Citrix DaaS para Azure

Machine translated content

Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

Contents

Citrix DaaS Standard para Azure

September 7, 2022

Introducción

Citrix DaaS Standard para Azure (anteriormente Citrix Virtual Apps and Desktops Standard para Azure) es la forma más sencilla y rápida de entregar aplicaciones y escritorios Windows desde Microsoft Azure. Citrix DaaS para Azure ofrece administración, aprovisionamiento y capacidad administrada basados en la nube para entregar aplicaciones y escritorios virtuales a cualquier dispositivo.

Esta solución incluye:

- Administración y aprovisionamiento basados en la nube para entregar escritorios virtuales de Azure alojados en Citrix y aplicaciones desde máquinas multisesión.
- Una experiencia de usuario de alta definición desde una amplia gama de dispositivos, mediante la aplicación Citrix Workspace.
- Flujos de trabajo de creación y administración de imágenes simplificados, junto con imágenes de sesión única y multisesión preparadas por Citrix para Windows y Linux que tienen instalado la última versión de Citrix Virtual Delivery Agent (VDA).
- Acceso remoto seguro desde cualquier dispositivo mediante puntos de presencia globales del Citrix Gateway Service Gateway.
- Capacidades avanzadas de supervisión y administración de mesa de ayuda.
- IaaS de Azure administrado, que incluye procesamiento, almacenamiento y redes de Azure para entregar escritorios virtuales.

La función Citrix Remote PC Access permite a los usuarios utilizar de forma remota las máquinas físicas existentes ubicadas en la oficina. Los usuarios disfrutan de la mejor experiencia posible al utilizar Citrix HDX para la entrega de sesiones de PC de oficina.

Si está familiarizado con otros productos de Citrix DaaS, Citrix DaaS para Azure simplifica la implementación de aplicaciones y escritorios virtuales. Citrix puede administrar la infraestructura para alojar esas cargas de trabajo.

Citrix DaaS para Azure es un servicio de Citrix Cloud. Citrix Cloud es la plataforma que aloja y administra los servicios de Citrix Cloud. Obtenga más información sobre Citrix Cloud.

Para obtener información sobre los componentes, el flujo de datos y las consideraciones de seguridad, consulte Descripción general de la seguridad técnica. En ese artículo también se describen las responsabilidades del cliente y de Citrix.

Cómo acceden los usuarios a los escritorios y las aplicaciones

Los usuarios (a veces denominados suscriptores) acceden a sus escritorios y aplicaciones directamente a través de su explorador, mediante el cliente HTML5 de Citrix. Los usuarios navegan hasta una URL de Citrix Workspace que usted, su administrador, proporciona. La plataforma Citrix Workspace enumera y entrega los recursos digitales a los usuarios. Los usuarios inician un escritorio o una aplicación desde su espacio de trabajo.

Después de configurar un catálogo de máquinas que entregan escritorios y aplicaciones (o un catálogo que contiene máquinas físicas para el acceso con Remote PC), Citrix DaaS para Azure muestra la URL del espacio de trabajo. A continuación, notifica a los usuarios que vayan a esa URL para iniciar su escritorio y sus aplicaciones.

Como alternativa a navegar a Citrix Workspace para acceder a sus escritorios y aplicaciones, los usuarios pueden instalar una aplicación Citrix Workspace en su dispositivo. Descargue la aplicación adecuada para el sistema operativo del dispositivo de punto final: https://www.citrix.com/downloads/workspace-app/.

Conceptos y terminología

En esta sección se presentan algunos de los elementos y términos que los administradores usan en Citrix DaaS para Azure:

- Catálogos
- Ubicaciones de recursos
- Imágenes
- Suscripciones de Azure
- Conexiones de red
- Unidas a un dominio y no unidas a un dominio

Catálogos

Un catálogo es un grupo de máquinas.

- Los escritorios y las aplicaciones que Citrix DaaS para Azure ofrece a los usuarios residen en máquinas virtuales (VM). Esas máquinas virtuales se crean (aprovisionan) en el catálogo.

  Cuando implementa escritorios, las máquinas del catálogo se comparten con los usuarios seleccionados. Al publicar aplicaciones, las máquinas multisesión alojan aplicaciones que se comparten con los usuarios seleccionados.

- Para el acceso con Remote PC, un catálogo contiene máquinas físicas de sesión única existentes. Una implementación común incluye máquinas ubicadas en su oficina. Controla el acceso de

los usuarios a esas máquinas mediante el método de asignación de usuarios configurado y los usuarios seleccionados.

Si está familiarizado con otros productos de Citrix DaaS, un catálogo en Citrix DaaS es similar a combinar un catálogo de máquinas y un grupo de entrega.

Para obtener más información, consulte:

- Cree catálogos para escritorios y aplicaciones publicados.
- Cree catálogos para acceso con Remote PC.
- Administre catálogos.
- Usuarios y autenticación.

Ubicaciones de recursos

Las máquinas de un catálogo residen en una ubicación de recursos. Una ubicación de recursos también contiene dos o más Cloud Connectors.

- Al publicar escritorios o aplicaciones, Citrix crea automáticamente la ubicación de recursos y Cloud Connectors al crear el primer catálogo.
- Para el acceso con Remote PC, el administrador crea la ubicación de recursos y los Cloud Connectors antes de crear un catálogo.

Cuando crea más catálogos para escritorios y aplicaciones publicados, la suscripción, la región y el dominio de Azure determinan si Citrix crea otra ubicación de recursos. Si esos criterios coinciden con un catálogo existente, Citrix intenta reutilizar esa ubicación de recursos.

Para obtener más información, consulte:

- Especifique la información de la ubicación de los recursos cuando cree un catálogo.
- Acciones de ubicación de recursos.

Imágenes

Al crear un catálogo para escritorios y aplicaciones publicados, se utiliza una imagen de máquina (con otras configuraciones) como plantilla para crear las máquinas.

- Citrix DaaS para Azure proporciona varias imágenes preparadas por Citrix:
  - Windows 10 Enterprise (sesión única)
  - Windows 10 Enterprise Virtual Desktop (multisesión)
  - Windows 10 Enterprise Virtual Desktop (multisesión) con Office 365 ProPlus
  - Windows Server 2012 R2
  - Windows Server 2016

  - Windows Server 2019
  - Linux

  Cada imagen preparada por Citrix tiene un VDA de Citrix y herramientas de solución de problemas instaladas. El VDA es el mecanismo de comunicación entre las máquinas de los usuarios y la infraestructura de Citrix Cloud que administra Citrix DaaS para Azure.

  Citrix actualiza las imágenes preparadas disponibles cuando se publica una nueva versión del VDA.

- También puede importar y usar sus propias imágenes de Azure. Debe instalar un VDA (y otro software) en la imagen antes de poder utilizarlo para crear un catálogo.

El términoVDA a menudo se refiere al equipo que entrega aplicaciones o escritorios, y al componente de software instalado en ese equipo.

Para obtener más información, consulte Imágenes.

Suscripciones de Azure

Puede crear catálogos para entregar escritorios y aplicaciones, y crear e importar imágenes en una suscripción de Azure administrada por Citrix o en su propia suscripción de Azure (administrada por el cliente).

Si solo solicita Citrix DaaS para Azure, debe importar (agregar) y usar sus propias suscripciones de Azure. Si también solicita un fondo de consumo de Citrix Azure, recibirá una suscripción a Citrix Managed Azure. A continuación, puede utilizar una suscripción de Azure administrada por Citrix o una de sus suscripciones de Azure importadas al crear un catálogo o crear una nueva imagen.

Para obtener más información, consulte:

- Los escenarios de implementación ilustran formas de usar las suscripciones de Azure con Citrix DaaS para Azure.
- Las suscripciones de Azure explican las diferencias entre las suscripciones de Azure administradas por Citrix y las suscripciones de Azure administradas por el cliente. En este artículo también se describe cómo ver, agregar y eliminar suscripciones.
- Ladescripción general de la seguridad técnica describe las diferencias de responsabilidad con las suscripciones de Azure administradas por Citrix y Azure administradas por el cliente.

Conexiones de red

Al crear un catálogo mediante una suscripción a Azure administrado por Citrix, indica si los usuarios pueden acceder a las ubicaciones y los recursos de su red local corporativa desde sus escritorios y

aplicaciones publicados y de qué manera pueden acceder a las ubicaciones y los recursos de su red corporativa en las instalaciones. Las opciones son no conectividad, interconexión de Azure VNet y Citrix SD-WAN.

Al usar su propia suscripción de Azure, no es necesario crear una conexión. Solo necesita importar (agregar) su suscripción de Azure al servicio.

Para obtener más información, consulte Conexiones de red.

Unidas a un dominio y no unidas a un dominio

Varias operaciones y funciones de servicio difieren en función de si las máquinas (VDA) están unidas a un dominio o no están unidas a un dominio. La pertenencia al dominio también afecta a los casos de implementación disponibles.

- Tanto las máquinas unidas a un dominio como las no unidas a un dominio admiten cualquiera de los métodos de autenticación de usuario disponibles en el espacio de trabajo del usuario.
- Puede publicar escritorios, aplicaciones o ambos desde máquinas unidas a un dominio y no unidas a un dominio. Las máquinas de los catálogos de acceso con Remote PC deben estar unidas a un dominio.

En la siguiente tabla se enumeran varias diferencias entre las máquinas que no están unidas a un dominio y las máquinas unidas a un dominio al entregar escritorios y aplicaciones.

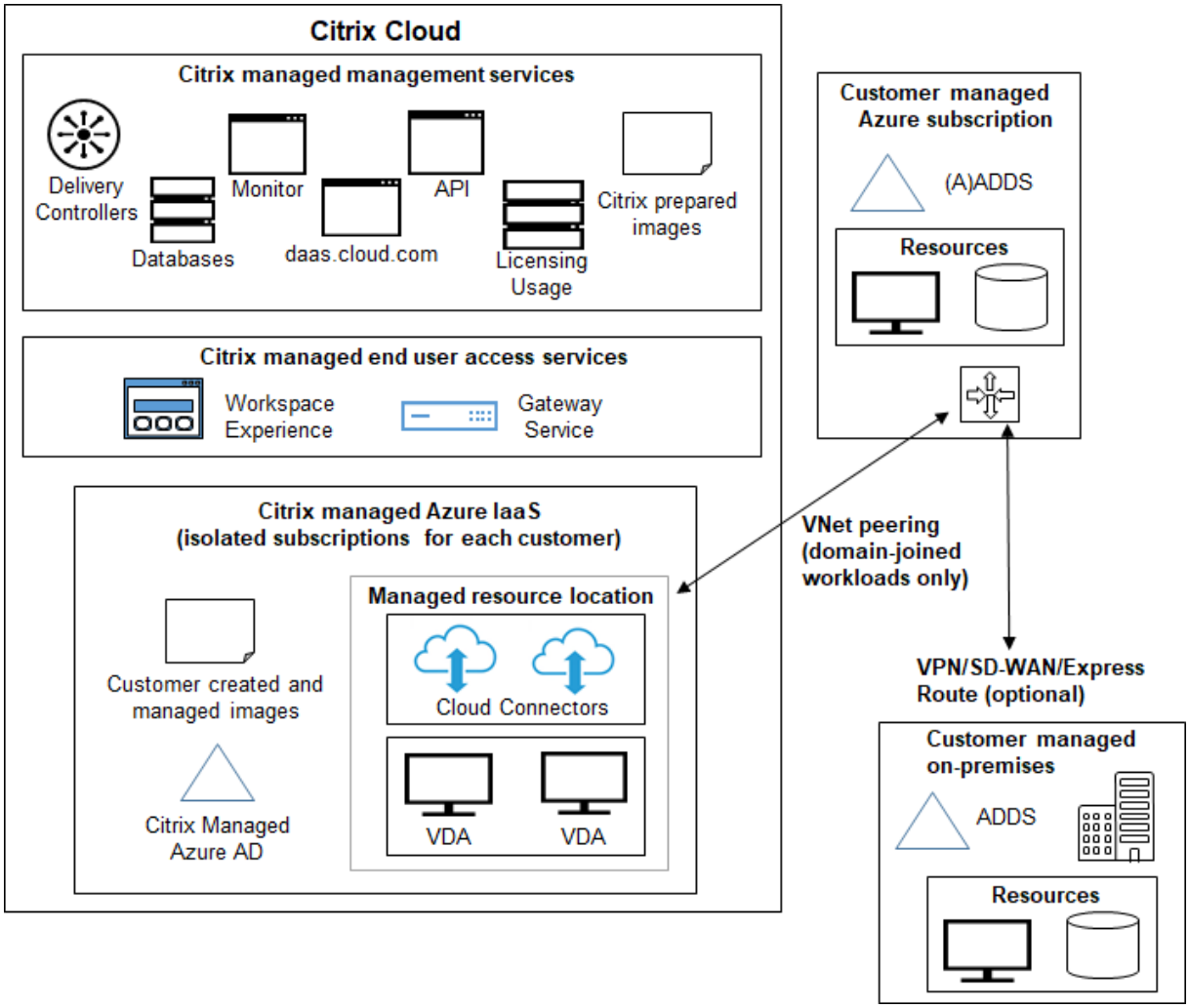
No unido a ningún dominio	Unidas a un dominio
Active Directory no se usa para máquinas. Las máquinas no están unidas a un dominio de AD.	Active Directory se usa para máquinas. Las máquinas se unen a un dominio de AD.
Las directivas de grupo de Active Directory no se pueden aplicar a las máquinas (VDA). (Puede aplicar el GPO local en la imagen que se utiliza para crear un catálogo).	Los VDA heredan directivas de grupo para la unidad organizativa de AD especificada durante la creación del catálogo.
Los usuarios inician sesión con el inicio de sesión único.	Cuando los usuarios inician sesión en su espacio de trabajo con un método de autenticación que no sea Active Directory, también se les pide que inicien sesión cuando se inicia un escritorio o una aplicación.
No necesita conexión a una red local.	(Cuando se usa una suscripción de Azure administrada por Citrix) Debe tener una conexión para acceder a una red local, mediante Microsoft Azure VNet o Citrix SD-WAN.

No unido a ningún dominio	Unidas a un dominio
Debe usar una suscripción de Citrix Managed Azure para aprovisionar los VDA. (No se pueden utilizar sus propias suscripciones de Azure para aprovisionar los VDA. Sin embargo, los usuarios se pueden conectar desde su propio Azure AD).	Puede usar una suscripción de Azure administrada por Citrix y sus propias suscripciones de Azure.
No se pueden solucionar problemas con una máquina bastión o RDP directo.	Puede solucionar problemas con una máquina bastión o RDP directo.
No se puede usar Citrix Profile Management. (Recomendar: utilizar catálogos persistentes).	Puede usar Citrix Profile Management o FSLogix.

Casos de implementación

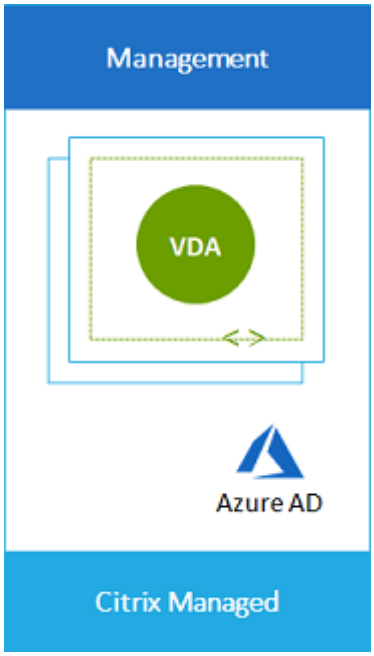
Los casos de implementación para escritorios y aplicaciones publicados varían en función de si utiliza una suscripción de Azure administrada por Citrix o su propia suscripción de Azure administrada por el cliente.

Implementación en una suscripción de Azure administrada por Citrix

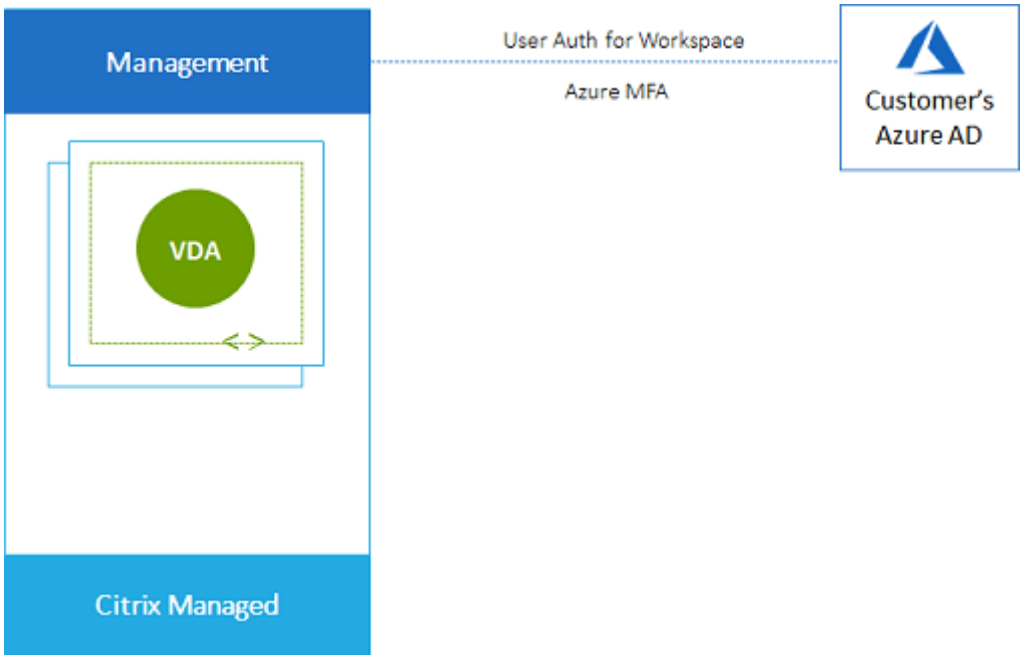


Citrix DaaS para Azure admite varios escenarios de implementación para la conexión y la autenticación de usuarios.

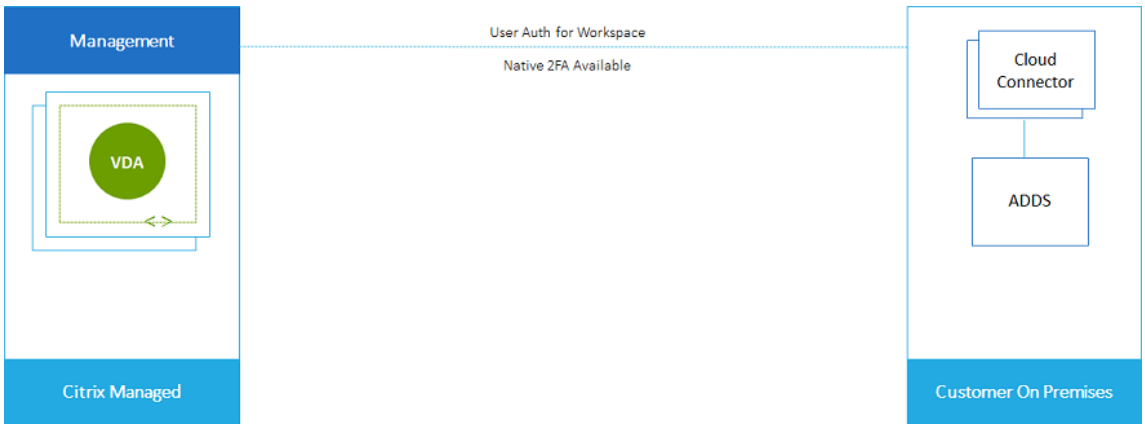
- **AD de Azure administrado:** esta es la implementación más sencilla, con agentes VDA no unidos a un dominio. Se recomienda para pruebas de concepto. Utilice el Azure AD administrado (que Citrix administra) para administrar los usuarios. Los usuarios no necesitan acceder a los recursos de la red local.



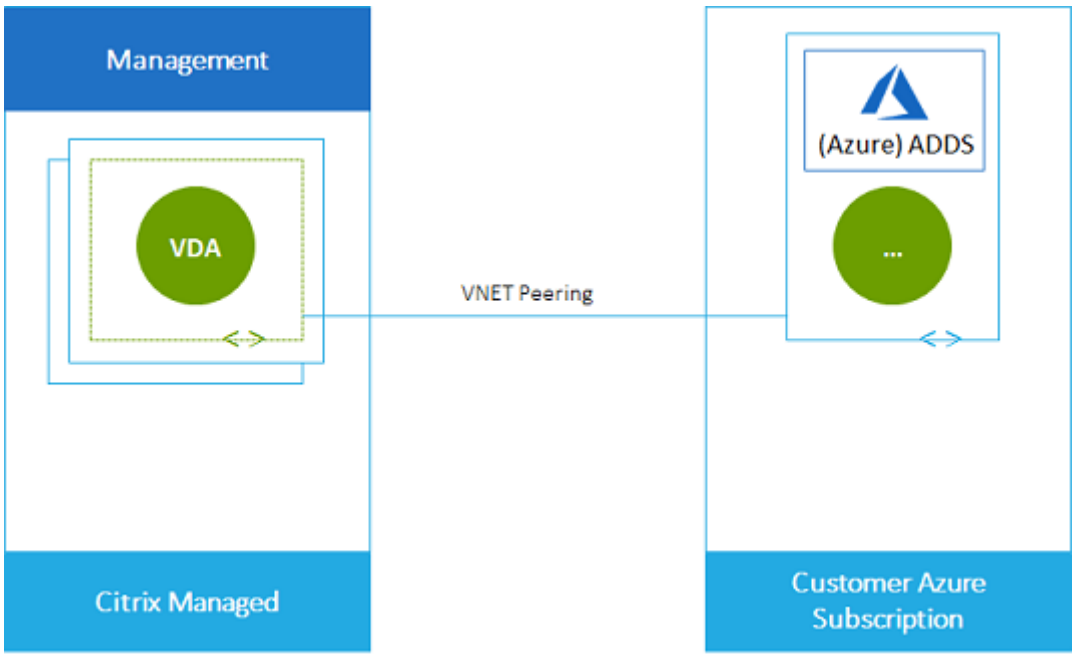
- **Azure Active Directory del cliente:** esta implementación contiene agentes VDA que no están unidos a un dominio. Utilice su propio Active Directory o Azure Active Directory (AAD) para la autenticación del usuario final. En este caso, los usuarios no necesitan acceder a los recursos de la red local.



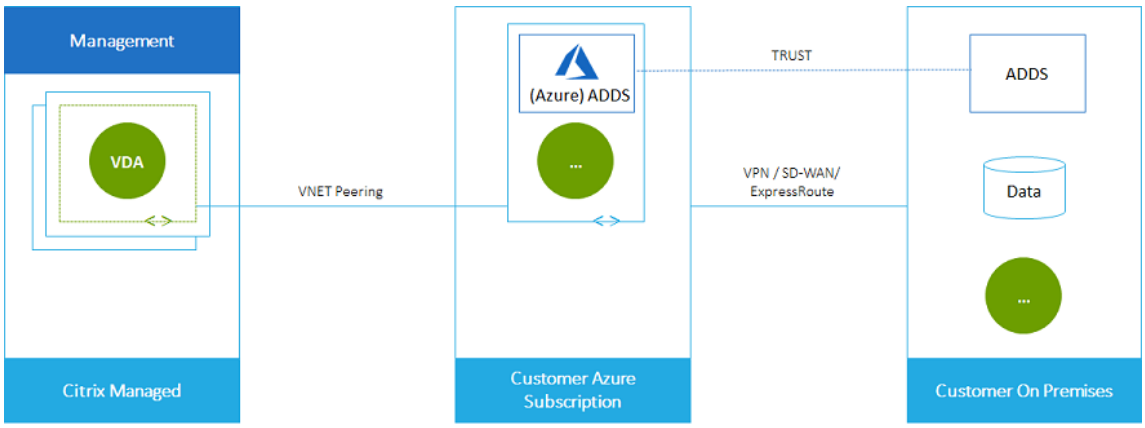
- **Azure Active Directory del cliente con acceso local:** esta implementación contiene agentes VDA que no están unidos a un dominio. Utilice su propio AD o AAD para la autenticación del usuario final. En este caso, la instalación de Citrix Cloud Connectors en la red local permite el acceso a los recursos de esa red.



- **Servicios de dominio de Azure Active Directory y interconexión de VNet del cliente:** Si su AD o AAD reside en su propia suscripción de Azure VNet y Azure, puede usar la función de interconexión de VNet de Microsoft Azure para una conexión de red y Azure Active Directory Domain Services (AADDS) para la autenticación de usuario final. Los VDA se unen a su dominio.

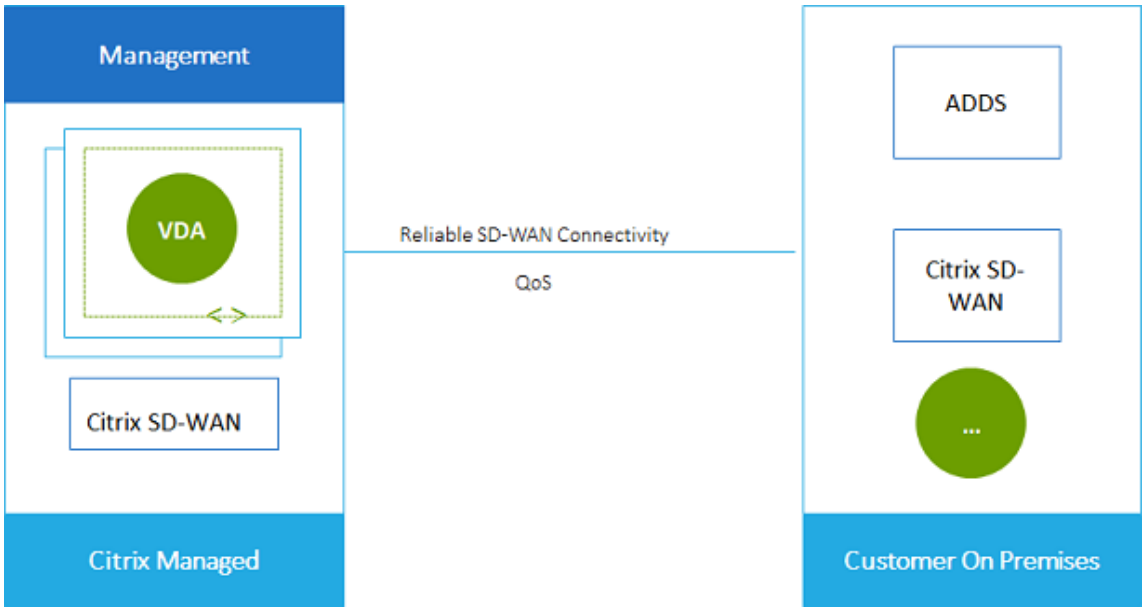


Para permitir que los usuarios accedan a los datos almacenados en su red local, puede usar su conexión VPN desde su suscripción de Azure hasta la ubicación local. La interconexión de Azure VNet se usa para la conectividad de red. Los Active Directory Domain Services Directory en la ubicación local se utilizan para la autenticación del usuario final.

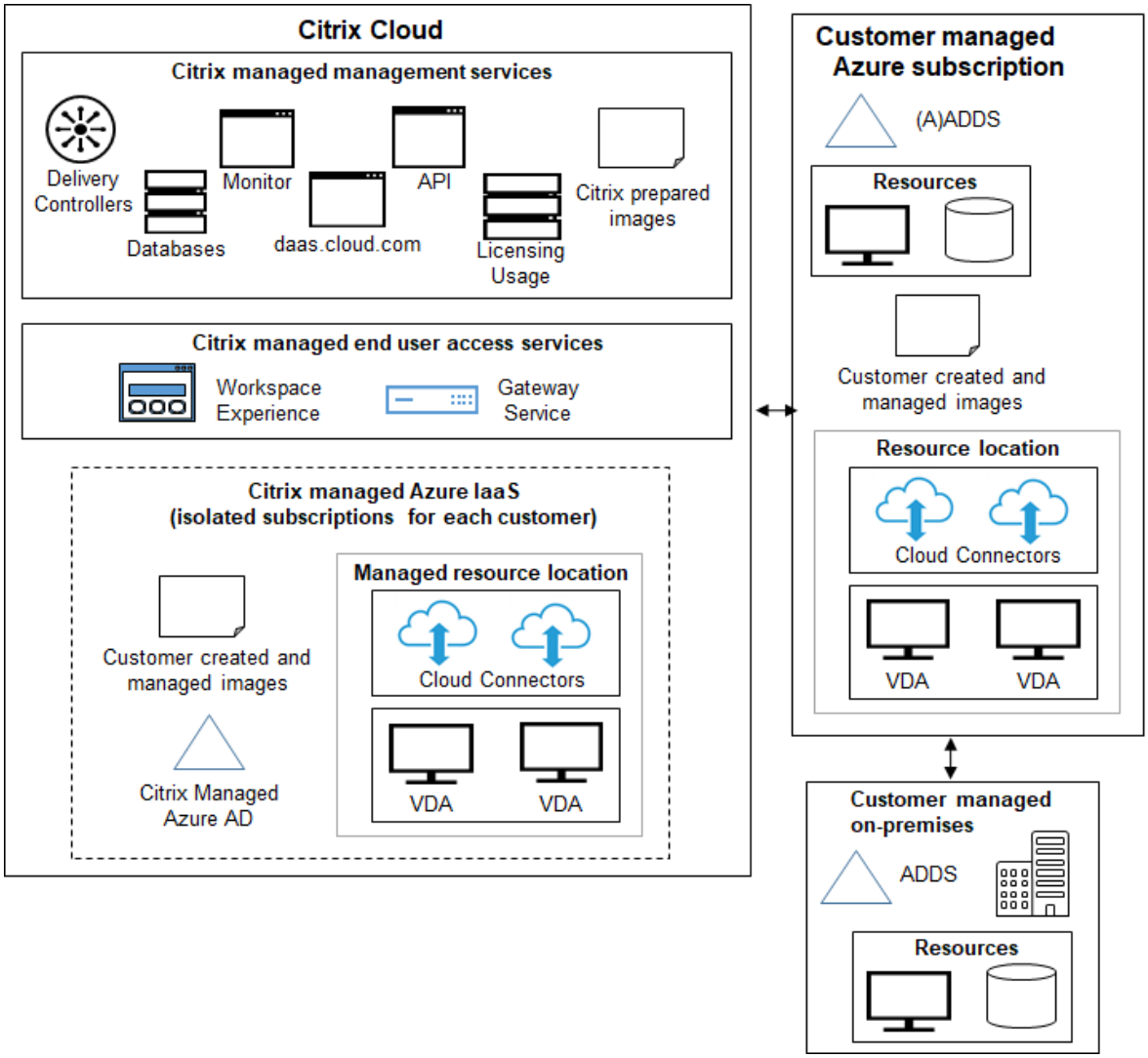


- **Active Directory y SD-WAN del cliente:** puede proporcionar a los usuarios acceso a archivos y otros elementos desde sus redes SD-WAN locales o en la nube.

  Citrix SD-WAN optimiza todas las conexiones de red que necesita Citrix DaaS para Azure. Al trabajar en conjunto con las tecnologías HDX, Citrix SD-WAN proporciona calidad de servicio y fiabilidad de conexión para ICA y Citrix DaaS fuera de banda para el tráfico de Azure.



Implementación en una suscripción de Azure administrada por el cliente



La implementación del gráfico anterior utiliza una suscripción de Azure administrada por el cliente. Sin embargo, la suscripción a Azure administrado por Citrix sigue siendo una opción para otros catálogos e imágenes, como lo indica el esquema punteado.

Interfaces de administración

Citrix DaaS para Azure tiene dos interfaces de administración gráfica: Distribución rápida y Configuración completa.

- **Distribución rápida** le permite crear catálogos rápidamente y empezar a entregar escritorios y aplicaciones a sus usuarios. (De ahí el nombre, Distribución rápida). Es la interfaz predeterminada al iniciar Citrix DaaS para Azure. También puede acceder a esta interfaz seleccionando

Administrar > Azure Quick Deploy. Las instrucciones de este conjunto de documentación del producto suponen que está utilizando Distribución rápida.

Si va a utilizar una suscripción de Azure administrada por Citrix al crear un catálogo o una imagen, debe usar Distribución rápida.

- La**configuración completa** ofrece funciones avanzadas y opciones de configuración para adaptar y administrar su implementación. Los catálogos que se crean en Distribución rápida aparecen automáticamente en Configuración completa. Para pasar de Distribución rápida a Configuración completa, seleccione **Administrar > Configuración completa**.

  Al crear un catálogo en Distribución rápida, se crean automáticamente un grupo de entrega y una conexión de host asociados en Configuración completa.

  La configuración completa también ofrece su propio proceso de creación de catálogos que incluye la creación de una conexión con el host de Azure y, a continuación, la creación de un catálogo y un grupo de entrega. Ese proceso solo se admite si usa su propia suscripción de Azure. Es mucho más fácil crear el catálogo en Distribución rápida.

  La configuración completa admite procesos relacionados con hipervisores y hosts de servicios en la nube distintos de Azure. No están disponibles para los clientes de Citrix DaaS para Azure.

Administrar catálogos creados en la interfaz de Distribución rápida

Después de crear un catálogo en la interfaz de Distribución rápida, puede seguir administrando ese catálogo en dicha interfaz. Para obtener más información, consulte Administrar catálogos. También puede utilizar la interfaz de Configuración completa.

Al crear un catálogo en Distribución rápida, a ese catálogo (además del grupo de entrega y la conexión de alojamiento que se crean automáticamente en segundo plano) se le asigna un ámbito de `Citrix managed object`. Los ámbitos se utilizan en la administración delegada para agrupar objetos.

Los catálogos, los grupos de entrega y las conexiones con el ámbito `Citrix managed object` tienen prohibido realizar determinadas acciones en la interfaz de Configuración completa. (Permitir esas acciones en Configuración completa puede afectar negativamente a la capacidad del sistema para admitir tanto Distribución rápida como Configuración completa, por lo que se inhabilitan). En la interfaz de Configuración completa:

- **Catálogo:** La mayoría de las acciones de administración de catálogos no están disponibles. No se puede eliminar un catálogo.
- **Grupo de entrega:** La mayoría de las acciones de administración de grupos de entrega están disponibles. No se puede eliminar el grupo de entrega.
- **Conexión:** La mayoría de las acciones de administración de conexiones no están disponibles. No se puede eliminar una conexión. No se puede crear una conexión basada en otra conexión que tenga el ámbito `Citrix managed object`.

Si crea un catálogo en Distribución rápida con su propia suscripción de Azure (que ha agregado a Distribución rápida) y quiere administrar el catálogo (y su grupo de entrega y conexión correspondientes) íntegramente en Configuración completa, puede *convertir* el catálogo.

- La conversión de un catálogo restringe su administración exclusivamente a la interfaz de Configuración completa. Después de convertir un catálogo, ya no podrá utilizar la interfaz de Distribución rápida para administrar ese catálogo.
- Una vez convertido un catálogo, se pueden seleccionar las acciones que anteriormente no estaban disponibles en Configuración completa. (El ámbito `Citrix managed object` se quita del catálogo convertido, del grupo de entrega y de la conexión de alojamiento).
- Para convertir un catálogo:

  En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, haga clic en cualquier parte de la entrada del catálogo. En la ficha **Detalles**, en **Parámetros avanzados**, seleccione **Convertir catálogo**. Cuando se le indique, confirme la conversión.
- No se puede convertir un catálogo creado en Distribución rápida mediante una suscripción a Azure administrado por Citrix.

Para obtener información sobre cómo administrar catálogos convertidos en Configuración completa, consulte:

- Administrar catálogos de máquinas (la configuración completa se refiere a los catálogos como catálogos de máquinas)
- Administrar grupos de entrega

Más información

Para obtener más detalles técnicos, consulte lo siguiente:

- Arquitectura de referencia de Citrix Tech Zone
- Resumen técnico de Citrix Tech Zone

Para obtener información sobre cómo automatizar sus implementaciones, consulte la vista previa de la API pública de escritorios administrados.

Cuando esté listo, comience.

Novedades

December 28, 2023

Uno de los objetivos de Citrix es ofrecer nuevas funciones y actualizaciones de productos a los clientes de Citrix DaaS para Azure cuando estén disponibles. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar. Para usted, el administrador del cliente, este proceso es transparente.

Citrix preparó actualizaciones de imágenes

Las imágenes preparadas por Citrix tienen instalado un Citrix Virtual Delivery Agent (VDA) actual. En general, las nuevas versiones de VDA se publican varias veces al año y las imágenes preparadas por Citrix disponibles se actualizan automáticamente con el VDA más reciente. Para obtener información sobre las funciones nuevas y mejoradas de la versión actual del VDA, consulte:

- agentes VDA de Windows
- VDA de Linux

Agosto de 2022

- Esta función está disponible de forma general: ahora puede crear catálogos de máquinas unidas a Azure Active Directory. Consulte Crear catálogos.

Mayo de 2022

- Ahora puede crear catálogos de máquinas unidas a Azure Active Directory. Esta función se encuentra en Tech Preview. Consulte Crear catálogos.
- Los proveedores de servicios de Citrix ahora pueden eliminar el servicio Citrix DaaS para Azure de los clientes. Consulte Eliminar un servicio.

Abril de 2022

- Ya está disponible la creación de conexiones de host para Citrix Hypervisor, Microsoft SCVMM, VMware vSphere, Prism Central y Nutanix AHV. Como tal, ahora puede usar hipervisores locales además de Azure.
- Cambio de nombre de producto de Citrix Virtual Apps and Desktops Standard para Azure a Citrix DaaS Standard para Azure. Para obtener más información sobre el cambio de marca de todas las ofertas de Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), consulte Novedades de Citrix DaaS. Obtenga más información sobre los cambios de nombre en nuestro anuncio en nuestro blog.

Enero de 2022

- Al crear catálogos, ahora puede almacenar sus máquinas en almacenamiento SSD estándar. Anteriormente, solo se admitían discos estándar (HDD) y SSD premium.
- Compatibilidad con estas nuevas regiones para alojar cargas de trabajo de VDA: sur de Brasil, India central, este de Japón, sur central de EE. UU. y sur del Reino Unido.
- Las instantáneas y la restauración ahora están disponibles para escritorios persistentes alojados en Citrix Managed Azure y BYO Azure. Consulte Instantánea y restauración de VDA.
- Ya está disponible la dirección IP pública estática para todo el tráfico saliente de los VDA alojados. Puede configurar Azure NAT Gateway para obtener la dirección IP. Consulte Crear una dirección IP estática pública.
- Azure VPN está disponible para obtener una vista previa técnica. Azure VPN le permite conectar Citrix Managed Azure directamente con los centros de datos locales. Consulte Vista previa técnica de Azure VPN.
- Hay nuevas imágenes de Linux disponibles para imágenes preparadas por Citrix.

Noviembre de 2021

- Los ensayos de 7 días aprobados automáticamente ya están disponibles (además de los ensayos aprobados por ventas).
- Los proveedores de servicios de Citrix ahora pueden administrar a los usuarios desde el panel **Administrar > Azure Quick Deploy** del servicio o desde la consola de Citrix Cloud. Para obtener más información, consulte Acceso de socios al proveedor de identidad del cliente.

Octubre de 2021

- Nueva información sobre la administración de catálogos creados en Distribución rápida.

Septiembre de 2021

- Elcontenido de la API de vista previa está disponible.
- Compatibilidad con Windows Server 2022 (requiere un VDA 2106 como mínimo).

Julio de 2021

- Interfaz de administración de Web Studio renombrada Configuración completa.

Junio de 2021

- Compatibilidad con dos interfaces de administración: Distribución rápida y Web Studio.

Mayo de 2021

- Este servicio admite la vista previa de Continuidad del servicio.
- Lasimágenes preparadas por Citrix ahora incluyen versiones de sesión única y multisesión de Ubuntu.
- Al agregar un Cloud Connector a una ubicación de recursos, mediante una suscripción de Azure administrado por Citrix, puede especificar el tipo de rendimiento de la máquina de Cloud Connector.
- Al crear un catálogo, las opciones de rendimiento de la máquina incluyen opciones que coinciden con el tipo de generación (gen1 o gen2) de la imagen seleccionada. Puede actualizar un catálogo con una imagen de tipo de generación diferente, si las máquinas del catálogo admiten ese tipo de generación.

Abril de 2022

- Cambio de nombre de producto de Citrix Virtual Apps and Desktops Standard para Azure a Citrix DaaS Standard para Azure.

Enero de 2021

- Compatibilidad con vistas previas para ver el uso del compromiso de consumo.

Octubre de 2020

- Puede utilizar la función Supervisar sombra para ver o trabajar en la VM o la sesión de un usuario.
- Compatibilidad con la producción para acceso con Remote PC.
- Opción de creación de catálogos mejorada para utilizar la licencia elegible de Azure Virtual Desktop o la ventaja híbrida de Azure
- Si una acción de reinicio en un equipo no se realiza correctamente, puede usar una acción de reinicio forzado.

Septiembre de 2020

- Los detalles sobre las imágenes se reorganizan y amplían. Por ejemplo, ahora puede agregar y modificar notas sobre las imágenes que preparó o importó. También puede limitar el acceso solo a direcciones IP especificadas.
- Al crear una conexión de emparejamiento de redes virtuales de Azure que utilizará una puerta de enlace de red virtual de Azure, ahora también puede habilitar la propagación de rutas de puerta de enlace de red virtual.
- Cambio de nombre del producto de Citrix Managed Desktops a Citrix Virtual Apps and Desktops Standard para Azure

Agosto de 2020

- Compatibilidad con vistas previas para acceso con Remote PC
- Ya está disponible una imagen de Windows Server 2019 preparada por Citrix.

July 2020

- Al agregar un Cloud Connector a una ubicación de recursos, mediante una suscripción de Azure administrada por el cliente, puede especificar el tipo de rendimiento de la máquina de Cloud Connector y el grupo de recursos de Azure. Para obtener información detallada, consulte Acciones de ubicaciones de recursos.
- Al crear un catálogo, puede especificar un esquema de nomenclatura de máquinas. Consulte Crear un catálogo mediante creación personalizada.

Junio de 2020

- En un entorno CSP, las conexiones SD-WAN se crean por arrendatario. Para que la opción de conexión SD-WAN esté disponible para el administrador del CSP, el arrendatario debe tener una autorización de servicio SD-WAN Orchestrator. Para obtener más información, consulte Filtrar recursos por cliente (implementaciones multiarrendatario).
- Soporte de producción para VDA de Linux cuando se usa una suscripción de Azure administrada por el cliente.
- El límite de agentes VDA por suscripción ahora es de 1200.

Mayo de 2020

- Puede agregar otra suscripción a Azure administrado por Citrix cuando necesite más máquinas del límite por suscripción a Citrix Managed Azure.

- Información adicional sobre los servidores DNS.

Marzo de 2020

- Compatibilidad con la producción para conexiones SD-WAN.

Febrero de 2020

- Para ver la información de uso de licencias de Citrix, siga las instrucciones de Supervisar la supervisión de licencias y uso de Citrix DaaS Standard para Azure.
- Compatibilidad con vistas previas para catálogos que contienen máquinas Red Hat Enterprise Linux o Ubuntu. Esta función solo es válida cuando se usa una suscripción de Azure administrada por el cliente y requiere una imagen importada que contenga un VDA de Citrix Linux.
- Ahora puede configurar el equilibrio de carga vertical u horizontal para todas sus máquinas multisesión. (Anteriormente, todas las máquinas utilizaban equilibrio de carga horizontal). Esta selección global se aplica a todos los catálogos de su implementación. Consulte Equilibrio de carga.
- Ahora puede agregar una suscripción de Azure si no es un administrador global.
- Ahora hay una imagen preparada por Citrix para Windows 10 Enterprise Virtual Desktop (multisesión) con Office 365 ProPlus.

Enero de 2020

- Agregue la funcionalidad para rutas personalizadas en conexiones de emparejamiento de redes virtuales.
- Actualizaciones del artículo de seguridad para mejorar la información sobre puertos y normas.

Noviembre de 2019

- Compatibilidad con vistas previas para conexiones SD-WAN.

Octubre de 2019

- En Sistemas operativos compatibles, se agregaron entradas para:
  - Windows 7 (solo admite VDA 7.15 con la última actualización acumulativa).
  - Windows Server 2019.
- Ya está disponible una imagen preparada por Citrix para Windows Server 2012 R2.

- Se agregó información de configuración de ubicación de recursos. Para obtener más información, consulte Acciones de ubicación de recursos y Configuración de ubicación de recursos al crear un catálogo.

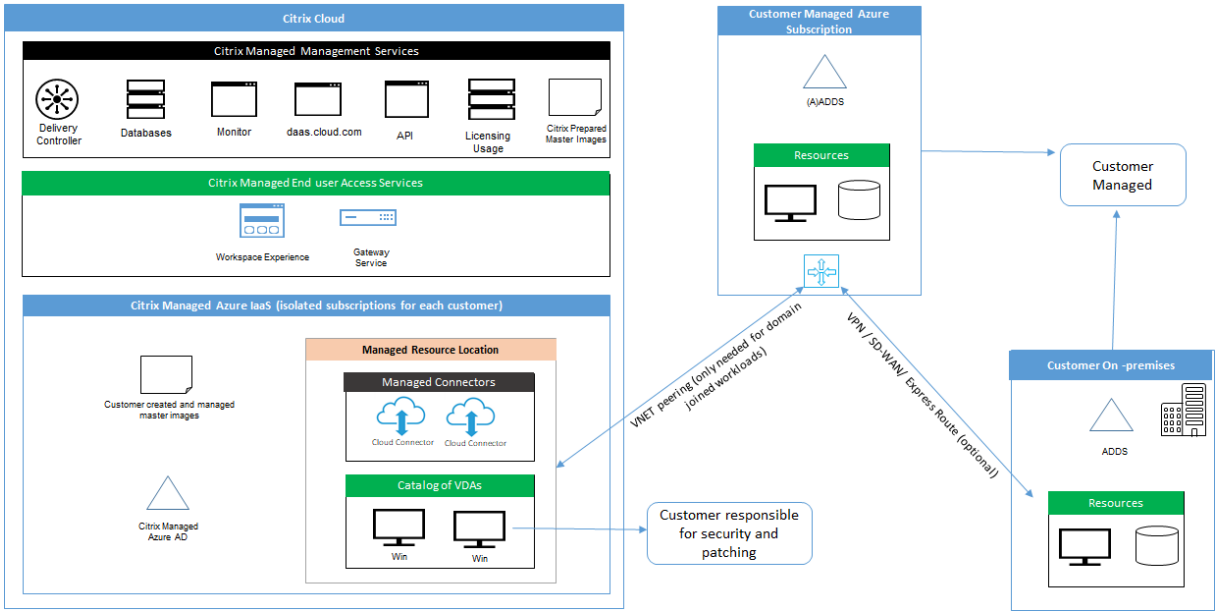
Septiembre de 2019

- De forma predeterminada, las máquinas se crean en una suscripción de Azure administrada por Citrix. Ahora también puede crear catálogos e imágenes en su propia suscripción de Azure administrada por el cliente.

Información técnica general sobre la seguridad

May 16, 2022

El siguiente diagrama muestra los componentes de una implementación de Citrix DaaS Standard para Azure (anteriormente Citrix Virtual Apps and Desktops Standard para Azure). En este ejemplo, se utiliza una conexión de emparejamiento de redes virtuales.



Con Citrix DaaS para Azure, los Virtual Delivery Agents (VDA) del cliente que entregan escritorios y aplicaciones, además de Citrix Cloud Connectors, se implementan en una suscripción y arrendatario de Azure que administra Citrix.

> **NOTA:**
>
> Este artículo proporciona una descripción general de los requisitos de seguridad para los clientes que implementan Citrix DaaS para Azure mediante una suscripción a Azure administrado por

> Citrix. Para obtener una descripción general de la arquitectura de una implementación de Citrix DaaS para Azure mediante una suscripción de Azure administrada por el cliente, incluida la información de seguridad, consulte Reference Architecture: Virtual Apps and Desktops Service - Azure.

Cumplimiento de normas basado en la nube de Citrix

En enero de 2021, el uso de la capacidad de Azure administrado por Citrix con varias ediciones de Citrix DaaS y Workspace Premium Plus no se ha evaluado para Citrix SOC 2 (tipo 1 o 2), la norma ISO 27001, la normativa HIPAA ni otros requisitos de cumplimiento de normas de la nube. Visite el Centro de confianza de Citrix para obtener más información sobre las certificaciones de Citrix Cloud y consúltelo con frecuencia para mantenerse al día de las novedades.

Responsabilidad de Citrix

Citrix Cloud Connectors para catálogos no unidos a un dominio

Citrix DaaS para Azure implementa al menos dos Cloud Connectors en cada ubicación de recursos. Algunos catálogos pueden compartir una ubicación de recursos si se encuentran en la misma región que otros catálogos del mismo cliente.

Citrix es responsable de las siguientes operaciones de seguridad en Cloud Connectors de un catálogo no unido a un dominio:

- Aplicación de actualizaciones del sistema operativo y parches de seguridad
- Instalación y mantenimiento de software antivirus
- Aplicación de actualizaciones de software de Cloud Connector

Los clientes no tienen acceso a los Cloud Connectors. Por lo tanto, Citrix es plenamente responsable del rendimiento de los Cloud Connectors del catálogo no unido al dominio.

Suscripción a Azure y Azure Active Directory

Citrix es responsable de la seguridad de la suscripción a Azure y de la instancia de Azure Active Directory (AAD) que se crean para el cliente. Citrix garantiza el aislamiento de los arrendatarios, de manera que cada cliente tenga su propia suscripción a Azure y AAD y se evite la intercomunicación entre diferentes arrendatarios. Citrix también restringe el acceso al AAD solo al personal de operaciones de Citrix DaaS para Azure y Citrix. El acceso por parte de Citrix a la suscripción de Azure de cada cliente se audita.

Los clientes que utilizan catálogos no unidos a un dominio pueden utilizar AAD administrado por Citrix como medio de autenticación para Citrix Workspace. Para estos clientes, Citrix crea cuentas de

usuario con privilegios limitados en la instancia de AAD administrada por Citrix. Sin embargo, ni los usuarios ni los administradores de los clientes pueden ejecutar ninguna acción en la instancia de AAD administrada por Citrix. Si estos clientes optan por utilizar su propio AAD, son plenamente responsables de su seguridad.

Redes virtuales e infraestructura

Dentro de la suscripción de Azure administrado por Citrix del cliente, Citrix crea redes virtuales para aislar las ubicaciones de recursos. Dentro de esas redes, Citrix crea máquinas virtuales para los agentes VDA, Cloud Connectors y máquinas del generador de imágenes, además de cuentas de almacenamiento, cajas fuerte de claves (Key Vaults) y otros recursos de Azure. Citrix, en asociación con Microsoft, es responsable de la seguridad de las redes virtuales, incluidos los firewalls de red virtual.

Citrix garantiza que la directiva de firewall predeterminada de Azure (grupos de seguridad de red) esté configurada para limitar el acceso a las interfaces de red en conexiones de emparejamiento de redes virtuales y SD-WAN. En general, esto controla el tráfico entrante a los VDA y Cloud Connectors. Para obtener más detalles, consulte:

- Directiva de firewall para las conexiones de emparejamiento de redes virtuales de Azure
- Directiva de firewall para las conexiones SD-WAN

Los clientes no pueden cambiar esta directiva de firewall predeterminada, pero pueden implementar reglas de firewall adicionales en máquinas VDA creadas por Citrix; por ejemplo, para restringir parcialmente el tráfico saliente. Los clientes que instalan clientes de red privada virtual u otro software capaz de eludir las reglas de firewall en máquinas VDA creadas por Citrix son responsables de los riesgos de seguridad que puedan surgir.

Al usar el generador de imágenes en Citrix DaaS para Azure para crear y personalizar una nueva imagen de máquina, los puertos 3389-3390 se abren temporalmente en la VNet administrada por Citrix, de modo que el cliente puede hacer RDP en la máquina que contiene la nueva imagen de máquina para personalizarla.

Responsabilidad de Citrix al utilizar conexiones de emparejamiento de redes virtuales de Azure

Para que los VDA de Citrix DaaS para Azure se pongan en contacto con controladores de dominio locales, recursos compartidos de archivos u otros recursos de intranet, Citrix DaaS para Azure proporciona un flujo de trabajo de emparejamiento de VNet como opción de conectividad. La red virtual administrada por Citrix del cliente se empareja con una red virtual Azure administrada por el cliente. La red virtual administrada por el cliente puede permitir la conectividad con los recursos locales del

cliente mediante la solución de conectividad de nube a local que elija el cliente, como Azure ExpressRoute o túneles IPSec.

La responsabilidad de Citrix por el emparejamiento de redes virtuales se limita a ofrecer el flujo de trabajo y la configuración de recursos de Azure relacionada para establecer una relación de emparejamiento entre Citrix y las redes virtuales de Azure administradas por el cliente

Directiva de firewall para las conexiones de emparejamiento de redes virtuales de Azure Citrix abre o cierra los siguientes puertos para el tráfico entrante y saliente que utiliza una conexión de emparejamiento de redes virtuales.

Red virtual de Azure administrada por Citrix con máquinas que no están unidas al dominio

- Reglas de entrada
  - Permitir los puertos 80, 443, 1494 y 2598 de entrada desde VDA a Cloud Connectors y desde Cloud Connectors a VDA.
  - Permitir los puertos 49152-65535 de entrada a los VDA desde un intervalo de direcciones IP utilizado por la función de remedo Supervisar. Consulte Communication Ports Used by Citrix Technologies.
  - Denegar todas las demás entradas. Esto incluye el tráfico interno en redes virtuales de Azure, de VDA a VDA y de VDA a Cloud Connector.
- Reglas de salida
  - Permitir todo el tráfico de salida.

Red virtual de Azure administrada por Citrix con máquinas unidas a un dominio

- Reglas de entrada:
  - Permitir los puertos 80, 443, 1494 y 2598 de entrada de VDA a Cloud Connectors y de Cloud Connectors a VDA.
  - Permitir los puertos 49152-65535 de entrada a los VDA desde un intervalo de direcciones IP utilizado por la función de remedo Supervisar. Consulte Communication Ports Used by Citrix Technologies.
  - Denegar todas las demás entradas. Esto incluye el tráfico interno en redes virtuales de Azure, de VDA a VDA y de VDA a Cloud Connector.
- Reglas de salida
  - Permitir todo el tráfico de salida.

Red virtual de Azure administrada por el cliente con máquinas unidas a un dominio

- Es responsabilidad del cliente configurar correctamente su red virtual. Esto incluye abrir los siguientes puertos para unión a dominios.
- Reglas de entrada:
  - Permitir la entrada en 443, 1494, 2598 desde sus IP de cliente para inicios internos.
  - Permitir la entrada en 53, 88, 123, 135-139, 389, 445 y 636 desde la red virtual de Citrix (intervalo de direcciones IP especificado por el cliente).
  - Permitir la entrada en los puertos abiertos con una configuración de proxy.
  - Otras reglas creadas por el cliente.
- Reglas de salida:
  - Permitir la salida en 443, 1494, 2598 a la red virtual de Citrix (intervalo de direcciones IP especificado por el cliente) para inicios internos.
  - Otras reglas creadas por el cliente.

Responsabilidad de Citrix al utilizar la conectividad SD-WAN

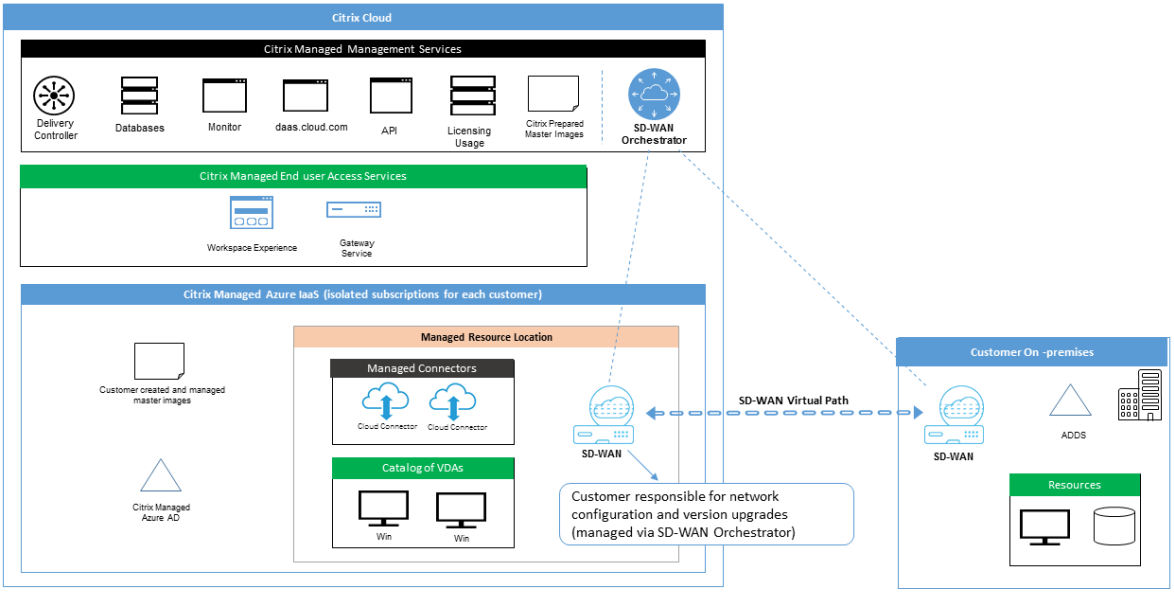
Citrix admite una forma totalmente automatizada de implementar instancias virtuales de Citrix SD-WAN para permitir la conectividad entre Citrix DaaS para Azure y los recursos locales. La conectividad de Citrix SD-WAN tiene una serie de ventajas en comparación con la interconexión de VNet, que incluyen:

Alta fiabilidad y seguridad de las conexiones de VDA a centro de datos y VDA a sucursal (ICA).

- La mejor experiencia de usuario final para los empleados de oficina, con capacidades avanzadas de QoS y optimizaciones de VoIP.
- Capacidad incorporada para inspeccionar, priorizar e informar sobre el tráfico de red de Citrix HDX y el uso de otras aplicaciones.

Citrix exige que los clientes que deseen aprovechar la conectividad SD-WAN para Citrix DaaS para Azure usen SD-WAN Orchestrator para administrar sus redes Citrix SD-WAN.

El siguiente diagrama muestra los componentes agregados en una implementación de Citrix DaaS para Azure mediante conectividad SD-WAN.



La implementación de Citrix SD-WAN para Citrix DaaS para Azure es similar a la configuración de implementación estándar de Azure para Citrix SD-WAN. Para obtener más información, consulte Implementación de una instancia de Citrix SD-WAN Standard Edition en Azure. En una configuración de alta disponibilidad, se implementa un par activo/en espera de instancias SD-WAN con equilibradores de carga de Azure como puerta de enlace entre la subred que contiene VDA y Cloud Connectors e Internet. En una configuración que no es de alta disponibilidad, solo se implementa una única instancia de SD-WAN como puerta de enlace. A las interfaces de red de los dispositivos SD-WAN virtuales se les asignan direcciones de un pequeño intervalo de direcciones aparte, dividido en dos subredes.

Al configurar la conectividad SD-WAN, Citrix realiza algunos cambios en la configuración de red de los escritorios administrados descritos anteriormente. En particular, todo el tráfico saliente de la VNet, incluido el tráfico a destinos de Internet, se enruta a través de la instancia de SD-WAN en la nube. La instancia de SD-WAN también está configurada para ser el servidor DNS de la red virtual administrada por Citrix.

El acceso de administración a las instancias virtuales de SD-WAN requiere un inicio de sesión de administrador y una contraseña. A cada instancia de SD-WAN se le asigna una contraseña segura única y aleatoria que los administradores de SD-WAN pueden utilizar para iniciar sesión y solucionar problemas de manera remota a través de la interfaz de usuario de SD-WAN Orchestrator, la interfaz de usuario de administración de dispositivos virtuales y la interfaz de línea de comandos.

Al igual que otros recursos específicos de arrendatario, las instancias SD-WAN virtuales implementadas en una red virtual específica de un cliente están totalmente aisladas de todas las demás redes virtuales.

Cuando el cliente habilita la conectividad de Citrix SD-WAN, Citrix automatiza la implementación ini-

cial de las instancias SD-WAN virtuales utilizadas con Citrix DaaS para Azure, mantiene los recursos subyacentes de Azure (máquinas virtuales, equilibradores de carga, etc.), proporciona valores predeterminados listos para usar seguros y eficientes para el inicio configuración de instancias SD-WAN virtuales y permite el mantenimiento continuo y la solución de problemas a través de SD-WAN Orchestrator. Citrix también adopta medidas razonables para efectuar la validación automática de la configuración de red SD-WAN, comprobar los riesgos de seguridad conocidos y mostrar las alertas correspondientes a través de SD-WAN Orchestrator.

Directiva de firewall para las conexiones SD-WAN Citrix utiliza las directivas de firewall de Azure (grupos de seguridad de red) y la asignación de direcciones IP públicas para limitar el acceso a las interfaces de red de los dispositivos SD-WAN virtuales:

- Solo a las interfaces WAN y de administración se les asignan direcciones IP públicas y se les permite la conectividad de salida a Internet.
- Las interfaces LAN, que actúan como puertas de enlace para la red virtual administrada por Citrix, solo pueden intercambiar tráfico de red con máquinas virtuales de la misma red virtual.
- Las interfaces WAN limitan el tráfico de entrada al puerto UDP 4980 (que Citrix SD-WAN utiliza para la conectividad de rutas virtuales) y deniegan el tráfico de salida a la red virtual.
- Los puertos de administración permiten el tráfico de entrada a los puertos 443 (HTTPS) y 22 (SSH).
- Las interfaces de alta disponibilidad solo pueden intercambiar tráfico de control entre sí.

Acceso a la infraestructura

Citrix puede acceder a la infraestructura administrada por Citrix del cliente (Cloud Connectors) para realizar determinadas tareas administrativas, como recopilar registros (incluido el Visor de eventos de Windows) y reiniciar los servicios sin notificarlo al cliente. Citrix es responsable de ejecutar estas tareas de forma segura y con un impacto mínimo para el cliente. Citrix también es responsable de garantizar que los archivos de registro se obtengan, transporten y manejen de forma segura. No se puede acceder a los agentes VDA de cliente de esta forma.

Copias de seguridad de catálogos no unidos a un dominio

Citrix no se hace responsable de realizar copias de seguridad de los catálogos que no están unidos a un dominio.

Copias de seguridad de imágenes de máquina

Citrix es responsable de realizar copias de seguridad de cualquier imagen de máquina cargada en Citrix DaaS para Azure, incluidas las imágenes creadas con el generador de imágenes. Citrix utiliza almacenamiento redundante local para estas imágenes.

Bastiones para catálogos no unidos a un dominio

El personal de operaciones de Citrix tiene la capacidad de crear un bastión, si es necesario, para acceder a la suscripción de Azure administrada por Citrix del cliente a fin de diagnosticar y solucionar problemas, potencialmente antes de que el propio cliente tenga conocimiento del problema. Citrix no requiere consentimiento del cliente para crear un bastión. Cuando crea el bastión, Citrix crea una contraseña segura, generada aleatoriamente, para el mismo y restringe el acceso RDP a las direcciones IP NAT de Citrix. Cuando el bastión ya no es necesario, Citrix lo desecha y la contraseña deja de ser válida. El bastión (y las reglas de acceso RDP que lo acompañan) se desechan cuando finaliza la operación. Citrix solo puede acceder a Cloud Connectors no unidos al dominio del cliente con el bastión. Citrix no tiene la contraseña para iniciar sesión en agentes VDA no unidos a un dominio o Cloud Connectors y VDA unidos a un dominio.

Directiva de firewall al utilizar herramientas para solución de problemas

Cuando un cliente solicita la creación de una máquina de bastión para solución de problemas, tienen lugar las siguientes modificaciones del grupo de seguridad en la red virtual administrada por Citrix:

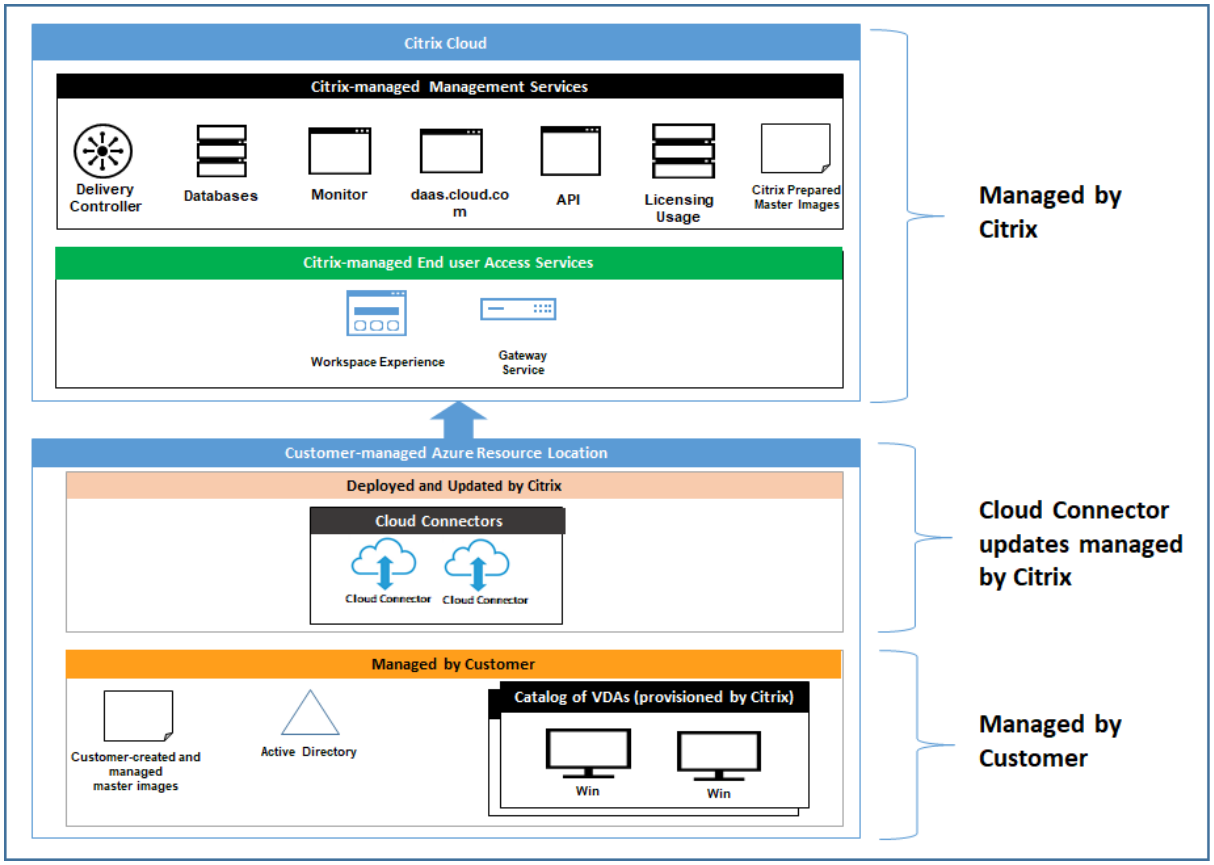
- Se permite temporalmente el tráfico de entrada por el puerto 3389 desde el intervalo de direcciones IP especificado por el cliente al bastión.
- Se permite temporalmente el tráfico de entrada por el puerto 3389 desde la dirección IP del bastión a cualquier dirección de la red virtual (VDA y Cloud Connectors).
- Se continúa bloqueando el acceso RDP entre Cloud Connectors, VDA y otros VDA.

Cuando un cliente habilita el acceso RDP para solución de problemas, tienen lugar las siguientes modificaciones del grupo de seguridad en la red virtual administrada por Citrix:

- Se permite temporalmente el tráfico de entrada por el puerto 3389 desde el intervalo de direcciones IP especificado por el cliente a cualquier dirección de la red virtual (VDA y Cloud Connectors).
- Se continúa bloqueando el acceso RDP entre Cloud Connectors, VDA y otros VDA.

Suscripciones administradas por el cliente

Para las suscripciones administradas por el cliente, Citrix cumple con las responsabilidades anteriores durante la implementación de los recursos de Azure. Después de la implementación, toda la responsabilidad anterior recae en el cliente, puesto que es este es el propietario de la suscripción a Azure.



Responsabilidad del cliente

VDA e imágenes de máquina

El cliente es responsable de todos los aspectos del software instalado en las máquinas VDA, incluidos:

- Actualizaciones del sistema operativo y parches de seguridad
- Antivirus y antimalware
- Actualizaciones de software de VDA y parches de seguridad
- Reglas de firewall de software adicionales (especialmente el tráfico saliente)
- Siga las Recomendaciones y consideraciones de seguridadde Citrix

Citrix proporciona una imagen preparada que sirve de punto de partida. Los clientes pueden utilizar esta imagen con fines de prueba de concepto o demostración o como base para construir su propia imagen de máquina. Citrix no garantiza la seguridad de esta imagen preparada. Citrix intentará mantener actualizados el sistema operativo y el software de VDA de la imagen preparada y habilitará Windows Defender en estas imágenes.

Responsabilidad del cliente al utilizar emparejamiento de redes virtuales

El cliente debe abrir todos los puertos especificados en Red virtual de Azure administrada por el cliente con máquinas unidas a un dominio.

Cuando se configura el emparejamiento de redes virtuales, el cliente es responsable de la seguridad de su propia red virtual y de su conectividad con los recursos locales. El cliente también es responsable de la seguridad del tráfico entrante de la red virtual emparejada administrada por Citrix. Citrix no realiza ninguna acción para bloquear el tráfico procedente de la red virtual que administra y dirigido a los recursos locales del cliente.

Los clientes tienen las siguientes opciones para restringir el tráfico entrante:

- Asignar a la red virtual administrada por Citrix un bloque de IP que no se utilice en ningún otro lugar de la red local del cliente o de la red virtual conectada administrada por el cliente. Esto es necesario para el emparejamiento de redes virtuales.
- Agregar grupos de seguridad de red y firewalls de Azure en la red virtual y la red local del cliente para bloquear o restringir el tráfico procedente del bloque de IP administrado por Citrix.
- Implementar medidas tales como sistemas de prevención de intrusiones, firewalls de software y motores de análisis del comportamiento en la red virtual del cliente y en la red local, dirigidas al bloque de IP administrado por Citrix.

Responsabilidad del cliente al utilizar conectividad SD-WAN

Cuando se configura la conectividad SD-WAN, los clientes tienen total flexibilidad para configurar las instancias SD-WAN virtuales que se utilizan con Citrix DaaS para Azure de acuerdo con sus requisitos de red, con la excepción de algunos elementos necesarios para garantizar el correcto funcionamiento de SD-WAN en la VNet administrada por Citrix. Las responsabilidades del cliente incluyen:

- Diseño y configuración de reglas de redirección y firewall, incluidas las reglas para el "breakout" del tráfico de Internet y DNS.
- Mantenimiento de la configuración de red SD-WAN.
- Supervisión del estado operativo de la red.
- Implementación oportuna de actualizaciones de software o correcciones de seguridad de Citrix SD-WAN. Dado que todas las instancias de Citrix SD-WAN en la red de un cliente deben ejecutar

la misma versión de software SD-WAN, los clientes deben administrar las implementaciones de versiones de software actualizadas en Citrix DaaS para instancias de Azure SD-WAN de acuerdo con los programas y restricciones de mantenimiento de la red.

La configuración incorrecta de las reglas de firewall y enrutamiento de SD-WAN, o la mala administración de las contraseñas de administración de SD-WAN, pueden provocar riesgos de seguridad tanto para los recursos virtuales de Citrix DaaS para Azure como para los recursos locales a los que se puede acceder a través de las rutas virtuales de Citrix SD-WAN. Otro posible riesgo para la seguridad se deriva del hecho de no actualizar el software Citrix SD-WAN con la versión de parches más reciente disponible. Si bien SD-WAN Orchestrator y otros servicios de Citrix Cloud proporcionan los medios para hacer frente a tales riesgos, los clientes son responsables, en definitiva, de garantizar que las instancias virtuales de SD-WAN estén configuradas correctamente.

Proxy

El cliente puede elegir si quiere utilizar un proxy para el tráfico de salida del VDA. Si se utiliza un proxy, el cliente es responsable de:

- La configuración de los parámetros del proxy en la imagen de máquina del VDA o, si el VDA está unido a un dominio, el uso de la directiva de grupo de Active Directory.
- El mantenimiento y la seguridad del proxy.

No se permite el uso de proxies con Citrix Cloud Connectors u otra infraestructura administrada por Citrix.

Resiliencia de catálogos

Citrix proporciona tres tipos de catálogos con diferentes niveles de resiliencia:

- **Estático:** Cada usuario se asigna a un solo VDA. Este tipo de catálogo no proporciona alta disponibilidad. Si el VDA de un usuario queda inactivo, tendrá que colocarse en uno nuevo para recuperación. Azure proporciona un SLA del 99,5% para máquinas virtuales de una sola instancia. El cliente puede realizar aún una copia de seguridad del perfil de usuario, pero se perderán todas las personalizaciones realizadas en el VDA (como instalar programas o configurar Windows).
- **Aleatorio:** Cada usuario se asigna aleatoriamente a un VDA de servidor durante el inicio. Este tipo de catálogo proporciona alta disponibilidad a través de redundancia. Si un VDA queda inactivo, no se pierde ninguna información, puesto que el perfil del usuario reside en otro lugar.
- **Multisesión de Windows 10:** Este tipo de catálogo funciona de la misma manera que el tipo aleatorio, pero utiliza VDA de estación de trabajo Windows 10, en lugar de VDA de servidor.

Copias de seguridad para catálogos unidos a dominios

Si el cliente utiliza catálogos unidos a un dominio con emparejamiento de redes virtuales, ese cliente es responsable de hacer copia de seguridad de sus perfiles de usuario. Citrix recomienda que los clientes configuren recursos compartidos de archivos locales y establezcan directivas en sus instancias de Active Directory o VDA para extraer perfiles de usuario de tales recursos compartidos de archivos. El cliente es responsable de hacer copia de seguridad y de garantizar la disponibilidad de estos recursos compartidos de archivos.

Recuperación ante desastres

En caso de pérdida de datos de Azure, Citrix recuperará tantos recursos de la suscripción a Azure administrada por Citrix como sea posible. Citrix intentará recuperar los Cloud Connectors y los VDA. Si Citrix no es capaz de recuperar correctamente estos elementos, los clientes son responsables de crear un nuevo catálogo. Citrix asume que se hace copia de seguridad de las imágenes de máquina y que los clientes han realizado copias de seguridad de sus perfiles de usuario, lo que permite reconstruir el catálogo.

En caso de pérdida de toda una región de Azure, el cliente es responsable de reconstruir su red virtual administrada por el cliente en una nueva región y de crear una nueva interconexión de VNet o una nueva instancia de SD-WAN dentro de Citrix DaaS para Azure.

Responsabilidades compartidas de Citrix y del cliente

Citrix Cloud Connector para catálogos unidos a dominios

Citrix DaaS para Azure implementa al menos dos Cloud Connectors en cada ubicación de recursos. Algunos catálogos pueden compartir una ubicación de recursos si se encuentran en la misma región, emparejamiento de redes virtuales y dominio que otros catálogos del mismo cliente. Citrix configura Cloud Connectors unidos al dominio del cliente para la siguiente configuración de seguridad predeterminada de la imagen:

- Actualizaciones del sistema operativo y parches de seguridad
- Software antivirus
- Actualizaciones de software de Cloud Connector

Normalmente, los clientes no tienen acceso a los Cloud Connectors. Sin embargo, pueden obtener acceso a través de pasos para solución de problemas de catálogos e iniciando sesión con credenciales de dominio. El cliente es responsable de los cambios que realice al iniciar sesión a través del bastión.

Los clientes también tienen control sobre los Cloud Connectors unidos a un dominio mediante la directiva de grupo de Active Directory. El cliente es responsable de garantizar que las directivas de

grupo que se aplican al Cloud Connector sean seguras y razonables. Por ejemplo, si el cliente decide inhabilitar las actualizaciones del sistema operativo mediante la directiva de grupo, el cliente es responsable de realizar las actualizaciones del sistema operativo en los Cloud Connectors. El cliente también puede optar por utilizar la directiva de grupo para garantizar una seguridad más estricta que la predeterminada del Cloud Connector, por ejemplo, instalando otro software antivirus. En general, Citrix recomienda que los clientes coloquen Cloud Connectors en su propia unidad organizativa de Active Directory sin directivas, ya que esto garantizará que los valores predeterminados de Citrix puedan aplicarse sin problemas.

Solución de problemas

En caso de que el cliente tenga problemas con el catálogo de Citrix DaaS para Azure, hay dos opciones para solucionar problemas: usar bastiones y habilitar el acceso RDP. Ambas opciones implican un riesgo de seguridad para el cliente. El cliente debe comprender este riesgo y dar su consentimiento de que lo asume antes de utilizar estas opciones.

Citrix es responsable de abrir y cerrar los puertos necesarios para llevar a cabo operaciones de solución de problemas y de restringir a qué máquinas se puede acceder durante estas operaciones.

Con bastiones o acceso RDP, el usuario activo que realiza la operación es responsable de la seguridad de las máquinas a las que se accede. Si el cliente accede al VDA o Cloud Connector a través de RDP y contrae accidentalmente un virus, el cliente es responsable. Si el personal de asistencia técnica de Citrix accede a estas máquinas, es responsabilidad de ese personal realizar las operaciones de forma segura. La responsabilidad por cualquier vulnerabilidad expuesta por cualquier persona que acceda al bastión u otras máquinas de la implementación (por ejemplo, la responsabilidad del cliente de agregar intervalos de direcciones IP a la lista de permitidos, la responsabilidad de Citrix de implementar correctamente los intervalos de direcciones IP) se trata en otras secciones de este documento.

En ambos casos, Citrix es responsable de crear correctamente excepciones de firewall para permitir el tráfico RDP. Citrix también es responsable de revocar estas excepciones después de que el cliente se deshaga del bastión o finalice el acceso RDP a través de Citrix DaaS para Azure.

Bastiones Citrix puede crear bastiones en la red virtual administrada por Citrix del cliente dentro de la suscripción administrada por Citrix del cliente para diagnosticar y resolver problemas, ya sea de forma proactiva (sin notificación al cliente) o en respuesta a un problema planteado por el cliente. El bastión es una máquina a la que el cliente puede acceder a través de RDP y luego utilizar para acceder, siempre a través de RDP, a los VDA y (para catálogos unidos a un dominio) a Cloud Connectors para recopilar registros, reiniciar servicios o realizar otras tareas administrativas. De forma predeterminada, la creación de un bastión abre una regla de firewall externa para permitir el tráfico RDP procedente de un intervalo de direcciones IP especificado por el cliente a la máquina de bastión. También abre una

regla de firewall interna para permitir el acceso a Cloud Connectors y VDA a través de RDP. La apertura de estas reglas plantea un gran riesgo para la seguridad.

El cliente es responsable de proporcionar una contraseña segura para la cuenta local de Windows. El cliente también es responsable de proporcionar un intervalo de direcciones IP externas que permita el acceso RDP al bastión. Si el cliente decide no proporcionar un intervalo de direcciones IP (permitiendo el acceso RDP a cualquiera), el cliente es responsable de cualquier acceso por parte de direcciones IP malintencionadas.

El cliente también es responsable de eliminar el bastión una vez finalizada la solución de problemas. El host de bastión expone una superficie de ataque adicional, por lo que Citrix apaga automáticamente la máquina ocho (8) horas después de que se encienda. Sin embargo, Citrix nunca elimina automáticamente un bastión. Si el cliente decide utilizar el bastión durante un período prolongado de tiempo, es responsable de aplicar parches y actualizarlo. Citrix recomienda que un bastión se utilice solo durante unos días antes de eliminarlo. Si el cliente quiere un bastión actualizado, puede eliminar el actual y crear un nuevo bastión, que aprovisionará una nueva máquina con los últimos parches de seguridad.

Acceso RDP En el caso de los catálogos unidos a un dominio, si el emparejamiento de redes virtuales del cliente funciona, dicho cliente puede habilitar el acceso RDP desde su red virtual emparejada a su red virtual administrada por Citrix. Si el cliente utiliza esta opción, es responsable de acceder a los VDA y Cloud Connectors a través del emparejamiento de redes virtuales. Se pueden especificar intervalos de direcciones IP de origen para que el acceso RDP se pueda restringir aún más, incluso dentro de la red interna del cliente. El cliente deberá utilizar credenciales de dominio para iniciar sesión en estas máquinas. Si el cliente está trabajando con Citrix Support para resolver un problema, es posible que tenga que compartir estas credenciales con el personal de asistencia técnica. Una vez resuelto el problema, el cliente es responsable de inhabilitar el acceso RDP. Mantener abierto el acceso RDP desde la red emparejada o local del cliente supone un riesgo para la seguridad.

Credenciales de dominio

Si el cliente elige usar un catálogo unido a un dominio, es responsable de proporcionar a Citrix DaaS para Azure una cuenta de dominio (nombre de usuario y contraseña) con permisos para unir máquinas al dominio. Al suministrar credenciales de dominio, el cliente es responsable de respetar los siguientes principios de seguridad:

- **Auditable:** la cuenta debe crearse específicamente para el uso de Citrix DaaS para Azure, de modo que sea fácil auditar para qué se usa la cuenta.
- **De ámbito limitado:** La cuenta solo requiere permisos para unir máquinas a un dominio. No debe ser un administrador de dominio completo.
- **Seguro:** Debe utilizarse una contraseña segura para la cuenta.

Citrix es responsable del almacenamiento seguro de esta cuenta de dominio en un depósito seguro de Azure (Key Vault) en la suscripción a Azure administrada por Citrix del cliente. La cuenta se recupera solo si una operación requiere la contraseña de la cuenta de dominio.

Más información

Para obtener información relacionada, consulte:

- Guía de implementación segura de la plataforma Citrix Cloud: Información de seguridad relativa a la plataforma Citrix Cloud.
- Información técnica general sobre la seguridad: Información de seguridad relativa a Citrix DaaS
- Third Party Notifications

Suscríbase a Citrix DaaS para Azure

December 22, 2022

Introducción

Puede suscribirse a Citrix DaaS Standard para Azure (anteriormente denominado servicio Citrix Virtual Apps and Desktops Standard para Azure) y solicitar el Fondo de consumo de Citrix Azure, a través de Citrix o Azure Marketplace. Puede evaluar Citrix DaaS para Azure a través de Citrix.

Si actualmente está suscrito a Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials, puede actualizar a Citrix DaaS Standard para Azure.

Un pedido integral se divide en dos partes:

- **Citrix DaaS Standard para Azure:** le permite usar sus propias suscripciones de Azure (administradas por el cliente).
- **Fondo de consumo de Citrix Azure:** además, le permite utilizar una suscripción de Azure administrada por Citrix, además de sus propias suscripciones de Azure. El uso de una suscripción a Azure administrado por Citrix ofrece los siguientes beneficios:
  - Facturación única de Citrix, en lugar de facturas de varias empresas.
  - Diferencias de funciones de suscripción de Azure
  - Asistencia premium de Microsoft a través de Citrix.

El Fondo de consumo de Citrix Azure no es obligatorio. Sin embargo, si no lo tiene, está restringido a usar solo sus propias suscripciones de Azure y no recibe las demás ventajas de las funciones.

El proceso de pedido varía ligeramente en función de si realiza un pedido a través de Citrix o Azure Marketplace:

- Cuando realiza un pedido a través de Citrix, puede solicitar Citrix DaaS Standard para Azure y Citrix Azure Consumption Fund al mismo tiempo.
- Cuando realiza un pedido a través de Azure Marketplace, primero solicita Citrix DaaS Standard para Azure. A continuación, solicite el Fondo de consumo de Citrix Azure.

  Si decide pedir solo Citrix DaaS para Azure, puede solicitar el Fondo de consumo de Citrix Azure más adelante, ya sea a través de Azure Marketplace o a través de su representante de cuentas de Citrix.

Independientemente de dónde pida Citrix DaaS Standard para Azure y el fondo de consumo, Citrix proporciona ayuda para la incorporación. También comprobaremos que Citrix DaaS Standard para Azure se ejecuta y configura correctamente.

Resumen de pedidos

Resumen de los pasos del pedido:

1. Obtenga una cuenta de Citrix Cloud.

   Si ya tiene una cuenta de Citrix Cloud y actualmente está suscrito a Citrix DaaS, consulte Si está suscrito actualmente a Citrix DaaS.

2. Solicite Citrix DaaS Standard para Azure y el fondo de consumo a través de Azure Marketplaceo haga el pedido a través de Citrix

juicios

Citrix DaaS Standard para Azure ofrece dos tipos de pruebas:

- **Aprobado por ventas:** en una prueba aprobada por ventas, puede usar una suscripción de Azure administrada por Citrix para crear catálogos, imágenes y otras tareas. En la versión de prueba, puede convertir a una suscripción de servicio de pago y solicitar el Fondo de consumo administrado de Azure de Citrix. Si no compra el consumo, los recursos que creó con la suscripción de Azure administrado por Citrix se eliminan automáticamente, lo que puede afectar a los usuarios.
- **Aprobado automáticamente:** en una prueba aprobada automáticamente, puede usar su propia suscripción de Azure (administrada por el cliente) para crear catálogos, imágenes y otras tareas. Desde la prueba, puede convertirte en una suscripción de pago. Para obtener más información, consulte Pruebas de servicio aprobadas automáticamente.

Para obtener más información sobre las pruebas, consulte Pruebas de servicios de Citrix Cloud.

Pruebas de servicio aprobadas

- Una prueba aprobada automáticamente de Citrix DaaS Standard para Azure dura 7 días naturales.
- Durante una prueba aprobada automáticamente, puede crear catálogos con su suscripción de Azure. Los catálogos contienen las máquinas que entregan escritorios o aplicaciones.
- Puede crear catálogos con una imagen preparada por Citrix, una imagen que importe de Azure o una imagen que cree en Citrix DaaS Standard para Azure.
- Los usuarios deben configurarse en un proveedor de identidad que admitaCitrix Workspace.
- Puede asignar hasta 25 usuarios a los catálogos en su implementación de prueba. Aunque puede asignar un usuario a más de un catálogo, se permiten un total de 25 usuarios nominales únicos en una implementación de prueba.
- Debe tener una cuenta de usuario de Microsoft Azure y al menos una suscripción de Azure en esa cuenta. (Las pruebas solo admiten casos de uso de suscripción de Azure propiedad del cliente (traiga el suyo propio).)

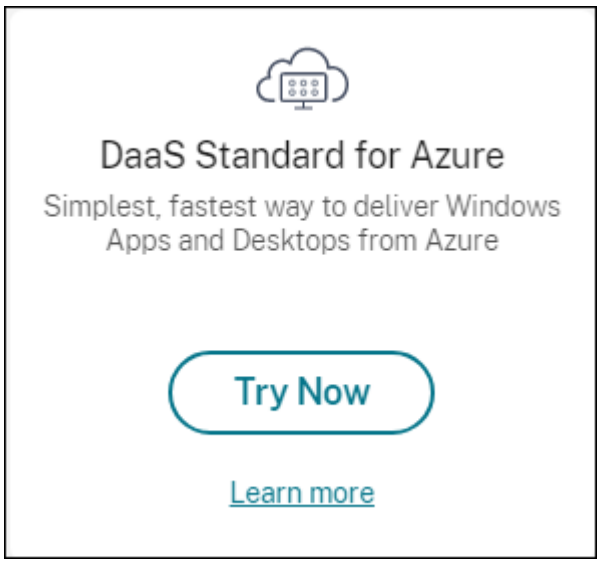
Solicitar y utilizar una prueba de servicio aprobada automáticamente

1. Regístrese para obtener una cuenta de Citrix Cloud (si aún no tiene una).

   a) Vaya a Citrix Cloud.
   b) Selecciona **Registrarse y pruébalo gratis**.
   c) Siga las instrucciones que aparecen en pantalla.

   En unos momentos, recibirá un correo electrónico sobre su cuenta de Citrix Cloud. Selecciona el enlace de inicio de sesión en el correo electrónico.

2. Solicite una prueba. En la consola de Citrix Cloud, seleccione **Probar ahora** en el mosaico **DaaS Standard para Azure**.



Recibirás un correo electrónico cuando la prueba de servicio esté activada y lista (normalmente unas dos horas después de solicitar la prueba).

3. Inicie sesión en Citrix Cloud.
4. Haga clic en **Administrar** en el mosaico **DaaS Standard para Azure**.
5. Configure y configure su entorno de prueba. Durante la configuración, realizarás lo siguiente:

   a) Agregue su suscripción de Azure al servicio.
   b) Conecte su proveedor de identidad a través de la consola de Citrix Cloud.
   c) Cree un catálogo.
   d) Agregue usuarios de su proveedor de identidad al catálogo.
   e) Notifique a los usuarios la URL de Citrix Workspace.

La interfaz gráfica lo guía a través del proceso de configuración. Para obtener más información, consulte la documentación del producto:

- Familiarízate con el producto y su terminología.
- Revisa los resúmenes y los detalles de la configuración.

Obtenga una cuenta de Citrix Cloud

Para registrarse en una cuenta de Citrix Cloud y solicitar una prueba, vaya a https://onboarding.cloud.com. Para obtener más información sobre ese proceso, consulte Inscríbase en Citrix Cloud. Su cuenta tiene un ID de organización (OrgID) que siempre aparece en la esquina superior derecha de la consola de Citrix Cloud.

Próximos pasos: solicite Citrix DaaS Standard para Azure a través de Citrix o Azure Marketplace.

Si actualmente está suscrito a Citrix DaaS

Una cuenta de Citrix Cloud (OrgID) le permite suscribirse a una sola edición de Citrix DaaS a la vez.

Puede actualizar de Citrix DaaS Standard para Azure a cualquiera de las siguientes ediciones:

- Citrix DaaS edición Advanced
- Edición Citrix DaaS Premium.

Póngase en contacto con su representante de Citrix para obtener información

Si actualmente está suscrito a una edición de Citrix DaaS que no sea Advanced o Premium (por ejemplo, Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials) y desea suscribirse a Citrix DaaS Standard para Azure, debe:

- Suscríbase a Citrix DaaS Standard para Azure con una cuenta de Citrix Cloud (OrgID) diferente. Para obtener más información, consulte Actualización a Citrix DaaS Standard para Azure.
- Desactive el servicio que tiene y, a continuación, solicite Citrix DaaS Standard para Azure. Para obtener instrucciones sobre la cancelación de servicios, consulte CTX239027.

Puede usar una suscripción a Citrix Managed Azure comprando Citrix Azure Consumption Fund con cualquiera de las siguientes ediciones de servicio:

- Citrix DaaS Standard para Azure
- Citrix DaaS Advanced
- Citrix DaaS Advanced Plus
- Citrix DaaS Premium

Realizar pedidos a través de Citrix

Puede solicitar Citrix DaaS Standard para Azure (incluido el fondo de consumo) a través de Citrix Cloud o a través de su representante de cuentas de Citrix.

A través de Citrix Cloud:

1. Inicie sesión en Citrix Cloud. Haga clic en **Probar ahora** en el mosaico **DaaS Standard para Azure**. Complete la información solicitada. El texto del mosaico cambia a **Prueba solicitada**.
2. Citrix contacta con usted. Cuando Citrix DaaS Standard para Azure esté disponible para su uso, el texto del mosaico cambia a **Administrar**.
3. Inicie sesión en Citrix Cloud. En el mosaico **DaaS Standard para Azure**, haga clic en **Administrar**. La primera vez que acceda a Citrix DaaS Standard para Azure, se le redirigirá a la página de **bienvenida** de Distribución rápida.

Cancelar una suscripción mensual a través de Citrix

Las suscripciones mensuales se renuevan automáticamente al comienzo de cada mes. Puede usar el panel de Citrix DaaS Standard para Azure para cancelar una suscripción mensual que haya pedido a través de Citrix.

(No puede usar el panel de Citrix DaaS Standard para Azure para cancelar otros tipos de suscripción que haya pedido a través de Citrix o los pedidos realizados a través de Azure Marketplace).

Para cancelar una suscripción mensual:

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
3. En el panel de mandos **Administrar > Distribución rápida de Azure**, expanda **General** a la derecha.
4. Haga clic en **Cancelar suscripción**.
5. Se enumeran sus recursos activos, como catálogos, imágenes y conexiones. En la página se describen las acciones que Citrix realiza durante una cancelación. También le informa de las acciones que debe tomar, si las hay. Indica por qué cancelas el servicio. Opcionalmente, proporcione más comentarios. Cuando haya terminado, haga clic en **Cancelar suscripción**.
6. Confirma que entiendes los términos de la cancelación.

Un banner en el panel de control de Citrix DaaS Standard para Azure indica la recepción de su solicitud de cancelación.

Si cancela la suscripción accidentalmente, póngase en contacto con su representante de ventas de Citrix o socio de Citrix antes de fin de mes para reactivar Citrix DaaS Standard para Azure.

Realizar pedidos a través de Azure Marketplace

Solicite primero Citrix DaaS Standard para Azure y, a continuación, solicite Citrix Azure Consumption Fund.

No puede solicitar el fondo de consumo a menos que haya comprado anteriormente Citrix DaaS Standard para Azure. No puede combinar Citrix DaaS Standard para Azure y el fondo de consumo en un solo pedido.

Citrix DaaS Standard para Azure no se ofrece a través del portal Azure Cloud Solutions Providers. Si es un cliente de asistencia prioritaria o le interesa la asistencia prioritaria, póngase en contacto con su representante de cuentas de Citrix.

Requisitos:

- El OrgID de su cuenta de Citrix Cloud.

  - Si tiene una cuenta de Citrix Cloud, pero no conoce el OrgID, busque en la esquina superior derecha de la consola de Citrix Cloud. También puede consultar el correo electrónico que recibió al crear la cuenta.
  - Si no tiene una cuenta de Citrix Cloud, siga las instrucciones en Obtener una cuenta de Citrix Cloud.

- Una cuenta de Azure y al menos una suscripción a Azure en esa cuenta.

Solicite Citrix DaaS Standard para Azure a través de Azure Marketplace

1. Inicie sesión en Azure Marketplace con las credenciales de su cuenta de Azure.
2. Busque y, a continuación, vaya a **Citrix DaaS Standard para Azure**.
3. Haga clic en **OBTENER AHORA**.
4. En el mensaje **Una cosa más**, active la casilla de verificación y, a continuación, haga clic en **Continuar**.
5. Las fichas contienen información sobre el producto, los planes, los precios y el uso. Cuando esté listo, seleccione un plan (si hay más de uno disponible) y, a continuación, haga clic en **Configurar suscripción +**.
6. En la ficha **Basics**:
   - **Suscripción**: indica el plan que seleccionó.
   - **Nombre**: introduzca un nombre para su pedido de suscripción.
   - La sección **Plan** muestra el precio del plan seleccionado, en función de términos mensuales y plurianuales (anuales).

     Para cambiar el plazo del plan (mensual o anual), selecciona **Cambiar plan**. Selecciona el plazo que quieras y haga clic en **Cambiar plan**.
7. En la ficha **Revisar y suscribirse**:
   - Revise los datos de contacto que proporcionó anteriormente para el perfil básico de Azure. Puede cambiar su dirección, número de teléfono o ambos.
   - Haga clic en **Suscribirse**
8. En la página **Suscripción en curso**, haga clic en **Configurar cuenta ahora**. (Si el botón está desactivado, espere un momento). Va a la página de activación de Citrix.
9. En la página de activación:
   - Use el enlace **Iniciar** sesión para iniciar sesión en Citrix Cloud. Unas credenciales de inicio de sesión correcto rellenan automáticamente el campo **Organization ID**.

- **Quantity:** Introduzca la cantidad de usuarios (un pedido inicial debe ser de al menos 25). Se muestra un precio estimado.
- Acepta los términos y condiciones y, a continuación, haga clic en **Activar pedido**.

Citrix le envía un correo electrónico cuando se haya aprovisionado el servicio. El aprovisionamiento puede llevar un tiempo. Si no recibe el correo electrónico al día siguiente, contacte con Citrix Support.

Cuando reciba el correo electrónico de Citrix, podrá empezar a usar Citrix DaaS Standard para Azure. Recuerde: Con solo Citrix DaaS Standard para Azure, solo puede usar sus propias suscripciones de Azure.

No elimine el recurso Citrix DaaS Standard para Azure en Azure. Al eliminar ese recurso, se cancela la suscripción.

Solicite el fondo de consumo a través de Azure Marketplace

1. Inicie sesión en Azure Marketplace con las credenciales de su cuenta de Azure.
2. Busque y, a continuación, navegue hasta **Citrix Azure Consumption Fund**.
3. Haga clic en **OBTENER AHORA**.
4. Haga clic en **Configurar + suscribirse**.
5. En la página **Suscribirse** :

   - En **Nombre**, introduzca un nombre fácilmente reconocible, como "Mis escritorios administrados". Puede usar este nombre más adelante si quiere cambiar la suscripción al servicio.
   - Indique cuántos usuarios quiere admitir, en el rango de 25 a 100000.
   - Introduzca su dirección de correo electrónico y número de teléfono.

   Cuando haya terminado, haga clic en **Suscribirse**.
6. En la página **Progreso de la suscripción**, cuando el botón **Configurar cuenta SaaS en el sitio del editor** se active (azul), haga clic en él. Se le dirigirá automáticamente a una página de activación de pedidos de Citrix.
7. En la página de activación de pedidos de Citrix, introduzca su OrgID de Citrix Cloud. Se muestra la dirección de correo electrónico que introdujo anteriormente. Puede cambiarlo si es necesario. Cuando termines, haga clic en **Activar pedido**.
8. El cumplimiento de la orden del fondo de consumo no lleva mucho tiempo. Cuando se notifica a Citrix del pedido, aparece un banner en la consola de Citrix DaaS para Azure que indica que se está preparando una suscripción a Citrix Managed Azure.

El panel **Suscripciones a la nube** a la derecha del panel **Administrar > Azure Quick Deploy** indica cuándo la suscripción está lista para su uso.

Aumentar o disminuir las plazas de los usuarios a través Azure Marketplace

Si necesita aumentar los puestos de usuario, cree un nuevo pedido de Azure Marketplace para el número adicional de puestos que quiere.

Para reducir el número de puestos que tiene, cancele Citrix DaaS Standard para Azure en Azure Marketplace y, a continuación, realice un pedido por el número deseado de puestos.

Cancelar Citrix DaaS Standard para Azure o fondo de consumo a través de Azure Marketplace

Para cancelar Citrix DaaS Standard para Azure o el fondo de consumo a través de Azure Marketplace:

1. Inicie sesión en Azure Marketplace.
2. Busque **DaaS**.
3. Seleccione **Nuevo > Vista**.
4. Seleccione el recurso que quiere cancelar.
5. En el menú de puntos suspensivos del recurso, selecciona **Eliminar**.
6. Haga clic en **Sí** en el cuadro de confirmación para reconocer que conoce la directiva de reembolsos y quiere cancelar el recurso.

> **Importante:**
>
> No cancele el Fondo de consumo de Citrix Azure si utiliza recursos administrados por Citrix, como catálogos o imágenes creados en la suscripción de Citrix Managed Azure.

Cuando se aprueba y procesa su pedido

Una vez que se aprueba la prueba o el servicio, aparecen varios mosaicos en la página de inicio de Citrix Cloud:

- Citrix DaaS para Azure
- Citrix DaaS
- Gateway

Citrix DaaS para Azure es el único servicio que está activado para su uso.

Para empezar a usar Citrix DaaS Standard para Azure, inicie sesión en Citrix Cloud. Acceda a Citrix DaaS Standard para Azure mediante uno de los siguientes métodos:

- En el mosaico **DaaS Standard para Azure**, haga clic en **Administrar**.
- En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.

Para obtener instrucciones de configuración, consulte Empezar.

Actualizar la versión a Citrix DaaS Standard para Azure

Si actualmente está suscrito al servicio Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials, actualice a Citrix DaaS Standard para Azure realizando las siguientes tareas.

1. Cree un nuevo ID de organización (OrgID) para usarlo con Citrix DaaS Standard para Azure en https://onboarding.cloud.com/. (Como se describió anteriormente en este artículo, no puede usar el mismo OrgID para suscribirse a más de una edición de Citrix DaaS).
2. Póngase en contacto con Ventas de Citrix para comprar Citrix DaaS Standard para Azure y el Fondo de consumo de Citrix Azure con el nuevo OrgID. (No está obligado a solicitar el fondo de consumo, pero sin él, no puede acceder a todas las funciones de Citrix DaaS Standard para Azure).
3. Inicie sesión en Citrix Cloud. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
4. Agregue al menos una de sus suscripciones de Azure a Citrix DaaS Standard para Azure.
5. Importe una o más imágenes de sus suscripciones de Azure a Citrix DaaS Standard para Azure.
6. Cree catálogoscon las imágenes que importó de sus suscripciones de Azure.
7. Agregue usuarios a los catálogos que ha creado.
8. Si quiere mantener la misma URL de Workspace que usó con Citrix Virtual Apps Essentials o Citrix Virtual Desktops Essentials:

    a) Inicie sesión en Citrix Cloud con el OrgID que usa con el servicio Essentials. Seleccione **Configuración del espacio de trabajo** en el menú superior izquierdo. Cambia la URL de su espacio de trabajo por otra diferente.

    b) Inicie sesión en Citrix Cloud con el OrgID que usa con Citrix DaaS Standard para Azure. Seleccione **Configuración del espacio de trabajo** en el menú superior izquierdo. Cambie la URL del espacio de trabajo por la que utilizó anteriormente para el servicio Essentials.

9. Inicie sesión en Azure y elimine todos los recursos que usó con el servicio Essentials. Para obtener orientación, consulte Cancelar Virtual Apps Essentials. (el procedimiento es el mismo para Citrix Virtual Desktops Essentials).
10. Para detener el servicio de Essentials, elimine el recurso de Azure Marketplace que hay en Azure.

Introducción

September 7, 2022

Este artículo resume las tareas de configuración para entregar escritorios y aplicaciones mediante Citrix Daas Standard para Azure (anteriormente el servicio Citrix Virtual Apps and Desktops Standard para Azure). Le recomendamos que revise cada procedimiento antes de hacerlo realmente, para saber lo que puede esperar.

Para las tareas de configuración de Acceso con Remote PC, consulte Accesocon Remo

> **Importante:**
>
> Para asegurarse de obtener información importante sobre Citrix Cloud y los servicios de Citrix a los que se suscribe, compruebe que recibe todas las notificaciones por correo electrónico. Por ejemplo, Citrix envía correos electrónicos de notificación informativos mensuales en los que se detalla el consumo (uso) de Azure.
>
> En la esquina superior derecha de la consola de Citrix Cloud, expanda el menú situado a la derecha de los campos de nombre del cliente y OrgID. Seleccione **Parámetros de cuenta**. En la ficha **Mi perfil**, seleccione todas las entradas de la sección **Notificaciones por correo electrónico**.

Resumen de tareas de configuración

Las siguientes secciones de este artículo le guían a través de las tareas de configuración:

1. Prepárate para la configuración.
2. Configure una implementación siguiendo las instrucciones en uno de los siguientes puntos:
    - Distribución rápida de prueba de concepto
    - Implementación de producción
3. Proporcione la URL del espacio de trabajo a los usuarios.

Preparar

- Si no está familiarizado con los catálogos, las imágenes, las conexiones de red o las suscripciones de Azure, revise los conceptos introductorios y la información terminológica.
- Lea la descripción general de la seguridad para aprender y comprender de qué son responsables usted (el cliente) y Citrix.
- Si aún no tiene una cuenta de Citrix Cloud que se pueda utilizar para este servicio, obtenga una y, a continuación, regístrese en el servicio.

- Consulte los requisitos del sistema.
- Revise los pasos de configuración: prueba de concepto o producción.

Configurar una implementación rápida de prueba de concepto

Este procedimiento requiere una suscripción a Azure administrado por Citrix.

1. Cree un catálogo con Creación rápida.
2. Agregue los usuarios a Azure AD administrado.
3. Agregue los usuarios al catálogo.
4. Notifique a los usuarios la URL del espacio de trabajo.

Configurar una implementación de producción

1. Si utiliza su propio Active Directory o Azure Active Directory para autenticar a los usuarios, conecte y configure dicho método en Citrix Cloud.
2. Si utiliza máquinas unidas a un dominio, compruebe que tiene entradas válidas del servidor DNS.
3. Si usa su propia suscripción de Azure (en lugar de una suscripción de Azure administrada por Citrix), importe su suscripción de Azure.
4. Cree o importe una imagen. Aunque puede utilizar una de las imágenes preparadas por Citrix tal como está en un catálogo, están diseñadas principalmente para implementaciones de prueba de concepto.
5. Si utiliza una suscripción de Azure administrado por Citrix y quiere que los usuarios puedan acceder a los elementos de la red (como servidores de archivos), configure un emparejamiento de redes virtuales de Azure o una conexión de Citrix SD-WAN.
6. Cree catálogos de manera personalizada.
7. Si piensa crear un catálogo de máquinas multisesión, agregue aplicaciones al catálogo si es necesario.
8. Si utiliza Azure AD administrado por Citrix para autenticar a los usuarios, agregue usuarios al directorio.
9. Agregue usuarios al catálogo.
10. Notifique a los usuarios la URL del espacio de trabajo.

Después de configurar la implementación, use el panel **Supervisar** en Citrix DaaS para Azure para ver el uso del escritorio, las sesionesy las máquinas.

Requisitos del sistema

Para todas las implementaciones:

- **Citrix Cloud:** Este servicio se entrega a través de Citrix Cloud y requiere una cuenta de Citrix Cloud para completar el proceso de incorporación. Para obtener más información, consulte Obtener una cuenta de Citrix Cloud.
- **Licencias de Windows:** Asegúrese de que tiene una licencia adecuada para Servicios de Escritorio remoto para ejecutar cargas de trabajo de Windows Server o Licencias de Azure Virtual Desktop para Windows 10.

Si usa una suscripción a Azure administrado por Citrix:

- **Suscripciones de Azure al usar el interconexión de Azure VNet (opcional):** si planea acceder a los recursos (como AD y otros recursos compartidos de archivos) en su propia red de Azure mediante conexiones de pares de Azure VNet, debe tener una suscripción a Azure.
- **Unir los VDA a Azure Active Directory (opcional):** para unir los VDA a un dominio mediante la directiva de grupo de Active Directory, debe ser un administrador con permiso para realizar esa acción en Active Directory. Para obtener información detallada, consulte Responsabilidad del cliente.

La configuración de las conexiones a la red corporativa local tiene requisitos adicionales.

- Cualquier conexión (emparejamiento de redes virtuales de Azure o SD-WAN): Requisitos para todas las conexiones.
- Conexiones de emparejamiento de redes virtuales de Azure: Requisitos y preparación del emparejamiento de redes virtuales.
- Conexiones SD-WAN: Preparación y requisitos de las conexiones SD-WAN.

Si quiere usar sus propias imágenes de Azure al crear un catálogo, esas imágenes deben cumplir ciertos requisitos antes de importarlas a Citrix DaaS para Azure.

Información adicional:

- Requisitos de conectividad a Internet: Requisitos del sistema y de conectividad.
- Límites de recursos en una implementación de servicios: Límites.

Sistemas operativos compatibles

Al usar una suscripción de Azure administrada por Citrix:

- Windows 7 (VDA debe ser 7.15 LTSR con la actualización acumulativa más reciente)
- Windows 10 de sesión única
- Windows 10 multisesión
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

- Windows Server 2022 (requiere un VDA 2106, como mínimo)
- Red Hat Enterprise Linux y Ubuntu

Al usar una suscripción de Azure administrada por el cliente:

- Windows 7 (VDA debe ser 7.15 LTSR con la actualización acumulativa más reciente)
- Windows 10 Enterprise de sesión única
- Windows 10 Enterprise Virtual Desktop multisesión
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022 (requiere un VDA 2106, como mínimo)
- Red Hat Enterprise Linux y Ubuntu

URL del espacio de trabajo

Después de crear un catálogo y asignar usuarios, notifique a estos dónde pueden encontrar sus escritorios y aplicaciones: la URL del espacio de trabajo. La dirección URL de Workspace es la misma para todos los catálogos y usuarios.

En el panel **Administrar > Implementación rápida de Azure**, vea la URL expandiendo **Acceso y autenticación de usuarios a** la derecha.

Puede cambiar la primera parte de la URL del espacio de trabajo en Citrix Cloud. Para obtener instrucciones, consulte Personalizar la URL del espacio de trabajo.

Obtener ayuda

Revise el artículo Solución de problemas.

Si sigue teniendo problemas con el servicio, abra un tíquet a partir de las instrucciones que aparecen en Cómo obtener ayuda y asistencia técnica.

Crear catálogos

October 7, 2022

Cuando se usa para escritorios y aplicaciones publicados, un catálogo es un grupo de máquinas virtuales idénticas. Cuando implementa escritorios, las máquinas del catálogo se comparten con los

usuarios seleccionados. Al publicar aplicaciones, las máquinas multisesión alojan aplicaciones que se comparten con los usuarios seleccionados.

> **Nota:**
>
> Para obtener información sobre la creación de catálogos de acceso con Remote PC, consulte Acceso con Remote PC.

Tipos de máquina

Un catálogo puede contener uno de los siguientes tipos de máquinas:

- **Estáticas:** El catálogo contiene máquinas estáticas de una sola sesión (también conocidas como escritorios personales, dedicados o persistentes). Estática significa que cuando un usuario inicia un escritorio, ese escritorio "pertenece"a ese usuario. Los cambios que el usuario realice en el escritorio se conservan al cerrar la sesión. Más tarde, cuando ese usuario vuelva a Citrix Workspace e inicie un escritorio, será el mismo escritorio.
- **Aleatorias:** El catálogo contiene máquinas aleatorias de una sola sesión (también conocidas como escritorios no persistentes). Aleatoria significa que, cuando un usuario inicia un escritorio, cualquier cambio que el usuario hace en ese escritorio se descarta después de cerrar la sesión. Más tarde, cuando ese usuario vuelve a Citrix Workspace e inicia un escritorio, podría ser o no el mismo escritorio.
- **Multisesión:** El catálogo contiene máquinas con aplicaciones y escritorios. A cada una de esas máquinas, puede acceder más de un usuario simultáneamente. Los usuarios pueden iniciar un escritorio o aplicaciones desde su espacio de trabajo. Las sesiones de aplicación se pueden compartir. No se permite compartir sesiones entre una aplicación y un escritorio.
  - Al crear un catálogo multisesión, selecciona la carga de trabajo: ligera (como la entrada de datos), media (como aplicaciones de oficina), pesada (como ingeniería) o personalizada. Cada opción representa una cantidad específica de máquinas y sesiones por máquina, que representa la cantidad total de sesiones que el catálogo admite.
  - Si selecciona la carga de trabajo personalizada, selecciona entre las combinaciones disponibles de CPU, RAM y almacenamiento. Escriba el número de máquinas y sesiones por máquina, lo que genera el número total de sesiones admitidas por el catálogo.

Al implementar escritorios, los tipos de máquinas estáticas y aleatorias a veces se denominan "tipos de escritorio".

Formas de crear un catálogo

Existen varias formas de crear y configurar un catálogo:

- **Creación rápida** es la forma más rápida de ponerse en marcha. Usted proporciona información mínima y Citrix DaaS para Azure se encarga del resto. Un catálogo de creación rápida es ideal para un entorno de prueba o para una prueba de concepto.
- **Creación personalizada** ofrece más opciones de configuración que la creación rápida. Es más apta para un entorno de producción que un catálogo de creación rápida.
- Los catálogos de **Acceso con Remote PC** contienen máquinas (normalmente físicas) a las que los usuarios acceden de forma remota. Para obtener información detallada e instrucciones sobre estos catálogos, consulte Acceso con Remote PC.

He aquí una comparación entre la creación rápida y la creación personalizada:

Creación rápida	Creación personalizada
Menos información que proporcionar.	Más información que proporcionar.
Menos opciones para algunas funciones.	Más opciones para algunas funciones.
Autenticación de usuarios de Azure Active Directory administrada por Citrix.	Selección de: Azure Active Directory administrado por Citrix o su Active Directory/Azure Active Directory.
Sin conexión a la red local.	Selección de: Sin conexión a la red local, emparejamiento de redes virtuales de Azure y SD-WAN.
Utiliza una imagen de Windows 10 preparada por Citrix. Esa imagen contiene un VDA de escritorio actual.	Elección de: imágenes preparadas por Citrix, las imágenes que importa de Azure o imágenes que ha creado en Citrix DaaS para Azure a partir de una imagen preparada o importada por Citrix.
Cada escritorio tiene almacenamiento en disco estándar (HDD) de Azure.	Varias opciones de almacenamiento disponibles.
Solo escritorios estáticos.	Escritorios estáticos, aleatorios o multisesión.
No se puede configurar un programa de administración de energía durante la creación. La máquina que aloja el escritorio se apaga cuando finaliza la sesión. (Puede cambiar esta configuración más adelante).	Se puede configurar una programación de administración de energía durante la creación.
Debe utilizar una suscripción de Azure administrado por Citrix.	Puede usar Citrix Managed Azure o su propia suscripción de Azure.

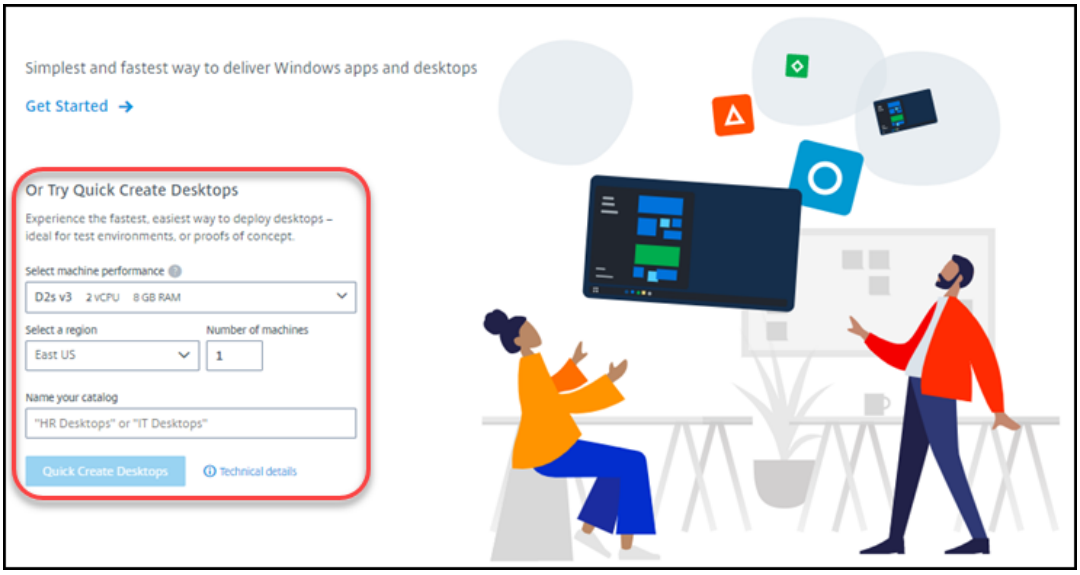
Para obtener más detalles, consulte:

- Crear un catálogo mediante la creación rápida
- Crear catálogos de manera personalizada

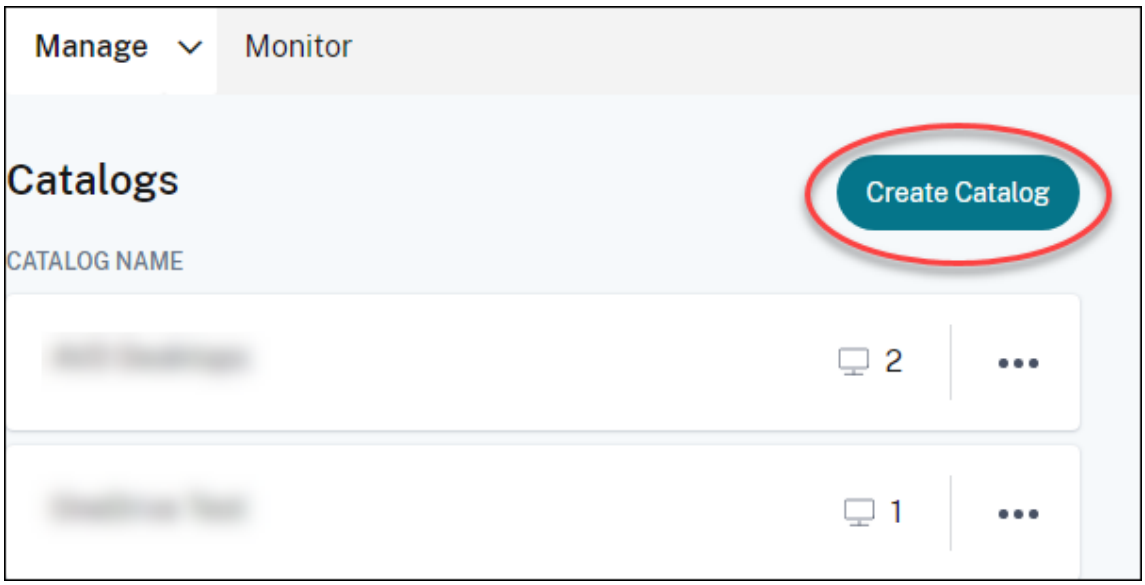
Crear un catálogo mediante la creación rápida

Este método de creación de catálogos siempre usa una suscripción a Azure administrada por Citrix.

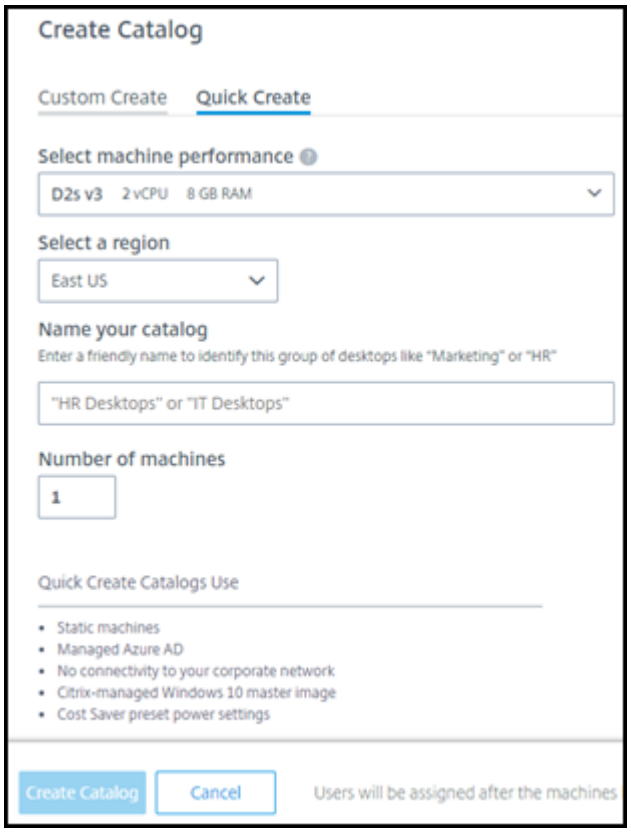
1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
3. Si aún no se ha creado un catálogo, accederá a la página de **bienvenida** de Distribución rápida. Elija una de las siguientes opciones:
   - Configurar el catálogo en esta página. Continúe con los pasos 6 a 10.



   - Haga clic en **Get Started**. Accede al panel **Administrar > Azure Quick Deploy** . Haga clic en **Crear catálogo**.
4. Si ya se ha creado un catálogo (y estás creando otro), accederás al panel **Administrar > Azure Quick Deploy** . Haga clic en **Crear catálogo**.



5. Haga clic en **Creación rápida** en la parte superior de la página, si aún no está seleccionada.



- **Rendimiento de la máquina:** Seleccione el tipo de máquina. Cada opción tiene una combinación única de CPU, RAM y almacenamiento. Las máquinas de mayor rendimiento tienen costes mensuales más altos.
- **Región:** Seleccione la región en la que quiera crear las máquinas. Puede seleccionar una región cercana a los usuarios.

- **Nombre:** Escriba un nombre para el catálogo. Este campo es obligatorio y no hay ningún valor predeterminado.
- **Número de máquinas:** Introduzca la cantidad de máquinas que quiera.

6. Cuando haya terminado, haga clic en **Crear catálogo**. (Si va a crear el primer catálogo desde la página de **bienvenida** de implementación rápida, haga clic en **Creación rápida de escritorios**).

Se le dirigirá automáticamente al panel **Administrar > Azure Quick Deploy** . Mientras se crea el catálogo, el nombre de este se agrega a la lista de catálogos y se indica el progreso en el proceso de creación.

Citrix DaaS para Azure también crea automáticamente una ubicación de recursos y agrega dos Cloud Connectors.

Qué hacer a continuación:

- Si utiliza Citrix Managed Azure AD para la autenticación de usuarios, puede agregar usuarios al directorio mientras se crea el catálogo.
- Independientemente del método de autenticación de usuario que utilice, después de crear el catálogo, agregue usuarios al catálogo.

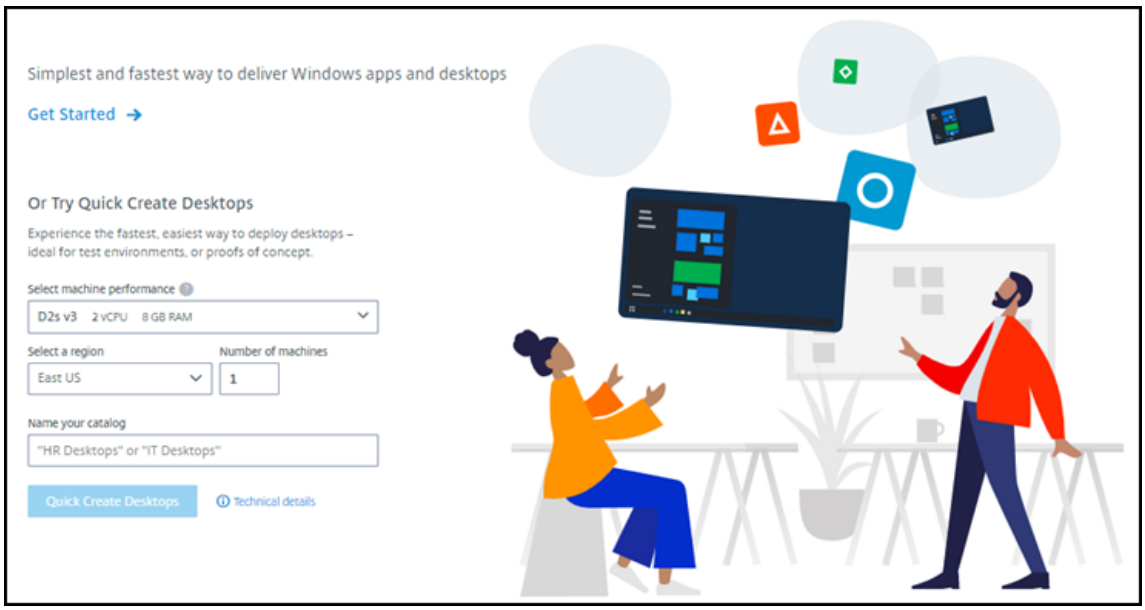
Crear catálogos de manera personalizada

Si utiliza una suscripción a Azure administrado por Citrix y piensa utilizar una conexión a los recursos de red locales, cree una conexión de red antes de crear el catálogo. Para que los usuarios puedan acceder a los recursos locales u otros recursos de red, también necesitará información de Active Directory para esa ubicación.

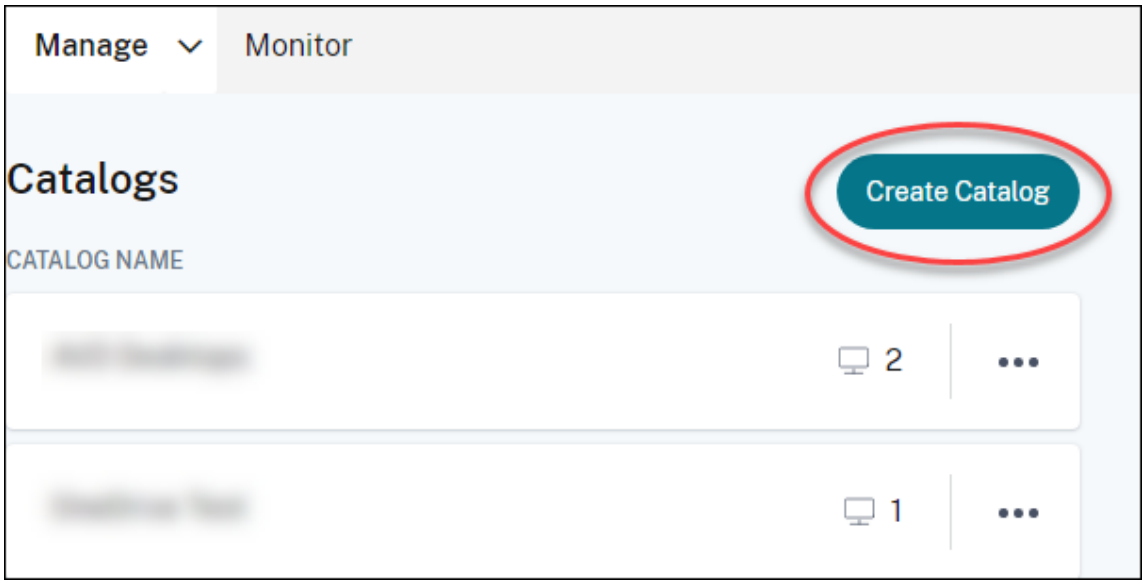
Si no tiene una suscripción a Citrix Managed Azure, debe importar (agregar) al menos una de sus propias suscripciones de Azure a Citrix DaaS para Azure antes de crear un catálogo.

Para crear un catálogo:

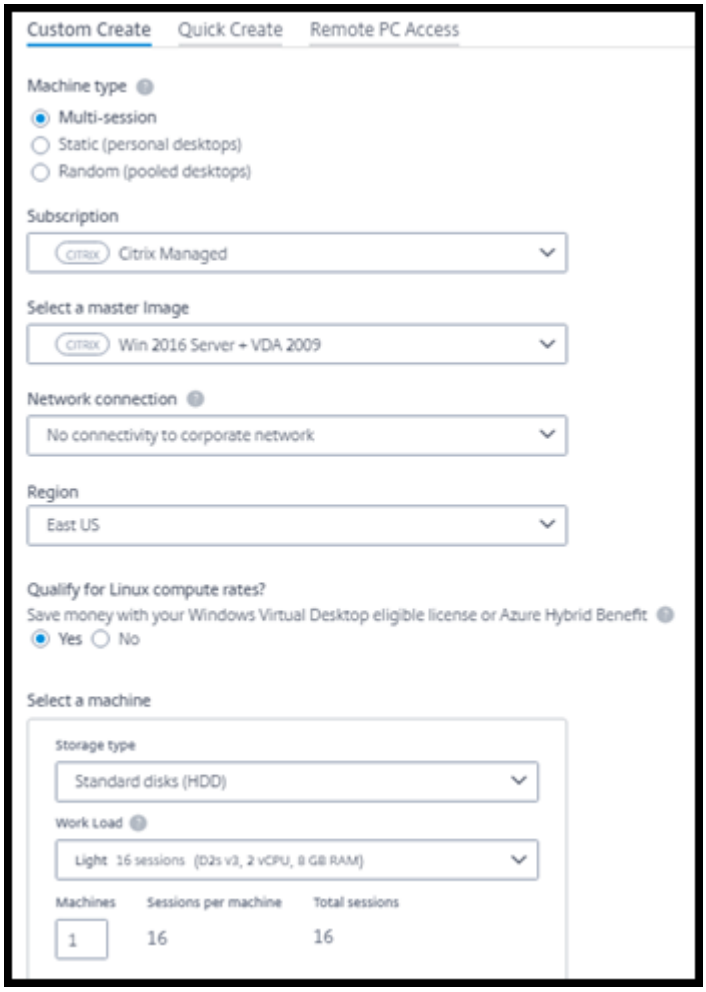
1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
3. Si aún no se ha creado un catálogo, accederá a la página de **bienvenida** de Distribución rápida. Haga clic en **Get Started**. Al final de la página de introducción, accederás al panel **Administrar > Azure Quick Deploy** . Haga clic en **Crear catálogo**.



Si ya se ha creado un catálogo, se le redirigirá al panel **Administrar > Distribución rápida de Azure**. Haga clic en **Crear catálogo**.



4. Seleccione **Creación personalizada** en la parte superior de la página, si la opción aún no está seleccionada.



5. Complete los siguientes campos. (Algunos campos son válidos solo para determinados tipos de máquinas. El orden de los campos puede ser diferente).

   - **Tipo de máquina**. Seleccione un tipo de máquina. Para obtener información detallada, consulte Tipos de máquinas.
   - **Suscripción**. Seleccione una suscripción de Azure. Para obtener más información, consulte Suscripciones de Azure.
   - **Imagen maestra:** seleccione una imagen del sistema operativo. Para obtener más información, consulte Imágenes.
   - **Conexión de red:** seleccione la conexión que se utilizará para acceder a los recursos de la red. Para obtener más información, consulte Conexiones de red.
     - Para una suscripción a Azure administrado por Citrix, las opciones son:
       * **Sin conectividad:** Los usuarios no pueden acceder a ubicaciones y recursos de la red corporativa local.

    * *Conexiones:* Seleccione una conexión, como un emparejamiento de red virtual o una conexión SD-WAN.

  - Para una suscripción de Azure administrada por el cliente, seleccione el grupo de recursos, la red virtual y la subred adecuados.

- **Región:** (Disponible solo si ha seleccionado **Sin conectividad** en **Conexión de red**). Seleccione una región en la que quiera crear los escritorios. Puede seleccionar una región cercana a los usuarios.

  Si seleccionó un nombre de conexión en **Conexión de red**, el catálogo utiliza la región de esa red.

- **¿Apto para las tarifas de proceso de Linux?** (Disponible solo si ha seleccionado una imagen de Windows). Puede ahorrar dinero cuando utiliza una licencia apropiada o Ventaja híbrida de Azure.

  Ventaja de Azure Virtual Desktop: licencias aptas para Windows 10 o Windows 7 por usuario para:

  - Microsoft 365 E3/ES
  - Ventajas de uso de Microsoft 365 A3/AS/Student
  - Microsoft 365 F3
  - Microsoft 365 Business Premium
  - Windows 10 Enterprise E3/E5
  - Windows 10 Education A3/A5
  - VDA de Windows 10 por usuario

  Licencia por usuario o por dispositivo CAL de RDS con Software Assurance para cargas de trabajo de Windows Server.

  Ventaja híbrida de Azure: Licencias de Windows Server con Software Assurance activo o licencias de suscripción aptas equivalentes. Consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/.

- **Máquina:**

  - **Tipo de almacenamiento**. Disco estándar (HDD), SSD estándar o SSD premium.
  - **Rendimiento de la máquina** (para tipo de máquina **estática** o **aleatoria**) o **Carga de trabajo** (para tipo de máquina multisesión). Las alternativas incluyen solo opciones que coinciden con el tipo de generación (gen1 o gen2) de la imagen seleccionada.

    Si selecciona la carga de trabajo personalizada, introduzca la cantidad de máquinas y sesiones por máquina en el campo **Rendimiento de la máquina**.

  - **Máquinas**. Cuántas máquinas quiere en este catálogo.

- **Esquema de nomenclatura de máquinas:**consulte Esquema de denominación de

- **Nombre:** Escriba un nombre para el catálogo. Este nombre aparece en el panel de mandos **Administrar**.
- **Horario de energía:** De forma predeterminada, está seleccionada la casilla de verificación **Lo configuraré más tarde**. Para obtener información detallada, consulte Programaciones de administración de energía

6. Cuando haya terminado, haga clic en **Crear catálogo**.

El panel **Administrar > Azure Quick Deploy** indica cuándo se ha creado el catálogo. Citrix DaaS para Azure también crea automáticamente una ubicación de recursos y agrega dos Cloud Connectors.

Qué hacer a continuación:

- Si aún no lo ha hecho, configure el método de autenticación para que los usuarios se autentiquen en Citrix Workspace.
- Una vez creado el catálogo, agregue usuarios al catálogo.
- Si ha creado un catálogo multisesión, agregue aplicaciones (antes o después de agregar usuarios).

Creación de catálogos de máquinas unidas a un dominio de Azure AD

Puede usar la creación personalizada para crear catálogos de máquinas unidas a Azure Active Directory.

Requisitos

La implementación debe incluir Citrix Cloud Connectors. Machine Creation Services implementa sus Cloud Connectors en función de la información que usted proporciona sobre su dominio de Azure AD al crear un catálogo.

Este tipo de catálogo solo se puede usar para aprovisionar máquinas estáticas o aleatorias. Por el momento, no se admite el aprovisionamiento de máquinas multisesión.

No una la imagen maestra a Azure AD antes de crear un catálogo. Citrix MCS une la imagen maestra a Azure AD cuando se crea el catálogo.

Utilice la versión 2203 o superior del VDA.

En el portal de Azure, asigne la función IAM de inicio de sesión de usuario de máquina virtual a las máquinas virtuales del catálogo. Puede hacerlo de varias maneras:

- Más seguro: si va a crear máquinas estáticas, asigne la función al usuario asignado a la máquina.
- Método alternativo: asigne la función en los grupos de recursos que contienen las máquinas virtuales a todos los usuarios con acceso al catálogo.

- Menos seguro: asigne la función en las suscripciones a todos los usuarios con acceso al catálogo.

Configure la autenticación de Workspace para usar Azure AD que va a unir a las máquinas del catálogo. Para obtener instrucciones, consulte Configurar la autenticación de usuarios en Citrix Cloud.

Para obtener más información sobre los requisitos, los problemas conocidos y las consideraciones, consulte la información sobre las configuraciones de VDA unidas a Azure AD puras en la configuración de VDA unida y no unida al dominio de Azure Active Directory.

Para crear un catálogo

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
3. Seleccione **Administrar > Distribución rápida de Azure**.
4. Si aún no se ha creado un catálogo, se le redirigirá a la página de **bienvenida**. Seleccione **Empiece aquí**. Al final de la página de introducción, accederá al panel **Administrar > Azure Quick Deploy** . Seleccione **Crear catálogo**. Si ya se ha creado un catálogo, se le redirigirá al panel **Administrar > Distribución rápida de Azure**. Seleccione **Crear catálogo**.
5. Seleccione **Creación personalizada** en la parte superior de la página, si la opción aún no está seleccionada.
6. Complete los siguientes campos.
   - **Tipo de máquina.** Seleccione **Estático (escritorios personales)** o **Aleatorio (escritorios agrupados)**.
   - **Suscripción**. Seleccione su suscripción de Azure.
   - **Imagen maestra.** Seleccione una imagen del sistema operativo para utilizarla en las máquinas de los catálogos.
   - **Conexión de red.** Seleccione el grupo de recursos, la red virtual y la subred apropiados.
   - **Configuración de dominios**. Seleccione **Azure Active Directory** como tipo de dominio. Puede que aparezca una advertencia que le recuerde que debe configurar la autenticación de Workspace para usar este Azure AD.
7. Complete el resto del asistente para crear el catálogo.

Parámetros de ubicación de recursos al crear un catálogo

Al crear un catálogo, puede configurar opcionalmente una serie de parámetros de la ubicación de recursos.

Al hacer clic en **Configuración avanzada** en el cuadro de diálogo de creación de catálogos de Distribución rápida, Citrix DaaS para Azure recupera la información de ubicación de recursos.

- Si ya tiene una ubicación de recursos para el dominio y la conexión de red seleccionados para el catálogo, puede guardarla para usarla en el catálogo que está creando.

  Si esa ubicación de recursos solo tiene un Cloud Connector, se instala otro automáticamente. Si lo quiere, puede especificar los parámetros avanzados del Cloud Connector que va a agregar.

- Si no tiene una ubicación de recursos configurada para el dominio y la conexión de red seleccionados para el catálogo, se le pedirá que configure una.

Configurar parámetros avanzados:

- (Obligatorio solo cuando la ubicación de recursos ya está configurada). Nombre para la ubicación de recursos.
- Tipo de conectividad externa: A través del servicio Citrix Gateway o desde la red corporativa.
- Parámetros de Cloud Connector:
  - (Disponible solo cuando se utiliza una suscripción a Azure administrada por el cliente) Rendimiento de la máquina. Esta selección se utiliza para los Cloud Connectors de la ubicación de recursos.
  - (Disponible solo cuando se utiliza una suscripción a Azure administrada por el cliente) Grupo de recursos de Azure. Esta selección se utiliza para los Cloud Connectors de la ubicación de recursos. El valor predeterminado es el grupo de recursos utilizado por última vez por la ubicación de recursos (si procede).
  - Unidad organizativa (OU). El valor predeterminado es la unidad organizativa utilizada por última vez por la ubicación de recursos (si procede).

Cuando haya terminado con la configuración avanzada, haga clic en **Guardar** para volver al cuadro de diálogo de creación del catálogo de Distribución rápida.

Después de crear un catálogo, hay varias acciones disponibles para la ubicación de recursos. Para obtener información detallada, consulte Acciones de ubicaciones de recursos.

Esquema de nomenclatura de máquinas

Para especificar un esquema de nomenclatura de máquinas al crear un catálogo mediante Distribución rápida, seleccione **Especificar esquema de nomenclatura de máquinas**. Utilice entre 1 y 4 comodines (marcas hash) para indicar dónde aparecen los números o letras secuenciales en el nombre. Reglas:

- El esquema de nomenclatura debe contener al menos un comodín, pero no más de cuatro comodines. Todos los comodines deben estar juntos.
- El nombre completo, incluidos los comodines, debe tener entre 2 y 15 caracteres.
- Un nombre no puede incluir espacios en blanco (espacios), barras diagonales, barras invertidas, dos puntos, asteriscos, corchetes angulares, barras verticales, comas, tildes, signos de

exclamación, arrobas, signos de dólar, signos de porcentaje, signos de intercalación, paréntesis, llaves o guiones bajos.
- Un nombre no puede empezar por un punto.
- Un nombre no puede contener solo números.
- No utilice las siguientes letras al final de un nombre: `-GATEWAY`, `-GW` y `-TAC`.

Indique si los valores secuenciales son números (0-9) o letras (A-Z).

Por ejemplo, un esquema de nomenclatura de `PC-Sales-##` (con **0-9** seleccionado) da como resultado cuentas de equipo denominadas `PC-Sales-01`, `PC-Sales-02`, `PC-Sales-03`, etc.

Deje suficiente espacio para que crezca.

- Por ejemplo, un esquema de nomenclatura con 2 comodines y otros 13 caracteres (por ejemplo, `MachineSales-##`) utiliza la cantidad máxima de caracteres (15).
- Una vez que el catálogo contenga 99 máquinas, ocurrirá un error al crear la siguiente máquina. El servicio intenta crear un equipo con tres dígitos (100), pero eso daría lugar a un nombre con 16 caracteres. El máximo es 15.
- Por lo tanto, en este ejemplo, un nombre más corto (por ejemplo `PC-Sales-##`) permite ampliar más allá de 99 máquinas.

Si no especifica un esquema de nombres de máquinas, Citrix DaaS para Azure utiliza el esquema de nombres predeterminado `DAS%%%%%-**-###`.

- `%%%%%` = cinco caracteres alfanuméricos aleatorios que coinciden con el prefijo de la ubicación de recursos
- `**` = dos caracteres alfanuméricos aleatorios para el catálogo
- `###` = tres dígitos.

Información relacionada

- Máquinas unidas a dominios y no unidas aun dominio.
- Catálogos de acceso con Remote PC
- Cree un catálogo en una red que utilice un servidor proxy.
- Muestra la información del catálogo.

Acceso con Remote PC

May 9, 2023

Introducción

> **Nota:**
>
> Este artículo describe cómo configurar el acceso con Remote PC cuando se usa la interfaz de administración de Distribución rápida en Citrix DaaS Standard para Azure (antes denominado servicio de Citrix Virtual Apps and Desktops Standard para Azure). Para obtener información sobre la configuración del acceso con Remote PC cuando se usa la interfaz de administración de configuración completa, consulte Acceso con Remote PC.

Acceso con Remote PC de Citrix permite a los usuarios utilizar de forma remota máquinas físicas Windows o Linux ubicadas en la oficina. Los usuarios disfrutan de la mejor experiencia posible al utilizar Citrix HDX para la entrega de sesiones de PC de oficina.

Acceso con Remote PC admite máquinas unidas a dominios.

Diferencias con respecto a la entrega de escritorios y aplicaciones virtuales

Si está familiarizado con la entrega de escritorios y aplicaciones virtuales, la funcionalidad de acceso con Remote PC presenta varias diferencias:

- Un catálogo de acceso con Remote PC suele contener máquinas físicas. Por lo tanto, no tiene que preparar una imagen ni aprovisionar máquinas para utilizar acceso con Remote PC. La entrega de escritorios y aplicaciones suele utilizar máquinas virtuales (VM), y una imagen sirve de plantilla para aprovisionar estas VM.
- Cuando se apaga una máquina de un catálogo agrupado aleatorio de acceso con Remote PC, no se restablece al estado original de la imagen.
- Para los catálogos de asignación de usuarios estáticos de acceso con Remote PC, la asignación se produce después de que un usuario inicie sesión (ya sea en la máquina o mediante RDP). Al entregar escritorios y aplicaciones, se asigna a un usuario si hay una máquina disponible.

Resumen de instalación y configuración

Revise esta sección antes de iniciar las tareas.

1. Antes de comenzar:
    a) Revise los requisitos y consideraciones.
    b) Complete las tareas de preparación.
2. Desde Citrix Cloud:
    a) Configure una cuenta de Citrix Cloud y suscríbase al servicio Citrix DaaS Standard para Azure.

b) Configure una ubicación de recursos que pueda acceder a los recursos de Active Directory. Instale, al menos, dos Cloud Connectors en la ubicación de recursos Los Cloud Connectors se comunican con Citrix Cloud.

   Siga las instrucciones para crear una ubicación de recursos e instalar Cloud Connectors en ella. Esta información incluye los requisitos del sistema, la preparación y los procedimientos.

c) Conecte Active Directory a Citrix Cloud.

3. Instale Citrix Virtual Delivery Agent (VDA) en cada máquina a la que los usuarios accedan de forma remota. Los agentes VDA se comunican con Citrix Cloud a través de los Cloud Connectors en la ubicación de recursos.
4. Desde la interfaz de administración de Citrix DaaS para Azure Quick Deploy:

   a) Cree un catálogo de acceso con Remote PC. En este procedimiento, especifica la ubicación de la ubicación de los recursos y selecciona el método de asignación de usuarios.
   b) Agregue suscriptores (usuarios) al catálogo, si es necesario. Agregue usuarios a un catálogo si el catálogo utiliza el método de asignación de usuarios "autoasignación estática" o "agrupada aleatoria". No es necesario agregar usuarios a un catálogo de preasignación estática.

5. Envíe la URL del espacio de trabajo a los usuarios. Desde su espacio de trabajo, los usuarios pueden iniciar sesión en sus máquinas de la oficina.

Requisitos y consideraciones

Las referencias a máquinas de esta sección aluden a las máquinas a las que los usuarios acceden de forma remota.

General:

- Las máquinas deben ejecutar un sistema operativo Windows 10 o Linux (Red Hat Enterprise Linux y Ubuntu) de sesión única.
- La máquina debe unirse a un dominio de Active Directory Domain Services.
- Si está familiarizado con el uso del acceso con Remote PC con Citrix Virtual Apps and Desktops, la función Wake-on-LAN no está disponible en Citrix DaaS para Azure.

Red:

- La máquina debe tener una conexión de red activa. Se recomienda una conexión por cable para una mayor fiabilidad y ancho de banda.
- Si utiliza Wi-Fi:

  - Configure los parámetros de energía para dejar encendido el adaptador inalámbrico.
  - Configure el adaptador inalámbrico y el perfil de red para permitir la conexión automática a la red inalámbrica antes de que el usuario inicie sesión. De lo contrario, el VDA no se registra hasta que el usuario inicia sesión. La máquina no está disponible para acceso remoto hasta que un usuario inicia sesión.
  - Asegúrese de que se pueda acceder a los Cloud Connectors desde la red Wi-Fi.

Dispositivos y periféricos:

- Se admiten los siguientes dispositivos:
  - Los conmutadores KVM u otros componentes que pueden desconectar una sesión.
  - Los equipos híbridos, incluidos los equipos portátiles y de sobremesa todo en uno y con NVIDIA Optimus.
  - Máquinas de arranque dual.
- Conecte el teclado y el mouse directamente a la máquina. La conexión al monitor u otros componentes que se pueden apagar o desconectar puede hacer que estos periféricos no estén disponibles. Si tiene que conectar los dispositivos de entrada a componentes como monitores, no apague esos componentes.
- Para portátiles y dispositivos Surface Pro: Asegúrese de que el portátil esté conectado a una fuente de alimentación, en lugar de funcionar con la batería. Configure las opciones de energía del portátil de manera que coincidan con las de una máquina 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.
  - Configure la acción *de presionar el botón de encendido* en **Apagar**.
  - Inhabilite las funciones de ahorro de energía de las tarjetas de vídeo y de las tarjetas de interfaz de red.

  Cuando utilice una base de acoplamiento, puede desacoplar y reacoplar portátiles. Al desacoplar un portátil, el VDA vuelve a registrarse con los Cloud Connectors a través de Wi-Fi. Sin embargo, cuando vuelve a acoplar el portátil, el VDA no cambia para utilizar la conexión por cable hasta que se desconecta el adaptador inalámbrico. Algunos dispositivos ofrecen una funcionalidad integrada para desconectar el adaptador inalámbrico al establecerse una conexión por cable. Otros dispositivos requieren soluciones personalizadas o utilidades de terceros para desconectar el adaptador inalámbrico. Consulte las consideraciones mencionadas anteriormente acerca de las redes Wi-Fi.

  Para habilitar el acoplamiento y el desacoplamiento de dispositivos de acceso con Remote PC:

  - En **Inicio > Configuración > Sistema > Inicio/apagado y suspensión**, establezca **Suspensión** en **Nunca**.

  - En **Administrador de dispositivos > Adaptadores de red > Adaptador Ethernet**, vaya a **Administración de energía** y desmarque la opción **Permitir que el equipo apague este dispositivo para ahorrar energía**. Asegúrese de que la opción **Permitir que este dispositivo reactive el equipo** está seleccionada.

Linux VDA:

- Utilice Linux VDA en máquinas físicas solo en modo no 3D. Debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no se puede oscurecer y muestra las actividades de la sesión cuando el modo HDX 3D está habilitado. Mostrar esta pantalla representa un riesgo para la seguridad.
- Los catálogos con máquinas Linux deben utilizar el método de asignación de usuarios "preasignación estática". Los catálogos con máquinas Linux no pueden utilizar métodos de asignación "preasignación estática"o "agrupada aleatoria".

Consideraciones sobre el espacio de trabajo:

- Varios usuarios con acceso al mismo PC de oficina ven el mismo icono de Citrix Workspace. Cuando un usuario inicia sesión en Citrix Workspace, una máquina aparece como no disponible si otro usuario ya la está utilizando.

Preparar

- Decida cómo quiere instalar el VDA en las máquinas. Existen varios métodos:
  - Instalar manualmente el VDA en cada máquina.
  - Insertar la instalación del VDA con una directiva de grupo, por medio de un script.
  - Haga una instalación de inserción del VDA con una herramienta de distribución electrónica de software (ESD), como Microsoft System Center Configuration Manager (SCCM). Para obtener más información, consulte Instalar agentes VDA mediante SCCM.
- Obtenga información sobre los métodos de asignación de usuarios y decida qué método prefiere utilizar. El método se especifica al crear un catálogo de acceso con Remote PC.
- Decida cómo se registrarán las máquinas (en realidad, los agentes VDA que instala en las máquinas) en Citrix Cloud. Un VDA debe registrarse para establecer comunicaciones con el broker de sesión en Citrix Cloud.

  Los agentes VDA se registran en su ubicación de recursos a través de Cloud Connectors. Puede especificar direcciones de Cloud Connector al instalar un VDA o más tarde.

  Para el primer registro (inicial) de un VDA, Citrix recomienda utilizar un objeto de directiva de grupo (GPO) o un objeto de directiva de grupo local (LGPO) basado en directivas. Tras el registro inicial, Citrix recomienda utilizar la actualización automática, que está habilitada de forma predeterminada. Obtenga más información sobre el registro de VDA.

Instalar un VDA

Descargue e instale un VDA en cada máquina física a la que los usuarios vayan a acceder de forma remota.

Descargar un VDA

- Para descargar Windows VDA:
  1. Con las credenciales de su cuenta de Citrix Cloud, vaya a la página de descargas de Citrix DaaS.
  2. Descargue el VDA más reciente. Hay dos tipos de paquetes de instalación disponibles. Los valores de año y mes del título del VDA varían.
- Para descargar Linux VDA para acceso con Remote PC, siga las instrucciones que se indican en la documentación de Linux VDA.

Tipos de paquetes de instalación de Windows VDA El sitio de descargas de Citrix proporciona dos tipos de paquetes de instalación de Windows VDA que se pueden utilizar con máquinas de acceso con Remote PC:

- Instalador de VDA básico de sesión única (la *versión* es *aamm*): `VDAWorkstationCoreSetup_release.exe`

  El instalador de VDA básico de sesión única está diseñado específicamente para acceso con Remote PC. Es ligero y más fácil de implementar (que otros instaladores de VDA) a través de la red en todas las máquinas. No incluye componentes que normalmente no se necesitan en estas implementaciones, como Citrix Profile Management, Machine Identity Service y la capa de personalización de usuarios.

  Sin embargo, sin Citrix Profile Management instalado, las pantallas de Citrix Analytics for Performance y algunos detalles del monitor no están disponibles. Para obtener más información sobre esas limitaciones, consulte la publicación del blog Monitor and troubleshoot Remote PC Access machines.

  Si quiere tener pantallas de análisis y monitorización completas, utilice el instalador de VDA completo de sesión única.

- Instalador de VDA completo de sesión única (la *versión* es *aamm*): `VDAWorkstationSetup_release.exe`

  Aunque el instalador de VDA completo de sesión única es un paquete más grande que el instalador de VDA básico de sesión única, puede personalizarlo para que instale solo los componentes que necesita. Por ejemplo, puede instalar los componentes que admiten Profile Management.

Instalar Windows VDA para acceso con Remote PC de forma interactiva

1. Haga doble clic en el archivo de instalación de VDA que ha descargado.
2. En la página **Entorno**, seleccione **Habilitar el acceso con Remote PC y, a**continuación, haga clic en **Siguiente**.
3. En la página **Delivery Controller**, seleccione una de las siguientes opciones:

   - Si conoce las direcciones de los Cloud Connectors, seleccione **Hacerlo manualmente**. Introduzca el FQDN de un Cloud Connector y haga clic en **Agregar**. Repita el procedimiento para los demás Cloud Connectors de la ubicación de recursos.
   - Si sabe dónde instaló los Cloud Connectors en la estructura de AD, seleccione **Elegir ubicaciones desde Active Directory** y, a continuación, vaya a esa ubicación. Repita el procedimiento para los demás Cloud Connectors.
   - Si desea especificar las direcciones de Cloud Connector en Directivas de grupo de Citrix, seleccione **Hacerlo más tarde (Avanzado)** y confirme esa selección cuando se le indique.

   Cuando haya terminado, haga clic en **Siguiente**.
4. Si está utilizando el instalador de VDA completo de sesión única, en la página **Componentes adicionales**, seleccione los componentes que quiere instalar, como Profile Management. (Esta página no aparece si utiliza el instalador de VDA básico de sesión única).
5. En la página **Funcionalidades**, haga clic en **Siguiente**.
6. En la página **Firewall**, selecciona **Automáticamente** (si aún no lo está). A continuación, haga clic en **Siguiente**.
7. En la página **Resumen**, haga clic en **Instalar**.
8. En la página **Diagnosticar**, haga clic en **Conectar**. Asegúrese de que la casilla de verificación esté seleccionada. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix Una vez validadas las credenciales, haga clic en **Siguiente**.
9. En la página **Finalizar**, haga clic en **Finalizar**.

Para obtener información detallada sobre la instalación, consulte Instalar agentes VDA.

Instalar Windows VDA para acceso con Remote PC desde una línea de comandos

- Si está utilizando el instalador de VDA básico de sesión única: Ejecute `VDAWorkstationCoreSetup.exe` e incluya las opciones `/quiet`, `/enable_hdx_ports` y `/enable_hdx_udp_ports`. Para especificar direcciones de Cloud Connector, utilice la opción `/controllers`.

  Por ejemplo, el siguiente comando instala un VDA básico de sesión única. La aplicación Citrix Workspace y otros servicios no principales no se instalan. Se especifica el FQDN de dos Cloud

Connectors, y los puertos del servicio Firewall de Windows se abrirán automáticamente. El administrador gestionará los reinicios.

```
VDAWorkstationCoreSetup .exe /quiet /controllers "Connector-East.domain.com"“Connector-East2.domain.com” /enable_hdx_ports /noreboot
```

- Si utiliza el instalador de VDA completo de sesión única y quiere incluir Profile Management (u otros componentes opcionales): Ejecute `VDAWorkstationSetup.exe` e incluya las opciones `/remotepc` y `/includeadditional`. La opción `/remotepc` evita la instalación de la mayoría de los componentes opcionales. La opción `/includeadditional` especifica exactamente qué componentes desea instalar.

  Por ejemplo, el siguiente comando impide la instalación de todos los componentes adicionales opcionales, excepto Profile Management.

  ```
  VDAWorkstationSetup.exe /quiet /remotepc /includeadditional “Citrix User Profile Manager”,“Citrix User Profile Manager WMI Plugin” /controllers “connector.domain.com” “connector2.domain.com” /enable_hdx_ports /noresume /noreboot
  ```

Para obtener información detallada, consulte Opciones de línea de comandos para instalar un VDA.

Instalar Linux VDA

Siga las instrucciones de la documentación de Linux para instalar Linux VDA de forma interactiva o desde la línea de comandos.

Cree un catálogo de acceso con Remote PC

Para poder crear correctamente un catálogo, debe existir una ubicación de recursos que contenga al menos dos Cloud Connectors.

> **Importante:**
>
> Una máquina solo puede pertenecer a un catálogo simultáneamente. Esta restricción no se aplica cuando especifica las máquinas que se van a agregar a un catálogo. Sin embargo, ignorar la restricción puede causar problemas más adelante.

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
3. Si aún no ha creado ningún catálogo, haga clic en **Empezar** en la página de **bienvenida** de Distribución rápida. Si ha creado un catálogo, haga clic en **Crear catálogo** en el panel **Administrar > Azure Quick Deploy** .

4. En la ficha **Acceso con Remote PC**, seleccione un método para asignar usuarios a máquinas.
5. Introduzca un nombre para el catálogo y seleccione la ubicación de recursos que ha creado.
6. Agregue máquinas.
7. Haga clic en **Crear catálogo**.
8. En la página **Se está creando su catálogo de acceso con Remote PC**, haga clic en **Listo**.
9. Aparecerá una entrada para el nuevo catálogo en el panel **Administrar**.

   Una vez que el catálogo se haya creado correctamente, haga clic en uno de los enlaces para agregar suscriptores (usuarios) al catálogo. Este paso se aplica si el catálogo utiliza el método de asignación de usuarios "autoasignación estática"o "grupo aleatorio sin asignar".

Después de crear un catálogo y agregar usuarios (si es necesario), envíe la URL del espacio de trabajo a sus usuarios.

Métodos de asignación de usuarios

El método de asignación de usuarios que elige al crear un catálogo indica cómo se asignan los usuarios a las máquinas.

- **Autoasignación estática:** La asignación de usuarios se produce cuando un usuario inicia sesión en la máquina (sin utilizar Citrix, por ejemplo, en persona o RDP), después de instalar un VDA en la máquina. Más adelante, si otros usuarios inician sesión en esa máquina (sin usar Citrix), también se asignan. Solo un usuario puede utilizar la máquina al mismo tiempo. Esta es una configuración típica para los trabajadores de oficina o los trabajadores por turnos que comparten un equipo.

  Este método es compatible con máquinas Windows. No se puede utilizar con máquinas Linux.

- **Preasignación estática:** Los usuarios están preasignados a máquinas. (Normalmente, esto se configura cargando un archivo CSV que contiene la asignación de usuarios a máquinas.) No es necesario iniciar sesión de usuario para establecer la asignación después de instalar el VDA. Tampoco es necesario asignar usuarios al catálogo una vez creado. Esta opción es mejor para empleados de oficina.

  Este método es compatible con máquinas Windows y Linux.

- **Grupo aleatorio sin asignar:** Los usuarios se asignan aleatoriamente a una máquina disponible. Solo un usuario puede utilizar la máquina al mismo tiempo. Es idóneo para laboratorios informáticos en colegios.

  Este método es compatible con máquinas Windows. No se puede utilizar con máquinas Linux.

Métodos para agregar máquinas a un catálogo

Recuerde: Cada máquina debe tener instalado un VDA.

Al crear o modificar un catálogo, hay tres formas de agregarle máquinas:

- Seleccionar cuentas de máquina una por una.
- Seleccionar unidades organizativas.
- Agregar en bloque mediante un archivo CSV. Hay disponible una plantilla para uso con el archivo CSV.

Agregar nombres de máquinas

Este método agrega cuentas de máquina una por una.

1. Seleccione su dominio.
2. Busque la cuenta de máquina.
3. Haga clic en **Agregar**.
4. Repita el procedimiento para agregar más máquinas.
5. Cuando haya terminado de agregar máquinas, haga clic en **Listo**.

Agregar unidades organizativas

Este método agrega cuentas de máquina según la unidad organizativa en la que residen.
Al seleccionar las unidades organizativas, elija las de menor nivel para obtener mayor granularidad. Si no se requiere una granularidad tan estricta, puede elegir unidades organizativas de nivel superior.

Por ejemplo, en el caso de `Bank`/`Officers`/`Tellers`, seleccione `Tellers` para obtener mayor granularidad. De lo contrario, puede seleccionar `Officers` o `Bank`, en función de los requisitos.

Mover o eliminar unidades organizativas después de que se hayan asignado a un catálogo de acceso con Remote PC afecta a las asociaciones de VDA y genera problemas con futuras asignaciones. Asegúrese de que su plan de cambios de AD tenga en cuenta las actualizaciones de asignaciones de unidades organizativas para los catálogos.

Para agregar unidades organizativas:

1. Seleccione su dominio.
2. Seleccione las unidades organizativas que contienen las cuentas de máquina que quiere agregar.
3. Indique en la casilla de verificación si quiere incluir las subcarpetas presentes en las selecciones.
4. Cuando haya terminado de seleccionar las unidades organizativas, haga clic en **Listo**.

Agregar en bloque

1. Haga clic en **Descargar plantilla CSV**.
2. En la plantilla, agregue la información de la cuenta de máquina (100 entradas como máximo). El archivo CSV también puede contener los nombres de los usuarios asignados a cada máquina.
3. Guarde el archivo.
4. Arrastre el archivo a la página **Agregar máquinas en bloque** o vaya al archivo.
5. Se muestra una vista previa del contenido del archivo. Si ese no es el archivo que quiere, puede crear otro archivo y, a continuación, arrastrarlo o ir hasta él.
6. Cuando haya terminado, haga clic en **Listo**.

Gestionar catálogos de acceso con Remote PC

Para mostrar o cambiar la información de configuración de un catálogo de Acceso con Remote PC, seleccione el catálogo en el panel **Administrar > Azure Quick Deploy** (haga clic en cualquier parte de la entrada).

- En la ficha **Detalles**, puede agregar o quitar máquinas.
- En la ficha **Suscriptores**, puede agregar o quitar usuarios.
- En la ficha **Máquinas**, puede:
  - Agregar o quitar máquinas: Botón **Agregar o quitar máquinas**.
  - Cambiar asignaciones de usuario: icono de papelera **Quitar asignación**, **Modificar asignación de máquinas** en el menú de puntos suspensivos.
  - Consultar qué máquinas están registradas y poner las máquinas en modo de mantenimiento o sacarlas de ese modo.

Suscripciones de Azure

December 28, 2023

Introducción

Citrix DaaS Standard para Azure (anteriormente denominado servicio Citrix Virtual Apps and Desktops Standard para Azure) admite tanto las suscripciones de Azure administrado por Citrix como sus propias suscripciones de Azure administradas por el cliente.

- Para usar sus propias suscripciones a Azure, primero debe importar (agregar) una o más de esas suscripciones a Citrix DaaS para Azure. Esa acción permite a Citrix DaaS para Azure acceder a sus suscripciones de Azure.
- El uso de una suscripción de Azure administrado por Citrix no requiere ninguna configuración de suscripción. Sin embargo, para tener disponible una suscripción a Citrix Managed Azure, debe haber pedido el Fondo de consumo de Citrix Azure (además de Citrix DaaS Standard para Azure).

Cuando crea un catálogo o crea una imagen, elige entre las suscripciones de Azure disponibles.

Algunas funciones del servicio varían en función de si las máquinas están en una suscripción de Azure administrada por Citrix o en su propia suscripción de Azure.

Suscripción a Azure administrado por Citrix	Su propia suscripción a Azure
Compatible con máquinas unidas a un dominio o no unidas a un dominio.	Compatible solo con máquinas unidas a un dominio.
Compatible con catálogos de creación rápida y creación personalizada.	Solo admite catálogos de creación personalizados.
Siempre disponible (y es la selección de suscripción predeterminada) al crear catálogos e imágenes.	Debe agregar la suscripción de Azure a Citrix DaaS para Azure antes de crear un catálogo.
Para la autenticación de usuarios, admite Azure Active Directory administrado por Citrix o su propio Active Directory.	Puede conectar su propio Active Directory y Azure Active Directory.
Las opciones de conexión de red incluyen **Sin conectividad**.	Las opciones de conexión de red incluyen solo sus propias redes virtuales.
Al usar la interconexión de VNet de Azure para conectarse a sus recursos, debe crear una conexión de pares de VNet en Citrix DaaS para Azure.	Seleccione una red virtual existente.
Al importar una imagen desde Azure, especifica el URI de la imagen.	Al importar una imagen, puede seleccionar un VHD o buscar en el almacenamiento en la suscripción de Azure.
Puede crear una máquina bastión en la suscripción a Azure del cliente para solucionar problemas de máquinas.	No es necesario crear una máquina de bastión porque ya puede acceder a las máquinas de su suscripción.

Ver suscripciones

Para ver los detalles de la suscripción, desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha. Luego haga clic en una entrada de suscripción.

- La página **Detalles** incluye el número de máquinas, además de los números y nombres de los catálogos y las imágenes de la suscripción.
- En la página **Ubicaciones de recursos** se enumeran las ubicaciones de recursos en las que se utiliza la suscripción.

Agregar suscripciones de Azure administradas por el cliente

Para usar una suscripción de Azure administrada por el cliente, debe agregarla a Citrix DaaS Standard para Azure antes de crear un catálogo o una imagen que utilice esa suscripción. Tiene dos opciones al agregar las suscripciones de Azure:

- **Si es administrador global del directorio y tiene privilegios de propietario para la suscripción:** Simplemente autentique en su cuenta de Azure.
- **Si no es administrador global y tiene privilegios de propietario en la suscripción:** Antes de agregar la suscripción a Citrix DaaS para Azure, cree una aplicación de Azure en Azure AD y, a continuación, agregue esa aplicación como contribuyente de la suscripción. Cuando agrega esa suscripción a Citrix DaaS para Azure, proporciona información relevante de la aplicación.

Agregar suscripciones de Azure administradas por el cliente si es administrador global

Esta tarea requiere privilegios de administrador global para el directorio y privilegios de propietario para la suscripción.

1. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha.
2. Haga clic en **Agregar suscripción de Azure**.
3. En la página **Agregar suscripciones**, haga clic en **Agregar su suscripción de Azure**.
4. Seleccione el botón que permite a Citrix DaaS para Azure acceder a sus suscripciones de Azure en su nombre.
5. Haga clic en **Autenticar cuenta Azure**. Vaya a la página de inicio de sesión de Azure.
6. Introduzca sus credenciales de Azure.
7. Volverá automáticamente a Citrix DaaS para Azure. En la página **Agregar suscripción** se enumeran las suscripciones de Azure detectadas. Utilice el cuadro de búsqueda para filtrar la lista, si es necesario. Seleccione una o más suscripciones. Cuando haya terminado, haga clic en **Agregar suscripciones**.

8. Confirme que quiere agregar las suscripciones seleccionadas.

Las suscripciones de Azure que ha seleccionado aparecen en la lista cuando expande **Suscripciones**. Las suscripciones agregadas están disponibles para su selección al crear un catálogo o una imagen.

Agregue suscripciones de Azure administradas por el cliente si no es administrador global

Agregar una suscripción de Azure cuando no es un administrador global es un proceso de dos partes:

- Antes de agregar una suscripción a Citrix DaaS para Azure, cree una aplicación en Azure AD y, a continuación, agregue esa aplicación como colaborador de la suscripción.
- Agregue la suscripción a Citrix DaaS for Azurecon información sobre la aplicación que creó en Azure.

Crear una aplicación en Azure AD y agregarla como colaborador

1. Registre una nueva aplicación en Azure AD:
    a) En un explorador web, vaya a https://portal.azure.com.
    b) En el menú superior izquierdo, seleccione **Azure Active Directory**.
    c) En la lista **Administrar**, haga clic en **Registros de aplicaciones**.
    d) Haga clic en **+ Nuevo registro**.
    e) En la página **Registrar una aplicación**, proporcione la siguiente información:
        - **Nombre:** Introduzca el nombre de la conexión
        - **Tipo de aplicación:** Seleccione **aplicación web/API**
        - **URI de redirección:** Déjelo en blanco
    f) Haga clic en **Crear**.
2. Cree la clave de acceso secreta de la aplicación y agregue la asignación de roles:
    a) En el procedimiento anterior, seleccione **Registro de aplicaciones** para ver los detalles.
    b) Anote el **ID de aplicación** y el **ID de directorio**. Lo usará más adelante cuando agregue su suscripción a Citrix DaaS para Azure.
    c) En **Administrar**, seleccione **Certificados y secretos**.
    d) En la página **Secretos del cliente**, seleccione **+ Nuevo secreto de cliente**.
    e) En la página **Agregar secreto de cliente**, proporcione una descripción y seleccione un intervalo de caducidad. A continuación, haga clic en **Agregar**.

f) Anote el valor del secreto de cliente. Lo usará más adelante cuando agregue su suscripción a Citrix DaaS para Azure.

g) Seleccione la suscripción de Azure que desea vincular (agregar) a Citrix DaaS para Azure y, a continuación, haga clic en **Control de acceso (IAM)**.

h) En el cuadro **Agregar una asignación de funciones**, haga clic en **Agregar**.

i) En la ficha **Agregar asignación de roles**, seleccione lo siguiente:

- **Rol:** Colaborador
- **Asignar acceso a:** Usuario, grupo o entidad de servicio de Azure AD
- **Seleccionar:** El nombre de la aplicación de Azure que creó anteriormente.

j) Haga clic en **Guardar**.

Agregue su suscripción a Citrix DaaS para Azure Necesitará el identificador de aplicación, el identificador de directorio y el valor secreto de cliente de la aplicación que creó en Azure AD.

1. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha.
2. Haga clic en **Agregar suscripción de Azure**.
3. En la página **Agregar suscripciones**, haga clic en **Agregar sus suscripciones de Azure**.
4. Seleccione **Tengo una aplicación de Azure con rol de colaborador para la suscripción**.
5. Introduzca el ID de arrendatario (ID de directorio), el ID de cliente (ID de aplicación) y el secreto de cliente de la aplicación que creó en Azure.
6. Haga clic en **Seleccionar su suscripción** y, a continuación, selecciona la suscripción que deseas.

Más adelante, desde la página **Detalles** de la suscripción en el panel de control de Citrix DaaS para Azure, puede actualizar el secreto del cliente o reemplazar la aplicación de Azure desde el menú de puntos suspensivos.

Si Citrix DaaS para Azure no puede acceder a una suscripción de Azure después de agregarla, no se permiten varias acciones de administración de energía de catálogo ni de máquinas individuales. Un mensaje ofrece una opción para agregar de nuevo la suscripción. Si la suscripción se agregó originalmente mediante una aplicación de Azure, puede reemplazar esa aplicación.

Agregar suscripciones de Azure administrado por Citrix

Una suscripción a Azure administrado por Citrix admite la cantidad de máquinas que se indica en Límites. (En este contexto, *máquinas* se refiere a las máquinas virtuales que tienen instalado un VDA de Citrix. Estas máquinas entregan aplicaciones y escritorios a los usuarios. No incluye otras máquinas de una ubicación de recursos, como Cloud Connectors.)

Si es probable que la suscripción de Azure administrado por Citrix alcance su límite pronto y tiene suficientes licencias de Citrix, puede solicitar otra suscripción de Azure administrado por Citrix. El panel de mandos incluye una notificación cuando se acerca al límite.

No puede crear un catálogo (ni agregar máquinas a un catálogo) si el número total de máquinas para todos los catálogos que usan esa suscripción a Azure administrada por Citrix superaría el valor indicado en Límites.

Asumamos, por ejemplo, un límite hipotético de 1000 máquinas por suscripción de Azure administrado por Citrix.

- Supongamos que tiene dos catálogos (`Cat1` y `Cat2`) que usan la misma suscripción a Azure administrado por Citrix. `Cat1` tiene actualmente 500 máquinas y `Cat2` tiene 250.
- A medida que planifica las necesidades de capacidad futuras, agrega 200 máquinas a `Cat2`. La suscripción a Azure administrado por Citrix admite ahora 950 máquinas (500 en `Cat 1` y 450 en `Cat 2`). El panel indica que la suscripción se acerca a su límite.
- Cuando necesite 75 máquinas más, no podrá usar esa suscripción para crear un catálogo con 75 máquinas (ni agregar 75 máquinas a un catálogo existente). Eso superaría el límite de suscripción. En su lugar, deberá solicitar otra suscripción de Azure administrado por Citrix. A continuación, podrá crear un catálogo mediante esa suscripción.

Cuando tiene más de una suscripción a Azure administrado por Citrix:

- No se comparte nada entre esas suscripciones.
- Cada suscripción tiene un nombre único.
- Puede elegir entre las suscripciones de Azure administrado por Citrix (y cualquier suscripción de Azure administrado por el cliente que haya agregado) al:
  - Crear un catálogo.
  - Crear o importar una imagen.
  - Crear un emparejamiento de redes virtuales o una conexión SD-WAN.

Requisito:

- Debe tener suficientes licencias de Citrix para argumentar la agregación de otra suscripción a Azure administrado por Citrix. Con el ejemplo hipotético anterior, si tiene 2000 licencias de Citrix en previsión de implementar al menos 1500 máquinas mediante suscripciones administradas por Citrix, puede agregar otra suscripción de Azure administrado por Citrix.

Para agregar una suscripción de Azure administrada por Citrix:

1. Póngase en contacto con su representante de Citrix para solicitar otra suscripción a Azure administrado por Citrix. Se le notificará cuándo puede proseguir.

2. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha.
3. Haga clic en **Agregar suscripción de Azure**.
4. En la página **Agregar suscripciones**, haga clic en **Agregar una suscripción de Azure administrada por Citrix**.
5. En la página **Agregar una suscripción administrada de Citrix**, haga clic en **Agregar suscripción** en la parte inferior de la página.

Si se le notifica que se ha producido un error durante la creación de una suscripción a Azure administrado por Citrix, póngase en contacto con Citrix Support.

Quitar suscripciones a Azure

Para eliminar una suscripción de Azure, primero debe eliminar todos los catálogos e imágenes que la utilizan.

Si tiene una o más suscripciones de Azure administrado por Citrix, no puede eliminarlas todas. Al menos debe quedar una.

1. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha.
2. Haga clic en la entrada de suscripción.
3. En la ficha **Detalles**, haga clic en **Eliminar suscripción**.
4. Haga clic en **Autenticar cuenta Azure**. Vaya a la página de inicio de sesión de Azure.
5. Introduzca sus credenciales de Azure.
6. Volverá automáticamente a Citrix DaaS para Azure. Confirme la eliminación en las casillas de verificación y, a continuación, haga clic en **Sí, eliminar suscripción**.

Conexiones de red

May 9, 2023

Introducción

En este artículo se proporcionan detalles sobre varios casos de implementación cuando se usa una suscripción a Azure administrado por Citrix.

Al crear un catálogo, debe indicar si los usuarios acceden a las ubicaciones y los recursos de su red local corporativa desde sus escritorios y aplicaciones Citrix DaaS Standard para Azure (anteriormente Citrix Virtual Apps and Desktops Standard para Azure) y cómo lo hacen.

Al utilizar una suscripción de Azure administrado por Citrix, las opciones son las siguientes:

- Sin conectividad
- Emparejamiento de redes virtuales de Azure
- SD-WAN

Al usar una de sus propias suscripciones de Azure administradas por el cliente, no es necesario crear una conexión a Citrix DaaS para Azure. Solo tiene que agregar la suscripción de Azure a Citrix DaaS para Azure.

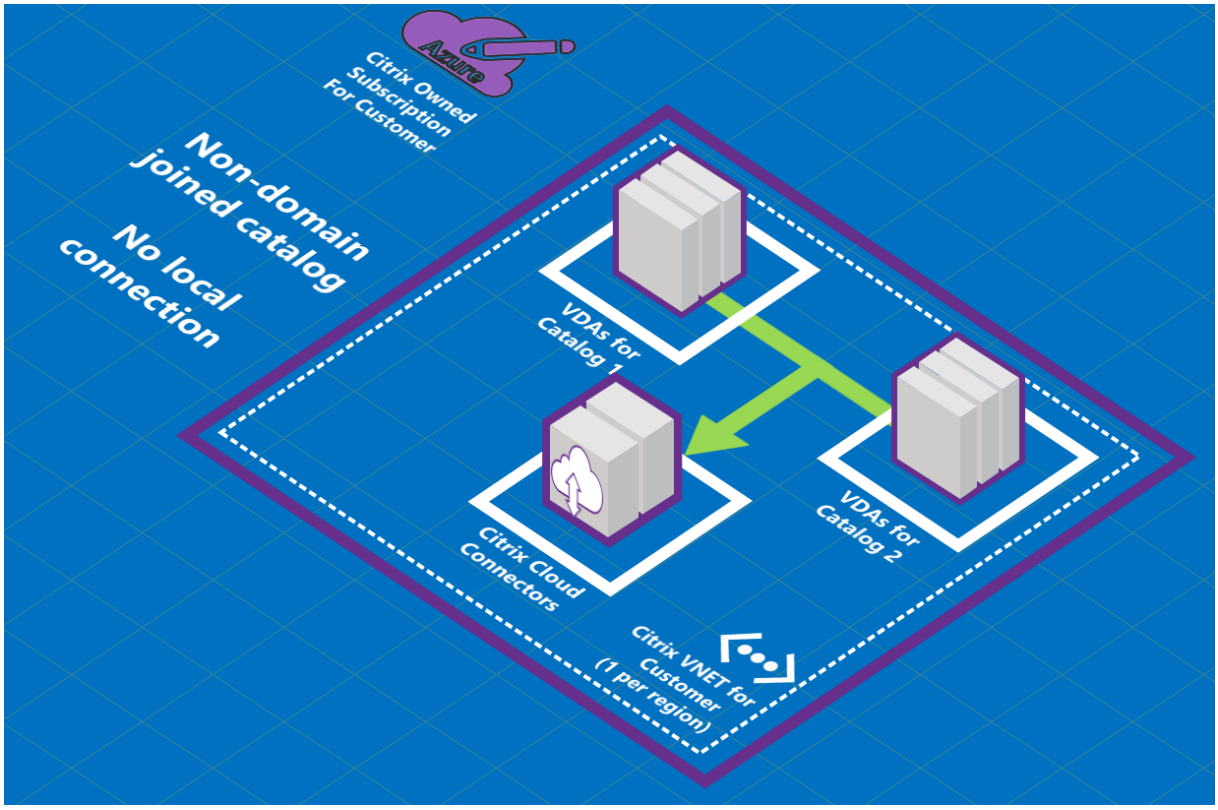
El tipo de conexión de un catálogo no se puede cambiar después de crearlo.

Requisitos para todas las conexiones de red

- Al crear una conexión, debe tener entradas de servidor DNS válidas.
- Al usar DNS seguro o un proveedor de DNS de terceros, debe agregar el rango de direcciones asignado para que lo use Citrix DaaS para Azure a las direcciones IP del proveedor de DNS en la lista de permitidos. Ese intervalo de direcciones se especifica al crear una conexión.
- Todos los recursos del servicio que utilizan la conexión (máquinas unidas a un dominio) deben poder llegar al servidor NTP para garantizar la sincronización horaria.

Sin conectividad

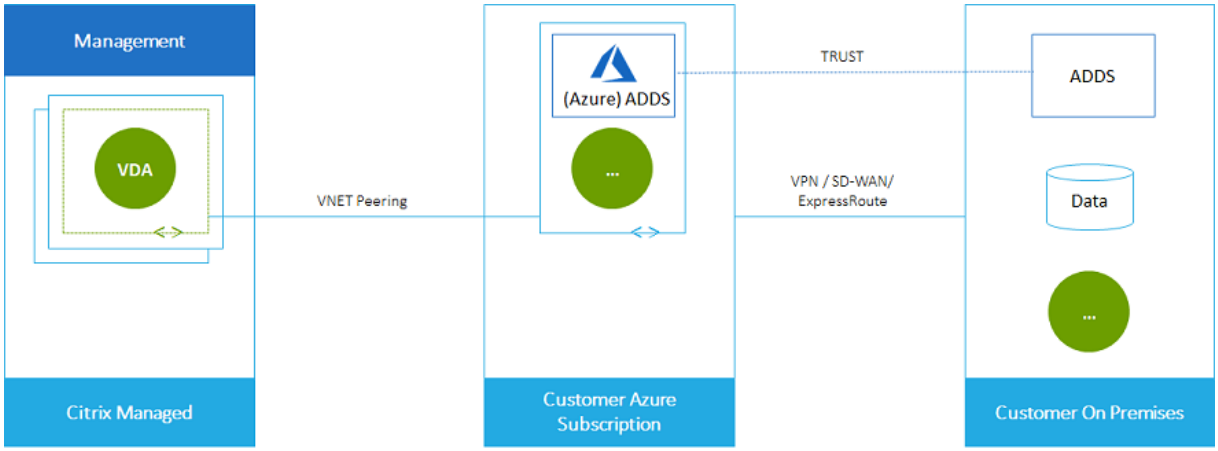
Cuando un catálogo se configura como **Sin conectividad**, los usuarios no pueden acceder a los recursos de sus redes locales o de otras redes. Esta es la única opción para crear un catálogo mediante creación rápida.



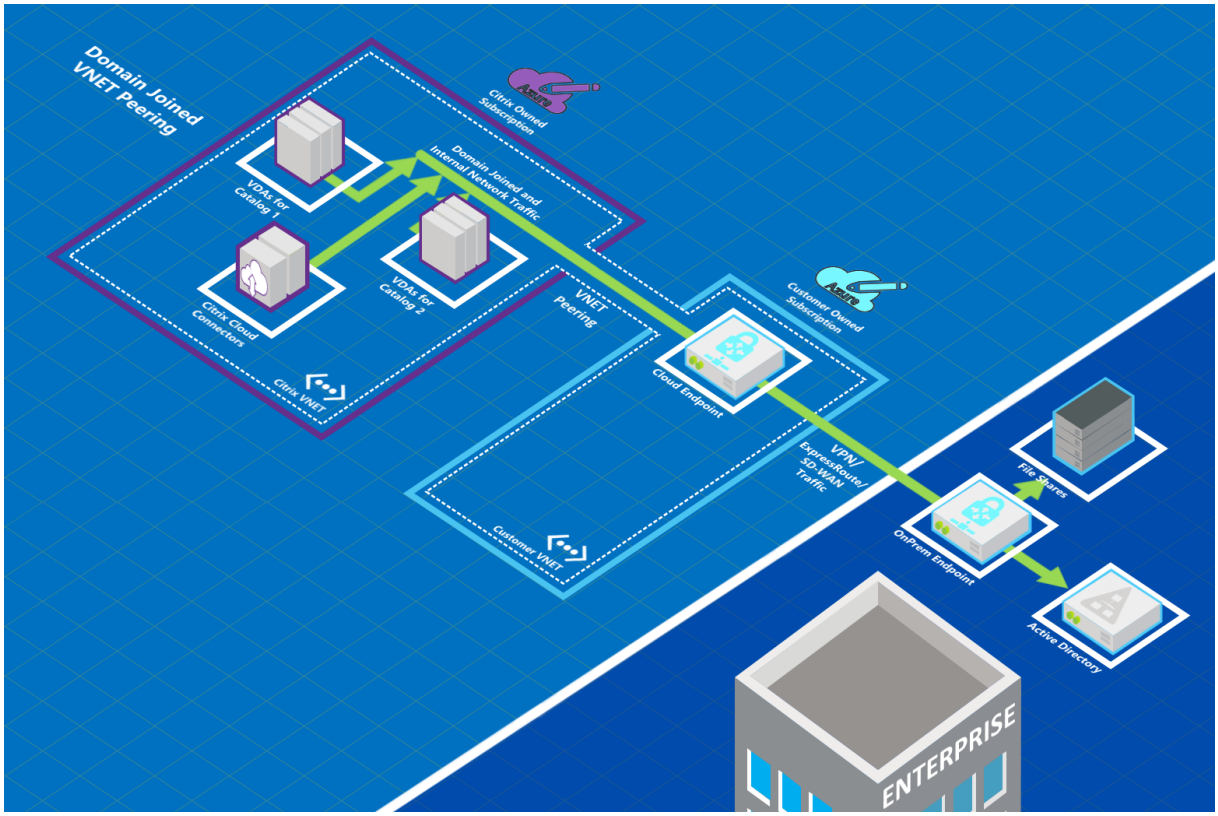
Acerca de las conexiones de emparejamiento de redes virtuales de Azure

La interconexión de redes virtuales conecta sin problemas dos redes virtuales de Azure (VNet): la suya y la de Citrix DaaS para Azure VNet. El emparejamiento también permite a los usuarios acceder a archivos y otros elementos de las redes locales.

Como se muestra en el siguiente gráfico, se crea una conexión mediante el emparejamiento de redes virtuales de Azure desde la suscripción de Azure administrado por Citrix a la red virtual de la suscripción a Azure de su empresa.



Esta es otra ilustración del emparejamiento de redes virtuales.



Los usuarios pueden acceder a sus recursos de red locales (como los servidores de archivos) uniéndose al dominio local al crear un catálogo. (Es decir, usted une al dominio de AD donde residen los recursos compartidos de archivos y otros recursos necesarios). Su suscripción a Azure se conecta a esos recursos (en los gráficos, mediante una VPN o Azure ExpressRoute). Al crear el catálogo, proporciona el dominio, la unidad organizativa y las credenciales de cuenta.

> **Importante:**
>
> - Obtenga información sobre la interconexión de VNet antes de utilizarla en Citrix DaaS para Azure.
> - Cree una conexión de emparejamiento de redes virtuales antes de crear un catálogo que la utilice.

Rutas personalizadas de emparejamiento de redes virtuales de Azure

Las rutas personalizadas o definidas por el usuario invalidan las rutas de sistema predeterminadas de Azure para dirigir el tráfico entre máquinas virtuales en un emparejamiento de redes virtuales, redes locales e Internet. Puede usar rutas personalizadas si hay redes a las que se espera que accedan los recursos de Citrix DaaS para Azure, pero que no están conectadas directamente a través de la interconexión de VNet. Por ejemplo, podría crear una ruta personalizada que fuerce el tráfico a través de

un dispositivo de red hacia Internet o hacia una subred de red local.

Para utilizar rutas personalizadas:

- Debe tener una puerta de enlace de red virtual de Azure existente o un dispositivo de red como Citrix SD-WAN en su entorno de Citrix DaaS para Azure.
- Cuando agrega rutas personalizadas, debe actualizar las tablas de rutas de su empresa con la información de la VNet de destino de Citrix DaaS para Azure para garantizar la conectividad de extremo a extremo.
- Las rutas personalizadas se muestran en Citrix DaaS para Azure en el orden en que se introducen. Este orden de presentación no afecta al orden en que Azure selecciona las rutas.

Antes de utilizar rutas personalizadas, revise el artículo Enrutamiento del tráfico de redes virtuales de Microsoft para obtener información sobre el uso de rutas personalizadas, los tipos de próximo salto y cómo selecciona Azure las rutas para el tráfico de salida.

Puede agregar rutas personalizadas al crear una conexión de pares de Azure VNet o a las existentes en su entorno de Citrix DaaS para Azure. Cuando esté listo para utilizar rutas personalizadas con el emparejamiento de redes virtuales, consulte las siguientes secciones de este artículo:

- Para rutas personalizadas con nuevos emparejamientos de redes virtuales de Azure: Cree una conexión de emparejamiento de redes virtuales de Azure
- Para rutas personalizadas con emparejamientos existentes de redes virtuales de Azure: Administre rutas personalizadas para conexiones de pares existentes de redes virtuales de Azure

Requisitos y preparación del emparejamiento de redes virtuales de Azure

- Credenciales del propietario de una suscripción de Azure Resource Manager. Debe ser una cuenta de Azure Active Directory. Citrix DaaS para Azure no admite otros tipos de cuentas, como live.com o cuentas externas de Azure AD (en un arrendatario diferente).
- Una suscripción de Azure, un grupo de recursos y una red virtual (VNet).
- Configure las rutas de red de Azure para que los VDA de la suscripción a Azure administrado por Citrix puedan comunicar con sus ubicaciones de red.
- Abra los grupos de seguridad de red de Azure desde su red virtual al intervalo de direcciones IP especificado.
- **Active Directory:** Para los casos en que se haya unido a un dominio, se recomienda tener algún tipo de servicios de Active Directory activo en la red virtual interconectada. Esto aprovecha las funciones de baja latencia de la tecnología de emparejamiento de redes virtuales de Azure.

  Por ejemplo, la configuración podría incluir Azure Active Directory Domain Services (AADDS), una máquina virtual de controlador de dominio en la red virtual o Azure AD Connect a Active Directory local.

Después de habilitar AADDS, no podrá mover el dominio administrado a otra red virtual sin eliminar el dominio administrado. Por lo tanto, es importante seleccionar la red virtual correcta para habilitar el dominio administrado. Antes de continuar, revise el artículo de Microsoft Networking considerations para Azure AD Domain Services.

- **Intervalo de direcciones IP de la red virtual:** Al crear la conexión, debe proporcionar un espacio de direcciones CIDR disponible (dirección IP y prefijo de red) que sea exclusivo entre los recursos de red y las redes virtuales de Azure que se están conectando. Este es el rango de IP asignado a las máquinas virtuales dentro de la VNet pareada de Citrix DaaS para Azure.

  Asegúrese de especificar un intervalo de direcciones IP que no se superponga a ninguna dirección que utilice en redes de Azure y locales.

  - Por ejemplo, si la VNet de Azure tiene un espacio de direcciones de 10.0.0.0 /16, cree la conexión de pares de VNet en Citrix DaaS para Azure como 192.168.0.0 /24.
  - En este ejemplo, crear una conexión de emparejamiento con un intervalo de direcciones IP 10.0.0.0 /24 se consideraría un intervalo de direcciones superpuesto.

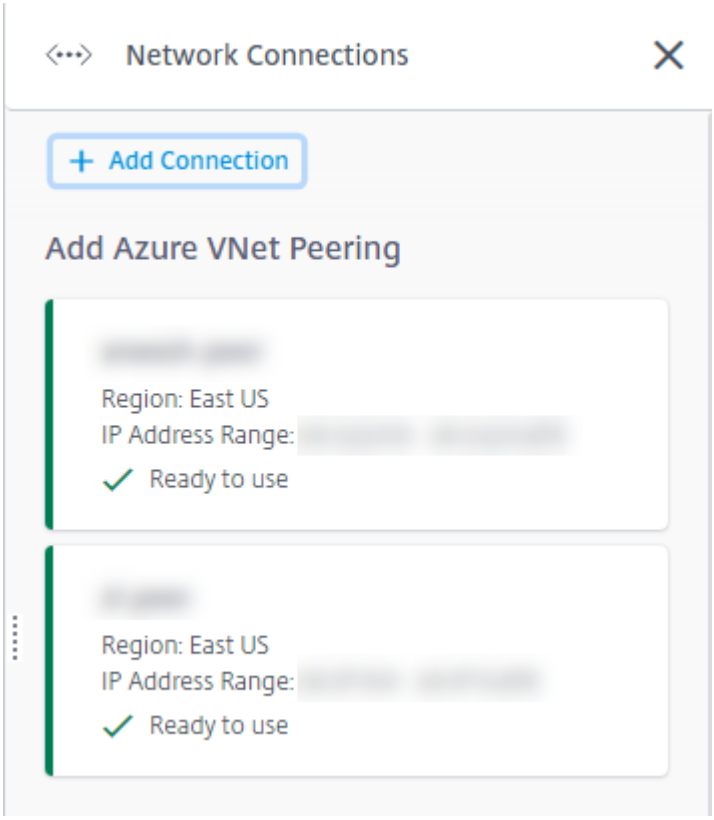
  Si las direcciones se superponen, es posible que la conexión de emparejamiento de redes virtuales no se cree correctamente. Tampoco funcionará correctamente para las tareas de administración del sitio.

Para obtener más información sobre el emparejamiento de redes virtuales, consulte los siguientes artículos de Microsoft.

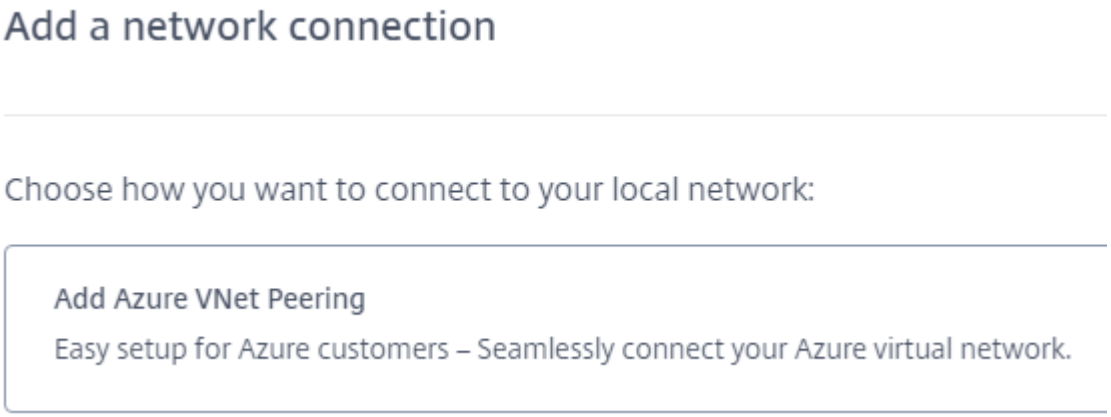
- Emparejamiento de redes virtuales
- Azure VPN Gateway
- Crear una conexión de sitio a sitio en Azure Portal
- Preguntas frecuentes de VPN Gateway (busque "superposición")

Crear una conexión de emparejamiento de redes virtuales de Azure

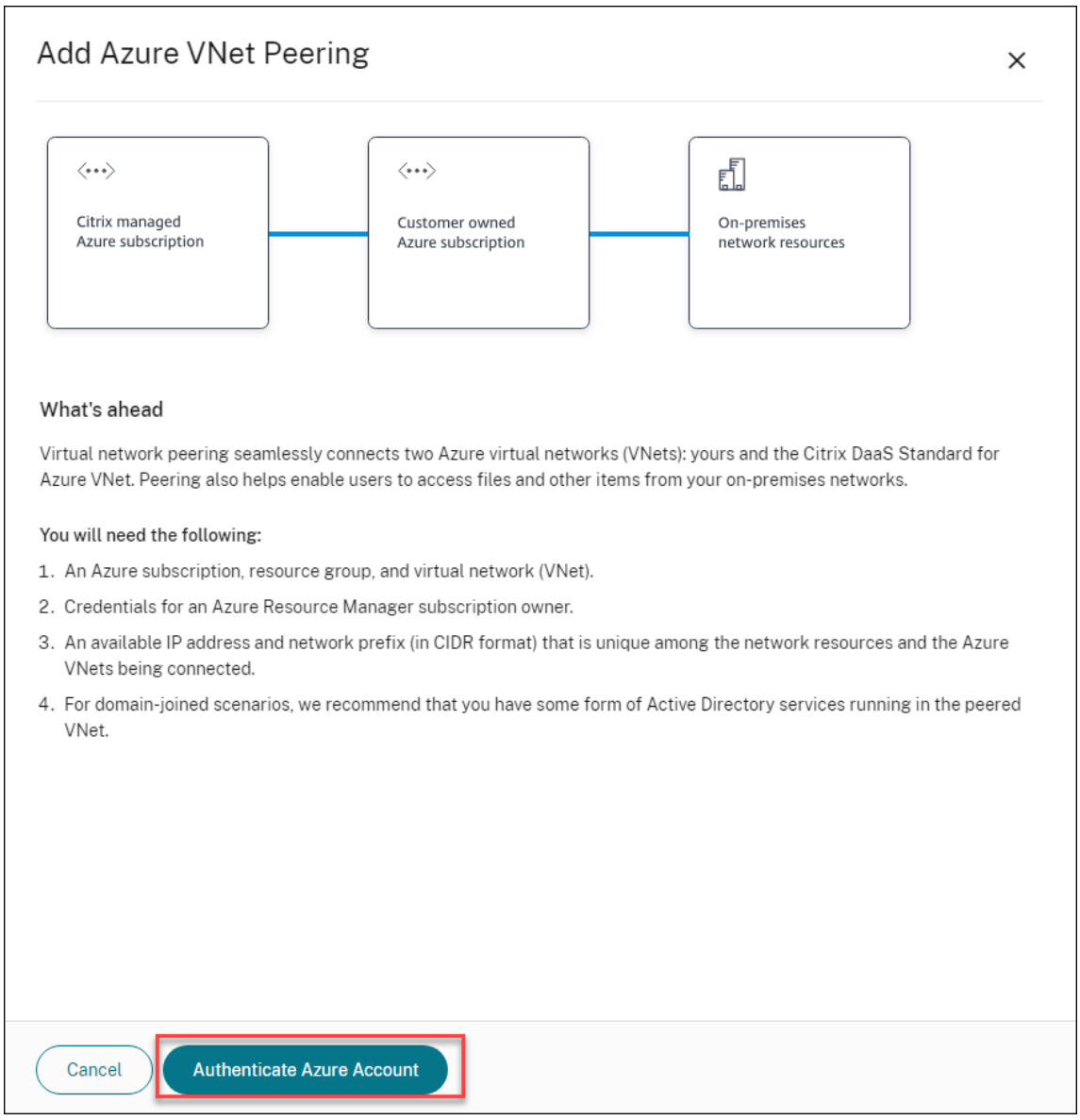
1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha. Si ya ha configurado conexiones, aparecerán en la lista.



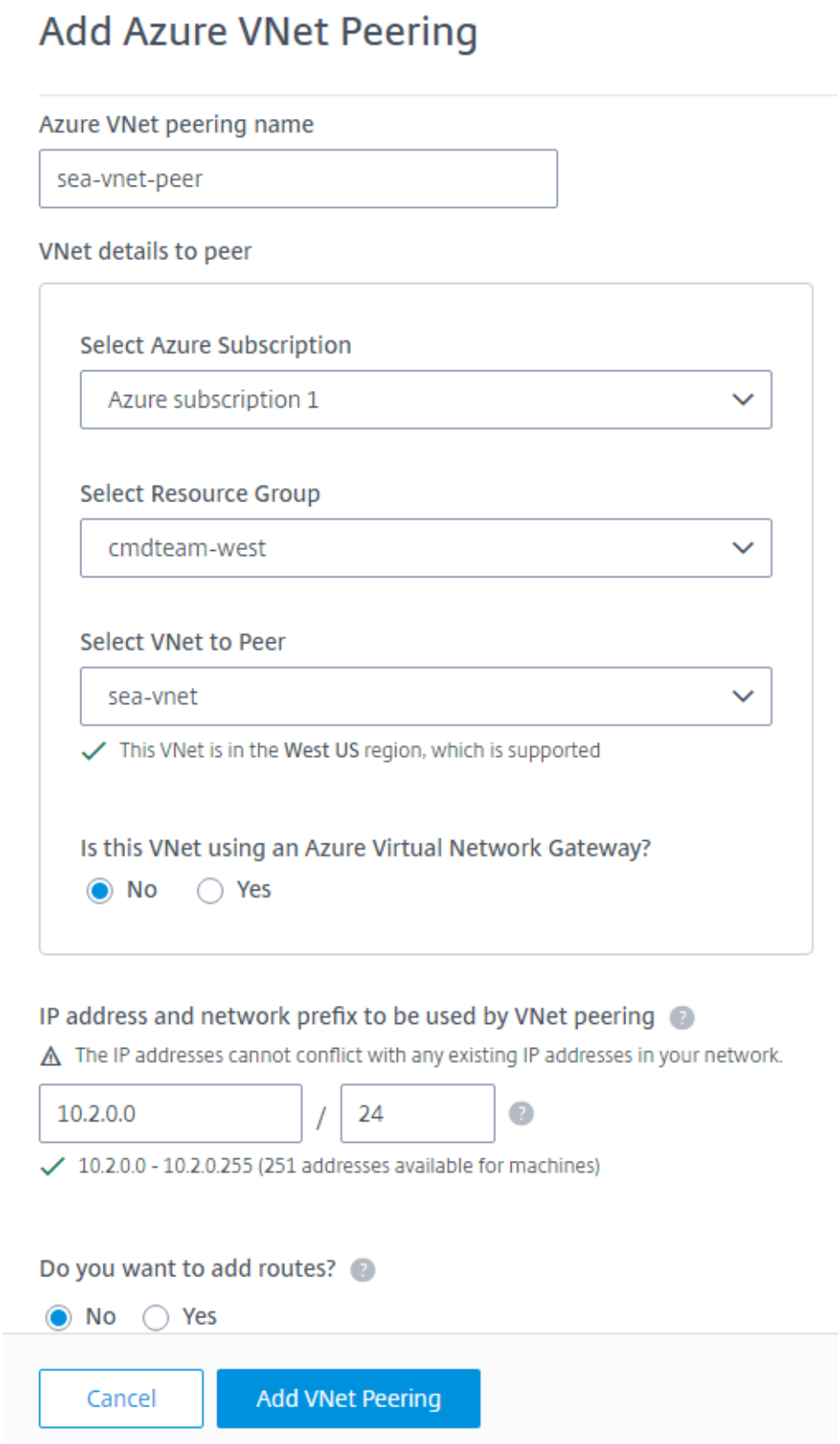
2. Haga clic en **Agregar conexión**.
3. Haga clic en cualquier parte del cuadro **Agregar emparejamiento de redes virtuales de Azure**.



4. Haga clic en **Autenticar cuenta Azure**.



5. Citrix DaaS para Azure lo lleva automáticamente a la página de inicio de sesión de Azure para autenticar sus suscripciones de Azure. Después de iniciar sesión en Azure (con las credenciales de la cuenta de administrador global) y aceptar los términos, volverá al cuadro de diálogo de detalles de creación de conexiones.



6. Escriba un nombre para el par de redes virtuales de Azure.
7. Seleccione la suscripción de Azure, el grupo de recursos y la red virtual que quiere emparejar.
8. Indique si la red virtual seleccionada utiliza Azure Virtual Network Gateway. Para obtener información, consulte el artículo de Microsoft Azure VPN Gateway.
9. Si respondió **Sí** en el paso anterior (la red virtual seleccionada utiliza una puerta de enlace de red virtual de Azure), indique si quiere habilitar la propagación de rutas de puerta de enlace de red virtual. Cuando está habilitada, Azure aprende (agrega) automáticamente todas las rutas a través de la puerta de enlace.

   Puede cambiar esta configuración más adelante en la página **Detalles** de la conexión. Sin embargo, cambiarlo puede provocar cambios en el patrón de redirección e interrupciones del tráfico del VDA. Además, si lo inhabilita más adelante, debe agregar manualmente las rutas a las redes que utilizarán los VDA.
10. Escriba una dirección IP y seleccione una máscara de red. Se muestra el intervalo de direcciones que se va a utilizar y cuántas direcciones admite el intervalo. Asegúrese de que el intervalo IP no se superponga a ninguna dirección que utilice en las redes locales y de Azure.

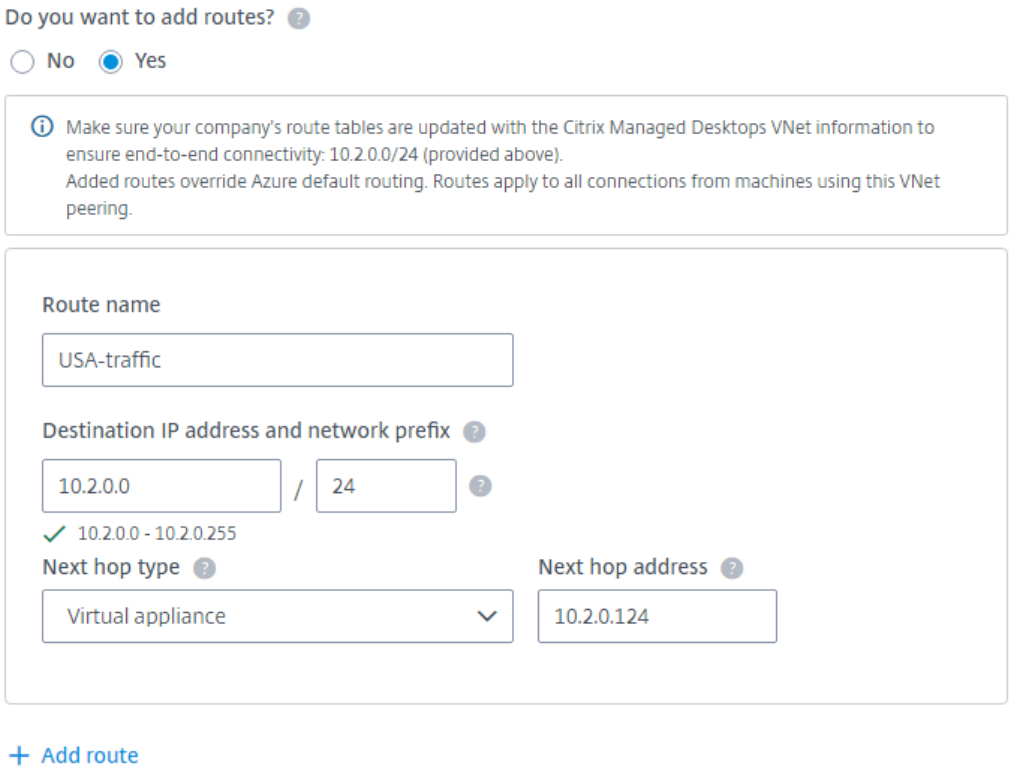
    - Por ejemplo, si su red virtual de Azure tiene un espacio de direcciones de 10.0.0.0 /16, cree la conexión de emparejamiento de redes virtuales en Citrix Virtual Apps and Desktops Standard como algo como 192.168.0.0 /24.
    - En este ejemplo, crear una conexión de emparejamiento de redes virtuales con un intervalo de direcciones IP 10.0.0.0 /24 se consideraría un intervalo de direcciones superpuesto.

    Si las direcciones se superponen, es posible que la conexión de emparejamiento de redes virtuales no se cree correctamente. Tampoco funcionará correctamente para las tareas de administración del sitio.
11. Indique si quiere agregar rutas personalizadas a la conexión de emparejamiento de redes virtuales. Si selecciona **Sí**, introduzca la siguiente información:

    a) Escriba un nombre descriptivo para la ruta personalizada.

    b) Introduzca la dirección IP de destino y el prefijo de red. El prefijo de red debe estar entre 16 y 24.

    c) Seleccione un tipo de próximo salto para la ubicación a la que quiere que se redirija el tráfico. Si selecciona **Dispositivo virtual**, introduzca la dirección IP interna del dispositivo.



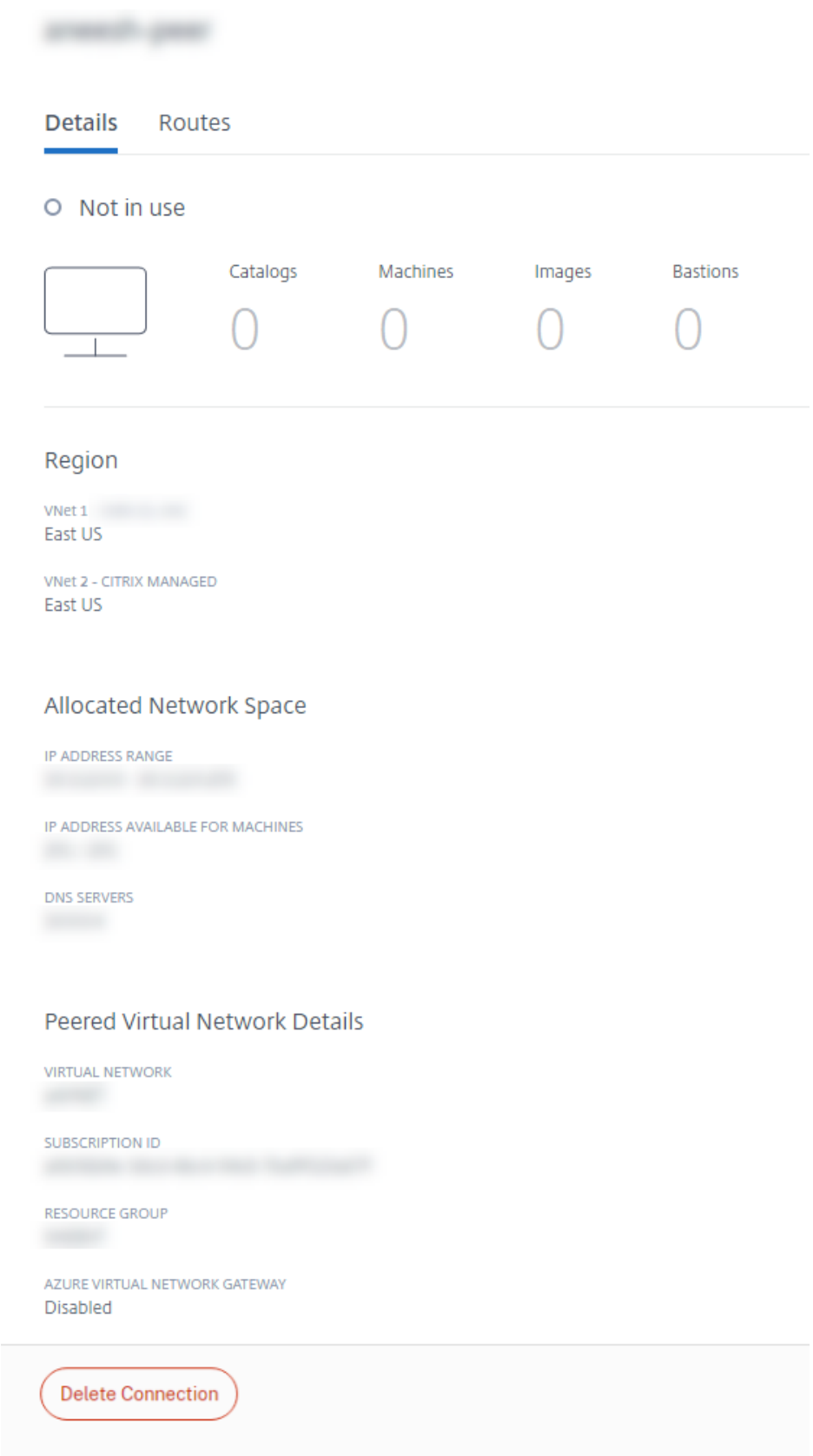
Para obtener más información sobre los tipos de salto siguiente, consulte Rutas personalizadas en el artículo de Microsoft Enrutamiento del tráfico de red virtual.

d) Haga clic en **Agregar ruta** para crear otra ruta personalizada para la conexión.

12. Haga clic en **Agregar emparejamiento de red virtual**.

Una vez creada la conexión, aparecerá en **Conexiones de red > Pares de redes virtuales de Azure**, en la parte derecha del panel de mandos **Administrar > Distribución rápida de Azure**. Al crear un catálogo, esta conexión se incluye en la lista de conexiones de red disponibles.

Ver detalles de la conexión de emparejamiento de redes virtuales de Azure



1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión de emparejamiento de redes virtuales de Azure que quiere mostrar.

Los detalles incluyen:

- El número de catálogos, máquinas, imágenes y bastiones que utilizan esta conexión.
- La región, el espacio de red asignado y las redes virtuales interconectadas.
- Las rutas configuradas actualmente para la conexión de emparejamiento de redes virtuales.

Administrar rutas personalizadas para conexiones de pares de Azure vNet existentes

Puede agregar nuevas rutas personalizadas a una conexión o modificar las rutas personalizadas ya existentes, incluido inhabilitar o eliminar rutas personalizadas.

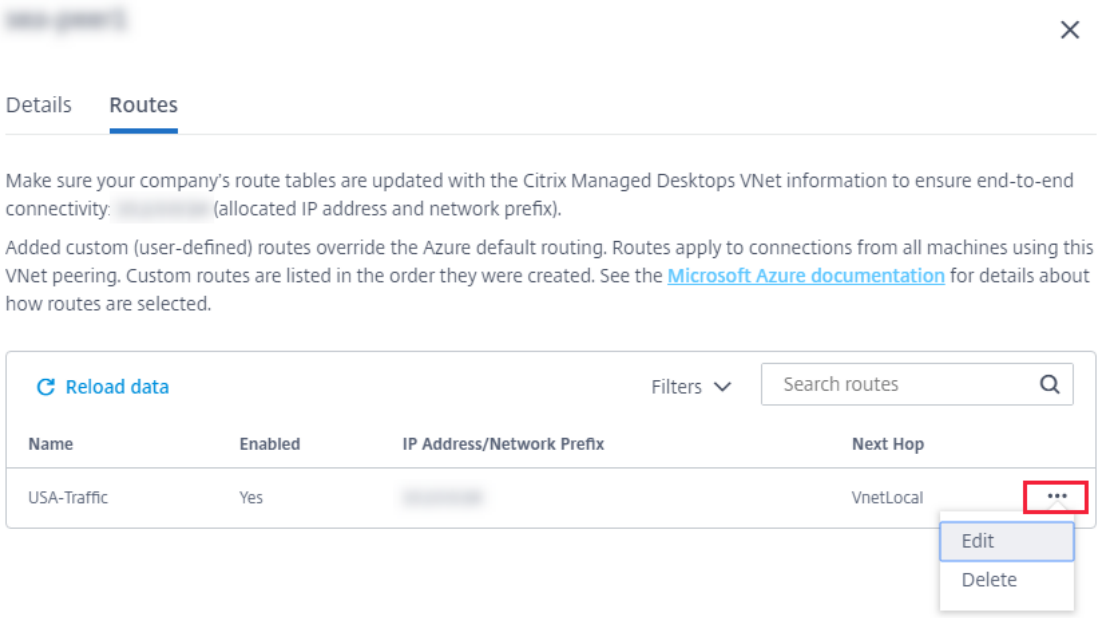
> **Importante:**
>
> Modificar, inhabilitar o eliminar rutas personalizadas cambia el flujo de tráfico de la conexión y podría interrumpir cualquier sesión de usuario que esté activa.

Para agregar una ruta personalizada:

1. Desde los detalles de conexión de emparejamiento de redes virtuales, seleccione **Rutas** y, a continuación, haga clic en **Agregar ruta**.
2. Introduzca un nombre descriptivo, la dirección IP de destino y el prefijo, y el tipo de próximo salto que quiere utilizar. Si selecciona **Dispositivo virtual** como tipo de próximo salto, introduzca la dirección IP interna del dispositivo.
3. Indique si quiere habilitar la ruta personalizada. De forma predeterminada, la ruta personalizada está habilitada.
4. Haga clic en **Agregar ruta**.

Para modificar o inhabilitar una ruta personalizada:

1. En los detalles de la conexión de emparejamiento de redes virtuales, seleccione **Rutas** y, a continuación, busque la ruta personalizada que quiere administrar.
2. En el menú de puntos suspensivos, seleccione **Modificar**.



3. Haga los cambios necesarios en el prefijo y la dirección IP de destino o en el tipo de próximo salto, según sea necesario.
4. Para habilitar o inhabilitar una ruta personalizada, en **¿Habilitar esta ruta?**, seleccione **Sí** o **No**.
5. Haz clic en **Guardar**.

Para eliminar una ruta personalizada:

1. En los detalles de la conexión de emparejamiento de redes virtuales, seleccione **Rutas** y, a continuación, busque la ruta personalizada que quiere administrar.
2. En el menú de puntos suspensivos, seleccione **Eliminar**.
3. Seleccione **El hecho de eliminar rutas puede interrumpir sesiones activas** para aceptar el impacto que puede tener eliminar la ruta personalizada.
4. Haga clic en **Eliminar ruta**.

Eliminar una conexión de emparejamiento de redes virtuales de Azure

Antes de poder eliminar un emparejamiento de redes virtuales de Azure, quite todos los catálogos asociados a él. Consulte Eliminar un catálogo.

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiere eliminar.
3. Desde los detalles de la conexión, haga clic en **Eliminar conexión**.

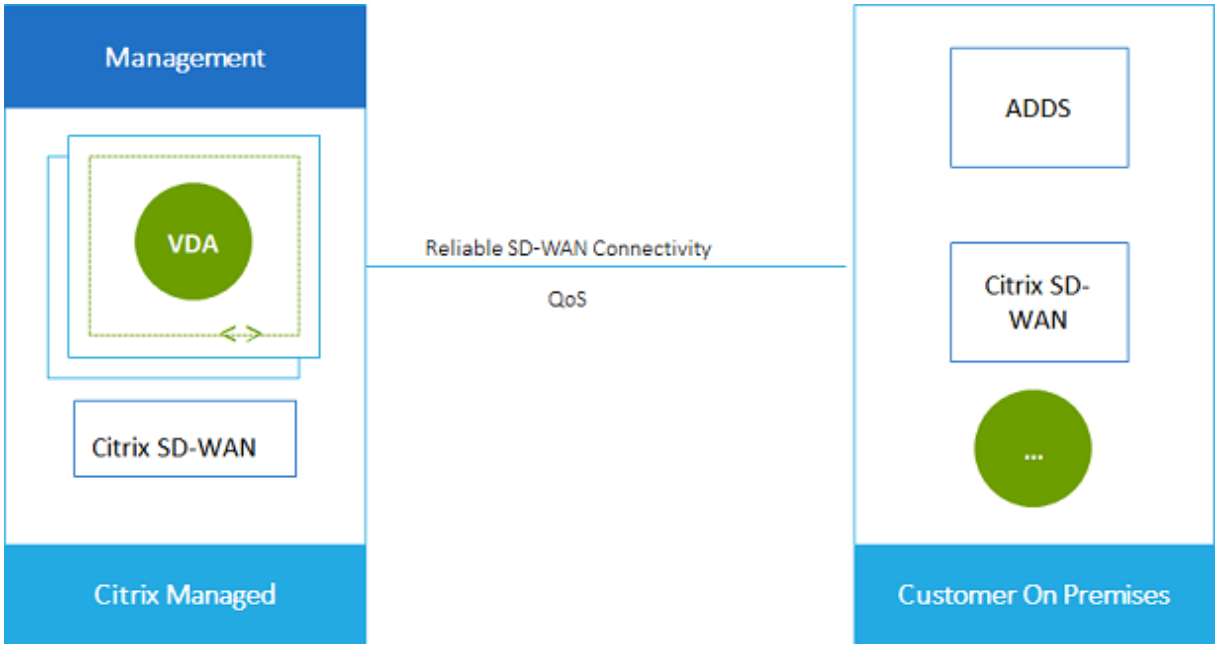
Acerca de las conexiones SD-WAN

> **Importante:**
>
> Citrix SD-WAN ha quedado obsoleto y todo el contenido relacionado se eliminará de la documentación en una versión futura. Le recomendamos que cambie a soluciones de red alternativas para garantizar un acceso ininterrumpido a los servicios de Citrix.

Citrix SD-WAN optimiza todas las conexiones de red que necesita Citrix Virtual Apps and Desktops Standard para Azure. Trabajando en conjunto con las tecnologías HDX, Citrix SD-WAN proporciona calidad de servicio y fiabilidad de conexión para el tráfico ICA y fuera de banda de Citrix Virtual Apps and Desktops Standard. Citrix SD-WAN admite las siguientes conexiones de red:

- Conexión ICA multisecuencia entre los usuarios y sus escritorios virtuales
- Acceso a Internet desde el escritorio virtual a sitios web, aplicaciones SaaS y otras propiedades en la nube
- Acceso desde el escritorio virtual a recursos locales como Active Directory, servidores de archivos y servidores de bases de datos
- Tráfico interactivo o en tiempo real transferido por RTP desde el motor de medios de la aplicación Workspace a servicios de comunicación unificada alojados en la nube, como Microsoft Teams
- Obtención del lado del cliente de vídeos de sitios como YouTube y Vimeo

Como se muestra en el siguiente gráfico, crea una conexión SD-WAN desde la suscripción de Azure administrado por Citrix a sus sitios. Durante la creación de la conexión, se crean dispositivos VPX SD-WAN en la suscripción de Azure administrado por Citrix. Desde la perspectiva de SD-WAN, esa ubicación se trata como una sucursal.



Requisitos de conexión SD-WAN y preparación

- Si no se cumplen los siguientes requisitos, la opción de conexión de red SD-WAN no está disponible.
  - Derechos de Citrix Cloud: Citrix Virtual Apps and Desktops Standard para Azure y SD-WAN Orchestrator.
  - Implementación de SD-WAN instalada y configurada. La implementación debe incluir un nodo de control maestro (MCN), ya sea en la nube o local, y administrarse con SD-WAN Orchestrator.
- Intervalo de direcciones IP de redes virtuales: Proporcione un espacio de direcciones CIDR disponible (dirección IP y prefijo de red) único entre los recursos de red que se conectan. Este es el intervalo de direcciones IP asignado a las máquinas virtuales dentro de la red virtual de Citrix Virtual Apps and Desktops Standard.

  Asegúrese de especificar un intervalo de IP que no se superponga a ninguna dirección que utilice en la nube y las redes locales.
  - Por ejemplo, si la red tiene un espacio de direcciones de 10.0.0.0 /16, cree la conexión en Citrix Virtual Apps and Desktops Standard como algo como 192.168.0.0 /24.
  - En este ejemplo, la creación de una conexión con un intervalo IP 10.0.0.0 /24 se consideraría un intervalo de direcciones superpuesto.

  Si las direcciones se superponen, es posible que la conexión no se cree correctamente. Tampoco funcionará correctamente para las tareas de administración del sitio.
- El proceso de configuración de la conexión incluye tareas que usted (el administrador de Citrix DaaS para Azure) y el administrador de SD-WAN Orchestrator deben completar. Además, para completar sus tareas, necesita información proporcionada por el administrador de SD-WAN Orchestrator.

  Antes de crear una conexión real, se recomienda que ambos revisen las instrucciones indicadas en este documento, además de la documentación de SD-WAN.

Crear una conexión SD-WAN

> **Importante:**
>
> Para obtener más información sobre la configuración de SD-WAN, consulte Configuración de SD-WAN para la integración de Citrix Virtual Apps and Desktops Standard para Azure.

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Haga clic en **Agregar conexión**.

3. En la página **Agregar una conexión de red**, haga clic en cualquier parte del cuadro SD-WAN.
4. En la página siguiente se resume lo que viene a continuación. Cuando termines de leer, haga clic en **Iniciar configuración de SD-WAN**.
5. En la página **Configurar SD-WAN**, introduzca la información proporcionada por el administrador de SD-WAN Orchestrator.

    - **Modo de implementación:** Si selecciona **Alta disponibilidad**, se crean dos dispositivos VPX (recomendado para entornos de producción). Si selecciona **Independiente**, se crea un dispositivo. No se puede cambiar esta configuración más adelante. Para cambiar al modo de implementación, tendrá que eliminar y volver a crear la sucursal y todos los catálogos asociados.
    - **Nombre:** Escriba un nombre para el sitio de SD-WAN.
    - **Rendimiento y cantidad de oficinas:** Esta información la proporciona el administrador de SD-WAN Orchestrator.
    - **Región:** La región en la que se crearán los dispositivos VPX.
    - **Subred VDA y subred SD-WAN:** Esta información la proporciona el administrador de SD-WAN Orchestrator. Consulte Requisitos de conexión SD-WAN y preparación para obtener información sobre cómo evitar conflictos.

6. Cuando haya terminado, haga clic en **Crear sucursal**.
7. En la página siguiente se resume lo que debe buscar en el panel de mandos **Administrar > Distribución rápida de Azure**. Cuando termines de leer, haga clic en **Entendido**.
8. En el panel de mandos **Administrar > Distribución rápida de Azure**, la nueva entrada SD-WAN en **Conexiones de red** muestra el progreso del proceso de configuración. Cuando la entrada se vuelve naranja con el mensaje **Esperando la activación por parte del administrador de SD-WAN, notifíquelo al administrador**de SD-WAN Orchestrator.
9. Para las tareas del administrador de SD-WAN Orchestrator, consulte la documentación del productoSD-WAN Orchestrator.
10. Cuando el administrador de SD-WAN Orchestrator finaliza, la entrada SD-WAN en **Conexiones de red** se vuelve verde, con el mensaje **Puede crear catálogos con esta conexión.**

Ver detalles de conexión SD-WAN

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione **SD-WAN** si no es la única opción.
3. Haga clic en la conexión que deseas mostrar.

La pantalla incluye:

- **Ficha Detalles:** Información especificada al configurar la conexión.
- **Ficha Conectividad de sucursales:** Nombre, conectividad en la nube, disponibilidad, nivel de ancho de banda, rol y ubicación para cada sucursal y MCN.

Eliminar una conexión de SD-WAN

Antes de poder eliminar una conexión de SD-WAN, elimine los catálogos asociados a ella. Consulte Eliminar un catálogo.

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione SD-WAN si no es la única opción.
3. Haga clic en la conexión que quiere eliminar para ampliar sus detalles.
4. En la ficha **Detalles**, haga clic en **Eliminar conexión**.
5. Confirme la eliminación.

Vista previa técnica de Azure VPN

La función Azure VPN está disponible para obtener una vista previa técnica.

Acerca de Azure conexiones de puerta de enlace

Una conexión de puerta de enlace de VPN de Azure proporciona un enlace de comunicación entre los VDA de Azure administrados por Citrix (escritorios y aplicaciones) y los recursos de su empresa, como redes locales o recursos en otras ubicaciones en la nube. Esto es similar a configurar y conectarse a una sucursal remota.

La conectividad segura utiliza los protocolos estándar de la industria Seguridad de protocolo de Internet (IPSec) e Intercambio de claves de Internet (IKE).

Durante el proceso de creación de la conexión:

- Proporciona la información que Citrix usa para crear la puerta de enlace y la conexión.
- Citrix crea una puerta de enlace VPN de Azure basada en rutas de sitio a sitio. La puerta de enlace de VPN forma un túnel de seguridad de protocolo de Internet (IPSec) directo entre la suscripción de Azure administrada por Citrix y el dispositivo host de la VPN.
- Después de que Citrix cree la puerta de enlace y la conexión de Azure VPN, debe actualizar la configuración de la VPN, las reglas de firewall y las tablas de enrutamiento. Para este proceso, utilice una dirección IP pública que proporciona Citrix y una clave previamente compartida (PSK) que proporcionó para crear la conexión.

Un ejemplo de conexión se ilustra en Crear una conexión de puerta de enlace de VPN de Azure.

No necesita su propia suscripción de Azure para crear este tipo de conexión.

También puede utilizar rutas personalizadas con este tipo de conexión.

Rutas Azure de puerta de enlace de VPN

Las rutas personalizadas o definidas por el usuario anulan las rutas predeterminadas del sistema para dirigir el tráfico entre las máquinas virtuales de las redes e Internet. Puede usar rutas personalizadas si hay redes a las que se espera que accedan los recursos de Citrix Virtual Apps and Desktops Standard, pero no están conectadas directamente a través de una puerta de enlace de VPN de Azure. Por ejemplo, podría crear una ruta personalizada que fuerce el tráfico a través de un dispositivo de red hacia Internet o hacia una subred de red local.

Cuando agrega rutas personalizadas a una conexión, esas rutas se aplican a todas las máquinas que usan esa conexión.

Para utilizar rutas personalizadas:

- Debe tener una puerta de enlace de red virtual existente o un dispositivo de red como Citrix SD-WAN en el entorno de Citrix Virtual Apps and Desktops Standard.
- Cuando agrega rutas personalizadas, debe actualizar las tablas de rutas de su empresa con la información de la VPN de destino para garantizar la conectividad de extremo a extremo.
- Las rutas personalizadas se muestran en la ficha **Conexión > Rutas** en el orden en que se introducen. Este orden de visualización no afecta al orden en que se seleccionan las rutas.

Antes de utilizar rutas personalizadas, revise el artículo Enrutamiento del tráfico de redes virtuales de Microsoft para obtener información sobre el uso de rutas personalizadas, los tipos de próximo salto y cómo selecciona Azure las rutas para el tráfico de salida.

Puede agregar rutas personalizadas al crear una conexión de puerta de enlace de VPN de Azure o a conexiones existentes en su entorno de servicio.

Requisitos y preparación de la conexión de Azure VPN Gateway

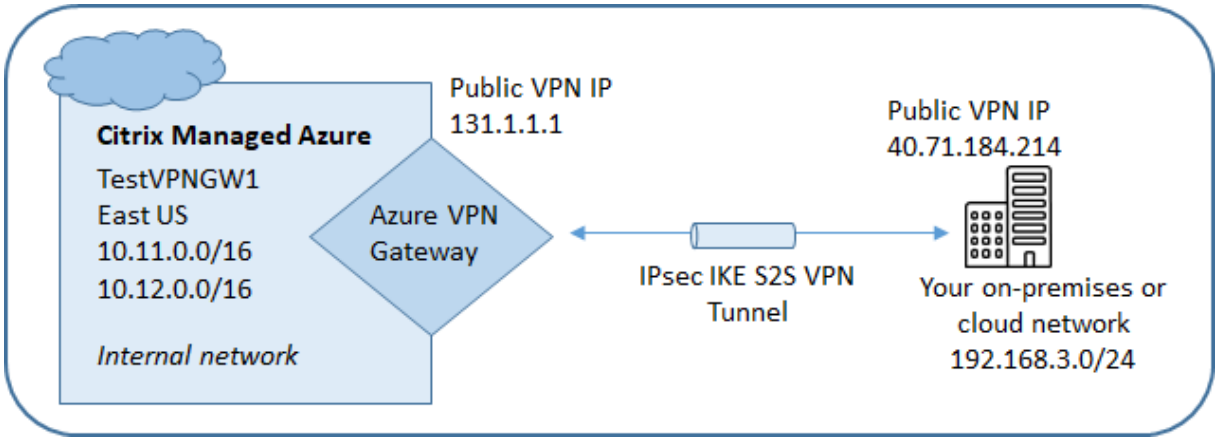
- Para obtener más información sobre Azure VPN Gateway, consulte el artículo de Microsoft ¿Qué es VPN Gateway?
- Revise los requisitos de todas las conexiones de red.
- Debe tener una VPN configurada. La red virtual debe poder enviar y recibir tráfico a través de la puerta de enlace VPN. Una red virtual no se puede asociar a más de una puerta de enlace de red virtual.

- Debe tener un dispositivo IPSec que tenga una dirección IP pública. Para obtener información sobre los dispositivos VPN validados, consulte el artículo de Microsoft Acerca de los dispositivos VPN.
- Revise el procedimiento Crear una conexión de Azure VPN Gateway antes de iniciarlo, de modo que pueda recopilar la información que necesita. Por ejemplo, necesitará direcciones permitidas en su red, intervalos de IP para los VDA y la puerta de enlace, el nivel de rendimiento y rendimiento deseados y las direcciones del servidor DNS.

Crear una conexión de puerta de enlace de Azure

Asegúrese de revisar este procedimiento antes de iniciarlo.

El siguiente diagrama muestra un ejemplo de configuración de una conexión de puerta de enlace de VPN de Azure. En general, Citrix administra los recursos en el lado izquierdo del diagrama y usted administra los recursos en el lado derecho. Algunas descripciones del siguiente procedimiento incluyen referencias a los ejemplos del diagrama.



1. En el panel **Administrar** de Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Haga clic en **Agregar conexión**.
3. Haga clic en cualquier parte del cuadro **Azure VPN Gateway**.
4. Revise la información en la página **Agregar conexión VPN** y, a continuación, haga clic en **Iniciar configuración de VPN**.
5. En la página **Agregar una conexión**, proporcione la siguiente información.
   - **Nombre:** Un nombre para la conexión (en el diagrama, el nombre es TestVPNGW1).
   - **Dirección IP de VPN:** su dirección IP pública.

     En el diagrama, la dirección es 40.71.184.214.

- **Redes permitidas:** uno o más rangos de direcciones a los que el servicio Citrix puede acceder en su red. Por lo general, este rango de direcciones contiene los recursos a los que los usuarios necesitan acceder, como los servidores de archivos.

  Para agregar más de un rango, haga clic en **Agregar más direcciones IP** e introduzca un valor. Repita según sea necesario.

  En el diagrama, el rango de direcciones es 192.168.3.0/24.

- **Clave previamente compartida:** un valor que utilizan ambos extremos de la VPN para la autenticación (similar a una contraseña). Tú decides cuál es este valor. Asegúrese de anotar el valor. Lo necesitará más adelante cuando configure su VPN con la información de conexión.

- **Rendimiento y rendimiento:** el nivel de ancho de banda que se debe utilizar cuando los usuarios acceden a los recursos de la red.

  Todas las opciones no son necesariamente compatibles con el Protocolo de puerta de enlace fronterizo (BGP). En esos casos, los campos de **configuración de BCP** no están disponibles.

- **Región:** región de Azure en la que Citrix implementa máquinas que entregan escritorios y aplicaciones (VDA), al crear catálogos que usan esta conexión. No puede cambiar esta selección después de crear la conexión. Si más adelante decide usar una región diferente, debe crear o usar otra conexión que especifique la región deseada.

  En el diagrama, la región es EastUS.

- **Modo activo-activo (alta disponibilidad): indica** si se crean dos puertas de enlace VPN para alta disponibilidad. Cuando este modo está habilitado, solo hay una puerta de enlace activa a la vez. Obtenga información sobre la puerta de enlace VPN de Azure activa-activa en el documento de Microsoft Conectividad entre instalaciones de alta disponibilidad.

- **Configuración de BGP:** (Disponible solo si el **rendimiento y el rendimiento** seleccionados admiten BGP). Si se debe usar el Protocolo de puerta de enlace fronterizo (BGP). Obtenga más información sobre BGP en el documento de Microsoft: Acerca de BGP con Azure VPN Gateway. Si habilita BGP, proporcione la siguiente información:

  - **Número de sistema autónomo (ASN):** a las puertas de enlace de red virtual de Azure se les asigna un ASN predeterminado de 65515. Una conexión habilitada para BGP entre dos puertas de enlace de red requiere que sus ASN sean diferentes. Si es necesario, puede cambiar el ASN ahora o después de crear la puerta de enlace.

  - Dirección**IP de interconexión de IP BGP:** Azure admite IP de BGP en el rango 169.254.21.*x* hasta 169.254.22.*x*.

- **Subred de VDA:** rango de direcciones en el que residirán los VDA de Citrix (máquinas que entregan escritorios y aplicaciones) y Cloud Connectors cuando cree un catálogo que util-

ice esta conexión. Después de introducir una dirección IP y seleccionar una máscara de red, se muestra el rango de direcciones, además del número de direcciones que admite el rango.

Si bien este rango de direcciones se mantiene en la suscripción de Azure administrada por Citrix, funciona como si fuera una extensión de la red.

- El rango de IP no debe superponerse a ninguna dirección que utilice en sus redes locales u otras redes en la nube. Si las direcciones se superponen, es posible que la conexión no se cree correctamente. Además, una dirección superpuesta no funcionará correctamente para las tareas de administración del sitio.
- El rango de subredes del VDA debe ser diferente de la dirección de subred de la puerta de enlace.
- No puede cambiar este valor después de crear la conexión. Para usar un valor diferente, cree otra conexión.

En el diagrama, la subred del VDA es 10.11.0.0/16.

- **Subred de puerta de enlace:** el rango de direcciones en el que residirá la puerta de enlace de Azure VPN cuando cree un catálogo que use esta conexión.
  - El rango de IP no debe superponerse a ninguna dirección que utilice en sus redes locales u otras redes en la nube. Si las direcciones se superponen, es posible que la conexión no se cree correctamente. Además, una dirección superpuesta no funcionará correctamente para las tareas de administración del sitio.
  - El rango de subredes de la puerta de enlace debe ser diferente de la dirección de subred del VDA.
  - No puede cambiar este valor después de crear la conexión. Para usar un valor diferente, cree otra conexión.

  En el diagrama, la subred de puerta de enlace es 10.12.0.9/16.
- **Rutas:** Indique si quiere agregar rutas personalizadas a la conexión. Si quiere agregar rutas personalizadas, proporcione la siguiente información:
  - Escriba un nombre descriptivo para la ruta personalizada.
  - Introduzca la dirección IP de destino y el prefijo de red. El prefijo de red debe estar entre 16 y 24.
  - Seleccione un tipo de próximo salto para la ubicación a la que quiere que se redirija el tráfico. Si selecciona Dispositivo **virtual, introduzca la dirección IP interna del dispositivo. Para obtener más información sobre los tipos de salto siguiente, consulte Rutas personalizadas en el artículo de Microsoft Enrutamiento del tráfico de red virtual.

Para agregar más de una ruta, haga clic en **Agregar ruta** e introduzca la información solicitada.

- **Servidores DNS:** introduzca las direcciones de sus servidores DNS e indique el servidor preferido. Aunque puede cambiar las entradas del servidor DNS más adelante, tenga en cuenta que cambiarlas puede provocar problemas de conectividad en las máquinas de los catálogos que usan esta conexión.

  Para agregar más de dos direcciones de servidor DNS, haga clic en **Agregar DNS alternativo** y, a continuación, introduzca la información solicitada.

6. Haga clic en **Crear conexión VPN**.

Una vez que Citrix crea la conexión, aparece en **Conexiones de red > Azure VPN Gateway** en el panel **Administrar** de Citrix DaaS para Azure. La tarjeta de conexión contiene una dirección IP pública. (En el diagrama, la dirección es 131.1.1.1).

- Use esta dirección (y la clave previamente compartida que especificó al crear la conexión) para configurar su VPN y sus firewalls. Si olvidó su clave previamente compartida, puede cambiarla en la página **Detalles** de la conexión. Necesitará la nueva clave para configurar su extremo de la puerta de enlace de VPN.

  Por ejemplo, permita excepciones en el firewall para los rangos de direcciones IP de subred de puerta de enlace y VDA que configuró.

- Actualice las tablas de rutas de su empresa con la información de conexión de Azure VPN Gateway para garantizar una conectividad de extremo a extremo.

  En el diagrama, se requieren nuevas rutas para el tráfico que va de 192.168.3.0/24 a 10.11.0.0/16 y 10.12.0.9/16 (las subredes de VDA y puerta de enlace).

- Si configuró rutas personalizadas, realice también las actualizaciones apropiadas para ellas.

Cuando ambos extremos de la conexión se configuran correctamente, la entrada de la conexión en **Conexiones de red > Azure VPN Gateway** indica **Listo para usar**.

Ver una conexión de gateway de VPN de Azure

1. En el panel **Administrar** de Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiera mostrar.

   Pantallas:

- La ficha **Detalles** muestra el número de catálogos, máquinas, imágenes y bastiones que utilizan esta conexión. También contiene la mayor parte de la información que configuró para esta conexión.
- La ficha **Rutas** muestra información de ruta personalizada para la conexión.

Administrar rutas personalizadas para una conexión de puerta de enlace de VPN de Azure

En una conexión de puerta de enlace VPN de Azure existente, puede agregar, modificar, inhabilitar y eliminar rutas personalizadas.

Para obtener información sobre cómo agregar rutas personalizadas al crear una conexión, consulte Crear una conexión de puerta de enlace de Azure VPN.

> **Importante:**
>
> La modificación, desactivación o eliminación de rutas personalizadas cambia el flujo de tráfico de la conexión y puede interrumpir las sesiones activas de los usuarios.

1. En el panel **Administrar** de Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiera mostrar.
    - Para agregar una ruta personalizada:
        a) En la ficha **Rutas** de la conexión, haga clic en **Agregar ruta**.
        b) Introduzca un nombre descriptivo, la dirección IP de destino y el prefijo, y el tipo de próximo salto que quiere utilizar. Si selecciona **Dispositivo virtual** como tipo de próximo salto, introduzca la dirección IP interna del dispositivo.
        c) Indique si quiere habilitar la ruta personalizada. De forma predeterminada, la ruta personalizada está habilitada.
        d) Haga clic en **Agregar ruta**.
    - Para modificar o habilitar/inhabilitar una ruta personalizada:
        a) En la ficha **Rutas** de la conexión, localice la ruta personalizada que quiere administrar.
        b) En el menú de puntos suspensivos, seleccione **Modificar**.
        c) Cambie la dirección IP y el prefijo de destino, o el tipo de salto siguiente, según sea necesario.
        d) Indique si quiere habilitar la ruta.
        e) Haz clic en **Guardar**.
    - Para eliminar una ruta personalizada:
        a) En la ficha **Rutas** de la conexión, localice la ruta personalizada que quiere administrar.
        b) En el menú de puntos suspensivos, seleccione **Eliminar**.
        c) Seleccione **El hecho de eliminar rutas puede interrumpir sesiones activas** para aceptar el impacto que puede tener eliminar la ruta personalizada.
        d) Haga clic en **Eliminar ruta**.

Restablecer o eliminar una conexión de puerta de enlace de Azure

> **Importante:**
>
> - Al restablecer una conexión, se pierde la conexión actual y ambos extremos deben restablecerla. Un restablecimiento interrumpe las sesiones de los usuarios activos.
> - Antes de poder eliminar una conexión, elimine todos los catálogos que la utilizan. Consulte Eliminar un catálogo.

Para restablecer o eliminar una conexión:

1. En el panel **Administrar** de Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiere restablecer o eliminar.
3. En la ficha **Detalles** de la conexión:
   - Para restablecer la conexión, haga clic en **Restablecer conexión**.
   - Para eliminar la conexión, haga clic en **Eliminar conexión**.
4. Si se le solicita, confirme la acción.

Crear una dirección IP estática pública

Si quiere que todas las máquinas VDA de una conexión usen una única dirección IP estática pública saliente (puerta de enlace) a Internet, habilite una puerta de enlace NAT. Puede habilitar una puerta de enlace NAT para las conexiones a catálogos que están unidos a un dominio o que no están unidos a un dominio.

Para habilitar una puerta de enlace NAT para una conexión:

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Conexiones de red** a la derecha.
2. En **Conexiones de red**, seleccione una conexión en **ADMINISTRADA POR CITRIX** o **EMPAREJAMIENTOS DE REDES VIRTUALES DE AZURE**.
3. En la tarjeta de detalles de conexión, haga clic en **Habilitar gateway NAT**.
4. En la página Habilitar puerta de enlace NAT, mueva el control deslizante a **Sí** y configure un tiempo de inactividad.
5. Haga clic en **Confirmar cambios**.

Al habilitar una puerta de enlace NAT:

- Azure asigna una dirección IP estática pública a la puerta de enlace de forma automática. (No puede especificar esta dirección). Todos los VDA de todos los catálogos que usen esta conexión usarán esa dirección para la conectividad saliente.

- Puede especificar un valor de tiempo de espera por inactividad. Ese valor indica el número de minutos que una conexión saliente abierta a través de la puerta de enlace NAT puede permanecer inactiva antes de que se cierre la conexión.
- Debe permitir la dirección IP estática pública en su firewall.

Puede volver a la tarjeta de detalles de conexión para habilitar o inhabilitar la puerta de enlace NAT y cambiar el valor del tiempo de espera.

Imágenes

September 7, 2022

Al crear un catálogo para entrega de escritorios o aplicaciones, se utiliza una imagen (con otros parámetros) como plantilla para crear las máquinas.

imágenes preparadas por Citrix

Citrix DaaS Standard para Azure (anteriormente Citrix Virtual Apps and Desktops Standard para Azure) proporciona varias imágenes preparadas por Citrix:

- Windows 10 Enterprise (sesión única)
- Windows 10 Enterprise Virtual Desktop (multisesión)
- Windows 10 Enterprise Virtual Desktop (multisesión) con Office 365 ProPlus
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Linux Ubuntu (sesión única y multisesión)

Las imágenes preparadas por Citrix tienen instalado un Citrix Virtual Delivery Agent (VDA) y herramientas de solución de problemas. El VDA es el mecanismo de comunicación entre las máquinas de los usuarios y la infraestructura de Citrix Cloud que administra Citrix DaaS para Azure. Las imágenes proporcionadas por Citrix se notan como **CITRIX**.

También puede importar y utilizar su propia imagen de Azure.

Formas de usar imágenes

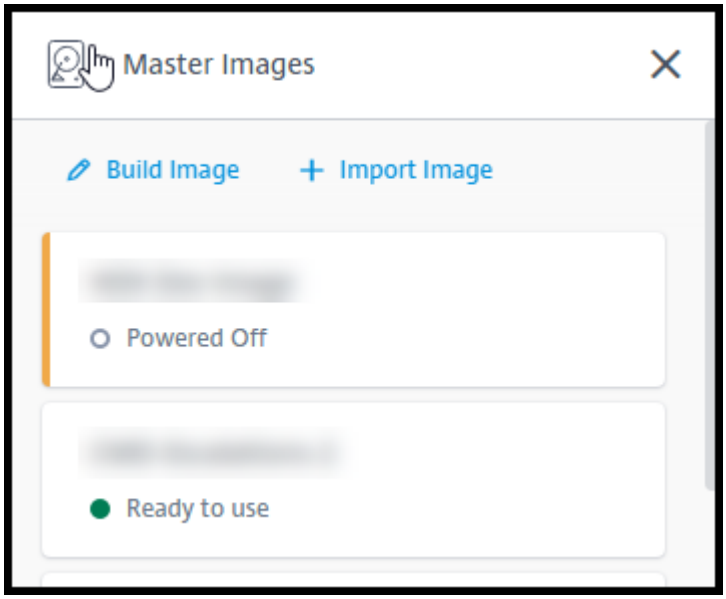
Puede hacer lo siguiente:

- **Utilizar una imagen preparada por Citrix al crear un catálogo.** Esta opción solo se recomienda para implementaciones de prueba de concepto.
- **Utilizar una imagen preparada por Citrix para crear otra imagen.** Después de crear la nueva imagen, la personaliza agregando aplicaciones y otro software que los usuarios necesiten. A continuación, puede utilizar esa imagen personalizada al crear un catálogo.
- **Importar una imagen de Azure.** Después de importar una imagen de Azure, puede utilizarla al crear un catálogo. O bien, puede usar esa imagen para crear una nueva imagen y, a continuación, personalizarla agregando aplicaciones. A continuación, puede utilizar esa imagen personalizada al crear un catálogo.

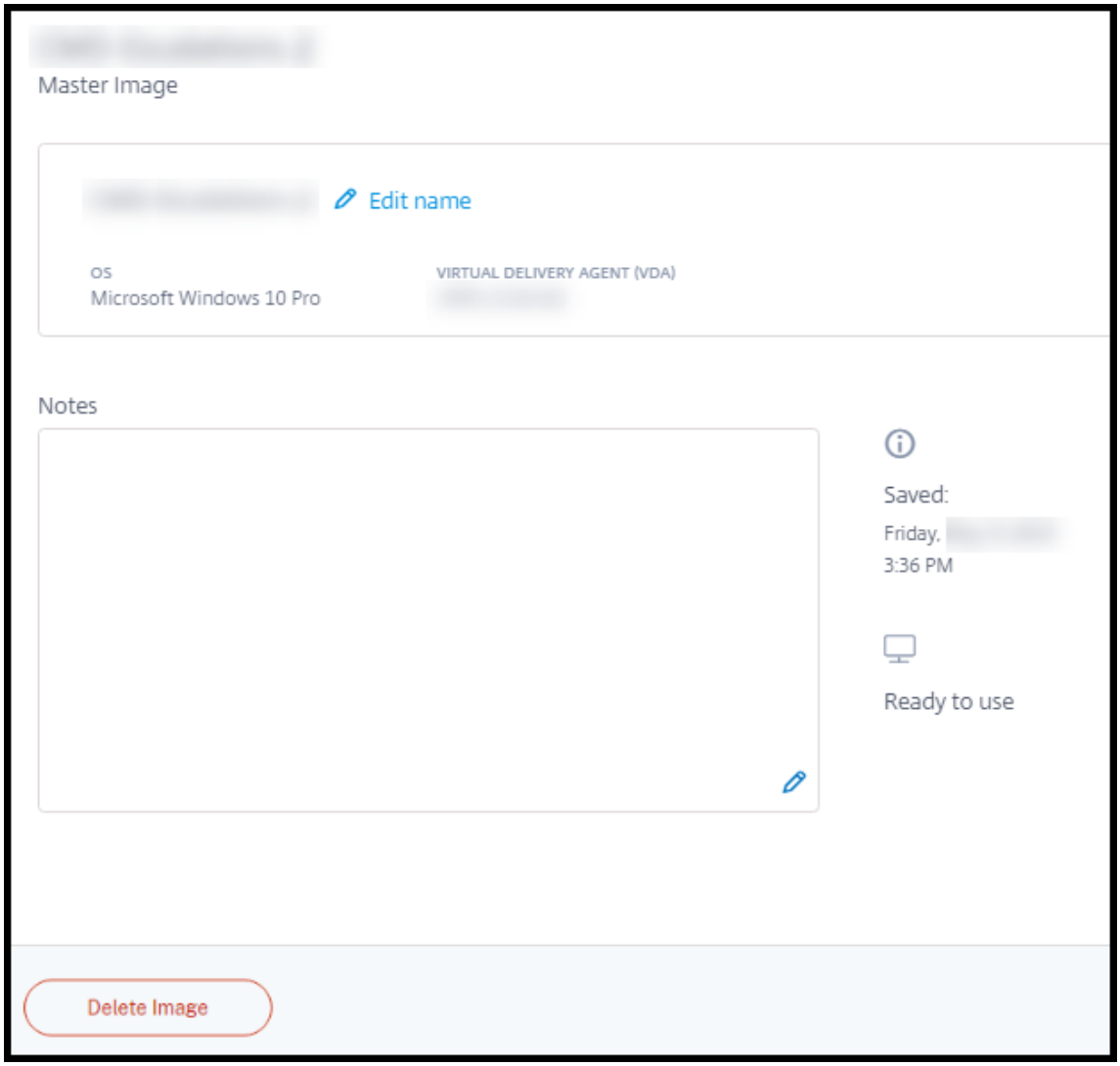
Al crear un catálogo, Citrix DaaS para Azure verifica que la imagen utilice un sistema operativo válido y que tenga instalados un VDA de Citrix y herramientas de solución de problemas (junto con otras comprobaciones).

Mostrar información de imagen

1. En el panel **Administrar > Azure Quick Deploy**, expanda **Imágenes maestras** a la derecha. La pantalla muestra las imágenes que proporciona Citrix y las imágenes que ha creado e importado.



2. Haga clic en una imagen para mostrar sus detalles.



Desde la ficha de detalles, puede hacer lo siguiente:

- Cambiar (modificar) el nombre de la imagen.
- Agregar y modificar notas (disponible solo para las imágenes que preparó o importó, no para las imágenes proporcionadas por Citrix).
- Eliminar la imagen.

Preparar una nueva imagen

La preparación de una nueva imagen incluye crear la imagen y, a continuación, personalizarla. Al crear una imagen, se crea una nueva máquina virtual para cargar la nueva imagen.

Requisitos:

- Conocer las funciones de rendimiento que necesitan las máquinas. Por ejemplo, ejecutar aplicaciones CAD puede requerir CPU, RAM y almacenamiento diferentes que otras aplicaciones de

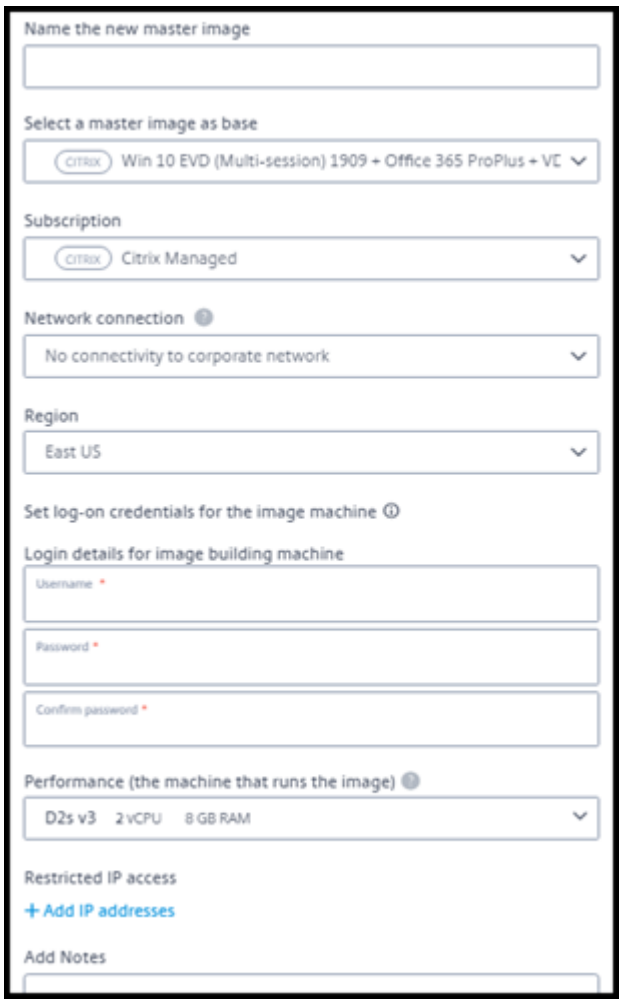
oficina.
- Si piensa utilizar una conexión a los recursos locales, configurar esa conexión antes de crear la imagen y el catálogo. Para obtener información detallada, consulte Conexiones de red.

Cuando se utiliza una imagen de Ubuntu preparada por Citrix para crear una nueva imagen, se crea una contraseña raíz para la nueva imagen. Puede cambiar esa contraseña raíz, pero solo durante el proceso de creación y personalización de la imagen. (No se puede cambiar la contraseña raíz después de utilizar la imagen en un catálogo).

- Cuando se crea la imagen, la cuenta de administrador especificada (**detalles de inicio de sesión de la máquina de creación de la imagen**) se agrega al grupo `sudoers`.
- Después de establecer conexión con RDP con la máquina que contiene la nueva imagen, inicie la aplicación de terminal y escriba `sudo passwd root`. Cuando se le indique, proporcione la contraseña que especificó al crear la imagen. Tras la verificación, se le pide que introduzca una nueva contraseña para el usuario raíz.

Para crear una imagen:

1. En el panel **Administrar > Azure Quick Deploy**, expanda **Imágenes maestras** a la derecha.
2. Haga clic en **Crear imagen**.



3. Introduzca valores en los siguientes campos:

   - **Nombre:** Introduzca un nombre para la nueva imagen.
   - **Imagen maestra:** Seleccione una imagen. Esta es la imagen de base que se utiliza para crear la nueva imagen.
   - **Suscripción:** Seleccione una suscripción de Azure. Para obtener más información, consulte Suscripciones de Azure.
   - **Conexión de red:**
     - Si utiliza una suscripción a Azure administrado por Citrix, seleccione **Sin conectividad** o una conexión creada anteriormente.
     - Si utiliza su propia suscripción de Azure administrado por el cliente, seleccione el grupo de recursos, la red virtual y la subred. A continuación, agregue los detalles del dominio: FQDN, unidad organizativa, nombre de cuenta de servicio y credenciales.
   - **Configuración de dominio:** seleccione el tipo de dominio: Active Directory o no unido a un dominio.

  - Si selecciona Active Directory, seleccione o agregue un dominio. Especifique una unidad organizativa (opcional), el nombre de la cuenta de servicio y la contraseña.
  - Si selecciona no estar unido a un dominio, no se necesita información adicional.

- **Región:** (Disponible solo para **Sin conectividad**). Seleccione la región en la que quiere crear la máquina que contiene la imagen.
- **Credenciales de inicio de sesión para la imagen bastión:** Utilizará estas credenciales más adelante cuando conecte (RDP) con la máquina que contiene la nueva imagen, de modo que pueda instalar aplicaciones y otro software.
- **Rendimiento de la máquina:** Información sobre CPU, RAM y almacenamiento de la máquina que ejecuta la imagen. Seleccione un rendimiento de máquina que satisfaga los requisitos de sus aplicaciones.
- **Acceso a IP restringido:** Si desea restringir el acceso a direcciones específicas, seleccione **Agregar direcciones IP** y, a continuación, introduzca una o varias direcciones. Después de agregar las direcciones, haga clic en **Listo** para volver a la tarjeta **Crear imagen**.
- **Notas:** Si lo desea, puede agregar hasta 1024 caracteres de notas. Después de crear la imagen, puede actualizar las notas desde la pantalla de detalles de la imagen.
- **Unirse al dominio local:** Indique si quiere unirse al dominio de Active Directory local.
  - Si selecciona **Sí**, introduzca la información de Azure: FQDN, OU, nombre de la cuenta de servicio y credenciales.
  - Si selecciona **No**, introduzca las credenciales de la máquina host.

4. Cuando haya terminado, haga clic en **Crear imagen**.

Una imagen puede tardar hasta 30 minutos en crearse. En el panel **Administrar > Implementación rápida de Azure**, expanda **Imágenes maestras** a la derecha para ver el estado actual (como **Imagen de creación** o **Listo para personalizar**).

Qué hacer a continuación: Conectar con una nueva imagen y personalizarla.

Conectar con una nueva imagen y personalizarla

Después de crear una imagen, su nombre se agrega a la lista de imágenes, con el estado **Listo para personalizar** (o texto similar). Para personalizar esa imagen, descargue primero un archivo RDP. Cuando utiliza ese archivo para conectar con la imagen, puede agregar aplicaciones y otro software a la misma.

1. En el panel **Administrar > Azure Quick Deploy**, expanda **Imágenes maestras** a la derecha. Haga clic en la imagen a la que quiere conectarse.

2. Haga clic en **Descargar archivo RDP**. Se descarga un cliente RDP.

   Es posible que la máquina de la imagen se apague si no se conecta con RDP a ella poco después de su creación. Esto permite ahorrar costes. Cuando eso ocurra, haga clic **en Encendido**.

3. Haga doble clic en el cliente RDP descargado. Intentará conectarse automáticamente a la dirección de la máquina que contiene la nueva imagen. Cuando se le indique, introduzca las credenciales especificadas al crear la imagen.

4. Después de conectarse a la máquina, agregue o quite aplicaciones, instale actualizaciones y finalice cualquier otro trabajo de personalización necesario.

   NO ejecute Sysprep en la imagen.

5. Cuando haya terminado de personalizar la nueva imagen, vuelva al cuadro **Imágenes maestras** y haga clic en **Finalizar construcción**. La nueva imagen se somete automáticamente a pruebas de validación.

Más adelante, al crear un catálogo, la nueva imagen se incluye en la lista de imágenes que puede seleccionar.

En el panel **Administrar > Distribución rápida**, las imágenes que se muestran a la derecha indican cuántos catálogos y máquinas utilizan cada imagen.

> **Nota:**
>
> Después de finalizar una imagen, no podrá modificarla. Debe crear una nueva imagen (mediante la imagen anterior como punto de partida) y, a continuación, actualizar la nueva imagen.

Importar una imagen de Azure

Cuando importa una imagen de Azure que tiene un VDA de Citrix y aplicaciones que los usuarios necesitan, puede utilizarla para crear un catálogo o reemplazar la imagen de un catálogo existente.

Requisitos de la imagen importada

> **Nota:**
>
> Citrix DaaS para Azure no admite la importación de discos que estén asociados con las máquinas virtuales de Azure de segunda generación.

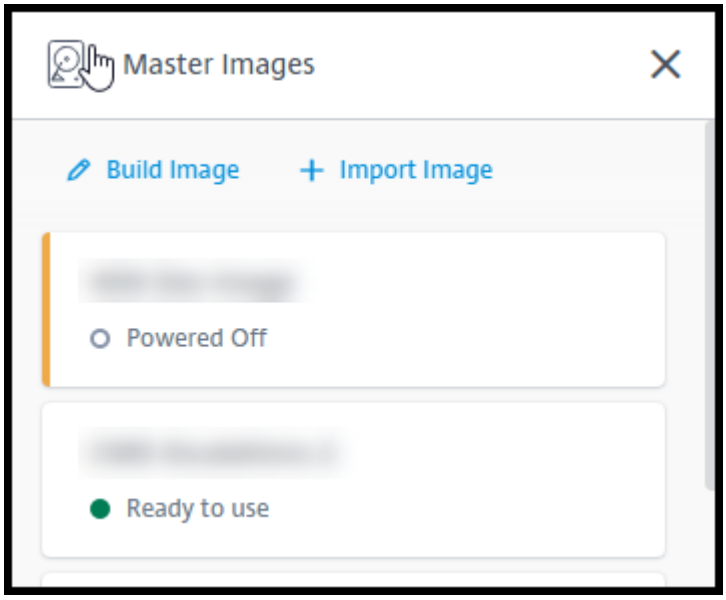
Citrix ejecuta pruebas de validación en la imagen importada. Asegúrese de que se cumplan los siguientes requisitos al preparar la imagen que va a importar a Citrix DaaS para Azure.

- **Sistema operativo compatible:** La imagen debe tener un sistema operativo compatible. Para comprobar una versión del sistema operativo Windows, ejecute `Get-WmiObject Win32_OperatingSystem`.

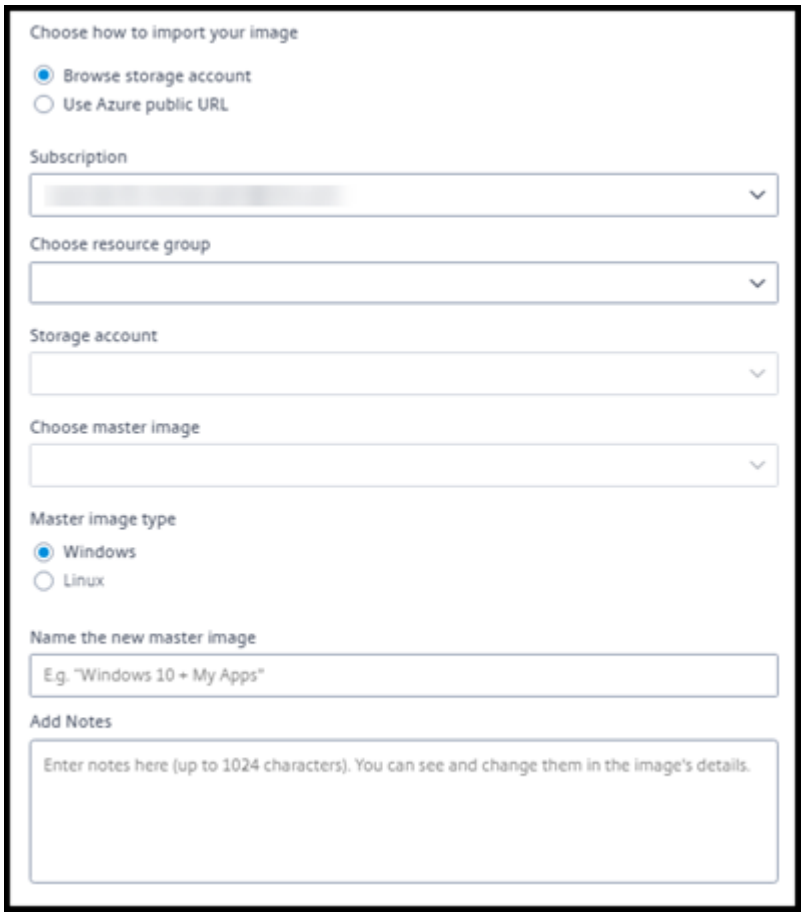
- **Generación compatible:** Solo se admiten máquinas virtuales de la generación 1.
- **No generalizada:** La imagen no debe ser generalizada.
- **Sin Delivery Controllers configurados:** Asegúrese de que no haya ningún Citrix Delivery Controller configurado en la imagen. Compruebe que se han borrado las siguientes claves de registro.
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`
- **Archivo Personality.ini:** El archivo `personality.ini` debe existir en la unidad del sistema.
- **VDA válido:** La imagen debe tener instalado un VDA Citrix más reciente que 7.11.
  - Windows: Para comprobar, use `Get HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Citrix Virtual Desktop Agent`. Para obtener directrices de instalación, consulte Instalar un VDA de Windows en una imagen.
  - Red Hat Enterprise Linux y Ubuntu: Para obtener información sobre la instalación, consulte la documentación del producto.
- **Agente de máquina virtual de Azure:** Antes de importar una imagen, asegúrese de que el agente de máquina virtual de Azure está instalado en la imagen. Para obtener más información, consulte el artículo de Microsoft Descripción general del agente de máquina virtual de Azure.

Importar la imagen

1. En el panel **Administrar > Azure Quick Deploy**, expanda **Imágenes maestras** a la derecha.



2. Haga clic en **Importar imagen**.



3. Elija cómo importar la imagen.

   - Para los discos administrados, utilice la función de exportación para generar una URL de SAS. Establezca el tiempo de caducidad en 7200 segundos o más.
   - En el caso de los discos duros de almacenamiento (VHD) de una cuenta de almacenamiento, elija una de las siguientes opciones:
     - Generar una URL de SAS para el archivo VHD.
     - Actualice el nivel de acceso de un contenedor de almacenamiento en bloque a blob o contenedor. A continuación, obtenga la URL del archivo.

4. Si seleccionó **Examinar cuenta de almacenamiento**:

   a) Seleccione secuencialmente una suscripción > grupo de recursos > cuenta de almacenamiento > imagen.
   b) Asigne un nombre a la imagen.

5. Si ha seleccionado la **URL pública de Azure**:

   a) Introduzca la URL generada por Azure para el VHD. Para obtener orientación, haga clic en

el enlace al documento de Microsoft Descargar un disco duro virtual de Windows desde Azure.

b) Seleccione una suscripción. (Una imagen de Linux solo se puede importar si selecciona una suscripción administrada por el cliente).

c) Asigne un nombre a la imagen.

6. Cuando haya terminado, haga clic en **Importar imagen**.

Actualizar un catálogo con una nueva imagen

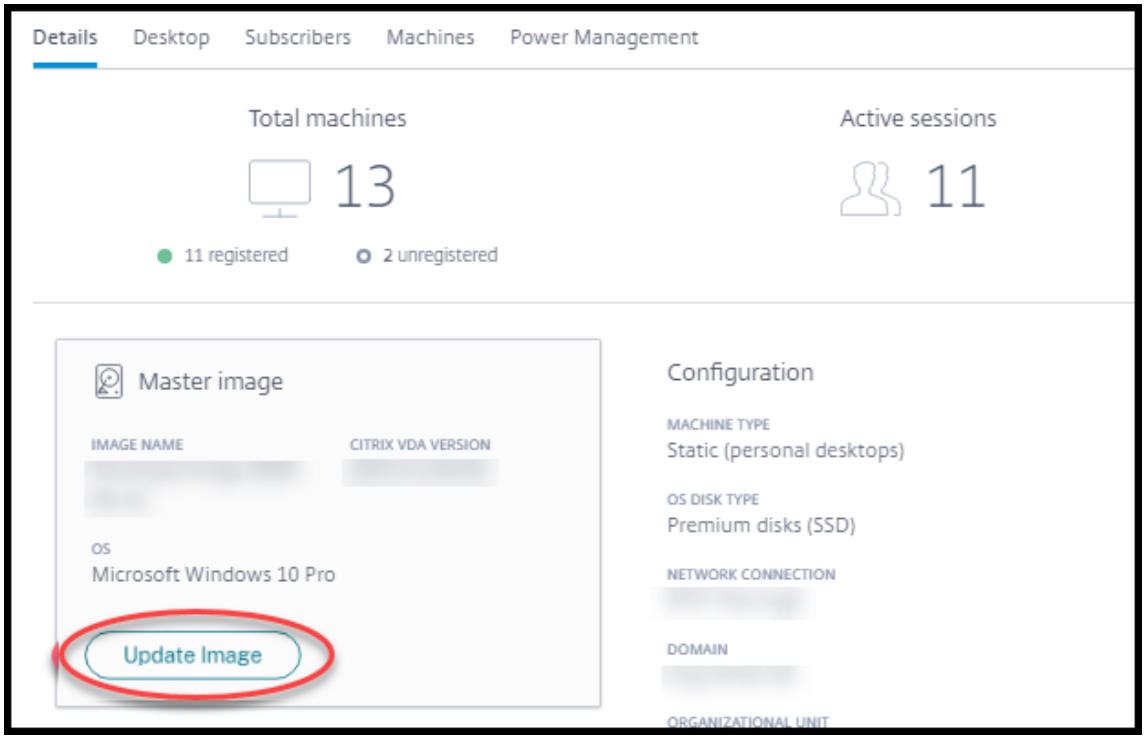
El tipo de catálogo determina qué máquinas se actualizan al actualizar el catálogo.

- En el caso de un catálogo aleatorio, todas las máquinas que se encuentran actualmente en el catálogo se actualizan con la imagen más reciente. Si agrega más escritorios a ese catálogo, se basan en la imagen más reciente.
- En el caso de un catálogo estático, las máquinas que se encuentran actualmente en el catálogo no se actualizan con la imagen más reciente. Las máquinas que se encuentran actualmente en el catálogo siguen utilizando la imagen a partir de la cual se crearon. Sin embargo, si agrega más máquinas a ese catálogo, se basan en la imagen más reciente.

Puede actualizar con una imagen gen2 un catálogo que contenga máquinas con imágenes gen1, si las máquinas del catálogo admiten gen2. Del mismo modo, puede actualizar con una imagen gen1 un catálogo que contenga máquinas gen2, si las máquinas del catálogo admiten gen1.

Para actualizar un catálogo con una nueva imagen:

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Detalles**, haga clic en **Actualizar imagen**.



3. Seleccione una imagen.
4. Para catálogos aleatorios o multisesión: Seleccione un intervalo de cierre de sesión. Después de que Citrix DaaS para Azure complete el procesamiento inicial de imágenes, los suscriptores reciben una advertencia para guardar su trabajo y cerrar la sesión en sus escritorios. El intervalo de cierre de sesión indica cuánto tiempo tienen los suscriptores tras recibir el mensaje hasta que la sesión finaliza automáticamente.
5. Haga clic en **Actualizar imagen**.

Eliminar una imagen

1. En el panel **Administrar > Azure Quick Deploy**, expanda **Imágenes maestras** a la derecha.
2. Haga clic en la imagen que quieres eliminar.
3. Haga clic en **Eliminar imagen** en la parte inferior de la tarjeta. Confirme la eliminación.

Instalar un VDA de Windows en una imagen

Utilice el siguiente procedimiento al preparar una imagen de Windows que vaya a importar a Citrix DaaS para Azure. Para obtener instrucciones sobre la instalación de Linux VDA, consulte la documentación del producto Linux VDA.

1. En el entorno de Azure, conéctese a la máquina virtual de la imagen (si aún no está conectado).

2. Puede descargar un VDA mediante el enlace **Descargas** en la barra de navegación de Citrix Cloud. O utilice un explorador para ir a la página de descargas de Citrix DaaS para Azure.

   Descargue un VDA en la máquina virtual. Existen paquetes de descarga de VDA independientes para SO de escritorio (sesión única) y SO de servidor (multisesión).

3. Inicie el instalador del VDA con un doble clic en el archivo descargado. Se iniciará el asistente de instalación.
4. En la página **Entorno**, seleccione la opción para crear una imagen con MCS y, a continuación, haga clic en **Siguiente**.
5. En la página **Componentes principales**, haga clic en **Siguiente**.
6. En la página **Delivery Controller**, seleccione **Dejar que Machine Creation Services lo haga automáticamente** y haga clic en **Siguiente**.
7. Deje la configuración predeterminada en las páginas **Componentes adicionales**, **Funciones** y **Firewall**, a menos que Citrix le indique lo contrario. Haga clic en **Siguiente** en cada página.
8. En la página **Resumen**, haga clic en **Instalar**. Los requisitos previos comienzan a instalarse. Cuando se le pida que reinicie, acepte.
9. La instalación del VDA se reanuda automáticamente. Se completa la instalación de los requisitos previos, y se instalan los componentes y las funciones. En la página **Call Home**, deje la configuración predeterminada (a menos que Citrix le indique lo contrario). Después de conectarte, haga clic en **Siguiente**.
10. Haga clic en **Finalizar**. La máquina se reinicia automáticamente.
11. Para comprobar que la configuración es correcta, inicie una o varias de las aplicaciones que haya instalado en la máquina virtual.
12. Apague la VM. No ejecute Sysprep en la imagen.

Para obtener más información sobre la instalación de agentes VDA, consulte Instalar agentes VDA.

Usuarios y autenticación

December 28, 2023

Métodos de autenticación de usuario

Los usuarios deben autenticarse cuando inician sesión en Citrix Workspace para iniciar su escritorio o aplicaciones.

Citrix DaaS para Azure admite los siguientes métodos de autenticación de usuarios:

- **Azure AD administrado:** Azure AD administrado es una instancia de Azure Active Directory (AAD) proporcionada y administrada por Citrix. No es necesario que proporcione su propia estructura de Active Directory. Solo tiene que agregar sus usuarios al directorio.
- **Su proveedor de identidades:** Puede utilizar cualquier método de autenticación disponible en Citrix Cloud.

> **Nota:**
>
> - Las implementaciones de acceso con Remote PC utilizan solo Active Directory. Para obtener más información, consulte Acceso con Remote PC.
> - Si usa servicios de dominio de Azure AD: Los nombres principales de usuario (UPN) de inicio de sesión de Workspace deben contener el nombre de dominio que se especificó al habilitar los servicios de dominio de Azure AD. Los inicios de sesión no pueden usar nombres UPN para un dominio personalizado creado por usted, incluso aunque ese dominio personalizado se designe como dominio principal.

La configuración de la autenticación de usuarios incluye los siguientes procedimientos:

1. Configurar el método de autenticación de usuarios en Citrix Cloud y en Configuración de Workspace.
2. Si utiliza Azure AD administrado para la autenticación de usuarios, agregue usuarios al directorio.
3. Agregar usuarios a un catálogo.

Configurar la autenticación de usuarios en Citrix Cloud

Para configurar la autenticación de usuarios en Citrix Cloud:

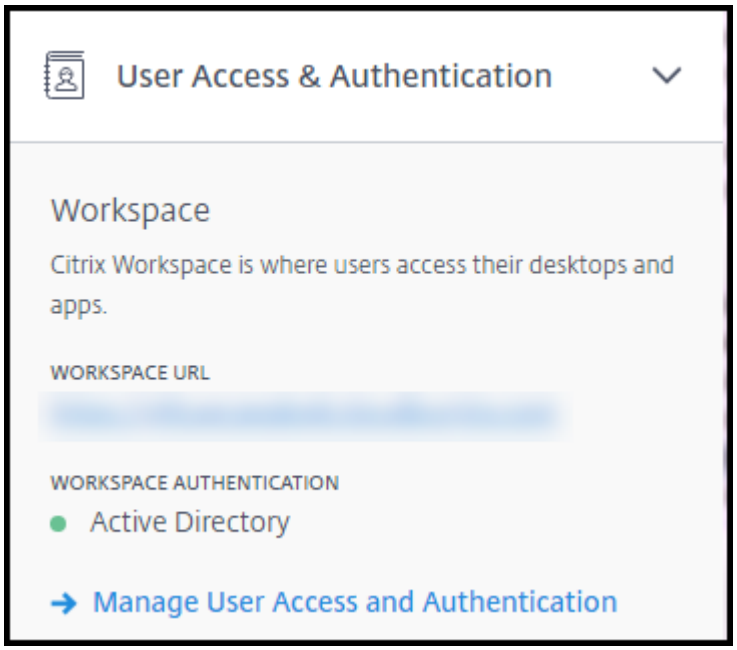
- Conéctese al método de autenticación de usuarios que quiera utilizar. (En Citrix Cloud, se "conecta"o "desconecta"de un método de autenticación.)
- En Citrix Cloud, configure la autenticación de Workspace para utilizar el método conectado.

> **Nota:**
>
> Está configurado el método de autenticación de Azure AD administrado de forma predeterminada. Es decir, se conecta automáticamente en Citrix Cloud y la autenticación de Workspace se establece automáticamente para usar Azure AD administrado para Citrix DaaS para Azure. Si desea utilizar este método (y no ha configurado previamente otro), continúe con Agregar y eliminar usuarios en Azure AD administrado.
> Si Azure AD administrado está desconectado, la autenticación de Workspace cambiará a Active

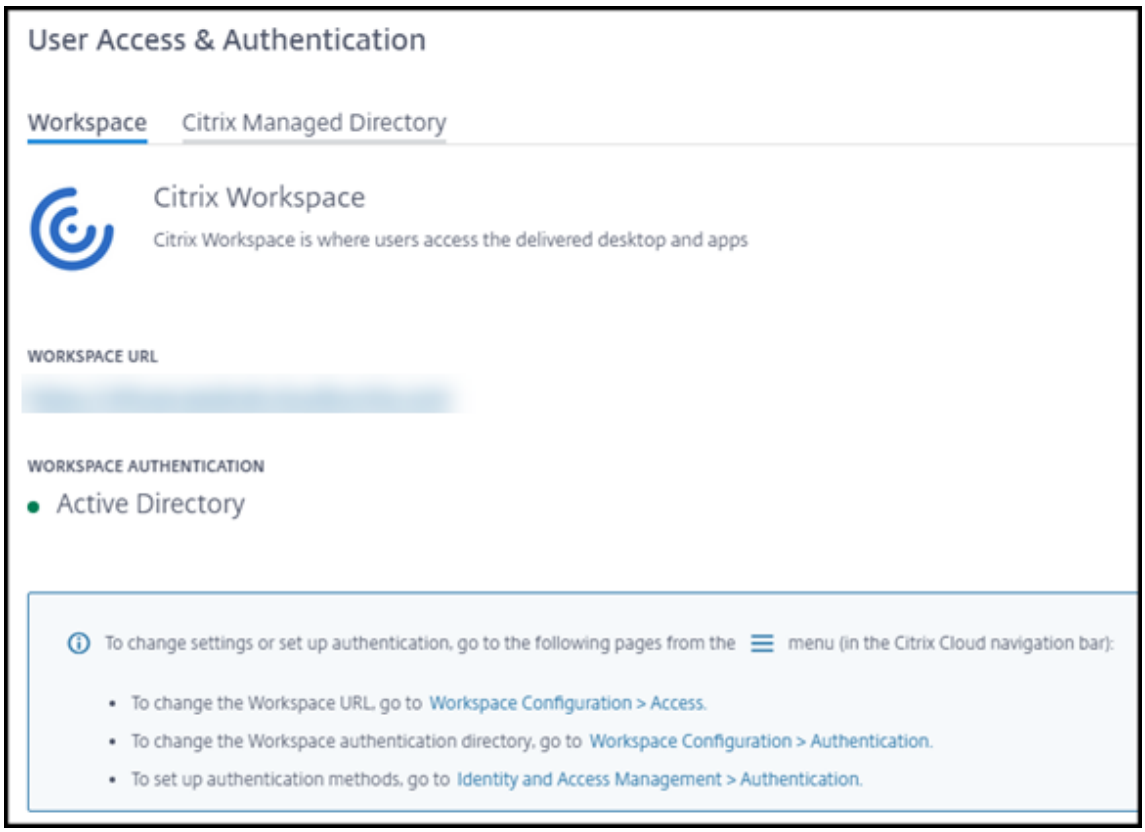
> Directory. Si quiere usar un método de autenticación diferente, siga los pasos que se indican a continuación.

Para cambiar el método de autenticación:

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, haga clic en **Acceso y autenticación de usuarios a** la derecha.



2. Haga clic en **Administrar acceso y autenticación de usuarios**. Seleccione la ficha **Área de trabajo**, si aún no está seleccionada. (La otra ficha indica qué método de autenticación de usuario está configurado actualmente).



3. Siga el enlace **Para configurar los métodos de autenticación**. Este enlace le lleva a Citrix Cloud. Seleccione **Conectar** en el menú de puntos suspensivos del método que quiera.
4. Mientras esté en Citrix Cloud, seleccione **Configuración de Workspace** en el menú superior de la izquierda. En la ficha **Autenticación**, seleccione el método que prefiera.

Qué hacer a continuación:

- Si utiliza Azure AD administrado, agregue usuarios al directorio.
- Para todos los métodos de autenticación, agregue usuarios al catálogo.

Agregar y eliminar usuarios en Azure AD administrado

Complete este procedimiento solo si utiliza Azure AD administrado para la autenticación de usuarios en Citrix Workspace.

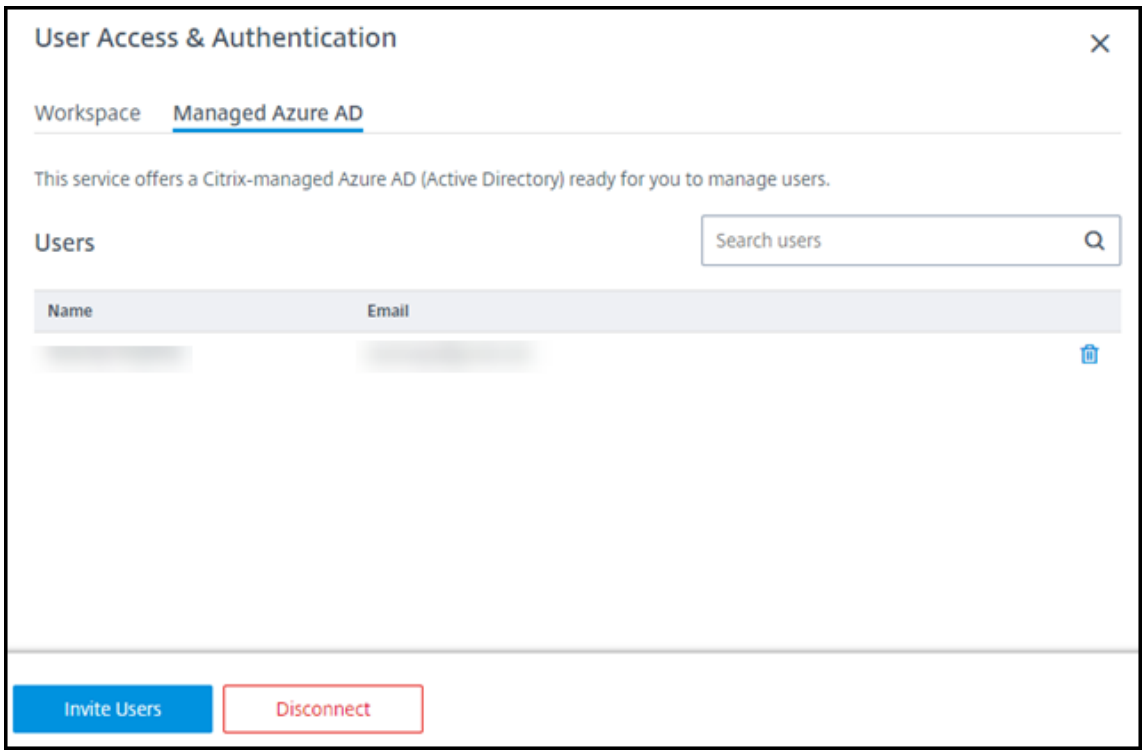
Debe proporcionar el nombre y las direcciones de correo electrónico de sus usuarios. A continuación, Citrix envía una invitación por correo electrónico a cada uno de ellos. El correo electrónico indica a los usuarios que hagan clic en un enlace que los une a Citrix Managed Azure AD.

- Si el usuario ya tiene una cuenta Microsoft con la dirección de correo electrónico que proporcionó, se utiliza esa cuenta.

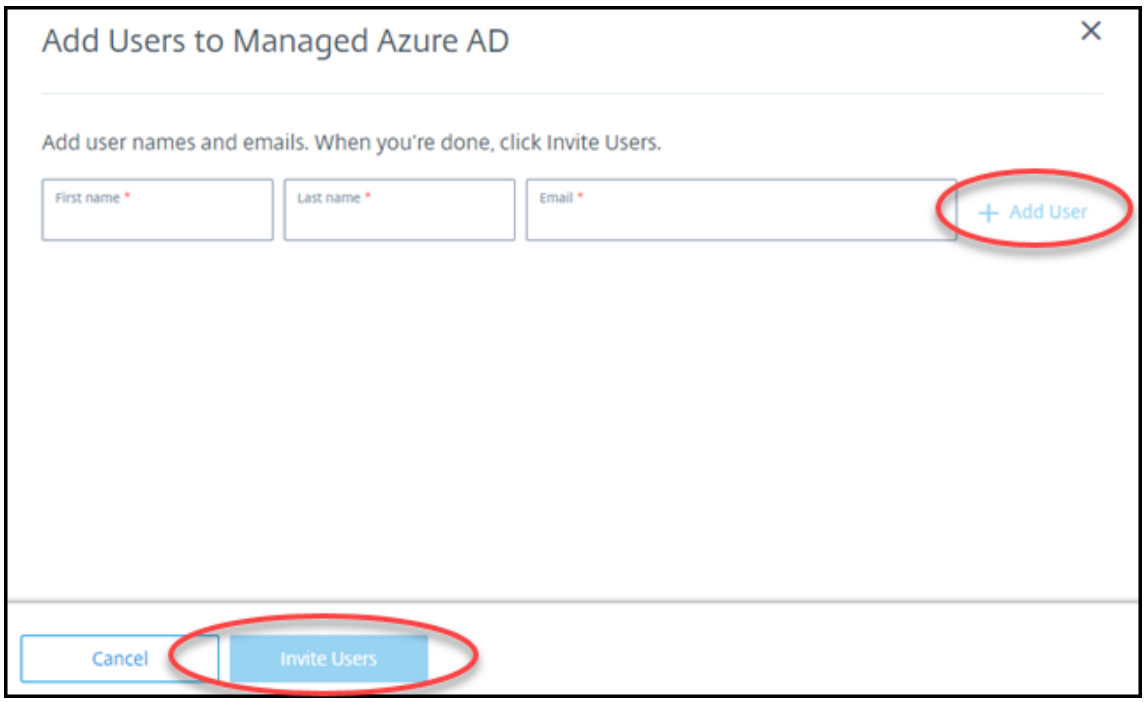
- Si el usuario no tiene una cuenta Microsoft con la dirección de correo electrónico, Microsoft crea una cuenta.

Para agregar e invitar usuarios a Azure AD administrado:

1. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Acceso y autenticación de usuarios a** la derecha. Haga clic en **Administrar acceso y autenticación de usuarios**.
2. Haga clic en la ficha **Azure AD administrado**.
3. Haga clic en **Invitar a usuarios**



4. Escriba el nombre y la dirección de correo electrónico de un usuario y, a continuación, haga clic en **Agregar usuario**.



5. Repita el paso anterior para agregar otros usuarios.
6. Cuando haya terminado de agregar la información de los usuarios, haga clic en **Invitar usuarios** en la parte inferior de la tarjeta.

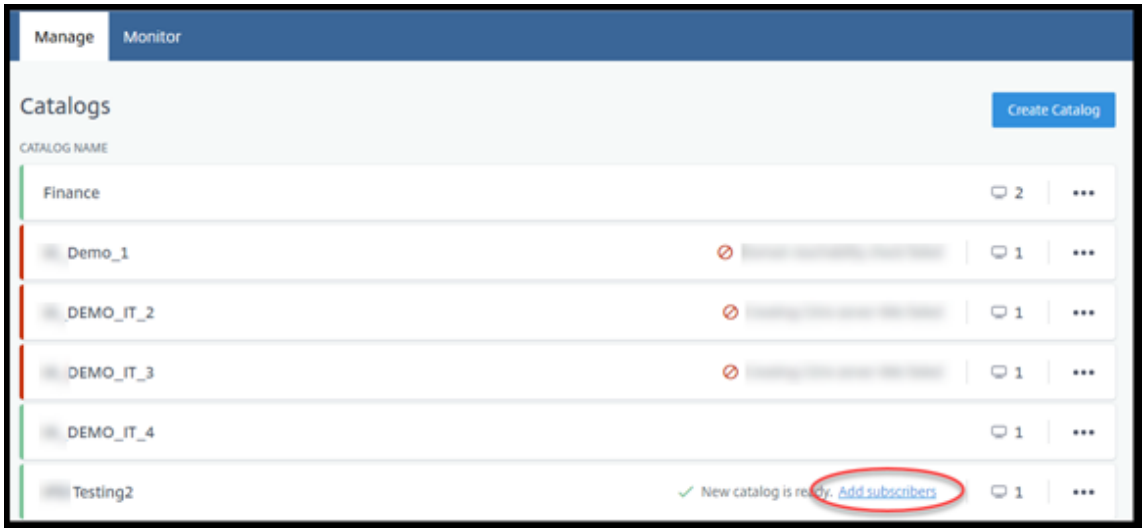
Para eliminar un usuario de Azure AD administrado, haga clic en el icono de papelera junto al nombre del usuario que desea eliminar del directorio. Confirme la eliminación.

Qué hacer a continuación: Agregar usuarios al catálogo

Agregar o quitar usuarios de los catálogos

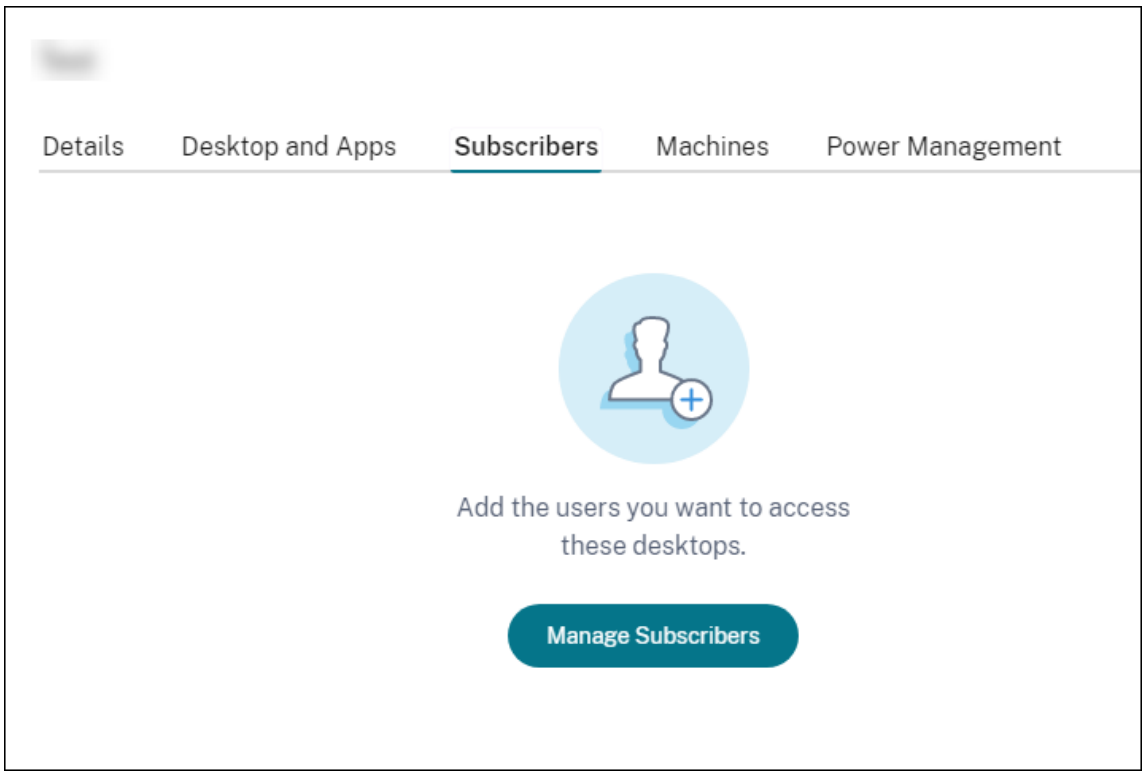
Complete este procedimiento, independientemente del método de autenticación que utilice.

1. En el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, si no ha agregado ningún usuario a un catálogo, haga clic en **Agregar suscriptores**.

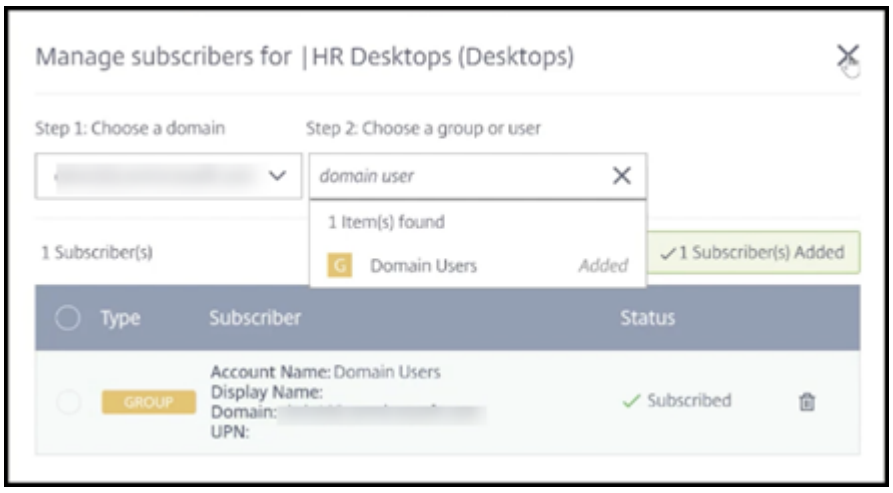


Para agregar usuarios a un catálogo que ya tiene usuarios, haga clic en cualquier parte de la entrada del catálogo.

2. En la ficha **Suscriptores**, haga clic en **Administrar suscriptores**.



3. Seleccione un dominio. (Si utiliza Azure AD administrado para la autenticación de usuarios, solo hay una entrada en el campo de dominio.) A continuación, seleccione un usuario.



4. Seleccione otros usuarios, según sea necesario. Cuando haya terminado, haga clic en la **X** en la esquina superior derecha.

Para quitar usuarios de un catálogo, siga los pasos 1 y 2. En el paso 3, haga clic en el icono de la papelera junto al nombre que quiere eliminar (en lugar de seleccionar un dominio y un grupo/usuario). Esta acción quita al usuario del catálogo, no del origen (como Azure AD administrado o su propio AD o AAD).

Qué hacer a continuación:

- Para un catálogo con máquinas multisesión, agregue aplicaciones, si aún no lo ha hecho.
- Para todos los catálogos, envíe la URL de Citrix Workspace a sus usuarios.

Más información

Para obtener más información sobre la autenticación en Citrix Cloud, consulte Administración de acceso e identidad.

Administrar catálogos

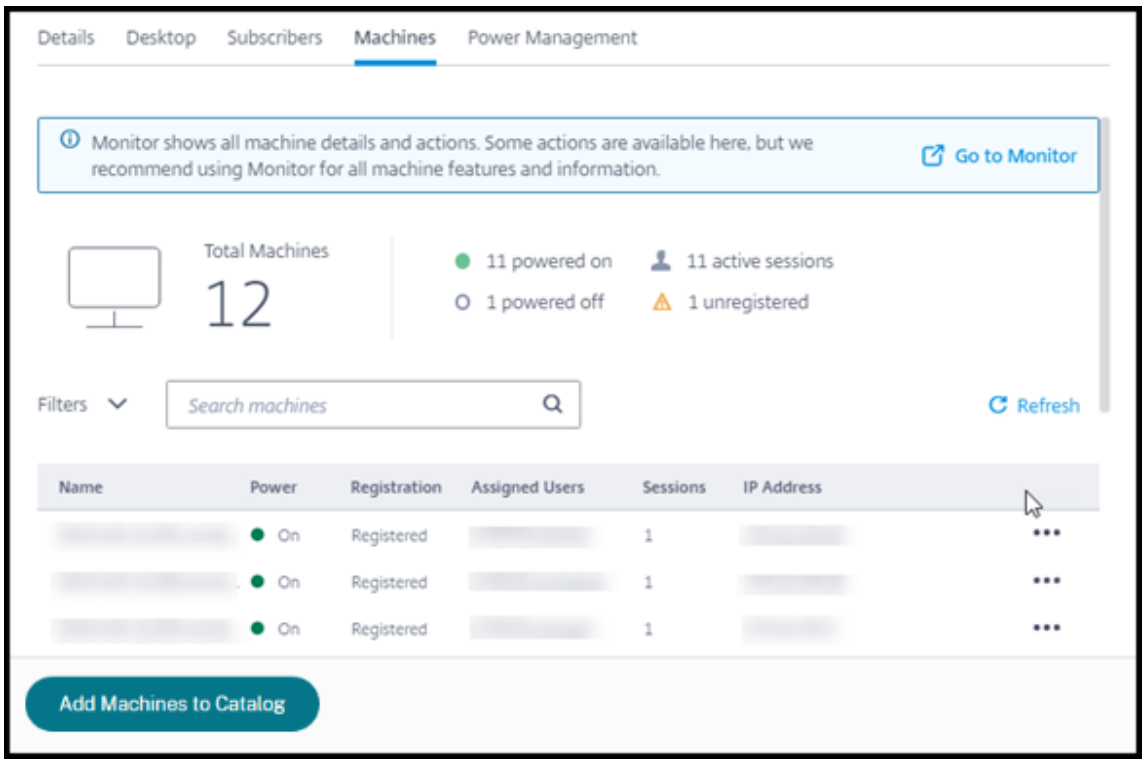
September 7, 2022

> **Nota:**
>
> En este artículo se describen las tareas que puede utilizar para administrar catálogos que se crearon en la interfaz de Distribución rápida. Para obtener información sobre la administración de catálogos mediante la interfaz de administración de configuración completa, consulte Administrar catálogos de máquinas.

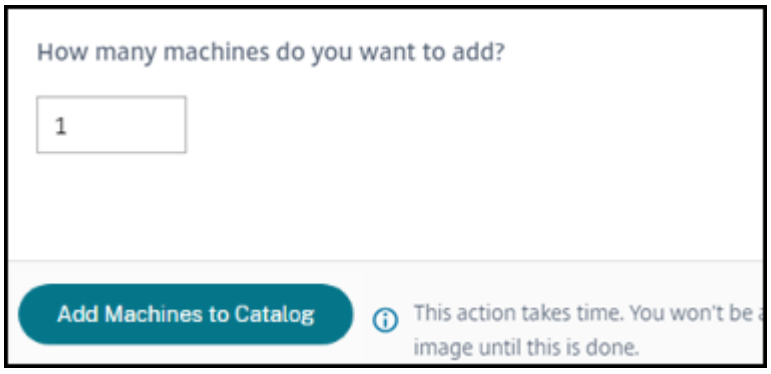
Agregar máquinas a un catálogo

Mientras las máquinas se agregan a un catálogo, no puede realizar ningún otro cambio en ese catálogo.

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Máquinas**, haga clic en **Agregar máquinas al catálogo**.



3. Introduzca la cantidad de máquinas que quiere agregar al catálogo.



4. (Válido solo si el catálogo está unido a un dominio.) Introduzca el nombre de usuario y la contraseña de la cuenta de servicio.
5. Haga clic en **Agregar máquinas al catálogo**.

No se puede reducir el recuento de máquinas de un catálogo. Sin embargo, puede utilizar los parámetros de programación de administración de energía para controlar cuántas máquinas se encienden o eliminar máquinas individuales de la ficha **Máquinas**. Consulte Administrar máquinas de un catálogo para obtener información sobre cómo eliminar máquinas en la ficha **Máquinas**.

Cambiar la cantidad de sesiones por máquina

Cambiar la cantidad de sesiones por máquina multisesión puede afectar a la experiencia de los usuarios. Aumentar este valor puede reducir los recursos de procesamiento asignados a sesiones simultáneas. Recomendación: Observe los datos de uso para determinar el equilibrio adecuado entre la experiencia de usuario y el coste.

1. En el panel **Administrar > Azure Quick Deploy**, seleccione un catálogo que contenga máquinas multisesión.
2. En la ficha **Detalles**, haga clic en **Modificar** junto a **Sesiones por máquina**.
3. Introduzca un nuevo número de sesiones por máquina
4. Haga clic en **Actualizar número de sesiones**.
5. Confirme la solicitud.

Este cambio no afecta a las sesiones actuales. Al cambiar el número máximo de sesiones a un valor inferior al de las sesiones activas actualmente de una máquina, el nuevo valor se implementa mediante la amortización habitual de sesiones activas.

Si se produce un error antes de que comience el proceso de actualización, la pantalla **Detalles** del catálogo conserva el número correcto de sesiones. Si se produce un error durante el proceso de actualización, la pantalla indica el número de sesiones que quería.

Administrar máquinas de un catálogo

> **Nota:**
>
> Muchas de las acciones que están disponibles en el panel **Administrar > Implementación rápida de Azure** también están disponibles en el panel **Supervisar** en Citrix DaaS Standard para Azure (anteriormente servicio Citrix Virtual Apps and Desktops Standard for Azure).

Para seleccionar acciones en el panel **Administrar > Azure Quick Deploy** :

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada de un catálogo.
2. En la ficha **Máquinas**, busque la máquina que quiere administrar. En el menú de puntos suspensivos de esa máquina, seleccione la acción deseada:

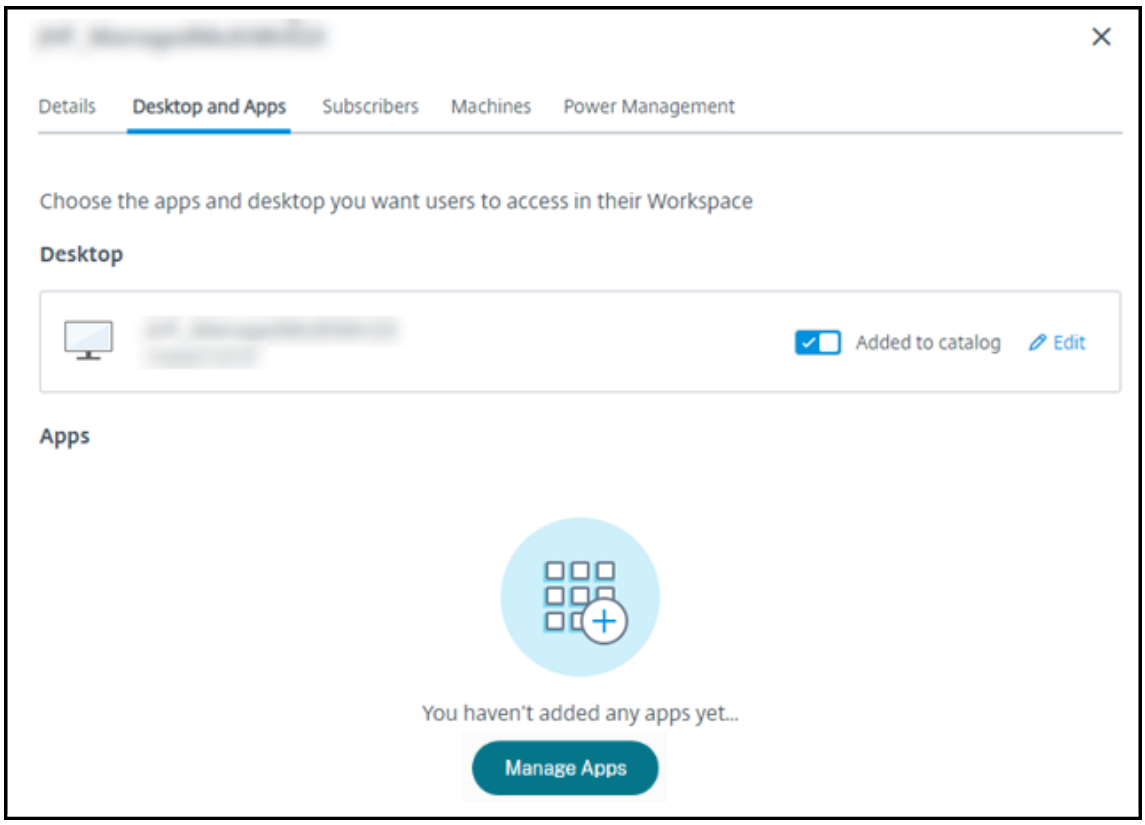
- **Reiniciar:** reinicie la máquina seleccionada.
- **Inicio:** inicie la máquina seleccionada. Esta acción solo está disponible si la máquina está apagada.
- **Apagar:** Apague la máquina seleccionada. Esta acción solo está disponible si la máquina está encendida.
- **Activar/desactivar el modo de mantenimiento:** Active el modo de mantenimiento (si está apagado) o apague (si está encendido) para la máquina seleccionada.

  De forma predeterminada, el modo de mantenimiento de una máquina está desactivado. Al activar el modo de mantenimiento de una máquina, se evitan nuevas conexiones a esa máquina. Los usuarios pueden conectarse a las sesiones existentes de esa máquina, pero no pueden iniciar nuevas sesiones en la misma. Puede poner una máquina en modo de mantenimiento antes de aplicar parches o para solucionar problemas.
- **Eliminar:** elimina la máquina seleccionada. Esta acción solo está disponible cuando el recuento de sesiones de la máquina es cero. Confirme la eliminación.

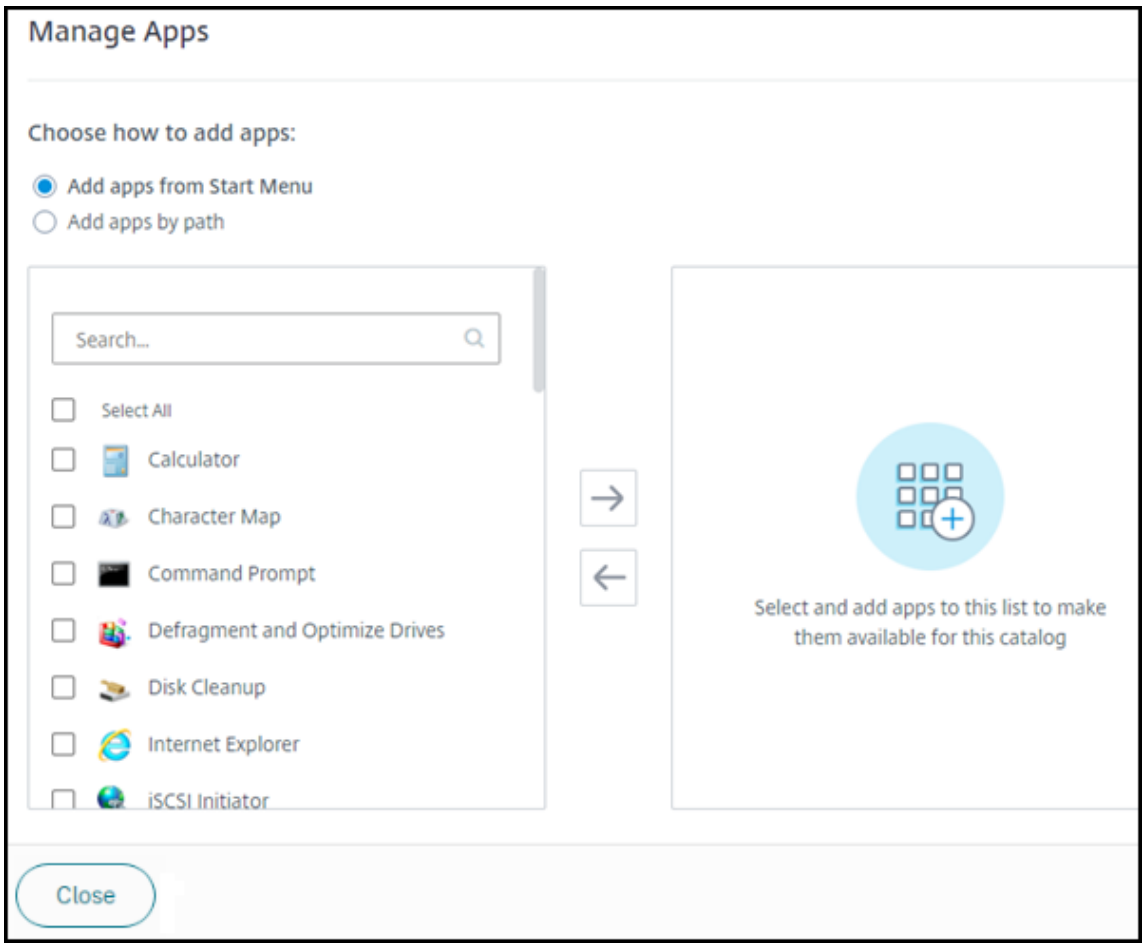
  Cuando se elimina una máquina, se eliminan todos los datos de la máquina.
- **Forzar reinicio:** fuerza el reinicio de la máquina seleccionada. Seleccione esta acción solo si falla una acción de **reinicio** para la máquina.

Agregar aplicaciones a un catálogo

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Escritorio y aplicaciones**, haga clic en **Administrar aplicaciones**.

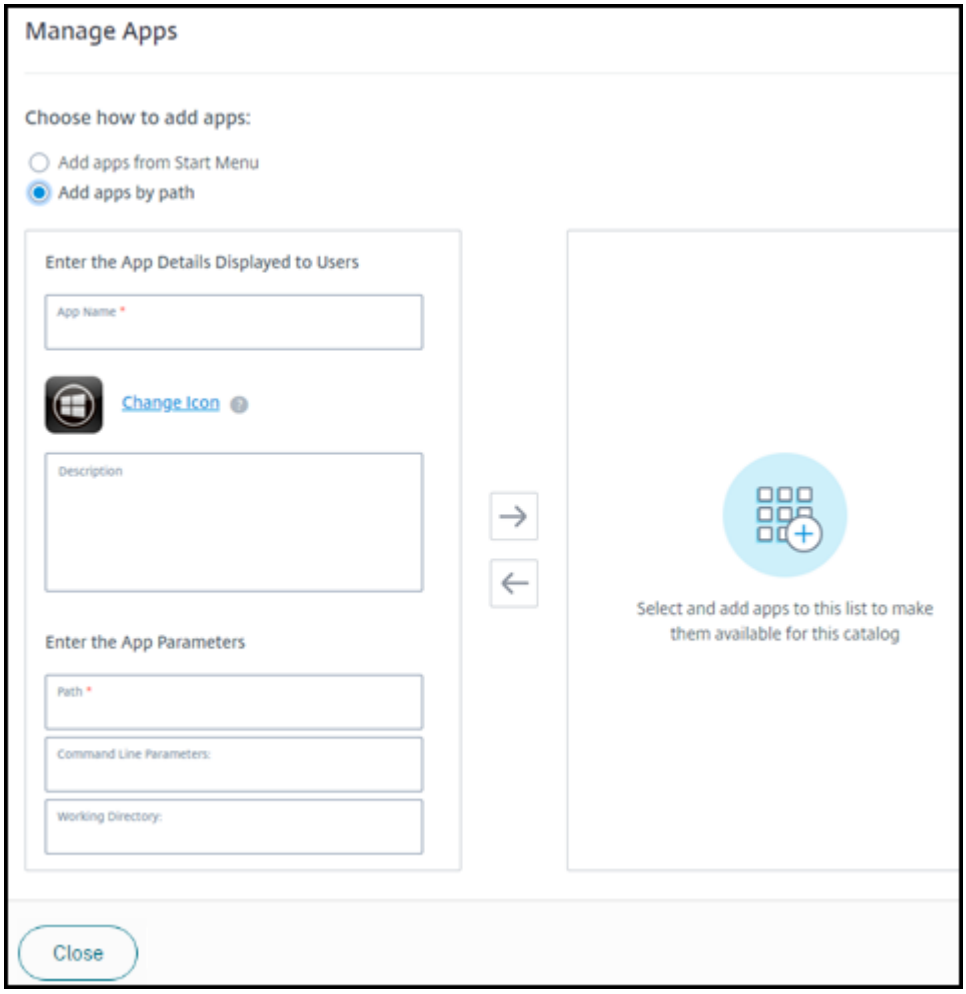


3. Seleccione cómo va a agregar aplicaciones: Desde el menú **Inicio** de las máquinas del catálogo o desde una ruta distinta de las máquinas.
4. Para agregar aplicaciones desde el menú **Inicio**:



- Seleccione las aplicaciones disponibles en la columna de la izquierda. (Use **Buscar** para personalizar la lista de aplicaciones). Haga clic en la flecha derecha entre las columnas. Las aplicaciones seleccionadas se desplazan a la columna derecha.
- Del mismo modo, para quitar aplicaciones, selecciónelas en la columna derecha. Haga clic en la flecha izquierda entre las columnas.
- Si el menú **Inicio** tiene más de una versión de la misma aplicación, con el mismo nombre, solo puede agregar una. Para agregar otra versión de esa aplicación, modifique el nombre de esa versión. A continuación, podrá agregar esa versión de la aplicación.

5. Para agregar aplicaciones por ruta:



- Introduzca el nombre de la aplicación. Este es el nombre que ven los usuarios en Citrix Workspace.
- El icono que se muestra es el que ven los usuarios en Citrix Workspace. Para seleccionar otro icono, haga clic en **Cambiar icono** y navegue hasta el icono que quiere mostrar.
- (Opcional) Introduzca una descripción de la aplicación.
- Introduzca la ruta de acceso a la aplicación. Este campo es obligatorio. Opcionalmente, agregue parámetros de línea de comandos y el directorio de trabajo. Para obtener más información sobre los parámetros de la línea de comandos, consulte Pasar parámetros a las aplicaciones publicadas.

6. Cuando haya terminado, haga clic en **Cerrar**.

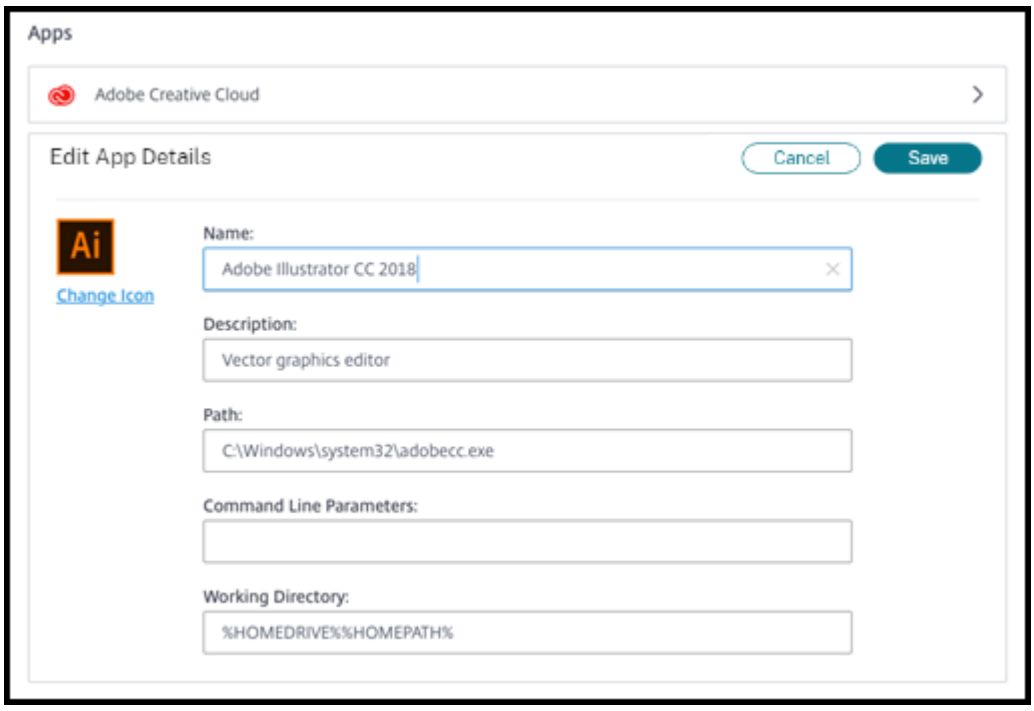
Qué hacer a continuación (si va a completar el flujo de creación y entrega del catálogo): envíe la URL de Citrix Workspace a los usuarios, si aún no lo ha hecho.

En los VDA de Windows Server 2019, es posible que los iconos de algunas aplicaciones no se muestren correctamente durante la configuración ni en el espacio de trabajo de los usuarios. Como solución alternativa, una vez publicada la aplicación, modifíquela y utilice la función **Cambiar icono** para asignar

otro icono que se muestre correctamente.

Modificación de una aplicación en un catálogo

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Escritorio y aplicaciones**, haga clic en cualquier parte de la fila que contiene la aplicación que quiere modificar.
3. Haga clic en el icono del lápiz.



4. Introduzca cambios en cualquiera de los siguientes campos:
   - **Nombre:** Nombre que ven los usuarios en Citrix Workspace.
   - **Descripción**
   - **Ruta:** La ruta al archivo ejecutable.
   - **Parámetros de línea de comandos:** Para obtener más información, consulte Transferir parámetros a aplicaciones publicadas.
   - **Directorio de trabajo**
5. Para cambiar el icono que los usuarios ven en su Citrix Workspace, haga clic en **Cambiar icono** y vaya al icono que quiere mostrar.
6. Haga clic en **Guardar** cuando haya terminado.

Transferir parámetros a aplicaciones publicadas

Al asociar una aplicación publicada a tipos de archivos, los símbolos de porcentaje y asterisco (entre comillas) se agregan al final de la línea de comandos. Estos símbolos actúan como marcadores de posición para los parámetros transferidos a los dispositivos de usuario.

- Si una aplicación publicada no se inicia cuando se espera, verifique que la línea de comandos contiene los símbolos correctos. De forma predeterminada, los parámetros proporcionados por los dispositivos de usuario se validan si se agregan los símbolos.

  Para las aplicaciones publicadas que utilizan parámetros personalizados suministrados por el dispositivo de usuario, se agregan los símbolos a la línea de comandos para omitir la validación de la línea de comandos. Si los símbolos no aparecen en la línea de comandos de la aplicación, agréguelos manualmente.

- Si la ruta del archivo ejecutable contiene nombres de directorios con espacios (como "C:\Archivos de programa"), escriba la línea de comandos de la aplicación entre comillas para indicar que los espacios pertenecen a la línea de comandos. Agregue comillas dobles al principio y al final de la ruta. Asimismo, deberá agregar otro conjunto de comillas dobles al principio y al final de los símbolos de porcentaje y asterisco. Incluya un espacio entre la comilla de cierre de la ruta y la de apertura de los símbolos de porcentaje y asterisco.

  Por ejemplo, la línea de comandos de la aplicación publicada Reproductor de Windows Media es: `" C:\Program Files\Windows Media Player\mplayer1.exe" "%*"`

Quitar aplicaciones de un catálogo

Al quitar una aplicación de un catálogo, no se quita de las máquinas. Simplemente impide que aparezca en Citrix Workspace.

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Escritorio y aplicaciones**, haga clic en el icono de papelera situado junto a las aplicaciones que quieras eliminar.

Eliminar un catálogo

Al eliminar un catálogo, todas las máquinas que contiene se destruyen permanentemente. La eliminación de un catálogo no se puede invertir.

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.

2. En la ficha **Detalles**, haga clic en **Eliminar catálogo** en la parte inferior de la ventana.
3. Confirme la eliminación seleccionando las casillas de verificación de reconocimiento y, a continuación, haciendo clic en el botón de confirmación.

Para ayudar a identificar cuentas de máquina residuales de Active Directory que debe eliminar, puede descargar una lista de nombres de máquina y Cloud Connector.

Administrar programaciones de administración de energía

Una programación de administración de energía afecta a todas las máquinas de un catálogo. Una programación proporciona:

- Experiencia de usuario óptima: Las máquinas están disponibles para los usuarios cuando las necesitan.
- Seguridad: Las sesiones de escritorio que permanecen inactivas durante un intervalo especificado se desconectan, lo que requiere que los usuarios inicien una nueva sesión en su espacio de trabajo.
- Administración de costes y ahorro de energía: Las máquinas con escritorios que permanecen inactivos se apagan. Las máquinas se encienden para satisfacer la demanda programada y real.

Puede configurar una programación de energía al crear un catálogo personalizado o hacerlo más tarde. Si no se selecciona ni configura ninguna programación, una máquina se apaga cuando finaliza una sesión.

No se puede seleccionar ni configurar una programación de energía al crear un catálogo con creación rápida. De forma predeterminada, los catálogos de creación rápida utilizan la programación preestablecida Ahorro de costes. Puede seleccionar o configurar una programación diferente más adelante para ese catálogo.

La administración de programaciones incluye:

- Saber qué información contiene una programación
- Crear una programación

Información en una programación

En el siguiente diagrama se muestran los parámetros de programación de un catálogo que contiene máquinas multisesión. Los parámetros de un catálogo que contiene máquinas de sesión única (aleatorias o estáticas) difieren ligeramente.

Una programación de administración de energía contiene la siguiente información.

Programaciones preestablecidas Citrix DaaS para Azure ofrece varios programas preestablecidos. También puede configurar y guardar programaciones personalizadas. Aunque puede eliminar parámetros preestablecidos personalizados, no puede eliminar los parámetros preestablecidos proporcionados por Citrix.

Zona horaria Se utiliza con la configuración de encendido de máquinas para establecer las horas de trabajo y fuera de horario, según la zona horaria seleccionada.

Esta configuración es válida para todos los tipos de máquinas.

Encender máquinas: Horas de trabajo y fuera de horario laboral Los días de la semana y las horas de inicio-parada del día que forman su horario de trabajo. Por lo general, indica los intervalos en los que quiere encender las máquinas. Cualquier momento fuera de esos intervalos se considera fuera del horario laboral. Varios parámetros de programación le permiten introducir valores separados para las horas de trabajo y fuera de horario. Otros parámetros son aplicables todo el tiempo.

Esta configuración es válida para todos los tipos de máquinas.

Desconectar sesiones de escritorio en caso de inactividad Cuánto tiempo puede permanecer inactivo (sin utilizar) un escritorio antes de que se desconecte la sesión. Después de desconectar una sesión, el usuario debe ir a Workspace e iniciar un escritorio de nuevo. Es un parámetro de seguridad.

Esta configuración es válida para todos los tipos de máquinas. Se aplica un parámetro todo el tiempo.

Apagar escritorios inactivos Cuánto tiempo puede permanecer desconectada una máquina antes de que se apague. Después de apagar una máquina, el usuario debe ir a Workspace e iniciar un escritorio de nuevo. Se trata de un parámetro de ahorro de energía.

Supongamos, por ejemplo, que quiere que los escritorios se desconecten después de que hayan estado inactivos durante 10 minutos. A continuación, las máquinas se apagan si permanecen desconectados durante otros 15 minutos.

Si Tom deja de usar su escritorio y se va a una reunión de una hora, el escritorio se desconectará después de 10 minutos. Después de otros 15 minutos, la máquina se apagará (25 minutos en total).

Desde el punto de vista del usuario, los dos parámetros de inactividad (desconexión y apagado) tienen el mismo efecto. Si Tom permanece alejado de su escritorio durante 12 minutos o una hora, debe volver a iniciar un escritorio desde Workspace. La diferencia entre los dos temporizadores afecta al estado de la máquina virtual que proporciona el escritorio.

Esta configuración es válida para máquinas de sesión única (estáticas o aleatorias). Puede introducir valores para horas de trabajo y fuera de horario laboral.

Cerrar las sesiones desconectadas Cuánto tiempo puede permanecer desconectada una máquina antes de que se cierre la sesión.

Esta configuración es válida para máquinas multisesión. Se aplica un parámetro todo el tiempo.

Demora de apagado La cantidad mínima de tiempo que una máquina debe estar encendida antes de que pueda apagarse (junto con otros criterios). Este parámetro evita que las máquinas se activen y se desactiven de forma intermitente durante demandas de sesión volátiles.

Esta configuración es válida para máquinas multisesión y se aplica todo el tiempo.

Mínimo de máquinas en ejecución Cuántas máquinas deben permanecer encendidas, independientemente de cuánto tiempo estén inactivas o desconectadas.

Esta configuración es válida para máquinas aleatorias y multisesión. Puede introducir valores para horas de trabajo y fuera de horario laboral.

Búfer de capacidad Un búfer de capacidad ayuda a adaptarse a los picos repentinos de demanda, al mantener un búfer de máquinas encendidas. El búfer se especifica como porcentaje de la demanda de sesiones actual. Por ejemplo, si hay 100 sesiones activas y el búfer de capacidad es del 10%, Citrix DaaS para Azure proporciona capacidad para 110 sesiones. Pueden producirse picos de demanda durante las horas de trabajo o al agregar nuevas máquinas al catálogo.

Un valor menor disminuye el coste. Un valor superior contribuye a garantizar una experiencia de usuario optimizada. Al iniciar sesiones, los usuarios no tienen que esperar a que se enciendan máquinas adicionales.

Cuando hay máquinas más que suficientes para admitir la cantidad necesaria de máquinas encendidas (búfer de capacidad incluido) en el catálogo, se apagan las máquinas adicionales. Es posible que se produzca un apagado debido a la menor actividad durante horas normales, al cierre de sesiones o a una cantidad menor de máquinas en el catálogo. La decisión de apagar una máquina debe cumplir con los siguientes criterios:

- La máquina está encendida y no en modo de mantenimiento.
- La máquina está registrada como disponible o en espera de registrarse después del encendido.
- La máquina no tiene sesiones activas. Las sesiones restantes han finalizado. (La máquina estuvo inactiva durante el período de tiempo de espera por inactividad.)
- La máquina ha estado encendida durante al menos “X”minutos, donde “X”representa la demora de apagado especificada para el catálogo.

  En un catálogo estático, una vez asignadas todas las máquinas del catálogo, el búfer de capacidad no juega ningún papel en el encendido o apagado de las máquinas.

Esta configuración es válida para todos los tipos de máquinas. Puede introducir valores para horas de trabajo y fuera de horario laboral.

Creación de un programa de administración de energía

1. En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Administración de energía**, determine si alguna de las programaciones preestablecidas (en el menú de la parte superior) satisface sus necesidades. Seleccione un parámetro preestablecido para ver los valores que utiliza. Si quiere utilizar un parámetro preestablecido, déjelo seleccionado.
3. Si cambia los valores de cualquier campo (como días, horas o intervalos), la selección preestablecida cambia a **Personalizado** automáticamente. Un asterisco indica que los parámetros personalizados no se han guardado.
4. Establezca los valores que quiera para la programación personalizada.
5. Haga clic en **Personalizado** en la parte superior y guarde los ajustes actuales como un nuevo ajuste preestablecido. Introduzca un nombre para el nuevo ajuste preestablecido y haga clic en la marca de verificación.
6. Cuando haya terminado, haga clic en **Guardar cambios**.

Más adelante, puede modificar o eliminar un parámetro preestablecido personalizado con los iconos de lápiz o papelera del menú **Parámetros preestablecidos**. Los parámetros preestablecidos comunes no se pueden modificar ni eliminar.

Instantánea y restauración de VDA

Las funciones de instantáneas y restauración de Citrix DaaS para Azure proporcionan una forma de recuperarse de la pérdida de datos no planificada u otros errores en los VDA que entregan escritorios y aplicaciones. La operación de instantánea toma y almacena una instantánea de la máquina. Más adelante, una operación de restauración utiliza una instantánea que seleccione.

- Puede configurar programaciones de instantáneas diarias y semanales para todas las máquinas de un catálogo. Estas instantáneas se denominan *instantáneas automáticas*. Se toma una instantánea de cada máquina del catálogo. No hay programaciones de instantáneas predeterminadas.
- Puede hacer una copia de seguridad de una sola V en un catálogo a petición. Esto se denomina instantánea manual. Puede crear una *instantánea manual* de una máquina incluso si el catálogo al que pertenece tiene instantáneas programadas. (Sin embargo, no puede programar instantáneas de un solo equipo).

> **Importante:**
>
> Las funciones de instantáneas y restauración de Citrix DaaS para Azure solo se admiten en máquinas de catálogos estáticos y se asignan a los usuarios.

Programaciones de instantáneas

Recuerde: Las programaciones de instantáneas se aplican a todas las máquinas de un catálogo.

De forma predeterminada, no hay programaciones de instantáneas.

Para administrar las programaciones de instantáneas:

1. En el panel **Administrar**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Detalles**, haga clic en **Programar instantáneas**.
3. En la página **Programar instantáneas**, configure programaciones para instantáneas automáticas semanales o diarias, o ambas:
    - Para agregar o cambiar instantáneas semanales, mueva el control deslizante de **Instantáneas automáticas semanales** hasta que aparezca una marca de verificación. Selecciona el día de la semana y la hora de inicio.
    - Para agregar o cambiar instantáneas diarias, mueva el control deslizante de **Instantáneas automáticas diarias** hasta que aparezca una marca de verificación. Selecciona la hora de inicio.
    - Para eliminar instantáneas semanales, mueva el control deslizante de **Instantáneas automáticas semanales** hasta que aparezca una **X**.
    - Para eliminar instantáneas diarias, mueva el control deslizante de **Instantáneas automáticas diarias** hasta que aparezca una **X**.
4. Cuando termine, haga clic en **Guardar** en la parte inferior de la página.

Instantáneas manuales

Una instantánea manual es para una sola máquina de un catálogo. (No puede crear un programa para tomar una instantánea de máquinas individuales).

1. En el panel **Administrar**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Máquinas**, busque la máquina de la que quiere tomar una instantánea. Seleccione **Instantáneas** en el menú de puntos suspensivos para esa máquina.
3. En la página **Snapshots for *VDA-name***, haga clic en **Crear instantánea manual**.
4. Proporcione un nombre para la instantánea. Recomendado: Elija un nombre que pueda identificar fácilmente más adelante.
5. Confirme la solicitud.

Ver y administrar instantáneas

1. En el panel **Administrar**, haga clic en cualquier parte de la entrada del catálogo.

2. En la ficha **Máquinas**, busque la máquina de la que quiere tomar una instantánea. Seleccione **Instantáneas** en el menú de puntos suspensivos para esa máquina.
3. En la página **Backups for *VDA-name***:

    - Si no hay instantáneas para la máquina, un mensaje lo guía para crear una instantánea manual para esta máquina o crear instantáneas programadas para todas las máquinas del catálogo que contiene esta máquina.
    - Puede seleccionar una de las instantáneas y restaurar el equipo. Consulte Restaurar.
    - Puede eliminar instantáneas. Seleccione las casillas de verificación de una o más instantáneas y, a continuación, haga clic en **Eliminar** en el encabezado de la tabla. Confirme la solicitud.

Sugerencia: Al eliminar un catálogo, se destruyen todas las instantáneas.

Restore

Puede restaurar una máquina desde cualquier instantánea disponible para esa máquina.

Durante una restauración, el equipo se apaga. Ninguna de las acciones del menú de puntos suspensivos de una máquina está disponible mientras se restaura una instantánea.

1. En el panel **Administrar**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Máquinas**, busque la máquina de la que quiere tomar una instantánea. Seleccione **Instantáneas** en el menú de puntos suspensivos para esa máquina.
3. En la página **Snapshots for *VDA-name (***), seleccione la casilla de verificación de la instantánea que quiere usar.
4. Haga clic en **Restaurar** en el encabezado de tabla.
5. Confirme la solicitud.

La columna **Estado** de la ficha **Máquinas** indica el progreso y el resultado de la operación de restauración.

Si un equipo no puede restaurar una instantánea, inténtelo de nuevo.

Información relacionada

- Actualizar un catálogo con una nueva imagen
- Agregar y quitar usuarios de un catálogo
- Unidas a un dominio y no unidas a un dominio

Supervisar

May 9, 2023

Desde el panel **Supervisar**, puede ver el uso del escritorio, las sesiones y las máquinas en la implementación de Citrix DaaS Standard para Azure (anteriormente Citrix Virtual Apps and Desktops Standard para Azure). También puede controlar sesiones, administrar la energía de máquinas y detener la ejecución de aplicaciones y procesos.

Para acceder al panel **Monitor** :

1. Inicie sesión en Citrix Cloud si aún no lo ha hecho. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**.
2. En el panel **Administrar**, haga clic en la ficha **Supervisar**.

Supervisar el uso de escritorios

Las pantallas de esta página se actualizan cada cinco minutos.

- **Descripción general de máquinas y sesiones:** Puede personalizar la pantalla para mostrar información sobre todos los catálogos (valor predeterminado) o de un catálogo seleccionado. También puedes personalizar el período de tiempo: el último día, semana o mes.

  Los recuentos de la parte superior de la pantalla indican el número total de máquinas, además del número de máquinas encendidas y apagadas. Sitúe el cursor sobre un valor para mostrar cuántos son sesión única y multisesión.

  El gráfico que aparece debajo de los recuentos muestra el número de máquinas encendidas y sesiones simultáneas pico en puntos regulares durante el período de tiempo seleccionado. Pase el puntero sobre un punto del gráfico para mostrar los recuentos en ese punto.

- **10 primeros:** Para personalizar una pantalla de los 10 primeros, seleccione un periodo de tiempo: la semana pasada (predeterminado), mes o tres meses. También puede personalizar la pantalla para mostrar solo información sobre la actividad de máquinas de sesión única, máquinas multisesión o aplicaciones.
  - **Los 10 usuarios más activos:** Enumera los usuarios que iniciaron escritorios con más frecuencia durante el período de tiempo. Al pasar el puntero sobre una línea, se muestra el total de inicios.
  - **10 catálogos activos principales:** Enumera los catálogos con mayor duración durante el período de tiempo seleccionado. La duración es la suma de todas las sesiones de usuario de ese catálogo.

Informe de uso de escritorios

Para descargar un informe que contenga información sobre los lanzamientos de máquinas durante el último mes, haga clic en **Iniciar actividad**. Un mensaje indica que la solicitud se está procesando. El informe se descarga automáticamente en la ubicación de descarga predeterminada del equipo local.

Filtrar y buscar para supervisar máquinas y sesiones

Cuando supervisa la información de sesiones y máquinas, se muestran todas las máquinas o sesiones de forma predeterminada. Puede hacer lo siguiente:

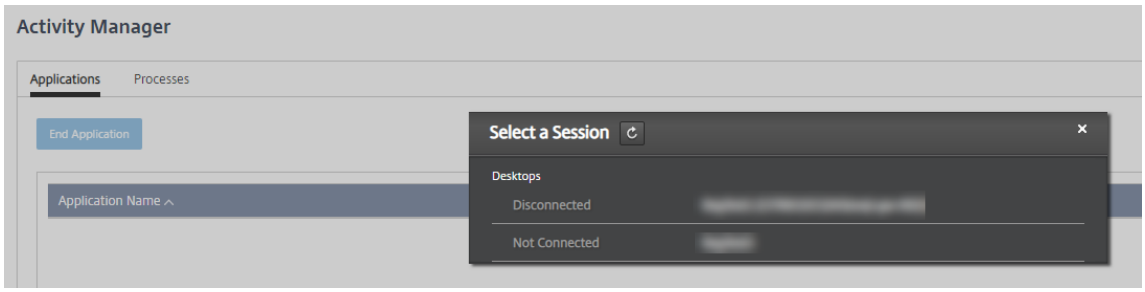
- La presentación se puede filtrar por máquinas, sesiones, conexiones o aplicaciones.
- Para filtrar la pantalla de sesiones o máquinas, elija los criterios que quiera, creando un filtro con expresiones.

- Puede guardar los filtros que cree para reutilizarlos.

Controlar las aplicaciones de un usuario

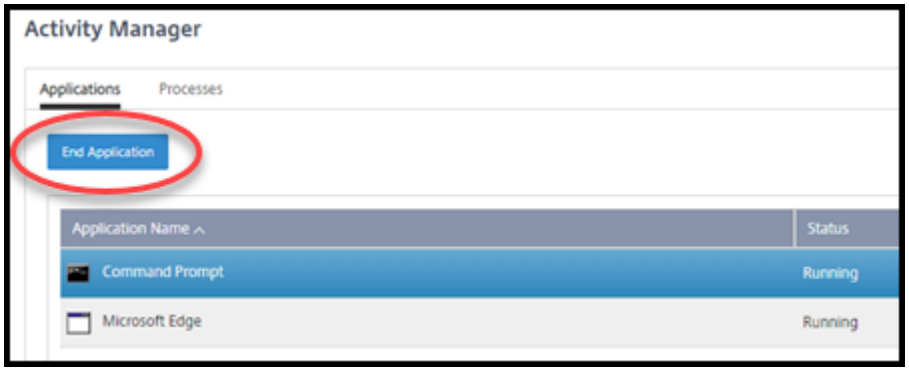
Puede mostrar y administrar las aplicaciones y procesos de un usuario que tenga una sesión en ejecución o un escritorio asignado.

1. En el panel **Supervisar**, haga clic en **Buscar** e introduzca el nombre de usuario (o los caracteres iniciales del nombre de usuario), la máquina o el punto final. En los resultados de búsqueda, seleccione el elemento que está buscando. (Para contraer el cuadro de búsqueda sin buscar, vuelva a hacer clic en **Buscar**).
2. Seleccione una sesión.



   Administrador de actividades enumera las aplicaciones y los procesos de la sesión del usuario.

3. Para finalizar una aplicación, en la ficha **Aplicaciones** del Administrador de actividades, haga clic en la fila de la aplicación para seleccionar esa aplicación y, a continuación, haga clic en **Finalizar aplicación**.



4. Para finalizar un proceso, en la ficha **Procesos** del Administrador de actividades, haga clic en la fila del proceso para seleccionar ese proceso y, a continuación, haga clic en **Finalizar proceso**.
5. Para mostrar los detalles de la sesión, haga clic en **Detalles** en la esquina superior derecha. Para volver a la pantalla de aplicaciones y procesos, haga clic en Administrador de actividades en la esquina superior derecha.

6. Para controlar la sesión, haga clic en **Control de sesión > Cerrar sesióno en Control de sesión > Desconectar**.

Remedar usuarios

Utilice la función Remedar para ver o trabajar directamente en la máquina virtual o la sesión de un usuario. Puede remedar agentes VDA para Windows y Linux. El usuario debe estar conectado a la máquina que se va a remedar. Para comprobarlo, consulte el nombre de máquina que aparece en la barra de título `User`.

El remedo se inicia en una nueva ficha de explorador. Asegúrese de que su explorador admite ventanas emergentes de la URL de Citrix Cloud.

En una suscripción de Azure gestionada por Citrix, el sombreado solo se admite para los usuarios de máquinas unidas a un dominio. Para ocultar una máquina que no esté unida a un dominio en una suscripción de Azure gestionada por Citrix, debe configurar una máquina bastión. Para obtener más información, consulte Acceso a bastiones.

El remedo debe iniciarse desde una máquina de la misma red virtual que las máquinas unidas al dominio y cumplir con todos los requisitos relativos a los puertos.

Habilitar el remedo

1. Desde el panel de mandos **Supervisar**, vaya a la vista **Detalles del usuario**.
2. Seleccione la sesión de usuario y, a continuación, haga clic en **Remedo** en la vista **Administrador de actividades** o en el panel **Detalles de la sesión**.

Remedar agentes Linux VDA

El remedo está disponible para agentes Linux VDA 7.16 y versiones posteriores que ejecutan las distribuciones Linux RHEL 7.3 o Ubuntu 16.04.

Supervisar utiliza el FQDN para conectarse al agente Linux VDA de destino. El cliente de Supervisar debe poder resolver el FQDN del agente Linux VDA.

- El VDA debe tener instalados los paquetes `python-websockify` y `x11vnc`.
- En la conexión `noVNC` al VDA, se utiliza el protocolo WebSocket. De forma predeterminada, se usa el protocolo WebSocket `ws://`. Por motivos de seguridad, Citrix recomienda usar el protocolo seguro `wss://`. Instale certificados SSL en cada cliente de Supervisar y Linux VDA.

Siga las instrucciones indicadas en Remedar sesiones para configurar el agente Linux VDA para el remedo.

1. Después de habilitar el remedo, se inicia la conexión de remedo y aparece un mensaje de confirmación en el dispositivo del usuario.
2. Indique al usuario que haga clic en **Sí** para empezar a compartir la máquina o la sesión.
3. El administrador solo puede ver la sesión a la que se aplica el remedo.

Remedar agentes Windows VDA

Las sesiones de Windows VDA se remedan mediante la Asistencia remota de Windows. Habilite la función `Use Windows Remote Assistance` al instalar el VDA.

1. Después de habilitar el remedo, se inicia la conexión de remedo y un cuadro de diálogo le pide que abra o guarde el archivo `.msrc incident`.
2. Abra el archivo del incidente con el Visor de Asistencia remota de Microsoft, si no está ya seleccionado de forma predeterminada. Aparecerá un mensaje de confirmación en el dispositivo del usuario.
3. Indique al usuario que haga clic en **Sí** para empezar a compartir la máquina o la sesión.
4. Para mayor control, pida al usuario que comparta su puntero y su teclado.

Supervisar y controlar sesiones

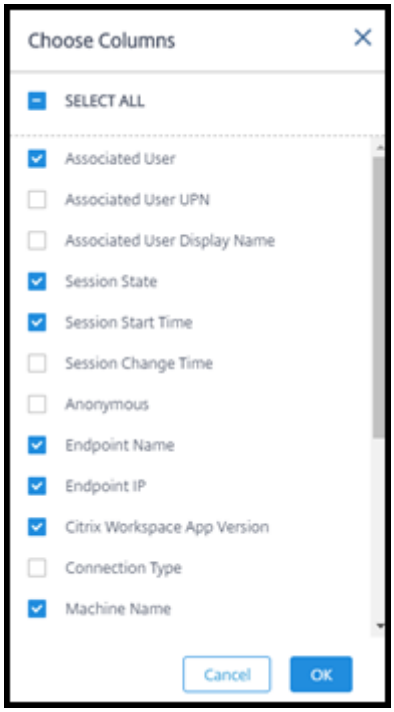
Las pantallas de sesión se actualizan cada minuto.

Además de ver sesiones, puede desconectar una o más sesiones o cerrar sesión de usuarios de sesiones.

1. En el panel **Supervisar**, haga clic en **Filtros**.

2. Seleccione la vista **Sesiones**.

3. Para personalizar la visualización, haga clic en **Elegir columnas** y active las casillas de verificación de los elementos que quiere que aparezcan. Cuando haya terminado, haga clic en **Aceptar**. La pantalla de sesiones se actualiza automáticamente.



4. Haga clic en la casilla de verificación situada a la izquierda de cada sesión que quiera controlar.
5. Para cerrar o desconectar la sesión, seleccione **Control de sesión > Cerrar sesión** o **Control de sesión > Desconectar**.

Recuerde que la programación de administración de energía del catálogo también puede controlar la desconexión de sesiones y cerrar las sesiones desconectadas de los usuarios.

Como alternativa al procedimiento anterior, también puede **Buscar** un usuario, seleccionar la sesión que quiere controlar y, a continuación, mostrar los detalles de esta. Las opciones de cierre de sesión y desconexión también están disponibles allí.

Informe de la sesión

Para descargar la información de la sesión, haga clic en **Exportar** en la pantalla de sesiones. Un mensaje indica que la solicitud se está procesando. El informe se descarga automáticamente en la ubicación de descarga predeterminada del equipo local.

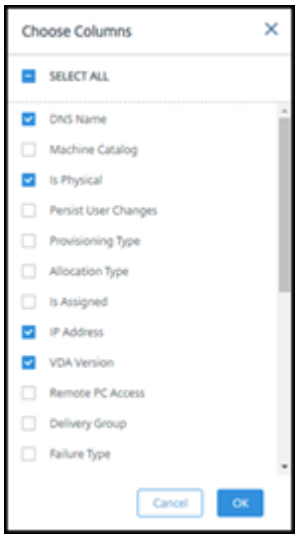
Supervisión y máquinas de control de potencia

Las pantallas de la máquina se actualizan cada minuto.

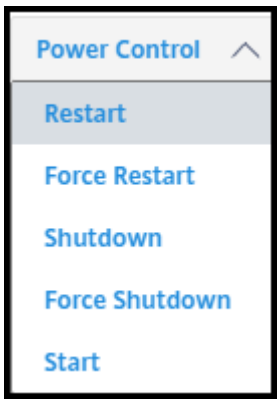
1. En el panel **Supervisar**, haga clic en **Filtros**.
2. Seleccione la vista **Máquinas**.

De forma predeterminada, la pantalla muestra las máquinas con SO de sesión única. Alternativamente, puede mostrar las máquinas multisesión.

3. Para personalizar la visualización, haga clic en **Elegir columnas** y active las casillas de verificación de los elementos que quiere que aparezcan. Cuando haya terminado, haga clic en **Aceptar**. La pantalla de las máquinas se actualiza automáticamente.



4. Para controlar las máquinas o colocarlas en o fuera del modo de mantenimiento, haga clic en la casilla de verificación a la izquierda de cada máquina que desee controlar.
5. Para controlar la alimentación de las máquinas seleccionadas, haga clic en **Control de energía** y seleccione una acción.



6. Para colocar las máquinas seleccionadas dentro o fuera del modo de mantenimiento, haga clic en Modo de **mantenimiento > ENCENDIDO o enModo de mantenimiento > APAGADO**.

Cuando utilice la función de búsqueda para encontrar y seleccionar una máquina, verá los detalles de esta, la utilización, la utilización histórica (de los últimos siete días) y la media de operaciones de entrada/salida por segundo (IOPS).

Informe de la máquina

Para descargar la información de la sesión, haga clic en **Exportar** en la pantalla de las máquinas. Un mensaje indica que la solicitud se está procesando. El informe se descarga automáticamente en la ubicación de descarga predeterminada del equipo local.

Comprobación del estado de aplicaciones y escritorios

El sondeo automatiza el proceso de comprobación del estado de las aplicaciones y escritorios publicados. Los resultados de la comprobación de estado están disponibles en el panel **Supervisar**. Para obtener más detalles, consulte:

- Sondeo de aplicaciones
- Sondeo de escritorios

Citrix DaaS para Azure para proveedores de servicios Citrix

September 7, 2022

Este artículo describe cómo los proveedores de servicios de Citrix (CSP) pueden configurar Citrix DaaS Standard para Azure (antes denominado el servicio Citrix Virtual Apps and Desktops Standard para Azure) para los clientes (arrendatarios) en Citrix Cloud.

Para obtener información general sobre las funciones disponibles para los socios de Citrix (Citrix Partners), consulte Citrix Cloud para socios.

Requisitos

- Ser socio de Citrix Service Provider.
- Tener una cuenta de Citrix Cloud.
- Tiene una suscripción a Citrix DaaS para Azure.

Limitaciones

- Los cambios de nombre del cliente pueden tardar hasta 24 horas en aplicarse en todas las interfaces.
- Al crear un cliente, la dirección de correo electrónico debe ser única.

Problemas conocidos

- Una vez que el usuario de un cliente se asigna a un recurso, no puede eliminarlo ni anular su asignación.
- La consola de administración no aplica la separación de los usuarios de los clientes. Usted es responsable de agregar usuarios a los catálogos y recursos adecuados.

Agregar un cliente

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. En el menú superior izquierdo, haga clic en **Clientes**.
2. En el panel de control **del cliente**, haga clic en **Invitar o Agregar**. Proporcione la información solicitada.

   Si el cliente no tiene una cuenta de Citrix Cloud, al agregarlo se creará una cuenta de cliente. Al agregar un cliente, usted también se agrega automáticamente como administrador de acceso completo para la cuenta de ese cliente.
3. Si el cliente tiene una cuenta de Citrix Cloud:

   a) Aparece una URL de Citrix Cloud, que usted copia y envía al cliente. Para obtener más información sobre este proceso, consulte Invitar a un cliente a conectarse.
   b) El cliente debe agregarle como administrador de acceso completo a su cuenta. Consulte Agregar administradores a una cuenta de Citrix Cloud.

Puede agregar más administradores más adelante y controlar qué clientes pueden ver en los paneles **Administrar** y **supervisar** de Citrix DaaS para Azure.

Agregar Citrix DaaS para Azure a un cliente

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. En el menú superior izquierdo, haga clic en **Clientes**.
2. En el panel de control del **cliente**, seleccione **Agregar servicio** en el menú de puntos suspensivos del cliente.
3. En **Seleccione un servicio para agregar**, haga clic en **Citrix DaaS Standard para Azure**.
4. Haga clic en **Continue**.

Después de completar este procedimiento, el cliente se incorpora a su suscripción de Citrix DaaS para Azure.

Cuando se completa la incorporación, se crea automáticamente un nuevo cliente en Citrix DaaS para Azure. El cliente está visible en **Administrar > Distribución rápida**.

Filtrar recursos por cliente

Puede filtrar los recursos por cliente en el panel Citrix DaaS for Azure **Manage > Azure Quick Deploy** . (De forma predeterminada, se muestran todos los recursos). Al trabajar con recursos como catálogos, imágenes de máquinas y suscripciones de Azure, puede seleccionar pantallas de clientes específicas para ayudar a organizar los recursos de sus arrendatarios.

Las conexiones SD-WAN se crean por cliente. El cliente debe tener un derecho de servicio de SD-WAN Orchestrator.

- Para crear una conexión SD-WAN para un cliente, siga las instrucciones en Crear una conexión SD-WAN. En la página **Agregar una conexión de red**, seleccione el cliente. Puede seleccionar la casilla Tipo de conexión SD-WAN solo si ese cliente tiene un derecho de servicio de SD-WAN Orchestrator.
- Para que la creación de la conexión tenga éxito, el cliente también debe tener instalado un nodo de control maestro (MCN). Sin embargo, solo la autorización de servicio de SD-WAN Orchestrator determina si se puede seleccionar el tipo de conexión SD-WAN.

Cree catálogos para entregar aplicaciones y escritorios

Un catálogo es un grupo de usuarios y la colección de máquinas virtuales a las que tienen acceso. Al crear un catálogo, se utiliza una imagen (con otros parámetros) como plantilla para crear las máquinas. Para obtener más información, consulte Crear catálogos.

Dominios federados

Los dominios federados permiten a los usuarios de los clientes utilizar credenciales de un dominio asociado a la ubicación de recursos para iniciar sesión en su espacio de trabajo. Puede proporcionar espacios de trabajo dedicados a sus clientes a los que sus usuarios puedan acceder mediante una URL de espacio de trabajo personalizada (por ejemplo, `customer.cloud.com`), mientras que la ubicación del recurso permanece en su cuenta de Citrix Cloud.

Puede proporcionar espacios de trabajo dedicados junto con el espacio de trabajo compartido a los que los clientes pueden acceder mediante la URL del espacio de trabajo del CSP (por ejemplo, `csppartner.cloud.com`). Para permitir que los clientes accedan a su espacio de trabajo dedicado, debe agregarlos a los dominios apropiados que administra.

Después de configurar el espacio de trabajo a través de Configuración del espaciode trabajo, los usuarios de los clientes pueden iniciar sesión en su espacio de trabajo y acceder a las aplicaciones y los escritorios que haya puesto a disposición.

Agregar un cliente a un dominio

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. En el menú superior izquierdo, haga clic en **Clientes**.
2. En el panel **Cliente**, seleccione **Identity and Access Management** en el menú superior izquierdo.
3. En la ficha **Dominios**, seleccione **Administrar el dominio federado** en el menú de tres puntos del dominio.
4. En la tarjeta **Administrar el dominio federado**, en la columna de **clientes disponibles**, seleccione el cliente que desea agregar al dominio. Haga clic en el signo más situado junto al nombre del cliente. El cliente seleccionado aparecerá ahora en la columna de **clientes federados**. Repita esta operación para agregar otros clientes.
5. Cuando haya terminado, haga clic en **Aplicar**.

Quitar un cliente de un dominio

Cuando quita un cliente de un dominio que administra, los usuarios de dicho cliente ya no pueden acceder a sus espacios de trabajo con las credenciales de su dominio.

1. En Citrix Cloud, seleccione **Administración de identidades y accesos** en el menú superior izquierdo.
2. En la ficha **Dominios**, seleccione **Administrar dominio federado** en el menú de puntos suspensivos del dominio que quiere administrar.

3. En la lista de clientes federados, localice o busque los clientes que quiere eliminar.

   - Haga clic en **X** para eliminar a un cliente.
   - Para eliminar todos los clientes listados del dominio, haga clic en **Eliminar todo**.

   Los clientes seleccionados se mueven a la lista de **clientes disponibles**.

4. Haga clic en **Aplicar**.
5. Revisa los clientes que seleccionaste y, a continuación, haga clic en **Eliminar clientes**.

Agregar un administrador con acceso restringido

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. En el menú superior izquierdo, haga clic en **Clientes**.
2. En el panel **Cliente**, seleccione **Identity and Access Management** en el menú superior izquierdo.
3. En la ficha **Administradores**, haga clic en **Agregar administradores desde** y, a continuación, seleccione **Identidad de Citrix**.
4. Escriba la dirección de correo electrónico de la persona que está agregando como administrador y, a continuación, haga clic en **Invitar**.
5. Configure los permisos correspondientes para el administrador. Citrix recomienda seleccionar **Acceso personalizado**, a no ser que quiera que el administrador tenga control de administración de Citrix Cloud y de todos los servicios suscritos.
6. Seleccione uno o más pares de funciones y ámbitos para Citrix DaaS para Azure, según sea necesario.
7. Cuando haya terminado, haga clic en **Enviar invitación**.

Cuando el administrador acepte la invitación, tendrá el acceso que le ha asignado.

Acceso de socios al proveedor de identidad del cliente

Puede administrar usuarios desde el panel Citrix DaaS for Azure **Manage > Azure Quick Deploy** o la consola de Citrix Cloud.

Cuando utiliza un proveedor de identidades que no sea de AD para los usuarios (como Citrix Managed Azure AD), debe ser administrador de Citrix Cloud Identity and Workspace para el cliente antes de poder administrar los usuarios para ese cliente. Si no es administrador de un cliente, no puede agregar ni eliminar usuarios para ese cliente.

Para administrar los usuarios de un cliente desde **Administrar > Panel de implementación rápida de Azure**, seleccione el socio o el cliente en **Mostrar elementos para**.

- **Ejemplo 1:** seleccione el cliente A de **Mostrar artículos para**. El panel ahora muestra solo los elementos del cliente A. Cuando selecciona un catálogo, solo verá los usuarios del cliente A en la ficha **Suscriptores**. Puede agregar o eliminar usuarios para el cliente A (suponiendo que seas administrador de ese cliente).
- **Ejemplo 2:** selecciona la entrada de socio en **Mostrar artículos para**. El panel ahora muestra solo los elementos de los socios. En la ficha **Suscriptores**, solo verá los usuarios creados para el socio. No aparecen entradas de clientes. Puede agregar o eliminar usuarios para ese socio (suponiendo que seas administrador de ese socio), pero no puede administrar ningún usuario de clientes desde esta ubicación.

Para administrar los usuarios de un cliente desde la consola de Citrix Cloud, seleccione el cliente cuando se le solicite después del inicio de sesión (o después, mediante **Cambiar cliente** en el área superior derecha de la consola de Citrix Cloud). Al utilizar la biblioteca para administrar usuarios, el contexto de visualización refleja al cliente seleccionado. Por ejemplo, si seleccionó el cliente A, la biblioteca solo muestra las ofertas del cliente A.

Modificar permisos de administración delegada para administradores

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. En el menú superior izquierdo, haga clic en **Clientes**.
2. En el panel **Cliente**, seleccione **Identity and Access Management** en el menú superior izquierdo.
3. En la ficha **Administradores**, seleccione **Modificar acceso** en el menú de tres puntos del administrador.
4. Seleccione o desactive los pares de roles y ámbitos de Citrix DaaS para Azure, según sea necesario. Asegúrese de habilitar solo las entradas que contengan el ámbito exclusivo que se creó para el cliente.
5. Haga clic en **Guardar**.

Acceder y configurar espacios de trabajo

Cada cliente obtiene su propio espacio de trabajo con una URL `customer.cloud.com` única. Esta URL es donde los usuarios del cliente acceden a sus aplicaciones y escritorios publicados.

- En**Citrix DaaS Standard for Azure:** en el panel **Administrar > Azure Quick Deploy**, vea la URL expandiendo **Acceso y autenticación de usuarios a** la derecha.
- En**Citrix Cloud: En** el panel **Cliente**, seleccione **Configuración del espacio** de trabajo en el menú superior izquierdo. Consulte la URL en la ficha **Acceso**.

Puede cambiar el acceso y la autenticación de un espacio de trabajo. También puede personalizar el aspecto y las preferencias. Para obtener más información, consulte los siguientes artículos:

- Configurar espacios de trabajo
- Espacios de trabajo seguros

Supervisar el servicio de un cliente

El panel de Citrix Daas para Azure **Supervisar** en un entorno CSP es esencialmente el mismo que el de un entorno no CSP. Consulte Supervisar para obtener información detallada.

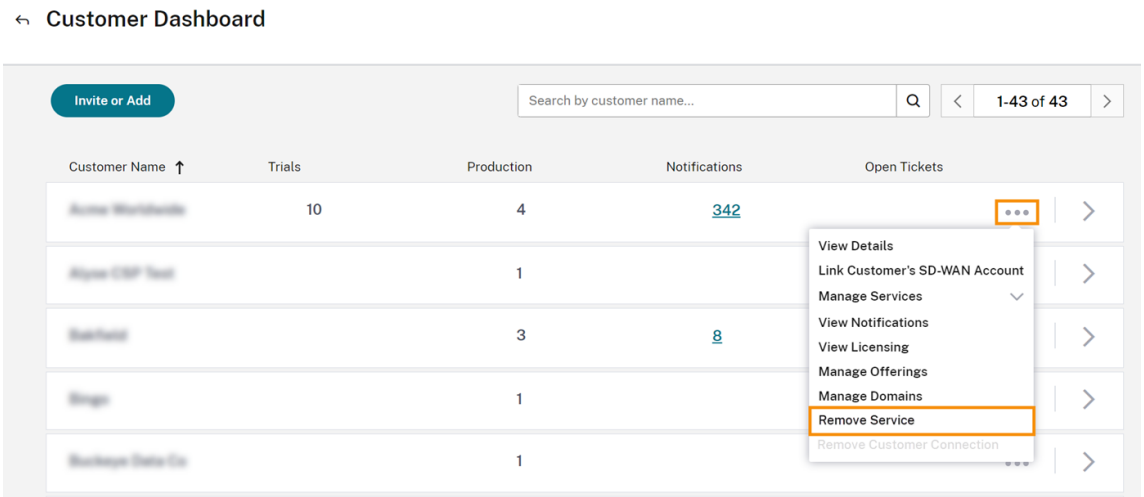
De forma predeterminada, el panel **Supervisar** muestra información acerca de todos los clientes. Para mostrar información acerca de un cliente, utilice **Seleccionar cliente**.

Tenga en cuenta que la capacidad de ver las pantallas del **monitor** de un cliente se controla mediante el acceso configurado del administrador.

Quitar un servicio

Antes de empezar, asegúrese de que el alcance del cliente no esté vinculado a ningún objeto de Citrix DaaS Standard para Azure. Si están vinculados, no puede quitar el servicio. Para desvincular ámbitos, vaya a **Citrix Studio > Administradores > Ámbitos** y modifique el ámbito. Para obtener más información sobre cómo desvincular ámbitos, consulte Crear y gestionar ámbitos.

1. Inicie sesión en Citrix Cloud con sus credenciales de Citrix Service Provider.
2. En el panel de mandos **Cliente**, haga clic en el menú de puntos suspensivos (**...**) del cliente del que quiere eliminar un servicio y seleccione **Quitar servicio**.

   Aparecerá la página **Servicio que quitar**.
3. Haga clic en **Quitar** para quitar el servicio.

Solucionar problemas

September 7, 2022

Introducción

Las ubicaciones de recursos contienen las máquinas que entregan los escritorios y aplicaciones. Esas máquinas se crean en catálogos, por lo que los catálogos se consideran parte de la ubicación de recursos. Cada ubicación de recursos también contiene Cloud Connectors. Los Cloud Connectors permiten a Citrix Cloud comunicarse con la ubicación de recursos. Citrix instala y actualiza Cloud Connectors.

Opcionalmente, puede iniciar varias acciones de ubicación de recursos y Cloud Connector. Consulte:

- Acciones de ubicaciones de recursos
- Parámetros de ubicación de recursos al crear un catálogo

Citrix DaaS para Azure tiene herramientas de solución de problemas y compatibilidad que pueden ayudar a resolver los problemas de configuración y comunicación con las máquinas que entregan escritorios y aplicaciones (los VDA). Por ejemplo, la creación de un catálogo podría fallar o los usuarios no podrían iniciar su escritorio o sus aplicaciones.

Esta instancia de solución de problemas incluye obtener acceso a la suscripción de Azure administrado por Citrix a través de una máquina bastión o RDP directo. Después de obtener acceso a la suscripción, puede utilizar las herramientas de compatibilidad de Citrix para localizar y resolver problemas. Para obtener más detalles, consulte:

- Solución de problemas de VDA mediante bastión o RDP directo
- Acceso a bastiones
- Acceso RDP directo

Solución de problemas de VDA mediante bastión o RDP directo

Las funciones de compatibilidad son para personas que tienen experiencia en la solución de problemas de Citrix. Esto incluye:

- Citrix Service Providers (CSP) y otros que tienen conocimientos técnicos y experiencia en solución de problemas con los productos Citrix DaaS.
- Personal de asistencia técnica de Citrix.

Si no está familiarizado o no se siente cómodo con la solución de problemas en componentes Citrix, puede solicitar ayuda a Citrix Support. Es posible que los representantes de Citrix Support le pidan

que configure uno de los métodos de acceso descritos en esta sección. Sin embargo, los representantes de Citrix efectúan la solución de problemas en sí, con herramientas y tecnologías de Citrix.

> **Importante:**
>
> Estas funciones de compatibilidad son válidas solo para máquinas unidas a dominios. Si las máquinas de los catálogos no están unidas al dominio, se le guía para solicitar la ayuda de Citrix Support para solucionar los problemas.

Métodos de acceso

Estos métodos de acceso son válidos solo para la suscripción de Azure administrado por Citrix. Para obtener más información, consulte Suscripciones de Azure.

Se proporcionan dos métodos de acceso a compatibilidad.

- Acceso a sus recursos a través de una máquina bastión en la suscripción dedicada de Azure administrado por Citrix del cliente. El bastión es un único punto de entrada que permite acceder a las máquinas de la suscripción. Proporciona una conexión segura a esos recursos al permitir el tráfico remoto desde direcciones IP de un intervalo específico.

  Los pasos de este método incluyen:

  - Crear la máquina bastión
  - Descargar un agente RDP
  - Acceder con RDP a la máquina bastión
  - Conectar desde la máquina bastión a las demás máquinas Citrix de la suscripción

  La máquina bastión está pensada para uso a corto plazo. Este método está diseñado para problemas relacionados con la creación de catálogos o máquinas imagen.

- Acceso RDP directo a las máquinas de la suscripción dedicada de Azure administrado por Citrix del cliente. Para permitir el tráfico RDP, debe estar definido el puerto 3389 en el grupo de seguridad de red.

  Este método está diseñado para problemas distintos de la creación de catálogos, como usuarios que no pueden iniciar sus escritorios.

Recuerde: Como alternativa a estos dos métodos de acceso, póngase en contacto con Citrix Support para obtener ayuda.

Acceso a bastiones

1. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Solución de problemas y soporte** a la derecha.

2. Haga clic en **Ver opciones de solución de problemas**.
3. En la página **Solucionar problemas**, seleccione uno de los dos primeros tipos de problemas y, a continuación, haga clic en **Utilizar nuestra máquina de solución de problemas**.
4. En la página **Solucionar problemas con la máquina bastión**, seleccione el catálogo.
    - Si las máquinas del catálogo seleccionado no están unidas al dominio, se le indicará que se ponga en contacto con Citrix Support.
    - Si ya se ha creado una máquina bastión con acceso RDP a la conexión de red del catálogo seleccionado, vaya al paso 8.
5. Se muestra el intervalo de acceso RDP. Si quiere restringir el acceso RDP a un intervalo inferior al permitido por la conexión de red, marque la casilla **Restringir el acceso RDP solo para los equipos del intervalo de direcciones IP** y, a continuación, introduzca el intervalo correspondiente.
6. Escriba un nombre de usuario y una contraseña que utilizará para iniciar sesión cuando acceda con RDP a la máquina bastión. Requisitos de contraseña.

    No utilice caracteres Unicode en el nombre de usuario.
7. Haga clic en **Crear máquina bastión**.

    Cuando la máquina de bastión se haya creado correctamente, el título de la página cambiará a **Bastion** —***conexión***.

    Si la creación de la máquina bastión falla (o si falla durante el funcionamiento), haga clic en **Eliminar** en la parte inferior de la página de notificación de fallos. Intente crear de nuevo la máquina bastión.

    Puede cambiar la restricción de intervalo RDP después de crear la máquina bastión. Haga clic en **Edit**. Introduzca el nuevo valor y, a continuación, haga clic en la marca de verificación para guardar el cambio (haga clic en **X** para cancelar el cambio).
8. Haga clic en **Descargar archivo RDP**.
9. Acceda con RDP al bastión con las credenciales especificadas al crearlo (la dirección de la máquina bastión está incrustada en el archivo RDP descargado).
10. Conecte desde la máquina bastión a las demás máquinas Citrix de la suscripción. A continuación, puede recopilar registros y ejecutar diagnósticos.

Las máquinas bastión se encienden al crearse. Para ahorrar costes, las máquinas se apagan automáticamente si permanecen inactivas tras el inicio. Las máquinas se eliminan automáticamente después de varias horas.

Puede administrar la energía o eliminar una máquina bastión con los botones situados en la parte inferior de la página. Si elige decide eliminar una máquina bastión, debe aceptar que cualquier sesión

activa en la máquina finalizará automáticamente. Además, se eliminarán los datos y archivos que se hayan guardado en la máquina.

Acceso RDP directo

1. Desde el panel **Administrar > Implementación rápida de Azure** en Citrix DaaS para Azure, expanda **Solución de problemas y soporte** a la derecha.
2. Haga clic en **Ver opciones de solución de problemas**.
3. En la página **Solucionar problemas**, seleccione **Otro problema del catálogo**.
4. En la página **Solucionar problemas con el acceso RDP**, seleccione el catálogo.

   Si RDP ya se ha habilitado para la conexión de red del catálogo seleccionado, vaya al paso 7.
5. Se muestra el intervalo de acceso RDP. Si quiere restringir el acceso RDP a un intervalo inferior al permitido por la conexión de red, marque la casilla **Restringir el acceso RDP solo para los equipos del intervalo de direcciones IP** y, a continuación, introduzca el intervalo correspondiente.
6. Haga clic en **Habilitar acceso RDP.**

   Cuando el acceso RDP está habilitado correctamente, el título de la página cambia a **Acceso RDP —*conexión***.

   Si el acceso RDP no está habilitado correctamente, haga clic en **Reintentar Habilitar RDP** en la parte inferior de la página de notificación de fallos.
7. Conéctese a las máquinas mediante las credenciales de administrador de Active Directory. A continuación, puede recopilar registros y ejecutar diagnósticos.

Obtener ayuda

Si sigue teniendo problemas, siga las instrucciones que aparecen en Cómo obtener ayuda y asistencia técnica para abrir un tíquet.

Límites

May 9, 2023

En este artículo se enumeran los límites de los recursos en una implementación de Citrix DaaS Standard para Azure (anteriormente el servicio Citrix Virtual Apps and Desktops Standard para Azure).

> **Nota:**
>
> Los límites son los recomendados por Citrix.

Límites de configuración

Recurso	Límite
Dominios de Active Directory	25
Catálogos	100
Ubicaciones de recursos	25
VDA por suscripción	2,500

Límites de ubicación de recursos

En la tabla siguiente, se enumeran los límites para cada ubicación de recursos. Si sus requisitos superan estos límites, Citrix recomienda utilizar más ubicaciones de recursos.

Recurso	Límite
Dominios de Active Directory	1
VDA de sesión única	10,000
VDA multisesión	1,000

Los Citrix Cloud Connectors se asignan a ubicaciones de recursos y vinculan las cargas de trabajo a Citrix DaaS for Azure. Para obtener información sobre los límites de Cloud Connector y las recomendaciones de tamaño y escala, consulte Consideraciones sobre el tamaño y la escala de Cloud Connectors.

Límites de aprovisionamiento

En la siguiente tabla se enumeran los máximos recomendados para una sola cuenta de Citrix Cloud.

Para implementaciones a mayor escala, Citrix recomienda un modelo de concentrador y radio, donde los VDA se distribuyen entre varias suscripciones y conexiones de red.

Recurso	Límite
VDA multisesión por catálogo	500
VDA de sesión única por catálogo	1,200
VDA por suscripción a Microsoft Azure	2,500

Límites de uso

Recurso	Límite
Administradores totales de monitores simultáneos	5
Usuarios finales simultáneos	100,000
Recursos publicados para un solo usuario	250
Inicios de sesión por minuto	3,000

Límites de prueba

En la siguiente tabla se enumeran los límites durante una prueba de Citrix DaaS para Azure.

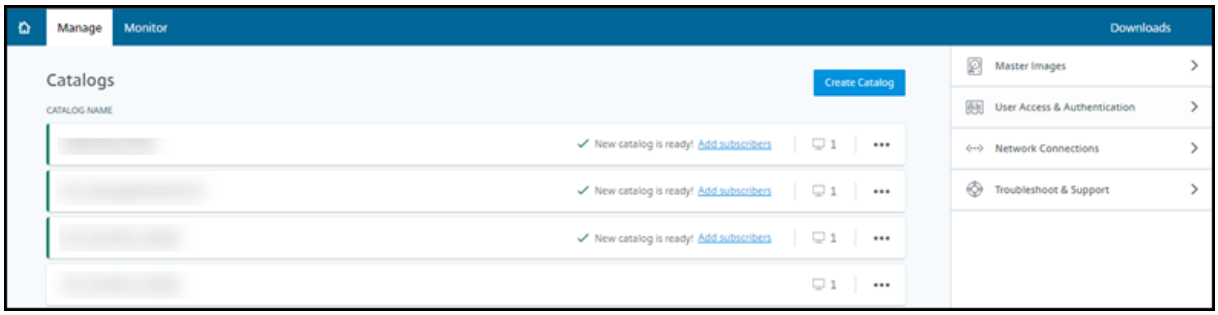
suscripción de Azure	Recurso	Límite
Suscripción a Azure administrado por Citrix	Número máximo de catálogos	3
	Número máximo de usuarios	25
	Número máximo de agentes VDA por catálogo	3
Suscripción a Azure administrada por el cliente	Número máximo de catálogos	10
	Número máximo de usuarios	25
	Número máximo de agentes VDA por catálogo	10

Referencia

September 7, 2022

Paneles

La mayoría de las actividades de administrador de Citrix DaaS Standard para Azure (anteriormente el servicio Citrix Virtual Apps and Desktops Standard para Azure) se pueden introducir a través de los paneles **Administrar** y **Supervisar**. Después de crear el primer catálogo, el panel **Administrar** se inicia automáticamente cuando inicia sesión en Citrix Cloud y selecciona Citrix DaaS para Azure.



Puede acceder a los paneles después de que se apruebe y complete su solicitud de prueba o compra.

Para acceder a los paneles:

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS Standard para Azure**. (También puede hacer clic en **Administrar** en el mosaico **DaaS Standard para Azure** en el área principal de la pantalla).
3. Si aún no se ha creado un catálogo, haga clic en **Comenzar** en la página de **bienvenida**. Accede al panel **Administrar > Azure Quick Deploy** .
4. Si ya se ha creado un catálogo, se lo dirigirá automáticamente al panel **Administrar > Azure Quick Deploy** .
5. Para acceder al panel de mandos **Supervisar**, haga clic en la ficha **Supervisar**.

Para obtener orientación sobre el producto desde el panel de control, haga clic en el icono en la esquina inferior derecha.

Fichas Catálogo en el panel Administrar

En el panel **Administrar > Azure Quick Deploy**, haga clic en cualquier parte de la entrada del catálogo. Las fichas siguientes contienen información sobre el catálogo:

- **Detalles:** Muestra la información especificada cuando se creó el catálogo (o su modificación más reciente). También contiene información sobre la imagen que se utilizó para crear el catálogo.

  Desde esta ficha, puede hacer lo siguiente:

  - Cambiar la imagen que se utiliza en el catálogo.
  - Eliminar el catálogo.
  - Acceder a la página que contiene detalles de la ubicación de recursos utilizada por el catálogo.

- **Escritorio:** Disponible solo para catálogos que contienen máquinas de sesión única (estáticas o aleatorias). En esta ficha, puede cambiar el nombre y la descripción del catálogo.

- **Escritorio y aplicaciones:** La ficha **Escritorios y aplicaciones** solo está disponible para catálogos que contienen máquinas multisesión. Desde esta ficha, puede hacer lo siguiente:

  - Agregar, modificar o quitar aplicaciones a las que los usuarios del catálogo pueden acceder en Citrix Workspace.
  - Cambiar el nombre y la descripción del catálogo.

- **Suscriptores:** Enumera todos los usuarios, incluidos su tipo (usuario o grupo), nombre de cuenta y nombre simplificado, además de su dominio de Active Directory y el nombre principal de usuario.

  Desde esta ficha, puede agregar o quitar usuarios de un catálogo.

- **Máquinas:** Muestra el número total de máquinas del catálogo, además del número de máquinas registradas, máquinas no registradas y máquinas que tienen el modo de mantenimiento activado.

  Para cada máquina del catálogo, la pantalla incluye el nombre de la máquina, el estado de energía (encendido/apagado), el estado de registro (registrada/no registrada), los usuarios asignados, el recuento de sesiones (0/1) y el estado del modo de mantenimiento (un icono que indica activado o desactivado).

  Desde esta ficha, puede hacer lo siguiente:

  - Agregar o eliminar una máquina
  - Iniciar, reiniciar, apagar o forzar el reinicio de una máquina
  - Activar o desactivar el modo de mantenimiento de una máquina

Para obtener más información, consulte Administrar catálogos. Muchas de las acciones de la máquina también están disponibles en el panel de mandos **Supervisar**. Consulte Máquinas de supervisión y control de la energía.

- **Administración de energía:** Permite administrar cuándo encender y apagar las máquinas del catálogo. Una programación también indica cuándo se desconectan las máquinas inactivas.

  Puede configurar una programación de energía al crear un catálogo personalizado o más adelante. Si no se establece explícitamente ninguna programación, una máquina se apaga al finalizar una sesión.

  Al crear un catálogo mediante creación rápida, no se puede seleccionar ni configurar una programación de energía. De forma predeterminada, los catálogos de creación rápida utilizan la programación preestablecida Ahorro de costes. Sin embargo, puede modificar ese catálogo más tarde y cambiar la programación.

  Para obtener información detallada, consulte Administrar programaciones de administración de energía.

Servidores DNS

Esta sección se aplica a todas las implementaciones que contienen máquinas unidas a un dominio. Puede ignorar esta sección si utiliza únicamente máquinas que no están unidas a un dominio.

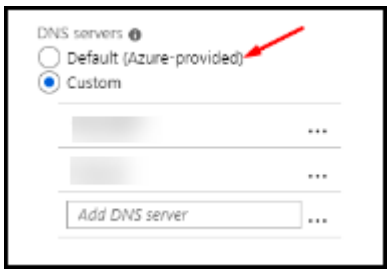
1. Antes de crear un catálogo unido a un dominio (o una conexión, si utiliza una suscripción a Azure administrado por Citrix), compruebe si tiene entradas de servidor DNS que puedan resolver nombres de dominio públicos y privados.

   Cuando Citrix DaaS para Azure crea un catálogo o una conexión, busca al menos una entrada de servidor DNS válida. Si no se encuentran entradas válidas, se produce un error en la operación de creación.

   Dónde comprobarlo:

   - Si utiliza su propia suscripción a Azure, compruebe la entrada **Servidores DNS** en su instancia de Azure.
   - Si utiliza una suscripción a Azure administrado por Citrix y está creando una conexión de emparejamiento de redes virtuales de Azure, compruebe la entrada **Servidores DNS** en la red virtual de Azure que está emparejando.
   - Si utiliza una suscripción a Azure administrado por Citrix y está creando una conexión SD-WAN, compruebe las entradas de DNS en SD-WAN Orchestrator.

2. En Azure, la configuración **Personalizado** debe tener al menos una entrada válida. Citrix DaaS para Azure no se puede usar con la configuración **Predeterminada (proporcionada por Azure)**.



- Si **Predeterminado (proporcionado por Azure)** está habilitado, cambie la configuración a **Personalizado** y agregue, al menos, una entrada de servidor DNS.
- Si ya tiene entradas de servidor DNS en **Personalizado**, compruebe que las entradas que desea usar con Citrix DaaS para Azure puedan resolver nombres IP de dominio público y privado.
- Si no tiene ningún servidor DNS que pueda resolver nombres de dominio, Citrix recomienda agregar un servidor DNS proporcionado por Azure que ofrezca esa funcionalidad.

3. Si cambia alguna entrada del servidor DNS, reinicie todas las máquinas que estén conectadas a la red virtual. El reinicio asigna los nuevos parámetros del servidor DNS. (Las máquinas virtuales continúan utilizando los parámetros de DNS actuales hasta el reinicio).

Si desea cambiar las direcciones DNS más adelante, después de crear una conexión:

- Cuando utiliza su propia suscripción a Azure, puede cambiarlas en Azure (como se describe en los pasos anteriores). O bien, puede cambiarlos en Citrix DaaS para Azure.
- Cuando se usa una suscripción a Azure administrado por Citrix, Citrix DaaS para Azure no sincroniza los cambios de dirección DNS que realiza en Azure. Sin embargo, puede cambiar la configuración de DNS para la conexión en Citrix DaaS para Azure.

Tenga en cuenta que cambiar las direcciones del servidor DNS puede provocar problemas de conectividad en las máquinas de los catálogos que utilizan esa conexión.

Agregar servidores DNS a través de Citrix DaaS para Azure

Antes de agregar una dirección de servidor DNS a una conexión, asegúrese de que el servidor DNS pueda resolver nombres de dominio públicos e internos. Citrix recomienda probar la conectividad a un servidor DNS antes de agregarla.

1. Para agregar, cambiar o eliminar una dirección de servidor DNS al crear una conexión, haga clic en **Modificar servidores DNS** en la página **Agregar** *tipo de conexión*. O bien, si un mensaje indica que no se encontraron direcciones de servidor DNS, haga clic en **Agregar servidores DNS**. Continúe con el paso 3.

2. Para agregar, cambiar o quitar una dirección de servidor DNS de una conexión existente:

    a) En el panel **Administrar > Azure Quick Deploy**, expanda **Conexiones de red** a la derecha.
    b) Seleccione la conexión que quiere modificar.
    c) Haga clic en **Modificar servidores DNS**.

3. Agregue, cambie o quite direcciones.

    a) Para agregar una dirección, haga clic en **Agregar servidor DNS** y, a continuación, introduzca la dirección IP.
    b) Para cambiar una dirección, haga clic dentro del campo de dirección y cambie los números.
    c) Para eliminar una dirección, haga clic en el icono de la papelera junto a la entrada de la dirección. No se pueden quitar todas las direcciones del servidor DNS. La conexión debe tener al menos una.

4. Cuando haya terminado, haga clic en **Confirmar cambios** en la parte inferior de la página.
5. Reinicie todas las máquinas que utilizan esa conexión. El reinicio asigna los nuevos parámetros del servidor DNS. (Las máquinas virtuales continúan utilizando los parámetros de DNS actuales hasta el reinicio).

Directivas

Establecer directivas de grupo para máquinas que no están unidas a un dominio

1. Conecte con RDP a la máquina que se está utilizando para la imagen.
2. Instale Administración de directivas de grupo de Citrix:

    a) Vaya a CTX220345. Descargue el archivo adjunto.
    b) Haga doble clic en el archivo descargado. En la carpeta `Group Policy Templates 1912 > Group Policy Management`, haga doble clic en `CitrixGroupPolicyManagement.msi`.

3. Use el comando **Ejecutar** para iniciar `gpedit.msc`, lo que abre el Editor de directivas de grupo.
4. En `User Configuration Citrix Policies > Unfiltered`, haga clic en **Modificar directiva**.

    Si falla la Consola de administración de directivas de grupo (como se describe en CTX225742), instale Microsoft Visual C++ 2015 Runtime (o una versión posterior de ese runtime).

5. Habilite los parámetros de la directiva según sea necesario. Por ejemplo:

- Cuando trabaje en **Configuración del equipo** o **Configuración de usuario** (según lo que quiera configurar) en la ficha **Parámetros**, en `Category > ICA / Printing`, seleccione **Crear automáticamente la impresora universal de PDF** y establezca el valor `Enabled`.
- Si quiere que los usuarios que hayan iniciado sesión sean administradores de su escritorio, agregue el grupo **Usuario interactivo** al grupo de administradores integrado.

6. Cuando haya terminado, guarde la imagen.
7. Actualice el catálogo existente o cree un catálogo con la nueva imagen.

Establecer directivas de grupo para máquinas que están unidas a un dominio

1. Asegúrese de que está instalada la funcionalidad Administración de directivas de grupo.
   - En una máquina multisesión Windows, agregue la funcionalidad Administración de directivas de grupo con la herramienta Windows para agregar roles y características (como **Agregar roles y características**).
   - En una máquina de sesión única Windows, instale las Herramientas de administración remota del servidor para el sistema operativo correspondiente (esta instalación requiere una cuenta de administrador de dominio). Tras la instalación, la consola Administración de directivas de grupo está disponible en el menú **Inicio**.
2. Descargue e instale el paquete de administración de directivas de grupo de Citrix desde la página de descargas de Citrix y, a continuación, configure los parámetros de directiva según sea necesario. Siga el procedimiento descrito en Establecer directivas de grupo para máquinas que no están unidas a un dominio, desde el paso 2 hasta el final.

> **Nota:**
>
> Aunque la consola de Citrix Studio no está disponible en Citrix DaaS para Azure, consulte los artículos de referencia de configuración de directivas para obtener información sobre lo que está disponible.

Acciones de ubicaciones de recursos

Citrix crea automáticamente una ubicación de recursos y dos Cloud Connectors cuando se crea el primer catálogo para publicar escritorios y aplicaciones. Puede especificar información relacionada con la ubicación de recursos al crear un catálogo. Consulte Parámetros de ubicación de recursos al crear un catálogo.

(Para el acceso con Remote PC, debe crear la ubicación de recursos y Cloud Connectors).

En esta sección se describen las acciones disponibles después de crear una ubicación de recursos.

1. Desde el panel **Administrar > Azure Quick Deploy**, expanda **Suscripciones a la nube** a la derecha.
2. Haga clic en la suscripción.

    - La ficha **Detalles** muestra el número y los nombres de los catálogos e imágenes de la suscripción. También indica la cantidad de máquinas que pueden entregar escritorios o aplicaciones. Ese recuento no incluye las máquinas utilizadas para otros fines, como imágenes, Cloud Connectors o servidores de licencias RDS
    - En la ficha **Ubicaciones de recursos**, se enumera cada ubicación de recursos. Cada entrada de ubicación de recursos incluye el estado y la dirección de cada Cloud Connector en la ubicación de recursos.

El menú de puntos suspensivos de la entrada de una ubicación de recursos contiene las siguientes acciones.

Realizar comprobación de estado

Al seleccionar **Realizar comprobación de estado**, se inicia la comprobación de conectividad inmediatamente Si la comprobación falla, se desconoce el estado de Cloud Connector, puesto que no se comunica con Citrix Cloud. Es posible que quiera reiniciar el Cloud Connector.

Reiniciar Connectors

Citrix recomienda no reiniciar más de un Cloud Connector a la vez. El reinicio desconecta el Cloud Connector e interrumpe el acceso de los usuarios y la conectividad de la máquina.

Seleccione la casilla de verificación del Cloud Connector que quiera reiniciar. Haga clic en **Reiniciar**.

Agregar conectores

La adición de un Cloud Connector normalmente tarda 20 minutos en completarse.

Proporcione la siguiente información:

- Cuántos Cloud Connectors agregar.
- Credenciales de la cuenta de servicio del dominio, que se utilizan para unir las máquinas de Cloud Connector al dominio.
- Rendimiento de la máquina.
- Grupo de recursos de Azure. El valor predeterminado es el grupo de recursos utilizado por última vez por la ubicación de recursos.

- Unidad organizativa (OU). El valor predeterminado es la unidad organizativa utilizada por última vez por la ubicación de recursos.
- Si su red necesita un servidor proxy para la conectividad a Internet. Si indica **Sí**, proporcione el FQDN del servidor proxy o la dirección IP y el número de puerto.

Cuando termines, haga clic en **Agregar conectores**.

Eliminar Connectors

Si un Cloud Connector no puede comunicarse con Citrix Cloud y la operación de reinicio no resuelve el problema, Citrix Support podría recomendar eliminar ese Cloud Connector.

Seleccione la casilla de verificación del Cloud Connector que quiera eliminar. A continuación, haga clic en **Eliminar**. Cuando se le solicite, confirme la eliminación.

También puede eliminar un Cloud Connector disponible. Sin embargo, si al eliminar ese Cloud Connector quedasen menos de dos Cloud Connectors disponibles en la ubicación de recursos, no se le permitirá eliminar el Cloud Connector seleccionado.

Seleccionar hora de actualización

Citrix proporciona automáticamente actualizaciones de software para los Cloud Connectors. Durante una actualización, un Cloud Connector se desconecta y se actualiza, mientras que otros Cloud Connectors permanecen en servicio. Cuando se completa la primera actualización, otro Cloud Connector se desconecta y se actualiza. Este proceso continúa hasta que se actualicen todos los Cloud Connectors de la ubicación de recursos. El mejor momento para iniciar las actualizaciones suele ser fuera del horario de trabajo habitual.

Elija la hora de inicio de las actualizaciones o indique que desea que se inicien cuando haya una actualización disponible. Haga clic en **Guardar** cuando haya terminado.

Cambio de nombre

Introduzca el nuevo nombre de la ubicación de recursos. Haga clic en **Guardar**.

Configurar conectividad

Indique si los usuarios pueden acceder a escritorios y aplicaciones a través de Citrix Gateway Service o solo desde la red corporativa.

Profile Management

Profile Management garantiza que los parámetros personales de los usuarios se apliquen a sus aplicaciones virtuales, independientemente de la ubicación de los dispositivos de esos usuarios.

La configuración de Profile Management es opcional.

Puede habilitar Profile Management con el servicio de optimización de perfiles. Este servicio ofrece una forma fiable de administrar estos parámetros en Windows. Con la administración de los perfiles, se garantiza una experiencia coherente al mantener un perfil único que sigue al usuario. Se fusiona automáticamente y optimiza los perfiles de usuario para minimizar los requisitos de administración y almacenamiento. El servicio de optimización de perfiles requiere una administración, asistencia e infraestructura mínimos. Además, la optimización de perfiles ofrece a los usuarios una mejor experiencia de inicio y cierre de sesión.

El servicio de optimización de perfiles requiere un recurso compartido de archivos donde persistan todos los parámetros personales. Usted gestiona los servidores de archivos. Recomendamos configurar la conectividad de red para permitir el acceso a estos servidores de archivos. Debe especificar el recurso compartido de archivos como una ruta UNC. La ruta puede contener variables de entorno del sistema, atributos de usuario de Active Directory o variables de Profile Management. Para obtener más información sobre el formato de la cadena de texto UNC, consulte Especificar la ruta al almacén de usuarios.

Al habilitar Profile Management, considere la posibilidad de optimizar aún más el perfil del usuario configurando la redirección de carpetas para minimizar los efectos del tamaño del perfil de usuario. Aplicar la redirección de carpetas complementa la solución Profile Management. Para obtener más información, consulte Redirección de carpetas de Microsoft.

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

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

Con este método, puede hacer que este servicio aplique los parámetros del servidor de licencias. Puede configurar el servidor de licencias y el modo por usuario en la consola RDS de la imagen. También puede configurar el servidor de licencias mediante la configuración de directivas de grupo de

Microsoft. Para obtener más información, consulte el documento License your RDS deployment with client access licenses (CALs) de Microsoft.

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

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

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

Uso del compromiso de consumo

> **Nota:**
>
> Esta función se encuentra en Tech Preview.

En la tarjeta **General** del panel **Administrar > Implementación rápida de Azure**, el valor **Consumo** indica cuánto consumo se ha utilizado en el mes natural actual. Este valor incluye compromisos mensuales y por plazos.

Al hacer clic en **General**, la ficha **Notificaciones** incluye:

- Consumo total utilizado durante el mes (mensual y por plazos).
- Número de unidades de compromiso de consumo mensual.
- Porcentaje del compromiso de consumo por plazos.

Los valores y las barras de progreso pueden avisarle de excedentes de uso potenciales o reales.

Los datos reales pueden tardar 24 horas en aparecer. Los datos de uso y facturación se consideran finales 72 horas después del final de un mes natural.

Para obtener más información de uso, consulte Supervisar las licencias y el uso de Citrix DaaS Standard para Azure.

Opcionalmente, puede solicitar notificaciones que aparezcan en el panel **Administrar** cuando el uso del consumo (para compromisos mensuales, plazos o ambos) alcance un nivel específico. De forma predeterminada, las notificaciones están inhabilitadas.

1. En la ficha **Notificaciones**, haga clic en **Modificar preferencias de notificaciones**.

2. Para habilitar las notificaciones, haga clic en el control deslizante para que aparezca la marca de verificación.
3. Introduzca un valor. Repita el procedimiento para el otro tipo de consumo, si es necesario.
4. Haga clic en **Guardar**.

Para inhabilitar las notificaciones, haga clic en el control deslizante para que la marca de verificación ya no aparezca y, a continuación, haga clic en **Guardar**.

Supervisar el uso de licencias de Citrix

Para ver la información de uso de licencias de Citrix, siga las instrucciones de Supervisar las licencias y el uso de Citrix DaaS Standard para Azure. Podrá ver lo siguiente:

- Resumen de las licencias
- Informes de uso
- Tendencias de uso y actividad de licencias
- Usuarios con licencias

También puede liberar licencias.

Equilibrio de carga

El equilibrio de carga se aplica a máquinas multisesión, no a máquinas de sesión única.

> **Importante:**
>
> Cambiar el método de equilibrio de carga afecta a todos los catálogos de la implementación. Esto incluye todos los catálogos creados con cualquier tipo de host compatible, locales y basados en la nube, independientemente de la interfaz utilizada para crearlos (como Studio o Distribución rápida).
>
> Asegúrese de que tiene configurados los límites máximos de sesión para todos los catálogos antes de continuar.
>
> - En la interfaz de administración de Distribución rápida de Citrix DaaS para Azure, esa configuración se encuentra en la ficha **Detalles** de cada catálogo.
> - En otros servicios y ediciones de Citrix DaaS, utilice la configuración de directivas de administración de carga.

El equilibrio de carga mide la carga de la máquina y determina qué máquina multisesión seleccionar para una sesión de usuario entrante en las condiciones actuales. Esta selección se basa en el método de equilibrio de carga configurado.

Puede configurar uno de dos métodos de equilibrio de carga: horizontal o vertical. El método se aplica a todos los catálogos multisesión (y, por lo tanto, a todas las máquinas multisesión) de la implementación del servicio.

- **Equilibrio de carga horizontal:** Una sesión de usuario entrante se asigna a la máquina encendida con menos carga disponible.

  Ejemplo sencillo: Tiene dos máquinas configuradas para 10 sesiones cada una. La primera máquina gestiona cinco sesiones simultáneas. La segunda máquina también gestiona cinco.

  El equilibrio de carga horizontal ofrece un alto rendimiento de usuario, pero puede aumentar los costes, al mantener más máquinas encendidas y ocupadas.

  Este método está habilitado de forma predeterminada.

- **Equilibrio de carga vertical:** Una sesión de usuario entrante se asigna a la máquina encendida con el índice de carga más alto. (Citrix DaaS para Azure calcula y, a continuación, asigna un índice de carga para cada máquina multisesión. El cálculo tiene en cuenta factores como la CPU, la memoria y la simultaneidad).

  Con este método, se saturan las máquinas existentes antes de pasar a otras máquinas. A medida que los usuarios se desconectan y liberan capacidad en las máquinas existentes, se asigna nueva carga a esas máquinas.

  Ejemplo sencillo: Tiene dos máquinas configuradas para 10 sesiones cada una. La primera máquina gestiona las 10 primeras sesiones simultáneas. La segunda máquina gestiona la undécima sesión.

  Con el equilibrio de carga vertical, las sesiones maximizan la capacidad de las máquinas encendidas, lo que puede ahorrar costes de máquina.

Para configurar el método de equilibrio de carga:

1. En el panel **Administrar > Azure Quick Deploy**, expanda **General** a la derecha.
2. En **Configuración global**, haga clic en **Ver todo**.
3. En la página **Parámetros globales**, en **Equilibrio de carga de catálogos multisesión**, elija el método de equilibrio de carga.
4. Haga clic en **Confirmar**.

Crear un catálogo en una red que utilice un servidor proxy

Siga este procedimiento si su red necesita un servidor proxy para la conectividad a Internet y utiliza su propia suscripción a Azure. (Con una red que requiera un servidor proxy, no se admite el uso de una suscripción a Azure administrado por Citrix).

1. Desde el panel **Administrar > Azure Quick Deploy**, inicie el proceso de creación del catálogo proporcionando la información necesaria y, a continuación, haciendo clic en **Crear catálogo** en la parte inferior de la página.
2. La creación del catálogo falla debido al requisito de proxy. Sin embargo, se crea una ubicación de recursos. El nombre de esa ubicación de recursos comienza por "DAS", a menos que haya proporcionado un nombre de ubicación de recursos al crear el catálogo. En la consola de Citrix DaaS para Azure, expanda **Cloud Subscriptions**. En la ficha **Ubicaciones de recursos**, compruebe si la ubicación de recursos recién creada contiene Cloud Connectors. Si es así, elimínelos.
3. En Azure, cree dos máquinas virtuales (consulte Requisitos de sistema de Cloud Connector). Una esas máquinas al dominio.
4. Desde la consola de Citrix Cloud, instale un Cloud Connector en cada máquina virtual. Asegúrese de que los Cloud Connectors estén en la misma ubicación de recursos que se creó anteriormente. Siga las instrucciones que se indican en:
    - Configuración del proxy y del firewall de Cloud Connector
    - Requisitos del sistema y de conectividad
5. Desde el panel **Administrar > Azure Quick Deploy**, repita el proceso de creación del catálogo. Cuando se crea el catálogo, utiliza la ubicación de recursos y los Cloud Connectors creados en los pasos anteriores.

Obtener ayuda

- Revise Solución de problemas.
- Si necesita más ayuda con Citrix DaaS para Azure, abra un tíquet de asistencia siguiendo las instrucciones de Cómo obtener ayuda y asistencia técnica.