida	Todas las versiones de VDA
Inicios de escritorio	Prohibida	VDA para SO de servidor, desde la versión 7 hasta la actual
EDT	Apagado	VDA 7.13 Consulte Transporte adaptable.
Tiempo de espera de la conexión de escucha ICA	120 000 milésimas de segundo	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

ICA/Entrega de Adobe Flash/Redirección de Flash

Nombre	Configuración predeterminada	VDA
Impedimento para recurrir al vídeo Flash	No configurada	Desde VDA 7.6 FP3 hasta la actual
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	Permitida	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	Permitida	Todas las versiones de VDA
Redirección de micrófonos del cliente	Permitida	Todas las versiones de VDA

ICA/Reconexión automática de clientes

Nombre	Configuración predeterminada	VDA
Reconexión automática de clientes	Permitida	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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

© 1999-2017 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/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

Nombre	Configuración predeterminada	VDA
Redirección de composición del escritorio	Inhabilitada (desde 7.6 FP3 hasta la actual) Habilitada (desde 5.6 hasta 7.6 FP2)	VDA 5.6, VDA para SO de escritorio desde la versión 7 hasta la actual
Calidad de gráficos de composición del escritorio	Medio	VDA 5.6, VDA para SO de escritorio desde la versión 7 hasta la actual
Tapiz del escritorio	Permitida	Todas las versiones de VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Animación de menús	Permitida	Todas las versiones de VDA
Ver contenido de las ventanas al arrastrar	Permitida	Todas las versiones de VDA

ICA/ Supervisión de usuario final

Nombre	Configuración predeterminada	VDA
Cálculo del tiempo de retorno ICA	Habilitado	Todas las versiones de VDA
Intervalo de cálculo del tiempo de retorno ICA	15 segundos	Todas las versiones de VDA
Cálculo del tiempo de retorno ICA para conexiones inactivas	Inhabilitado	Todas las versiones de VDA

ICA/Enhanced Desktop Experience

Nombre	Configuración predeterminada	VDA
Enhanced Desktop Experience	Permitida	VDA para SO de servidor, desde la versión 7 hasta la actual

ICA/Redirección de archivos

Nombre	Configuración predeterminada	VDA
Conectar automáticamente las unidades del cliente	Permitida	Todas las versiones de VDA
Redirección de unidades del cliente	Permitida	Todas las versiones de VDA
Unidades fijas del cliente	Permitida	Todas las versiones de VDA
Unidades de disco flexible del cliente	Permitida	Todas las versiones de VDA
Unidades de red del cliente	Permitida	Todas las versiones de VDA
Unidades ópticas del cliente	Permitida	Todas las versiones de VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Unidades extraíbles del cliente	Permitida	Todas las versiones de VDA
Redirección del host al cliente	Inhabilitado	VDA para SO de servidor, desde la versión 7 hasta la actual
Conservar las letras de unidad del cliente	Inhabilitado	VDA 5, 5.5, 5.6 FP1, VDA para SO de escritorio, desde la versión 7 hasta la actual
Acceso de lectura solamente a unidades del cliente	Inhabilitado	VDA 5.5, 5.6 FP1, VDA para SO 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	Permitida	Solo implementaciones de Interfaz Web; VDA para SO de servidor, desde la versión 7 hasta la versión actual
Usar escrituras asíncronas	Inhabilitado	Todas las versiones de VDA

ICA/Gráficos

Nombre	Configuración predeterminada	VDA
Permitir compresión sin pérdida visual	Inhabilitado	Desde VDA 7.6 hasta la actual
Límite de memoria de presentación	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	Habilitado	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	Habilitado	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	Inhabilitado	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		hasta la actual
Profundidad de color máxima permitida	32 bits por píxel	Todas las versiones de VDA
Notificar al usuario cuando se degrada la presentación	Inhabilitado	VDA para SO de servidor, desde la versión 7 hasta la actual
Cola y descarte	Habilitado	Todas las versiones de VDA
Usar códec de vídeo para compresión	Usar códec de vídeo si se prefiere	Desde VDA 7.6 FP3 hasta la actual
Usar codificación por hardware para códec de vídeo	Habilitado	Desde VDA 7.11 hasta la actual

ICA/Gráficos/Almacenamiento en caché

Nombre	Configuración predeterminada	VDA
Umbral de caché persistente	3 000 000 bps	VDA para SO de servidor, desde la versión 7 hasta la actual

ICA/Gráficos/Framehawk

Nombre	Configuración predeterminada	VDA
Canal de presentación Framehawk	Inhabilitado	Desde VDA 7.6 FP2 hasta la actual
Intervalo de puertos del canal de presentación Framehawk	3224, 3324	Desde VDA 7.6 FP2 hasta la actual

ICA/Keep Alive

Nombre	Configuración predeterminada	VDA
Tiempo de espera de ICA Keep Alive	60 segundos	Todas las versiones de VDA
ICA Keep Alive	No enviar mensajes de ICA Keep Alive	Todas las versiones de VDA

ICA/Acceso a aplicaciones locales

© 1999-2017 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	Permitida	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.
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 configurada	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	Permitida	Todas las versiones de VDA
Optimización de la redirección de medios de Windows Media	Permitida	VDA para SO de servidor,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sobre WAN		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 configurada	Desde VDA 7.6 FP3 hasta la actual
Obtención de contenido de Windows Media en el lado del cliente	Permitida	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 Windows Media	Permitida	Todas las versiones de VDA
Tamaño del búfer para la redirección de Windows Media	5 segundos	VDA 5, 5.5, 5.6 Feature Pack 1
Uso del tamaño de búfer para redirección de Windows Media	Inhabilitado	VDA 5, 5.5, 5.6 Feature Pack 1

ICA/Conexiones de multisecuencia

Nombre	Configuración predeterminada	VDA
Audio por UDP	Permitida	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 de 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	Inhabilitado	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
multisecuencia Configuración de usuario para multisecuencia	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Conectar automáticamente puertos LPT del cliente	Inhabilitado	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Redirección de puertos COM del cliente	Prohibida	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.
Redirección de puertos LPT del cliente	Prohibida	Todas las versiones de VDA; para las versiones desde VDA 7.0 hasta la versión 7.8, configure este parámetro mediante el Registro.

ICA/Impresión

Nombre	Configuración predeterminada	VDA
Redirección de impresoras del cliente	Permitida	Todas las versiones de VDA
Impresora predeterminada	Definir la impresora principal del cliente como la impresora predeterminada	Todas las versiones de VDA
Asignaciones de impresoras	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	Inhabilitado	Todas las

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
(escritorio)		versiones de VDA

ICA/Impresión/Impresoras del cliente

Nombre	Configuración predeterminada	VDA
Crear automáticamente las impresoras del cliente	Crear automáticamente todas las impresoras cliente	Todas las versiones de VDA
Crear automáticamente una impresora universal genérica	Inhabilitado	Todas las versiones de VDA
Nombres de impresora del cliente	Nombres de impresora estándar	Todas las versiones de VDA
Conexiones directas con servidores de impresión	Habilitado	Todas las versiones de VDA
Asignación y compatibilidad de controladores de impresora	No se especifica ninguna regla	Todas las versiones de VDA
Retención de las propiedades de impresora	Mantener en el perfil del usuario si no se guardan en el cliente	Todas las versiones de VDA
Impresoras del cliente retenidas o restauradas	Permitida	VDA 5, 5,5, 5.6 FP1

ICA/Impresión/Controladores

Nombre	Configuración predeterminada	VDA
Instalación automática de controladores de impresora	Habilitado	Todas las versiones de VDA
Preferencia de controlador universal	EMF; XPS; PCL5c; PCL4; PS	Todas las versiones de VDA
Uso de controladores de impresión universal	Usar impresión universal solo si el controlador solicitado no está disponible	Todas las versiones de VDA

ICA/Impresión/Universal Print Server

Nombre	Configuración predeterminada	VDA
Habilitar Universal Print Server	Inhabilitado	Todas las versiones de VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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 = False Almacenamiento en caché de imágenes y fuentes • Permitir el almacenamiento en caché de imágenes incrustadas = True • Permitir el almacenamiento en caché de fuentes incrustadas = True	Todas las versiones de VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
	Permitir a los no administradores modificar estos parámetros = False	
Preferencia de vista previa en impresión universal	No usar vista previa en las impresoras de creación automática o universales genéricas	Todas las versiones de VDA
Límite de calidad de la impresión universal	Sin límite	Todas las versiones de VDA

ICA/Seguridad

Nombre	Configuración predeterminada	VDA
Nivel de cifrado mínimo de SecureICA	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	Inhabilitado	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	Inhabilitado	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

© 1999-2017 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	Permitida	Todas las versiones de VDA
Número de puerto para fiabilidad de la sesión	2598	Todas las versiones de VDA
Tiempo de espera de fiabilidad de la sesión	180 segundos	Todas las versiones de VDA

ICA/Control de zona horaria

Nombre	Configuración predeterminada	VDA
Calcular hora local para clientes antiguos	Habilitado	VDA para SO 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

Nombre	Configuración predeterminada	VDA
Redirección de dispositivos TWAIN del cliente	Permitida	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	Habilitada (desde VDA 7.6 FP3 hasta la actual) Inhabilitada (desde VDA 7.11 hasta la actual) De forma predeterminada, no se	Desde VDA 7.6 FP3 hasta la actual

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	especifica ninguna regla.	
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	Permitida	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

Nombre	Configuración predeterminada	VDA
Preferencia de profundidad de color para gráficos sencillos	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	Habilitado	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	Ninguno	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

© 1999-2017 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	Inhabilitado	Todas las versiones de VDA
Umbral de compresión de color adicional	8192 Kbps	Todas las versiones de VDA
Compresión intensa	Inhabilitado	Todas las versiones de VDA
Nivel de compresión con pérdida	Medio	Todas las versiones de VDA
Valor de umbral de compresión con pérdida	2 147 483 647 Kbps	Todas las versiones de VDA

ICA/WebSockets

Nombre	Configuración predeterminada	VDA
Conexiones con WebSockets	Prohibida	VDA para SO de servidor, desde la versión 7 hasta la actual, VDA para SO de escritorio, desde la versión 7 hasta la actual
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	Inhabilitado	VDA para SO de servidor, desde la versión 7 hasta la actual
Prioridad de procesos excluidos para el	Por debajo de lo normal o	VDA para SO de servidor, desde la versión 7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
uso de CPU	baja	hasta la actual
Uso del disco	Inhabilitado	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	Inhabilitado	VDA para SO de servidor, desde la versión 7 hasta la actual
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	Inhabilitado	Todas las versiones de VDA
Cerrar la sesión del usuario si hay algún problema	Inhabilitado	Todas las versiones de VDA
Reintentos de acceso a archivos bloqueados	5	Todas las versiones de VDA
Procesar cookies de Internet al cerrar la sesión	Inhabilitado	Todas las versiones de VDA

Profile Management/ Parámetros básicos

Nombre	Configuración predeterminada	VDA
Reescritura activa	Inhabilitado	Todas las versiones de VDA
Habilitar Profile Management	Inhabilitado	Todas las versiones de VDA
Grupos excluidos	Inhabilitada Se procesan los miembros de todos los grupos de usuarios.	Todas las versiones de VDA
Respaldo para perfiles sin conexión	Inhabilitado	Todas las versiones de VDA
Ruta al almacén de usuarios	Windows	Todas las versiones de VDA
Procesar inicios de sesión de administradores locales	Inhabilitado	Todas las versiones de VDA

© 1999-2017 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	Inhabilitado	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	Inhabilitado	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

Profile Management/ Sistema de archivos/Sincronización

Nombre	Configuración predeterminada	VDA
Directorios para sincronizar	Inhabilitada Solo se sincronizan las carpetas no excluidas.	Todas las versiones de VDA
Archivos para sincronizar	Inhabilitada Solo se sincronizan los archivos no excluidos.	Todas las versiones de VDA
Carpetas para 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	Inhabilitado	Todas las versiones de VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Incluir nombre de dominio	Inhabilitado	Todas las versiones de VDA

Profile Management/ Redirección de carpetas/AppData(Roaming)

Nombre	Configuración predeterminada	VDA
Ruta de AppData(Roaming)	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

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

© 1999-2017 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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

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

Nombre	Configuración predeterminada	VDA
Acciones de Active Directory	Inhabilitado	Todas las versiones de VDA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Información común	Inhabilitado	Todas las versiones de VDA
Advertencias comunes	Inhabilitado	Todas las versiones de VDA
Habilitar registro	Inhabilitado	Todas las versiones de VDA
Acciones del sistema de archivos	Inhabilitado	Todas las versiones de VDA
Notificaciones del sistema de archivos	Inhabilitado	Todas las versiones de VDA
Cierre de sesión	Inhabilitado	Todas las versiones de VDA
Índice	Inhabilitado	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	Inhabilitado	Todas las versiones de VDA
Valores de directivas al iniciar y cerrar la sesión	Inhabilitado	Todas las versiones de VDA
Acciones del Registro del sistema	Inhabilitado	Todas las versiones de VDA
Diferencias en el Registro del sistema al cerrar sesión	Inhabilitado	Todas las versiones de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA VDA

Management/ Profile Management/Gestión de perfiles

Nombre	Configuración predeterminada	VDA
Demora antes de eliminar perfiles en caché	0	Todas las versiones de VDA
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitado	Todas las versiones de VDA
Gestión de conflictos de perfiles locales	Usar el perfil local	Todas las versiones de VDA
Migración de perfiles existentes	Locales y móviles	Todas las versiones de VDA
Ruta al perfil de plantilla	Inhabilitada Los perfiles de usuario nuevos se crean a partir del perfil de usuario predeterminado ubicado en el equipo donde el usuario inicia sesión por primera vez.	Todas las versiones de VDA
El perfil de plantilla anula el perfil local	Inhabilitado	Todas las versiones de VDA
El perfil de plantilla sobrescribe el perfil móvil	Inhabilitado	Todas las versiones de VDA
Perfil de plantilla utilizado como perfil de Citrix obligatorio para todos los inicios de sesión .	Inhabilitado	Todas las versiones de VDA

Profile Management/ Registro del sistema

Nombre	Configuración predeterminada	VDA
Lista de exclusión	Inhabilitada Todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra 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 sesión.	Todas las versiones de VDA

Profile Management/ Perfiles de usuario de streaming

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Guardar siempre en caché	Inhabilitado	Todas las versiones de VDA
Tamaño de caché	0 Mb	Todas las versiones de VDA
Streaming de perfiles	Inhabilitado	Todas las versiones de VDA
Grupos de perfiles de usuarios de streaming	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
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nombre	Configuración predeterminada	VDA
Habilitar actualización automática de Controller	Habilitado	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	Inhabilitado	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	Habilitado	VDA 5.5, 5.6 Feature Pack 1
Parámetros de calidad de HDX 3D Pro		VDA 5.5, 5.6 Feature Pack 1

Virtual Delivery Agent/Monitoring

Nombre	Configuración predeterminada	VDA
Habilitar supervisión de procesos	Inhabilitado	Desde VDA 7.11 hasta la actual
Habilitar supervisión de recursos	Habilitado	Desde VDA 7.11 hasta la actual

IP virtual

Nombre	Configuración predeterminada	VDA
Respaldo para bucle invertido de IP virtual	Inhabilitado	Desde VDA 7.6 hasta la actual
Lista de programas para bucle invertido de IP virtual	Ninguno	Desde VDA 7.6 hasta la actual

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Referencia para configuraciones de directivas

Dec 05, 2017

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.

Sonido

Para esta tarea	Use este parámetro 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aceleración multimedia HDX MediaStream	Límite de ancho de banda de aceleración multimedia HDX MediaStream; o Porcentaje límite de ancho de banda de aceleración multimedia HDX MediaStream
Sesión del cliente	Límite de ancho de banda global de la sesión
Impresión	Límite de ancho de banda de redirección de impresoras; o Porcentaje límite de ancho de banda de redirección de impresoras
Dispositivos TWAIN (como cámaras o escáneres)	Límite de ancho de banda de redirección de dispositivos TWAIN; o Porcentaje límite de ancho de banda de redirección de dispositivos TWAIN
Dispositivos USB	Límite de ancho de banda de redirección de dispositivos USB del cliente; o Porcentaje límite de ancho de banda de redirección de dispositivos USB del cliente

Redirección de dispositivos del cliente y dispositivos del usuario

Para esta tarea	**Use esta configuración de directiva**
Controlar si se conectan las unidades del dispositivo del usuario cuando los usuarios inician sesión en el servidor	Conectar automáticamente las unidades del cliente
Controlar la transferencia de datos mediante cortar y pegar entre el servidor y el portapapeles local	Redirección del portapapeles del cliente
Controlar la forma en que se deben asignar las unidades del dispositivo del usuario	Redirección de unidades del cliente
Controlar si los discos duros local de los usuarios están disponibles en una sesión	Unidades fijas del cliente y Redirección de unidades del cliente
Controlar si las unidades de disco flexible locales de los	Unidades de disco flexible del cliente y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

usuarios están disponibles en una sesión	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 de disco óptico 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 Nivel de compresión TWAIN
Controlar si los dispositivos USB están disponibles en una sesión	Redirección de dispositivos USB del cliente, y Reglas de redirección de dispositivos USB del cliente
Mejorar la velocidad de escritura y copia de archivos en los discos del cliente en redes WAN	Usar escrituras asíncronas

Redirección de contenido

Para esta tarea	**Use esta configuración de directiva**
Controlar si se utiliza la redirección de contenido desde el servidor al dispositivo del usuario	Redirección del host al cliente

Interfaz de usuario de escritorio

Para esta tarea	**Use esta configuración de directiva**
Controlar si se usa el papel tapiz del escritorio en las sesiones de los usuarios	Tapiz del escritorio
Ver el contenido de las ventanas al arrastrarlas	Ver contenido de las ventanas al arrastrar

Gráficos y multimedia

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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 directiva de 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 de puertos múltiples
Habilitar el respaldo para conexiones de multisecuencia entre servidores y dispositivos de usuario	Multisecuencia (configuración de equipo y usuario)

Impresión

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Controlar la ubicación donde se guardan las propiedades de la impresora	Retención de las propiedades de impresora
Controlar si las solicitudes de impresión se procesan en el cliente o en el servidor	Conexiones directas con servidores de impresión
Controlar si los usuarios pueden acceder a las impresoras conectadas a sus dispositivos	Redirección de impresoras del cliente
Controlar la instalación de controladores nativos de Windows al crear automáticamente impresoras de cliente y de red	Instalación automática de controladores de impresora
Decidir cuándo utilizar el controlador de impresora universal	Uso de controladores de impresión universal
Elegir una impresora en función de la información de sesión de un usuario 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 un escritorio o una sesión de aplicación. Para los usuarios que necesiten salvapantallas, estos se pueden implementar en el dispositivo del usuario.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de ICA

Dec 05, 2017

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, la funcionalidad Enlightened Data Transport está **desactivada** y se usa siempre TCP.

1. En Studio, habilite la configuración de directiva "HDX Adaptative Transport" (inhabilitada de forma predeterminada). 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**.

    Preferido. Se utiliza el transporte adaptable por EDT cuando sea posible; cuando no lo sea, se recurre a TCP.

    Modo de diagnóstico. Se obliga el uso de EDT y la opción de recurrir a TCP está inhabilitada. Esta configuración se recomienda solamente para la solución de problemas.

    Desactivado. Se obliga el uso de TCP y EDT está inhabilitado.

Para obtener más información, consulte Transporte adaptable.

Tiempo de espera de inicio de la aplicación

Esta configuración especifica el tiempo (en milisegundos) que una sesión debe esperar para que se inicie la primera aplicación. Si el inicio de la aplicación supera este período de tiempo, la sesión se termina.

Puede elegir el tiempo predeterminado (10 000 milisegundos) o puede especificar una cantidad de tiempo en milisegundos.

Redirección del portapapeles del cliente

Esta configuración permite o impide la asignación del portapapeles del dispositivo del usuario al portapapeles del servidor.

La redirección del portapapeles está permitida de forma predeterminada.

Para impedir la transferencia entre una sesión y el portapapeles local de datos que se hayan cortado y pegado, seleccione Prohibida. Los usuarios podrán seguir copiando y pegando datos entre las aplicaciones ejecutadas en sesiones.

Una vez habilitada esta configuración, defina el ancho de banda máximo permitido que puede consumir el portapapeles en una conexión de cliente mediante las configuraciones 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 la configuración Restringir escritura en el portapapeles del cliente está habilitada, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Los siguientes formatos personalizados están predefinidos en XenApp y XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- Formato HTML

El formato HTML está inhabilitado de forma predeterminada. Para habilitar esta funcionalidad:

- Compruebe que la opción **Redirección del portapapeles del cliente** está permitida.
- Compruebe que la opción **Restringir escritura en el portapapeles del cliente** está habilitada.
- Agregue una entrada para el **formato HTML** (y otros formatos que quiera admitir) en la opción **Formatos permitidos de escritura en el portapapeles del cliente**.

Nota: Si se permite copiar contenido en formato HTML al portapapeles (en otras palabras, si se habilita el formato HTML), se copian los scripts (si los hay) 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.

Se pueden agregar más formatos personalizados. El nombre del formato personalizado debe coincidir con los formatos para registrar con el sistema. Los nombres de formato distinguen entre mayúsculas y minúsculas.

Esta configuración no se aplicará si Redirección del portapapeles del cliente o Restringir escritura en el portapapeles del cliente están configuradas como "Prohibidas".

Inicios de escritorio

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 65535, 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 Citrix Receiver o plugin que se conecte con ese servidor.

Inicio de 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.

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.

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 la configuración Formatos permitidos de escritura en el

© 1999-2017 Citrix Systems, Inc. All rights reserved.

portapapeles de la sesión.

De forma predeterminada, esta configuración está prohibida.

Formatos permitidos de escritura en el portapapeles de la sesión

Cuando la configuración Restringir escritura en el portapapeles de la sesión está permitida, los datos de portapapeles del cliente no se pueden compartir con las aplicaciones de la sesión. Puede usar esta configuración para permitir que formatos específicos de datos se puedan compartir con el portapapeles de la sesión.

Los siguientes formatos de portapapeles están definidos por el sistema:

- CF_TEXT
- CF_BITMAP
- CF_METAFILEPICT
- CF_SYLK
- CF_DIF
- CF_TIFF
- CF_OEMTEXT
- CF_DIB
- CF_PALETTE
- CF_PENDATA
- CF_RIFF
- CF_WAVE
- CF_UNICODETEXT
- CF_ENHMETAFILE
- CF_HDROP
- CF_LOCALE
- CF_DIBV5
- CF_OWNERDISPLAY
- CF_DSPTEXT
- CF_DSPBITMAP
- CF_DSPMETAFILEPICT
- CF_DISPENHMETAFILE

Los siguientes formatos personalizados están predefinidos en XenApp y XenDesktop:

- CFX_RICHTEXT
- CFX_OfficeDrawingShape
- CFX_BIFF8
- Formato HTML

El formato HTML está inhabilitado de forma predeterminada. Para habilitar esta funcionalidad:

- Compruebe que la opción **Redirección del portapapeles del cliente** está permitida.
- Compruebe que la opción **Restringir escritura en el portapapeles de la sesión** está habilitada.
- Agregue una entrada para el **formato HTML** (y otros formatos que quiera admitir) en la opción **Formatos permitidos de escritura en el portapapeles de la sesión**.

Nota: Si se permite copiar contenido en formato HTML al portapapeles (en otras palabras, si se habilita el formato HTML), se copian los scripts (si los hay) del origen del contenido al destino. Antes de proceder a copiar contenido, compruebe el

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Se pueden 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Reconexión automática de clientes

Dec 05, 2017

La sección Reconexión automática de clientes contiene configuraciones de directiva 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, 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 Citrix Receiver que contiene la clave del ID de sesión y las credenciales, la reconexión automática puede derivar en el inicio de una nueva sesión. Es decir, se inicia una nueva sesión en vez de reconectarse a una sesión existente. La cookie no se utiliza si está caducada, por ejemplo, por retrasos en la reconexión o si las credenciales tienen que volver a introducirse. No hay reconexión automática de clientes si los usuarios se desconectan voluntariamente.

La ventana de la sesión se oscurece mientras tiene lugar una reconexión. Aparece un temporizador que muestra el tiempo restante antes de volver a conectarse a la sesión. Cuando se supera el tiempo de espera, la sesión se desconecta.

En las sesiones de aplicaciones, cuando la Reconexión automática está permitida, en el área de notificaciones aparece un temporizador que indica el tiempo restante antes de volver a conectarse a la sesión. Citrix Receiver intenta repetidamente reconectarse a la sesión hasta que lo logra o hasta que el usuario cancela los intentos de reconexión.

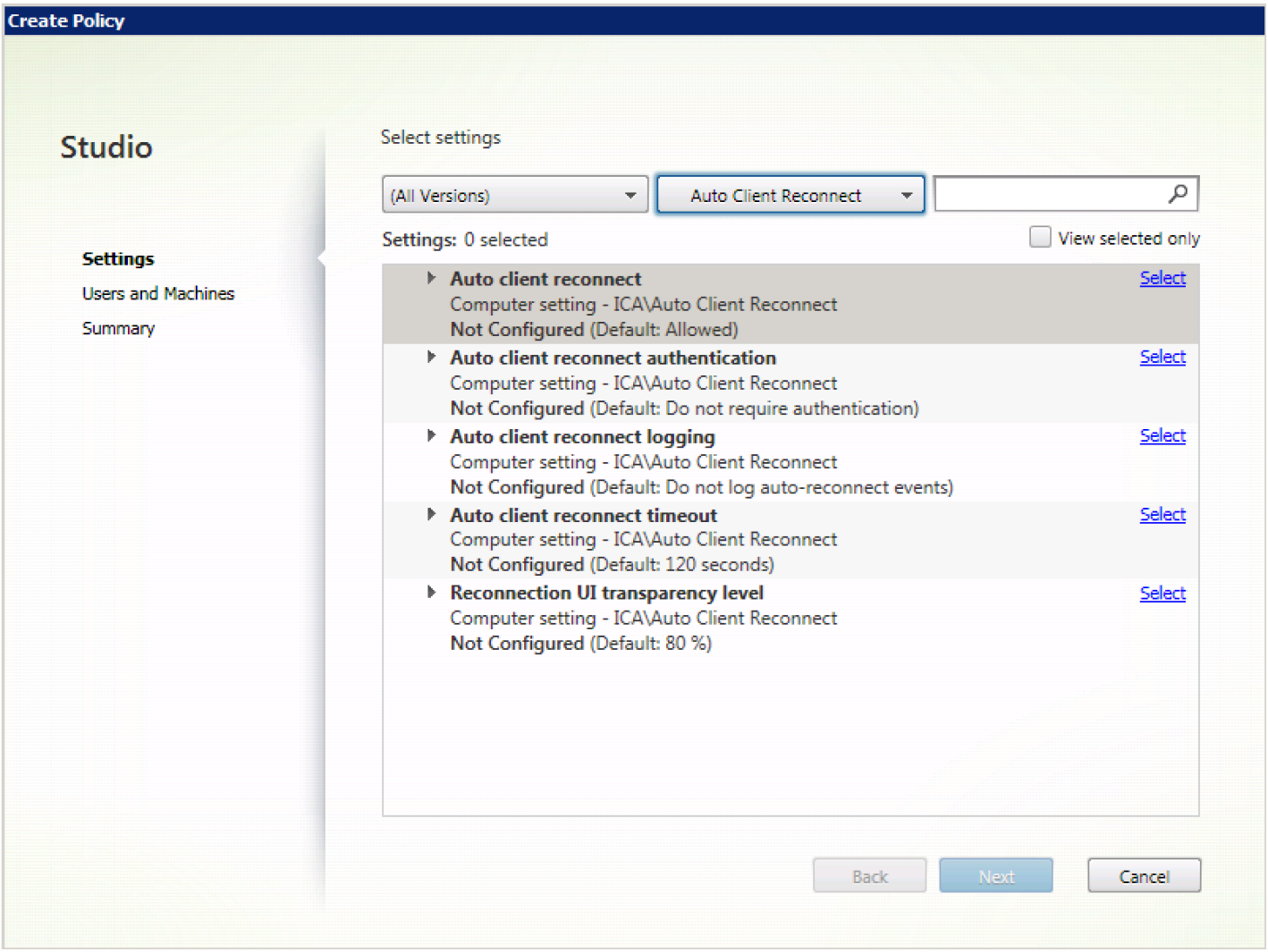
Para las sesiones de usuario, cuando la Reconexión automática está permitida, Citrix Receiver intenta volver a conectarse a la sesión durante un período de tiempo especificado, a menos que se produzca una reconexión o el usuario cancele el intento de reconexión. De forma predeterminada, este período 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 el valor **Prohibida**.

© 1999-2017 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 Citrix Receiver. Si se define este parámetro, no se usan las cookies. En su lugar, aparece un cuadro de diálogo que solicita que los usuarios introduzcan sus credenciales cuando Citrix Receiver 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. Haga clic en **Aceptar**.

Registro de reconexión automática de clientes

Esta configuración habilita o inhabilita el registro de las reconexiones automáticas de clientes en el registro de sucesos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Haga clic en **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. Haga clic en **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. Haga clic en **Aceptar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Sonido

Dec 05, 2017

La sección Sonido contiene las configuraciones de directiva 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

Este parámetro permite o impide la transmisión y la recepción de sonido entre VDA y el dispositivo del usuario a través de RTP mediante el protocolo UDP. Cuando esta configuración está inhabilitada, el sonido se envía y se recibe sobre TCP.

De forma predeterminada, el sonido sobre UDP está permitido.

Sonido Plug and Play

Este parámetro 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 (Voz sobre IP) o bien 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, lo que lo hace ideal para usarlo con programas softphone y aplicaciones de comunicaciones unificadas, cuando se necesita un procesamiento de medios en el lado del servidor.
  El sonido enviado al dispositivo del usuario se comprime hasta 64 Kbps. Esta compresión provoca un ligero descenso en la calidad del sonido que se reproduce en el dispositivo del usuario, pero la latencia es mucho menor y consume muy poco ancho de banda. Si la calidad de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

consumo de ancho de banda se duplica.

Para especificar el ancho de banda máximo, configure las directivas de 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

Este parámetro especifica si las aplicaciones alojadas en el servidor puede reproducir sonidos a través de 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 habilitado este parámetro, 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 consume 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 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 el parámetro Sonido Plug and Play está habilitado 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.

Redirección de micrófonos del cliente

Este parámetro habilita o inhabilita la redirección de micrófonos del cliente. Cuando está habilitado, 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 avisa 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 Citrix Receiver.

En las máquinas con SO de servidor Windows, compruebe también que el parámetro Sonido Plug and Play está habilitado para respaldar varios dispositivos de sonido.

Si se inhabilita el parámetro Redirección de sonido del cliente en el dispositivo del usuario, esta regla no tiene ningún efecto.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Ancho de banda

Dec 05, 2017

La sección Ancho de banda contiene configuraciones de directiva que pueden configurarse 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, compruebe que la configuración de directiva 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 y la grabación de sonido en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de sonido, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de sonido

Esta configuración permite especificar el límite máximo permitido de ancho de banda para la reproducción y la grabación de sonido, como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de sonido, se aplicará el más restrictivo (el de valor más bajo).

Si 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 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 define esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica

© 1999-2017 Citrix Systems, Inc. All rights reserved.

el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de redirección del portapapeles

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para la transferencia de datos entre una sesión y el portapapeles local.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección del portapapeles , se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección del portapapeles

Esta configuración permite especificar el valor máximo permitido de ancho de banda para la transferencia de datos entre una sesión y el portapapeles local como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección del portapapeles, se aplicará el más restrictivo (el de valor más bajo).

Si 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 puertos COM

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure este parámetro con el Registro; consulte Configurar la redirección de puertos COM y puertos LPT mediante el Registro.
Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a un puerto COM en una conexión de cliente. Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de puertos COM, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de puertos COM

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure este parámetro con el Registro; consulte Configurar la redirección de puertos COM y puertos LPT mediante el Registro.
Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a puertos COM en una conexión de cliente, como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de puertos COM, se aplicará el más restrictivo (el de valor más bajo).

Si define esta configuración, también debe definir la configuración Límite de ancho de banda global de la sesión, que indica el ancho de banda total disponible para las sesiones de cliente.

Límite de ancho de banda de redirección de archivos

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a una unidad del cliente en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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 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 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 puertos LPT

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure este parámetro con el Registro; consulte Configurar la redirección de puertos COM y puertos LPT mediante el Registro.
Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para trabajos de impresión mediante un puerto LPT en una sesión de usuario individual.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de puertos LPT, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de puertos LPT

Nota: Para los agentes Virtual Delivery Agent 7.0 a 7.8, configure este parámetro con el Registro; consulte Configurar la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (10 000 Kbps). De forma predeterminada, no se especifica ningún valor máximo (cero).

Al limitar el ancho de banda de las conexiones de cliente, se puede mejorar el rendimiento cuando otras aplicaciones fuera de la conexión de cliente compiten por un ancho de banda limitado.

Límite de ancho de banda de redirección de impresoras

Esta configuración permite especificar el valor máximo permitido de ancho de banda, en kilobits por segundo, para el acceso a impresoras del cliente en una sesión de usuario.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Porcentaje límite de ancho de banda de redirección de impresoras, se aplicará el más restrictivo (el de valor más bajo).

Porcentaje límite de ancho de banda de redirección de impresoras

Esta configuración permite especificar el valor máximo permitido de ancho de banda para el acceso a impresoras del cliente como porcentaje del ancho de banda total de la sesión.

De forma predeterminada, no se especifica ningún valor máximo (cero).

Si introduce un valor para esta configuración y otro para la configuración Límite de ancho de banda de redirección de impresoras, se aplicará el más restrictivo (el de valor más bajo).

Si 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva Redirección de contenido bidireccional

Dec 05, 2017

La sección Redirección de contenido bidireccional contiene configuraciones de directiva 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 Citrix Receiver.

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 XenApp o XenDesktop 7.13 o una versión posterior más Citrix Receiver para Windows 4.7 o una versión posterior.

Important

- 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 Registro de 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 se admite Citrix Receiver 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 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.

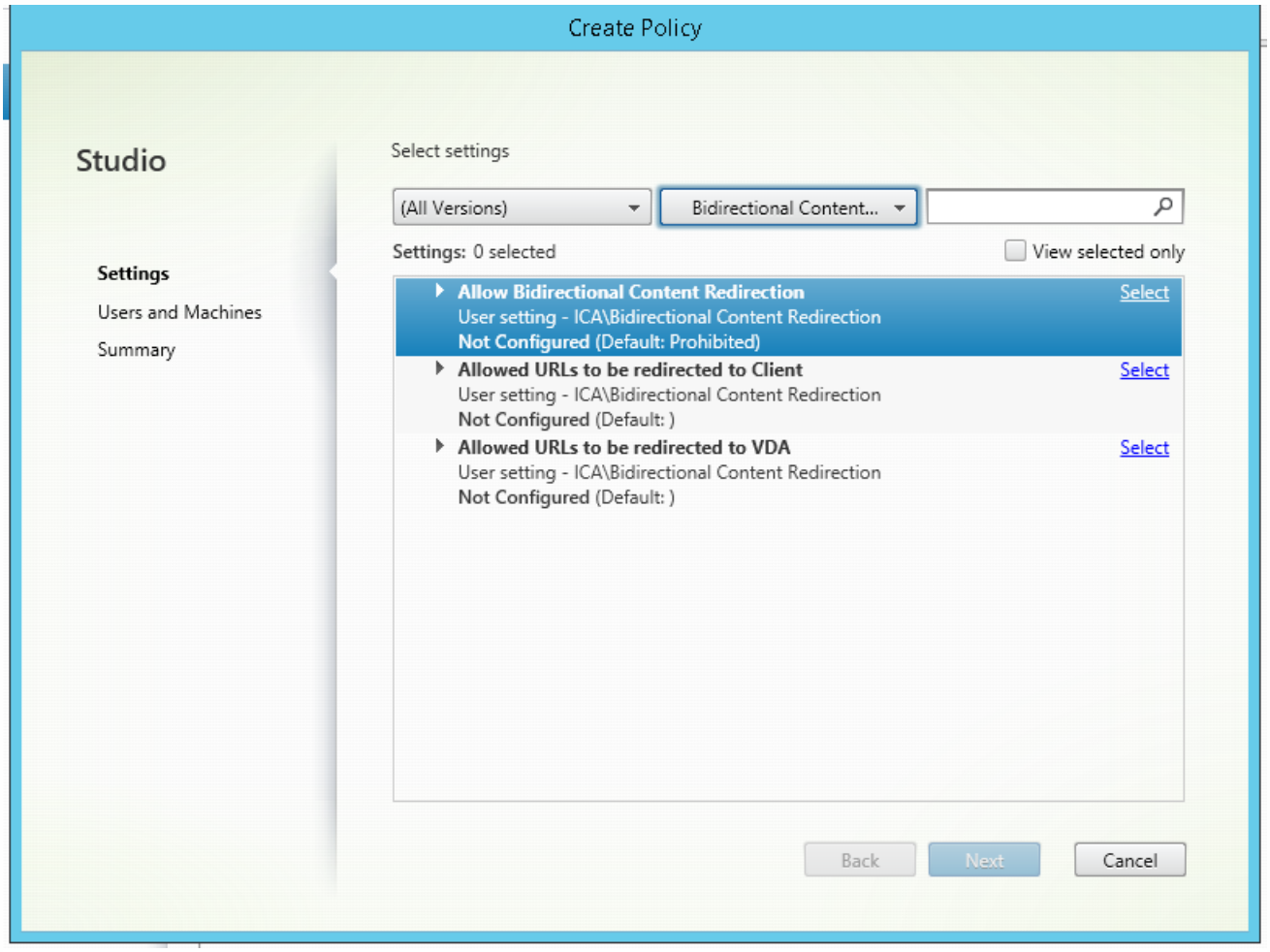
Para habilitar la redirección de contenido bidireccional

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



Redirección de cliente a host (VDA) y de cliente a cliente

Utilice la plantilla administrativa del objeto de directiva de grupo de Citrix Receiver para configurar la redirección de cliente a host (VDA) y de cliente a cliente (cliente).

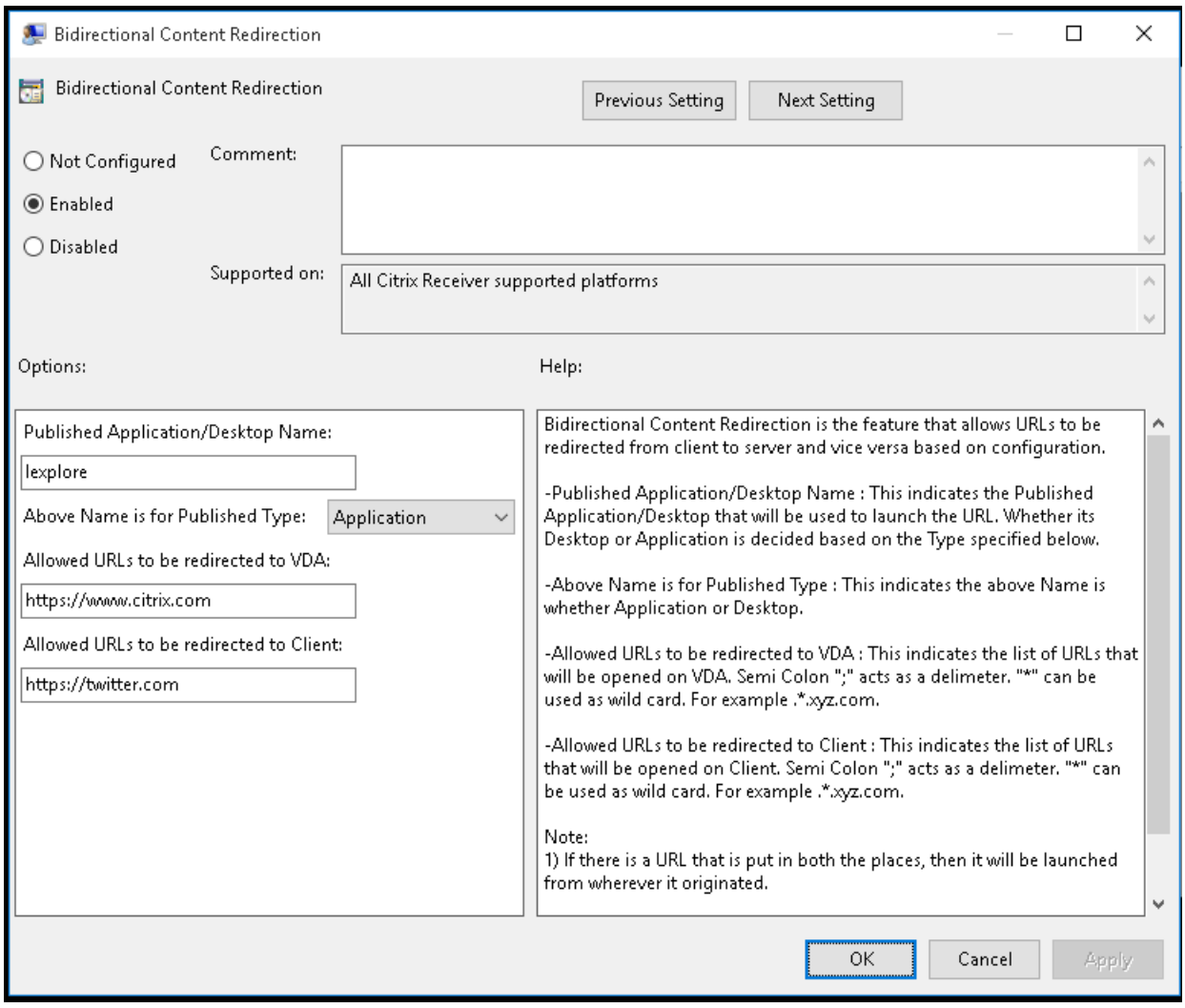
Para habilitar la redirección de contenido bidireccional

Al incluir direcciones URL, puede especificar una sola dirección URL o una lista de direcciones URL, delimitadas por punto y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

coma. Puede utilizar un asterisco (*) como comodín.

Para obtener más información, consulte Configuración de la redirección de contenido bidireccional en la documentación de Citrix Receiver.



Registro de 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

Por ejemplo, el siguiente comando registra un complemento de Internet Explorer en un dispositivo que ejecuta Citrix Receiver.

```
C:\Archivos de programa\Citrix\ICA Client\redirector.exe/regIE
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Sensores del cliente

Dec 05, 2017

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 Citrix Receiver 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.
  - Dar al usuario la opción de borrar la información de ubicación almacenada en caché por la aplicación. (Citrix Receiver no almacena en caché 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.
- Una conexión segura (por ejemplo, con TLS o una red VPN) es imprescindible para usar servicios de ubicación. Citrix Receiver se debe conectar a servidores de confianza solamente.
- Consulte la información legal referente al uso de servicios de ubicación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Interfaz de usuario de escritorio

Dec 05, 2017

La sección Interfaz de usuario de escritorio contiene configuraciones de directiva 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.

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.

Calidad gráfica de la redirección de composición del escritorio.

Esta configuración especifica la calidad de los gráficos utilizados para la redirección de composición del escritorio.

De forma predeterminada, esta opción se establece en 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.

La animación de menús es un parámetro 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 aparece al apuntar a dicha flecha.

La animación de menús se habilita en un escritorio si esta configuración de directiva se define como Permitida y el parámetro de preferencia personal de animación de menús de Microsoft está habilitado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: Los cambios en el parámetro de preferencia personal de animación de menús de Microsoft son cambios hechos en el escritorio. Esto significa que, 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 el parámetro de Microsoft en la imagen maestra del escritorio para garantizar que el escritorio conserva los cambios del usuario.

Ver contenido de las ventanas al arrastrar

Esta configuración permite o evita que se muestre el contenido de las ventanas al arrastrarlas por la pantalla.

La presentación del contenido de las ventanas está habilitada de forma predeterminada.

Si se establece en Permitida, parecerá que toda la ventana se mueve al arrastrarla. Si se establece en Prohibida, parecerá que solo los bordes se mueven hasta que se suelta la ventana.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Supervisión de usuario final

Dec 05, 2017

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de directiva de Enhanced Desktop Experience

Dec 05, 2017

Con la configuración de directiva de 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, asegúrese de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de archivos

Dec 05, 2017

La sección Redirección de archivos contiene configuraciones de directiva relacionadas con la asignación y la optimización de unidades del cliente.

Conectar automáticamente las unidades del cliente

Esta configuración permite o impide la conexión automática de unidades del cliente cuando los usuarios inician sesión.

La conexión automática está permitida de forma predeterminada.

Cuando agregue esta configuración a una directiva, debe habilitar también las configuraciones correspondientes a los tipos de unidades que quiera que se conecten automáticamente. Por ejemplo, para permitir la conexión automática de las unidades de CD-ROM de los usuarios, use esta configuración y la configuración Unidades ópticas del cliente.

Configuraciones de directiva relacionadas:
- Redirección de unidades del cliente
- Unidades de disco flexible del cliente
- Unidades ópticas del cliente
- Unidades fijas del cliente
- Unidades de red del cliente
- Unidades extraíbles del cliente

Redirección de unidades del cliente

Esta configuración habilita o inhabilita la redirección de archivos hacia el dispositivo del usuario y desde él.

De forma predeterminada, la redirección de archivos está habilitada.

Si está habilitada, los usuarios pueden guardar archivos en todas las unidades del cliente. Si está inhabilitada, se impide cualquier redirección de archivos, independientemente del estado de las configuraciones individuales de redirección de archivos, como Unidades de disco flexible del cliente y Unidades de red del cliente.

Configuraciones de directiva relacionadas:
- Unidades de disco flexible del cliente
- Unidades ópticas del cliente
- Unidades fijas del cliente
- Unidades de red del cliente
- Unidades extraíbles del cliente

Unidades fijas del cliente

Esta configuración permite o impide que los usuarios accedan a las unidades fijas del dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades fijas del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está

© 1999-2017 Citrix Systems, Inc. All rights reserved.

presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, las unidades fijas del cliente no se asignan y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades fijas del cliente.

Para 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 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 desde 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 que las unidades de red se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Unidades ópticas del cliente

Esta configuración permite o impide que los usuarios tengan acceso a las unidades de CD-ROM, DVD-ROM y BD-ROM en el dispositivo del usuario o guarden archivos en ellas.

De forma predeterminada, el acceso a las unidades ópticas del cliente está permitido.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida. Si esta configuración está inhabilitada, no se asignan las unidades ópticas del cliente y los usuarios no pueden acceder a ellas de forma manual, independientemente del estado de la configuración Unidades ópticas del cliente.

Para que las unidades ópticas se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Unidades extraíbles del cliente

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 que las unidades extraíbles se conecten automáticamente cuando los usuarios inician sesión, configure Conectar automáticamente las unidades del cliente.

Redirección del host al cliente

Esta configuración habilita o inhabilita las asociaciones de tipos de archivos para direcciones URL y contenido multimedia que se abren en el dispositivo del usuario. Si está inhabilitada, el contenido se abre en el servidor.

De forma predeterminada, la asociación de tipos de archivo está inhabilitada.

Cuando se habilita esta configuración, los siguientes tipos de direcciones URL se abren de forma local:

- Protocolo HTTP
- Protocolo HTTP seguro (HTTPS)
- Real Player y QuickTime (RTSP)
- Real Player y QuickTime (RTSPU)
- Real Player (PNM) antiguo
- Microsoft Media Server (MMS)

Conservar las letras de unidad del cliente

Esta configuración habilita o inhabilita la asignación de unidades del cliente a la misma letra de unidad en la sesión.

De forma predeterminada, las letras de las unidades del cliente no se conservan.

Al agregar esta configuración a una directiva, compruebe que la configuración Redirección de unidades del cliente está presente y establecida en la opción Permitida.

Acceso de solo lectura a unidades del cliente

Esta configuración permite o evita 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 Citrix Receiver y de la Interfaz Web vean las carpetas especiales locales Documentos y Escritorio desde una sesión.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de StoreFront, la Interfaz Web o Citrix Receiver.

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 la opción Permitida.

Usar escrituras asíncronas

Esta configuración habilita o inhabilita las escrituras asíncronas en los discos.

De forma predeterminada, las escrituras asíncronas están inhabilitadas.

En redes WAN, caracterizadas por un alto ancho de banda y alta latencia, 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 cuando vuelva 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 realizarán escrituras asíncronas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de Flash

Dec 05, 2017

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, el parámetro Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario también debe estar habilitado.

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 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, es posible que este parámetro no establezca los colores clave de la URL. Si esto ocurre, modifique el Registro en la máquina de agente VDA.

En caso de máquinas de 32 bits, use este parámetro de Registro:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ForceHDXFlashEnabled"=dword:00000001

En caso de 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 anteriores de Citrix Receiver (antes denominado Citrix Online Plug-in).

De manera predeterminada, esta configuración está habilitada.

En el dispositivo del usuario, el parámetro Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario también debe estar habilitado.

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 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. La redirección de Flash y la generación en el lado del servidor no se utilizan. 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, el parámetro Habilitar la redirección de HDX MediaStream para Flash en el dispositivo de usuario también debe estar habilitado 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, la captura de registros está permitida.

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.

Respaldo inteligente de Flash

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 generar el contenido Flash en el dispositivo del usuario. Si la latencia es superior al umbral, el servidor de red genera el contenido si dispone de un reproductor de Adobe Flash.

Cuando habilite esta configuración, compruebe que 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 archivo *.swf de error.
- **Solo contenido pequeño, con un cliente respaldado**. Solo se genera contenido de respaldo inteligente en el servidor si el cliente usa la redirección de Flash; el resto del contenido se reemplazará por un *.swf. de error.
- **Sin contenido del lado del servidor**. Todo el contenido en el servidor se reemplazará por un *.swf de error.

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.

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://nombredominio.tld/muestra/ruta/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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 opción Habilitar obtención de contenido del lado del servidor.

La redirección de Flash de segunda generación incluye la opción de recurrir a la obtención del contenido del lado del servidor para archivos SWF de Flash. Si el dispositivo del usuario no puede obtener contenido Flash desde un sitio Web y el sitio Web está incluido en la lista de URL para obtener contenido Flash del lado del servidor, la obtención en el lado del servidor 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

Este parámetro 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, las acciones y las ubicaciones de generación de contenido más importantes en la parte superior.
- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Gráficos

Dec 05, 2017

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.

Límite de memoria de presentación

Esta configuración permite especificar el tamaño máximo de búfer para vídeo, en kilobytes, asignado a la sesión.

El límite de memoria de presentación predeterminado es de 65536 kilobytes.

Permite especificar el tamaño máximo de búfer para vídeo, en kilobytes, asignado a la sesión. Especifique una cifra en kilobytes de 128 a 4 194 303. El valor máximo (4,194,303) no limita la memoria de presentación. La memoria de presentación predeterminada es de 65536 kilobytes. Si se utiliza mayor profundidad de color y mayor resolución para las conexiones, se necesitará más memoria. En el modo de gráficos antiguos, si se alcanza el límite de memoria, la presentación se degrada según esté definida la configuración Preferencia de degradación de presentación.

Para las conexiones que requieran mayor profundidad de color y mayor resolución, aumente el límite. Puede calcular la memoria máxima necesaria con la siguiente ecuación:

Profundidad de memoria en bytes = (profundidad de color en bits por píxel) / 8) * (resolución vertical en píxeles) * (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) * (600) * (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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cuando se alcanza el límite de memoria para presentación, se puede reducir la calidad de la imagen presentada e indicar si se degradará primero la profundidad de color o la resolución. Cuando se degrada primero la profundidad de color, se usan menos colores para las imágenes. Cuando se degrada primero la resolución, se muestran las imágenes con menos píxeles por pulgada.

Para notificar a los usuarios de la degradación de la profundidad de color o de la resolución, defina la configuración Notificar al usuario cuando se degrada la presentación.

Vista previa de ventanas dinámicas

Esta configuración 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.

Modo de gráficos antiguo

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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.

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, el parámetro "Cola y descarte" está habilitado.

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 (H.264) para comprimir gráficos cuando la descodificación 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 descodificación de vídeo no está disponible en el punto final, o bien cuando se especifica la opción **No usar códec de vídeo**, se utilizan la compresión de imágenes estáticas y la memoria caché de mapas de bits. Si se selecciona **Usar**

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 códec de vídeo 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 (H.264).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 NVENC, se puede usar cualquier Citrix Receiver que admita la decodificación de H.264.

Se admiten la compresión con pérdida de información (4:2:0) y sin pérdida visual (4:4:4).La compresión sin pérdida visual (en la directiva de gráficos, la configuración Permitir compresión sin pérdida visual) requiere Receiver para Windows 4.5 o versiones posteriores.

NVIDIA

Para las GPU de NVIDIA GRID, la codificación por hardware se admite en agentes VDA para SO de escritorio en modo HDX 3D Pro.

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.

Sin pérdida de texto, una funcionalidad de VDA cuando se configura en modo estándar (no HDX 3D Pro) no es compatible con la codificación por hardware NVENC. Si se ha habilitado en el modo HDX 3D Pro, Sin pérdida de texto tiene prioridad sobre la codificación por hardware NVENC.

En cambio, no se admite el uso selectivo del códec de hardware H.264 para áreas en cambio constante.

Intel

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para procesadores de gráficos Intel Iris Pro, la codificación por hardware se admite en agentes VDA para SO de escritorio (en modo estándar o HDX 3D Pro) 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.

Se admite la compresión sin pérdida de texto.

Se admite el uso selectivo del códec de hardware H.264 para áreas en cambio constante.

Compatible con Windows 10, Windows Server 2012 y versiones posteriores.

En los VDA en modo 3D Pro, el codificador de 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 configurar esta configuración de directiva por usuario o por máquina.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Almacenamiento en caché

Dec 05, 2017

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 3 000 000 bits por segundo.

Este valor representa el umbral por debajo del cual tendrá efecto la función de caché persistente. Es decir, con el valor predeterminado, los mapas de bits se almacenan en la memoria caché del disco duro del dispositivo del usuario cuando el ancho de banda está por debajo de 3 000 000 bps.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Framehawk

Dec 05, 2017

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Keep Alive

Dec 05, 2017

La sección Keep Alive contiene configuraciones de directiva para gestionar los mensajes de ICA Keep Alive.

Tiempo de espera de ICA Keep Alive

Esta configuración permite especificar cuántos segundos deben transcurrir entre los mensajes sucesivos de ICA Keep Alive.

El intervalo predeterminado para los mensajes de Keep Alive es de 60 segundos.

Especifique un intervalo entre 1 y 3600 segundos para el envío de mensajes de ICA Keep Alive. No configure esto si tiene un software de supervisión de red que se encarga de cerrar las conexiones inactivas.

ICA Keep Alive

Esta configuración habilita o inhabilita el envío periódico de mensajes de ICA Keep Alive.

De manera predeterminada, no se envían mensajes de Keep Alive.

Si se habilita esta configuración, se evita la desconexión de las conexiones interrumpidas. Si el servidor no detecta ninguna actividad, esta configuración evita que los Servicios de Escritorio remoto (RDS) desconecten la sesión. El servidor envía mensajes de Keep Alive cada pocos segundos para detectar si la sesión está activa. Si la sesión ya no está activa, el servidor la marca como desconectada.

La función ICA Keep Alive no funciona si se usa Fiabilidad de la sesión. Configure ICA Keep Alive únicamente para conexiones que no usen Fiabilidad de la sesión.

Configuraciones de directiva relacionadas: Conexiones de fiabilidad de la sesión.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Acceso a aplicaciones locales

Dec 05, 2017

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.

Lista negra de redirección de URL

Esta configuración especifica 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 newsgoogle.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 sitios Web que se generan en el entorno en el que se inician.

De forma predeterminada, no hay ningún sitio especificado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Experiencia móvil

Dec 05, 2017

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 Citrix Receiver, ya que permite o prohíbe una interfaz táctil intuitiva, optimizada para dispositivos tipo tableta.

De forma predeterminada, se utiliza una interfaz táctil intuitiva.

Para usar solo la interfaz de Windows, defina esta configuración de directiva como Prohibida.

Control remoto de cuadros combinados

Esta configuración determina los tipos de cuadros combinados que se pueden ver en sesiones de dispositivos móviles. Para mostrar el control de cuadros combinados nativo del dispositivo, defina esta configuración de directiva como Permitida. Cuando esta configuración está permitida, un usuario puede cambiar el parámetro en la sesión de Citrix Receiver para iOS y utilizar el cuadro combinado de Windows.

De forma predeterminada, la función Control remoto de cuadros combinados está prohibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Multimedia

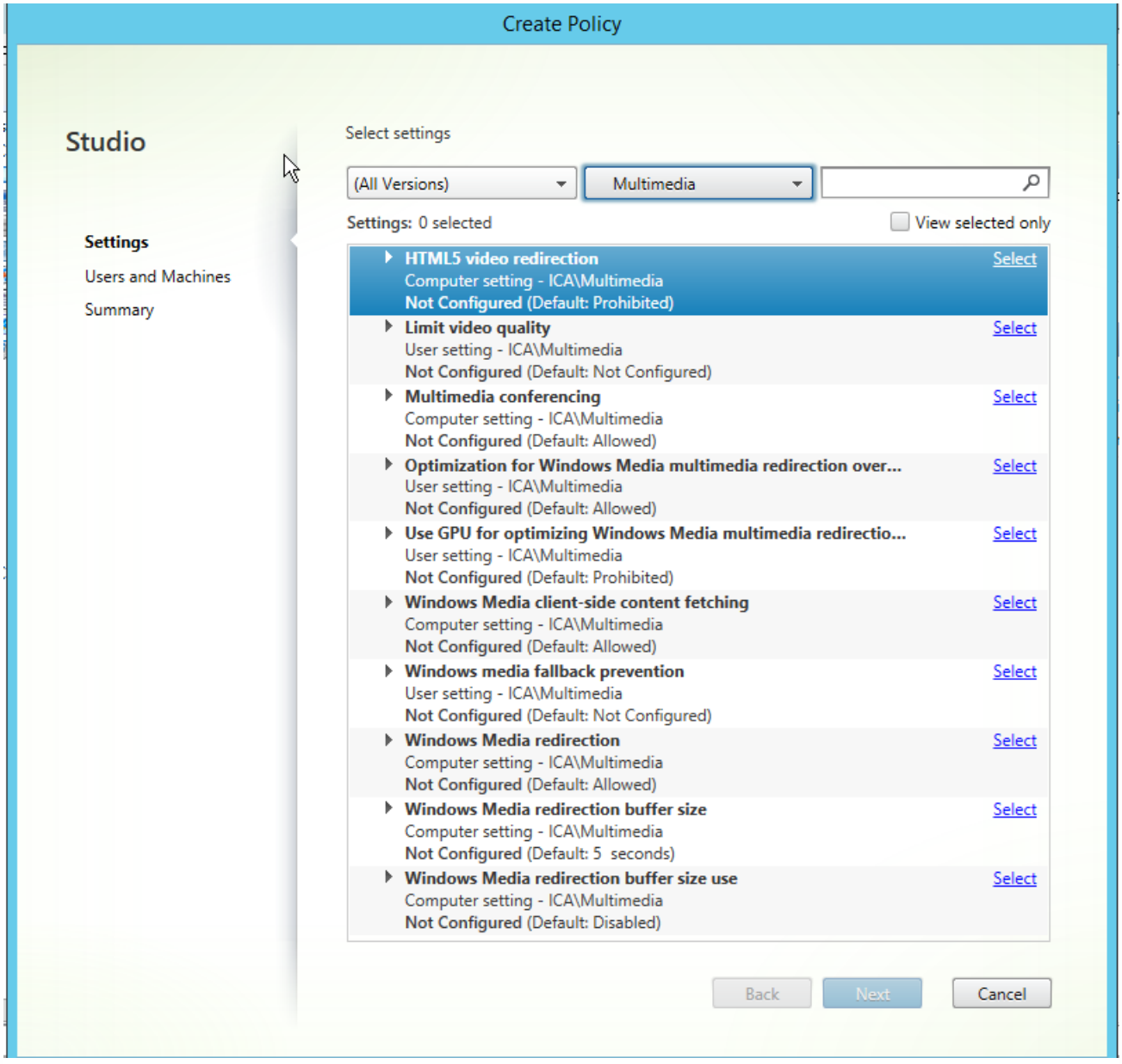
Jan 05, 2018

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.

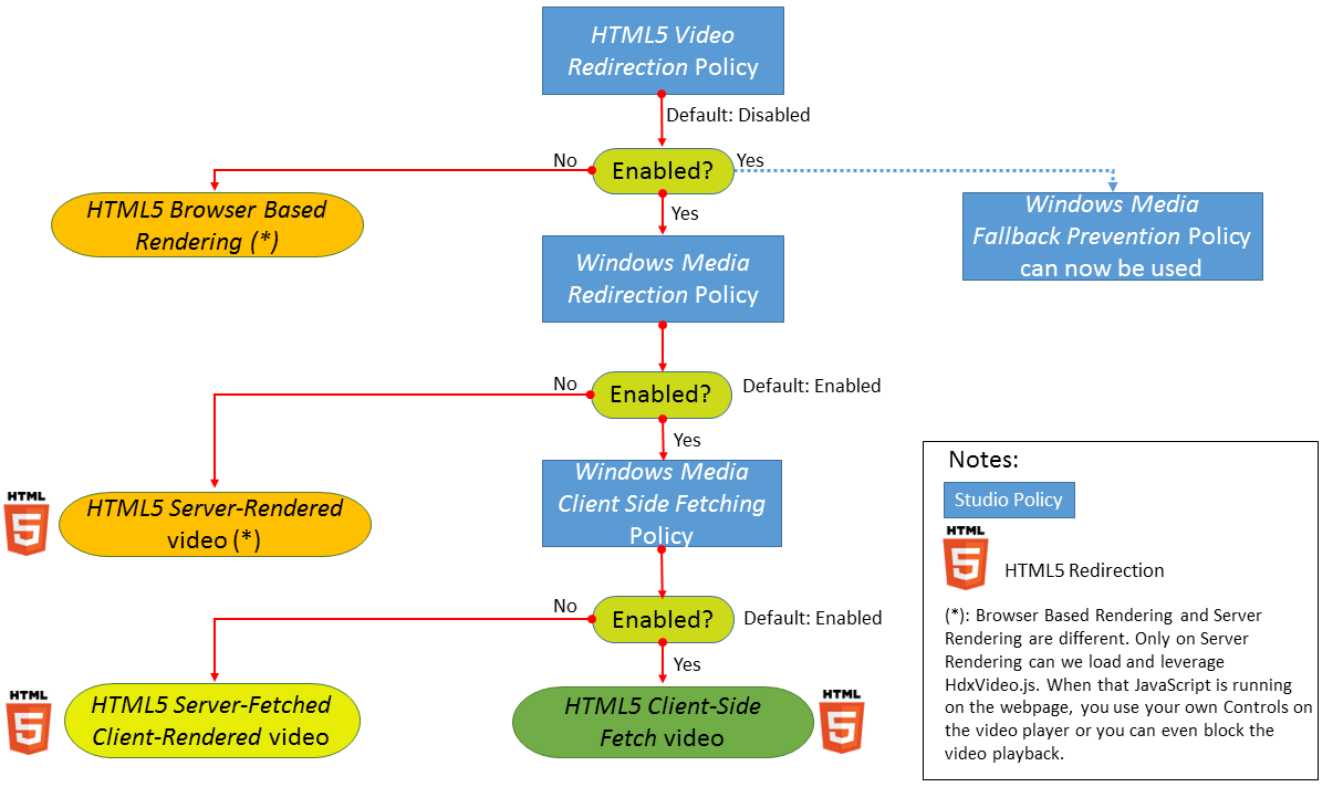
Redirección de vídeo HTML5

Controla y optimiza el modo en que los servidores XenApp y XenDesktop entregan contenido multimedia Web de HTML5 a los usuarios.

De forma predeterminada, esta configuración está inhabilitada.



© 1999-2017 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):

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, XenApp y XenDesktop recurrirán a la generación en el lado del servidor.

Debe estar permitida la ***redirección de Windows Media*** para que la redirección de vídeo HTML5 funcione correctamente. Esta directiva es obligatoria para Obtención en servidor, generación en cliente, y es necesaria para Obtención del lado del cliente (que a su vez requiere que *Obtención de contenido de Windows Media en el lado del cliente* esté permitida).

Microsoft Edge no admite esta función.

HdxVideo.js reemplaza los controles del reproductor HTML5 del explorador por los suyos propios. Para comprobar que la directiva Redirección de vídeo HTML5 está en vigor para un determinado sitio Web, compare los controles del reproductor con un caso en que la directiva ***Redirección de vídeo HTML5*** está prohibida:

(Controles personalizados de Citrix cuando la directiva está permitida)

© 1999-2017 Citrix Systems, Inc. All rights reserved.



(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

Puede ver una página de prueba para la redirección de vídeo HTML5 en https://www.citrix.com/virtualization/hdx/html5-redirect.html.

TLS y la redirección de vídeo 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*.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 (valor predeterminado).

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.

De forma predeterminada, la entrega de contenido de Windows Media a través de WAN está optimizada.

Al agregar esta configuración a una directiva, compruebe 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

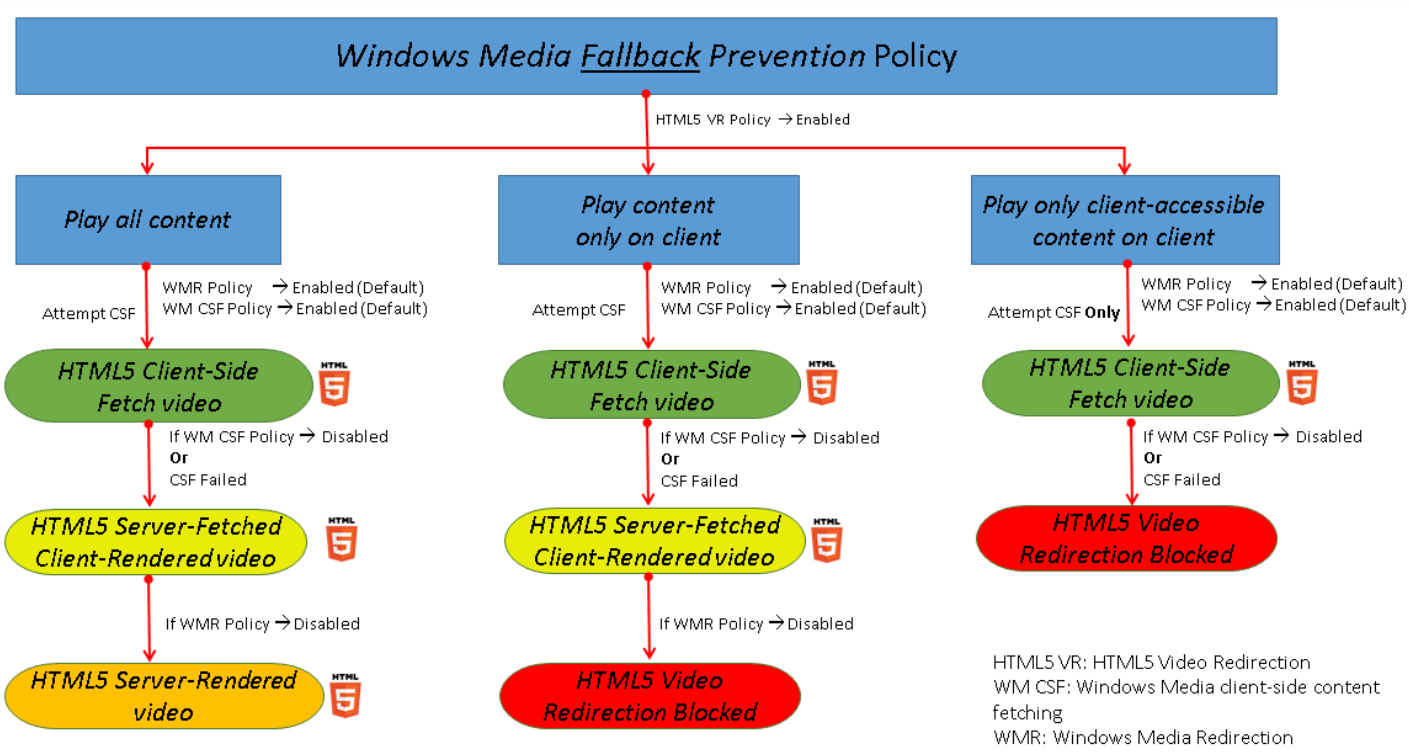
Los administradores pueden usar la directiva Prevención de respaldo de Windows Media para especificar los métodos que se utilizarán para entregar contenido por streaming a los usuarios.

De manera predeterminada, esta configuración no está definida. Cuando la configuración está establecido en No configurada, el comportamiento es el mismo que **Reproducir todo el contenido**.

Para definir esta configuración, elija alguna de estas opciones:

- **Reproducir todo el contenido**. Intentar obtener contenido del lado del cliente; luego Redirección de Windows Media. Si no se realiza correctamente, reproducir contenido en el servidor.
- **Reproducir todo el contenido solo en el cliente**. Intentar obtener contenido del lado del cliente; luego Redirección de Windows Media. Si no se realiza correctamente, no se reproduce el contenido.
- **Reproducir solo el contenido accesible por el cliente**. Solo intentar la obtención de contenido del lado del cliente. Si no se realiza correctamente, no se reproduce el contenido.

Si el contenido no se reproduce, aparece el mensaje de error "La empresa ha bloqueado el vídeo debido a falta de recursos" en la ventana del reproductor (durante 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> ## Advertencia
>
> Si edita 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

La ruta del Registro varía en función de la arquitectura del VDA:

\HKLM\SOFTWARE\Wow6432Node\Citrix\HdxMediastream

o

\HKLM\SOFTWARE\Citrix\HdxMediastream

Clave del Registro:

Nombre: VideoLoadManagementErrDuration

Tipo: DWORD

Intervalo: 1 - hasta el límite DWORD (predeterminado = 5)

Unidad: segundos

Obtención de contenido de Windows Media en el lado del cliente

Esta configuración 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, compruebe 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 sonido 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 sonido está inhabilitado en Citrix Receiver. Para permitir que los usuarios ejecuten aplicaciones multimedia en sesiones ICA, habilite el sonido u otorgue permisos a los usuarios para que habiliten el sonido en su interfaz de Citrix Receiver.

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 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Conexiones de multisecuencia

Dec 05, 2017

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 habilitado en el servidor.

Cuando está habilitada, esta configuración abre un puerto UDP en el servidor para admitir todas las conexiones configuradas para usar el Transporte de sonido en tiempo real sobre UDP.

Intervalo de puertos UDP de sonido

Esta configuración especifica el intervalo de números de puerto (en el formato lowest port number,highest port number) que Virtual Delivery Agent (VDA) utiliza para intercambiar datos de paquetes de sonido 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 de 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 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 (por ejemplo, al puerto CGP 1 y al puerto CGP 3).

Para quitar un puerto del sistema de prioridades, defina el número de puerto en 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Esta configuración habilita o inhabilita la multisecuencia en el servidor.

De forma predeterminada, la multisecuencia está inhabilitada.

Si usa Citrix NetScaler SD-WAN con respaldo para multisecuencia en el entorno, no es necesario configurar este parámetro. 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) deseado.

Cuando defina esta configuración, reinicie el servidor para que los cambios tengan efecto.
Importante: El uso de esta configuración de directiva junto con otras configuraciones de límite de ancho de banda, tales 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, compruebe que no haya configuraciones de límite de ancho de banda ya incluidas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de puertos

Dec 05, 2017

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 Configuración de la redirección de puertos COM y puertos LPT mediante el Registro. Para los agentes VDA de la versión **7.9**, utilice las siguientes configuraciones de directiva.

Conectar automáticamente puertos COM del cliente

Esta configuración habilita o inhabilita la conexión automática de los puertos COM en los dispositivos del usuario cuando este inicia sesión en un sitio.

Los puertos COM del cliente no se conectan automáticamente de forma predeterminada.

Conectar automáticamente puertos LPT del cliente

Esta configuración habilita o inhabilita la conexión automática de los puertos LPT en los dispositivos del usuario cuando este inicia sesión en un sitio.

Los puertos LPT del cliente no se conectan automáticamente de forma predeterminada.

Redirección de puertos COM del cliente

Esta configuración permite o impide el acceso a los puertos COM en el dispositivo del usuario.

La redirección de puertos COM está prohibida de forma predeterminada.

Configuraciones de directiva relacionadas:

- Límite de ancho de banda de redirección de puertos COM
- Porcentaje límite de ancho de banda de redirección de puertos COM

Redirección de puertos LPT del cliente

Esta configuración permite o impide el acceso a los puertos LPT en el dispositivo del usuario.

La redirección de puertos LPT está prohibida de forma predeterminada.

Los puertos LPT solo se utilizan por aplicaciones antiguas que envían trabajos de impresión a los puertos LPT y no a los objetos de impresión del dispositivo de usuario. La mayoría de las aplicaciones que se utilizan hoy en día pueden enviar trabajos de impresión a objetos de impresora. Esta configuración de directiva solo es necesaria para los servidores que alojan aplicaciones antiguas que imprimen en puertos LPT.

Tenga en cuenta que, aunque la redirección de puertos COM del cliente es bidireccional, la redirección de puertos LPT es solo de salida y se limita a \\client\LPT1 y \\client\LPT2 en una sesión ICA.

Configuraciones de directiva relacionadas:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Límite de ancho de banda de redirección de puertos LPT
- Porcentaje límite de ancho de banda de redirección de puertos LPT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Impresión

Dec 05, 2017

La sección Impresión contiene configuraciones de directiva para administrar la impresión del cliente.

Redirección de impresoras del cliente

Este parámetro 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 de 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 en el 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 será 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 impresoras

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, en una sesión, la impresora predeterminada en los dispositivos de usuario enumerados.

De forma predeterminada, la impresora actual del usuario se usa como predeterminada durante la sesión.

También especifica las impresoras de red que se crearán de forma automática en una sesión para cada dispositivo de usuario. De forma predeterminada, no hay impresoras especificadas.

- Al configurar el valor de impresora predeterminada:
  Para usar la impresora predeterminada actual para el dispositivo del usuario, seleccione No ajustar.

  Para usar el parámetro de impresora predeterminada existente en el perfil del usuario de Windows o en Servicios de Escritorio remoto, seleccione No ajustar. Si elige esta opción, la impresora predeterminada no se guarda en el perfil y no

© 1999-2017 Citrix Systems, Inc. All rights reserved.

cambia de acuerdo con otras propiedades de la sesión o del cliente. La impresora predeterminada de la sesión será 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 quiere crear automáticamente. Después de agregar la impresora, puede aplicar parámetros personalizados para la sesión actual en cada inicio de sesión.

Preferencia de registro de sucesos de creación automática de impresoras

Esta configuración permite especificar los sucesos que se registran durante el proceso de creación automática de impresoras. Puede optar por no registrar los errores ni las advertencias, registrar solamente los errores o registrar los errores y las advertencias.

De forma predeterminada, se registran los errores y las advertencias.

Un ejemplo de advertencia es un suceso en el cual no se pudo instalar el controlador original de una impresora y se instaló el controlador de impresión universal. Para utilizar controladores de impresión universal en esta circunstancia, configure Uso de controladores de impresión universal en Usar solo impresión universal o Usar impresión universal solo si el controlador solicitado no está disponible.

Impresoras de la sesión

Esta configuración permite especificar qué impresoras de red se crearán automáticamente en una sesión.

De forma predeterminada, no hay impresoras especificadas.

Para agregar impresoras, escriba la ruta UNC de la impresora que quiera crear automáticamente. Después de agregar la impresora, puede aplicar parámetros personalizados para la sesión actual en cada inicio de sesión.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Impresoras del cliente

Dec 05, 2017

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 de Redirección de impresoras del cliente está presente y establecida en Permitida.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Crear automáticamente todas las impresoras del cliente. Crea de forma automática todas las impresoras del dispositivo del usuario.
- Crear automáticamente solo la impresora predeterminada del cliente. Crea de forma automática solo la impresora seleccionada como predeterminada en el dispositivo del usuario.
- Crear automáticamente solo las impresoras locales (no de red) del cliente. Crea de forma automática solo las impresoras conectadas directamente con el dispositivo del usuario por un puerto LPT, COM, USB, TCP/IP u otro puerto local.
- No crear automáticamente las impresoras del cliente. Desactiva la creación automática de todas las impresoras del cliente cuando el usuario inicia sesión. Esto hace que los parámetros de creación automática de impresoras del cliente de los Servicios de Escritorio remoto reemplacen esta configuración en las directivas que tengan menor prioridad.

Crear automáticamente una impresora universal genérica

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 genérico de impresora universal de Citrix (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

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”.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Seleccione Nombres de impresoras antiguos para usar nombres similares a los asignados a las impresoras cliente más antiguas y mantener la compatibilidad con versiones anteriores para usuarios o grupos que utilicen MetaFrame Presentation Server 3.0 u otra versión anterior. Un ejemplo de nombre de impresora antiguo es: “Cliente/nombre_cliente#/HPLaserJet 4”. Esta opción es menos segura.
Nota: Esta opción se ofrece únicamente para mantener la compatibilidad con versiones anteriores de XenApp y XenDesktop.

Conexiones directas con servidores de impresión

Esta configuración habilita o inhabilita las conexiones directas desde el escritorio virtual o desde el servidor que aloja las aplicaciones a 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 el 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 el 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.

Este parámetro está configurado para excluir Microsoft OneNote y 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.

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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 las versiones de 9 a 12.x de Citrix Online Plug-in 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 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 XenApp 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de directivas de Controladores

Dec 05, 2017

La sección Controladores contiene configuraciones de directiva relacionadas con los controladores de impresoras.

Instalación automática de controladores de impresora

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 que se usan los controladores de impresión universal, comenzando por la primera entrada en la lista.

De forma predeterminada, el orden de preferencia es:

- EMF
- XPS
- PCL5c
- PCL4
- PS

Es posible agregar, modificar o eliminar controladores y cambiar el orden de los controladores mostrados en la lista.

Uso de controladores de impresión universal

Esta configuración permite especificar cuándo se usa la impresión universal.

De forma predeterminada, la impresión universal se utiliza exclusivamente si el controlador solicitado no está disponible.

La impresión universal emplea controladores de impresora genéricos en lugar de controladores específicos de modelos de impresora, lo que simplifica la gestión de los controladores en los equipos host. La disponibilidad de los controladores de impresión universal depende de la capacidad del software del dispositivo de usuario, del host y del servidor de impresión. En algunas configuraciones, es posible que la impresión universal no esté disponible.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Usar solo los controladores específicos de la impresora indica que la impresora cliente usa solamente los controladores estándar específicos de modelo de impresora, los cuales se crean automáticamente al iniciar sesión. Si el controlador solicitado no está disponible, la impresora cliente no podrá crearse de forma automática.
- Usar solo impresión universal . Especifica que no se usen los controladores específicos del modelo de impresora. Solo se usan controladores de impresión universal para crear impresoras.
- Usar impresión universal solo si el controlador solicitado no está disponible utiliza los controladores estándar específicos del modelo de impresora para la creación de impresoras, si están disponibles. Si el controlador no está disponible en el servidor, la impresora cliente se crea automáticamente mediante un controlador de impresora universal adecuado.
- Usar controladores específicos de la impresora solo si la impresión universal no está disponible usa el controlador de impresión universal si está disponible. Si el controlador no está disponible en el servidor, la impresora cliente se crea de forma automática con el controlador específico del modelo de impresora adecuado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Universal Print Server

Dec 05, 2017

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 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 los 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, a efectos prácticos, 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 Universal Print Server está inhabilitada. No se intenta conectar con Universal Print Server al conectarse a 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 de escucha del flujo de datos de impresión de Universal Print Server (CGP). Aplique esta configuración de directiva solamente a las unidades organizativas que contienen el servidor de impresión.

De forma predeterminada, el número de puerto es el 7229.

Los números de puerto válidos deben estar en el intervalo de 1 a 65535.

Límite de ancho de banda del flujo de entrada de impresión de Universal Print Server (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 mediante CGP. Aplique esta configuración de directiva a las unidades organizativas que contienen el escritorio virtual o el servidor que aloja aplicaciones.

De forma predeterminada, el valor es 0, lo cual no especifica un límite superior.

Puerto del servicio Web de Universal Print Server (HTTP/SOAP)

Esta configuración especifica el número de puerto TCP que utiliza el agente de escucha (HTTP/SOAP) del servicio Web de Universal Print Server. Universal Print Server es un componente optativo que permite el uso de controladores de impresión

© 1999-2017 Citrix Systems, Inc. All rights reserved.

universal de Citrix para la impresión en red. Cuando se utiliza Universal Print Server, los comandos de impresión se envían de los hosts de XenApp y XenDesktop 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 opción de configuración cambia el agente VDA de XenApp y XenDesktop. Además, debe cambiar el puerto predeterminado en Universal Print Server.

De forma predeterminada, el número de puerto es el 8080.

Los números de puerto válidos deben estar en el intervalo de 0 a 65535.

Universal Print Servers para equilibrio de carga

Esta configuración enumera los servidores de impresión universal que se usarán para equilibrar la carga de las conexiones de impresora establecidas al comienzo de las sesiones, después de evaluar otras configuraciones de impresión de Citrix. Para optimizar la creación de impresoras, Citrix recomienda que todos los servidores de impresión tengan el mismo conjunto de impresoras compartidas. No hay límite máximo para la cantidad de servidores de impresión que se pueden agregar para el equilibrio de carga.

Esta configuración también implementa la detección de fallos de impresora para la conmutación por error y la recuperación de conexiones de impresora. La disponibilidad de los servidores de impresión se comprueba periódicamente. Si se detecta un error del servidor, ese servidor se quita del esquema de equilibrio de carga y las conexiones de impresora en ese servidor se redistribuyen entre los otros servidores de impresión disponibles. Cuando el servidor de impresión que falló se recupera, se lo devuelve al esquema de equilibrio de carga.

Haga clic en **Validar servidores** para comprobar que cada servidor es un servidor de impresión y que todos los servidores tienen un conjunto de impresoras compartidas idéntico. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Impresión universal

Dec 05, 2017

La sección Impresión universal contiene configuraciones de directiva para administrar la impresión universal.

Modo de procesamiento EMF de la impresión universal

Esta configuración controla el método de procesamiento del archivo de cola de impresión EMF en el dispositivo de usuario Windows.

De forma predeterminada, los registros EMF se envían directamente a la impresora.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Reprocesar EMF para la impresora fuerza el reprocesamiento del archivo de cola de EMF y su envío a través del subsistema GDI en el dispositivo del usuario. Puede usar esta configuración para los controladores que requieren el reprocesamiento de EMF pero que puede que no se seleccionen automáticamente en una sesión.
- Enviar directamente a la cola de impresión , cuando se usa con el controlador de impresora universal de Citrix, asegura que los registros EMF se envíen a la cola y se entreguen al dispositivo del usuario para el procesamiento. Normalmente, estos archivos de cola de impresión EMF se transfieren directamente a la cola de impresión del cliente. Para las impresoras y controladores que son compatibles con el formato EMF, este es el método de impresión más rápido.

Límite de compresión de imagen para la impresión universal

Esta configuración define la calidad máxima y el nivel de compresión mínimo disponibles para las imágenes impresas con el controlador de impresora universal de Citrix.

De forma predeterminada, el límite de compresión de imagen está definido en Mejor calidad (compresión sin pérdida).

Si se ha seleccionado Sin compresión, la compresión está inhabilitada para la impresión EMF solamente.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Sin compresión
- Mejor calidad (compresión sin pérdida)
- Alta calidad
- Calidad estándar
- Calidad reducida (compresión máxima)

Cuando agregue esta configuración a una directiva que incluye ya la configuración Valores predeterminados de optimización de impresión universal, tenga en cuenta lo siguiente:

- Si el nivel de compresión en Límite de compresión de imagen para la impresión universal es inferior al nivel definido en Valores predeterminados de optimización de impresión universal, las imágenes se comprimen según el nivel definido en la configuración Límite de compresión de imagen para la impresión universal.
- Si la compresión está inhabilitada, las opciones Calidad de imagen deseada y Habilitar la compresión intensa de la configuración Valores predeterminados de optimización de impresión universal no tienen ningún efecto en la directiva .

Valores predeterminados de optimización de la 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

universal. De forma predeterminada, la Calidad estándar está habilitada, de manera que los usuarios solo pueden imprimir imágenes con la compresión de calidad estándar o reducida.
- Habilitar la compresión intensa habilita o inhabilita la reducción de ancho de banda más allá del nivel de compresión definido por Calidad de imagen deseada, sin pérdida de calidad de imagen. La compresión intensa está inhabilitada de forma predeterminada.
- La configuración de Almacenamiento en caché de imágenes y fuentes especifica si las imágenes y fuentes que aparecen varias veces en el flujo de impresión se almacenan en caché, para que cada imagen individual se envíe solo una vez a la impresora. De forma predeterminada, las fuentes e imágenes incrustadas se almacenan en caché. Tenga en cuenta que estas configuraciones solo se aplican si el dispositivo del usuario admite este comportamiento.
- Permitir a los no administradores modificar estos parámetros especifica si los usuarios pueden cambiar los parámetros predeterminados de optimización de la impresión en una sesión. De forma predeterminada, los usuarios no pueden cambiar los parámetros predeterminados de la optimización de impresión.

Nota: Todas estas opciones reciben respaldo con la impresión EMF. En el caso de la impresión XPS, solo se admite la opción Calidad de imagen deseada.
Cuando agregue esta configuración a una directiva que incluye ya la configuración Límite de compresión de imagen para la impresión universal, tenga en cuenta lo siguiente:
- Si el nivel de compresión en Límite de compresión de imagen para la impresión universal es inferior al nivel definido en Valores predeterminados de optimización de impresión universal, las imágenes se comprimen según el nivel definido en la configuración Límite de compresión de imagen para la impresión universal.
- Si la compresión está inhabilitada, las opciones Calidad de imagen deseada y Habilitar la compresión intensa de la configuración Valores predeterminados de optimización de impresión universal no tienen ningún efecto en la directiva.

Preferencia de vista previa en impresión universal

Esta configuración permite especificar si se usará la función de vista previa de impresión para las impresoras universales genéricas o creadas automáticamente.

De forma predeterminada, no se utiliza la vista previa de impresión para estas impresoras.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:
- No usar vista previa en las impresoras de creación automática o universales genéricas
- Usar vista previa solo para impresoras de creación automática
- Usar vista previa solo para impresoras universales genéricas
- Usar vista previa para impresoras de creación automática y universales genéricas

Límite de calidad de la impresión universal

Esta configuración especifica la cantidad máxima de puntos por pulgada (ppp) disponibles para generar los productos impresos en una sesión.

De forma predeterminada, Sin límite está habilitado, y permite a los usuarios seleccionar la calidad de impresión máxima permitida por la impresora a la que están conectados.

Cuando esta configuración está definida, limita la calidad de impresión máxima disponible para los usuarios en términos de resolución de salida. Tanto la calidad de impresión misma como la capacidad de calidad de impresión de la impresora a la que se conectan los usuarios quedan limitadas por el parámetro configurado. Por ejemplo, si se configura como Resolución media (600 ppp), los usuarios están limitados a imprimir con una calidad máxima de 600 ppp y la configuración "Calidad de impresión" en la ficha "Avanzado" del cuadro de diálogo "Impresora universal" muestra parámetros de resolución solo hasta la calidad media inclusive (600 ppp).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Seguridad

Nov 27, 2017

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 XenApp y XenDesktop.

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 la opción Habilitar Secure ICA para el grupo de entrega, los datos de la sesión se cifran con RC5 (128 bits). Si no se selecciona la opción Habilitar Secure ICA para el grupo de entrega, los datos de la sesión se cifran con Cifrado básico.

Al agregar esta configuración a una directiva, seleccione una de las siguientes opciones:

- Básico. Cifra la conexión de cliente mediante un algoritmo distinto de RC5. Este nivel de cifrado protege el flujo de datos para que no pueda leerse directamente, pero puede ser descifrado. De forma predeterminada, el servidor utiliza el cifrado básico para el tráfico entre el cliente y el servidor.
- RC5 (128 bits) solo inicios de sesión. Cifra los datos de inicio de sesión con un cifrado RC5 de 128 bits y cifra la conexión de cliente con cifrado básico.
- RC5 (40 bits). Cifra la conexión de cliente con un cifrado RC5 de 40 bits.
- RC5 (56 bits). Cifra la conexión de cliente con un cifrado RC5 de 56 bits.
- RC5 (128 bits). Cifra la conexión de cliente con 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Límites de servidor

Dec 05, 2017

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).

> **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Límites de sesión

Dec 05, 2017

La sección Límites de sesión contiene configuraciones de directiva para controlar el tiempo que las sesiones pueden permanecer conectadas antes de un cierre forzoso.Estos valores no se aplican a agentes VDA de Windows Server.

Temporizador de sesión desconectada

Esta configuración habilita o inhabilita un temporizador que determina cuánto tiempo puede permanecer desconectado y bloqueado un escritorio antes de que se cierre la sesión.

De forma predeterminada, las sesiones desconectadas no se cierran.

Intervalo de temporizador de sesiones desconectadas

Esta configuración especifica cuánto tiempo, en minutos, puede permanecer desconectado y bloqueado un escritorio antes de que se cierre la sesión.

De forma predeterminada, este período es de 1440 minutos (24 horas).

Temporizador de conexión de sesión

Esta configuración habilita o inhabilita un temporizador que especifica la duración máxima de una conexión sin interrupciones entre un dispositivo del usuario y un escritorio.

De manera predeterminada, este temporizador está inhabilitado.

Intervalo de temporizador de conexión de sesiones

Esta configuración especifica la cantidad máxima de minutos que puede durar 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 una conexión sin interrupciones de un dispositivo de usuario con un escritorio, si el usuario no realiza ninguna entrada.

De manera predeterminada, este temporizador está habilitado.

Intervalo de temporizador de sesiones inactivas

Esta configuración especifica cuánto tiempo se mantendrá la conexión ininterrumpida del dispositivo del usuario con un escritorio, si el usuario no realiza entradas.

De forma predeterminada, las conexiones inactivas se mantienen durante 1440 minutos (24 horas).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Fiabilidad de la sesión

Dec 05, 2017

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 Citrix Receiver después de recuperarse de una interrupción en la red.

A partir de Citrix Receiver para Windows 4.7, la Fiabilidad de la sesión solo usa las configuraciones de directiva de Citrix Studio. Las actualizaciones de estas directivas en Studio sincronizan la Fiabilidad de la sesión 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.

Nota: Si establece la opción **Habilitar fiabilidad de la sesión** en **Inhabilitada** en la plantilla administrativa del objeto de directiva de grupo de Citrix Receiver o en la directiva de Citrix Studio, se inhabilita la Fiabilidad de la sesión. Si no define la opción **Habilitar fiabilidad de la sesión** en la directiva de Citrix Studio, pero sí la **inhabilita** en la plantilla administrativa del objeto de directiva de grupo de Citrix Receiver, se habilita la Fiabilidad de la sesión.

Cuando la conectividad de red se ve interrumpida, la fiabilidad de la sesión mantiene las sesiones activas y en la pantalla del usuario. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Con la función de 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.

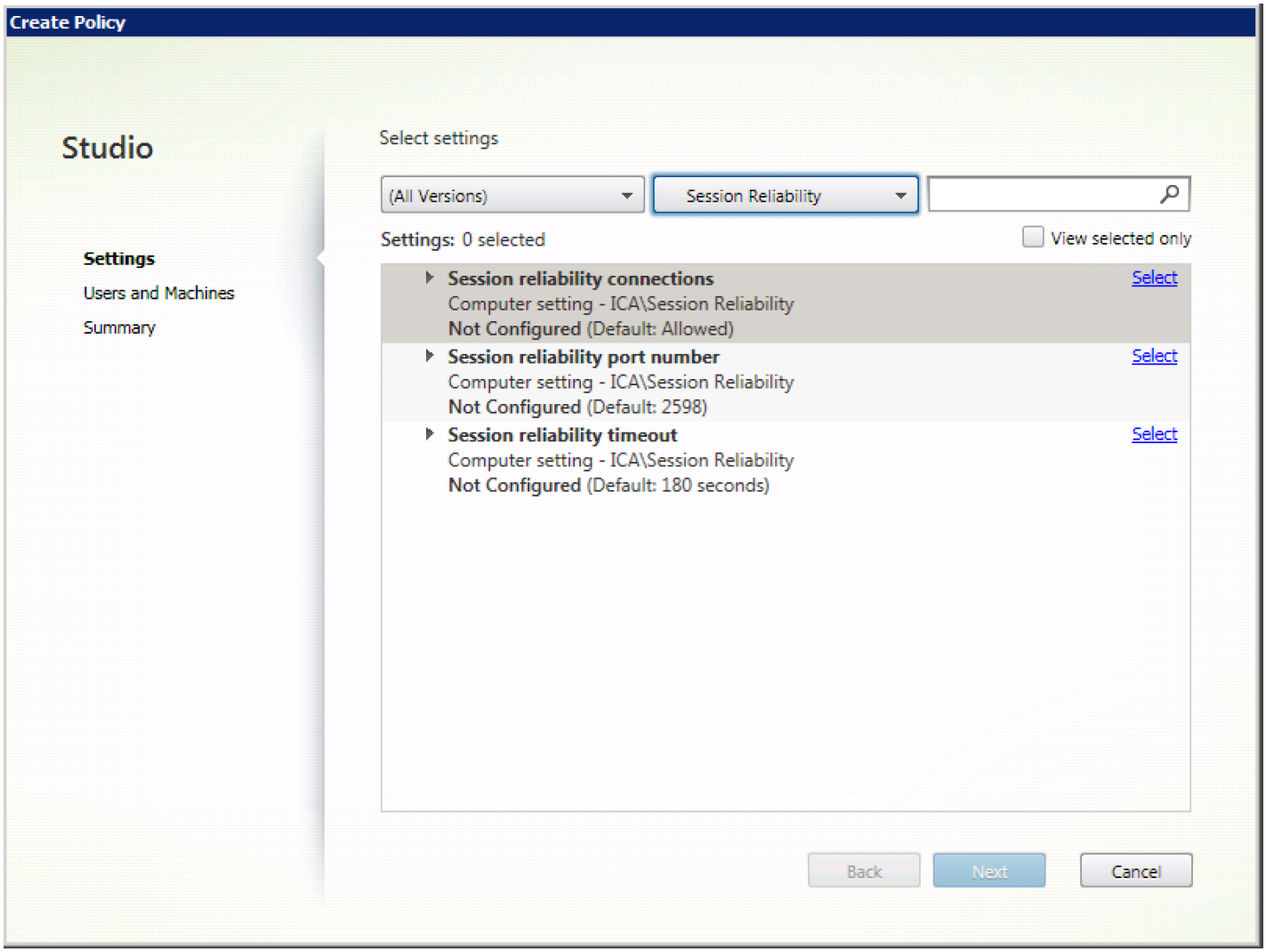
Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La Fiabilidad de la sesión cierra (o desconecta) la sesión del usuario una vez haya trascurrido el tiempo especificado en Tiempo de espera de fiabilidad de la sesión. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

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 el valor **Prohibida**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 modificar el número de puerto de Fiabilidad de la sesión:

1. Inicie Citrix Studio.
2. Abra la opción **Número de puerto para fiabilidad de la sesión**.
3. Modifique el número de puerto.
4. Haga clic en **Aceptar**.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 opción **Tiempo de espera de fiabilidad de la sesión**.
3. Cambie el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Control de zona horaria

Dec 05, 2017

La sección Control de zona horaria contiene configuraciones de directiva relacionadas con la hora local usada para las sesiones.

Calcular hora local para clientes antiguos

Esta configuración 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.

Esta configuración está diseñada 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.

Usar la hora local del cliente

Esta configuración permite determinar la configuración de zona horaria de la sesión del usuario. Esta puede ser la zona horaria de la sesión del usuario o la zona horaria del dispositivo del usuario.

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 (Configuración de equipo > Plantillas administrativas > Componentes de Windows > Servicios de Escritorio remoto > Host de sesión de Escritorio remoto > Redirección de dispositivo o recurso).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Dispositivos TWAIN

Dec 05, 2017

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.

Redirección de dispositivos TWAIN del cliente

Esta configuración permite o impide el acceso de los usuarios a los dispositivos TWAIN presentes en el 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Dispositivos USB

Dec 05, 2017

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 el dispositivo está permitido según la configuración de la directiva de USB. Si el dispositivo está permitido, entonces el host comprueba 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 degrade con la latencia alta, los administradores pueden habilitar el modo interactivo (02). Consulte las descripciones que se indican a continuación para conocer los modos disponibles.

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 esta tarea.
- 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 XenApp y XenDesktop.
- Los dispositivos de firma funcionan en XenApp y XenDesktop, y no requieren un controlador 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 entrada de dibujo pueden ser dispositivos de interfaz humana (HID) en buses PCI o ACPI y no se admiten. Esos dispositivos deben conectarse a un controlador de host USB en el cliente para que se redirijan dentro de una sesión de XenDesktop.

Las reglas de directivas tienen el formato de expresiones etiqueta=valor, separadas por un espacio en blanco. Se admiten las siguientes etiquetas:

Nombre de la etiqueta	Descripción
Modo	El modo de optimización se admite para dispositivos de entrada de class=**03**. Los modos compatibles 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 proveniente del descriptor del

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	dispositivo.
PID	Identificador del producto proveniente del descriptor del dispositivo.
REL	Identificador de la versión proveniente del descriptor del dispositivo.
Clase	Clase, proveniente del descriptor del dispositivo o de un descriptor de la interfaz.
Subclass	Subclase, proveniente del descriptor del dispositivo o de un descriptor de la interfaz.
Prot	Protocolo proveniente del descriptor del dispositivo o de un descriptor de la interfaz.

Ejemplos

Mode=00000004 VID=1230 PID=1230 class=03 #El dispositivo de entrada opera en el modo de captura

Mode=00000002 VID=1230 PID=1230 class=03 #El dispositivo de entrada opera en el modo interactivo (opción predeterminada)

Mode=00000001 VID=1230 PID=1230 class=03 #El dispositivo de entrada opera sin optimización

Mode=00000100 VID=1230 PID=1230 # Configuración de optimización inhabilitada en el dispositivo (opción predeterminada)

Mode=00000200 VID=1230 PID=1230 # Configuración de optimización habilitada en el dispositivo

Cómo 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. Haga clic en **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, los dispositivos USB no se redirigen.

Reglas de redirección de dispositivos USB del cliente

Esta configuración especifica las reglas de redirección para dispositivos USB.

De forma predeterminada, no se especifica ninguna regla.

Cuando un usuario conecta un dispositivo USB, el dispositivo host consulta cada regla de directiva hasta que encuentra una coincidencia, es decir una directiva donde figure el dispositivo en cuestión. La primera coincidencia para cualquier dispositivo se considera definitiva. Si la primera coincidencia es una regla para Permitir (Allow), el dispositivo se coloca en comunicación remota con el escritorio virtual. Si la primera coincidencia es una regla para Denegar (Deny), el dispositivo solamente está disponible en el escritorio local. Si no hay coincidencias, se usan las reglas predeterminadas.

Las reglas de directivas tienen el formato {Allow:|Deny:} seguidas de un conjunto de expresiones etiqueta=valor, separadas por un espacio en blanco. Se admiten las siguientes etiquetas:

Nombre de la etiqueta	Descripción
VID	Identificador del proveedor tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
Clase	Clase, proveniente 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 nuevas 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=1230_).
- Cada regla debe comenzar en una línea nueva o formar parte de una lista de reglas, separadas por punto y coma.
- Consulte los códigos de clase USB que están disponibles en el sitio Web de USB Implementers Forum, Inc.

Ejemplos de reglas de directivas USB definidas por el administrador:

- Allow: VID=1230 PID=0007 # Otra Industria, Otra unidad de Flash
- Deny: 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 (como cámaras o terminales de punto de venta POS) se usen en las sesiones de cliente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 establecen como Prohibida, ningún dispositivo se redirige.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Presentación visual

Dec 05, 2017

La sección Presentación visual contiene configuraciones de directiva para controlar la calidad de las imágenes enviadas desde los escritorios virtuales al dispositivo del usuario.

Preferencia de profundidad de color para gráficos sencillos

Esta configuración de directiva se encuentra disponible en las versiones de VDA 7.6 FP3 y las versiones posteriores. La opción de 8 bits está disponible en las versiones de VDA 7.12 y las versiones posteriores.

Esta configuración hace posible reducir la profundidad de color en los gráficos sencillos que se envían a través de la red. Reducir el color a 8 o 16 bits por píxel ofrece una mejora potencial de la capacidad de respuesta en conexiones de poco ancho de banda, a costa de una pequeña degradación de la calidad de imagen. La profundidad de color de 8 bits no se admite cuando la configuración de directiva Usar códec de vídeo para compresión está definida en "Para la pantalla entera".

El valor predeterminado es la profundidad de color preferida de 24 bits por píxel.

Los VDA vuelven a la profundidad de color de 24 bits (predeterminada) si la opción de 8 bits se aplica a VDA 7.11 y versiones anteriores.

Velocidad de fotogramas de destino

Esta configuración especifica la cantidad máxima de fotogramas por segundo que se envían desde el escritorio virtual al dispositivo de usuario.

De forma predeterminada, el valor máximo es 24 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**
- **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; este parámetro 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 (por ejemplo, al mostrar radiografías, donde una pérdida de calidad sería inaceptable), seleccione Siempre sin pérdida para que nunca se envíen datos incompletos al dispositivo del usuario.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si está habilitada la configuración **Modo de gráficos antiguo**, la configuración **Calidad visual** no tendrá efecto en esa directiva.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Imágenes en movimiento

Dec 05, 2017

La sección Imágenes en movimiento contiene configuraciones que le permiten quitar o modificar la compresión para imágenes dinámicas.

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.

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.

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 normal con pérdida. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de compresión normal con pérdida.
Configuraciones de directiva relacionadas:

- Valor de umbral de compresión progresiva
- Compresión intensa 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 al indicado.

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

Esta configuración especifica la velocidad de fotogramas por segundo mínima que el sistema intenta mantener para imágenes dinámicas cuando la conexión cuenta con poco ancho de banda.
De forma predeterminada, el valor es de 10 fps.

Desde la versión 7.0 hasta la versión 7.6 de VDA, esta opción de configuración se aplica solo cuando el modo de gráficos antiguo está habilitado. A partir de la versión 7.6 FP1 de VDA, esta opción de configuración se aplica cuando el modo de gráficos antiguo está habilitado o inhabilitado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva para imágenes fijas

Dec 05, 2017

La sección de Imágenes fijas contiene configuraciones que le permiten quitar o modificar la compresión para imágenes estáticas.

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.

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 ancho de banda máximo 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 del 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.

Nota : Para Virtual Delivery Agent 7.x, esta configuración de directiva solo se aplica cuando la configuración de directiva Modo de gráficos antiguo está habilitada.
Esta configuración habilita o inhabilita la reducción del ancho de banda más allá de la compresión progresiva sin reducir la calidad de la imagen, 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 habilita, la compresión intensa se aplica a todas las configuraciones de compresión con pérdida. Está respaldada en Citrix Receiver, pero no tiene ningún efecto en otros plugins.

Configuraciones de directiva relacionadas:
- Nivel de compresión progresiva
- Valor del 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 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (por ejemplo, para imágenes de rayos X) en situaciones en las que no es aceptable perder calidad, se recomienda no utilizar la compresión con pérdida.

Configuración de directiva relacionada: 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 ancho de banda máximo (en kilobits por segundo) de una conexión a la que se aplicará la compresión con pérdida.

El umbral predeterminado es de 2147483647 kilobits por segundo.

Si se agrega 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 (como fotografías) en una LAN.

Configuración de directiva relacionada: Nivel de compresión con pérdida

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de WebSockets

Dec 05, 2017

La sección WebSockets contiene configuraciones de directiva para acceder con Citrix Receiver para HTML5 a los escritorios virtuales y las aplicaciones alojadas. La función de 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.

Esta configuración permite o prohíbe conexiones de WebSockets.

De forma predeterminada, las conexiones de WebSockets están prohibidas.

Esta configuración identifica el puerto para conexiones entrantes de WebSockets.

De forma predeterminada, el valor es de 8008.

Esta configuración proporciona una lista separada por comas de los servidores de origen de confianza, normalmente Citrix Receiver 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 Citrix Receiver para Web.

Para escribir una dirección en la lista, use la siguiente sintaxis:

<protocol>://<Fully qualified domain name of host>:[port]

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. *. *).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Administración de carga

Dec 05, 2017

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.

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

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.

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.

Esta configuración especifica la longitud de la cola de disco en la que el servidor notifica carga completa al 75 %. Cuando está habilitada, el valor predeterminado para la longitud de la cola de disco es 8.

De forma predeterminada, esta configuración está inhabilitada y el uso del disco queda excluido al calcular la carga.

Esta configuración especifica la cantidad máxima 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Profile Management

Dec 05, 2017

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetros avanzados de directiva

Dec 05, 2017

La sección Parámetros avanzados contiene configuraciones de directiva relacionadas con una configuración avanzada de Profile Management.

Esta configuración habilita Profile Management para 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 funcionalidad 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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.

Esta configuración habilita Profile Management para 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se ofrece un perfil temporal.

Esta configuración especifica la cantidad de intentos que realiza Profile Management para acceder a archivos bloqueados.

De forma predeterminada, este valor está establecido en cinco reintentos.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se utiliza el valor predeterminado.

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 prolongada exploración, la cual puede dar lugar a una sobrecarga del perfil. Al habilitarla, los cierres de sesión tardan más, de manera que se recomienda habilitarla solamente si es necesario.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

De forma predeterminada, esta configuración está inhabilitada y Profile Management no procesa el archivo index.dat al cerrar la sesión.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se procesará el archivo index.dat.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Parámetros básicos de directiva

Dec 05, 2017

La sección Parámetros básicos contiene configuraciones de directiva relacionadas con una configuración básica de Profile Management.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se considera habilitado.

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.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si el parámetro no se configurado ni aquí ni en el archivo INI, Profile Management no procesa los perfiles de usuario de Windows de ninguna manera.

Esta configuración especifica qué grupos locales de equipo y de dominio (locales, globales y universales) se excluyen del 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: <DOMAIN NAME>\<GROUP NAME>.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se procesan los miembros de todos los grupos de usuarios.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cuando se produce una desconexión de red, los perfiles permanecen intactos en el equipo portátil o dispositivo móvil, incluso después 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, el respaldo para perfiles sin conexión está inhabilitado.

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.
Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si el parámetro no se configura ni aquí ni en el archivo INI, se utiliza el directorio Windows de la unidad principal.

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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

asignados, puedan omitir el procesamiento, y puedan iniciar sesión y solucionar problemas de Profile Management en el escritorio.

Si este parámetro está inhabilitado, o si no está configurado 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se procesan los inicios de sesión de administrador local.

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: <DOMAIN NAME>\<GROUP NAME>.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se procesan los miembros de todos los grupos de usuarios.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Multiplataforma

Dec 05, 2017

La sección Multiplataforma contiene configuraciones de directiva relacionadas con la función de configuración multiplataforma de Profile Management.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se procesarán todos los grupos de usuarios.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se aplicarán configuraciones 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se aplicarán configuraciones 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se utiliza el valor predeterminado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Esta configuración especifica una plataforma como plataforma base si la configuración está habilitada para la unidad organizativa de esa plataforma. Los datos de los perfiles de la plataforma base se 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Sistema de archivos

Dec 05, 2017

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 que está instalado el perfil y el almacén de usuarios.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Exclusiones

Dec 05, 2017

La sección Exclusiones contiene configuraciones de directiva para establecer qué archivos y directorios de un perfil de usuario se excluyen del proceso de sincronización.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se sincronizan todas las carpetas del perfil de usuario.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se sincronizan todos los archivos del perfil de usuario.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Sincronización

Dec 05, 2017

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.

Esta configuración especifica los archivos que desea que Profile Management incluya 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 Inclusión y exclusión de 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se sincronizarán solo las carpetas que no se han excluido del perfil de usuario.

Esta configuración especifica los archivos que desea que Profile Management incluya 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 Inclusión y exclusión de 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
- 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se sincronizan solo los archivos que no se han excluido del perfil de usuario.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 este parámetro no está configurado 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Redirección de carpetas

Dec 05, 2017

La sección Redirección de carpetas contiene configuraciones de directiva para especificar si quiere redirigir las carpetas que suelen aparecer en perfiles a una ubicación de red compartida.

Esta configuración permite que un administrador pueda acceder al contenido de las carpetas redirigidas de un usuario.

De forma predeterminada, esta configuración está inhabilitada y los usuarios tienen acceso exclusivo al contenido de sus carpetas redirigidas.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de AppData(Roaming)

Dec 05, 2017

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.

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Contactos

Dec 05, 2017

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

Esta configuración especifica cómo redirigir el contenido de la carpeta Contactos.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Escritorio

Dec 05, 2017

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

Esta configuración especifica cómo redirigir el contenido de la carpeta Escritorio.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Documentos

Dec 05, 2017

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.

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 este parámetro no está configurado 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.

Esta configuración especifica cómo redirigir el contenido de la carpeta Documentos.

De forma predeterminada, el contenido se redirige a una ruta UNC.

Para controlar cómo redirigir el contenido de la carpeta Documentos, elija una de las siguientes opciones:

- Redirigir a esta ruta UNC. Redirige contenido a la ruta UNC especificada en la configuración de directiva 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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Descargas

Dec 05, 2017

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

Esta configuración especifica cómo redirigir el contenido de la carpeta Descargas.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Favoritos

Dec 05, 2017

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

Esta configuración especifica cómo redirigir el contenido de la carpeta Favoritos.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Vínculos

Dec 05, 2017

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

Esta configuración especifica cómo redirigir el contenido de la carpeta Vínculos.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Música

Dec 05, 2017

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Imágenes

Dec 05, 2017

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.

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.

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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Juegos guardados

Dec 05, 2017

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 este parámetro no está configurado 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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Búsquedas

Dec 05, 2017

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

Estos parámetros especifican cómo redirigir el contenido de la carpeta Búsquedas.

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.

Ruta de Búsquedas

Este parámetro 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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Menú Inicio

Dec 05, 2017

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 este parámetro no está configurado 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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Vídeos

Dec 05, 2017

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 este parámetro no está configurado 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 este parámetro no está configurado aquí, Profile Management no redirige la carpeta especificada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de registros

Dec 05, 2017

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 la información común.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Advertencias comunes

Esta configuración habilita o inhabilita el registro detallado de advertencias comunes.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Habilitar registro

Esta configuración habilita o inhabilita el registro de Profile Management en el modo de depuración (registro detallado). En modo de depuración, la información detallada de estado se registra en los archivos de registro ubicados en "%SystemRoot%\System32\Logfiles\UserProfileManager".

De forma predeterminada, esta configuración está inhabilitada y solo se registran los errores.

Citrix recomienda habilitar esta configuración solo cuando vaya a solucionar problemas de Profile Management.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, solo se registran los errores.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Acciones del sistema de archivos

Esta configuración habilita o inhabilita el registro detallado de las acciones realizadas en el sistema de archivos.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Notificaciones del sistema de archivos

Esta configuración habilita o inhabilita el registro detallado de las notificaciones de los sistemas de archivos.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Cierre de sesión

Esta configuración habilita o inhabilita el registro detallado de los cierres de sesión de los usuarios.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Inicio de sesión

Esta configuración habilita o inhabilita el registro detallado de los inicios de sesión de los usuarios.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de registro supera el tamaño máximo indicado, se elimina una copia de seguridad (.bak) del archivo, se cambia el nombre del archivo de registro a .bak y se crea un nuevo archivo de registro.

El archivo de registro se crea en %SystemRoot%\System32\Logfiles\UserProfileManager.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se utiliza el valor predeterminado.

Ruta al archivo de registro

Esta configuración especifica una ruta alternativa en la que guardar el archivo de registros de Profile Management.

De forma predeterminada, esta configuración está inhabilitada y los archivos de registro se guardan en la ubicación predeterminada: %SystemRoot%\System32\Logfiles\UserProfileManager.

La ruta puede corresponder a una unidad local o a una unidad remota en la red (una ruta UNC). Las rutas remotas pueden ser útiles en entornos distribuidos de gran tamaño, pero pueden crear un tráfico de red significativo, lo cual puede ser inadecuado para los archivos de registros. En el caso de máquinas virtuales aprovisionadas, con una unidad de disco duro persistente, defina una ruta local a dicha unidad. Esto garantiza que los archivos de registro se conservarán cuando la máquina se reinicie. Para máquinas virtuales sin disco duro persistente, la definición de una ruta UNC permite conservar los archivos de registros, pero la cuenta de sistema de las máquinas debe tener acceso de escritura en el recurso compartido UNC. Use una ruta local para los equipos portátiles gestionados con la función de perfiles sin conexión.

Si se usa una ruta UNC para los archivos de 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 los equipos autorizados.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 personalizada del usuario.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 los valores de directivas cuando un usuario inicia y cierra sesión.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Acciones del Registro del sistema

Esta configuración habilita o inhabilita el registro detallado de las acciones realizadas en el Registro del sistema.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

Diferencias en el Registro del sistema al cerrar la sesión

Esta configuración habilita o inhabilita el registro detallado de las diferencias en el Registro cuando un usuario cierra sesión.

De forma predeterminada, esta configuración está inhabilitada.

Cuando habilite esta configuración, compruebe que la configuración Habilitar registro también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se registran los errores y la información general.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Gestión de perfiles

Dec 05, 2017

La sección Gestión de perfiles contiene configuraciones de directiva para definir la forma en que Profile Management gestiona los perfiles de usuario.

Demora antes de eliminar perfiles en caché

Esta configuración especifica una extensión opcional para el intervalo de demora, en segundos, antes de que Profile Management elimine los perfiles almacenados en caché local al cerrar sesión.

Un valor de 0 elimina los perfiles inmediatamente al final del proceso de cierre de sesión. Profile Management comprueba los cierres de sesión cada minuto, por lo que un valor de 60 garantiza que los perfiles se eliminan entre uno y dos minutos después de que los usuarios hayan cerrado la sesión (dependiendo de cuando tuvo lugar la última comprobación). Ampliar la demora es útil si sabe que un proceso mantiene abiertos los archivos o el subárbol User del Registro durante el cierre de sesión. Con grandes perfiles, esto también puede acelerar el cierre de sesión.

De forma predeterminada, este valor está establecido en 0 y Profile Management elimina inmediatamente los perfiles almacenados en caché local.

Cuando habilite esta configuración, compruebe que Eliminar perfiles guardados en caché local al cerrar la sesión también está habilitada.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 esta configuración, la memoria caché local de perfiles del usuario se borra después del cierre de sesión. Citrix recomienda habilitar esta configuración para servidores de terminales.

De forma predeterminada, esta configuración está inhabilitada y la caché local de perfiles de un usuario se conserva después de cerrar sesión.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, los perfiles almacenados en caché no se eliminan.

Gestión de conflictos de perfiles locales

Esta configuración define el comportamiento de Profile Management si el mismo perfil de usuario consta en el almacén de usuarios y en Windows como perfil local (no un perfil de usuario de Citrix).

De forma predeterminada, Profile Management utiliza el perfil de Windows local, pero no lo cambia de ninguna manera.

Para controlar el comportamiento de Profile Management, elija una de las siguientes opciones:

- Usar el perfil local . Profile Management utiliza el perfil local, pero no lo cambia de ninguna manera.
- Eliminar el perfil local . Profile Management elimina el perfil de usuario local de Windows y, a continuación, importa el perfil de usuario de Citrix desde el almacén de usuarios.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Cambiar el nombre del perfil local . Profile Management cambia el nombre del perfil de usuario local de Windows (para conservar una copia de seguridad) y, a continuación, importa el perfil de usuario de Citrix desde el almacén de usuarios.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 guardado 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
- Móviles
- Ninguno (inhabilitado)

Si selecciona Ninguno, el sistema utiliza el mecanismo de Windows existente para la creación de nuevos perfiles, como si fuera en un entorno en el que Profile Management no está instalado.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se migran los perfiles locales y móviles existentes.

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.dat, se definiría la ubicación como \\MiServidor\MisPerfiles\plantillas.
Utilice rutas absolutas, que pueden ser rutas UNC o rutas del equipo local. Puede utilizar estas 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se utiliza ninguna plantilla.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se utiliza ninguna plantilla.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Registro del sistema

Dec 05, 2017

La sección de 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 del 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 sesión.

De forma predeterminada, esta configuración está inhabilitada y todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra sesión.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, no se excluye ninguna clave de Registro del procesamiento.

Lista de inclusión

Esta configuración especifica la lista de claves del 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 sesión.

De forma predeterminada, esta configuración está inhabilitada y todas las claves del Registro en el subárbol HKCU se procesan cuando un usuario cierra sesión.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado ni aquí ni en el archivo INI, se procesará toda la sección HKCU.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva para Perfiles de usuario de streaming

Dec 05, 2017

La sección Perfiles de usuario de streaming contiene configuraciones de directiva para especificar la forma en que Profile Management procesará 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 opción junto con Streaming de perfiles.

De forma predeterminada, esta configuración está inhabilitada y los archivos distribuidos por streaming no se almacenan en caché tan pronto como sea posible cuando un usuario inicia sesión.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado aquí ni en el archivo .ini, se considera inhabilitado.

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.

De forma predeterminada, este valor está establecido en 0 (cero) y se usa la función de guardado del perfil entero en caché. Cuando la función de guardado del perfil entero en caché está habilitada, Profile Management obtiene todo el contenido del perfil en el almacén de usuarios, cuando un usuario inicia sesión, como una tarea en segundo plano.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado aquí ni en el archivo .ini, se considera inhabilitado.

Streaming de perfiles

Esta configuración habilita o inhabilita la función de streaming de perfiles de usuario de Citrix. Cuando está habilitada, las carpetas y los archivos incluidos en un perfil se obtienen del almacén de usuarios y se envían al equipo local solo cuando los usuarios acceden a estos archivos y carpetas después de iniciar una sesión. Las entradas del Registro y los archivos del área de archivos pendientes se obtienen inmediatamente.

De forma predeterminada, el streaming de perfiles está inhabilitado.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado aquí ni en el archivo .ini, se considera inhabilitado.

Grupos de perfiles de usuarios de streaming

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de la forma habitual.

De forma predeterminada, esta configuración está inhabilitada y todos los perfiles de usuario dentro de una unidad organizativa se procesan de la forma habitual.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado 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 Para habilitar la exclusión de streaming de perfiles.

Tiempo de espera (en días) 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 responda. Esto evita la saturación en el área de archivos pendientes y garantiza que el almacén de usuarios siempre contenga los archivos más actualizados.

De forma predeterminada, este valor está establecido en 1 (un) día.

Si este parámetro no está configurado aquí, se utiliza el valor del archivo INI.

Si este parámetro no está configurado aquí ni en el archivo .ini, se utiliza el valor predeterminado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Receiver

Dec 05, 2017

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: On/Off (habilitado o inhabilitado).
- Descripción de la tienda. La descripción que se muestra a los usuarios de la tienda.

Por ejemplo: Almacén de ventas;https://sales.mycompany.com/Citrix/Store/discovery;On;Almacén para personal de Ventas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Virtual Delivery Agent

Dec 05, 2017

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 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 el VDA a una sola subred preferida (en lugar de una dirección IP global, si consta alguna). Esta configuración especifica la dirección IPv6 y la red en que se registrará el VDA. El 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 utiliza el VDA para registrarse en un Controller cuando se usa un registro basado en el Registro del sistema.

De forma predeterminada, el número de puerto es 80.

Identificadores SID de Controller

Use esta configuración solamente si Habilitar actualización automática de Controller está inhabilitada.

Esta configuración especifica una lista separada por espacios de identificadores de seguridad (SID) de Controllers que el VDA usa para registrarse en 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 en un Controller cuando se usa un registro basado en el Registro del sistema. Esta es una

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configuración optativa que puede utilizarse junto con la configuración Identificadores SID de Controller.

De forma predeterminada, esta configuración está en blanco.

Habilitar actualización automática de Controllers

Esta configuración permite que el VDA se registre automáticamente en un Controller después de la instalación.

Después de que el VDA se registre, el Controller en el que se registró envía una lista actualizada de los SID y FQDN de los Controllers al VDA. El VDA escribe esta lista en un almacenamiento persistente. Cada Controller también consulta 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 consulta o si se ha producido un cambio en la directiva, el Controller envía listas actualizadas a los VDA registrados. Los VDA aceptarán conexiones de todos los Controllers que consten en la lista más reciente que hayan recibido.

De manera predeterminada, esta configuración está habilitada.

Usar solo registro de Controller con IPv6

Esta configuración controla qué tipo de dirección usa el VDA para registrarse en un Controller:

- Cuando está habilitada, el VDA se registra en el Controller con la dirección IPv6 de la máquina. Cuando el VDA se comunica con el Controller, 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 en un Controller cuando se usa el registro basado en Active Directory.

De forma predeterminada, esta configuración está en blanco.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de HDX 3D Pro

Dec 05, 2017

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

Este parámetro especifica si los usuarios pueden o no habilitar e inhabilitar la compresión sin pérdida mediante la herramienta de configuración de la calidad de imagen. De forma predeterminada, los usuarios no tienen la opción de habilitar la compresión sin pérdida.

Cuando un usuario habilita la compresión sin pérdida, la calidad de imagen se establece automáticamente en el valor máximo disponible en la herramienta de configuración de la imagen. De forma predeterminada, se puede utilizar la compresión basada en CPU o GPU, según la capacidad del dispositivo del usuario y el equipo host.

Parámetros de calidad de HDX 3D Pro

Estos parámetros especifican 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de Supervisión

Dec 05, 2017

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 este parámetro 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 este parámetro es Inhabilitada.

Habilitar supervisión de recursos

Habilite este parámetro para permitir la supervisión de los contadores de rendimiento en las máquinas con agentes VDA. Las estadísticas (por ejemplo, acerca de la CPU y la memoria, IOPS y la latencia de datos) se envían a Monitoring Service. Las estadísticas se utilizan para notificaciones en tiempo real e informes históricos en Director.

La opción predeterminada de este parámetro 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si se habilitan los datos de procesos, con la configuración predeterminada de retención de datos, consumirían aproximadamente 1,5 MB por cada VDA y 3 MB por cada VDA de Terminal Services (VDA de TS) en un periodo de un año.

Cantidad de máquinas	Almacenamiento aproximado requerido para el VDA	Almacenamiento aproximado requerido para el VDA de Terminal Services
1	1,5 MB	3 MB
1000	1,5 GB	3 GB

> **Nota**
>
> Estos números no incluyen el espacio de índice. Además, todos esos cálculos son aproximados y pueden variar de una implementación a otra.

Configuraciones opcionales

Puede modificar la configuración de retención predeterminada para que se adapte a sus necesidades. Sin embargo, eso consume almacenamiento extra. Al habilitar los siguientes parámetros, puede obtener más precisión en los datos de uso de procesos. Las configuraciones que se pueden habilitar son:

EnableMinuteLevelGranularityProcessUtilization

EnableDayLevelGranularityProcessUtilization

Estas configuraciones se pueden habilitar desde el cmdlet Monitoring de PowerShell: Set-MonitorConfiguration

Directivas para la supervisión de fallos de aplicaciones

De forma predeterminada, la ficha **Fallos y errores de aplicación** muestra solo los errores de aplicaciones en los VDA de SO de servidor. Puede modificar los parámetros de supervisión de fallos de aplicaciones con las siguientes directivas de supervisión:

Habilitar supervisión de fallos y errores de aplicación

Use este parámetro para configurar 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 este parámetro es "Solo fallos de aplicación".

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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, este parámetro está establecido en **Prohibida**.

Lista de aplicaciones excluidas de la supervisión de fallos y errores

Especifique una lista de las aplicaciones que no se supervisarán para buscar fallos.
De forma predeterminada, esta lista está vacía.

Sugerencias para la planificación de almacenamiento

Directiva de grupo.Si no quiere supervisar los datos de recursos o procesos, ambos se pueden desactivar mediante la directiva de grupo. Para obtener más información, consulte la sección Directiva de grupo de Creación de directivas.

Limpieza de datos. La configuración predeterminada de retención de datos se puede modificar para limpiar los datos antes y así liberar espacio de almacenamiento. Para obtener más información sobre los parámetros de limpieza de datos, consulte Granularidad y retención de datos en Acceso a datos usando la API.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuraciones de directiva de IP virtual

Dec 05, 2017

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de la redirección de puertos COM y puertos LPT mediante el Registro

Feb 19, 2018

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.

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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Clave del Registro	Descripción	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 imagen maestra o el

© 1999-2017 Citrix Systems, Inc. All rights reserved.

equipo físico actualizado. Los escritorios se actualizan con la nueva configuración la próxima vez que los usuarios cierran la sesión.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de directivas de Connector para Configuration Manager 2012

Dec 05, 2017

La sección de Connector para Configuration Manager 2012 contiene las configuraciones 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 de 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

Esta configuración define el intervalo de frecuencia con que aparecen los mensajes de advertencia para los usuarios.

Los intervalos se definen 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.
- mm son los minutos, con un rango de 0 a 59.
- ss 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

Esta configuración contiene el texto a modificar del mensaje para los usuarios, donde se les notifica que va a haber actualizaciones de software o un periodo de mantenimiento para lo cual necesitan cerrar sesión.

De forma predeterminada, el mensaje contiene este texto: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}.

Título del mensaje de advertencia por adelantado

Esta configuración 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 periodo se define 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- mm son los minutos, con un rango de 0 a 59.
- ss 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

Esta configuración 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

Esta configuración 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

Esta configuración 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 periodo se define 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.
- mm son los minutos, con un rango de 0 a 59.
- ss 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

Esta configuración 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

Esta configuración 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

Connector Agent detecta automáticamente si se está ejecutando en una máquina clonada administrada por Provisioning Services o por 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 organizar el reinicio de los clones del catálogo de MCS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Connector Agent organiza automáticamente el reinicio de los clones del catálogo de PVS durante los intervalos 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

Esta configuración 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.

Intervalo regular para ejecutar la tarea del agente

Esta configuración determina la frecuencia con la que se ejecuta la tarea del agente Citrix Connector Agent.

El periodo se define 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.
- mm son los minutos, con un rango de 0 a 59.
- ss son los segundos, con un rango de 0 a 59.

De forma predeterminada, la configuración del intervalo regular es de 5 minutos (00:05:00).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administración

Dec 05, 2017

La administración de un sitio de XenDesktop o XenApp implica diversos elementos y tareas.

Licencia

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. El almacenamiento y la red de esa conexión forman sus *recursos*. Posteriormente, puede cambiar esa conexión y sus recursos, además de crear nuevas conexiones. También puede administrar las máquinas que usan una conexión configurada.

Memoria caché del host local

La Memoria caché del 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. Es la funcionalidad de alta disponibilidad más completa que Citrix ofrece para XenApp y XenDesktop.

Concesión de conexiones

Citrix recomienda probar la Memoria caché del host local en lugar de la Concesión de conexiones. La Memoria caché del host local es una alternativa más eficaz.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Uso de las búsquedas en Studio

Si quiere ver información acerca de las máquinas, las sesiones, los catálogos de máquinas, las aplicaciones o los grupos de entrega en Studio, utilice la función flexible de búsqueda.

Etiquetas

Utilice etiquetas para identificar elementos tales como máquinas, aplicaciones, grupos y directivas. A continuación, puede ajustar determinadas operaciones para aplicarlas a elementos con una etiqueta determinada.

IPv4 o IPv6

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Licencia

Dec 05, 2017

> **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:

Productos	Ediciones	Modelos de licencia
XenApp	• Platinum • Empresarial • Avanzado	Concurrente
XenDesktop	• Platinum • Empresarial • Apps (Aplicación) • VDI	• Dispositivo o usuario • 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 name:port, donde "name" es una dirección DNS, NetBIOS o IP. Si no especifica un número de puerto, se utiliza el puerto predeterminado (27000).

Para seleccionar el tipo de licencia que se va a utilizar:

- Al configurar el sitio, después de especificar el servidor de licencias, se le solicita que seleccione el tipo de licencia que va a utilizar. Si no existen licencias en el servidor, se selecciona automáticamente la opción para utilizar el producto durante un período de prueba de 30 días sin una licencia.
- Si existen licencias en el servidor, se muestran los detalles y se puede seleccionar una de ellas. O bien puede agregar un archivo de licencia al servidor y seleccionar ese archivo.

Para cambiar la edición y el modelo de licencia del producto:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione **Modificar edición de producto** en el panel Acciones.
3. Actualice las opciones pertinentes.

Para acceder a la consola License Administration Console, en el panel Acciones, seleccione **License Administration Console**. La consola aparece inmediatamente o bien, si el panel de mandos está configurado con la protección por contraseña, se le pedirán las credenciales de la consola License Administration Console. Para obtener más información acerca de cómo usar la consola, consulte la documentación de licencias.

Para agregar un administrador de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central.
3. Seleccione **Agregar administrador de licencias** en el panel Acciones.
4. Vaya al usuario que quiere agregar como administrador y elija los permisos correspondientes.

Para modificar los permisos de un administrador de licencias o eliminarlo:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central y, a continuación, seleccione el administrador en cuestión.
3. Seleccione **Modificar administrador de licencias** o **Eliminar administrador de licencias** en el panel Acciones.

Para agregar un grupo de administradores de licencias:

1. Seleccione **Configuración > Licencias** en el panel de navegación de Studio.
2. Seleccione la ficha Administradores de licencias en el panel central.
3. Seleccione **Agregar grupo de administradores de licencias** en el panel Acciones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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 grupo de administradores en cuestión.
3. Seleccione **Modificar grupo de administradores de licencias** o **Eliminar grupo de administradores de licencias** en el panel Acciones.

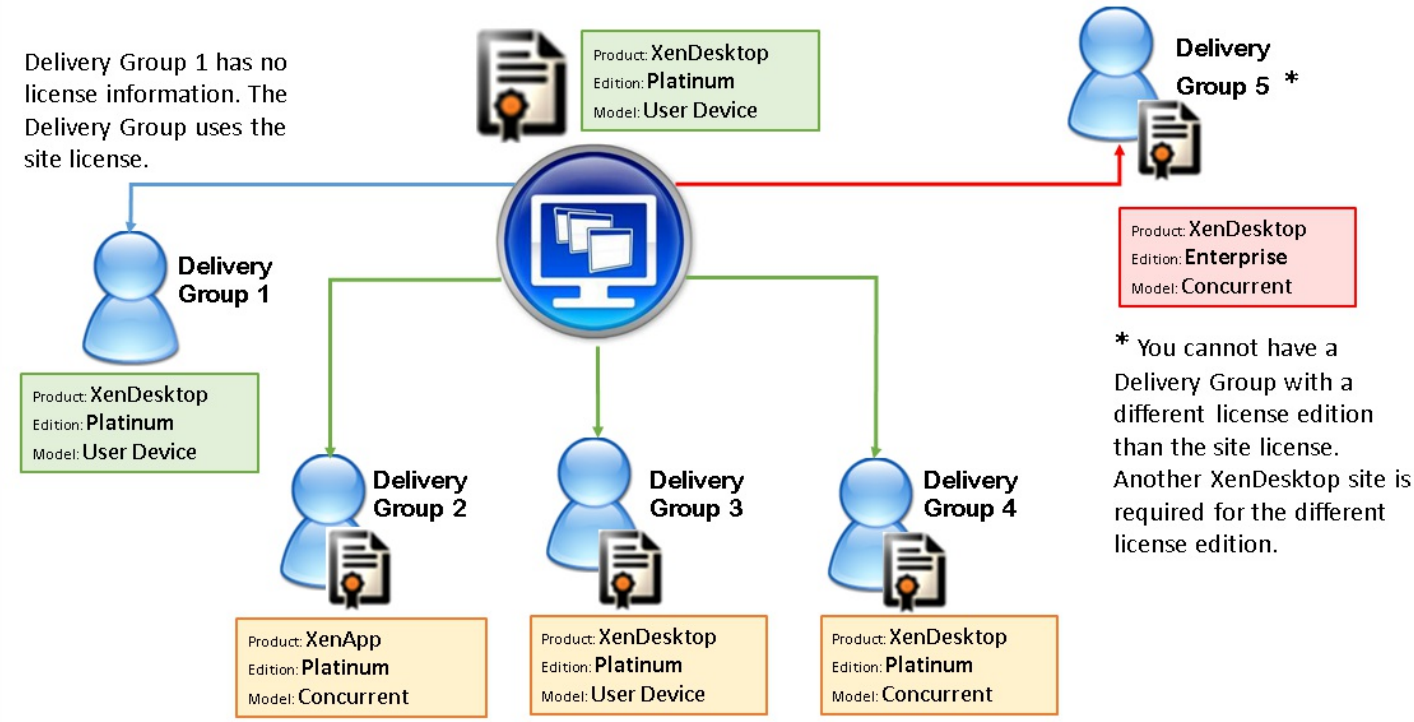
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Licencias de varios tipos

Dec 05, 2017

Con licencias de varios tipos, puede usar tipos de licencias diferentes para grupos de entrega en un único sitio de XenApp o XenDesktop. **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. Los grupos de entrega que se configuren de manera diferente podrían tener diferentes fechas de Subscription Advantage entre sí.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SDK de Broker PowerShell

El objeto **DesktopGroup** tiene estas dos propiedades que puede manipular mediante los cmdlets New-BrokerDesktopGroup y Set-BrokerDesktopGroup asociados.

Name	Value	Restriction
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 XenDesktop) o MPS (para XenApp) 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 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 XenApp Platinum Concurrent" -ProductCode MPS -LicenseModel Concurrent
2. El segundo grupo de entrega se establece como XenDesktop y Concurrent.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Set-BrokerDesktopGroup -Name "Delivery Group for XenDesktop Platinum 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 XenDesktop Platinum 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 XenApp y XenDesktop.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aplicaciones

Dec 05, 2017

Introducción

Si su implementación usa solo grupos de entrega (y no grupos de aplicaciones), tiene que agregar aplicaciones a los grupos de entrega. Si también tiene grupos de aplicaciones, por lo general, debe agregar aplicaciones a los grupos de aplicaciones. Esta recomendación facilita la administración. Una aplicación siempre debe pertenecer al menos a un grupo de entrega o un grupo de aplicaciones.

En el asistente Agregar aplicaciones, seleccione uno o varios grupos de entrega, o uno o más grupos de aplicaciones, pero no ambos. Aunque puede cambiar posteriormente la asociación de una aplicación a un grupo (por ejemplo, puede mover la aplicación desde un grupo de aplicaciones a un grupo de entrega), se recomienda no hacerlo para no incrementar la complejidad. Mantenga sus aplicaciones en un tipo de grupo.

Al asociar una aplicación a más de un grupo de entrega o más de un grupo de aplicaciones, puede producirse un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos. En tales casos, consulte a un administrador con más permisos o haga que amplíen su ámbito para incluir todos los grupos a los que se haya agregado la aplicación.

Si publica dos aplicaciones con el mismo nombre (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 Citrix Receiver.

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 información sobre:

- Los grupos de entrega, consulte el artículo Creación de grupos de entrega.
- Los grupos de aplicaciones, consulte Creación de grupos de aplicaciones.
- Las etiquetas, que se pueden agregar a aplicaciones, consulte el artículo Etiquetas.

Cómo 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.

Tenga en cuenta:

- No se pueden agregar aplicaciones a grupos de entrega de acceso con Remote PC.
- El asistente para agregar aplicaciones no puede usarse para quitar aplicaciones de los grupos de entrega o de los grupos de aplicaciones. Se trata de dos operaciones diferentes.

Para agregar una o varias aplicaciones:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Resumen.

Como alternativa al paso 1 si quiere agregar aplicaciones a un grupo de entrega o un grupo de aplicaciones:

- Para agregar aplicaciones a un solo grupo de entrega, en el paso 1, seleccione **Grupos de entrega** en el panel de navegación de Studio, 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, seleccione un **Grupo de aplicaciones** en el panel central y, a continuación, seleccione la entrada **Agregar aplicaciones** en el nombre del grupo de aplicaciones del 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.

Origen	Descripción
Desde el menú Inicio	Las aplicaciones que se han detectado en una máquina de los grupos de entrega seleccionados. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**. Este origen no se puede seleccionar si usted (1) seleccionó grupos de aplicaciones que no tienen grupos de entrega asociados, (2) seleccionó grupos de aplicaciones con grupos de entrega asociados que no contienen máquinas, o (3) seleccionó un grupo de entrega que no contiene máquinas.
Definidas manualmente	Se trata de 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	Las aplicaciones que fueron previamente agregadas al sitio. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, haga clic en **Aceptar**. Este origen no se puede seleccionar si el sitio contiene ninguna aplicación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App-V	Aplicaciones de paquetes 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**.

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 bien, seleccionar otra carpeta. 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**.

Cómo 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 se pueden seleccionar grupos de entrega que contengan máquinas compartidas que entreguen escritorios, si (1) el grupo de entrega contiene máquinas compartidas y se creó con una versión anterior de XenDesktop 7.x, y (2) usted tiene el permiso de Modificar grupo de entrega. El tipo de grupo de entrega se convierte automáticamente a "escritorios y aplicaciones" cuando se confirma la selección en el diálogo de propiedades.

1. Seleccione **Aplicaciones** en el panel de navegación de Studio y, a continuación, seleccione la aplicación en el panel central.
2. Seleccione **Propiedades** en el panel Acciones.
3. Seleccione la página **Grupos**.
4. Para agregar un grupo, haga clic en la lista desplegable **Agregar** y seleccione **Grupos de aplicaciones** o **Grupos de entrega**. (Si aún no ha creado ningún grupo de aplicaciones, la única entrada que verá será Grupos de entrega). A continuación, seleccione uno o varios grupos disponibles. Los grupos que no son compatibles con la aplicación, o que ya están asociados 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 bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Cómo duplicar, habilitar, inhabilitar, cambiar de nombre o eliminar una aplicación

Uso de estas acciones:

- **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 moverla 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Cómo 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.

Cómo 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.

Cómo 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Propiedad	**Seleccione esta página**
Categoría/carpeta donde aparece la aplicación en Receiver	Entrega
Argumentos de línea de comandos (consulte la sección Transferencia de 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 Configuración de límites para aplicaciones)	Entrega
Nombre: los nombres que ven el usuario y el administrador	Identificación
Ruta al archivo ejecutable (consulte la sección Transferencia de 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 Citrix Receiver (aunque una aplicación sea invisible, se la puede iniciar; para que además de no estar visible, tampoco esté disponible, agréguela a un grupo distinto)	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.

Cómo configurar límites para aplicaciones

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Importante: Esta función limita la cantidad de inicios de aplicaciones que usan como intermediario el Controller (por ejemplo, desde Citrix Receiver o StoreFront), no la cantidad de las aplicaciones 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 dos configuraciones de límite para aplicaciones. Puede definir una o las dos:

- 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.

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.

Ejemplos de uso de los límites para aplicaciones:

- **Límite para la cantidad máxima de instancias simultáneas.** En un grupo de entrega, se configura la cantidad máxima de 15 instancias simultáneas de la aplicación Alfa. Posteriormente, los usuarios de ese grupo de entrega tienen 15 instancias de esa aplicación que se ejecutan al mismo tiempo. Si un usuario de ese grupo de entrega intenta iniciar Alfa, se generará un mensaje de error y Alfa no se iniciará porque eso superaría el límite de instancias simultáneas de aplicación (15).
- **Límite para una instancia de aplicación por usuario.** En otro grupo de entrega, se habilita la opción de una instancia por usuario para la aplicación Beta. El usuario Marcos inicia correctamente la aplicación Beta. Más tarde en la misma jornada, mientras esa aplicación se sigue ejecutando en la sesión de Marcos, este intenta iniciar otra instancia de Beta. Se generará un mensaje de error y Beta no se iniciará porque eso superaría el límite de una instancia por usuario.
- **Límites de cantidad máxima de instancias simultáneas y una instancia de aplicación por usuario.** En otro grupo de entrega, se configura una cantidad máxima de 10 instancias simultáneas y se habilita la opción de una instancia por usuario de la aplicación Delta. Posteriormente, cuando diez usuarios de ese grupo de entrega tienen cada uno una instancia de Delta en ejecución, si otro usuario de ese grupo intenta iniciar Delta, recibirá un mensaje de error y Delta no se iniciará. Si alguno de los diez usuarios actuales intenta iniciar una segunda instancia de esa aplicación, recibirá un mensaje de error y la segunda instancia no se iniciará.

Si también se inician instancias de aplicación sin Controller como broker (por ejemplo, mientras un Controller está en modo de conexión por concesión) 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 límites para aplicaciones:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.(Cuando haya terminado, haga clic en **Aceptar** o **Aplicar**. Si hace clic en **Aceptar**, se aplica el cambio y se cierra el cuadro de diálogo Modificar propiedades de aplicación; si hace clic en **Aplicar**, se aplica el cambio, pero el cuadro de diálogo permanece abierto.)

- 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.
- 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.

Transferencia de 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 el 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:\Archivos de programa\Windows Media Player\mplayer1.exe” “%*”

Cómo 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 otra carpeta cuando cree el grupo de entrega, agregue una aplicación o más tarde.

Tenga en cuenta:

- No se puede eliminar o cambiar el nombre a la carpeta Aplicaciones, pero puede mover todas las aplicaciones que

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Sugerencia: La forma más fácil de mover una carpeta es arrastrarla y colocarla en el sitio correspondiente.
- Para cambiar el nombre de una carpeta, seleccione esa carpeta y, a continuación, seleccione **Cambiar nombre de carpeta** en el panel Acciones. Escriba un nombre.
- Para eliminar una carpeta, seleccione esa carpeta y, a continuación, seleccione **Eliminar carpeta** en el panel Acciones.Si elimina una carpeta que contiene aplicaciones y otras carpetas, esos objetos también se eliminarán. Cuando se elimina una aplicación, se quita la asignación de la misma del grupo de entrega; no se quita la aplicación de la máquina.
- Para mover aplicaciones a una carpeta, seleccione una o varias aplicaciones. A continuación, seleccione **Mover aplicación** en el panel Acciones. Seleccione la carpeta.

También puede colocar las aplicaciones en una carpeta específica (incluso una nueva) en la página **Aplicación** de los asistentes Crear grupo de entrega y Crear grupo de aplicaciones. De forma predeterminada, las aplicaciones agregadas se colocan en la carpeta Aplicaciones; haga clic en **Cambiar** para seleccionar o crear una carpeta.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aplicaciones de la Plataforma universal de Windows

Dec 05, 2017

XenApp y XenDesktop 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 funcionalidades de XenApp y XenDesktop no reciben respaldo o reciben un respaldo limitado cuando se usan aplicaciones universales:

- La asociación de tipo de archivo no está respaldada.
- La funcionalidad de 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 continuación, el sistema operativo actualiza su base de datos de AppX para indicar la aplicación "como instalada" al usuario que la haya iniciado.

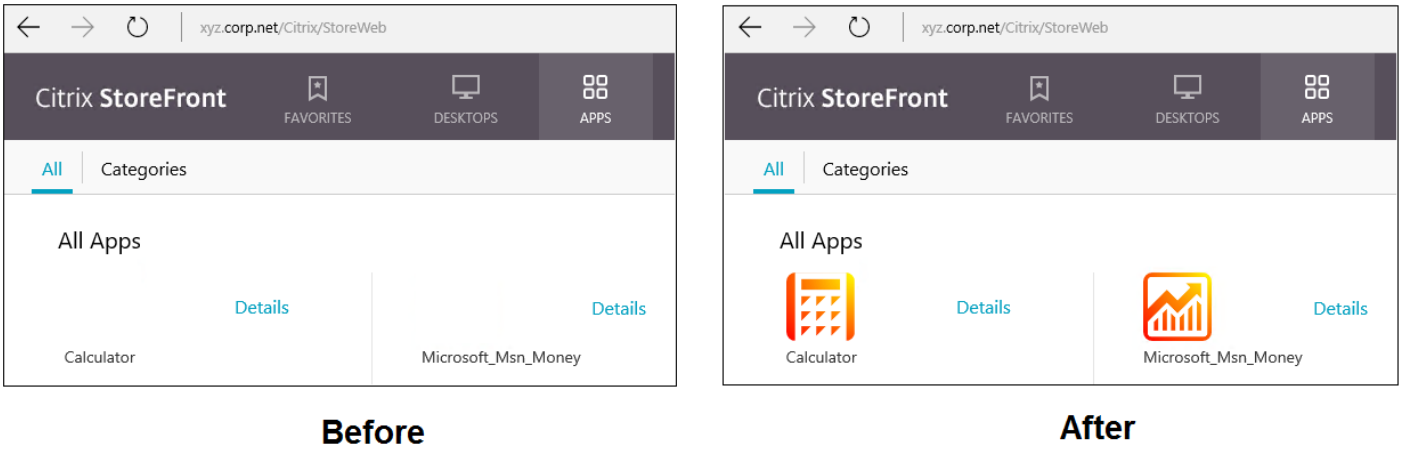
Cerrar correctamente una aplicación universal publicada que se haya iniciado en una ventana integrada o fija podría provocar que la sesión no se cierre y, en cambio, se cierre la sesión del usuario. En tales casos, varios procesos restantes en la sesión impiden que la sesión se cierre correctamente. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Consulte el artículo 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.



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/.

Instalación y publicación de aplicaciones universales

El respaldo para las aplicaciones universales está habilitado de forma predeterminada.

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**.

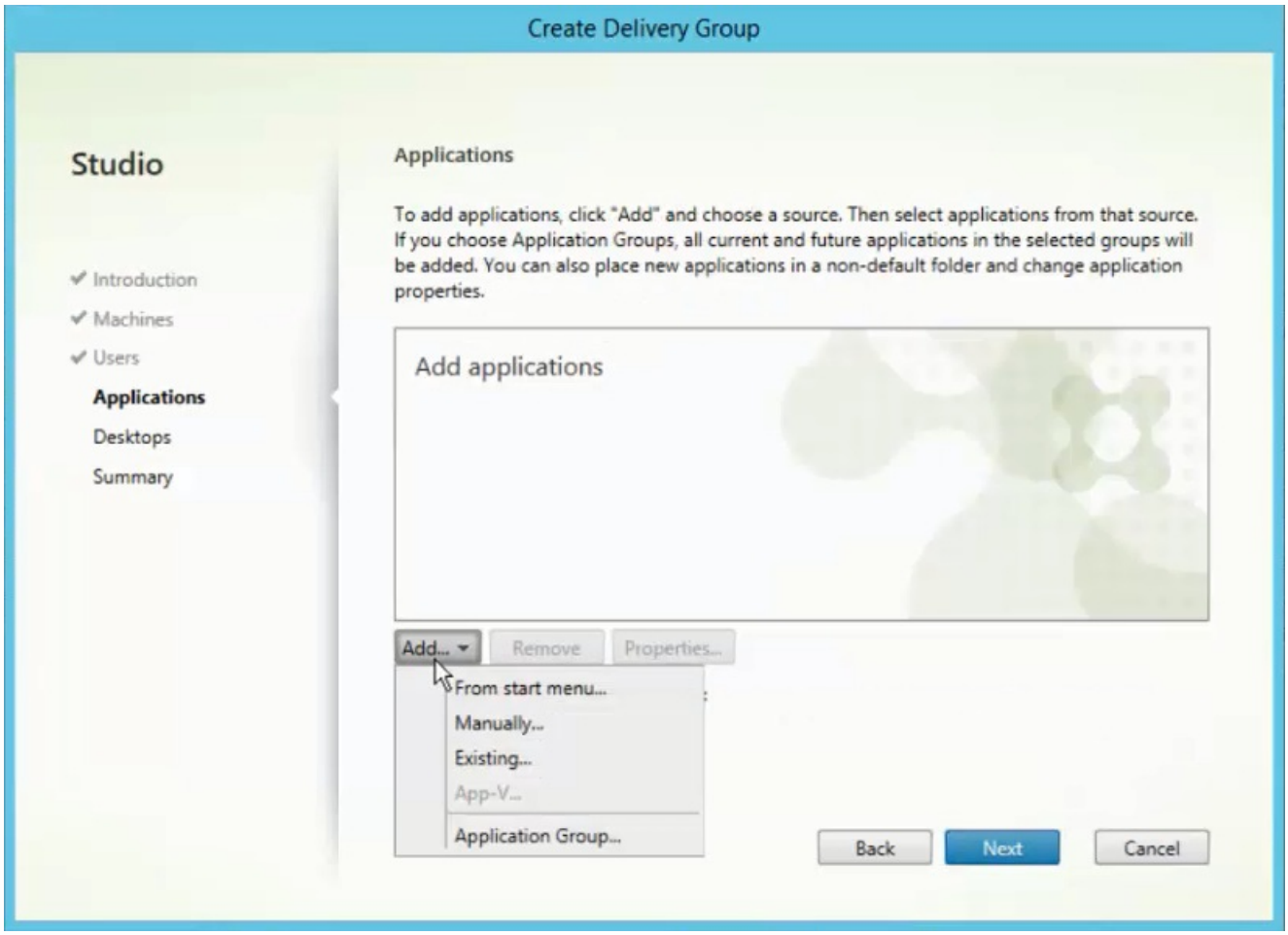
Para instalar una o más aplicaciones universales en agentes VDA (o en una imagen maestra), use uno de los siguientes métodos:

- 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/es-es/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 XenApp o XenDesktop:

> 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" del asistente, seleccione la opción de origen **Desde el menú Inicio**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cuando aparezca la lista de aplicaciones, marque las casillas de las aplicaciones universales que quiera publicar. A continuación, haga clic en **Siguiente**.

Desinstalación de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Zonas

Dec 12, 2017

Las implementaciones que incluyen ubicaciones muy alejadas, conectadas mediante una red WAN, pueden presentar problemas debido a la latencia de la red y la confiabilidad. Existen dos opciones para mitigar esos problemas:

- Implementar varios sitios, cada uno con su propia base de datos SQL Server del sitio.

  Se recomienda esta opción para implementaciones de empresa de gran tamaño. Se trata de varios sitios que se administran por separado, y cada uno necesita su propia base de datos SQL Server del sitio. Cada sitio es una implementación independiente de XenApp.

- 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 de zonas en su sitio de XenDesktop o XenApp a no más de 50 zonas.

  Nota: 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

servidores SQL de alta disponibilidad, si los hay), Studio, Director, Citrix StoreFront, el servidor de licencias Citrix y NetScaler Gateway. La base de datos del sitio debe estar siempre en la zona principal.

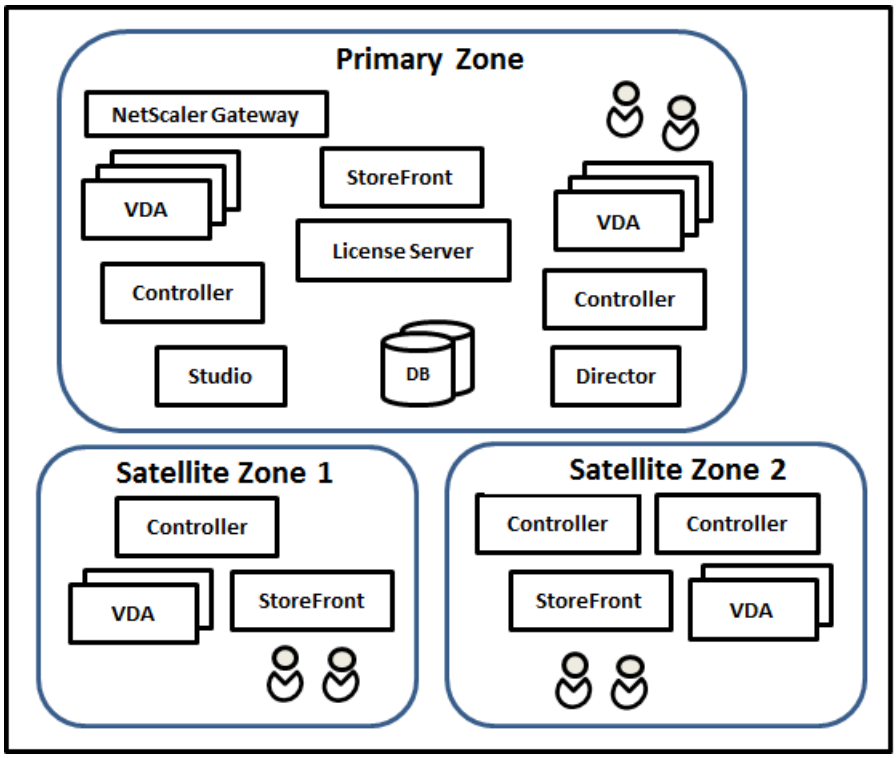
La zona principal también debe tener al menos dos Controllers para la redundancia. Asimismo, puede tener uno o varios VDA con aplicaciones estrechamente ligadas a la base de datos y la infraestructura.

Zona satélite

Una zona satélite contiene uno o varios VDA, Controllers, servidores StoreFront y servidores NetScaler 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.



- La 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 NetScaler Gateway.
- Zona satélite 1. Agentes VDA con Controller

  La zona satélite 1 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si se produce un error en la red WAN, la función de concesión de conexiones 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. Agentes VDA con Controllers redundantes

  La zona satélite 2 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 en los Controllers de la zona a la que se haya movido el catálogo. (Si se mueve un catálogo a una zona mal conectada a la zona actual (por ejemplo, a través de una red de alta latencia o poco ancho de banda), también debe mover cualquier conexión de host asociada a la misma zona.)
- Los Controllers de la zona principal conservan datos de concesión de conexiones para todas las zonas. Los Controllers de las zonas satélite conservan datos de concesión de conexiones de su propia zona y la zona principal, pero no disponen de datos para las demás zonas satélite.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Importante: Para usar la funcionalidad Preferencia de zonas, debe utilizar como mínimo StoreFront 3.7 y NetScaler Gateway 11.0-65.x.

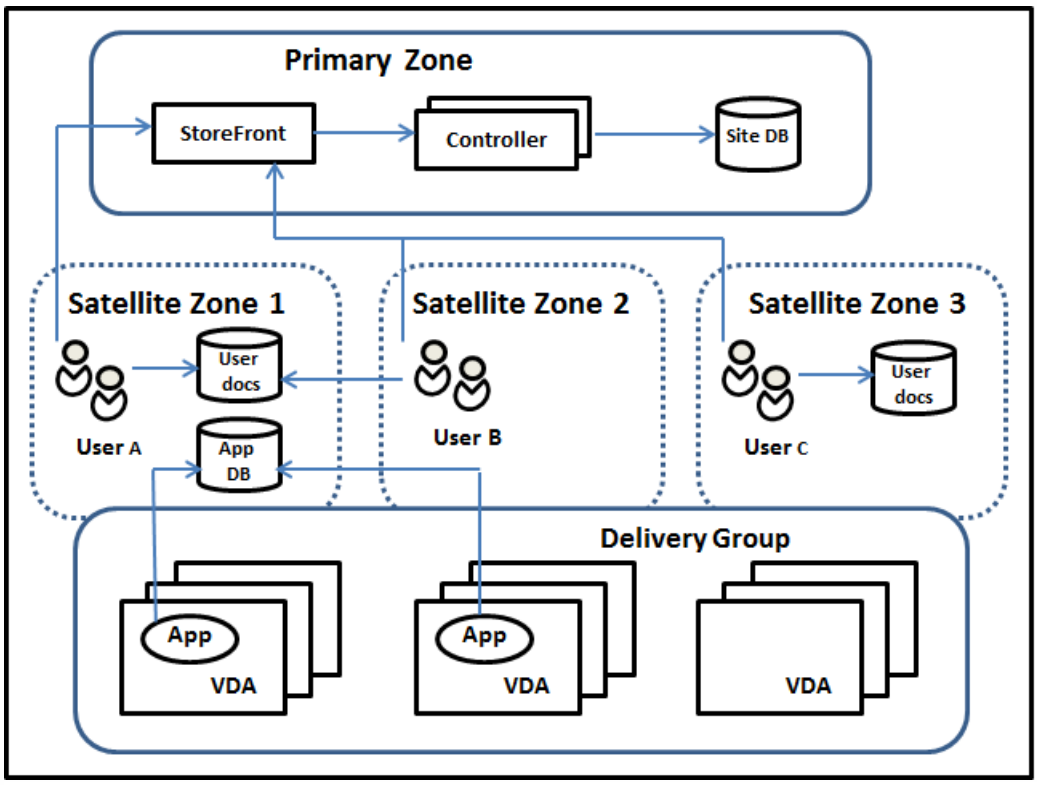
En un sitio de varias zonas, la funcionalidad Preferencia de zonas ofrece más flexibilidad al administrador para controlar qué VDA se utiliza para iniciar una aplicación o un escritorio.

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 Citrix Receiver). Esto se conoce como ubicación del usuario.

En el gráfico siguiente, se muestra un ejemplo de configuración de varias zonas.



En este ejemplo, los VDA están distribuidos en tres zonas satélite, pero pertenecen todos al mismo grupo de entrega. Por lo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

tanto, el intermediario (broker) puede elegir qué VDA usar cuando un usuario lanza una solicitud de inicio. En este ejemplo, se indican varios lugares donde los usuarios pueden ejecutar sus puntos finales de Citrix Receiver: el usuario A usa un dispositivo con Citrix Receiver 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.A usted le corresponde:

- Configurar la zona particular de un usuario agregándolo a una zona.
- Configurar la zona particular de una aplicación modificando las propiedades de esta.

Un usuario o una aplicación pueden tener solo una zona particular en un momento dado. (Puede darse una excepción para los usuarios cuando hay varias pertenencias a zonas porque esos usuarios forman parte de grupos de usuarios; consulte la sección "Otras consideraciones" para resolverla. Sin embargo, incluso en este caso, el broker utiliza una sola zona particular.)

Aunque se puedan configurar las preferencias de zonas para usuarios y aplicaciones, el broker selecciona una sola zona preferida para el inicio.El orden predeterminado de prioridad para seleccionar la zona preferida es: zona particular de la aplicación > zona particular del usuario > ubicación del usuario. (Puede restringir la secuencia siguiendo las indicaciones de la sección siguiente.) 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 Citrix Receiver (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.

Ajustes en 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 Citrix Receiver se está ejecutando), puede indicarlo mediante la preferencia de zona "ubicación del usuario" aunque algunos usuarios tengan otra zona particular.

© 1999-2017 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 NetScaler Gateway a través del que el dispositivo de punto final se conecta detecte Citrix Receiver en ese dispositivo de punto final. El dispositivo NetScaler debe estar configurado para asociar rangos de direcciones IP a zonas concretas, y la identidad de la zona detectada debe transferirse a través de StoreFront al Controller.

Para obtener más información acerca de la preferencia de zona, consulte Preferencia de zonas.

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 a fin de que la conexión entre ambos tenga una latencia baja y alto ancho de banda.
- Colocar elementos en una zona satélite afecta al modo en que el sitio interactúa con ellos y con otros objetos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 puede asociar instancias de NetScaler Gateway con 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 hacerlo como parte de la configuración del sitio de XenApp o XenDesktop. Cuando se asocia un NetScaler Gateway a una zona, se utiliza preferentemente ese NetScaler 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 inicialmente solo un Controller, por lo que puede crear zonas satélite antes o después de crear un catálogo de máquinas y un grupo de entrega.)
- Cuando crea la primera zona satélite con uno o varios elementos, todos los demás elementos de su sitio siguen estando en la zona principal.
- La zona principal se denomina "Principal" de forma predeterminada, y usted puede cambiar ese nombre. Aunque la pantalla de Studio indica cuál es la zona principal, se recomienda usar un nombre de fácil identificación para la zona principal. Puede reasignar la zona principal (es decir, puede convertir otra zona en la zona principal), pero esta debe contener siempre la base de datos del sitio y los servidores de alta disponibilidad.
- La base de datos del sitio debe estar siempre en la zona principal.
- Después de crear una zona, puede mover elementos de una zona a otra. Tenga en cuenta que esta flexibilidad permite llegar a separar elementos que funcionan mejor en cercanía; por ejemplo, mover un catálogo de máquinas a otra zona que la conexión (host) que crea las máquinas del catálogo podría afectar al rendimiento. Por lo tanto, tenga en mente los posibles efectos imprevistos antes de mover elementos entre zonas.Mantenga el catálogo y la conexión de host que éste usa en la misma zona o en zonas bien conectadas (por ejemplo, conectadas a través de una red de baja latencia y alto ancho de banda).
- Para obtener un rendimiento óptimo, instale Studio y Director solo en la zona principal. Si quiere otra instancia de Studio en una zona satélite (por ejemplo, si una zona satélite que contiene Controllers se usa para la conmutación por error en caso de que la zona principal deje de ser accesible), ejecute Studio como una aplicación publicada localmente. Asimismo, puede acceder a Director desde una zona satélite porque se trata de una aplicación Web.
- Preferiblemente, NetScaler 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 funcionalidad Preferencia de zonas, debe utilizar como mínimo StoreFront 3.7 y NetScaler Gateway 11.0-65.x.
- Para obtener información más técnica y consideraciones de rendimiento, consulte Zones Deep Dive.

Límites a la calidad de conexión

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Los Controllers de la zona satélite llevan a cabo interacciones SQL directamente con la base de datos del sitio. Eso impone algunos límites en la calidad del enlace entre la zona satélite y la zona principal que contiene la base de datos del sitio. Los límites concretos dependen de la cantidad de agentes VDA y sesiones de usuario en esos VDA que se implementan en la zona satélite. Por lo tanto, zonas satélite con pocos VDA y pocas sesiones pueden funcionar con una conexión de peor calidad a la base de datos que las zonas satélite que tengan grandes cantidades de agentes VDA y muchas sesiones.

Para obtener más información, consulte Latency and SQL Blocking Query Improvements.

Impacto de latencia en la intermediación de rendimiento

Aunque las zonas permiten a los usuarios estar en los enlaces de mayor latencia, siempre que haya un broker local, la latencia adicional influye inevitablemente en la experiencia del usuario final. Para la mayor parte de las tareas, los usuarios experimentan lentitud provocada por viajes de ida y vuelta entre los Controllers de la zona satélite y la base de datos del sitio.

En el inicio de aplicaciones, se producen demoras extras mientras el proceso de intermediación de sesiones identifica al VDA adecuado al que enviar las solicitudes de inicio de sesión.

Creación y administración de 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 Provisioning Services. La consola Provisioning Services Console 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 zonas satélite. Use el asistente de Studio para crear el catálogo y especificar la zona satélite correspondiente. A continuación, utilice la consola de Provisioning Services para aprovisionar las máquinas de ese catálogo. (Si crea el catálogo mediante el asistente de Provisioning Services, este se colocará en la zona principal y deberá usar Studio para moverlo posteriormente a la zona satélite.)

Creación de 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.

Cambio de nombre o 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

Transferencia de 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.

Eliminación de una zona

Una zona debe estar vacía antes de que se pueda eliminar. No se puede eliminar la zona principal.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio.
2. Seleccione una zona en el panel central.
3. Seleccione **Eliminar zona** en el panel Acciones. Si la zona no está vacía (contiene elementos), se le pedirá que seleccione la zona a la que se moverán los elementos.
4. Confirme la eliminación.

Agregar una zona particular a un usuario

Configurar la zona particular de un usuario también se conoce como *agregar un usuario a una zona*.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio y, a continuación, seleccione una zona en el panel central.
2. Seleccione **Agregar usuarios a la zona** en el panel Acciones.
3. En el cuadro de diálogo **Agregar usuarios a la zona**, haga clic en **Agregar** y, a continuación, seleccione los usuarios y los grupos de usuarios que quiera agregar a la zona. Si especifica usuarios que ya tienen su zona particular, aparecerá un mensaje con dos opciones: **Sí**, que equivale a agregar solo a los usuarios especificados que no tengan ninguna zona particular; **No**, que equivale a volver al diálogo de selección de usuarios.
4. Haga clic en **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Eliminar la zona particular de un usuario

Este procedimiento también se conoce como quitar un usuario de una zona.

1. Seleccione **Configuración > Zonas** en el panel de navegación de Studio y, a continuación, seleccione una zona en el panel central.
2. Seleccione **Quitar usuarios de la zona** en el panel Acciones.
3. En el cuadro de diálogo **Agregar usuarios a la zona**, haga clic en **Quitar** y, a continuación, seleccione los usuarios y los grupos que quiera quitar de la zona. Tenga en cuenta que esta acción solo quita a los usuarios de la zona; esos usuarios siguen formando parte de los grupos de entrega y los grupos de aplicaciones.
4. Confirme la eliminación cuando se le solicite.

Administrar zonas particulares de aplicaciones

Configurar la zona particular de una aplicación también se conoce como agregar una aplicación a una zona. De forma predeterminada, en un entorno de varias zonas, una aplicación no tiene ninguna zona particular.

La zona particular de una aplicación se especifica en las propiedades de la aplicación. Puede configurar las propiedades de una aplicación cuando la agregue a un grupo o más adelante. Para ello, deberá seleccionar la aplicación en Studio y modificar sus propiedades.

- Al crear un grupo de entrega, crear un grupo de aplicaciones o al agregar aplicaciones a grupos existentes, seleccione **Propiedades** en la página **Aplicaciones** del asistente.
- Para cambiar las propiedades de una aplicación después de agregarla, seleccione **Aplicaciones** en el panel de navegación de Studio. Seleccione una aplicación y, a continuación, seleccione **Modificar propiedades de aplicación** en el panel Acciones.

En la página **Zonas** de las propiedades o ajustes de la aplicación:

- Si quiere que la aplicación tenga una zona particular:
  - Marque el botón de opción **Usar la zona seleccionada para determinar donde se inicia esta aplicación** y, a continuación, seleccione la zona de la lista desplegable.
  - Si quiere que la aplicación solo se inicie desde la zona seleccionada (ninguna otra), marque la casilla situada debajo de la selección de zonas.
- Si no quiere que la aplicación tenga una zona particular:
  - Seleccione la opción **No configurar una zona particular para esta aplicación**.
  - Si no quiere que el broker tenga en cuenta ninguna de las zonas de usuario configuradas cuando se inicie esta aplicación, marque la casilla situada bajo el botón de opción. En ese caso, no se utilizará ninguna zona particular de aplicación o usuario para determinar dónde iniciar esta aplicación.

Otras acciones que implican especificar zonas

Cuando se agrega una conexión de host o se crea un catálogo de máquinas (aparte del momento en que se crea un sitio), se puede especificar una zona a la que se asignará el objeto, si ya se ha creado al menos una zona satélite.

En la mayoría de los casos, la zona principal es la opción predeterminada. Si utiliza Machine Creation Services para crear un catálogo de máquinas, se selecciona automáticamente la zona que esté configurada para la conexión de host.

Si el sitio no contiene zonas satélite, se presupone la selección de la zona principal y el cuadro de selección de zonas no aparece.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conexiones y recursos

Dec 05, 2017

En este artículo:

- Introducción
- Dónde encontrar información acerca de los tipos de conexión
- Almacenamiento de host
- Crear una conexión y recursos
- Modificar parámetros de conexión
- Activar o desactivar el modo de mantenimiento de una conexión
- Eliminar una conexión
- Cambiar de nombre o probar una conexión
- Ver detalles de máquinas en una conexión
- Administrar máquinas en una conexión
- Modificar la opción de almacenamiento
- Eliminar, cambiar el nombre o probar recursos
- Usar IntelliCache para conexiones XenServer
- Temporizadores de conexión

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.

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 el artículo 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 XenApp o XenDesktop. 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 Hyper-V

- Artículo Entornos de virtualización de Microsoft System Center Virtual Machine Manager.
- Documentación de Microsoft.

Microsoft Azure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Artículo Entornos de virtualización de Microsoft Azure.
- Documentación de Microsoft.

Administrador de recursos de Azure de Microsoft

- 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.
- 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.

CloudPlatform

- 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.

Citrix XenServer

- Documentación de Citrix XenServer.
- Cuando se crea una conexión, 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.

Nutanix Acropolis

- Artículo Entornos de virtualización de Nutanix.
- Documentación de Nutanix.

VMware

- Artículo Entornos de virtualización de VMware.
- Documentación del producto VMware.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Almacenamiento de host

Cuando se aprovisionan máquinas, los datos se clasifican por tipo:

- Datos de sistema operativo (SO), que incluye las imágenes maestras.
- Datos temporales, que incluyen todos los datos no persistentes escritos en las máquinas aprovisionadas por MCS, archivos de paginación de Windows, datos de los perfiles de usuario y todos los datos que se sincronicen con ShareFile. Estos datos se descartan cada vez que la máquina se reinicia.
- Datos personales guardados en los Personal vDisks.

Si se ofrece un almacenamiento por separado para cada tipo de datos se puede reducir la carga y mejorar el rendimiento de IOPS en cada dispositivo de almacenamiento, lo que hace un uso óptimo de los recursos del host. También habilita el almacenamiento apropiado para los distintos tipos de datos, ya que la persistencia y resistencia son más importantes para algunos tipos de datos que para otros.

El almacenamiento puede ser compartido (ubicado centralmente, separado de los hosts y utilizado por todos los hosts) o local, en un hipervisor. Por ejemplo, el almacenamiento compartido central puede ser uno o varios volúmenes de almacenamiento en clúster de servidores Windows Server 2012 (con o sin almacenamiento conectado), o un dispositivo de un proveedor de almacenamiento. El almacenamiento central también puede ofrecer sus propias optimizaciones, tales como rutas de control del almacenamiento del hipervisor y acceso directo a través de plugins asociados.

El almacenamiento local de los datos temporales evita que haya que atravesar la red para acceder al almacenamiento compartido. 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.

Nota: Si 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 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Consulte el artículo Crear catálogos de máquinas para ver información detallada.

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.

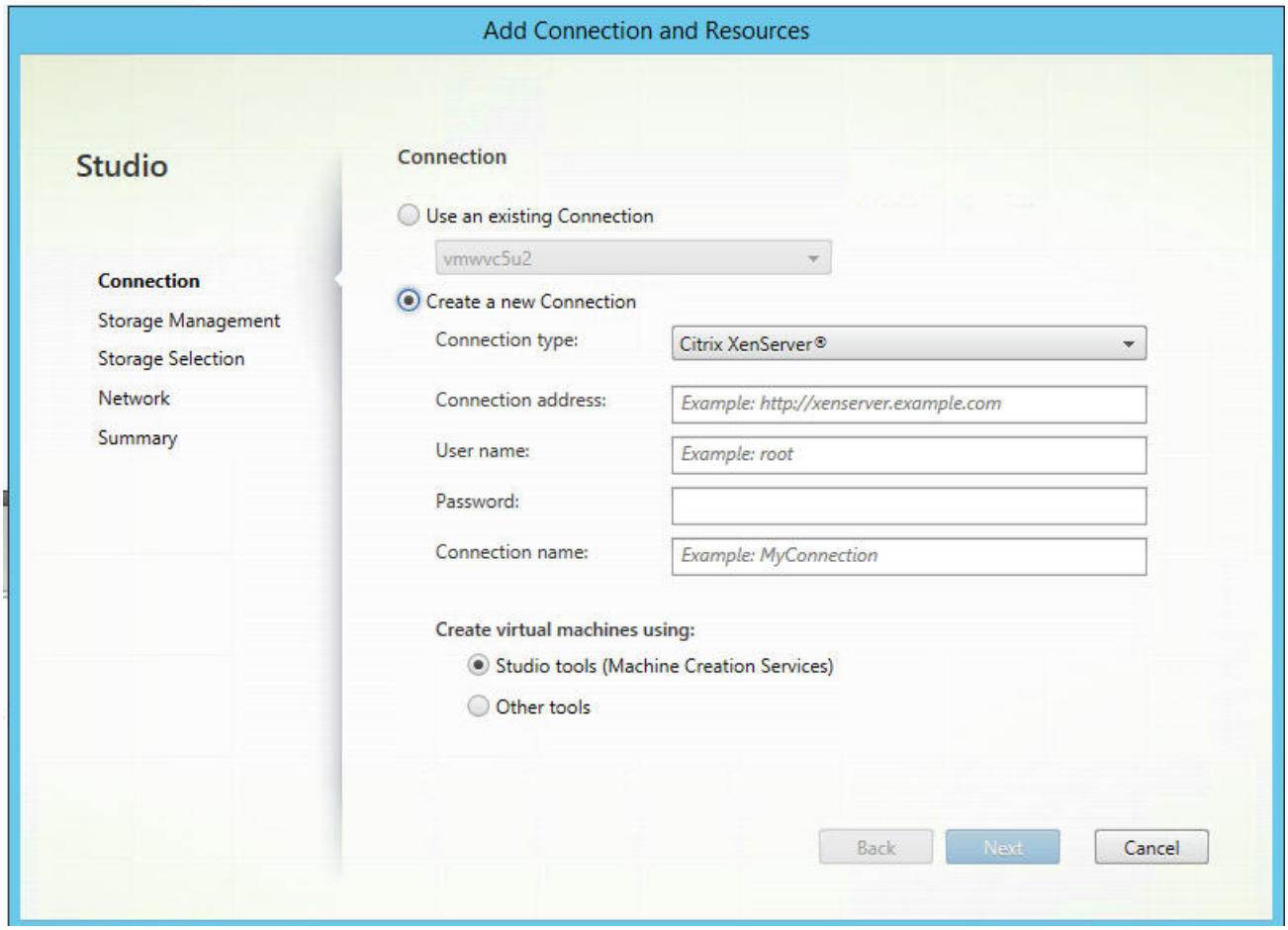
Si crea una conexión después de crear un sitio, empiece en el paso 1.

Importante: Los recursos de host (almacenamiento y red) deben estar disponibles antes de crear la conexión.

- Seleccione **Configuración > Alojamiento** en el panel de navegación de Studio.
- Seleccione **Agregar conexiones y recursos** en el panel Acciones.
- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

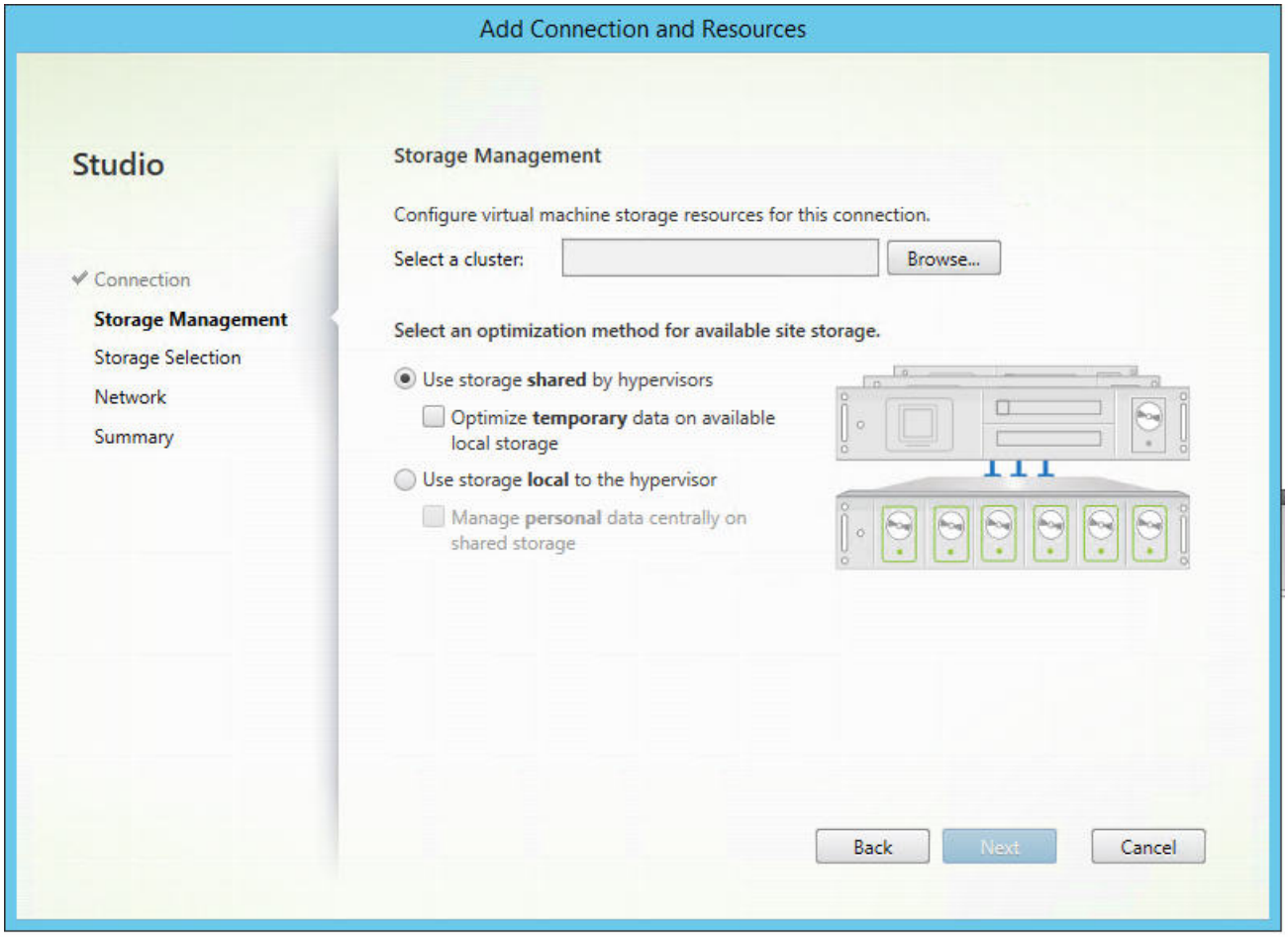


En la página **Conexión**:

- 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 el 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.
- 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 Provisioning Services) u otras herramientas.

Administración del almacenamiento

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para obtener más información sobre los tipos y métodos de administración del almacenamiento, consulte Almacenamiento de host.

Si está configurando una conexión con un host de Hyper-V o VMware, busque y seleccione el nombre del clúster. Otros tipos de conexión no requieren un nombre de clúster.

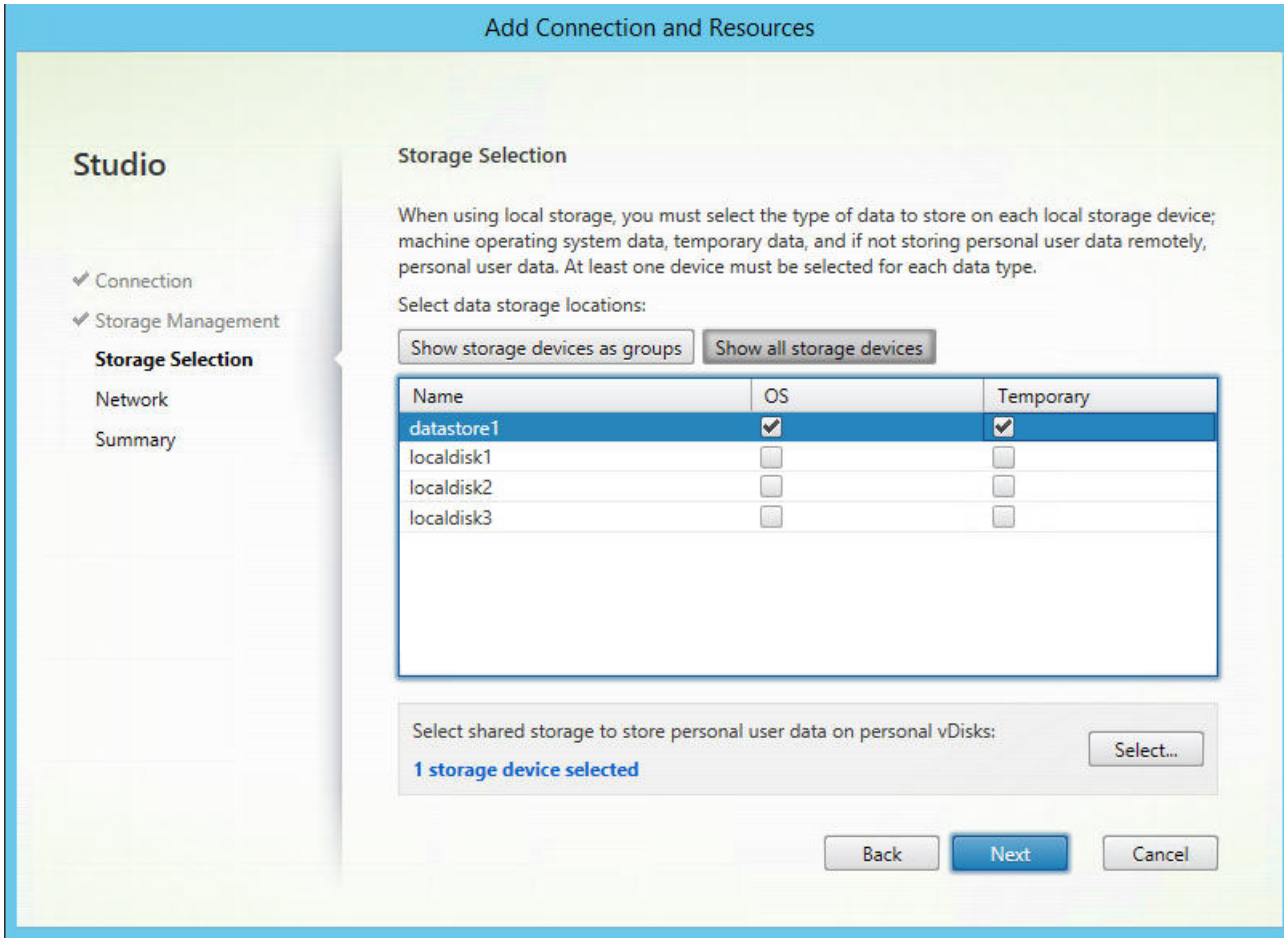
Seleccione un método de administración del almacenamiento: puede ser almacenamiento compartido por los hipervisores o almacenamiento local en cada hipervisor.

- Si elige el almacenamiento compartido por los hipervisores indique si quiere conservar los datos temporales en almacenamiento local disponible. (Puede especificar valores no predeterminados para el tamaño del almacenamiento en los catálogos de máquinas que usen esta conexión.) **Excepción**: Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite crear discos de caché de datos temporales en el almacenamiento local, por lo que el intento de configurar esa administración de almacenamiento en Studio 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

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 en sí (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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de almacenamiento, y haga clic en **Aceptar**.

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

Revise lo que ha seleccionado y si quiere hacer cambios, vuelva a las páginas anteriores del asistente. Una vez revisado, 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 el artículo Crear 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.

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 dejar 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 parámetros** 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

demasiadas o demasiado pocas máquinas al mismo tiempo.Todos los tipos de conexión tienen valores predeterminados concretos que se adecúan a 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.

Nota: Escriba la información en el campo **Opciones de conexión** únicamente con la ayuda de un representante de asistencia técnica de Citrix.

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

- **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 de la máquina que se apague.
- **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, 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**. Quitar una máquina de un grupo de entrega no la elimina del catálogo de máquinas que utiliza el grupo de entrega. 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 conexión 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 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.

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**.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenApp y XenDesktop 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 desde Studio:
  - Seleccione el tipo de almacenamiento **Compartido**.
  - Marque la casilla **Usar IntelliCache**.

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 de un dispositivo de usuario con 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 en ese estado 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Memoria caché del host local

Mar 12, 2018

Para que la base de datos del sitio de XenApp y XenDesktop 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. (En la sección "Bases de datos" del artículo Requisitos del sistema, se ofrece una lista de las funcionalidades de alta disponibilidad de SQL Server que se admiten en XenApp y XenDesktop.) Sin embargo, las interrupciones y los problemas de red pueden tener como resultado que los usuarios no puedan conectarse a sus aplicaciones o escritorios.

La funcionalidad Caché de host local (LHC) permite que las operaciones de intermediación (broker) de las conexiones en un sitio de XenApp o XenDesktop continúen cuando se produce una interrupción. Se produce una interrupción cuando falla la conexión entre un Delivery Controller y la base de datos del sitio.La función Caché de host local se activa cuando no se puede acceder a la base de datos del sitio durante 90 segundos.

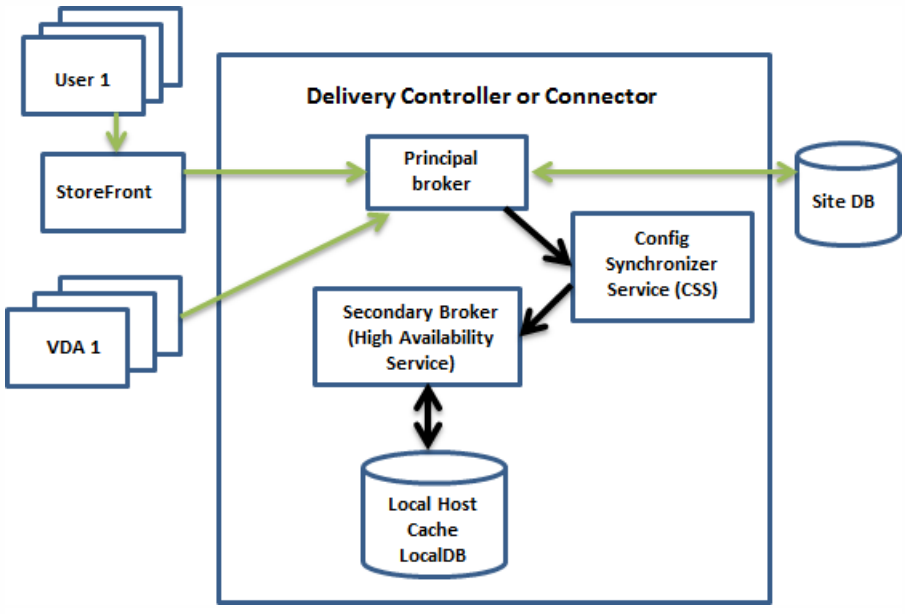
Caché de host local es la funcionalidad más completa que existe para la alta disponibilidad en XenApp y XenDesktop. Es una alternativa más eficaz que la funcionalidad Concesión de conexiones que se introdujo en XenApp 7.6.

Nota: Aunque la concesión de conexiones se admite en la versión 7.15 LTSR, esta funcionalidad se quitará de la siguiente versión.

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; siga leyendo para saber cómo funciona.

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.

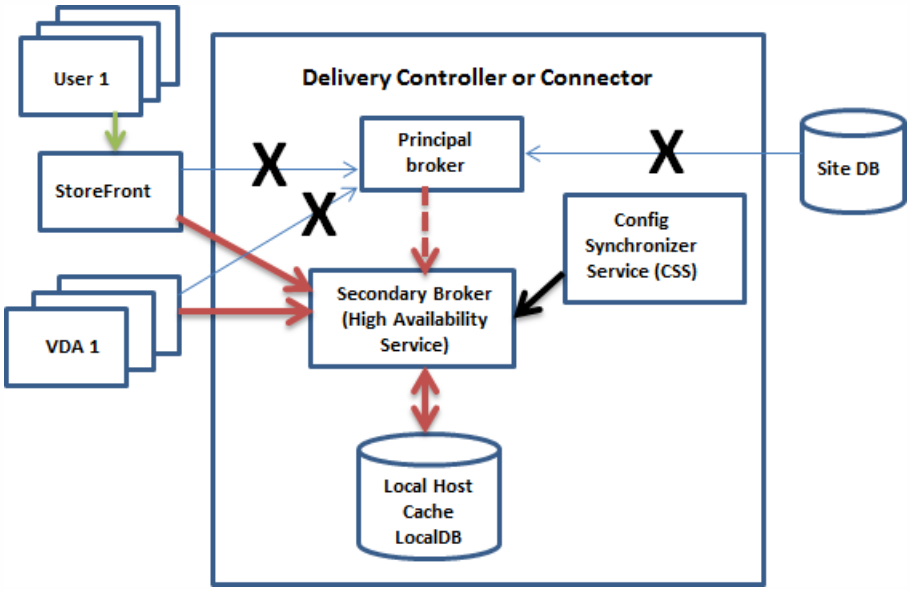


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Durante el funcionamiento normal:

- 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.
- Cada dos minutos, se comprueba 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 realiza un cambio desde la última comprobación, el broker principal usa Citrix Config Synchronizer Service (CSS) para sincronizar (copiar) información a un *broker secundario* (Citrix High Availability Service) en el Controller. Se copian todos los datos de configuración del broker, no solo los elementos que hayan cambiado desde la comprobación anterior. El broker secundario 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 que presenta el broker secundario 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:



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 broker secundario (High Availability Service) que empiece a escuchar y a procesar solicitudes de conexión (marcado con una línea discontinua de color rojo en el gráfico).
- Cuando empieza la interrupción, el broker secundario no dispone de datos actuales de registro de agentes VDA, pero, en cuanto un VDA se comunica con él, comienza un proceso de re-registro. Durante este proceso, el broker secundario también obtiene información de sesión actualizada acerca de ese VDA.
- Mientras el broker secundario gestiona las conexiones, el broker principal sigue supervisando la conexión a la base de datos del sitio. Cuando se restaura la conexión, el broker principal indica al secundario que deje de escuchar para obtener

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 broker secundario 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.

En el caso improbable de que se inicie una interrupción durante una sincronización, la importación de ese momento se descarta y se utiliza la última configuración conocida.

El registro de eventos proporciona información sobre sincronizaciones e interrupciones. 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 broker secundario información sobre todos los Controllers de la zona. (Si su entorno no contiene varias zonas, esta acción afecta a todos los Controllers del sitio.) Con esta información, cada broker secundario obtiene datos de todos los demás brokers secundarios de su nivel.

Los brokers secundarios 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 broker secundario 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 broker secundario que se haya elegido. Los brokers secundarios 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 broker secundario elegido falla durante una interrupción, se elegirá otro broker secundario para que le releve, y los VDA volverán a registrarse en el broker secundario que acaba de elegirse.

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

La función Caché de host local se admite para aplicaciones y escritorios alojados en servidores y escritorios estáticos (asignados). En cambio, no se admite para escritorios VDI agrupados (creados por Machine Creation Services o Provisioning Services).

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cambios o elementos no disponibles durante una interrupción

- 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 broker (secundario) actualmente activo o elegido. Durante una interrupción, no se admiten inicios entre zonas (desde un broker de una zona en un VDA de otra zona).

De forma predeterminada, los escritorios VDA con la energía administrada que formaran parte de grupos de entrega agrupados que tuvieran habilitada la propiedad "ShutdownDesktopsAfterUse" se colocaban en el modo de mantenimiento cuando ocurría 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 "<nombre>" -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.

Tamaño de la 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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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, el intermediario (broker) debe tener suficiente espacio en la unidad donde está instalada LocalDB para permitir el cambio de 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 varias cientos de miles de lecturas.

Rendimiento

Durante una interrupción, un solo broker se encarga de todas las conexiones, por lo que, en los sitios (o las zonas) con carga equilibrada entre varios Controllers durante el funcionamiento normal, es posible que el broker 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 broker del sitio (zona) debe ser capaz de gestionar la carga adicional que impone LocalDB y todos los VDA afectados porque el broker 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 broker, este puede no disponer de información completa sobre las sesiones actuales. Por lo tanto, si un usuario solicita conectarse durante ese intervalo, puede que se cree una nueva sesión aunque la reconexión a una sesión existente fuera posible. Este intervalo (mientras el nuevo "broker" 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 en otro broker:

- Comienza una interrupción: Al migrar desde un broker principal a un broker secundario.
- Error de broker durante una interrupción: Al migrar desde un broker secundario en que se produjo un error a otro broker secundario que acaba de elegirse.
- Recuperación de una interrupción: Cuando se reanudan las operaciones normales y el broker principal retoma el control.

Puede reducir el intervalo si disminuye el valor de Registro HeartbeatPeriodMs del protocolo del broker de Citrix (el valor

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
```

El intervalo no se puede eliminar por completo, independientemente de lo rápido que se registren los VDA.

El tiempo que tarda la sincronización entre brokers aumenta con la cantidad de objetos (como agentes VDA, aplicaciones, grupos). Por ejemplo, sincronizar 5000 VDA podría llevar diez minutos o más. Consulte la siguiente sección "Supervisión" para obtener información sobre las entradas de sincronización en el registro de eventos.

Administración de la Caché de host local

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. Solo el broker secundario se comunica con esta base de datos; no puede usar cmdlets de PowerShell para cambiar nada en esta base de datos. La LocalDB no se puede compartir entre los Controllers.

La base de datos LocalDB de SQL Server Express se instala independientemente de si la Caché de host local está habilitada.

> Para impedir la instalación, instale o actualice el Controller con el comando XenDesktopServerSetup.exe e incluya la opción /exclude "Local Host Cache Storage (LocalDB)". No obstante, tenga en cuenta que la funcionalidad Caché de host local no funcionará sin la base de datos, y no se puede usar otra base de datos con el broker secundario.

Nota: Instalar esta base de datos LocalDB no influye en si instala SQL Server Express para usarla como la base de datos del sitio.

Parámetros predeterminados después de la instalación y la actualización de XenApp o XenDesktop

Durante una nueva instalación de XenApp y XenDesktop, la caché de host local está habilitada de forma predeterminada. (En cambio, la función de concesión de conexiones está inhabilitada de forma predeterminada.)

Después de una actualización, no se modifica la configuración de la caché de host local. Por ejemplo, si la caché de host local estaba habilitada en la versión anterior, permanece habilitada en la versión actualizada. En cambio, si la caché de host local estaba inhabilitada (o no se admitía) en la versión anterior, permanece inhabilitada en la versión actualizada.

Habilitar o inhabilitar la Caché de host local

Para habilitar la Caché de host local, escriba:

```
Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled $false
```

Este cmdlet también inhabilita la funcionalidad Concesión de conexiones. No habilite la Caché de host local y la Concesión de conexiones a la vez.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para saber si la Caché de host local está habilitada, escriba:

Get-BrokerSite

Compruebe que la propiedad LocalHostCacheEnabled es True, y la propiedad ConnectionLeasingEnabled es False.

Para inhabilitar la Caché de host local (y habilitar la Concesión de conexiones), escriba:

Set-BrokerSite -LocalHostCacheEnabled $false -ConnectionLeasingEnabled $true

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.)
- En caso de Citrix Cloud, el conector entra en modo de interrupción independientemente del estado de la conexión al plano de control o la zona principal.

Supervisión

Los registros de eventos indican cuándo tienen lugar las sincronizaciones y las interrupciones.

Config Synchronizer Service (Servicio de sincronización de configuraciones)

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 (broker secundario).

- 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.

High Availability Service (Servicio de alta disponibilidad)

- 3502: Se ha producido una interrupción y el broker secundario (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 broker secundario elegido, además de otros brokers que hayan participado en la elección.

Solución de problemas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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\CitrixBrokerConfigSyncReport.htmll

Una vez generado el informe, inhabilite la funcionalidad de informes:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTraceMode -Value 0
```

Exportar la configuración de broker: Proporciona la configuración exacta con fines de depuración.

```
Export-BrokerConfiguration | Out-File < ruta y nombre del archivo>
```

Por ejemplo, Export-BrokerConfiguration | Out-File C:\BrokerConfig.xml.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Concesión de conexiones

Dec 05, 2017

Importante: La Caché de host local (LHC) es la solución de alta disponibilidad que se prefiere en XenApp y XenDesktop, en lugar de la Concesión de conexiones.Para obtener más información, consulte Caché de host local.

- En esta versión, durante una nueva instalación de XenApp y XenDesktop, la concesión de conexiones se inhabilita de forma predeterminada.
- La concesión de conexiones ya no se ofrecerá a partir de la versión siguiente a esta versión XenApp y XenDesktop 7.15 Long Term Service Release.

Para que la base de datos del sitio esté siempre disponible, Citrix recomienda empezar con una implementación de SQL Server con tolerancia a fallos, resultado de las prácticas recomendadas para la alta disponibilidad de Microsoft. Sin embargo, las interrupciones y los problemas de red pueden impedir que los Delivery Controllers accedan a la base de datos, lo que provoca que los usuarios no puedan conectarse al escritorio o a las aplicaciones.

La función Concesión de conexiones 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.

Aunque los usuarios tengan una gran cantidad de recursos publicados a su disposición, suelen usar solo algunos de ellos con regularidad. Cuando se habilita la concesión de conexiones, cada Controller almacena en caché las conexiones de usuario a las aplicaciones y los escritorios usados recientemente durante las operaciones habituales (cuando la base de datos está disponible).

Las concesiones generadas en cada Controller se cargan a la base de datos del sitio para una sincronización periódica con otros Controllers del sitio. Además de las concesiones, la memoria caché de cada Controller guarda la información relativa a aplicaciones, escritorios, iconos y máquinas de trabajo. La concesión y su información relacionada se guardan en el disco local de cada Controller. Si la base de datos deja de estar disponible, el Controller entra en modo de conexión por concesión y "reproduce" las operaciones guardadas en caché cuando un usuario intenta conectarse o volver a conectarse a un escritorio o aplicación usados recientemente en StoreFront.

Las conexiones se almacenan en caché durante un período de concesión de dos semanas. De esta manera, si la base de datos deja de estar disponible, los escritorios y las aplicaciones que un usuario haya iniciado en las dos semanas previas seguirán siendo accesibles para ese usuario a través de StoreFront. Por el contrario, los escritorios y las aplicaciones que no se hayan iniciado antes de las dos semanas del período de concesión no están accesibles cuando la base de datos no está disponible. Por ejemplo: si una aplicación se inició por última vez hace tres semanas, su período de concesión ha concluido y el usuario no podrá iniciar la aplicación si la base de datos no se encuentra disponible en ese momento. Los períodos de concesión para sesiones de aplicaciones o escritorios desconectados o activos durante mucho tiempo se extienden para que no se consideren concluidos.

De forma predeterminada, la concesión de conexiones afecta a todo el sitio. No obstante, puede revocar todas las concesiones para usuarios concretos, lo que les impide acceder a las aplicaciones o los escritorios cuando el Controller se encuentra en modo de conexión por concesión. La aplicación de otros parámetros de registro se rige por el Controller.

Consideraciones y limitaciones

Si bien la función de concesión de conexiones puede mejorar la resistencia de conexión y la productividad del usuario, existen aspectos a tener en cuenta relacionados con la disponibilidad, el funcionamiento y el rendimiento de otras

© 1999-2017 Citrix Systems, Inc. All rights reserved.

funciones.

La función de concesión de conexiones se admite en casos de escritorios y aplicaciones alojados en servidor, y escritorios estáticos (asignados). No se admite en caso de escritorios VDI agrupados o usuarios a los que no se ha asignado ningún escritorio cuando la base de datos deja de estar disponible.

Cuando el Controller está en modo de conexión por concesión:

- Los administradores no pueden usar Studio, Director, o la consola de PowerShell.
- El control del espacio de trabajo no está disponible. Cuando un usuario inicia sesión en Citrix Receiver, las sesiones no se reconectan automáticamente; el usuario debe volver a iniciar la aplicación.
- Si se crea una nueva concesión inmediatamente antes de que la base de datos deje de estar disponible, pero la información de concesión todavía no se ha sincronizado en todos los Controllers, es posible que el usuario no pueda abrir ese recurso una vez que la base de datos deje de estar disponible.
- Los usuarios de aplicaciones y escritorios alojados en servidor pueden usar más sesiones que la cantidad establecida en el límite configurado de sesiones. Por ejemplo:
  - Es posible que la sesión que un usuario inicie desde un dispositivo (conectado de forma externa a través de NetScaler Gateway) con un Controller que no está en modo de conexión por concesión no esté disponible cuando ese usuario se conecte desde otro dispositivo en la red LAN con un Controller que sí está en modo de conexión por concesión.
  - Si se inicia una aplicación justo antes de que la base de datos deje de estar disponible, es posible que la reconexión de la sesión falle. En estos casos, se inicia una nueva sesión y una nueva instancia de aplicación.
- No se administra la energía de escritorios estáticos (asignados). Los VDA que están apagados cuando el Controller entra en modo de conexión por concesión permanecen no disponibles hasta que se restaure la conexión de la base de datos, a menos que el administrador los encienda de forma manual.
- Si las funciones de preinicio de sesiones y persistencia de sesiones están habilitadas, no se inician nuevas sesiones preiniciadas. Mientras la base de datos no esté disponible, las sesiones preiniciadas y las persistentes no se finalizarán en función de los umbrales configurados.
- La administración de carga del sitio puede verse afectada. Las conexiones basadas en servidor se enrutan al último VDA usado. Es posible que se superen los patrones de carga (especialmente, las reglas de recuento de sesiones).
- Controller no entra en modo de concesión de conexiones si se usa SQL Server Management Studio para desconectar la base de datos. En su lugar, use una de las siguientes instrucciones Transact-SQL:
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>

  Cualquiera de estas instrucciones cancela todas las transacciones pendientes y hace que el Controller pierda la conexión con la base de datos. El Controller, a continuación, entra en modo de concesión de conexiones.

Cuando la función de concesión de conexiones está habilitada, hay dos breves intervalos en que los usuarios no pueden conectarse o volver a conectarse: (1) desde el momento en que la base de datos deja de estar disponible hasta el momento en que el Controller entra en modo de conexión por concesión, y (2) desde el momento en que el Controller cambia del modo de conexión por concesión hasta el momento en que el acceso a la base de datos está totalmente restaurado y los VDA se han vuelto a registrar.

Si define un valor personalizado de movilidad de sesión, la reconexión de la sesión vuelve a su valor predeterminado cuando un Controller entra en el modo de conexión por concesión. Para obtener más información, consulte Concesión de conexiones y movilidad de sesión.

Consulte el artículo Zonas para obtener información sobre dónde se guardan los datos de la concesión de conexiones.

Para obtener más información, consulte XenDesktop 7.6 Connection Leasing Design Considerations.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración e implementación

A la hora de configurar una implementación para admitir la concesión de conexiones:

- Los VDA deben ser como mínimo de la versión 7.6. Además, los catálogos de máquinas y los grupos de entrega que utilizan esas máquinas deben estar en ese nivel mínimo (o una versión posterior respaldada).
- Van a aumentar los requisitos de tamaño de la base de datos del sitio.
- Cada Controller necesita más espacio en disco para los archivos de concesión guardados en caché.

Puede activar o desactivar la función de concesión de conexiones desde el SDK de PowerShell o el Registro de Windows. Desde el SDK de PowerShell, también se pueden quitar las concesiones actuales. Los siguientes cmdlets de PowerShell afectan a la concesión de conexiones; consulte la ayuda del cmdlet para obtener más detalles.

- Set-BrokerSite -ConnectionLeasingEnabled $true | $false: Activa o desactiva la concesión de conexiones. De forma predeterminada = $true.
- Get-BrokerServiceAddedCapability: Devuelve “ConnectionLeasing” para el Controller local.
- Get-BrokerLease: Obtiene todas las concesiones actuales o un conjunto filtrado de ellas.
- Remove-BrokerLease: Marca una concesión, o un grupo filtrado de concesiones, para eliminarlas.
- Update-BrokerLocalLeaseCache. Actualiza la memoria caché de la concesión de conexiones en el Controller local. Los datos se vuelven a sincronizar durante la próxima operación de sincronización.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

IP virtual y bucle invertido virtual

Dec 05, 2017

Nota: Esas características solo son válidas para máquinas de servidor Windows compatibles. 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 XenApp, 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 XenApp del mismo modo que acceden a cualquier otra aplicación publicada. Un proceso requiere IP virtual en cualquiera de los siguientes casos:

- El proceso utiliza un número de puerto TCP integrado en el código.
- El proceso utiliza Windows Sockets y requiere una dirección IP exclusiva o un número de puerto TCP específico.

Para determinar si una aplicación necesita utilizar direcciones IP virtuales:

1. Obtenga la herramienta TCPView de Microsoft. Esta herramienta muestra todas las aplicaciones que enlazan puertos y direcciones IP específicas.
2. Inhabilite la función de resolución de direcciones IP, de forma que vea las direcciones en lugar de los nombres de host.
3. Ejecute la aplicación y, con ayuda de TCPView, puede ver las direcciones IP y los puertos que abre la aplicación y los nombres de los procesos que abren esos puertos.
4. Configure los procesos que abren la dirección IP del servidor, 0.0.0.0 ó 127.0.0.1.
5. Para que ninguna aplicación abra 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

obtener instrucciones.

- Después de habilitar la función, al comenzar una sesión, el servidor solicita al servidor DHCP las direcciones IP asignadas dinámicamente.
- La función Virtualización de IP de Escritorio remoto asigna direcciones IP a las conexiones a escritorios remotos por sesión o por programa. Si asigna direcciones IP a varios programas, estos compartirán 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 por parte de la aplicación de escuchar comunicaciones TCP o UDP se vincula inmediatamente a su dirección IP virtual asignada (o dirección de bucle invertido) y cualquier conexión de origen abierta por la aplicación se origina desde la dirección IP vinculada a la aplicación.

En funciones que devuelven una dirección (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 (como bind o connect).

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 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 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, 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 (127.0.0.1) en una invocación de Winsock, la función de bucle virtual solo sustituye 127.0.0.1 por 127.X.X.X, donde X.X.X es la 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.
- 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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:
- El bucle invertido preferido solo se admite en Windows Server 2008 R2 y Windows Server 2012 R2.
- Utilice el bucle invertido preferido solo cuando tanto IP virtual como Bucle invertido virtual están habilitados; en caso contrario, podría obtener resultados inesperados.
- Si edita 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Ejecute regedit en los servidores donde residen las aplicaciones.
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VIP para máquinas de 32 bits)
- Nombre: PreferLoopback, Tipo: REG_DWORD, Datos: 1
- Nombre: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Datos: <list of processes>

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Delivery Controllers

Dec 05, 2017

Delivery Controller es el componente de servidor que es responsable de la administración del acceso de los usuarios, además de la intermediación y optimización de las conexiones. Los Controllers también proporcionan los Machine Creation Services que crean imágenes de escritorio y servidor.

Un sitio debe tener al menos un Controller. Después de instalar el primer Controller, se pueden agregar más al crear un sitio o más adelante. Tener más de un Controller en un sitio ofrece dos ventajas principales.

- Redundancia. Se recomienda que un sitio de producción siempre tenga al menos dos Controllers en diferentes servidores físicos. De este modo, si falla un Controller, los demás pueden gestionar las conexiones y administrar el sitio.
- Escalabilidad. A medida que aumenta la actividad de un sitio, también aumenta el uso de CPU en el Controller y la actividad de la base de datos. Los Controllers adicionales 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.

(En la documentación de las versiones anteriores de XenApp y XenDesktop 7.x, la información sobre el registro de agentes VDA se incluía en este artículo. Esa información se ha mejorado y ahora se encuentra en el enlace anterior.)

Cómo 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*.

Nota: No se respalda 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 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 programa de instalación 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.**Importante:** 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.
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Mover un VDA a otro sitio

Si un VDA se aprovisionó mediante Provisioning Services 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 programa de instalación o mediante directivas de Citrix.

Programa de instalación: Ejecute el programa de instalación y agregue un Controller, especificando el FQDN (entrada DNS) de un Controller en el sitio 2. **Importante:** Especifique los Controllers en el programa de instalación solo si la configuración de directiva de Controllers no se utiliza.

Editor de directivas de grupo: En el siguiente ejemplo se mueven varios VDA entre sitios.

1. Cree una directiva en el Sitio 1 que contenga la siguiente configuración y, a continuación, filtre la directiva al nivel de grupo de entrega para iniciar una migración de VDA entre sitios, por fases.
   Controllers. Contiene los nombres de dominio completo o FQDN (entradas de DNS) de uno o más Controllers del sitio 2.
   Habilitar actualización automática de Controller. Defínala como inhabilitada.
2. Cada VDA en el grupo de entrega recibe un aviso sobre la nueva directiva en los siguientes 90 minutos. El VDA ignora la lista de Controllers que recibe (porque la actualización automática está inhabilitada). 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Registro de VDA

Jan 02, 2018

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 XenApp y XenDesktop, los VDA se registran en los Controllers. En una implementación de XenApp y XenDesktop Service, los VDA se registran en Cloud Connectors.) El VDA busca un Controller o un Connector en una lista llamada ListofDDCs. En un VDA, la lista ListOfDDCs consta de entradas DNS que le indican los Controllers o Cloud Connectors del sitio. Para conseguir un equilibrio de carga, el VDA distribuye automáticamente las conexiones entre todos los Controllers o Cloud Connectors de la lista.

¿Por qué es tan importante que el VDA se registre?

- Desde el punto de vista de la seguridad, el registro es una operación confidencial: se establece una conexión entre el Delivery 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* a continuación.

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.

XenApp y XenDesktop 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

El administrador es quien selecciona el método de configuración a utilizar cuando el VDA se registra por primera vez. Esto se denomina registro inicial. Durante ese registro inicial, se crea una memoria caché persistente en el VDA. Durante los registros subsiguientes, el VDA obtiene la lista de Controllers o Cloud Connectors desde esa memoria caché local, a menos que se detecte un cambio de configuración.

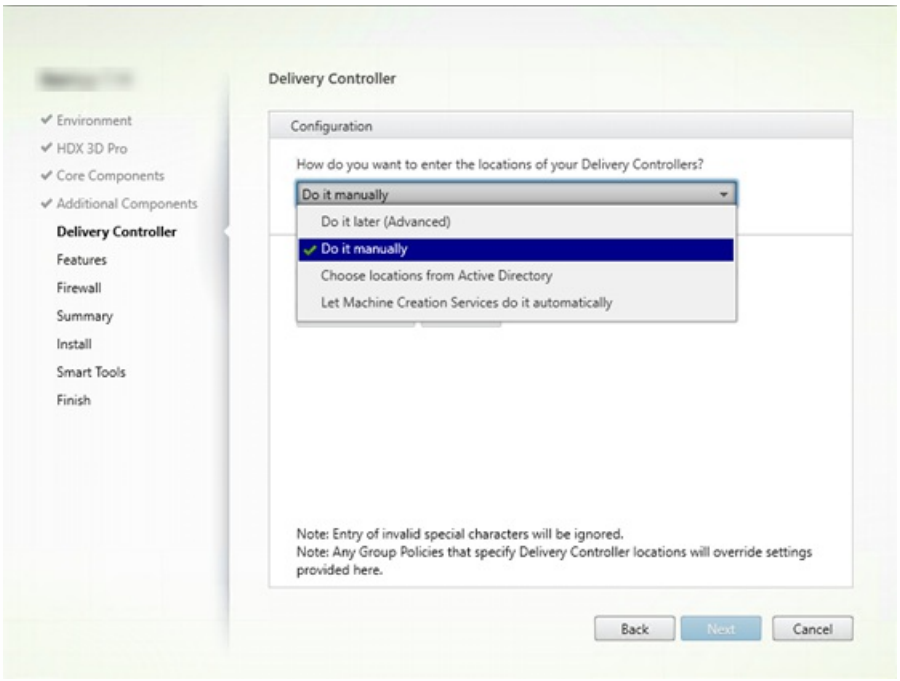
La forma más fácil de recuperar esa lista en los registros subsiguientes es mediante la función de actualización automática. De forma predeterminada, la actualización automática está habilitada. Para obtener más información, consulte Actualización automática.

Existen varios métodos para configurar direcciones de Controller o Cloud Connector en un VDA.

- Método basado en directivas (LGPO o GPO)
- Método basado en el Registro (manual, GPP, direcciones especificadas durante la instalación de VDA)
- Método basado en unidades organizativas de Active Directory (detección de OU antiguas)
- Método basado en MCS (personality.ini)

El método de registro inicial se indica cuando se instala un VDA. (Si se inhabilita la actualización automática, el método seleccionado durante la instalación del VDA también se utilizará para los registros posteriores.)

En la siguiente imagen, se muestra la página **Delivery Controller** del Asistente de instalación de VDA.



Método basado en directivas (LGPO o GPO)

Citrix recomienda usar GPO para el registro inicial del VDA. Tiene la prioridad más alta. (Aunque la actualización automática se haya indicado como la máxima prioridad, solo se usa después del registro inicial.) El registro basado en directivas ofrece las ventajas de las directivas de grupo centralizadas para la configuración.

Para especificar este método, complete los dos siguientes pasos:

- En la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Hacerlo más tarde (Avanzado)**. El asistente le recordará varias veces que indique direcciones de Controller, incluso aunque no las indique durante la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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).

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* a continuación):

HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)

Recuerde: Si habilita también el registro de VDA basado en directivas mediante la directiva de Citrix, esta configuración sobrescribe los parámetros especificados durante la instalación de VDA, porque es un método de mayor prioridad.

Método basado en unidades organizativas de Active Directory (antiguo)

Este no es el método recomendado; se admite principalmente para la compatibilidad con versiones anteriores. Si aún lo utiliza, Citrix recomienda cambiar a otro método.

Para especificar este método, complete los dos siguientes pasos:

- En la página **Delivery Controller** del Asistente de instalación de VDA, seleccione **Elegir ubicaciones desde Active Directory.**
- Use el script Set-ADControllerDiscovery.ps1 (disponible en cada Controller). Además, configure la entrada del registro

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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 PVS para aprovisionar las máquinas, salvo para la caché del servidor PVS (que no es un caso frecuente porque no hay almacenamiento persistente para la caché de actualización automática).

Para especificar este método:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

Por ejemplo:

- Una implementación contiene tres Controllers: A, B y C. Un VDA se registra en el Controller B (el cual se especificó durante la instalación del VDA).
- Más tarde, dos Controllers (D y E) se agregan al sitio. En los 90 minutos siguientes, los VDA reciben listas actualizadas y aceptan conexiones provenientes de los Controllers A, B, C, D y E. (La carga no se reparte equitativamente entre todos los Controllers hasta que se reinicien los VDA.)
- Posteriormente, se traslada al Controller B a otro sitio. En los 90 minutos siguientes, los VDA del sitio original reciben listas actualizadas porque se ha producido un cambio de Controllers desde la última comprobación. El VDA que se registró en su momento en el Controller B (que ya no está en la lista) vuelve a registrarse y elige entre los Controllers de la lista actual (A, C, D y E).

En una implementación de varias zonas, la actualización automática de una zona satélite almacena automáticamente en caché primero todos los Controllers locales. Todos los Controllers de la zona principal se almacenan en caché en un grupo de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

MODIFIQUE ESTE ARCHIVO. Cualquier modificación en este archivo o carpeta resulta en una configuración no respaldada.

```
Get-WmiObject -Namespace “Root\Citrix\DesktopInformation”
-Class “Citrix_VirtualDesktopInfo” -Property “PersistentDataLocation”
```

Si necesita configurar manualmente la lista ListOfSIDs por razones de seguridad (a diferencia de motivos como la reducción de carga de Active Directory), no puede usar la función de actualización automática. Para obtener más información, consulte *ListOfSIDs* a continuación.

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 de configuración

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 un equilibrador de carga de red como, por ejemplo, NetScaler. 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" 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:

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Introducción a Kerberos: https://blogs.technet.microsoft.com/askds/2008/03/06/kerberos-for-the-busy-admin/

Autenticación mutua con Kerberos: https://msdn.microsoft.com/en-us/library/ms677600

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.

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).

ListOfSIDs

La lista de Controllers con los que un VDA puede contactar para el registro se llama ListOfDDCs. Asimismo, un VDA también debe saber en qué Controllers puede confiar; los VDA no confían automáticamente en los Controllers de la lista ListOfDDCs. La lista ListOfSIDs (identificadores de seguridad) identifica a los Controllers de confianza. Los agentes VDA solo intentarán registrarse en los Controllers de confianza.

En la mayoría de los entornos, la lista ListOfSIDs se genera automáticamente a partir de la lista ListOfDDCs. Puede 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.

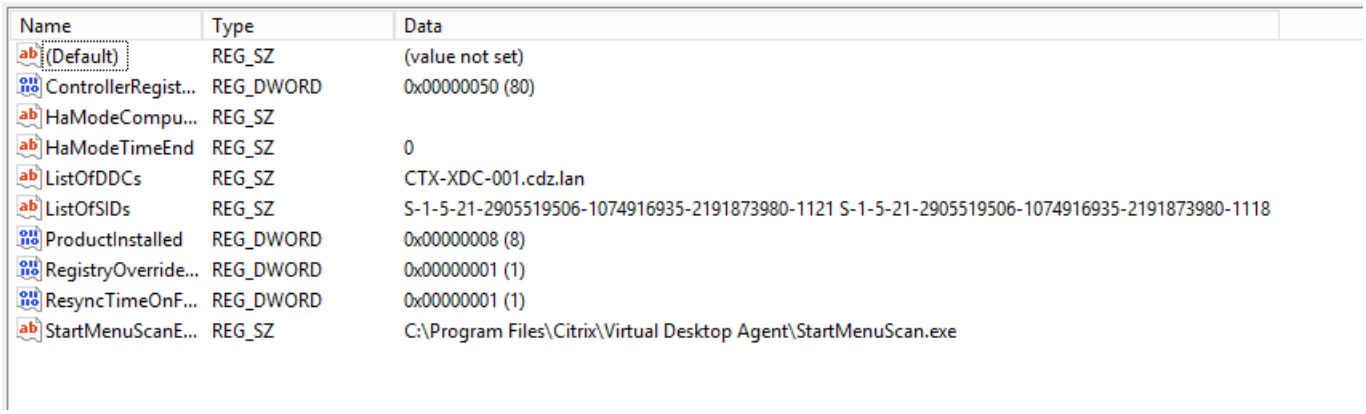
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 lo hace, debe inhabilitar 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).



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

Solución de problemas de 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 estar registrado, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

máquinas de ese catálogo que tengan una versión anterior de VDA no podrán registrarse.

Identificación de problemas después de crear los grupos de entrega:

Después de crear un grupo de entrega, Studio muestra información sobre las máquinas asociadas a ese grupo. El panel de detalles de un grupo de entrega indica la cantidad de máquinas que deberían estar registradas pero no se han registrado. En otras palabras, una o varias máquinas que están activadas y no están en modo de mantenimiento, pero no están actualmente registradas en el Controller. Al ver una máquina que "no está registrada pero debería estarlo", consulte la ficha Solución de problemas del panel Detalles, porque ahí se ofrecen las posibles causas y las acciones correctivas recomendadas.

Para obtener más información acerca de niveles funcionales, consulte la sección *Versiones de VDA y niveles funcionales* en Creación de catálogos de máquinas.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sesiones

Dec 05, 2017

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.

Use las siguientes funciones para optimizar la fiabilidad de sesiones y reducir 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.

- Fiabilidad de la sesión
- Reconexión automática de clientes
- ICA Keep-Alive
- Control del espacio de trabajo
- Movilidad de sesión

En la sección Intervalo de inicio de sesión, se describe cómo cambiar la configuración predeterminada.

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 el artículo Administración de grupos de entrega.

Fiabilidad de la sesión

La fiabilidad de la sesión mantiene las sesiones activas y en la pantalla de los usuarios cuando se interrumpe la conexión de red. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Esta función es especialmente útil para usuarios móviles con conexiones inalámbricas. Pensemos, por ejemplo, en un usuario con una conexión inalámbrica que se encuentra viajando en un tren y entra en un túnel, y pierde por un momento la conectividad. Por lo general, la sesión se desconecta y desaparece de la pantalla del usuario y después debe volver a conectarse. Con la función Fiabilidad de la sesión, la sesión permanece activa en la máquina. Para indicar que se ha perdido la conectividad, la pantalla del usuario se congela y el cursor se convierte en un reloj de arena giratorio hasta que se recupera la conectividad al salir del túnel. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Los usuarios de Citrix Receiver 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 NetScaler 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 (tres minutos). Aunque puede ampliar la cantidad de tiempo que Fiabilidad de la sesión mantiene abierta

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 un usuario una vez 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, Citrix Receiver puede detectar desconexiones accidentales de las sesiones ICA y volver a conectar automáticamente a los usuarios de las sesiones afectadas. Cuando esta función está habilitada en el servidor, los usuarios no tienen que volver a conectarse de forma manual para continuar trabajando.

En sesiones de aplicación, Citrix Receiver trata de reconectarse a la sesión hasta que lo logra o el usuario cancela el intento de reconexión.

En sesiones de escritorio, Citrix Receiver 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;

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 mediante Citrix Receiver 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 Citrix Receiver una cookie que contiene la clave de cifrado. Citrix Receiver 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Citrix Receiver 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 Citrix Receiver para Windows mediante el archivo icaclient.adm. Para obtener más información, consulte la documentación correspondiente a su versión de Citrix Receiver para Windows.

Las configuraciones de las conexiones también influyen en la función de reconexión automática de clientes:

- De forma predeterminada, la reconexión automática de clientes se habilita a través de las configuraciones de directiva en el nivel del sitio, como se describe anteriormente. No es necesario repetir la autenticación de los usuarios. Sin embargo, si la conexión ICA TCP del servidor está configurada para restablecer sesiones con un vínculo de comunicación interrumpido, la reconexión automática no se produce. La reconexión automática de clientes 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 Citrix Receiver 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 Citrix Receiver o el plugin envía 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.

Nota: La función ICA Keep-Alive solo funciona si no se usa la función Fiabilidad de la sesión. Fiabilidad de la sesión tiene su propio mecanismo para impedir que las conexiones interrumpidas se desconecten. Configure ICA Keep-Alive únicamente para las conexiones que no usen Fiabilidad de la sesión.

Los parámetros de ICA Keep-Alive sobrescriben los parámetros de Keep-Alive configurados en la directiva de grupo de Microsoft Windows.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Habilite y configure ICA Keep-Alive con las siguientes configuraciones de directiva:

- **Tiempo de espera de ICA Keep Alive**. Especifica el intervalo de envío de mensajes de ICA Keep-Alive (de 1 a 3600 segundos). No seleccione esta opción si desea que su software de supervisión de red cierre las conexiones inactivas en los entornos en los que las conexiones interrumpidas son tan poco frecuentes que permitir que los usuarios se vuelvan a conectar a las sesiones no es relevante.
  El intervalo predeterminado es 60 segundos: los paquetes de ICA Keep-Alive se envían a los dispositivos de usuario cada 60 segundos. Si un dispositivo del usuario no responde en 60 segundos, el estado de las sesiones ICA cambia a "Desconectado".
- **ICA Keep Alive**. Envía o impide el envío de mensajes de ICA Keep-Alive.

Control del espacio de trabajo

Con el control del espacio de trabajo, los escritorios y las aplicaciones permanecen disponibles para el usuario cuando éste pasa de un dispositivo a otro. Esta capacidad para moverse entre dispositivos permite que un usuario pueda acceder a todos sus escritorios o aplicaciones abiertas, desde cualquier lugar, simplemente iniciando una sesión, sin tener que reiniciar dichos escritorios y aplicaciones cuando cambia de dispositivo. Por ejemplo, el control del espacio de trabajo puede ser muy útil para los trabajadores de un hospital, que se desplazan rápidamente entre estaciones de trabajo y necesitan acceder al mismo conjunto de aplicaciones cada vez que inician una sesión. Si configura las opciones de control del espacio de trabajo con este propósito, estos trabajadores pueden desconectarse de varias aplicaciones en un dispositivo cliente y reconectarse a las mismas en un dispositivo cliente distinto.

El control del espacio de trabajo afecta a las siguientes actividades:

- **Inicio de sesión.** De manera predeterminada, el control del espacio de trabajo permite a los usuarios reconectarse automáticamente a todos los escritorios y las aplicaciones que estén ejecutándose simplemente iniciando una sesión, sin tener que volver a abrirlos manualmente. Mediante el control del espacio de trabajo, los usuarios pueden abrir aplicaciones y escritorios desconectados, así como otros que estén activos en otro dispositivo cliente. Cuando el usuario se desconecta de una aplicación o de un escritorio, estos siguen ejecutándose en el servidor. Si hay usuarios móviles que necesitan mantener en ejecución ciertas aplicaciones o escritorios en un dispositivo cliente, mientras se reconectan con un subconjunto de sus aplicaciones y escritorios en otro dispositivo cliente distinto, puede configurar el comportamiento de reconexión durante el inicio de sesión para que se abran solo los escritorios y aplicaciones de los que se haya desconectado el usuario anteriormente.
- **Reconexión.** Después de iniciar 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 desde 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 Citrix Receiver que acceden a escritorios y aplicaciones a través de una conexión de Citrix StoreFront. De manera predeterminada, el control del espacio de trabajo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar la movilidad de sesión, use los siguientes cmdlets de la regla de directiva de derechos con la propiedad "SessionReconnection". Si lo prefiere, también puede especificar la propiedad "LeasingBehavior"; para ello, consulte el apartado siguiente, Concesión de conexiones y movilidad de sesión.

Para sesiones de escritorio:

> Set-BrokerEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed|Disallowed

Para sesiones de aplicaciones:

> Set-BrokerAppEntitlementPolicyRule <*Delivery-Group-name*> -SessionReconnection <*value*> -LeasingBehavior Allowed|Disallowed

Donde <*value*> puede ser una de las siguientes opciones:

- **Always**. Las sesiones siempre se mueven, independientemente del dispositivo cliente y si la sesión está conectada o desconectada. Este es el valor predeterminado.
- **DisconnectedOnly**. 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.

Concesión de conexiones y movilidad de sesión

Si no está familiarizado con la función de concesión de conexiones, consulte el artículo Concesión de conexiones.

Cuando un Controller entra en el modo de concesión de conexiones, la reconexión de la sesión vuelve a su valor predeterminado, y reconecta al usuario a solo una de las sesiones activas o desconectadas de escritorio o aplicación.

Para mayor seguridad, si ha configurado un valor no predeterminado de movilidad de sesión y tiene varios usuarios que comparten las credenciales de inicio de sesión en varios dispositivos, puede inhabilitar la función de concesión de conexiones para el grupo de entrega que incluye esa cuenta de usuario.

¿Por qué? En este caso, una sesión se comparte entre todos los dispositivos. Esto puede ser negativo si, por ejemplo, una persona muestra información confidencial que no debe ver otra persona que se reconecta con las mismas credenciales mientras el Controller está en el modo de concesión de conexiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Inhabilitar la concesión de conexiones en la directiva de derechos elimina esta posibilidad: un usuario no podrá ver la sesión de otro usuario con el mismo inicio de sesión incluso aunque el Controller esté en el modo de concesión de conexiones. Las demás directivas de derechos pueden no modificarse, ya que las cuentas de usuario individuales pueden usar la función de concesión de conexiones a través de distintos derechos.

Para inhabilitar la función de concesión de conexiones en una directiva de derechos, agregue la propiedad "LeasingBehavior Disallowed" al cmdlet de la directiva de derechos. Si inhabilita la función Concesión de conexiones, debe eliminar manualmente las concesiones de inicio que ya se hayan creado y almacenado en caché en la directiva de derechos. De lo contrario, los usuarios podrán volver a conectarse durante una interrupción de la base de datos.

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.

Nota: Esta configuración solo se aplica a las máquinas virtuales con agentes VDA de escritorio (estaciones de trabajo); Microsoft controla el tiempo de espera de inicio de sesión en máquinas con agentes VDA de servidor.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Uso de búsquedas en Studio

Dec 05, 2017

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.
   Nota: 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.

De forma alternativa, haga clic en el botón de expandir búsqueda (doble corchete angular hacia abajo) para ver una lista desplegable de propiedades de búsqueda. Puede realizar una búsqueda avanzada si crea una expresión a partir de las propiedades de la lista desplegable.

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), 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Etiquetas

Dec 05, 2017

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 ver ejemplos y obtener más información, consulte la sección "Creación de varias programaciones de reinicios para las máquinas de un grupo de entrega" en el artículo Administración de grupos de entrega.

- Personalizar la aplicación (asignación) de las directivas de Citrix a un subconjunto de las máquinas de los grupos de entrega, tipos de grupos de entrega o unidades organizativas que contienen (o no) una etiqueta especificada.

  Por ejemplo, si quiere aplicar una directiva de Citrix solo a las estaciones de trabajo más potentes, agregue una etiqueta llamada "potencia alta" a esas máquinas. A continuación, en la página **Asignar directiva** del asistente para la creación de directivas, seleccione la etiqueta y marque la casilla **Habilitar**. También puede agregar una etiqueta a un grupo de entrega y, a continuación, aplicar una directiva de Citrix a ese grupo. Para obtener más información, consulte el artículo Creación de directivas y esta entrada de blog. (Tenga en cuenta que 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 los siguientes elementos:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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

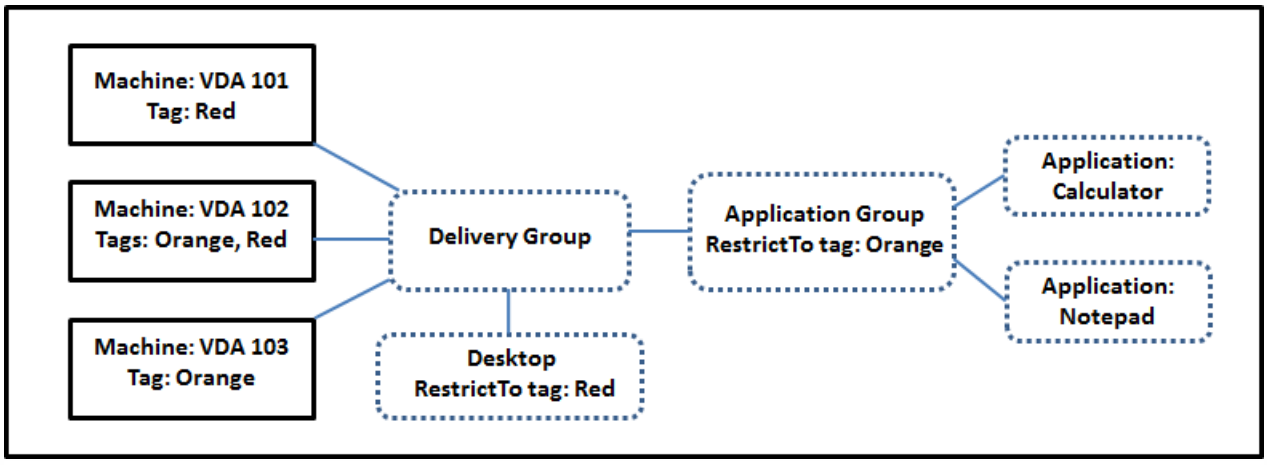
Una restricción de etiqueta implica varios pasos:

- 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

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.



- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

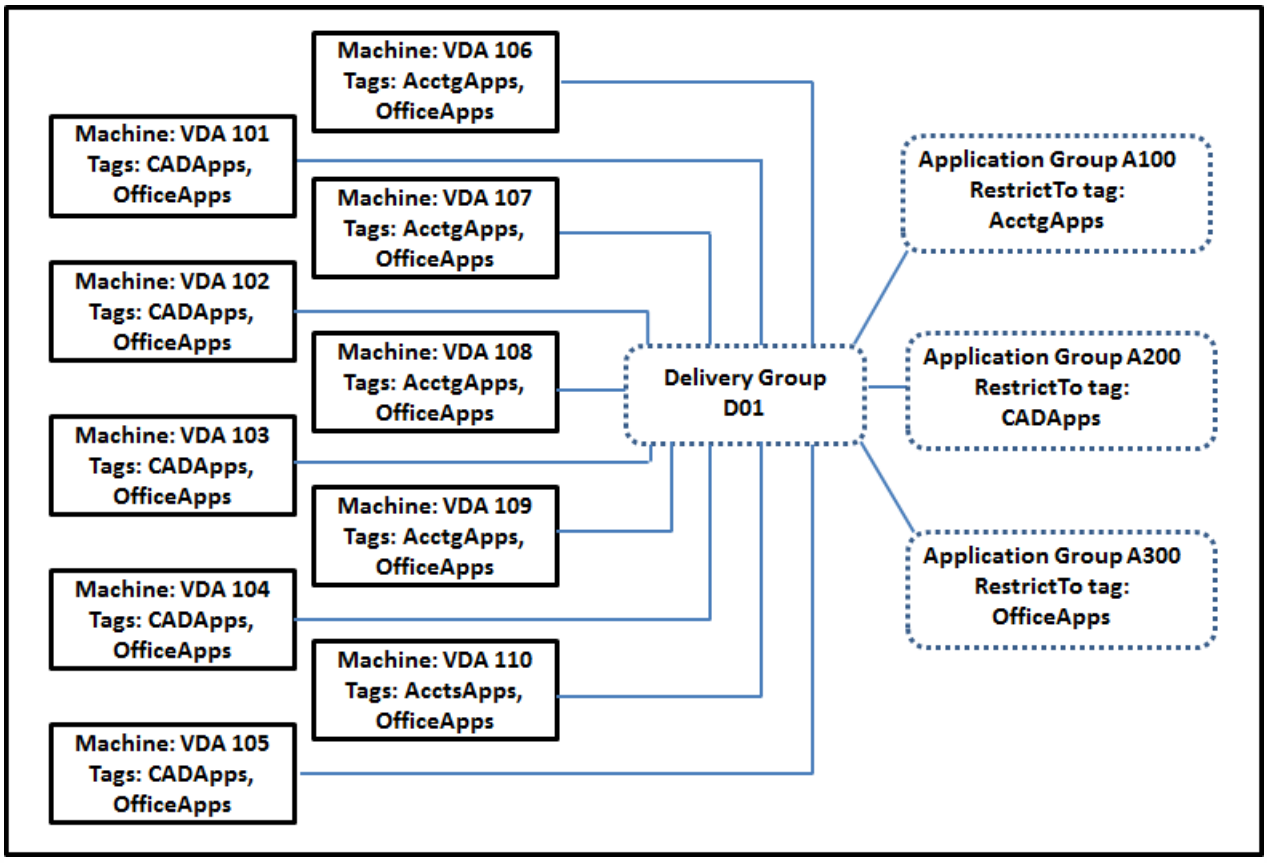
- El grupo de aplicaciones se creó con la restricción de etiqueta "Naranja", por lo que cada una de sus aplicaciones (Calculadora y Bloc de notas) solo se pueden iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta "Naranja": VDA 102 y 103.

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

En este ejemplo, existen varios grupos de aplicaciones que se han creado con restricciones de etiqueta. Por eso, se pueden entregar más aplicaciones con menos máquinas de las que se necesitarían si solo se usaran grupos de entrega.

(En la sección "Ejemplo 2: Cómo configurar", se describen los pasos a seguir para crear, aplicar las etiquetas y configurar las restricciones de etiqueta de este ejemplo.)



En este ejemplo, se utilizan 10 máquinas (agentes VDA de 101 a 110), un grupo de entrega (D01) y tres grupos de aplicaciones (A100, A200 y A300). Si aplica etiquetas a cada máquina y especifica las restricciones 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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (asignan) en el momento de crear la directiva. Consulte el artículo Creación de directivas para obtener más información.

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. Para obtener más información sobre la creación y la modificación de grupos, consulte los siguientes artículos:

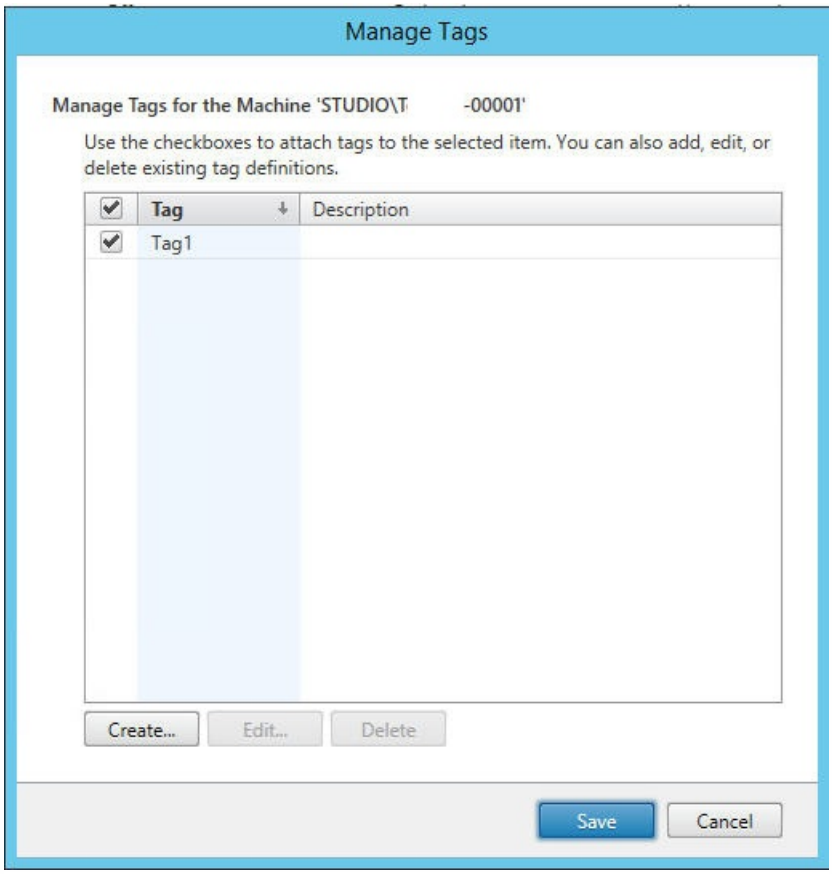
- Creación de grupos de entrega
- Administración de grupos de entrega
- Creación de grupos de aplicaciones
- Administración de grupos de aplicaciones

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Puede llevar a cabo las siguientes acciones desde el cuadro de diálogo Administrar etiquetas. No olvide consultar la sección Precaución.

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. A continuación, 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. **Nota:** Si marca varios elementos y la casilla ubicada junto a una etiqueta contiene un guión (para indicar que algunos pero no todos los elementos seleccionados ya tienen aplicada la etiqueta), cambiar ese guión a una marca de verificación afectará a todas las máquinas seleccionadas.

Si intenta agregar una etiqueta a una o varias máquinas y resulta que esa etiqueta se usa como una restricción en un grupo de aplicaciones, se le advertirá de que la acción puede provocar que esas máquinas estén disponibles para el inicio. Si es lo que pretende, continúe.

Para quitar una o varias etiquetas:

Desmarque la casilla de verificación situada junto al nombre de la etiqueta. **Nota:** 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

seleccionadas.

Si intenta quitar una etiqueta desde una máquina que la utiliza como una restricción, aparecerá un mensaje de advertencia que indicará 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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 agregar, quitar o eliminar etiquetas de los elementos

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 lo que pretende, 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 tendrán un efecto sobre el próximo ciclo de reinicios. Lo que no afecta a los ciclos de reinicios en vigor mientras se realizan los cambios. (Consulte el artículo "Administración de grupos de entrega".)

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.
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Más información

Entrada de blog: How to assign desktops to specific servers. Esa entrada también contiene el siguiente vídeo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Compatibilidad con IPv4/IPv6

Dec 05, 2017

Esta versión es compatible con solo IPv4, con solo IPv6, así como con implementaciones de doble pila que usan redes IPv4 e IPv6 superpuestas .

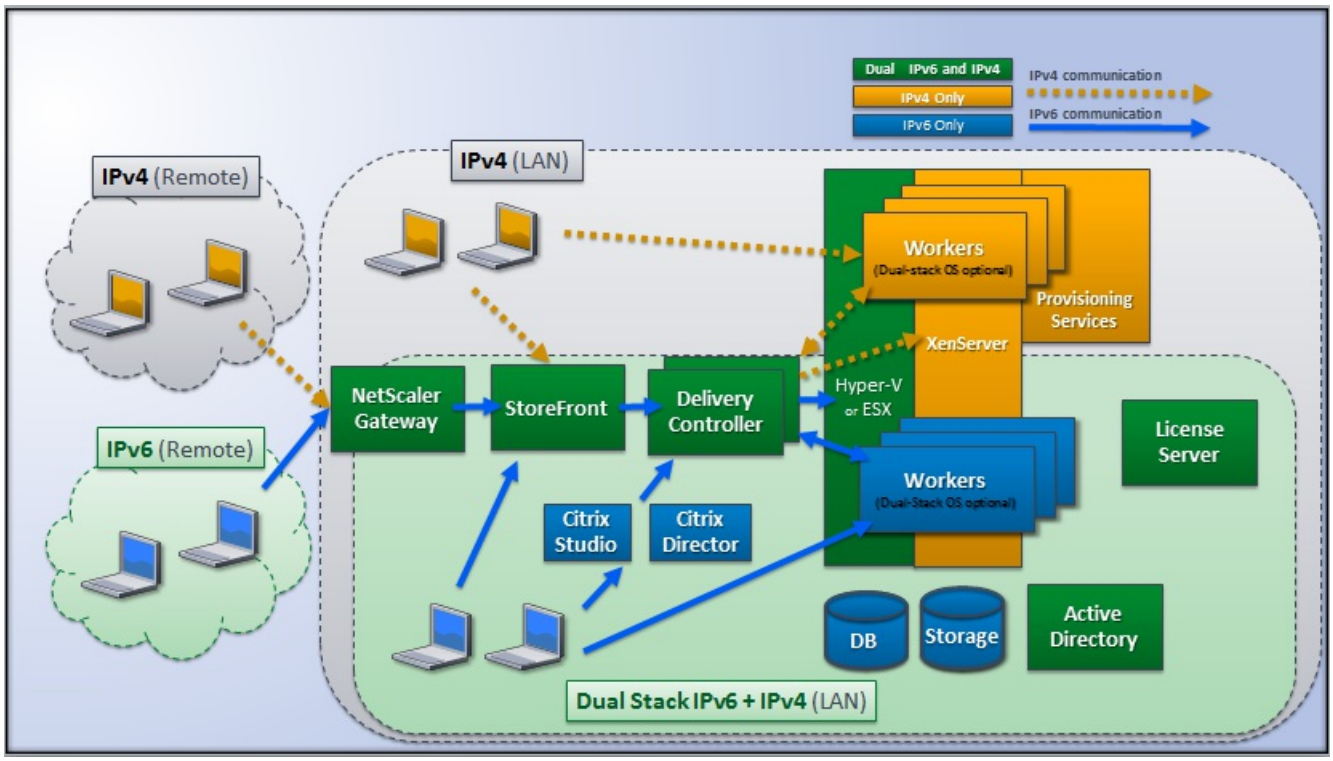
Las comunicaciones de IPv6 se controlan con dos configuraciones de directiva de Citrix relacionadas con las conexiones del Virtual Delivery Agent (VDA):

- Una configuración principal que aplica el uso de IPv6: Usar solo registro de Controller con IPv6.
- Una configuración dependiente que define una máscara de red IPv6: Máscara de red IPv6 para registro de Controller.

Cuando la configuración de directiva Usar solo registro de Controller con IPv6 está habilitada, el VDA se registra en un Delivery Controller para las conexiones entrantes mediante una dirección IPv6.

Implementación de doble pila IPv4/IPv6

La siguiente figura ilustra una implementación de doble pila de IPv4/IPv6. En este caso, un trabajador es un VDA instalado en un hipervisor o en un sistema físico, y se utiliza principalmente para habilitar las conexiones de aplicaciones y escritorios. Los componentes 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:

- Provisioning Services
- XenServer versión 6.x
- Los VDA no controlados por la configuración de directiva **Usar solo registro de Controller con IPv6**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Versiones de XenApp anteriores a 7.5, versiones de XenDesktop anteriores a 7 y Director

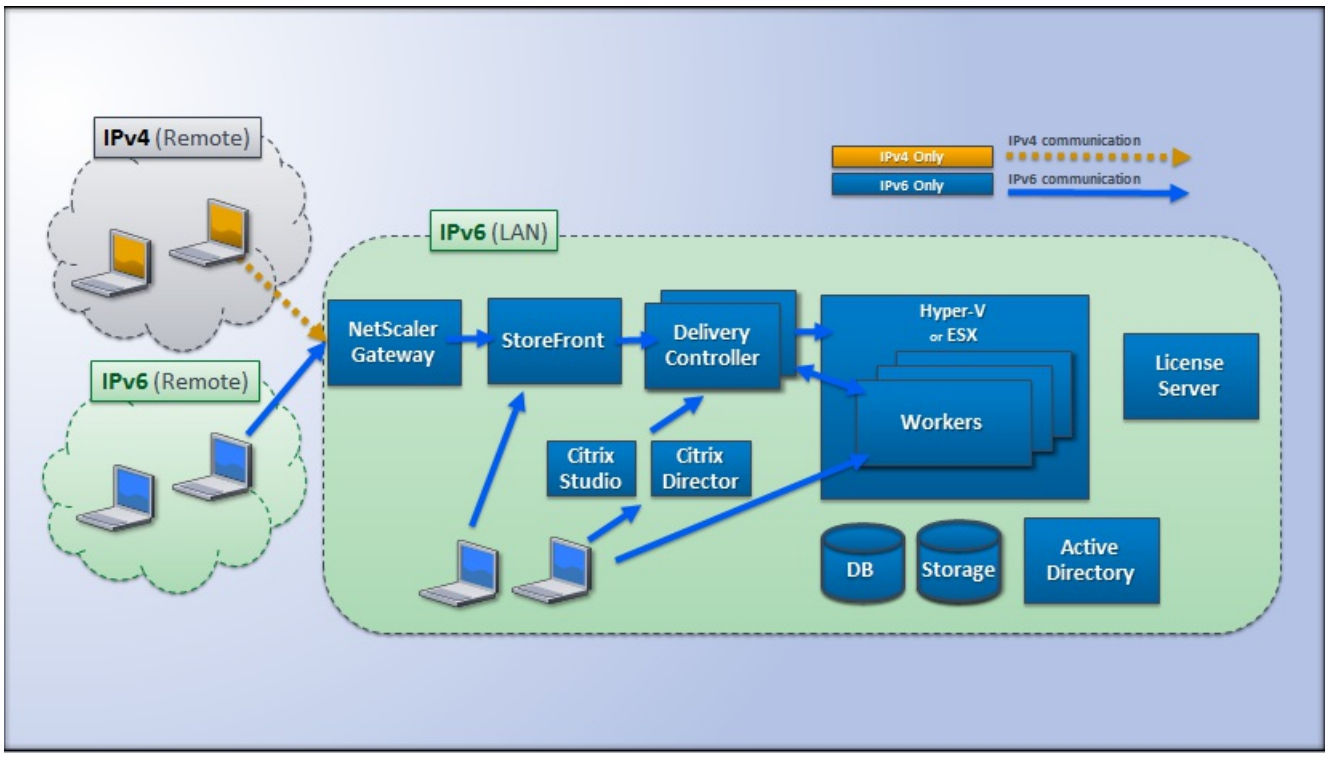
En esta implementación:

- Si un grupo de usuarios usa una red IPv6 de manera habitual y el administrador desea que use el tráfico IPv6, publicará escritorios y aplicaciones con IPv6 para esos usuarios a partir de una imagen de trabajo o de una unidad organizativa (OU) que tiene la configuración de directiva principal de IPv6 habilitada (es decir, la configuración Usar solo registro de Controller con IPv6 está habilitada).
- Si un grupo de usuarios usa una red IPv4 de manera habitual, el administrador publicará los escritorios y las aplicaciones con IPv4 para esos usuarios a partir de una imagen de trabajo o unidad organizativa que tiene la configuración de directiva de IPv6 inhabilitada (es decir, Usar solo registro de Controller con IPv6 está inhabilitada), que es el valor predeterminado.

Implementación de solo IPv6

La siguiente figura 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. Configure las siguientes configuraciones de directiva relacionadas con las conexiones:

- **Usar solo registro de Controller con IPv6**. Controla el formato de dirección que utiliza Virtual Delivery Agent (VDA) para registrarse en el Delivery Controller. Valor predeterminado = inhabilitado
  - Cuando el VDA se comunica con el Controller, utiliza una sola dirección IPv6 seleccionada según las siguientes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Aspectos a tener en cuenta para 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Perfiles de usuario

Dec 05, 2017

De forma predeterminada, Citrix Profile Management se instala de forma silenciosa en las imágenes maestras al instalar el Virtual Delivery Agent, pero no tiene que utilizar Profile Management necesariamente como solución de administración de perfiles.

Para responder a las distintas necesidades de los usuarios, puede aplicar, mediante las directivas de XenApp y XenDesktop, 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 XenApp y XenDesktop, trabaje 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 XenApp y XenDesktop 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 XenApp y XenDesktop.

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 funcionalidad conserva las configuraciones de directiva no predeterminadas, no las sobrescribe. Consulte la documentación de Profile Management para obtener información sobre cada directiva. Los tipos de máquinas que crean perfiles afectan a las directivas que se ajustan. Los factores principales son si las máquinas son persistentes o aprovisionadas y si están compartidas entre 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 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. Un disco RAM o un

© 1999-2017 Citrix Systems, Inc. All rights reserved.

disco de red imitan el almacenamiento local; una red SAN suministra normalmente el disco de red con un enlace de alta velocidad. La tecnología de aprovisionamiento es normalmente Provisioning Services o Machine Creation Services (o un producto equivalente de terceros). Algunas veces, los sistemas aprovisionados tienen un almacenamiento local persistente que puede estar compuesto de 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 con SO de escritorio con una asignación estática pero sin Personal vDisk, creadas con Provisioning Services .
- **Aprovisionadas y compartidas** . Por ejemplo, máquinas con SO de escritorio con una asignación aleatoria, creadas con Provisioning Services; 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 para adaptarlas a su entorno.

Importante: Eliminar perfiles guardados en caché local al cerrar la sesión, Streaming de perfiles y Guardar siempre en caché se aplican obligatoriamente mediante la función de configuración automática. Ajuste el resto de las directivas manualmente.

Máquinas persistentes

Directiva	Persistentes y dedicadas	Persistentes y compartidas
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitado	Habilitado
Streaming de perfiles	Inhabilitado	Habilitado
Guardar siempre en caché	Habilitada (nota 1)	Inhabilitada (nota 2)
Reescritura activa	Inhabilitado	Inhabilitada (nota 3)
Procesar inicios de sesión de administradores locales	Habilitado	Inhabilitada (nota 4)

Máquinas aprovisionadas

Directiva	Aprovisionadas y dedicadas	Aprovisionadas y compartidas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Directiva	Aprovisionadas y dedicadas	Aprovisionadas y compartidas
Eliminar perfiles guardados en caché local al cerrar la sesión	Inhabilitada (nota 5)	Habilitado
Streaming de perfiles	Habilitado	Habilitado
Guardar siempre en caché	Inhabilitada (nota 6)	Inhabilitado
Reescritura activa	Habilitado	Habilitado
Procesar inicios de sesión de administradores locales	Habilitado	Habilitada (nota 7)

1. Puesto que Streaming de perfiles está inhabilitado para este tipo de máquina, el parámetro Guardar siempre en caché se omite siempre.
2. Inhabilite Guardar siempre en caché. No obstante, para que los archivos de gran tamaño se carguen en los perfiles tan pronto como sea posible después de iniciar 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 la memoria 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 XenApp. 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. Conserva los perfiles guardados en caché local. Puesto que las máquinas se restablecen al cerrar 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 que los archivos de gran tamaño se carguen en los perfiles tan pronto como sea posible después de iniciar 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 la memoria 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 XenApp y XenDesktop. En ese caso, inhabilite esta directiva.

Redirección de carpetas

La redirección de carpetas permite almacenar datos de usuario en recursos compartidos de red en una ubicación que no sea 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 requieren 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.

- Compruebe 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.

Nota: Configure la redirección de carpetas con las directivas de Citrix o con los objetos de directiva de grupo de Active

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Directory, pero no ambos a la vez. Si configura la redirección de carpetas con ambos motores de directivas, puede que obtenga resultados inesperados.

Redirección de carpetas avanzada

En las implementaciones con varios sistemas operativos (SO), puede ser conveniente que cada SO comparta una porción del perfil de usuario. El resto del perfil no se comparte y solo lo utiliza un sistema operativo. Para garantizar una experiencia de usuario coherente en todos los sistemas operativos, necesita una configuración diferente para cada sistema operativo. 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 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 coherente 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, el comportamiento de la redirección puede ser inesperado.

Para redirigir carpetas en implementaciones avanzadas:

- Use un grupo de entrega distinto para cada sistema operativo.
- Es necesario conocer dónde se 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. En este ejemplo, se incluyen 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 ello, 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 a redirigir y compartir depende de una serie de factores que son específicos de la implementación en cuestión.

- Mediante directivas aplicadas a los grupos de entrega, se eligen las siguientes carpetas a redirigir.

Carpeta	¿Redirigida en Windows 8?	¿Redirigida en Windows Server 2008?
Mis documentos	Sí	Sí
Datos de programa	NO	NO
Contactos	Sí	Sí

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Carpeta	¿Redirigida en Windows 8?	¿Redirigida en Windows Server 2008?
Escritorio	Sí	NO
Descargas	NO	NO
Favoritos	Sí	Sí
Enlaces	Sí	NO
Mi música	Sí	Sí
Mis imágenes	Sí	Sí
Mis vídeos	Sí	Sí
Búsquedas	Sí	NO
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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Insight Services

Dec 05, 2017

Citrix Insight Services (CIS) es una plataforma de Citrix para instrumentación, telemetría y generación de información empresarial. Sus capacidades de instrumentación y telemetría permiten a los usuarios técnicos (clientes, socios e ingenieros) emitir ellos mismos diagnósticos de los problemas y corregirlos, optimizando así sus entornos de trabajo. Para obtener la información más reciente y detallada sobre CIS y saber cómo funciona, consulte https://cis.citrix.com/ (se necesitan credenciales de cuenta de Citrix).

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:

- Citrix Insight Services Policy, https://cis.citrix.com/legal
- Directiva de privacidad de Citrix, http://www.citrix.com/about/legal/privacy.html

Esta versión de XenApp y XenDesktop admite las siguientes herramientas y tecnologías.

- Datos de análisis de instalación y actualización de XenApp y XenDesktop
- Customer Experience Improvement Program (CEIP) de Citrix
- Citrix Smart Tools
- Citrix Call Home (parte de Citrix Smart Tools)
- Citrix Scout

Datos de análisis de instalación y actualización

Cuando se usa el programa de instalación del producto completo para implementar o actualizar los componentes de XenApp o XenDesktop, se recopila información anónima sobre el proceso de instalación y se guarda en la máquina donde se está realizando la instalación o actualización del componente. Esta información se utiliza para ayudar a Citrix a mejorar la experiencia de instalación de sus clientes. Para obtener más información, consulte http://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.
- Puede anular la configuración predeterminada si instala o actualiza con la interfaz de línea de comandos y especifica esa opción con el comando.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 la carga automática con el comando XenDesktopServerSetup.exe o XenDesktopVDASetup.exe, incluya la opción /disableexperiencemetrics.

Para habilitar la carga automática 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 http://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 de XenApp o XenDesktop (después de instalar el primer Delivery Controller). La primera carga de datos tiene lugar aproximadamente siete días después de crear el sitio. Puede interrumpir su participación en el programa en cualquier momento después de crear el sitio; seleccione el nodo **Configuración** en el panel de navegación de Studio (ficha Asistencia para productos) y siga las instrucciones.

Al actualizar una implementación de XenApp o XenDesktop:

- 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.
- 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):

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ubicación: HKLM:\Software\Citrix\Telemetry\CEIP
Nombre: Enabled
Valor: 0 = inhabilitado, 1 = habilitado

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:

New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name Enabled -PropertyType DWORD -Value 0

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 el CEIP al instalar productos, componentes y tecnologías de Citrix relacionados, tales como Provisioning Services, AppDNA, Citrix License Server, Citrix Receiver para Windows, Universal Print Server y la funcionalidad Grabación de sesiones. Consulte la documentación para obtener más detalles sobre los valores predeterminados de instalación y participación en el programa.

Citrix Smart Tools

Puede habilitar el acceso a Citrix Smart Tools cuando instale un Delivery Controller.

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 **Connect**. 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.

Citrix Call Home

Al instalar determinados componentes y funciones de XenApp o XenDesktop, 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 XenApp y XenDesktop, Call Home se ejecuta como un servicio en segundo plano con el nombre de Citrix Telemetry Service. Para obtener más información, consulte http://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 para solucionar errores comunes como, por

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ejemplo, los registros de VDA e inicios de aplicaciones o escritorios. Esta tecnología se conoce como seguimiento permanente (Always-On Tracing o AOT). 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:

- Claves de Registro creadas por XenApp y XenDesktop en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
- 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 seguimiento utiliza un mecanismo circular para conservar los seguimientos en memoria.

HTM

Puntos de datos clave para Call Home

Call Home collects these key datapoints.

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 a. m.

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.

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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

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.

Habilitar cargas programadas

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.

Habilitar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Crear una programación personalizada

Cree una programación semanal o diaria para recopilaciones y cargas de diagnósticos.

```
$timespan = New-TimeSpan –Hours -Minutes
Set-CitrixCallHomeSchedule –TimeOfDay $timespan –DayOfWeek -UploadFrequency {Daily|Weekly}
```

Cancelar cargas programadas

Después de cancelar las cargas programadas, aún puede cargar datos de diagnóstico mediante cmdlets de PowerShell.

```
Disable-CitrixCallHome
```

Para confirmar que las cargas programadas se han inhabilitado, escriba Get-CitrixCallHome. Este comando debe devolver IsEnabled=False and IsMasterImage=False.

Ejemplos

El cmdlet siguiente crea una programación para crear un paquete con los datos y cargarlos a las 23:20 de la noche. Tenga en cuenta que el parámetro de horas se usa un reloj de 24 horas. Cuando el valor del parámetro UploadFrequency es Daily, el parámetro DayOfWeek se ignora aunque se haya especificado.

```
$timespan – New-TimeSpan –Hours 22 –Minutes 20
Set-CitrixCallHomeSchedule –TimeOfDay $timespan -UploadFrequency Daily
```

Para confirmar la programación, introduzca Get-CitrixCallHomeSchedule. En el ejemplo anterior, debe devolver StartTime=22:20:00, DayOfWeek=Sunday (se ignora), 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
```

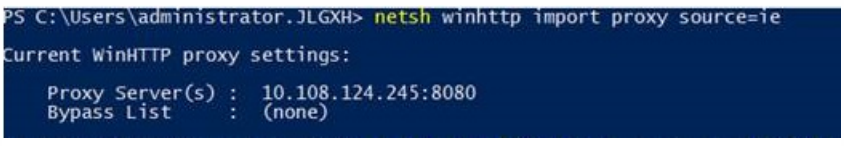
Para confirmar la programación, introduzca Get-CitrixCallHomeSchedule. En el ejemplo anterior, debe devolver StartTime=22:20:00, DayOfWeek=Wednesday, Upload Frequency=Weekly.

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.

Paso 1. Agregue información del servidor proxy al 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.

Paso 2. En PowerShell, ejecute **netsh winhttp import proxy source=ie**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paso 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 este cuadro rojo.



Paso 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Start-CitrixCallHomeUpload [-Credential] [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploadHeader] [-AppendHeaders] [-Collect] []

Recopilar datos para guardarlos localmente

Start-CitrixCallHomeUpload -OutputPath [-InputPath] [-Description] [-IncidentTime] [-SRNumber] [-Name] [-UploaderHeader] [-AppendHeaders] [-Collect] []

Parámetro	Descripción
Credencial	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.
Hora del incidente y descripción	Información en formato libre sobre la carga.
SRNumber	Número de incidente de Citrix Technical Support.
Nombre	Nombre que identifica el paquete.
UploadHeader	Cadena en formato JSON que especifica los encabezados cargados en CIS.
AppendHeaders	Cadena en formato JSON que especifica los encabezados anexados cargados en CIS.
Collect	Cadena en formato JSON que especifica qué datos hay que recopilar u omitir, con el formato {'collector':{'enabled':Boolean}}", donde Boolean es True o False. Los valores válidos de recopilador para el parámetro 'collector' son: • 'wmi' • 'process' • 'registry' • 'crashreport' • 'trace' • 'localdata' • 'sitedata' • 'sfb' De forma predeterminada, están habilitados todos los recopiladores salvo "sfb". El recopilador "sfb" está diseñado para utilizarse a petición para diagnosticar problemas de Skype Empresarial. Además del parámetro "enabled", el recopilador 'sfb' admite los parámetros "account" y "account" para especificar usuarios de destino. Utilice uno de los formatos: "-Collect "{'sfb':{'account':'domain\\user1'}}"

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	-Collect "{'sfb':{'accounts':['domain\\user1', 'domain\\user2']}}"
Parámetros comunes	Consulte la ayuda de PowerShell.

Cargar datos previamente guardados localmente

Send-CitrixCallHomeBundle -Credential -Path []

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 tienen relación con los fallos de registros de VDA de PVS, notificados a las 2:30 p.m. 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.

C:\PS>Start-CitrixCallHomeUpload -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Registration failures with PVS VDAs" -IncidentTime "14:30" -SRNumber 123456 -Name "RegistrationFailure-021812016" -Collect "{'wmi': {'enabled':false}}" -UploadHeader "{'key1':'value1'}" -AppendHeaders "{'key2':'value2'}"

El siguiente cmdlet guarda los datos de Call Home relacionados con el caso de asistencia técnica de Citrix Support número 223344, notificado a las 8:15 a.m. Los datos se guardan en el archivo mydata.zip en un recurso compartido de red. Además de los datos de Call Home, se incorporará el archivo "c:\Diagnostics\ExtraData.zip" al paquete guardado.

C:\PS>Start-CitrixCallHomeUpload -OutputPath \\mynetwork\myshare\mydata.zip -InputPath "c:\Diagnostics\ExtraData.zip" -Description "Diagnostics for incident number 223344" -IncidentTime "8:15" -SRNumber 223344

El cmdlet siguiente carga el paquete de los datos que guardó previamente.

$cred=Get-Credential
C:\PS>Send-CitrixCallHomeBundle –Credential $cred -Path \\mynetwork\myshare\mydata.zip

Citrix Scout

Para obtener información completa, consulte Citrix Scout.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Scout

Dec 05, 2017

En este artículo:

- Introducción
- Consideraciones y requisitos
- Recopilar diagnósticos
- Rastrear y reproducir
- Programar recopilaciones

Introducción

Citrix Scout recopila diagnósticos que pueden usarse para el mantenimiento proactivo de la implementación de XenApp y XenDesktop. 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:

- En una implementación local de XenApp y XenDesktop, 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 nube de Citrix que usa XenApp and XenDesktop Service, 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

información de rastreo de eventos para Windows (ETW).

Los datos capturados incluyen:

- Entradas de Registro creadas por XenApp y XenDesktop en HKEY_LOCAL_MACHINE\SOFTWARE\CITRIX.
- 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 un máximo de 10 MB de la información de rastreo más reciente comprimida, con un tiempo límite máximo de ocho días.
- Los rastreos se guardan en memoria a fin de evitar operaciones E/S en las máquinas aprovisionadas.
- El búfer de rastreo utiliza un mecanismo circular para conservar los rastreos en memoria.

Para ver una lista de los puntos de datos que recopila Citrix Scout, consulte Puntos de datos clave para Scout.

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 estar ejecutando una versión de Scout que se incluye en XenApp y XenDesktop 7.14 o una versión posterior respaldada.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Error message	Corrective action
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.
Cómo habilitar PSRemoting y WinRM	Puede habilitar la comunicación remota de PowerShell y WinRM al mismo tiempo. Con la opción "Ejecutar como administrador", ejecute el cmdlet **Enable-PSRemoting**. Para obtener más información, consulte la Ayuda de Microsoft para el cmdlet.
Scout requiere PowerShell 3.0 (como mínimo)	Instale PowerShell 3.0 (o una versión posterior) en la máquina y habilite la comunicación remota de PowerShell.
No se puede acceder al directorio LocalAppData en esta máquina	Compruebe que su cuenta tiene permiso para escribir en el directorio LocalAppData de la máquina.
No se encuentra Citrix Telemetry Service	Asegúrese de que 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 XenApp y XenDesktop 7.14 como mínimo.

Se proporciona una versión anterior de Scout con las implementaciones anteriores de XenApp y XenDesktop. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Feature	Scout 2.23	Scout 3.0
Respaldo para Citrix XenApp y XenDesktop 7.14 (mínimo)	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 Always-on Traces (AOT)	NO	Sí
Permitir recopilación de diagnósticos	Un máximo de 10 máquinas a la vez (de forma predeterminada)	Sin límite (sujeto a la disponibilidad de recursos)
Permitir que los datos de diagnóstico se envíen a Citrix	Sí	Sí
Permitir que los datos de diagnóstico se guarden localmente	Sí	Sí
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)

Instalación

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenDesktop o XenApp.

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.
- 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.

Recopilación de 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).

Paso 1. Inicie Citrix Scout

Desde el menú de inicio de la máquina: **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Recopilar**.

Paso 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:

© 1999-2017 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 diagnóstico en esa máquina.

Cuando las pruebas de verificación se completen, haga clic en **Continue**.

Paso 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 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**.

Paso 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 **Done** para volver a la página de inicio de Citrix Scout. No es necesario completar más pasos en este procedimiento.

Paso 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
- Para una cuenta de Citrix, introduzca las credenciales.

Cuando haya terminado, haga clic en **Continuar**.

Paso 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 **Done** 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paso 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**.

Paso 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 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 seguimiento ni diagnóstico en esa máquina.

Cuando las pruebas de verificación se completen, haga clic en **Continue**.

Paso 3. Rastree los datos

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.

Paso 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

ese botón y confirma la solicitud del sistema, se pierde la recopilación.

Cuando la recopilación se complete, haga clic en **Continuar**.

Paso 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.

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.

Paso 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 **Configure 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**.

Paso 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **Done** 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.)

Paso 1. Inicie Citrix Scout

Desde el menú de inicio de la máquina: **Citrix > Citrix Scout**. En la página de inicio, haga clic en **Programar**.

Paso 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:

- 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 seguimiento ni diagnóstico en esa máquina.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cuando las pruebas de verificación se completen, haga clic en **Continue**.

En la página de resumen, se ofrece una lista de las máquinas a las que se aplicarán las programaciones. Haga clic en **Continuar**.

Paso 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**.

Paso 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 Configure 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**.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Supervisión

Dec 05, 2017

Los administradores y el personal de asistencia técnica pueden supervisar los sitios de XenDesktop y XenApp 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.

Grabación de sesiones

La función de grabación de sesiones permite grabar la actividad en pantalla de cualquier sesión de usuario, en cualquier tipo de conexión desde cualquier servidor XenApp (sujeto a las normas de su empresa y las leyes aplicables). La funcionalidad Grabación de sesiones graba, cataloga y archiva sesiones para poder recuperarlas y reproducirlas.

Grabación de sesiones usa una serie de directivas flexibles para activar la grabación de sesiones automáticamente. Esto permite a los encargados de TI supervisar y examinar el uso de las aplicaciones, tales como operaciones financieras y los sistemas de información de pacientes, para el control interno y asegurar así el cumplimiento de normas y legislación vigentes y supervisar la seguridad. Asimismo, la grabación de sesiones contribuye a facilitar las tareas de asistencia técnica haciendo más rápida la identificación del problema y por tanto reduciendo el tiempo que se tarda en resolverlo.

Para obtener información más detallada, consulte los artículos de Grabación de sesiones.

Registros de configuración

El registro de configuración 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. Asimismo, puede ver los elementos registrados en Director desde la vista Tendencias para ofrecer notificaciones acerca de los cambios de configuración. Esta función es útil para los administradores que no tienen acceso a Studio.

La vista Tendencias ofrece datos históricos de cambios de configuración realizados a lo largo de un período de tiempo, de forma que los administradores puedan ver qué cambios se hicieron en el sitio, quién los hizo y cuándo tuvieron lugar, para averiguar la causa de algún problema. Esta vista ordena la información de configuración en tres categorías.

- Fallos de conexión

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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. En los artículos de Director, se describe cómo consultar la información registrada con dicha herramienta.

Registros de eventos

Los servicios de XenApp y XenDesktop registran los eventos que tienen lugar. Los registros de eventos se pueden usar para supervisar y solucionar problemas de las operaciones.

Para obtener más información, consulte el artículo Registros de eventos. Los artículos referidos a funcionalidades individuales también pueden contener información de eventos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Grabación de sesiones

Dec 05, 2017

La Grabación de sesiones permite grabar la actividad en pantalla de cualquier sesión de usuario alojada desde un VDA con SO de servidor o escritorio, en cualquier tipo de conexión y sujeta al cumplimiento de las normas y directivas de empresa. La funcionalidad Grabación de sesiones graba, cataloga y archiva sesiones para poder recuperarlas y reproducirlas.

Grabación de sesiones usa una serie de directivas flexibles para activar la grabación de sesiones automáticamente. Esto permite a los encargados de TI supervisar y examinar el uso de las aplicaciones, tales como operaciones financieras y los sistemas de información de pacientes, para el control interno y asegurar así el cumplimiento de normas y legislación vigentes y supervisar la seguridad. Asimismo, la grabación de sesiones contribuye a facilitar las tareas de asistencia técnica haciendo más rápida la identificación del problema y por tanto reduciendo el tiempo que se tarda en resolverlo.

Ventajas

Seguridad mejorada mediante captura de registros y supervisión. La Grabación de sesiones permite a las empresas grabar la actividad en pantalla del usuario cuando se trata de aquellas aplicaciones que manejan información confidencial. Esto es especialmente importante en sectores regulados , tales como salud y finanzas. Cuando hay información personal que no debe grabarse, se pueden aplicar unos controles de directiva que permiten la grabación selectiva.

Supervisión de actividad. La Grabación de sesiones captura y archiva actualizaciones de pantalla, incluidos los clics del puntero y el resultado visible de las acciones con el teclado, en grabaciones de vídeo protegidas, para proporcionar registros de actividad de usuarios, aplicaciones y servidores específicos.

La Grabación de sesiones no está diseñada ni se creó con el fin de contribuir a la recopilación de pruebas para procesos judiciales . Citrix recomienda que las organizaciones que usan grabación de sesiones usen otras técnicas para la recopilación de pruebas, tales como registros de video convencionales combinados con herramientas eDiscovery tradicionales basadas en texto.

Resolución rápida de problemas. Cuando los usuarios llaman al centro de asistencia técnica con un problema que es difícil de reproducir, el personal de asistencia técnica puede habilitar la grabación de las sesiones de usuario. Cuando el problema vuelve a ocurrir, la grabación de sesiones brinda un registro visual del error con una marca de fecha y hora, lo que puede usarse para encontrar una solución más rápidamente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Introducción a la grabación de sesiones

Dec 05, 2017

Después de realizar los siguientes pasos ya puede empezar a grabar y consultar sesiones de XenApp y XenDesktop.

1. Familiarícese con los componentes de la función de grabación de sesiones.
2. Seleccione los escenarios de implementación del entorno.
3. Compruebe los requisitos de instalación.
4. Instale los roles y las funcionalidades de Windows como requisitos previos.
5. Instale la funcionalidad de grabación de sesiones.
6. Configure los componentes de la grabación de sesiones para poder grabar y ver las sesiones.

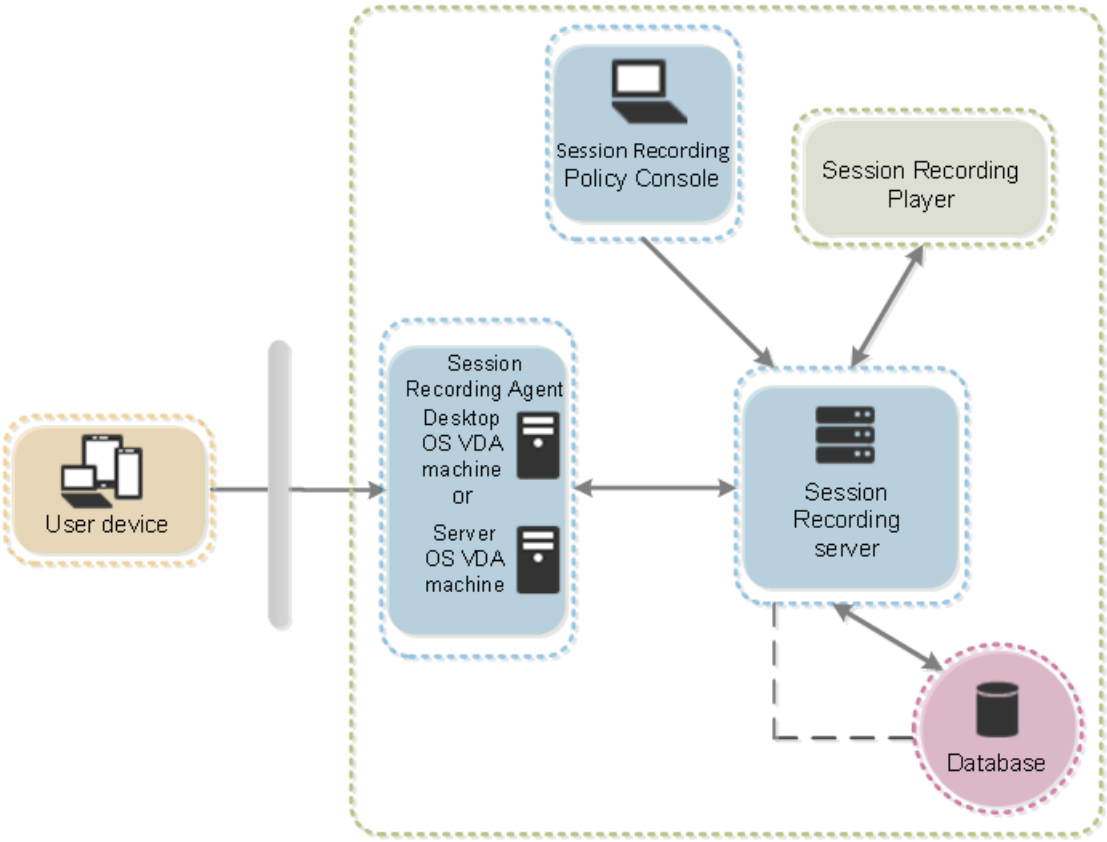
La funcionalidad Grabación de sesiones consta de cinco componentes:

- **Agente de grabación de sesiones.** Un componente instalado en cada VDA de SO de servidor o escritorio para permitir la grabación. Se encarga de grabar los datos de las sesiones.
- **Servidor de grabación de sesiones.** Un servidor que aloja lo siguiente:
  - El Broker. Una aplicación Web alojada en IIS 6.0+ que se encarga de las consultas de búsqueda y las solicitudes de descarga de archivos desde el Reproductor de grabación de sesiones, de las solicitudes de directivas administrativas desde la Consola de directivas de grabación de sesiones y que evalúa las directivas de grabación para cada sesión de XenApp y XenDesktop.
  - El Administrador de almacenamiento. Un servicio de Windows que administra los archivos de grabación de sesión recibidos desde cada equipo habilitado para la grabación de sesiones que ejecuta XenApp y XenDesktop.
  - Registro de administrador.Un subcomponente opcional que se instala con el Servidor de grabación de sesiones para registrar las actividades de administración. Todos los datos de registros se guardan en una base de datos de SQL Server aparte llamada **CitrixSessionRecordingLogging**.
- **Reproductor de grabación de sesiones.** Una interfaz de usuario a la que los usuarios acceden desde una estación de trabajo para reproducir archivos de sesiones grabadas de XenApp y XenDesktop.
- **Base de datos de grabación de sesiones.**Un componente que administra la base de datos de SQL Server para almacenar los datos de las sesiones grabadas. Cuando se instala este componente, se crea una base de datos denominada **CitrixSessionRecording**. No se le puede cambiar el nombre.
- **Consola de directivas de grabación de sesiones.** Una consola utilizada para crear directivas para especificar qué sesiones se graban.

Esta imagen muestra los componentes de la funcionalidad Grabación de sesiones y la relación entre ellos:

En el ejemplo de implementación ilustrado aquí, el Agente de grabación de sesiones, el Servidor de grabación de sesiones, la Base de datos de grabación de sesiones, la Consola de directivas de grabación de sesiones y el Reproductor de grabación de sesiones residen todos detrás de un firewall. El Agente de grabación de sesiones se instala en un VDA de SO de servidor o escritorio. Un segundo servidor aloja la Consola de directivas de grabación de sesiones, un tercer servidor actúa como Servidor de grabación de sesiones, y un cuarto servidor aloja la Base de datos de grabación de sesiones. El Reproductor de grabación de sesiones se instala en una estación de trabajo. Un dispositivo cliente fuera del firewall se comunica con la máquina de SO de servidor donde está instalado el Agente de grabación de sesiones. Dentro del firewall, el Agente de grabación de sesiones, la Consola de directivas de grabación de sesiones, el Reproductor de grabación de sesiones y la Base de datos de grabación de sesiones se comunican todos con el Servidor de grabación de sesiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Planificación de la implementación

Dec 05, 2017

Limitaciones y advertencias

La funcionalidad Grabación de sesiones no admite el modo de visualización para la redirección de composición del escritorio (DCR). De forma predeterminada, la Grabación de sesiones inhabilita DCR en una sesión si ésta se grabará con la directiva de grabación. Puede configurar este comportamiento en las propiedades del Agente de grabación de sesiones.

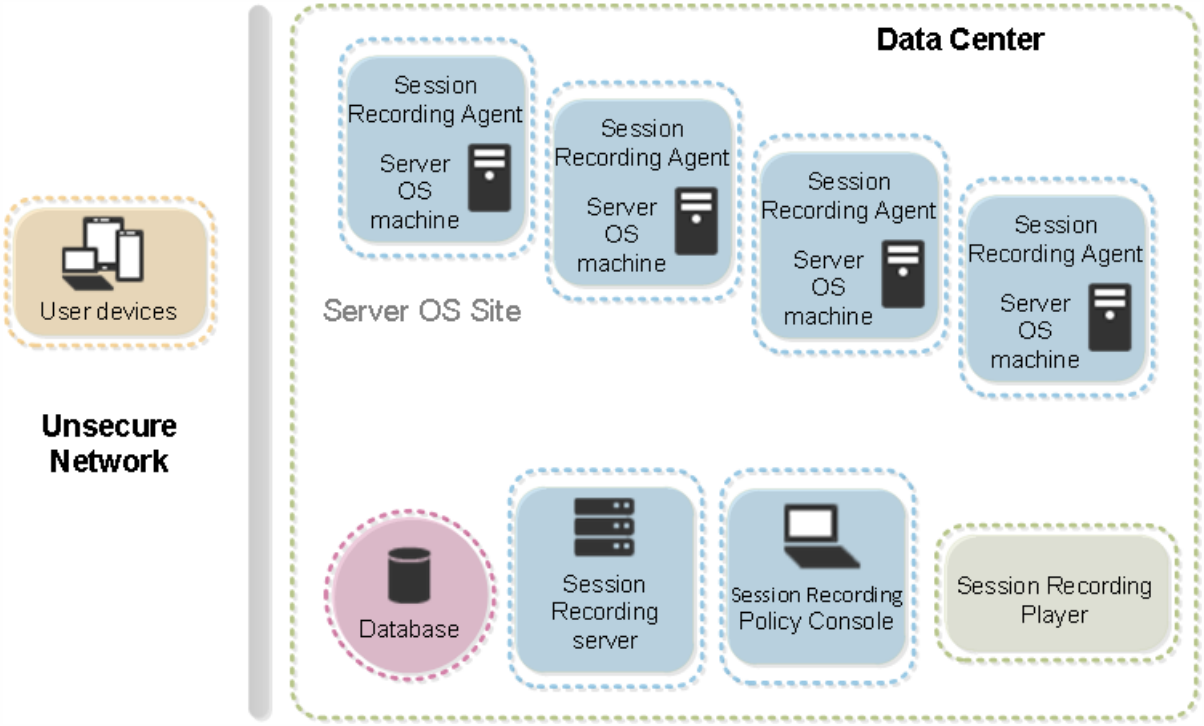
Dependiendo del entorno, los componentes de grabación de sesiones se pueden implementar en diferentes escenarios.

Una implementación de grabación de sesiones no tiene que limitarse necesariamente a un único sitio. Con la excepción del Agente de grabación de sesiones, todos los componentes son independientes del sitio de servidores. Por ejemplo, puede configurar varios sitios para que usen un único Servidor de grabación de sesiones.

Si tiene un sitio muy grande, con muchos agentes, y planea grabar aplicaciones con muchos gráficos (por ejemplo, aplicaciones de AutoCAD) o tiene que grabar muchas sesiones, el Servidor de grabación de sesiones puede experimentar una demanda de rendimiento elevada. Para evitar problemas de rendimiento, se pueden instalar varios servidores de grabación de sesiones en diferentes equipos y dirigir los agentes de grabación de sesiones a ellos. Un agente solo puede dirigirse a un servidor a la vez.

Implementación recomendada en sitios de servidores

Use este tipo de implementación para la grabación de sesiones de una o varios sitios de servidores. El Agente de grabación de sesiones está instalado en cada VDA de SO de servidor del sitio. El sitio reside en un centro de datos detrás de un firewall. Los componentes de administración de la funcionalidad Grabación de sesiones (la Base de datos, el Servidor y la Consola de directivas de grabación de sesiones) se instalan en otros servidores y el Reproductor de grabación de sesiones se instala en una estación de trabajo, todo ello detrás de un firewall, no en el centro de datos. Fuera del firewall, en un entorno de red no seguro, se encuentran los clientes de XenApp, tales como estaciones de trabajo, dispositivos móviles y equipos portátiles.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Notas de implementación importantes

- Para habilitar la comunicación entre los componentes de la función Grabación de sesiones, debe instalarlos en el mismo dominio o en dominios de confianza que tengan una relación de confianza transitiva. El sistema no puede instalarse en un grupo de trabajo o en dominios que tienen una relación de confianza externa.
- Debido a la gran cantidad de gráficos y al uso intensivo de memoria involucrados en la reproducción de grabaciones largas, Citrix no recomienda la instalación del Reproductor de grabación de sesiones como aplicación publicada.
- La instalación de la funcionalidad de grabación de sesiones está configurada para comunicaciones TLS/HTTPS. Asegúrese de instalar un certificado en el Servidor de grabación de sesiones y que la entidad del certificado raíz es de confianza en los componentes de grabación de sesiones.
- Si instala la Base de datos de grabación de sesiones en un servidor independiente que ejecuta SQL Server 2016 Express Edition, SQL Server 2014 Express Edition, SQL Server 2012 Express Edition o SQL Server 2008 R2 Express Edition, el servidor debe tener el protocolo TCP/IP habilitado y el servicio SQL Server Browser en ejecución. Estos parámetros se encuentran inhabilitados de forma predeterminada, pero es necesario habilitarlos para que el Servidor de grabación de sesiones se comunique con la base de datos. Para obtener más información sobre cómo habilitar estos parámetros, consulte los artículos de Microsoft Habilitar el protocolo de red TCP/IP para SQL Server y Servicio SQL Server Browser.
- Considere los efectos del uso compartido de sesiones cuando planifique la implementación de la grabación de sesiones. El hecho de que las aplicaciones publicadas compartan sesiones puede entrar en conflicto con las reglas de directiva de Grabación de sesiones para aplicaciones publicadas. La funcionalidad Grabación de sesiones asigna la directiva activa a la primera aplicación publicada que abra el usuario. Después de que el usuario abre la primera aplicación, toda aplicación que se abra posteriormente durante la misma sesión seguirá la directiva que se utilizó para la primera aplicación. Por ejemplo, si una directiva indica que solamente Microsoft Outlook debe grabarse, la grabación se iniciará cuando el usuario abra Outlook. Sin embargo, si el usuario abre seguidamente una aplicación publicada Microsoft Word (mientras Outlook se está ejecutando), Word se grabará también. Por el contrario, si la directiva activa no especifica que se deba grabar Word, y el usuario inicia Word antes que Outlook (que debe grabarse, según la directiva), Outlook no se grabará.
- Aunque puede instalar el Servidor de grabación de sesiones en un Delivery Controller, Citrix no lo recomienda debido a problemas de rendimiento.
- Puede instalar la Consola de directivas de grabación de sesiones en un Delivery Controller.
- Puede instalar el Servidor de grabación de sesiones y la Consola de directivas de grabación de sesiones en el mismo sistema.
- Compruebe que el nombre NetBIOS del Servidor de grabación de sesiones no supera los 15 caracteres (Microsoft tiene un límite de 15 caracteres en la longitud del nombre de host).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recomendaciones de seguridad

Dec 05, 2017

La funcionalidad de grabación de sesiones está diseñada para ser implementada dentro de una red segura y para que los administradores accedan a ella. La instalación estándar se diseñó para que sea simple y las funciones de seguridad tal como la firma digital y el cifrado son configuraciones opcionales.

La comunicación entre los componentes de grabación de sesiones se logra a través de Internet Information Services (IIS) y Microsoft Message Queuing (MSMQ). IIS proporciona el vínculo de comunicación de servicios Web entre cada componente de la grabación de sesiones. MSMQ ofrece un mecanismo fiable de transporte de datos para enviar los datos de las sesiones grabadas desde el Agente de grabación de sesiones al Servidor de grabación de sesiones.

> ## Advertencia
>
> Modificar el Registro de forma incorrecta puede generar problemas graves que requieran 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Tenga en cuenta estas recomendaciones de seguridad cuando planee la instalación:

- Debe aislar adecuadamente los diferentes roles de administrador en la red de la empresa, en el sistema de Grabación de sesiones o en máquinas individuales. De no hacerlo, es posible que existan riesgos de seguridad que pueden afectar al funcionamiento del sistema o producir malos usos en el mismo. Citrix recomienda asignar roles de administrador distintos a personas o cuentas diferentes. Asimismo, recomienda no permitir que usuarios generales de sesión tengan privilegios de administrador en el sistema de VDA.
  - Los administradores de XenApp y XenDesktop no deben conceder el rol de administrador local de VDA a usuarios de escritorios o aplicaciones publicadas.Si el rol de administrador local es un requisito, proteja los componentes del Agente de grabación de sesiones con mecanismos de Windows o soluciones de terceros.
  - Asigne por separado al administrador de la Base de datos de grabación de sesiones y al administrador de directivas de Grabación de sesiones.
  - Citrix recomienda no asignar privilegios de administrador de VDA a usuarios generales de sesión, sobre todo cuando se utiliza el acceso con Remote PC.
  - Es crucial proteger la cuenta del administrador local del Servidor de grabación de sesiones.
  - Controle el acceso a las máquinas donde se instaló el Reproductor de grabación de sesiones. Si un usuario no está autorizado (con el rol Reproductor), no conceda a ese usuario el rol de administrador local para máquinas del Reproductor. Inhabilite el acceso anónimo.
  - Citrix recomienda usar una máquina física como servidor de almacenamiento para la Grabación de sesiones.
- La funcionalidad Grabación de sesiones graba actividades de gráficos de sesión sin tener en cuenta el carácter confidencial de los datos. En ciertos casos, pueden grabarse accidentalmente datos confidenciales (como las credenciales de usuario, la información confidencial y las pantallas de terceros, entre otros). Lleve a cabo las siguientes medidas para evitar riesgos:

  + Inhabilite el volcado de la memoria principal de agentes VDA, a menos que sea para la solución de problemas concretos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para inhabilitar el volcado de memoria principal:

1. Haga clic con el botón secundario en **Mi PC** y, a continuación, haga clic en **Propiedades**.
2. Haga clic en la ficha **Avanzado**, y, a continuación, en **Inicio y recuperación**, haga clic en **Configuración**.
3. En **Escribir información de depuración**, seleccione **(ninguno)**.

Consulte el artículo de Microsoft https://support.microsoft.com/es-es/kb/307973.

+ Los propietarios de la sesión deben notificar a los asistentes que las reuniones en línea y el software de asistencia remota pueden grabarse si se está grabando una sesión de escritorio.

+ Compruebe que no aparece ninguna información de seguridad ni credenciales de inicio de sesión en las aplicaciones Web ni locales publicadas o utilizadas dentro de la empresa. De lo contrario, se grabarán mediante la Grabación de sesiones.

+ Los usuarios deben cerrar las aplicaciones que puedan exponer información confidencial antes de cambiar a una sesión remota de ICA.

+ Le recomendamos solo los métodos de autenticación automática (por ejemplo, tarjetas inteligentes o Single Sign-On) para acceder a los escritorios publicados o a aplicaciones de Software como servicio (SaaS).

- La funcionalidad Grabación de sesiones necesita cierto hardware e infraestructura de hardware (por ejemplo, dispositivos de red empresarial, sistema operativo) para funcionar correctamente y para satisfacer las necesidades de seguridad. Tome medidas en las infraestructuras para impedir daños o mal uso de ellas y haga de la Grabación de sesiones una función segura y fiable.
  - Proteja apropiadamente la infraestructura de red que respalda la Grabación de sesiones y manténgala disponible.
  - Citrix recomienda usar una solución de seguridad externa o un mecanismo de Windows para proteger los componentes de Grabación de sesiones. Los componentes de Grabación de sesiones son:
    - En el Servidor de grabación de sesiones
      - Procesos: SsRecStoragemanager.exe y SsRecAnalyticsService.exe
      - Servicios: CitrixSsRecStorageManager y CitrixSsRecAnalyticsService
      - Todos los archivos de la carpeta de instalación del Servidor de grabación de sesiones
      - Las claves del Registro de HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Server
    - En el Agente de grabación de sesiones
      - Proceso: SsRecAgent.exe
      - Servicio: CitrixSmAudAgent
      - Todos los archivos de la carpeta de instalación del Agente de grabación de sesiones
      - Las claves del Registro de HOTKEY_LOCAL_MACHINE\Software\Citrix\SmartAuditor\Agent
- Defina la lista de control de acceso (ACL) para Message Queuing (MSMQ) en el Servidor de grabación de sesiones para restringir las máquinas VDA o VDI que pueden enviar datos de MSMQ al Servidor de grabación de sesiones y evitar que máquinas no autorizadas envíen datos al Servidor de grabación de sesiones.

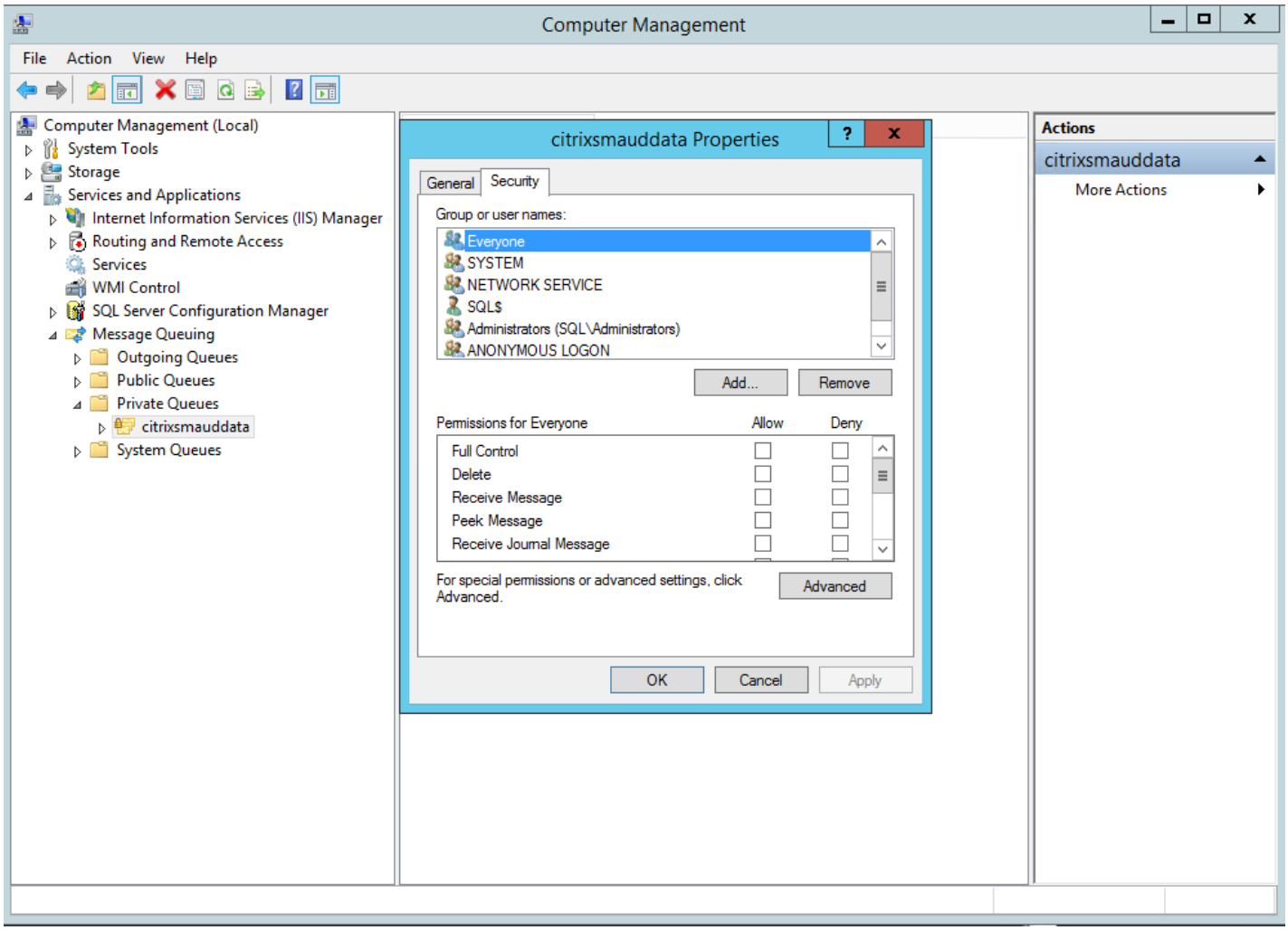
  1) Instale la funcionalidad de servidor Directory Service Integration (Integración del servicio de directorios) en cada Servidor de grabación de sesiones y máquina VDA o VDI donde esté habilitada la funcionalidad Grabación de sesiones y, a continuación, reinicie el servicio Message Queuing Server.

  2) Desde el menú **Inicio** de Windows en cada Servidor de grabación de sesiones, abra **Herramientas administrativas** > **Administración del equipo**.

  3) Abra **Servicios y aplicaciones** > **Cola de mensajes** > **Colas privadas**.

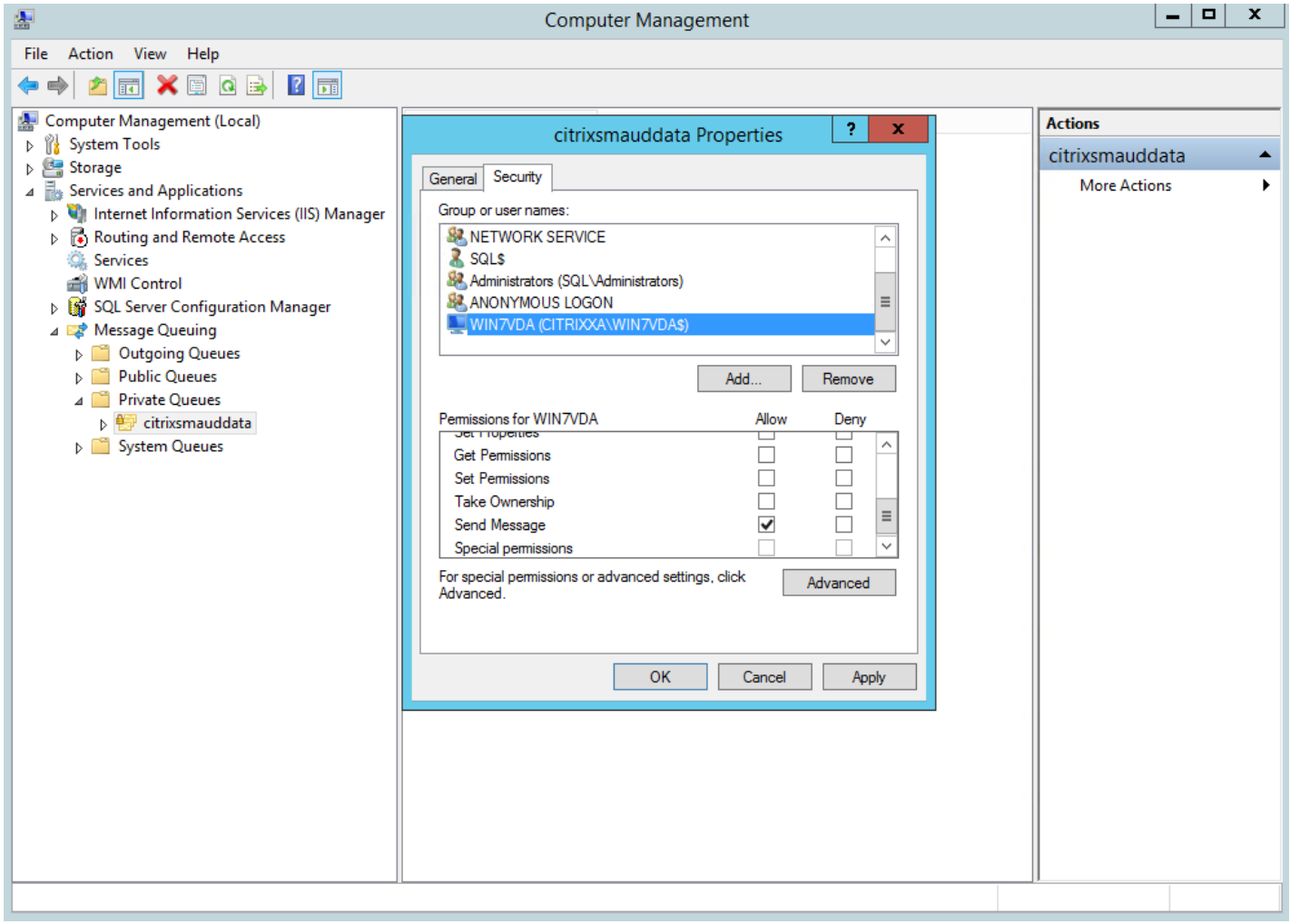
© 1999-2017 Citrix Systems, Inc. All rights reserved.

4) Haga clic en la cola privada **citrixsmauddata** para abrir la página **Propiedades** y seleccione la ficha **Seguridad**.



5) Agregue los equipos o los grupos de seguridad de los VDA que van a enviar datos de MSMQ a ese servidor y concédales el permiso **Enviar mensaje**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- Proteja adecuadamente el registro de eventos del Servidor de grabación de sesiones y de los Agentes de grabación de sesiones. Se recomienda utilizar una solución de registro remoto de Windows o de terceros para proteger el registro de eventos o redirigirlo al servidor remoto.
- Los servidores que ejecutan los componentes de Grabación de sesiones deben estar protegidos físicamente. Si es posible, coloque estos componentes bajo llave en una habitación segura a la cual solamente personal autorizado tenga acceso.
- Aísle los servidores que ejecutan los componentes de Grabación de sesiones en un dominio o una subred diferente.
- Proteja los datos de las sesiones grabadas frente al posible acceso de usuarios que acceden a otros servidores mediante la instalación de un firewall entre el Servidor de grabación de sesiones y los demás servidores.
- Mantenga actualizados el servidor de administración de grabación de sesiones y la base de datos SQL con las actualizaciones de seguridad más recientes de Microsoft.
- Restrinja el inicio de sesión de usuarios no administradores en la máquina de administración.
- Limite quién puede autorizar cambios de directivas de grabación y puede ver sesiones grabadas.
- Instale certificados digitales, utilice la función de firma de archivos de la grabación de sesiones y configure comunicaciones TLS en IIS.
- Configure MSMQ para usar HTTPS como transporte. Para ello, establezca el protocolo de MSMQ de **Propiedades del Agente de grabación de sesiones** en HTTPS. Para obtener más información, consulte Solución de problemas de MSMQ.
- Use TLS 1.1 o TLS 1.2 (recomendado) e inhabilite SSLv2, SSLv3 y TLS 1.0 en el Servidor de grabación de sesiones y la Base de datos de grabación de sesiones. Para obtener más información, consulte el artículo de Microsoft

© 1999-2017 Citrix Systems, Inc. All rights reserved.

http://support.microsoft.com/default.aspx?scid=kb;en-us;187498.

Inhabilite los conjuntos de cifrado RC4 para TLS en el Servidor de grabación de sesiones y la Base de datos de grabación de sesiones:

1. Desde el editor de directivas de grupo de Microsoft, vaya a **Configuración del equipo** > **Plantillas administrativas** > **Red** > **Opciones de configuración SSL**.
2. Establezca la directiva **Orden de conjuntos de cifrado SSL** en **Habilitada**.De manera predeterminada, esta directiva está establecida en **No configurada**.
3. Quite todos los conjuntos de cifrado RC4.

- Utilice la protección de reproducción. La protección de la reproducción es una función de grabación de sesiones que cifra los archivos grabados antes de que se descarguen al Reproductor de grabación de sesiones. De forma predeterminada, esta opción está habilitada y se encuentra en las **Propiedades del Servidor de grabación de sesiones**.
- Siga las instrucciones de NSIT para la longitud de claves y los algoritmos de cifrado.
- Configure TLS 1.2 para dar respaldo a la funcionalidad Grabación de sesiones.
  - Citrix recomienda TLS 1.2 como protocolo de comunicación para garantizar la seguridad de extremo a extremo de los componentes de Grabación de sesiones.

    Para configurar el respaldo a TLS 1.2 de la funcionalidad Grabación de sesiones:

  1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones, instale el componente y el controlador cliente de la base de datos de SQL Server y establezca una criptografía segura para .NET Framework (4 y versiones posteriores)

     a.Instale el controlador ODBC 11 (o una versión posterior) para Microsoft SQL Server.

     b. Aplique la última revisión hotfix consolidada (Hotfix Rollup) de .NET Framework.

     c.Instale ADO.NET, un cliente SQL basado en la versión de .NET Framework. Para obtener más información, consulte https://support.microsoft.com/en-us/kb/3135244.

     d. Agregue un valor DWORD SchUseStrongCrypto = 1 en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319 and HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319.

     e. Reinicie el equipo.
  2. Inicie sesión en el equipo donde se encuentra la Consola de directivas de grabación de sesiones para aplicar la última revisión hotfix consolidada de .NET Framework y establecer una criptografía segura para .NET Framework (4 y versiones posteriores). El método para establecer una criptografía segura es el mismo que en los subpasos 1-d y 1-e. No es necesario realizar estos pasos si decide instalar la Consola de directivas de grabación de sesiones en el mismo equipo que el Servidor de grabación de sesiones.

Para configurar el respaldo de TLS 1.2 en SQL Server con versiones anteriores a 2016, consulte https://support.microsoft.com/en-us/kb/3135244. Para usar TLS 1.2, configure HTTPS como el protocolo de comunicación de los componentes de Grabación de sesiones.

Para obtener información sobre cómo configurar las funcionalidades de seguridad de Grabación de sesiones, consulte el artículo CTX200868 en Knowledge Center.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Consideraciones de escalabilidad

Dec 05, 2017

La instalación y ejecución de la función de grabación de sesiones requiere pocos recursos adicionales además de los necesarios para ejecutar XenApp. Sin embargo, si planea utilizar la grabación de sesiones para grabar un gran número de sesiones o si las sesiones que planea grabar van a producir archivos de grabación muy grandes (por ejemplo, aplicaciones con muchos gráficos), tenga en cuenta los efectos en el rendimiento del sistema al planificar la implementación de la grabación de sesiones.

Para obtener más información sobre cómo implementar un sistema de Grabación de sesiones con posibilidades de ampliación, consulte el artículo de Citrix CTX200869.

Recomendaciones de hardware

Tenga en cuenta cuántos datos se enviarán a cada Servidor de grabación de sesiones y con qué rapidez pueden los servidores procesar y almacenar estos datos. La tasa a la cual los sistemas pueden almacenar los datos entrantes debe ser mayor que la tasa de entrada de datos.

Para estimar la tasa de entrada de datos, multiplique el número de grabación de sesiones por el tamaño promedio de cada grabación y divida por el período de tiempo por el cual se grabarán sesiones. Por ejemplo, puede grabar 5 000 sesiones de Microsoft Outlook de 20 MB cada una por un día de trabajo de 8 horas. En este caso, la tasa de entrada de datos es de aproximadamente 3,5 Mbps (5000 sesiones multiplicadas por 20 MB y luego dividido por 8 horas y dividido por 3600 segundos por hora).

Se puede mejorar el rendimiento optimizando el rendimiento de un solo Servidor de grabación de sesiones o instalando varios servidores de grabación de sesiones en distintas máquinas.

Hardware de disco y almacenamiento

El hardware de disco y almacenamiento son los factores más importantes a considerar cuando se planifica una implementación de grabación de sesiones. El correcto rendimiento de almacenamiento es especialmente importante. Entre más rápido se pueda escribir al disco, mayor será el rendimiento del sistema.

Las soluciones de almacenamiento adecuadas para utilizarlas con la grabación de sesiones incluyen un conjunto de discos locales controlados como matrices RAID por un controlador de disco local o por una red SAN conectada a ellos.

Nota: La funcionalidad Grabación de sesiones no debe utilizarse con almacenamiento de red (NAS), debido a los problemas de rendimiento y seguridad asociados con la escritura de datos de grabación en unidades de red.
Para una configuración de unidad local, un controlador de disco con memoria caché incorporada mejora el rendimiento. Un controlador de disco con memoria caché debe tener una batería de respaldo para asegurar la integridad de los datos en caso de interrupción de suministro eléctrico.

Capacidad de la red

Un enlace de red de 100 Mbps es adecuado para conectar con un Servidor de grabación de sesiones. Una conexión Gigabit Ethernet puede mejorar el rendimiento, pero no mejorará el rendimiento 10 veces más que un enlace de 100 Mbps.

Compruebe que los conmutadores de red utilizados por la funcionalidad Grabación de sesiones no se comparten con aplicaciones de terceros que puedan competir por el ancho de banda disponible de la red. Preferiblemente, los conmutadores de red están dedicados para usarse con el Servidor de grabación de sesiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Capacidad de procesamiento del equipo

Considere las siguientes especificaciones para el equipo en el cual se instala el Servidor de grabación de sesiones:

- Se recomienda un doble CPU o un núcleo dual de CPU
- Se recomienda 4 GB de RAM.

Especificaciones mayores que estas no mejoran el rendimiento significativamente.

Implementación de varios servidores de grabación de sesiones

Si un único servidor de grabación de sesiones no se ajusta a las necesidades de rendimiento, se pueden instalar varios servidores de grabación de sesiones en máquinas diferentes. En este tipo de implementación, cada servidor de grabación de sesiones tiene su propio almacenamiento, conmutadores de red y bases de datos dedicados. Para distribuir la carga, haga que los Agentes de grabación de sesiones de la implementación utilicen distintos servidores de grabación de sesiones.

Escalabilidad de la base de datos

La base de datos de Grabación de sesiones requiere Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 o Microsoft SQL Server 2008 R2. El volumen de datos que se envía a la base de datos es muy pequeño ya que la base de datos almacena solamente metadatos de las sesiones grabadas. Los archivos de las sesiones grabadas en sí se escriben a un disco aparte. Normalmente, cada sesión grabada necesita solamente 1KB de espacio en la base de datos, a menos que se utilice la API de eventos de grabación de sesiones para agregar eventos en la sesión.

Las ediciones Express de Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012 y Microsoft SQL Server 2008 R2 imponen una limitación de tamaño de 10 GB a la base de datos. En 1KB por sesión grabada, la base de datos puede catalogar aproximadamente cuatro millones de sesiones. Otras ediciones Microsoft SQL Server no tienen restricciones de tamaño de la base de datos y están limitadas solamente por el espacio de disco disponible. Cuando aumenta el número de sesiones en la base de datos, el rendimiento de ésta y la velocidad de las búsquedas disminuye de forma insignificante.

Si no realiza personalizaciones mediante la API de eventos de grabación de sesiones, cada sesión grabada genera cuatro transacciones de base de datos: dos cuando se inicia la grabación, una cuando el usuario se conecta a la sesión que se está grabando y otra cuando la grabación finaliza. Si utiliza la API de eventos de grabación de sesiones para personalizar sesiones, cada evento grabado, susceptible de búsquedas, genera una transacción. Ya que incluso la instalación de base de datos más básica puede manipular cientos de transacciones por segundo, la carga de proceso en la base de datos no se ve afectada. El impacto es tan poco que la Base de datos de grabación de sesiones puede ejecutarse en el mismo servidor SQL Server donde hay otras base de datos, incluido el almacén de datos de XenApp o XenDesktop.

Si la implementación de la funcionalidad de grabación de sesiones requiere la catalogación de millones de sesiones grabadas en la base de datos, siga las instrucciones de Microsoft relativas a la escalabilidad de SQL Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación, actualización y desinstalación de Grabación de sesiones

Dec 05, 2017

En este capítulo, se describe cómo instalar la Grabación de sesiones desde el programa de instalación de XenApp o XenDesktop. Contiene las siguientes secciones:

Lista de verificación de instalación

Instalación de los componentes de Administración de grabación de sesiones

Configuración de Director para usar el Servidor de grabación de sesiones

Instalación del Agente de grabación de sesiones

Instalación del Reproductor de grabación de sesiones

Instalaciones automáticas

Actualización de Grabación de sesiones

Desinstalación de Grabación de sesiones

Lista de verificación de instalación

A partir de la versión 7.14, puede instalar los componentes de la Grabación de sesiones mediante el programa de instalación de XenApp o XenDesktop.

Antes de iniciar la instalación, complete esta lista:

✔	**Paso**
	Seleccione las máquinas en las que se instalarán los componentes de Grabación de sesiones y compruebe que cada equipo cumple los requisitos de hardware y software para los componentes a instalar.
	Utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de XenApp y XenDesktop. Descargue el archivo ISO del producto. Descomprima el archivo ISO o grabe un DVD del mismo.
	Si quiere utilizar el protocolo TLS para la comunicación entre los componentes de Grabación de sesiones, instale los certificados adecuados para el entorno.
	Instale todas las revisiones hotfix necesarias para los componentes de grabación de sesiones. Las revisiones hotfix se encuentran disponibles en la página de asistencia Citrix Support.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Configure Director para crear y activar las directivas de Grabación de sesiones. Para obtener más información, consulte Configuración de Director para usar el Servidor de grabación de sesiones.

Nota:

- Citrix recomienda dividir las aplicaciones publicadas en distintos grupos de entrega según sus directivas de grabación, porque compartir sesiones de aplicaciones publicadas puede entrar en conflicto con las directivas activas si se encuentran en el mismo grupo de entrega. La funcionalidad de grabación de sesiones asigna la directiva activa a la primera aplicación publicada que abra el usuario.
- Si va a usar Machine Creation Services (MCS) o Provisioning Services con XenApp, prepare el servidor para un QMId único. Si no se cumple este requisito, pueden perderse datos de las grabaciones.
- SQL Server requiere la habilitación de TCP/IP, la ejecución del servicio SQL Server Browser y el uso de la autenticación de Windows.
- Si quiere usar HTTPS, configure los certificados de servidor para TLS/HTTPS.
- Compruebe que los usuarios y los grupos locales (**Usuarios y grupos locales** > **Grupos** > **Usuarios**) tienen permiso de escritura en esta carpeta.

Instalación de los componentes de Administración de grabación de sesiones

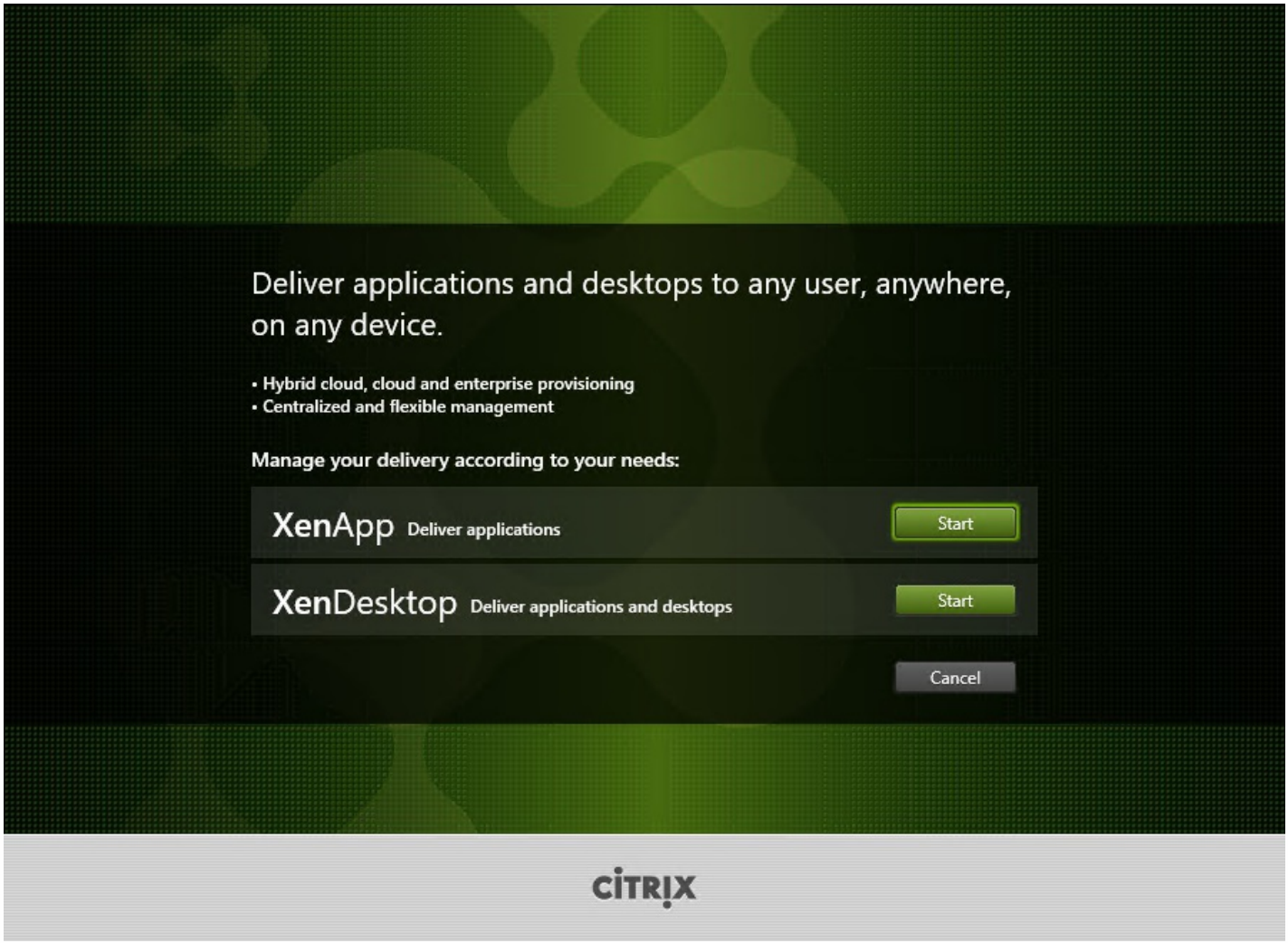
Citrix recomienda instalar los componentes de Administración de grabación de sesiones, el Agente de grabación de sesiones y el Reproductor de grabación de sesiones en servidores independientes. Los componentes de Administración de grabación de sesiones son la base de datos, el servidor y la Consola de directivas de grabación de sesiones. Con Autorun se puede elegir cuáles de estos componentes se instalarán en un servidor.

Paso 1. Descargue el software del producto e inicie el asistente

1. Si aún no ha descargado la imagen ISO de XenApp y XenDesktop, utilice las credenciales de su cuenta de Citrix para acceder a la página de descargas de XenApp y XenDesktop. Descargue el archivo ISO del producto. Descomprima el archivo ISO o grabe un DVD del mismo.
2. Utilice una cuenta de administrador local para iniciar sesión en la máquina donde quiere instalar los componentes de Administración de grabación de sesiones. Introduzca el DVD en la unidad o monte el ISO archivo. Si el programa de instalación no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.
   Se iniciará el asistente de instalación.

Paso 2. Elija el producto a instalar

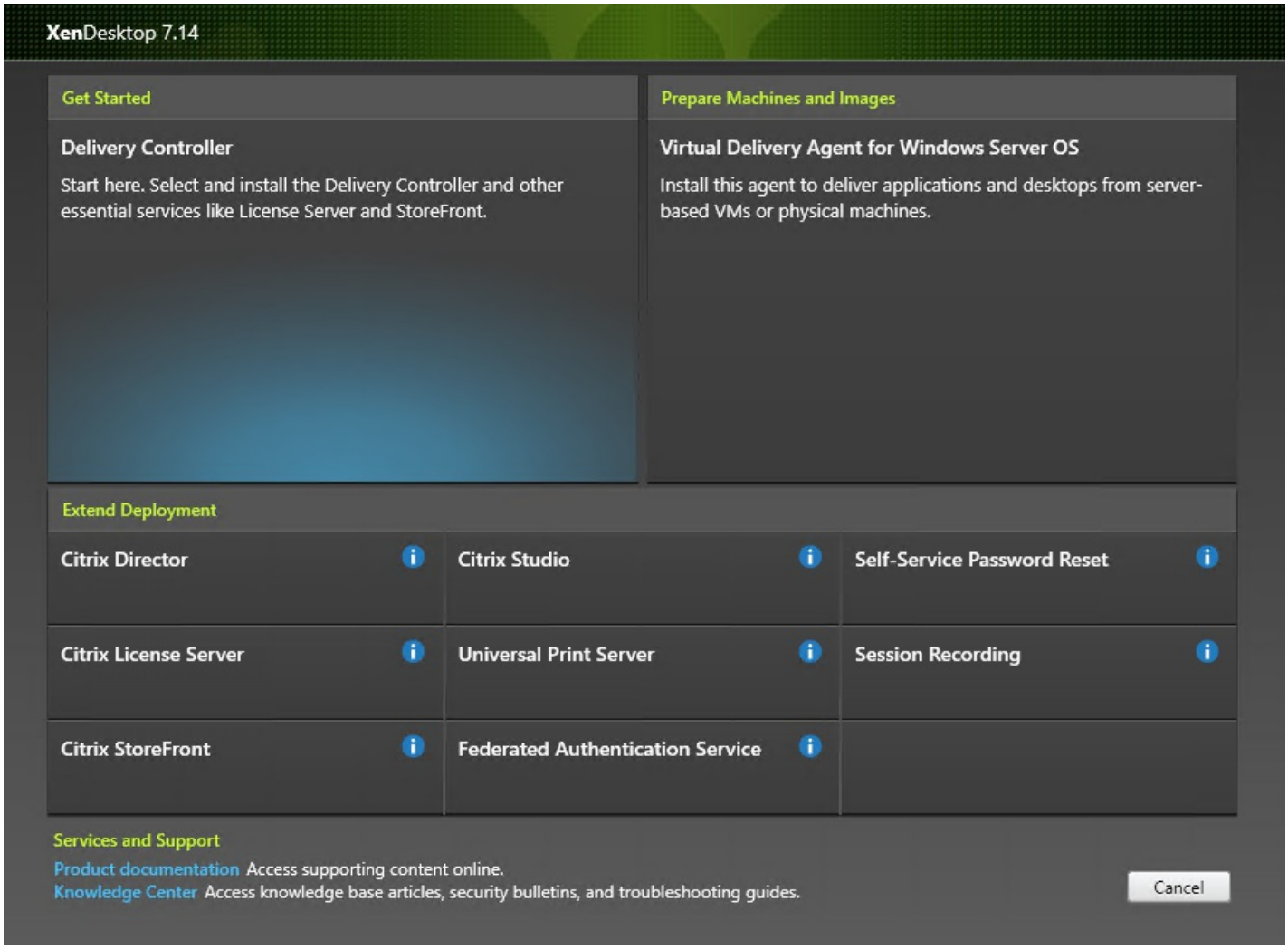
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Haga clic en **Iniciar** situado junto al producto que quiera instalar: **XenApp** o **XenDesktop**.

Paso 3. Seleccione Grabación de sesiones

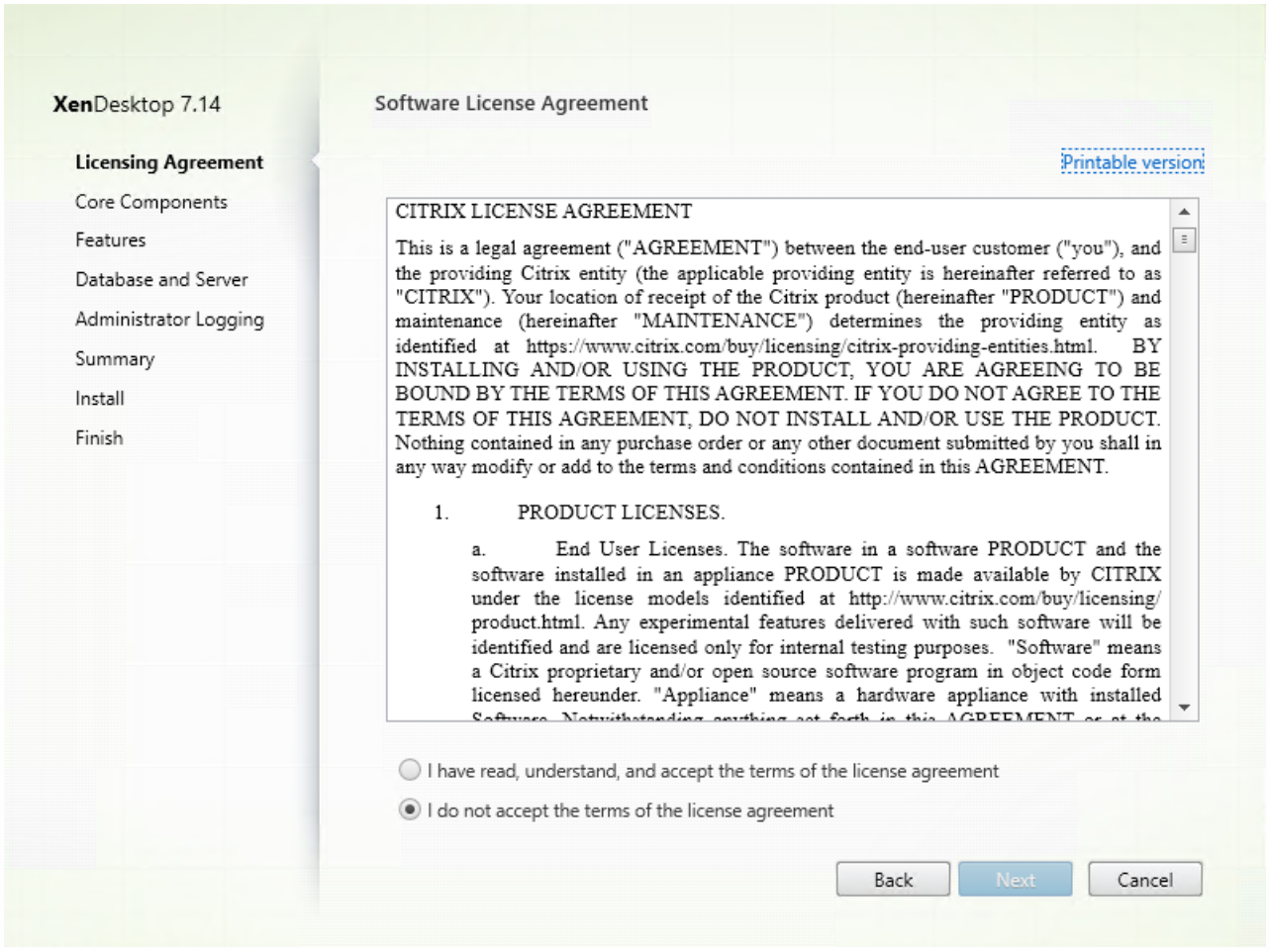
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Seleccione la entrada **Grabación de sesiones**.

Paso 4. Lea y acepte el contrato de licencia

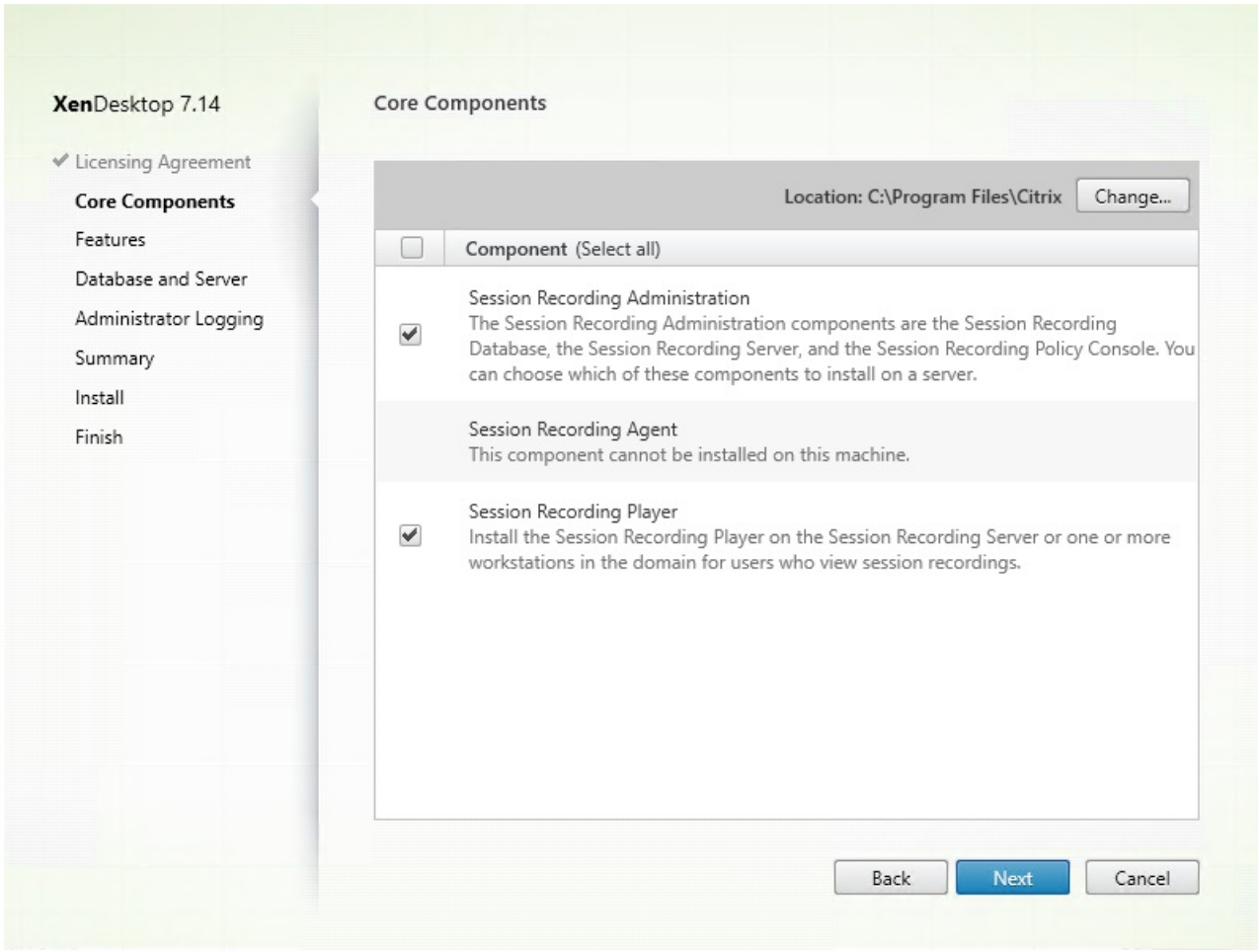
© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Contrato de licencia de software**, lea el contrato de licencia, acéptelo y haga clic en **Siguiente**.

Paso 5. Seleccione los componentes a instalar y la ubicación de la instalación

© 1999-2017 Citrix Systems, Inc. All rights reserved.

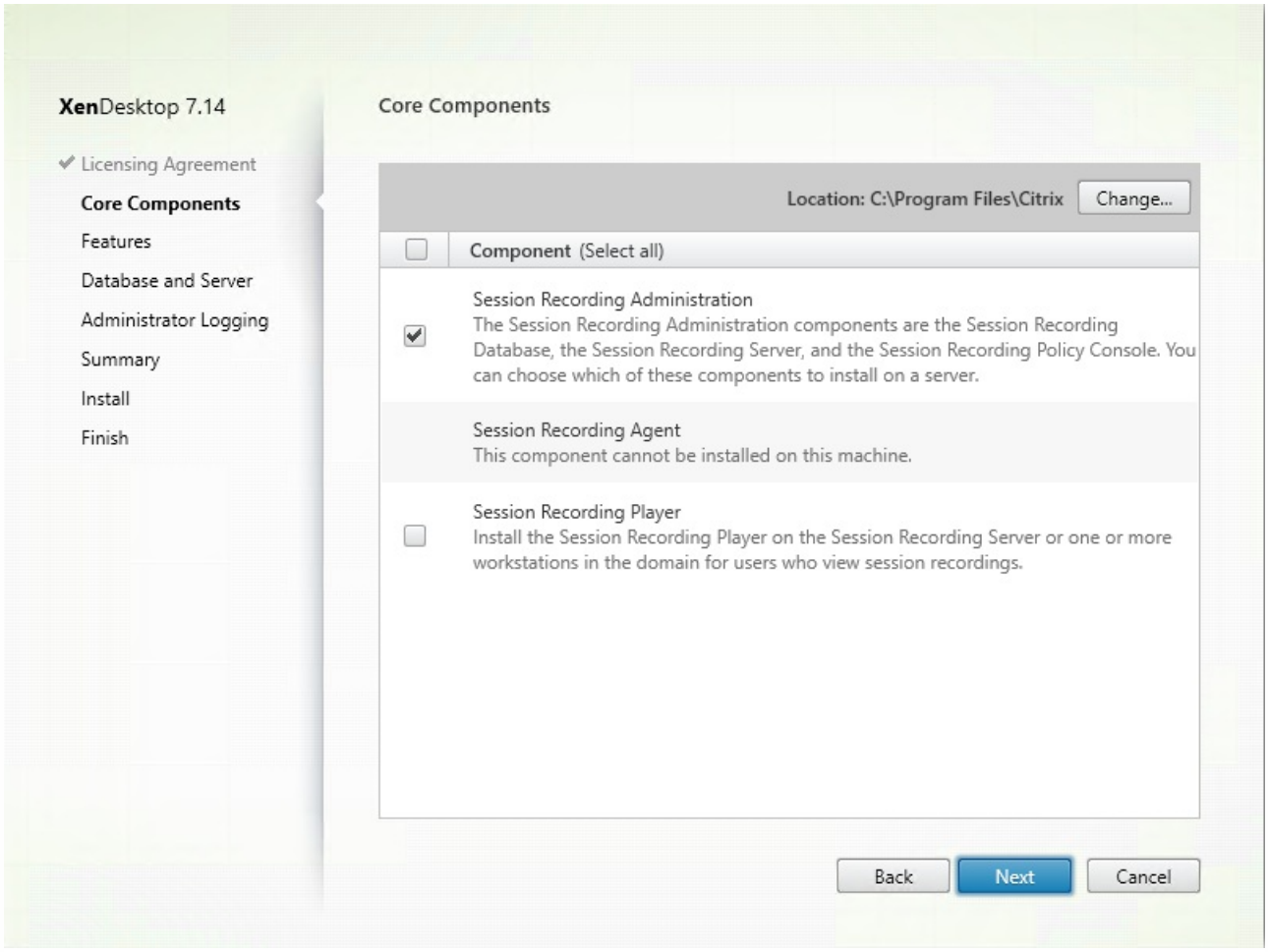


En la página **Componentes principales**:

- **Ubicación**. De forma predeterminada, los componentes se instalan en C:\Archivos de programa\Citrix. La ubicación predeterminada no pone problemas para la mayoría de las implementaciones. Aun así, puede especificar una ubicación de instalación personalizada.
- **Componente**. De forma predeterminada, están marcadas todas las casillas de verificación situadas junto a los componentes que pueden instalarse. El programa de instalación detecta si se está ejecutando en un sistema operativo de escritorio o un sistema operativo de servidor. Permite que los componentes de Administración de grabación de sesiones se instalen únicamente en un sistema operativo de servidor. No permite que el Agente de grabación de sesiones se instale en una máquina que no tiene ningún agente VDA instalado. Si intenta instalar el Agente de grabación de sesiones en una máquina que no tiene un VDA instalado, la opción **Agente de grabación de sesiones** no está disponible.

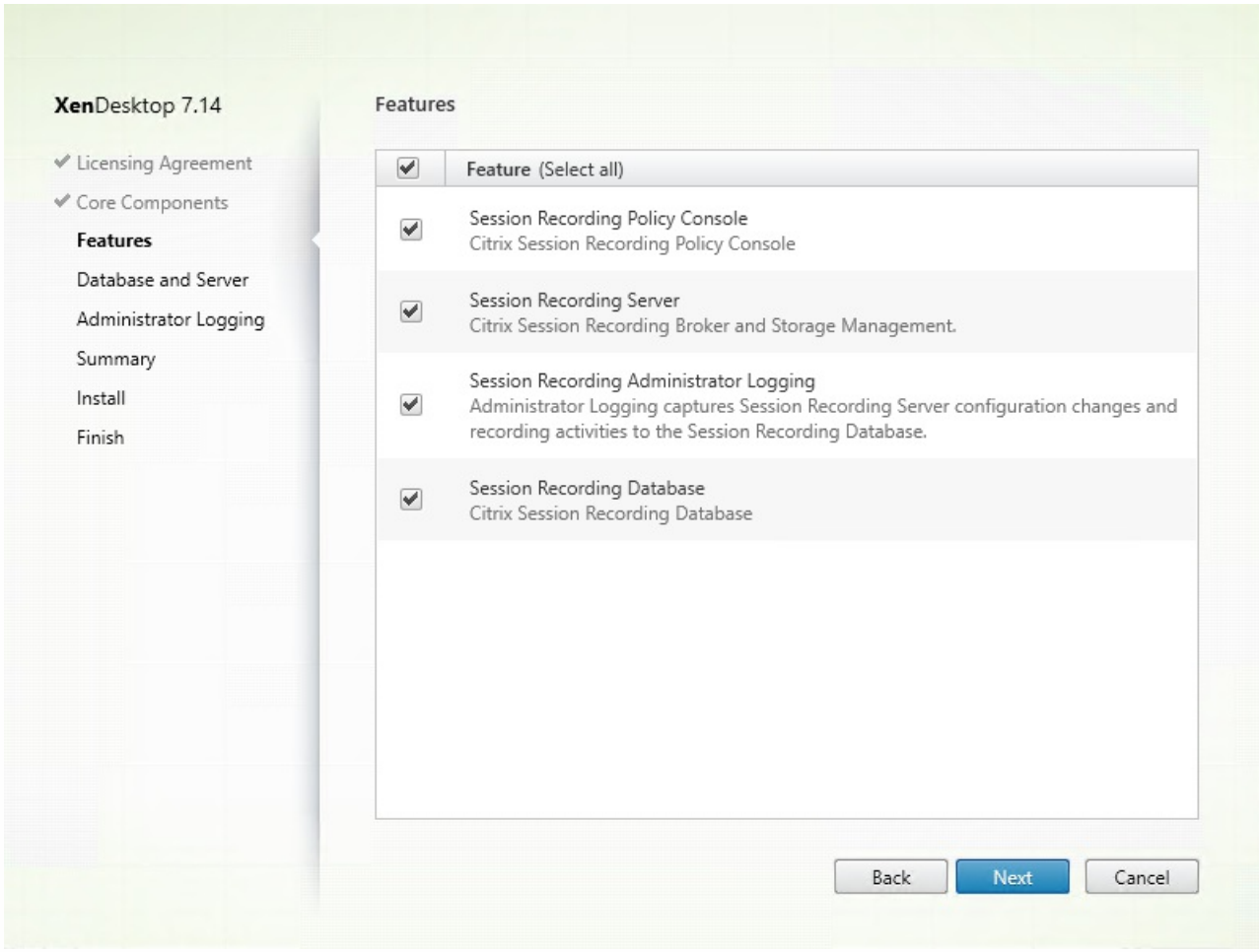
Seleccione **Administración de grabación de sesiones** y haga clic en **Siguiente**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Paso 6. Seleccione las características a instalar

© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Características**:

- De forma predeterminada, se seleccionan las casillas de verificación junto a las características que pueden instalarse. La instalación de todas estas características en un único servidor no es un problema para una prueba de concepto. Sin embargo, para un entorno de producción de gran tamaño, Citrix recomienda instalar la consola de directivas de grabación de sesiones en un servidor y el Servidor de grabación de sesiones, el Registro del administrador de grabación de sesiones y Base de datos de grabación de sesiones en otro servidor aparte. Tenga en cuenta que "Captura de registros del administrador de grabación de sesiones" es una subfunción opcional del Servidor de grabación de sesiones. Debe seleccionar el Servidor de grabación de sesiones para poder seleccionar "Captura de registros del administrador de grabación de sesiones".
- Para agregar otra característica al mismo servidor después de seleccionar e instalar unas características en él, solo puede ejecutar el paquete msi, no puede volver a ejecutar el instalador.

Seleccione las características que quiera instalar y haga clic en **Siguiente**.

Paso 6. Instalación de la Base de datos de grabación de sesiones

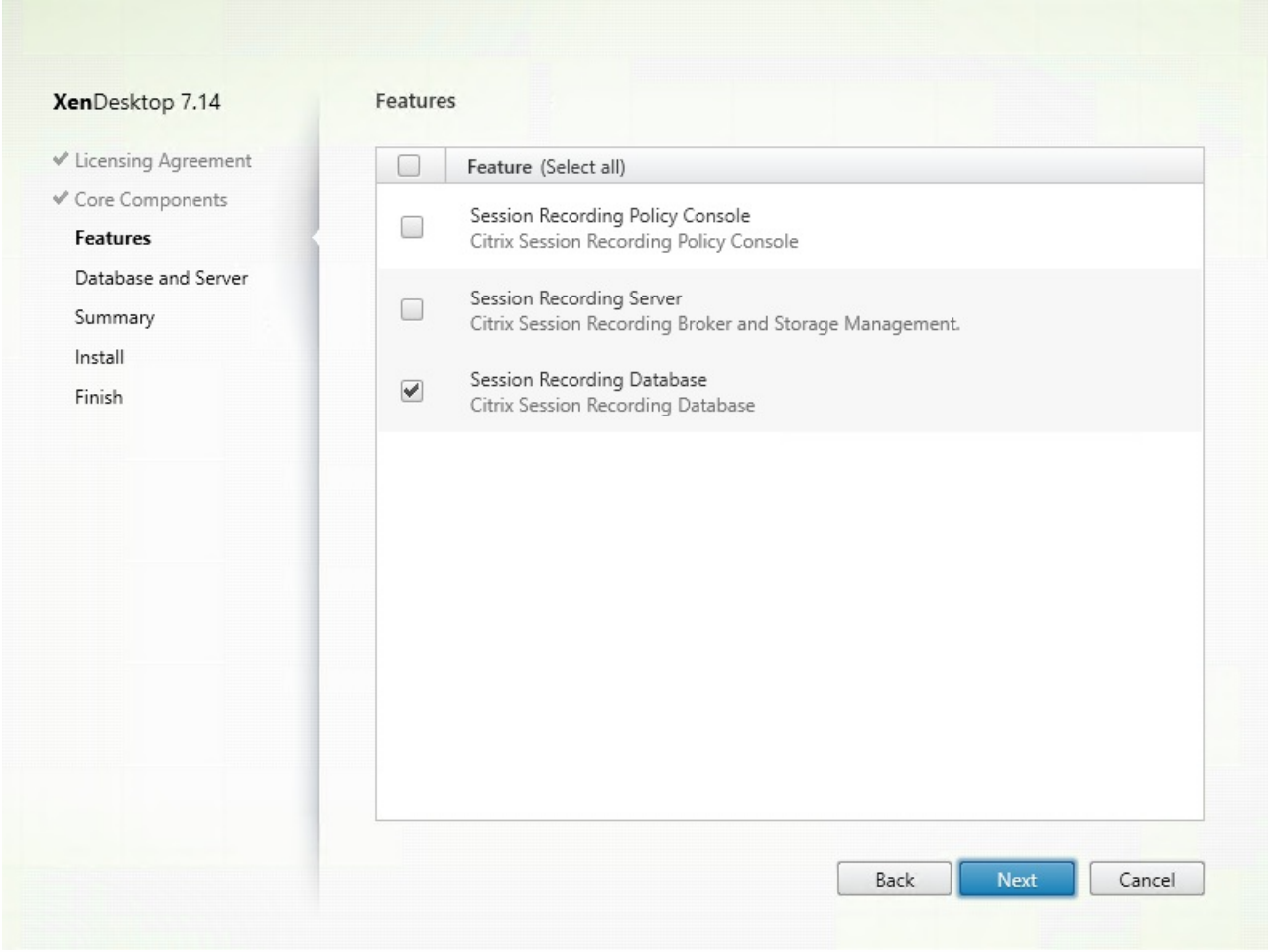
Nota: La Base de datos de grabación de sesiones no es una base de datos en sí. Es el componente que se encarga de crear y configurar las bases de datos requeridas en la instancia de Microsoft SQL Server durante la instalación. La Grabación de sesiones admite tres soluciones para la alta disponibilidad de la base de datos en función de Microsoft SQL Server. Para obtener más información, consulte Instalación de Grabación de sesiones con alta disponibilidad de base de datos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Por lo general, existen tres tipos de implementaciones de la Base de datos de grabación de sesiones y Microsoft SQL Server:

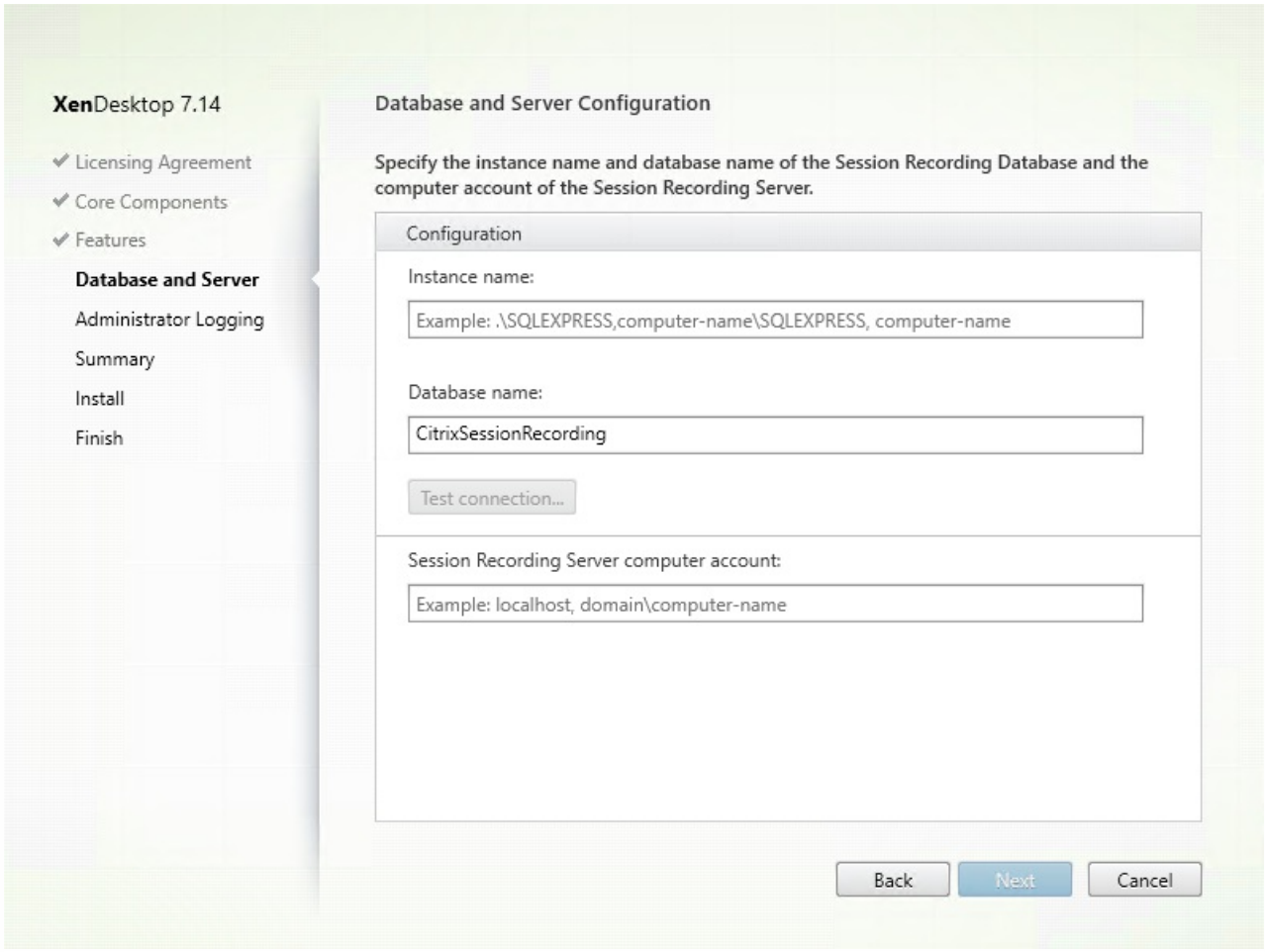
- Implementación 1. Instalar el Servidor de grabación de sesiones y la Base de datos de grabación de sesiones en la misma máquina y Microsoft SQL Server en una máquina remota. (**Opción recomendada.**)
- Implementación 2. Instalar el Servidor de grabación de sesiones, la Base de datos de grabación de sesiones y Microsoft SQL Server en la misma máquina.
- Implementación 3. Instalar el Servidor de grabación de sesiones en una máquina e instalar la Base de datos de grabación de sesiones y Microsoft SQL Server juntos en otra máquina. (**Opción no recomendada.**)

1. En la página **Características**, marque **Base de datos de grabación de sesiones** y haga clic en **Siguiente**.



2. En la página **Configuración del servidor y la base de datos**, especifique el nombre de la instancia y el nombre de la Base de datos de grabación de sesiones y la cuenta de equipo del Servidor de grabación de sesiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Configuración del servidor y la base de datos**:

- **Nombre de la instancia**. Si la instancia de la base de datos no se configuró como una instancia con nombre, solo puede usar el nombre del equipo de SQL Server. Si le dio un nombre a la instancia, use nombre-de-equipo\nombre-de-instancia como nombre de instancia de la base de datos. Para determinar el nombre de instancia de servidor que está usando, ejecute **select @@servername** en SQL Server y el valor devuelto es el nombre exacto de la instancia de la base de datos.
- **Nombre de la base de datos**. Escriba un nombre personalizado de base de datos en el cuadro de texto **Nombre de la base de datos** o use el nombre predeterminado de la base de datos mostrado en el cuadro de texto). Haga clic en **Probar conexión** para probar la conectividad a la instancia de SQL Server y la validez del nombre de la base de datos.

> ## Important
>
> Un nombre personalizado de base de datos debe contener solo mayúsculas (A-Z), minúsculas (a-z) y números (0-9), y no puede superar los 123 caracteres.

- Debe tener los permisos del rol de servidor **securityadmin** y **dbcreator** de la base de datos. Si no tiene los permisos, puede:
  - Pedir al administrador de la base de datos que le asigne esos permisos para la instalación. Una vez completada la instalación, los permisos del rol de servidor **securityadmin** y **dbcreator** ya no son necesarios y se pueden retirar sin riesgo alguno.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- O bien, utilice el paquete SessionRecordingAdministrationx64.msi (descomprima el archivo ISO y encontrará este paquete msi en ...\x64\Session Recording). Durante la instalación del msi, aparece un cuadro de diálogo que requiere las credenciales de un administrador de base de datos con los permisos del rol de servidor **securityadmin** y **dbcreator**. Especifique las credenciales correctas y haga clic en **Aceptar** para continuar con la instalación.

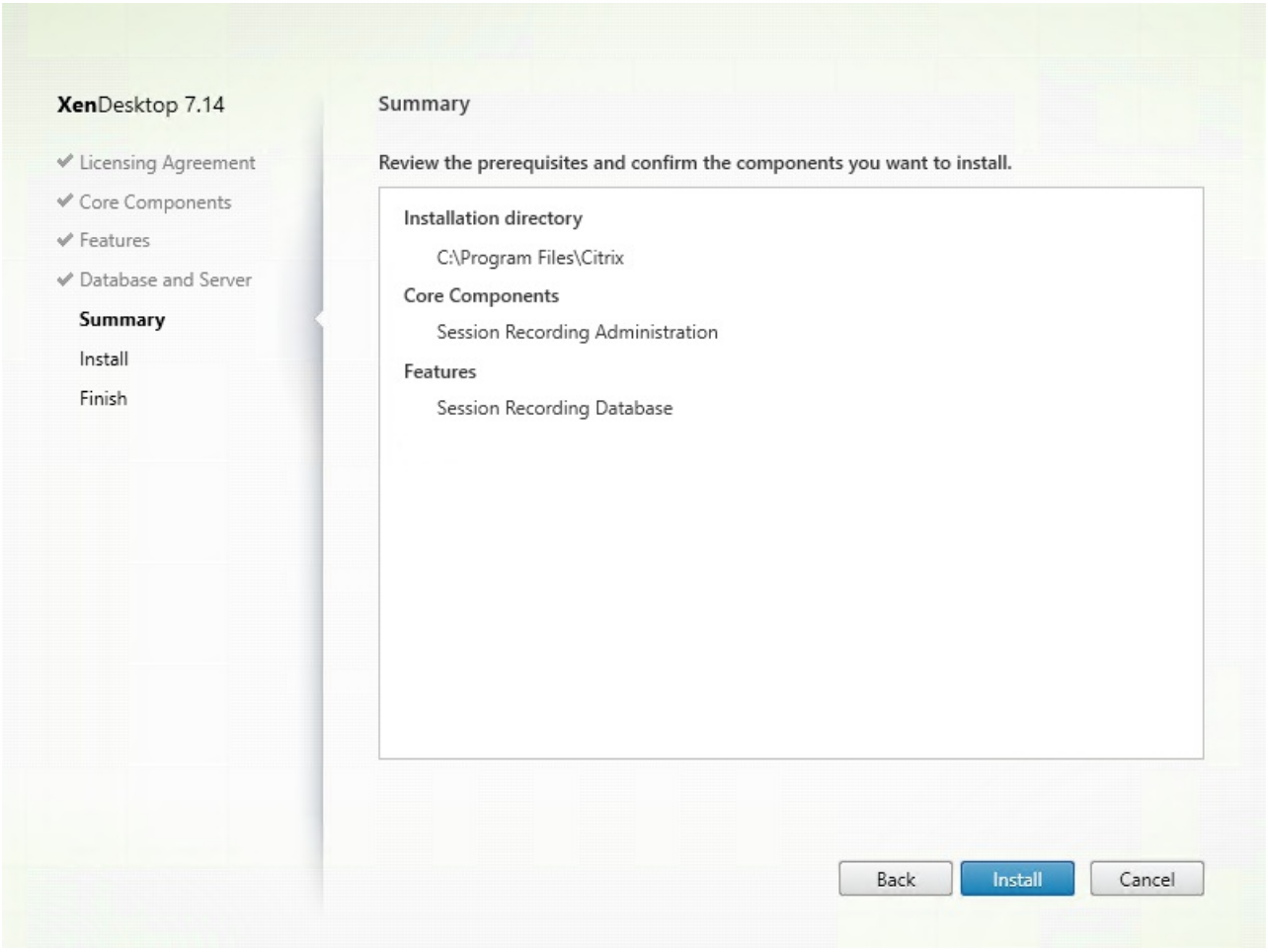
  La instalación crea la nueva base de datos para la Grabación de sesiones y agrega la cuenta de máquina del Servidor de grabación de sesiones como **db_owner**.

- **Cuenta de equipo del Servidor de grabación de sesiones**.
  - **Implementaciones 1 y 2**. Escriba **localhost** en el campo **Cuenta de equipo del Servidor de grabación de sesiones**.
  - **Implementación 3**. Escriba el nombre del equipo que aloja el Servidor de grabación de sesiones en el formato dominio\nombre-de-equipo. La cuenta de equipo del Servidor de grabación de sesiones es la cuenta de usuario para acceder a la Base de datos de grabación de sesiones.

    Nota: La instalación de los componentes de Administración de grabación de sesiones puede fallar con el código de error 1603 cuando se establece un nombre de dominio en el campo **Cuenta de equipo del Servidor de grabación de sesiones**. Como solución temporal, escriba **localhost** o el nombre de dominio\máquina de NetBIOS en el campo **Cuenta de equipo del Servidor de grabación de sesiones**.

Haga clic en **Siguiente**.

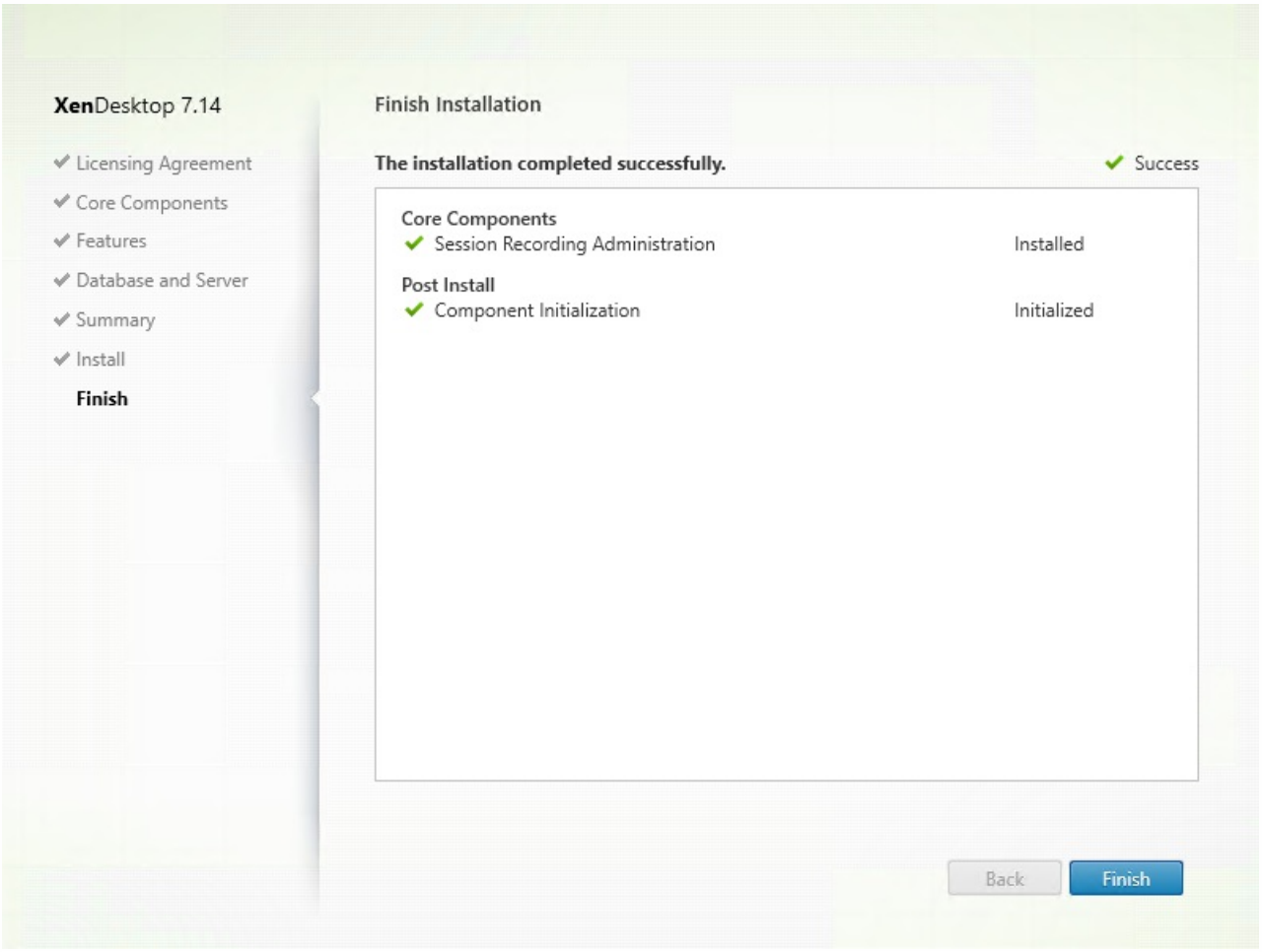
3. Revise los requisitos previos y confirme la instalación.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

La página **Resumen** muestra las opciones de instalación. Puede usar el botón **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones. O bien, haga clic en **Instalar** para iniciar la instalación.

4. Finalice la instalación.



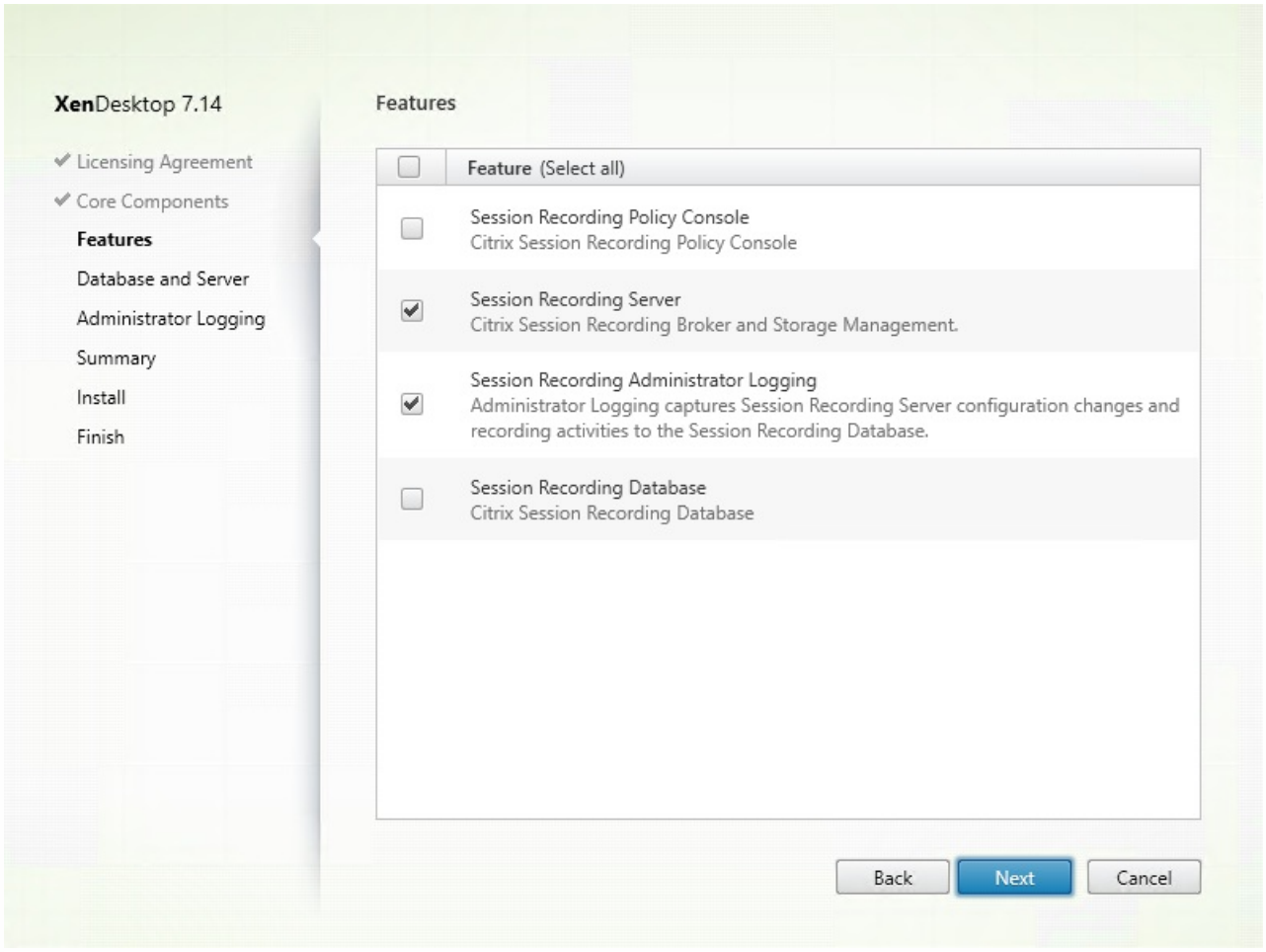
La página **Finalizar instalación** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar** para completar la instalación de la Base de datos de grabación de sesiones.

Paso 6.2. Instale el Servidor de grabación de sesiones

1. En la página **Características**, seleccione **Servidor de grabación de sesiones** y **Captura de registros del administrador de grabación de sesiones.**Haga clic en **Siguiente**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

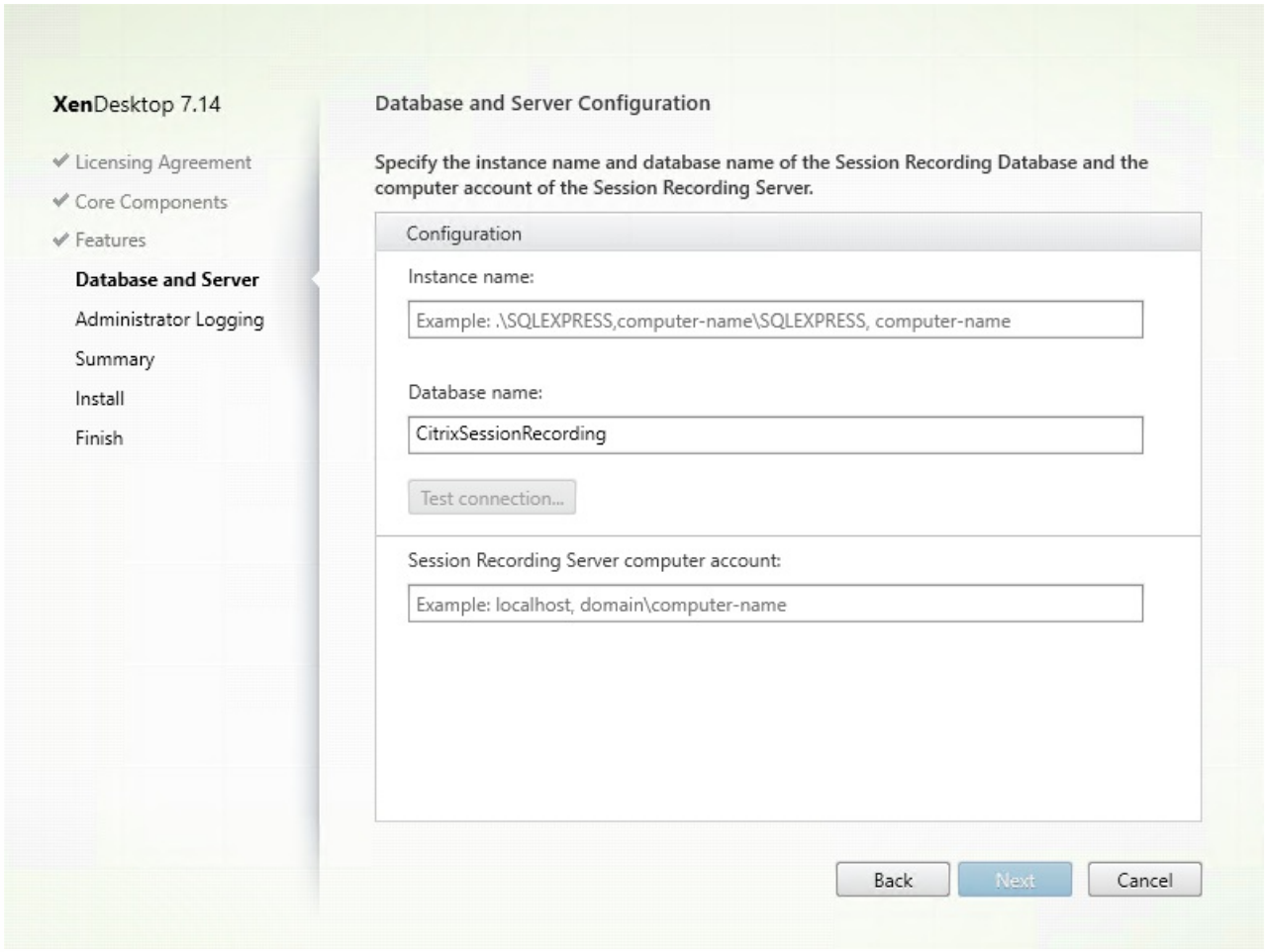


Nota:

- "Captura de registros del administrador de grabación de sesiones" es una subfunción opcional del Servidor de grabación de sesiones. Debe seleccionar el Servidor de grabación de sesiones para poder seleccionar "Captura de registros del administrador de grabación de sesiones".
- Citrix recomienda instalar la "Captura de registros del administrador de grabación de sesiones" junto con el Servidor de grabación de sesiones al mismo tiempo. Si no quiere que la "Captura de registros del administrador de grabación de sesiones" esté habilitada, puede inhabilitarla en una página posterior. Sin embargo, si decide no instalar esta característica al principio pero luego cambia de opinión y decide agregarla, solo puede agregarla manualmente desde el paquete SessionRecordingAdministrationx64.msi.

2. En la página **Configuración del servidor y la base de datos**, especifique las configuraciones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



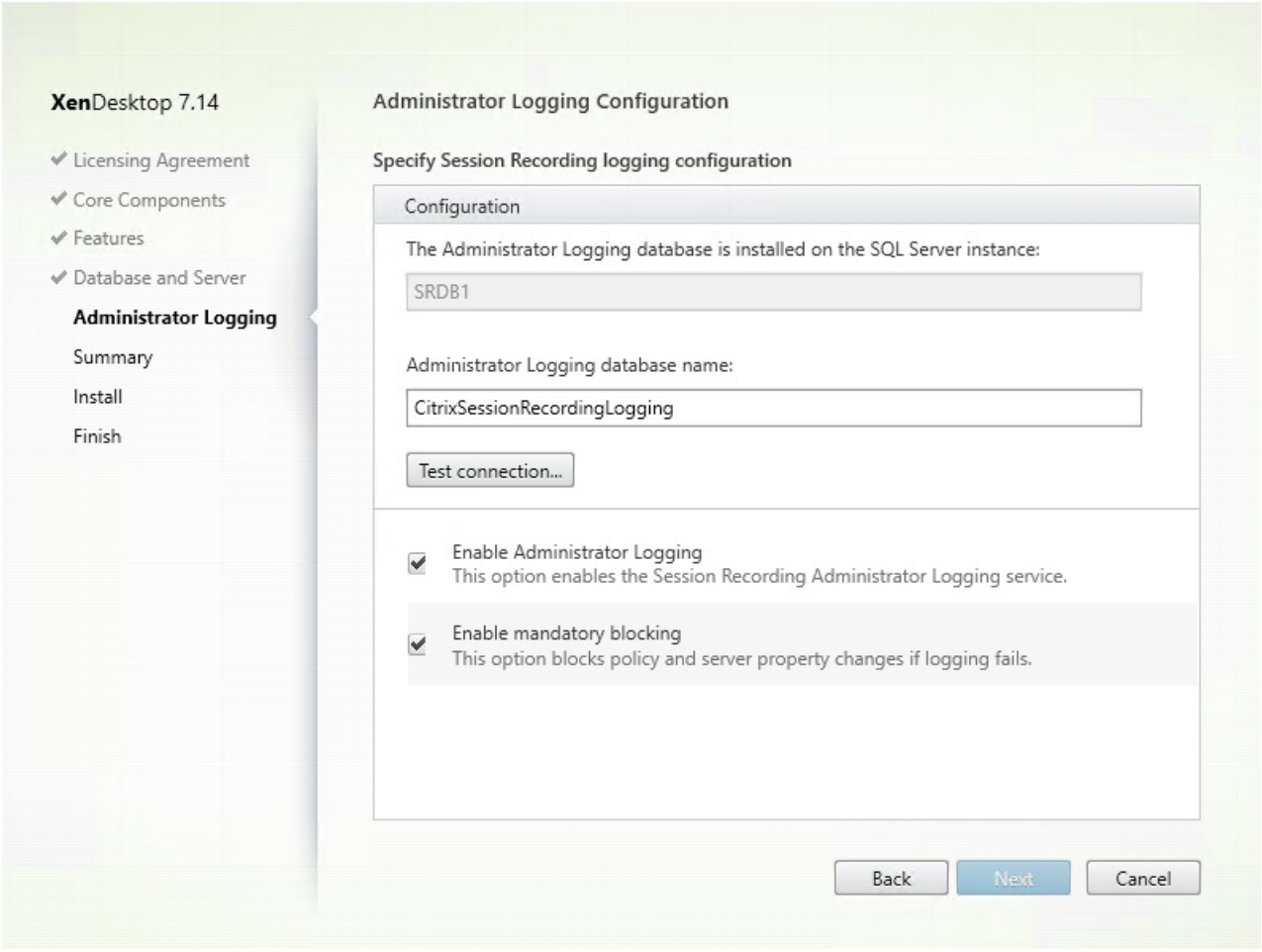
En la página **Configuración del servidor y la base de datos**:

- **Nombre de la instancia**. Introduzca el nombre del servidor SQL Server en el cuadro de texto **Nombre de la instancia**. Si está usando una instancia con nombre, introduzca nombre-de-equipo\nombre-de-instancia; de lo contrario, introduzca solo el nombre-de-equipo.
- **Nombre de la base de datos**. Escriba un nombre personalizado de base de datos en el cuadro de texto **Nombre de la base de datos** o use el nombre predeterminado **CitrixSessionRecording** en el cuadro de texto.
- Debe tener los permisos del rol de servidor **securityadmin** y **dbcreator** de la base de datos. Si no tiene los permisos, puede:
  - Pedir al administrador de la base de datos que le asigne esos permisos para la instalación. Una vez completada la instalación, los permisos del rol de servidor **securityadmin** y **dbcreator** ya no son necesarios y se pueden retirar sin riesgo alguno.
  - O bien, utilice el paquete SessionRecordingAdministrationx64.msi para instalar el Servidor de grabación de sesiones. Durante la instalación del msi, aparece un cuadro de diálogo que requiere las credenciales de un administrador de base de datos con los permisos del rol de servidor **securityadmin** y **dbcreator**. Especifique las credenciales correctas y haga clic en **Aceptar** para continuar con la instalación.
- Después de escribir el nombre de instancia y el nombre de la base de datos, haga clic en **Probar conexión** para probar la conectividad con la Base de datos de grabación de sesiones.
- Especifique la cuenta de equipo del Servidor de grabación de sesiones y, a continuación, haga clic en **Siguiente**.

3. En la página **Configuración de registro de administrador**, especifique las configuraciones para la característica de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

captura de registros de administrador.



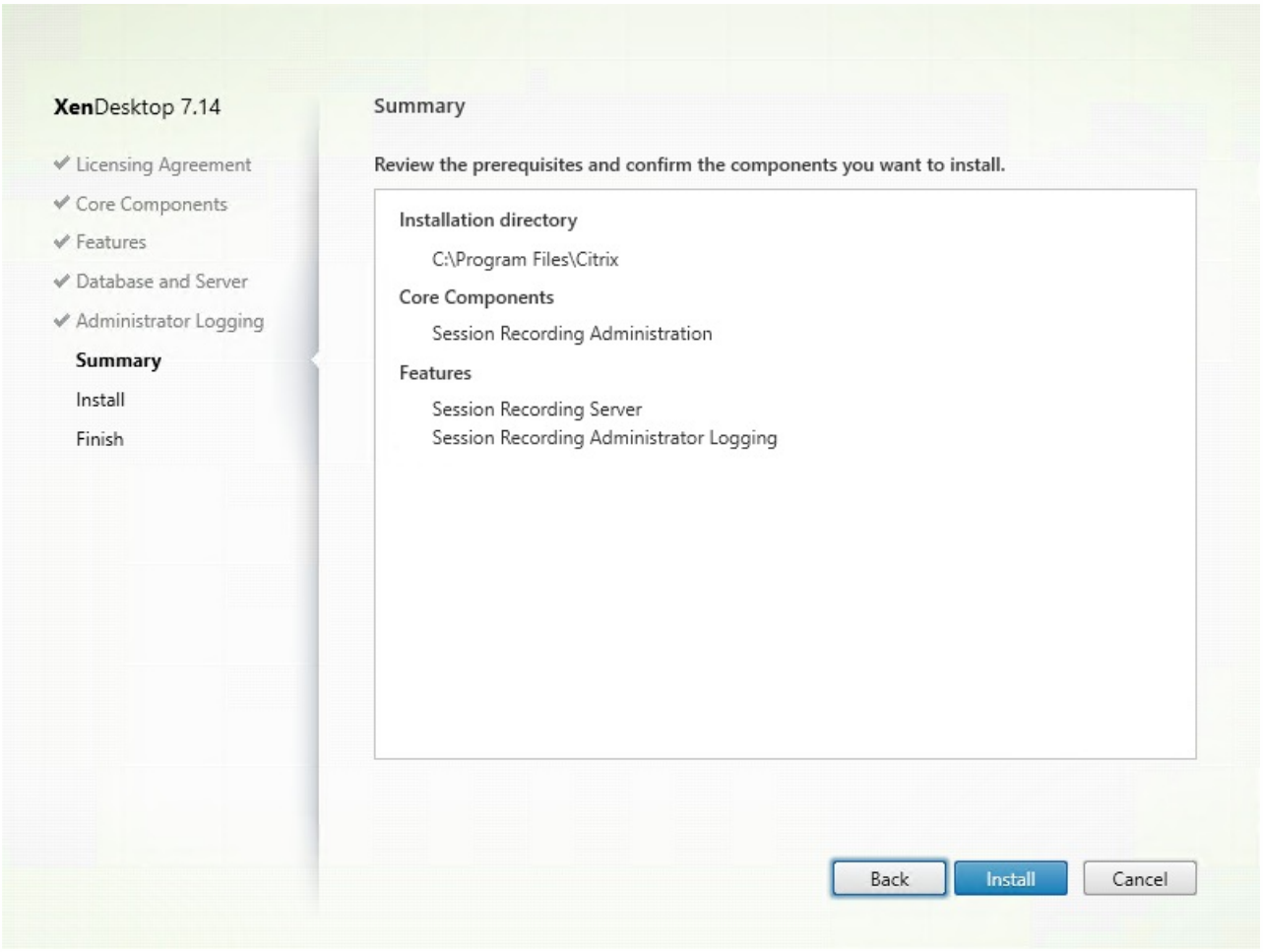
En la página **Configuración de registro de administrador**:

- **The Administration Logging database is installed on the SQL Server instance** (La base de datos de captura de registros de administrador se instala en la instancia de SQL Server). Este cuadro de texto no se puede modificar. El nombre de instancia de SQL Server para la base de datos de registros de administrador se obtiene automáticamente a partir del nombre de instancia que escribió en la página **Configuración del servidor y la base de datos**.
- **Nombre de base de datos de registro de administrador**. Si decide instalar la funcionalidad Captura de registros del administrador de grabación de sesiones, escriba un nombre personalizado para la base de datos de registros de administrador en el cuadro de texto o use el nombre predeterminado **CitrixSessionRecordingLogging**.
  Nota: El nombre de la base de datos de registros de administrador debe ser diferente del nombre de la Base de datos de grabación de sesiones establecido en el cuadro de texto **Nombre de base de datos** de la página anterior **Configuración de servidor y base de datos**.
- Después de escribir el nombre de la base de datos de registros de administrador, haga clic en **Probar conexión** para probar la conectividad con la base de datos de registros de administrador.
- **Habilitar registro de administrador**. De forma predeterminada, la característica Registro de administrador está habilitada. Puede inhabilitarla si desmarca la casilla de verificación.
- **Habilitar bloqueo obligatorio**. De forma predeterminada, el bloqueo obligatorio está habilitado. Las características normales podrían bloquearse si se produce un error en la captura de registros. Puede inhabilitar el bloqueo obligatorio si desmarca la casilla de verificación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A continuación, haga clic en **Siguiente** para continuar con la instalación.

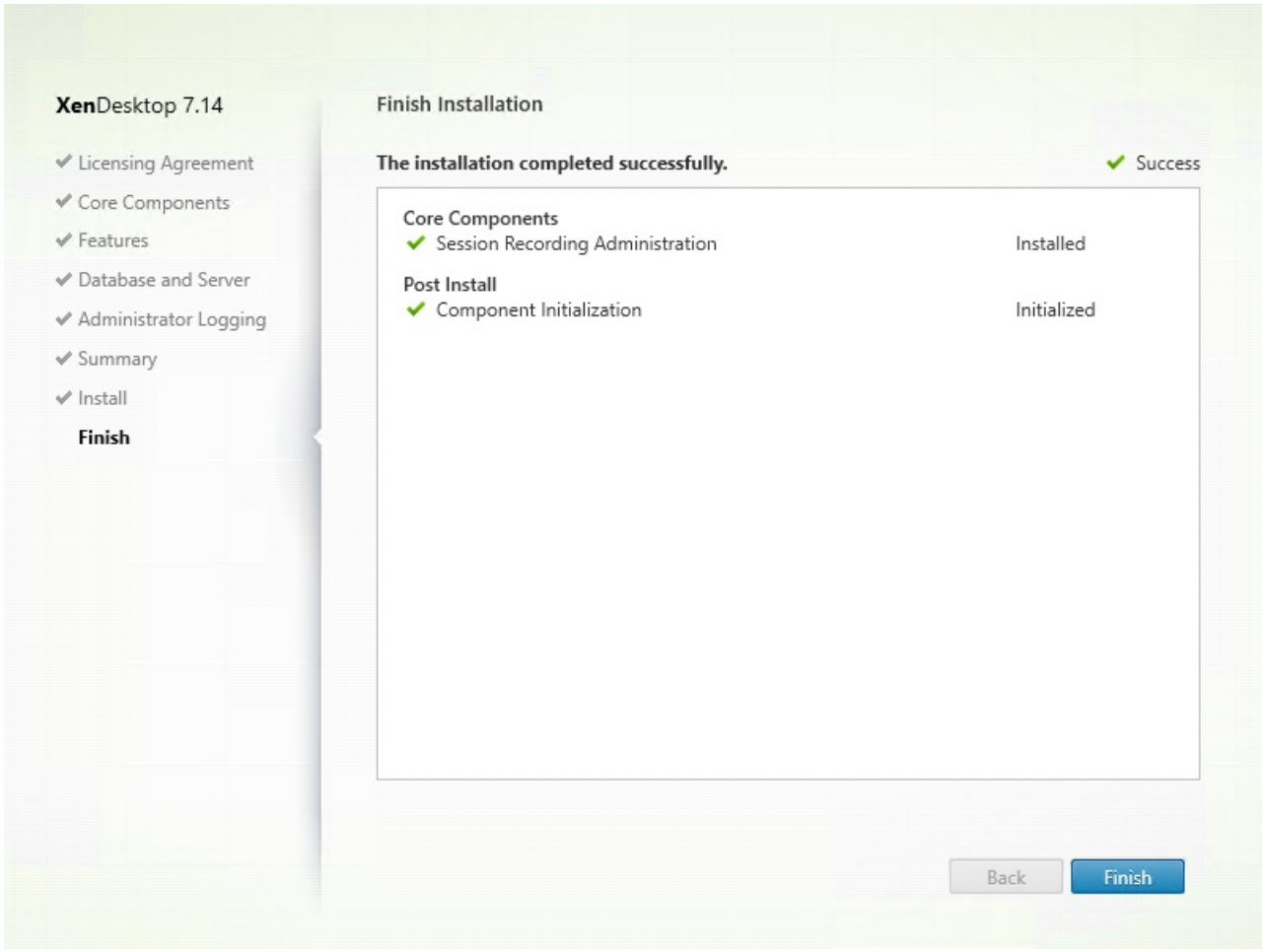
4. Revise los requisitos previos y confirme la instalación.



La página **Resumen** muestra las opciones de instalación. Puede hacer clic en **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones. O bien, haga clic en **Instalar** para iniciar la instalación.

5. Finalice la instalación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Finalizar instalación** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

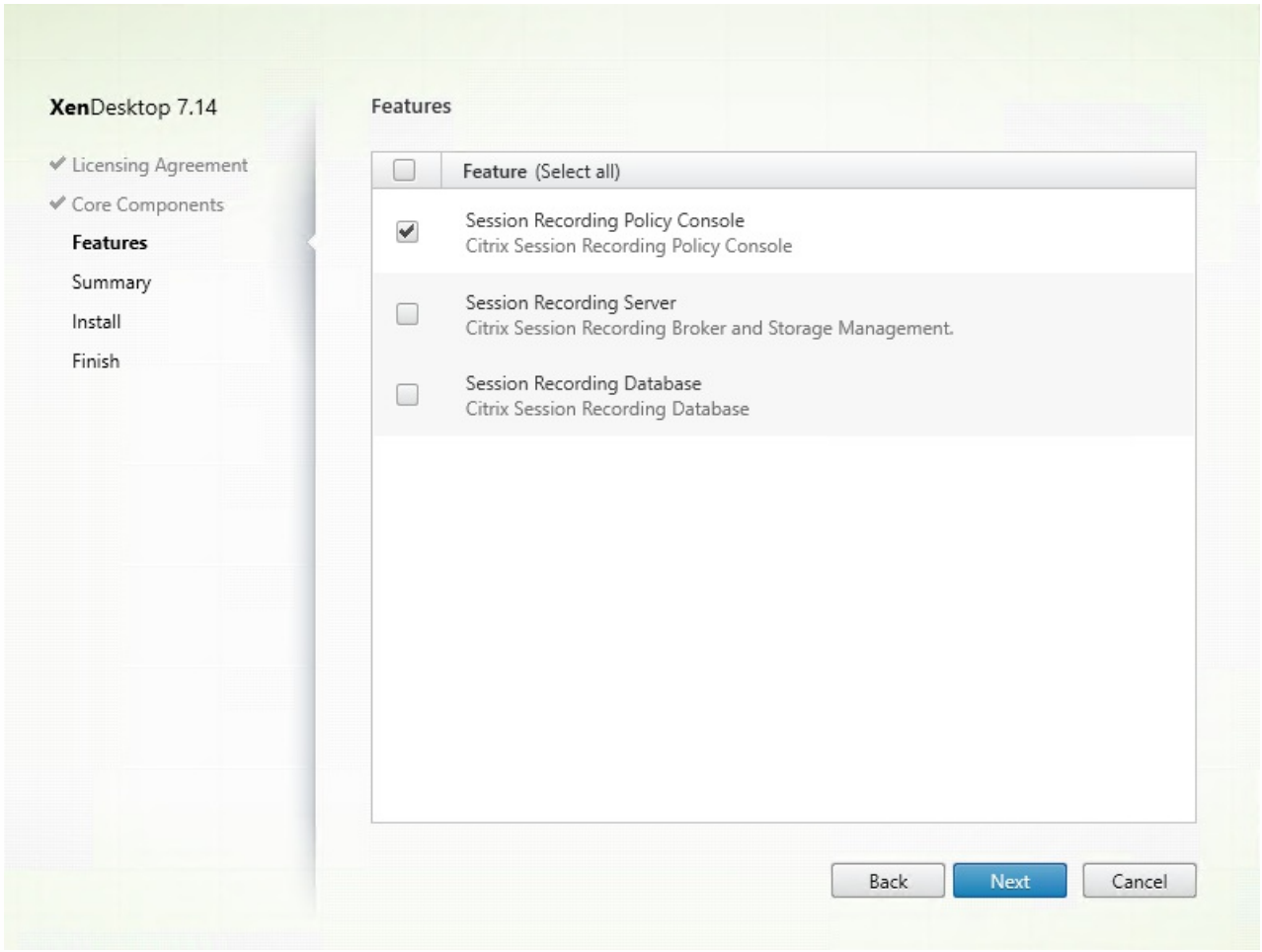
Haga clic en **Finalizar** para completar la instalación del Servidor de grabación de sesiones.

Nota: De manera predeterminada, en la instalación del Servidor de grabación de sesiones, se usa HTTPS/TLS para proteger las comunicaciones. Si TLS no está configurado en el sitio IIS predeterminado del Servidor de grabación de sesiones, use HTTP. Para ello, desmarque SSL en la consola de administración de IIS: en el sitio de Broker de grabación de sesiones, abra los parámetros de SSL y desmarque la casilla **Requerir SSL**.

Paso 6.3. Inicie la Consola de directivas de grabación de sesiones

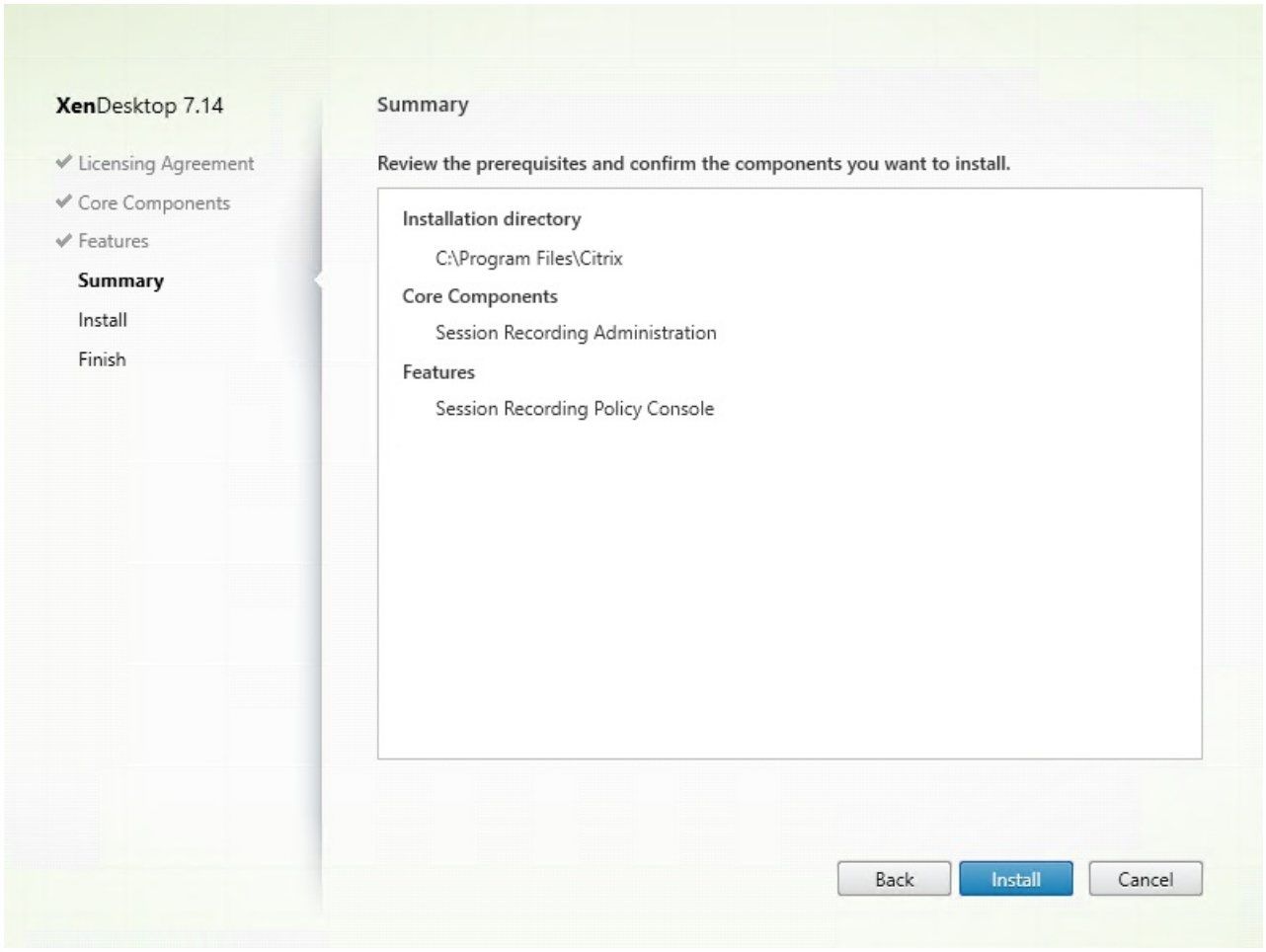
1. En la página **Características**, marque **Consola de directivas de grabación de sesiones** y haga clic en **Siguiente**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Revise los requisitos previos y confirme la instalación.

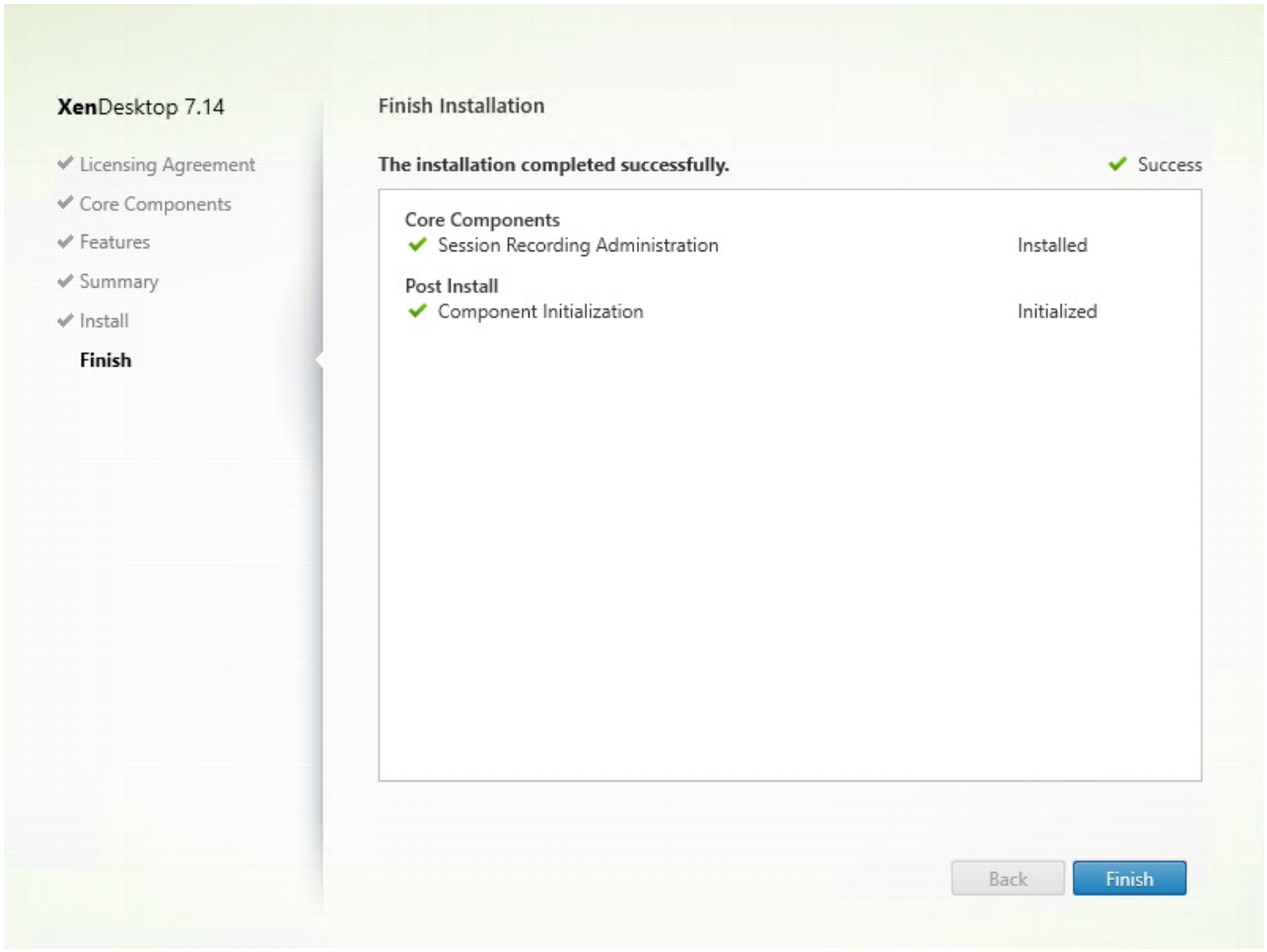
© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Resumen** muestra las opciones de instalación. Puede usar el botón **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones. O bien, haga clic en **Instalar** para iniciar la instalación.

3. Finalice la instalación.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Finalizar instalación** presenta marcas de verificación verdes para el componente y todos los requisitos previos que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar** para completar la instalación de la Consola de directivas de grabación de sesiones.

Paso 7. Instale Broker_PowerShellSnapIn_x64.msi

Importante: Para usar la consola de directivas de grabación de sesiones, debe tener instalado el complemento Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi). El programa de instalación no instala automáticamente este complemento. Busque el complemento en la imagen ISO de XenApp/XenDesktop (\layout\image-full\x64\Citrix Desktop Delivery Controller) y siga las instrucciones para instalarlo manualmente. Si no se siguen las instrucciones puede producirse un error.

Configuración de Director para usar el servidor de grabación de sesiones

Puede utilizar la consola de Director para crear y activar las directivas de Grabación de sesiones.

1. Para una conexión HTTPS, instale el certificado para confiar en el Servidor de grabación de sesiones en los Certificados raíz de confianza del servidor de Director.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Si quiere configurar el servidor de Director para usar el Servidor de grabación de sesiones, ejecute el comando: **C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording**.
3. Escriba la dirección IP o el nombre FQDN del Servidor de grabación de sesiones, el número de puerto y el tipo de conexión (HTTP o HTTPS) que usa el Agente de grabación de sesiones para conectarse al Broker de grabación de sesiones en el servidor de Director.

Instalación del Agente de grabación de sesiones

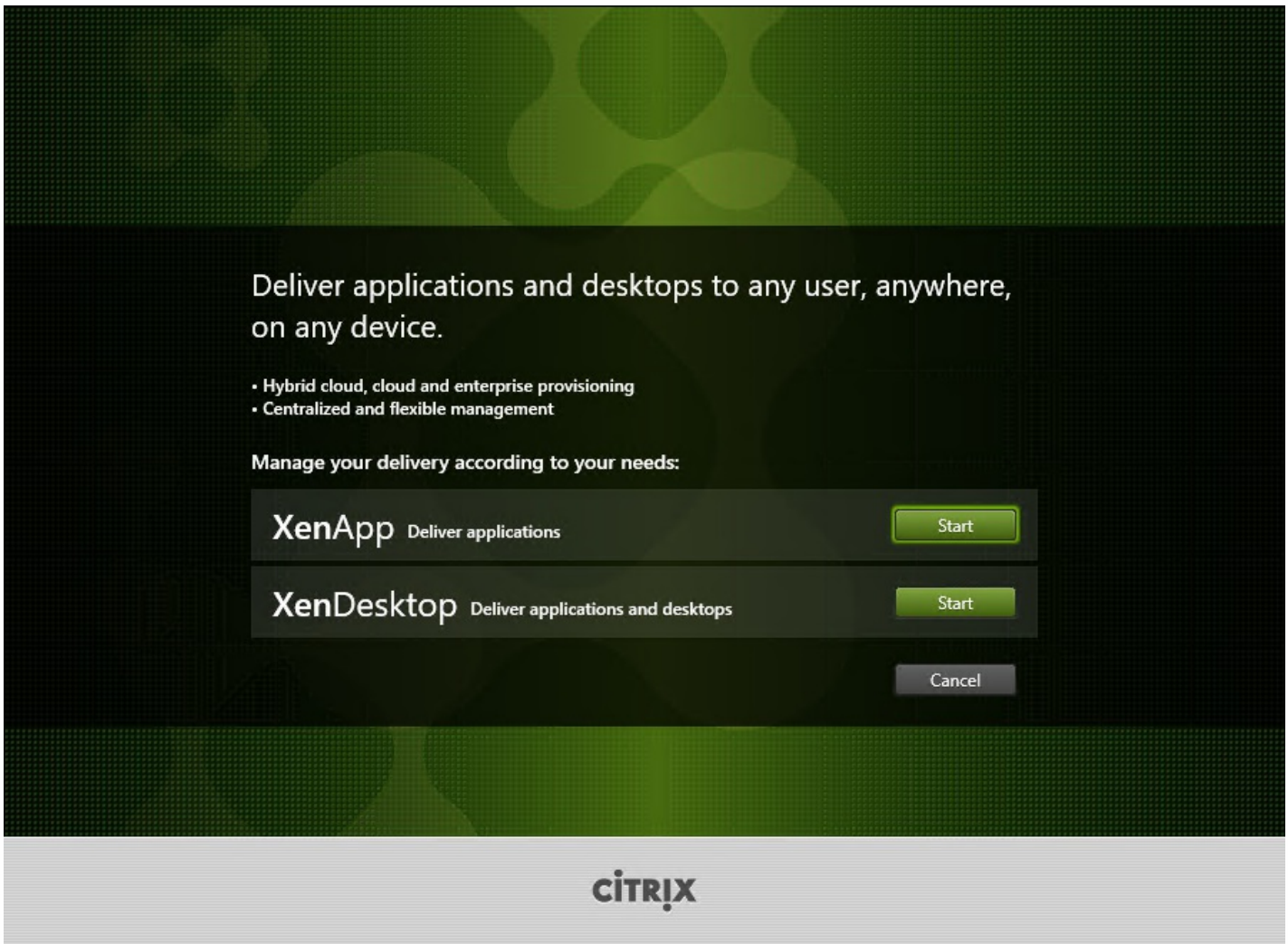
El Agente de grabación de sesiones debe instalarse en la máquina VDA o VDI donde quiera grabar sesiones.

Paso 1. Descargue el software del producto e inicie el asistente

Utilice una cuenta de administrador local para iniciar sesión en la máquina donde quiere instalar el componente Agente de grabación de sesiones. Introduzca el DVD en la unidad o monte el ISO archivo. Si el programa de instalación no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

Se iniciará el asistente de instalación.

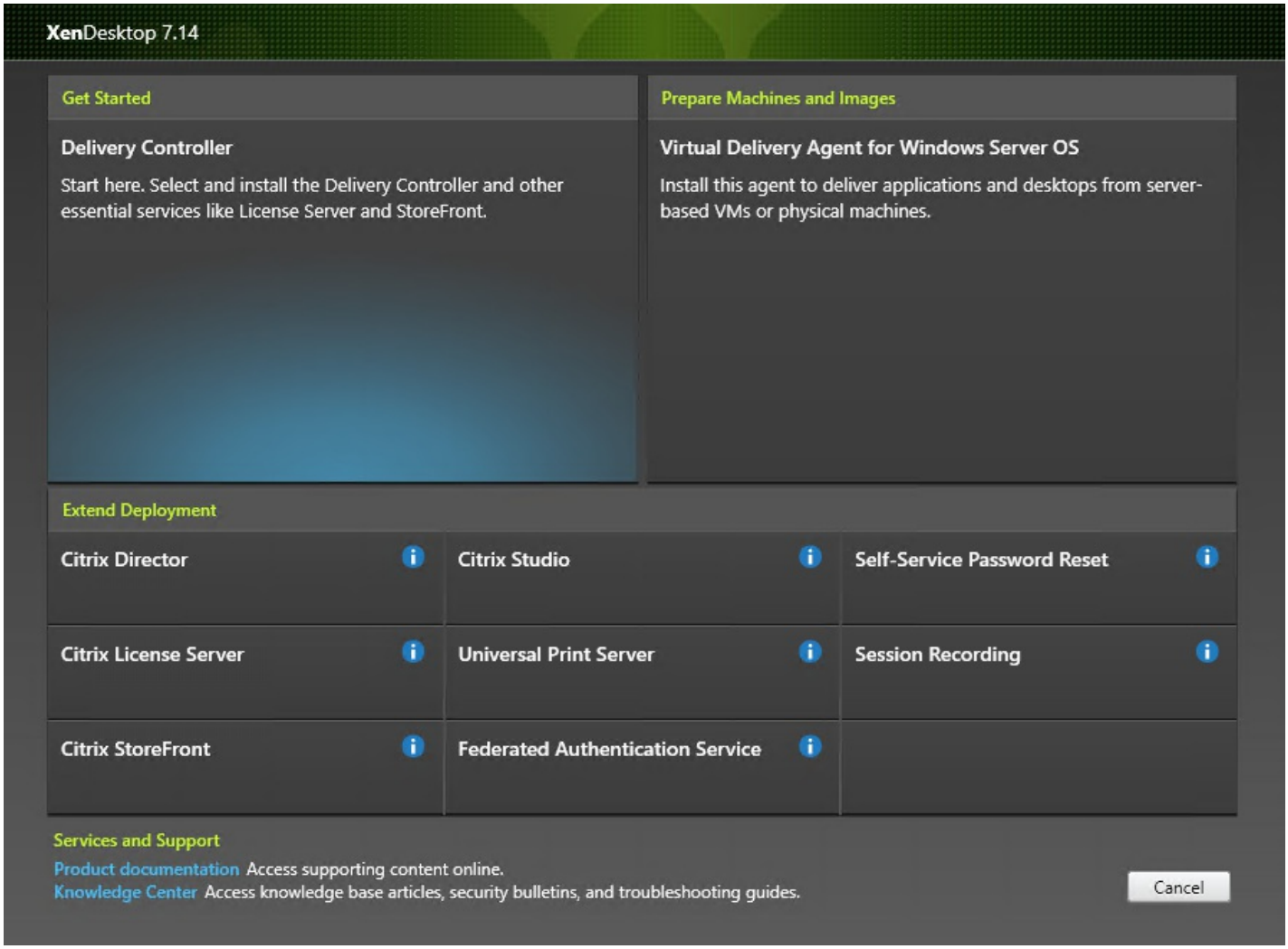
Paso 2. Elija el producto a instalar



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Haga clic en **Iniciar** situado junto al producto que quiera instalar: **XenApp** o **XenDesktop**.

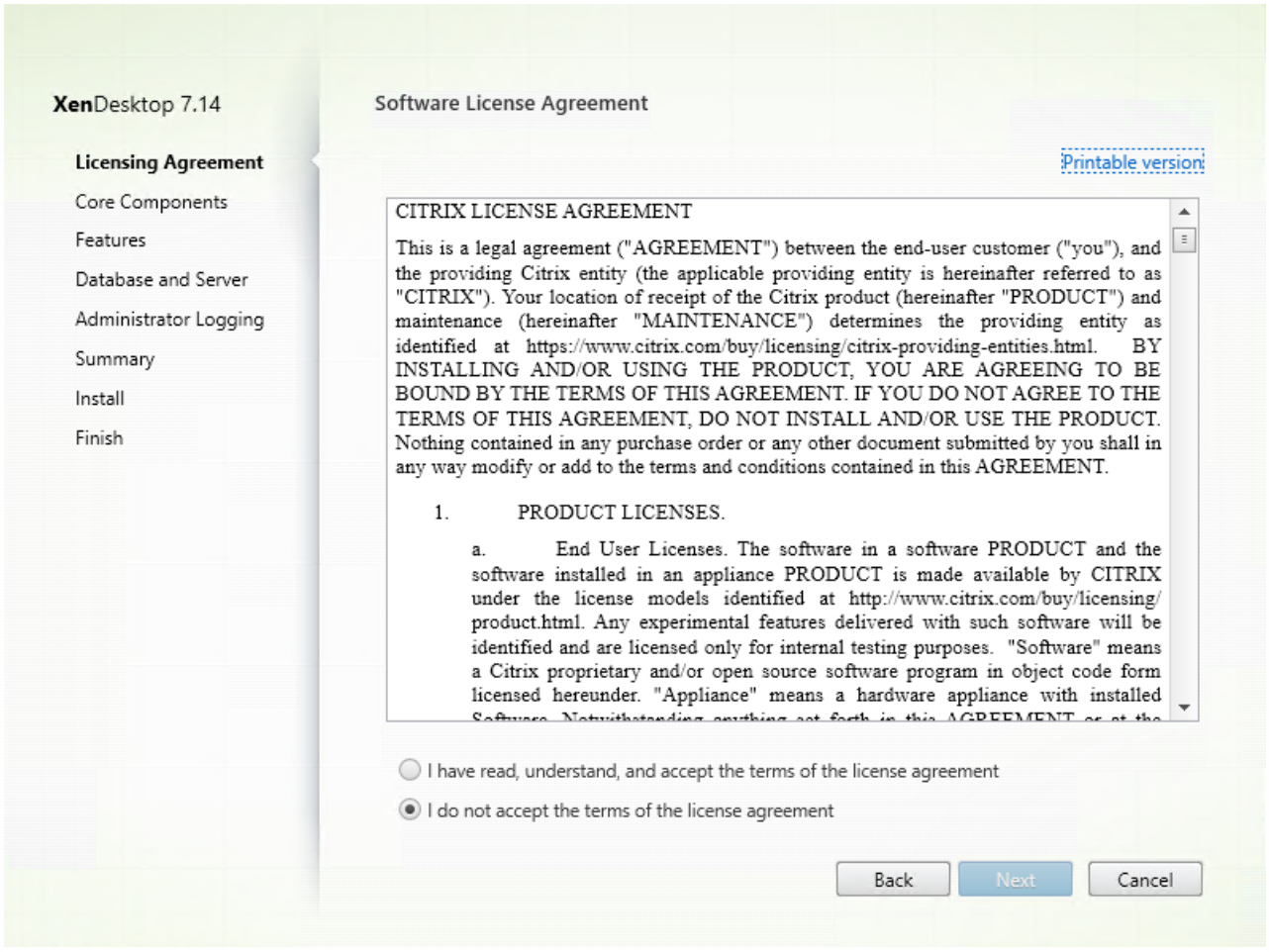
Paso 3. Seleccione Grabación de sesiones



Seleccione la entrada **Grabación de sesiones**.

Paso 4. Lea y acepte el contrato de licencia

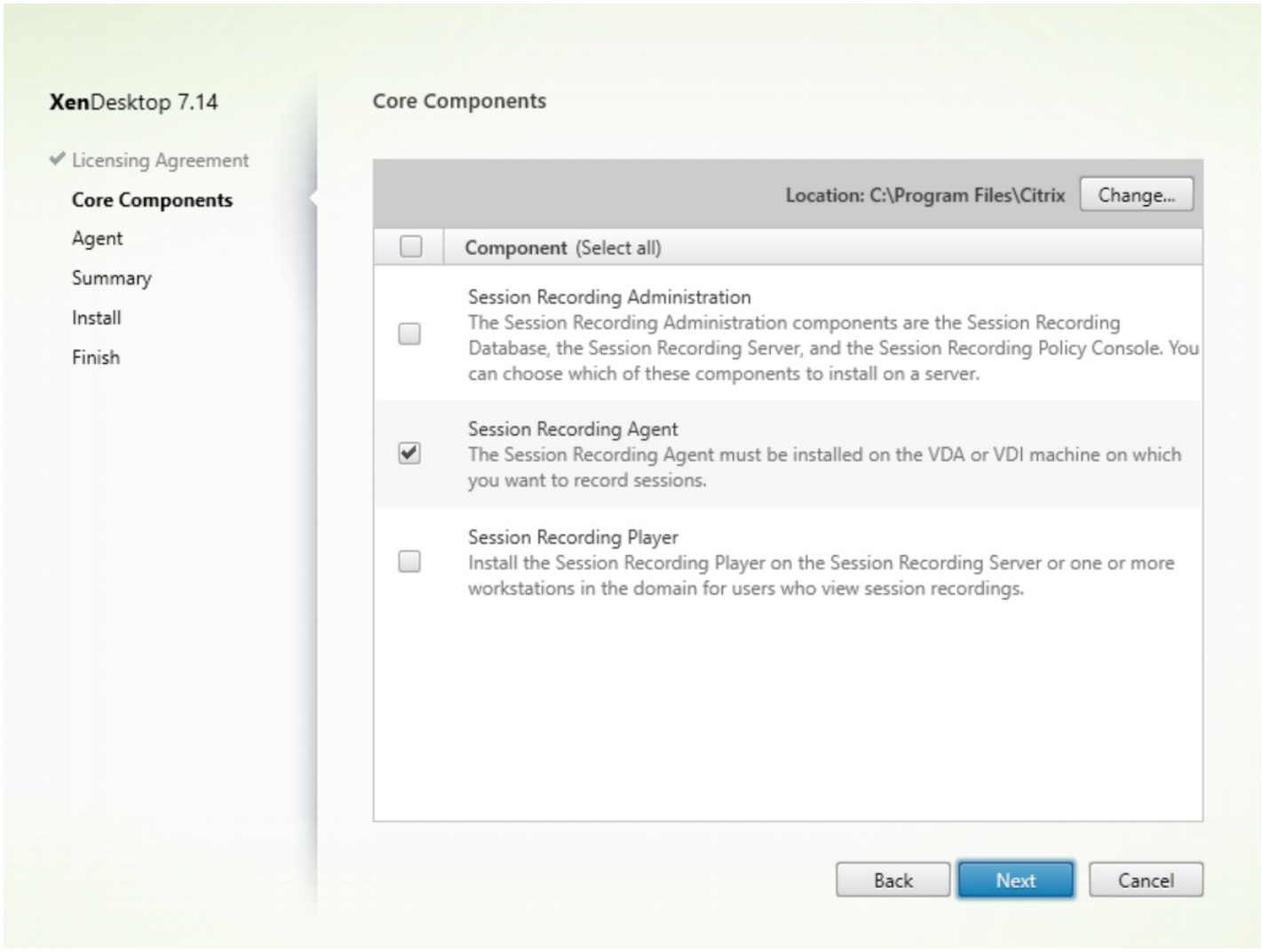
© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Contrato de licencia de software**, lea el contrato de licencia, acéptelo y haga clic en **Siguiente**
.

Paso 5. Seleccione el componente a instalar y la ubicación de la instalación

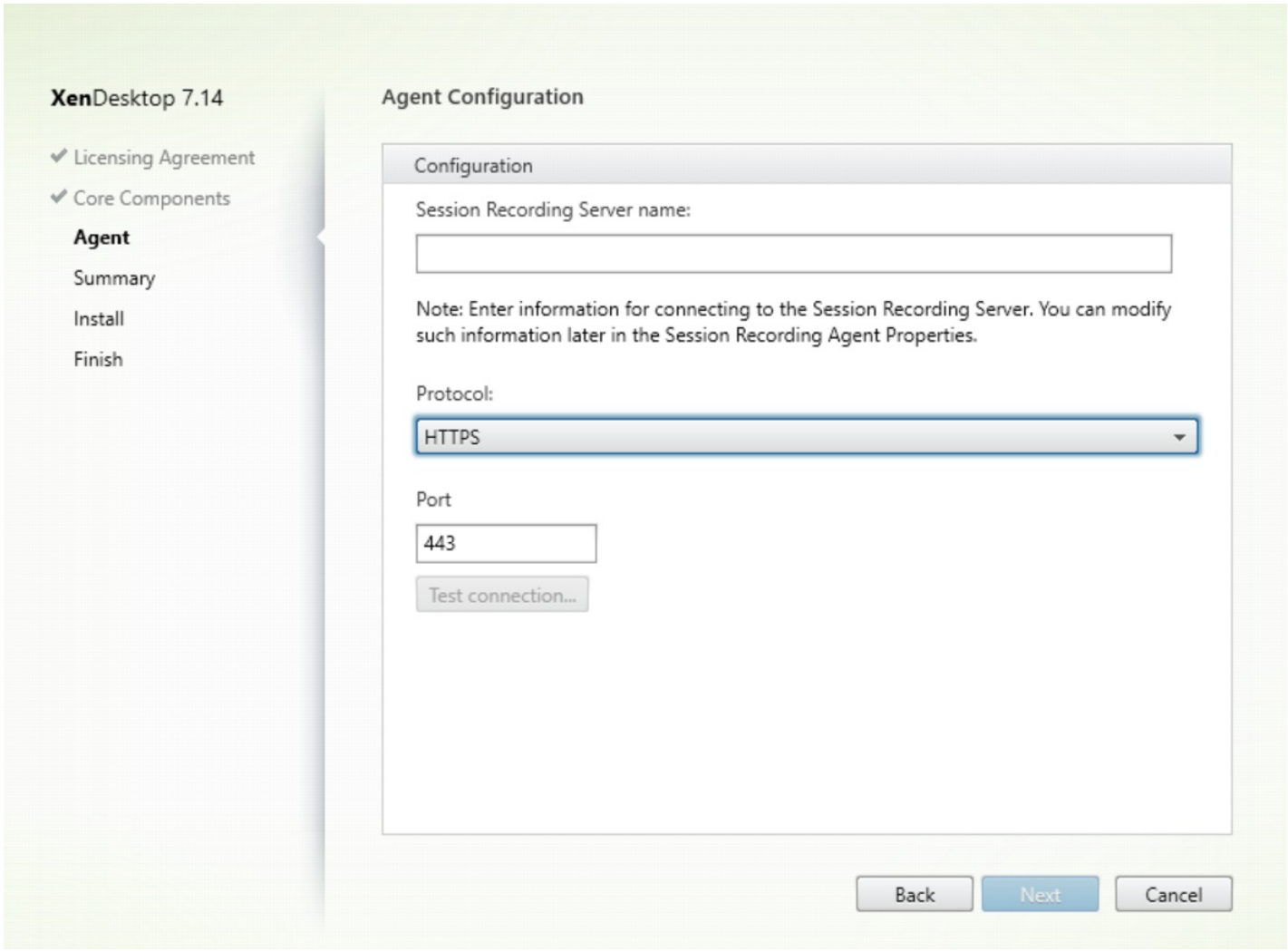
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Seleccione **Agente de grabación de sesiones** y haga clic en **Siguiente**.

Paso 6. Especifique la configuración del agente

© 1999-2017 Citrix Systems, Inc. All rights reserved.



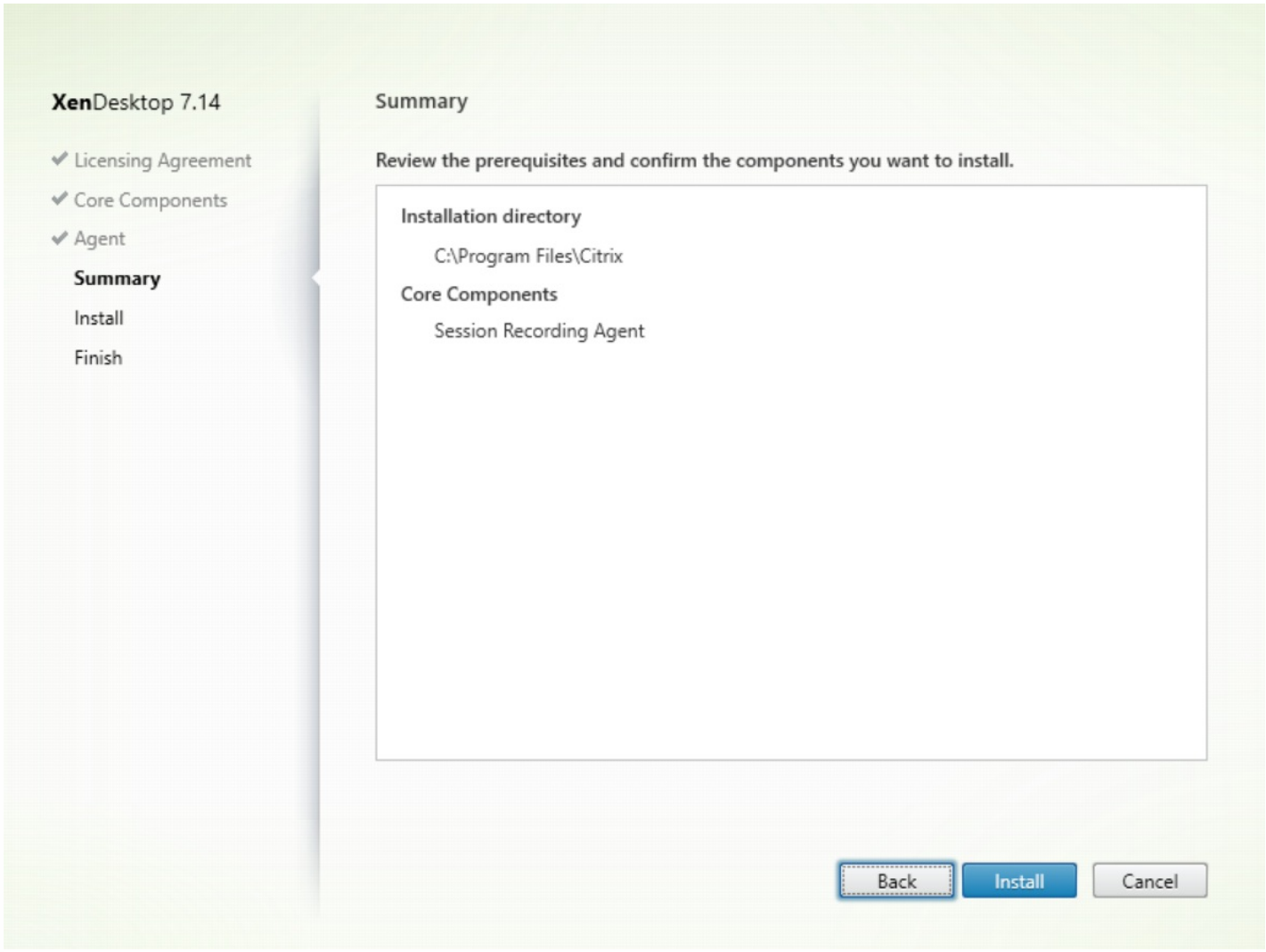
En la página **Configuración del agente**:

- Si ha instalado ya el Servidor de grabación de sesiones, escriba el nombre del equipo donde lo instaló, así como la información del protocolo y el puerto que deben utilizarse para la conexión con dicho servidor. Si todavía no ha instalado la Grabación de sesiones, puede modificar esta información más adelante en **Propiedades del Agente de grabación de sesiones**.

Nota: La función "Probar conexión" presenta una limitación en el programa de instalación. No admite el caso "HTTPS requiere TLS 1.2". Si utiliza el programa de instalación en este caso, se produce un error en la conexión de prueba. Puede ignorarlo y hacer clic en **Siguiente** para continuar con la instalación. No afecta al funcionamiento normal.

Paso 7. Revise los requisitos previos y confirme la instalación

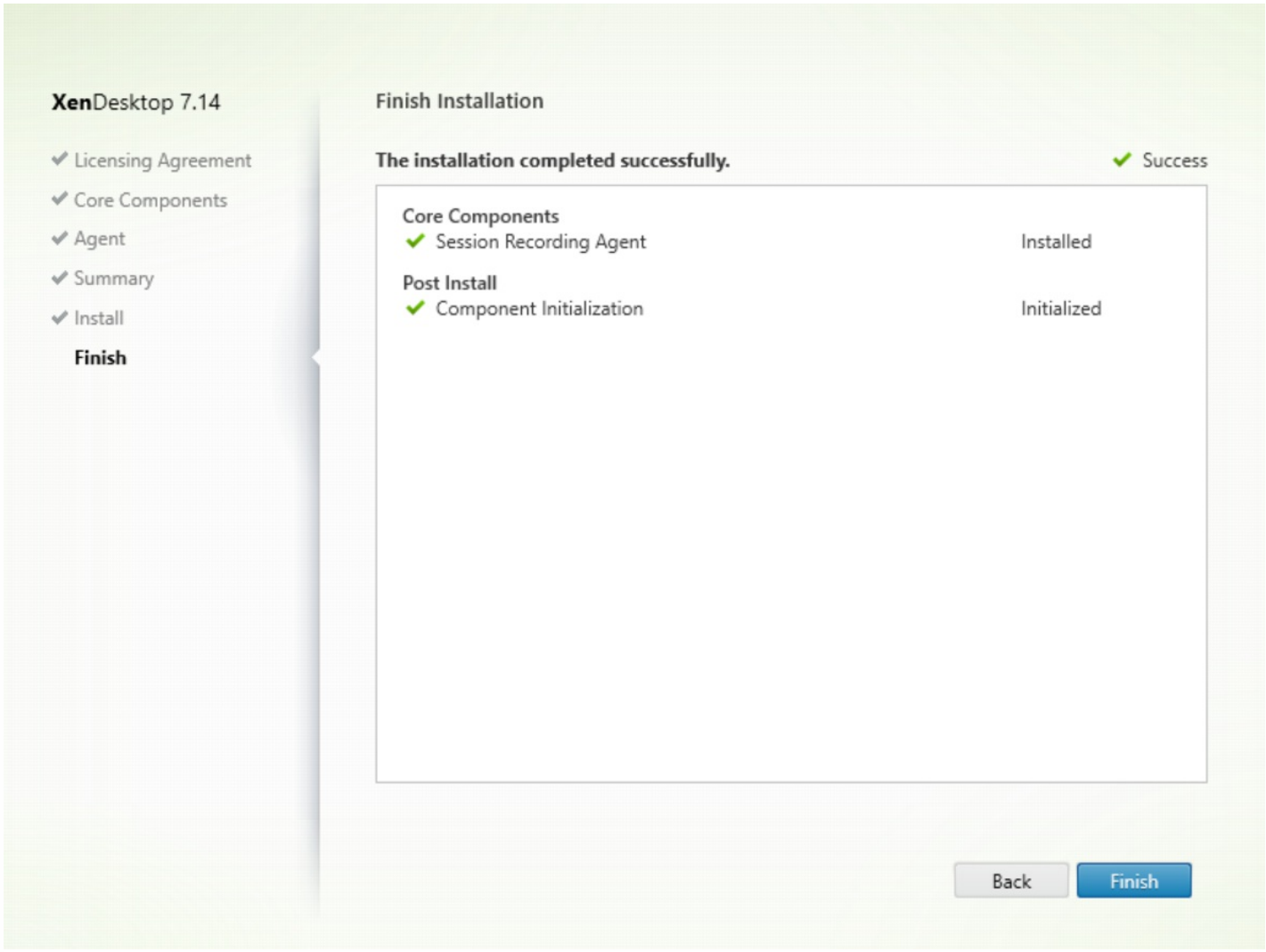
© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Resumen** muestra las opciones de instalación. Puede usar el botón **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones. O bien, haga clic en **Instalar** para iniciar la instalación.

Paso 8. Finalice la instalación

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Finalizar instalación** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar** para completar la instalación del Agente de grabación de sesiones.

Nota: Cuando Machine Creation Services (MCS) o Provisioning Services (PVS) crean varios agentes VDA con una imagen maestra configurada y Microsoft Message Queuing (MSMQ) instalado, esos VDA pueden tener el mismo QMId en ciertos casos. Esto puede causar diversos problemas, como:

- Las sesiones pueden no grabarse aunque el acuerdo de grabación se acepte.
- El Servidor de grabación de sesiones puede no recibir la señal del cierre de sesión, lo que hace que la sesión se quede en estado "Activo" permanentemente.

La solución temporal consiste en crear un QMId único para cada VDA; esta solución varía según el método de implementación utilizado.

No se requieren acciones adicionales si los agentes VDA de SO de escritorio con el Agente de grabación de sesiones instalado se crean con PVS 7.7 o una versión posterior y MCS 7.9 o una versión posterior en el modo de escritorios estáticos; por ejemplo, configurados para que todos los cambios sean permanentes con un disco Personal vDisk o un disco local del VDA aparte.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para agentes VDA de SO de escritorio o servidor creados con MCS o PVS y configurados para descartar todos los cambios cuando el usuario cierra sesión, use un script (GenRandomQMID.ps1) para modificar el QMId al iniciar el sistema. Modifique la estrategia de administración de energía a fin de garantizar que se ejecuten los VDA suficientes antes de que los usuarios intenten iniciar sesión.

Para usar el script GenRandomQMID.ps1, haga lo siguiente:

1. Compruebe que la directiva de ejecución esté establecida en **RemoteSigned** o **Unrestricted** en PowerShell.

   Set-ExecutionPolicy RemoteSigned

2. Cree una tarea programada y establezca el desencadenador en Al iniciar el sistema y ejecútela con la cuenta SYSTEM en la máquina de imagen maestra de PVS o MCS.

3. Agregue el comando como una tarea de inicio del sistema.

   powershell .exe -file C:\GenRandomQMID.ps1

Resumen del script GenRandomQMID.ps1:

1. Quitar el QMId actual del Registro.
2. Agregue SysPrep = 1 a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters.
3. Detener los servicios relacionados, incluidos CitrixSmAudAgent y MSMQ.
4. Para generar un QMId aleatorio, inicie los servicios detenidos previamente.

GENRANDOMQMID.PS1 de referencia COPIAR

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
# Remove old QMId from registry and set SysPrep flag for MSMQ

Remove-Itemproperty -Path HKLM:Software\Microsoft\MSMQ\Parameters\MachineCache -Name QMId -Force

Set-ItemProperty -Path HKLM:Software\Microsoft\MSMQ\Parameters -Name "SysPrep" -Type DWord -Value 1

# Get dependent services

$depServices = Get-Service -name MSMQ -dependentservices | Select -Property Name

# Restart MSMQ to get a new QMId

Restart-Service -force MSMQ

# Start dependent services

if ($depServices -ne $null) {

    foreach ($depService in $depServices) {

        $startMode = Get-WmiObject win32_service -filter "NAME = '$($depService.Name)'" | Select -Property StartMode

        if ($startMode.StartMode -eq "Auto") {

            Start-Service $depService.Name

        }

}

}
```

Instalación del Reproductor de grabación de sesiones

El Reproductor de grabación de sesiones se puede instalar en el Servidor de grabación de sesiones o en varias estaciones de trabajo del dominio para los usuarios encargados de ver las grabaciones.

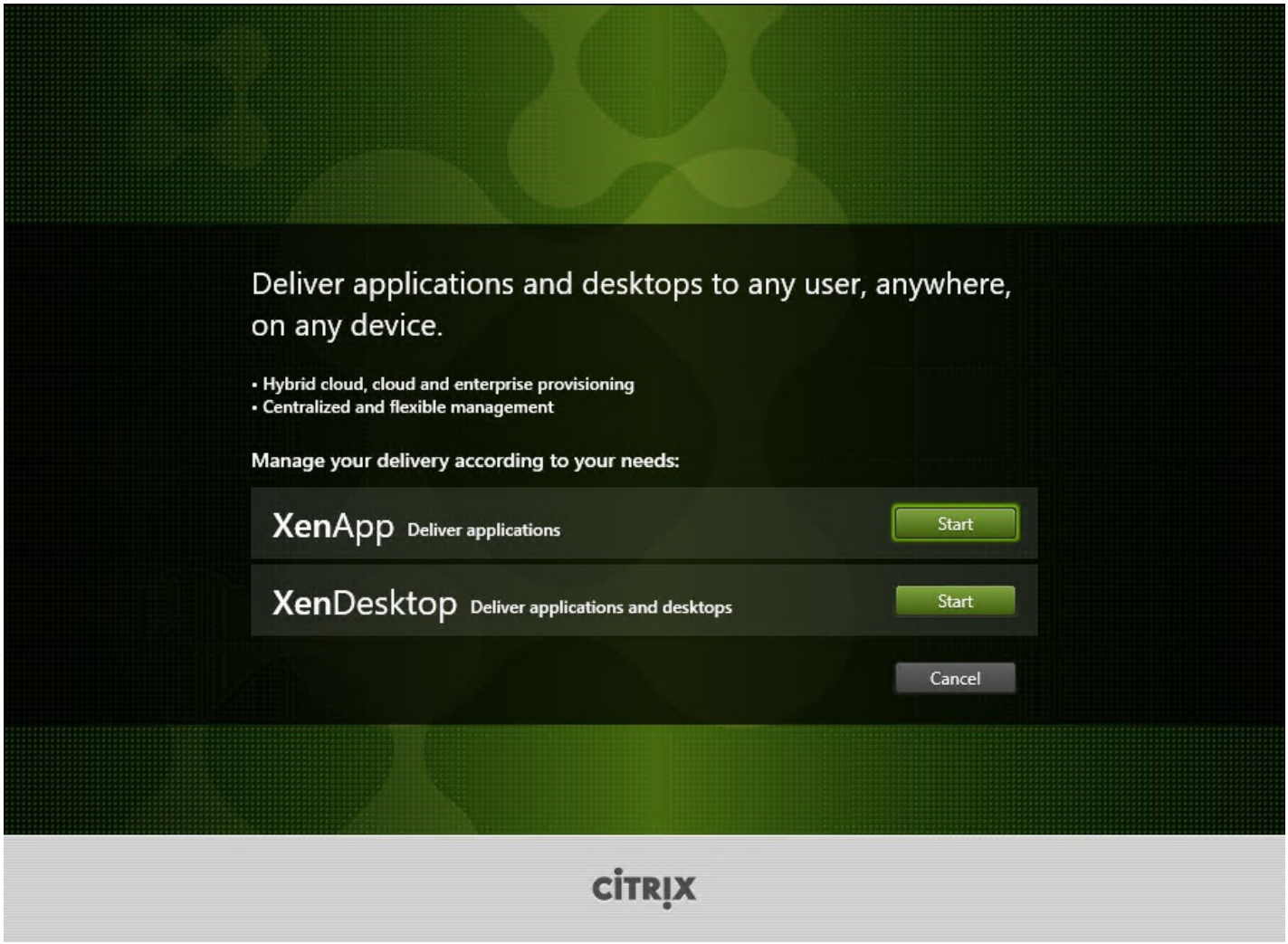
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paso 1. Descargue el software del producto e inicie el asistente

Utilice una cuenta de administrador local para iniciar sesión en la máquina donde quiere instalar el componente Reproductor de grabación de sesiones. Introduzca el DVD en la unidad o monte el ISO archivo. Si el programa de instalación no se inicia automáticamente, haga doble clic en la aplicación **AutoSelect** o la unidad montada.

Se iniciará el asistente de instalación.

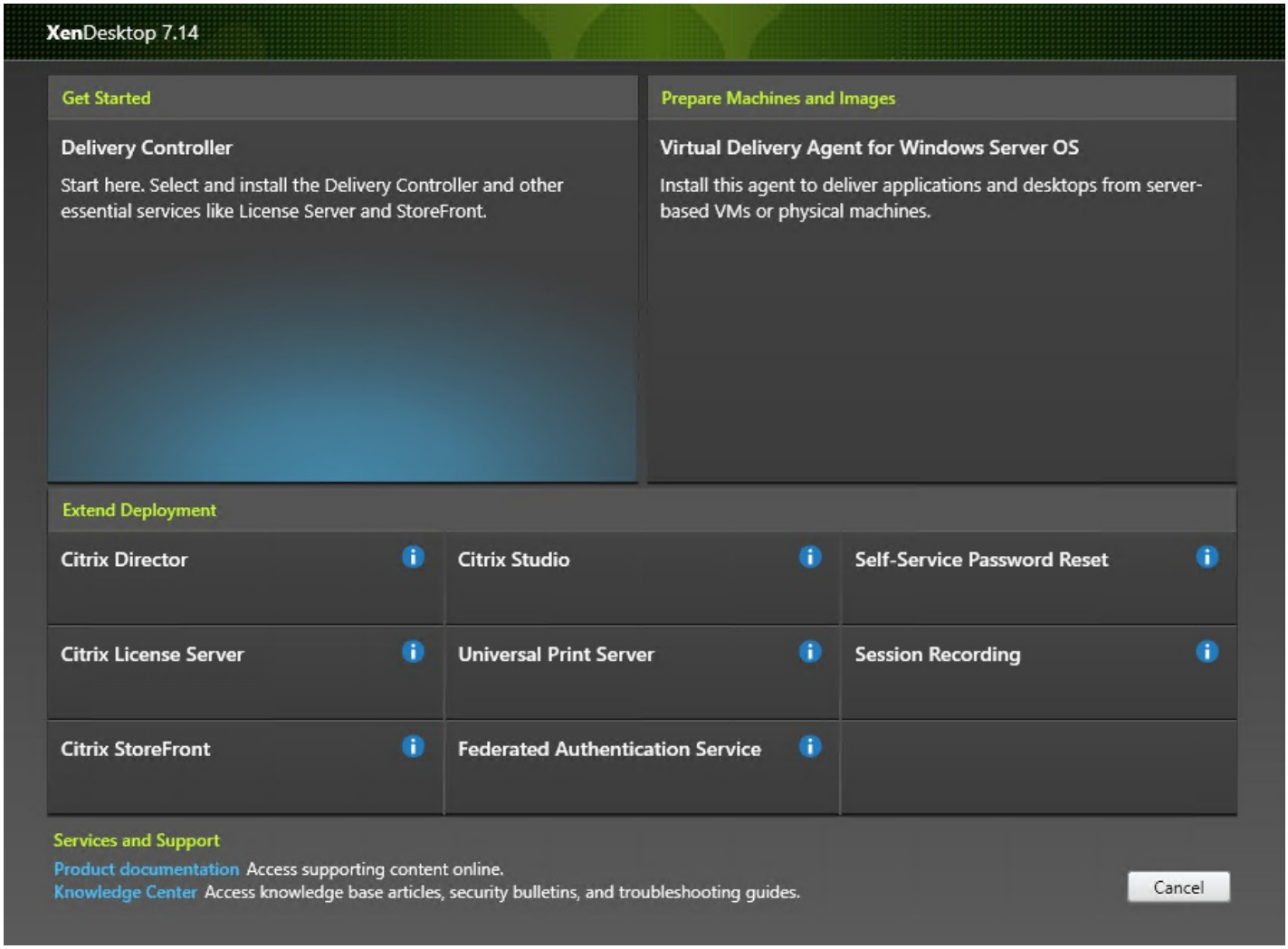
Paso 2. Elija el producto a instalar



Haga clic en **Iniciar** situado junto al producto que quiera instalar: **XenApp** o **XenDesktop**.

Paso 3. Seleccione Grabación de sesiones

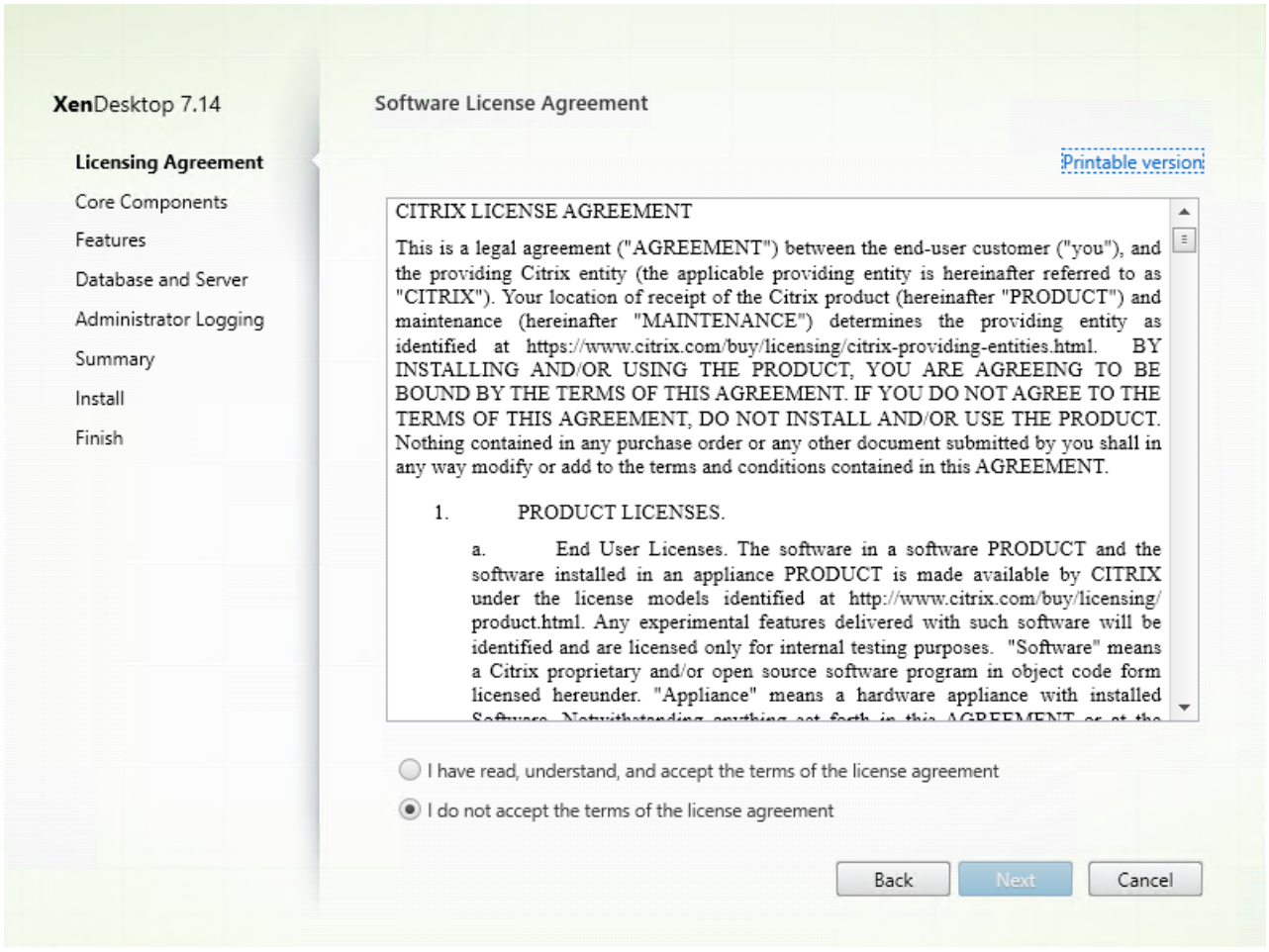
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Seleccione la entrada **Grabación de sesiones**.

Paso 4. Lea y acepte el contrato de licencia

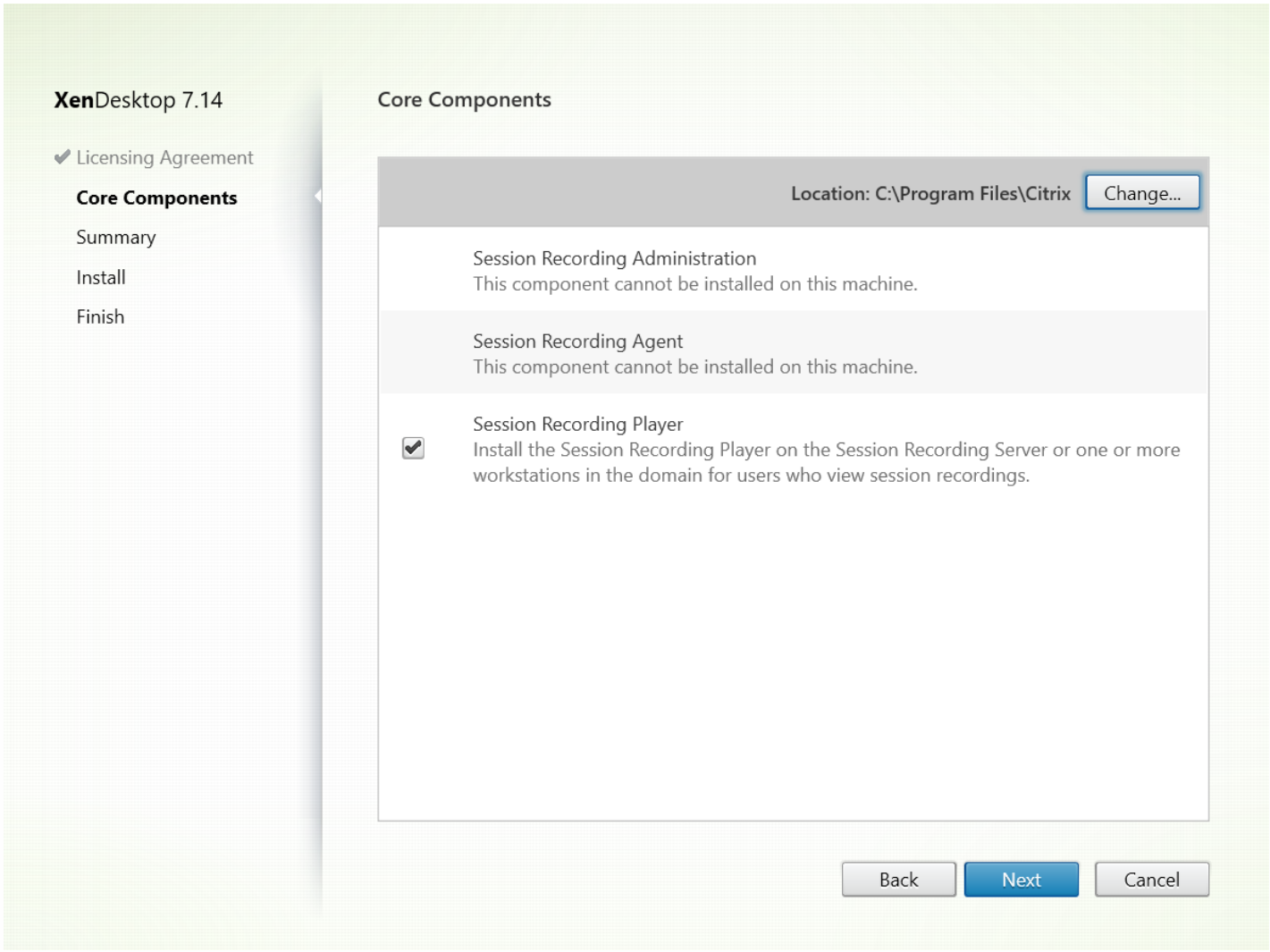
© 1999-2017 Citrix Systems, Inc. All rights reserved.



En la página **Contrato de licencia de software**, lea el contrato de licencia, acéptelo y haga clic en **Siguiente**
.

Paso 5. Seleccione el componente a instalar y la ubicación de la instalación

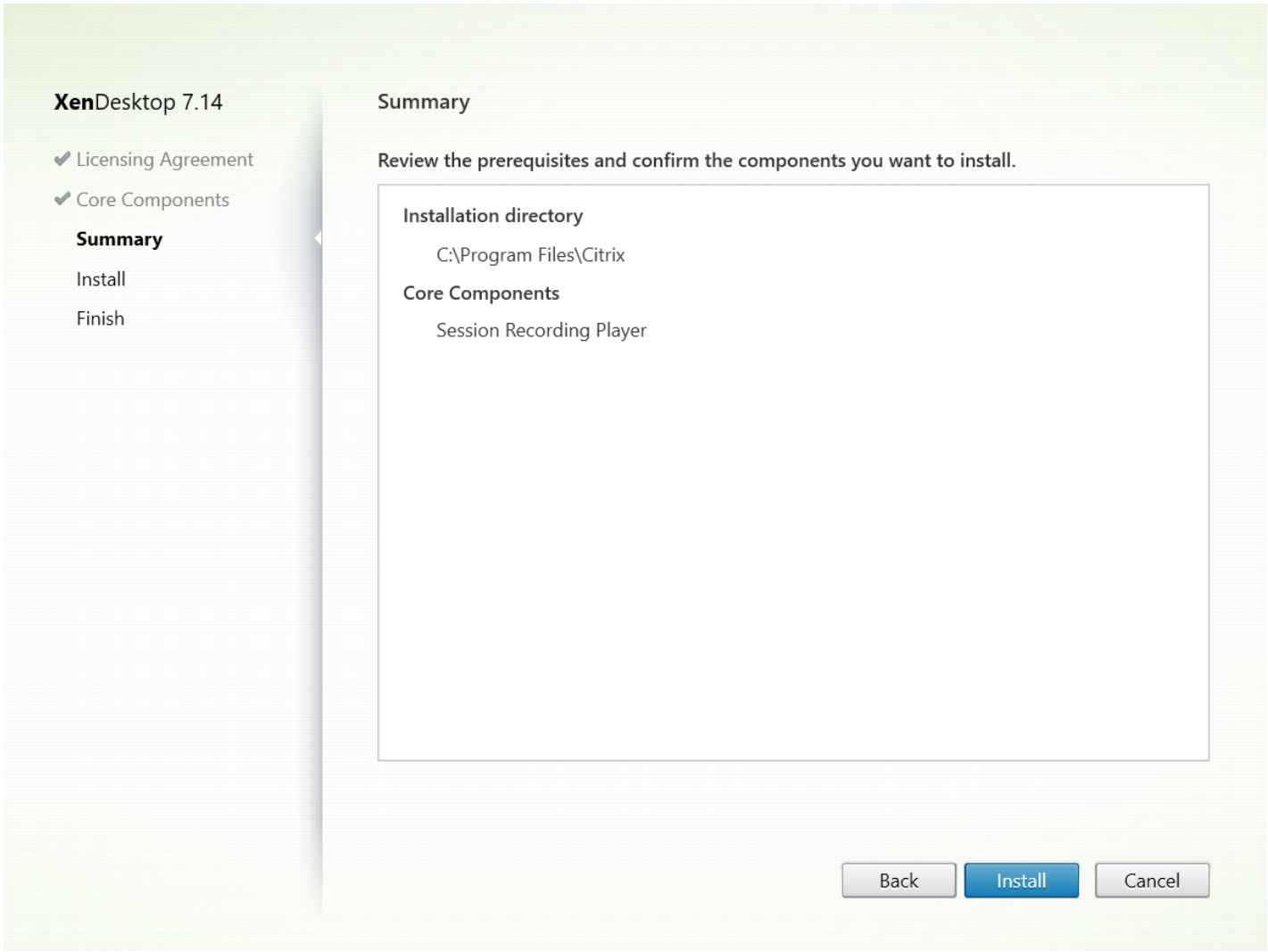
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Seleccione **Reproductor de grabación de sesiones** y haga clic en **Siguiente**.

Paso 6. Revise los requisitos previos y confirme la instalación

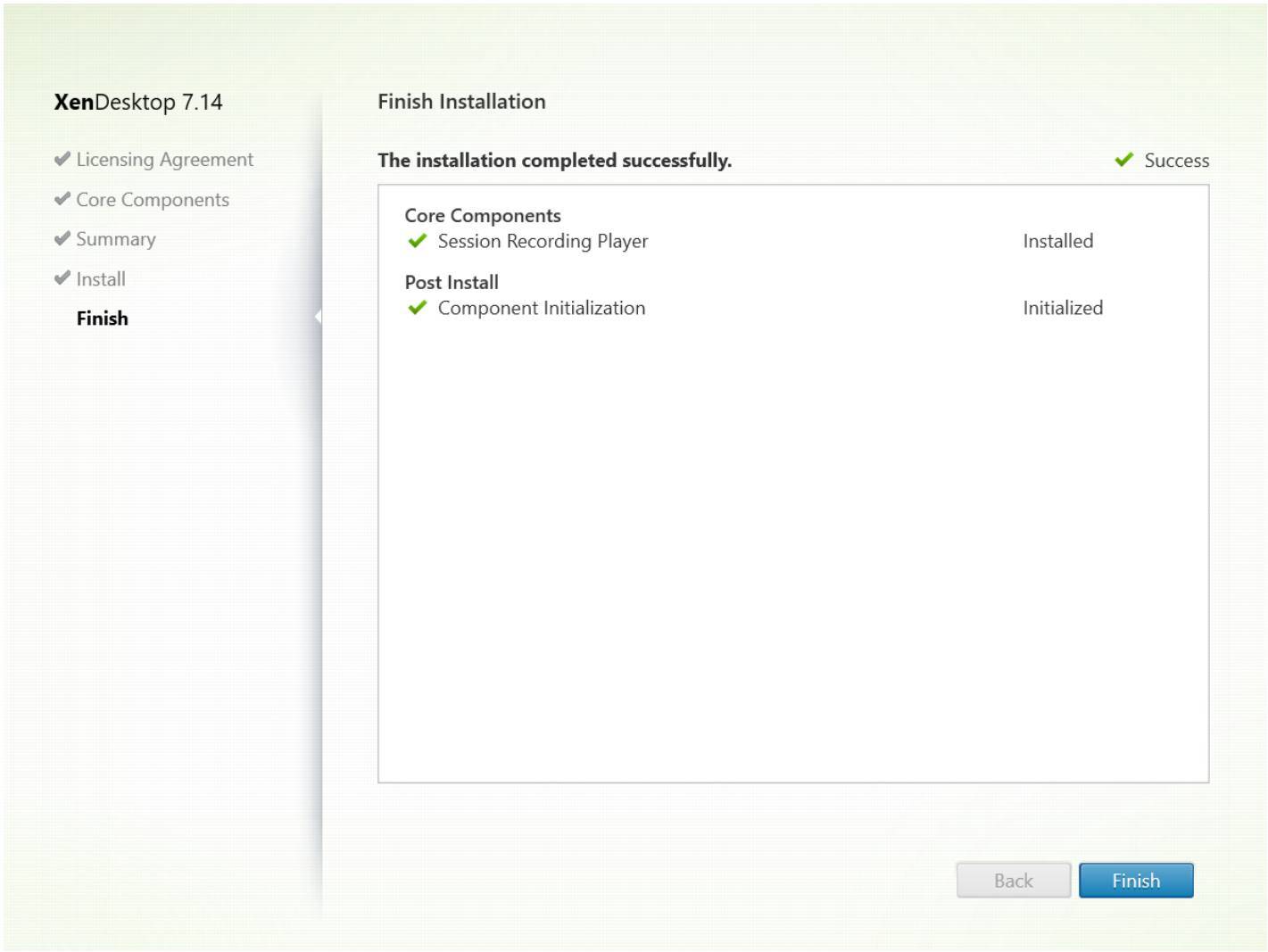
© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Resumen** muestra las opciones de instalación. Puede usar el botón **Atrás** para volver a las páginas anteriores del asistente y cambiar las opciones. O bien, haga clic en **Instalar** para iniciar la instalación.

Paso 7. Finalice la instalación

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La página **Finalizar instalación** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Haga clic en **Finalizar** para completar la instalación del Reproductor de grabación de sesiones.

Instalaciones automáticas

Para instalar el Agente de grabación de sesiones en varios servidores, escriba un script que use instalación automática.

La siguiente línea de comandos instala el Agente de grabación de sesiones y crea un archivo de registros para capturar la información de la instalación.

Para sistemas de 64 bits:

msiexec /i SessionRecordingAgentx64.msi /q /l*vx *sus registro de instalación* SESSIONRECORDINGSERVERNAME=su nombre de servidor
SESSIONRECORDINGBROKERPROTOCOL=su protocolo de broker SESSIONRECORDINGBROKERPORT=su puerto de broker

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: El archivo SessionRecordingAgentx64.msi en la imagen ISO de XenDesktop o XenApp está en \layout\image-full\x64\Session Recording.

Para sistemas de 32 bits:

msiexec /i SessionRecordingAgent.msi /q /l*vx *su registro de instalación* SESSIONRECORDINGSERVERNAME=su nombre de servidor
SESSIONRECORDINGBROKERPROTOCOL=su protocolo de broker SESSIONRECORDINGBROKERPORT=su puerto de broker

Nota: El archivo SessionRecordingAgent.msi en la imagen ISO de XenApp o XenDesktop está en \layout\image-full\x86\Session Recording.

donde:

yourservername es el nombre NetBIOS o nombre completo de dominio (FQDN) del equipo donde está el Servidor de grabación de sesiones. Si no se especifica, este valor es **localhost**.

yourbrokerport es un número entero que representa el puerto que el Agente de grabación de sesiones utiliza para comunicarse con el broker de grabación de sesiones. Si no se especifica, este valor es HTTPS.

yourbrokerport es un número entero que representa el puerto que el Agente de grabación de sesiones utiliza para comunicarse con el broker de grabación de sesiones. Si no se especifica, el valor es cero, lo cual hace que el Agente de grabación de sesiones utilice el número de puerto predeterminado para el protocolo seleccionado: 80 para HTTP o 443 para HTTPS.

/l*v especifica el modo de registro detallado.

yourinstallationlog es la ubicación del archivo de registro de la instalación.

/q especifica el modo silencioso.

Actualización de la funcionalidad Grabación de sesiones

Puede actualizar algunas implementaciones a versiones más recientes sin tener que configurar antes nuevas máquinas o sitios. Puede actualizar desde la Grabación de sesiones 7.6 (o una versión posterior) a la última versión (actual) de Grabación de sesiones.

Notas:

- Si actualiza la Administración de grabación de sesiones de 7.6 a 7.13 o posterior y elige **Modificar** en Administración de grabación de sesiones para agregar el servicio de Registros de administrador, el nombre de la instancia de SQL Server no aparece en la página **Configuración de registros de administrador**. Aparece el siguiente mensaje de error al hacer clic en **Siguiente**: "La prueba de conexión con la base de datos falló. Introduzca el nombre correcto de la instancia de la base de datos". Como solución temporal, agregue el permiso de lectura a los usuarios de localhost para la siguiente carpeta de registro del servidor SmartAuditor: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
- La Base de datos de grabación de sesiones puede no actualizarse si solo se tiene este componente instalado en una máquina. En este caso, compruebe si existen las siguientes entradas del registro en

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\SmartAuditor\Database. Si no, agregue manualmente esas entradas antes de actualizar.

Nombre de la clave	Tipo de clave	Valor de la clave
SmAudDatabaseInstance	Cadena	El nombre de instancia de la Base de datos de grabación de sesiones
DatabaseName	Cadena	El nombre de la Base de datos de grabación de sesiones

Requisitos, preparación y limitaciones

Nota: No se puede actualizar desde una versión de Technology Preview.

- Debe usar la interfaz gráfica o de línea de comandos del programa de instalación de la funcionalidad Grabación de sesiones para actualizar los componentes de Grabación de sesiones en la máquina donde se instalaron esos componentes.
- Antes de iniciar cualquier actividad de actualización, realice una copia de seguridad de la base de datos llamada CitrixSessionRecording ubicada en la instancia de SQL Server, de forma que pueda restaurarla si se detecta algún problema después de la actualización de la base de datos.
- Además de ser un usuario del dominio, usted debe ser un administrador local en las máquinas donde quiere actualizar los componentes de Grabación de sesiones.
- Si el Servidor de grabación de sesiones y la Base de datos de grabación de sesiones no están instalados en el mismo servidor, debe tener el permiso del rol de base de datos para actualizar la Base de datos de grabación de sesiones. De lo contrario, puede:
  - Pedir al administrador de la base de datos que le asigne los permisos del rol de servidor **securityadmin** y **dbcreator** para la actualización. Una vez completada la actualización, los permisos del rol de servidor **securityadmin** y **dbcreator** ya no son necesarios y se pueden retirar sin riesgo alguno.
  - O bien, utilice el paquete SessionRecordingAdministrationx64.msi para actualizar. Durante la actualización del msi, aparece un cuadro de diálogo que requiere las credenciales de un administrador de base de datos con los permisos del rol de servidor **securityadmin** y **dbcreator**. Especifique las credenciales correctas y haga clic en **Aceptar** para continuar con la actualización.
- Si no quiere actualizar todos los Agentes de grabación de sesiones al mismo tiempo, el Agente de grabación de sesiones 7.6.0 (o una versión posterior) puede funcionar con la última versión (actual) del Servidor de grabación de sesiones. Sin embargo, algunas de las nuevas funcionalidades y correcciones de errores pueden no surtir efecto.
- No se grabará ninguna sesión iniciada durante la actualización del Servidor de grabación de sesiones.
- La opción **Ajuste de gráficos** en Propiedades del agente de grabación de sesiones está habilitada de forma predeterminada después de una instalación nueva o una actualización para mantener la compatibilidad con el modo de redirección de composición del escritorio. Puede inhabilitar manualmente esta opción después de una instalación nueva o una actualización.
- La funcionalidad Registros de administrador no se instala después de actualizar Grabación de sesiones de una versión anterior que no la contenía. Para agregar esta nueva funcionalidad, modifique la instalación después de la actualización.
- Si hay grabaciones de sesiones en directo cuando se inicia el proceso de actualización, es muy posible de que esas grabaciones no se completen.

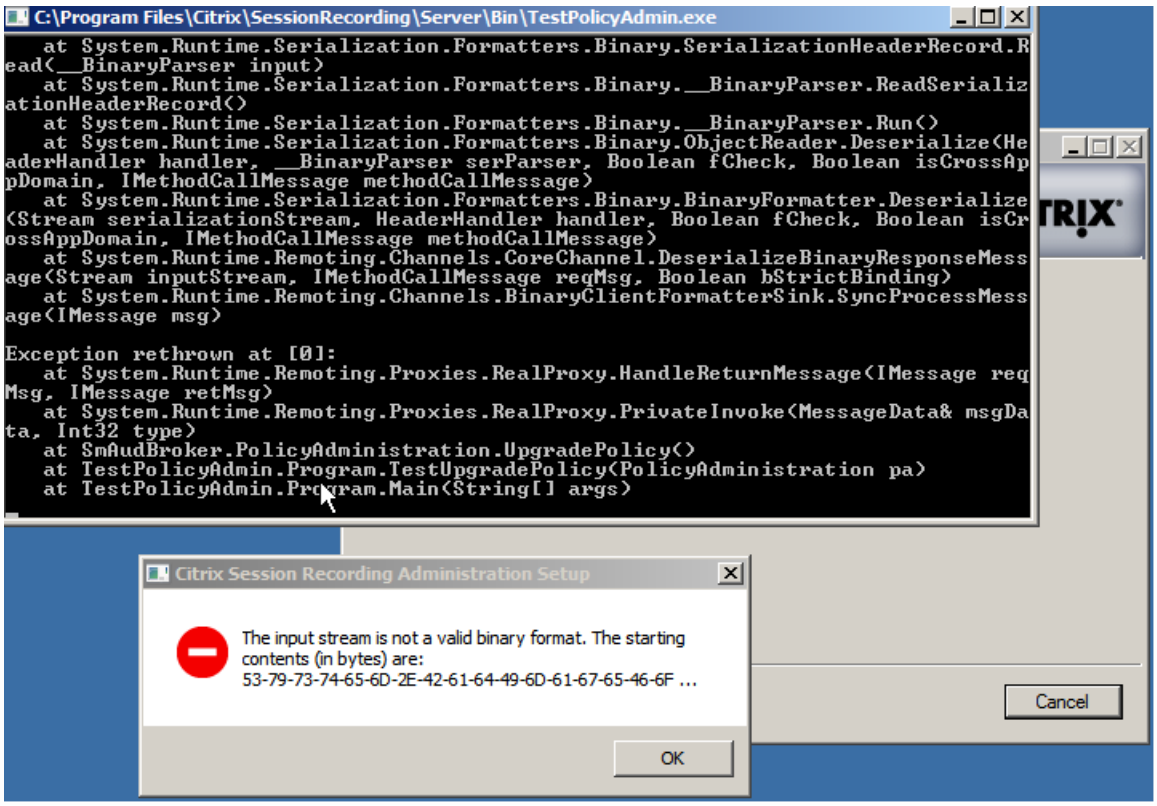
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Revise la siguiente secuencia de actualización para prevenir y mitigar posibles interrupciones.

Secuencia de actualización

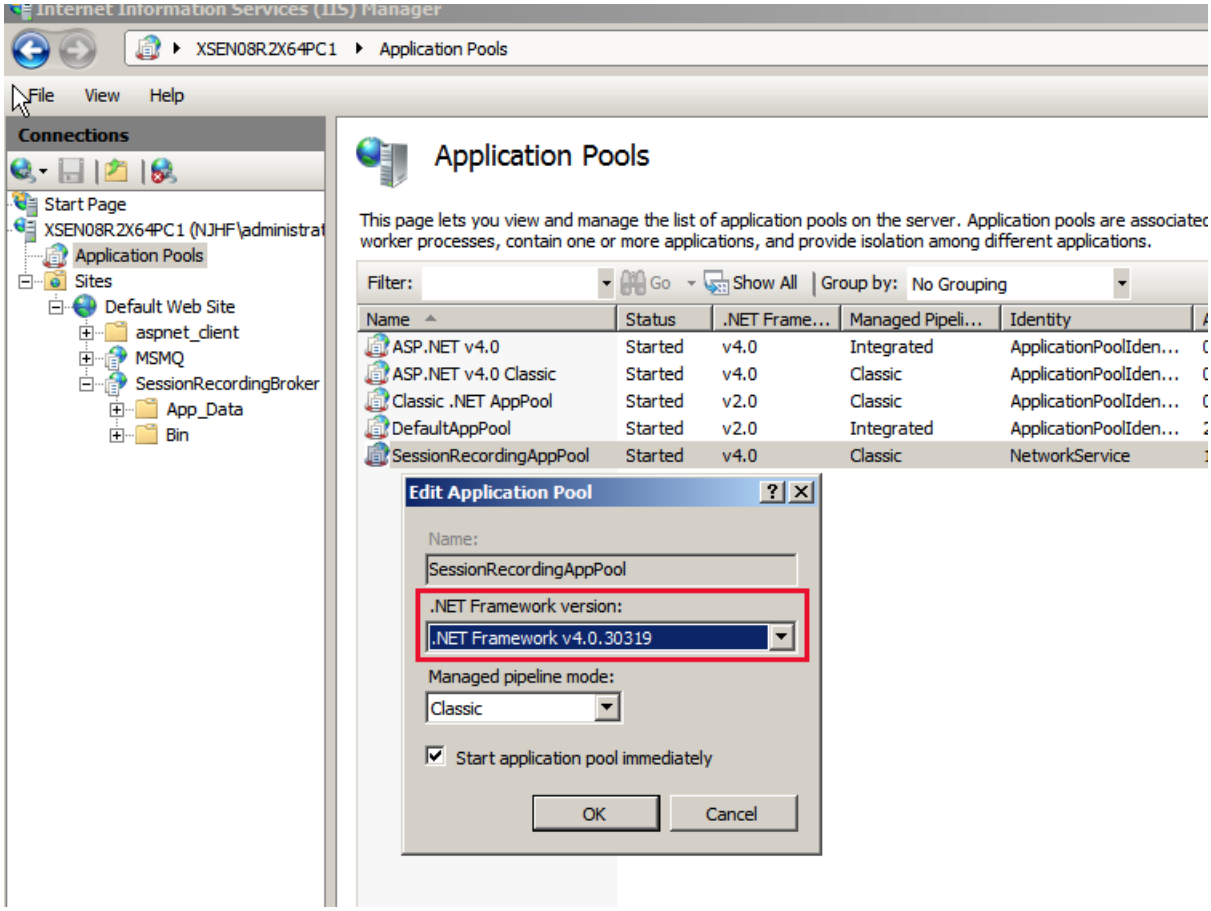
1. Si la Base de datos de grabación de sesiones y el Servidor de grabación de sesiones están instalados en servidores diferentes, detenga manualmente el servicio del Administrador de almacenamiento de grabación de sesiones en el Servidor de grabación de sesiones y, a continuación, actualice primero la Base de datos de grabación de sesiones.
2. Compruebe que el Broker de grabación de sesiones se está ejecutando con el servicio IIS. Actualice el Servidor de grabación de sesiones. Si la Base de datos de grabación de sesiones y el Servidor de grabación de sesiones están instalados en el mismo servidor, también se actualizará la Base de datos de grabación de sesiones.
3. El servicio Grabación de sesiones volverá a funcionar automáticamente cuando se complete la actualización del Servidor de grabación de sesiones.
4. Actualice el Agente de grabación de sesiones (en la imagen maestra).
5. Actualice la Consola de directivas de grabación de sesiones junto con o después del Servidor de grabación de sesiones.
6. Actualice el Reproductor de grabación de sesiones.

Nota: Puede darse este error cuando actualice el componente de Administración de grabación de sesiones en Windows Server 2008 R2.



En ese caso, cambie la "versión de .NET Framework" de "SessionRecordingAppPool" a ".NET Framework v4" en IIS y actualice de nuevo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Desinstalación de la grabación de sesiones

Para quitar componentes de Grabación de sesiones de un servidor o estación de trabajo, use la función para desinstalar o quitar programas del Panel de control de Windows. Para quitar la Base de datos de grabación de sesiones, debe tener los mismos permisos de rol **securityadmin** y **dbcreator** de SQL Server que tenía cuando la instaló.

Por razones de seguridad, la base de datos de Registro de administrador no se elimina una vez desinstalados los componentes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de la grabación de sesiones

Dec 05, 2017

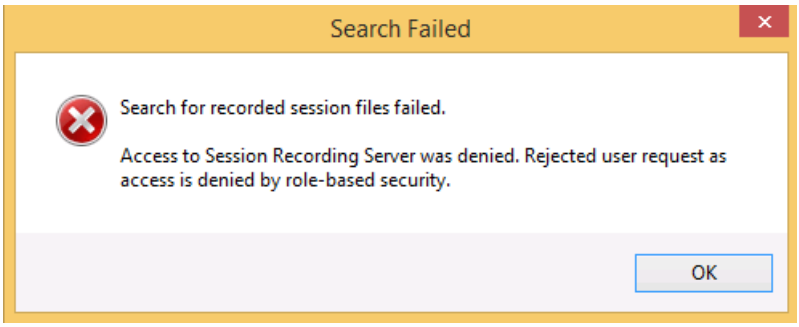
Configuración de la grabación de sesiones para reproducir y grabar sesiones

Después de instalar los componentes de Grabación de sesiones, lleve a cabo los siguientes pasos para configurar la Grabación de sesiones para grabar las sesiones de XenApp o XenDesktop y permitir verlas a otros usuarios:

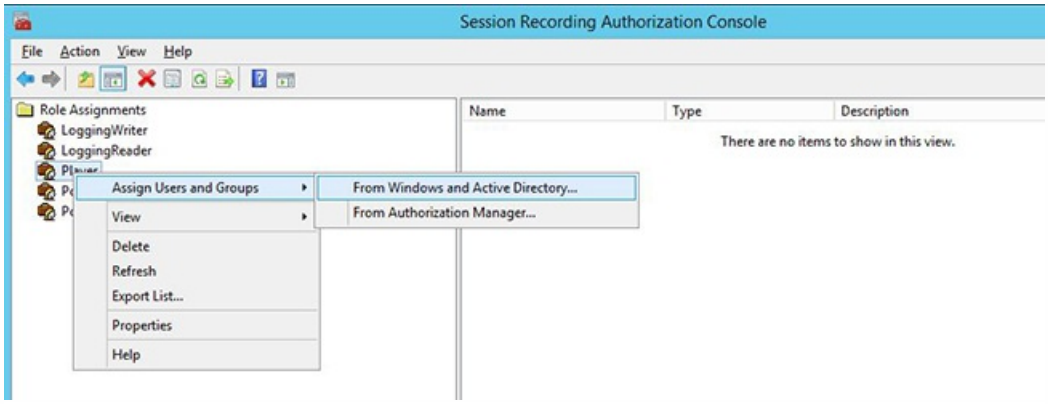
- Autorizar a usuarios para reproducir grabaciones
- Autorizar a usuarios para administrar las directivas de grabación
- Configurar la directiva de grabación activa para grabar sesiones
- Configurar permisos personalizados
- Configure el reproductor de grabación de sesiones para conectar con el servidor de grabación de sesiones

Autorizar a usuarios para reproducir sesiones grabadas

Cuando se instala la funcionalidad Grabación de sesiones, ningún usuario tiene todavía permiso para reproducir sesiones grabadas. Debe asignar permiso a cada usuario, incluso al administrador. Un usuario sin permiso para reproducir sesiones grabadas recibe el siguiente mensaje de error al intentar reproducir una sesión grabada:



1. Inicie una sesión como administrador en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. Inicie la Consola de autorización de grabación de sesiones.
3. En la Consola de autorización de la grabación de sesiones, seleccione Reproductor.
4. Agregue los usuarios y los grupos que quiera que tengan autorización para ver sesiones grabadas; estos aparecerán en el panel derecho.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autorizar a usuarios para administrar las directivas de grabación

Cuando se instala la funcionalidad Grabación de sesiones, los administradores del dominio tienen concedido el permiso de gestionar las directivas de grabación de manera predeterminada. Puede cambiar esta configuración de autorización.

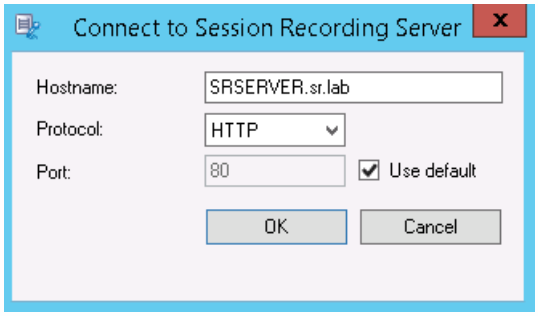
1. Inicie sesión como administrador en la máquina donde se encuentra el Servidor de grabación de sesiones.
2. Inicie la Consola de autorización de grabación de sesiones y seleccione PolicyAdministrators.
3. Agregue los usuarios y los grupos que pueden administrar directivas de grabación.

Configurar la directiva de grabación activa para grabar sesiones

La directiva de grabación activa especifica el comportamiento de la grabación de sesiones en todos los VDA o VDI que tienen instalado el Agente de grabación de sesiones y están conectados a un servidor de grabación de sesiones. Cuando se instala la función de grabación de sesiones, la directiva activa de grabación es **No grabar**. No es posible grabar sesiones hasta que se cambie la directiva de grabación activa.

Importante: Una directiva puede contener muchas reglas, pero solo puede haber una directiva activa ejecutándose en un momento dado.

1. Inicie la sesión como administrador de directivas autorizado en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie la Consola de directivas de grabación de sesiones.
3. Si una ventana emergente pide **Conectar con el servidor de grabación de sesiones**, compruebe que el nombre de host del Servidor de grabación de sesiones, el protocolo y el puerto son correctos.



4. En la Consola de directivas de grabación de sesiones, expanda **Directivas de grabación**. Esto muestra las directivas de grabación disponibles cuando se instala la función de grabación de sesiones, con una marca junto a la directiva que está activa:
   - **No grabar**. Ésta es la directiva predeterminada. Si no especifica otra directiva, no se grabarán sesiones.
   - **Grabar a todos con notificación**. Si elige esta directiva, se grabarán todas las sesiones. Aparecerá una ventana para notificar de la grabación.
   - **Grabar a todos sin notificación**. Si elige esta directiva, se grabarán todas las sesiones. No aparecerá ninguna ventana para notificar de la grabación.
5. Seleccione la directiva que quiera activar.
6. En la barra de menús, elija **Acción** > **Activar directiva**.

La Grabación de sesiones le permite crear su propia directiva de grabación. Cuando se crean directivas de grabación, éstas aparecen en la carpeta Directivas de grabación de la Consola de directivas de grabación de sesiones.
La directiva de grabación genérica puede no ajustarse a sus necesidades. Puede configurar directivas y reglas basadas en usuarios, agentes VDA y servidores VDI, grupos de entrega y aplicaciones. Para obtener más información acerca de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

directivas personalizadas, consulte Creación de directivas de grabación personalizadas.

Nota: La funcionalidad Registro de administrador de Grabación de sesiones permite capturar en un registro los cambios que se realizan en la directiva de grabación. Para obtener más información, consulte Registro de las actividades de administración.

Configuración del Reproductor de grabación de sesiones

Antes de que un reproductor de grabación de sesiones pueda reproducir sesiones, es necesario configurarlo para que se conecte con un servidor de grabación de sesiones que almacena las sesiones grabadas. Todos los reproductores de grabación de sesiones se pueden configurar para que puedan elegir entre varios servidores de grabación de sesiones a los que conectarse, pero solo pueden conectarse a un servidor cada vez. Si el reproductor se configura con permiso de conectarse a varios Servidores de grabación de sesiones, los usuarios pueden cambiar el Servidor de grabación de sesiones al cual se conecta el reproductor marcando una casilla de verificación en la ficha **Conexiones**, en **Herramientas** > **Opciones**.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. Inicie el Reproductor de grabación de sesiones.
3. En la barra del menú del Reproductor de grabación de sesiones, elija **Herramientas** > **Opciones**.
4. En la ficha **Conexiones**, haga clic en **Agregar**.
5. En el campo **Nombre de host**, escriba el nombre o la dirección IP del equipo que aloja el Servidor de grabación de sesiones y seleccione el protocolo. De manera predeterminada, la funcionalidad Grabación de sesiones se configura para usar HTTPS/SSL para proteger las comunicaciones. Si SSL no está configurado, seleccione HTTP.
6. Si quiere configurar el Reproductor de grabación de sesiones de modo que pueda conectarse a varios Servidores de grabación de sesiones, repita los pasos 4 y 5 para cada Servidor de grabación de sesiones.
7. Debe marcar la casilla de verificación del Servidor de grabación de sesiones al que quiera conectarse.

Configuración de la conexión con el Servidor de grabación de sesiones

La conexión entre el Agente de grabación de sesiones y el Servidor de grabación de sesiones se configura generalmente en el momento de instalar el agente. Para configurar esta conexión después de instalar el Agente de grabación de sesiones, use las Propiedades del Agente de grabación de sesiones.

1. Inicie una sesión en el servidor donde está instalado el Agente de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Agente de grabación de sesiones**.
3. Haga clic en la ficha **Conexiones**.
4. En el campo **Servidor de grabación de sesiones**, escriba el nombre del servidor o su dirección IP.
5. En la sección de la **Cola de mensajes del Administrador de almacenamiento de grabación de sesiones**, seleccione el protocolo que utiliza el Administrador de almacenamiento de grabación de sesiones para comunicarse, y cambie el número de puerto predeterminado, si es necesario.
6. En el campo **Vida del mensaje**, acepte los 7200 segundos (dos horas) predeterminados o escriba un valor nuevo para la cantidad de segundos que cada mensaje se mantiene en la cola si falla la comunicación. Después de este período de tiempo, el mensaje se borra y el archivo se reproduce hasta el punto donde se perdieron los datos.
7. En la sección **Broker de grabación de sesiones**, seleccione el protocolo de comunicación que usa el broker de grabación de sesiones para comunicarse, y cambie el número de puerto predeterminado, si es necesario.
8. Cuando se le solicite, reinicie el **Servicio del Agente de grabación de sesiones** para aceptar los cambios.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Concesión de acceso a los usuarios

Dec 05, 2017

> **Important**
>
> Por razones de seguridad, otorga a los usuarios solamente los permisos que necesitan para realizar funciones específicas, tales como ver sesiones grabadas.

Los derechos para los usuarios de grabaciones de sesiones se conceden agregando dichos usuarios a roles, usando la Consola de autorización de grabación de sesiones en el servidor de grabación de sesiones. Los usuarios de la grabación de sesiones tienen tres roles:

- **Reproductor.** Otorga permiso de ver sesiones grabadas de XenApp. No hay miembros predeterminados para este rol.
- **Consulta de directivas.** Permite a los servidores que alojan el Agente de grabación de sesiones solicitar evaluaciones de las directivas de grabación. De forma predeterminada, los usuarios autenticados son miembros de este rol.
- **Administrador de directivas.** Otorga permiso para ver, crear, modificar, eliminar y activar las directivas de grabación. De forma predeterminada, los administradores del equipo host del servidor de grabación de sesiones son miembros de este rol.

La grabación de sesiones es compatible con los grupos y los usuarios definidos en Active Directory.

Asignación de usuarios a roles

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones, como administrador o como miembro del rol Administrador de directivas.
2. Inicie la Consola de autorización de grabación de sesiones.
3. Seleccione el rol al que desea asignar usuarios.
4. Desde la barra de menú, elija **Acción** > **Asignar usuarios y grupos de Windows**.
5. Agregar usuarios y grupos.

Cualquier cambio a la consola tomará efecto durante la actualización que se da cada minuto.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación y activación de directivas de grabación

Dec 05, 2017

Utilice la Consola de directivas de grabación de sesiones para crear y activar las directivas que determinan qué sesiones se grabarán.

Importante: Para usar la consola de directivas de grabación de sesiones, debe tener instalado el complemento Broker PowerShell Snap-in (Broker_PowerShellSnapIn_x64.msi). El programa de instalación no instala automáticamente este complemento. Busque el complemento en la imagen ISO de XenApp/XenDesktop (\layout\image-full\x64\Citrix Desktop Delivery Controller) y siga las instrucciones para instalarlo manualmente. Si no se siguen las instrucciones puede producirse un error.

Puede activar las directivas de sistema que están disponibles cuando se instala la funcionalidad de grabación de sesiones, o puede crear y activar sus propias directivas personalizadas. Las directivas del sistema de grabación de sesiones aplican una única regla a todos los usuarios, aplicaciones publicadas y servidores. Las directivas personalizadas especifican cuáles usuarios, aplicaciones publicadas y servidores graban.

La directiva activa determina cuáles son las sesiones que se graban. Solamente una directiva está activa en un momento dado.

Directivas del sistema

La funcionalidad de grabación de sesiones proporciona estas directivas de sistema:

- **No grabar**. Ésta es la directiva predeterminada. Si no especifica otra directiva, no se grabarán sesiones.
- **Grabar a todos con notificación**. Si elige esta directiva, se grabarán todas las sesiones. Aparecerá una ventana emergente que notificará que se graba la sesión.
- **Grabar a todos sin notificación**. Si elige esta directiva, se grabarán todas las sesiones. No aparecerá ninguna ventana emergente para notificar que se graba la sesión.

Las directivas del sistema no pueden modificarse o borrarse.

Activación de una directiva

1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie la Consola de directivas de grabación de sesiones.
3. Si una ventana emergente pide **Conectar con el Servidor de grabación de sesiones**, compruebe que el nombre del Servidor de grabación de sesiones, el protocolo y el puerto son correctos. Haga clic en **Aceptar**.
4. En la Consola de directivas de grabación de sesiones, expanda **Directivas de grabación**.
5. Seleccione la directiva que desee para habilitar la directiva activa.
6. En la barra de menús, elija **Acción** > **Activar directiva**.

Creación de directivas de grabación personalizadas

Cuando el usuario crea sus propias directivas, establecerá reglas para especificar las sesiones que se grabarán de cuáles usuarios y grupos, aplicaciones publicadas y servidores. La consola de directivas de grabación de sesiones cuenta con un asistente para ayudarle a crear reglas. Para obtener la lista de aplicaciones publicadas y servidores, debe tener el permiso de lectura de administrador del sitio. Configúrelo en el Delivery Controller de este sitio.

Para cada regla que se cree, hay que especificar una acción de grabación y un criterio de regla. La acción de grabación se

© 1999-2017 Citrix Systems, Inc. All rights reserved.

aplica a las sesiones que cumplan con el criterio de la regla.

Para cada regla seleccione una acción de grabación:

- **No grabar**. (Seleccione **Inhabilitar la grabación de sesiones** en el **Asistente de reglas**.) Esta acción de grabación especifica que no se grabarán las sesiones que cumplan el criterio de la regla.
- **Grabar con notificación**. (Seleccione **Habilitar la grabación de sesiones con notificación** en el **Asistente de reglas**.) Esta acción de grabación especifica que se grabarán las sesiones que cumplan el criterio de la regla. Aparecerá una ventana emergente que notificará que se graba la sesión.
- **Grabar sin notificación**. (Seleccione **Habilitar la grabación de sesiones sin notificación** en el **Asistente de reglas**.) Esta acción de grabación especifica que se grabarán las sesiones que cumplan el criterio de la regla. Los usuarios no saben que se está grabando su sesión.

Para cada regla, elija al menos una de las siguientes opciones para crear el criterio de regla:

- **Usuarios o grupos**. Crea una lista de usuarios o grupos a los que se aplica la acción de grabación de la regla.
- **Recursos publicados**.Crea una lista de escritorios o aplicaciones publicadas a las que se aplica la acción de grabación de la regla. En el **Asistente de reglas**, elija el sitio o sitios de XenApp o XenDesktop donde están disponibles los escritorios o las aplicaciones.
- **Grupos de entrega o máquinas**. Crea una lista de máquinas o grupos de entrega a los que se aplicará la acción de grabación de la regla. En el **Asistente de reglas**, elija la ubicación donde residen las máquinas o los grupos de entrega.
- **Dirección IP o rango de IP**. Crea una lista de direcciones IP o intervalos de direcciones IP a las que se aplica la acción de grabación de la regla.En la pantalla **Seleccionar dirección IP y rango de IP**, agregue una dirección IP o intervalo IP válido para los que la grabación estará habilitada o inhabilitada.

Nota: La Consola de directivas de grabación de sesiones permite configurar varios criterios en una sola regla. Cuando se aplica una regla, se utilizan los operadores lógicos "AND" y "OR" para calcular la acción final. En términos generales, el operador "OR" se utiliza entre elementos de un criterio, y el operador "AND" se utiliza entre criterios independientes. Si el resultado es true, el motor de la directiva Grabación de sesiones toma la acción de la regla. De lo contrario, pasa a la siguiente regla y repite el proceso.

Cuando se crea más de una regla en la directiva de grabación, algunas sesiones pueden cumplir el criterio de más de una regla. En estos casos, la regla con la prioridad mayor es la que se aplica a las sesiones.

La acción de grabación de una regla determina su prioridad:

- Las reglas con la acción **No grabar** tienen mayor prioridad.
- Las reglas con la acción **Grabar con notificación** tienen el siguiente nivel de prioridad.
- Las reglas con la acción **Grabar sin notificación** tienen el nivel más bajo de prioridad.

Es posible que algunas sesiones no cumplan ningún criterio de regla en una directiva de grabación. Para estas sesiones, se aplica la regla alternativa de la acción de grabación de las directivas. La acción de grabación de la regla alternativa siempre es **No grabar**. La regla alternativa no se puede modificar o borrar.

Para configurar directivas personalizadas, haga lo siguiente:

1. Inicie la sesión como administrador de directivas autorizado en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie la Consola de directivas de grabación de sesiones y seleccione **Directivas de grabación** en el panel izquierdo. En la barra de menú, elija **Acción** > **Agregar nueva directiva**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Haga clic con el botón secundario en **Nueva directiva** y seleccione **Agregar regla**.
4. Seleccione una opción de grabación. En el **Asistente de reglas**, seleccione **Inhabilitar la grabación de sesiones**, **Habilitar la grabación de sesiones con notificación** (o **sin notificación**) y, a continuación, haga clic en **Siguiente**.
5. Seleccione los criterios de regla. Puede elegir una opción o cualquier combinación de ellas:
   Usuarios o grupos
   Recursos publicados
   Grupos de entrega o máquinas
   Dirección IP o rango de IP
6. Modificar el criterio de la regla. Para modificarlo, haga clic en los valores subrayados. Los valores se subrayan en función de los criterios que eligió en el paso anterior.
   Nota: Tenga en cuenta que, si elige el valor subrayado de **Recursos publicados**, la **Dirección del sitio** es la dirección IP, una URL o un nombre de máquina si el Controller está en una red local. La lista **Nombre de aplicación** muestra el nombre simplificado.
7. Siga las instrucciones del asistente para completar la configuración.

Uso de grupos de Active Directory

La funcionalidad de grabación de sesiones permite el uso de grupos de Active Directory al crear directivas. El uso de los grupos de Active Directory en lugar de usuarios individuales simplifica la creación y manejo de las reglas y directivas. Por ejemplo, si los usuarios del departamento financiero de la empresa se encuentran en un grupo de Active Directory denominado Finanzas, puede crear una regla que se aplique a todos los miembros de este grupo al seleccionar el grupo Finanzas en el **Asistente de reglas** cuando cree dicha regla.

Usuarios de la lista blanca

Se pueden crear directivas de grabación de sesiones para garantizar que las sesiones de algunos usuarios de la empresa nunca se graben. Se les llama usuarios de la *lista blanca*. Agregar a la lista blanca es útil para usuarios que gestionan información privada o cuando la organización no quiere grabar las sesiones de algún tipo de empleados.

Por ejemplo, si todos los jefes en la empresa son miembros del grupo de Active Directory denominado Ejecutivos, puede asegurarse que las sesiones de estos usuarios nunca se grabarán con la creación de una regla que desactive el grabado de sesiones para el grupo Ejecutivos. Mientras la directiva que contiene esta regla esté activa, ninguna sesión de los miembros del grupo Ejecutivo se grabará. Las sesiones de los demás miembros de la empresa se graban según las otras reglas de la directiva activa.

Criterios de uso para la regla de dirección IP o intervalo IP

Puede usar direcciones IP del cliente como criterios para la regla de coincidencia de directivas. Por ejemplo, si quiere grabar sesiones de aquellos clientes que tengan direcciones IP específicas o se encuentren dentro de un intervalo de direcciones IP concreto, utilice el **Asistente de reglas** para crear una regla que solo se aplique a esos clientes.

Crear una nueva directiva

Nota: Cuando utilice el **Asistente de reglas**, se le puede pedir que “haga clic en el valor subrayado que se modificará” aunque no haya ningún valor subrayado. Los valores aparecen subrayados solamente cuando es debido. Si no hay valores subrayados, ignore el paso.

1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie la Consola de directivas de grabación de sesiones.
3. Si una ventana emergente pide **Conectar con el servidor de grabación de sesiones**, compruebe que el nombre del

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Servidor de grabación de sesiones, el protocolo y el puerto son correctos. Haga clic en **Aceptar**.
4. En la Consola de directivas de grabación de sesiones, seleccione **Directivas de grabación**.
5. Desde el menú, elija **Agregar nueva directiva**. Una directiva denominada **Nueva directiva** aparece en el panel izquierdo.
6. Haga clic con el botón secundario en la nueva directiva y seleccione **Cambiar nombre** en el menú.
7. Escriba un nombre para la directiva que va a crear y pulse **Entrar** o haga clic en cualquier lugar fuera del nuevo nombre.
8. Haga clic con el botón secundario en la directiva, elija **Agregar nueva regla** en el menú para iniciar el **Asistente de reglas**.
9. Siga las instrucciones para crear las reglas de esta directiva.

Modificar una directiva

1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie la Consola de directivas de grabación de sesiones.
3. Si una ventana emergente pide **Conectar con el Servidor de grabación de sesiones**, compruebe que el nombre del Servidor de grabación de sesiones, el protocolo y el puerto son correctos. Haga clic en **Aceptar**.
4. En la Consola de directivas de grabación de sesiones, expanda **Directivas de grabación**.
5. Seleccione la directiva que desee modificar. Las reglas para esta directiva aparecen en el panel derecho.
6. Para agregar una regla nueva, modificar una regla o eliminar una regla:
   - En la barra de menús, elija **Acción** > **Agregar nueva regla.**Si la directiva está activa, aparece una ventana emergente solicitando que se confirme la acción. Utilice el **Asistente de reglas** para crear una nueva regla.
   - Seleccione la regla que quiera modificar, haga clic con el botón secundario y elija **Propiedades**. Use el **Asistente de reglas** para modificar la regla.
   - Seleccione la regla que quiera eliminar, haga clic con el botón secundario y elija **Eliminar regla**.

Eliminar una directiva

Nota: No se puede eliminar una directiva del sistema o una directiva que está activa.

1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie la Consola de directivas de grabación de sesiones.
3. Si una ventana emergente pide **Conectar con el Servidor de grabación de sesiones**, compruebe que el nombre del Servidor de grabación de sesiones, el protocolo y el puerto son correctos. Haga clic en **Aceptar**.
4. En la Consola de directivas de grabación de sesiones, expanda **Directivas de grabación**.
5. En el panel izquierdo, seleccione la directiva que desea eliminar. Si la directiva está activa, debe activar otra directiva.
6. En la barra de menús, elija **Acción** > **Eliminar directiva**.
7. Seleccione **Sí** para confirmar la acción.

Nota: Existe una limitación de las sesiones de aplicación preiniciadas:

- Si la directiva activa intenta que el nombre de aplicación coincida, las aplicaciones iniciadas en la sesión preiniciada no coincidirán, lo que provoca que la sesión no se grabe.
- Si la directiva activa graba todas las aplicaciones, cuando el usuario inicie sesión en Citrix Receiver para Windows (al mismo tiempo que se establece la sesión preiniciada), aparecerá una notificación de la grabación y se grabará la sesión preiniciada (vacía), así como las aplicaciones que se inicien más tarde en esa sesión.

Como solución alternativa, publique las aplicaciones en grupos de entrega diferentes, distribuidas según la directiva de grabación. No use el nombre de la aplicación como condición de grabación. Esto garantiza que se graben las sesiones preiniciadas. Sin embargo, las notificaciones seguirán apareciendo.

Comportamiento de la función Renovar

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Cuando se activa una directiva, la directiva anterior permanece en efecto hasta que la sesión del usuario finalice. Sin embargo, en algunos casos, la nueva directiva entra en efecto cuando se renueva el archivo. Los archivos se renuevan cuando llegan al límite de tamaño máximo. Para obtener información acerca del tamaño máximo de archivo para las grabaciones, consulte Especificación del tamaño del archivo para las grabaciones.

La siguiente tabla explica los detalles de lo que sucede cuando se aplica una nueva directiva mientras una sesión se está grabando y se da una renovación:

Si la directiva anterior era:	Y la directiva nueva es:	Después de una renovación, la directiva será:
No grabar.	Cualquier otra directiva	Sin cambios. La nueva directiva entra en efecto solamente cuando el usuario inicia una nueva sesión.
Grabar sin notificación	No grabar	La grabación se detiene.
	Grabar con notificación	La grabación continúa y aparece un mensaje de notificación.
Grabar con notificación	No grabar	La grabación se detiene.
	Grabar sin notificación	La grabación continúa. La próxima vez que el usuario inicia una sesión no aparece ningún mensaje.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Creación de mensajes de notificación

Dec 05, 2017

Si la directiva de grabación activa especifica que se debe notificar a los usuarios cuando sus sesiones se graben, aparecerá una ventana emergente con un mensaje de notificación después de que los usuarios escriban sus credenciales. La notificación predeterminada es la siguiente: “La actividad con uno o más de los programas que se iniciaron recientemente se está grabando. Si no está de acuerdo con esto, cierre los programas”. El usuario hace clic en **Aceptar** para cerrar la ventana y continuar la sesión.

El mensaje de notificación predeterminado se muestra en el idioma del sistema operativo de los equipos que alojan el servidor de grabación de sesiones.

Puede crear notificaciones personalizadas en los idiomas que quiera; sin embargo, solo puede tener un mensaje de notificación para cada idioma. Los usuarios verán el mensaje de notificación en el idioma en el que tengan la configuración regional.

Creación de un mensaje de notificación nuevo

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. En **Propiedades del Servidor de grabación de sesiones**, haga clic en la ficha **Notificaciones**.
4. Haga clic en **Agregar**.
5. Seleccione el idioma del mensaje y escriba el nuevo mensaje. Sólo puede crear un mensaje para cada idioma.

Después de aceptar y activar, el nuevo mensaje aparece en Mensajes de notificación por idioma.
Nota: La funcionalidad Registros de administrador de Grabación de sesiones permite capturar en un registro los cambios de directiva que se realizan en el Servidor de grabación de sesiones. Para obtener más información, consulte Registro de las actividades de administración.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Habilitar o inhabilitar la grabación

Dec 05, 2017

Debe instalar el Agente de grabación de sesiones en cada VDA con SO de servidor para el que quiera grabar sesiones. Cada agente tiene un parámetro de configuración que habilita la grabación en el servidor donde está instalado. Después de habilitar la grabación, la función Grabación de sesiones evalúa la directiva de grabación que está activa para determinar qué sesiones deben grabarse.

Cuando se instala el Agente de grabación de sesiones, la función de grabación está habilitada. Citrix recomienda inhabilitar la grabación de sesiones en los servidores donde no se vaya a grabar, porque esta función tiene cierto impacto en el rendimiento incluso aunque no se realice ninguna grabación.

Habilitar o inhabilitar la grabación en un servidor

1. Inicie una sesión en el servidor donde está instalado el Agente de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Agente de grabación de sesiones**.
3. En Grabación de sesiones, marque o desmarque la casilla **Habilitar la grabación de sesiones para este VDA de SO de servidor** para especificar si se puede o no grabar las sesiones de este servidor.
4. Cuando se le solicite, reinicie el servicio del Agente de grabación de sesiones para aceptar el cambio.

Nota: Cuando se instala la funcionalidad Grabación de sesiones, la directiva activa es **No grabar** (no se graban sesiones en ningún servidor). Para empezar a grabar, utilice la Consola de directivas de grabación de sesiones para activar otra directiva.

Habilitar la grabación con eventos personalizados

La funcionalidad de grabación de sesiones permite el uso de aplicaciones de terceros para agregar datos personalizados, conocidos como eventos, en las sesiones grabadas. Estos eventos aparecen cuando se ven las sesiones en el Reproductor de grabación de sesiones. Son parte del archivo de grabación de sesión y no se pueden modificar después de grabar la sesión.

Por ejemplo, un suceso puede decir lo siguiente: "Usuario abrió un explorador". Cada vez que un usuario abre un explorador durante una sesión que se está grabando, se agrega ese texto en ese punto de la grabación. Cuando se reproduce la sesión con el Reproductor de grabación de sesiones, la persona que examina la grabación puede ubicar y contar las veces que el usuario abrió un explorador Web sumando el número de marcadores que aparecen en la lista Eventos y marcadores del Reproductor de grabación de sesiones.

Para introducir eventos personalizados en las grabaciones en un servidor:

- Use las **Propiedades del Agente de grabación de sesiones** para habilitar un parámetro en cada servidor donde quiera introducir eventos personalizados. Cada servidor debe habilitarse por separado. No se pueden habilitar globalmente todos los servidores de un sitio.
- Escriba aplicaciones creadas en la API de sucesos que se ejecuta en cada sesión XenApp del usuario (para agregar los datos a la grabación).

La instalación de la funcionalidad de grabación de sesiones incluye una aplicación COM (API) para grabar eventos que permite la inserción de texto en la grabación desde aplicaciones de terceros. Puede usar la interfaz API con muchos lenguajes de programación entre ellos Visual Basic, C++ o C#. Para obtener más información, consulte el artículo CTX226844 de Citrix. El archivo .dll de la API de eventos de grabación de sesiones se instala como parte de la instalación de la funcionalidad de grabación de sesiones. Se encuentra en C:\Archivos de programa\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para habilitar las grabaciones con eventos personalizados en un servidor, lleve a cabo lo siguiente:

1. Inicie una sesión en el servidor donde está instalado el Agente de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Agente de grabación de sesiones**.
3. En **Propiedades del Agente de grabación de sesiones**, haga clic en la ficha **Grabación**.
4. En **Grabación de evento personalizado**, marque la casilla **Permitir que las aplicaciones de otros fabricantes graben datos personalizados en este servidor**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Habilitación o inhabilitación de la reproducción en directo de sesiones y la protección de la reproducción

Dec 05, 2017

Para habilitar o inhabilitar la reproducción de sesiones en directo

Con el reproductor de grabación de sesiones se puede ver una sesión mientras se está grabando o después de grabarla. Ver una sesión mientras se está grabando es similar a ver las acciones ejecutadas en tiempo real; sin embargo, hay un retraso de uno o dos segundos mientras los datos se propagan desde el servidor XenApp o XenDesktop.

Algunas funciones no están habilitadas cuando se ven sesiones que se están grabando:

- No se puede asignar una firma digital hasta que se complete la grabación. Si la firma digital está activada, es posible ver sesiones en directo, pero éstas no están firmas digitalmente y no es posible ver certificados hasta que se complete la sesión.
- La protección de reproducción no se puede aplicar hasta que se finalice la grabación. Si la protección de reproducción está habilitada, es posible ver sesiones en directo, pero estas no están cifradas hasta que la sesión finalice.
- No es posible guardar en caché un archivo hasta que la grabación finalice.

De forma predeterminada, la reproducción en directo de sesiones está habilitada.

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. En **Propiedades del Servidor de grabación de sesiones**, haga clic en la ficha **Reproducción**.
4. Marque o desmarque la casilla de verificación **Permitir la reproducción en directo de sesiones**.

Para habilitar o inhabilitar la protección de la reproducción

Como medida de seguridad, la grabación de sesiones automáticamente cifra los archivos de grabaciones antes de descargarlos para verlos en el Reproductor de grabación de sesiones. Esta protección de reproducción impide que alguien que no sea el usuario que descargó el archivo copie o reproduzca el archivo grabado. Estos archivos no pueden ser reproducidos en otra estación de trabajo o por otro usuario. Los archivos cifrados se identifican con una extensión .icle, los archivos no cifrados se identifican con una extensión .icl. Los archivos permanecen cifrados mientras están en el caché de la estación de trabajo donde está instalado el Reproductor de grabación de sesiones hasta que los abre un usuario autorizado.

Citrix recomienda el uso de HTTPS para proteger la transferencia de datos.

De forma predeterminada, la protección de reproducción está habilitada.

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. En **Propiedades del Servidor de grabación de sesiones**, haga clic en la ficha **Reproducción**.
4. Marque o desmarque la casilla **Cifrar archivos de grabación de sesiones descargados para reproducirlos**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Habilitar e inhabilitar la firma digital

Dec 05, 2017

Si instala certificados en los equipos donde están instalados los componentes de Grabación de sesiones, puede mejorar la seguridad de la implementación de esta funcionalidad asignando firmas digitales a la Grabación de sesiones.

De forma predeterminada, las firmas digitales no están habilitadas.Después de seleccionar el certificado para firmar las grabaciones, la Grabación de sesiones concede el permiso de lectura al Servicio de almacenamiento de grabación de sesiones.

Habilitar la firma digital

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. En **Propiedades del Servidor de grabación de sesiones**, haga clic en la ficha **Firma**.
4. Busque el certificado que permite la comunicación segura entre los equipos donde están instalados los componentes de grabación de sesiones.

Inhabilitar la firma digital

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. En **Propiedades del Servidor de grabación de sesiones**, haga clic en la ficha **Firma**.
4. Haga clic en **Borrar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cómo especificar dónde se almacenan las grabaciones

Dec 05, 2017

Use las propiedades del servidor de grabación de sesiones para especificar dónde se guardan las grabaciones y dónde se restauran las grabaciones que están ya archivadas para reproducirlas.

Nota: Para archivar grabaciones o restaurar archivos eliminados, utilice el comando ICLDB. Para obtener más información, consulte cómo archivar y restaurar grabaciones.

Especificar directorios para almacenar las grabaciones

De forma predeterminada, las grabaciones se guardan en el directorio drive:**\SessionRecordings** del equipo que aloja el servidor de grabación de sesiones. Puede cambiar el directorio donde se guardan las grabaciones, agregar directorios adicionales para equilibrar la carga en varios volúmenes o utilizar espacio adicional. Varios directorios en la lista indican que las grabaciones tienen la carga equilibrada a través de los directorios. Se puede agregar un directorio varias veces. El equilibrio de carga cambia a través de los directorios.

1. Inicie sesión en el equipo donde se encuentra el servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del servidor de grabación de sesiones**.
3. En **Propiedades del servidor de grabación de sesiones**, haga clic en la ficha **Almacenamiento**.
4. Use la lista de los **Directorios de almacenamiento de archivos** para trabajar con los directorios donde se guardan las grabaciones.

Después de seleccionar los directorios, la Grabación de sesiones les concede el servicio con permiso de control total.

Se pueden crear directorios de almacenamiento de archivos en la unidad local, el volumen de red SAN o un lugar especificado por una ruta UNC. No se respaldan las letras de unidades de red asignadas. No utilice la Grabación de sesiones con almacenamiento NAS (Network-Attached Storage), ya que existen ciertos problemas de seguridad y rendimiento asociados con la escritura de datos en una unidad de red.

Especificar un directorio para restaurar las grabaciones archivadas para reproducirlas

De forma predeterminada, las grabaciones archivadas se restauran en el directorio drive:**\SessionRecordingsRestore** del equipo donde se encuentra el servidor de grabación de sesiones. Puede cambiar el directorio.

1. Inicie sesión en el equipo donde se encuentra el servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del servidor de grabación de sesiones**.
3. En **Propiedades del servidor de grabación de sesiones**, haga clic en la ficha **Almacenamiento**.
4. En el campo **Directorio de restauración de archivos**, escriba el directorio donde se van a restaurar las grabaciones archivadas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Especificar el tamaño de archivo para las grabaciones

Dec 05, 2017

A medida que van aumentando de tamaño las grabaciones, los archivos pueden tardar más en descargarse y en reaccionar cuando se utiliza el control deslizante para navegar durante la reproducción. Para controlar el tamaño de los archivos, especifique un límite para un archivo. Cuando la grabación alcanza este límite, la función de grabación de sesiones cierra el archivo y abre uno nuevo para continuar grabando. Esta acción se llama renovar.

Importante: La opción de renovación no se aplica a sesiones de escritorio VDI para XenDesktop 7.8 ni para el Agente de grabación de sesiones. En esos casos, cada archivo de grabación tiene un límite de tamaño máximo de 1 GB y las actividades no se registran pasado ese límite.

Se pueden especificar dos límites para la renovación:

- **Tamaño de archivo.** Cuando el archivo alcance un número específico de megabytes, la función de grabación de sesiones cierra el archivo y abre uno nuevo. De forma predeterminada, los archivos se renuevan a los 50 megabytes, sin embargo se puede especificar un límite entre 10 megabytes y un gigabyte.
- **Duración.** Cuando una sesión se haya grabado una cantidad concreta de horas, el archivo se cierra y se abre uno nuevo. De forma predeterminada, los archivos se renuevan a las 12 horas, sin embargo se puede especificar un límite entre una y 24 horas.

La función Grabación de sesiones comprueba ambos campos para determinar cuál de estos eventos ocurre antes y determinar así cuándo realizar la renovación. Por ejemplo, si especifica que el tamaño de archivo es de 17 MB y seis horas de duración y la grabación llega a 17 MB en tres horas, la función de grabación de sesiones reacciona al tamaño de archivo de 17 MB y lo cierra para abrir uno nuevo.

Para evitar que se creen muchos archivos pequeños, la Grabación de sesiones no hace una renovación para grabaciones de menos de una hora (este es el mínimo que se puede especificar) independientemente del valor especificado para el tamaño de archivo. La excepción a esta regla se da cuando el tamaño de archivo sobrepasa un gigabyte.

Especificar el tamaño máximo de archivo para las grabaciones

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. En **Propiedades del Servidor de grabación de sesiones**, haga clic en la ficha **Renovación**.
4. Elija un número entero entre 10 y 1024 para especificar el tamaño máximo del archivo en megabytes.
5. Elija un número entero entre 1 y 24 para especificar el tiempo máximo de grabación en horas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Registro de las actividades de administración

Dec 05, 2017

La funcionalidad Captura de registros del administrador de grabación de sesiones registra las siguientes actividades:

- Los cambios en las directivas de grabación que se realizan en Citrix Director o en la Consola de directivas de grabación de sesiones.
- Los cambios en las Propiedades del servidor de grabación de sesiones.
- Las descargas de grabaciones del Reproductor de grabación de sesiones.
- La grabación de una sesión mediante la Grabación de sesiones después de la consulta de la directiva.
- Intentos de acceso no autorizado al servicio de Registro de administrador.

> ## 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

Habilitación o inhabilitación de Registro de administrador

Después de la instalación, puede habilitar o inhabilitar la característica de Captura de registros del administrador de grabación de sesiones en Propiedades del Servidor de grabación de sesiones.

1. Inicie sesión como administrador en el servidor donde está instalada la Captura de registros del administrador de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Servidor de grabación de sesiones**.
3. Haga clic en la ficha **Registro**.

Si Captura de registros del administrador de grabación de sesiones está inhabilitado, no se captura en registro ninguna actividad nueva. Puede consultar los registros existentes desde la interfaz de usuario basada en Web.

Cuando el **bloqueo obligatorio** está habilitado, se bloquean las siguientes actividades si falla la captura de registros. Un evento del sistema se registra también con un ID de evento 6001:

- Los cambios en las directivas de grabación que se realizan en Citrix Director o en la Consola de directivas de grabación de sesiones.
- Los cambios en las Propiedades del servidor de grabación de sesiones.

La Grabación de sesiones no se ve afectada por el parámetro de bloqueo obligatorio.

Concesión de acceso a los usuarios

Por razones de seguridad, conceda a los usuarios solamente los permisos que necesiten para realizar funciones específicas, tales como consultar los registros de Registro de administrador.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Los permisos se conceden agregando usuarios a roles, desde la Consola de autorización de grabación de sesiones, en el Servidor de grabación de sesiones. Registro de administrador tiene dos roles:

- **LoggingWriter**. Otorga permiso de escritura en los registros de Registro de administrador. De forma predeterminada, los administradores locales y los servicios de red son miembros de este rol.

  Nota: Si modifica la pertenencia predeterminada de **LoggingWriter**, es posible que se produzca un error al escribir en el registro.

- **LoggingReader.** Otorga permiso para consultar los registros de Registro de administrador. No hay miembros predeterminados para este rol.

Para asignar usuarios a los roles

1. Como administrador, inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. Inicie la **Consola de autorización de grabación de sesiones**.
3. Seleccione el rol al que desea asignar usuarios.
4. Desde la barra de menú, elija **Acción** > **Asignar usuarios y grupos de Windows**.
5. Agregar usuarios y grupos.

Cualquier cambio a la consola tomará efecto durante la actualización que se da cada minuto.

Configuración de la cuenta de servicio del Registro de administrador

De forma predeterminada, la funcionalidad Registro de administrador se ejecuta como una aplicación Web en Internet Information Services (IIS), y es su identidad es Servicio de red. Para mayor seguridad, puede cambiar la identidad de esta aplicación Web a una cuenta de servicio o una cuenta de dominio específico.

1. Como administrador, inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. En el Administrador de IIS, haga clic en **Grupos de aplicaciones.**
3. En **Grupos de aplicaciones**, haga clic con el botón secundario en **SessionRecordingLoggingAppPool** y, a continuación, seleccione **Configuración avanzada**.
4. Cambie el atributo **identidad** a la cuenta que quiere usar.
5. Conceda el permiso **db_owner** a la cuenta de la base de datos **CitrixSessionRecordingLogging** en Microsoft SQL Server.
6. Conceda a la cuenta el permiso de lectura para la clave de Registro ubicada en **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.

Habilitación o inhabilitación del registro de acciones de grabación

De forma predeterminada, la funcionalidad Registro de administrador registra toda acción de grabación una vez completada la consulta de la directiva. Lo que puede generar una gran cantidad de registros. Para mejorar el rendimiento y ahorrar espacio de almacenamiento, inhabilite este tipo de registro en el Registro.

1. Como administrador, inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. Abra el Editor del Registro.
3. Vaya a **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server**.
4. Establezca el valor de **EnableRecordingActionLogging**:

   0 equivale a inhabilitar la captura de registros para acciones de grabación

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1 equivale a habilitar la captura de registros para acciones de grabación

Consulta de datos de Registro de administrador

La funcionalidad Grabación de sesiones ofrece una interfaz de usuario basada en Web para consultar todos los registros capturados por Registro de administrador.

En el equipo donde se encuentra el Servidor de grabación de sesiones:

1. En el menú **Inicio**, elija **Captura de registros del administrador de grabación de sesiones**.
2. Introduzca las credenciales de un usuario **LoggingReader**.

En otros equipos:

1. Abra un explorador Web y vaya a la página de Registro de administrador.

   Para HTTPS: https://*servername*/SessionRecordingLoggingWebApplication/, donde *servername* es el nombre del equipo que aloja el Servidor de grabación de sesiones.

   Para HTTP: http://*servername*/SessionRecordingLoggingWebApplication/, donde *servername* es el nombre del equipo que aloja el Servidor de grabación de sesiones.

2. Introduzca las credenciales de un usuario **LoggingReader**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalación de Grabación de sesiones con alta disponibilidad de base de datos

Dec 05, 2017

La Grabación de sesiones admite las siguientes soluciones de alta disponibilidad de base de datos en función de Microsoft SQL Server. Las bases de datos automáticamente pueden conmutar por error cuando falle el hardware o el software de un servidor de SQL principal o primario, lo que garantiza que la Grabación de sesiones funcione sin interrupciones.

- Grupos de disponibilidad AlwaysOn

  La función Grupos de disponibilidad AlwaysOn es una solución de alta disponibilidad y recuperación ante desastres que ofrece una alternativa a nivel empresarial para la creación de reflejo de base de datos. Introducida en SQL Server 2012, Grupos de disponibilidad AlwaysOn maximiza la disponibilidad de un conjunto de bases de datos de usuario para una empresa. 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: http://msdn.microsoft.com/en-us/library/hh510230.

- Agrupación en clústeres de SQL Server

  La tecnología de agrupación en clústeres de SQL de Microsoft permite que un servidor tome el control automáticamente de las tareas y las responsabilidades de otro servidor que ha fallado. No obstante, la instalación de esta solución es 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. Para obtener más información, consulte: https://msdn.microsoft.com/en-us/library/ms189134.aspx.

- Creación de reflejo de base de datos de SQL Server

  Crear reflejos de base de datos permite que una conmutación por error automática se produzca en segundos si se produce un error en el servidor activo de la base de datos. Esta solución es más costosa que las otras dos soluciones debido a que se requieren licencias de SQL Server completas en cada servidor de la base de datos. No se puede usar la edición SQL Server Express en un entorno reflejado. Para obtener más información, consulte: https://msdn.microsoft.com/en-us/library/ms189852.aspx.

Métodos de instalación de Grabación de sesiones con alta disponibilidad de base de datos

Para instalar Grabación de sesiones con alta disponibilidad de base de datos, lleve a cabo una de las siguientes opciones:

- Instale primero los componentes del Servidor de grabación de sesiones y, a continuación, configure la alta disponibilidad de las bases de datos creadas.
  Puede instalar los componentes de Administración de grabación de sesiones con bases de datos configuradas que se van a instalar en la instancia preparada de SQL Server y, a continuación, configurar la alta disponibilidad de las bases de datos creadas.
  - Para la agrupación en clústeres y la función Grupos de disponibilidad AlwaysOn, debe cambiar manualmente el nombre de la instancia de SQL Server por el nombre del agente de escucha del grupo de disponibilidad o la red de SQL Server en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\SmAudDatabaseInstance.
  - Para crear el reflejo de la base de datos, debe agregar manualmente los servidores de conmutación por error de las bases de datos en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\DatabaseFailoverPartner y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\LoggingDatabaseFailoverPartner.

- Configure la alta disponibilidad de las bases de datos vacías e instale los componentes de Administración de grabación de sesiones.
  Puede crear dos bases de datos vacías en calidad de Base de datos de grabación de sesiones y Base de datos de registros de administrador en la instancia principal de SQL Server y configurar la alta disponibilidad de estas. A continuación, deberá introducir el nombre de la instancia de SQL Server cuando instale los componentes del Servidor de grabación de sesiones:
  - Para usar la solución Grupos de disponibilidad AlwaysOn, introduzca el nombre del agente de escucha del grupo de disponibilidad
  - Para usar la solución de reflejo de bases de datos, escriba el nombre del servidor SQL principal
  - Para usar la solución de agrupación en clústeres, escriba el nombre de red del servidor SQL

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ver las grabaciones

Dec 05, 2017

Use el Reproductor de grabaciones de sesión para ver, buscar y añadir marcadores a las sesiones grabadas de XenApp o XenDesktop.

Si la función de reproducción en directo está habilitada cuando se graba la sesión, es posible ver las sesiones que se están grabando con solo un retraso de pocos segundos como también aquellas sesiones que ya han sido grabadas.

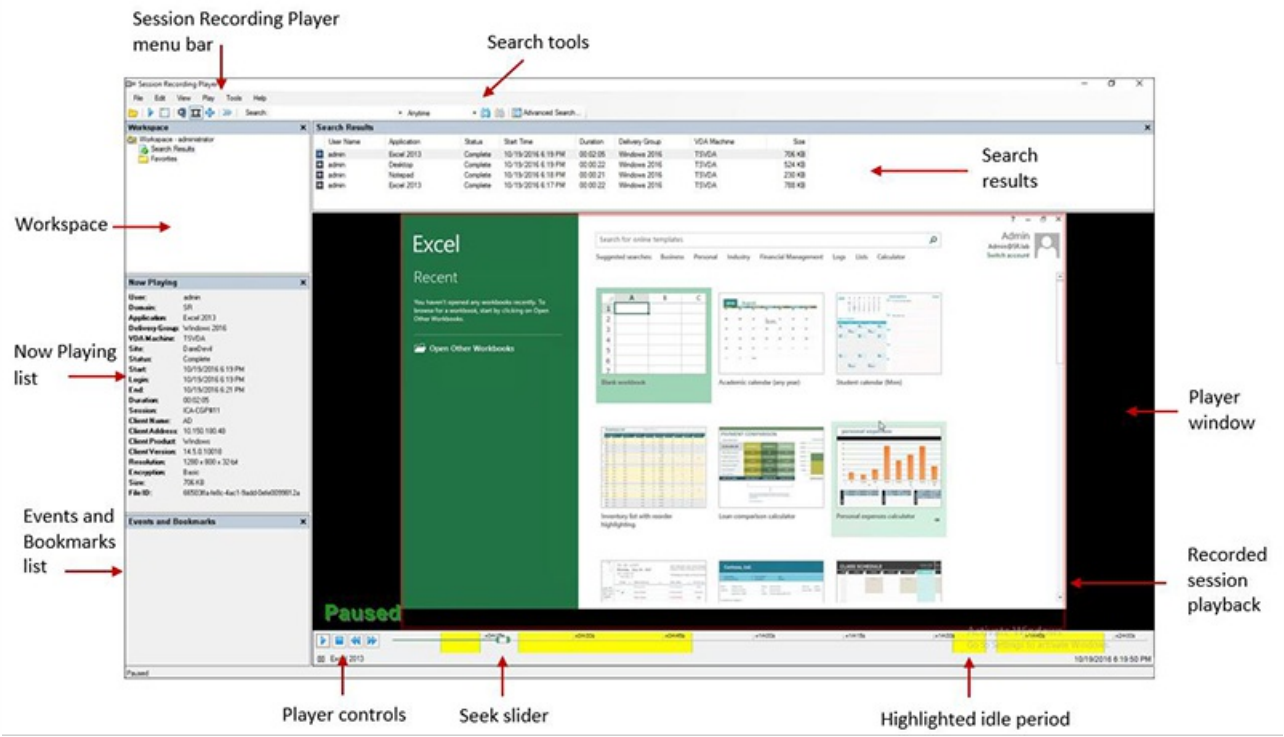
Las sesiones de mayor duración o con un tamaño de archivo mayor que el límite configurado por el administrador de Grabación de sesiones aparecen en más de un archivo de sesión.

Nota: Un administrador de Grabación de sesiones debe conceder a los usuarios acceso a las sesiones grabadas en agentes VDA de SO de servidor. Si se le deniega el acceso a ver las sesiones, póngase en contacto con su administrador de grabación de sesiones.
Cuando se instala el Reproductor de grabaciones de sesiones, normalmente el administrador de grabación de sesiones establece una conexión entre el Reproductor de grabaciones de sesiones y el servidor de grabación de sesiones. Si esta conexión no está configurada, la primera vez que realice una búsqueda de archivos se le pedirá que la configure. Póngase en contacto con el administrador de Grabación de sesiones para obtener la información para la configuración.

Iniciar el Reproductor de grabación de sesiones

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio** , elija **Reproductor de grabación de sesiones**.
   Aparecerá el Reproductor de grabación de sesiones.

Esta ilustración muestra el Reproductor de grabación de sesiones e indica los componentes más importantes. Las funciones de estos elementos se describen en los siguientes artículos.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mostrar u ocultar elementos de la ventana

El Reproductor de grabación de sesiones tiene elementos de ventana que se pueden cambiar entre activado y desactivado.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio** , elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Ver**.
4. Seleccione los elementos que desea mostrar. Cuando se selecciona un elemento, éste aparece de inmediato. Una marca indica que se seleccionó el elemento.

Cambiar de Servidores de grabación de sesiones

Si el administrador de Grabación de sesiones configuró su Reproductor de grabación de sesiones para que se conectara a varios Servidores de grabación de sesiones, puede seleccionar entre ellos el servidor al que quiere conectar el reproductor. El Reproductor de grabación de sesiones solo puede conectarse a un único servidor de grabación de sesiones a la vez.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio** , elija **Reproductor de grabación de sesiones**.
3. En la barra del menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Conexiones** .
4. Seleccione el Servidor de grabación de sesiones al que quiere conectarse.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Abrir y reproducir grabaciones

Dec 05, 2017

Puede abrir las grabaciones de sesiones en el Reproductor de grabación de sesiones de tres maneras:

- Realice una búsqueda con el Reproductor de grabación de sesiones. Las sesiones grabadas que cumplen con el criterio de búsqueda aparecerán en el área de resultados.
- Acceda a los archivos de grabación de sesión directamente desde la unidad de disco local o desde una unidad compartida.
- Acceda a los archivos de grabaciones grabadas desde la carpeta Favoritos.

Cuando abra un archivo que se grabó sin firma digital, aparecerá un mensaje de advertencia indicando que el origen y la integridad del archivo no se verificaron. Si está seguro de la integridad del archivo, haga clic en **Yes** en el mensaje de advertencia y abra el archivo.

Nota: La funcionalidad Registros de administrador de Grabación de sesiones permite registrar las descargas de los archivos de grabaciones del Reproductor de grabación de sesiones. Para obtener más información, consulte Registro de las actividades de administración.

Abrir y reproducir una grabación en el área de resultados

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Realice una búsqueda.
4. Si no ve el área de resultados, seleccione **Resultados de la búsqueda** en el panel del área de trabajo.
5. En el área de resultados, seleccione la sesión que desea reproducir.
6. Lleve a cabo alguna de las siguientes acciones:
   - Haga doble clic en la sesión
   - Haga clic con el botón secundario y seleccione **Reproducir**
   - En la barra de menú del **Reproductor de grabación de sesiones**, seleccione **Reproducir** > **Reproducir**

Abrir y reproducir una grabación al acceder al archivo

Los nombres de archivo de las sesiones grabadas empiezan con una "i_", tienen luego una identificación de archivo alfanumérica única y después una extensión de archivo .icl o .icle. La extensión .icl caracteriza las grabaciones donde no se aplica la protección de reproducción, mientras que la extensión .icle significa que las grabaciones tienen aplicada la protección de reproducción. Los archivos de las sesiones grabadas se guardan en una carpeta con la fecha en que se grabaron. Por ejemplo, el archivo de una grabación realizada el 22 de diciembre de 2014 se guarda en la ruta de carpeta 2014\12\22.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Lleve a cabo alguna de las siguientes acciones:
   - En la barra de menú del **Reproductor de grabación de sesiones**, seleccione **Archivo** > **Abrir** y vaya al archivo
   - En el explorador Windows, vaya al archivo y arrástrelo hasta la ventana del **Reproductor**
   - En el explorador Windows, navegue hasta el archivo y haga doble clic
   - Si creó Favoritos en el panel del área de trabajo, elija **Favoritos** y abra el archivo en el área de Favoritos de la misma forma que se abren los archivos del área de resultados

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Uso de los favoritos

La creación de carpetas de Favoritos permite el acceso rápido a grabaciones que el usuario ve con frecuencia. Las carpetas de Favoritos hacen referencia a archivos de grabación de sesión que están guardados en la estación de trabajo o en una unidad de red. Estos archivos pueden importarse y exportarse en otras estaciones de trabajo y las carpetas se pueden compartir con otros usuarios del Reproductor de grabación de sesiones.

Nota: Solamente los usuarios con derechos de acceso al Reproductor de grabación de sesiones pueden descargar los archivos de sesiones grabadas asociados a carpetas de Favoritos. Póngase en contacto con el administrador de la funcionalidad Grabación de sesiones para obtener derechos de acceso.
Para crear una subcarpeta de Favoritos:

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la ventana **Reproductor de grabación de sesiones**, elija la carpeta **Favoritos** en su panel de área de trabajo.
4. En la barra de menú, elija **Archivo** > **Carpeta** > **Nueva carpeta**. Aparecerá una nueva carpeta en la carpeta **Favoritos**.
5. Escriba el nombre de la carpeta y luego presione la tecla **Entrar** o haga clic en cualquier lugar para aceptar el nuevo nombre.

Utilice las demás opciones que aparecen en el menú **Archivo** > **Carpeta** para eliminar, cambiar el nombre, copiar, importar y exportar las carpetas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Búsqueda de sesiones grabadas

Dec 05, 2017

El reproductor de grabación de sesiones permite realizar búsquedas rápidas, búsquedas avanzadas y también permite especificar opciones aplicables a todas las búsquedas. Los resultados de las búsquedas aparecen en el área de resultados del reproductor de grabación de sesiones.

Nota: Para ver todas las sesiones grabadas disponibles, hasta llegar a la cantidad máxima de sesiones que pueden aparecer en una búsqueda, realice la búsqueda sin especificar ningún parámetro.

Búsqueda rápida

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Defina el criterio de búsqueda:
   - Indique el criterio de búsqueda en el campo **Búsqueda**. Para mayor facilidad:
   - Mueva el puntero sobre la etiqueta **Búsqueda** para ver una lista de los parámetros que se pueden utilizar como guía.
   - Haga clic en la flecha a la derecha del campo **Búsqueda** para ver las últimas 64 búsquedas realizadas.
   - Use la lista desplegable situada a la derecha del campo **Búsqueda** para seleccionar un período o duración de la grabación de la sesión.
4. Haga clic en el icono de binóculos a la derecha de la lista para iniciar una búsqueda.

Búsqueda avanzada

Sugerencia: Las búsquedas avanzadas pueden tardar hasta 20 segundos en devolver resultados que contengan más de 150 000 entidades. Citrix recomienda usar condiciones de búsqueda más precisas, tales como un intervalo de fechas o un usuario específico, para reducir la cantidad de resultados.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la ventana **Reproductor de grabación de sesiones**, haga clic en **Búsqueda avanzada** en la barra de herramientas o elija **Herramientas** > **Búsqueda avanzada**.
4. Defina el criterio de búsqueda en las fichas del cuadro de diálogo **Búsqueda avanzada**:
   - **Común**. Permite buscar por dominio o autoridad de cuentas, sitio, grupo, VDA con SO de servidor, aplicación o ID de archivo.
   - **Fecha/Hora**. Permite buscar por fecha, día de la semana y hora del día.
   - **Eventos**. Permite buscar en los eventos personalizados que agregó a las sesiones el Administrador de grabación de sesiones.
   - **Otro**. Permite buscar por nombre de la sesión, nombre del cliente, dirección del cliente y duración de la grabación. También permite especificar para esta búsqueda el número máximo de resultados a mostrar y si se incluirán o no archivos ya archivados.

   Tal y como se va especificando el criterio de búsqueda, la consulta que se está creando aparece en el panel de abajo del cuadro de diálogo.
5. Haga clic en **Búsqueda** para iniciar la búsqueda.

Sugerencia: Las búsquedas avanzadas se pueden guardar y volver a obtener. Haga clic en **Guardar** en el cuadro de diálogo **Búsqueda avanzada** para guardar la consulta actual. Haga clic en **Abrir** en el cuadro de diálogo **Búsqueda avanzada** para abrir una consulta guardada. Las consultas se guardan como archivos con una extensión .isq.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Opciones de búsqueda

Las opciones de búsqueda del Reproductor de grabación de sesiones permiten limitar la cantidad de grabaciones de sesión a mostrar en los resultados. También permiten especificar si deben incluirse o no las grabaciones de sesión ya archivadas.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra del menú **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Búsqueda**.
4. En el campo **Resultados máximos a mostrar**, escriba la cantidad de resultados que se mostrarán. Se pueden mostrar un máximo de 500 resultados.
5. Para definir si se van a incluir o no archivos ya archivados en las búsquedas, marque o desmarque **Incluye archivos ya archivados**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Reproducción de sesiones grabadas

Dec 05, 2017

Después de abrir una sesión grabada en el Reproductor de grabación de sesiones, se puede navegar a través de las grabaciones con uno de los siguientes métodos:

- Con los controles del reproductor para reproducir, detener, pausar y aumentar o disminuir la velocidad de reproducción
- Use el control deslizante para moverse hacia adelante o hacia atrás

Si se han agregado marcadores a la grabación o si las sesiones grabadas contienen eventos personalizados, es posible navegar a través de las sesiones grabadas utilizando los marcadores y los eventos.

Nota:

- Es posible que durante la reproducción de una grabación de sesión aparezca un segundo puntero. El segundo puntero aparece cuando durante la grabación el usuario navegó dentro de Internet Explorer e hizo clic en una imagen que originalmente era más grande que la pantalla pero que de forma automática Internet Explorer redujo de tamaño. Aunque aparezca un solo puntero durante la sesión, es posible que aparezcan dos al reproducirla.
- Esta versión de la función de grabación de sesiones no respalda la Aceleración multimedia SpeedScreen para XenApp ni la configuración de directiva Ajuste de calidad Flash para XenApp. Cuando se habilita esta opción, la reproducción muestra un cuadrado negro.
- La funcionalidad de grabación de sesiones no puede grabar el vídeo de la cámara Web de Lync cuando se usa HDX RealTime Optimization Pack para Microsoft Lync.
- Cuando se graba una sesión con una resolución mayor o igual a 4096 x 4096, es posible que la grabación aparezca fragmentada.
- No se pueden grabar correctamente sesiones de escritorio Windows 7 si el **Modo de gráficos antiguo** está habilitado en la directiva del sitio de XenDesktop y si **Almacenamiento en caché de disco** está habilitado en la directiva de Citrix Receiver para Windows. En esas grabaciones, aparece una pantalla en negro.
  Como solución temporal, inhabilite **Almacenamiento en caché de disco** con la ayuda de los objetos de directiva de grupo ubicados en las máquinas donde se instaló Citrix Receiver para Windows. Para obtener más información sobre cómo inhabilitar **Almacenamiento en caché de disco**, consulte CTX123169 y Configuración con la plantilla administrativa de objeto de directiva de grupo.
- La Grabación de sesiones no admite el modo de presentación Framehawk. Por eso, las sesiones que tienen el modo de presentación Framehawk no pueden grabarse ni reproducirse correctamente. Es posible que las sesiones grabadas en el modo de presentación Framehawk no contengan las actividades de las sesiones.

Uso de los controles del reproductor

Puede hacer clic en los controles de la ventana del Reproductor, o bien, puede acceder a ellos si selecciona **Reproducir** en la barra de menú del **Reproductor de grabación de sesiones**. Use los controles del reproductor para:

	Reproducir el archivo de sesión seleccionado.
	Pausar la reproducción.
	Detener la reproducción. Si hace clic en **Detener**, luego en **Reproducir**, la reproducción volverá al inicio del archivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Disminuir la velocidad actual de la reproducción a un mínimo de un cuarto de la velocidad normal.
	Aumentar la velocidad actual de la reproducción a un máximo de 32 veces la velocidad normal.

Uso del control deslizante

Use el control deslizante de la parte inferior de la ventana del reproductor para ir a otra posición dentro de la sesión grabada. Se puede arrastrar el control deslizante al lugar en la grabación que se desea ver o se puede hacer clic en cualquier parte del control deslizante para ir a ese lugar.

También se pueden utilizar las siguientes teclas para controlar el control deslizante:

Clave:	**Buscar acción:**
Página de inicio	Busca el inicio.
Fin	Busca el final.
Flecha derecha	Busca cinco segundos hacia adelante.
Flecha izquierda	Busca cinco segundos hacia atrás.
Mover la rueda del puntero una posición hacia abajo	Busca 15 segundos hacia adelante.
Mover la rueda del puntero una posición hacia arriba	Busca 15 segundos hacia atrás.
Ctrl + Flecha derecha	Busca 30 segundos hacia adelante.
Ctrl + Flecha izquierda	Busca 30 segundos hacia atrás.
Av Pág	Busca un minuto hacia adelante.
Re Pág	Busca un minuto hacia atrás.
Ctrl + Mover la rueda del puntero una posición hacia abajo	Busca 90 segundos hacia adelante.
Ctrl + Mover la rueda del puntero una posición hacia arriba	Busca 90 segundos hacia atrás.
Ctrl + Av Pág	Busca seis minutos hacia adelante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Clave:	Buscar acción:
Ctrl + Re Pág	Busca seis minutos hacia atrás.

Nota: Para ajustar la velocidad del control deslizante: en la barra de menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Reproductor** y arrastre el control para aumentar o disminuir el tiempo de respuesta de búsqueda. Un tiempo de respuesta más rápido necesita más memoria. La respuesta puede ser lenta, porque depende del tamaño de las grabaciones y el hardware de la máquina.

Cambiar la velocidad de reproducción

Se puede configurar el Reproductor de grabación de sesiones para que reproduzca las sesiones grabadas en incrementos exponenciales desde un cuarto de la velocidad normal hasta 32 veces la velocidad normal de reproducción.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones**, seleccione **Reproducir** > **Velocidad de reproducción**.
4. Elija una opción de velocidad.

La velocidad se ajustará inmediatamente. Aparecerá un número debajo de la ventana de controles del reproductor que indica el aumento o disminución de velocidad. En la ventana del reproductor aparecerá brevemente un texto en verde indicando la tasa exponencial.

Resaltar los periodos de inactividad de las sesiones grabadas

Los periodos de inactividad de una sesión grabada son las partes en que no se lleva a cabo ninguna acción. El Reproductor de grabación de sesiones puede destacar los periodos de inactividad que haya en las sesiones grabadas cuando se reproducen.La opción está **activada** de manera predeterminada.

Tenga en cuenta que no se resaltan los periodos de inactividad cuando se reproducen sesiones en directo con el Reproductor de grabación de sesiones.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Desde la barra de menú del **Reproductor de grabación de sesiones**, elija **Ver** > **Periodos de inactividad** y marque o deje sin marcar la casilla.

Saltarse los espacios donde no ocurre ninguna acción

El modo de revisión rápida permite configurar el Reproductor de grabación de sesiones para que se salte las porciones de las sesiones grabadas en las que no se realiza acción alguna. Este parámetro ahorra tiempo, sin embargo no se salta las secuencias animadas tales como punteros animados, cursores parpadeantes o relojes con movimientos de agujas.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Reproducir** > **Modo de revisión rápida**.

La opción cambia entre encendida y apagada. Cada vez que se selecciona, su estado aparece en verde brevemente en la ventana del reproductor.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para usar eventos y marcadores

Dec 05, 2017

Los eventos y marcadores se pueden utilizar para navegar a través de las sesiones grabadas.

Los eventos se agregan a las sesiones tal y como se van grabando con la API de eventos y con aplicaciones de terceros. Los eventos se guardan como parte del archivo de la sesión. No se puede eliminarlos ni cambiarlos con el reproductor de grabación de sesiones.

Los marcadores son marcas que se agregan a las sesiones grabadas mediante el reproductor de grabación de sesiones. Los marcadores se asocian a las sesiones grabadas hasta que se borren, pero no se guardan como parte del archivo de la sesión. De forma predeterminada, cada marcador tiene la etiqueta **Marcador**, pero la anotación se puede cambiar a cualquier otra con una extensión de 128 caracteres.

Los eventos y los marcadores aparecen como puntos debajo de la ventana del reproductor. Los eventos aparecen como puntos amarillos y los marcadores como puntos azules. Cuando se coloca el puntero sobre estos puntos se muestra la etiqueta asociada con ellos. Es posible también mostrar los eventos y marcadores en la lista **Eventos y marcadores** del Reproductor de grabación de sesiones. Estos aparecen en dicha lista con las etiquetas de texto y el número de veces que aparecen en la sesión grabada en orden cronológico.

Los eventos y marcadores se pueden utilizar para navegar a través de las sesiones grabadas. Al ir a un evento o un marcador, se puede saltar hasta el punto en la sesión grabada donde se inserta ese evento o marcador.

Mostrar eventos y marcadores en la lista

En la lista **Eventos y marcadores**, se muestran los eventos y los marcadores que se insertaron en la sesión que está reproduciéndose. Puede mostrar eventos solamente, marcadores solamente o ambos.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Mueva el puntero al área de la lista **Eventos y marcadores**, y haga clic con el botón secundario para ver el menú.
4. Seleccione **Mostrar solo eventos**, **Mostrar marcadores solamente** o **Mostrar todo**.

Agregar un marcador

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Empiece a reproducir la sesión grabada donde se desea agregar el marcador.
4. Mueva el control deslizante a la posición donde se va a agregar el marcador.
5. Mueva el puntero al área de la ventana del reproductor y haga clic con el botón secundario para mostrar el menú.
6. Agregue un marcador con la etiqueta predeterminada **Marcador** o cree una anotación:
   - Para agregar un marcador con la etiqueta predeterminada **Marcador**, elija **Agregar Marcador**.
   - Para agregar un marcador con una etiqueta descriptiva creada por el usuario, elija **Agregar Anotación**. Escriba el texto que desea asignar al marcador, puede tener una extensión de hasta 128 caracteres. Haga clic en **Aceptar**.

Agregar o cambiar una anotación

Después de crear un marcador se le puede agregar una anotación o se puede modificar la anotación que tiene.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Empiece a reproducir la sesión grabada que contiene el marcador.
4. Asegúrese que la lista de eventos y marcadores muestre los marcadores.
5. Seleccione el marcador en la lista **Eventos y marcadores**, y haga clic con el botón secundario para ver el menú.
6. Elija **Modificar anotación**.
7. En la ventana que aparece, escriba la anotación y haga clic en **Aceptar**.

Eliminar un marcador

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Empiece a reproducir la sesión grabada que contiene el marcador.
4. Asegúrese que la lista de eventos y marcadores muestre los marcadores.
5. Seleccione el marcador en la lista de eventos y marcadores y haga clic con el botón secundario para mostrar el menú.
6. Elija **Eliminar**.

Vaya a un evento o un marcador

Cuando se va a un evento o a un marcador, el reproductor de grabación de sesiones va al punto en la sesión grabada donde se agregó el evento o marcador.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. Empiece a reproducir una grabación de sesión que contenga eventos o marcadores.
4. Vaya a un evento o un marcador:
   - En el área inferior de la ventana del reproductor, haga clic en el punto que representa el evento o el marcador para ir a él.
   - En la lista **Eventos y marcadores**, haga doble clic en el evento o marcador para ir a él. Para ir al siguiente evento o marcador, elija cualquiera de estos de la lista, haga clic con el botón secundario para mostrar el menú y seleccione **Buscar hasta marcador**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para cambiar la visualización de la reproducción

Dec 05, 2017

Las opciones permiten cambiar la forma en que aparecen las sesiones grabadas en la ventana del reproductor. La imagen se puede desplazar y también se le puede cambiar el tamaño, se puede ver la reproducción en pantalla completa, mostrar la ventana del reproductor en una ventana separada y mostrar un borde rojo alrededor de la sesión grabada para diferenciarla del fondo de la ventana del reproductor.

Mostrar la ventana del reproductor en pantalla completa

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Ver** > **Reproductor en pantalla completa**.
4. Para volver al tamaño original, presione ESC o F11.

Mostrar la ventana del reproductor en una ventana separada

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones, elija Ver** > **Reproductor en ventana separada**. Aparecerá una nueva ventana que contiene la ventana del Reproductor. Es posible arrastrar la ventana a una nueva posición y también cambiarle el tamaño.
4. Para incrustar la ventana del reproductor en la ventana principal, elija **Ver** > **Reproductor en ventana separada** o pulse **F10**.

Cambiar el tamaño de la reproducción de la sesión para ajustarla a la ventana del reproductor

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Reproducir** > **Desplazamiento y modificación de la escala** > **Ajustar el tamaño**.
   - **Ajustar el tamaño (Generación rápida)** contrae la imagen con una buena calidad. Las imágenes se generan más rápidamente que cuando se usa lo opción de alta calidad, pero las imágenes y el texto no son tan claros. Use esta opción si está teniendo problemas de rendimiento cuando utiliza el modo de alta calidad.
   - **Ajustar el tamaño (Alta calidad)** contrae la imagen con una buena calidad. El uso de esta opción puede ocasionar que la imagen se genere más lentamente que la opción de generación rápida.

Desplazar la imagen

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Reproducir** > **Desplazamiento y modificación de la escala** > **Desplazamiento**. El puntero cambia a una mano y una pequeña representación de la ventana aparece en la esquina superior derecha de la ventana del reproductor.
4. Distribuya la imagen. La pequeña representación indica dónde se encuentra el usuario en la imagen.
5. Para detener el desplazamiento, elija una de las opciones de modificación de la escala.

Mostrar un borde rojo alrededor de la grabación de la sesión

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra del menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Reproductor**.
4. Marque la casilla **Mostrar el borde alrededor de la grabación de la sesión**.
   Sugerencia : Si no se marca la casilla **Mostrar el borde alrededor de la grabación de la sesión** , se puede ver temporalmente un borde rojo al hacer clic y mantener presionado el botón del puntero mientras este se encuentra en la ventana del Reproductor.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Caché de archivos de sesiones grabadas

Dec 05, 2017

Cada vez que se abre un archivo de grabación de sesión, el Reproductor de grabación de sesiones lo descarga desde la ubicación donde se almacenan las grabaciones. Si se descargan los mismos archivos con frecuencia, se puede ahorrar tiempo almacenando en caché los archivos en la estación de trabajo. Los archivos almacenados en caché en la estación de trabajo se guardan en esta carpeta:

userprofile**AppData\Local\Citrix\SessionRecording\Player\Cache**

Se puede especificar cuánto espacio de disco se va a utilizar en el almacenamiento en caché. Cuando las grabaciones llenan el espacio especificado, se eliminan las grabaciones más antiguas y menos utilizadas para dar espacio a las grabaciones nuevas. Es posible vaciar el caché en cualquier momento para abrir espacio en el disco.

Habilitar caché

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra del menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Caché**.
4. Marque la casilla **Almacenar en caché local los archivos descargados**.
5. Si quiere limitar el espacio que se utilizará para el almacenamiento en caché, marque la casilla **Limitar el espacio de disco a utilizar** y especifique la cantidad de megabytes que se dedicarán a la memoria caché.
6. Haga clic en **Aceptar**.

Vaciar memorias caché

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
3. En la barra del menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Caché**.
4. Marque la casilla **Almacenar en caché local los archivos descargados**.
5. En el Reproductor de grabación de sesiones, elija **Herramientas** > **Opciones** > **Caché**.
6. Haga clic en **Vaciar caché** y, a continuación, en **Aceptar** para confirmar la acción.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Solución de problemas de grabación de sesiones

Dec 05, 2017

Esta información contiene soluciones para algunos de los problemas que puede encontrar durante o después de la instalación de los componentes de Grabación de sesiones:

- Los componentes no se pueden conectar entre sí
- La grabación de sesiones falla
- Problemas con el Reproductor de grabación de sesiones o la Consola de directivas de grabación de sesiones
- Problemas con el protocolo de comunicación

> ## 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. Debe hacer una copia de seguridad del Registro antes de editarlo.

El Agente de grabación de sesiones no se puede conectar

Cuando el Agente de grabación de sesiones no se puede conectar, se registra el mensaje de evento **Exception caught while sending poll messages to Session Recording Broker** seguido del texto de la excepción. El texto de la excepción indicará las razones por las que falló la conexión. Los motivos son:

- **La conexión subyacente se cerró. No se pudo establecer una relación de confianza para el canal seguro de SSL/TLS.** Esta excepción significa que el Servidor de grabación de sesiones está utilizando un certificado que está firmado por una CA en la cual no confía el servidor donde reside el Agente de grabación de sesiones o, para la cual dicho servidor no tiene un certificado. También es posible que el certificado haya caducado o se haya revocado.

  Solución: Verifique que se instaló el certificado de CA correcto en el servidor donde se encuentra el Agente de grabación de sesiones o utilice una CA de confianza.

- **El servidor remoto generó un error: (403) prohibido.** Este es un error estándar de HTTPS que aparece cuando se intenta conectar a través de HTTP (protocolo no seguro). El equipo que aloja el Servidor de grabación de sesiones rechaza la conexión porque solo acepta conexiones seguras.

  Solución: Use las propiedades del Agente de grabación de sesiones para cambiar el protocolo del broker de grabación de sesiones a **HTTPS**.

El broker de grabación de sesiones devolvió un error desconocido mientras evaluaba una consulta de directivas de grabación. Código de error 5 (Acceso denegado).Consulte el registro de eventos en el Servidor de grabación de sesiones para obtener más detalles. Este error sucede cuando las sesiones se inician y se hace una solicitud de evaluación de la directiva de grabación. El error se da cuando el grupo de Usuarios autenticados (este es el miembro predeterminado) se elimina del rol de consulta de directivas (PolicyQuery) de la Consola de autorización de grabación de sesiones.

Solución: Agregue el grupo Usuarios autenticados de nuevo a este rol, o agregue cada uno de los servidores que alojan el Agente de grabación de sesiones al rol PolicyQuery.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

La conexión subyacente se cerró. Una conexión que se esperaba mantuviera activa el servidor se cerró. Este error significa que el Servidor de grabación de sesiones está desconectado o no puede aceptar solicitudes. Esto puede suceder porque IIS está desconectado o se reinició, o bien, porque el servidor está desconectado.

Solución: Verifique que el servidor de grabación de sesiones se inició, que IIS se está ejecutando en el servidor y que el servidor está conectado a la red.

Error en la instalación de componentes del servidor de grabación de sesiones

La instalación de los componentes del servidor de grabación de sesiones produce un error con los códigos de error 2502 y 2503.
Solución:
Consulte la lista de control de acceso (ACL) de la carpeta C:\windows\Temp para comprobar que los usuarios y los grupos locales tienen permiso de escritura en esta carpeta. Si no, agregue manualmente el permiso de escritura.

El Servidor de grabación de sesiones no se puede conectar a la Base de datos de grabación de sesiones

Cuando el Servidor de grabación de sesiones no se puede conectar a la Base de datos de grabación de sesiones, es posible que vea un mensaje similar a uno de los siguientes:

Origen del evento:

Se produjo un error específico de la instancia o relacionado con la red al establecer una conexión con SQL Server. Este error aparece en el registro de eventos de aplicación con el ID 2047 en el Visor de eventos del equipo que aloja el Servidor de grabación de sesiones.

Administrador de almacenamiento de grabación de sesiones de Citrix. Descripción: Se encontró una excepción al establecer una conexión a la base de datos. Este error aparece en el registro de eventos de aplicación en el Visor de eventos del equipo donde se encuentra el Servidor de grabación de sesiones.

No se puede conectar con el Servidor de grabación de sesiones. Asegúrese de que el Servidor de grabación de sesiones se está ejecutando. Este mensaje de error aparece cuando se inicia la Consola de directivas de grabación de sesiones.

Solución:

- La edición Express de Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, Microsoft SQL Server 2014 o Microsoft SQL Server 2016 se instala en un servidor independiente y no tiene los servicios o los parámetros correctos configurados para la Grabación de sesiones. El servidor tiene que tener el protocolo TCP/IP habilitado y debe ejecutarse el explorador del servidor SQL. Consulte la documentación de Microsoft para obtener información sobre cómo habilitar estos parámetros.
- Durante la instalación de los componentes de grabación de sesiones (la parte administrativa), se especificó información incorrecta para el servidor y la base de datos. Desinstale la Base de datos de grabación de sesiones y vuelva a instalarla, proporcionando la información correcta.
- El servidor de la Base de datos de grabación de sesiones no está en funcionamiento. Verifique el servidor se puede conectar.
- El equipo que aloja el Servidor de grabación de sesiones o el equipo que aloja el servidor de la Base de datos de grabación de sesiones no puede resolver el nombre FQDN o NetBIOS del otro. Use el comando Ping para verificar que los nombres se pueden resolver.
- Revise la configuración del firewall de la Base de datos de grabación de sesiones y verifique que se permiten las conexiones del servidor SQL Server. Para obtener más información, consulte el artículo de Microsoft en

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

https://msdn.microsoft.com/en-us/library/ cc646023.aspx.

Logon failed for user 'NT_AUTHORITY\ANONYMOUS LOGON'. Este mensaje de error significa que los servicios se iniciaron incorrectamente con .\administrator.

Solución: Reinicie los servicios como usuario de sistema local y reinicie los servicios SQL.

Las sesiones no se graban

Si las sesiones de aplicación no se están grabando, empiece por consultar el registro de eventos de aplicación en el Visor de eventos en la máquina con SO de servidor donde se ejecuta el Agente de grabación de sesiones y el servidor de grabación de sesiones. Puede obtener de ello una valiosa información de diagnóstico.

Si las sesiones no se graban, estos problemas pueden deberse a:

- **Conectividad y certificados de los componentes**. Si los componentes de grabación de sesiones no se pueden comunicar entre sí, la grabación de sesiones puede fallar. Para solucionar los problemas de grabación, verifique que todos los componentes se configuren correctamente y que todos los certificados son válidos y están instalados correctamente.
- **Entornos de dominios que no son de Active Directory**. La funcionalidad de grabación de sesiones está diseñada para ejecutarse en entornos de dominio de Microsoft Active Directory. Si no se está ejecutando en un entorno Active Directory, se podrían experimentar problemas con la grabación. Asegúrese de que todos los componentes de grabación de sesiones se están ejecutando en equipos que son miembros de un dominio de Active Directory.
- **El uso compartido de sesiones entra en conflicto con la directiva activa.** La funcionalidad de grabación de sesiones asigna la directiva activa a la primera aplicación publicada que abra el usuario. Las aplicaciones que se abran posteriormente durante la misma sesión seguirán la directiva que se utilizó para la primera aplicación. Para evitar conflictos de uso compartido de sesiones con la directiva activa, publique las aplicaciones en conflicto en diferentes agentes VDA con SO de servidor.
- **Grabación no activada.** De forma predeterminada, la instalación del Agente de grabación de sesiones en un VDA con SO de servidor habilita el servidor para la grabación. No se podrá grabar hasta que se configure una directiva de grabación que lo permita.
- **La directiva de grabación activa no permite la grabación.** Para que una sesión se grabe, la directiva de grabación activa debe permitir que las sesiones para el usuario, el servidor o la aplicación publicada se puedan grabar.
- **Los servicios de grabación de sesiones no se están ejecutando.** Para poder grabar sesiones, el servicio del Agente de grabación de sesiones debe estar ejecutándose en el VDA con SO de servidor y el servicio del Administrador de almacenamiento de grabación de sesiones debe estar ejecutándose en el equipo donde se encuentra el Servidor de grabación de sesiones.
- **MSMQ no está configurado.** Si MSMQ no está correctamente configurado en el servidor que ejecuta el Agente de grabación de sesiones y en el equipo que aloja el Servidor de grabación de sesiones, puede haber problemas al grabar.

No se puede ver la reproducción de sesiones en directo

Si utiliza el Reproductor de grabación de sesiones para ver grabaciones y tiene dificultades, puede aparecer el siguiente mensaje de error:

La descarga del archivo de la grabación de la sesión falló. No se permite la reproducción en directo de sesiones. El servidor se configuró para que no permita esta función. Este mensaje de error indica que el servidor está configurado para que no permita la acción.

Solución: En el cuadro de diálogo **Propiedades del servidor de grabación de sesiones**, elija la ficha **Reproducir** y marque

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

la casilla **Permitir la reproducción en directo de sesiones**.

Las grabaciones están dañadas o incompletas

- Si las grabaciones se dañan o no están completas al visualizarlas en el Reproductor de grabación de sesiones, es posible que también vea advertencias en los registros de eventos del Agente de grabación de sesiones.

  Origen del evento: Administrador de almacenamiento de grabación de sesiones de Citrix

  Descripción: Datos perdidos durante la grabación del archivo

  Suele ocurrir cuando se utilizan Machine Creation Services (MCS) o Provisioning Services (PVS) para crear agentes VDA a partir de una imagen maestra configurada y Microsoft Message Queuing (MSMQ) instalado. En esta situación, los agentes VDA tienen el mismo identificador QMId para MSMQ.

  Como solución temporal, cree un QMId único para cada VDA. Para obtener más información, consulte aquí la sección Instalación, actualización y desinstalación de Grabación de sesiones.

- Es posible que el Reproductor de grabación de sesiones informe de un error interno con este mensaje: "**El archivo que se está reproduciendo informó de un error interno de sistema (código de error: 9) durante la grabación original. El archivo se puede reproducir hasta el punto donde sucedió el error de grabación**" cuando se reproduzca un archivo de grabación concreto.

  Suele deberse a un tamaño de búfer insuficiente para el Agente de grabación de sesiones al grabar sesiones con uso intensivo de gráficos.

  Como solución temporal, cambie el valor de Registro HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\SmAudBufferSizeMB a un valor más alto en el Agente de grabación de sesiones y, a continuación, reinicie la máquina.

Ha fallado la prueba de la conexión desde la instancia de la base de datos al instalar la Base de datos de grabación de sesiones o el Servidor de grabación de sesiones

Cuando se instalan la Base de datos de grabación de sesiones o el Servidor de grabación de sesiones, la conexión de prueba falla y aparece el mensaje de error **Database connection test failed (Ha fallado la prueba de conexión a la base de datos). Corrija el nombre de la instancia de la base de datos** aunque el nombre de esa instancia sea correcto.

En este caso, compruebe que el usuario actual tiene el permiso de rol de SQL Server público para corregir fallos debidos a limitaciones de permisos.

Registros de administrador

En Windows Server 2008 R2 SP1, antes de instalar la funcionalidad Registro de administrador, debe instalar **Características de .NET Framework 3.5** > **Activación WCF** > **Activación HTTP** y, a continuación, instalar .NET Framework 4.5 o una versión posterior. No instale estos dos requisitos en orden inverso. Si lo hace, es posible que la funcionalidad Registro de administrador no funcione de la forma esperada. Es posible que sus operaciones se vean bloqueadas cuando intente cambiar la configuración de Grabación de sesiones desde la consola de propiedades del servidor o cuando intente actualizar las directivas de Grabación de sesiones desde la consola de directivas con el registro obligatorio habilitado.

Para solucionar este problema:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Abra el Administrador de Internet Information Services (IIS) y vaya al nodo **Grupos de aplicaciones**.
2. Haga clic con el botón secundario en **SessionRecordingLoggingAppPool** y abra el cuadro de diálogo **Configuración básica**.
3. Cambie la versión de .NET Framework a 4.0.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Verificación de las conexiones de componentes

Dec 05, 2017

Durante la instalación de la funcionalidad Grabación de sesiones, algunos componentes pueden no conectar con otros. Todos los componentes se comunican con el Servidor de grabación de sesiones (broker). De forma predeterminada, el broker (un componente IIS) está protegido usando el certificado predeterminado del sitio Web de IIS. Si un componente no puede conectarse al Servidor de grabación de sesiones, es posible que los demás componentes tampoco puedan hacerlo.

El Agente de grabación de sesiones y el servidor de grabación de sesiones (Administrador de almacenamiento y Broker) registran los errores de conexión en el registro de eventos de aplicación en el Visor de eventos del equipo que aloja el servidor de grabación de sesiones, mientras que la Consola de directivas de grabación de sesiones y el reproductor de grabación de sesiones muestran mensajes de error en pantalla cuando no pueden realizar la conexión.

Verificar si el Agente de grabación de sesiones está conectado

1. Inicie una sesión en el servidor donde está instalado el Agente de grabación de sesiones.
2. En el menú **Inicio**, elija **Propiedades del Agente de grabación de sesiones**.
3. En las **Propiedades del Servidor de grabación de sesiones**, haga clic en **Conexión**.
4. Compruebe que el valor de Servidor de grabación de sesiones es el nombre de servidor correcto del equipo donde se encuentra el Servidor de grabación de sesiones.
5. Compruebe que la máquina de SO de servidor puede contactar con el servidor especificado como valor de Servidor de grabación de sesiones.

Nota: Consulte el registro de eventos de aplicación para ver errores y advertencias.

Cómo verificar si el Servidor de grabación de sesiones está conectado

Precaución: El uso del Editor del Registro del sistema 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.

1. Inicie sesión en el equipo donde se encuentra el Servidor de grabación de sesiones.
2. Abra el Editor del Registro.
3. Vaya a HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Compruebe si el valor de **SmAudDatabaseInstance** hace referencia correctamente a la Base de datos de grabación de sesiones que se instaló en la instancia del servidor SQL Server.

Cómo verificar si la Base de datos de grabación de sesiones está conectada

1. Con una herramienta administrativa de SQL, abra la instancia de SQL que contiene la base de datos de grabación de sesiones instalada.
2. Abra los permisos de seguridad de la Base de datos de grabación de sesiones.
3. Verifique que la cuenta de equipo de grabación de sesiones tiene acceso a la base de datos. Por ejemplo, si el equipo donde se encuentra el Servidor de grabación de sesiones se llama **SsRecSrv** en el dominio MIS, la cuenta del equipo en la base de datos debe configurarse como **MIS\SsRecSrv$**. Este valor se configura durante la instalación de la Base de datos de grabación de sesiones.

Prueba de conectividad de IIS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Probar las conexiones con el sitio IIS del Servidor de grabación de sesiones desde un explorador Web para acceder a la página Web del Broker de grabación de sesiones puede ayudarle a determinar si los problemas relacionados con la comunicación entre los componentes de Grabación de sesiones provienen de una configuración incorrecta de los protocolos, de problemas de certificado o de problemas para iniciar el Broker de grabación de sesiones.

Para verificar la conectividad a IIS del Agente de grabación de sesiones:

1. Inicie una sesión en el servidor donde está instalado el Agente de grabación de sesiones.
2. Inicie un explorador Web y escriba la siguiente dirección:
   - Para HTTPS: **https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**, donde *servername* es el nombre del equipo donde se encuentra el Servidor de grabación de sesiones
   - Para HTTP: **http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl**, donde *servername* es el nombre del equipo donde se encuentra el Servidor de grabación de sesiones
3. Si se le solicita una autenticación de NTLM (NT LAN Manager), inicie la sesión con una cuenta de administrador del dominio.

Para verificar la conectividad a IIS del Reproductor de grabación de sesiones:

1. Inicie sesión en la estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
2. Inicie un explorador Web y escriba la siguiente dirección:
   - Para HTTPS: **https://servername/SessionRecordingBroker/Player.rem?wsdl**, donde *servername* es el nombre del equipo donde se encuentra el Servidor de grabación de sesiones
   - Para HTTP: **http://servername/SessionRecordingBroker/Player.rem?wsdl**, donde *servername* es el nombre del equipo donde se encuentra el Servidor de grabación de sesiones
3. Si se le solicita una autenticación de NTLM (NT LAN Manager), inicie la sesión con una cuenta de administrador del dominio.

Para verificar la conectividad a IIS de la Consola de directivas de grabación de sesiones:

1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
2. Inicie un explorador Web y escriba la siguiente dirección:
   - Para HTTPS: **https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**, donde *servername* es el nombre del equipo donde se encuentra el Servidor de grabación de sesiones
   - Para HTTP: **http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl**, donde *servername* es el nombre del equipo donde se encuentra el Servidor de grabación de sesiones
3. Si se le solicita una autenticación de NTLM (NT LAN Manager), inicie la sesión con una cuenta de administrador del dominio.

Si ve un documento XML en el explorador, esto verifica que el equipo donde se ejecuta la Consola de directivas de grabación de sesiones está conectado al equipo que aloja el Servidor de grabación de sesiones mediante el protocolo configurado.

Solución de problemas de certificados

Si está utilizando HTTPS como protocolo de comunicación, el equipo donde se encuentra el Servidor de grabación de sesiones debe estar configurado con un certificado de servidor. Todas las conexiones de los componentes con el Servidor de grabación de sesiones deben tener la autoridad de una entidad de certificación (CA). De otro modo, los intentos de conexión entre los componentes fallan.

Los certificados se pueden probar accediendo a la página Web del Broker de grabación de sesiones, de la misma manera que

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

cuando se prueba la conectividad de IIS. Si puede acceder a la página XML de cada componente, los certificados están configurados correctamente.

Algunos problemas comunes que hace que los certificados provoquen fallos de conexión son:

- **Certificados no válidos o falta de certificados.** Si el servidor que ejecuta el Agente de grabación de sesiones no tiene un certificado raíz para confiar en el certificado de servidor, no podrá confiar y conectarse al Servidor de grabación de sesiones vía HTTPS, y la conectividad fallará. Verifique que el certificado de servidor del Servidor de grabación de sesiones es de confianza para todos los componentes.
- **Nomenclatura inconsistente.** Si el certificado de servidor asignado al equipo donde se encuentra el Servidor de grabación de sesiones se crea con un nombre completo de dominio (FQDN), todos los componentes deben utilizar el FQDN para conectarse al Servidor de grabación de sesiones. Si se utiliza un nombre NetBIOS, todos los componentes deben configurarse con un nombre NetBIOS para el Servidor de grabación de sesiones.
- **Certificados caducados.** Si un certificado de servidor caduca, la conectividad con el Servidor de grabación de sesiones vía HTTPS fallará. Verifique que el certificado de servidor asignado al equipo donde se encuentra el Servidor de grabación de sesiones es válido y no haya caducado. Si se utiliza el mismo certificado para la firma digital de grabaciones de sesión, el registro de eventos del equipo donde se encuentra el Servidor de grabación de sesiones dará mensajes de error indicando que el certificado caducó o mensajes de advertencia indicando que está a punto de caducar.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Búsqueda de grabaciones si el Reproductor de grabación de sesiones falla

Dec 05, 2017

Si tiene problemas para buscar grabaciones con el Reproductor de grabación de sesiones, aparecerán los siguientes mensajes en la pantalla:

- **La búsqueda de archivos de grabación de sesiones falló. No se pudo resolver el nombre del servidor remoto: servername.**, donde servername es el nombre del servidor al que el Reproductor de grabación de sesiones está intentando conectarse. El Reproductor de grabación de sesiones no puede establecer contacto con el Servidor de grabación de sesiones. Hay dos razones por las cuales puede suceder esto, el nombre del servidor se escribió incorrectamente o el DNS no puede resolver el nombre del servidor.
  Solución: En la barra de menú del Reproductor, seleccione **Herramientas** > **Opciones** > **Conexiones** y compruebe que el nombre del servidor en la lista **Servidores de grabación de sesiones** sea correcto. Si es correcto, desde la línea de comandos ejecute el comando ping para ver si es posible resolver el nombre. Cuando el Servidor de grabación de sesiones está apagado o desconectado, la búsqueda de archivos de grabaciones falla y mensaje de error es **No se puede establecer contacto con el servidor remoto**.

- **No se puede establecer contacto con el servidor remoto.** Este error se produce cuando el Servidor de grabación de sesiones está apagado o desconectado.
  Solución: Verifique que el Servidor de grabación de sesiones está conectado.

- **Acceso denegado.** Puede darse un error de acceso denegado si al usuario no se le otorga permiso para buscar y descargar archivos de grabación de sesión.
  Solución: Asigne el usuario al rol de Reproductor usando la Consola de autorización de grabación de sesiones.

- **Acceso denegado cuando se asigna el rol de Reproductor.** Este error ocurre normalmente cuando se instala el Reproductor de grabación de sesiones en el mismo equipo que el Servidor de grabación de sesiones y el Control de cuentas de usuario está habilitado. Cuando se asigna el rol de Reproductor al grupo de usuarios de administradores o administradores de dominio, es posible que una cuenta no predefinida de administrador que se incluya en ese grupo falle en la comprobación de basada en roles cuando se buscan archivos de grabaciones en el Reproductor de grabación de sesiones.
  Soluciones:

  + Ejecute el Reproductor de grabación de sesiones como administrador.

  + Asigne el rol de Reproductor a usuarios específicos en lugar de asignarlos al grupo entero.

  + Instale el Reproductor de grabación de sesiones en otra máquina que el Servidor de grabación de sesiones.

- **La búsqueda de archivos de grabación de sesiones falló. La conexión subyacente se cerró. No se pudo establecer una relación de confianza para el canal seguro de SSL/TLS.** Esta excepción se debe a que el Servidor de grabación de sesiones está usando un certificado firmado por una CA que no es de confianza para el dispositivo cliente, o para la cual el dispositivo cliente no tiene ningún certificado.
  Solución: Instale el certificado de CA correcto o de confianza en la estación de trabajo donde se encuentra instalado el Reproductor de grabación de sesiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **El servidor remoto generó un error: (403) prohibido.** Este es un error estándar de HTTPS que sucede cuando se intenta conectar a través de HTTP (protocolo no seguro). El servidor rechaza la conexión porque de forma predeterminada está configurado para aceptar conexiones seguras solamente.
  Solución: En la barra de menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Conexiones**. Seleccione el servidor en la lista **Servidores de grabación de sesiones** y, a continuación, haga clic en **Modificar**. Cambie el protocolo de **HTTP** a **HTTPS**.

Solución de problemas de MSMQ

Si los usuarios pueden ver el mensaje de notificación pero la persona que visualiza la grabación no puede encontrar las grabaciones después de realizar una búsqueda en el Reproductor de grabación de sesiones, es posible que haya un problema con MSMQ. Compruebe que la cola está conectada al Servidor de grabación de sesiones (Administrador de almacenamiento) y utilice un explorador Web para determinar si existen errores de conexión (si está utilizando HTTP o HTTPS como protocolo de comunicación MSMQ).

Para verificar si la cola se conectó:

1. Inicie una sesión en el servidor donde se encuentra el Agente de grabación de sesiones y vea las colas salientes.
2. Compruebe que la cola al equipo donde se encuentra el Servidor de grabación de sesiones muestra un estado conectado.
   - Si el estado es **esperando para conectarse**, hay una serie de mensajes en la cola y el protocolo es HTTP o HTTPS (correspondiente al protocolo seleccionado en la ficha **Conexiones** de **Propiedades del Agente de grabación de sesiones**), lleve a cabo el paso 3.
   - Si el estado es **conectado** y no hay mensajes en la cola, es posible que exista un problema con el servidor donde se encuentra el Servidor de grabación de sesiones. Omita el paso 3 y realice el paso 4.
3. Si hay varios mensajes en la cola, inicie un explorador Web y escriba la siguiente dirección:
   - Para HTTPS: **https://servername/msmq/private$/CitrixSmAudData**, donde *servername* es el nombre del equipo que aloja el Servidor de grabación de sesiones
   - Para HTTP: **http://servername/msmq/private$/CitrixSmAudData**, donde *servername* es el nombre del equipo que aloja el Servidor de grabación de sesiones

   Si la página genera un error del tipo **El servidor solamente acepta conexiones seguras**, cambie el protocolo MSQM en **Propiedades del Agente de grabación de sesiones** a HTTPS. Si la página indica un problema con el certificado de seguridad del sitio Web, puede existir un problema con la relación de confianza con el canal seguro de TLS. En ese caso, instale un certificado de CA correcto o utilice una CA que sea de confianza.
4. Si no hay mensajes en la cola, inicie una sesión en el equipo donde se encuentra el Servidor de grabación de sesiones y vea las colas privadas. Seleccione **citrixsmauddata**. Si hay varios mensajes en la cola (columna Número de mensajes), compruebe que el servicio del Administrador de almacenamiento (Storage Manager) de grabación de sesiones se inició. Si no, reinicie el servicio.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cambio del protocolo de comunicación

Dec 05, 2017

Por razones de seguridad, Citrix no recomienda el uso de HTTP como protocolo de comunicación. La instalación de la grabación de sesiones está configurada para que use HTTPS. Para utilizar HTTP en lugar de HTTPS, debe cambiar varios parámetros.

Usar HTTP como el protocolo de comunicación

1. Inicie sesión en el equipo donde se encuentra el servidor de grabación de sesiones e inhabilite las conexiones seguras del broker de grabación de sesiones en IIS.
2. Cambie el parámetro del protocolo de HTTPS a HTTP en **Propiedades del agente de grabación de sesiones** en cada servidor donde esté instalado el Agente de grabación de sesiones:
    1. Inicie una sesión cada servidor donde esté instalado el Agente de grabación de sesiones.
    2. En el menú **Inicio**, elija **Propiedades del agente de grabación de sesiones**.
    3. En **Propiedades del agente de grabación de sesiones**, seleccione la ficha **Conexiones**.
    4. En el área **Broker de grabación de sesiones**, seleccione **HTTP** en la lista desplegable **Protocolo** y luego haga clic en **Aceptar** para realizar el cambio. Si se le solicita reiniciar el servicio, seleccione **Sí**.
3. Cambie el parámetro del protocolo de HTTPS a HTTP en los parámetros del Reproductor de grabación de sesiones:
    1. Inicie sesión en cada estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
    2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
    3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Conexiones**, seleccione el servidor y luego elija **Modificar**.
    4. Seleccione **HTTP** de la lista desplegable **Protocolo** y haga doble clic en Aceptar para aceptar el cambio y cerrar el cuadro de diálogo.
4. Cambie el parámetro del protocolo de HTTPS a HTTP en la Consola de directivas de grabación de sesiones:
    1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
    2. En el menú **Inicio**, elija **Consola de directivas de grabación de sesiones**.
    3. Elija **HTTP** de la lista desplegable **Protocolo** y seleccione Aceptar para conectarse. Si se establece la conexión, este parámetro se recordará la próxima vez que se inicie la Consola de directivas de grabación de sesiones.

Regresar a HTTPS como el protocolo de comunicación

1. Inicie sesión en el equipo donde se encuentra el servidor de grabación de sesiones y habilite las conexiones seguras para el broker de grabación de sesiones en IIS.
2. Cambie el parámetro del protocolo de HTTP a HTTPS en **Propiedades del agente de grabación de sesiones en cada servidor donde esté instalado el Agente de grabación de sesiones:**
    1. Inicie una sesión cada servidor donde esté instalado el Agente de grabación de sesiones.
    2. En el menú **Inicio**, elija **Propiedades del agente de grabación de sesiones**.
    3. En **Propiedades del agente de grabación de sesiones**, seleccione la ficha **Conexiones**.
    4. En el área **Broker de grabación de sesiones**, seleccione **HTTPS** en la lista desplegable **Protocolo** y luego haga clic en **Aceptar** para realizar el cambio. Si se le solicita reiniciar el servicio, seleccione **Sí**.
3. Cambie el parámetro del protocolo de HTTP a HTTPS en los parámetros del Reproductor de grabación de sesiones:
    1. Inicie sesión en cada estación de trabajo donde está instalado el Reproductor de grabación de sesiones.
    2. En el menú **Inicio**, elija **Reproductor de grabación de sesiones**.
    3. En la barra de menú del **Reproductor de grabación de sesiones**, elija **Herramientas** > **Opciones** > **Conexiones**, seleccione el servidor y luego elija **Modificar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Seleccione **HTTPS** de la lista desplegable **Protocolo** y haga doble clic en **Aceptar** para aceptar el cambio y cerrar el cuadro de diálogo.

4. Cambie el parámetro del protocolo de HTTP a HTTPS en la Consola de directivas de grabación de sesiones:
    1. Inicie una sesión en el servidor donde está instalada la Consola de directivas de grabación de sesiones.
    2. En el menú **Inicio**, elija **Consola de directivas de grabación de sesiones**.
    3. Elija **HTTPS** de la lista desplegable **Protocolo** y seleccione **Aceptar** para conectarse. Si se establece la conexión, este parámetro se recordará la próxima vez que se inicie la Consola de directivas de grabación de sesiones.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Referencia: Administración de los registros de la base de datos

Dec 05, 2017

La utilidad Registro de la base de datos ICA (ICLDB) es una utilidad de línea de comandos que se usa para manipular los registros de la base de datos de las grabaciones de sesión. Esta utilidad se instala durante la instalación de la función Grabación de sesiones en el directorio drive:\Archivos de programa\Citrix\SessionRecording\Server\Bin, en el servidor donde se encuentra el Servidor de grabación de sesiones.

Cuadro de referencia rápida

La siguiente tabla enumera los comandos y opciones disponibles en la utilidad ICLDB. Escriba los comandos con el siguiente formato:

icldb [version | locate | dormant | import | archive | remove | removeall] opciones de comando [/l] [/f] [/s] [/?]

Nota: Se ofrecen instrucciones más completas en la ayuda asociada a la utilidad. Para acceder a la ayuda, desde una línea de comandos, escriba drive:**\Archivos de programa\Citrix\SessionRecording\Server\Bin**, **icldb /?**. Para acceder a la ayuda de comandos específicos, escriba **icldb *command* /?**.

Comando	Descripción
archive	Archiva los archivos de grabaciones de sesiones más antiguos que el período de retención especificado. Use este comando para archivar los archivos.
dormant	Muestra o cuenta los archivos de grabaciones de sesiones que se consideran inactivas. Los archivos inactivos son las grabaciones de sesiones que no se completaron debido a la pérdida de datos. Use este comando para comprobar si sospecha que está perdiendo datos. Puede comprobar si los archivos de grabación de sesiones se están convirtiendo en inactivos para toda la base de datos o solamente para grabaciones realizada dentro de un número de días, horas o minutos específicos.
import	Importa archivos de grabación de sesiones en la base de datos de grabación de sesiones. Use este comando para reconstruir la base de datos si pierde registros de ésta. Además, use este comando para combinar bases de datos (si tiene dos bases de datos puede importar los archivos de una de ellas).
locate	Busca y muestra la ruta completa a un archivo de grabación de sesión con el ID del archivo como criterio. Use este comando cuando está buscando la ubicación del almacenamiento del archivo de grabación de sesión. Es también una forma de comprobar si la base de datos está al día con un archivo específico.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Comando	Descripción
quitaria.	Elimina las referencias a los archivos de grabaciones de sesiones de la base de datos. Use este comando (con cuidado) para limpiar la base de datos. Especifique el período de retención que se usará como criterio. Puede también eliminar el archivo asociado.
removeall	Elimina todas las referencias a los archivos de grabación de sesiones de la base de datos y la devuelve a su estado original. Los archivos no se eliminan, pero ya no es posible buscarlos en el reproductor de grabación de sesiones. Use este comando (con cuidado) para limpiar la base de datos. Las referencias eliminadas solo pueden revertirse con la restauración del respaldo.
versión	Muestra la versión de esquema de la base de datos de grabación de sesiones.
/l	Registra resultados y errores en el registro de eventos de Windows.
/f	Hace que el comando se ejecute sin hacer solicitudes.
/s	Elimina el mensaje de copyright.
/?	Muestra una ayuda para los comandos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Registros de configuración

Dec 05, 2017

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 de un sitio; si un Controller falla, el servicio instalado en otro Controller pasa automáticamente a gestionar las solicitudes de captura de registros.

De forma predeterminada, la función Registros de configuración está habilitada y usa la base de datos que se crea en el momento de crear un sitio (la base de datos de configuración del sitio). Puede especificar otra ubicación para la base de datos. La base de datos de registros de configuración (Configuration Logging) respalda 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 leerá 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:

- Administración de 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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).

Administración de 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.

Nota: 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, los registros de configuración (Configuration Logging) están habilitados, 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 la captura de registros de configuración, seleccione el botón de opción **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 la captura de registros de configuración, seleccione el botón de opción **Inhabilitar**. Si la captura de registros estuvo habilitada previamente, los registros existentes se conservan y se pueden seguir consultando con el SDK de PowerShell.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para habilitar la captura obligatoria de registros, seleccione el botón de opción **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 el botón de opción **Habilitar** está seleccionado. Si el servicio de registros de configuración (Configuration Logging Service) falla y no se usa la alta disponibilidad, se asume que se aplica el registro obligatorio. En tales casos, las operaciones que normalmente se registrarían no se llevan a cabo.

Para inhabilitar la captura obligatoria de registros, seleccione el botón de opción **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

Nota: 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. Los formatos válidos se ofrecen en el artículo Bases de datos.
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 obtener acceso a la base de datos usando las credenciales del usuario actual de Studio; si falla, el sistema pedirá credenciales de usuario para 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.

Cómo 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

llamada a uno o varios servicios y SDK, que son operaciones de bajo nivel. Cuando se selecciona una operación de alto nivel en el panel central superior, el panel inferior central 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, la pantalla en el panel central muestra el contenido de las entradas de los registros por orden cronológico (primero las entradas más recientes), separadas por su fecha.

Para filtrar por	Realice esta acción
Resultados de búsqueda	Escriba texto en el cuadro Buscar en la parte superior del panel central. La presentación filtrada incluye la cantidad de resultados de la búsqueda. Para volver a la versión estándar de la presentación de los registros, borre el texto del cuadro Buscar.
Título de columna	Haga clic en el título de una columna para ordenar la presentación por ese campo.
Un intervalo de fechas	Seleccione un intervalo en la lista desplegable situada junto al cuadro Buscar en la parte superior del panel central.

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) solo 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.

© 1999-2017 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.

Cómo 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 integrado de 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 hacer esto:
  - 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.
    3. En Pertenencia al rol de la base de datos, especifique al menos uno de los miembros de rol para el usuario de la base de datos: ConfigurationLoggingSchema_ROLE o dbowner.

    Para obtener información adicional, consulte la documentación sobre SQL Server Management Studio.

Para eliminar los registros de configuración:

1. Seleccione **Registros** en el panel de navegación de Studio.
2. Seleccione **Eliminar registros** en el panel Acciones.
3. Verá la opción para crear una copia de respaldo de los registros antes de eliminarlos. Si decide crear una copia de respaldo, vaya a la ubicación donde se debe guardar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Registros de eventos

Dec 05, 2017

Los siguientes enlaces contienen listas y descripciones de los eventos que registran los servicios de XenApp y XenDesktop.

Esta información es general; debe consultar los artículos de las características concretas para obtener más información sobre los eventos.

HTML Eventos de Citrix Broker Service

HTML Eventos del SDK del servicio Citrix FMA

HTML Eventos del servicio de configuración de Citrix

HTML Eventos del servicio de administración delegada de Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Director

Dec 05, 2017

En este artículo:

Acerca de Director

Implementar y configurar Director

Instalar Director

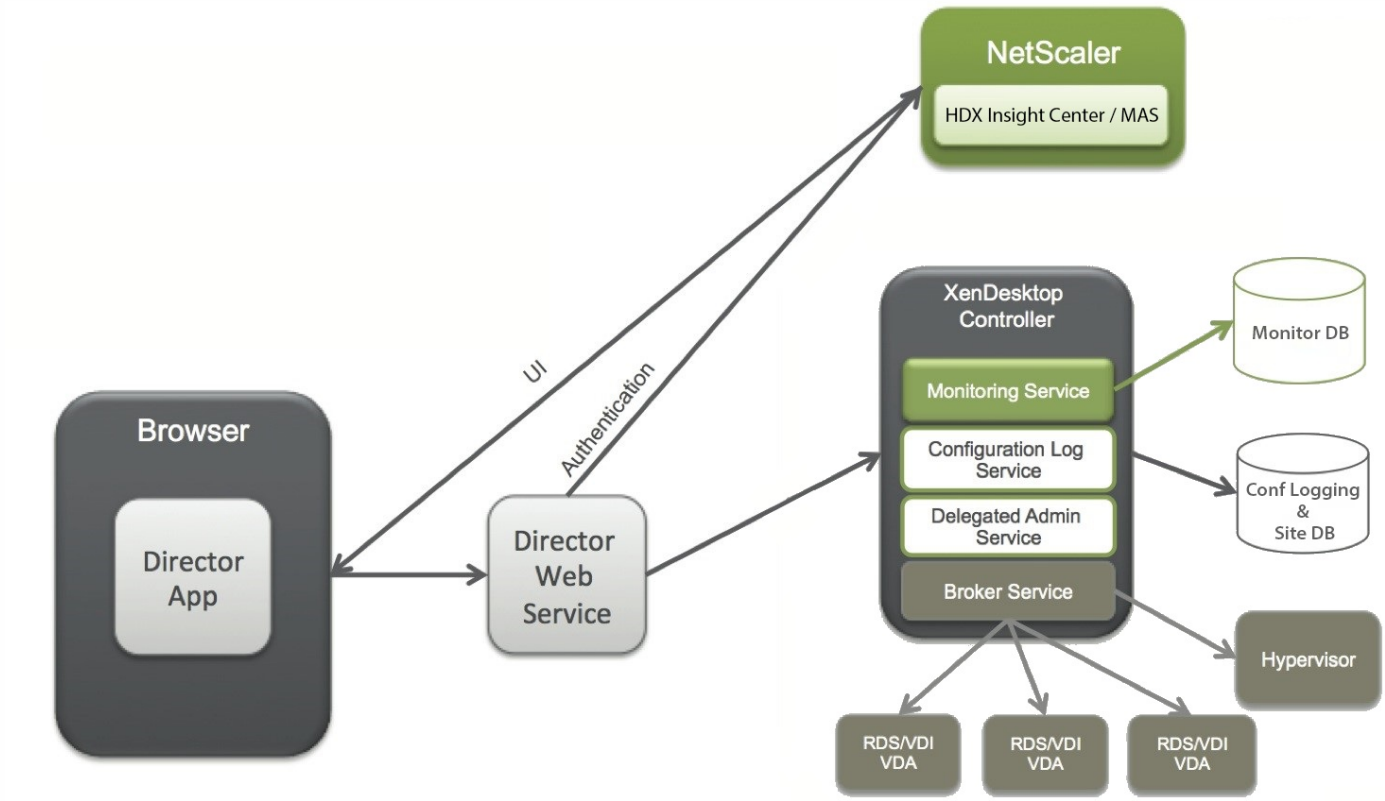
Instalar Director para XenApp 6.5

Iniciar sesión en Director

Usar Director con la autenticación integrada de Windows

Acerca de Director

Director es una consola de supervisión y solución de problemas para XenApp y XenDesktop.



Director pueden 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

implementación y el análisis de red y tendencias históricas, con tecnología de NetScaler Insight Center o NetScaler MAS, con el fin de identificar posibles cuellos de botella debido a problemas de red en el entorno de XenApp o XenDesktop.

- 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 Insight Center o NetScaler MAS.
  - Consiga visibilidad de la experiencia del usuario final para aplicaciones y escritorios virtuales y usuarios de XenApp o XenDesktop.
  - Correlacione datos de red con los datos de aplicaciones y mediciones en tiempo real para una solución de problemas más eficaz.
  - Integración con la herramienta de supervisión de Director de XenDesktop 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 XenApp o XenDesktop. Esta característica permite ver los fallos en tiempo real, lo que proporciona una mejor idea de la experiencia del usuario final.

Para obtener más información acerca de la compatibilidad de las funciones de Director con Delivery Controller (DC), VDA y cualquier otro componente dependiente, consulte Matriz de compatibilidad de características.

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, realizar operaciones de remedo en la máquina del usuario, reiniciar la máquina o restablecer el perfil de usuario.

En cambio, los administradores totales pueden ver y administrar todo el sitio, y pueden ejecutar comandos para varios usuarios y máquinas. El panel de mandos ofrece información general de los aspectos clave de la implementación, tales como el estado de las sesiones, los inicios de sesión de los usuarios y la infraestructura del sitio. La información se actualiza cada minuto. En caso de problemas, aparecen automáticamente los detalles sobre la cantidad y el tipo de fallos que se han producido.

Implementar y configurar Director

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.

Esta versión de Director no es compatible ni con las implementaciones de XenApp anteriores a 6.5 ni con las implementaciones de XenDesktop anteriores a la versión 7.

Cuando Director se usa en un entorno que contiene más de un sitio, asegúrese de sincronizar los relojes del sistema en

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

todos los servidores donde estén instalados los Controllers, Director y otros componentes principales. De lo contrario, los sitios podrían no mostrarse correctamente en Director.

Sugerencia: Si va a supervisar sitios de XenApp 6.5 además de sitios de XenApp 7.5 o XenDesktop 7.x, Citrix recomienda instalar Director en un servidor independiente de la consola de Director que se usa para supervisar los sitios de XenApp 6.5.

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.

Para configurar permisos

Para iniciar sesión en Director, los administradores con permisos para Director deben ser usuarios del dominio de Active Directory y deben contar con los siguientes derechos:

- Derechos de lectura en todos los bosques de AD en los que se realizarán búsquedas (consulte Configuración avanzada).
- Roles configurados de administrador delegado (consulte Administración delegada y Director).
- Para remedar usuarios, los administradores deben configurarse mediante una directiva de grupo de Microsoft para la Asistencia remota de Windows. Además:
  - Durante la instalación de VDA, compruebe que la función Asistencia remota de Windows está habilitada en todos los dispositivos de usuario (seleccionada de forma predeterminada).
  - Al instalar Director en un servidor, asegúrese de que la Asistencia remota de Windows está instalada (seleccionada de forma predeterminada). Sin embargo, en el servidor está inhabilitada de forma predeterminada. La función no necesita estar habilitada para que Director proporcione asistencia a los usuarios finales. Citrix recomienda dejar la función inhabilitada para mejorar la seguridad en el servidor.
  - Para permitir que otros usuarios inicien la Asistencia remota de Windows, debe concederles los permisos requeridos desde las configuraciones de directiva de grupo de Microsoft adecuadas para la Asistencia remota. Para obtener más información, consulte CTX127388: How to Enable Remote Assistance for Desktop Director.
- Para los dispositivos de usuario con VDA anteriores a 7, se requiere una configuración adicional. Consulte Configurar permisos para VDA anteriores a XenDesktop 7.

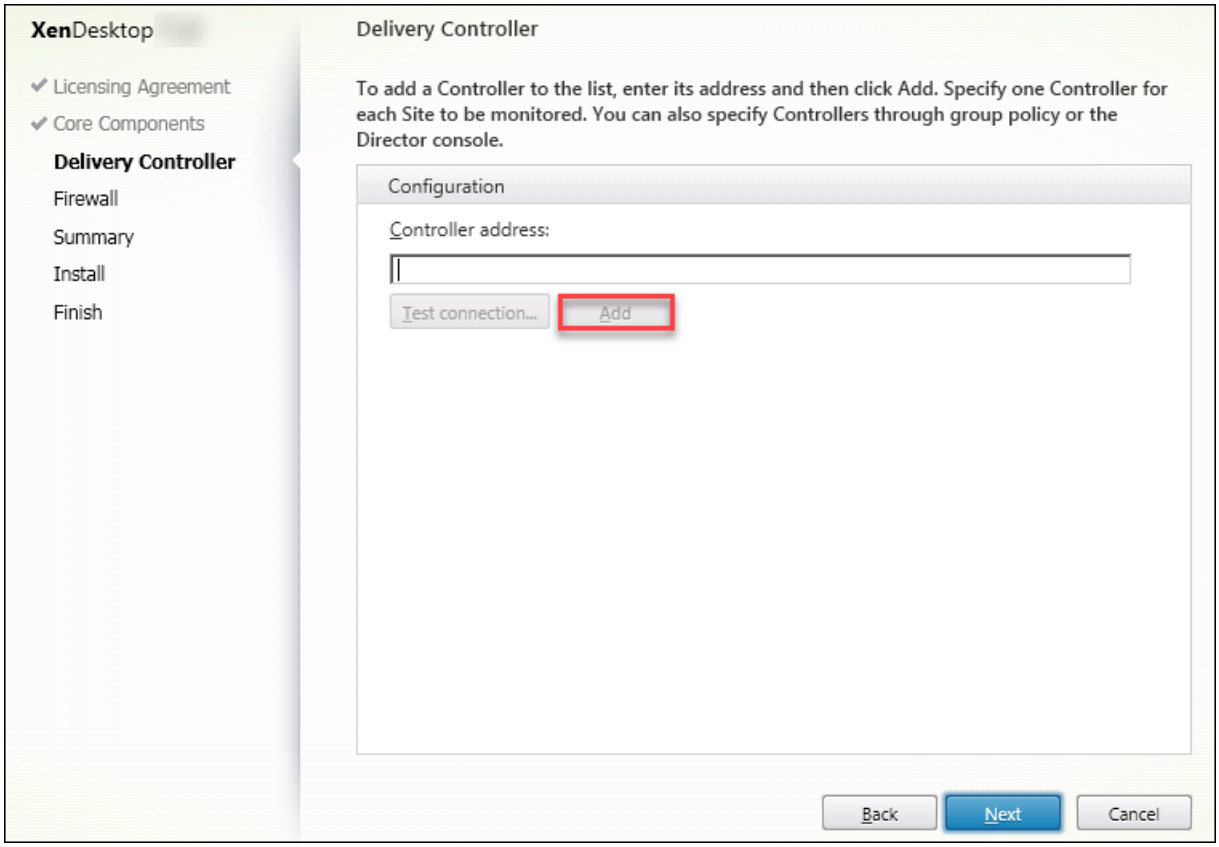
Instalar Director

Instale Director desde la ISO del instalador de producto completo de XenApp y XenDesktop, que verifica los requisitos previos, instala los componentes que falten, configura el sitio Web de Director y realiza la configuración básica. 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.

© 1999-2017 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.

Instalar Director para XenApp 6.5

Para instalar Director para XenApp 6.5, siga estos pasos. Por lo general, Director se instala en un equipo aparte de los Controllers de XenApp.

1. Instale Director desde los medios de instalación de XenApp.Si Director ya está instalado en XenDesktop, omita este paso y vaya al siguiente.
2. Utilice la consola del Administrador de IIS en cada servidor de Director para actualizar la lista de direcciones de servidor XenApp en la configuración de la aplicación, como se describe en **Para agregar sitios en Director** en la sección Configuración avanzada.
   Deberá proporcionar la dirección de servidor de un Controller por cada sitio de XenApp; los demás Controllers del sitio XenApp se usan automáticamente para la conmutación por error. Director no equilibra la carga entre los Controllers.
   Importante: Para las direcciones de XenApp, utilice el parámetro Service.AutoDiscoveryAddressesXA, no el parámetro predeterminado Service.AutoDiscoveryAddresses.
3. El instalador del proveedor WMI de Director se encuentra en la carpeta **Support\DirectorWMIProvider** del DVD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instálelo en todos los servidores XenApp correspondientes (Controllers y servidores de trabajo donde se ejecutan las sesiones).
Si **winrm** no está configurado, utilice el comando **winrm qc**.

4. Configure cada servidor de trabajo de XenApp para que acepte las consultas de WinRM como se describe en Configurar permisos.
5. Configure una excepción de firewall para el puerto 2513, utilizado para la comunicación entre Director y XenApp.
6. 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.

Nota: Para permitir que Director busque todas las máquinas de trabajo XenApp de la comunidad, deberá agregar una zona DNS inversa para las subredes donde los servidores XenApp residen en los servidores DNS que use la comunidad.

Iniciar sesión en Director

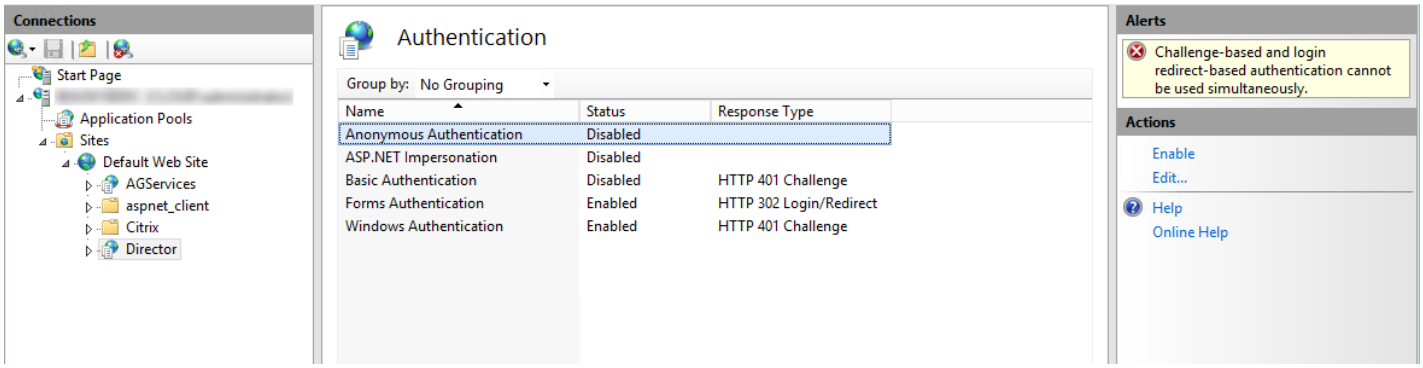
El sitio Web de Director está ubicado en: https o http:///Director.

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 al sitio que está inactivo.

Usar Director con la autenticación integrada de Windows

Con la autenticación integrada de Windows, 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 **Deshabilitar**.
  5. Haga clic con el botón secundario en **Autenticación de Windows** y seleccione **Habilitar**.



- Configure el permiso de delegación de Active Directory para la máquina de Director. Esto solo es necesario si Director y el

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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** y 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 la delegación a 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 con las opciones **Inicio de sesión automático** o **Credenciales de usuario**.

Recopilación de datos de uso con 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 la página Tendencias y sus fichas.La recopilación de datos se habilita de forma predeterminada cuando se instala Director.

Para no participar en la recopilación de datos de Google Analytics, modifique la clave de Registro HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall en la máquina donde está instalado Director como se describe en la sección "Datos de análisis de instalación y actualización" en Citrix Insight Services.

Nota: La clave del Registro HKEY_LOCAL_MACHINE\Software\Citrix\MetaInstall controla la recopilación de datos de uso mediante Citrix Insight servicios y mediante Google Analytics. Cualquier cambio en el valor de la clave afecta a la recopilación por parte de ambos servicios.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración avanzada

Dec 05, 2017

En este artículo:

Configuración recomendada de Director para un entorno multibosque

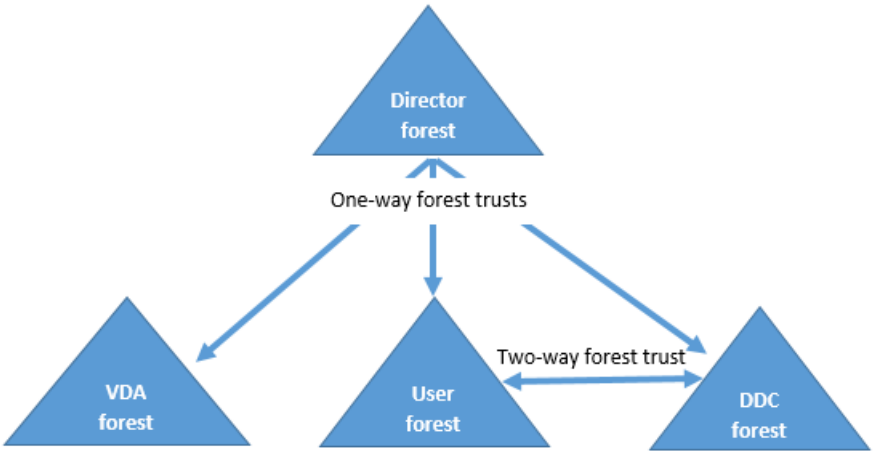
Agregar sitios a Director

Inhabilitación de la visibilidad de las aplicaciones en ejecución en el Administrador de actividades

Director puede respaldar entornos que abarcan varios bosques en que usuarios, Delivery Controllers de dominio (DDC), 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 de Director 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 controladores de dominio ubicados en varios bosques.

La configuración avanzada necesaria para que Director respalde varios bosques se controla mediante los 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 con IIS:

1. Abra la consola del Administrador de Internet Information Services (IIS).
2. Vaya al sitio Web de Director bajo el sitio Web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Haga doble clic en un parámetro para modificarlo.

Las licencias Platinum conservan los datos durante 90 días de manera predeterminada. Para obtener más información sobre las configuraciones, consulte Granularidad y retención de datos.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 el siguiente parámetro:

```
Connector.ActiveDirectory.Domains = (user),(server)
```

Los atributos de valor user y server representan los dominios del usuario de Director (el administrador) y el servidor de Director respectivamente.

Para habilitar búsquedas desde un dominio o bosque adicionales, agregue el nombre del dominio a la lista, tal y como se muestra en el ejemplo:

```
Connector.ActiveDirectory.Domains = (usuario),(servidor),,
```

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.

Nota: En un entorno de varios bosques, Director no muestra los datos de sesión de los usuarios de otros bosques que han sido asignados al grupo de entrega de XenDesktop mediante el grupo local del dominio.

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.

Para los sitios de XenApp 6.5, agregue la dirección de un Controller desde cada comunidad de servidores XenApp al siguiente parámetro:

Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController

donde *FarmAController* y *FarmBController* son direcciones de Controllers de XenApp de dos comunidades diferentes.

Para los sitios de XenApp 6.5, otra manera de agregar un Controller desde una comunidad de XenApp es:

DirectorConfig.exe /xenapp nombreDelController

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Inhabilitación de 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 en ejecución de la sesión de un 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 modifica el Registro de forma incorrecta, pueden ocurrir 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.

1. En el VDA, modifique la clave de Registro ubicada en HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. De forma predeterminada, el valor de la clave es 1. Cambie el valor a 0 para que la información no se recopile desde el VDA y, por tanto, no se muestre en el Administrador de actividades.
2. En el servidor que tiene Director instalado, modifique el parámetro que controla la visibilidad de las aplicaciones en ejecución. De forma predeterminada, el valor es true, lo que permite la visibilidad de las aplicaciones en ejecución en la ficha Aplicaciones. Cambie el valor a false, lo que inhabilita la visibilidad. Esta opción solo afecta al Administrador de actividades de Director, no al VDA.
   Modifique el valor del parámetro siguiente:
   UI.TaskManager.EnableApplications = false

Importante: Para inhabilitar la vista de las aplicaciones en ejecución, Citrix recomienda realizar ambos cambios para asegurarse de que los datos no se muestran en el Administrador de actividades.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Supervisión de implementaciones

Feb 01, 2018

En este artículo:

Supervisar sitios

Supervisar sesiones

Filtrar datos para solucionar fallos

Supervisar tendencias históricas en un sitio

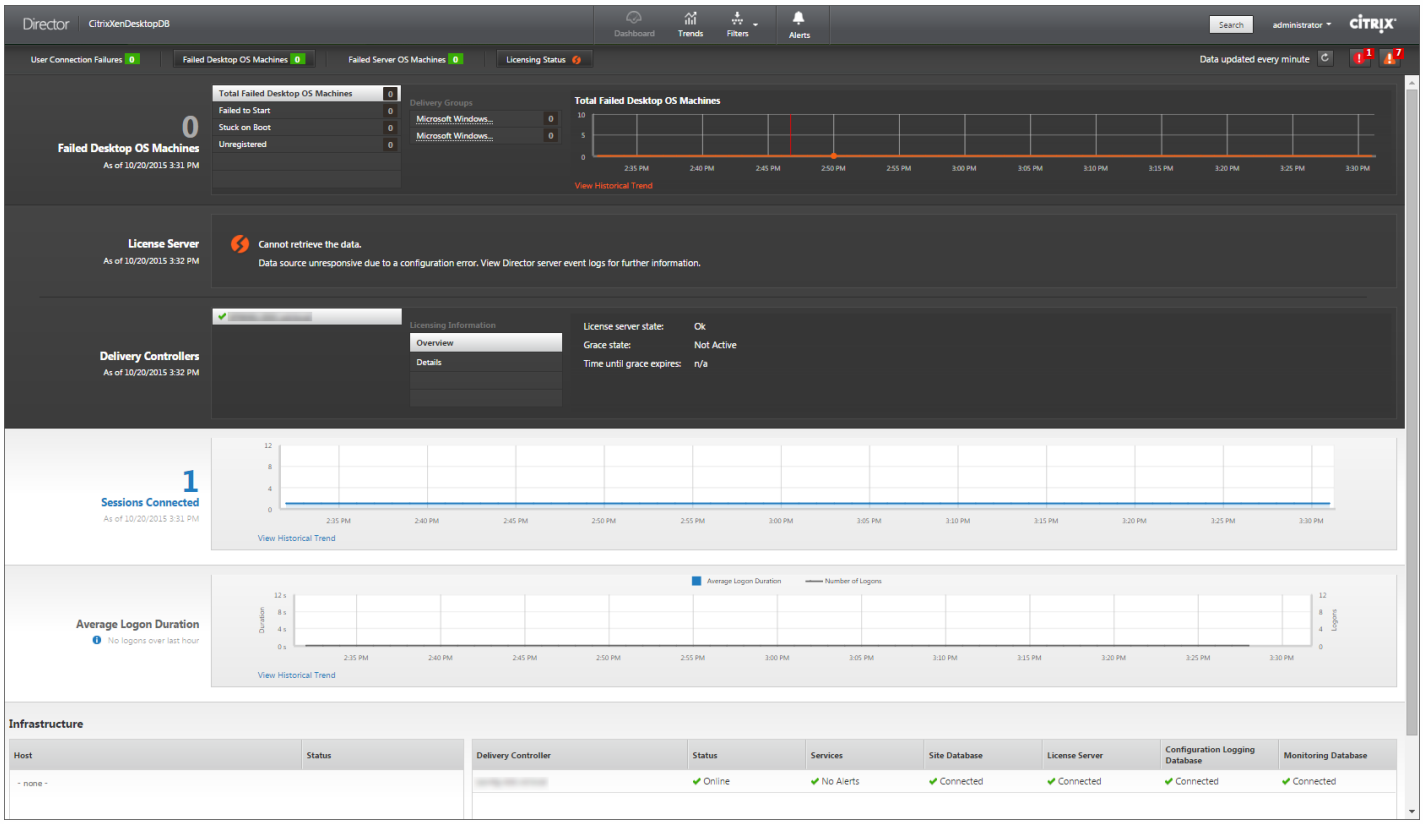
Supervisar revisiones hotfix

Controlar los estados de energía de la máquina del usuario

Impedir conexiones a máquinas

Supervisar sitios

Con permisos de administrador completos, al abrir Director, el Panel de mandos ofrece una ubicación centralizada desde la que puede supervisar el estado y el uso de un sitio.



Si no hay fallos y no se han producido fallos en los últimos 60 minutos, los paneles permanecen contraídos. Cuando hay fallos, el panel de fallos específicos aparecerá automáticamente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: Es posible que algunas opciones o funciones no estén disponibles, ya que dependen de la licencia que tenga su organización y de sus privilegios de administrador.

Panel	Descripción
Fallos de conexión de usuario	Fallos de conexión en los últimos 60 minutos. Haga clic en las categorías junto al número total para ver las mediciones para ese tipo de fallo. En la tabla adyacente, esa cantidad se desglosa por grupos de entrega. Los fallos de conexión incluyen fallos provocados por haberse alcanzado el límite de las aplicaciones. Para obtener más información acerca de los límites para aplicaciones, consulte 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	• Alertas de servidor de licencias muestra las alertas enviadas por el servidor de licencias y las acciones necesarias para resolverlas. Requiere License Server 11.12.1 o una versión posterior. • Alertas de Delivery Controller muestra 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.
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 situado 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 se incluyen en esta media. Para obtener más información, consulte Cómo 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, en Citrix XenServer 7.0 Administrator's Guide, consulte "XenCenter Performance Alerts".

Nota: Si no aparece el icono para una métrica concreta, significa que el tipo de métrica no es compatible con el tipo de host

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
- 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.

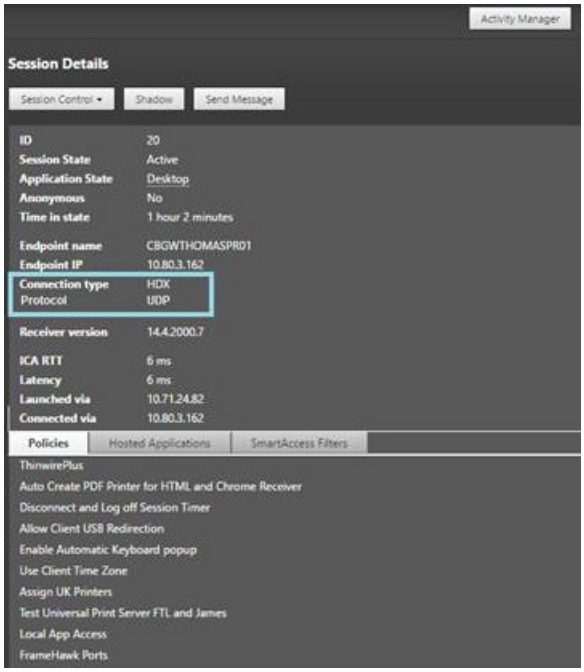
Acción	Descripción
Ver la máquina o sesión a la que está conectado un usuario	En las vistas Administrador de actividades y Detalles del usuario, se puede ver la máquina o la sesión a la que está conectado un usuario en ese momento, así como una lista de todas las máquinas y sesiones a las que dicho usuario 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.
Ver datos para un periodo de tiempo más largo	En la vista Tendencias, seleccione la ficha Sesiones para profundizar más y ver datos de uso más específicos sobre 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 agente VDA anterior a la versión 7 o Linux VDA), Director no puede mostrar información completa sobre la sesión. En vez de ello, aparece un mensaje donde se indica que la información no está disponible.

Puede ver el protocolo de transporte que se utiliza para el tipo de conexión HDX en la sesión actual desde el panel Detalles

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de la sesión. Esta información está disponible para las sesiones iniciadas en los VDA 7.13 o una versión posterior.



- Para el tipo de conexión **HDX**:
  - El protocolo que se muestra es **UDP** si se utiliza EDT para la conexión HDX.
  - El protocolo que se muestra es **TCP** si se utiliza TCP para la conexión HDX.
- Para el tipo de conexión **RDP**, el protocolo se muestra como **n/d**.

Cuando se configura el transporte adaptable, el protocolo de transporte de la sesión cambia dinámicamente entre EDT (sobre UDP) y TCP, según las condiciones de red. Si no se puede establecer la sesión HDX por el protocolo EDT, se recurre al protocolo TCP.

Para obtener más información sobre cómo configurar el transporte adaptable, consulte Transporte adaptable.

Filtrar datos para solucionar fallos

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Instancias de aplicación**. Esta vista muestra las propiedades de todas las instancias de aplicación que haya en los VDA de SO de escritorio y de servidor. Las mediciones del tiempo de inactividad de la sesión están disponibles para las instancias de aplicación 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.
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 aplicaciones) y, a continuación, seleccione el filtro guardado.
8. Si es necesario, para 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.
9. 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 errores de máquinas y conexiones están disponibles en Citrix Director 7.12 Failure Reasons Troubleshooting Guide.
10. En la vista **Máquinas**, haga clic en un enlace del nombre de la máquina para ir a la página **Detalles de la máquina** de la máquina correspondiente. Esta página muestra los datos de la máquina, ofrece controles de alimentación, y muestra gráficos de CPU, memoria, supervisión de disco y supervisión de GPU. Además, puede hacer clic en **Ver utilización histórica** para ver las tendencias de utilización de los recursos en la máquina. Para obtener más información, consulte Solucionar problemas de máquinas.
11. En la vista **Instancias de aplicación**, ordene o filtre en función del **Tiempo de inactividad** superior al período de tiempo del umbral. Seleccione las instancias de aplicación inactivas que quiere finalizar. Cerrar o desconectar una instancia de aplicación finaliza todas las instancias de aplicación activas que haya en la misma sesión. Para obtener más información, consulte Solucionar problemas de aplicaciones.
    Nota: La página de filtro "Instancias de aplicación" 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.

Supervisar tendencias históricas en un sitio

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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- En los sitios con la licencia Platinum, están disponibles los informes de tendencias del último año (365 días) como máximo.
- En los sitios con la licencia Enterprise, están disponibles los informes de tendencias del último mes (31 días) como máximo.
- En los sitios con licencias que no sean ni Platinum ni Enterprise, están disponibles los informes de tendencias de la última semana (7 días) como máximo.

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.
- Los valores predeterminados de las tendencias en la retención de la limpieza de datos por el servicio de supervisión están disponibles en la sección Granularidad y retención de datos.Los clientes de los sitios con licencia Platinum pueden cambiar la retención de la limpieza de datos a la cantidad de días de retención que quieran.

Acción	Descripción
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 de las fases de inicio de sesión, tales como la duración de la intermediación de los brokers 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 se puede ver 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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 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.
Ver utilización de recursos	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 uso de CPU, promedio de uso de memoria, promedio de operaciones de E/S, latencia de disco y picos 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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. **Nota**: 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 IOPS son las IOPS medias por hora recopiladas en el VDA.)
Ver datos de análisis de red	**Nota:** La disponibilidad de esta función depende de la licencia de su organización y sus permisos de administrador.Esta característica requiere Delivery Controllers **7.11** o posterior. Desde la ficha Red se puede supervisar el análisis de red, que ofrece una vista en contexto de los usuarios, las aplicaciones y los escritorios de la red. Con esta función, Director ofrece un análisis avanzado del tráfico ICA en la implementación, mediante informes de HDX Insight desde NetScaler Insight Center o NetScaler MAS.Para obtener más información, consulte Configurar análisis de red.
Ver fallos de aplicación	La ficha "Fallos y errores de aplicación" muestra los fallos asociados a las aplicaciones publicadas en los VDA. **Nota**: 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 Supervisión de fallos históricos de aplicaciones en "Solucionar problemas de aplicaciones". De forma predeterminada, solo se muestran los fallos de aplicaciones en los VDA de SO de servidor. Puede configurar la supervisión de los fallos de aplicación mediante las directivas de supervisión. Para obtener más información, consulte Configuraciones de directiva de supervisión.
Crear informes personalizados	La ficha Informes personalizados proporciona una interfaz de usuario para generar informes personalizados que contienen datos históricos y en tiempo real sobre la base de datos de supervisión en formato tabular. Nota**: Esta función requiere Delivery Controllers de la versión 7.12** o posterior. Desde la lista de las consultas de "Informe personalizado" previamente guardadas, puede hacer clic en **Ejecutar** 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 aplicación. Especifique las condiciones de filtro, que pueden establecerse en función de campos como la máquina, el grupo de entrega o el período de tiempo. Especifique columnas adicionales necesarias en el informe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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.

Notas:

- Los datos de inicio de sesión de conexiones HDX no se recopilan para versiones del VDA anteriores a la versión 7. Para los VDA anteriores, los datos gráficos se muestran como 0.
- Los grupos de entrega eliminados en Citrix Studio pueden seleccionarse en los filtros de tendencias de Director hasta que los datos relacionados con ellos se hayan limpiado y eliminado. Si se selecciona un grupo de entrega eliminado se muestran gráficos para los datos disponibles durante el 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, esto hace que las tablas de **Utilización de recursos e Índice de patrón de carga** del nuevo grupo de entrega muestren mediciones consolidadas de ambos grupos de entrega, el antiguo y el nuevo.

Exportar informes

Puede exportar los datos de tendencias para generar informes de uso habitual y administración de capacidad. En la exportación, se admiten los formatos PDF, Excel y CSV. Los informes en formatos PDF o Excel contienen datos de tendencias representados en gráficos y tablas. Los informes en formato CSV contienen datos tabulares que se pueden procesar para generar vistas, o bien se pueden archivar.

Para exportar un informe:

1. Vaya a la ficha **Tendencias**.
2. Establezca los criterios de filtrado y el período de tiempo. 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

cantidad de filas o registros que haya en la tabla. La cantidad predeterminada de registros admitidos se define en función del formato de informe.

Puede cambiar el límite predeterminado ajustando los parámetros de aplicaciones de Director en Internet Information Services (IIS).

Formato del informe	**Cantidad predeterminada de registros admitidos**	**Campos de "Configuración de aplicaciones" en Director**	**Cantidad máxima admitida de registros**
PDF	500	UI.ExportPdfDrilldownLimit	5000
Excel	100 000	UI.ExportExcelDrilldownLimit	100 000
CSV	100 000 (10.000.000 en la ficha Sesiones)	UI.ExportCsvDrilldownLimit	100 000

Para cambiar el límite de la cantidad de registros que se pueden exportar:

1. Abra la consola del Administrador IIS.
2. Vaya al sitio Web de Director en el sitio Web predeterminado.
3. Haga doble clic en **Configuración de aplicaciones**.
4. Modifique el campo o agregue uno nuevo.

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 respalda.

Solución 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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:

comando COPIAR

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -MonitorQueryTimeoutSeconds <timeout value>
```

- **Se excedió la cantidad máxima de operaciones simultáneas de exportación o vista previa**

  Director admite una instancia de Exportar o Vista previa. Si recibe el error **Cantidad máxima de operaciones simultáneas de exportación o vista previa en curso**, vuelva a intentar más tarde la operación de exportación.

  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:

  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.

Control sobre 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Alertas y notificaciones

Dec 05, 2017

En este artículo:

Supervisar alertas

Crear directivas de alertas

Condiciones para directivas de alertas

Configurar directivas de alertas con webhooks de Octoblu

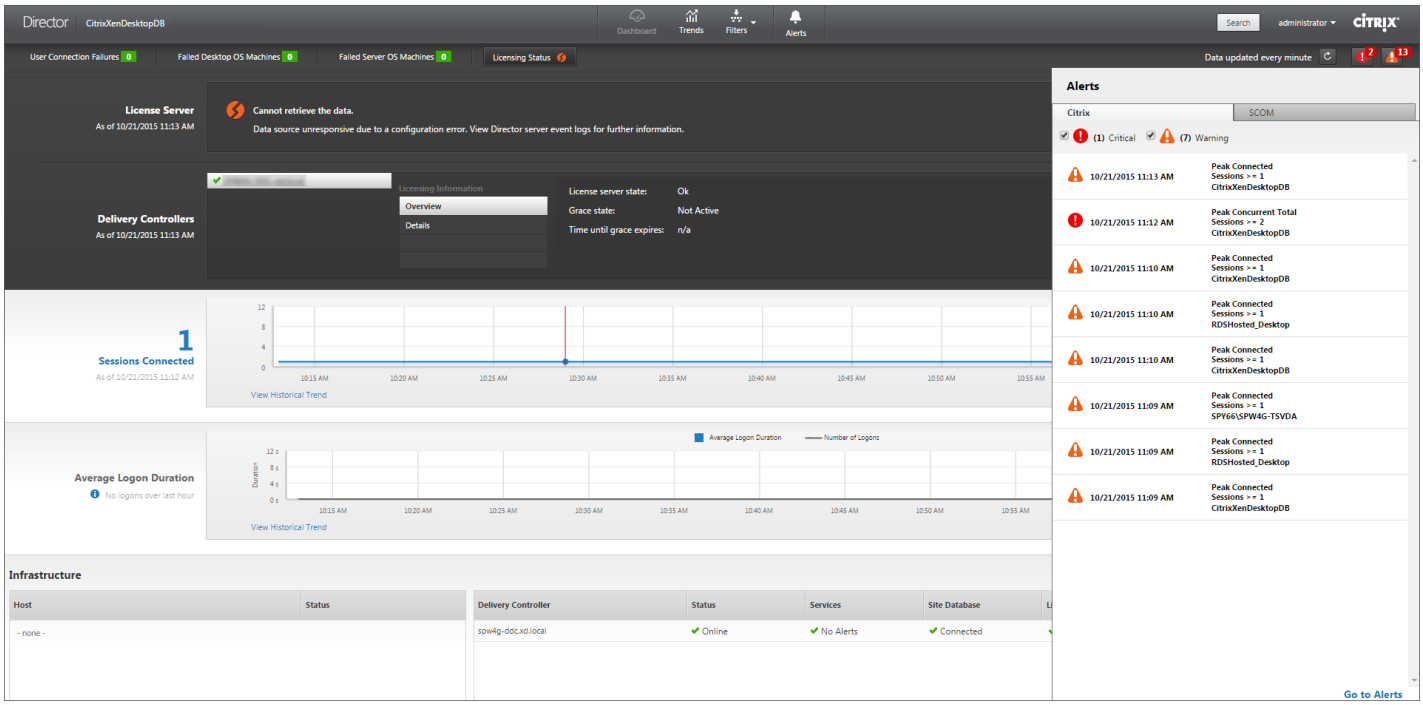
Configurar directivas de alertas con capturas de SNMP

Alertas de SCOM

Configurar la integración de SCOM

Supervisar alertas

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 **Platinum**. Las alertas se actualizan automáticamente cada minuto, aunque también se pueden actualizar a petición.



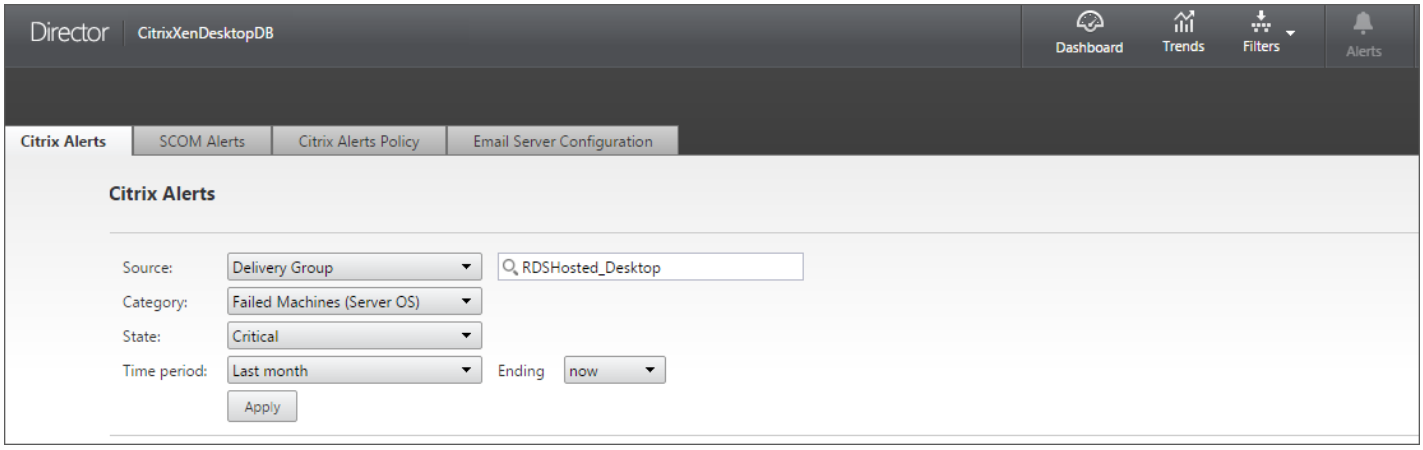
Una alerta de advertencia (un triángulo amarillo) indica que se ha alcanzado o superado el umbral de advertencia de una condición.

Una alerta crítica (un círculo rojo) indica que se ha alcanzado o superado el umbral crítico de una condición.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Puede ver 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.



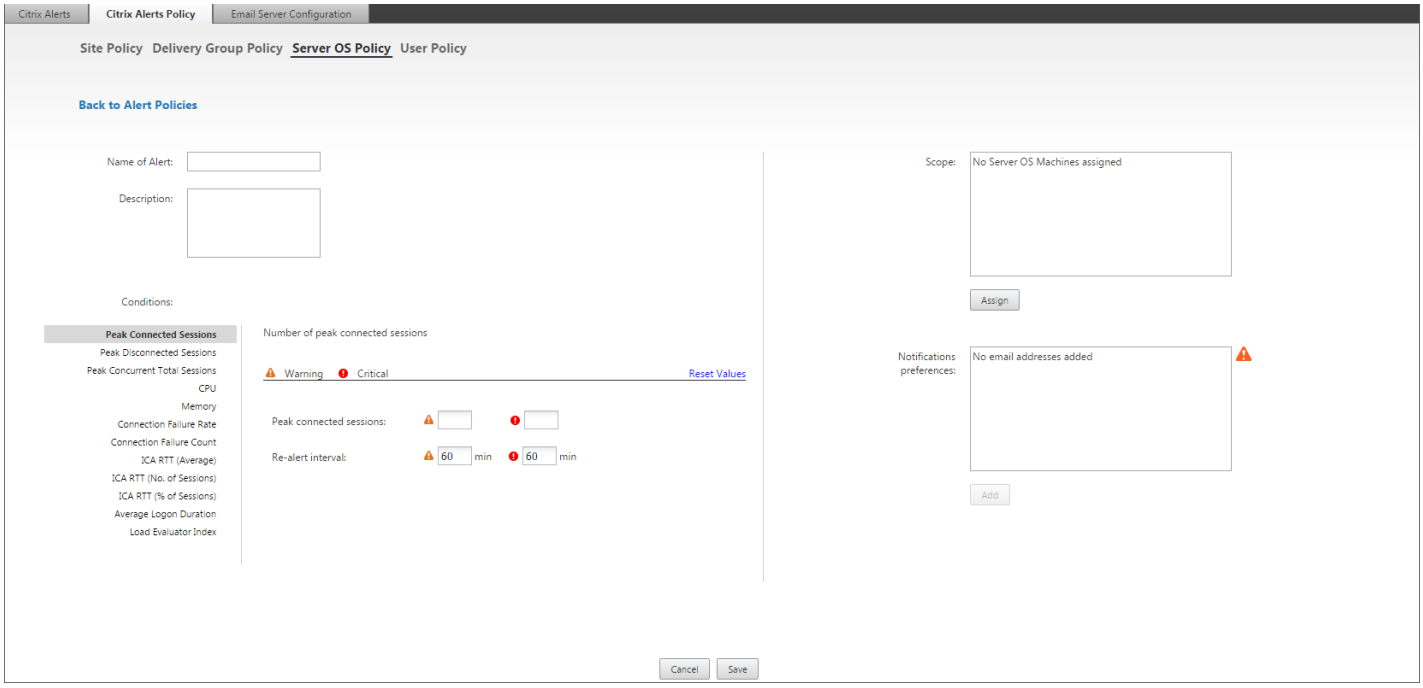
Alertas de Citrix. Estas alertas son avisos que se supervisan en Director y que se originan en componentes de Citrix. Puede configurar las alertas de Citrix desde Director, en **Alertas** > **Directiva de alertas de Citrix**. Como parte de la configuración, también puede definir notificaciones, que se enviarán por correo electrónico a usuarios y grupos cuando las alertas alcancen o superen los umbrales que haya configurado. Puede configurar la notificación como webhooks de Octoblu, o también capturas de SNMP.Para obtener más información acerca de la configuración de alertas de Citrix, consulte Crear directivas de alertas.

Alertas de SCOM. Las alertas de SCOM muestran información de alertas de Microsoft System Center 2012 Operations Manager (SCOM). Con ellas, se ofrece información más detallada acerca del estado y el rendimiento del centro de datos desde Director. Para obtener más información, consulte Alertas 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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, 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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Condición para directiva de alertas	**Descripción y acciones recomendadas**
Máximo de sesiones conectadas	Cantidad máxima de sesiones conectadas. • En Director, comprobar la vista Tendencias de sesiones para ver la cantidad máxima de sesiones conectadas. • Comprobar que haya capacidad suficiente para admitir la carga de las sesiones. • Agregar más máquinas si fuera necesario.
Pico de sesiones desconectadas	Cantidad máxima de sesiones desconectadas. • En Director, comprobar la vista Tendencias de sesiones para ver la cantidad máxima de sesiones desconectadas. • Comprobar que haya capacidad suficiente para admitir la carga de las sesiones. • Agregar más máquinas si fuera necesario. • Cerrar sesiones desconectadas, si es necesario.
Pico de total de sesiones simultáneas	Cantidad máxima de sesiones simultáneas. • En Director, comprobar la vista Tendencias de sesiones para ver la cantidad máxima de sesiones simultáneas. • Comprobar que haya capacidad suficiente para admitir la carga de las sesiones. • Agregar más máquinas si fuera necesario. • Cerrar sesiones desconectadas, si es necesario.
CPU	Porcentaje de uso de CPU. • Identificar los procesos o recursos que consumen la CPU. • Finalizar 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, agregar más recursos de CPU en el futuro. **Nota**: De forma predeterminada, la configuración de directiva **Habilitar supervisión de recursos** está habilitada para la supervisión de la CPU y los contadores de rendimiento de memoria 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.
	Porcentaje de uso de memoria.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Memoria	• Identificar los procesos o recursos que consumen la memoria. • Finalizar 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, agregar más capacidad de memoria en el futuro. **Nota**: De forma predeterminada, la configuración de directiva **Habilitar supervisión de recursos** está habilitada para la supervisión de la CPU y los contadores de rendimiento de memoria 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.
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, consultar la vista Tendencias de fallos de conexión para ver eventos registrados en el registro de configuración. • Determinar si las aplicaciones o los escritorios son accesibles.
Recuento de fallos de conexión	Cantidad de fallos de conexión durante la última hora. • En Director, consultar la vista Tendencias de fallos de conexión para ver eventos registrados en el registro de configuración. • Determinar si las aplicaciones o los escritorios son accesibles.
RTT de ICA (promedio)	Tiempo medio de ida y vuelta del protocolo Independent Computing Architecture. • Consulte NetScaler HDX Insight o MAS para ver un desglose de los tiempos de ida y vuelta de ICA y determinar la causa raíz.Para obtener más información, consulte la documentación de NetScaler Insight Center - HDX Insight o NetScaler MAS - Analytics: HDX Insight. • Si NetScaler no está disponible, consulte la vista Detalles del usuario de Director para ver el RTT de ICA y la latencia, y determinar si se trata de un problema de red o de XenApp o XenDesktop.
RTT de ICA (nº de sesiones)	Cantidad de sesiones que superan el umbral de tiempos de ida y vuelta (RTT) de ICA. • Consulte NetScaler HDX Insight para ver la cantidad de sesiones que tienen tiempos RTT de ICA altos.Para obtener más información, consulte la documentación de NetScaler Insight Center - HDX Insight o NetScaler MAS - Analytics: HDX Insight. • Si NetScaler no está disponible, póngase en contacto con el equipo de red para determinar con ellos la causa del problema.
RTT de ICA (% de sesiones)	Porcentaje de sesiones que superan el tiempo medio de ida y vuelta de ICA. • Consulte NetScaler HDX Insight o MAS para ver la cantidad de sesiones que tienen tiempos RTT de ICA altos.Para obtener más información, consulte la documentación de NetScaler Insight Center - HDX Insight o NetScaler MAS - Analytics: HDX Insight.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	• Si NetScaler no está disponible, póngase en contacto 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.
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.
Promedio de duración de inicio de sesión	Duración media de los inicios de sesión que se han producido durante la última hora. • Comprobar 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. • Comprobar la línea base y desglosar los inicios de sesión para determinar la causa. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.
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. • Consultar Director para ver máquinas con sistema operativo de servidor que tengan un máximo de carga. • Consultar el panel de mandos (para ver errores) y el informe de tendencias en el índice del patrón de carga.

Configuración de directivas de alertas con webhooks de Octoblu

Además de las notificaciones de correo electrónico, se pueden configurar directivas de alertas con webhooks de Octoblu para iniciar servicios de IoT.

Nota: Esta característica requiere Delivery Controllers de la versión 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 más 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 nueva directiva de alertas con una URL de webhook:

```
comando                                                
```

"Value": ,

"Timestamp": ,

"PolicyName": ,

"Description": ,

"Scope": <Ámbito de la directiva de alertas>,

"NotificationState": ,

"Site": }

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 característica 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:

```
comando                                                                    COPIAR

Get-MonitorNotificationSnmpServerConfiguration
```

- Establezca la configuración del servidor para SNMP versión 2:

```
comando                                                                    COPIAR

Set-MonitorNotificationSnmpServerConfiguration -ServerName <Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -Com
```

- Establezca la configuración del servidor para SNMP versión 3:

```
comando                                                                    COPIAR
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
$authpass = "<authentication password>" | ConvertTo-SecureString -AsPlainText -Force

$privpass = "<Privacy password>" | ConvertTo-SecureString -AsPlainText -Force

Set-MonitorNotificationSnmpServerConfiguration -ServerName <Server IP> -PortNumber <Port ID> -SnmpSender <Sender name> -Engi
```

- Habilite la captura de SNMP para una directiva de alertas existente:

comando COPIAR

```
Set-MonitorNotificationPolicy -IsSnmpEnabled $true -Uid <Policy ID>
```

- Cree una nueva directiva de alertas con la configuración de capturas de SNMP:

comando COPIAR

```
$policy = New-MonitorNotificationPolicy -Name <Policy name> -IsSnmpEnabled $true -Description <Policy description> -Enabled $true
```

La estructura de los OID en los mensajes de captura SNMP de Director es la siguiente:
1.3.6.1.4.1.3845.100.1.
Aquí, el 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.** para filtrar y gestionar mensajes de captura de alertas concretas.

Utilice el siguiente cmdlet para obtener los UID de las directivas de alertas definidas en su entorno:

comando COPIAR

```
Get-MonitorNotificationPolicy
```

Puede reenviar capturas de SNMP a SCOM. Para ello, configure SCOM con el Delivery Controller para escuchar los mensajes de captura.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Alertas de SCOM

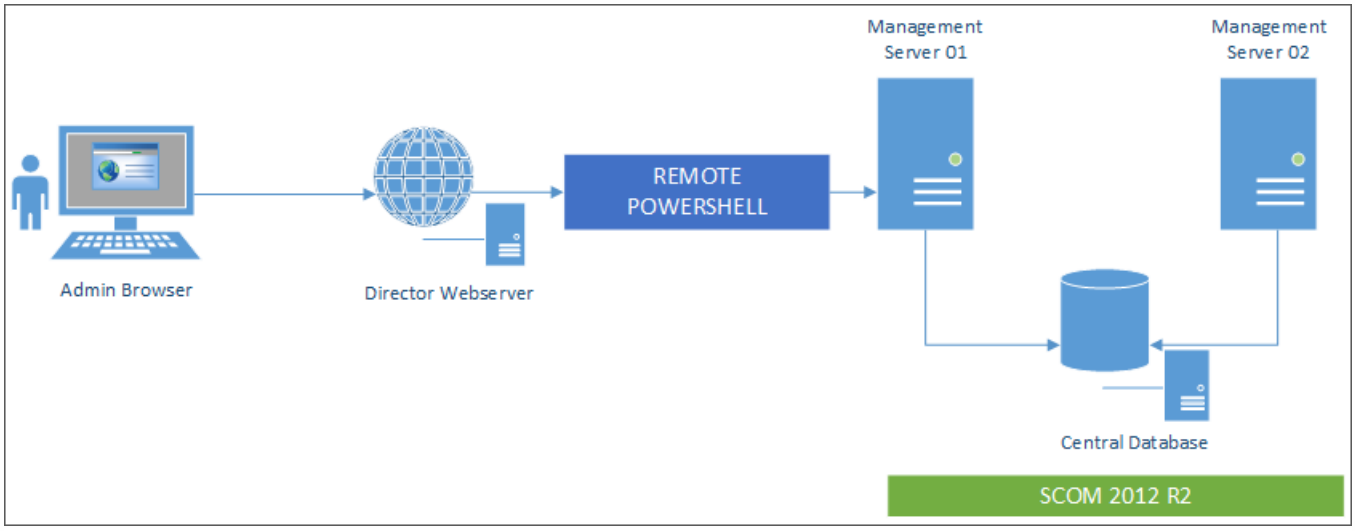
La integración de SCOM con Director permite ver la información de alertas provenientes de SCOM en el panel de mandos y en otras vistas de alto nivel de Director.

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.

Configurar la integración de SCOM

La integración de SCOM usa PowerShell 3.0 (o una versión posterior) de forma remota para consultar datos en el servidor de administración de SCOM y mantiene una conexión persistente en el espacio de ejecución de la sesión de usuario en Director. Director y el servidor SCOM deben tener la misma versión de PowerShell.



Los requisitos para la integración de SCOM son:

- Windows Server 2012 R2
- System Center 2012 R2 Operations Manager
- PowerShell 3.0 o una versión posterior (las versiones de PowerShell en Director y en el servidor SCOM deben coincidir)
- CPU de cuatro núcleos con 16 GB de RAM (recomendado)
- Debe configurarse un servidor de administración principal para SCOM en el archivo web.config de Director. Puede hacerlo mediante la herramienta DirectorConfig.

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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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:

a. Obtenga la lista actual de TrustedHosts

comando COPIAR

```
Get-Item WSMAN:\localhost\Client\TrustedHosts
```

b. Agregue el nombre de dominio completo (FQDN) del servidor de administración de SCOM a la lista TrustedHosts. representa el conjunto de entradas devuelto por el cmdlet Get-Item.

comando COPIAR

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value "<FQDN SCOM Management Server>,<Old Values>"
```

3. Configure SCOM mediante la herramienta DirectorConfig.

comando COPIAR

```
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 nuevo 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 al administrador de Director un rol distinto al de Operador
:

i.Si hay varios servidores de administración configurados, y el servidor de administración principal no está

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 haya 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.

ii. 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 desde la función de usuario especificada.

2.Agregue administradores de Director al grupo de Usuarios de administración remota en el servidor de administración de SCOM. Esto permite a los administradores de Director establecer una conexión remota con PowerShell.

3.Escriba **Enable-PSRemoting** para habilitar la comunicación remota de PowerShell.

4.Establezca los límites de las propiedades de WS-Management:

a.Modifique MaxConcurrentUsers:

En la interfaz de línea de comandos:

```
comando
```

COPIAR

```
winrm set winrm/config/winrs @{MaxConcurrentUsers = "20"}
```

En PowerShell:

```
comando
```

COPIAR

```
Set-Item WSMan:\localhost\Shell\MaxConcurrentUsers 20
```

b. Modifique MaxShellsPerUser:

En la interfaz de línea de comandos:

```
comando
```

COPIAR

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
winrm set winrm/config/winrs @{MaxShellsPerUser="20"}
```

En PowerShell:

comando COPIAR

```
Set-Item WSMan:\localhost\Shell\MaxShellsPerUser 20
```

c.Modifique MaxMemoryPerShellMB:

En la interfaz de línea de comandos:

comando COPIAR

```
winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
```

En PowerShell:

comando COPIAR

```
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: Una modificación incorrecta del Registro puede provocar problemas graves, que pueden obligar a la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Debe hacer una copia de seguridad del Registro antes de editarlo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Una vez configurada la integración de SCOM, es posible que aparezca el mensaje "No se pueden obtener las alertas recientes de SCOM. Revise los registros de eventos del servidor de Director para obtener más información". Los registros de eventos del servidor ayudarán a identificar y corregir el problema. Las causas pueden ser:

- Pérdida de conectividad de red a la máquina de SCOM o Director.
- El servicio de System Center Operations Manager no está disponible o está demasiado ocupado para responder.
- Error de autorización debido a un cambio en los permisos del usuario configurado.
- Un error en Director al procesar datos de SCOM.
- Las versiones de PowerShell en Director y en el servidor SCOM no coinciden.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administración delegada y Director

Dec 05, 2017

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 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 del 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.
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	Sin acceso. Este administrador no es compatible en Director y no puede ver datos. Este usuario puede tener acceso a la página Detalles de la máquina (búsqueda de máquinas).
Administrador de host	Sin acceso. Este administrador no es compatible en Director y no puede ver datos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar roles personalizados de 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 técnica (Help Desk) integrado para que el administrador no pueda cerrar sesiones.

Si crea un rol personalizada con permisos de Director, también debe dar a ese rol otros permisos genéricos:

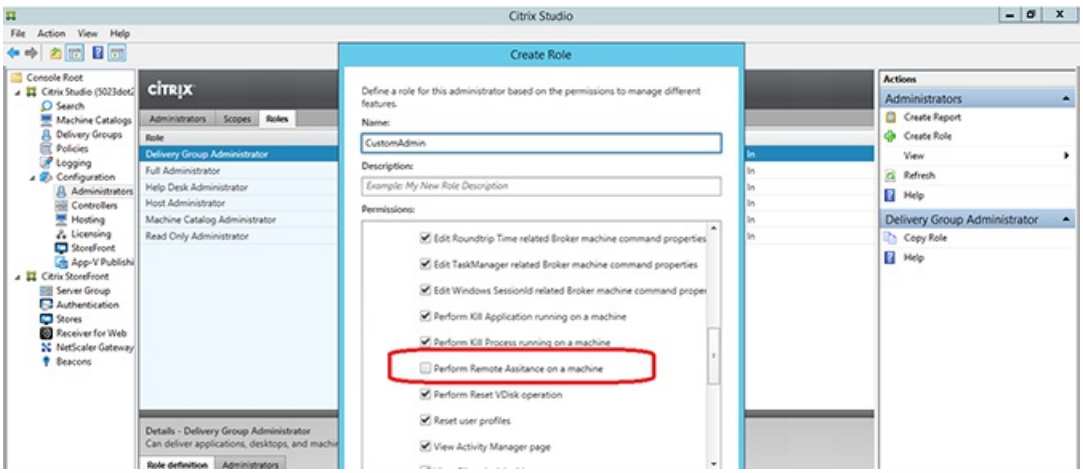
- Permiso de Delivery Controller para iniciar sesión en Director. Al menos el acceso de solo lectura en el nodo Administrador
- Permisos para que los grupos de entrega vean los datos relacionados con esos grupos de entrega en Director. Al menos el acceso de solo lectura

También puede crear un rol personalizado mediante la copia de un rol existente e incluir permisos adicionales para vistas diferentes. Por ejemplo, puede copiar el rol del servicio de asistencia e incluir permisos para ver las páginas Panel de mandos o Filtros.

Seleccione los permisos de Director para el rol personalizado, incluidos:

- Terminar aplicación ejecutada en una máquina
- Terminar proceso ejecutado en una máquina
- Asistencia remota en una máquina
- Restablecer disco virtual
- Restablecer perfiles de usuario
- Ver página Detalles de cliente
- Ver página Panel de mandos
- Ver página Filtros
- Ver página Detalles de la máquina
- Ver página Tendencias
- Ver página Detalles del usuario

En este ejemplo, el Remedo (Asistencia remota en una máquina) está desactivado.



Un permiso puede depender de otros para que se pueda aplicar en la interfaz de usuario. Por ejemplo, seleccionar el permiso **Terminar aplicación ejecutada en una máquina** habilita la funcionalidad **Finalizar aplicación** solo en aquellos paneles a los que tiene permiso el rol. Se pueden seleccionar los siguientes permisos de panel:

- Ver página Filtros
- Ver página Detalles del usuario

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Implementación segura de Director

Feb 01, 2018

En este artículo se muestran las áreas que pueden afectar a la seguridad del sistema durante la implementación y la configuración de Director.

Configuración de Microsoft Internet Information Services (IIS)

Director puede configurarse con una configuración restringida de IIS. Esta no es la configuración predeterminada de IIS.

Extensiones de nombres 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
- HEAD

Director no requiere:

- Filtros de ISAPI
- Extensiones ISAPI
- Programas CGI
- Programas FastCGI

Importante:

- Director requiere Plena confianza. No configure el nivel de confianza global de .NET en 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.

Configuración de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Comunicaciones de Director

En un entorno de producción, Citrix recomienda el uso del protocolo IPsec o los protocolos HTTPS para proteger la transferencia de los datos entre Director y los servidores. IPsec es un conjunto de extensiones estándar para el protocolo de Internet. Proporciona comunicaciones autenticadas y cifradas con integridad de datos y protección contra reproducción. Como IPsec es un conjunto de protocolos de capa de red, los protocolos con niveles más elevados pueden utilizarlo sin realizar ninguna modificación. HTTPS utiliza el protocolo Transport Layer Security (TLS) para brindar un cifrado de datos avanzado.

Nota:

- Citrix recomienda no habilitar conexiones a Director que no sean seguras en un entorno de producción.
- Para proteger las comunicaciones desde Director, se requiere una configuración aparte para cada conexión.
- No se recomienda usar el protocolo SSL. En su lugar, use el protocolo TLS, que es más seguro.
- Debe proteger las comunicaciones con NetScaler mediante TLS, no IPsec.

Para proteger las comunicaciones entre Director y los servidores XenApp y XenDesktop (para supervisión e informes), consulte Data Access Security.

Para proteger las comunicaciones entre Director y NetScaler (para NetScaler Insight), consulte Configuración del análisis de red.

Para proteger las comunicaciones entre Director y el servidor de licencias, consulte Seguridad de License Administration Console.

Separación de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración de permisos para VDA anteriores a XenDesktop 7

Dec 05, 2017

Si los usuarios tienen agentes VDA anteriores a XenDesktop 7, Director complementa la información de la implementación con estados y métricas en tiempo real a través de la Administración remota de Windows (WinRM).

Además, use este procedimiento para configurar WinRM para su uso con Remote PC en XenDesktop 5.6 Feature Pack 1.

De forma predeterminada, solo los administradores locales de la máquina de escritorio (por lo general, los administradores de dominio y otros usuarios con privilegios) tienen los permisos necesarios para ver los datos en tiempo real.

Para obtener más información acerca de la instalación y la configuración de WinRM, consulte CTX125243.

Para permitir que otros usuarios vean los datos en tiempo real, debe concederles permisos. Por ejemplo, supongamos que hay varios usuarios de Director (HelpDeskUserA, HelpDeskUserB, etc.) que son miembros de un grupo de seguridad de Active Directory denominado HelpDeskUsers. Al grupo se le ha asignado el rol de administrador del servicio de asistencia de Studio, por lo que los miembros obtienen los permisos necesarios de Delivery Controller. Sin embargo, el grupo necesita además obtener acceso a la información desde la máquina de escritorio.

Para otorgar el acceso necesario, puede configurar los permisos requeridos mediante uno de los siguientes métodos:

- Concesión de permisos a los usuarios de Director (modelo de suplantación)
- Concesión de permisos al servicio de Director (modelo de subsistema de confianza)

Para conceder permisos a los usuarios de Director (modelo de suplantación)

De forma predeterminada, Director utiliza un modelo de suplantación: la conexión de WinRM con la máquina de escritorio se realiza mediante la identidad del usuario de Director. De este modo, el usuario debe tener los permisos correspondientes en el escritorio.

Puede configurar estos permisos de dos formas distintas (descritas más adelante en este documento):

1. Agregar usuarios al grupo de administradores local en la máquina de escritorio.
2. Conceder a los usuarios los permisos específicos requeridos por Director. Esta opción impide conceder permisos administrativos completos en la máquina a los usuarios de Director (por ejemplo, el grupo HelpDeskUsers).

Para conceder permisos al servicio de Director (modelo de subsistema de confianza)

En lugar de proporcionar a los usuarios de Director permisos en las máquinas de escritorio, puede configurar Director para que realice las conexiones de WinRM mediante una identidad de servicio y que conceda los permisos adecuados solo a esa identidad de servicio.

Con este modelo, los usuarios de Director no tienen permisos para realizar llamadas de WinRM por sí mismos. Solo pueden obtener acceso a los datos mediante Director.

El grupo de aplicaciones Director en IIS está configurado para que se ejecute como la identidad de servicio. De forma predeterminada, esta es la cuenta virtual APPPOOL\Director. Cuando establece conexiones remotas, esta cuenta aparece como la cuenta del equipo de Active Directory del servidor, por ejemplo, MyDomain\DirectorServer$. Debe configurar esta cuenta con los permisos adecuados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si se implementan varios sitios Web de Director, debe colocar cada cuenta de equipo del servidor Web en un grupo de seguridad de Active Directory configurado con los permisos adecuados.

Para configurar Director de modo que utilice la identidad de servicio para WinRM en lugar de la identidad del usuario, configure el siguiente parámetro como se describe en Configuración avanzada:

Service.Connector.WinRM.Identity = Service
Puede configurar estos permisos de una de las siguientes maneras:

1. Agregar la cuenta del servicio al grupo de administradores local en la máquina de escritorio.
2. Conceda a la cuenta de servicio los permisos específicos requeridos por Director (descritos a continuación). Esta opción impide conceder permisos administrativos completos a la cuenta de servicio en la máquina.

Para asignar permisos a un usuario o grupo específico

Los siguientes permisos son obligatorios para que Director acceda a la información que requiere desde la máquina de escritorio a través de WinRM:

- Permisos de lectura y ejecución en RootSDDL de WinRM
- Permisos de espacio de nombres WMI:
  - root/cimv2: acceso remoto
  - root/citrix: acceso remoto
  - root/RSOP: acceso remoto y ejecución
- Pertenencia a estos grupos locales:
  - Usuarios de Performance Monitor
  - Lectores de registros de sucesos

La herramienta ConfigRemoteMgmt.exe se utiliza para conceder automáticamente estos permisos. En los medios de instalación, se encuentra en las carpetas x86\Virtual Desktop Agent y x64\Virtual Desktop Agent, así como en la carpeta C:\inetpub\wwwroot\Director\tools de los medios de instalación. Debe conceder permisos a todos los usuarios de Director.

Para conceder permisos a un grupo de seguridad, usuario o cuenta de equipo de Active Directory, o para acciones como Finalizar aplicación y Finalizar proceso, ejecute la herramienta con privilegios administrativos desde un símbolo del sistema con los siguientes argumentos:

ConfigRemoteMgmt.exe /configwinrmuser domain\name
donde name es un grupo de seguridad, usuario o cuenta de equipo.

Para conceder los permisos necesarios a un grupo de seguridad de usuarios:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers
Para conceder los permisos a una cuenta de equipo específica:

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer$
Para acciones de Finalizar proceso, Finalizar aplicación y Remedar:

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all
Para conceder permisos a un grupo de usuarios:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all
Para mostrar la ayuda de la herramienta:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ConfigRemoteMgmt.exe

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuración del análisis de red

Dec 05, 2017

Nota: La disponibilidad de esta función depende de la licencia de la empresa y los permisos de administrador.

Director se integra con NetScaler Insight Center o NetScaler MAS para ofrecer análisis de la red y administración del rendimiento:

- El análisis de red utiliza informes de HDX Insight desde NetScaler Insight Center o NetScaler MAS para proporcionar una visión en contexto de los escritorios y 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:

- El tiempo de retorno de sesión ICA (RTT) muestra datos correctamente para Receiver para Windows 3.4 o posterior y Receiver para Mac 11.8 o posterior. Para las versiones anteriores de estos paquetes de Receiver, los datos no se muestran correctamente.
- 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 NetScaler Insight Center o NetScaler MAS en Director. Director requiere NetScaler MAS versión 11.1 compilación 49.16 o una versión posterior.Insight Center y MAS son dispositivos virtuales que se ejecutan 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 NetScaler Insight Center o NetScaler MAS.

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 NetScaler Insight Center o NetScaler MAS (el nombre de dominio completo o la dirección IP), el nombre de usuario, la contraseña, el tipo de conexión (HTTP o HTTPS) y elija la integración con NetScaler Insight o con NetScaler MAS.
3. Para comprobar los cambios, cierre la sesión y vuelva a iniciarla.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Solución de problemas de usuarios

Dec 05, 2017

Use el **Servicio de asistencia** de Director (página **Administrador de actividades**) para ver información sobre el usuario:

- Consulte información acerca del inicio de sesión, la conexión y las aplicaciones del usuario.
- Haga un remedo de 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 red
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 las búsquedas

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

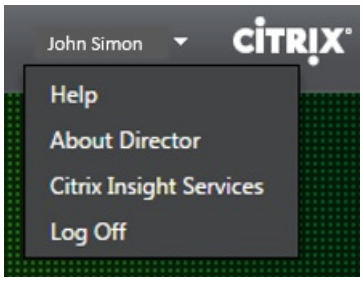
Los resultados de la búsqueda incluyen también usuarios que no están utilizando máquinas en ese momento o no tienen asignada ninguna.

- 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.

Acceso 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.



Carga de información sobre la solución de problemas a 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 de forma segura datos 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 XenApp o XenDesktop. Según la versión de Windows, Scout aparece en el menú Inicio de Windows o en la pantalla Inicio al instalar o actualizar a XenDesktop 7.1, XenDesktop 7.5, XenApp 7.5, XenDesktop 7.6, XenApp 7.6, XenDesktop 7.7 o XenApp 7.7.

Para iniciar Citrix Scout, desde el menú Inicio o la pantalla Inicio, seleccione Citrix > Citrix Scout.

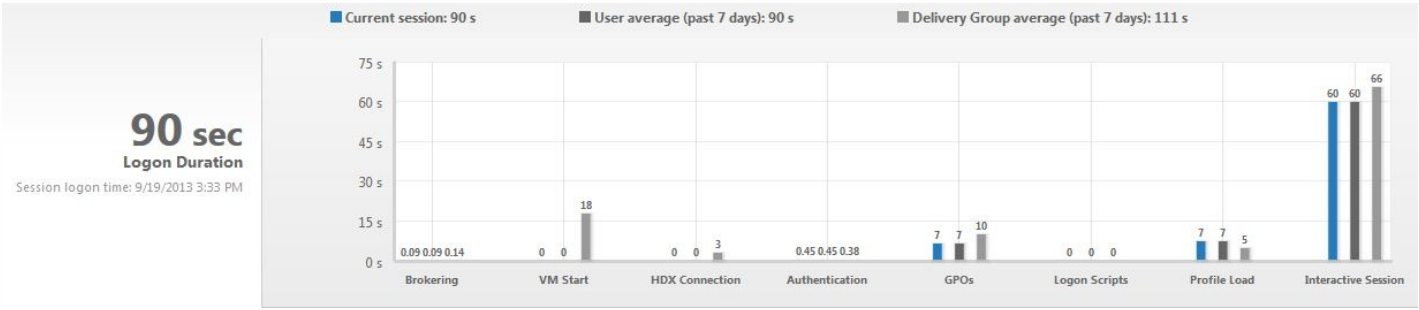
Para obtener información sobre el uso y la configuración de Citrix Scout, y para ver las preguntas frecuentes, consulte CTX130147.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cómo diagnosticar problemas de inicio de sesión de los usuarios

Dec 05, 2017

Use los datos de Duración de inicio de sesión para solucionar problemas de inicio de sesión. En la vista Detalles del usuario, la duración se muestra como un valor numérico y debajo de este aparece la hora a la que tuvo lugar el inicio de sesión, y un gráfico de las fases del proceso de inicio de sesión.



Panel Duración de inicio de sesión en la vista Detalles del usuario

A medida que los usuarios inician sesión en XenApp y XenDesktop, Monitor Service supervisa las etapas 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 alto número de la parte izquierda es el tiempo total del 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.

Use estos pasos generales para solucionar problemas de 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.

Fase del proceso de inicio de sesión	**Descripción**
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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.
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.
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. Normalmente esta es 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 de escritorio preparado (EventId 1000 en el VDA) - Marca de hora del evento de perfil de usuario cargado (EventId 2 en el VDA)

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.

Nota: El gráfico Duración de inicio de sesión muestra las fases de inicio de sesión en segundos. Los valores por debajo de un segundo se muestran en valores inferiores al segundo. Los valores por encima de 1 segundo se redondean al medio (0,5) segundo más cercano. El gráfico se ha diseñado para mostrar el valor más alto del eje Y como 200 segundos. Cualquier valor por encima de los 200 segundos se muestra con el valor real mostrado encima de la barra.

Sugerencias para solución de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remedo de usuarios

Dec 05, 2017

En Director, utilice la función Remedar usuario para ver y trabajar directamente en la máquina virtual o la sesión de un usuario. El usuario debe estar conectado a la máquina que desea remedar. Verifique esto comprobando el nombre de máquina que aparece en la barra de título del usuario.

1. En la vista Detalles del usuario , seleccione la sesión del usuario.
2. Active el remedo de la sesión de usuario seleccionada:
   - Para la supervisión de máquinas, en la vista Administrador de actividades, haga clic en Remedar.
   - Para la supervisión de sesiones, en la vista Detalles del usuario , busque el panel de Detalles de la sesión y haga clic en Remedar.
3. Una vez se inicie la conexión, un cuadro de diálogo le solicitará que abra o guarde el archivo .msrcincident.
4. 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.
5. Indique al usuario que haga clic en Sí para empezar a compartir la máquina o la sesión.

Para mayor control, pida al usuario que comparta su puntero y su teclado.

Optimización de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Envío de mensajes a los usuarios

Dec 05, 2017

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 envía correctamente, aparece un mensaje de confirmación en Director. Si la máquina del usuario está conectada, el mensaje aparece allí.

Si el mensaje no se envía 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 el texto del mensaje de nuevo y haga clic en Intentar de nuevo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cómo resolver fallos de aplicación

Dec 05, 2017

En la vista Administrador de actividades, haga clic en la ficha Aplicaciones. Puede ver todas las aplicaciones de todas las máquinas a las que el usuario tiene acceso, incluidas las aplicaciones locales y las alojadas para la máquina conectada actualmente, y el estado actual de cada una de ellas.

Nota: Si la ficha Aplicaciones aparece atenuada, póngase en contacto con un administrador con permisos para habilitarla. La lista incluye solo las aplicaciones que se han iniciado en la sesión.

Para máquinas con sistema operativo de 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.
Reiniciar la máquina del usuario	Si se trata solo de máquinas con sistema operativo de escritorio, para la sesión seleccionada, haga clic en **Reiniciar**. De forma 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restauración de conexiones de red

Dec 05, 2017

Desde Director, compruebe el estado de conexión del usuario a la máquina actual en la barra de título del usuario.

Si ha fallado la conexión de escritorio, se mostrará el error que hizo que fallara la conexión, lo que puede ayudarle a solucionar el problema.

Acción	Descripción
Comprobar que la máquina no está en modo de mantenimiento	En la página Detalles del usuario, asegúrese de que el modo de mantenimiento está desactivado.
Reiniciar la máquina del usuario	Seleccione la máquina y haga clic en Reiniciar. Utilice esta opción si la máquina del usuario no responde o no puede conectarse a ella porque, por ejemplo, está utilizando una cantidad inusualmente alta de recursos de la CPU, lo que puede inutilizar la CPU.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restauración de sesiones

Dec 05, 2017

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 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 su lugar, se muestra un mensaje que informa de que la información no está disponible. Estos mensajes pueden aparecer en la página Detalles del usuario y Administrador de actividades.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ejecución de informes de sistema de canales HDX

Dec 05, 2017

En la vista Detalles del usuario, se puede comprobar el estado de los canales HDX en la máquina del usuario en el panel HDX. Este panel solo está disponible si la máquina del usuario está conectada mediante HDX.

Si aparece un mensaje que indica que la información no está disponible actualmente, espere un minuto para que se actualice la página o haga clic en el botón Actualizar. Los datos de HDX tardan un poco más que otros datos en actualizarse.

Haga clic en el icono de advertencia o error para obtener más información.

Sugerencia: Puede ver información acerca de otros canales en el mismo cuadro de diálogo. Para ello, haga clic en las flechas izquierda y derecha situadas en la esquina izquierda de la barra de título.

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 de informe XML.
   - 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restablecimiento de Personal vDisk

Dec 05, 2017

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 de En ejecución. Si sitúa el puntero sobre la X, aparece información sobre el fallo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restablecimiento de perfiles de usuario

Dec 05, 2017

Precaución: Cuando un perfil se restablece, aunque las carpetas y los archivos del usuario se guardan y se copian en el 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 una sesión. Las carpetas y archivos del perfil de usuario que se guardaron, se copian en el nuevo perfil.
   Importante: Si el usuario tiene perfiles en varias plataformas (por ejemplo, en Windows 8 y en Windows 7), indíquele que inicie sesión primero en el mismo escritorio o aplicación que notificó como un problema. Esto garantiza el restablecimiento del perfil adecuado.
   Si el perfil es un perfil de usuario de Citrix, el perfil se habrá restablecido para cuando aparezca el escritorio del usuario. Si el perfil es un perfil 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 XenDesktop (VDA de escritorio). Si está usando XenApp (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

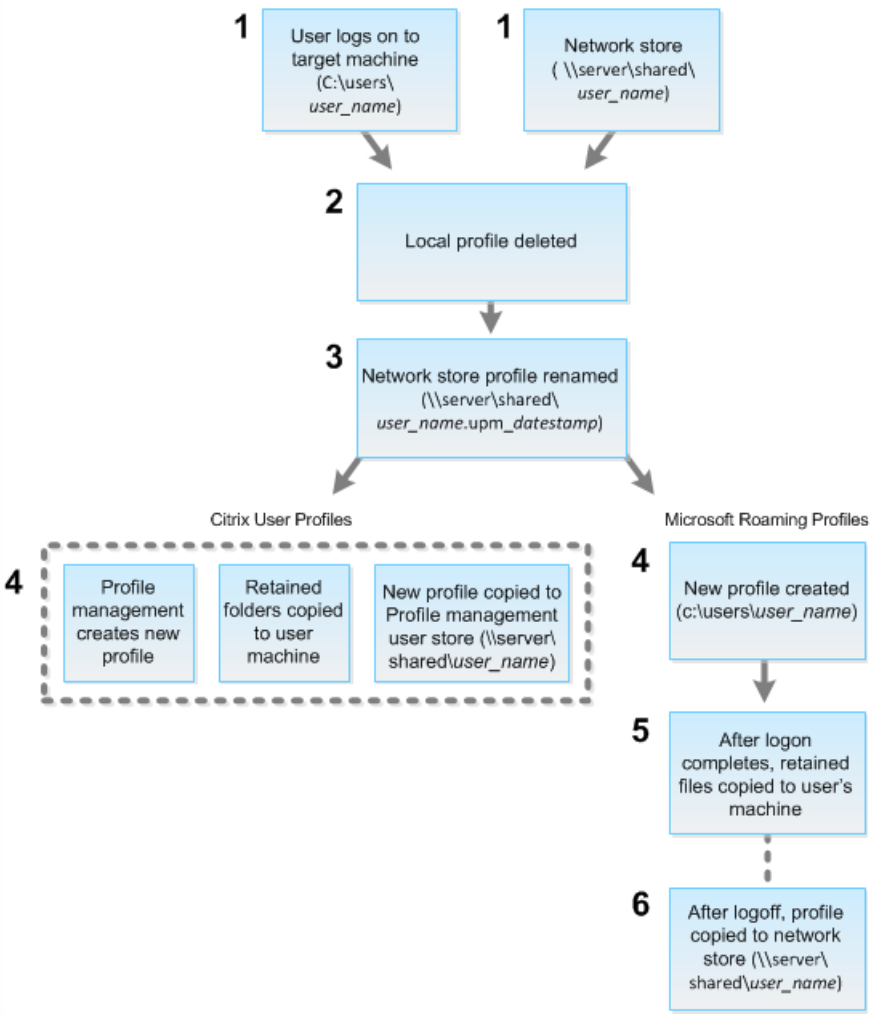
Nota: En Windows 8 y versiones posteriores, las cookies no se copian cuando los perfiles se restablecen.

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 un usuario inicia una sesión.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. 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).
2. Si hay un perfil local está presente, se elimina.
3. El perfil de red se cambia de nombre.
4. 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 importación de Profile Management, y las carpetas se copian de vuelta en el perfil de red, y el usuario puede iniciar una sesión como lo hace normalmente. Si se usa un perfil 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 uno.
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_datestamp.
4. Elimine el nombre del perfil actual; es decir, el que no tiene la extensión .upm_datestamp.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Cambie el nombre de la carpeta archivada por el nombre de perfil original; es decir, quite la extensión de fecha y hora. Con ello, habrá devuelto el perfil a su estado original, pre-restablecido.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Grabación de sesiones

Dec 05, 2017

En Director, puede grabar sesiones ICA mediante los controles de 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 **Platinum**.

Para configurar la Grabación de sesiones en Director mediante la herramienta DirectorConfig, consulte la sección "Configuración de Director para usar el servidor de grabación de sesiones" en Instalación, actualización y desinstalación de Grabación de sesiones.

Los controles de la Grabación de sesiones solo están disponibles en Director si el usuario que ha iniciado sesión tiene el permiso para modificar las directivas de la Grabación de sesiones. Este permiso puede establecerse en la consola de autorización de la Grabación de sesiones, como se describe en Creación y activación de directivas de grabación.

Nota: Los cambios realizados en los parámetros de la Grabación de sesiones a través de Director o la Consola de directivas de grabación de sesiones surten efecto a partir de la siguiente sesión ICA.

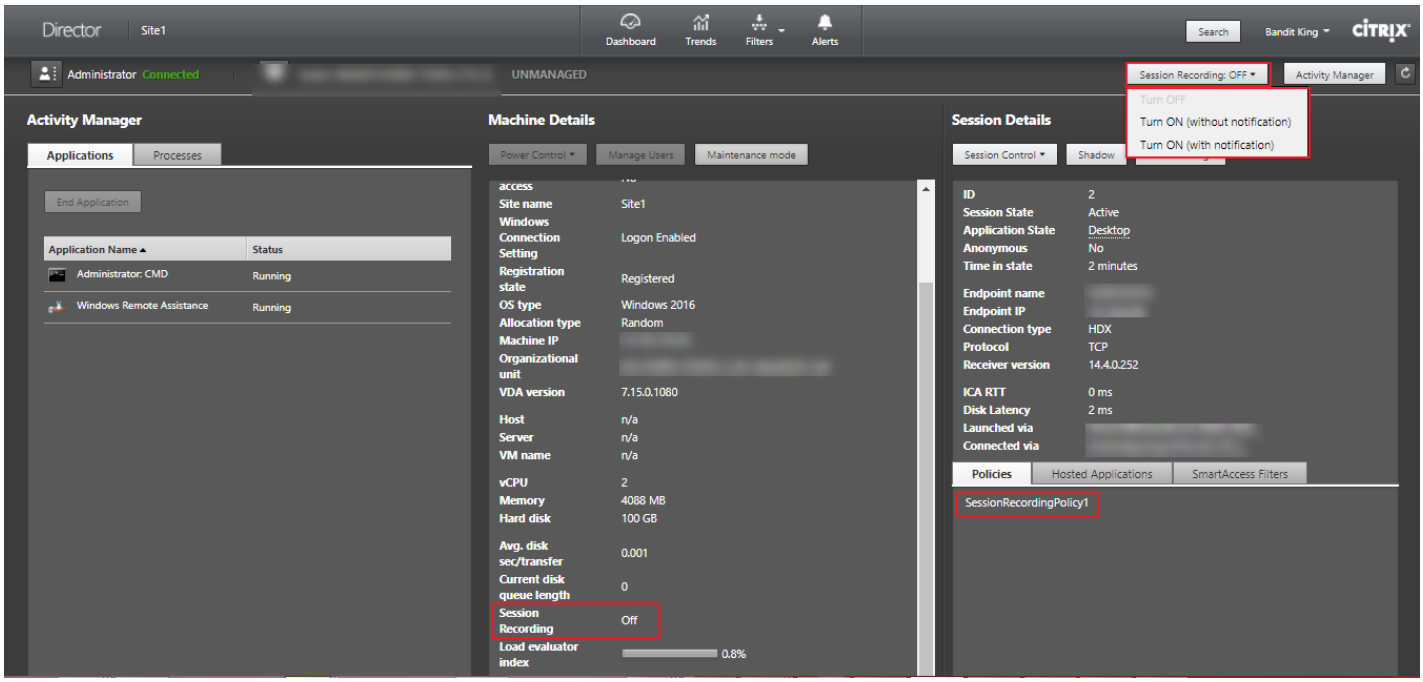
Controles de Grabación de sesiones en Director

Puede habilitar la Grabación de sesiones para un usuario específico desde la pantalla **Administrador de actividades** o **Detalles del usuario**. Las sesiones subsiguientes de ese usuario específico se grabarán en todos los servidores respaldados.

Puede:

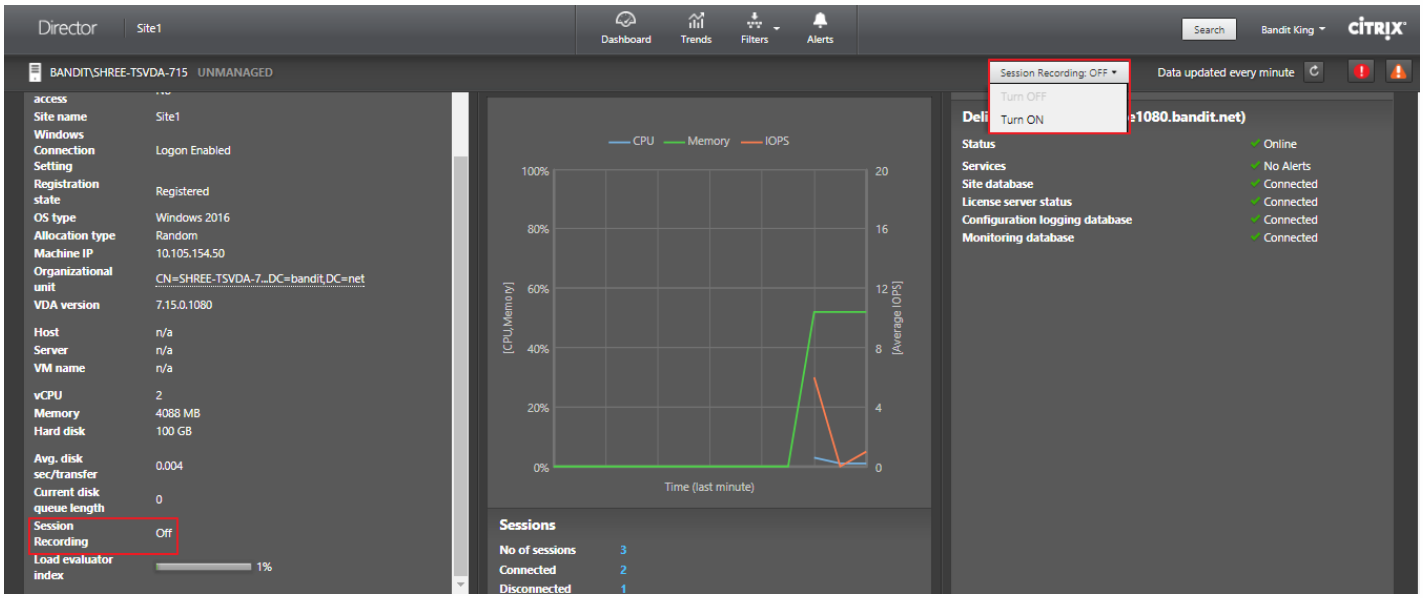
- Activar (con notificación). Se notifica al usuario de que la sesión se está grabando cuando este inicia una sesión ICA.
- Activar (sin notificación). La sesión se graba de forma silenciosa, sin notificar al usuario.
- Desactivar. Inhabilitar la grabación de las sesiones del usuario.

El nombre de la directiva activa de Grabación de sesiones aparece en el panel Directivas.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Solución de problemas de aplicaciones

Dec 05, 2017

Supervisión de aplicaciones en tiempo real

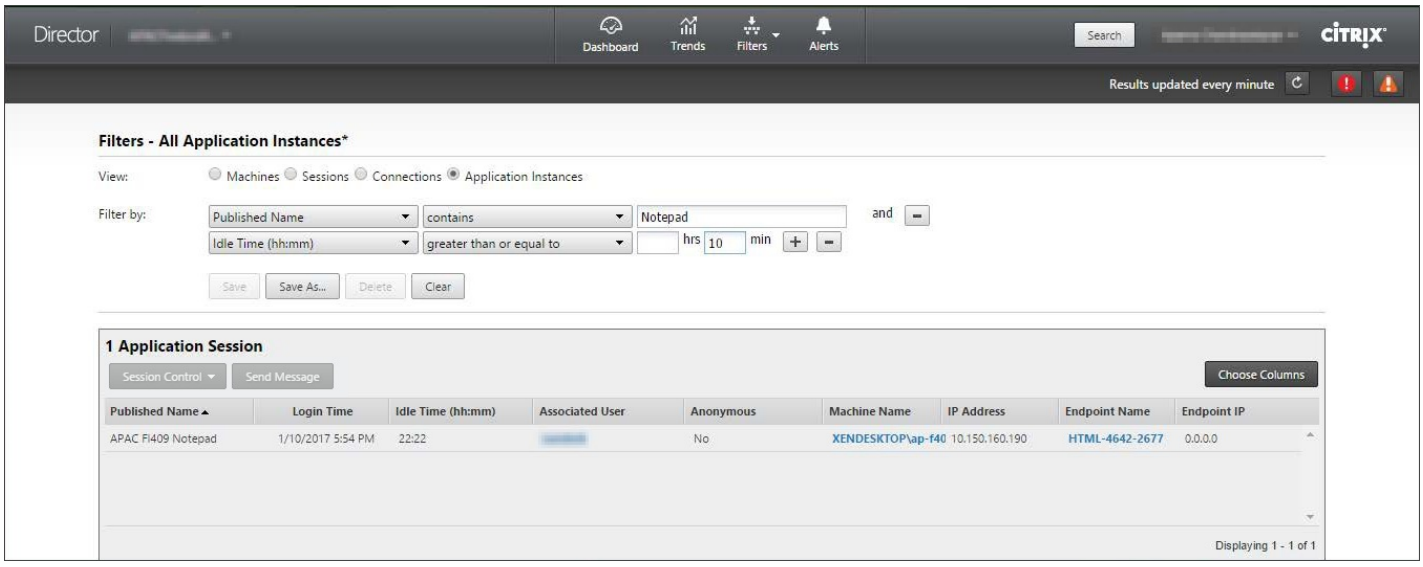
Puede solucionar las aplicaciones y las sesiones con la ayuda de métricas de inactividad para identificar las instancias que llevan inactivas más de un límite de tiempo concreto.

Los casos típicos donde solucionar problemas de aplicaciones pertenecen al sector de la asistencia médica, donde los empleados comparten licencias de aplicación. Allí, debe terminar las sesiones inactivas y las instancias de aplicaciones inactivas para purgar el entorno de XenApp y XenDesktop, 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.

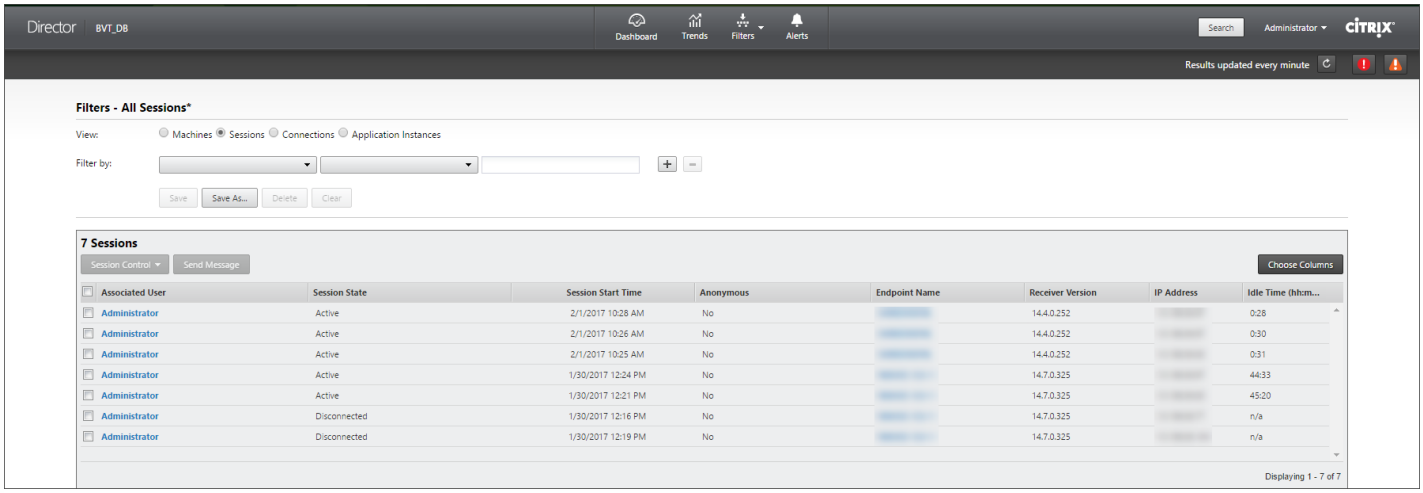


A continuación, se ofrece un filtro de ejemplo. Como criterio **Filtrar por**, elija **Nombre publicado** (de la aplicación) y **Tiempo de inactividad**. A continuación, establezca **Tiempo de inactividad** en **mayor o igual que** un límite de tiempo concreto y guarde el filtro si quiere volver a utilizarlo 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 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.

Supervisión de fallos históricos de aplicaciones

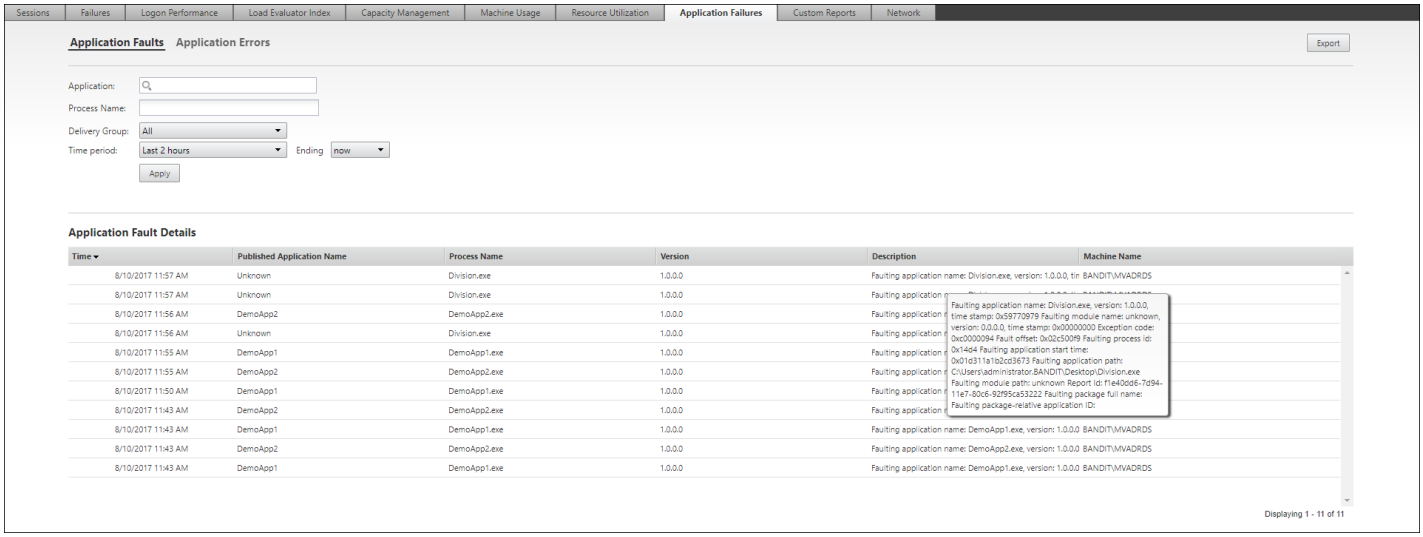
La ficha **Tendencias** > **Fallos y errores de aplicación** muestra los fallos asociados a las aplicaciones publicadas en los VDA.

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 Platinum y Enterprise. 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 Platinum. Puede cambiar este parámetro mediante el comando de PowerShell:

Set-MonitorConfiguration -

© 1999-2017 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 derivar el nombre de la aplicación correspondiente. Esto ocurre normalmente cuando falla una aplicación iniciada en una sesión de escritorio, o bien cuando falla debido a una excepción no controlada ocasionada por un archivo ejecutable de dependencia.

De forma predeterminada, se supervisan solo los fallos de las aplicaciones alojadas en agentes VDA de SO 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 la supervisión de fallos de aplicación en "Configuraciones de directiva de Supervisión".

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Solución de problemas de máquinas

Dec 05, 2017

En la vista **Filtros > Máquinas**, seleccione **Máquinas con SO de escritorio** o **Máquinas con SO de servidor** para ver las máquinas configuradas en el sitio. La ficha "Máquinas con 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.

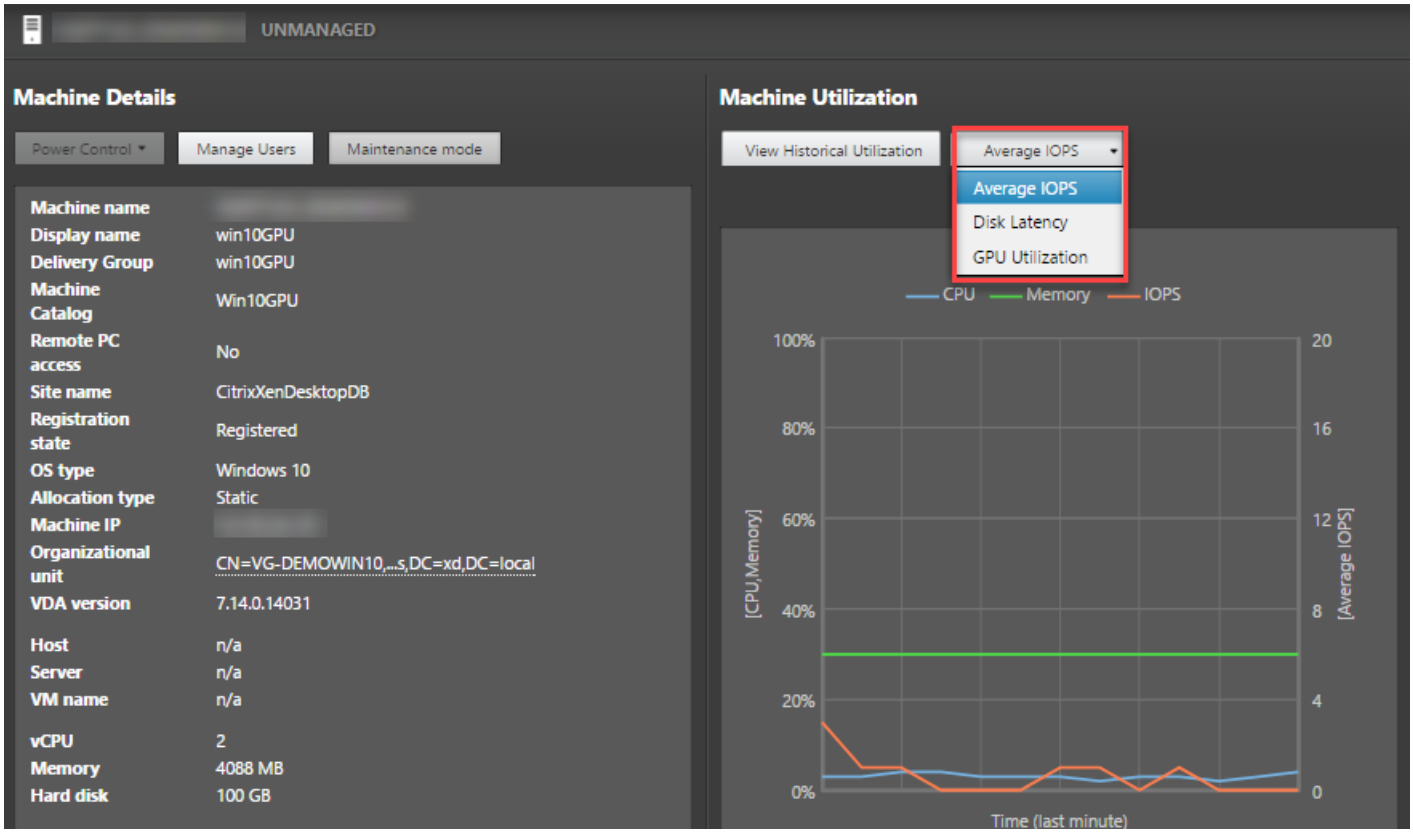
Haga clic en **Motivo del fallo** de la máquina donde se ha producido el error para obtener una descripción detallada del error y las acciones recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para errores de máquinas y conexiones están disponibles en Citrix Director 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. El panel **Utilización de máquinas** muestra gráficos sobre el uso de las máquinas.

Uso de 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 con supervisión de disco y 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

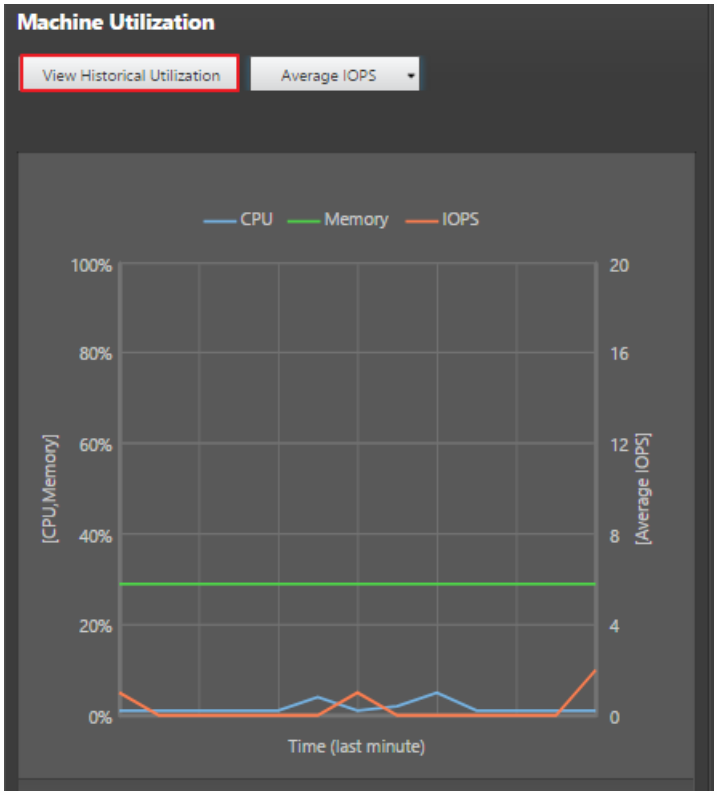
Seleccione **Utilización de GPU** para ver, en porcentajes, el uso de la GPU, la memoria de la GPU y del codificador y el decodificador para solucionar problemas relacionados con la GPU en los agentes VDA de SO de escritorio o servidor. Los gráficos de uso de la GPU están únicamente disponibles para 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.

Uso de recursos histórico en cada máquina

En el panel **Utilización de máquinas**, haga clic en **Ver utilización histórica** para ver el historial del uso de los recursos en la máquina seleccionada.
Los gráficos de utilización contienen contadores de rendimiento de la CPU, la memoria, el pico de sesiones simultáneas, el promedio de IOPS y la latencia de disco.

Nota: La configuración de la directiva de supervisión **Habilitar supervisión de procesos** debe estar establecida en "Permitida" para recopilar y mostrar datos en la tabla "10 procesos principales" de la página "Utilización histórica de máquinas". La recopilación de datos está inhabilitada de forma predeterminada.

De forma predeterminada, se recopilan los datos referentes al uso de la CPU, la memoria, el promedio de IOPS y la latencia de disco. Puede inhabilitar la recopilación mediante el parámetro de directiva **Habilitar supervisión de recursos**.



1. En el panel **Utilización de máquinas** de la vista **Detalles de la máquina**, seleccione **Ver utilización histórica**.Se abrirá

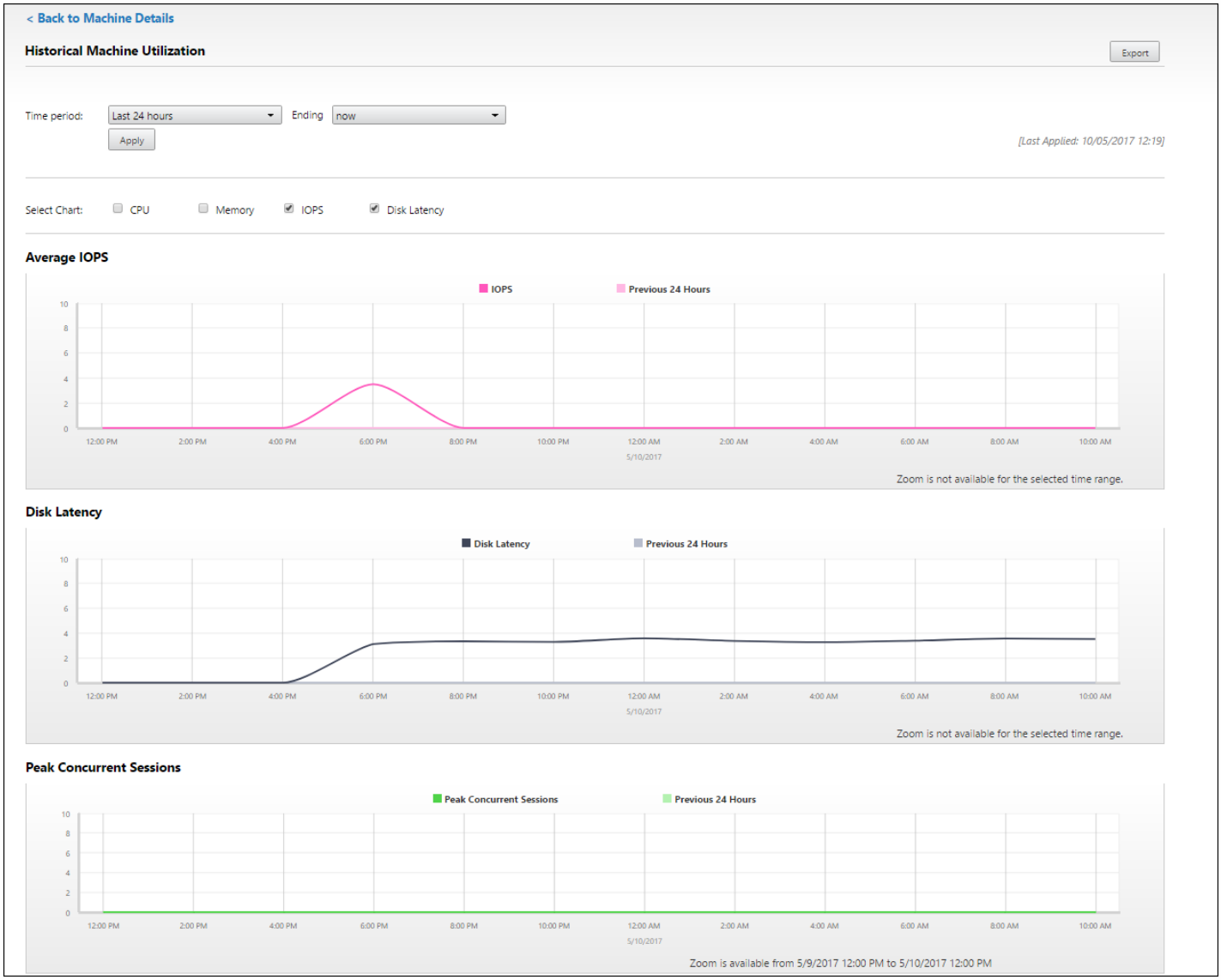
© 1999-2017 Citrix Systems, Inc. All rights reserved.

una nueva página: **Utilización histórica de máquinas**.

2. Establezca el **período de tiempo** para ver las últimas 2 horas, 24 horas, 7 días, o bien el último mes o año.
Nota: Los datos de uso del promedio de IOPS y la latencia de disco están disponibles solamente para las últimas 24 horas, el último mes y el último año contando hasta el momento actual. No se admite establecer un tiempo de finalización personalizado.

3. Haga clic en **Aplicar** y seleccione los gráficos necesarios.

4. Pase el cursor sobre las diferentes secciones del gráfico para ver más información sobre un período de tiempo seleccionado.



Por ejemplo, si selecciona **Últimas 2 horas**, el período de referencia será de 2 horas antes del intervalo de tiempo seleccionado. Verá las tendencias de uso de la CPU, la memoria y la sesión entre las últimas 2 horas y el punto de referencia. Si selecciona **Último mes**, el período de referencia será el mes anterior. Seleccione esta opción para ver la latencia de disco y el promedio de IOPS entre el último mes y el punto de referencia.

5. Haga clic en **Exportar** para exportar los datos de utilización de recursos durante el período seleccionado. Para obtener

© 1999-2017 Citrix Systems, Inc. All rights reserved.

más información, consulte la sección Exportar informes en Supervisión de implementaciones.

6. 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.

7. Para ver la tendencia histórica en el consumo de recursos de un proceso concreto, consulte los detalles de cualquiera de los diez procesos principales.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Matriz de compatibilidad de características

Dec 05, 2017

En cada sitio, aunque se pueden usar las versiones anteriores de VDA o Delivery Controller, es posible que no estén disponibles todas las funcionalidades de la versión más reciente de Director si las utiliza. Además, la disponibilidad de las funciones depende de la edición de la licencia del sitio.Citrix recomienda tener la misma versión de Director, el Delivery Controller y el 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 Actualización de una implementación.

La siguiente tabla contiene las características de Director y la versión mínima de Delivery Controller (DC), el VDA y los demás componentes dependientes requeridos, junto con la edición de las licencias.

Versión de Director	Característica	Dependencias: versión mínima requerida	Edición
7.15	Supervisión de fallos de aplicaciones	DC 7.15 || VDA 7.15	Todas
7.14	Solución de problemas centrada en las aplicaciones	DC 7.13 || VDA 7.13	Todas
	Supervisión de discos	DC 7.14 || VDA 7.14	Todas
	Supervisión de GPU		
7.13	Solución de problemas centrada en las aplicaciones	DC 7.13 || VDA 7.13	Platinum
	Protocolo de transporte en el panel Detalles de la sesión	DC 7.x || VDA 7.13	Todas
7.12	Descripciones claras de los errores de conexión y de máquina	DC 7.12 || VDA 7.x	Todas
	Mayor disponibilidad de datos históricos en la edición Enterprise		Enterprise
	Informes personalizados		Platinum
	Automatización de notificaciones de		Platinum

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Director con capturas de SNMP		
7.11	Informes de utilización de recursos	DC 7.11 || VDA 7.11	Todas
	Alertas extendidas para condiciones de CPU, memoria y RTT de ICA		Platinum
	Mejoras en la exportación de informes	DC 7.11 || VDA 7.x	Todas
	Automatización de las notificaciones de Director con Citrix Octoblu		Platinum
	Integración con NetScaler MAS	DC 7.11 || VDA 7.x || MAS versión 11.1 compilación 49.16	Platinum
7.9	Desglose de duraciones de inicios de sesión	DC 7.9 || VDA 7.x	Todas
7.7	Supervisión y alertas automáticas	DC 7.7 || VDA 7.x	Platinum
	Integración de SCOM	DC 7.7 || VDA 7.x || SCOM 2012 R2 || PowerShell 3.0 o posterior*	Platinum
	Integración con la autenticación de Windows	DC 7.x || VDA 7.x	Todas
	Uso de SO de escritorio y servidor	DC 7.7 || VDA 7.x	Platinum
7.6.300	Respaldo para canal virtual Framehawk	DC 7.6 || VDA 7.6	Todas
7.6.200	Integración con Grabación de sesiones	DC 7.6 || VDA 7.x	Platinum
7	Integración con HDX Insight	DC 7.6 || VDA 7.x || NetScaler Insight Center	Platinum

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Granularidad y retención de datos

Apr 24, 2018

Agregación de los 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 de mediciones 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.

Evaluación de 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.

Correlación de las tablas de resumen con los datos sin procesar

El modelo de datos representa las métricas de dos maneras diferentes:

- Las tablas de resumen representan vistas agregadas de las mediciones por minuto, por hora y por día .
- Los datos sin procesar representan eventos individuales o estados actuales rastreados en 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 mediciones están diseñados para satisfacer las necesidades de tendencias históricas en períodos de tiempo prolongados. Estas mediciones se agregan a 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), 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 mediciones 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 mediciones agregadas en tablas de resumen pueden ser ligeramente inexactas si hay eventos perdidos o latentes en el período de agregación. Aunque Monitor Service intenta mantener un alto nivel de precisión del estado actual, no vuelve atrás en el tiempo para recalcular la agregación en las tablas de resumen para eventos perdidos o latentes .
- **Alta disponibilidad de conexiones .** Durante la alta disponibilidad de conexiones (HA), habrá huecos en los recuentos de conexiones actuales en los datos de resumen, pero las instancias de sesión seguirán ejecutándose en los datos sin procesar.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Períodos de retención de datos.** Los datos de las tablas de resumen se conservan en una programación de limpieza distinta de la programación para datos de eventos sin procesar. Puede que falten datos porque se hayan limpiado las tablas de resumen y de datos sin procesar. Los períodos de retención también pueden diferir según las distintas granularidades de los datos de resumen. Una granularidad de datos menor (minutos) se limpia más rápidamente que una granularidad de datos mayor (días). Si faltan datos de una granularidad debido a una limpieza, puede que los 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 mediciones 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 de datos

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 Platinum 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:

comando COPIAR

```
asnp Citrix.*

Get-MonitorConfiguration

Set-MonitorConfiguration -<setting name> <value>
```

Los parámetros siguientes se usan para controlar la limpieza:

	Nombre del parámetro	Limpieza afectada	Valor predeterminado Platinum (días)	Valor predeterminado sin Platinum (días)
1	GroomSessionsRetentionDays	Retención de registros de conexión y de sesión	90	7

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		después de cerrar la sesión		
2	GroomFailuresRetentionDays	Registros de MachineFailureLog y ConnectionFailureLog	90	7
3	GroomLoadIndexesRetentionDays	Registros de LoadIndex	90	7
4	GroomDeletedRetentionDays	Entidades de catálogo de máquinas, grupo de escritorios e hipervisor cuyo estado de ciclo de vida (LifecycleState) es 'Eliminado' (Deleted). Esta acción también elimina los registros de Session, SessionDetail, Summary, Failure o LoadIndex relacionados.	90	7
5	GroomSummariesRetentionDays	Registros de DesktopGroupSummary, FailureLogSummary y LoadIndexSummary. Datos agregados, de granularidad diaria.	90	7
6	GroomMachineHotfixLogRetentionDays	Revisiones hotfix aplicadas a las máquinas de VDA y Controllers	90	90
7	GroomMinuteRetentionDays	Datos agregados: granularidad de minuto	3	3
8	GroomHourlyRetentionDays	Datos agregados: granularidad horaria	32	7
3082	GroomApplicationInstanceRetentionDays	Historial de instancia de aplicación	90	0
10	GroomNotificationLogRetentionDays	Registros del registro de notificaciones	90	
11	GroomResourceUsageRawDataRetentionDays	Datos de utilización de	1	1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		recursos: datos sin procesar		
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
35	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
18	GroomProcessUsageDayDataRetentionDays	Datos de utilización de procesos: granularidad de día	30	7
19	GroomSessionMetricsDataRetentionDays	Datos de métricas de sesiones	7	7
20	GroomMachineMetricDataRetentionDays	Datos de métricas de máquinas	3	3
21	GroomMachineMetricDaySummaryDataRetentionDays	Datos resumidos de métricas de máquinas	90	7
22	GroomApplicationErrorsRetentionDays	Datos de errores de aplicaciones	1	1
23	GroomApplicationFaultsRetentionDays	Datos de fallos de aplicaciones	1	1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Precaución: La modificación de los valores de 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 la limpieza de datos:

- Sitios con licencias Platinum: se puede actualizar la configuración de retención de limpieza de datos con cualquier cantidad de días.
  - Excepción: GroomApplicationErrorsRetentionDays y GroomApplicationFaultsRetentionDays se limitan a 31 días.
- Sitios con licencias Enterprise: la retención de limpieza de datos para todos los parámetros se limita a 31 días.
- Todo los demás sitios: la retención de limpieza de datos para todos los parámetros se limita a 7 días.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SDK y API

Dec 05, 2017

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 XenApp y XenDesktop. Consulte la siguiente sección Group Policy SDK para obtener más información.

Delivery Controller SDK

El SDK se compone de una serie de complementos de PowerShell que se instalan automáticamente mediante el asistente de instalación al instalar el Delivery Controller o el componente de 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 XenApp o XenDesktop, Citrix recomienda crear administradores Citrix con los derechos adecuados para un funcionamiento normal, en lugar de usar la cuenta de administradores locales. Si está en Windows Server 2008 R2, debe ejecutar el shell o el script como administrador Citrix, no como miembro del grupo de administradores locales.

Para acceder a los cmdlets y ejecutarlos:

1. Inicie un shell en PowerShell 3.0: 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 cmdlet **Add -PSSnapin** en la consola de Windows PowerShell.

   V1 y V2 indican la versión del complemento (los complementos de XenDesktop 5 son la versión 1; los de XenDesktop 7 son la versión 2). Por ejemplo, para instalar los complementos de XenDesktop 7, 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.

NOTA: Para ver la ayuda de los cmdlets de PowerShell para XenApp y XenDesktop actuales:

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 Windows PowerShell.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Group Policy SDK

Para utilizar Group Policy SDK, es necesario tener instalado Studio o el SDK de XenApp y XenDesktop.

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 <*cadena*>,** donde la cadena de Controller es el nombre de dominio completo de un Controller en el sitio al que quiere conectarse y del que quiere cargar la configuración.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Prácticas recomendadas de Citrix VDI para XenApp y XenDesktop 7.15 LTSR

Jan 19, 2018

PDF Citrix VDI Handbook and Best Practices

In traditional business environments, workers suffer from productivity loss in many ways, including downtime during PC refreshes, patches and updates, or simply when they are away from the office. Application and desktop virtualization centralizes apps and desktops in the datacenter, rather than on local devices. This allows IT to deliver apps and desktops to users on demand, to any device, anywhere.

Take the following response from a desktop virtualization user:

Experience from the Field

"As a remote employee for [company], I struggled every time I needed to access the company's intranet, which forced me to VPN into the network. I also kept data on my local device because trying to access it over my broadband connection was too slow. Some coworkers did the same and lost data due to a virus, thankfully I was luckier.

Depending on my mood (and the weather), changing devices and locations was a challenge as I had to have my applications and data copied to many different endpoints. I know this was unsecure, but I didn't care because I was more concerned with flexibility.

Since moving to a virtual desktop, I'm able to use any device. I'm able to work from any location. And best of all, I don't have to worry about copying my data and applications onto all of my personal devices."

Unfortunately, organizations sometimes struggle to achieve this level of success. Why does one organization succeed while another organization struggles?

If we compare the factors between success and failure between desktop virtualization and other technology related projects, we see that there is little difference:

Lack of justification – Without a solid business reason, desktop virtualization is simply a new way to deliver a desktop. A business justification gives the project team a goal to strive towards.

Lack of a methodology – Many people who try and struggle to deploy a desktop virtualization solution do so because they jump right in without understanding or implementing the appropriate prerequisites. A structured methodology provides the path for the project.

Lack of experience – For many who embark on a desktop virtualization project, there is a lack of experience, which creates a lack of confidence in the design. Architects begin to second-guess themselves and the project stalls.

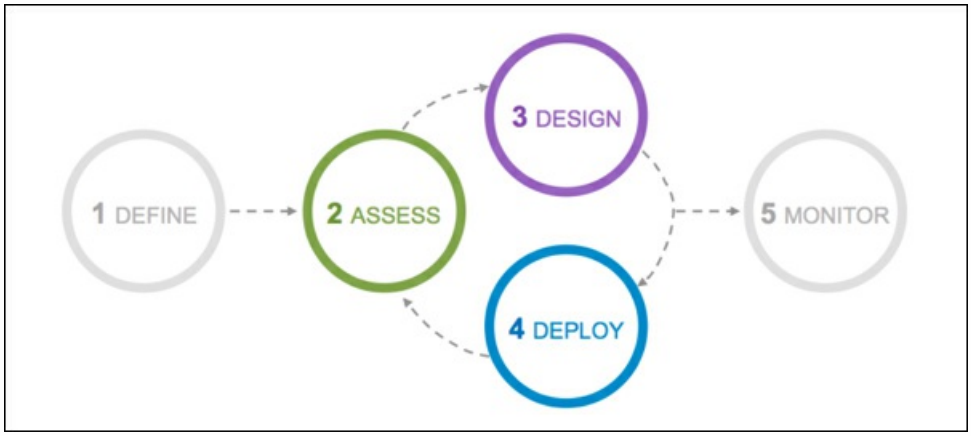
Our hope is that this handbook can alleviate the anxiety associated with desktop virtualization by showing how challenges can be resolved in a manner that is technically sound, but also feasible and effective for organizations facing deadlines and other organizational challenges.

Citrix has successfully employed the methodology, experience and best practices shared within this handbook across thousands of desktop virtualization projects.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Methodology

The Citrix VDI Handbook follows the Citrix Consulting methodology. A proven methodology that has been successfully employed across thousands of desktop virtualization projects. Each phase includes guidance on the important questions to ask, what tools to use and tips to help you succeed. The Citrix Consulting methodology consists of five phases:



1. Define – Builds the business case for desktop virtualization by creating a high-level project roadmap, prioritizing activities and estimating storage and hardware requirements.

2. Assess – Key business drivers are rated so that work effort can be prioritized accordingly. In addition, the current environment is reviewed for potential problems and to identify use cases for the project. This information will be used to set the direction of the Citrix deployment, upgrade, or expansion.

3. Design – Define architecture required to satisfy key business drivers and success criteria identified during the assess phase. Topics such as environment scalability, redundancy and high availability are addressed.

4. Deploy – During the deploy phase, the infrastructure is installed and configured as described in the design phase. All components of the infrastructure should be thoroughly unit and regression tested before users are provided with access to the environment.

5. Monitor – Define architectural and operational processes required to maintain the production environment.

The Citrix Consulting methodology follows an iterative Assess > Design > Deploy process for each major initiative of your project. In doing so, your organization is left with tangible improvements to the environment at the end of each engagement. For example, high priority user groups can progress through the assess, design and deploy phases earlier than other user groups.

> ### Nota
>
> The VDI Handbook provides content on the Assess, Design and Monitor phases of the Citrix Consulting methodology.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

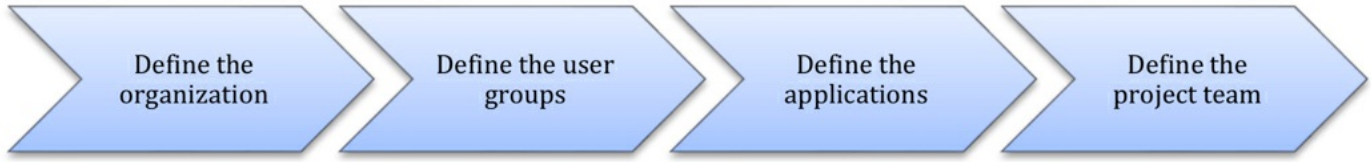
Assess

Jan 29, 2018

Creating an app and desktop delivery solution begins with a proper assessment. Architects that fail to properly assess the current environment find that they require the assess information later on, forcing them to backtrack, which can potentially stall and put the project at risk.

By gathering all of the information from the outset, the architect will gain an appreciation for the current environment and be able to work from the beginning on properly aligning business and user requirements with the overall solution.

The assess phase is a four-step, simple to follow process:



Step 1: Define the Organization

The first step in your virtual desktop project should be to understand and prioritize the strategic imperatives of the organization. This enables the project management team to define success criteria and allows the design team to create a tailored and optimized architecture.

Requirements can be captured during meetings or by distributing questionnaires. Meetings are more time consuming, but allow for follow-up questions to be asked and help to simplify the prioritization process. It is important that this exercise be completed jointly by both business managers and IT decision makers since both groups will have significantly different viewpoints.

Take the following examples of what certain organizations faced, which drove their selection of desktop virtualization.

Experience from the Field

- Finance – A large financial institution had a base of operations in the city designated as the host city for an upcoming G8 summit. As these types of meetings historically include riots, protests and other issues that can disrupt business and the safety of their employees, the financial organization needed an alternative allowing their users to work from the safety of their homes.
- Agriculture – Due to thin margins, an agriculture organization wanted to save money by extending the life of desktop PCs while still being able to run the latest applications.
- Healthcare – A large healthcare organization was in need of a solution to simplify application updates as the main application required updates on a weekly basis. Due to the distributed nature of the endpoint devices, the organization was in need of a better application delivery solution.

These are just a few examples, but they demonstrate how organizations think about their priorities. Most organizations do not focus on technology, they focus on the needs of the user and of the organization. These needs can be met with technical solutions but it is imperative the team understands the “Why” of the project.

In addition to the three real-world examples, the following table identifies a few other priorities often stated from many

© 1999-2017 Citrix Systems, Inc. All rights reserved.

organizations:

Requester	Requirement
Business Managers	**Better IT agility and responsiveness** – Flexible desktop solution that is capable of accommodating periods of change such as rapid growth or downsizing. For example, enabling the business to setup project offices or temporary points of sale very rapidly without long delays, hardware acquisitions or IT notification periods. **Bring your own device** – Empower employees to choose their own devices to improve productivity, collaboration and mobility. **Collaboration** – With an increase in both globalization and mobility, team members are often dispersed across multiple physical locations. Powerful collaboration capabilities are required to ensure high levels of productivity, efficiency and quality. **Work from anywhere** – The business needs to support home workers in order to attract and retain top talent, and / or travelling employees
IT decision makers	**Better desktop management** – Simplify the management of desktop infrastructure. IT is not as proactive as they would like and spend too much time "fighting fires". **Increase security** – Data theft or the loss of devices containing sensitive data is a big risk and preventive measures are a top priority. **Extend desktop hardware lifecycle** – Replacing workstations every three to five years in order to keep up with the requirements of the operating system or the applications has been very costly. **Reducing IT Management Scope** – Improve IT efficiency by focusing on only the aspects driving the business while offloading remaining functions to 3rd parties via cloud or service providers. **Improving user experience** - Increasing performance or enabling features which would otherwise not be possible with a geographically dispersed user population

The prioritization process should be completed in collaboration with the project team, business managers and IT managers so that all views are considered.

Step 2: Define the User Groups

Although there are multiple approaches towards defining user groups, it is often easiest to align user groups with departments as most users within the same department or organizational unit consumes the same set of applications.

User Segmentation

Depending on the size of the department, there might be a subset of users with unique requirements. Each defined user group should be evaluated against the following criteria to determine if the departmental user group needs to be further divided into more specialized user groups.

- Primary datacenter – Each user will have a primary datacenter or cloud resource location assigned that will be used to host their virtual desktop, data, and application servers. Identify the datacenter that the user should be assigned to rather than the datacenter they are currently using. Users will be grouped based on their primary datacenter so that a unique design can be created for each one.
- Personalization – Personalization requirements are used to help determine the appropriate VDI model for each user group. For example, if a user group requires complete personalization, a personal desktop will be recommended as the optimal solution. There are three classifications available:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personalization	Requirement
None	User cannot modify any user or application settings, for example - kiosk.
Basic	User can modify user-level settings of desktops and applications.
Complete	User can make any change, including installing applications.

- Security – Security requirements are used to help determine the appropriate desktop and policy (or policies) for each user group. For example, if a user group requires high security, a hosted pooled desktop or a local VM desktop will be recommended as the optimal solution. There are three classifications available:

Security level	Description
Low	Users are allowed to transfer data in and out of the virtualized environment.
Medium	All authentication and session traffic should be secured; users should not be able to install or modify their virtualized environment.
High	In addition to traffic encryption, no data should leave the data center (such as through printing or copy/paste); all user access to the environment should be audited.

- Mobility – Mobility requirements are used to help determine the appropriate desktop model for each user group. For example, if a user group faces intermittent network connectivity, then any VDI model requiring an active network connection is not applicable. There are four classifications available:

Mobility	Requirement
Local	Always uses the same device, connected to an internal, high-speed and secured network.
Roaming Local	Connects from different locations on an internal, high-speed, secured network.
Remote	Sometimes connects from external variable-speed, unsecure networks.
Mobile	Often needs access when the network is intermittent or unavailable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Desktop Loss Criticality – Desktop loss criticality is used to determine the level of high availability, load balancing and fault tolerance measures required. For example, if there is a high risk to the business if the user's resource is not available, the user should not be allocated a local desktop because if that local desktop fails, the user will not be able to access their resources. There are three classifications available:

Desktop loss criticality	Requirement
Low	No major risk to products, projects or revenue.
Medium	Potential risk to products, projects or revenue.
High	Severe risk to products, projects or revenue.

- Workload – Types and number of applications accessed by the user impacts overall density and the appropriate VDI model. Users requiring high-quality graphics will either need to utilize a local desktop implementation or a professional graphics desktop. There are three classifications available:

User type	Characteristics
Light	1-2 office productivity apps or kiosk.
Medium	2-10 office productivity apps with light multimedia use.
Heavy	Intense multimedia, data processing or application development.

> ## Nota
>
> Performance thresholds are not identified based on processor, memory or disk utilization because these characteristics will change dramatically following the application rationalization and desktop optimization process. In addition, it is likely that the user's management tools and operating system will change during the migration process. Instead, workload is gauged based on the number and type of applications the user runs.

Experience from the Field

- Utility company – A large utility company collected data on every user in their organization. During the user segmentation process, it was realized that the organization's existing role definitions were sufficiently well defined that all the users within a role shared the same requirements. This allowed a significant amount of time to be saved by reviewing a select number of users per group.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Government – A government organization discovered that there was significant deviation between user requirements within each role, particularly around security and desktop loss criticality. As such, each user needed to be carefully reviewed to ensure that they were grouped appropriately.

Assign VDI Models

As with physical desktops, it is not possible to meet every user requirement with a single type of VDI. Different types of users need different types of resources. Some users may require simplicity and standardization, while others may require high levels of performance and personalization. Implementing a single VDI model across an entire organization will inevitably lead to user frustration and reduced productivity.

Citrix offers a complete set of VDI technologies that have been combined into a single integrated solution. Because each model has different strengths, it is important that the right model is chosen for each user group within the organization.

The following list provides a brief explanation of each VDI model.

- Hosted Apps – The hosted apps model delivers only the application interface to the user. This approach provides a seamless way for organizations to deliver a centrally managed and hosted application into the user's local PC. The Hosted Apps model is often utilized when organizations must simplify management of a few line-of-business applications. Hosted apps includes a few variants:
  - Windows Apps – The Windows apps model utilizes a server-based Windows operating system, resulting in a many users accessing a single VM model.
  - VM Hosted Apps – The VM hosted apps model utilizes a desktop-based Windows operating system, resulting in a single user accessing a single VM model. This model is often used to overcome application compatibility challenges with a multi-user operating system, like Windows 2008, Windows 2012 and Windows 2016.
  - Linux Apps – The Linux apps model utilizes a server-based Windows operating system, resulting in a many users accessing a single VM model.
  - Browser Apps – The browser apps model utilizes a server-based Windows operating system to deliver an app as a tab within the user's local, preferred browser. This approach provides a seamless way for organizations to overcome browser compatibility challenges when users want to use their preferred browser (Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, etc.) but the web application is only compatible with a specific browser.
- Shared Desktop – With the shared desktop model, multiple user desktops are hosted from a single, server-based operating system (Windows 2008, 2012, 2016, Red Hat, SUSE, CentOS and Ubuntu). The shared desktop model provides a low-cost, high-density solution; however, applications must be compatible with a multi-user server based operating system. In addition, because multiple users share a single operating system instance, users are restricted from performing actions that negatively impact other users, for example installing applications, changing system settings and restarting the operating system.
- Pooled Desktop – The pooled desktop model provides each user with a random, temporary desktop operating system (Windows 7, Windows 8 and Windows 10). Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, pooled desktops remove the requirement that applications must be multi-user aware and support server based operating systems.
- Personal Desktop – The personal desktop model provides each user with a statically assigned, customizable, persistent desktop operating system (Windows 7, Windows 8, Windows 10, Red Hat, SUSE, CentOS and Ubuntu). Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, personal desktops remove the requirement that applications must be multi-user aware and support server based operating systems.
- Pro Graphics Desktop – The pro graphics desktop model provides each user with a hardwarebased graphics processing unit (GPU) allowing for higher-definition graphical content.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Local Streamed Desktop – The local streamed desktop model provides each user with a centrally managed desktop, running on local PC hardware.
- Local VM Desktop – The local VM desktop model provides each user with a centrally managed desktop, running on local PC hardware capable of functioning with no network connectivity.
- Remote PC Access – The remote PC access desktop model provides a user with secure remote access to their statically assigned, traditional PC. This is often the fastest and easiest VDI model to deploy as it utilizes already deployed desktop PCs.

Each user group should be compared against the following table to determine which VDI model best matches the overall user group requirements. In many environments, a single user might utilize a desktop VDI model and an app VDI model simultaneously.

In this table:

- Y indicates "Recommended"
- N indicates "Not Recommended"
- o indicates "Viable"

Segmentation Characteristic	Hosted Apps	Hosted Shared Desktop	Hosted Pooled Desktop	Hosted Personal Desktop	Hosted Pro Graphics Desktop	Local Streamed Desktop	Local VM Desktop	Remote PC Access
Workload								
Light	**Y**	**o**	**o**	**o**	**N**	**o**	**o**	**o**
Medium	**o**	**Y**	**Y**	**o**	**o**	**o**	**o**	**o**
Heavy	**N**	**N**	**N**	**o**	**Y**	**Y**	**Y**	**o**
Mobility								
Local	**Y**	**Y**	**Y**	**o**	**o**	**Y**	**o**	**o**
Roaming Local	**Y**	**Y**	**Y**	**o**	**o**	**N**	**o**	**o**
Remote	**Y**	**Y**	**Y**	**o**	**o**	**N**	**o**	**Y**
Mobile	**N**	**N**	**N**	**N**	**N**	**N**	**Y**	**N**
Personalization								

© 1999-2017 Citrix Systems, Inc. All rights reserved.

None	**Y**	**Y**	**Y**	**N**	**o**	**o**	**o**	**o**
Basic	**Y**	**Y**	**Y**	**N**	**o**	**o**	**o**	**o**
Complete	**N**	**N**	**N**	**Y**		**N**	**Y**	**Y**
Security								
Low	**o**	**o**	**o**	**o**	**o**	**o**	**o**	**o**
Medium	**Y**	**Y**	**Y**	**o**	**o**	**o**	**o**	**o**
High	**o**	**o**	**Y**	**N**	**o**	**Y**	**Y**	**N**
Desktop Loss Criticality								
Low	**o**	**o**	**o**	**o**	**o**	**o**	**o**	**o**
Medium	**Y**	**Y**	**Y**	**o**	**o**	**o**	**o**	**N**
High	**Y**	**Y**	**Y**	**N**	**o**	**o**	**N**	**N**

Don't forget to follow these top recommendations from Citrix Consulting based on years of experience:

Citrix Consulting Tips for Success

1. Start with Windows apps, shared and pooled desktops – As you can see in the VDI capability table above, the Windows apps, hosted shared and pooled desktop models can be used in the majority of situations. The local streamed and local VM desktop models should only be used on an exception basis. By reducing the number of VDI models required, you will help to reduce deployment time and simplify management.
2. Perfect match – It may not be possible to select a VDI model that is a perfect match for the user group. For example, you can't provide users with a desktop that is highly secure and offers complete personalization at the same time. In these situations, select the VDI model which is the closest match to the organization's highest priorities for the user group.
3. Desktop loss criticality – There are only three VDI models that meet the needs of a high desktop loss criticality user group (backup desktops available) – none of which allow for complete personalization. If a high-desktop loss criticality user group also requires the ability to personalize their desktop they could be provided with a pool of backup desktops (hosted shared, pooled) in addition to their primary desktop. Although these desktops would not include customizations made to their primary desktop, they would allow users to access core applications such as mail, Internet and Microsoft Office.
4. Consider Operations & Maintenance – The ongoing support of each VDI model should be factored in when deciding on a VDI model. For example, pooled desktops can be rebooted to a known good state which often leads to reduced

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

maintenance versus a personal desktop where each desktop is unique.

Step 3: Define the Applications

Once the users have been divided up in to groups the next step is to determine which applications they require. This is a two-step process:

1. Application rationalization – Help to simplify the application assessment by removing redundant applications from the inventory that were captured during the data capture.

2. Link apps to users – Use the results from the data capture process to map applications to user groups.

Application Rationalization

The number of applications identified during the inventory is often surprising, even for organizations that believe they have a high-level of control over applications. To help reduce complexity as well as overall time required, it's important to take the time to consolidate the list of applications. The following guidelines will help ensure that your application list is consolidated appropriately:

- Multiple versions – Different versions of the same application may have been identified during the inventory. There are various reasons for this, including an inconsistent patching or upgrade process, decentralized application management, limited licenses and situations where users require specific application versions for compatibility with other applications, macros and document formats. Where possible, work with the application owners to reduce the number of versions required. The leading practice is to standardize on a single version of each application, typically the latest.
- Non-business applications – Applications that are not required by the business should be removed from the application inventory to reduce resource requirements and to help simplify the overall project. Non-business related applications are typically found in an application inventory when users have been provided with the ability to install their own applications and typically include games, communication clients, screen savers, peripheral software and media players.
- Legacy applications – The inventory may identify legacy applications that have since been retired or that are no longer required within the business. These applications may not have been removed from the desktops because there is no established process to do so or because there are always more high-priority activities to complete. These applications should be consolidated during the rationalization stage of the application assessment.
- Management applications – The antivirus, application delivery, monitoring, inventory, maintenance and backup applications will be completely re-designed across the organization during the desktop virtualization project. These applications should also be consolidated during this stage.

Experience from the field:

Government: A government organization identified that there were 2,660 applications installed across their desktop estate. Most of which were installed by users with local administrative rights. By following the application rationalization recommendations above, it was possible to reduce the number of applications required to 160.

Application Categorization

Each application included in the project should be categorized based on certain criteria, which will help determine the most appropriate way to host and integrate the app. Each application can be installed directly into the image, virtualized in an isolated container and streamed to the desktop (Microsoft App-V), captured in a unique layer and attached to the virtual machine (Citrix App Layering) or installed locally on the user's endpoint device and seamlessly integrated into the user's virtual desktop (Citrix Local App Access). Due to the uniqueness of every application, many large-scale deployments simultaneously utilize multiple approaches. Each application should be categorized as follows:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Common Apps - Every organization includes a suite of applications utilized by almost every user, Microsoft Office for example. This suite of applications is often the most utilized application in a desktop VDI model.
- Departmental Apps - A certain set of applications are only relevant for a unique business unit or department. For example, an engineering department will often require software development applications.
- User Apps - Often making up the largest grouping of apps are the apps used by very few individual users. In a traditional PC implementation, these applications are installed by the user as a temporary requirement or a personal requirement, often not directly impacting the business.
- Management Apps – Many desktop deployments include a combination of antivirus, monitoring, inventory, maintenance and backup applications. Many of these applications have unique virtualization requirements and are often required across the entire organization.

Application Characterization

Workload	Requirement
Resource intensive	Application requires 1 GB or more of RAM or averages 50% or more CPU utilization.
None	The application is not resource intensive.

The following characteristics should be identified for each application so that the right application delivery model can be selected during the design phase of the project:

- Complex – An application should be classified as complex or technically challenging if it is difficult to set up, has extensive dependencies on other applications or requires a specialized configuration, for example an Electronic Medical Records (EMR) application. Complex applications need to be identified during the application assessment because they are not generally appropriate for installation in a pooled/personal desktop model or delivery by application streaming. Delivering complex applications as a hosted app often helps to reduce the complexity of the base desktop image.
- Demanding – Collecting application resource requirements allows the virtualization infrastructure to be sized and an appropriate application delivery model to be selected. For example, demanding or resource intensive applications will not be delivered via a pooled/personal desktop model because there is limited control over how the resources are shared between users. There are two classifications available in the user assessment worksheet:

- Mobile – Some user groups may require the ability to work while mobile, sometimes when offline. If so, it is important that the design can determine which applications will work without a network connection and which ones will not. Applications that require backend infrastructure such as web and database servers are not typically available offline.
- Peripherals – If applications require connectivity with peripheral devices, identify the interface required so that it can be made available to the application when it is run from a virtual session.
- Restrictions – Application access may need to be restricted due to insufficient licenses /resources and to protect sensitive data / tools. For example, applications with a limited number of licenses should not be installed on a base image that is shared with unlicensed users. There are three restricted access categories in the application assessment workbook:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restricted Access	Requirement
No	There are no restrictions for the application and it can be accessed by any user within the organization.
User Group	The application may be installed on a multi-user operating system but only a specific group of users should be provided with an icon.
Virtual machine	Application should only be installed on a virtual machine that is accessible by authorized users, often because of licensing requirements.

Step 4: Define the Project Team

Desktop virtualization is a fundamental change that requires close collaboration between various business and technical teams in order to be successful. For example, the virtualization and desktop teams need to work together to ensure that the virtual desktop image meets user needs while also being optimized for the datacenter. Failure to build a cohesive project team that consists of the right roles and skillsets can negatively impact performance, availability, user experience and supportability while also increasing costs and risk.

The following tables identify the business and technical roles required during an enterprise virtual desktop deployment. Although the list may seem quite large, many of these roles are only required for a short time and multiple roles may be performed by a single person. The project manager and Citrix architect are considered to be full time roles with other team members being brought in only when required. The project manager role is key to ensuring that the right people are involved in the project at the right time.

Business Roles

Role	Description	Example Responsibilities
Project sponsor	The project sponsor is a senior company executive who recognizes the benefits that desktop virtualization will bring to the business. The project sponsor role is often performed by the chief technology officer (CTO).	**Pre-project** • Promote desktop virtualization within business. • Identify members of the steering committee. **Secure funding** • Assess general costs associated with solution. • Identify and prioritize key business drivers.
		All steps • Define key project

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Project manager	The project manager directs the project team and is responsible for ensuring that project objectives are completed on time and within budget.	• Create and update project plan. • Track progress against plan. • Track expenditure against budget. • Maintain issue and risk register. • Manage scope changes. • Create weekly project reports. • Brief steering committee on progress. • Organize project workshops and meetings. • Ensure project teams are synchronized. • Ensure pre-requisites are in place. • Creates change control requests.
Business manager	Depending on company structure and size, business managers oversee planning and performance at a department, region or company level. A business manager understands the requirements necessary for their employees to be successful.	**Assess** • Assist with application consolidation project. • Provide details on connectivity requirements of user group, including offline usage. • Provide details on risk tolerance of user group. • Identify requirements for peripherals. **Deploy** • Promote benefits of desktop virtualization. • Assist with coordinating the rollout.
		Assess • Provide Citrix architect with detailed understanding of the current business

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Business continuity manager	The business continuity manager ensures that an organization can continue to function after a disruptive event such as natural disaster, crime or human/computer error.	**Design** • Update business continuity plan to incorporate the new Citrix infrastructure. **Deploy** • Test business continuity plan.
Test manager	The test manager is responsible for ensuring that the test and user acceptance environments match the production environment as closely as possible. The test manager helps to reduce risk by ensuring that changes are fully tested before being implemented in production.	**Assess** • Provide Citrix architect with detailed understanding of current testing infrastructure and processes. **Design** • Work with Citrix architect to design an appropriate testing infrastructure and test plan for new Citrix environment. **Deploy** • Ensure that testing design is implemented correctly and new Citrix infrastructure is fully tested before rollout.
Application owners	An application owner is a subject matter expert on specific applications deployed within the business. Application owners are responsible for ensuring that problems with the applications are resolved and that upgrades/updates are performed without issue. Application owners are also responsible for managing support agreements with the application vendors.	**Assess** • Assist with application consolidation project. • Identify application licensing limitations. • Provide details on security restrictions. • Provide details on application dependencies. • Provide location of backend resources. **Deploy** • Provide installation pre-requisites and install guide

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
		installing and testing applications in VDI environment
Service desk manager	The service desk manager helps to improve productivity and end-user satisfaction by ensuring that production issues are logged, escalated and resolved in a timely manner. The service desk manager is also responsible for reporting on common issues, call volumes and service desk performance.	**Assess** • Identify common issues with existing environment. • Provide details on support tools currently used. **Design** • Assist Citrix architect with designing a delegated administration model. • Participate in operations and support design workshops. • Work with training manager to identify training requirements. **Deploy** • Monitor helpdesk calls for rollout related issues.
Training manager	The training manager ensures that support staff and end-users are proficient with new areas of technology. The training manager also has responsibility for ensuring that the training plan is up-to-date and followed appropriately.	**Assess** • Determine current skill set for support staff and end users. **Design** • Create training plan for support staff and end users. **Deploy** • Implement training plan for support staff and end users.
		Design • Work with project manager to create communications plan. **Deploy**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
		• desktop virtualization. • Inform users of key migration dates. • Ensure expectations are set accordingly.

Technical Roles

Role	Description	Example Responsibilities
Citrix desktop architect	The Citrix architect acts as the design authority for all Citrix products and liaises with other architects to ensure that the Citrix infrastructure is successfully integrated into the organization.	**Assess** • Work with project sponsor and key stakeholders to identify and prioritize key business drivers. • Oversee user segmentation and app. assessment. • Map VDI models to user groups. • Perform capabilities assessment to determine current state of readiness. • Identify areas of risk and provides remedial actions. **Design** • Create Citrix design that includes hardware and storage estimates. • Coordinate with other architects to integrate Citrix infrastructure into organization. • Work with monitoring architect to ensure that Citrix environment is monitored appropriately. • Create operations and support design. • Create implementation and rollout design. • Create test plan **Deploy** • Ensure that the Citrix environment is implemented in accordance with design. • Verify that implementation passes test plan. • Ensure that the Citrix design is implemented correctly.
Archive directory architect	Design authority on Microsoft Active Directory, including Organizational Units (OU) and Group Policy Objects (GPOs).	**Assess** • Provide Citrix architect with detailed understanding of current Active Directory architecture. **Design** • Work with the Citrix architect to design OU structure, group policies, permissions, service accounts, etc. for new Citrix environment. • Update Active Directory infrastructure design to reflect centralization of user data and accounts. **Deploy**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		correctly.
Role	**Description**	**Example Responsibilities**
Visualization architect	Design authority on server and desktop virtualization using Citrix XenServer, Microsoft Hyper-V, Nutanix Acropolis or VMware vSphere.	**Assess** • Provide Citrix architect with detailed understanding of current virtualization architecture **Design** • Work with Citrix architect to design hardware, networking, storage, high availability, etc. for server and desktop virtualization • Work with monitoring architect to ensure that virtualization environment is monitored appropriately **Deploy** • Ensure that the virtualization design is implemented correctly
Network architect	Design authority on networking, including routing, VLANs, DHCP, DNS, VPN and firewalls.	**Assess** • Provide Citrix architect with detailed understanding of current networking architecture. **Design** • Work with Citrix architect to design physical network, virtual networks, routing, firewalls, quality of service, remote access, network optimization, etc. for new Citrix environment. • Work with monitoring architect to ensure that network is monitored appropriately. **Deploy** • Ensure that network design is implemented correctly.
Desktop architect	Design authority on Microsoft desktop operating systems, including Windows XP, Windows 7 and Windows 8.	**Assess** • Provide Citrix architect with detailed understanding of current desktop environment. **Design** • Work with Citrix architect to design core desktop virtual image, core applications, desktop optimizations, etc. for new Citrix environment. • Work with monitoring architect to ensure that the virtual desktops are monitored appropriately. **Deploy** • Ensure that desktop design is implemented correctly.
		Assess • Provide Citrix architect with detailed understanding of current shared storage environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Description	Example Responsibilities
Storage architect	Design authority on storage solutions, including directattached storage, storageattached networks and network attached storage.	• Work with Citrix architect to design storage architecture, tiers, sizing, connectivity, etc. for new Citrix environment. • Work with monitoring architect to ensure that storage is monitored appropriately. **Deploy** • Ensure that storage design is implemented correctly.
Backup architect	Design authority on backup and recovery, including virtual machines, desktops, servers, user data and databases.	**Assess** • Provide Citrix architect with detailed understanding of current backup architecture and processes **Design** • Work with Citrix architect and disaster recovery architect to design backup architecture, process, schedule, retention, etc. for new Citrix environment **Deploy** • Ensure that backup design is implemented correctly
Application package architect	Design authority on packaging applications for deployment via the systems management team	**Assess** • Provide Citrix architect with detailed understanding of current application packaging process and status **Deploy** • Ensure that all required applications are packaged according to design
Monitoring architect	Design authority on monitoring, including hardware, network, servers, storage and security appliances.	**Assess** • Provide Citrix architect with detailed understanding of current monitoring architecture and processes. **Design** • Work with Citrix architect to design monitoring architecture, metrics, alerts, etc. for new Citrix environment and supporting infrastructure. **Deploy** • Ensure that monitoring design is implemented correctly. • Provide regular reports on capacity and trends during rollout .
System management	Design authority on systems management, including server/desktop build process, patching and automated	**Assess** • Provide Citrix architect with a detailed understanding of the current systems management processes. **Design** • Works with Citrix architect to define server/desktop build process, patching and application delivery

© 1999-2017 Citrix Systems, Inc. All rights reserved.

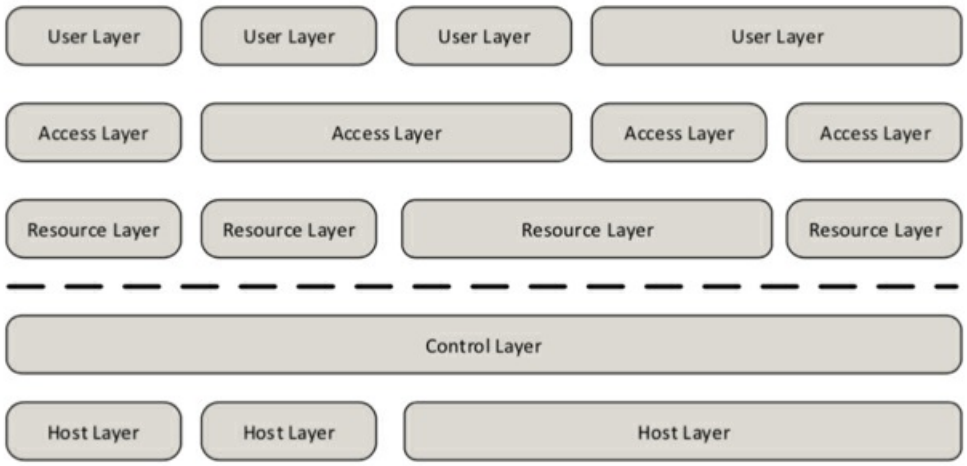
Role	Description	Example Responsibilities
		Deploy • Ensure that the systems management design is implemented correctly.
Security architect	Design authority on security, including desktops, servers, networks and VPNs.	**Assess** • Provide Citrix architect with detailed understanding of current security policy. **Design** • Work with Citrix architect to design security standards for new Citrix environment, including authentication, encryption, port numbers, firewall rules, etc. **Deploy** • Ensure that security design is implemented correctly.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design

Jan 30, 2018

Designing a desktop virtualization solution is simply a matter of following a proven process and aligning technical decisions with organizational and user requirements. Without the standardized and proven process, architects tend to randomly jump from topic to topic, which leads to confusion and mistakes. The recommended approach focuses on working through five distinct layers:



The top three layers are designed for each user group independently, which were identified during the user segmentation section of the assess phase. These layers define the users' resources and how users access their resources. Upon completion of these three layers, the foundational layers (control and hardware) are designed for the entire solution.

This process guides the design thinking in that decisions made higher up impact lower level design decisions.

Layer 0: Conceptual Architecture

The conceptual architecture helps define the overarching strategies for the entire solution based on business objectives and organizational structure.

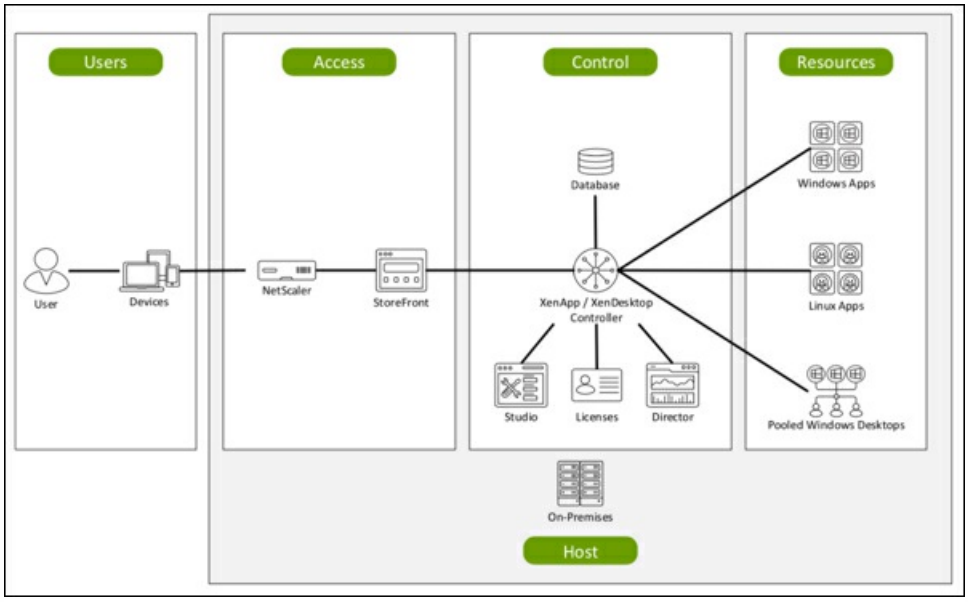
Although an organization's conceptual architecture will change over the coming years, it is worthwhile to start the design phase by defining the long-term objectives around delivery models and the physical, geographical distribution of solution.

Decision: Delivery Model

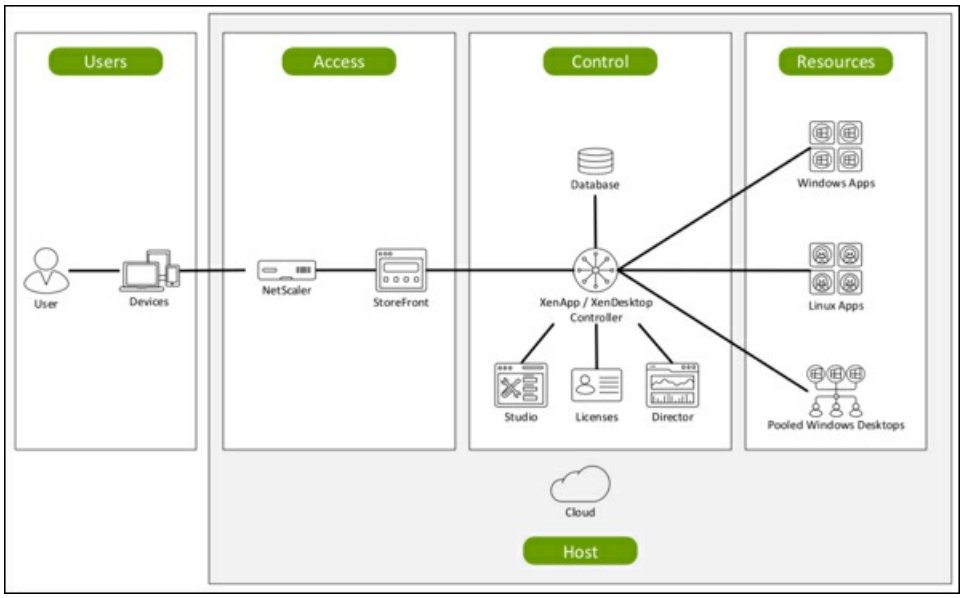
A XenDesktop and XenApp solution can take on many delivery forms. The organization's business objectives help select the right approach. Even though the infrastructure remains the same for all delivery models, the local IT team's management scope changes.

- **On Premises** - All components hosted from the organization's local data center. The onpremises model requires the local IT team to manage every aspect of the solution.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

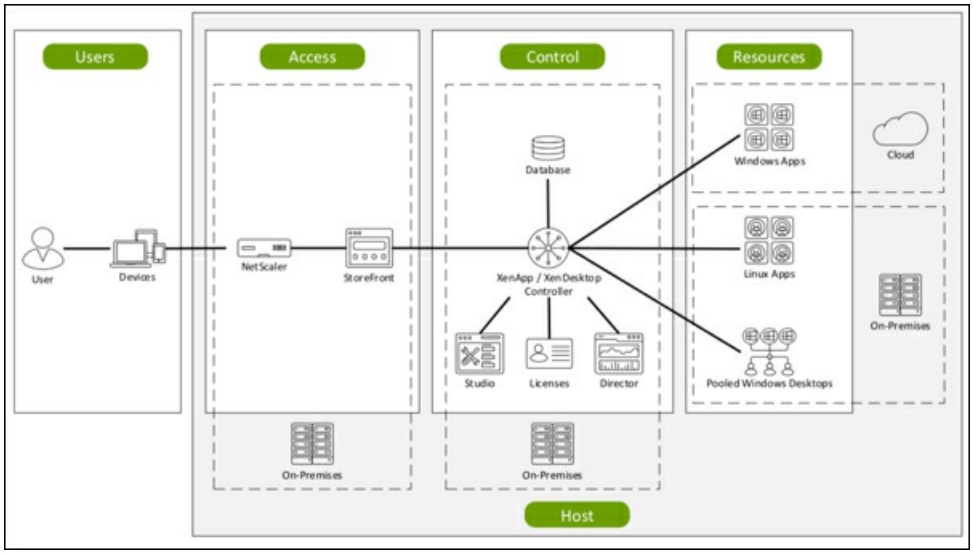


- **Public Cloud** - All components hosted from a public cloud infrastructure using Infrastructure as a Service (IaaS). The public cloud model eliminates hardware management from the local IT team's management scope.

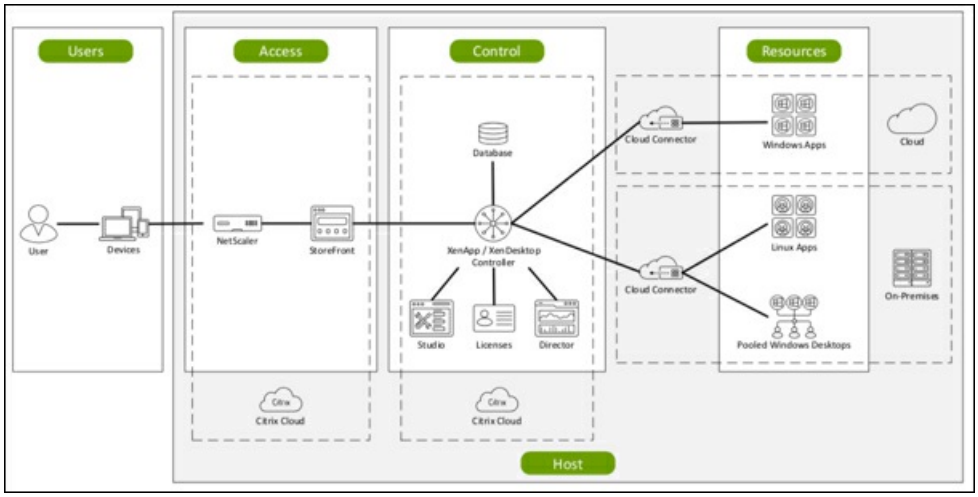


- **Hybrid Cloud** - A single implementation executes from an on-premises data center as well as the public cloud. Even though components of the solution are using different hosting providers, the entire solution is a single solution using the same code and managed as a single entity. The local IT team continues to manage all aspects of the solution except for the hardware associated with the cloud-hosted resources.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Citrix Cloud** - The XenApp and XenDesktop Service offering from Citrix Cloud breaks a typical deployment into multiple management domains. The access and control layer components are hosted and managed in the Citrix cloud by Citrix while the resource layer components continues to be managed by the local IT team either as an on-premises, public cloud or hybrid cloud model. Citrix manages the hardware, sizing and updates to the access and control components while the local IT team manages the resources. In addition, if the public cloud hosts the resources, the local IT team does not have to manage the resource hardware. Citrix Cloud continues to expand the number of offerings to help solve specific user cases. To learn more and understand the full array of offerings, please explore the workspace services within the Citrix Cloud.

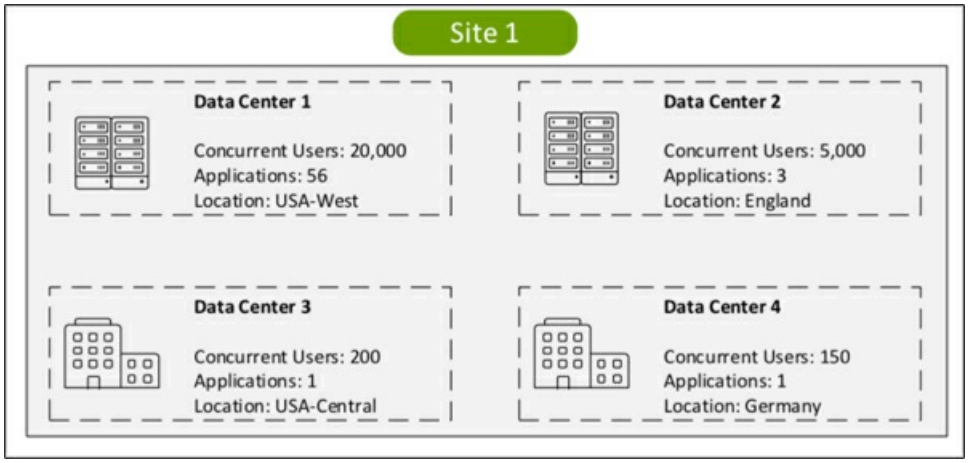


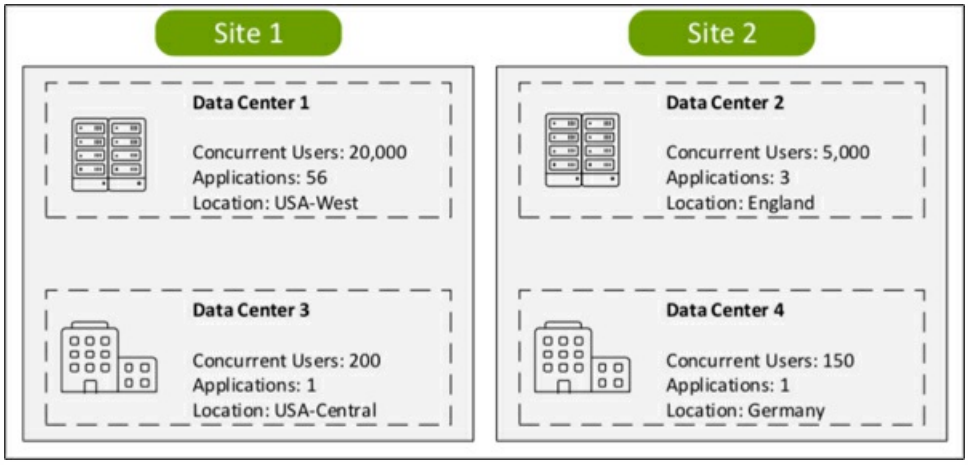
Decision: Site Topology

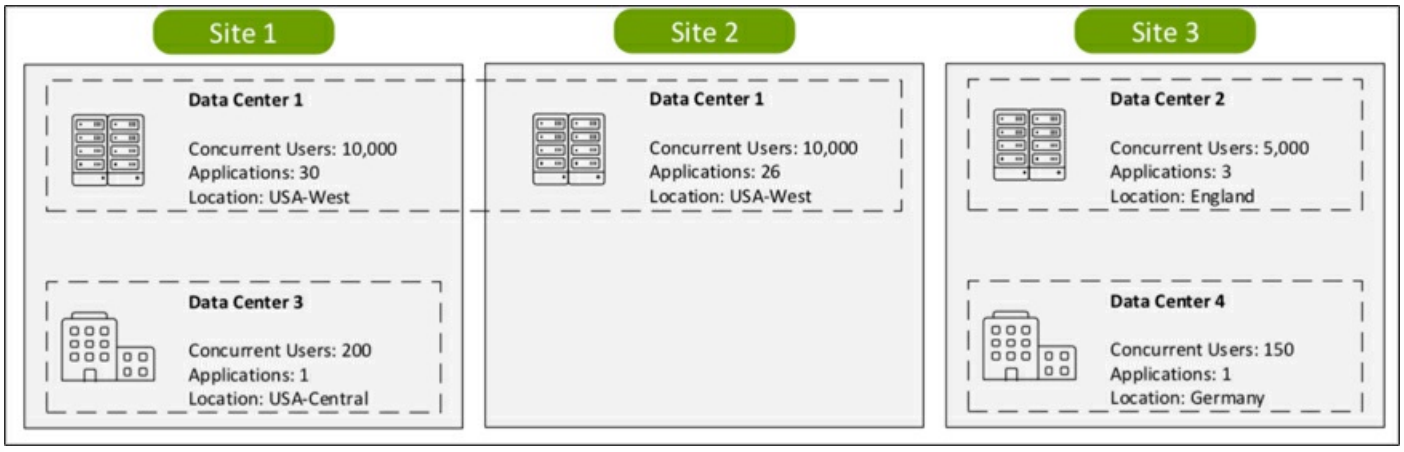
A XenApp and XenDesktop site groups desktops and applications together to form a single architectural and management entity. All persistent and dynamic data for the site, including site configuration, desktop assignments, and session state, is stored in a site's database.

A site can be contained within a single location, span across multiple locations or be a partial location. Through rigorous testing, a single XenApp/XenDesktop site can support 40,000 or more concurrent sessions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.







Zones subdivide single sites, often associated with geographical locations. There are several factors to consider when determining the overall topology of the XenApp and XenDesktop solution:

- **Risk Tolerance** – Create multiple XenDesktop sites to minimize the impact from a site-wide outage. For example, corruption of the XenDesktop site database could affect site-wide availability. For many organizations, the decreased risk from implementing multiple sites outweighs the additional management overhead and supporting infrastructure required.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Experience from the Field

Finance – A large financial institution hosts 10,000 desktops from a single datacenter. To reduce risk, it was decided that no site should exceed 5,000 desktops. Therefore, despite the desktops being connected by a fast and redundant network, two sites were created.

- **Security** – Although delegated administration is available, high-security organizations may require complete separation between environments to demonstrate compliance with specific service level agreements.

Experience from the Field

Retail – A retail organization required complete separation for employees responsible for managing financial data. To meet this requirement, two separate sites were created within the same datacenter – one for t he financial employees and a second for all other employees.

- **Administrative Boundaries** – Due to billing/charge back requirements or how IT is structured, multiple sites might be required to separate administrative boundaries.
- **Geographical Connectivity** – Although the implementation of zones does allow a single site to span geographical locations, there must be enough bandwidth between the satellite zone and primary zone for the site database to capture the session information. Higher latency or larger zones impacts response times for the user.

Variable	XenApp and XenDesktop 7.13	XenApp and XenDesktop 7.11
Latency (ms)	90	250
Concurrent requests	48	48
Average response time	3.7	7.6
Brokering requests per second	12.6	6.3
Time to launch 10,000 users	13 minutes	26 minutes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Session count	Max concurrent sessions launches	Min site-to-site bandwidth	Max site-to-site round trip latency
Less than 50	20	1 Mbps	250 ms
50 to 500	25	1.5 Mbps	100 ms
500 to 1,000	30	2 Mbps	50 ms
1,000 to 3,000	60	8 Mbps	10 ms
Over 3,000	60	8 Mbps	5 ms

In general, administrators should minimize the number of XenDesktop sites and zones to reduce architectural complexity and administrative effort.

Decision: Image Management Strategy

A XenApp and XenDesktop solution requires the creation and management of master images. Organizations must decide early what strategy to pursue for image management.

Installed Images

An installed image requires the administrator to install the operating system and applications for each image. This approach is straightforward but creates a duplication of effort as the admin installs the same operating system and core applications across multiple master images.

Maintaining master images also includes duplication of effort as the same operating system version and core applications are part of multiple images, each requiring the same update process.

Scripted Images

Administrators can automate many of the tasks associated with installed images with scripting or automation tools. Many operating system and application installs support automated scripting, which mitigates the duplication of effort impact on the administrator's time with installed images.

Unfortunately, learning, creating, and maintaining a scripting framework for the entire image is challenging and time consuming. Scripting an entire build takes time and often results in unexpected failures if directory structures change, processes take too long to complete or a filename changes.

Layered Images

Each unique operating system (Windows 10, Windows 2012R2 and Windows 2016), platform (XenApp/XenDesktop 7.13 VDA, XenApp/XenDesktop 7.14 VDA and XenApp/XenDesktop 7.15 VDA) and application (Microsoft Office, Adobe Acrobat, Google Chrome and Mozilla Firefox) is a layer. A master image is the merging of one operating system layer, one platform and many applications.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A layered image approach eliminates the duplication of effort challenges associated with installed and scripted images. Each unique layer is available to any master image. When an application requires an update, that layer receives the updates and all master images utilizing the layer receives the update. If an organization requires ten unique Windows 10 images, each of the ten images shares the same Windows 10 layer. When the administrator needs to upgrade the VDA from version 7.14 to 7.15 across ten images, the administrator only updates a single platform layer.

Initially, the layered image approach does require more time to deploy because the administrator must build the organization's library of layers. However, once the layers are available, the time to maintain the images is drastically reduced.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology user layer

Jan 30, 2018

The top layer of the design methodology is the user layer, which each unique user group defines.

The user layer appropriately sets the overall direction for each user group's environment. This layer incorporates the assessment criteria for business priorities and user group requirements in order to define effective strategies for endpoints and Citrix Receiver. These design decisions affect the flexibility and functionality for each user group.

Endpoint Selection

There are a variety of endpoints devices available, all with differing capabilities, including:

- Tablet based
- Laptop
- Desktop PC
- Thin client
- Smartphone

The user's primary endpoint device must align with the overall business objectives as well as each user's role and associated requirements. In many circumstances, multiple endpoints may be suitable, each offering differing capabilities.

Decision: Endpoint Ownership

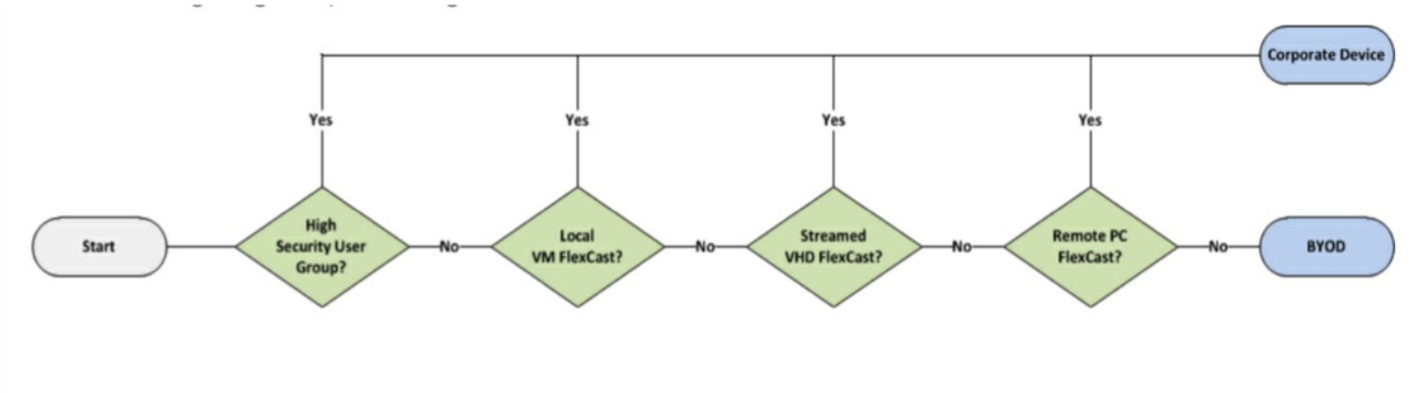
In many organizations, endpoint devices are corporate owned and managed. However, more and more organizations are now introducing bring your own device (BYOD) programs to improve employee satisfaction, reduce costs and to simplify device management. Even if BYOD is a business priority, it does not mean that every user should be allowed to use a personal device in the corporate environment.

Certain user requirements, which were identified during the user segmentation, can greatly impact the suitability of personal devices:

- **Security** – Users requiring a high-level of security might not be able to bring a personal device into the secured environment for risk of data theft.
- **Mobility** – Users operating in a disconnected mode might not be able to use a personal device, as the local VM desktop VDI model associated with this type of requirement can have specific hardware requirements, or special maintenance requirements.
- **Desktop loss criticality** – Users with a high desktop loss criticality rating might require redundant endpoints in the event of failure. This would require the user to have an alternative means for connecting in the event their personal device fails, likely making these users poor candidates for a BYOD program.
- **VDI models** – A personal device should not be recommended for user groups utilizing a local VDI model like a local streamed desktop, local VM desktop or Remote PC Access. These VDI models typically require a specific hardware configuration or installation that will restrict device selection.

The following diagram provides guidance on when user owned devices could be used:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Decision: Endpoint Lifecycle

Organizations may choose to repurpose devices in order to extend refresh cycles or to provide overflow capacity for contract workers. Endpoints now offer more capabilities allowing them to have longer useful lifespans. In many cases, these hardware capabilities vastly outstrip the needs of a typical user. When coupled with the ability to virtualize application and desktop workloads, this provides new options to administrators such as repurposing existing workstations. These options go well beyond the simple three-year PC refresh cycle. However, the benefits of repurposing or reallocating a workstation should be balanced against the following considerations.

- **Minimum standards** – While cost factors of repurposing existing workstations may be compelling, certain minimum standards should be met to guarantee a good user experience. At a minimum, it is recommended that repurposed workstations have a 1GHz processor, 1GB of RAM, 16GB of free disk space and a GPU that is capable of supporting HDX features.
- **Business drivers** – Priorities underpin the success of any major project. Those organizations that have prioritized reducing capital expenditure by means of prolonging the hardware refresh cycle can benefit from repurposing hardware. Conversely, if an organization's business drivers include reducing power consumption as part of an overall green initiative, purchasing newer endpoints may be beneficial in order to take advantage of the latest generation of power management capabilities available in the most modern devices.
- **Workload** – The type of work and VDI model for an end user can determine whether they are a good candidate for a repurposed endpoint, or may be better served with a new device. If the work performed by the individual involves locally installed applications, the individual may be best served by a new endpoint that offers the most powerful and recently updated processor and graphics architecture. However, if a user is largely performing tasks associated with virtualized applications that do not involve the latest multimedia capabilities such as webcams, VoIP and media redirection, then a repurposed workstation should be a viable alternative.

The following planning matrix outlines considerations when repurposing existing hardware:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Endpoint provisioning criteria	Repurpose existing	Procure new
Capital restrained environment	X	
High number of virtualized applications	X	
Desire to prolong hardware refresh cycle	X	
High failure rate among existing desktops		X
Outmoded client-side feature set		X
Power consumption or green initiative(s)		X

Decision: Unified Endpoint Management (UEM)

VDI allows users to work on any device from any location while still getting access to their apps and data. With distributed users accessing the environment across multiple devices, including mobile devices, administrators need to be able to centrally secure and support the mobile devices. Administrators need to:

- Selectively wipe a device if the device is lost, stolen, or out of compliance.
- Require passcode security standards.
- Define geo-location device restrictions.
- Simplify Exchange ActiveSync configuration.
- Define WiFi parameters for office locations.
- Integrate certificates to secure communications.

Managing the distributed endpoints is only part of the challenge. Administrators need to define levels of access. Administrators need to secure and control access to the apps and data. Security becomes a greater concern when users have access to corporate XenApp and XenDesktop resources from personal devices. A few things to consider when delivering XenApp and XenDesktop apps to mobile devices:

- What resources can a jailbroken device access?
- Can users copy/paste between personal apps and XenApp and XenDesktop apps?
- Can a device with no configured passcode get access to corporate resources?
- Can users continue to use a native or untrusted third party email client?
- Can mobile device users access Intranet sites with a browser optimized for mobile devices or with a published desktop browser?

UEM Solutions, like Citrix XenMobile, protects app data and lets admins control app data sharing. UEM also allows for the management of corporate data and resources, separately from personal data.

Decision: Mobile Device Management (MDM)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

VDI allows users to work on any device from any location while still getting access to their apps and data. With distributed users accessing the environment across multiple devices, including mobile devices, administrators need to be able to centrally secure and support the mobile devices, which is knows as Mobile Device Management (MDM).

MDM solutions, like Citrix XenMobile, enables organizations to protect devices and data on devices at a system level. For example,

- Selectively wipe a device if the device is lost, stolen, or out of compliance.
- Require passcode security standards.
- Define geo-location device restrictions.
- Simplify Exchange ActiveSync configuration.
- Define Wi-Fi parameters for office locations.
- Integrate certificates to secure communications.

MDM is typically suitable for corporate-owned mobile devices because most users with personal devices do not want to give the IT team that much control over their personal devices.

Decision: Mobile Application Management (MAM)

With a distributed workforce accessing the XenApp and XenDesktop environment across numerous devices, administrators need to secure and control access to the apps and data. Security becomes a greater concern when users have access to corporate XenApp and XenDesktop resources from personal devices. A few things to consider when delivering XenApp and XenDesktop apps to mobile devices:

- What resources can a jailbroken device access?
- Can users copy/paste between personal apps and XenApp and XenDesktop apps?
- Can a device with no configured passcode get access to corporate resources?
- Can users continue to use a native or untrusted third party email client?
- Can mobile device users access Intranet sites with a browser optimized for mobile devices or with a published desktop browser?

MAM solutions, like Citrix XenMobile, protects app data and lets admins control app data sharing. MAM also allows for the management of corporate data and resources, separately from personal data.

MAM is often suitable for bring-your-own (BYO) devices because, although the device is unmanaged, corporate data remains protected.

Decision: Endpoint Form Factor

The capabilities of endpoints have grown along with efficiencies offered in thin client form factors. Even mid-range thin clients now have graphics capabilities that allow utilization of HDX features such as multi-monitor support while offering management and power efficiency benefits. Citrix has developed a three-tiered classification for thin clients based on their HDX capabilities: HDX Ready, HDX Premium, and HDX 3D Pro, which can be used to help narrow the field of appropriate thin client devices based on the use case requirements. This expansion of capabilities has given IT administrators more options and flexibility than ever before.

Most organizations will likely deploy a mixture of fully featured clients as well as thin clients. However, certain endpoint devices are more appropriate when used in combination with certain VDI models as explained in the following table.

In the table:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Yes** indicates recommended.
- **No** indicates not recommended.
- o indicates viable.

VDI model	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Hosted Windows Apps	Yes	Yes	Yes	Yes	Yes
Hosted Browser Apps	Yes	Yes	Yes	Yes	Yes
Hosted Shared Desktop	Yes	Yes	Yes	o	o
Hosted Pooled Desktop	Yes	Yes	Yes	o	o
Hosted Personal Desktop	Yes	Yes	Yes	o	o
Hosted Pro Graphics Desktop	Yes	Yes	o	o	o
Local Streamed Desktop	No	Yes	No	No	No
Local VM Desktop	No	o	Yes	No	No
Remote PC Access	No	Yes	Yes	o	o

Experience from the Field

- **Large systems integrator** – A large systems integrator recommended that a customer deploy a single type of low-end, limited capability endpoint for all users. Upon deployment to production, users immediately complained that they received a poor user experience when viewing multimedia content over the WAN. At great cost, the systems integrator and customer re-assessed the environment and chose to deploy endpoints that supported HDX MediaStream. The mistake caused a schism between systems integrator and the customer, resulting in lost time, capital and the end of a business relationship that was fostered over many years. It is critical that the endpoints assigned to each user group can support their requirements.

Receiver Selection

Citrix Receiver is an easy-to-install software client that provides access to applications, desktops and data easily and securely from any device, including smartphones, tablets, PCs and Macs.

The following section provides a series of design decisions that should be considered when deploying Citrix Receiver.

Decision: Receiver Type

© 1999-2017 Citrix Systems, Inc. All rights reserved.

While most organizations should simply deploy the latest Citrix Receiver compatible with their endpoint, it is important to recognize that there are certain differences between editions. The following table should be referenced to determine the most appropriate edition of Citrix Receiver for each user group. For the latest feature matrix, please refer to Receiver Feature Matrix.

Decision: Initial Deployment

There are several deployment options available for delivering Citrix Receiver to an endpoint. Although it is usually a best practice to have a full version of Citrix Receiver deployed to an endpoint to provide the greatest level of functionality, it is important to consider fallback options such as the HTML5 Receiver for those situations where the installation of Citrix Receiver is simply not possible. Note that although the HTML5 Receiver can be used as a fallback option, like the Java client was with Web Interface, it is not generally recommended as the primary Receiver for enterprises to standardize on due to the limited feature set and common browser restrictions around unsecured WebSockets connections (see CTX134123 for more information).

Experience from the Field

- **Furniture distributor** – A furniture distributor maintains a configurator application for various furniture options. The configurator application is accessed via a limited functionality kiosk that is deployed at various furniture outlets, including small, independent retailers with little to no IT staff present. The kiosks are completely locked down in many situations, to the point where even the running of Java applications is limited. The kiosks do feature a modern browser (Google Chrome), and therefore, are able to utilize the HTML5 Receiver in order to provide access to the configurator application.
- **County government** – A government IT organization provides services to all agencies operating in the county. A mixture of full desktops are applications are deployed to both Windows based desktops and iPads. Since the desktops are joined to the Active Directory domain, GPOs are utilized to deploy and configure Citrix Receiver. Mobile users accessing the Citrix environment via an iPad install and configure Receiver from the App Store. To allow for seamless provisioning, email based discovery was configured. This allows users to configure Receiver for both internal and external access through NetScaler Gateway by entering in their email address.

The following mechanisms are commonly used to deploy and update Citrix Receiver:

- **StoreFront** – If Citrix StoreFront is available, administrators can deploy Citrix Receiver via a Receiver for Web site by enabling the “Client Detection” feature. When deployed, a Receiver for Web site enables users to access StoreFront stores through a web page. If the Receiver for Web site detects that a user does not have a compatible version of Citrix Receiver, the user is prompted to download and install Citrix Receiver. The Receiver clients can be hosted on the StoreFront server, or users can be directed to citrix.com for the latest Receiver files.
- **Internal download site** – Users may be prevented from downloading software from the Internet, even if they have permission to install applications. Administrator can create an internal website for supported Citrix Receivers or host them on a common software distribution point for a more seamless user experience. This could be an alternative to enabling Client Detection on the StoreFront Receiver for Web site, which can result in an inconsistent user experience depending on browser’s ActiveX settings.
- **Markets and stores** – Citrix Receiver is available on the Windows, Android and iOS stores.
- **Enterprise software deployment** – Many organizations employ an enterprise software deployment (ESD) or Mobile Application Management (MAM) solution. ESD/MAM solutions can be used to deploy Citrix Receiver to managed endpoint devices. Employee-owned devices can only be managed if the user successfully registered the device with the management tool.
- **Master image** – Most organizations have a group of master desktop images, which are deployed to each business owned desktop, laptop, server, or virtual desktop. A common mechanism to ensure access to virtual desktops and applications is to include a supported version of Citrix Receiver in the master image. Subsequent updates to Citrix

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Receiver are handled either by enterprise software deployment tools or manually.

- **Group policy** – For customers without a robust ESD solution, it is possible to deploy and configure Citrix Receiver via Microsoft Group Policy. Sample start-up scripts that deploy and remove Citrix Receiver are available on Citrix XenApp and XenDesktop media:

  Citrix Receiver and Plugins\Windows\Receiver\Startup_Logon_Scripts

- **Manual install** – All supported versions of Citrix Receiver are available from the Citrix Receiver Download site. Upon landing on this site, client detection is performed and a platform and operating system specific link is provided to allow users to download an appropriate edition of Citrix Receiver. It is important to note that no configuration will be accomplished via this download, so users will receive the first time use prompt to enter a server URL or email address. This option is likely to be utilized in a BYOD environment.

Selecting the appropriate deployment method is based on the type of Citrix Receiver selected. The following table should be referenced to help identify the appropriate deployment options for Citrix Receiver.

In the table,

- **Y** indicates "recommended.
- **N** equals "not recommended.

Deployment options	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Base image	Y	Y	Y	N	N
EDS/MAM	N	Y	Y	N	N
Group Policy	N	Y	Y	N	N
Receiver for Web site	N	Y	Y	N	N
Internal download site	N	Y	Y	N	N
App store	N	N	N	Y	Y

Decision: Initial Configuration

Citrix Receiver must be configured in order to provide access to enterprise resources. The method of configuration varies by Citrix Receiver edition, the form factor of the device, and lastly the access method (local or remote) that is involved. Several methods may be viable for an organization. The method utilized is contingent on the resources (people, systems, time) available as well as larger organizational initiatives such as BYOD programs.

The following methods can be used to configure Citrix Receiver:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Email based discovery** – The latest releases of Citrix Receiver can be configured by entering an email address. Email based discovery requires Citrix StoreFront as well as an SRV DNS record which points to the FQDN of the StoreFront server.

  Note: Any DNS platform should support email-based discovery, however only Windows DNS has been explicitly tested.

  For remote access, NetScaler Gateway must be utilized with the corresponding SRV record in external DNS. A valid server certificate on the NetScaler Gateway appliance or StoreFront server must be present in order to enable email-based account discovery. This configuration assumes that the portion of the email address after the "@" is the DNS namespace that should be queried for this SRV record. This can be challenging for customers with different external and internal namespaces or email addresses that are different from DNS namespaces.

- **Group policy** – Microsoft Group Policy can be used to configure Citrix Receiver. This can be done via start up scripts used to deploy Receiver by ensuring there is a value for the SERVER_LOCATION=Server_URL parameter or by using the ADMX/ADML template files included with the installation of Citrix Receiver to set the StoreFront Account List option in conjunction with another Receiver deployment method. Provide the URL of the server running Citrix StoreFront in the format https://baseurl/Citrix/storename/discovery.
- **Provisioning file** – For environments running StoreFront, it is possible to provide users with a provisioning file that contains store information. Provisioning files are exported from the StoreFront console. The file is saved with a "*.cr" extension and can then be placed on a shared network resource, a Receiver for Web site, or other web based resource or emailed to users. The file can then be launched from an endpoint, which automatically configures Citrix Receiver to use the store(s). If users browse to the Receiver for Web site and select the "Activate" option under their username, this also automatically downloads this same ".cr" file and configure the Receiver client for users.
- **Manually** – If allowed, it is usually possible to configure Citrix Receiver manually by entering the server URL. This method should be reserved for administrators or users that have advanced knowledge.
- **Studio** – In addition to the above methods, in order to configure Receiver deployed on a virtual desktop or server image (within a XenDesktop or XenApp environment), it is possible to set the StoreFront address via the properties of the Delivery Group.

Decision: Updates

Citrix Receiver is in active development. As such, periodic updates are released that provide enhanced functionality or address user issues. As with any actively developed product, the latest version of these products should be deployed to the endpoints so that users benefit from the latest functionality and to maintain compliance with product support lifecycles. There are multiple methods available to update Citrix Receiver and, if applicable, associated plug-ins.

- **Auto-Update** – Receiver for Windows 4.8+ and Receiver for Mac 12.6+ includes an autoupdate capability that automatically checks for newer versions of Receiver. The autoupdate service can be configured to allow users to defer updates as well as to skip any updates that are not long-term service release (LTSR) versions. Receiver for iOS and Android are automatically updated through their appropriate store.
- **Enterprise software deployment** – ESD tools provide an organization with direct control over the time/frequency of Receiver updates to managed devices. Additional thought must be given to updating unmanaged devices and endpoints outside of the corporate firewall.
- **Manual updates** – When no automated solution is available, manual methods can be used to update Citrix Receiver. Whether deployed on Receiver for Web site, StoreFront, an internal Citrix Receiver site, or an external site, these options will require user involvement in updating Citrix Receiver. Due to the involved nature of manual updates coupled with the opportunity for a user mistake, this option should only be considered as a last resort.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology access layer

Apr 24, 2018

The second layer of the design methodology is the access layer, which is defined for each user group.

Creating an appropriate design for the access layer is an important part of the desktop virtualization process. This layer handles user validation through authentication and orchestrates access to all components necessary to establish a secure virtual desktop connection.

The access layer design decisions are based on the mobility requirements of each user group as well as the endpoint devices used.

Authentication

Getting access to resources is based on the user's identity. Defining the authentication strategy takes into account the user's entry point into the environment as well as how the user will authenticate.

Decision: Authentication Provider

Traditionally, users required an Active Directory username and password to get access to their XenApp and XenDesktop resources. As most organizations standardized on an on-premises Active Directory deployment, this particular requirement was simple to achieve.

Organizations are using external contractors, which requires an account to get access to the XenApp and XenDesktop resources.Organizations are investigating the use of a third party identity provider (IdP) like Azure Active Directory, Google, LinkedIn, etc., instead of managing their own.

With the implementation of Citrix Federated Authentication Service, XenApp and XenDesktop supports the use of a third party IdP. An administrator can have a contractor use their Google account to gain access to their approved applications and desktops, simplifying onboarding.

Decision: Authentication Point

Before a user connects to a virtual resource, they must first authenticate. The place of authentication is often determined by the user group's mobility requirements, which were defined during the user segmentation process. There are two authentication points available in XenDesktop:

- **StoreFront** – Citrix StoreFront provides authentication and resource delivery services for Citrix Receiver, enabling centralized enterprise stores to deliver desktops, applications and other resources.
- **NetScaler Gateway** – NetScaler Gateway is an appliance providing secure application access and granular application-level policy controls to applications and data while allowing users to work from anywhere.

The following table lists preferred authentication points according to user group mobility requirements:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Group's Mobility Requirement	Preferred Authentication Point
Local	StoreFront
Roaming Local	StoreFront
Remote	NetScaler Gateway
Local	NetScaler Gateway

Authentication for user groups with a mobility requirement of remote or mobile may occur directly on StoreFront where required. For example, DMZ security policies may prohibit access from the NetScaler Gateway to the domain, which is required to support Smartcard client certificate authentication. Access to StoreFront for authentication may then be delivered via a NetScaler SSL_BRIDGE virtual server, which provides a conduit for https traffic. Typically, the virtual server would be hosted alongside a NetScaler Gateway on the same NetScaler configured to provide HDX Proxy access to the virtual desktop environment. Although such a use case may sometimes be necessary, the recommended best practice is to authenticate external users via NetScaler Gateway.

Decision: Authentication Policy

Once the authentication point has been identified, the type of authentication must be determined. The following options are the primary methods available:

- **StoreFront** – Supports a number of different authentication methods, although not all are recommended depending on the user access method, security requirements and network location. Note that by default StoreFront authenticates users directly with Active Directory, not via XML as Web Interface did. StoreFront 3.0+ can be optionally configured to delegate authentication to XML if required (such as if the StoreFront servers are in a domain that does not trust the user domains).
  - **User name and password** – Requires users to logon directly to the site by entering a user name and password.
  - **Domain pass-through** – Allows pass-through of domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores.
  - **NetScaler Gateway pass-through** – Allows pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.
  - **Smart card** – Allows users to authenticate using smart cards and PINs through Citrix Receiver for Windows and NetScaler Gateway. To enable smart card authentication, user accounts must be configured either within the Microsoft Active Directory domain containing the StoreFront servers or within a domain that has a direct two-way trust relationship with the StoreFront server domain. Multi-forest deployments involving one-way trust or trust relationships of different types are not supported.
  - **Anonymous** – Allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. Local anonymous accounts are created on demand on the Server VDA when sessions are launched. This requires a StoreFront store configured for authenticated access, a Server OS based VDA, and a XenApp Delivery Group configured for unauthenticated users.
- **NetScaler Gateway** – The NetScaler Gateway supports several authentication methods. The list below includes those

© 1999-2017 Citrix Systems, Inc. All rights reserved.

primarily used in virtual desktop environments. Each may be used individually, but are often combined to provide multi-factor authentication.

- **LDAP** – The lightweight directory access protocol (LDAP) is used to access directory information services such Microsoft Active Directory. NetScaler Gateway uses LDAP to authenticate users and extract their group membership information.
- **RADIUS (token)** – Remote authentication dial in user service (RADIUS) is a UDP based network security protocol that provides authentication, authorization and accounting. A network access server (NetScaler Gateway in this case) forwards credentials to a RADIUS server that can either check the credentials locally, or check them against a directory service. The RADIUS server could then accept the connection, reject the connection, or challenge and request a second form of authentication such as a token.
- **Client certificate** – Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the attributes of a client certificate presented to the virtual server. Client certificates are usually disseminated to users in the form of smartcards or common access cards (CACs) that are read by a reader attach to each user's device.

The authentication type for a user group is often determined based on security requirements as well as the authentication point used. The following table helps define the appropriate solution for each user group based on the level of security required:

Authentication Point	Security Requirement	Authentication Type
StoreFront	• Low • Medium • High	Low: • LDAP user name and password • Pass-through Medium • LDAP user name and password • Pass-through High: LDAP and/or Smartcard
NetScaler Gateway	• Low • Medium • High	Low: LDAP user name and password Medium: LDAP user name and password High: • LDAP and Token • LDAP and Smartcard • Token and Smartcard

Experience from the Field

- **Retail** – A small private retail company provides virtual desktop users with access to non-sensitive data such as marketing catalogs and email. They are not required to adhere to security regulations such as Sarbanes Oxley. Therefore, LDAP authentication has been implemented based on user name and password.
- **Financial** – A medium financial enterprise provides their virtual desktop users with access to confidential data such as banking transaction records. They are governed by security regulations such as the Statement on Accounting Standards (SAS) 70 and are required to utilize multi-factor authentication for remote access users. LDAP authentication has been implemented based on user name and password along with RADIUS authentication using tokens.
- **Government** – A large federal institution provides virtual desktop users with access to highly confidential data such as

© 1999-2017 Citrix Systems, Inc. All rights reserved.

private citizens' personal records. They are subject to regulation by Department of Defense (DOD) security standards. LDAP authentication has been implemented based on user name and password, along with Client Certificate authentication using CAC cards.
- **Healthcare** - A hospital is using XenApp to deliver their EMR application to users. ThinClient devices on stationary and mobile carts are being used by doctors and nurses to capture and retrieve patient data. Unauthenticated access has been configured to prevent medical staff from having to authenticate to the domain as well as the EMR application.

StoreFront

Citrix StoreFront authenticates users to XenApp and XenDesktop resources. StoreFront enumerates and aggregates available desktops and applications into a single interface that users access through Citrix Receiver for Windows, iOS, Android, or the StoreFront web site.

Decision: High Availabiity

If the server hosting StoreFront is unavailable, users will not be able to launch new virtual desktops, published applications or manage their subscriptions. Therefore at least two StoreFront servers should be deployed to prevent this component from becoming a single point of failure. By implementing a load balancing solution, users will not experience an interruption in their service. Options include:

- **Hardware load balancing** – An intelligent appliance, which is capable of verifying the availability of the StoreFront service and actively load balance user requests appropriately. Citrix NetScaler is a great example of a hardware load balancer. Citrix NetScaler is an ideal load balancer, coming pre-configured with StoreFront health checks.
- **DNS round robin** – Provides rudimentary load balancing across multiple servers without performing any checks on availability. If a StoreFront server becomes unavailable, DNS round robin would still route users to the failed server. Because of this, DNS round robin is not recommended by Citrix.
- **Windows network load balancing** – A Windows service capable of performing rudimentary checks to verify the server is available but cannot determine the status of individual services. This can cause users to be forwarded to StoreFront servers which are not able to process new requests. The user would then not be able to access applications or desktops.

Decision: Delivery Controller Reference

To provide users with desktops and applications, StoreFront must be configured with the IP address or DNS name of at least one Controller in each XenDesktop and XenApp site. For fault tolerance, multiple controllers should be entered for each site and/or farm specified. By default, StoreFront treats a list of servers in failover order (active/passive).

For large deployments or environments with a high logon load an active distribution of the user load (active/active) is recommended. This can be achieved by means of a load balancer with built-in XML monitors, such as Citrix NetScaler or by configuring StoreFront to load balance the list of Controllers instead of treating them as an ordered list.

Decision: Beacons

Citrix Receiver uses beacons (websites) to identify whether a user is connected to an internal or external network. Internal users are connected directly to StoreFront for authentication while external users are connected via Citrix NetScaler Gateway. It is possible to control what a user sees by restricting applications due to which beacon they have access to.

The internal beacon should be a site that is not resolvable externally. By default, the internal beacon is the StoreFront base URL. This will have to be adjusted if the same external and internal URL is configured. The external beacon can be any external site that produces an http response. Citrix Receiver continuously monitors the status of network connections (for example, link up, link down or change of the default gateway). When a status change is detected, Citrix Receiver first verifies that the internal beacon points can be accessed before moving on to check the accessibility of external beacon

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

points. StoreFront provides Citrix Receiver with the http(s) addresses of the beacon points during the initial connection/configuration download process and provides updates as necessary. It is necessary to specify at least two highly available external beacons that can be resolved from public networks.

Decision: Resource Presentation

By default, StoreFront allows users to choose (subscribe) to the resources they want to regularly use after they logon (favorites). This approach, deemed “Self-Service,” allows users to restrict the resources that they see on their home screen to the ones that they use on a regular basis. The resources chosen by every user for each store are recorded by the subscription store service and stored locally on each StoreFront server (synced automatically between servers in the same server group) so that they can be displayed on the Citrix Receiver home screen from any device that the user connects from. Although by default subscriptions are per store and per server group, administrators can configure two stores within a server group to share a subscription database and/or sync subscriptions between two identically named stores in two separate server groups on a defined schedule if required.

Administrators should determine which applications should always be displayed to users on their home screen or the featured tab. In general, these applications are common applications such as the Microsoft Office Suite and any other applications that every user in an environment may need. StoreFront can filter/present these resources using Keywords defined within the published application properties Description field.

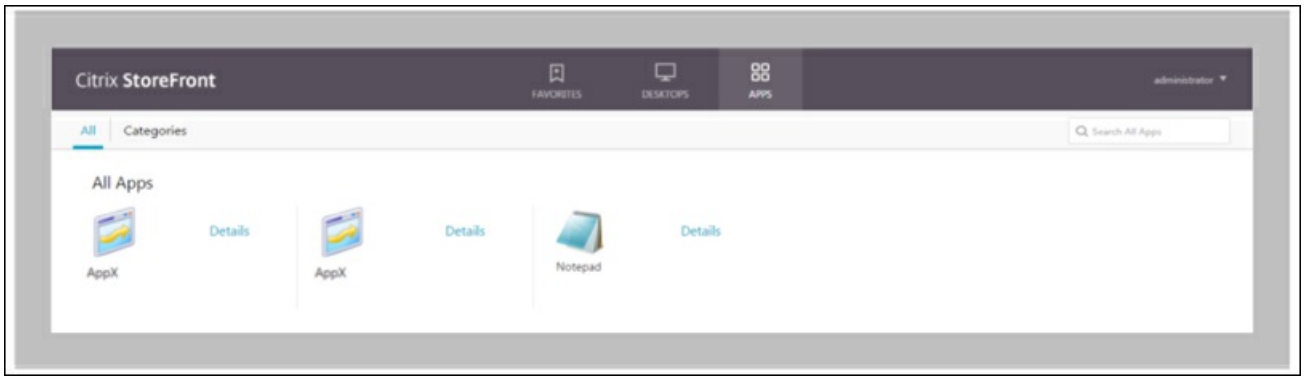
The following table explores the Keyword options:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Keyword	Description
Auto	Automatically subscribes all users of a store to an application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application. Users can choose to subsequently remove this subscription if desired.
Mandatory	New in StoreFront 2.5, the Mandatory keyword will make applications automatically be subscribed to users of the store. However, users will not have the option to remove the application. This setting is useful when creating a core set of applications which must always be presented to all users.
Featured	Advertise applications to users or make commonly used applications easier to find by listing them in the Receiver Featured list.
Prefer	Specify a locally installed application should be used instead of an application available in Receiver. Receiver searches for the specified name/path to determine if the application is installed locally. If it is, Receiver subscribes the application and does not create a shortcut. When the user starts the application from the Receiver window, Receiver starts the locally installed (preferred) application. If a user uninstalls a preferred application outside of Receiver, the application is unsubscribed during the next Receiver refresh. If a user uninstalls a preferred application from the Receiver window, Receiver unsubscribes the application but does not uninstall it.
TreatAsApp	By default, XenDesktop VDI desktops and XenApp hosted shared desktops are treated like other desktops by Receiver for Web sites. By using the keyword "TreatAsApp," the desktop will be displayed in the application views of Receiver for Web sites rather than the desktop views. Users are required to subscribe before they can access the desktop.
Primary	When in a multi-site deployment, using this keyword ensures that an application is delivered from a designated site. If an application is available from multiple sites, with the same name, the application from the secondary site will only be displayed if the application is not available from the primary site.
Secondary	A same property as the "Primary" keyword, except it designates an application in the secondary site.

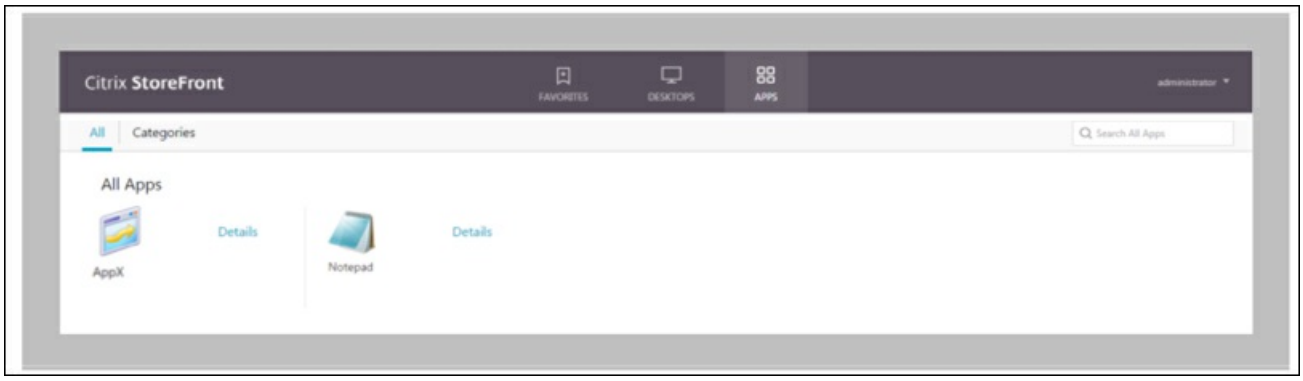
Decision: Aggregation Groups

If the XenApp/XenDesktop solution includes multiple delivery sites, StoreFront merges the available resources together so the user has a single interface for all published resources. However, if multiple sites publish the same resources, the user might experience confusion as a single application appears multiple times.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

StoreFront aggregation groups define how the resources in multiple sites merge to provide the user with a single, easy to understand view. StoreFront aggregates duplicate published resources into a single icon.



The administrator must determine how to load balance users across the different XenApp/XenDesktop sites when the icon is an aggregation. The options are:

- **Load Balancing** – Used when the duplicate sites are created based on capacity recommendations. StoreFront distributes user requests across all configured sites.
- **Failover** – Used when geographies need to have resources available in the event of an outage or when migrating users from one site to another site (like a XenApp migration project).

It is advisable to document the users, stores and aggregation methods during the design phase.

User Group	Available Store(s)	Load Balancing Stores	Failover Stores
NA_FinanceUsers	NA_West_Store NA_East_Store EMEA_Store	NA_West_Store NA_East_Store	EMEA_Store
EMEA_SalesUsers	EMEA_Store NA_East_Store	EMEA_Store	NA_East_Store

Decision: Scalability

The number of Citrix Receiver users supported by a single StoreFront server depends on the resources assigned and level of user activity. Note that Receiver for Web users will consume more RAM on average than native Receiver users, but a minimum of 4 GB of RAM is recommended per StoreFront server in all cases as a baseline. Additionally, more sites/farms enumerated per store will increase both CPU utilization and server response time, with XenApp IMA farms having a greater scalability impact than XenApp/XenDesktop FMA site.

StoreFront deployment	CPU Usage	Simultaneous activities
Standalone deployment • 4CPUs	75%	291 per second

© 1999-2017 Citrix Systems, Inc. All rights reserved.

• 4 GB RAM • Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)	90%	375 per second
Cluster StoreFront deployment 2 Nodes each with: • 4 CPUs • 4 GB RAM • Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)	75%	529 per second
	90%	681 per second

Tests have shown diminishing returns after a single StoreFront deployment grows beyond 3-4 StoreFront nodes with a maximum of 5-6 servers supported in a single server group.

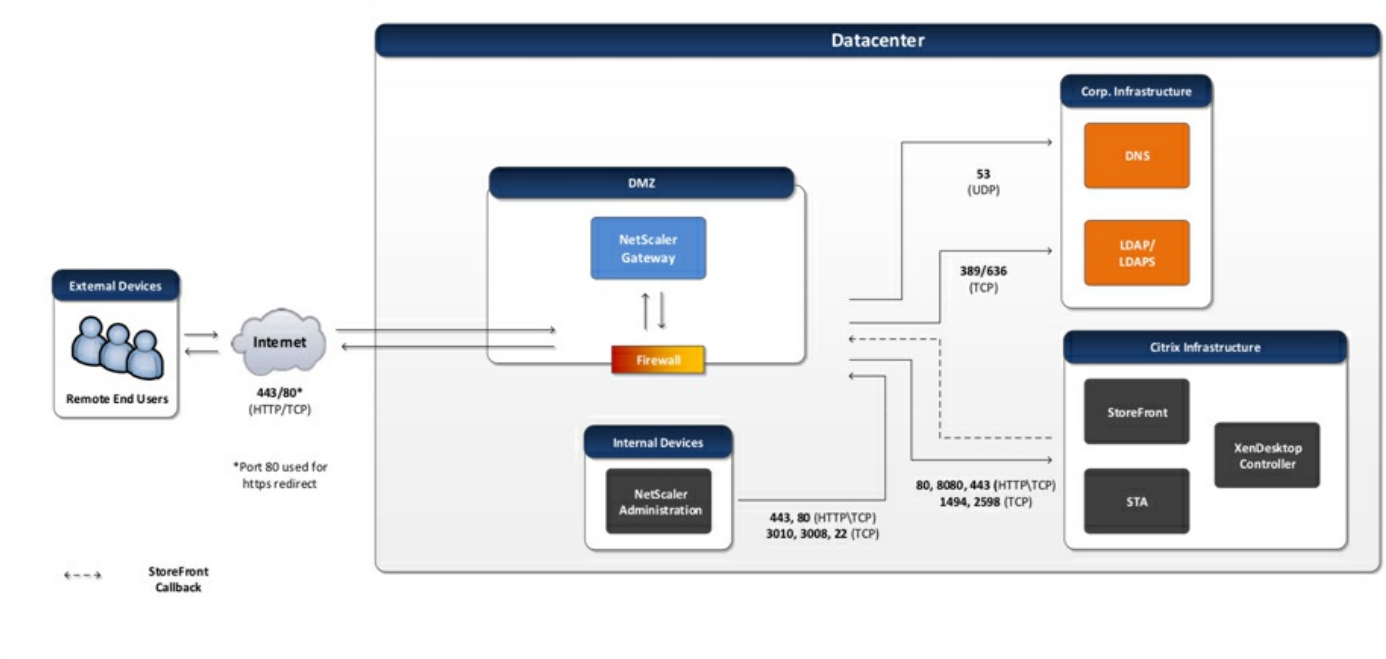
NetScaler Gateway

User groups utilizing NetScaler Gateway as their authentication point have additional design decisions to consider. These design decisions are not applicable for non-NetScaler Gateway authentication points.

Decision: Topology

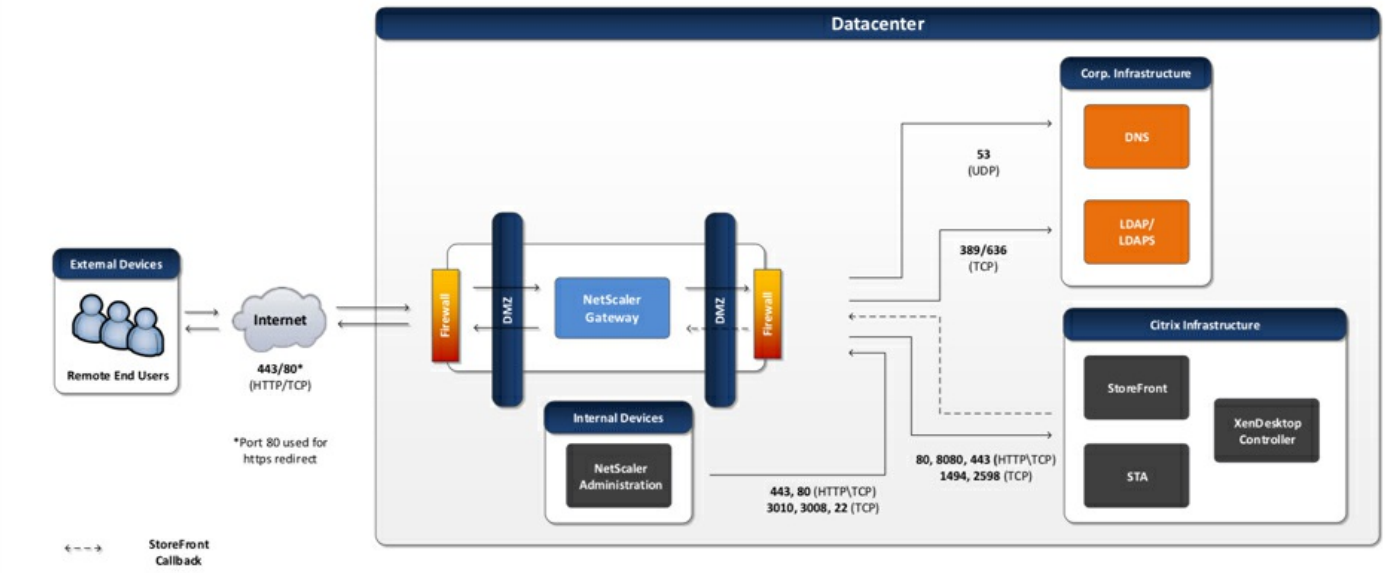
Selection of the network topology is central to planning the remote access architecture to ensure that it can support the necessary functionality, performance and security. The design of the remote access architecture should be completed in collaboration with the security team to ensure adherence to corporate security requirements. There are two primary topologies to consider, each of which provides increasing levels of security:

- **1-Arm (normal security)** – With a 1-arm topology, the NetScaler Gateway utilizes one physical or logical bonded interface, with associated VLAN and IP subnet, to transport both frontend traffic for users and backend traffic for the virtual desktop infrastructure servers and services.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **2-Arm (high security)** – With a 2-arm topology, the NetScaler Gateway utilizes two or more physically or logically bonded interfaces, with associated VLANS and IP subnets. Transport of the frontend traffic for users is directed to one of these interfaces. The frontend traffic is isolated from backend traffic, between the virtual desktop infrastructure servers and services, which is directed to a second interface. This allows the use of separate demilitarized zones (DMZs) to isolate frontend and backend traffic flows along with granular firewall control and monitoring.



Decision: High Availabiity

If the NetScaler Gateway is unavailable, remote users will not be able to access the environment. Therefore at least two NetScaler Gateway hosts should be deployed to prevent this component from becoming a single point of failure.

When configuring NetScaler Gateway in a high availability (active/passive) pair, the secondary NetScaler Gateway monitors the first appliance by sending periodic messages, also called a heartbeat message or health check, to determine if the first appliance is accepting connections. If a health check fails, the secondary NetScaler Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. If the secondary appliance confirms the health check failure, the secondary NetScaler Gateway takes over for the primary NetScaler Gateway.

Note that in firmware 10.5 and above, clustering is also possible with multiple NetScaler Gateway instances to provide high availability, although support for spotted versus stripped configurations varies by firmware and Gateway configuration (full SSL VPN versus ICA proxy).

(http://docs.citrix.com/en-us/netscaler/11-1/clustering/cluster-features-supported.html)

Decision: Platform

In order to identify an appropriate NetScaler platform to meet project requirements, the key resource constraints must be identified. Since all remote access traffic will be secured using the secure sockets layer (SSL), transported by Hypertext Transfer Protocol (HTTP) in the form of HTTPs, there are two resource metrics that should be targeted:

- **SSL throughput** – The SSL throughput is the gigabits of SSL traffic that may be processed per second (Gbps).
- **SSL transactions per second (TPS)** – The TPS metric identifies how many times per second an Application Delivery Controller (ADC) may execute an SSL transaction. The capacity varies primarily by the key length required. TPS capacity is

© 1999-2017 Citrix Systems, Inc. All rights reserved.

primarily a consideration during the negotiation phase when SSL is first setup and it is less of a factor in the bulk encryption / decryption phase, which is the majority of the session life. While TPS is an important metric to monitor, field experience has shown that SSL throughput is the most significant factor in identifying the appropriate NetScaler Gateway.

The SSL bandwidth overhead average is often considered negligible relative to the volume of virtual desktop traffic and is not typically accounted for as part of required SSL throughput. However, making provisions for SSL bandwidth will help ensure the total throughput estimated is sufficient. The fixed bandwidth added to packet headers can vary according to the encryption algorithms used and the overall percentage of bandwidth may vary widely according to packet size. Ideally, the overhead should be measured during a proof of concept or pilot. However, in the absence of such data incrementing the workload bandwidth by 2% is a reasonable rule of thumb. Therefore, to determine the SSL throughput required by a NetScaler platform, multiply the maximum concurrent bandwidth for a datacenter by 1.02:

□□□ □*h*□□□□*h*□□□ = □□□□□□□ □□□□□□□□□□ □□□□□□□□*h* ∗ 1.02

For example, assuming 128Mbps maximum concurrent bandwidth, the appropriate NetScaler model can be determined as follows:

~130□□□□ = 128□□□□ ∗ 1.02

The SSL throughput value should be compared to the throughput capabilities of various NetScaler platforms to determine the most appropriate one for the environment. There are three main platform groups available, each of which provides broad scalability options.

- **VPX** – A NetScaler VPX device provides the same full functionality as hardware NetScaler. However, NetScaler VPXs can leverage 'off the shelf' servers for hosting and are suitable for small to medium sized environments. Typically, organizations create a baseline cap for the VPX instances at 500 users.
- **MPX** – A NetScaler MPX is the hardware version of the NetScaler devices. The MPX device is more powerful than the virtual NetScaler and can support network optimizations for larger scale enterprise deployments, particularly when SSL offload will be configured as this is done in software on the VPX versus dedicated SSL chips on the MPX.
- **SDX** – A NetScaler SDX is a blend between the virtual and physical NetScaler devices. An SDX machine is a physical device capable of hosting multiple virtual NetScaler devices. This consolidation of devices aids with reducing required shelf space and device consolidation. NetScaler SDXs are suitable for handling network communications for large enterprise deployments and/or multi-tenant hosting providers.

SSL throughput capabilities of the NetScaler platforms may be found in the Citrix NetScaler data sheet. Therefore, based on the example calculation above, a NetScaler MPX 5550 appliance would be sufficient to handle the required load. However, actually scalability will depend on security requirements. NetScaler SSL throughput decreases with the use of increasingly complex encryption algorithms and longer key lengths. Also, this calculation represents a single primary NetScaler. At a minimum, N+1 redundancy is recommended which would call for an additional NetScaler of the identical platform and model.

> ## Nota
>
> The Citrix NetScaler data sheet typically represents throughput capabilities under optimal conditions for performance. However, performance is directly affected by security requirements. For example, if the RC4 encryption algorithm and a 1k key length are used, a VPX platform may be able to handle more than 500 HDX proxy connections. However, if a 3DES encryption algorithm and 2k key length are used (which are becoming more common), the throughput may be halved.

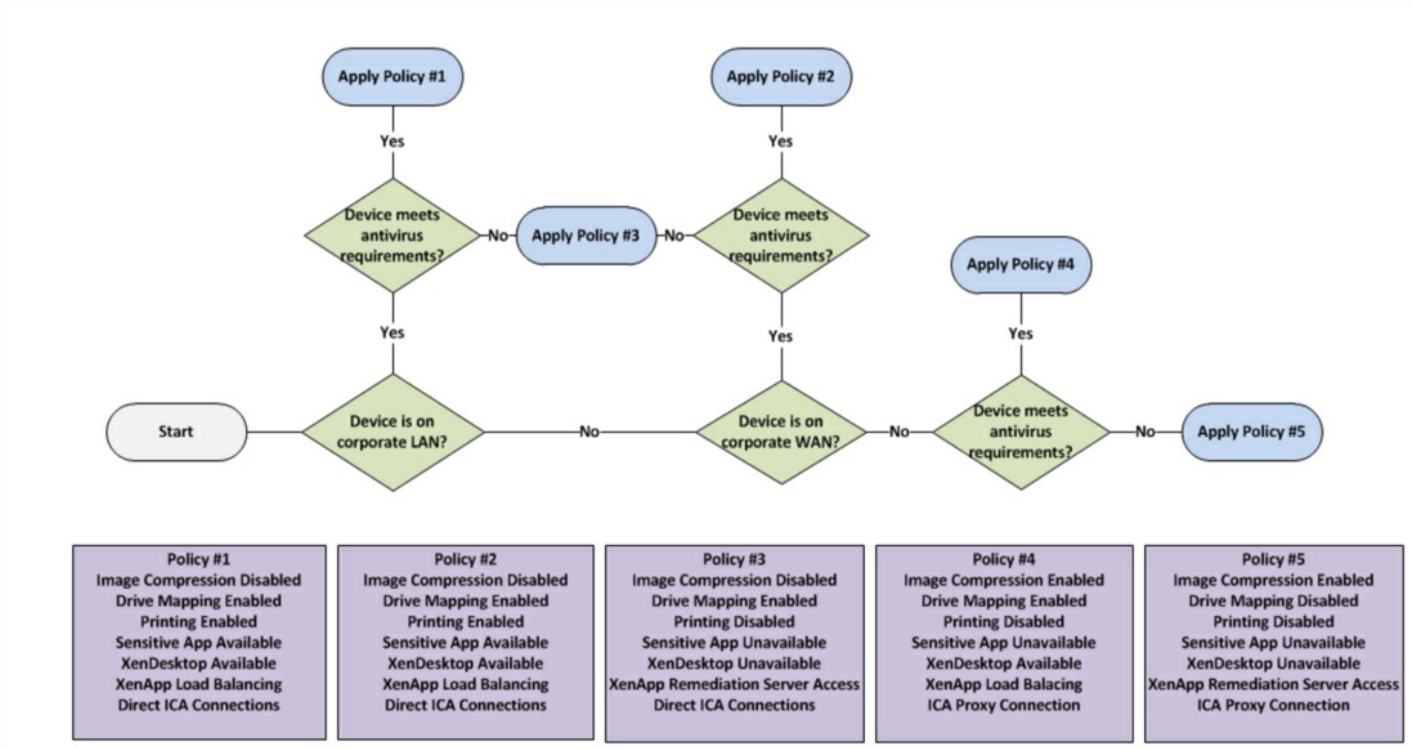
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Pre-Authentication Policy

An optional pre-authentication policy may be applied to user groups with NetScaler Gateway as their authentication point. Pre-authentication policies limit access to the environment based on whether the endpoint meets certain criteria through Endpoint Analysis (EPA) Scans.

Pre-authentication access policies can be configured to test antivirus, firewall, operating system, or even registry settings. These policies can be used to prevent access entirely or can be used by XenDesktop to control session features such as clipboard mapping, printer mapping and even the availability of specific applications and desktops. For example, if a user device does not have antivirus installed, a filter can be set to hide sensitive applications.

The following figure provides an overview of how multiple policies can be used to customize the features of a virtualization resource:



Experience from the Field

- **Retail** – A small private retail company use EPA to scan for the presence of updated antivirus definitions prior to allowing access.
- **Financial** – A medium financial enterprise use EPA scans of the Domain SID to verify that users are members of the enterprise domain prior to allowing access.
- **Government** – A large federal institution use EPA to scan endpoint devices to ensure that a specific certificate (or set of certificates) has been installed on the device prior to allowing access.

Decision: Session Policy

User groups with NetScaler Gateway as their authentication point must have corresponding session policies defined. Session policies are used to define the overall user experience postauthentication.

Organizations create sessions policies based on the type of Citrix Receiver used. For the purpose of session policy

© 1999-2017 Citrix Systems, Inc. All rights reserved.

assignment, devices are commonly grouped as either non-mobile (such as Windows, Mac and Linux OS based), or mobile (such as iOS or Android). Therefore, a decision on whether to provide support for mobile devices, non-mobile devices, or both should be made based on client device requirements identified during the assess phase.

To identify devices session policies, include expressions such as those discussed in this article.

- **Mobile devices** – The expression is set to REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver which is given a higher priority than the non-mobile device policy to ensure mobile devices are matched while non-mobile devices are not.
- **Non-mobile devices** – The expression is set to ns_true which signifies that it should apply to all traffic that is sent to it.

An alternative use of session policies is to apply endpoint analysis expressions. These session policies are applied post authentication yet mimic the previously mentioned pre-authentication policies. Use of session policies is an option to provide a fallback scenario to endpoints that do not meet full security requirements such read-only access to specific applications.

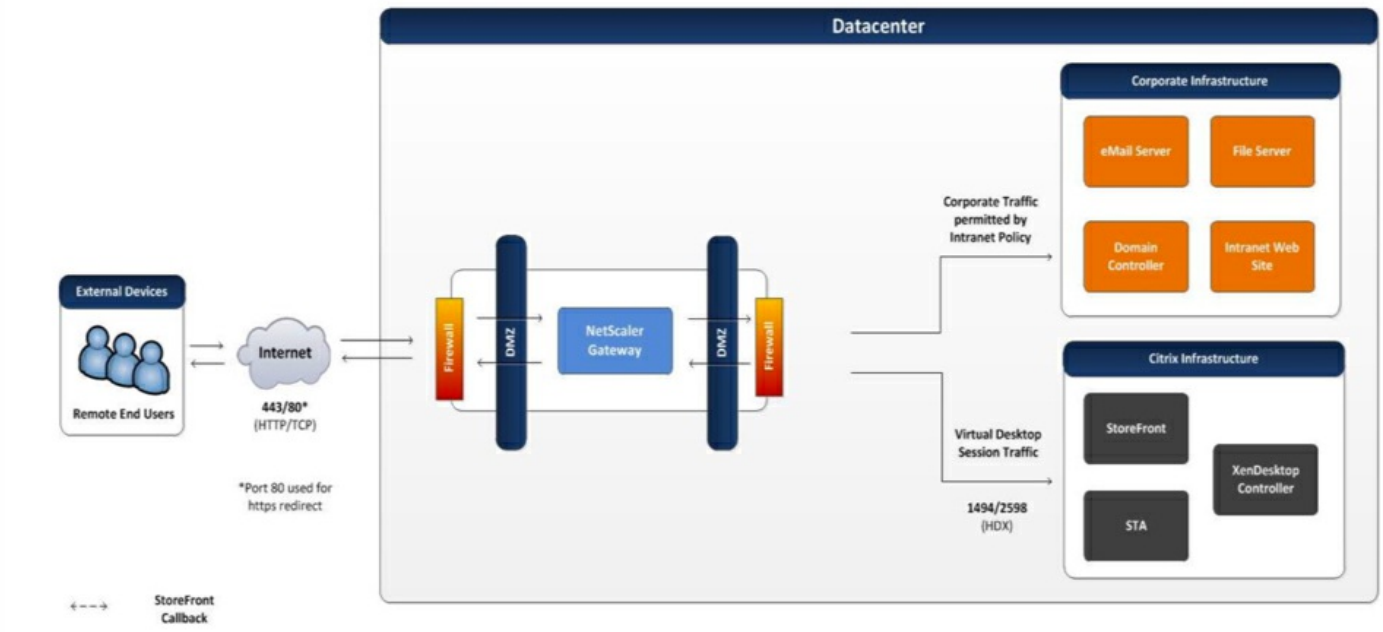
Decision: Session Profile

Each session policy must have a corresponding session profile defined. The session profile defines details required for the user group to gain access to the environment. There are two primary forms of session profiles that determine the access method to the virtual desktop environment:

- **SSLVPN** – Users create a virtual private network and tunnel all traffic configured by IP addresses through the internal network. The user's client device is able to access permitted intranet resources as if it were on the internal network. This includes XenDesktop sites and any other internal traffic such as file shares or intranet websites. This is considered a potentially less secure access method since network ports and routes to services outside of the virtual desktop infrastructure may be opened leaving the enterprise susceptible to risks that may come with full VPN access. These risks may include denial of service attacks, attempts at hacking internal servers, or any other form of malicious activity that may be launched from malware, Trojan horses, or other viruses via an Internet based client against vulnerable enterprise services via routes and ports.

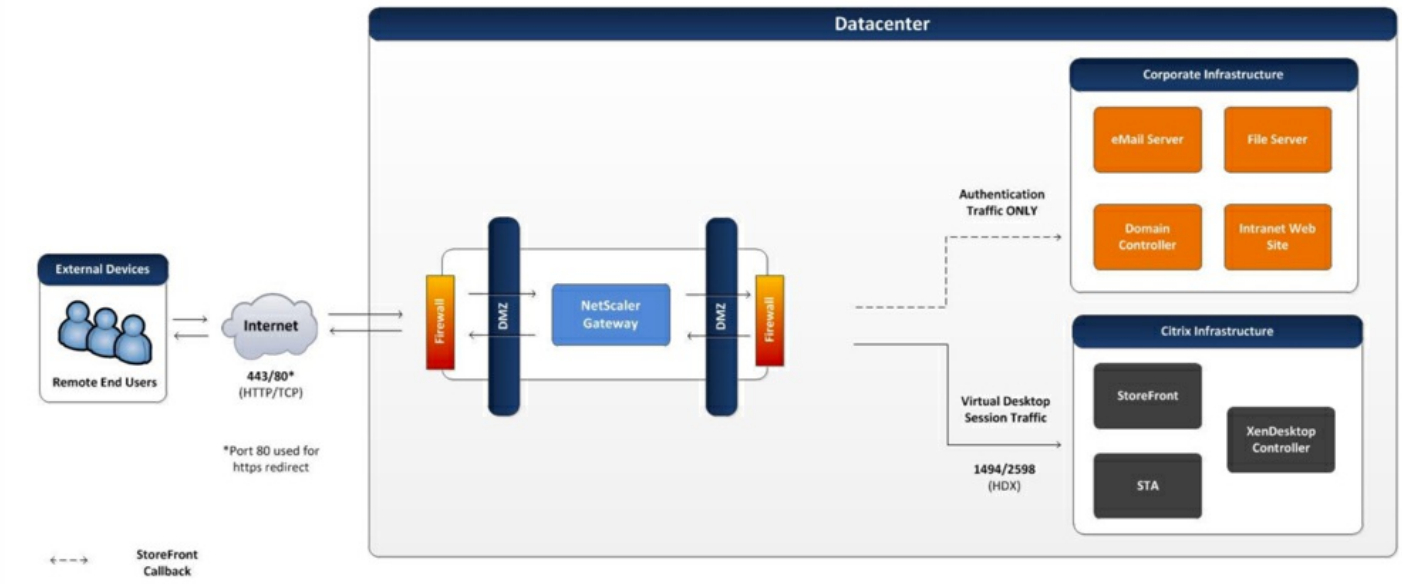
  Another decision to consider when SSLVPN is required is whether to enable split tunneling for client network traffic. By enabling split tunneling, client network traffic directed to the intranet by Citrix Receiver may be limited to routes and ports associated with specific services. By disabling split tunneling, all client network traffic is directed to the intranet, therefore both traffic destined for internal services as well as traffic destined for the external services (Internet) traverses the corporate network. The advantage of enabling split tunneling is that exposure of the corporate network is limited and network bandwidth is conserved. The advantage of disabling split tunneling is that client traffic may be monitored or controlled through systems such as web filters or intrusion detection systems

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **HDX proxy** – With HDX Proxy, users connect to their virtual desktops and applications through the NetScaler Gateway without exposing internal addresses externally. In this configuration, the NetScaler Gateway acts as a micro VPN and only handles HDX traffic. Other types of traffic on the client's endpoint device, such as private mail or personal Internet traffic do not use the NetScaler Gateway.

  Based on the endpoint and Citrix Receiver used, a decision must be made as to whether this method is supported for each user group. HDX Proxy is considered a secure access method for remote virtual desktop access since only traffic specific to the desktop session is allowed to pass through to the corporate infrastructure. Most Citrix Receivers support HDX Proxy and it is the preferred method:



Decision: Preferred Datacenter

Enterprises often have multiple active datacenters providing high availability for mission critical applications. Some virtual

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

desktops or applications may fall into that category while others may only be accessed from a specific preferred datacenter. Therefore, the initial NetScaler Gateway that a user authenticates to in a multi-active datacenter environment may not be within the preferred datacenter corresponding to the user's VDI resources. StoreFront is able to determine the location of the user's assigned resources and direct the HDX session to those resources; however, the resulting path may be sub-optional (WAN connection from the NetScaler Gateway to the virtual desktop/application resources as opposed to LAN connection).

There are static and dynamic methods available to direct HDX sessions to their virtual desktop resources in their primary datacenter. The decision regarding which method to select should be based on the availability of technology to dynamically assign sites links such as Global Server Load Balancing (GSLB) along with the network assessment of intranet and Internet bandwidth as well as Quality of Service (QoS) capabilities.

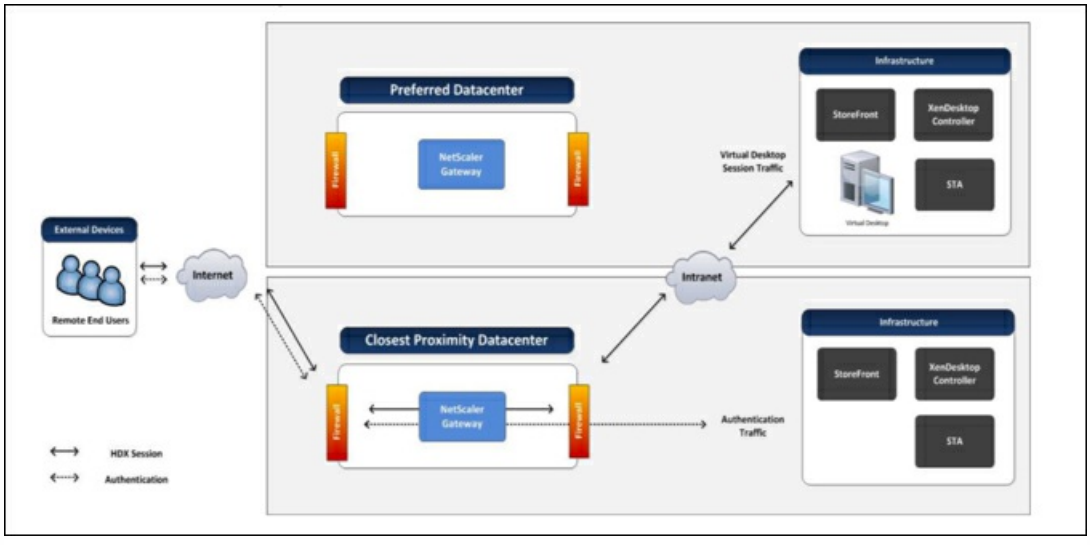
> ## Nota
>
> For more information on configuring the static and dynamic methods of GSLB, please refer to Citrix Product Documentation - Configuring GSLB for Proximity.

Static

- **Direct** – The user may be given a FQDN mapped to an A record that is dedicated to the primary datacenter NetScaler Gateway(s) allowing them to access their virtual desktop directly wherever they are in the world. This approach eliminates a layer of complexity added with dynamic allocation. However, it also eliminates fault tolerance options such as the ability to access the virtual desktop through an alternative intranet path when a primary datacenter outage is limited to the access infrastructure.

Dynamic

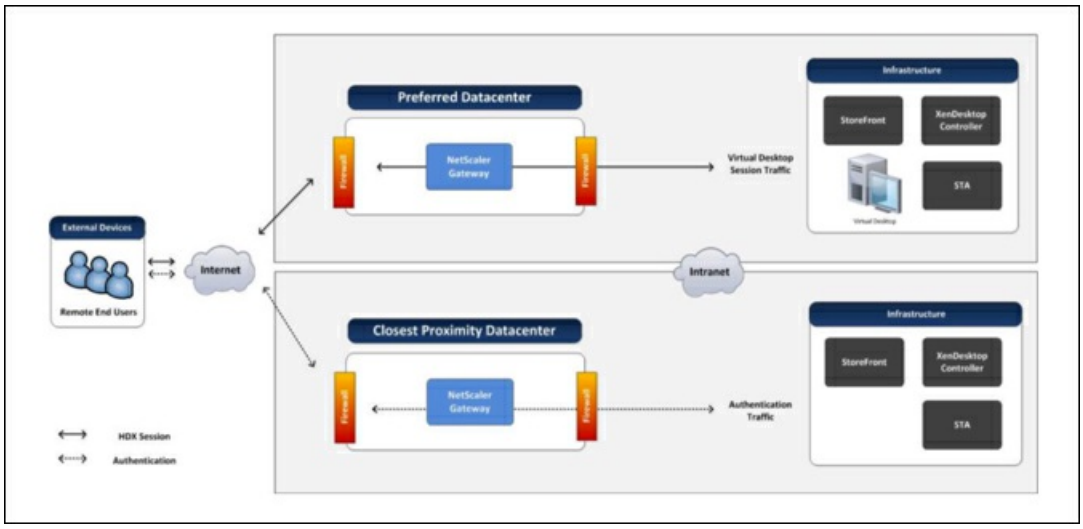
- **Intranet** – For most dynamic environments, the initial datacenter selected for authentication is the one closest to the user. Protocols such as GSLB dynamic proximity calculate the least latency between the user's local DNS server and the NetScaler Gateway. Thereafter, by default, the HDX session is routed through the same NetScaler Gateway to whichever datacenter is hosting the user's virtual desktops and applications. The advantage of this approach is that the majority of the HDX session would traverse the corporate WAN where quality of service may be used.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Internet** - Alternatively, the HDX session can be re-routed through an alternate NetScaler Gateway proximate to the backend VDI desktop / XenApp server, resulting in most of the HDX session travelling over the Internet. For example, a user with a dedicated desktop in the United Stated, traveling in Europe may be directed to a NetScaler Gateway hosted in a European datacenter based on proximity. However, when the user launches their desktop, an HDX connection will be established to the virtual desktop via a NetScaler Gateway hosted in the preferred datacenter in the United States.

  This conserves WAN network usage (at the cost of QoS) and is recommended in cases where the user's Internet connection may provide a more reliable experience than the corporate WAN.



Some customers will use a combination of these methods, such as geo-specific dynamic URLs such that fault tolerance is provided within a geographic area (such as North America) without incurring the complexity of global GSLB.

Site-to-Site Connectivity

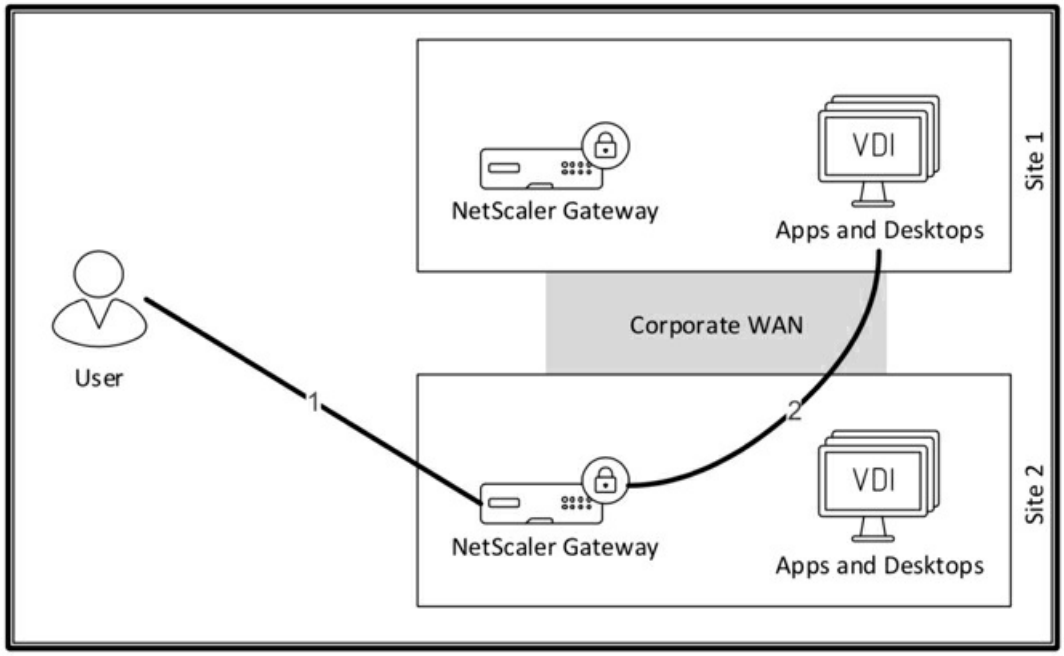
A XenApp and XenDesktop site is capable of spanning multiple locations, In order to successfully implement a multi-site solution, the design must take into account the site-to-site links and XenApp and XenDesktop session routing between locations in order to provide the best user experience.

Decision: HDX Optimized Routing

In a multi-site XenApp and XenDesktop solution, certain criteria, like fastest response time or closest proximity, routes users to the optimal site. These algorithms do not take into account the resources a user wants to access.

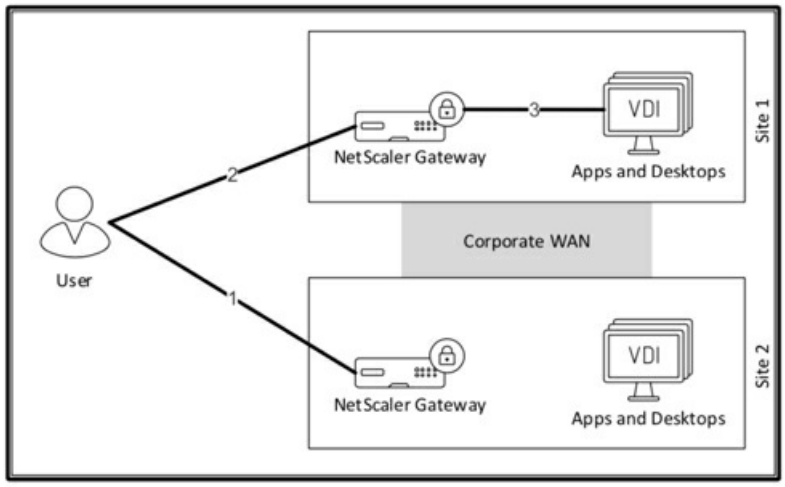
Improper routing of a user's session results in the following:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. User routed to the most preferred site, based on proximity or response time
2. NetScaler Gateway proxies the ICA traffic to the correct resource, which could be across the corporate WAN.

Ideally, optimized routing should resemble the following:



1. User routed to the most preferred site, based on proximity or response time
2. Based on the selected resource, NetScaler Gateway reroutes the session to a NetScaler Gateway in the preferred site.
3. NetScaler Gateway proxies the ICA traffic to the correct resource, which stays on the local LAN.

Using the optimized HDX routing option within StoreFront offloads traffic from the corporate WAN and places it on the public network

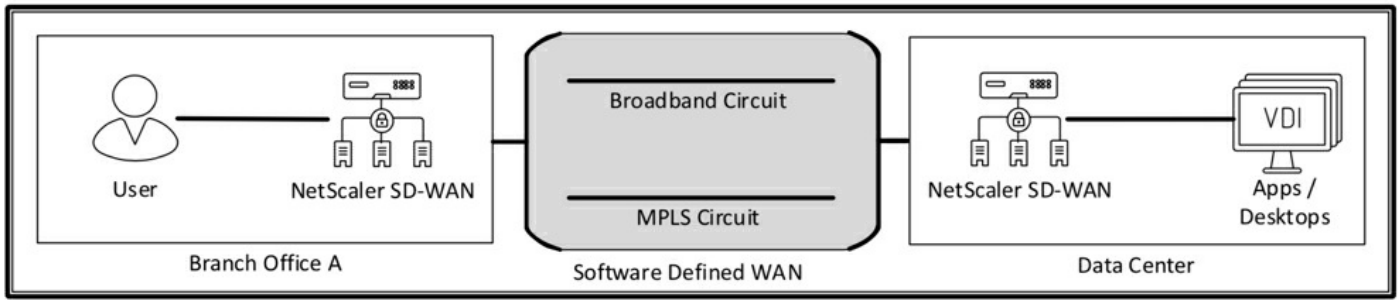
Decision: Virtual WAN

In branch office scenarios, a XenApp and XenDesktop design must evaluate the branch office's connection to the data centers hosting the application and desktop resources. If the WAN connection between the branch office and data center

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

is not able to meet the user requirements, the overall user experience degrades. Organizations have a couple of options on their WAN connections:

- **Scale Up** – Organizations can simply increase the size of the WAN pipe connecting the branch offices to the data center, typically at a sizable cost.
- **Scale Out** – Organizations can maintain their current WAN connection and augment it with multiple low-cost alternatives. The integration of all connections between the branch office and data center creates a software defined virtual WAN, like NetScaler SDWAN. The appliance sends duplicate network packets across all WAN connections defined within the virtual WAN. The appliance on the other end of the WAN uses the first arriving packet, discarding all subsequent packets. As the conditions of the multiple links change throughout the day, this approach guarantees the best experience possible.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology resource layer

Apr 24, 2018

The resource layer is the third layer of the design methodology and the final layer focused specifically on the user groups.

The overall user acceptance of the solution is defined by the decisions made within the resource layer. Profiles, printing, applications and overall desktop image design play a pivotal role in how well the desktop is aligned with the user group's requirements, which were identified within the assess phase.

User Experience

Perception is everything when it comes to a good VDI experience. Users expect an experience similar to or better than that of a traditional, physical desktop.

Codecs, transport protocols and self-service capabilities affects the overall experience. Poor quality graphics, lagging video or 120 second logon times can destroy the user experience. A proper user experience design can meet any network challenge.

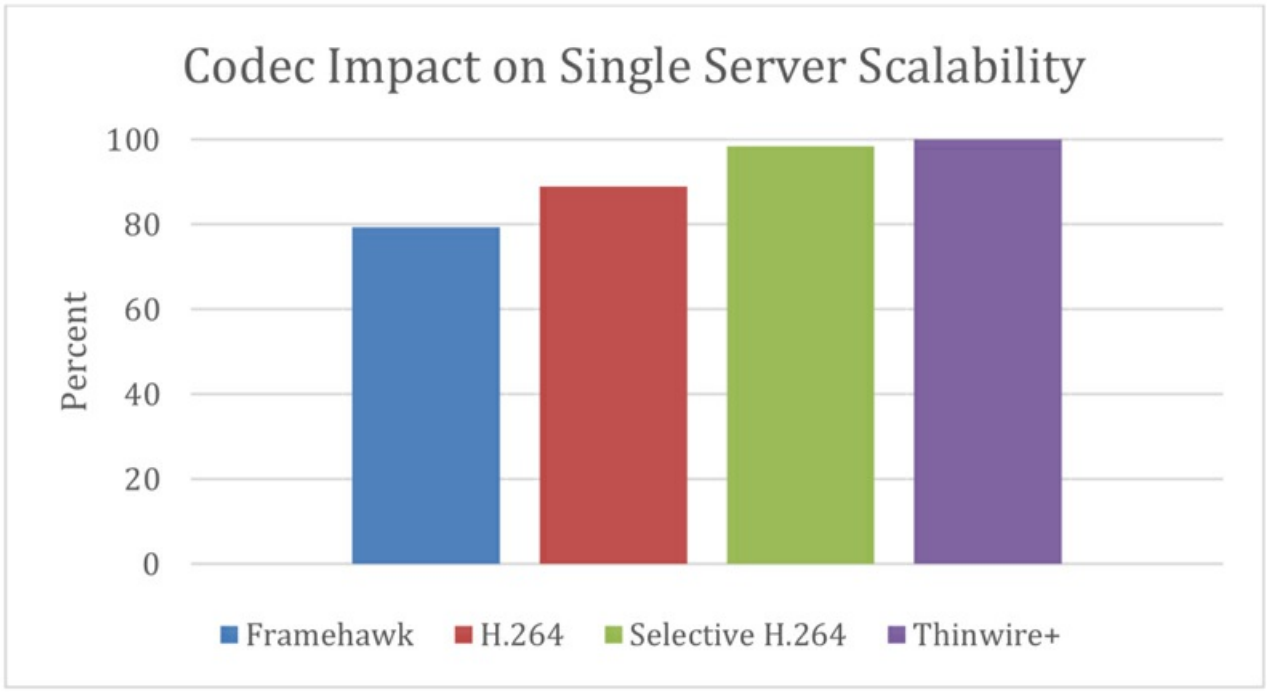
Decision: Display Protocol

Selecting the correct display protocol determines the quality of static images, video and text within the user's session as well as determining the impact on single server scalability. Administrators have the following options:

- Legacy - optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+).
- Desktop Composition Redirection – offloads desktop Windows manager DirectX commands to the endpoint, but only supports a Windows desktop VDA. Plus, in the 7.15 LTSR release, Desktop Composition Redirection is a depreciated feature.
- Framehawk – a UDP-based protocol that is able to provide high refresh rates in environments with high latency and high packet loss scenarios at the cost of greater network bandwidth utilization, commonly found on broadband wireless connections.
- H.264 – Often referred as the video codec, which provides the highest frame rates required for high quality video while saving network bandwidth. It does come at the expense of CPU processing time, reducing single server scalability. H.264 is the preferred codec when users predominately use multimedia applications.
- Thinwire – Based on the original Citrix patents from the 1990s that thinly transfers data over a wire. Use Thinwire in the majority of use cases as it provides a good user experience with minimal resource costs. There are two variations of Thinwire:
  - Legacy - Optimized for Windows 7 and Windows 2008R2 graphic engines (GDI/GDI+).
  - Thinwire+ - Optimized for Desktop Windows Manager (DWM) graphics engine in Windows 8, Windows 10, Windows 2012 and Windows 2016
- Selective H.264 (Adaptive Display) - utilizes multiple codecs (H.264 and Thinwire+) simultaneously for portions of the screen
  - Do not use – Only uses Thinwire+ and not H.264. Best for users without server-rendered video or other graphically intense applications.
  - For entire screen – Only uses H.264. Best for users with heavy use of server-rendered video and 3D graphics, especially in low-bandwidth situations.
  - For actively changing regions – Uses H.264 for the portions of the screen that are constantly changing while the remainder of the screen uses Thinwire+. This is the best option for most users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Selecting the right codec not only has an impact on the overall user experience, but also on the scalability of the server.



Decision: Transport Protocol

There are three ways to transport the HDX protocol across the network:

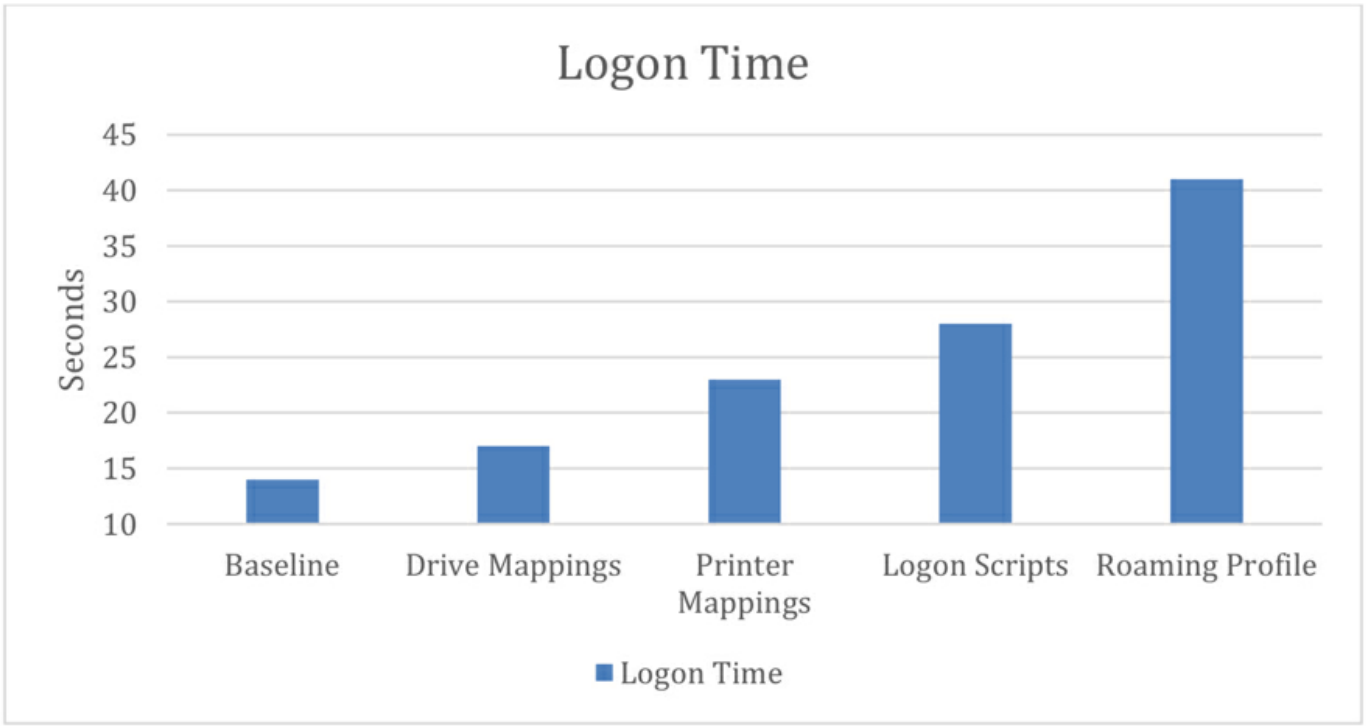
- **TCP** – Uses the industry standard TCP transport protocol. Common transport protocol over LAN and low-latency WAN connections, but suffers when connection distances increases, thus increasing latency and incurring more retransmissions.
- **EDT** – Uses a Citrix proprietary transport protocol called Enlightened Data Transport, based on UDP. Meant for high latency/packet loss networks, most common on long-distance WAN links. Provides a more interactive experience for the user without increasing CPU load on the server, but consumes more network bandwidth than TCP.
- **Adaptive Transport** – Uses TCP and EDT transport protocols. EDT used unless the network does not support transporting EDT over the network, which then automatically changes to TCP.

Most environments will use Adaptive Transport as the standard transport option unless the network does not have the appropriate firewall ports opened or NetScaler Gateway configured appropriately.
Decision: Logon Optimization

Every time a user logs onto a XenApp/XenDesktop session, the logon process must complete, which includes session initialization, user profile loading, group policy preferences execution, drive mapping, printer mapping, logon script execution and desktop initialization. Each process takes time and increases logon duration.

Most organizations include many mappings and complex logon scripts. When each of these items executes, the logon time drastically increases.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Workspace Environment Management removes drive mappings, printer mappings, logon scripts and roaming profiles from the standard logon process. With logon optimization, Workspace Environment Management applies the mappings/scripts/profiles in the background after the session and desktop initializes. The user receives the same environment but they receive their desktop interface faster. To learn more, review the following Logon Optimization video.

Most environments should enable logon optimization as a default configuration.

Decision: User Self Service

Self-service allows users to modify, update and troubleshoot their environments on their own without requiring help desktop intervention. Most organizations have policies in place that require users to change their passwords every 60-90 days. When users have multiple endpoint devices with saved passwords, it is extremely easy for their account to be locked out until each device is updated.

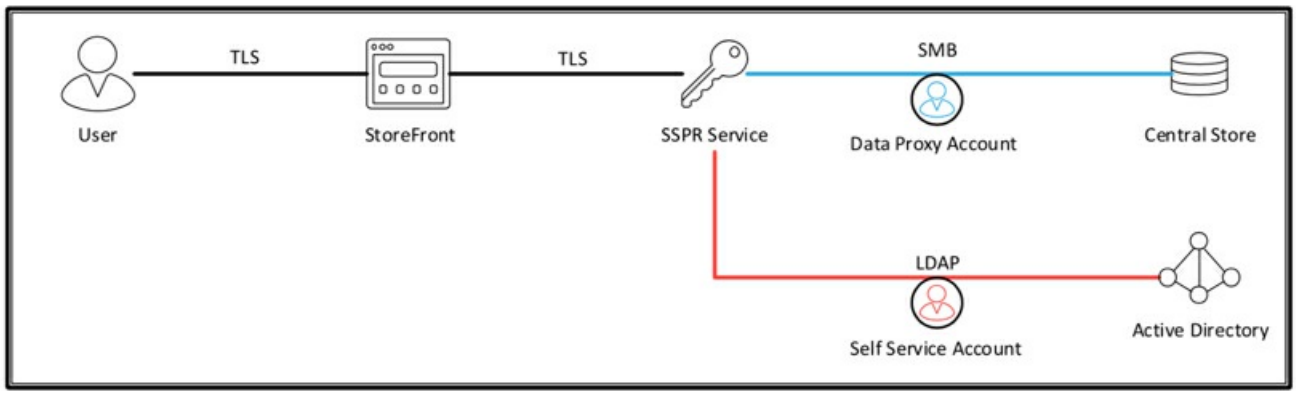
With StoreFront, can save time by self-servicing their own accounts with the following capabilities:

- **Account Unlock** – When the user's account is locked due to too many failed logon attempts, common with multiple devices, they can unlock their account if they know answers to their security questions.
- **Password Reset** – When users forgot their newly created password, they can reset their password if they know the answers to their security questions.

The self-service password reset architecture introduces the SSPR Service, Central Store and two accounts:

- **Data Proxy Account** – Responsible for accessing the central store, which contains encrypted answers to the user's security questions.
- **Self Service Account** – An Active Directory account with password reset and account unlock rights.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



In addition, properly designing self-service password reset requires the admin to create security questions that users will answer. Ideally, admins should create groups of questions around different categories then require users to answer a subset of questions for each group. The questions must be something the user knows that does not change and is not known by others.

User Profiles

A user's profile plays a critical role in delivering a consistently positive experience within a virtual desktop or virtual application scenario. Even a well-designed virtual desktop solution can fail if users are frustrated due to lengthy logon times or lost settings.

The user profile solution chosen must align with the personalization characteristics of the user group captured during the assess phase as well as the VDI model selected.

Decision: Profile Type

This section provides an overview on the different profile types available and provides guidance on the optimal user profile for each VDI model.

- **Local profiles** – Local profiles are stored on each server or desktop operating system and are initially created based on the default user profile. Therefore, a user accessing these resources would create an independent profile on each system. Users are able to retain changes to their local profile on each individual system, but changes are only accessible for future sessions on that system. Local profiles require no configuration; if a user logging into a server or desktop operating system does not have a profile path administratively defined, a local profile is created by default.
- **Roaming profiles** – Roaming profiles are stored in a centralized network repository for each user. Roaming profiles differ from local profiles in that the information in the profile (whether it is a printer, a registry setting, or a file stored in the documents folder) can be made available to user sessions accessed from all systems in the environment. Configuring a user for a roaming profile requires an administrator to designate the user's profile path (for virtual desktops) or terminal server profile path to a particular network share. The first time the user logs on to a server or desktop operating system, the default user profile is used to create the user's roaming profile. During logoff, the profile is copied to the administrator-specified network location.
- **Mandatory profiles** – Mandatory profiles are typically stored in a central location for many users. However, the user's changes are not retained at logoff. Configuring a user for a mandatory profile requires an administrator to create a mandatory profile file (NTUSER.MAN) from an existing roaming or local profile and assign users with a terminal services profile path. This can be achieved by means of Microsoft Group Policy, customizing the user properties in Active Directory or Citrix Profile Management.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Hybrid profiles** – Hybrid profiles combine a robust profile core (a mandatory profile or a local default profile) with user specific registry keys or files that are merged during logon. This technique enables administrators to tightly control which changes are retained and to keep the user profiles small in size. Furthermore, hybrid profiles address the last write wins issue using mature queuing techniques that automatically detect and prevent simultaneous writes that could potentially overwrite changes made in another session. Thus minimizing user frustration resulting from lost profile changes when accessing multiple servers or virtual desktops simultaneously. In addition, they capture and record only the changes within the profile, rather than writing the entire profile at logoff. A good example of a hybrid profile solution is Citrix Profile Management, which will be discussed in detail within this chapter.
  The following table compares the capabilities of each profile type.

  In the table:
  - **Y** indicates Functionality available.
  - **o** indicates Optional.
  - **N** indicates Functionality not available.

Feature	Local	Roaming	Mandatory	Hybrid
Central management / roams with user	N	Y	o	Yes
User settings are stored persistently	Y	Y	N	Yes
Granular capture of user settings	N	N	N	Yes

In order to select the optimal profile type for each user group it is important to understand their personalization requirements in addition to the VDI model assigned.

The following table provides recommendations on selecting the appropriate user profile type based on VDI resource:

In the table:

- **Y** indicates Recommended.
- **X** indicates Not Recommended.
- **o** indicates Viable.

	Local	Roaming	Mandatory	Hybrid
User setting persistence required (personalization characteristic: basic / complete)				
Hosted Windows App	X	Y	X	Y
Hosted Browser App	X	Y	X	Y

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hosted Shared Desktop	X	Y	X	Y
Hosted Pooled Desktop	X	Y	X	Y
Hosted Personal Desktop	º	Y	X	Y
Hosted Pro Graphics Desktop	º	Y	X	Y
Local Streamed Desktop	X	Y	X	Y
Local VM Desktop	Y	º	X	º
Remote PC Access	Y	º	X	º
User setting persistence not required or not desired (personalization characteristic: none)				
Hosted Windows App	X	X	Y	X
Hosted Browser App	X	X	Y	X
Hosted Shared Desktop	X	X	Y	X
Hosted Pooled Desktop	Y	X	Y	X
Hosted Personal Desktop	X	X	Y	X
Hosted Pro Graphics Desktop	º	X	Y	X
Local Streamed Desktop	Y	X	Y	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Local VM Desktop	o	X	Y	X
Remote PC Access	o	X	Y	X

Decision: Folder Redirection

Redirecting special folders can supplement any of the described profile types. While redirecting profile folders, such as user documents and favorites, to a network share is a good practice to minimize profile size, architects need to be aware that applications may frequently read and write data to profile folders such as AppData, causing potential issues with file server utilization and responsiveness. It is important to thoroughly test profile redirection before implementation in production to avoid these issues. Therefore, it is important to research profile read / write activities and to perform a pilot before moving to production. Microsoft Outlook is an example of an application that regularly performs profile read activities, as the user signature is read from the user profile every time an email is created.

The following table provides general recommendations to help identify the appropriate folders to redirect:

In the table:

- **Y** indicates Recommended.
- **X** indicates Not Recommended.
- **o** indicates Viable.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Folder	Local	Roaming	Mandatory	Hybrid
Application Data	X	o	X	o
Contacts	X	Y	X	o
Desktop	X	Y	X	o
Downloads	X	o	X	o
Favorites	o	Y	o	Y
Links	X	Y	X	o
My Documents	o	Y	o	Y
My Music	o	Y	o	o
My Pictures	o	Y	o	o
My Videos	o	Y	o	o
Saved Games	X	o	X	o
Searches	X	Y	X	o
Start Menu	X	X	X	X

Decision: Folder Exclusion

Excluding folders from being persistently stored as part of a roaming or hybrid profile can help to reduce profile size and logon times. By default Windows excludes the AppData\Local and AppData\LocalLow folders, including all subfolders, such as History, Temp and Temporary Internet Files. In addition, the downloads and saved games folders should also be excluded. All folders that are redirected should be excluded from the profile solution.

Decision: Profile Caching

Local caching of roaming or hybrid user profiles on a server or virtual desktop is default Windows behavior and can reduce login times and file server utilization / network traffic. With profile caching, the system only has to download changes made

© 1999-2017 Citrix Systems, Inc. All rights reserved.

to the profile. The downside of profile caching is that it can consume significant amounts of local disk storage on multi-user systems, such as a hosted shared desktop hosts.

In certain VDI models and configurations, the VDI resource is reset to a pristine state. Having locally cached profiles be deleted upon logoff is an unnecessary consumption of resources. Based on this, the leading recommendation is to not deleting locally cached profiles for the following VDI models:

- Hosted Personal Desktops
- Hosted Pooled Desktops – only in situations where a reboot occurs after logoff.
- Local VM Desktops
- Remote PC Access

Configuring the "Delay before deleting cached profiles" Citrix policy sets an optional extension to the delay before locally cached profiles are deleted at logoff. Extending the delay is useful if a process keeps files or the user registry hive open during logoff. This can also reduce logoff times for large profiles.

Decision: Profile Permissions

For security reasons, administrators, by default, cannot access user profiles. While this level of security may be required for organizations that deal with very sensitive data, it is unnecessary for most environments and can complicate operations and maintenance. Therefore, consider enabling the "Add the Administrators security group to roaming user profiles" policy setting. The configuration of this policy should be aligned with the security characteristics of the user groups captured during the assess phase. For more information on the permissions required for the file share hosting user profiles and data, please refer to Microsoft TechNet - Deploying Roaming Profiles.

Decision: Profile Path

Determining the network path for the user profiles is one of the most significant decisions during a user profile design process. In general, it is strongly recommended to leverage a redundant and high performance file server or NAS device. There are four topics that must be considered for the profile share:

- **Performance** – File server performance will affect logon and logoff times, and depending on other decisions such as redirected folders and profile streaming, can impact the user's experience within the session. For large virtual desktop infrastructures, a single file server cluster may not be sufficient to handle periods of peak activity. In order to distribute the load across multiple file servers, the file server address and share name will need to be adjusted.
- **Location** – User profiles are transferred over the network by means of the SMB protocol, which does not perform well on high-latency network connections. Furthermore, WAN connections are typically bandwidth constrained, which can add additional delay to the profile load process. Therefore, the file server should be located in close proximity to the servers and virtual desktops to minimize logon times.
- **Operating system platforms** – User profiles have a tight integration with the underlying operating system and it is not supported to reuse a single user profile on different operating systems or different platforms like 64-Bit (x64) and 32-Bit (x86).
  For more information, please refer to the Microsoft knowledge base article KB2384951 – Sharing 32 and 64-bit User Profiles. Windows 2008 and Windows Vista introduced a new user profile structure, which can be identified by .V2 profile directory suffix, which makes older user profiles incompatible with newer operating systems such as Windows 2012, 7 and 8. In order to ensure that a separate profile is used per platform, the profile directory has to be adapted.
- **Indexing capabilities** – To take full advantage of Windows Search functionality on a user's redirected data, Windows file servers that index the user's data must be used, as opposed to a share on a NAS appliance. This is important for use cases that are heavily dependent on Windows Search or are especially sensitive to perception of slowness or latency

© 1999-2017 Citrix Systems, Inc. All rights reserved.

There are two methods that can be used to address these challenges that are based on Windows built-in technology:

- **User object** – For every user object in Active Directory, an individual profile path, which contains file server name and profile directory, can be specified. Since only a single profile path can be specified per user object, it is not possible to ensure that a separate profile is loaded for each operating system platform.
- **Computer group policy** or **system variables** – The user profile path can also be configured by means of computer specific group policies or system variables. This enables administrators to ensure that a user profile is dedicated to the platform. Since computer specific configurations affect all users of a system, all user profiles will be written to the same file server. To load balance user profiles across multiple servers dedicated XenDesktop delivery groups have to be created per file server.

Note: Microsoft does not support DFS-N combined with DFS-R for actively used user profiles.

For more information, please refer to the Microsoft articles:

- Information about Microsoft support policy for a DFS-R and DFS-N deployment scenario
- Microsoft Support Statement Around Replicated User Profile Data

When using Citrix Profile Management, a third option is available to address these challenges:

User object attributes and variables – Citrix Profile Management enables the administrator to configure the profile path by means of a computer group policy using attributes of the user object in Active Directory to specify the file server dynamically. In order to achieve this, three steps are required:

1. Create a DNS alias (for example, fileserver1) that refers to the actual file server
2. Populate an empty LDAP attribute of the user object (for example, l or UID) with the DNS Alias
3. Configure Citrix Profile Management by means of GPO to use a profile path that refers to the LDAP attribute (for example, if attribute UID is used the profile path becomes \\#UlD#\Profiles\profiledirectory)

In addition, Citrix Profile Management automatically populates variables to specify the profile path dynamically based on the operating system platform. Valid profile management variables are:

- !CTX_PROFILEVER! – Expands to v1 or v2 depending on the profile version.
- !CTX_OSBITNESS! – Expands to x86 or x64 depending on the bit-level of the operating system.
- !CTX_OSNAME! – Expands to the short name of the operating system, for example- Windows 7.

By combining both capabilities of Citrix Profile Management, a fully dynamic user profile path can be created, which can be load balanced across multiple file servers and ensure profiles of different operating system platforms are not mixed. An example of a fully dynamic user profile path is shown below:

\\#UID#\profiles$\%USERNAME%.%USERDOMAIN%\!CTX_OSNAME!!CTX_OSBITNESS!

Decision: Profile Streaming

Note: The following design decision only applies to those environments that use Citrix Profile Management.

With user profile streaming, files and folders contained in a profile are fetched from the user store (file server) to the local computer when a user accesses them. During the logon process, Citrix Profile Management immediately reports that the profile load process has completed reducing profile load time to almost zero.

Citrix recommends enabling profile streaming for all scenarios. If it is desired to keep a local cached copy of the user profile for performance reasons, it is recommended to enable the “Always Cache” setting and configure a size of 0. This ensures

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

that the user profile is downloaded in the background and enables the system to use this cached copy going forward.

Experience from the Field

- General – Some poorly written applications might load faster if their AppData has already been streamed to the VDI resource. Enabling the "Always Cache" option for profile streaming can help improve performance when the AppData folder is not redirected.

Decision: Active Write Back

Note: The following design decision only applies to those environments that use Citrix Profile Management.

By enabling the active write back feature, Citrix Profile Manager detects when an application has written and closed a file and copies the file back to the network copy of the profile during idle periods. In scenarios where a single user leverages multiple virtual desktops or hosted shared desktops simultaneously, this feature can be tremendously beneficial. However, Citrix Profile Management does not copy any registry changes back to the network, except during an ordered logoff. As such, there is a risk that the registry and files may get out of alignment on non-persistent systems, where locally cached profile information is wiped upon reboot. Therefore, it is recommended to disable active write back functionality for non-persistent scenarios.

Decision: Configuration Approach

Note: The following design decision only applies to those environments that use Citrix Profile Management.

Citrix Profile Management can be configured by means of an ".ini" file, Microsoft Group Policy and Citrix Policy (Citrix Profile Management 5.0 and newer). While each option offers the same configuration settings, Group Policy is recommended because it allows administrators to perform Windows and Citrix profile configurations from a single point, minimizing the tools necessary for profile management.

Note: With Citrix Profile Management 5.0 and newer, the desktop type is automatically detected and Citrix Profile Management policies set accordingly. For more information, please refer to Citrix Docs – How automatic configuration works.

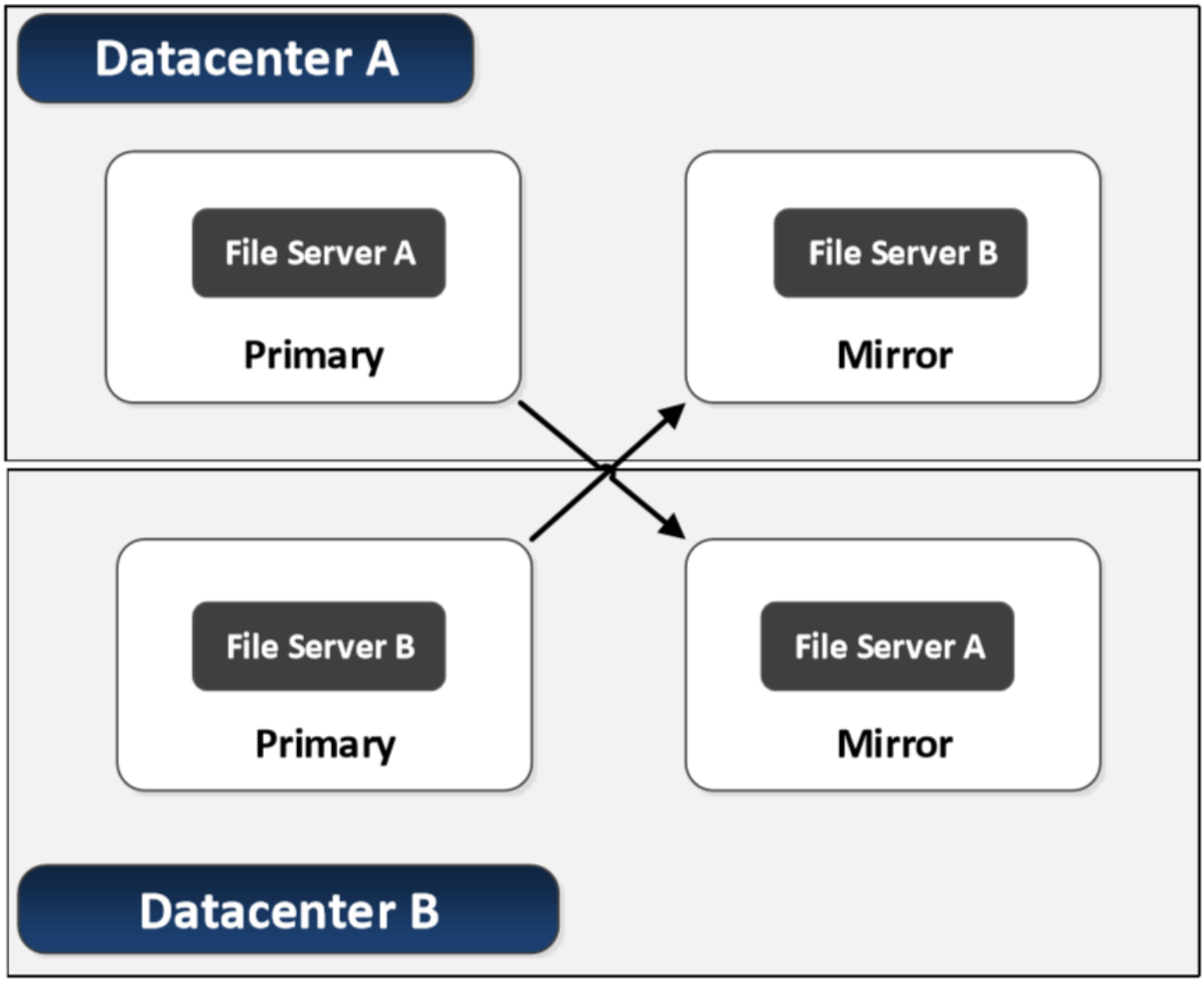
Decision: Replication

While having an active/active datacenter on a network level is easily accomplished with GSLB, the replication of user data makes having a fully active/active deployment complex in most situations. To have an active/active configuration where users are not statically assigned to a specific datacenter, will require users to have no form of personalization requirements. This will limit the user's ability to make any configuration changes and will not allow them to create any documents or persistent data. The exception to this is when a high-speed, low latency connection such as dark fiber is available between datacenters. This will let resources in both locations can point to the same file server allowing for a true active/active solution. Also, an active/active configuration can be accomplished when applications are used that rely solely on a backend database that is actively replicated between datacenters and do not store any data in the user profile.

For redundancy and failover purposes, user data such as Windows profiles and documents should be synchronized between datacenters. Although it is recommended to replicate user data between datacenters, the replication would be an active/passive configuration. This means the data can only be actively consumed from a single datacenter. The reason for this limitation is the distributed file locking method inside Windows that only allows a single user to actively write to a file. Therefore, active/active replication of user data is not supported. Any supported configuration consists of a one-way replication of data that is active in a single datacenter at any point in time.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For example, the figure below describes a scenario where user data is passively replicated from Datacenter A to Datacenter B. In this example, File Server A is the primary location for user data in Datacenter A and File Server B is the primary location in Datacenter B. One-way replication of the user data occurs for each fileserver to allow for the user data to be available in the opposite datacenter if a failover occurs. Replication technologies such as Microsoft DFS can be configured to mirror user profiles and documents to a file server in another datacenter. DFS Namespaces can also be used to have a seamless path for the location of the user data. However, implementing a replication solution like this requires an administrator familiar with Microsoft DFS and user profiles.



User Data

In order to be effective, users must access their data. The data must be in close proximity to the application for the user to have a good experience. As the distance between the application and data increases, latency also increases, which slows down any file operation (opening, saving, modifying).

In a VDI-based environment, administrators must understand where users store their data and impact of access.

Decision: User Data Location

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Users traditionally stored their data on their local device or on a network file server designated with a drive mapping. Due to IT storage space limitations or the inability to have the data follow the user to other mobile devices, users turned to free, cloud-based storage offerings like OneDrive, DropBox and Box. To get access to the data, the user would install the storage vendor's agent on their traditional Windows PC, allowing them direct access to the cloud-hosted storage repository.

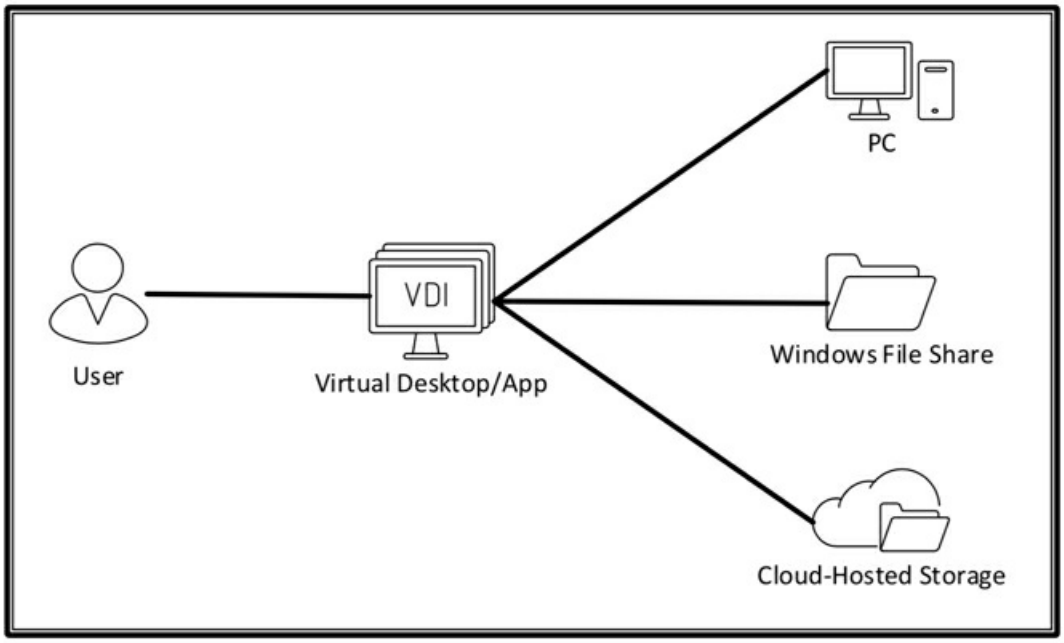
Administrators must design the solution to take into account user storage by looking at the following options:

- **Multi-Agent Strategy** – In VDI, users require the admin to install and configure the agent for each storage provider, which assumes the storage agent supports the non-persistent VDI model. Each agent is a new application that the admin must manage and maintain.
- **Storage Connector Strategy** – A single agent consolidates storage repositories from numerous cloud-hosted and on-premises providers into a single folder structure. For example, when a user connects to Citrix ShareFile, they see a consolidated folder structure containing their user data from the cloud (ShareFile, OneDrive, DropBox, Box and Google Drive) and from on-premises (SharePoint, Windows network shares and local endpoint shares).

Decision: User Data Access

A critical aspect to a successful VDI solution is for the user experience to remain the same as it was with a traditional PC. If users open files from within the application, that functionality must continue to function. If users navigate with Explorer to access a file, that functionality must continue to function.

A user's data can exist on the local PC, on a network file share and hosted in the cloud.



With local PC, on-premises network shares and cloud-hosted storage options available to users, administrators need to understand how users accessing their data affects the infrastructure and VDI experience.

- **Direct Data Access** – Users access a file on a remote server (on-premises Windows server or cloud-hosted storage provider). The distance between the application and file directly affects the experience. Longer distances equates to higher latency. Each file operation (navigate, open, close, save, etc.) takes more time as the latency between application and file storage increases. Windows file servers are often located in the same data center as the user's VDI desktop

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

making direct data access feasible; but cloud-hosted solutions and local PC Access will experience poor response times if the connection between the VDI desktop and the storage repository has high latency.

- **Local Synchronization** – With a traditional PC, users are accustomed to having files local, which mitigates any slow application response times due to extremely low latency. Many cloud-hosted solutions provide data synchronization to enable access speeds similar to a local storage model. Many of the cloud-hosted solutions provide full synchronization or user-configured partial synchronization of certain folders and files. With partial synchronization, only the synchronized files are visible and accessible on the device, causing user confusion. Full and partial synchronization increases VDI costs. Each session is an entirely new desktop requiring synchronization of user's folders/files, which takes time, network bandwidth and VDI storage space. Every file synchronized to the VDI desktop must be stored within the organization's data center for the duration of the VDI session.
- **On-Demand Synchronization** – When navigating Explorer, users see a complete, but virtual, file/folder structure even though those files/folders do not physically exist on the desktop. Selecting a file begins an automatic synchronization to the VDI desktop for that single file. At this point, file access is local, which creates a user experience like that of a traditional PC. When the user saves or closes the file, the file synchronizes back to the cloud. Only the files accessed synchronize, eliminating the waste incurred with the local data access model. Citrix ShareFile includes Drive Mapper, allowing the user to interact with their data via Explorer while utilizing on-demand synchronization when accessing a file. As only accessed files synchronize, the impact to the underlying storage infrastructure and associated storage costs are minimal.

In the table:

- **Y** indicates recommended.
- **N** indicates Not recommended.

	Direct Data Access	Local Synchronization	On-Demand Synchronization
Network File Server	Y		
Cloud-hosted	N	N	Y
Local PC	N	N	Y

Decision: Data Recovery

File corruption is an issue most users experience. Improperly shutting down the application or PC (hitting the power button instead of closing the application and shutting down the operating system gracefully) often causes many corruption issues.

A few options exist to provide users with data recovery options:

- **Multi-File** – With a traditional PC, users have few recovery options if the files are local. Users often manually create a new copy of the file each day in order to provide some level of recovery. This solution is hard to manage.
- **Backup/Restore** – Administrators can implement a backup and restore solution to help with file recovery. However, these solutions rarely work with local files and for a network file share, the backup process usually only runs nightly or weekly. In addition, restoring a corrupted file requires the user to call support.
- **Versioning** – Cloud-hosted options, like Citrix ShareFile, include file versioning, which automatically creates new versions

© 1999-2017 Citrix Systems, Inc. All rights reserved.

of the file as changes are saved. Versioning requires no user intervention and allows users to recover from corruption quickly and with little loss of data.



Uploaded	Title	Creator
7/20/17 3:22 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 2:15 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:16 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:08 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 1:07 ...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:5...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:5...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller
7/20/17 12:1...	Citrix VDI Handbook (7.15 LTSR) - v20170717.d...	D. Feller

Policies

Policies provide the basis to configure and fine tune XenApp and XenDesktop environments, allowing organizations to control connection, security and bandwidth settings based on various combinations of users, devices or connection types.

When making policy decisions it is important to consider both Microsoft and Citrix policies to ensure that all user experience, security and optimization settings are considered. For a list of all Citrix-related policies, please refer to the Citrix Policy Settings Reference.

Decision: Preferred Policy Engine

Organizations have the option to configure Citrix policies via Citrix Studio or through Active Directory group policy using Citrix ADMX files, which extend group policy and provide advanced filtering mechanisms.

Using Active Directory group policy allows organizations to manage both Windows policies and Citrix policies in the same location, and minimizes the administrative tools required for policy management. Group policies are automatically replicated across domain controllers, protecting the information and simplifying policy application.

Citrix administrative consoles should be used if Citrix administrators do not have access to Active Directory policies. Architects should select one of the above two methods as appropriate for their organization's needs and use that method consistently to avoid confusion with multiple Citrix policy locations.

It is important to understand how the aggregation of policies, known as policy precedence flows in order to understand how a resultant set of policies is created. With Active Directory and Citrix policies, the precedence is as follows:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Policy Precedence	Policy Type
Processed first (lowest precedence)	Local server policies
Processed second	Citrix policies created using the Citrix administrative consoles
Processed third	Site level AD policies
Processed fourth	Domain level AD policies
Processed fifth	Highest level OU in domain
Processed sixth and subsequent	Next level OU in domain
Processed last (highest precedence)	Lowest level OU containing object

Policies from each level are aggregated into a final policy that is applied to the user or computer. In most enterprise deployments, Citrix administrators do not have rights to change policies outside their specific OUs, which will typically be the highest level for precedence. In cases where exceptions are required, the application of policy settings from higher up the OU tree can be managed using “block inheritance” and “no override” settings. Block inheritance stops settings from higher-level OUs (lower precedence) from being incorporated into the policy. However, if a higher-level OU policy is configured with no override, the block inheritance setting will not be applied. Given this, care must be taken in policy planning, and available tools such as the “Active Directory Resultant Set of Policy” tool or the “Citrix Group Policy Modeling” wizard should be used to validate the observed outcomes with the expected outcomes.

> ## Nota
>
> Some Citrix policy settings, if used, need to be configured through Active Directory group policy, such as Controllers and Controller registration port, as these settings are required for VDAs to register.

Decision: Policy Integration

When configuring policies, organizations often require both Active Directory policies and Citrix policies to create a completely configured environment. With the use of both policy sets, the resultant set of policies can become confusing to determine. In some cases, particularly with respect to Windows Remote Desktop Services (RDS) and Citrix policies, similar functionality can be configured in two different locations. For example, it is possible to enable client drive mapping in a Citrix policy and disable client drive mapping in a RDS policy. The ability to use the desired feature may be dependent upon the combination of RDS and Citrix policy. It is important to understand that Citrix policies build upon functionality available in Remote Desktop Services. If the required feature is explicitly disabled in RDS policy, Citrix policy will not be able to affect a configuration as the underlying functionality has been disabled.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

In order to avoid this confusion, it is recommended that RDS policies only be configured where required and there is no corresponding policy in the XenApp and XenDesktop configuration, or the configuration is specifically needed for RDS use within the organization. Configuring policies at the highest common denominator will simplify the process of understanding resultant set of policies and troubleshooting policy configurations.

Decision: Policy Scope

Once policies have been created, they need to be applied to groups of users and/or computers based on the required outcome. Policy filtering provides the ability to apply policies against the requisite user or computer groups. With Active Directory based policies, a key decision is whether to apply a policy to computers or users within site, domain or organizational unit (OU) objects. Active Directory policies are broken down into user configuration and computer configuration. By default, the settings within the user configuration apply to users who reside within the OU at logon, and settings within the computer configuration are applied to the computer at system startup, and will affect all users who logon to the system. One challenge of policy association with Active Directory and Citrix deployments revolves around three core areas:

- **Citrix environment specific computer policies** – Citrix servers and virtual desktops often have computer policies that are created and deployed specifically for the environment. Applying these policies is easily accomplished by creating separate OU structures for the servers and the virtual desktops. Specific policies can then be created and confidently applied to only the computers within the OU and below and nothing else. Based upon requirements, virtual desktops and servers may be further subdivided within the OU structure based on server roles, geographical locations or business units.
- **Citrix specific user policies** – When creating policies for XenApp and XenDesktop there are a number of policies specific to user experience and security that are applied based on the user's connection. However, the user's account could be located anywhere within the Active Directory structure, creating difficulty with simply applying user configuration based policies. It is not desirable to apply the Citrix specific configurations at the domain level as the settings would be applied to every system any user logs on to. Simply applying the user configuration settings at the OU where the Citrix servers or virtual desktops are located will also not work, as the user accounts are not located within that OU. The solution is to apply a loopback policy, which is a computer configuration policy that forces the computer to apply the assigned user configuration policy of the OU to any user who logs onto the server or virtual desktop, regardless of the user's location within Active Directory. Loopback processing can be applied with either merge or replace settings. Using replace overwrites the entire user GPO with the policy from the Citrix server or virtual desktop OU. Merge will combine the user GPO with the GPO from the Citrix server or desktop OU. As the computer GPOs are processed after the user GPOs when merge is used, the Citrix related OU settings will have precedence and be applied in the event of a conflict. For more information, please refer to the Microsoft TechNet article - Understand User Group Policy Loopback Mode.
- **Active Directory policy filtering** – In more advanced cases, there may be a need to apply a policy setting to a small subset of users such as Citrix administrators. In this case, loopback processing will not work, as the policy should only be applied to a subset of users, not all users who logon to the system. Active Directory policy filtering can be used to specify specific users or groups of users to which the policy is applied. A policy can be created for a specific function, and then a policy filter can be set to apply that policy only to a group of users such as Citrix administrators. Policy filtering is accomplished using the security properties of each target policy.

Citrix policies created using Citrix Studio have specific filter settings available, which may be used to address policy-filtering situations that cannot be handled using group policy. Citrix policies may be applied using any combination of the following filters:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Filter Name	Filter Description	Scope
Access control	Applies a policy based on access control conditions through which a client is connecting. For example, users connecting through a Citrix NetScaler Gateway can have specific policies applied.	User settings
Citrix CloudBridge	Applies a policy based on whether or not a user session was launched through Citrix CloudBridge.	User settings
Client IP address	Applies a policy based on the IPv4 or IPv6 address of the user device used to connect the session. Care must be taken with this filter if IPv4 address ranges are used in order to avoid unexpected results.	User settings
Client name	Applies a policy based on the name of the user device used to connect the session.	User settings
Delivery group	Applies a policy based on the delivery group membership of the desktop running the session.	User settings
Delivery group type	Applies a policy based on the type of machine running the session. For example, different policies can be set depending upon whether a desktop is pooled, dedicated or streamed.	User and computer settings
Organizational unit	Applies a policy based on the OU of the desktop or server running the session.	User and computer settings
Tag	Applies a policy based on any tags applying to the desktop running the session. Tags are strings that can be added to virtual desktops in XenDesktop environments that can be used to search for or limit access to desktops.	User and computer settings
User or Group	Applies a policy based on the Active Directory group membership of the user connecting to the session.	User settings

Nota

Citrix policies in XenDesktop 7.x provide a merged view of settings that apply at the user and computer level. In table 24, the Scope column identifies whether the specified filter applies to user settings, computer settings, or both.

Decision: Baseline Policy

A baseline policy should contain all common elements required to deliver a high-definition experience to the majority of users within the organization. A baseline policy creates the foundation for user access, and any exceptions that may need to be created to address specific access requirements for groups of users. It should be comprehensive to cover as many use cases as possible and should have the lowest priority, for example 99 (a priority number of “1” is the highest priority), in order to create the simplest policy structure possible and avoid difficulties in determining the resultant set of policies. The unfiltered policy set provided by Citrix as the default policy may be used to create the baseline policy as it is applied to all users and connections. In the baseline configuration, all Citrix policy settings should be enabled, even those that will be

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configured with the default value, in order to explicitly define desired/expected behavior, and to avoid confusion should default settings change over time.

Citrix Policy templates can be used to configure Citrix policies to effectively manage the end-user experience within an environment and can serve as an initial starting point for a baseline policy. Templates consist of pre-configured settings that optimize performance for specific environments or network conditions. The built-in templates included in XenDesktop are shown below:

Built-in Templates	Description
High definition user experience	Includes settings for providing high quality audio, graphics, and video to users.
High server scalability	Includes settings for providing an optimized user experience while hosting more users on a single server.
Optimized bandwidth for WAN	Includes settings for providing an optimized experience to users with low bandwidth or high latency connections.
Security and control	Includes settings for disabling access to peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices.

For more information on Citrix policy templates, please refer to Citrix Docs - Manage Citrix Policy Templates.

A baseline policy configuration should also include Windows policies. Windows policies reflect user specific settings that optimize the user experience and remove features that are not required or desired in a XenDesktop environment. For example, one common feature turned off in these environments is Windows update. In virtualized environments, particularly where desktops and servers may be streamed and non-persistent, Windows update creates processing and network overhead, and changes made by the update process will not persist a restart of the virtual desktop or application server. Also in many cases, organizations use Windows software update service (WSUS) to control Windows updates. In these cases, updates are applied to the master disk and made available by the IT department on a scheduled basis.

In addition to the above considerations, an organization's final baseline policy may include settings specifically created to address security requirements, common network conditions, or to manage user device or user profile requirements:

Printing

Citrix XenApp and Citrix XenDesktop support a variety of different printing solutions. In order to plan and successfully implement the proper printing solution it is important to understand the available technologies as well as their benefits and limitations.

Decision: Printer Provisioning

The process of creating printers at the start of a XenApp or XenDesktop session is called printer provisioning. There are multiple approaches available:

- **User Added** – Allowing users to manually add printers gives them the flexibility to select printers by convenience. The drawback to manually adding network-based printers is that it requires the users to know the network name or path of the printers. There is also a chance that the native print driver is not installed in the operating system and the Citrix

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Universal Print Driver is not compatible, thereby requiring the user to seek administrative assistance. Manually adding printers is best suited in the following situations:

- Users roam between different locations using the same client device (i.e. laptop, tablet).
- Users work at assigned stations or areas whose printer assignments will rarely change.
- Users have personal desktops with sufficient rights to install necessary printer drivers.

- **Auto Created** – Auto-creation is a form of dynamic provisioning that attempts to create some or all of the available printers on the client device at the start of a user session. This includes locally attached printers as well as network-based printers. Auto-creating all client printers can increase the session logon time as each printer is enumerated during the logon process.
- **Session Based** – Session printers are a set of network-based printers assigned to users through a Citrix policy at the start of each session.
  - Proximity based session printers are filtered by IP subnet. The network printers created under this policy may vary based on where the user's endpoint device is located. Proximity printing is recommended in situations where: Users roam between different locations using the same endpoint device (i.e. laptop, tablet) and where thin clients are used, which do not have the ability to connect to network-based printers directly.
  - Session printers may be assigned using the "Session Printer" policy or the "Printer Assignments" policy. The "Session printer" policy is intended to be used to set default printers for a farm, site, large group, or OU. The "Printer Assignments" policy is used to assign a large group of printers to multiple users. If both policies are enabled and configured, the session printers will be merged into a single list.
- **Universal Printer** – The Citrix Universal Printer is a generic printer object that is autocreated at the start of a session and is not linked to a printing device. When using the Citrix Universal Printer, it is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. By default, the Citrix Universal Printer will print to the client's default printer, however the behavior can be modified to allow the user to select any of their compatible local or network-based printers.

The Citrix Universal Printer is best suited for the following scenarios:

- The user requires access to multiple printers both local and network-based which may vary with each session.
- The user's logon performance is a priority and the Citrix policy "Wait for printers to be created" must be enabled due to application compatibility.
- The user is working from a Windows based device or thin client.

> ### Nota
>
> Other options for provisioning printers, such as Active Directory group policy, "follow-me" centralized print queue solutions, and other 3rd party print management solutions can be used to provision printers into a Citrix session.

Decision: Printer Drivers

Managing print drivers in XenApp and XenDesktop can be a tedious task, especially in large environments with hundreds of printers. In XenApp and XenDesktop there are several methods available to assist with print driver management.

- **User Installed** – When adding a printer within a XenApp or XenDesktop session and the native print driver is not available, the drivers can be installed manually, by the user. Many different print drivers can potentially be installed on different resources creating inconsistencies within the environment. Troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, user installed drivers is not recommended.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Automatic Installation** – When connecting a printer within a XenApp or XenDesktop session, a check is made to see if the required print driver is already installed in the operating system. If the print driver is not already installed, the native print driver, if one exists, will be installed automatically. If users roam between multiple endpoints and locations, this can create inconsistencies across sessions since users may access a different hosted resource every time they connect. When this type of scenario occurs, troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, automatic installed drivers is not recommended.
- **Universal Print Driver** – The Citrix Universal Printer Driver (UPD) is a device independent print driver, which has been designed to work with most printers. The Citrix Universal Printer Driver (UPD) simplifies administration by reducing the number of drivers required on the master image. For auto created client printers, the driver records the output of the application and sends it, without any modification, to the end-point device. The endpoint uses local, device-specific drivers to finish printing the job to the printer. The UPD can be used in conjunction with the Citrix Universal Print Server (UPServer) to extend this functionality to network printers.

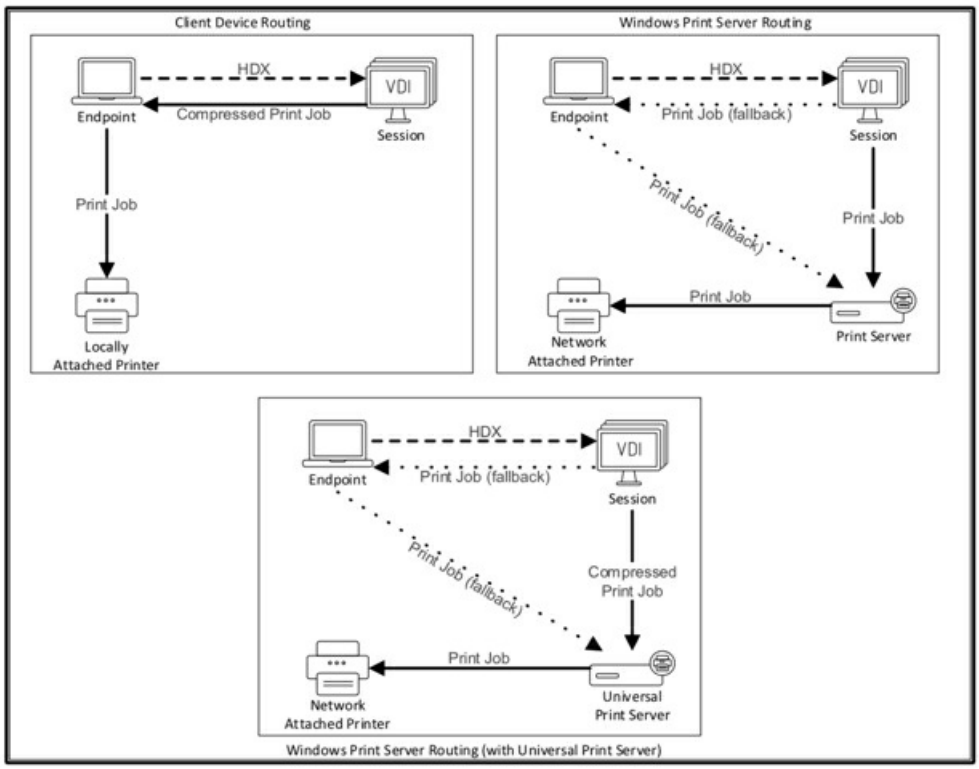
Decision: Printer Routing

Print jobs can be routed along different paths: through a client device or through a print server.

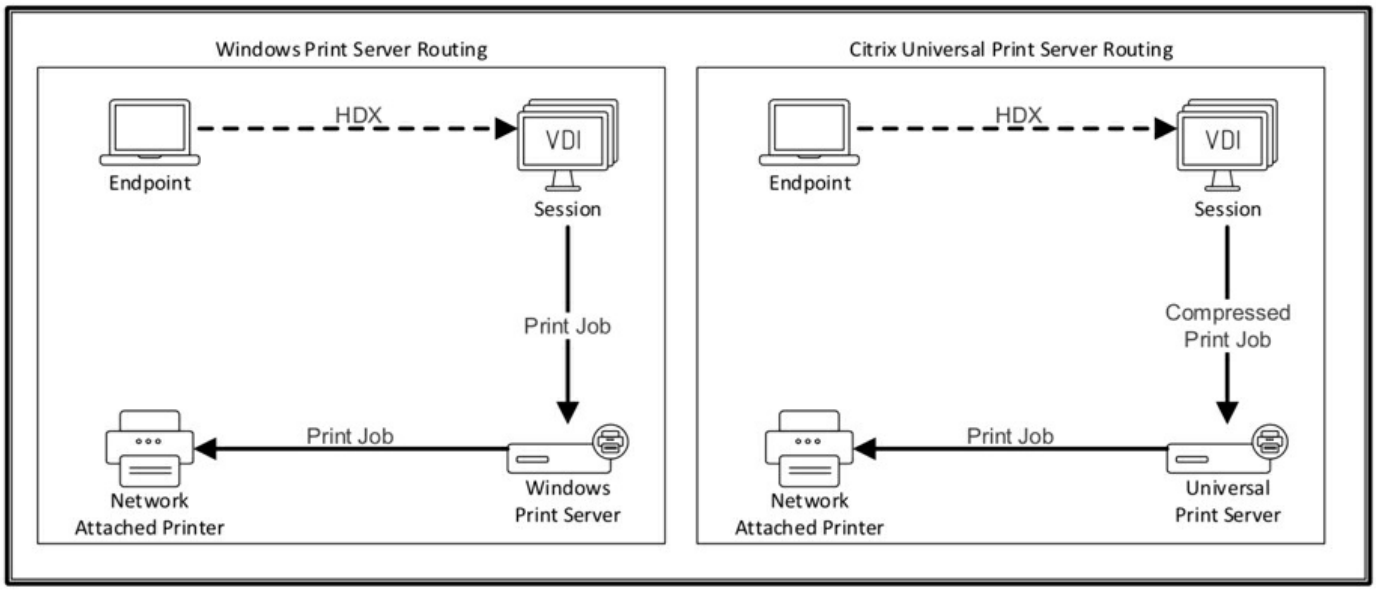
- **Client Device Routing** – Client devices with locally attached printers (printers attached through USB, LPT, COM, TCP, etc.) will route print jobs directly from the client device to the printer.
- **Windows Print Server Routing** – By default, print jobs sent to auto-created networkbased printers will be routed from the user's session to the print server. However, the print job will take a fallback route through the client device when any of the following conditions are true:
  - The session cannot contact the print server
  - The print server is on a different domain without a trust established.
  - The native print driver is not available within the user's session
- **Citrix Universal Print Server Routing** – Print job routing follows the same process as Windows Print Server Routing except that the Universal Print Driver is used between the user's session and the Citrix Universal Print Server.

The specifics with print job routing are based on the printer provisioning method. Auto-created and user-added printers can route print jobs based on the following diagrams:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



However, if the printers are provisioned as session printers, the print job routing options changes slightly. The jobs are no longer able to route through the user's endpoint device.



The recommended option is based on the network location of the endpoint device, the user's session and the print server.

- **Client Device Routing**
  - Use for locally attached printer implementations.
  - Use if a Windows endpoint device and printer are on the same high-speed, lowlatency network as the Windows Print

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Server.

- **Windows Print Server Routing**
  - Use if the printer is on the same high-speed, low-latency network as the Windows Print Server and user session.
- **Windows Print Server Routing (with Universal Print Server)**
  - Use if non-Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.

Decision: Print Server Redundancy

Network-based printers, managed with a Microsoft print server or the Citrix Universal Print Server should be configured with redundancy in order to eliminate a single point of failure. The Citrix Universal Print Server redundancy should be defined within a Citrix Policy.

Experience from the Field

A print media company leverages Thin Clients and Windows-based workstations at the company headquarters. Network based printers are placed throughout the building (one per floor). Windows print servers reside in the datacenter and manage the network printers. XenDesktop and XenApp servers also reside in the datacenter.

A regional office has numerous Windows, Linux and Mac endpoints with network attached printers. A remote branch office has a few Windows workstations with locally attached printers.

Three different print strategies are applied:

- **Headquarters** - A Citrix Universal Print Server is used for printing within the XenApp and XenDesktop session. Native print drivers are not required on the Windows based workstations. A session printer policy is configured per floor which connects the floor printer as the default printer. The policies are filtered based on the subnet of the thin client for proximity printing. Quality of Service (QoS) policies are implemented. Inbound and outbound network traffic on ports TCP 1494 and TCP 2598 are prioritized over all other network traffic. This will prevent HDX user sessions from being impacted by large print jobs.
- **Regional Office** - A Universal Print Server is deployed within the regional office. The print job uses the Universal Print Driver and is compressed and delivered from the user's session to the Universal Print Server, across the WAN. The job is then sent to the network-attached printer in the office.
- **Branch Office** - Since all branch users work on Windows based workstations, auto-created client printers in conjunction with the Citrix Universal Printer Driver are used. Since the print job is delivered over ICA, the print data is compressed which saves bandwidth. The Citrix Universal Printer Driver ensures all printers connected to the client can be used within the XenApp or XenDesktop session without concern of the printer model used.

Applications

Properly integrating an application requires understanding compatibility and how the user/business requirements influences the appropriate delivery method.

Decision: Compatibility

VDI typically requires significant changes to be made to an organization's application delivery and management strategy. For example, many organizations will take the opportunity to upgrade their desktop operating system and to simplify management by reducing the number of applications installed into the base image using techniques such as application streaming and application layering. These are significant changes that require comprehensive compatibility testing. Important compatibility requirements that may need to be verified include:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Operating system** – The application must be compatible with the preferred operating system.
- **Multi-User** – Some applications may be more appropriate for delivery via a hosted shared desktop or a hosted Windows App. In these situations, the compatibility of the application must be verified against the multi-user capabilities of a server operating system like Windows Server 2012R2.
- **Application architecture** – It is important to understand whether the application includes 16-bit, 32-bit or 64-bit code so that an appropriate operating system can be selected. 16-bit code cannot be executed on a 64-bit operating system. However, a 16-bit application can be delivered to users as a Hosted Windows App from a 32-bit desktopbased operating system like x86 editions of Windows 7, 8 or 10.
- **Interoperability** – Some applications may experience complications if they coexist on the same operating system. Possible causes include shared registry hives, dll files or INI files as well as incompatible dependencies. Application interoperability issues should be identified so that appropriate remediation steps can be taken or an alternative delivery model selected.
- **Dependency** – Applications may need to interact with each other to provide the users with a seamless experience. For example, applications that present information in a PDF format require a suitable PDF viewer to be available. Many times, the dependent (child) applications are version specific to the parent application.
- **Application virtualization** – The use of application virtualization techniques, like streaming and layering, helps to simplify image management by reducing the number of applications installed into the base image. However, not all applications are suitable for streaming and layering because they may install device drivers, use COM+ or form part of the operating system.

Application compatibility can be achieved by doing a combination of manual, user testing, utilizing pre-verified lists maintained by the software vendor, or using an automated application compatibility solution, like Citrix AppDNA, which runs through thousands of tests to verify compatibility.

Decision: Application Delivery Method

It is unlikely that a single delivery method will meet all requirements. Based on the outcome of the application categorization assessment process and the overall image management strategy (installed images, scripted images and layered images), several application delivery methods can be considered.

Choosing one of the appropriate application delivery method helps improve scalability, management and user experience.

- **Installed app** – The application is part of the base desktop image. The install process involves dll, exe and other files copied to the image drive as well as registry modifications.
- **Streamed App (Microsoft App-V)** – The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings placed in a container on the virtual desktop and isolated from the base operating system and each other, which helps to address compatibility issues.
- **Layered App (Citrix App Layering)** – Each layer contains a single application, agent or operating system. Layering simplifies ongoing maintenance, as an OS, agent and application exists in a single layer; update the layer and all deployed images containing that layer are updated. App Layering has two different delivery options:
  - **Layered Image** – By integrating one OS layer, one platform layer (XenApp/XenDesktop VDA, Provisioning Services agent) and many application layers, an administrator can easily create new, deployable images.
  - **Elastic Layer** – A XenApp and XenDesktop user can dynamically receive a new app layer based at logon. On a XenApp host, an elastic layer is session-aware, where an attached layer is only available to a user's session granted access to the layer.
- **Hosted Windows App** - An application installed on a multi-user XenApp host and deployed as an application and not a desktop. A user accesses the hosted Windows app seamlessly from the VDI desktop or endpoint device, hiding the fact that the app is executing remotely.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Local App** – An application deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it executes on the endpoint.

The following table provides recommendations on the preferred approaches for integrating applications into the overall solution.

In the table:

- **Y** indicates Recommended.
- **N** indicates Not Recommended.
- **o** indicates Viable.

App Category	Installed App	Streamed App	Layered App	Hosted Windows App	Local App
Common	Y	o	Y	o	N
Departmental	o	Y	Y	Y	N
User	N	o	Y	o	Y
Management	Y	N	Y	o	N

Experience from the Field

- **Energy** – An energy company installs applications on the base image for the majority of users and streams departmental applications as required.
- **Financial** – A banking customer maintains and deploys multiple desktop images containing user group focused applications as required by various departments.

Virtual Machines

Virtual resources require proper allocation of the processor, memory and disk. These decisions have a direct impact on the amount of hardware required as well as the user experience.

The key to successful resource allocation is to ensure that virtual desktops and applications offer similar levels of performance to physical desktops. Otherwise, productivity and overall user satisfaction will be affected. Allocating resources to the virtual machines above their requirements however is inefficient and expensive for the business.

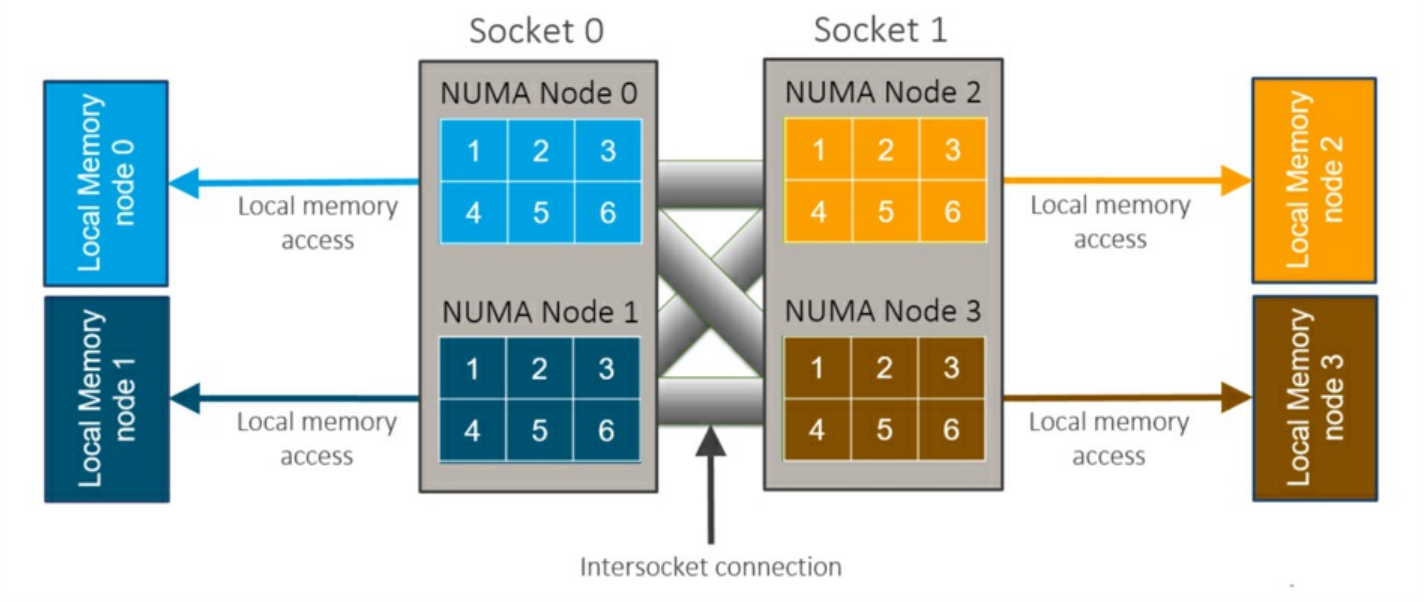
The resources allocated should be based on the workload characteristic of each user group, identified during the assess phase.

Decision: Virtual Processor (vCPU)

For hosted desktop-based VDI models (hosted pooled desktops and hosted personal desktops), the general recommendation is two or more vCPUs per virtual machine so that multiple threads can be executed simultaneously. Although a single vCPU could be assigned for extremely light workloads, users are more likely to experience session hangs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For hosted server-based VDI models (hosted Windows apps, hosted browser apps, hosted shared desktops), the proper vCPU allocation is based on the Non-Uniform Memory Access (NUMA) architecture of the processors.



Each socket is divided into one or more NUMA nodes. Hosted server-based VDI models will often utilize 4 or more processors. Allocating more vCPU than the NUMA node contains results in a performance hit. Allocating a portion of a NUMA node to a virtual machine results in a performance hit if the portion allocated is not easily divisible by the size of the NUMA node. It is often ideal to allocate the number of cores within a NUMA node to a virtual machine or allocate ½ of the cores to a virtual machine, while doubling the number of virtual machines.

User Workload	**Operating System**	**vCPU Configured for Scale**	**vCPU Configured for Experience**
Light	Windows 7	2 vCPU	2 vCPU
	Windows 10	2 vCPU	2 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA
	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA
Medium	Windows 7	2 vCPU	3 vCPU
	Windows 10	2 vCPU	3 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA
Heavy	Windows 7	3 vCPU	4 vCPU
	Windows 10	3 vCPU	4 vCPU
	Windows 2012R2	NUMA or ½ of NUMA	NUMA or ½ of NUMA
	Windows 2016	NUMA or ½ of NUMA	NUMA or ½ of NUMA

> ## Nota
>
> Windows 2012 R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

Decision: CPU Optimization

In a shared and virtualized environment, a single user can monopolize CPU resources due to a runaway process or an intense data processing operation in Excel. If the processor is oversubscribed, it will not be able to fulfill other users' requests, resulting in a hung session.

Citrix Workspace Environment Management, a component of XenApp and XenDesktop, incorporates CPU optimization. When a process consumes a certain percentage of the CPU over a defined timeframe, the process priority lowers from normal to low or very low, giving all remaining processes a higher priority and overcoming the runaway process risk. CPU optimization will also remember processes that triggered CPU protection and automatically start the process at a lower priority on future launches.

Most environments should enable CPU optimization as a default configuration.

Decision: Virtual Memory (vRAM)

The amount of memory allocated to each resource is a function of the user's expected workload and application footprint. Assigning insufficient memory to the virtual machines will cause excessive paging to disk, resulting in a poor user experience; allocating too much RAM increases the overall cost of the solution.

The following table provides guidance on the virtual RAM that should be assigned based on workload.

User Workload	**Operating System**	**vRAM Configured for Scale**	**vRAM Configured for Experience**
Light	Windows 7	2 GB	3 GB
	Windows 10	2 GB	3 GB

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2012R2	256 MB per user	
	Windows 2016	320 MB per user	
Medium	Windows 7	3 GB	4 GB
	Windows 10	3 GB	4 GB
	Windows 2012R2	512 MB per user	
	Windows 2016	640 MB per user	
Heavy	Windows 7	6 GB	8 GB
	Windows 10	6 GB	8 GB
	Windows 2012R2	1024 MB per user	
	Windows 2016	1280 MB per user	

Nota

- Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.
- Memory allocation above 4GB requires a 64-bit operating system.
- If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

Decision: RAM Optimization

Even though users only work within a single application at a time, most have five or more applications running but idle. When a process moves from active to idle, the application and operating system releases a portion of the process's active working set of memory to free up system resources. However, this is only a small percentage of the applications working set. The rest remains locked for the application, severely limiting available system resources.

Using RAM Optimization within Citrix Workspace Environment Management, applications that are idle (have not been interacted with by a user) for a certain time are forced to release excess memory until they are no longer idle. When the application returns to an active state, the released memory is loaded back into the active working set.

Most environments should enable RAM optimization as a default configuration. A RAM optimization exclusion list is available if certain processes encounter issues with optimization.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Disk Cache

The amount of storage that each VM requires will vary based on the workload and the image type. If creating hosted personal desktop without leveraging an image management solution, each VM will require enough storage for the entire OS and locally installed applications.

Deploying machines through Machine Creation Services or Provisioning Services can substantially reduce the storage requirements for each virtual machine. Disk space requirements for the write cache and difference disk will depend on application usage and user behavior. However, the following table provides a starting point for estimating disk space requirements based on machine sized with vCPU and vRAM as per the following guidelines:

User Workload	**Operating System**	**Storage Space (Differencing Disk / Write Cache Disk)**
Light	Windows 7	10 GB
	Windows 10	10 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB
Medium	Windows 7	15 GB
	Windows 10	15 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB
Heavy	Windows 7	20 GB
	Windows 10	20 GB
	Windows 2012R2	40 GB
	Windows 2016	60 GB

Decision: RAM Cache

Provisioning Services and Machine Creation Services have the capability to utilize a portion of the virtual machine's RAM as a buffer for the storage cache. The RAM cache is used to improve the performance of traditional storage by sharing the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

virtual machine's non-paged pool memory.

User Workload	Operating System	RAM Cache Configured for Scale	RAM Cache Configured for Experience
Light	Windows 7	128 MB	256 MB
	Windows 10	128 MB	256 MB
	Windows 2012R2	2GB	
	Windows 2016	4GB	
Medium	Windows 7	256 MB	512 MB
	Windows 10	256 MB	512 MB
	Windows 2012R2	4GB	
	Windows 2016	8GB	
Heavy	Windows 7	512 MB	1024 MB
	Windows 10	512 MB	1024 MB
	Windows 2012R2	6GB	
	Windows 2016	10 GB	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota

- If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.
- If additional RAM is available on the host, the RAM Cache amounts can be increased to provide even greater levels of performance.

Decision: Storage IOPS

Storage performance is limited by the number of operations it can handle per second, referred to as IOPS. Under allocating storage IOPS results in a VDI desktop where apps, web pages and data are slow to load.

The following table provides guidance on the number of storage IOPS generated per user based on workload and operating system. Storage IO activity will be higher during user logon/logoff.

User Workload	**Operating System**	**Storage IOPS (without RAM-Based Cache)**	**Storage IOPS (with RAM-Based Cache)**
Light	Windows 7	10 IOPS	1 IOPS
	Windows 10	12 IOPS	1 IOPS
	Windows 2012R2	3 IOPS	0.5 IOPS
	Windows 2016	4 IOPS	1 IOPS
Medium	Windows 7	15 IOPS	1 IOPS
	Windows 10	20 IOPS	1.5 IOPS
	Windows 2012R2	4 IOPS	0.5 IOPS
	Windows 2016	6 IOPS	1 IOPS
Heavy	Windows 7	25 IOPS	2 IOPS
	Windows 10	35 IOPS	3 IOPS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 2012R2	5 IOPS	0.5 IOPS
	Windows 2016	8 IOPS	1 IOPS

Decision: IO Prioritization

With shared environments, every user's IO process receives an equal share of resources. A user running some IO intensive task can affect mission critical applications. Citrix Workspace Environment Management allows administrators to define IO priorities for processes.

If a process requires more IO resources or the process is monopolizing IO resources, the process and process priority is manually increased or decreased via the console. This advanced configuration is only used in special circumstances.

Decision: Graphics (GPU)

Without a graphical processing unit (GPU), graphical processing is rendered with software by the CPU. A graphical processing unit (GPU) can be leveraged to improve server scalability and user experience or enable the use of graphically intensive applications. During the desktop design it is important to decide how the GPU (if used) will be mapped to the virtual machines. There are three methods available.

- **Pass-Through GPU** – Each physical GPU is passed through to a single virtual machine (hosted apps or hosted desktops).
- **Hardware Virtualized GPU** – Using a hypervisor's vGPU technology, an NVIDIA GRID or Intel Iris Pro is virtualized and shared between multiple machines. Each virtual machine has the full functionality of GPU drivers and direct access to the GPU.
- **Software Virtualized GPU** – The GPU is managed by the hypervisor and intercepts requests made by the VDI desktops. This process is used if a GPU is not installed within the host.

In the table:

- **Y** indicates Available.
- **X** indicates Not Supported.

	Pass-Through GPU	**Hardware Virtualized GPU (NVidia)**	**Hardware Virtualized GPU (Intel)**	**Hardware Virtualized GPU (AMD)**	**Software Emulated GPU**
Citrix XenServer					
XenDesktop	**Y**	**Y**	**Y**	**X**	**Y**
XenApp	**Y**	**Y**	**Y**	**X**	**Y**
Microsoft Hyper-V					
XenDesktop	**Y**	**X**	**X**	**X**	**Y**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp	**Y**	**X**	**X**	**X**	**Y**
VMware vSphere					
XenDesktop	**Y**	**Y**	**X**	**Y**	**Y**
XenApp	**Y**	**Y**	**X**	**Y**	**Y**

User groups with a heavy use of graphical applications will often require the use of a NVidia hardware virtualized GPU. User groups who rely on office-based applications can have an observable benefit with the use of a hardware virtualized GPU from Intel.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology control layer

Apr 24, 2018

The control layer is the fourth layer of the design methodology.

Active Directory

Decision: Forest Design

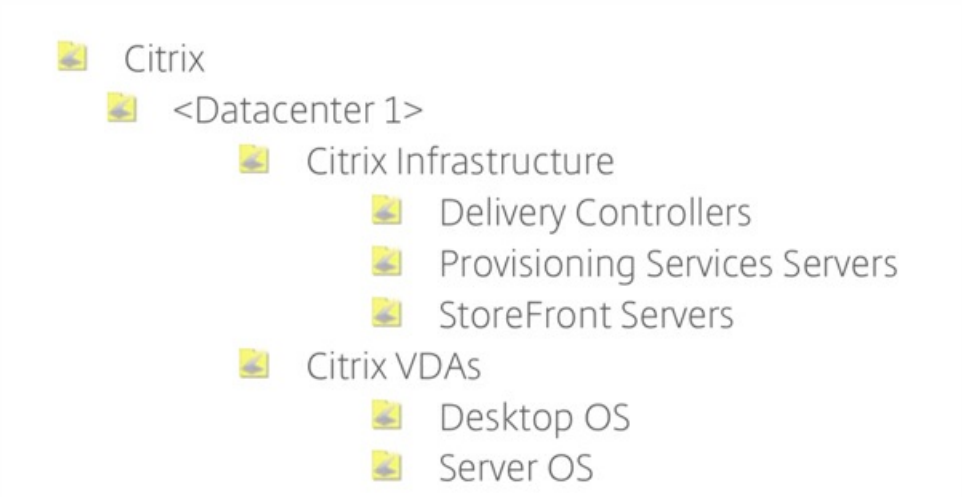
Multi-forest deployments, by default, do not have inter-domain trust relationships between the forests. An AD administrator can establish trust relationships between the multiple forests, allowing the users and computers from one forest to authenticate and access resources in another forest.

For forests that have inter-domain trusts, it is recommended that the appropriate settings be configured to allow the Delivery Controllers to communicate with both domains. When the appropriate trusts are not configured, multiple XenDesktop sites for each forest must be configured. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX134971 – Successfully Deploying XenDesktop in a Complex Active Directory Environment

Decision: Organizational Unit Structure

Infrastructure components for a XenApp and XenDesktop deployment should reside within their own dedicated organizational units (OUs); separating workers and controllers for management purposes. By having their own OUs, the objects inside will have greater flexibility with their management while allowing Citrix administrators to be granted delegated control.

A sample Citrix OU structure can be seen below.



Decision: User Groups

Whenever possible, permissions and authorization should be assigned to user groups rather than individual users, thereby eliminating the need to edit a large amount of resource permissions and user rights when creating, modifying, or deleting user accounts. Permission application example:

- An application published to one group of 1,000 users requires the validation of only one object for all 1,000 users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- The same application published to 1,000 individual user accounts requires the validation of all 1,000 objects.

Database

The majority of Citrix products discussed within this document require a database. The following table outlines the usage on a per product basis:

In this table:

- **Y** indicates Available.
- **O** indicates Optional.

Product	Configuration Data	Runtime Data	Audit/Change Log Data	Monitoring Data
XenDesktop	Y	Y	Y	Y
Provisioning Services	Y		O	
Desktop Player	Y	Y	Y	

Decision: Edition

There are multiple editions of Microsoft SQL Server 2012: Express, Web, Standard, Business Intelligence, and Enterprise. Based on the capabilities of the various SQL Server editions available, the Standard edition is often used for hosting the XenApp and XenDesktop databases in production environments.

The Standard edition provides an adequate amount of features to meet the needs of most environments. For more information on the databases supported with Citrix products please refer to the Citrix Database Support Matrix. Different versions of Citrix products support different versions of the SQL server; therefore, it is important to check the support matrix to ensure the version of SQL server used is compatible with the Citrix product being deployed.

Decision: Database Server Sizing

The SQL Server must be sized correctly to ensure the performance and stability of an environment. Since every Citrix product uses SQL server in a different way, no generic all-encompassing sizing recommendations can be provided. Instead, per-product SQL server sizing recommendations are provided below.

XenApp and XenDesktop

XenApp and XenDesktop Brokers use the database as a message bus for broker communications, storing configuration data and storing monitoring and configuration log data. The databases are constantly in use and the performance impact on the SQL server can be considered as high.

Based on results from Citrix internal scalability testing the following SQL server specification for a server hosting all XenDesktop databases are recommended:

- 2 Cores / 4 GB RAM for environments up to 5,000 users
- 4 Cores / 8 GB RAM for environments up to 15,000 users

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 8 Cores / 16 GB RAM for environments with 15,000+ users

The database files and transaction logs should be hosted on separate hard disk subsystems in order to cope with a high number of transactions. For example, registering 20,000 virtual desktops during a 15-minute boot storm causes ~500 transactions / second and 20,000 users logging on during a 30-minute logon storm causes ~800 transactions / second on the XenDesktop Site Database.

Provisioning Services

In addition to static configuration data provisioning servers store runtime and auditing information in the database. Depending on the boot and management pattern, the performance impact of the database can be considered as low to medium.

Based on this categorization, a SQL server specification of 4 Cores and 4 GB RAM is recommended as a good starting point. The SQL server should be carefully monitored during the testing and pilot phase in order to determine the optimal configuration of the SQL server.

Decision: Instance Sizing

When sizing a SQL database, two aspects are important:

- **Database file** – Contains the data and objects such as tables, indexes, stored procedures and views stored in the database.
- **Transaction log file** – Contains a record of all transactions and database modifications made by each transaction. The transaction log is a critical component of the database and, if there is a system failure, the transaction log might be required to bring the database back to a consistent state. The usage of the transaction log varies depending on which database recovery model is used:
  - **Simple recovery** – No log backups required. Log space is automatically reclaimed, to keep space requirements small, essentially eliminating the need to manage the transaction log space. Changes to the database since the most recent backup are unprotected. In the event of a disaster, those changes must be redone.
  - **Full recovery** – Requires log backups. No work is lost due to a lost or damaged database data file. Data of any arbitrary point in time can be recovered (for example, prior to application or user error). Full recovery is required for database mirroring.
  - **Bulk-logged** – Requires log backups. This is an adjunct of the full recovery model that permits high-performance bulk copy operations. It is typically not used for Citrix databases.

For further information, please refer to the Microsoft Developer Network – SQL Server Recovery Models.

In order to estimate storage requirements, it is important to understand the disk space consumption for common database entries. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX139508 – XenDesktop 7.x Database Sizing.

XenDesktop General

XenApp 7.x and XenDesktop 7.x use three distinct databases:

- **Site Configuration database** – Contains static configuration and dynamic runtime data
- **Monitoring database** – Contains monitoring data which is accessible via Director
- **Configuration logging database** – Contains a record for each administrative change performed within the site (accessible via Studio)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Site Database

Since the database of a XenApp or XenDesktop site contains static configuration data and dynamic runtime data, the size of the database file depends not only on the physical size of the environment but also user patterns. The following factors all impact the size of the database file:

- The number of connected sessions
- The number of configured and registered VDAs
- The number of transactions occurring during logon
- VDA heartbeat transactions

The size of the Site Database is based on the number of VDAs and active sessions. The following table shows the typical maximum database size Citrix observed when scale testing XenApp and XenDesktop with a sample number of users, applications, and desktop delivery methods.

Users	Applications	Desktop Types	Expected Maximum Size (MB)
1,000	50	Hosted Shared	30
10,000	100	Hosted Shared	60
100,000	200	Hosted Shared	330
1,000	N/A	Hosted Pooled	30
10,000	N/A	Hosted Pooled	115
40,000	N/A	Hosted Pooled	390

> **Nota**
>
> This sizing information is a guide only. Actual database sizes may differ slightly by deployment due to how databases are maintained.

Determining the size of the transaction log for the Site database is difficult due to factors that can influence the log including:

- The SQL Database recovery model
- Launch rate at peak times
- The number of desktops being delivered

© 1999-2017 Citrix Systems, Inc. All rights reserved.

During XenDesktop scalability testing, Citrix observed the transaction log growth rate at 3.5MB an hour when the system is idle, and a per user per day growth rate of ~32KB. In a large environment, transaction log usage requires careful management and a regular backup, to prevent excessive growth. This can be achieved by means of scheduled jobs or maintenance plans.

Monitoring Database

Of the three databases, the Monitoring database is expected to be the largest since it contains historical information for the site. Its size is dependent on many factors including:

- Number of Users
- Number of sessions and connections
- Number of workers
- Retention period configuration – Platinum customers can keep data for over a year (default 90 days). Non-platinum customers can keep data for up to 7 days (default 7 days).
- Number of transaction per second. Monitoring service tends to execute updates in batches. It is rare to have the number of transactions per second go above 20.
- Background transaction caused by regular consolidation calls from the Monitoring service.
- Overnight processing carried out to remove data outside the configured retention period.

The following table shows the estimated size of the Monitoring database over a period of time under different scenarios. This data is an estimate based on data seen within scale testing XenApp and XenDesktop (assuming a 5 day working week).

Users	**Type**	**1 week (MB)**	**1 month (MB)**	**3 months (MB)**	**1 year (MB)**
1,000	HSD	20	70	230	900
10,000	HSD	160	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500
40,000	VDI	464	1,700	5,400	21,500
Estimates with 2 connections and 1 session per user with a 5 day work week					
Users	**Type**	**1 week (MB)**	**1 month (MB)**	**3 months (MB)**	**1 year (MB)**
1,000	HSD	30	100	330	1,300

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10,000	HSD	240	925	3,000	12,000
100,000	HSD	2,400	9,200	30,000	119,000
1,000	VDI	25	85	280	1,100
10,000	VDI	200	750	2,500	9,800
40,000	VDI	800	3,000	9,700	38,600

Nota

The 100,000 HSD tests are based on a test environment consisting of:

- 2 Delivery Controllers
- 43 Hosted Shared Desktop workers
- 3 SQL servers, configured with databases held within one Always On Availability Group.

For more information please see the Citrix Support article – XenDesktop 7.x Database Sizing.

The size of the transaction log for the Monitoring Database is very hard to estimate, but XenApp and XenDesktop scalability testing showed a growth rate of about 30.5 MB an hour when the system is idle, and a per user per day growth rate of ~9 KB.

Configuration Logging Database

The Configuration Logging Database is typically the smallest of the three databases. Its size and the size of the related transaction log depends on the daily administrative activities initiated from Studio, Director or PowerShell scripts, therefore its size is difficult to estimate. The more configuration changes are performed, the larger the database will grow. Some factors that can affect the size of the database include:

- The number of actions performed in Studio, Director and PowerShell.
- Minimal transactions which occur on the database when no configuration changes are taking place.
- The transaction rate during updates. Updates are batched whenever possible.
- Data manually removed from the database. Data within the Configuration Logging Database is not subject to any retention policy, therefore it is not removed unless done so manually by an administrator.
- Activities that have an impact on sessions or users, for example, session logoff and reset.
- The mechanism used for deploying desktops.

In XenApp environments not using MCS, the database size tends to fall between 30 and 40MB. For MCS environments, database size can easily exceed 200MB due to the logging of all VM build data.

Temporary Database

In addition to the Site, Monitoring, and Configuration Logging databases, a system-wide temporary database (tempdb) is

© 1999-2017 Citrix Systems, Inc. All rights reserved.

provided by SQL Server. This temporary database is used to store Read-Committed Snapshot Isolation data. XenApp 7.x and XenDesktop 7.x uses this SQL Server feature to reduce lock contention on the XenApp and XenDesktop databases. Citrix recommends that all XenApp 7.x and XenDesktop 7.x databases use Read-Committed Snapshot Isolation. For more information please see How to Enable Read-Committed Snapshot in XenDesktop.

The size of the tempdb database will depend on the number of active transactions, but in general it is not expected to grow more than a few MBs. The performance of the tempdb database does not impact the performance of XenApp and XenDesktop brokering, as any transactions that generate new data require tempdb space. XenApp and XenDesktop tend to have short-lived transactions, which help keep the size of the tempdb small.

The tempdb is also used when queries generate large intermediate result sets. Guidance and sizing the tempdb can be found on the Microsoft TechNet article Optimizing tempdb Performance.

Provisioning Services

The Provisioning Services farm database contains static configuration and configuration logging (audit trail) data. The record size requirements outlined below can be used to help size the database:

Configuration Item	DB Space Required (KB)	Number of Items (Example)	Total (KB)
Base farm configuration	112	-	112
User group w/ farm access	50	10	250
Site	4	5	20
Device collection	10	50	500
Farm view	4	10	40
Farm view to device relationship	5	1	5,000
Site View	4	5	20
Site view to device relationship	5	1	5,000
Device	2	5,000	10,000

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Device bootstrap	10	-	-
Device to disk relationship	35	1	175,000
Device printer relationship	1	-	-
Device personality data	1	-	-
Device status (when booted)	1	5,000	5,000
Device custom property	2	-	-
vDisk	1	20	20
vDisk version	3	5	300
Disk locator	10	1	200
Disk locator custom property	2	-	-
Server	5	10	50
Server IP	2	1	20
Server status (when booted)	1	20	20
Server custom property	2	-	-
vDisk store	8	5	40

© 1999-2017 Citrix Systems, Inc. All rights reserved.

vDisk store to server relationship	4	1	40
Connection to XenServer (VirtualHostingPool)	4	-	-
vDisk update task	10	10	100
Administrative change (auditing enabled)	1	10,000	10,000
Total			**211,732KB (~212MB)**

During the PVS farm setup, a database with an initial file size of 20MB is created. Due to the nature of the data in the PVS farm database the transaction log is not expected to grow very quickly, unless a large amount of configuration is performed.

In contrast to XenApp, which also offers the ability to track administrative changes, the related information is not written to a dedicated database but directly to the Provisioning Services farm database. In order to limit the size of the Provisioning Services database it is recommended to archive the audit trail data on a regular schedule.

Decision: Database Location

By default, the Configuration Logging and Monitoring databases are located within the Site Configuration database. Citrix recommends changing the location of these secondary databases as soon as the configuration of the site has been completed, in order to simplify sizing, maintenance and monitoring. All three databases can be hosted on the same server or on different servers. An ideal configuration would be to host the Monitoring database on a different server from the Site Configuration and Configuration Logging databases since it records more data, changes occur more frequently and the data is not considered to be as critical as the other databases. For more information, please refer to Citrix Docs – Change secondary database locations.

> ## Nota
>
> The location of the Configuration Logging database cannot be changed when mandatory logging is enabled.

Decision: High-Availability

The following table highlights the impact to XenApp, XenDesktop and Provisioning Services when there is a database outage:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Impact of Database Outage
Site configuration database	Users will be unable to connect or reconnect to a virtual desktop. **Note**: Local Host Cache allows users with Hosted Shared Desktops, Hosted Windows and Browser Applications, and Personal Desktops to reconnect to their applications and desktops even when the site database is unavailable.
Monitoring database	Director will not display any historical data and Studio cannot be started. Brokering of incoming user requests and existing user sessions will not be affected.
Configuration logging database	If allow changes when the database is disconnected has been enabled within XenApp and XenDesktop logging preferences, an outage of the configuration logging database will have no impact (other than configuration changes not being logged). Otherwise, administrators will be unable to make any changes to the XenApp and XenDesktop site configuration. Users are not impacted.
Provisioning Services farm database	When offline database support is enabled and the database becomes unavailable, the stream process uses a local copy of the database to retrieve information about the provisioning server and the target devices supported by the server. This allows provisioning servers and the target devices to remain operational. However, when the database is offline, the console and the management functions listed below become unavailable: • Auto Add target devices • vDisk creation and updates • Active Directory password changes • Stream process startup • Image update service • PowerShell and MCLI based management If offline database support has not been enabled, all management functions become unavailable and the boot and failover of target devices will fail.

> ## Nota
>
> Please review HA options for 3rd party databases (for example, App-V, SCVMM or vCenter) with the respective software vendor.

In addition to the built-in database redundancy options, Microsoft SQL Server, as well as the underlying hypervisor (in virtual environments), offer a number of high availability features. These enable administrators to ensure single server outages will have a minimal impact (if any) on the XenApp and XenDesktop infrastructure. The following the SQL / hypervisor high availability features are available:

- **VM-level HA** – This high availability option is available for virtual SQL servers only, which need to be marked for High Availability at the hypervisor layer. In case of an unexpected shutdown of the virtual machine or the underlying hypervisor host, the hypervisor will try to restart the VM immediately on a different host. While VM-level HA can minimize downtimes in power-outage scenarios, it cannot protect from operating system level corruption. This solution is less expensive than mirroring or clustering because it uses a built-in hypervisor feature. However, the automatic failover process is slower, as it can take time detect an outage and start the virtual SQL server on another host. This may interrupt the service to users.
- **Mirroring** – Database mirroring increases database availability with almost instantaneous failover. Database mirroring can be used to maintain a single standby or mirror database, for a corresponding principal or production database.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Database mirroring runs with either synchronous operation in high-safety mode, or asynchronous operation in high-performance mode. In high-safety mode with automatic failover (recommended for XenDesktop) a third server instance, known as a witness, is required, which enables the mirror server to act as a hot standby server. Failover from the principal database to the mirror database happens automatically and is typically completed within a few seconds. It is a good practice to enable VM-level HA (or a similar automatic restart functionality) for at least the witness to ensure SQL service availability in case of a multi-server outage.

> ## Nota
>
> Microsoft is planning to remove mirroring as a high availability option in a future release of SQL Server and is discouraging its use in new network development. Please refer to the Microsoft article – Database Mirroring (SQL Server) for more information

- **AlwaysOn Failover Cluster Instances** – Failover clustering provides high-availability support for an entire instance of Microsoft SQL Server. A failover cluster is a combination of two or more nodes, or servers, using a shared storage. A Microsoft SQL Server AlwaysOn Failover Cluster Instance, introduced in SQL Server 2012, appears on the network as a single computer, but has functionality that provides failover from one node to another if the current node becomes unavailable. The transition from one node to the other node is seamless for the clients connected to the cluster. AlwaysOn Failover cluster Instances require a Windows Server Failover Clustering (WSFC) resource group. The number of nodes supported in the WSFC resource group will depend on the SQL Server edition. (Please refer to the table in the Decision: Edition earlier in this chapter.) For more information please refer to MSDN – AlwaysOn Failover Cluster Instances (SQL Server).
- **AlwaysOn Availability Groups** – AlwaysOn Availability Groups is an enterprise-level highavailability and disaster recovery solution introduced in Microsoft SQL Server 2012, which enables administrators to maximize availability for one or more user databases. AlwaysOn Availability Groups require that the Microsoft SQL Server instances reside on Windows Server failover clustering (WSFC) nodes. Similar to failover clustering a single virtual IP / network name is exposed to the database users. In contrast to failover clustering, shared storage is not required since the data is transferred using a network connection. Both synchronous and asynchronous replication to one or more secondary servers is supported. As opposed to mirroring or clustering secondary servers can be actively used for processing incoming read-only requests, backups or integrity checks. This feature can be used to offload user resource enumeration requests to a secondary SQL server in XenDesktop environments to essentially scale-out a SQL server infrastructure. Since the data on active secondary servers can lag multiple seconds behind the primary server, the read-only routing feature cannot be used for other XenDesktop database requests at this point in time. For more information, please refer to MSDN – AlwaysOn Availability Groups (SQL Server).

The following table outlines the recommended high availability features for Citrix databases:

In the table:

- **Y** indicates Recommended.
- **o** indicates Viable.
- **N** indicated Not Supported.
- **T** indicates for test environments only.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	VM Level - HA	Mirroring	AlwaysOn Failover Cluster Instances	AlwaysOn Availability Groups
Site database	T	Y	o	o
Configuration logging database	T	o	o	o
Monitoring database	T	Y	o	o
Provisioning Services farm database	T	Y	o	N
DesktopPlayer database	T	N	o	o

Citrix Licensing

Citrix offers organizations the flexibility of multiple licensing models that align with common usage scenarios. The different licensing models vary based on the Citrix product used, but can include per user/device and per concurrent user. Several Citrix products use the license server, while other products require a license to be installed on the product itself.

Citrix License Server

- XenDesktop
- XenApp
- Provisioning Services
- XenServer

On the product:

- NetScaler
- NetScaler Gateway

For more information on XenDesktop 7.x licensing, please refer to CTX128013 - XenDesktop Licensing.

For more information on Microsoft Licensing, please refer to the Microsoft document – Licensing Microsoft's Virtual Desktop Infrastructure Technology.

Decision: Sizing

Internal scalability testing has shown that a single virtual license server with two cores and 2GB of RAM can issue approximately 170 licenses per second or 306,000 licenses per half hour. If necessary, the specification of the license server can be scaled out to support a higher number of license requests per second.

Decision: High Availabiity

For a typical environment, a single license server is sufficient. Should the license server become unavailable, dependent Citrix products will enter a 30-day grace period, which provides more than enough time to resolve connectivity issues and/or

© 1999-2017 Citrix Systems, Inc. All rights reserved.

restore or rebuild the license server.

> **Nota**
>
> - If the license server and the Citrix product do not communicate within 2 heartbeats (5-10 min), the Citrix product will enter a grace period and will allow connections for up to 30 days. Once communication with the license server is re-established, the license server will reconcile the temporary and actual licenses.
> - A CNAME record in DNS is a convenient way to reference the license server. Using CNAMEs allows the license server name to be changed without updating the Citrix products.

If additional redundancy is required, Citrix supports the following high availability solutions for the license server.

- **Windows Clustering** – Cluster servers are groups of computers that work together in order to increase availability. Clustering allows the license server role to automatically failover in the event of a failure. For more information on clustering, please see the Citrix Docs article – Clustered License Servers.
- **Duplication of license server** – Create a VM level backup of the license server. This backup should not be stored on the same host as the license server. Instead, it should be stored in a safe location, such as a highly available storage solution, or backed up to tape or disk. The duplicate server is not active, and will remain on standby until the need arises to restore the active license server. Should the license server be restored using this backup, any new licenses must be re-downloaded to the server.

For more information, please refer to Citrix eDocs – Licensing Architecture Overview.

Each method allows an administrator to exchange a single license server for another without an interruption in service; assuming that the change occurs during the grace period and that the following limitations are considered.

- License files will reference the server specified during the allocation process. This means that the license files can only be used on a server with the same binding information (Hostname) as the server that was previously specified.
- Two Windows-based, domain joined license servers cannot share the same name and be active in the environment at the same time.
- Because license servers do not communicate with each other, any additional licenses must be placed on both the active and backup license server.

Decision: Optimization

License server performance can be optimized by tuning the number of “receive” and “processing” threads. If the thread count is set too low, requests will be queued until a thread becomes available. Conversely, if the thread count is set too high, the license server will become overloaded.

The optimal values are dependent on the server hardware, site configuration, and license request volume. Citrix recommends testing and evaluating different values to determine the proper configuration. Setting the maximum number of processing threads to 30 and the maximum number of receiving threads to 15 is a good starting point for large scale deployments.

This optimization will improve the Citrix License Server ‘s ability to provide licenses by increasing its ability to receive and process license requests.

For more information, please refer to the Citrix Docs – Improving Performance by Specifying Thread Use.

Delivery Controllers

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Server Sizing

Delivery Controller scalability is based on CPU utilization. The more processor cores available, the more virtual desktops a controller can support. Each desktop startup, registration, enumeration and launch request impacts the controller's processor. As the storm increases in intensity, the CPU utilization of the controller will increase. If the CPU reaches a critical threshold, roughly 80%, the site will need to either scale up or scale out.

Adding additional CPU cores to a Delivery Controller will lower the overall CPU utilization, thus allowing for greater numbers of desktops supported by a single controller. This is really only feasible when dealing with virtualized controllers as adding virtual CPUs is fairly easy and straightforward. The other alternative is to add another controller into the site configuration. The controller would have the same configuration as other controllers, and the load would be evenly distributed across all controllers, thus helping to reduce the overall load on each single controller.

Testing has shown that a single Delivery Controller, using the following configuration, can support more than 5,000 desktops.

Component	Specification
Processor	4 vCPU
Memory	4 GB RAM
Network	Bonded virtual NIC
Host Storage	40-GB shared storage
Operating System	Windows Server 2012 R2
XenDesktop	7

The following formula can be used to calculate the number of Delivery Controllers required for a Citrix site.

$$Number\ of\ Delivery\ Controllers = \frac{Number\ of\ Active\ Sessions\ per\ Site}{5{,}000} + 1$$

Decision: High Availability

If the server hosting the Delivery Controller is unavailable, users will not be able to access their virtual desktops or published applications. Therefore at least two Delivery Controllers (N+1 redundancy) should be deployed per zone on different physical servers to prevent this component from becoming a single point of failure. If one controller fails, the others can manage connections and administer the site.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The locations of all Delivery Controllers are specified on the VDA, allowing it to automatically failover if communication with one Delivery Controller is unavailable. The VDA checks the following locations, in order, stopping at the first place it finds the Delivery Controller:

1. A persistent storage location maintained for the auto-update feature. This location contains controller information when auto-update is enabled and after the VDA successfully registers for the first time after installation.
   For its initial registration after installation, or when auto-update is disabled, the VDA checks the following locations.
2. Policy settings (Delivery Controllers, Delivery Controller SIDs).
3. The Delivery Controller information under the VDA ListofDDCs registry key. The VDA installer initially populates these values, based on the information specified when installing the VDA.
4. OU-based discovery. This is a legacy method maintained for backward compatibility.
5. The Personality.ini file created by Machine Creation Services.

Citrix Consulting recommends utilizing the auto-update feature (enabled by default). This feature will simplify management of the environment by keeping VDA's updated when adding and removing Delivery Controllers.

Decision: Local Host Cache

Even if the SQL database is highly available, there is the risk of not having access to the database if the network connection between the delivery controller and SQL database fails, which is an important concern for sites that span geographical locations.

To overcome this risk, the delivery controllers can utilize the local host cache feature that creates a local copy of the SQL database, used only if the delivery controller loses contact with the database.

The following must be considered when using local host cache:

- **Elections** – When the zones loses contact with the SQL database, an election occurs nominating a single delivery controller as master. All remaining controllers go into idle mode. A simple alphabetical order determines the winner of the election.
- **Sizing** – When using local host cache mode, a single delivery controller is responsible for all VDA registrations, enumerations, launches and updates. The elected controller must have enough resources (CPU and RAM) to handle the entire load for the zone. A single controller can scale to 10,000 users, which influences the zone design.
  - **RAM** – The local host cache services can consume 2+GB of RAM depending on the duration of the outage and the number of user launches during the outage.
  - **CPU** – The local host cache can use up to 4 cores in a single socket.
  - **Storage** – During local host cache mode, storage space increased 1MB every 2-3 minutes with an average of 10 logons per second.
- **Power Options** – Powered off virtual resources will not start when the delivery controller is in local host cache mode. Pooled virtual desktops that reboot at the end of a session are placed into maintenance mode.
- **Consoles** – When using local host cache mode, Studio and PowerShell are not available.

Decision: XML Service Encryption

In a typical session, the StoreFront server passes credentials to the Citrix XML Service on a Delivery Controller. The Citrix XML protocol uses clear text to exchange all data, with the exception of passwords, which are transmitted using obfuscation.

If the traffic between the Storefront servers and the XenDesktop Controllers can be intercepted it will be vulnerable to the following attacks:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Attackers can intercept the XML traffic and steal resource set information and tickets.
- Attackers with the ability to crack the obfuscation can obtain user credentials.
- Attackers can impersonate the XenDesktop Controller and intercept authentication requests.

For most organizations, the Citrix XML traffic will be isolated on a dedicated physical or virtual datacenter network making interception unlikely. However, for safety consider using SSL encryption to send StoreFront data over a secure HTTP connection.

Decision: Server OS Load Management

Default Load Management policies are applied to all Server OS delivery groups. The default settings specify the maximum number of sessions a server can host at 250 and do not consider CPU and Memory usage. Capping session count does not provide a true indication of load, which can lead to an overburdening of Server OS delivery groups resulting in a degradation of performance or an underutilization of Server OS delivery groups resulting in an inefficient usage of resources.

Citrix Consulting recommends creating unique "custom" Load Management policies for each Delivery Group based on performance and scalability testing. Different rules and thresholds can be applied to each Delivery Group depending on the different resource bottlenecks identified during testing. For more information on the available Load Management policy configurations refer to Citrix Docs – Load Management policy settings.

If adequate testing cannot be performed prior to production, Citrix Consulting recommends implementing the following "custom" Load Management policy which can be applied to all servers as a baseline:

- **CPU Usage** - Full Load: 80%
- **CPU usage excluded process priority** – Below Normal or Low
- **Memory Usage** - Full Load: 80%
- **Memory Usage base load** – Report zero load (MBs): 786
- **Maximum number of sessions** – X

The "Maximum number of sessions" policy is included for capping purposes – this is considered a best practice for resiliency. Organizations can choose an initial value of 250 (denoted by "X" above). **It is highly recommended that this value and others be customized based on the results from scalability testing**.

Coud Connector

The XenApp and XenDesktop Service within Citrix Cloud utilize a set of services contained within the Citrix Cloud Connector. A redundant set of Cloud Connector virtual machines must be placed in each data center/resource location containing VDA hosts.

Decision: Server Sizing

Cloud Connector scalability is based on CPU utilization. The more processor cores available, the more virtual desktops a cloud connector can support. Each desktop startup, registration, enumeration and launch request affects the cloud connector's processor. As the storm increases in intensity, the CPU utilization of the cloud connector will increase. If the CPU reaches a critical threshold, roughly 80%, the site will need to either scale up or scale out.

Testing has shown that a single Cloud Connector Controller, using the following configuration, can support 5,000 desktops.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	On Premises Specifications	Azure Hosted Specifications
Number of VMs (with N+1 Fault Tolerance)	3	6 Standard_A2_V2 instances
Processors per VM	4 vCPU	2 vCPU
Memory per VM	4 GB RAM	4 GB RAM
Host Storage per VM	40 GB shared storage	200 GB temp storage
Operating System	Windows Server 2012 R2	Windows Server 2012 R2

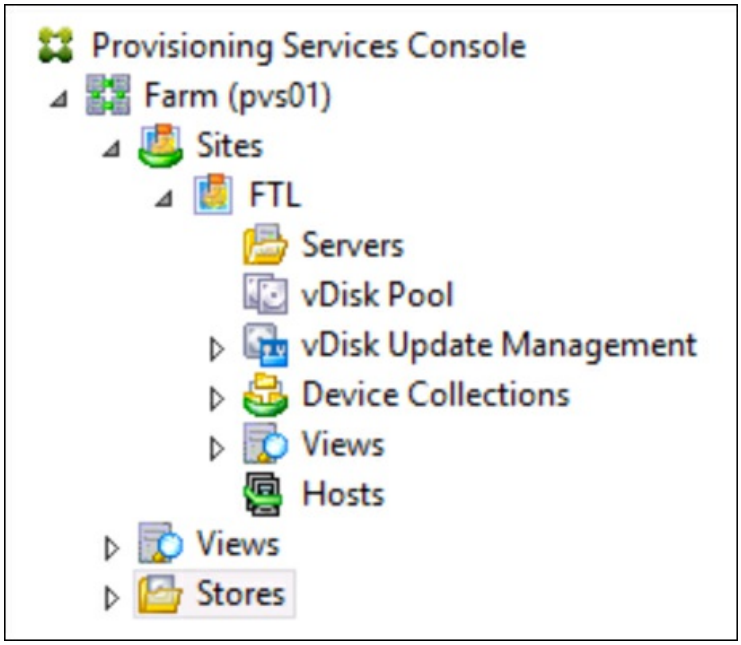
Provisioning Services

Citrix Provisioning Services (PVS) uses streaming technology to simplify the deployment of virtual and physical machines. Computers are provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can completely eliminate the need to manage and patch individual systems. Instead, all image management is performed on the master image.

Decision: Topology

A Provisioning Services farm represents the top level of the Provisioning Services infrastructure, which can be further broken down into sites. All provisioning servers in a farm share the same SQL database and Citrix license server.

Each site is a logical entity containing provisioning servers, vDisk pools and target device collections. Although all sites within a farm share the same database, target devices can only fail over to other provisioning servers within the same site.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

There are factors that must be considered when determining the overall Provisioning Services topology:

- **Network** – Provisioning servers are constantly communicating with the farm database to retrieve system configuration settings. Therefore, separate farms should be created for each physical location where target devices reside, unless they are connected to the database server by a fast and robust connection.
- **Administration** – Organizations may need to maintain the separation of administrative duties at a departmental, regional or countrywide basis. Additional Provisioning Services farms will add some complexity to the management of the environment. However, this overhead is typically limited to initial configuration, desktop creation and image updates.
- **Organization** – A practical reason for building multiple sites is due to organizational changes. For example, two companies may have recently merged through acquisition, but need to keep resources separate while integration takes place. Configuring the organization to use separate sites is one way to keep the businesses separate but managed centrally through the Provisioning Services console.

Only create additional sites if the business requirements warrant it. A single site per farm is easier to manage and requires no additional configuration.

Decision: Device Collections

Device collections provide the ability to create and manage logical groups of target devices. Creating device collections simplifies device management by allowing actions to be performed at the collection level rather than the target device level.



Device collections can represent physical locations, subnet ranges, chassis or different departments within an organization. Collections can also be used to logically separate production target devices from test and maintenance ones.

Consider creating device collections based on vDisk assignment so that the status of all target devices assigned to a particular vDisk can be quickly identified.

Decision: High Availability

Provisioning Services is a critical component of the virtual desktop infrastructure. The following recommendations should be followed to eliminate single points of failure:

- **Provisioning Server** – A minimum of two provisioning servers should always be implemented per site. Sufficient redundancy should be incorporated into the design so that a single server failure does not reduce the total number of target devices that can be supported per site. The Provisioning Services boot file should be configured for high availability. Up to four Provisioning Servers may be listed in the boot file. Target devices will try to contact the servers in the order that they are listed. The server that responds may not necessarily be the server that will provide streaming services to the target device. If Load Balancing is enabled, the target device may be reassigned to another server in the site that is less loaded than the others.
- **vDisks and Storage** – For vDisk stores hosted on local, Direct Attached Storage (DAS) or Storage Area Network (SAN),

© 1999-2017 Citrix Systems, Inc. All rights reserved.

replication should be used to synchronize the vDisks. If using Network Attached Storage (NAS), ensure that the vDisks are hosted on a highly available network share.

- **Networking** – The provisioning servers should have redundant NICs. If the provisioning server is deployed as a physical server, redundant NICs should be teamed and if the provisioning server is deployed as a virtual server, the underlying hypervisor should incorporate redundant NICs.

> ### Nota
>
> The target devices will only failover to NICs that are on the same subnet as the PXE boot NIC.

Trivial File Transfer Protocol (TFTP) is a communications protocol used for transferring configuration or boot files between machines. Provisioning services can use TFTP to deliver the bootstrap file to target devices. There are several options available to make the TFTP service highly available. Some of the more commonly used options are:

- **DNS Round Robin** – A DNS entry is created for the TFTP service with multiple A records corresponding to the TFTP services running on the provisioning servers in the farm. This method is not recommended since the state of the TFTP service is not monitored. Clients could potentially be sent to a non-functioning server.
- **Hardware load balancer** – Use a hardware load balancer, such as Citrix NetScaler, to create virtual IPs that corresponds to the provisioning servers. The NetScaler can intelligently route traffic between the provisioning servers. In the event that one of the servers becomes unavailable, NetScaler will automatically stop routing TFTP requests to that server. This is the best method for making TFTP highly available, but can be complicated to setup.
- **Multiple DHCP Option 66 entries** – This method is easy to implement but requires a DHCP service that supports entering multiple entries in option 66. Microsoft DHCP server allows one option 66 entry so this method would not be feasible in environments with Microsoft DHCP services. If using a non-Microsoft DHCP server or appliance, check with the manufacturer to verify that multiple option 66 entries is supported.

There are other options available that can achieve the same result without having to use TFTP:

- **Proxy DHCP** – Use the provisioning servers PXE service to provide the bootstrap information. If one of the servers is down, the next available server in the farm can provide the bootstrap information. This method requires the provisioning servers to be on the same broadcast domain as the target devices. If there are other PXE services running on the network (Altiris, SCCM, etc.) then multiple VLANs may be required to keep the PXE services from interfering with each other.
- **Boot Device Manager** – Use the Boot Device Manager to create a bootstrap file that is either placed on the local hard drive, or used as a bootable ISO file. If the ISO file is used, configure the target devices to boot from the CD/DVD-ROM drive, and place the ISO file on a highly available shared network location or local storage of each target device. When either method is utilized, the TFTP service is not used at all.

High availability should always be incorporated into the Provisioning Services design. Although high availability may require additional resources and increased costs, it will provide a highly stable environment so that users experience minimal impact due to service outages.

Decision: Bootstrap Delivery

A target device initiates the boot process by first loading a bootstrap program which initializes the streaming session between the target device and the provisioning server. There are three methods in which the target device can receive the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

bootstrap program:

Using DHCP Options –

1. When the target device boots, the target device sends a broadcast for IP address and boot information. DHCP will process this request and provide an IP as well as scope option settings 66 (the name or IP address of the Provisioning Services TFTP server) and 67 (the name of the bootstrap file).

> ## Nota
>
> If using a load balancer for the TFTP service then the address of the load balancer is entered in option 66.

2. Using TFTP, a request for the bootstrap file is sent from the target device to the provisioning server. The target device downloads the boot file from the provisioning server.

3. The target device boots the assigned vDisk image.

> ## Nota
>
> Requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the DHCP servers in order to receive PXE broadcasts.

Using PXE Broadcasts –

1. When a target device boots from the network, the target device sends a broadcast for an IP address and boot information. DHCP will process this request and provide an IP address. In addition, all provisioning servers that receive the broadcast will return boot server and boot file name information. The target device will merge the information received and start the boot process.

2. Using TFTP, a request for the bootstrap file is sent from the target device to the provisioning server which responded first. The target device downloads the boot file from the provisioning server.

> ## Nota
>
> - Make sure no other PXE services are in use on the same subnet, such as the Altiris PXE service, or isolate using VLANs otherwise conflicts may occur with Provisioning Services.
> - Requires UDP/DHCP Helper to be configured when targets are not on the same subnet as the DHCP and PVS servers in order to receive PXE broadcasts.

Using Boot Device Manager – The Boot Device Manager (BDM) creates a boot file that target devices obtain through a physical CD/DVD, a mounted ISO image or as a virtual hard disk assigned to the target device. A BDM partition can be upgraded in one of three ways:

- By collection

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- By a group of highlighted devices
- By a single device

A summary of the advantages and disadvantages for each delivery method is listed in the following table:

Delivery Method	Advantages	Disadvantages
DHCP Options	Easy to implement	Requires changes to production DHCP service. DHCP service may only allow one option 66 entry. Requires UDP/DHCP helper for targets on different subnets.
PXE	Easy to implement	Can interfere with other running PXE services on the same subnet. Requires UDP/DHCP helper for targets on different subnets.
BDM ISO	Does not require PXE or TFTP services	Extra effort required to boot physical target devices. BDM ISO is regarded as a single point of failure if a single file is used.
BDM Partition	The BDM boot partition upgrade does not require PXE, TFTP, or TSB; it's considered a single stage bootloader, at boot time it automatically finds all relevant PVS server information and does not need external services provided by PXE, TFTP, or TSB.	An extra 8MB partition is created for each target device.

> ## Nota
>
> When configuring the bootstrap file, up to four provisioning servers may be listed. The order in which the provisioning servers appear in the list determines the order which the provisioning servers are accessed. If the first server does not respond, the next server in the list is contacted.

Decision: vDisk Format

Provisioning Services supports the use of fixed-size or dynamic vDisks:

- **Fixed-size disk** – For vDisks in private mode, fixed-size prevents disk fragmentation, and offers improved write

© 1999-2017 Citrix Systems, Inc. All rights reserved.

performance over dynamic disks.

- **Dynamic disk** – Dynamic disks require less storage space than fixed-size disks, but offer significantly lower write performance. Although vDisks in Shared mode do not perform writes to the vDisk, the time required to complete vDisk merge operations will increase with dynamic disks. This is not a common occurrence as more environments choose to create new vDisks when updating.

Since most reads will be to the System Cache in RAM, there is no significant change in performance when utilizing fixed-size or dynamic disks. In addition, dynamic disks require significantly less storage space. Therefore, dynamic disks are recommended.

Decision: vDisk Replication

vDisks hosted on a local, Direct Attached Storage or a SAN must be replicated between vDisk stores whenever a vDisk is created or changed. Provisioning Services supports the replication of vDisks from stores that are local to the provisioning server as well as replication across multiple sites that use shared storage. The replication of vDisks can be performed manually or automatically:

- **Manual** – Manual replication is simple, but can be time consuming, depending on the number of vDisks and vDisk stores. If an error occurs during the replication process, administrators can catch them straight away and take the appropriate steps to resolve them. The risk of manual replication is vDisk inconsistency across the provisioning servers which will result in load balancing and failover to not work properly. For example, if a vDisk is replicated across three servers and then one of the vDisks is updated, that vDisk is no longer identical and will not be considered if a server failover occurs. Even if the same update is made to the other two vDisks, the timestamps on each will differ, and therefore the vDisks are no longer identical.
- **Automated** – For large environments, automated replication is faster than the manual method due to the number of vDisks and vDisk Stores required. Some automated tools, such as Microsoft DFS-R, support bandwidth throttling and Cross File Remote Differential Compression (CF-RDC), which use heuristics to determine whether destination files are similar to the file being replicated. If so, CF-RDC will use blocks from these files to minimize the amount of data transferred over the network. The risk of automated replication is that administrator do not typically monitor replication events in real-time and do not respond quickly when errors occur, unless the automation tool has an alerting feature. Some tools can be configured to automatically restart the copy process in the event of a failure. For example, Robocopy supports “resume copying” in the event that the network connection is interrupted.

For medium and large projects, use a tool to automate vDisk replication. Select a tool that is capable of resuming from network interruptions, copying file attributes and preserving the original timestamp.

> ## Nota
>
> Load balancing and high availability will not work unless the vDisks have identical timestamps.

Decision: Server Sizing

Generally, a Provisioning Server is defined with the following specifications:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Specification
Model	Virtual
Processor	4 - 8 vCPU
Memory	2GB + (# of vDisks * 2GB)
Network	10 GBps NIC
Network	40 GB shared storage
vDisk Storage	Depending on number of images/revisions
Operating System	Windows Server 2012 R2

Model

Citrix Provisioning Services can be installed on virtual or physical servers:

- **Virtual** – Offers rapid server provisioning, snapshots for quick recovery or rollback scenarios and the ability to adjust server resources on the fly. Virtual provisioning servers allow target devices to be distributed across more servers helping to reduce the impact from server failure. Virtualization makes more efficient use of system resources.
- **Physical** – Offers higher levels of scalability per server than virtual servers. Physical provisioning servers mitigate the risks associated with virtual machines competing for underlying hypervisor resources.

  In general, virtual provisioning servers are preferred when sufficient processor, memory, disk and networking resources can be made available and guaranteed to be available.

> ## Nota
>
> For high availability, ensure that virtual Provisioning Servers are distributed across multiple virtualization hosts. Distributing the virtual servers across multiple hosts will eliminate a single point of failure and not bring down the entire Provisioning Services farm in the event of a host failure.

CPU

Provisioning Services is not CPU intensive. However, under allocating the number of CPUs does impact the optimization of the network streams. The number of streams that a Provisioning Services server can run concurrently can be determined by the following formula:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

□□□ □□□□□□ □□ □□□□□□□ = # □□ □□□□□ ∗ # □□ □*h*□□□□/□□□□

By default, the Streaming Service is configured with 20 sequential network ports, and 8 threads per port. Therefore, by default, a provisioning server can support 160 concurrent targets. If more than 160 streams are required, Provisioning Services continuously switches between streaming different target devices

Ideally, if the environment needs to support more than 160 concurrent targets, the number of ports, and threads per port can be adjusted in the Provisioning Services console. Best performance is attained when the threads per port is not greater than the number of cores available on the provisioning server. If the provisioning server does not have sufficient cores, the server will show a higher CPU utilization, and target devices waiting for requests to be processed will have a higher read latency.

Even though Provisioning Services is not CPU intensive, allocating 2 CPUs will require a larger contiguous network port range.

- Small environments (up to approximately 500 virtual machines) 4 vCPUs are recommended.
- Larger environments 8 vCPUs are recommended.

RAM

The Windows operating system hosting Provisioning Services partially caches the vDisks in memory (system cache) reducing the number of reads required from storage. Reading from storage is significantly slower than reading from memory. Therefore, Provisioning Servers should be allocated sufficient memory to maximize the benefit from this caching process.

The following formula can be used to determine the optimal amount of memory that should be allocated to a provisioning server:

□□□□□ □□□□□□ □□□ = 2□□ + (# □□ □□□□□□ ∗ 2□□)

Network

Unlike most other XenApp and XenDesktop components, Provisioning Services does not bottleneck the CPU. Provisioning Services scalability is based on network throughput.

The following table shows the approximate amount of data that Provisioning Services requires to boot different operating systems:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Operating system	Avg Boot Data Usage (MB)
Windows 10 x64	240
Windows 8 x86	178
Windows 8 x64	227
Windows 7 x86	166
Windows 7 x64	210
Windows 2012	225
Windows 2012 R2	232
Windows 2008 R2	251
Windows Vista x86	190
Windows Vista x64	240

Determining how much time will be required to boot the target devices can be estimated using the following formula:

$$Seconds\ to\ Boot = \frac{(Number\ of\ Targets\ *\ MB\ Usage)}{\text{Network Throughput}}$$

Operating System	Number of VMs	Network Throughtput	Time to boot
Windows 10 x64	500	1 GBps	960 Seconds (16 minutes)
Windows 10 x64	500	10 GBps	96 Seconds (1 minute, 36 seconds)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A 10Gbps network is recommended for use with Provisioning Services. If a 10Gbps network is not available, consider link aggregation to provide additional bandwidth to the provisioning servers, or a dedicated physical streaming network.

> ## Sugerencia
>
> Firewalls can add latency and create bandwidth bottlenecks in Provisioning Services environments. If the use of firewalls cannot be avoided, refer to the Citrix whitepaper CTX101810 – Communication Ports Used By Citrix Technologies, for the list of ports that should be enabled for full functionality.

Growth

As the farm grows, administrators will need to decide whether to add more resources to the provisioning servers or to add more provisioning servers to the farm.

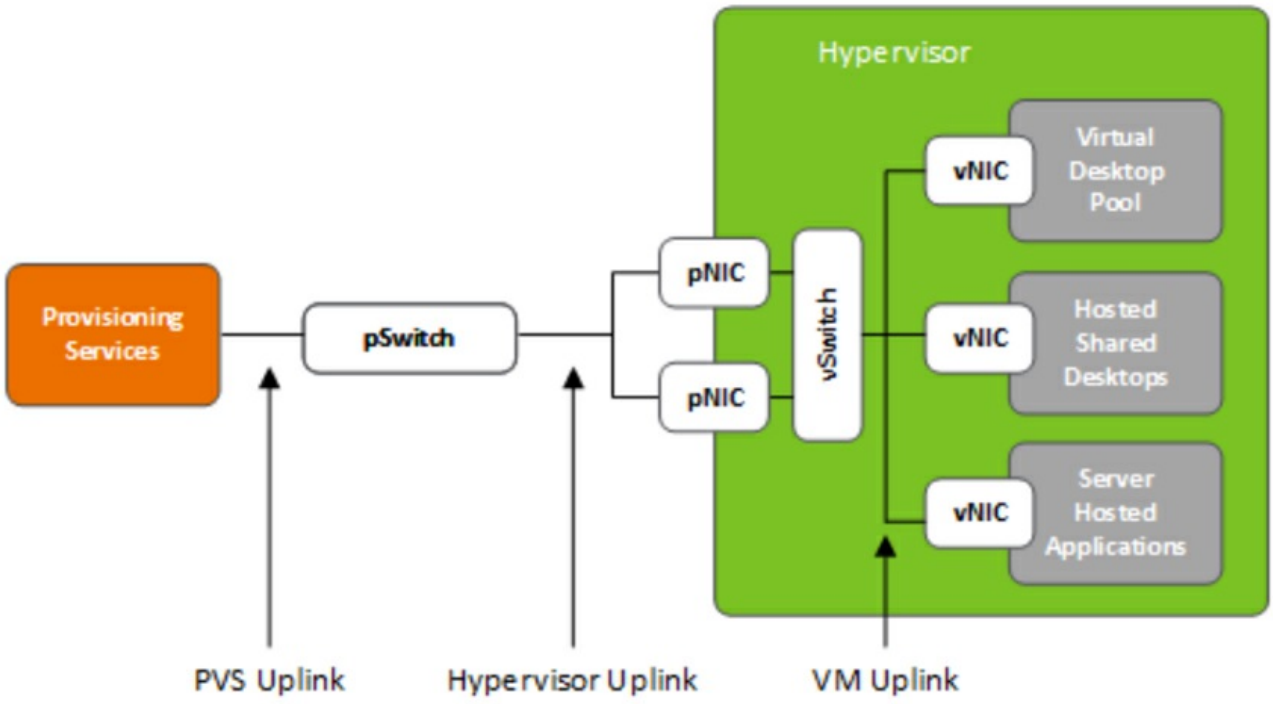
There are a number of environmental factors that need to be considered when determining whether the Provisioning Servers should be scaled up or scaled out:

- **Redundancy** – Spreading user load across additional less-powerful servers helps reduce the number of users affected from a single provisioning server failure. If the business is unable to accept the loss of a single high-specification server, consider scaling out.
- **Failover times** – The more target devices connected to a single provisioning server, the longer it will take for them to failover in the event that the server fails. Consider scaling out to reduce the time required for target devices to failover to another server.
- **Data center capacity** – The data center may have limited space, power and/or cooling available. In this situation, consider scaling up.
- **Hardware costs** – Initially, it may be more cost effective to scale up. However, there will be a point where scaling out actually becomes more cost effective. A cost analysis should be performed to make that determination.
- **Hosting costs** – There may be hosting and/or maintenance costs based on the number of physical servers used. If so, consider scaling up to reduce the long-term cost of these overheads.

Decision: Network Configuration

As mentioned before it is essential that the network is sized correctly to prevent network bottlenecks causing high disk access times and directly affecting virtual desktop performance. The following diagram outlines a common Provisioning Services network infrastructure:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



The following network configuration is recommended for the network sections outline within the diagram:

- **PVS Uplink** – All disk access from the target devices will be transferred via the PVS network uplink. This means hundreds or even thousands of devices will use this network connection. Therefore, it is vital that this connection is redundant and can failover without any downtime. Furthermore, Citrix recommends a minimum bandwidth of 1Gbps per 500 target devices. For virtual provisioning servers a respective QoS quota or a dedicated physical network uplink should be configured to ensure best performance.
- **Hypervisor Uplink** – Used by all PVS target devices hosted on a particular hypervisor host. Therefore, redundancy with transparent failover is strongly recommended. Unless the target devices run a very I/O intensive workload or perform I/O intensive tasks (e.g. booting) simultaneously, a bandwidth of 1Gbps is sufficient for this uplink.
- **VM Uplink** – All network traffic for a virtual machine, including PVS streaming traffic, will traverse this virtual network connection. Unless the workload is extremely I/O intensive a bandwidth of 100 Mbps is sufficient to handle even peak loads during I/O intensive tasks, such as booting from vDisk. For example, a Windows 2012 R2 Server will read approximately 232MB during a period of 90 seconds from the vDisk until the Windows Logon Screen is shown. During this period an average data rate of 20.5 Mbps with peaks up to 90 Mbps can be observed.

The following switch settings are recommended for Provisioning Services:

- **Disable Spanning Tree** or **Enable PortFast** – In a switching environment the Spanning Tree Protocol (STP) places ports into a blocked state while it transmits Bridged Protocol Data Units (BPDUs) and listens to ensure the BPDUs are not in a loopback configuration. The port is not placed in a forwarding state until the network converges, which depending on the size of the network, may incur enough time to cause Preboot Execution Environment (PXE) timeouts. To eliminate this issue, disable STP on edgeports connected to clients or enable PortFast.
- **Storm Control** - Storm Control is a feature available on Cisco switches that allows a threshold to be set whereby, multicast, broadcast, or unicast traffic may be suppressed. Its purpose is to prevent malicious or erroneous senders from flooding a LAN and affecting network performance. PVS Servers may send a large amount of traffic by design that falls within a storm control threshold, therefore the feature should be configured accordingly.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Broadcast Helper** – The broadcast helper is required to direct broadcasts from clients to servers that would otherwise not be routed. In a PVS environment it is necessary to forward PXE boot requests when clients are not on the same subnet as the servers. If possible the recommended network design is to have PVS servers residing on the same subnet as the target devices. This mitigates the risk of any service degradation due to other networking infrastructure components.

The following network interface features should be taken into consideration when selecting a network interface for Provisioning Services:

- **TCP Offloading** – Offloading I/O tasks to the network interface reduces CPU usage and improves overall system performance, however, PVS Streaming Services can be negatively impacted when Large Send Offload is enabled due to the extra work placed on the network adapter. Many network adapters will have Large Send Offload and TCP checksum offload enabled by default.

> ### Nota
>
> If Large Send Offload is enabled and the switch that the traffic is passing through does not support the frame size sent by the Large Send Offload engine, the switch will drop the frame causing data retransmission. When retransmitting, the operating system will segment the frames instead of the network adapter, which can lead to severe performance degradation.

- **Receive Side Scaling (RSS)** – Receive side scaling enables packets received from a network adapter to be balanced across multiple CPUs which allows incoming TCP connections to be load balanced, preventing bottlenecks from occurring to a single CPU. In Windows Server 2008 R2 and Windows Server 2012/2012 R2, RSS is enabled by default.

> ### Nota
>
> For more information on PVS networking best practices please refer to Best Practices for Configuring Provisioning Services Server on a Network.
>
> For Provisioning Services implementations on low bandwidth networks (1Gbps or slower), performance may be improved by isolating streaming traffic from other network traffic on the LAN.
>
> Microsoft does not support NIC teaming with Hyper-V on Windows Server 2008 R2; however, third party solutions are available. Microsoft does support NIC teaming with Hyper-V on Windows Server 2012/2012 R2. All support queries regarding teaming with Hyper-V should be directed to the NIC OEM.

Decision: Subnet Affinity

The Provisioning Services Subnet Affinity is a load balancing algorithm that helps to ensure target devices are connected to the most appropriate provisioning server. When configuring subnet affinity, the following options are available:

- **None** – Ignore subnets; uses the least busy server.
- **Best Effort** – Uses the least busy server/NIC combination from within the same subnet. If no server/NIC combination is available within the subnet, select the least busy server from outside the subnet. If more than one server is available within the selected subnet, perform load balancing between those servers. This is the default setting.
- **Fixed** – Use the least busy server/NIC combination from within the same subnet. Perform load balancing between servers within that subnet. If no server/NIC combination exists in the same subnet, do not boot target devices assigned

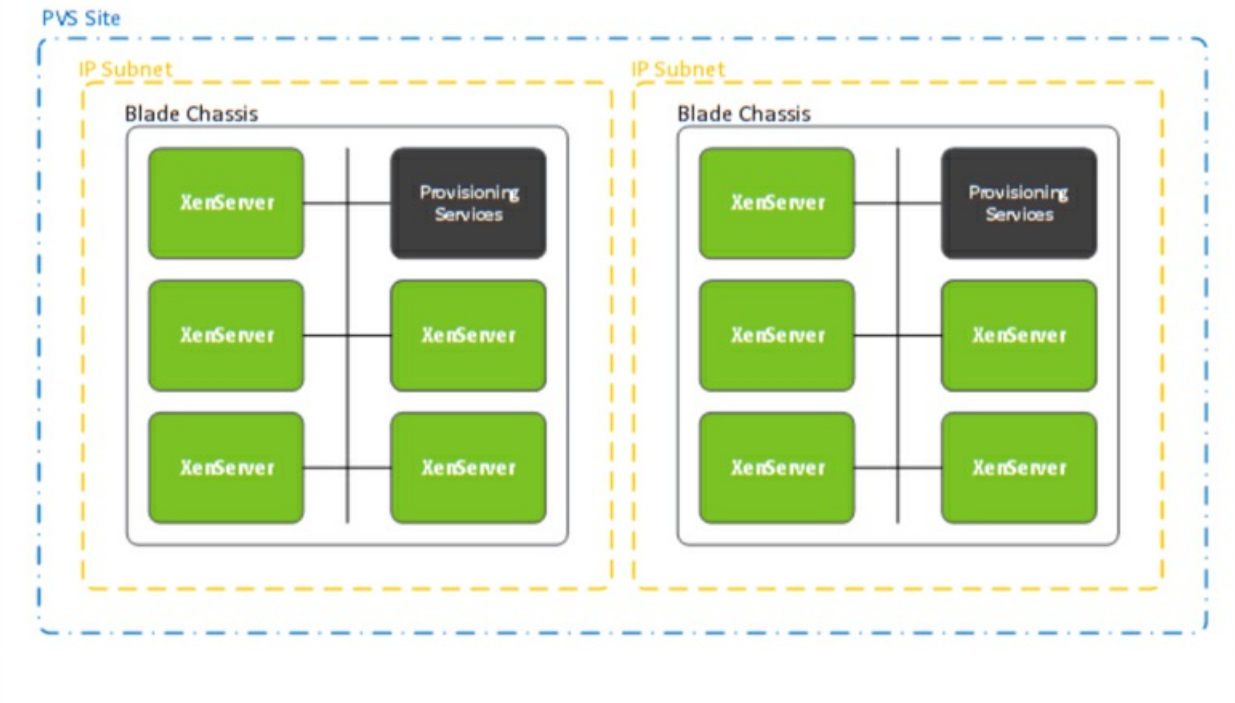
© 1999-2017 Citrix Systems, Inc. All rights reserved.

to this vDisk.

The following examples show common network configurations for physical provisioning servers. Similar configurations can be implemented for virtual provisioning servers without compromising on performance or functionality.

Blade Design

The provisioning servers and the target devices that they support reside within the same chassis. In most cases, the chassis will have a dedicated 10Gbps switch shared among all blade servers within the chassis.

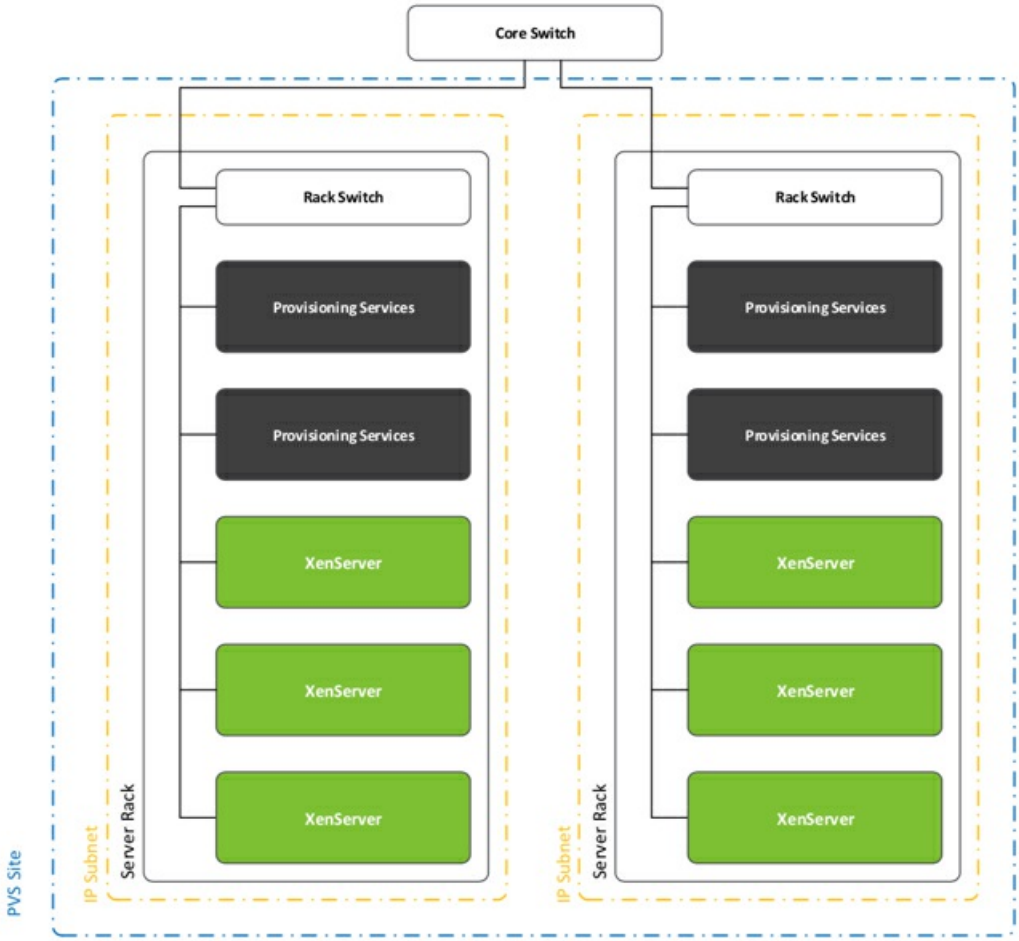


The “Best Effort” subnet affinity option is used to keep Provisioning Services traffic within the same chassis. Should the provisioning server become unavailable, the targets will failover to the second provisioning server in the second chassis, but same Provisioning Services site.

Rack Design

The second example is based on a rack design that uses rack switches to keep the provisioning traffic within the rack.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



As opposed to the blade chassis design, the subnet affinity feature is not used. Instead a Provisioning Services site with two provisioning servers will be configured per server rack. This will ensure that the target devices are streamed from provisioning servers within the same rack.

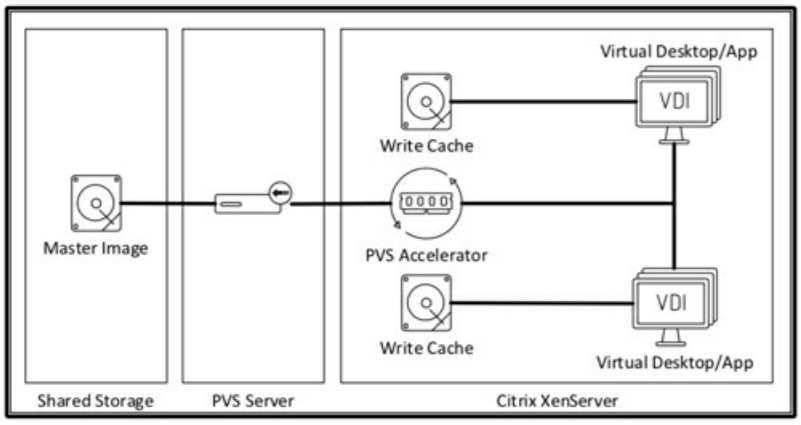
Experience from the Field

Manufacturing – A manufacturing company is designing a Provisioning Services solution to support five thousand virtual desktops. The company has concerns that Provisioning Services streaming traffic will create a bottleneck on the network affecting other applications. The company chose to build the environment on blade servers so that provisioning traffic is contained within the blade enclosure and will not impact other traffic on the network.

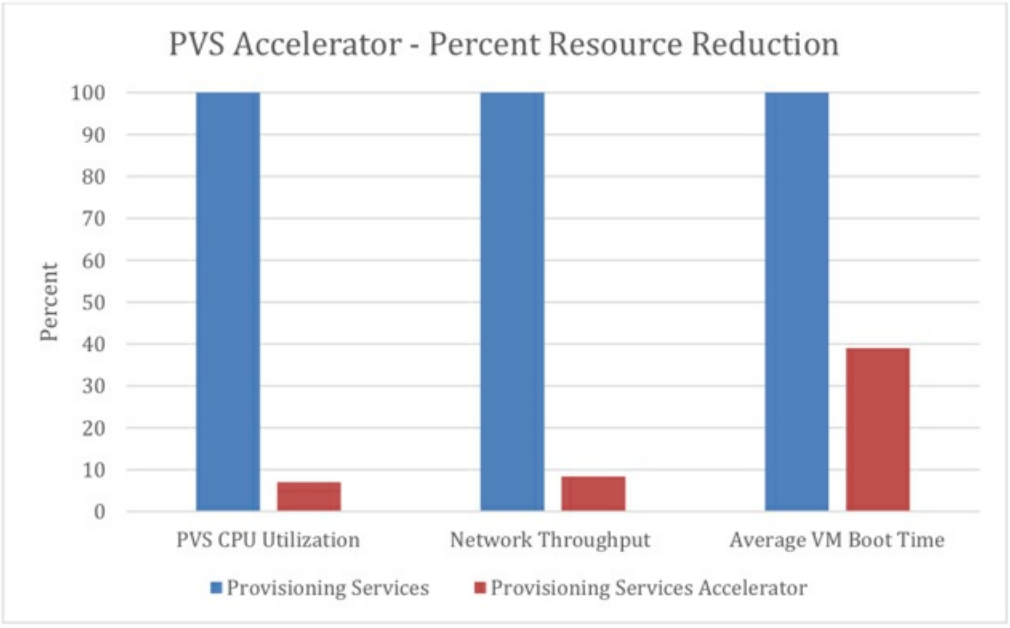
Decision: Read Cache

PVS Accelerator enables a PVS proxy to reside in the XenServer's Control Domain on a host where streaming of a Provisioning Services vDisk is cached at the proxy before being forwarded to the virtual machine. Using the cache, subsequent booting (or any I/O requests) of the virtual machine on the same host can be streamed from the proxy rather than streaming from the server over the network. PVS Accelerator requires more local resources on the XenServer host, but streaming from the server over the network saves resources, effectively improving performance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



PVS Accelerator is a XenServer only capability. Utilizing this integrated technology reduces the load on the PVS server, reduces the overall network utilization and reduces the time it takes to boot a virtual machine.



For more information on the relationship among XenServer and Provisioning Services, see the blog XenServer and PVS: Better Together.

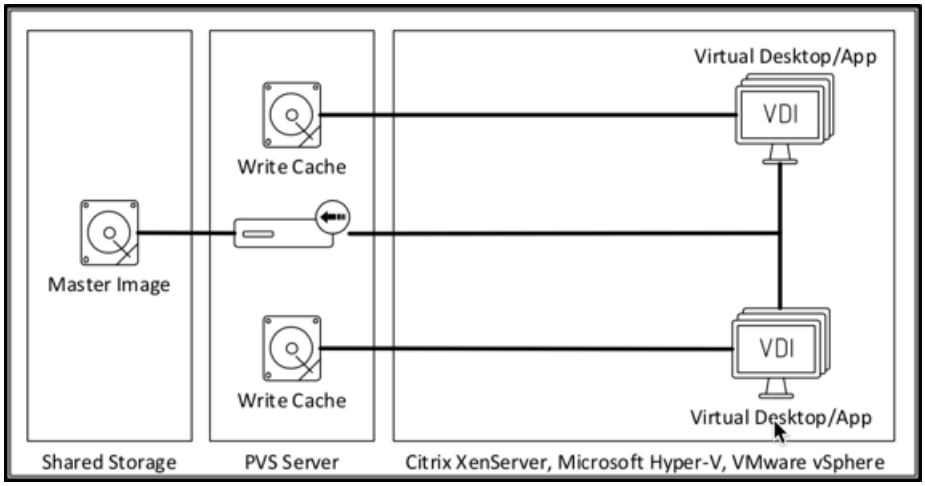
Decision: Write Cache

Because the master image is read-only, each virtual machine has a writable disk to store all changes. The administrator must decide where to store the write cache disk.

PVS Server – Local Storage

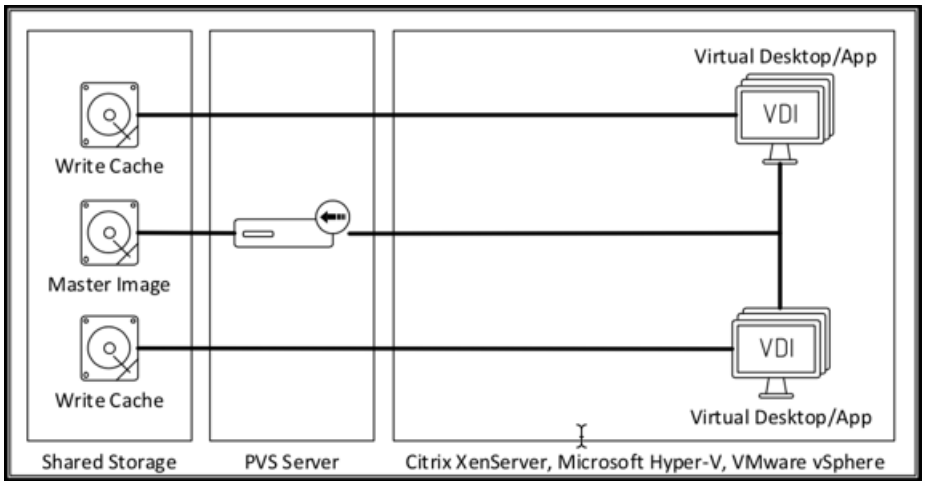
The Provisioning Services local storage holds the write cache drives for each target virtual machine. Although this is the default setting, it does increase network bandwidth requirements and increases the utilization of the Provisioning Services server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



PVS Server – Shared Storage

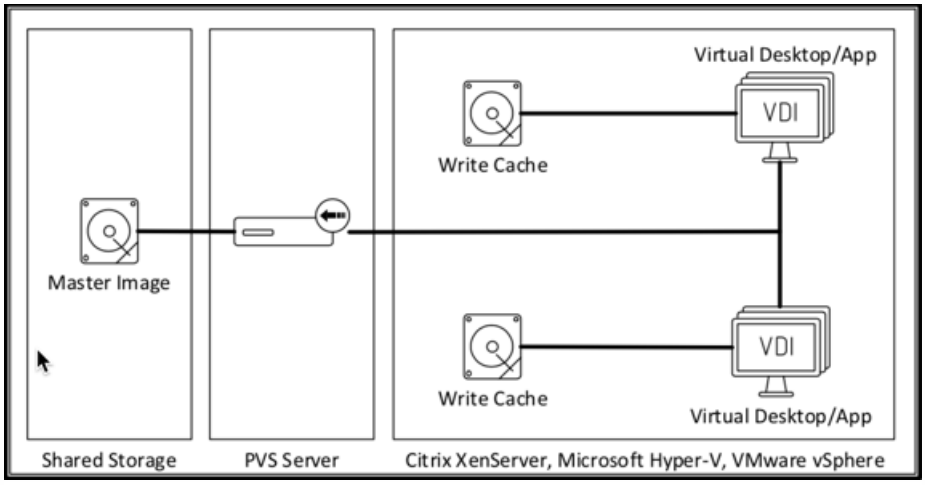
Shared storage associated with the Provisioning Services server holds the write cache drives for each target virtual machine. This option does increase network bandwidth requirements and increases the utilization of the Provisioning Services server. It also places temporary data (write cache) on expensive shared storage.



VM – Local Storage

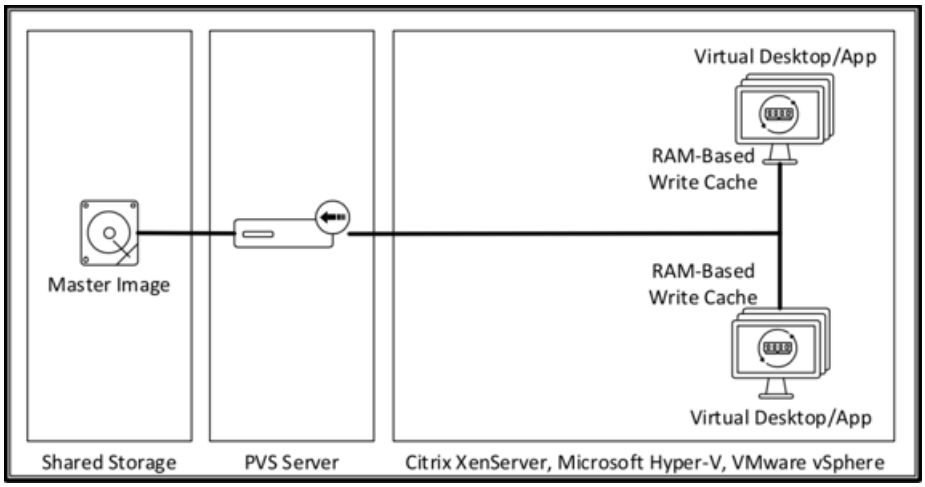
Local storage associated with the virtual machine holds the write cache drives for each target virtual machine. This option uses low cost local storage and does not consume additional resources on the Provisioning Services server. However, the local storage must be capable of support the IOPS of all virtual machines on the host.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



VM – Cache in RAM

RAM associated with the virtual machine holds the write cache drives for each target virtual machine. This option provides high performance due to the speed of RAM. However, if the RAM cache runs out of space, the virtual machine will become unusable. In order to use this option, significant amounts of RAM must be allocated to each virtual machine, increasing the overall cost.

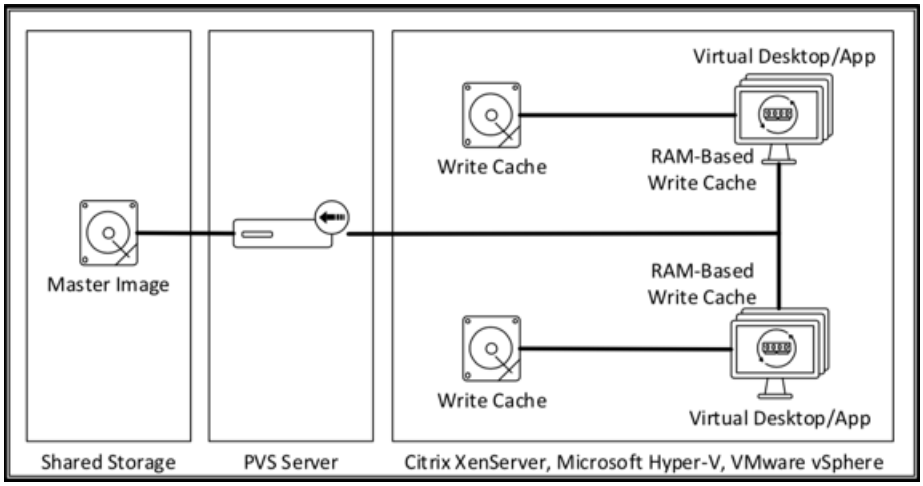


VM – Cache in RAM with Overflow to Disk

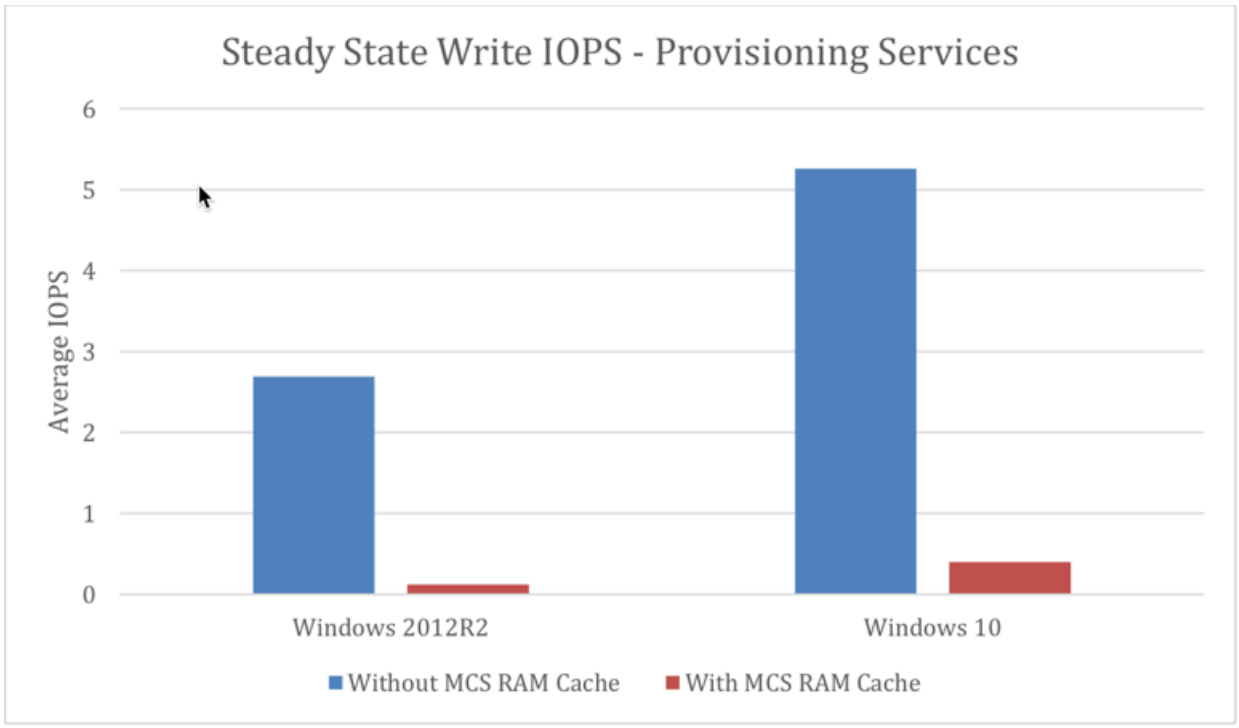
A combination of RAM and local storage is used for the write cache. First, writes are stored within the RAM cache, providing high performance. As the RAM cache is consumed, large blocks are removed from the RAM cache and placed onto the local storage write cache disk. This option provides high-levels of performance with the low cost of local storage.

Utilizing this integrated technology reduces write IOPS by 95%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cache in RAM with Overflow to Disk is the recommended option.



Decision: Antivirus

By default, most antivirus products scan all files and processes, which has a significant impact on Provisioning Services performance. For details on how antivirus software can be optimized for Provisioning Services, please refer to CTX124185 – Provisioning Services Antivirus Best Practices.

Antivirus software can cause file-locking issues on provisioning servers. The vDisk Store and write cache should be excluded from antivirus scans in order to prevent file contention issues.

When a virtual disk is running in standard mode and needs to be restarted, it downloads all of the previously loaded virus definitions. This can cause performance degradation when restarting several target devices at a time, often causing network congestion while the operation persists. In extreme cases, the target device and provisioning server can become

© 1999-2017 Citrix Systems, Inc. All rights reserved.

sluggish and consume more resources than necessary. If the antivirus software supports it, definition files should be redirected to the write cache drive so that they are preserved between reboots.

Machine Creation Services

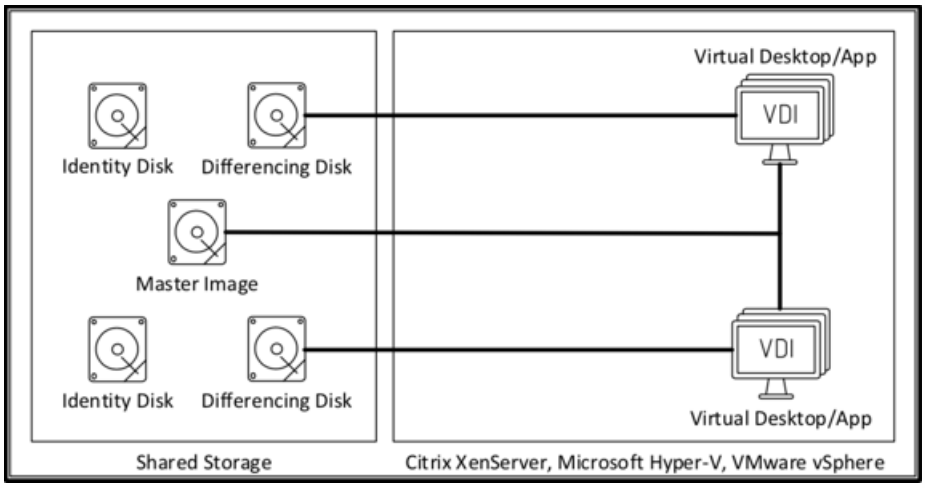
Machine Creation Services (MCS) uses disk-cloning technology to simplify the deployment of virtual machines. Computers are provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can eliminate the need to manage and patch individual systems. Instead, administrators perform all image management on the master image.

Decision: Storage Location

Machine Creation Services allows administrators to break up a virtual desktop into multiple components and store those pieces on different storage arrays.

Shared Storage

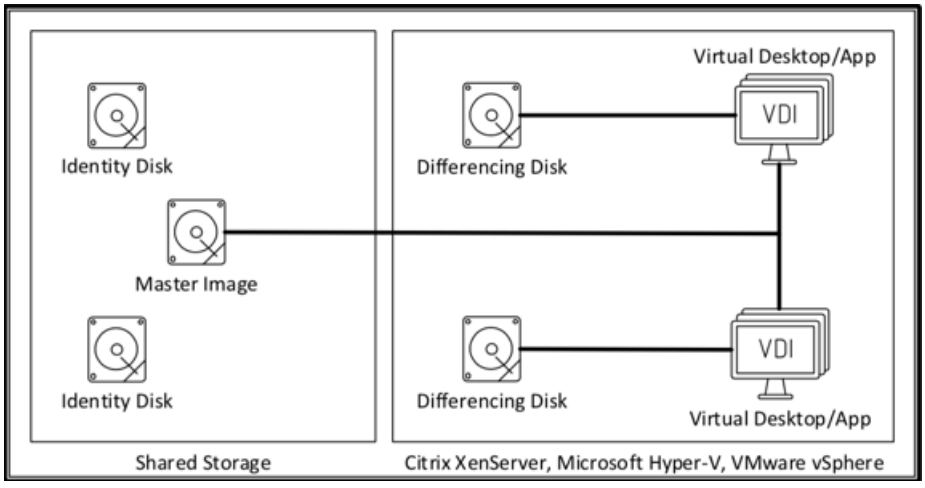
The first option utilizes shared storage for the operating system disk and the differencing disk.



Although this option allows the sharing of the master image across multiple hypervisor hosts, it puts more strain on the storage array because it must also host the differencing disk, which is temporary data.

Hybrid Storage

The second option uses shared storage for the operating system disk and local hypervisor storage for the differencing disk.



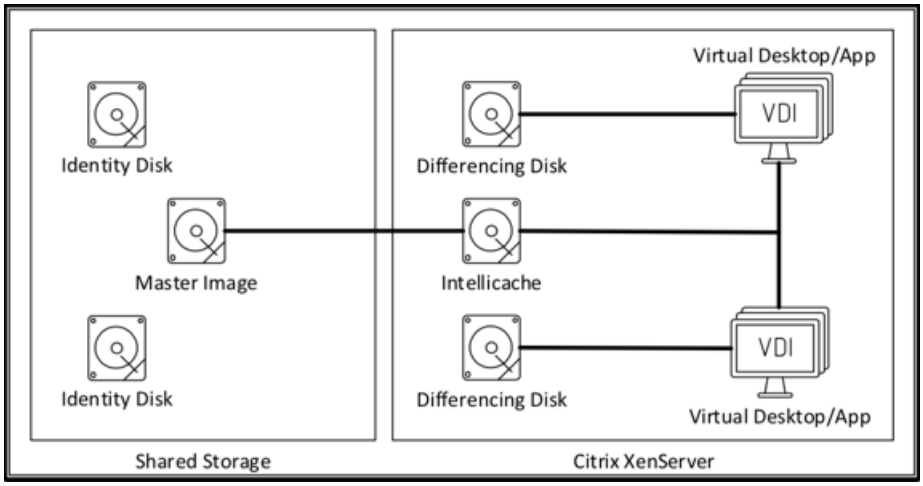
© 1999-2017 Citrix Systems, Inc. All rights reserved.

This is the most common option giving the administrator the benefits of sharing of the master image across multiple hypervisor hosts while offloading expensive, temporary write IOPS to cheap, local hypervisor storage.

XenServer IntelliCache Storage

The third option uses shared storage for the operating system disk and local hypervisor storage for the differencing disk and local XenServer storage for a local cache of the operating system disk.

This is only an option for XenServer implementations. It provides the same value as the hybrid storage approach while also reducing read IOPS from shared storage. IntelliCache can coexist with the XenServer RAM-based read cache, if XenServer RAM is limited.



Decision: Cloning Type

Machine Creation Services incorporates two types of cloning techniques.

- **Thin** - Every VM within the catalog utilizes a single, read-only virtual disk for all reads. A second virtual disk, unique for each VM, captures all write IO activity.
- **Full** – Every VM within the catalog receives a full copy of the master disk image. Each VM fully owns the disk, allowing for read/write activity. Full cloning technology is only available for personal virtual desktops, where a dedicated virtual machine saves all changes to a local disk.

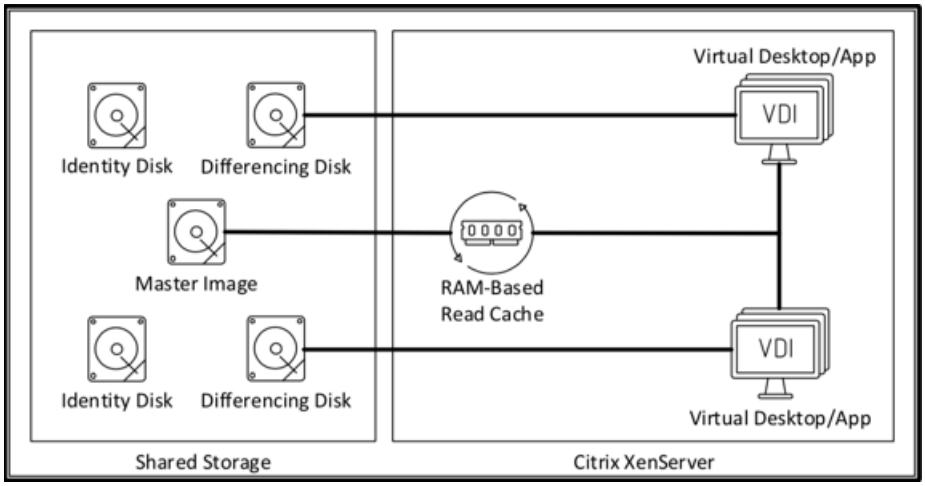
Administrators should consider the following when deciding between thin and full cloning technologies:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Thin Clone	Full Clone
Storage space requirements	Has greatest storage space savings. A single master disk image is shared across multiple VMs. Only the differencing disk (writes) consume space, which continues to grow until the VM reboots	High storage space requirements Each VM receives a full copy of the master image. The size continues to grow as changes are made to the VM.
Backup/Restore	Difficult Many 3rd party Backup/DR solutions do not support snapshot/delta disks, making thin provisioned VMs hard/impossible to backup or move to other storage arrays.	Easy The VM exists within a single virtual disk, making it easy to backup and restore.
Provisioning Speed	Fast Only requires a single disk image	Slow (can be mitigated) Each VM requires a full copy of the master image. Storage optimization technologies can help mitigate.
Performance	Slower A read I/O can occur twice, one for master disk and one for differencing disk, increasing read IOPS.	Faster All read/write direct to a single disk.
Boot Storm	High Impact In a boot storm, all differencing disks re- size to hold all writes from Windows start up; placing a high load on the storage as it happens all at once.	Low Impact

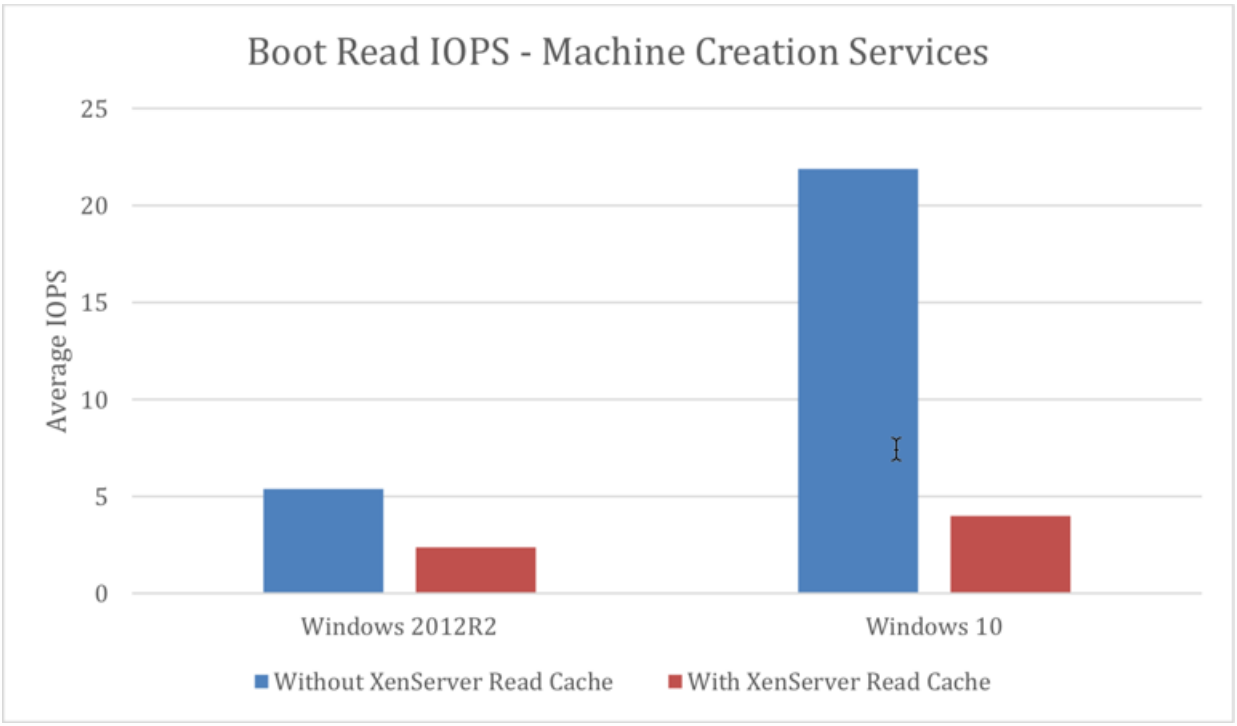
Decision: Read Cache

During boot and logon, virtual desktops incur high levels of storage read IOPS, which can put a strain on the underlying storage subsystem. When deployed on Citrix XenServer, Shared and Pooled VDI modes utilize a RAM-based read cache hosted on each XenServer.



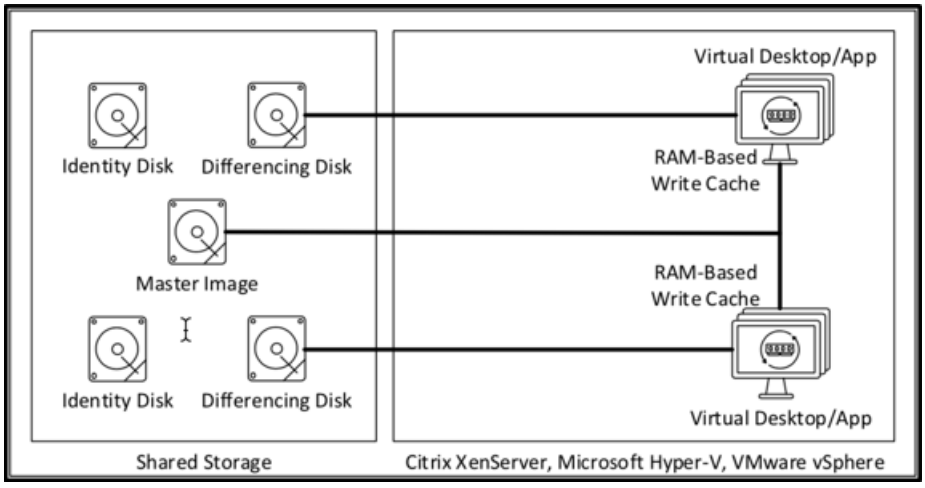
Utilizing this integrated technology reduces read IOPS by 50-80%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



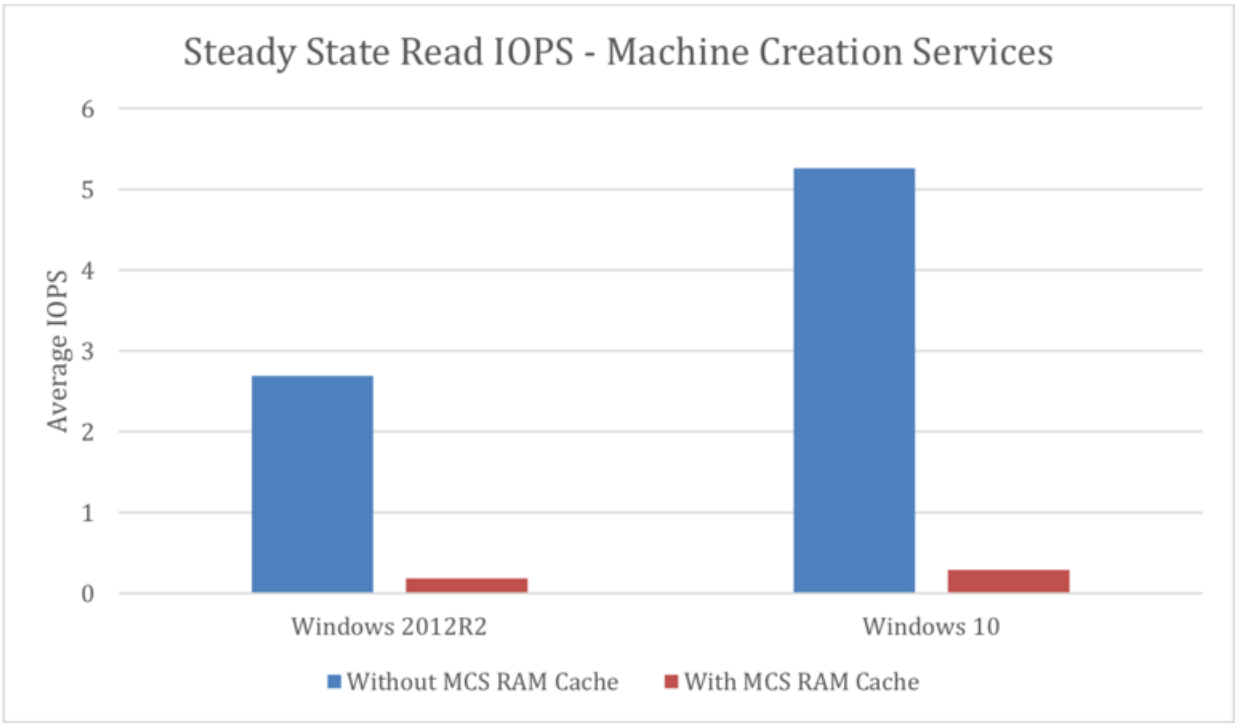
Decision: Write Cache

During steady state, virtual desktops incur high levels of storage write IOPS, which can put a strain on the underlying storage subsystem. Shared and Pooled VDI modes can utilize a RAMbased write cache by using non-paged pool RAM from the virtual machines operating system.



Utilizing this integrated technology reduces write IOPS by 95%.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Security

Depending on the requirements of the organization, different security standards should be implemented within the solution. It is advisable refer to the following papers:

- Getting Started Guide for Security
- End-to-End Encryption
- System Hardening Guide
- Common Criteria
- Secure Browsing

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Design methodology hardware layer

Apr 24, 2018

This section covers hardware sizing for the virtual infrastructure servers, virtual desktops, and virtual application hosts. The sizing of these servers is typically done in two ways.

- The first and preferred way is to plan ahead and purchase hardware based on the workload requirements.
- The second way is to use existing hardware in the best configuration to support the different workload requirements.

This section will discuss decisions related to both methods.

Decision: Workload Separation

When implementing a XenApp and XenDesktop deployment, the workloads for the infrastructure, XenDesktop, and XenApp workloads can be separated into dedicated resource clusters or mixed on the same physical hosts. Citrix recommends using resource clusters to separate the workloads, especially in an enterprise deployment. This allows better host sizing as each workload has unique requirements such as overcommit ratios and memory usage.

In smaller environments where resource clusters are cost prohibitive, the workloads may be mixed in a manner which still allows for a highly available environment. Citrix leading practice is to separate the workloads however mixed workloads is a cost based business decision.
Decision: Physical Processor (pCPU)

The following table provides guidance on the number of virtual desktops that can be supported for light, medium and heavy workloads per physical core. Each desktop correlates to a single concurrent user, with the assumption that the operating system underwent optimization.

User Workload	Operating System	Users per Physical Core
Light	Windows 7	13
	Windows 8	12
	Windows 10	12
	Windows 2008R2	18
	Windows 2012R2	21
	Windows 2016	21
Medium	Windows 7	10
	Windows 8	9

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Windows 10	9
	Windows 2008R2	12
	Windows 2012R2	14
	Windows 2016	14
Heavy	Windows 7	5
	Windows 8	4
	Windows 10	4
	Windows 2008R2	6
	Windows 2012R2	7
	Windows 2016	7

The estimate for "Users per Physical Core" is a baseline number running Microsoft Office 2010. The baseline number must be adjusted based on specific infrastructure requirements. As a general guideline, the following characteristics are baseline changes to server density.

Characteristic	Server Density Impact
Antivirus (not optimized)	25% decrease
Real-time Monitoring	15% decrease
Office 2013	20% decrease
Office 2016	25% decrease
Hyper-threading	20% increase

© 1999-2017 Citrix Systems, Inc. All rights reserved.

To estimate the total number of physical cores required for the XenApp and XenDesktop workload, use the following formula for each user group:

$$\text{Total XenDesktop pCPU} = \sum Usersi \,/ UsersPerCorei * (1 + (AV + Mon + Off13 + Off16 - HV))$$

$$\text{Total XenApp pCPU} = \sum Usersi \,/ UsersPerCoreii * (1 + (AV + Mon + Off13 + Off16 - HV))$$

∑ represents the sum of all user group combinations “i”.

Usersi = Number of concurrent users per user groups

UsersPerCorei = Number of users per physical core

AV = Antivirus impact (default = 0.25)

Mon = Monitoring tools impact (default = 0.15)

Off13 = Office 2013 impact (default = .2)

Off16 = Office 2016 impact (default = .25)

HT = Hyper-Threading impact (default = .2)

If workloads will be separated (XenApp and XenDesktop workloads), the formula should be calculated twice, once for all XenDesktop users and the second for all XenApp users in order

Decision: Physical Memory (pRAM)

The recommended method for sizing memory to a physical host is to size based on the total memory required to support the virtual machines and the CPU capacity of the host. In order to calculate the total memory required for XenApp and XenDesktop, simply multiply the number of virtual machines by the amount of memory allocated to the virtual machines. The sum of all of the machine catalogs will be the total RAM required for XenApp and XenDesktop hosts. This is shown in the formula below.

$$Total\ XenDesktop\ pRAM = \sum_i VM_i * vRAM_i$$

$$Total\ XenApp\ pRAM = \sum_i VM_i * vRAM_i$$

∑ represents the sum of all user group combinations “i”.

VMi = Number of concurrent users per user groups

vRAMi = Amount of RAM assigned to each virtual machine

If workloads will be separated onto different hosts (XenApp and XenDesktop workloads), the formula should be calculated twice, once for all XenDesktop users and the second for all XenApp users.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Physical Host (pHost)

In most situations, the number of physical hosts (pHost) to support the XenApp and XenDesktop workloads will be limited on the number of processor cores available. The following formula provides an estimate for the number of hosts required for the user workloads. The formula is based on the best practice of separating the XenApp and XenDesktop workloads due to the different recommended CPU overcommit ratios for each.

[illegible] = ([illegible] [illegible] [illegible]/ [illegible] [illegible] [illegible] +1)

[illegible] = ([illegible] [illegible] [illegible]/ [illegible] [illegible] [illegible]+ 1)

Once the number of physical hosts has been determined based on processor cores, the amount of RAM for each host is calculated.

[illegible] [illegible] [illegible] [illegible] = [illegible] + ([illegible] [illegible] [illegible] /[illegible] [illegible] – 1)

[illegible] [illegible] [illegible] [illegible] = [illegible] + ([illegible] [illegible] [illegible]/[illegible] [illegible] – 1)

Decision: GPU

Hosts used to deliver graphical workloads require graphics processors to deliver a high end user experience. Specific hardware hosts and graphics cards are required to support high end graphics using HDX 3D Pro. An updated list of tested hardware is available in a knowledge base article. Sizing of the desktop and application hosts of high end graphics users should be based on the GPU requirements ensuring that the host then has adequate CPU and memory resource to support the workload.

NVIDIA GRID cards can be leveraged with vGPU profiles to support multiple users. Sizing guidelines are provided from NVIDIA in the table below.

In the table, **Y** indicates that application certificates are available.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NVIDIA GRID Graphics Board	Virtual GPU Profile	Application Certifications	Graphics Memory	Max Displays Per User	Max Resolution Per Display	Max vGPU Per Graphics Board	Use Case
GRID K2	K280Q	Y	4,096 MB	4	2560 x 1600	2	Designer
	K260Q	Y	2,048 MB	4	2560 X 1600	4	Designer / Power User
	K240Q	Y	1,024 MB	2	2560 x 1600	8	Designer / Power User
	K220Q	Y	512 MB	2	2560 x 1600	16	Knowledge Worker
	K200		256 MB	2	1900 x 1200	16	Power User
GRID K1	K180Q	Y	4,096 MB	4	2560 x 1600	4	Power User
	K160Q	Y	2,048 MB	4	2560 x 1600	8	Power User
	K140Q	Y	1,024 MB	2	2560 x 1600	16	Power User
	K120Q	Y	512 MB	2	2560 x 1600	32	Power User
	K100		256 MB	2	1900 x 1200	32	Knowledge Worker

Storage Sizing

Decision: Storage Architecture

The primary storage architectures are as follows:

- **Local Storage** - Uses hard disks directly attached to the computer system. The disks cannot be shared with other computer systems, but if the computer is hosting pooled or hosted shared desktops, a shared storage solution is not necessary. In many cases local storage can perform as well as shared storage. Scalability is limited to the number of drive bays available in the computer system. Many blade servers for example have just two drive bays, so using local storage to support a XenDesktop deployment may not be optimal.
- **DAS** - Storage sub-system directly attached to a server or workstation using a cable. It uses block-level storage and can be a hard disk local to the computer system or a disk shelf with multiple disks attached by means of external cabling. Unlike local disks, disk shelves require separate management. Storage shelves can be connected to multiple servers so the data or disks can be shared.
- **NAS** - Provides file-level storage to computer systems through network file shares. The NAS operates as a file server, and

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NAS systems are networked appliances which contain one or more hard drives, often arranged into logical, redundant storage containers or RAID arrays. Access is typically provided using standard Ethernet and network file sharing protocols such as NFS, SMB/CIFS, or AFP.

> ## Nota
>
> NAS can become a single point of failure. If the network share becomes unavailable, all target devices streamed from the disk will be unavailable as well.

- **SAN** - Dedicated storage network that provides access to consolidated, block-level storage. SANs allow computers to connect to different storage devices, so no server has ownership of the storage subsystem enabling data to be shared among multiple computers. A SAN will typically have its own dedicated network of storage devices that are generally not accessible through the network by standard means. In order to connect a device to the SAN network a specialized adapter called the Host Bus Adapter (HBA) is required. SANs are highly scalable with no noticeable change in performance as more storage and devices are connected. SANs can be a costly investment both in terms of capital and the time required to learn, deploy and manage the technology.
- **Hybrid** - A NAS head refers to a NAS which does not have any on-board storage, but instead connects to a SAN. In effect, it acts as a translator between the file-level NAS protocols (NFS, CIFS, etc.) and the block-level SAN protocols (Fibre Channel and iSCSI). Thus it can combine the advantages of both technologies and allows computers without Host Bus Adapters (HBA) to connect to centralized storage.

The following table summarizes the storage options available and rates their suitability for XenDesktop deployments.

Storage Properties	Local	DAS	NAS	SAN
Implementation costs	Low	Medium	Medium	High
Administration	Low	Medium	Medium	High
Performance	High	Med - High	Med - High	High
Redundancy	Low - Med	Med - High	Med - High	High
Scalability	Low	Med - High	Med - High	High
Typical use case	Small to medium production and test environments	Small to medium production environments	Small to medium production environments	Medium to large production environments

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota

Hyper-V 2008 R2 does not support NAS technology. Hyper-V 2012/2012 R2 only supports NAS solutions that support the SMB 3.0 protocol. For more information please refer to the HyperV 2008 R2 and Hyper-V 2012 R2 sections of the handbook.

Local storage is best suited for storing virtual machines which do not have high availability requirements or persistent data attached such as random (pooled) desktops or hosted shared desktops. Local and DAS is suited for storing user data and home directory files. If using Machine Creation Services, master images as well as any updates must be replicated to each server.

NAS and SAN storage is best suited for infrastructure servers supporting the XenDesktop environment, and virtual machines with persistent data such as static (dedicated) desktops.

Decision: RAID Level

To choose the optimal RAID level, it is necessary to consider the IOPS and read/write ratio generated by a given application or workload in combination with the individual capabilities of a RAID level. For hosting read intensive workloads, such as the Provisioning Services vDisk store, RAID levels that are optimized for read operations such as RAID 1, 5, 6, 10 are optimal. This is because these RAID levels allow read operations to be spread across all disks within the RAID set simultaneously.

For hosting write intensive workloads, such as Provisioning Services write cache and Machine Creation Services differencing disks, RAID levels such as RAID 1 or 10 are optimal, as these are optimized for writes and have a low write penalty.

The following table outlines the key quantitative attributes of the most commonly used RAID levels:

RAID	Capacity (%)	Fault Tolerance	Read Performance	Write Performance	Minimum number of disks
0	100	None	Very High	High (Write Penalty 1)	2
1	50	Single-drive failure	Very High	Medium (Write Penalty 2)	2
5	67 - 94	Single-drive failure	High	Low (Write Penalty 4)	3
6	50 - 88	Dual-drive failure	High	Low (Write Penalty 6)	4
10	50	Single-drive failure in each sub array	Very High	Medium (Write Penalty 2)	4

Nota

The write penalty is inherent in RAID data protection techniques, which require multiple disk I/O requests for each application write request, and ranges from minimal (mirrored arrays) to substantial (RAID levels 5 and 6).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Number of Disks

To determine the number of disks required it is important to understand the performance characteristics of each disk, the characteristics of the RAID level and the performance requirements of the given workload. The basic calculation for determining the total number of disks needed is:

□□□□□ # □□ □□□□□ =
(□□□□□ □□□□ □□□□ + (□□□□□ □□□□□ □□□□ ∗ □□□□ □□□□□□□))/□□□□ □□□□□ □□□□

For example, a disk manufacturer is reporting that a particular disk array which they have developed has a total workload IOPS of 2000. The raw IOPS per disk is 175. To determine how many disks are required to support a workload with 20% read operations and 80% write operations on RAID 10:

□□□□□ # □□ □□□□□ =((20% ∗ 2000) + (80% ∗ 2000) ∗ 2) /175= 20.57 □□ 21 □□□□□

Based on the previous example, the following table shows how the disk count will vary based on the RAID level and the read/write ratio.

RAID	RAW IOPS (per disk)	Workload IOPS	Read %	Write %	Disk Count
0	175	2000	20	80	12
	175	2000	80	20	12
1 / 10	175	2000	20	80	21
	175	2000	80	20	14
5	175	2000	20	80	39
	175	2000	80	20	19

Decision: Disk Type

Hard disk drives (HDDs) are the traditional variation of disk drives. These kinds of disks consist of rotating platters on a motor-driven spindle within a protective enclosure. The data is magnetically written to and read from the platter by read/write heads.

Different implementations of this technology are available on the market, which differ in terms of performance, cost and reliability.

- Serial ATA (SATA) disk transmit data serially over two pairs of conductors. One pair is for differential transmission of data,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

and the other pair is for differential receiving of data. SATA drives are widely found in consumer desktop and laptop computers. Typical SATA drives have transfer speeds ranging from 1500 – 6000Mbps and support hot-swapping by design.

- Small Computer Systems Interface (SCSI) disks use a buffered, peer to peer interface that uses handshake signals between devices. Many SCSI devices require a SCSI initiator to initiate SCSI transactions between the host and SCSI target. SCSI disks are common in workstations and servers and have throughputs ranging from 40 – 5120Mbps. iSCSI (Internet Small Computer System Interface) is a mapping of the regular SCSI protocol over TCP/IP, more commonly over Gigabit Ethernet.
- Fibre Channel (FC) disk is the successor to the parallel SCSI disk and is common in SAN storage devices. Fibre Channel signals can run on an electrical interface or fibre-optic cables. Throughput can range from 1 – 20Gbps, and connections are hot-pluggable.
- Serial Attached SCSI (SAS) disk uses a new generation serial communication protocol to allow for higher speed data transfers than SATA disks. Throughput can range from 2400 – 9600Mbps.

In contrast to traditional hard disks, Solid State Disks (SSDs) use microchips to retain data in either NAND non-volatile memory chips (flash) or DRAM and contain no moving parts. SSDs are less susceptible to physical shock, have lower access times and latency and have higher I/O rates. SSDs have significantly higher random read performance. An SSD drive can attain anywhere from 5,000 to 20,000 random reads per second. SSDs are also more expensive per gigabyte (GB) and typically support a limited number of writes over the life of the disk.

Flash memory-based SSDs can be either based on multi-level cells (MLC) or single-level cells (SLC). SLC devices only store one bit of information in each cell. MLC devices can store multiple bits of information with each cell. Flash based SSDs cost lower than DRAM based SSDs but perform slower. DRAM based SSD devices are used primarily to accelerate applications that would otherwise be held back by the latency of flash SSDs or traditional HDDs.

SSDs were previously not viable for enterprise storage solutions because of the high cost, low capacity and fast wear of the drives. Improvements in SSD technology and lowering costs are making them more favorable over HDDs. Solid state hybrid drives (SSHD) combine the features of SSDs and HDDs, by containing a large HDD drive with an SSD cache to improve performance of frequently accessed data.

Comparing SSDs and HDDs is difficult since HDD benchmarks are focused on finding the performance aspects such as rotational latency time and seek time. As SSDs do not spin, or seek, they may show huge superiority in such tests. However, SSDs have challenges with mixed reads and writes and their performance may degrade over time.

The following table compares the transfer rates of some of the more common storage types available on the market today.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Technology	Rate (MBps)
iSCI over Fast Ethernet	100
Ultra-2 wide SCSI (16 bits/40 MHz)	640
iSCI over Gigabit Ethernet	1,000
SATA rev 3	6,000
SAS 3	9,600
FCoE over 10 GbE	10,000
SATA rev 3.2 - SATA Express	16,000
iSCI over Infiniband	32,000

SCSI and SATA disks are best suited for storing data that does not have high performance requirements like the PVS vDisk store. SAS, Fibre Channel, or SSD drives are best suited for storing data that have high performance requirements like the PVS write cache.

Decision: Storage Bandwidth

Storage bandwidth is the connectivity between servers and the storage subsystem. Understanding bandwidth requirements can help determine the proper hardware for delivering data and applications at speeds for a positive end user experience. For most datacenters 10Gbps Ethernet or 10Gbps FCoE is sufficient for storage connections. Smaller environments however may only need 1Gbps bandwidth. In virtualized environments it is not just important to look at the bandwidth requirements of the physical host and storage subsystem, but determining how much bandwidth is required for each virtual machine plays a factor too.

In order to plan for the required bandwidth, it is necessary to determine the throughputs for every individual system that uses a shared component or network path. For example, the following information is provided for an environment with 100 similar virtual machines (hosted on 10 virtualization hosts and connected to one NAS head).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Average	Peak
Throughput per VM	10 MBps	30 MBps
Throughput per host	100 MBps (10 VMs x 10 MBps)	300 MBps (10VMs x 30 MBps)
Throughput per storage	1 GBps (10 hosts x 100 MBps)	3 GBps (10 hosts x 300 MBps)

The NIC used for storage communication needs to be a 1Gbps adapter in order to handle the peak load. The NAS head as well as its network connection need to support 3Gbps worth of data traffic in order to support the peak load of all systems.

Decision: Tiered Storage

A one-size-fits-all storage solution is unlikely to meet the requirements of most virtual desktop implementations. The use of storage tiers provides an effective mechanism for offering a range of different storage options differentiated by performance, scalability, redundancy and cost. In this way, different virtual workloads with similar storage requirements can be grouped together and a similar cost model applied.

For example, a XenDesktop implementation using tiered storage may look like the following:

- **Tier 1 storage group** - Write intensive files such as the write cache and differencing disks are placed in a storage group consisting of SSDs.
- **Tier 2 storage group** - Mission critical data, or data that requires high availability, are placed in a storage group consisting of less expensive high performing drives.
- **Tier 3 storage group** - Seldom used data files, read-only files, or other non-mission critical data placed in a storage group consisting of low cost and lower performing drives.

Decision: Thin Provisioning

Thin provisioning allows more storage space to be presented to the virtual machines than is actually available on the storage repository. This lowers storage costs by allowing virtual machines access to disk space that is often unused. This is particularly beneficial to Machine Creation Services which uses a linked-clone approach to provisioning virtual machines. Thin provisioning minimizes the storage space required for the master image copies used to build virtual machines. Thin provisioning is possible at the physical storage layer, a feature usually available with most SAN solutions, and at the virtual layer. NFS based storage solutions will usually have thin provisioning enabled by default.

At the physical storage layer, it is important to ensure that sufficient storage is available to prevent the risk of virtual machines not being available in a storage “overcommit” scenario when available disk space is exhausted. Organizations should decide if the cost savings thin provisioning provides outweighs the associated risk and consider enabling if the storage solution supports it.

> ## Nota
>
> Virtual machines may not function if disk space is exhausted so it is important to have a process in place, either through alerts or

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> notifications that will give administrators enough time to add more disks to the storage solution so that the XenDesktop environment is not impacted.

Decision: Data De-Duplication

Data de-duplication is a data compression technique whereby duplicate data is replaced with pointers to a single copy of the original item. This reduces storage requirements and costs by improving storage utilization, however it can impact storage performance.

There are two implementations of de-duplication available:

- **Post-process de-duplication** – The de-duplication is performed after the data has been written to disk. Post-process de-duplication should be scheduled outside business hours to ensure that it does not impact system performance. Post Process de-duplication offers minimal advantages for random desktops as the write-cache/difference disk is typically reset on a daily basis.
- **In-line de-duplication** – Examines data before it is written to disk so that duplicate blocks are not stored. The additional checks performed before the data is written to disk can sometimes cause slow performance. If enabled, in-line duplication should be carefully monitored to ensure that it is not affecting the performance of the XenDesktop environment.

If the storage solution supports it, enabling post-process data de-duplication is recommended for minimal impact to XenDesktop performance.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Monitor

Jan 29, 2018

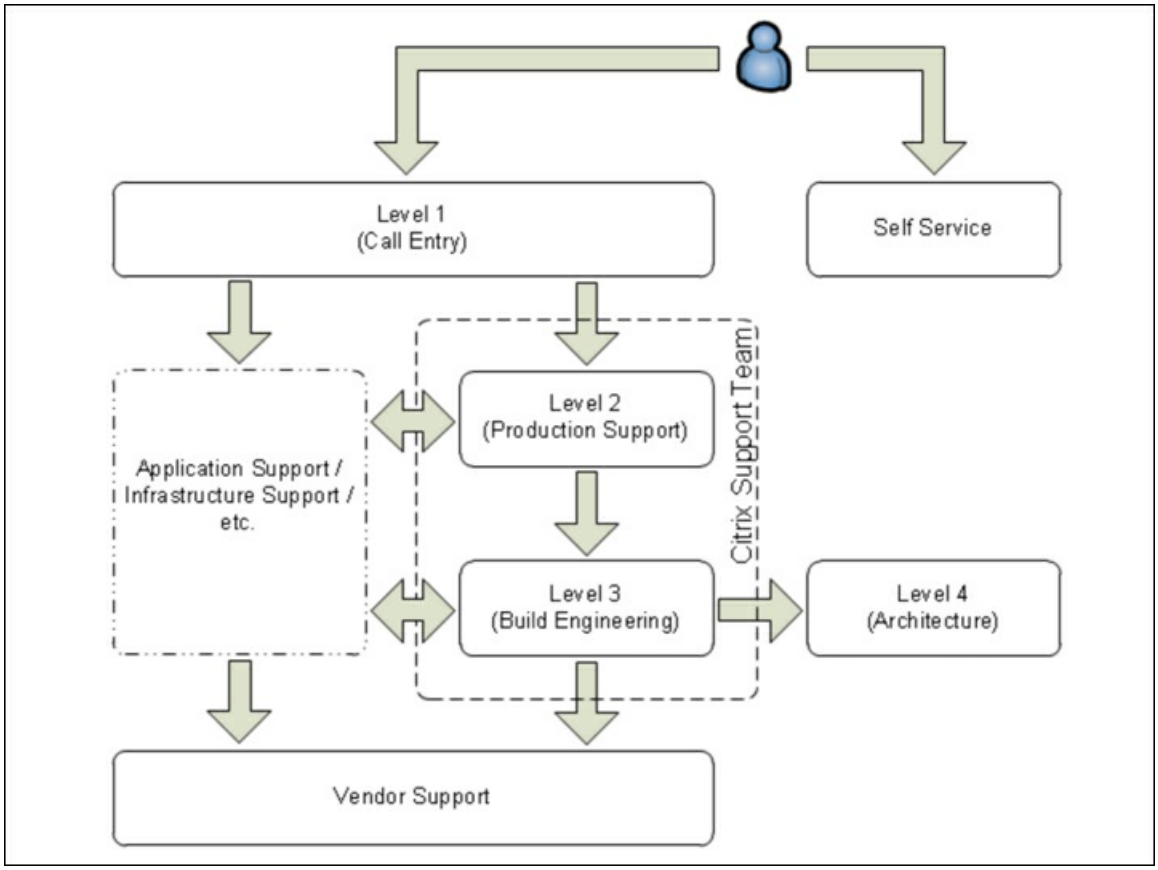
Like any integrated system, monitoring and maintenance is critical to the overall health of the solution. Without proper support, operations and health monitoring systems in place, the user experience will slowly start to degrade.

Process 1: Support

When problems arise, technical support is the first point of contact. This section addresses the proper staffing, organization, training, delegated administration and tools that should be used to maintain the Citrix deployment.

Decision: Support Structure

Multiple levels of support have been found to be the most effective ways of addressing support issues. Low criticality, low complexity or frequently occurring issues should be managed and resolved at the lower support levels. High criticality and complex issues are escalated to more experienced architects or infrastructure owners. The diagram below outlines a common multi-level support structure.



If a user encounters an issue, Level-1 support (help desk) is the entry point to the support system. Level-1 should resolve 75% of all issues encountered, of which a majority will be routine problems that only require a limited knowledge of the Citrix environment. At this level, issues are quickly resolved and some may be automated (self-service), for example password resets and resource provisioning.

Non-routine problems that exceed Level-1's abilities are escalated to Level-2 (Operators). This support level is generally

© 1999-2017 Citrix Systems, Inc. All rights reserved.

comprised of administrators supporting the production Citrix environment. Information on the end user's problem and attempted troubleshooting steps are documented at the first level allowing Level-2 technicians to immediately begin addressing the problem. Level-2 technicians should handle only 20% of the support tickets and are highly knowledgeable on the Citrix environment.

Complex issues that exceed Level-2's abilities should be escalated to Level-3 (Implementers). Level-2 and Level-3 support may often both be members of the Citrix Support Team, with Level-3 comprising the senior staff maintaining the Citrix environment. Level-3 issues are complicated and often mission critical requiring expert knowledge of the virtual desktop and application environment. Level-3 support tickets should amount to no more than 5% of all support issues.

The final level, Level-4 (Architects), is focused on the strategic improvements for the solution, testing new technologies, planning migrations, and other high level changes. Generally, Level-4 is not involved in active support of a production environment.

Should support discover an issue that is related to an application or underlying infrastructure, the ticket is handed to the appropriate team for troubleshooting. If a program bug is discovered, the issue is then re-escalated and a ticket is established with the appropriate vendor.

Decision: Support Responsibilities and Skill Set

The following table highlights the recommended characteristics of each support level.

Support level	Description	Responsibilities	Skill set
Level 1 - Help	Provide first-line support of reported issues. Initially, servicing support messages and phone calls. This level needs to perform	• Perform issue definition, initial analysis and basic issue resolution • Perform initial troubleshooting to determine the nature of the issue • Create ticket, collect user information, and log all troubleshooting steps performed • Resolve basic Citrix related issues, connectivity problems and application related issues using existing knowledge base articles • Escalate issue to Level-2 if advanced skills or elevated	• General Citrix XenApp/XenDesktop knowledge (CCA, CCA-V) • General Windows client OS/server OS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
	issue resolution. Often processes requests for application access or support with configuring plugins.	required • Ability to isolate the issue to be Citrix related, Microsoft related or third party Application related • If it affects the production environment or is potentially causing a system level outage, escalate directly to Level-3 • Generate requests for additional issue resolution guides as necessary • Follow up with end users when a support ticket is closed to ensure the problem has been satisfactorily resolved	• General Active Directory knowledge • General Networking knowledge (CCNA)
		• Perform intermediate issue analysis and resolution. • Identify root cause of issues. • Respond to server alerts and system outages. • Create weekly report on number of issues, close rate, open issues, etc. • Review vendor knowledge base articles. • Respond to out-of-hours helpdesk calls. • Respond to critical monitoring alerts. • Generate internal knowledge base articles and issue	Experience with Microsoft Windows Server including but not limited to: • Configuring operating system options • Understanding Remote Desktop Services policies and profiles • Using Active Directory • Creating users/managing permissions and administrator rights • Creating and modifying Active Directory group policies Basic administration

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
Level-2 (Operators)	Primarily supporting day-to-day operations of the Citrix environment, may include proactive monitoring and management. In addition, this role should also perform intermediate level troubleshooting and utilize available monitoring or troubleshooting tools. Assist with resolving issues escalated by Level-1 support.	Level-1 troubleshooting workflows. • Perform basic server maintenance and operational procedures. • Manage user profiles and data. • Escalate ticket to Level-3 or appropriate technology owner if advanced skills or elevated permissions are required. • Generate requests for additional issue resolution scripts and knowledge base articles as necessary. • Able to read built-in event logs for Windows and Citrix to do basic troubleshooting following public information via Google/Bing.	protocols (TCP) • An understanding of firewall concepts • An understanding of email administration and account creation • An understanding of Remote Desktop Services policies and profiles • The ability to create shares and give access to shared folders/files Experience performing the following: • Managing, maintaining, monitoring and troubleshooting Citrix solutions • Backing up components in Citrix environments • Updating components in Citrix environments • Creating reports for trend analysis
		• Perform advanced issue analysis and resolution. • Perform maintenance and environment upgrades. • Addresses high severity issues and service outages. • Manage the Citrix environment. • Oversee and lead administrative tasks performed by Level-2. • Manage network and storage	Knowledge of how the following Windows components integrate with Citrix technologies: • Active Directory Domain Services • Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skillset
		relates to the Citrix environment (depending on size	• Policies • Domain Name System (DNS)
Level-3 (Implementer)	Central point for implementing, administering and maintaining Citrix desktop and application virtualization infrastructure. This role focuses on deploying new use cases and leading lifecycle management initiatives. Generally, one Implementer could focus on one use-case at a time. For example, three new concurrent use cases would require three Implementers. Escalates issues to software vendor specific technical support and notifies Level-4 about this issue.	of company or Citrix environment). • Review periodic reports of server health, resource usage, user experience, and overall environment performance. • Review vendor knowledge base articles and newly released updates. • Perform policy-level changes and make Active Directory updates. • Review change control requests that impact the Citrix environment. • Perform advanced server and infrastructure maintenance. • Review knowledge base articles and issue resolution scripts for accuracy, compliance, and feasibility. • Create knowledge base articles and issue resolution scripts to address Level-2 requests. • Escalate ticket to vendor specific technical support, when necessary, and notify Level-4 of the issue.	• Dynamic Host Configuration Protocol (DHCP) • Group Policy Objects (GPOs) • NTFS Permissions • Authentication and Authorization • Knowledge of IIS • Microsoft Windows Operating Systems: Windows 10, Windows 8.1, Windows 7 Windows Server 2012 R2 Windows Server 2008 R2 • Roles and features of Windows Server • Knowledge of SQL 2008 R2 and newer • Knowledge of SQL Clustering, Mirroring and AlwaysOn Availability Groups. • General networking skills (i.e. routing, switching) • Knowledge of hypervisors. • Knowledge of shared storage configuration and management.
		• Provide technical leadership for	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support level	Description	Responsibilities	Skill set
Level-4 (Architect)	The Level-4 team has minimal exposure to administrative tasks but focuses on scoping, planning and executing Citrix-specific service and project requests. An architect translates business requirements into a technical design.	• Lead design updates and architecture revisions. • Address high severity issues and service outages. • Oversee technology integration workflows. • Review periodic reports of server health, resource usages, user experience, and overall environment performance to determine next steps and upgrade paths. • Initiate load testings to determine capacity of environment. • Review frequently recurring helpdesk issues. • Ensure technical specifications continue to meet business needs. • Update design documentation.	Advanced architectural assessment and design skills for: • Citrix XenApp • Citrix XenDesktop • Citrix XenServer, VMware vSphere, Microsoft Hyper-V • Citrix Provisioning Services • Citrix NetScaler • Citrix StoreFront • Active Directory • Storage solutions • Networking • Application delivery • Disaster recovery • Policies/policy structures and security restrictions • Licensing • Methodology Intermediate knowledge of: • General networking skills • Change control process • Project management • Risk assessment
Vendor support	Vendor assistance may be necessary should defects in a program be discovered. At this stage, Level-3 engineers need to establish a support ticket with the appropriate vendor to assist with finding a solution.		
Self-service	A self-service portal should be utilized for noncritical tasks, such as application access, permissions, password resets, etc. The portal can range from a simple FAQ page to a fully automated process requiring no human interaction. The purpose of the self-service portal is to add an additional touch point for end users to address basic issues, preventing the creation of new support tickets.		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Certifications and Training

The following table details the recommended training, certifications and experience for each support level.

Role	Recommended training	Recommended course(s)	Recommended certification	Relevant experience
Help Desk (Level 1)	Level-1 support personnel should be provided with basic training on Citrix XenApp, Citrix XenDesktop and supporting technologies. This can include internal training from subject matter experts or from a Citrix Authorized Learning Center. The training provided should focus on the following topics: • High level overview of the XenApp and XenDesktop implementation • Using Citrix Director to manage user sessions • Troubleshooting Citrix XenApp and XenDesktop sessions • Troubleshooting methodology In addition, regular training should be provided to the Tier-1 team members on the latest troubleshooting recommendations from the Level-2 and Level-3 teams as well as details on any relevant changes to the environment. This will help to ensure a good baseline knowledge level across the team and consistent customer service.	CXD-105: Citrix XenApp and XenDesktop Help Desk Support	N/A	1+ years (Entry level also acceptable)
Operator (Level 2)	Level-2 personnel should conduct regular team training sessions to refine administrative skills and ensure a baseline knowledge level across the team. Formalized trainings are also essential when there are architectural updates to the environment and the Level-2 team is working with unfamiliar technologies. All members of the Level-2 team should achieve the Citrix Certified Associate (CCA) certification for Citrix XenApp and XenDesktop. Advanced training on Windows concepts will also be essential for Level-2 team members who do not have desktop or server support experience. Finally, on-the-job training along with close integration with Level-3 administrators is essential as the Level-2 roles are formalized and responsibilities are handed over from Level-3 to Level-2.	CXD-210 XenApp and XenDesktop 7.1x Administration	Citrix Certified Associate - Virtualization	2-3 years
Implementer (Level-3)	Level-3 support team members hold a minimum of three years of enterprise experience implementing and supporting XenApp, XenDesktop, Provisioning Services and Windows operating systems. Level-3 staff should also complete the Citrix Certified Professional (CCP) certification track as this will prepare them to proactively manage the user community and implement Citrix solutions according to Citrix leading practices.	CXD-400: Designing App and Desktop Solutions with Citrix XenApp and XenDesktop after completion of level-3 CXD-310	Citrix Certified Expert - Virtualization	3-4 years
	Experience is essential for Level-4 staff. A qualified Level-4			

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role	Recommended training	Recommended course(s)	Recommended certification	Relevant experience
Architect (Level 4)	implementing, supporting, and serving in a technology architect role for a XenApp and/or XenDesktop environment as well as additional administrative experience with integrated technologies such as application and profile management solutions. The ideal candidate will have served in such a capacity at two or more environments for purposes of product exposure and in at least one environment of over 1,200 concurrent users. A Citrix Certified Expert (CCE) certification or comparable training and experience should be a prerequisite of the role.	CXD-400: Designing App and Desktop Solutions with Citrix XenApp and XenDesktop after completion of level-3 CXD-310	Citrix Certified Expert - Virtualization	5+ years

Decision: Support Staffing

The following table provides guidance on the recommended number of support staff.

Role	Small Environment: Sites: 1; Users: <500; Images: 1-2	Mid-size Environment: Sites: 1-2; Users: 1000-5000; Images: 3-5	Large Environment: Sites: 2+; Users: >5000; Images: 5+
Help Desk (Level-1)	3	5-10	15-20
Operator (Level-2)	1-2	2-3	4-5
Implementer (Level-3)	1	1-2	2-3
Architect (Level-4)	1	1	1-2

Nota

This table should only be used as a baseline. Support staffing decisions should be evaluated against the defined requirements, projected workloads, and operational procedures of an organization. Multiple levels can be combined, for example there may be insufficient design projects to have a dedicated architect role or a more senior member of the Citrix team can act as an Operator and Implementer.

Decision: Job Aids

General Support Tools: The following table details tools that should be made available to all support levels.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tools	Details
Ticket Management System	Used to document customer information and issues. A typical ticket management system provides the following functionality: • Monitoring the queue of tickets. • Setting a limit on the number of open tickets. • Establishing thresholds such as how long a certain type of ticket should take to be answered. • Identifying a group of users or individuals who require higher priority assistance. Informing the user when their ticket is open, updated, or closed. • Provide an internal knowledge base for the support professionals to search for known resolved issues.
Call Scripts	The first contact help desk personnel should have documented scripts to ensure that all relevant data is captured while the user is on the phone. This practice also assists in proper triage and allows the next support level to perform research prior to customer contact. A sample call script is provided for reference.
Remote Assistance Tools	Remote assistance tools are useful when troubleshooting user issues. Support technicians and administrators can remotely observe a user's actions.
Knowledge Base	Documentation should be created and maintained in a knowledge base or library of known issues. Articles should be searchable for quick recovery. Knowledge bases help support staff to quickly resolve known issues and reduce the need to perform time consuming research.

Citrix Support Tools

The following table provides recommendations on the Citrix support tools that should be made available to each support level.

Tool	Description	Products				Support Level			
		XenDesktop	XenApp	Provisioning Services Console	XenServer	L1	L2	L3	L4
Citrix Director	Citrix Director provides an overview of hosted desktops and application sessions. It enables support teams to monitor and troubleshoot issues.	X	X			X	X	X	X
Citrix Studio	Citrix Studio enables administrators to								

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	perform configuration as well as maintenance tasks for a XenApp and XenDesktop site and associated virtual desktops or hosted applications.	X	X			X	X	X	X
Citrix Insights Services	Run from a single Citrix Delivery Controller to capture key data points and CDF traces for selected computers followed by a secure and reliable upload of the data package to Citrix Technical Support for escalation.	X	X	X	X			X	X
HDX Monitor	HDX Monitor is a tool to validate the operation of the Citrix ICA/HDX stack of a user session. HDX Monitor provides information about client capabilities, network performance/activity, session settings and many more items.	X	X			X	X	X	X
Provisioning Services Console	The Provisioning Services Console enables administrators to perform configuration and maintenance tasks for a Provisioning Services farm.			X				X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenCenter	XenCenter enables administrators to perform configuration and maintenance tasks for a XenServer Resource Pool.				X			X	X

Citrix Insight Services

Administrators can utilize Citrix Insight Services to simplify the support and troubleshooting of the Citrix environment. Citrix Insight Services is run locally to collect environment information. Online analysis capabilities analyze that information and provide administrators recommendations based on their Citrix environment and configuration. Additional information regarding Citrix Insight Services can be referenced in the Citrix Support article CTX131233 - FAQ: Citrix Insight Services.

A full list of the available tools provided by Citrix Support to assist with troubleshooting can be referenced in Citrix Supportability Pack.

Call Script

The following call script can be used as an initial baseline for a Citrix Help Desk team. Citrix Consulting recommends reviewing this sample call guide and adding any environment specific details that may need to be collected.

1. **What is the name and location of the user?**
   This question will identify if the user is accessing the environment from an external or internal network location.
2. **Is the problem always reproducible?**
   If it is a Yes, get the exact reproduce steps. This question is very important for the support team to troubleshooting an issue.
3. **Do any other users at the site/location experience the same issue? Can they have a colleague logon from same and/or different workstation?**
   These questions help to determine if this is a workstation issue or a user issue.
4. **What type of endpoint device is the user utilizing? (Corporate device, BYOD, thin client, pc, laptop, etc.)**
   This question will help determine if the issue is related to the user's endpoint.
5. **What is the Citrix Receiver version and connection information?**
   This question will verify if the user is using the right version of Receiver (the latest Receiver version or the version standardized by the company).
6. **Can the user see the StoreFront authentication page?**
   This question helps to identify network issues.
7. **What is the name of the application (or virtual desktop) the user is attempting to use? Does the user see the appropriate application or desktop icon on the StoreFront site?**
   These questions help to determine if there is an issue with user access and/or group membership.
8. **Does the application (or desktop) launch when the icon is selected? Does the application logon screen appear (if applicable)?**
   These questions help to determine if a connection is made into the Citrix XenDesktop infrastructure.
9. **Can the user authenticate into the application (if applicable)? Does the issue occur after the application is launched?**
   This question helps to determine if the issue is with the application rather than the application delivery infrastructure.
10. **What is the specific error seen (if applicable)?**
    This question identifies the specific error. The user should be requested to provide a screenshot, if available.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Delegated Administration

Each support level must be provided with sufficient rights to effectively perform their role. The following tables provide guidance on the recommended privileges per support level.

XenApp/XenDesktop Delegated Rights

Administrator role	Support Level
Help Desk Administrator	Level-1
Full Administrator	Level-2
Full Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a XenApp/XenDesktop Site, please refer to Citrix Product Documentation - XenApp and XenDesktop Delegated Administration.

Provisioning Services Delegated Rights

Administrator Role	Support Level
N/A	Level-1
Site Administrator	Level-2
Farm Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a Provisioning Services Site, please refer to Citrix eDocs - Provisioning Services Managing Administrative Roles.

StoreFront Delegated Rights

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrator Role	Support Level
N/A	Level-1
N/A	Level-2
Local Administrator on StoreFront Server	Level-3
Full Administrator	Level-4

Users with local administrator rights have access to view and manage all objects within StoreFront or Web Interface. These users can create new sites and modify existing ones.

Citrix License Server Delegated Rights

Administrator Role	Support Level
N/A	Level-1
N/A	Level-2
Administrator	Level-3
Administrator	Level-4

By default, the account used during the installation of the license server becomes the administrator for the console. Often the accounts used for the installation are not the intended accounts for the regular administration tasks. For the steps on how to change the default administrator, please reference CTX135841 - How to Change the Default Administrator for the Citrix Licensing Server Version 11.10. All users created through this process are full administrators of the Citrix License Server.

XenServer Delegated Rights

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administrator Role	Support Level
N/A	Level-1
Virtual Machine Operator	Level-2
Pool Administrator	Level-3
Full Administrator	Level-4

For further information about delegated rights within a XenServer Resource Pool, please refer to XenServer 7.0 Administrators Guide (see chapter Role Based Access Control).

Process 2: Operations

This section defines routine operations for the Citrix environment that help to improve stability and performance.

Decision: Administrative Tasks

The Citrix Support Team should perform regular operations and maintenance tasks to ensure a stable, scalable Citrix environment. Each operation is categorized by the associated component of the solution as well as the frequency of the operation (ongoing, daily, weekly and yearly). Tasks have been aligned to the roles described within Decision: Support Responsibilities and Skill Set.

If the administrators performing operations are the same the support team, then the designations are linked as follows:

- Level 2 Support = Operators
- Level 3 Support = Implementers

Daily Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a daily basis.

Component	Task	Description	Responsible
Generic	Review Citrix Director, Windows Performance Monitor, Event Log, and other monitoring software alerts	Check for warnings or alerts within Citrix Director, event logs, or other monitoring software. Investigate the root cause of the alert if any. **Note**: A computer and monitor can be set up to display the Citrix Director dashboard to create a Heads Up Display for the Citrix department. This ensures the status of the environment is clearly visible. Monitoring recommendations for XenDesktop and XenApp 7.x are included in the Monitoring section of the VDI Handbook.	Operators
		Verify all scheduled backups have been completed successfully.	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
		• User data (user profiles/home folders) • Application data	
Generic	Verify backups completed successfully	• Citrix databases • StoreFront configuration • Web Interface configuration • Provisioning Services vDisks (virtual desktops and application servers) • XenServer VM/Pool metadata (or equivalent for other hypervisors) • Dedicated virtual desktops • License files	Operators
Generic	Test environment access	Simulate a connection both internally and externally to ensure desktop and application resources are available before most users log on for the day. This should be tested throughout the day and may even be automated.	Operators
XenApp and XenDesktop	Virtual machine power checking	Verify that the appropriate number of idle desktops and application servers are powered on and registered with the Delivery Controllers to ensure availability for user workloads.	Operators
XenApp and XenDesktop	Perform incremental backup of Citrix related databases	Perform incremental-data backups of the following Citrix databases: • Site Database • Configuration Logging Database • Monitoring Database	Operators, Database team (if Citrix environment is using a shared SQL)
Provisioning Services	Check Citrix Provisioning Server utilization	Check the number of target devices connected to the Citrix Provisioning Servers and balance the load across servers, if required.	Operators
Provisioning Services	Perform incremental backup of Citrix PVS database	Incremental backup of Citrix Provisioning Server database hosted on SQL Server infrastructure.	Operators, Database team (if Citrix environment is using a shared SQL)

Weekly Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a weekly basis.

Component	Task	Description	Responsible
Generic	Review latest hotfixes and patches	Review, test, and deploy the latest Citrix hotfixes and ascertain whether the Delivery Controllers and Server-Based OS / Desktop-Based OS virtual machines require them. **Note**: Any required hotfixes should be tested using the recommended testing process prior to implementation in production.	Operators, Implementers (review process)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
Generic	Create Citrix environment status report	Create report on overall environment performance (server health, resource usage, user experience) and number of Citrix issues (close rate, open issues, and so on).	Operators
Generic	Review status report	Review Citrix status report to identify any trends or common issues.	Implementers, Architect
Generic	Maintain internal support knowledge base	Create knowledge base articles and issue resolution scripts to address Level-1 and Level-2 support requests. Review knowledge base articles and issue resolution scripts for accuracy, compliance, and feasibility.	Operators (Level-2 requests), Implementers (Level-3 requests, and review process)
XenApp and XenDesktop	Check Configuration Logging report	Confirm that Citrix site-wide changes implemented during the previous week were approved through change control.	Auditors
XenApp and XenDesktop	Perform full backup of Citrix related databases	Perform full-data backups of the following Citrix databases: • Site Database • Configuration Logging Database • Monitoring Database	Operators, Database team (if Citrix environment is using a shared SQL)
Provisioning Services	Check storage capacity (only prior to updating a vDisk)	Review storage utilization, used and free storage space, for vDisk store and each vDisk. **Note**: Lack of space within the vDisk repository will be an issue only when the vDisks are updated using versioning or when a vDisk is placed in private mode during an update procedure. Storage utilization within vDisk should also be investigated. For example, a 20GB vDisk may only have 200MB of free storage. If the vDisk itself is limited for storage, then it needs to be extended. Citrix does not support resizing of a VHD file. Refer to the Microsoft link Resize-VHD for information on resizing a VHD file.	Operators
Provisioning Services	Perform vDisk updates (as necessary)	Perform a full backup of the vDisk before implementing any updates. Update the master vDisk image files and apply the following: • Windows software updates and patches • Operating system and application changes • Anti-virus pattern and definitions updates **Note**: Updates should be tested using the recommended testing process prior to implementation in production.	Auditors
Provisioning Services	Check auditing reports	Review the Citrix Provisioning Services auditing Logs. **Note**: Provisioning Server auditing is off by default and can be enabled to record configuration actions on components within the Provisioning Services farm. To enable auditing refer to the Citrix production documentation article, Enabling Auditing Information.	Operators, Database team (if Citrix environment is using a shared SQL)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Task	Description	Responsible
Provisioning Services	Backup of Citrix PVS database	Backup of Citrix Provisioning Server database hosted on SQL Server infrastructure.	Citrix environment administrator (or shared SQL)

Monthly Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a monthly basis.

Component	Task	Description	Responsible
Generic	Perform capacity assessment	Perform capacity assessment of the Citrix environment to determine environment utilization and any scalability requirements. **Note**: Recommendations for performing a capacity assessment are included in Decision: Capacity Management in the Monitoring section below.	Architect

Yearly Periodic Tasks

The following table outlines the tasks that should be performed by the Citrix Support Team on a yearly basis.

Component	Task	Description	Responsible
Generic	Conduct Citrix policy assessment	Review Citrix policies and determine whether new policies are required and existing policies need to be updated.	Implementers
Generic	Review software upgrades	Review and assess the requirement for new Citrix software releases or versions.	Implementers
Generic	Business Continuity Plan (BCP)/ Disaster Recovery (DR) test	Conduct functional BCP/DR test to confirm DR readiness. This plan should include a yearly restore test to validate the actual restore process from backup data is functioning correctly.	Architect
Generic	Perform application assessment	Review the usage of applications outside and within the Citrix environment. Assess the validity of adding additional applications to the Citrix site, removing applications that are no longer required, or upgrading the applications to the latest version.	Architect
Provisioning Services	Archive audit reports	Perform an archive of the Citrix Provisioning Server Audit Trail Information for compliance requirements.	Auditors

Decision: Backup Location

The location of backups directly effects the recovery time and reliability of the Citrix environment. It is recommended to store backups of critical data both onsite and at an offsite location. If offsite backups are not possible due to costs

© 1999-2017 Citrix Systems, Inc. All rights reserved.

associated or sensitivity of the data, backups should be placed at separate physical locations within the same datacenter.

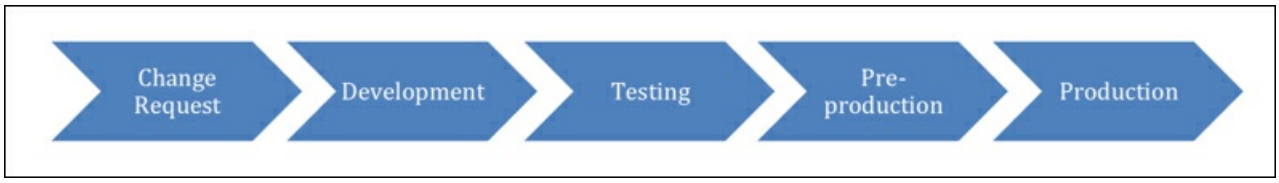
Each backup option is discussed further below.

- Onsite Backups – Onsite backups should be located on a storage device in the datacenter that will allow the data to be recovered quickly in the event of a failure. Onsite backups are ideal for issues that only affect a small subnet of hardware in the datacenter. Backups can also be stored on a cold storage solution such as tape. While this medium is slower to recover from, it provides additional protection since it is only active during the backup process.
- Offsite Backups – Although the time to recover is much higher, offsite backups provide additional protection in the event of a disaster. Offsite backups may require transferring data over the Internet to a third party provider or they are created onsite and then transported to a remote location on storage mediums such as tape. It is typical to put a limited number of backups offsite. For example, one backup a week or month.

Decision: Testing Process

Regular updates and maintenance are an everyday part of IT operations. Standard processes must be followed to ensure updates do not negatively impact the production environment. This includes maintaining a dedicated testing infrastructure where modifications can be validated prior to being implemented in production.

Since changes to Citrix infrastructure can impact thousands of virtual desktop and application users, multi-phase testing is critical for the reliability and performance of the environment. As such, the process for testing should resemble the following:



- Development - The development infrastructure exists outside of the production network. Typically, it consists of short-lived virtual machines whose configuration matches production as closely as possible. The purpose of the development phase is to provide change requestors a non-production environment to perform proof of concepts, determine integration requirements and perform iterative testing as part of a discovery phase. Proposed changes should be documented so they can be applied in the test phase.
- Testing - The test environment is a standalone 1:1 copy of the production infrastructure and is used to confirm that the proposed changes can be easily repeated prior to the preproduction staging environment. The changes made should follow documentation from the development stage. If testing fails within the testing stage, the architect must determine the severity of failure and determine whether minor updates to documentation is sufficient or a full development cycle is needed.
- Pre-production - The pre-production environment should mimic the current production environment. The goal of staging is to implement the proposed changes with little risk or uncertainty. It is expected that any changes made to the staging infrastructure have been tested and documented for repeatability. There should not be any iterations or adjustments required within this phase. During this phase and within this environment User Acceptance Testing (UAT) should be performed.
- Production - The production environment is a fully redundant and scalable solution designed for normal usage by end users. There should be minimal changes to the environment. If possible, all approved changes should be rolled out in stages to the production environment. This process is known as a staged rollout and mitigates risk by allowing changes to be rolled back, if necessary, without impacting the entire environment.

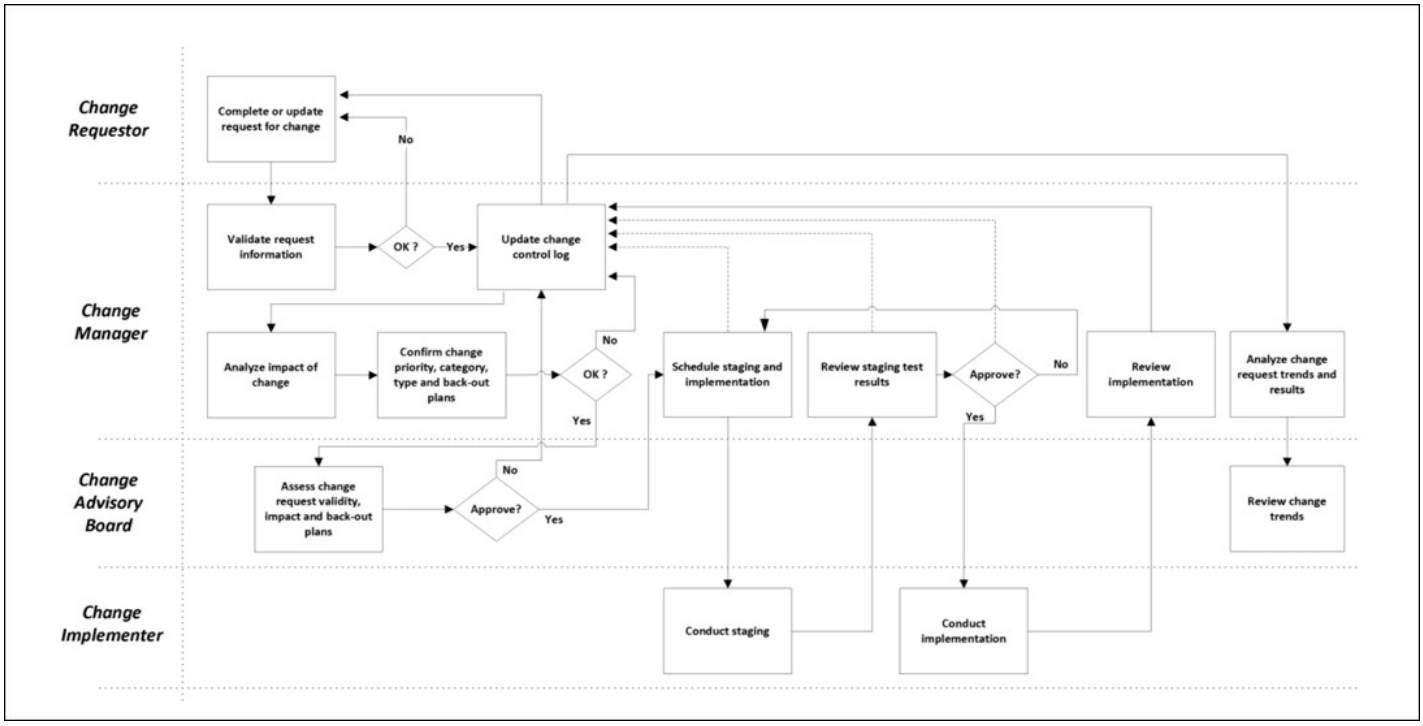
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Decision: Change Control

Standardized processes that manage changes throughout a system's lifecycle are necessary to ensure consistent and accountable performance. The following change control leading practices should be considered.

- Use a change control window so that all applicable parties know when there might be downtime. Make sure that all teams are represented in the Change Advisory Board (CAB).
- Every change should have a roll back plan.
- If a change fails have a "hot wash" to determine what went wrong.
- Always use an automated change control system so that support staff can quickly and easily identify changes.
- When available, ensure configuration logging is enabled to track any changes made to the Citrix environment.

The change control process should be closely followed starting with a change request. A change request form should be filled out detailing changes requested, reasons for the change, and intended timeframes for the action. This is then reviewed and edited if required by a Change Manager and advisory board. When the change request has gone through the entire change approval process it is given to a change implementer who stages the change for testing, and finally conducts the implementation in production. A sample change control process, including detailed steps, is provided in the diagram below:



The process is as follows:

1. The Change Request (CR) form is completed by any person requesting a change.

2. After appropriate manager approvals have been acquired, the CR is forwarded to the appropriate Change Manager(s).

3. The Change Manager validates the CR for completeness and logs the CR information into the Change Control Log for tracking. Incomplete change requests are returned to the requestor for update and re-submission.

4. The Change Manager assesses the impact of the change in conjunction with subject matter experts and/or managers of

© 1999-2017 Citrix Systems, Inc. All rights reserved.

the teams associated/affected by this change.

5. The Change Manager works with the associated/affected teams as well as the change requestor in order to confirm the priority, category and type of the change as well as the proposed rollback plan.

6. If the change is approved by the Change Manager, the CR is forwarded to the CAB for approval. If the change is rejected, the Change Control Log is updated with the current status as well as the reason of the rejection and the CR is send back to the requestor.

7. The CAB reviews and validates the change in detail, and discusses and evaluates purpose, reasons, impact, cost and benefits. Each board member represents their department and provides guidance on the change requests. The CAB also reviews multiple requests to coordinate implementations and "package" requests into a single release schedule.

8. Upon approval the change is sent back to the Change Manager to schedule the change for implementation into the staging environment.

9. The change is implemented and tests are conducted. The results are sent back to the Change Manager.

10. If the staging implementation and testing are successful, the change is scheduled for production implementation. In case the staging phase was not successful another staging iteration will be conducted.

11. If possible, the change is rolled out in stages to the production environment. This process is known as a staged rollout and mitigates risk by allowing changes to be rolled back, if necessary, without impacting the entire environment. A rollback plan should be in place if there is an issue implementing a change in the production environment.

12. The Change Manager reviews the implementation and finally updates the Change Control Log.

13. On a periodic basis, the Change Manager reviews the Change Control Log to identify trends on type, frequency and size of changes and forwards the results to the CAB for review. In an emergency, the processes may be expedited. Should an issue be declared an emergency, a change request form is still filled out and delivered to the appropriate change management representative. When approved, the requested change is immediately implemented and the advisory board notified.

Decision: Availability Testing

Availability testing is focused on ensuring resources are still available in the instance of a component failure. These tests are essential to ensuring users always have access to business critical resources. The testing should be conducted during nonbusiness hours or during a scheduled maintenance weekend when appropriate notice has been given to end users to make them aware if any unforeseen issues arise.

The following is a list of the key components that should be tested on a regular basis.

- StoreFront – StoreFront should be load balanced and health checked by a NetScaler or other load balancing device. To validate its configuration, all but one of the StoreFront servers should be shutdown. This will validate that the load balancing device is detecting the failure and directing users to the functioning server.
- SQL – SQL Server should be in a high availability configuration. To validate the configuration, the primary SQL server should be taken offline and then the Citrix Studio console should be opened. Since Citrix Studio will not be accessible without a functioning SQL server, it will validate that the SQL server failover mechanisms are functioning properly.
- Delivery Controllers - Resources deployed should be configured with a list of multiple Delivery Controllers. If one is made unavailable, desktops and application hosts will automatically establish a connection to another server in the list. To validate this, shutdown one of the Delivery Controller hosts and determine if the resources initially connected to it

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

automatically register to another server. This can be determined by viewing the registration status of the resources inside Citrix Studio.

Sample Testing Workflow: Citrix Provisioning Services

Prerequisites and configuration requirements:

- Hypervisor, XenApp, and XenDesktop services are up and running.
- At least two PVS servers are installed and configured, providing the streamed disk image.
- Resilient networking and storage infrastructure with multiple links to each server.
- Test users are active on the XenApp or XenDesktop machines.

Steps	Expected Results
PVS Server Outage • Shutdown one of the Provisioning Servers. • Validate PVS continues to function. • Restart PVS Server. • Validate connections rebalance between PVS Servers. • Try the other(rest) PVS server(s) one by one.	• Existing XenApp/XenDesktop machines connect to another PVS server. • There is limited to no impact to the users utilizing that server. • New XenApp/XenDesktop machines can be booted and start correctly. • SCOM reports that the PVS server is down/not available. • Live connections are rebalanced between both PVS servers once both PVS servers are made available again.
PVS Bond Disruption: Disable / unplug a NIC in the PVS Streaming Bond on the PVS server.	Provisioning Server continues to stream over remaining NICS in PVS Streaming Bond.
SQL Server PVS Database Mirror Failover • Admin logs on to Principle SQL Server. • Initiate failover of PVS database. • Validate PVS continues to function. • Initiate failback of PVS database. • Validate PVS continues to function.	PVS continues to function.
SQL Service Outage • Admin reboots both Principle & Mirror SQL Servers simultaneously. • Validate PVS continues to function, but that administration is not possible. • Wait for the SQL Server to come back online. • Validate PVS administrative functions are once again possible.	• PVS continues to function. • PVS administrative functions are no longer available. • PVS administrative functions are available once the SQL services are restored.

Sample Testing Workflow: Citrix XenDesktop and XenApp Services

Prerequisites and configuration requirements:

- Hypervisor, XenDesktop, and StoreFront services are up and running.
- Network and storage services available.
- Provisioning Services is providing the streamed disk images.
- Test users are active on the virtual machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- SQL (Mirroring) and XenDesktop servers are up and running.
- Ensure multiple StoreFront servers are running.
- NetScaler load balancing services.

Steps	Expected Results
XenApp/XenDesktop 7.x Delivery Controller Citrix Broker Service Outage: • Stop the Citrix Broker Service on one of the Delivery Controller servers. • Validate virtual desktops or applications can still be enumerated and launched. • Start the Citrix Broker Service on the Delivery Controller server. • Shutdown one of the Desktop Controllers. • Validate virtual desktops or applications can still be enumerated and launched. • With a desktop launched, determine which Controller owns the host connection. Shut the Controller down and verify that another Controller takes over the session. **Note**: This should be done during the maintenance window. Once complete, the VDI resources should be rebooted so the VDAs are evenly distributed across all controllers.	• StoreFront correctly identifies service as being unavailable and redirects connections to remaining Delivery Controller. • Desktops continue to be enumerated and launch successfully. • Launched desktop can be supported if a hosting Controller goes down.
SQL Server Database Mirror Failover: • Admin logs on to principle SQL Server. • Initiate failover of XenApp/XenDesktop database. • Validate XenApp/XenDesktop continues to function.	• The database should failover and the Citrix Studio should pick up the failover database with no issues. • Existing sessions are not impacted. • New sessions are possible. • Administrative functions are possible.
SQL Service Outage: • Admin restarts both principle & mirror SQL Servers simultaneously. • Validate XenApp/XenDesktop continues to function, but that administration is not possible. Wait for the SQL Service to come back online. • Validate administrative functions are once again possible.	• Existing XenDesktop sessions are not impacted • Recently used applications, hosted shared desktops and assigned VDI can be accessed due to local host cache. • XenDesktop Administrative functions are not possible • XenDesktop Administrative functions are possible once SQL service is available.

Sample Testing Workflow: Citrix Licensing Services

Prerequisites and configuration requirements:

- Citrix Licensing Server up and running (with valid licenses installed).
- Hypervisor, XenApp/XenDesktop and StoreFront services are up and running.
- Users are active on the Server OS or Desktop OS machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Steps	Expected Results
Server: • Shutdown the Citrix Licensing server. • Reboot an existing Server OS machine. • Logon to the Citrix StoreFront and launch a published application. • Reboot an existing Desktop OS machine. • Logon to the Citrix StoreFront and launch a virtual desktop.	• License Server connectivity error posted in Event Log. • Provisioned Server OS boots successfully. • Users are able to launch published applications. • Provisioned Desktop OS boots successfully. • User is able to launch a virtual desktop. • Administrators will have 30 days grace to recover the Citrix Licensing Server.

Process 3: Monitoring

By having an in-depth understanding of current and expected behavior of the Citrix environment and its components, administrators are better equipped to discover an issue before it affects the user community. Furthermore, the data tracked during normal operations is beneficial for trending and capacity planning. This section defines the monitoring recommendations for a Citrix environment as well as some recommended tools.

Decision: Automated Monitoring

Depending on the size and scope of the XenApp and XenDesktop solution, it can take considerable time for an administrator to verify services, events, capacity and performance. It is advisable for administrators to investigate automation into their monitoring strategy.

Citrix includes a cloud-hosted monitoring solution called Smart Check (https://smart.cloud.com), which is a free service for any organization with active Citrix Customer Success Services: Select offering. Smart Check executes the following in a XenApp and XenDesktop environment:

- Site Health Checks – Evaluates all services with the XenApp and XenDesktop site
- Apps and Desktops Checks = Verifies delivery group availability
- Update Checks – Tracks and recommends patches and hotfixes for delivery controllers
- LTSR Checks – Verifies the delivery controllers and VDAs within the site comply with LTSR versions.
- Custom Checks – Allows administrators to import their own custom scripts to test across their XenApp and XenDesktop site.

A list of the current Smart Check capabilities, review the Smart Check documentation.

Decision: Performance Monitor Metrics

Monitoring the performance of the overall environment is crucial towards making sure all components are available and performing effectively to ensure users have a high quality experience.

Different components within the overall solution require monitoring of unique metrics with appropriately set thresholds. The metrics and thresholds presented are based on real world experience but may not apply to all environments. Organizations will need to perform their own baselining, validity testing and validation before implementing within a production environment.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota

Some hypervisors, such as VMware vSphere and Hyper-V, provide specific performance counters for tracking CPU and Memory utilization within virtual machines (i.e. “VM Processor \ % Processor Time”). These performance counters should be used in addition to the general counters listed below.

General

These performance counters should be used to monitor the key performance metrics of the Citrix infrastructure, application servers, and virtual desktops.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Processor - % Processor Time	% Processor Time is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the duration of the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.	80% for 15 minutes	95% for 15 minutes	Identify the processes/services consuming processor time using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of CPU consumption is an expected behavior it should be considered to add additional CPU resources to this system in the future. If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
System - Processor Queue Length	Processor queue length is the number of threads in the processor queue. Unlike the disk counters, this counter shows ready threads only, not threads that are running. There is a single queue for processor time even on computers with multiple processors. Therefore, if a computer has multiple processors, you need to divide this value by the number of processors servicing the workload. A sustained processor queue of less than ten threads per processor is normally acceptable, dependent of the workload.	5 (per core) for 5 minutes or 6 (per core) for 15 minutes	10 (per Core) for 10 minutes or 12 (per core) for 30 minutes	A long CPU queue is a clear symptom of a CPU bottleneck. Please follow the steps outlined for counter “Processor - % Processor Time”.
				Identify the processes/services consuming memory using Task

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Memory – Available Bytes	Available memory indicates the amount of memory that is left after nonpaged pool allocations, paged pool allocations, process' working sets, and the file system cache have all taken their piece.	<30% of total RAM or 20% of physical memory over 6 minutes	<15% of total RAM or 5% of physical memory over 6 minutes	all processes/services work within normal parameters and the level of memory consumption is an expected behavior it should be considered to add additional memory to this system in the future. If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
Memory – Pages/sec	Pages/sec is the rate at which pages are read from or written to disk to resolve hard page faults.	>10	>20	A high value reported for this counter typically indicates a memory bottleneck, except if "Memory – Available Bytes" reports a high value at the same time. In this case most likely an application is sequentially reading a file from memory. Please refer to Microsoft Knowledge Base article KB139609 – High Number of Pages/Sec Not Necessarily Low Memory for further information.
Paging File - %Usage	This is the percentage amount of the Page File instance in use.	>40% or 80% over 60 minutes	>70% or 95% over 60 minutes	Review this value in conjunction with "Memory - Available Bytes" and "Memory - Pages/sec" to understand paging activity on the affected system.
LogicalDisk/PhysicalDisk - % Free Space	% Free Space is the percentage of total usable space on the selected logical disk drive that is free.	<20% of physical disk or 20% reported after 2 minutes	<10% of physical disk or 15% reported after 1 minute	Identify which files or folders consume disk space and delete obsolete files if possible. In case no files can be deleted, consider increasing the size of the affected partition or add additional disks.
LogicalDisk/PhysicalDisk - % Disk Time	% Disk Time marks how busy the disk is.	>70% consistently or 90% over 15 minutes (_Total)	>90% consistently or 95% over 15 minutes (_Total)	Identify the processes / services consuming disk time using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of disk consumption is an expected behavior it should be considered to move the affected partition to a more capable disk subsystem in the future. If a process/service can be

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
				normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.
LogicalDisk/PhysicalDisk – Current Disk Queue Length	Current disk queue length provides a primary measure of disk congestion. It is an indication of the number of transactions that are waiting to be processed.	>=1 (per spindle) consistently or 3 over 15 minutes (_Total)	>=2 (per spindle) consistently or 10 over 30 minutes (_Total)	A long disk queue length typically indicated a disk performance bottleneck. This can be caused by either processes/services causing a high number of I/Os or a shortage of physical memory. Please follow the steps outlined for counter "LogicalDisk/PhysicalDisk - % Disk Time" and counter "Memory – Available Bytes"
LogicalDisk/PhysicalDisk – Avg. Disk Sec/Read – Avg. Disk Sec/Write – Avg. Disk Sec/Transfer	The Average Disk Second counters show the average time in seconds of a read/write/transfer from or to a disk.	>=15ms consistently	>=20ms consistently	High disk read or write latency indicates a disk performance bottleneck. Systems affected will become slow, unresponsive and application or services may fail. Please follow the steps outlined for counter "LogicalDisk/PhysicalDisk - % Disk Time"
Network Interface – Bytes Total/sec	Bytes Total/sec shows the rate at which the network adaptor is processing data bytes. This counter includes all application and file data, in addition to protocol information, such as packet headers.	<8MB/sfor 100 Mbit/s adaptor <80 MB/s for 1000 Mbit/s adaptor or 60% of NIC speed inbound and outbound traffic for 1 min.	70% of NIC speed inbound and outbound traffic for 1 min.	Identify the processes / services consuming network using Task Manager or Resource Monitor. If all processes/services work within normal parameters and the level of bandwidth consumption is an expected behavior it should be considered to move the respective process/service to a dedicated NIC (or team of NICs). If a process/service can be identified which works outside normal parameters, the process should be killed. Please note that killing a process can cause unsaved data to be lost.

XenApp/XenDesktop

These performance counters are specific to the Delivery Controllers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Database Avg. Transaction Time	The time on average, in seconds, taken to execute a database transaction. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values	In case the reported values exceed the baseline response time constantly, a potential performance issue needs to be investigated at the SQL server level.
Database Connected	Indicates whether this service is in contact with its database. (1 is connected; 0 is not connected).	0	0 (for over 30 minutes)	Both values report connectivity issues of the XenDesktop Broker service with the database. In case issues are reported, SQL server and network availability needs to be verified.
Database Transaction Errors/sec	The rate at which database transactions are failing.	None	> 0	Both values report connectivity issues of the XenDesktop Broker service with the database. In case issues are reported, SQL server and network availability needs to be verified.

StoreFront

These performance counters are specific to the StoreFront servers.

Metric	Description	Warning (Yellow)	Critical (Red)
ASP.NET – Request Queued	The number of requests waiting to be processed by ASP. A baseline needs to be established in the environment in order to accurately establish threshold values.	Based on baseline values	Based on baseline values
ASP.NET – Requests Rejected	The number of requests rejected because the request queue was full.	None	> = 1
APP_POOL_WAS\Current Application Pool State\Citrix Receiver for Web	3		
APP_POOL_WAS\Current Application Pool State\Citrix Delivery Services Authentication	3		
APP_POOL_WAS\Cur rent Application Pool State\Citrix Delivery Services Resource	3		
Request response	Regardless it is authentication, enumerate or subscription) should be 3 to 5 seconds (http://www.perftestplus.com/resources/how_fast.pd f		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix License Server

These performance counters are specific to the Citrix License Server

Metric	Description	Warning (Yellow)	Critical (Red)	Troubleshooting/Remediation
Citrix Licensing – Last Recorded License Check-Out Response Time	Displays the last recorded license check-out response time in milliseconds.	>2000 ms	> 5000 ms	If the reported values exceed the 5000 ms response time, a potential performance issue needs to be investigated in the Citrix License Server.
Citrix Licensing – License Server Connection Failure	Displays the number of minutes that XenDesktop has been disconnected from the License Server.	> 1 minute	> 1440 minutes	Both values report connectivity issues with the License Server. In case issues are reported, License Server and network availability needs to be verified.

Decision: Services Monitoring

Windows services that are critical to basic server functionality should be automatically monitored to ensure that they are running properly. The following table provides a list of the common Windows services that should be monitored. When any of these services are restarted or stopped a warning (Yellow) or critical (Red) alert should be assigned respectively. The recommended recovery actions for the services listed below are as follows:

- First failure: Restart the Service
- Second Failure: Restart the Service
- Subsequent Failures: Put the server in maintenance mode and investigate the root cause

XenApp/XenDesktop

Service	Functionality	Administration Risk
Citrix AD Identity Service	Manages Active Directory computer accounts. Dependencies: WMI Service	Machine Creation Service relies on this service to create virtual machines. Administrators will be unable to create new or modify existing Machine Catalogs. Administrators will be unable to establish new connections to Citrix Studio.
Citrix Broker Service	Manages connections to virtual machines and applications.	If this service is stopped administrators will be unable to make changes to the environment or establish new connections to Citrix Studio. Any existing administrator connections to Citrix Studio can also be terminated. If this service is stopped existing user connections are not affected. No new connections can be established. Users logging into StoreFront will be unable to see any resources available for selection. Once the service is restarted users will need to re-login to StoreFront to establish connections.
Citrix Configuration Logging	Logs administrator activity and configuration changes	If this service is stopped XenApp/XenDesktop will be unable to communicate with the Configuration Logging Database. Administrators will be unable make changes to the

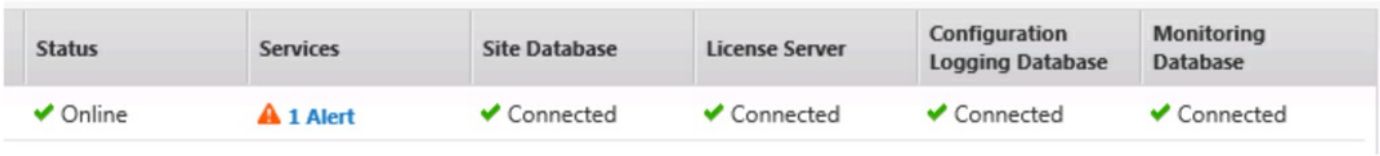
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Administration Risk
	deployment.	
Citrix Configuration Service	Stores service configuration information. Dependencies: WMI Service	If this service is stopped administrators will be unable to make changes to the environment or establish new connections to Citrix Studio.
Citrix Delegated Administration Service	Manages configuration of delegated administration permissions.	If this service is stopped XenApp/XenDesktop cannot assign administrative permissions. Administrators will be unable to make changes to the environment or establish new connections to Citrix Studio. Administrators will be unable to establish new connections to Citrix Director and existing sessions within Citrix Director will be interrupted.
Citrix Diagnostic Facility COM Server Service	Manages and controls Citrix diagnostic trace sessions on the system. Dependencies: RPC Service	This service has no impact on the production environment. It is used to generate CDF trace files which aid in troubleshooting issues.
Citrix Environment Test Service	Manages tests for evaluating the state of a XenDesktop Site.	If this service is stopped administrators will be unable to establish new connections to Citrix Studio. Administrators will also be unable to check the status of the Citrix site configuration, machine catalogs, and delivery groups by running the tests under "Common Tasks" in the Citrix Studio administration console.
Citrix Host Services	Manages host and hypervisor connections. Dependencies: WMI Service	Administrators will be unable to create new Machine Catalogs or control virtual machine power settings via Citrix Studio. Administrators will be unable to establish new connections to Citrix Studio. Users may experience issues connecting to virtual desktops when this service is not available. If this service is stopped existing connections are not affected.
Citrix Machine Creation Service	Creates new virtual machines. Dependencies: WMI Service	Administrators will be unable to create new or modify existing Machine Catalogs or establish new connections to Citrix Studio. Administrators will be unable to establish new connections to Citrix Studio.
Citrix Monitor Service	Monitors the FlexCast system.	If this service is stopped XenApp/XenDesktop will be unable to communicate with the Monitoring Database. Citrix Director will be unable to retrieve any data on the environment. Administrators will be unable to establish new connections to Citrix Studio.
Citrix StoreFront Service	Manages deployment of StoreFront.	Administrators will be unable to establish new connections to Citrix Studio.

Delivery Controller Services Monitoring in Citrix Director

The Infrastructure pane within the Citrix Director dashboard provides status of the services running on the Delivery Controllers and will provide warning indications if a service or Controller is unavailable. These alerts can be accessed by clicking the Alert hyperlink within the Infrastructure pane.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Status	Services	Site Database	License Server	Configuration Logging Database	Monitoring Database
✔ Online	⚠ 1 Alert	✔ Connected	✔ Connected	✔ Connected	✔ Connected

Provisioning Services

Service	Functionality	Risk
Citrix PVS PXE Service	Provides the PVS PXE Boot Server functionality. **Note**: Only applicable when PXE boot is used.	On failure of this service target devices may not be able to boot successfully if PXE booting is leveraged.
Citrix PVS Stream Service	Streams contents of the vDisk to the target device on demand.	If this service stopped it will not be possible to stream vDisk images.
Citrix PVS SOAP Service	Provides framework for external or existing solutions to interface with Provisioning services. **Note**: Only impacts console operations. User is unaffected	If this service fails PVS Server to PVS Server communication as well as PVS Console to PVS Server communication is not possible.
Citrix PVS TFTP Service	Provides the TFTP Server functionality. **Note**: Only applicable when TFTP is used.	On failure of this service target devices may not be able to boot if this server is used as TFTP server for the bootstrap.
Citrix PVS Two-Stage Boot Service	Provides the bootstrap functionality for devices booting by means of a BDM ISO file. **Note**: Only when BDM boot partitions are used.	On failure of this service target devices may not be able to boot if a BDM ISO file is used.

StoreFront

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Risk
Citrix Cluster Join Service	Provides Server Group join services.	This service is started when adding additional StoreFront servers to a Server Group. If this service does not start or is interrupted when this process is initiated the additional server will be unable to join the indicated Server Group and the process will result in an error.
Citrix Configuration Replication	Provides access to Delivery Services configuration information.	This service only exists on the primary StoreFront server of a Server Group. If this service is stopped additional StoreFront servers will be unable to join the Server Group and any changes made to the primary StoreFront server will not be replicated to other servers. This can result in servers within the Server Group being out of sync.
Citrix Credential Wallet	Provides a secure store of credentials. Dependencies: Citrix Peer Resolution Service	If this service is stopped users will be unable to login to access their desktops or applications. Users logged into StoreFront will be unable to launch new application or desktop sessions. Existing application or desktop sessions are unaffected.
Citrix Default Domain Services	Provides authentication, change password, and other domain services.	If this service is stopped users will be unable to login to access their desktops or applications. Users currently logged in will not be affected.
Citrix Peer Resolution Service	Resolves peer names within peer-to-peer meshes.	On failure of this service both the Citrix Credential Wallet and Citrix Subscriptions store are stopped generating the risks associated with those services.
Citrix Storefront Privileged Administration Service	Manages privileged operations on Storefront	
Citrix Subscriptions Store	Provides a store and replication of user subscriptions. Dependencies: Citrix Peer Resolution Service	If this service is stopped Citrix Receiver cannot add, remove, and reposition applications within StoreFront. Users will need to re-add applications and all changes made to their selection of applications within the StoreFront store will not be saved or replicated to other sessions. Original user configuration will be restored once the service is restarted.
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. Dependencies: • HTTP • RPC Service	Access to published applications or published desktops will not be available through StoreFront. Users will be unable to resolve the Receiver for Web login page. Users logged into StoreFront will be unable to launch new application or desktop sessions and will need to reenter credentials when the service is restarted. Existing application or desktop sessions are unaffected.

Web Interface

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Service	Functionality	Risk
World Wide Web Publishing Service	Provides web connectivity and administration through the Internet Information Services Manager. Dependencies: • HTTP • RPC Service	Access to published applications or published desktops will not be available through Web Interface if the WWW service is not available.

Citrix License Server

Service	Functionality	Risk
Citrix Licensing Service	Provides licensing services for Citrix products.	Licensing mode changes to grace period when service is stopped or License Server cannot be contacted. If not monitored, functionality of Citrix products will cease after grace period expires.
Citrix Licensing Support Service	This account controls reading the license files and updating strings with license trailers (data dictionary functionality).	None
Citrix Licensing WMI	The Citrix License Management Console collects license data information using the WMI service.	None

Decision: Events Monitoring

Monitoring the Windows Event Log for unknown or critical events can help to proactively discover issues and allow administrators to understand event patterns:

- Licensing - Errors in the Event Log dealing with Remote Desktop licensing should be investigated. This might be a result of the installed Citrix product not being able to contact the Remote Desktop Licensing Server or the Citrix Licensing Server. If errors in the Event Log are not reviewed, users might eventually be denied access because they cannot acquire a valid license.
- Hardware Failure - Any event notification that relates to a hardware failure should be looked at immediately. Any device that has failed will have an impact on the performance of the system. At a minimum, a hardware failure will remove the redundancy of the component.
- Security Warnings - Customers should investigate security warnings or audit failure events regarding failed logons in the security log. This could be an indication that someone is attempting to compromise the servers.
- Disk Capacity - As the drives of a Windows system reach 90% of capacity, an event error message will be generated. To ensure continuous service, customers should poll these event errors. As the system runs out of hard disk space, the system is put at severe risk. The server might not have enough space left to service the requests of users for temporary file storage.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Application / Service errors - Any event notification that relates to application or services errors should be investigated.
- Citrix errors - All Citrix software components will leverage the Windows Event Log for error logging. A list of the known Event Log warnings and errors issued by Citrix components can be found at the following links:
  - Event Codes Generated by PVS
  - XenDesktop 7 - Event Log Messages

It is important to periodically check the Event Viewer for Citrix related warnings or errors. Warnings or errors that repeatedly appear in the logs should be investigated immediately, because it may indicate a problem that could severely impact the Citrix environment if not properly resolved.

In multi-server environments it becomes easier to administer the servers when logs can be collected and reviewed from a central location. Most enterprise grade monitoring solutions provide this functionality. More sophisticated monitoring solutions enable an administrator to correlate event information with other data points such as performance metrics or availability statistics. In case the selected monitoring solution does not provide this functionality the Windows Server 2008 R2 or Windows Server 2012/2012 R2 Event Log subscription feature can be used. This feature allows administrators to receive events from multiple servers and view them from a designated collector computer. Please see Microsoft TechNet article Manage Subscriptions for more information.

XenServer is also capable of sending its logs to a central syslog server. The administrator sets the IP address of the syslog daemon server in the properties of each XenServer in the pool. This configuration allows administrators to capture real-time activity across multiple XenServer hosts. Further information can be found within the XenServer Admin Guide.
Decision: Capacity Management

In addition to the day-to-day monitoring of system-level metrics, performance metrics should be tracked from a historical perspective to help plan for future growth as more users access the environment.

A baseline of the environment performance should be taken so that it can be compared against performance over time. For example, if a user complains of poor performance, this baseline can be used for comparison purposes to identify if the issues are related to the user load exceeding the capacity of the environment.

An example of baseline performance metrics for capacity management would include historical data for CPU, Memory, and network utilization on the Delivery Controller and application servers or desktops.

Citrix Director

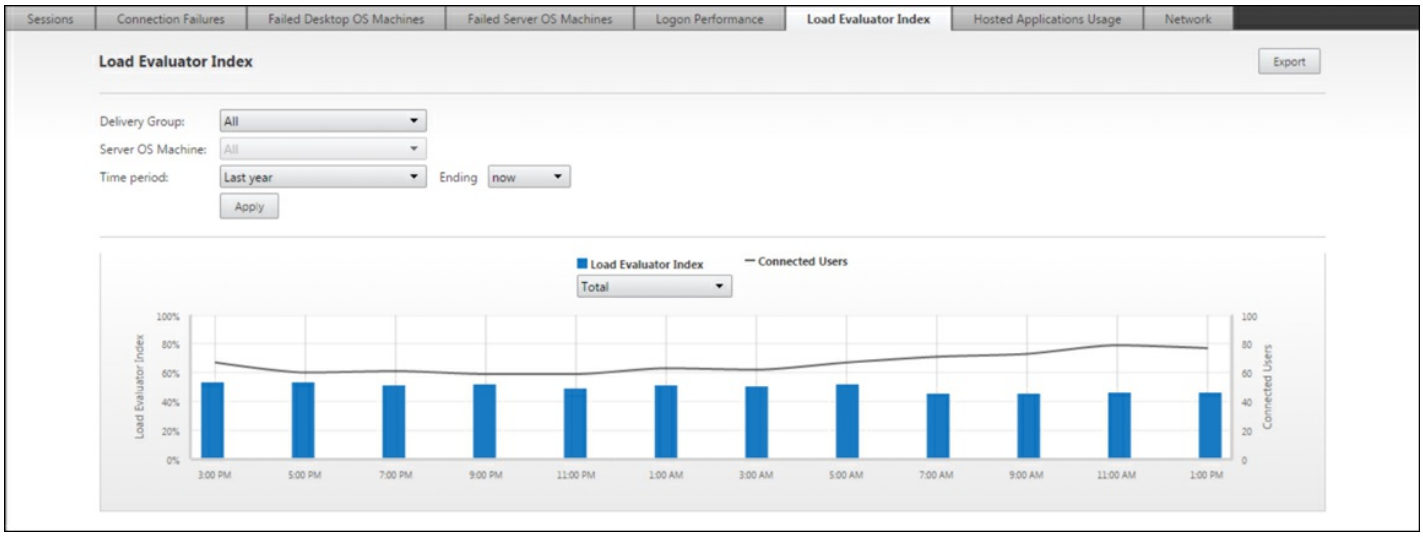
Administrators can utilize the Trends view within Citrix Director to track different parameters of the Citrix XenApp/XenDesktop deployment over time. These parameters can be leveraged for capacity planning of the Citrix environment.

From the Trends view, administrators can see historical data that is broken up into several categories including:

- **Sessions** - Provides the concurrent session usage over time enabling the ability to size the environment appropriately.
- **Connection Failures** - Gives an overview of the different types of connection failures that have occurred across different Delivery Groups.
- **Failed Desktop OS Machines** – Gives an overview of the different problems associated with failures in desktop machines.
- **Failed Server OS Machines** - Gives an overview of the different problems associated with failures in server machines.
- **Logon Performance** – Shows how long it takes for users to log on to their applications and desktops.
- **Load Evaluator Index** – Provides various performance counter-based metrics, including CPU, Memory, and Disk Usage for Server OS machines.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Capacity Management** – Shows utilization of published applications and desktops.
- **Resource Utilization** – Provides information on CPU, Memory and storage resource utilization.
- **Custom Reports** – Allows administrators to create custom historical reports on numerous metrics captured by the system.
- **Hosted Application Usage** – Details all applications published in the site and can provide usage information about each individual applications in detail (concurrent instances, launches, usage duration, and so on). **Note**: Requires XenApp or XenDesktop Platinum licensing
- **Network** – Network analytics provided through NetScaler HDX Insight.



For more information on Citrix Director Trends, please refer to the following.

- Citrix Blogs – Citrix Director: Trends Explained
- Citrix Support – CTX139382 - Best Practices for Citrix Director

The creation of the handbook is a time consuming process and requires real deployment experience across many scenarios. Citrix would like to thank the authors and subject matter experts who contributed to the Citrix VDI Handbook.

© 1999-2017 Citrix Systems, Inc. All rights reserved.