Citrix DaaS

Contents

Información general 11

Novedades 22

Problemas conocidos 141

Elementos retirados 142

Requisitos del sistema 146

Límites 153

Información técnica general sobre la seguridad 157

Información técnica general sobre la seguridad para Azure administrado por Citrix 165

Lista de canales virtuales permitidos 179

Métodos de entrega 183

Introducción: Planificar y crear una implementación 188

Registrarse en Citrix DaaS 195

Citrix HDX Plus para Windows 365 200

Citrix DaaS for Amazon WorkSpaces Core (Tech Preview) 200

Citrix DaaS para Google Cloud 214

Guía de introducción a DaaS (Tech Preview) 215

Identidades de las máquinas 231

Unidos a Azure Active Directory 233

Unidos a Azure Active Directory 234

Microsoft Intune 238

Unidos a Azure Active Directory híbrido 239

No unida a ningún dominio 242

Configurar ubicaciones de recursos 244

Entornos de virtualización de AWS **248**

Entornos de virtualización de Google Cloud **255**

Entornos de virtualización de HPE Moonshot **266**

Entornos de virtualización de Microsoft Azure Resource Manager **267**

Entornos de virtualización de Microsoft System Center Virtual Machine Manager **268**

Entornos de virtualización de Nutanix **270**

Soluciones de Nutanix Cloud y de partners **271**

Entornos de virtualización de VMware **273**

Soluciones de VMware Cloud y de partners **274**

Entornos de virtualización de XenServer **300**

Consideraciones de tamaño y escala para los Cloud Connectors **300**

Instalar VDA **311**

Instalar los VDA mediante la línea de comandos **332**

Crear y administrar conexiones y recursos **341**

Conexión con AWS **356**

Conexión con entornos de Google Cloud **373**

Conexión a HPE Moonshot **388**

Conexión con Microsoft Azure **391**

Conexión con Microsoft System Center Virtual Machine Manager **419**

Conexión con Nutanix **420**

Conexión con soluciones de Nutanix Cloud y de partners **422**

Conexión con VMware **424**

Conexión con soluciones de VMware Cloud y de partners **433**

Conexión a XenServer **433**

Crear catálogos de máquinas **437**

Crear un catálogo de AWS **468**

Crear un catálogo de Google Cloud Platform **482**

Crear un catálogo de máquinas de HPE Moonshot **508**

Crear un catálogo de Microsoft Azure **509**

Crear un catálogo de Microsoft System Center Virtual Machine Manager **625**

Crear un catálogo de Nutanix **629**

Crear un catálogo de VMware **631**

Crear un catálogo de XenServer **637**

Crear catálogos de diferentes tipos de unión **640**

Crear catálogos unidos a Azure Active Directory **640**

Crear catálogos con Microsoft Intune habilitado **652**

Crear catálogos unidos a Azure Active Directory híbrido **654**

Crear catálogos que no estén unidos a ningún dominio **657**

Administrar catálogos de máquinas **659**

Administrar un catálogo de AWS **713**

Administrar un catálogo de Google Cloud Platform **717**

Administrar un catálogo de HPE Moonshot **725**

Administrar un catálogo de Microsoft Azure **726**

Administrar un catálogo de Microsoft System Center Virtual Machine Manager **748**

Administrar un catálogo de VMware **749**

Administrar un catálogo de XenServer **754**

Administración de energía **756**

Administrar la energía de las VM de AWS **757**

Administrar la energía de las VM de Azure **760**

Directivas de seguridad **776**

Grupo de seguridad **776**

Arranque seguro **777**

Prestaciones de cifrado **779**

Distribución rápida **781**

Introducción a Distribución rápida **786**

Crear catálogos con Distribución rápida **789**

Administrar catálogos en Distribución rápida **800**

Suscripciones a Azure en Distribución rápida **813**

Imágenes en Distribución rápida **820**

Conexiones de red en Distribución rápida **832**

Usuarios y autenticación en Distribución rápida **850**

Acceso con Remote PC en Distribución rápida **857**

Supervisar en Distribución rápida **867**

Solucionar problemas en Distribución rápida **874**

Referencia de Distribución rápida **878**

Crear grupos de entrega **890**

Administrar grupos de entrega **900**

Crear grupos de aplicaciones **932**

Administrar grupos de aplicaciones **942**

Acceso con Remote PC **949**

Eliminar componentes **963**

Capa de personalización de usuarios **964**

Actualizar la versión de los VDA **983**

Migrar la configuración a Citrix Cloud **1000**

Migrar configuraciones locales a la nube **1016**

Fusionar varios sitios en uno **1020**

Migrar de la nube a la nube **1028**

Cmdlets de la herramienta de Configuración automatizada **1031**

Solucionar problemas con Configuración automatizada e información adicional **1061**

Migrar cargas de trabajo entre ubicaciones de recursos mediante Image Portability Service **1070**

Imprimir **1092**

Directivas **1093**

Trabajar con directivas **1095**

Plantillas de directiva **1098**

Crear directivas **1103**

Conjuntos de directivas (Tech Preview) **1109**

Priorizar, modelar, comparar y solucionar problemas de directivas **1113**

Descripción general de HDX **1118**

Canales virtuales ICA de Citrix **1129**

Doble salto en Citrix DaaS **1139**

Conectividad HDX **1142**

Transporte adaptable **1143**

Enlightened Data Transport **1147**

Solución de problemas **1148**

Protocolo Rendezvous **1152**

Rendezvous V1 **1152**

Rendezvous V2 **1156**

HDX Direct (Technical Preview) **1162**

Compatibilidad con NAT **1168**

Solución de problemas **1170**

Secure HDX (Tech Preview) **1173**

Lista de canales virtuales permitidos **1177**

Solución de problemas **1181**

Canales virtuales de terceros conocidos **1184**

Dispositivos **1185**

Asignación de unidades del cliente (CDM) **1186**

Dispositivos USB genéricos **1188**

Compatibilidad con dispositivos cliente móviles y con pantalla táctil **1189**

Puertos serie **1193**

Teclados especiales **1199**

Dispositivos TWAIN **1201**

Cámaras web **1201**

Dispositivos WIA **1202**

Gráficos **1203**

HDX 3D Pro **1205**

Aceleración de GPU para SO Windows multisesión **1206**

Aceleración de GPU para SO Windows de sesión única **1209**

Thinwire **1213**

Marca de agua de sesión basada en texto **1220**

Contenido multimedia **1221**

Funciones de audio **1225**

Redirección de contenido de explorador web **1234**

Conferencias de vídeo de HDX y compresión de vídeo para cámaras web de HDX **1244**

Redirección multimedia HTML5 **1248**

Optimización para Microsoft Teams **1251**

Supervisión, solución de problemas y asistencia para Microsoft Teams **1295**

Redirección de Windows Media **1304**

Redirección de contenido general **1305**

Redirección de carpetas del cliente **1305**

Configuración de redirección de contenido bidireccional **1306**

Redirección del host al cliente **1309**

Redirección bidireccional de contenido **1313**

Acceso a aplicaciones locales y redirección de URL **1316**

Consideraciones sobre unidades del cliente y redirección de USB genérico **1326**

Administración **1337**

Acceso adaptable **1338**

Device Posture **1339**

Servicio de autenticación adaptable **1339**

Acceso adaptable en función de la ubicación de red del usuario **1340**

Paquetes de aplicaciones **1351**

AutoScale **1363**

Introducción a Autoscale **1364**

Parámetros basados en la programación y en la carga **1371**

Tiempos de espera de sesión dinámicos **1395**

Autoscale de máquinas etiquetadas (ampliación en la nube) 1397

Aprovisionar máquinas de forma dinámica 1406

Notificaciones de cierre de sesión del usuario (antes denominado "forzar el cierre de sesión del usuario") 1413

Analizar la eficacia de los parámetros de Autoscale 1416

Comandos del SDK de Broker PowerShell 1419

Comprobación de estado de Cloud 1423

Registro de configuraciones 1460

Administración delegada 1467

Página de inicio de la interfaz de Configuración completa 1488

Licencias 1492

Licencias de varios tipos 1493

Equilibrar la carga de las máquinas 1497

Caché de host local 1499

Supervisar y administrar máquinas y sesiones con Buscar 1513

Acciones y columnas de máquina 1520

Acciones y columnas de sesión 1534

Administrar las claves de seguridad 1538

Parámetros de resistencia de las sesiones 1554

Etiquetas 1562

Configuración de la zona horaria 1575

Solucionar problemas de registro de VDA e inicio de sesión 1576

Acceso de usuarios 1579

IP virtual y bucle invertido virtual 1583

Zonas **1587**

Supervisar **1599**

Análisis de sitios **1600**

Alertas y notificaciones **1610**

Filtrar datos para solucionar fallos **1623**

Supervisar tendencias históricas en un sitio **1625**

Supervisar máquinas administradas con Autoscale **1630**

Solucionar problemas de implementaciones **1633**

Solucionar problemas de aplicaciones **1634**

Sondeo de aplicaciones **1638**

Sondeo de escritorios **1643**

Solucionar problemas de máquinas **1648**

Solucionar problemas de usuarios **1661**

Diagnóstico de problemas de inicio de sesión **1665**

Diagnosticar problemas de inicio de sesión de los usuarios **1671**

Remedar usuarios **1678**

Enviar mensajes a usuarios **1680**

Resolver fallos de aplicación **1681**

Restaurar conexiones de escritorio **1683**

Restaurar sesiones **1683**

Generar informes del sistema de canales HDX **1684**

Restablecer un perfil de usuario **1685**

Grabar sesiones **1688**

Tabla de compatibilidad de funciones **1691**

Administración delegada y supervisión **1694**

Granularidad y retención de datos **1699**

Diagnóstico de inicio de sesión **1705**

Citrix DaaS para Citrix Service Providers **1756**

Citrix Gateway service **1764**

SDK y API **1765**

Información general

March 30, 2024

Introducción

Citrix DaaS es un servicio que proporciona virtualización de aplicaciones y escritorios, lo que permite al departamento de TI controlar las máquinas virtuales, las aplicaciones y la seguridad locales o alojadas en la nube, a la vez que proporciona acceso desde cualquier lugar para cualquier dispositivo. Los usuarios finales pueden utilizar aplicaciones y escritorios independientemente de la interfaz y del sistema operativo del dispositivo que estén utilizando.

Con Citrix DaaS, puede entregar aplicaciones y escritorios virtuales seguros a cualquier dispositivo, y dejar que Citrix se ocupe en mayor parte de la instalación, la configuración y las actualizaciones. Este servicio le permite mantener un control total sobre las aplicaciones, las directivas y los usuarios, al mismo tiempo que ofrece la mejor experiencia de usuario en cualquier dispositivo.

Citrix DaaS le permite administrar cargas de trabajo de centros de datos locales y de nube pública conjuntamente en una implementación híbrida. Puede conectarse a servicios de nube pública, como Microsoft Azure, Amazon Web Services (AWS) y Google Cloud, además de hipervisores locales, como XenServer, Microsoft Hyper-V, Nutanix AHV y VMware vSphere. El enfoque híbrido multinube le ofrece la flexibilidad necesaria para implementar diferentes aplicaciones en distintas ubicaciones de recursos de todo el mundo.

Citrix DaaS ofrece varias formas de entregar aplicaciones y escritorios.

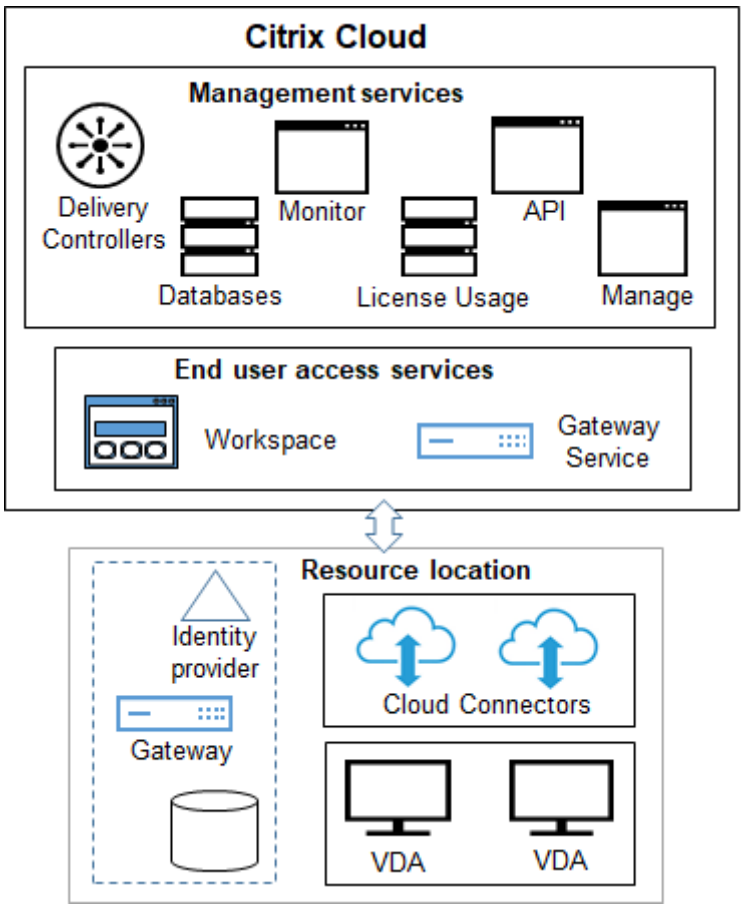
- Métodos de entrega describe las formas principales, con casos de uso y pros/contras.
- Modelos de entrega enumera más opciones y también ofrece comparaciones de modelos VDI.

Azure administrado por Citrix simplifica aún más la implementación de aplicaciones y escritorios virtuales. Con Azure administrado por Citrix, Citrix también administra el alojamiento de las cargas de trabajo de Azure.

Obtenga más información sobre las ventajas de utilizar este servicio.

Vista general del sitio

En el siguiente gráfico, se muestran los servicios y componentes con los que trabajan los administradores de Citrix en una implementación de producción de Citrix DaaS (también conocido como sitio).



Como se muestra en el gráfico, Citrix administra los servicios y componentes de administración y acceso de usuarios en Citrix Cloud. Las aplicaciones y escritorios que se entregan a los usuarios residen en máquinas de una o más ubicaciones de recursos. En una implementación de Citrix DaaS, una ubicación de recursos contiene componentes de la capa de acceso y de las capas de recursos. Cada ubicación de recursos se considera una zona.

Si ha migrado recientemente desde Citrix Virtual Apps and Desktops, observará que Citrix DaaS elimina la mayor parte del trabajo de configuración de componentes necesario en una implementación local.

Componentes y servicios administrados por Citrix

- **Delivery Controllers:** Citrix DaaS proporciona la funcionalidad para equilibrar la carga de aplicaciones y escritorios, autenticar usuarios y hacer de intermediario en conexiones o priorizarlas directamente desde la nube, sin necesidad de administrar Delivery Controllers, como ocurre con Citrix Virtual Apps and Desktops.
- **Bases de datos:** El servicio de la nube almacena los datos de configuración de sitios, supervisión y registro de configuraciones, lo que elimina el requisito de una base de datos SQL del

producto local de Citrix Virtual Apps and Desktops.

- **Licencias:** Administra las licencias y proporciona estadísticas de uso.
- **Interfaces de administración:** Consulte Interfaces de administración. Muchas tareas también están disponibles en las API de servicio.
- **Interfaz de supervisión:** La interfaz Supervisar permite a los equipos de asistencia técnica de TI supervisar entornos, solucionar problemas antes de que se conviertan en críticos y realizar tareas de asistencia para los usuarios finales. Las pantallas incluyen:
  - Datos de sesión en tiempo real procedentes del Broker Service en el Controller, que incluye datos que el agente intermediario obtiene del en el Virtual Delivery Agent (VDA).
  - Datos históricos de los sitios, procedentes de Monitor Service en el Controller.
  - Datos sobre el tráfico HDX (también conocido como tráfico ICA).
- **Cloud Connectors:** Un Cloud Connector es el canal de comunicación entre los componentes que se encuentran en Citrix Cloud y los componentes que se encuentran en la ubicación de recursos. En la ubicación de recursos, el Cloud Connector actúa como proxy para el Delivery Controller en Citrix Cloud.

  Cada ubicación de recursos contiene al menos un Cloud Connector. Se recomiendan al menos dos Cloud Connectors para que haya redundancia.

  - Cuando utilice Configuración completa para aprovisionar máquinas, instale primero Cloud Connectors desde la consola de Citrix Cloud. Para obtener más información, consulte Cloud Connectors.
  - Cuando utiliza Distribución rápida para aprovisionar máquinas de Azure, Citrix crea la ubicación de recursos y los Cloud Connectors por usted al crear un catálogo.

  Después de instalar los Cloud Connectors, Citrix los administra y actualiza. Las únicas tareas que gestiona el cliente son las actualizaciones de Windows para los Cloud Connectors y la aplicación de parches.

Interfaces de administración

En la ficha **Administrar** de Citrix DaaS, puede seleccionar estas interfaces.

Configuración completa

Desde la interfaz **Administrar > Configuración completa**, puede:

- Obtenga una descripción general de la implementación de Citrix DaaS y las funciones más recientes en la página de inicio.

- Crear y administrar conexiones con hosts.
- Crear y administrar catálogos de máquinas que contienen aplicaciones y escritorios que entrega a los usuarios.
- Crear y administrar grupos de entrega (y, de forma opcional, grupos de aplicaciones).
- Crear y administrar directrices de Citrix que afectan al uso y el comportamiento de las tecnologías y funcionalidades HDX, además de la administración a nivel de sitio. Esto incluye la configuración de directivas para sesiones, transporte adaptable, dispositivos, gráficos, multimedia, redirección de contenido y agentes VDA.
- Personalizar la administración delegada para crear administradores basados en roles que tengan ámbitos específicos de autoridad.
- Administrar la función Autoscale para administrar de forma proactiva la energía en las máquinas que entregan aplicaciones y escritorios.
- Equilibrar la carga de las máquinas
- Ejecutar comprobaciones de estado en los VDA para identificar posibles problemas y sugerencias para correcciones.
- Mostrar el contenido del registro de configuración para ver cuándo se produjeron cambios en la configuración y otras actividades administrativas y quién inició los procesos correspondientes.

Distribución rápida

En la interfaz **Administrar > Distribución rápida**, puede distribuir y administrar fácilmente cargas de trabajo de Microsoft Azure que empleen una suscripción de Azure administrado por Citrix o su propia suscripción a Azure. Para obtener más información, consulte Distribución rápida y Azure administrado por Citrix. Desde Distribución rápida, puede:

- Crear y administrar catálogos.
- Crear y personalizar imágenes, ya sea a partir de distintas imágenes preparadas por Citrix o de imágenes importadas desde su suscripción a Azure.

Para obtener más información, consulte Distribución rápida.

Administración del entorno

Desde la interfaz de **Administración del entorno**, puede utilizar tecnologías de administración inteligente de recursos y Profile Management para ofrecer el mejor rendimiento, inicio de sesión en escritorio y tiempo de respuesta de las aplicaciones posible. Para obtener más información, consulte Workspace Environment Management.

Componentes y tecnologías gestionados por el cliente

- **Citrix Gateway:** Cuando los usuarios se conectan desde fuera del firewall de la empresa, Citrix DaaS puede usar la tecnología de Citrix Gateway para proteger esas conexiones con TLS. Citrix Gateway o el dispositivo virtual VPX es un dispositivo de VPN SSL que se implementa en la zona desmilitarizada (DMZ). Proporciona un punto de acceso único y seguro a través del firewall corporativo.

  Citrix instala y administra Citrix Gateway Service en Citrix Cloud. También puede instalar Citrix Gateway en ubicaciones de recursos.

- **Active Directory:** Para la autenticación y la autorización se usa Active Directory. Autentica a los usuarios y garantiza que obtengan acceso a los recursos correspondientes. La identidad de un suscriptor define los servicios a los que tiene acceso en Citrix Cloud. Esta identidad proviene de las cuentas de dominio de Active Directory proporcionadas por los dominios dentro de la ubicación de recursos.

- **Proveedor de identidades (IdP):** El IdP es la autoridad final con respecto a la identidad del usuario. Los IDP admitidos incluyen: Active Directory local, Active Directory más token, Azure Active Directory, Citrix Gateway y Okta. Para obtener más información, consulte:

  - Identidad del espacio de trabajo
  - Administración de acceso e identidad

- **Virtual Delivery Agents (VDA):** Cada máquina física o virtual que entrega recursos (aplicaciones y escritorios) debe tener instalado un Citrix VDA en ella. Los VDA establecen y administran la conexión entre la máquina en que están instalados y el dispositivo del usuario, y aplican las directivas que se hayan configurado para la sesión.

  El VDA se registra en un Delivery Controller y usa un Cloud Connector en la ubicación de recursos como proxy.

  Hay varios tipos de VDA disponibles:

  - Los VDA para sistemas operativos multisesión de Windows permiten que varios usuarios se conecten a la máquina al mismo tiempo. Este tipo de VDA generalmente se instala en servidores Windows.
  - Los VDA para sistemas operativos de sesión única de Windows permiten que solo un usuario se conecte a una máquina. Este tipo de VDA se utiliza generalmente para VDI.

    Hay versión básica de este tipo de VDA disponible con la función de acceso con Remote PC. Contiene un subconjunto de las funciones del VDA completo de sesión única.
  - Los VDA de Linux admiten aplicaciones y escritorios virtuales basados en distribuciones RHEL, CentOS, SUSE y Ubuntu.

En la documentación de este servicio, la palabra "VDA"se refiere tanto al agente en sí como a la máquina donde está instalado.

- **Hipervisores y servicios en la nube:** En la mayoría de los sitios de producción, las instancias de aplicaciones y escritorios (cargas de trabajo) que se ponen a disposición de los usuarios (publican) están "alojadas"por un hipervisor o servicio en la nube compatible. (la función de acceso con Remote PC se utiliza normalmente con máquinas físicas; por lo tanto, no utiliza hipervisores ni servicios en la nube para el aprovisionamiento de máquinas).

  - Cuando se utiliza la interfaz de Configuración completa, se crea una conexión a un hipervisor de host o servicio en la nube compatibles. A continuación, desde Configuración completa, se utiliza una imagen (creada a través de ese host) para crear un catálogo de máquinas que contengan las instancias de aplicaciones y escritorios. A continuación, se crea un grupo de entrega. Citrix proporciona muchas herramientas para simplificar y facilitar la creación y mantenimiento de estos hosts de sesión.
  - Cuando utiliza Distribución rápida para entregar cargas de trabajo de Azure, solo necesita crear el catálogo. Aunque puede usar su propia suscripción de Azure al crear el catálogo, el uso de una suscripción de Azure administrado por Citrix elimina también la necesidad de administrar el host.

  Las instancias de aplicaciones y escritorios que publique pueden ser locales, estar alojadas en nubes públicas o ser una mezcla híbrida de ambas.

- **Citrix StoreFront:** Citrix StoreFront es el predecesor de Citrix Workspace alojado en la nube. Se utiliza como interfaz web para acceder a aplicaciones y escritorios.

  Opcionalmente, puede instalar servidores StoreFront en ubicaciones de recursos. Tener almacenes locales puede ayudar a entregar aplicaciones y escritorios durante las interrupciones de red. La función Caché de host local requiere un almacén de StoreFront administrado por el cliente en cada ubicación de recursos.

  Para obtener más información sobre el uso de StoreFront en un entorno de servicio, consulte Acceso de usuarios.

Objetos configurados para entregar escritorios y aplicaciones

Para entregar aplicaciones y escritorios en un entorno de producción, se configuran los siguientes elementos.

- **Conexión de host:** Una conexión de host (mencionada anteriormente) ayuda a habilitar la comunicación entre los componentes del plano de control (Citrix Cloud) y los VDA en una ubicación de recursos. A continuación, se presentan las especificaciones de las conexiones:

  - La dirección y las credenciales para acceder al host

  - El método de almacenamiento a utilizar y las máquinas que se utilizarán para el almacenamiento
  - Qué red pueden utilizar las máquinas virtuales

  Recuerde: Al usar Distribución rápida, no es necesario crear una conexión. Y si utiliza Azure administrado por Citrix, Citrix también administra el alojamiento.

- **Catálogo:** En las interfaces de Configuración completa y Supervisar, los catálogos se denominan "catálogos de máquinas".
  Un catálogo es una colección de máquinas virtuales o físicas que tienen el mismo tipo de sistema operativo (por ejemplo, SO multisesión de Windows o SO de sesión única de Ubuntu).

  When creating a catalog, you usually use an image, which is also known as a template. (Remote PC Access catalogs usually contain physical machines, so no image is needed.)

  - When using Quick Deploy, Citrix provides several Citrix prepared images you can use to create your own customized images. Or, you can import images from your own Azure subscription.
  - When using Full Configuration to create VMs using a supported host type, the image usually must be created and reside on a host machine. When creating the catalog, you provide the path to that image.

  Regardless of where the image resides, you can install applications on the image, if you want those apps on all machines created from that image (and don't want to virtualize those apps).

  After the image is ready, you create the catalog.

  - For VMs, MCS creates the machines and the catalog.
  - For Remote PC Access, MCS simply creates the catalog, because the physical machines already exist.

  For more information about MCS, see Image management.

- **Grupo de entrega:** Un grupo de entrega especifica:

  - Una o más máquinas de un catálogo.
  - Los usuarios autorizados para acceder a esas máquinas.
  - Las aplicaciones y escritorios a los que los usuarios pueden acceder a través de Workspace.

  Cuando se utiliza Distribución rápida, se crea automáticamente un grupo de entrega (solo aparece en la interfaz de Configuración completa).

- **Grupos de aplicaciones:** Los grupos de aplicaciones le permiten administrar colecciones de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega. Los grupos de aplicaciones son opcionales.

Azure administrado por Citrix

Azure administrado por Citrix es una opción disponible en varias ediciones de Citrix DaaS. Utilizar Azure administrado por Citrix simplifica la implementación de aplicaciones y escritorios virtuales desde Azure. Citrix administra la infraestructura para alojar cargas de trabajo de Azure.

Con Azure administrado por Citrix, obtiene una ubicación de recursos y una suscripción de Azure administrada por Citrix dedicadas. En esa suscripción de Azure, debe crear un catálogo de máquinas virtuales. Puede hacer lo siguiente:

- Implementar máquinas con SO de sesión única y multisesión de Windows o máquinas con SO Linux desde varias versiones compatibles.
- Elegir tipos de equipos y opciones de almacenamiento de una lista selecta en regiones determinadas.
- Aprovisionar cargas de trabajo persistentes o no persistentes en esas máquinas.
- Elegir entre varias imágenes proporcionadas por Citrix que tengan instalado el VDA más reciente. A continuación, desde la interfaz de Citrix, usted crea su propia imagen a partir de esa plantilla y la personaliza. También puede importar y usar imágenes desde su propia suscripción de Azure.

Aunque Citrix administra la capacidad de Azure, si quiere comunicarse con recursos existentes en su propia suscripción de Azure, puede usar el emparejamiento de redes virtuales de Azure para conectar recursos. También puede utilizar Citrix SD-WAN para conectarse directamente a los recursos locales.

Para obtener información acerca de la seguridad y las responsabilidades al usar Azure administrado por Citrix, consulte Información técnica general sobre la seguridad para Azure administrado por Citrix.

Realizar un pedido de Azure administrado por Citrix

Para obtener una suscripción de Azure administrado por Citrix, debe suscribirse a una oferta de servicio de Citrix disponible y, a continuación, realizar un pedido de Citrix Managed Azure Consumption Funds. Puede realizar un pedido de Citrix DaaS y de los fondos de consumo a través de Citrix o desde Azure Marketplace.
Azure administrado por Citrix está disponible en las siguientes ofertas de servicio:

- Citrix Workspace Premium Plus
- Ediciones Citrix DaaS, Advanced, Advanced Plus y Premium
- Edición Citrix DaaS Standard para Azure

Para obtener información detallada, consulte Inscribirse en Citrix DaaS.

Resumen de las ventajas de Azure administrado por Citrix

Usar Azure administrado por Citrix Azure ofrece varias ventajas:

- Es el camino más rápido hacia las ventajas de la nube híbrida.
- Descarga la administración de infraestructuras para los equipos de TI. Ofrece una experiencia de administración a los equipos de TI sin los problemas habituales de administración y mantenimiento.
- Le permite escalar rápidamente soluciones de trabajo.
- Proporciona una suscripción independiente de Azure administrada y mantenida por Citrix. Esto aísla la actividad de otras suscripciones de Azure que pueda tener.
- Conserva la flexibilidad necesaria para crear y administrar cargas de trabajo con sus propias suscripciones de Azure. La implementación puede incluir cargas de trabajo que utilizan la suscripción de Azure administrado por Citrix y cargas de trabajo que usan suscripciones de Azure (administrado por el cliente).
- Utiliza un verdadero modelo de infraestructura como servicio (IaaS) basado en el consumo.
- Hay varias tecnologías disponibles para crear conexiones a sus propias redes locales (como el emparejamiento de redes virtuales de Azure y SD-WAN). Esto permite a los usuarios acceder a los recursos de su red, como, por ejemplo, servidores de archivos.

La implementación y la administración de Azure administrado por Citrix desde este servicio emplea la interfaz de administración de Distribución rápida.

Para obtener más información, póngase en contacto con un representante de Citrix.

Entregar aplicaciones y escritorios a los usuarios

Citrix Workspace

Los suscriptores (usuarios) acceden a sus escritorios y aplicaciones a través de Citrix Workspace.

Una vez instalado y configurado Citrix DaaS, se le proporciona un enlace con la URL del espacio de trabajo. La URL del espacio de trabajo se publica en dos lugares:

- En la consola de Citrix Cloud, seleccione **Configuración de Workspace** en el menú de la esquina superior izquierda. La ficha **Acceso** contiene la URL del espacio de trabajo.
- En la página de **bienvenida** de Citrix DaaS, la URL del espacio de trabajo aparece en la parte inferior de la página.

Pruebe y, a continuación, comparta la URL del espacio de trabajo con los suscriptores (usuarios) para que accedan a sus aplicaciones y escritorios. Los suscriptores pueden acceder a la URL del espacio de trabajo sin necesidad de configurar nada más.

Los espacios de trabajo los configura desde Citrix Cloud.

- Especificar los servicios integrados con Citrix Workspace.
- Personalizar la URL que utilizan sus suscriptores para acceder a su espacio de trabajo.
- Personalizar la apariencia de los espacios de trabajo de los suscriptores, como logotipos, colores y preferencias.
- Especificar cómo se autentican los suscriptores en su espacio de trabajo: por ejemplo, mediante Active Directory o Azure Active Directory.
- Especificar la conectividad externa para las ubicaciones de recursos utilizadas por sus suscriptores.

Para obtener más información, consulte Citrix Workspace.

Aplicación Citrix Workspace

Para los usuarios, la aplicación Citrix Workspace se instala en los dispositivos de usuario y en otros dispositivos de punto final, como los escritorios virtuales. La aplicación Citrix Workspace ofrece a los usuarios un acceso seguro y de autoservicio a documentos, aplicaciones y escritorios desde cualquier dispositivo, incluidos smartphones, tabletas y PC. La aplicación Citrix Workspace también ofrece acceso a demanda a aplicaciones Windows, web y de Software como servicio (SaaS).

Para los dispositivos donde no se puede instalar el software de la aplicación Citrix Workspace, la aplicación Citrix Workspace para HTML5 ofrece una conexión a través de un explorador web compatible con HTML5.

La aplicación Citrix Workspace está disponible para varios sistemas operativos. Para obtener más información, consulte la aplicación Citrix Workspace.

Contrato de nivel de servicio

Citrix DaaS se ha diseñado teniendo en cuenta las prácticas recomendadas del sector con el fin de lograr un alto grado de disponibilidad de los servicios y alta escalabilidad de nube.

Para obtener detalles completos sobre el compromiso de Citrix con la disponibilidad de los servicios de Citrix Cloud, consulte el Acuerdo de nivel de servicio.

El rendimiento de este objetivo puede supervisarse constantemente en https://status.cloud.com.

Limitaciones

En el cálculo de este objetivo de nivel de servicio no se incluirá la pérdida de disponibilidad debida a las causas siguientes:

- El cliente no cumple los requisitos de configuración de Citrix DaaS documentados en https://docs.citrix.com.

- A causa de un componente que no administre Citrix, incluidos, entre otros: máquinas físicas y virtuales que controle el cliente, sistemas operativos que controle y administre el cliente, equipos de red u otro hardware que instale y controle el cliente; parámetros de seguridad que defina y controle el cliente, directivas de grupo y otras directivas de configuración; fallos del proveedor de nube pública, fallos del proveedor de servicios de Internet u otros externos al control de Citrix.
- La interrupción del servicio por razones que se encuentren más allá del control de Citrix, incluidos los desastres naturales, las guerras o los actos terroristas y las acciones gubernamentales.

Más información

- Diagramas de Citrix DaaS
- Arquitectura y métodos de implementación de referencia de Citrix DaaS
- Información técnica general sobre la seguridad
- Puertos de red
- Avisos legales de terceros
- Requisitos del sistema
- Funciones
  - Una introducción a las tecnologías HDX, además de detalles sobre dispositivos, gráficos y multimedia.
  - Acceso con Remote PC: Permite a los usuarios iniciar sesión de forma remota en el PC físico Windows de la oficina desde cualquier lugar. Puede configurar el acceso con Remote PC desde Configuración completa o Distribución rápida.
  - Publicar contenido: Publique una aplicación que es simplemente una ruta URL o UNC a un recurso.
  - Servidor VDI: Entregue un escritorio desde un sistema operativo de servidor para un solo usuario.
- Para Citrix DaaS Standard para Azure, consulte la documentación de producto dedicada.
- Para obtener información sobre la disponibilidad de funciones en los productos y ediciones de Citrix DaaS, consulte la tabla de funciones de Citrix DaaS.
- La serie de aprendizaje de Citrix Cloud ofrece cursos educativos para ponerle al día de Citrix Cloud y sus servicios. Puede ver todos los módulos seguidos, desde las presentaciones hasta la planificación y la creación de los servicios. También puede elegir módulos individuales o segmentos de tareas específicas dentro de un módulo. Consulte Cloud Learning Series.

Introducción

Para aprender a configurar la implementación, empiece por Planificar y crear una implementación. Este resumen le guía por los principales pasos del proceso y proporciona enlaces a información y procedimientos detallados adicionales.

Novedades

June 13, 2024

Citrix tiene como objetivo entregar nuevas funciones y actualizaciones de sus productos a los clientes de Citrix DaaS tan pronto como estén disponibles. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar. Las actualizaciones continuas de Citrix DaaS se publican aproximadamente cada 3 semanas.

Para usted, este proceso es transparente. Las actualizaciones iniciales se aplican solo en los sitios internos de Citrix y luego se aplican gradualmente en los entornos de los clientes. La entrega de actualizaciones por fases ayuda a garantizar la seguridad de los productos y maximizar su disponibilidad.

Para obtener más información sobre el acuerdo de nivel de servicio en cuanto a su disponibilidad y la escalabilidad en la nube, consulte Acuerdo de nivel de servicio. Para supervisar las interrupciones de servicio y el mantenimiento programado, consulte el Panel de estado del servicio.

Agentes Virtual Delivery Agent (VDA)

Los VDA para máquinas Windows se publican generalmente al mismo tiempo que el producto Citrix Virtual Apps and Desktops.

- Para obtener información sobre las funciones nuevas de VDA y HDX, consulte los artículos Novedades y Problemas conocidos de la versión actual de Citrix Virtual Apps and Desktops.
- Para obtener información acerca de las plataformas y las funciones de VDA que ya no se desarrollan, consulte Elementos retirados. Ese artículo también incluye plataformas y funciones para las que está previsto retirar la compatibilidad en una versión futura (por ejemplo, los sistemas operativos que disponen de la función de instalación de VDA).

> **Importante:**
>
> Si el componente Personal vDisk (PvD) se ha instalado alguna vez en un VDA, dicho VDA no se puede actualizar a la versión 1912 LTSR ni a ninguna posterior. Para utilizar el nuevo VDA, debe desinstalar el VDA actual y, a continuación, instalar el nuevo (este paso debe seguirse incluso aunque se haya instalado PvD, pero nunca se ha utilizado). Para obtener más información, con-

> sulte Si el VDA tiene un disco Personal vDisk instalado.

junio de 2024

Funciones nuevas y mejoradas

Función para crear grupos de recursos durante la creación del catálogo de Azure (para PVS). Anteriormente, al crear catálogos de Azure mediante la Configuración completa, había que crear los grupos de recursos mediante comandos de PowerShell. Con esta función, ahora puede crear sin problemas un grupo de recursos como parte de la creación de catálogos en Web Studio. Esta mejora simplifica el flujo de trabajo general de creación. Para obtener más información, consulte Crear un catálogo de Citrix Provisioning mediante la interfaz de configuración completa.

Mayo de 2024

Funciones nuevas y mejoradas

Secure HDX (Tech Preview). Ahora puede usar esta función para evitar que cualquier elemento de red existente en la ruta del tráfico pueda inspeccionar el tráfico HDX. Para obtener más información, consulte Secure HDX.

Compatibilidad con la hibernación de GPU de Azure (Tech Preview). Ahora tiene la opción de usar hibernación para las SKU de máquinas de Azure que son compatibles con GPU.
Para obtener más información sobre los tamaños de máquinas virtuales compatibles, consulte la documentación de Microsoft.

La función de los catálogos de Citrix Provisioning para la unión híbrida de Azure AD se extendió a la configuración completa. Al crear un catálogo de Citrix Provisioning, el tipo de identidad **Unido a Azure Active Directory híbrido** ahora está disponible en la página **Configuración del catálogo de máquinas > Identidades de máquinas**. Con esta nueva opción, puede crear máquinas unidas a Azure AD híbrido a través de Citrix Provisioning. Para obtener más información, consulte este artículo de Citrix Provisioning.

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

- Acceda a los documentos clave relacionados específicamente con el nodo seleccionado.
- Manténgase informado sobre las actualizaciones del servicio, como la hoja de ruta de Citrix, los problemas conocidos, los límites, los requisitos del sistema y las funciones nuevas.

- Acceda a recursos ampliados, como: blogs de Citrix, comunidad de Citrix, funciones de Citrix explicadas, documentación de productos de Citrix, Citrix Support y documentación para desarrolladores.

Registro de configuración mejorado: seguimiento de los cambios de membresía para los grupos de entrega. Con esta mejora, el registro de configuración ahora captura y muestra los ID de usuario y grupo agregados o quitados de los grupos de entrega. Para ver los registros de configuración, vaya a **Configuración completa > Registros > Eventos**.

Personalice el orden de las fichas en el nodo Búsqueda. Ahora puede personalizar el orden de las fichas del nodo **Búsqueda** según sus patrones de uso, lo que mejora la experiencia de navegación. Para ello, haga clic en el icono de tres puntos situado junto a las fichas, arrastre las fichas al orden que prefiera y después haga clic en **Aplicar**.

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

Función para crear catálogos de Citrix Provisioning mediante comandos de MCS PowerShell en VMware. Ahora puede crear catálogos de Citrix Provisioning mediante comandos de MCS PowerShell en VMware.

Esta implementación le ofrece las siguientes ventajas:

- Una única API unificada para administrar los catálogos de MCS y de Citrix Provisioning.
- Hay nuevas funciones para los catálogos de Citrix Provisioning, como la solución de administración de identidades, el aprovisionamiento bajo demanda, etc.

Para obtener más información, consulte Crear catálogos de Citrix Provisioning en Citrix Studio.

Detección y mitigación de errores en el servicio de actualización de VDA durante el proceso de actualización del VDA (versión preliminar). Nuestro servicio ahora incorpora mecanismos de detección avanzados. Si se detecta algún problema que pueda provocar un fallo en la IPU del VDA e inutilizar el VDA, el servicio tomará medidas proactivas. Dejará de actualizar máquinas adicionales y saldrá correctamente del flujo de trabajo actual. Este enfoque proactivo tiene como objetivo minimizar el impacto y garantizar una experiencia fluida, incluso en caso de desafíos inesperados, reduciendo las posibles consecuencias de cualquier problema que surja. Para obtener más información, consulte Detección y mitigación de errores en el servicio de actualización de VDA

Compatibilidad con las actualizaciones de VDA desde un recurso compartido de archivos local al que tienen acceso los VDA (Tech Preview). Con el control de acceso mejorado al instalador de VDA, ahora puede disponer de mayor flexibilidad y control sobre qué VDA pueden conectarse y recuperar los MSI de descarga necesarios sin preocuparse por conceder acceso a la red para que los VDA obtengan actualizaciones de la CDN de Azure administrada por Citrix. Esto le permite aplicar reglas

de red más estrictas y, al mismo tiempo, garantizar un acceso sin problemas a las actualizaciones esenciales. Para obtener más información, consulte Compatibilidad con las actualizaciones de VDA desde un recurso compartido de archivos local al que tienen acceso los VDA

Compatibilidad con la Configuración completa para entregar aplicaciones empaquetadas a equipos de oficina y a escritorios estáticos de sesión única. Con esta mejora, ahora puede entregar aplicaciones empaquetadas a todos los tipos de escritorios mediante la Configuración completa. Las ventajas de ofrecer aplicaciones empaquetadas a los escritorios *estáticos de sesión única* incluyen:

- Las aplicaciones están disponibles en el VDA al iniciar sesión y no se pueden organizar bajo demanda a través de Workspace o StoreFront.
- Mejora del tiempo de inicio al acceder a las aplicaciones empaquetadas.
- Facilita el mantenimiento de las aplicaciones empaquetadas de forma independiente, separada de la imagen base del VDA.

Para entregar aplicaciones empaquetadas a los escritorios, agregue esas aplicaciones a los grupos de entrega de estas maneras:

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

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

Compatibilidad con la Configuración completa para entregar aplicaciones empaquetadas en formato FlexApp. En **Configuración completa > Paquetes de aplicaciones**, ahora puede cargar aplicaciones empaquetadas FlexApp a Citrix Cloud y entregarlas a sus usuarios. Para obtener más información, consulte Paquetes de aplicaciones.

Paginación OData. Monitor mejora el límite de paginación de OData. Todos los dispositivos de punto final de OData 4 devuelven un máximo de 1000 registros por página con un enlace a los siguientes 1000 registros en la respuesta. Puesto que cada página devuelve grandes conjuntos de datos, puede obtener la misma cantidad de datos totales con menos consultas de OData. Por lo tanto, esta función reduce el tiempo necesario para obtener los datos totales y mejora la experiencia del usuario. Para obtener más información, consulte la documentación Accessing Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Función para crear y administrar máquinas virtuales confidenciales de Azure mediante la Configuración completa. Las máquinas virtuales confidenciales de Azure proporcionan un límite estricto impuesto por hardware para ayudar a satisfacer sus necesidades en términos de seguridad. Con la interfaz de usuario de Configuración completa, ahora puede crear y administrar máquinas virtuales

confidenciales en Azure. Para obtener más información, consulte Máquinas virtuales confidenciales de Azure (Technical Preview).

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

Función para capturar propiedades adicionales mediante el origen del perfil de máquina en AWS. En los entornos de AWS, con esta mejora, ahora puede crear o actualizar un catálogo basado en perfiles de máquinas para incluir lo siguiente:

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

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

Para obtener más información, consulte Crear un catálogo de máquinas basado en perfiles de máquina con PowerShell.

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

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

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

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

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

Configurar grupos de seguridad por interfaz de red en AWS. Al modificar una conexión de host para entornos de AWS, ahora puede configurar la cantidad máxima de grupos de seguridad permitidos por interfaz de red elástica (ENI) mediante un comando de PowerShell. Por lo tanto, si aumenta la cuota de sus grupos de seguridad por interfaz de red, puede configurar el mismo valor para la conexión de host. Para obtener información sobre la configuración, consulte Configurar grupos de seguridad por interfaz de red.

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

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

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

El **Ahorro estimado** sirve de ayuda a la hora de evaluar un uso eficiente de los recursos de infraestructura. El ahorro de costes se muestra en dólares estadounidenses o como un porcentaje del coste incurrido. Puede ver los resultados de los últimos 3, 6 y 12 meses. El gráfico **Ahorro estimado** muestra lo siguiente:

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

El **Informe de ahorro de Autoscale** muestra información sobre el grupo de entrega para el que Autoscale está configurado y habilitado. Este informe solo incluye las máquinas con administración de energía. Para obtener más información, consulte la página Optimización de costes.

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

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

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

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

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

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

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

Abril de 2024

Funciones nuevas y mejoradas

Compatibilidad con la versión más reciente de Microsoft Teams. Supervisar de Citrix es compatible ahora con la versión 2.1 o anterior de Microsoft Teams.

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

- Crear un catálogo de máquinas MCS con un conjunto de cifrado de disco (DES) distinto del DES de la imagen maestra.
- Cambiar el tipo de cifrado del disco de una clave DES a otra clave DES de un catálogo de máquinas de MCS existente y de las máquinas virtuales existentes.

- Actualizar una máquina virtual y un catálogo de máquinas de MCS que antes no estuvieran habilitados para CMEK para que tengan cifrado (DES) con clave de cifrado administrada por el cliente (CMEK), cifrado de disco en el host o cifrado doble.
- Actualizar una máquina virtual y un catálogo de máquinas de MCS cifrados para que dejen de estarlo.
- Habilitar el cifrado de discos con un dispositivo de punto final privado (un catálogo de máquinas MCS que use una conexión de host habilitada con `ProxyHypervisorTrafficThroughConnector`).

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

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

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

Comprobar la presencia de varias tarjetas NIC en VMware. En entornos de VMware, hemos introducido varias comprobaciones preliminares cuando la plantilla de perfil de la máquina y la unidad de alojamiento tienen varias redes y el parámetro `-NetworkMapping` se usa en los comandos `New-ProvScheme` y `Set-ProvScheme`. Para obtener más información sobre la lista de verificación preliminar sobre varias tarjetas NIC, consulte Comprobar la presencia de varias tarjetas NIC.

Función para crear máquinas virtuales de Windows 11 en GCP. Ahora puede crear máquinas virtuales de Windows 11 en GCP. Si instala Windows 11 en la imagen maestra, debe habilitar vTPM durante el proceso de creación de la imagen maestra. Además, debe habilitar vTPM en el origen del perfil de máquina (plantilla de instancia o máquina virtual).

Esta función se aplica a:

- Catálogos de máquinas de MCS persistentes y no persistentes.
- Solo grupos de nodos de arrendatario único.

Para obtener información sobre la creación de máquinas virtuales de Windows 11 en el nodo de arrendatario único, consulte Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único.

Compatibilidad con listas de canales virtuales permitidos para variables de entorno.
Ahora puede usar variables de entorno del sistema en la ruta de los procesos de confianza. Para obtener más información, consulte Uso de variables de entorno del sistema.

Funciones retiradas en la Configuración completa. Las siguientes funciones y parámetros se han retirado en Configuración completa:

Compatibilidad con los PC en la nube con HDX Plus para Windows 365 y Azure Virtual Desktop. Monitor ahora es compatible con los PC en la nube con HDX Plus para Windows 365 y Azure Virtual Desktop (AVD). Para obtener más información, consulte Solucionar problemas de máquinas.

Cambio de cuenta de servicio de Cloud Build. GCP está introduciendo cambios en el comportamiento predeterminado de los servicios de Cloud Build y en el uso de cuentas de servicio en los nuevos proyectos creados a partir del 29 de abril de 2024. Para obtener más información, consulte Cambio de la cuenta de servicio de Cloud Build. No obstante, los proyectos de Google y los catálogos de Citrix existentes no se ven afectados por este cambio. Para obtener más información, consulte:

- Configurar y actualizar cuentas de servicio
- Permisos de GCP requeridos

Compatibilidad con los PC en la nube con HDX Plus para Windows 365 y Azure Virtual Desktop. Monitor ahora es compatible con los PC en la nube con HDX Plus para Windows 365 y Azure Virtual Desktop (AVD). Para obtener más información, consulte Solucionar problemas de máquinas.

Entornos de VDA con proxies para el filtrado de URL e Internet (Tech Preview). Ahora puede usar el servicio de actualización de VDA para actualizar los VDA cuando tenga proxies para la conectividad a Internet y el filtrado web. El proxy configurado en la directiva tiene prioridad sobre el proxy configurado en el registro. Para obtener más información, consulte Instalar agentes VDA. Consulte también la lista de URL que deben figurar en la lista de permitidas del proxy.

Cambio de cuenta de servicio de Cloud Build. GCP está introduciendo cambios en el comportamiento predeterminado de los servicios de Cloud Build y en el uso de cuentas de servicio en los nuevos proyectos creados a partir del 29 de abril de 2024. Para obtener más información, consulte Cambio de la cuenta de servicio de Cloud Build. No obstante, los proyectos de Google y los catálogos de Citrix existentes no se ven afectados por este cambio. Para obtener más información, consulte:

- Configurar y actualizar cuentas de servicio
- Permisos de GCP requeridos

Marzo de 2024

Funciones nuevas y mejoradas

Grabación dinámica de sesiones. Ahora puede grabar la sesión activa actual mediante los controles de grabación de sesiones de la pantalla **Detalles del usuario** sin necesidad de restablecer la sesión. Esta función permite solucionar de forma más rápida y eficaz los problemas relacionados con la experiencia de sesión a los que se enfrentan los usuarios. Esto es útil para depurar problemas que son difíciles de reproducir.

Para obtener más información sobre la grabación dinámica de sesiones, consulte el artículo Servicio de grabación de sesiones.

Herramienta de inscripción para registrar los VDA mediante WebSockets en catálogos de máquinas. Ahora puede usar esta herramienta de inscripción para registrar de forma segura sus VDA que no estén unidos a un dominio en catálogos de máquinas. Esta función ofrece las ventajas de usar solo el puerto TLS 443 para la comunicación del VDA al Delivery Controller y eliminar el tráfico del puerto 80. Para obtener más información, consulte Inscribir máquinas en catálogos mediante la herramienta de inscripción de VDA de WebSocket.

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

Configuración completa: Posibilidad de actualizar más parámetros de VM de Azure mediante perfiles de máquina. Con la Configuración completa, ahora puede actualizar una gama más amplia de parámetros de las VM de Azure aprovisionadas por MCS a través de perfiles de máquina, lo que incluye:

- Tamaño de la máquina
- Tipo de licencia
- Zona de disponibilidad
- ID de grupo de hosts dedicado

Tras actualizar el perfil de la máquina, Configuración completa compara los parámetros actuales con los nuevos. Si existen diferencias, se le pedirá que confirme cuáles aplicar. Este diseño garantiza actualizaciones transparentes y eficientes de la configuración de las máquinas virtuales.

Configuración completa: Posibilidad de cambiar las propiedades de la caché de reescritura para las VM de Azure aprovisionadas por MCS. En el caso de las VM de Azure aprovisionadas con Machine Creation Services (MCS), ahora puede cambiar sus propiedades de caché de reescritura (WBC), como **Tamaño de la caché de disco**, **Tamaño de la caché de memoria** y **Habilitar el ahorro de costes de almacenamiento**, mediante la Configuración completa. Además, al seleccionar un nuevo tamaño de máquina o perfil de máquina para esas VM, la Configuración completa valida los parámetros de WBC para evitar conflictos, como superar el límite de memoria de la nueva selección. Si se producen conflictos, se le pedirá que vuelva a configurar los parámetros de WBC.

Febrero de 2024

Funciones nuevas y mejoradas

Suspender VM de la interfaz de Workspace.. Ahora puede suspender las máquinas virtuales persistentes con sesiones activas desde la interfaz de usuario de Workspace. Esta mejora ofrece las sigu-

ientes ventajas:

- Posibilidad de reanudar el sistema desde donde lo dejó.
- Tiempo de inicio más rápido en comparación con una máquina desasignada detenida.
- Rentabilidad y eficiencia energética.
- Eficiencia en la asignación de recursos mediante la función Autoscale.

Nueva función MCSIO, optimización del almacenamiento de Machine Creation Services (MCS): ahora tiene la opción de que Image Portability Service agregue o quite MCSIO al preparar una imagen para el aprovisionamiento de MCS.
Para obtener más información, consulte Automatizar la configuración de VDA.

Mejoras en la descripción general de los sondeos: Ya está disponible un resumen de las métricas del sondeo y las Fases de fallo de sondeo en la página **Sonda** > **Descripción general**. Las métricas del sondeo muestran el número de ejecuciones programadas, fallidas, omitidas y correctas. La representación gráfica de las fases de fallo ayuda a analizar las fases en las que se produjeron la mayoría de los fallos. Esta información ayuda a solucionar rápidamente los resultados del sondeo. Para obtener más información, consulte el artículo Sondeo de aplicaciones y escritorios.

Información de las imágenes en la página Catálogos de máquinas. Ahora puede ver la siguiente información de una imagen a través de las **Propiedades de plantilla** del catálogo de máquinas:

- Sistema operativo
- Machine Identity Service
- Almacenamiento de Machine Creation Services
- Ruta de archivo de `pagefile.sys` para implementaciones de Azure

Esta mejora proporciona una mayor claridad en la información de la imagen y garantiza que los administradores tengan toda la información sobre el catálogo de máquinas en un único lugar.

Compatibilidad con la Configuración completa para la administración de tokens para la inscripción de VDA. La inscripción de VDA basada en tokens reduce la carga en los Cloud Connector, así como los puntos de fallo potenciales, lo que resulta ideal para los casos de uso en que se preparan las máquinas con tecnología que no es Citrix Provisioning. Mediante Configuración completa, ahora puede generar y administrar los tokens de inscripción para los VDA que no están aprovisionados por Citrix, lo que agiliza las implementaciones basadas en tokens de inscripción. Para obtener más información, consulte Generar y administrar los tokens de inscripción.

Registro de PowerShell. En Configuración completa, ahora puede ver los comandos de PowerShell correspondientes a sus acciones de interfaz de usuario diarias. Esta función le ayuda a obtener información informaciósobre los comandos subyacentes de PowerShell con fines de aprendizaje. Para ver los registros de PowerShell, vaya a **Registro > PowerShell**. Para obtener más información, consulte Registro de configuraciones.

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

Citrix Hypervisor cambió su nombre a XenServer en Configuración completa. De acuerdo con nuestra estrategia de cambio de marca, hemos actualizado todas las instancias de Citrix Hypervisor dentro de Configuración completa a XenServer.

Vista de salto de red de extremo a extremo. La vista de salto de red de extremo a extremo es el siguiente paso para mejorar los flujos de trabajo de solución de problemas en Citrix Monitor. La sección **Detalles del usuario** > **Rendimiento de la sesión** > **Topología de la sesión** proporciona una representación visual de la vista de salto de red de extremo a extremo para las sesiones HDX conectadas. La ruta durante la sesión ayuda a comprender los componentes que intervienen en la ruta de sesión con sus metadatos, el enlace entre los componentes y las aplicaciones publicadas en el VDA. La topología de sesión ayuda a los flujos de datos y a identificar el salto específico que podría estar provocando problemas de rendimiento.

Además, las mediciones de la latencia de ICA e ICA RTT se muestran para la sesión cuando esta está conectada. Para obtener más información, consulte la vista de salto de red de extremo a extremo.

Use el ID del conjunto de cifrado de disco (ID de DES) de la imagen maestra para cifrar todos los discos de las máquinas virtuales del catálogo. En los entornos de Azure, anteriormente, el ID del conjunto de cifrado de disco (ID de DES) de un catálogo de máquinas MCS se derivaba de un perfil de máquina o de propiedades personalizadas. Con esta función, un catálogo de máquinas también puede derivar el ID de DES de la imagen maestra para cifrar todos los discos de la máquina virtual de un catálogo.

Actualice las etiquetas MCS para detectar los recursos huérfanos después de la migración. Cuando migra la configuración de local a un sitio en la nube o de la nube a otro sitio en la nube, los recursos huérfanos no se detectan correctamente debido a la etiqueta antigua de identificación del sitio. Mediante un comando de PowerShell, con esta función puede actualizar las etiquetas de identificación del sitio MCS de un catálogo persistente, después de la migración, para que los recursos huérfanos se puedan detectar correctamente. Actualmente, esta función se aplica a Azure. Para obtener más información, consulte Actualizar las etiquetas MCS para detectar recursos huérfanos después de la migración.

Valide la configuración antes de crear un catálogo de máquinas MCS. Con esta función, ahora puede validar los parámetros de configuración antes de crear un catálogo de máquinas MCS mediante el parámetro `-validate` del comando `New-ProvScheme`. Después de ejecutar este comando de PowerShell con ese parámetro, se muestra el mensaje de error correspondiente si se usa un parámetro

incorrecto o si un parámetro tiene conflictos con otro parámetro. A continuación puede usar el mensaje de error para resolver el problema y crear sin problemas un catálogo de máquinas MCS con PowerShell.

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

Compatibilidad con copia de etiquetas de un origen de perfil de máquina a una máquina virtual en AWS. En entornos de virtualización de AWS, con esta función se pueden copiar las etiquetas de las NIC y los discos (disco de identidad, disco de caché de reescritura y disco de sistema operativo) que se especifican en el perfil de la máquina a las máquinas virtuales recién creadas en un catálogo de máquinas de MCS. Puede especificar estas etiquetas en cualquiera de los orígenes de perfiles de máquinas (instancia de AWS EC2 o versión de plantilla de inicio de AWS). Esta función se aplica a máquinas virtuales y catálogos de máquinas persistentes y no persistentes. Para obtener más información, consulte Copiar etiquetas en máquinas virtuales.

Compatibilidad con SCVMM para perfiles de máquinas. Con esta función, ahora puede usar un perfil de máquina para crear y actualizar un catálogo de máquinas MCS en entornos de System Center Virtual Machine Manager (SCVMM). También puede habilitar la virtualización anidada y el vTPM. Para obtener más información, consulte Crear un catálogo con un perfil de máquina.

Compatibilidad de Azure para el uso de máquinas virtuales puntuales con MCS. Las máquinas virtuales Azure Spot le permiten aprovechar la capacidad informática no usada de Azure con un importante ahorro de costes. Sin embargo, debido a su directiva de desalojo, las máquinas virtuales de Azure Spot solo son válidas para algunas aplicaciones y escritorios no críticos.

Con esta función, puede crear un catálogo de máquinas MCS de máquinas virtuales de Azure Spot mediante un perfil de máquina (especificación de máquina virtual o plantilla). Puede actualizar un catálogo existente para que las máquinas virtuales de Azure Spot sean las máquinas virtuales recién creadas o cambiarlas para tener máquinas virtuales de Azure estándar. También puede actualizar las máquinas virtuales existentes para que sean máquinas virtuales de Azure Spot. Para obtener más información, consulte Crear un catálogo con máquinas virtuales de Azure Spot.

Compatibilidad con la captura de parámetros de diagnóstico de un perfil de máquina. En los entornos de Azure, MCS ahora presenta una función disponible para la captura de los parámetros de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina al crear o actualizar un catálogo de máquinas MCS o al actualizar las máquinas virtuales existentes. Por lo tanto, con esta implementación, los datos de diagnóstico se pueden transmitir sin problemas a los dispositivos de puntos finales de destino designados de Azure, como los espacios de trabajo de análisis de registros o los centros de eventos, para un análisis y una visualización en profundidad. Para obtener más información, consulte Capturar los parámetros de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina.

Función disponible de MCS para administrar diferentes versiones de un catálogo de máquinas. Con esta función, puede administrar las versiones de configuración de un catálogo de máquinas mediante los comandos de PowerShell. Cada cambio de configuración con ayuda de `Set-ProvScheme` trae consigo una nueva versión de configuración. Puede hacer lo siguiente:

- Ver la lista de versiones.
- Use cualquier versión anterior para actualizar un catálogo de máquinas.
- Elimine manualmente una versión si no la usa ninguna máquina virtual.
- Cambie el número máximo de versiones que debe conservar un catálogo de máquinas.

Para obtener más información, consulte Administrar versiones de un catálogo de máquinas.

Publique App-V, MSIX y la conexión de aplicaciones MSIX empaquetadas en VDA de escritorio compartido y de sesión única. Ahora puede acceder a las aplicaciones empaquetadas, por ejemplo, App-V, MSIX y conexión de aplicaciones MSIX en los VDA de escritorio compartido y de sesión única. Esta mejora garantiza que las aplicaciones empaquetadas estén disponibles para su uso al iniciar sesión. Esta función facilita el lanzamiento más rápido de las aplicaciones empaquetadas y mejora su experiencia de manera significativa al acercarla al acceso a una aplicación instalada localmente. Para obtener más información, consulte Publicar aplicaciones empaquetadas en VDA de escritorio compartido o de sesión única.

Reproducir sesiones grabadas y en directo: Citrix Monitor ahora dispone de la función de reproducir sesiones de usuario grabadas y en directo que se graban mediante el servicio Grabación de sesiones. Después de reproducir la sesión, podrá comprender rápidamente los problemas relacionados con la sesión tuvo el usuario. Con esta función, puede acceder fácilmente a las grabaciones junto con las métricas relacionadas con la sesión en la consola de Supervisar. Ayuda a correlacionar los problemas descubiertos en las grabaciones con las métricas de rendimiento. Elimina la necesidad de buscar grabaciones en varios servidores de grabación de sesiones o de buscar aplicaciones de terceros para ver las grabaciones.

Esta función requiere el VDA y la versión 2308 o una posterior del Servidor de grabación de sesiones.

Supervisar almacena las grabaciones en un repositorio centralizado y las muestra en el modal del **Selector de sesiones**. El enlace **Sesiones con grabaciones** muestra las grabaciones de las sesiones que estuvieron activas durante las últimas 24 horas o los últimos 2 días. La grabación se reproduce en una ficha nueva mediante el servidor de reproducción de grabación de sesiones de Citrix.

Para obtener más información, consulte Grabar sesiones.

Optimización de Microsoft Teams: Supervisar muestra el estado de la optimización de HDX disponible para Microsoft Teams. La nueva **Optimización de Microsoft Teams** se puede ver en la página **Detalles del usuario**, en el panel **Detalles de la sesión**. Supervisar muestra el estado de la optimización de Microsoft Teams solo si Microsoft Teams se ejecuta como una aplicación publicada o dentro de un escritorio publicado. Esta mejora proporciona a los administradores visibilidad para

facilitar la solución de problemas de rendimiento de las sesiones en Microsoft Teams notificados por los usuarios. Para obtener más información, consulte Solucionar problemas de usuarios.

Mejoras en la interfaz de usuario: la interfaz de usuario de Citrix Monitor ahora se ha actualizado con un aspecto renovado. La nueva y mejorada interfaz de usuario ofrece una navegación más sencilla y una mejor representación de los datos. La experiencia mejorada es intuitiva y está diseñada para comprender fácilmente los datos necesarios para supervisar y solucionar problemas en una sesión de Citrix.

Resolución de pantalla óptima: la resolución de pantalla óptima recomendada para ver Citrix Monitor se actualizó a 1440 x 1024.

Enero de 2024

Funciones nuevas y mejoradas

Configuración mejorada de redirección bidireccional de contenido Anteriormente, la configuración de la redirección bidireccional de contenido implicaba la administración de tres directivas distintas: Permitir redirección bidireccional de contenido, Permitir la redirección de direcciones URL al VDA y Permitir la redirección de direcciones URL al cliente. Estas directivas requieren configuraciones tanto en el lado del servidor (configuración en **DaaS > Configuración completa**) como en el lado del cliente (configuración mediante Directivas de grupo). A partir de esta versión, hemos consolidado las tres directivas en una directiva única y unificada. No solo simplifica y mejora el proceso de configuración, sino que también elimina la necesidad de hacer configuraciones del lado del cliente. Para obtener más información, consulte Configuración de redirección bidireccional de contenido.

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

Función para acceder a Global App Configuration Service desde Configuración completa. Hemos incluido elementos de acción en la interfaz de Configuración completa para enlazar con Global App Configuration Service. Con esta integración, puede acceder fácilmente a Global App Configuration Service para administrar parámetros del usuario final a través de la Configuración completa.

Para acceder a este servicio desde Configuración completa, tiene dos opciones:

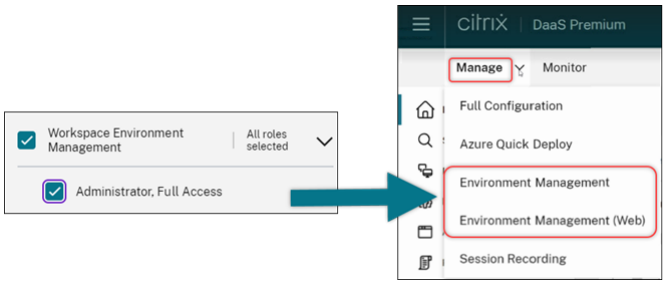
- Seleccione el nodo **StoreFront**, haga clic en un registro del servidor y, a continuación, seleccione **Configurar parámetros del cliente** en la barra de acciones.

- Seleccione el nodo **Directivas** y, a continuación, seleccione **Configurar parámetros del cliente** en la barra de acciones.

Posibilidad de administrar las asignaciones de usuarios para los grupos de entrega administrados por Citrix Cloud mediante la Configuración completa. Como parte de nuestro plan para migrar la administración de las asignaciones de usuarios de la biblioteca de Cloud a Configuración completa, ahora puede administrar las asignaciones de usuarios para los grupos de entrega administrados por Citrix Cloud a través de Configuración completa. Para ello, modifique un grupo de entrega de destino en **Configuración completa > Grupos de entrega** y designe a los usuarios autorizados para usar escritorios o aplicaciones a través de uno de estos menús: **Escritorios** (o **Reglas de asignación de escritorios**) o **Regla de asignación de aplicaciones**. Para obtener más información, consulte Administrar grupos de entrega.

Las actualizaciones realizadas en un portal se sincronizarán de forma fluida con el otro, lo que garantiza la coherencia de las actualizaciones en ambos portales.

Limitar el acceso a la consola de WEM al rol de administrador con acceso total de WEM. Hemos habilitado el control de acceso para las consolas de Workspace Environment Management (WEM) a fin de evitar la entrada no autorizada. Ahora, solo los usuarios con el rol **Administrador con acceso total de Workspace Environment Management** pueden usar **DaaS > Administrar** para acceder a las consolas de WEM.



Configuración completa: Los catálogos de Azure pueden heredar los parámetros de DES de las imágenes maestras. Anteriormente, Configuración completa establecía los parámetros de DES predeterminados de los catálogos de Azure solo en función de los perfiles de máquina. Ahora hemos ampliado esta capacidad. Con esta mejora, en los siguientes casos, Configuración completa establece los parámetros de DES predeterminados de un catálogo de Azure directamente basados en la imagen maestra:

- Si no se ha seleccionado un perfil de máquina
- Si el perfil especifica una clave administrada por la plataforma (PMK)

Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.

Búsqueda mejorada: Más filtros para una mayor precisión. Hemos mejorado la búsqueda en el nodo Buscar para incluir dos nuevos filtros, Zona y Tipo de aprovisionamiento, a fin de mejorar la

precisión y la usabilidad.

Configuración completa: Función para seleccionar el tipo de máquina de Google Cloud para los catálogos de máquinas de GCP. Con esta función, los administradores tienen la flexibilidad para seleccionar las configuraciones de memoria y procesador necesarias para las máquinas virtuales de GCP aprovisionadas, adaptándolas a requisitos operativos específicos. Para obtener más información, consulte Crear un catálogo de máquinas mediante la interfaz de configuración completa.

Compatibilidad con claves de cifrado administradas por el cliente (CMEK) globales y regionales para aprovisionar máquinas virtuales de GCP. Ahora puede usar claves CMEK globales y regionales para aprovisionar máquinas virtuales desde cualquier proyecto de aprovisionamiento. Esta mejora proporciona una mayor flexibilidad a la hora de seleccionar claves para aprovisionar máquinas virtuales y mejorar la seguridad de las máquinas virtuales.

Diciembre de 2023

Funciones nuevas y mejoradas

Progreso del envío de mensajes. Ahora puede ver el progreso de la operación **Enviar mensaje** en **Supervisar** > **Filtros**. Esta operación permite enviar mensajes en bloque a todas las sesiones conectadas de su sitio. El progreso de la operación se muestra en forma de porcentaje. Una vez finalizada la operación, el sistema muestra la cantidad de mensajes que se enviaron y la cantidad de mensajes fallidos. El estado del envío del mensaje es útil cuando se administran sitios de gran tamaño. Ayuda a entender si es necesario reenviar el mensaje a ciertos usuarios. El envío de mensajes puede fallar si las máquinas no están registradas o si las sesiones presentan fallos. Para obtener más información sobre el envío de mensajes, consulte Enviar mensajes a usuarios.

Citrix Probe Agent permite la autenticación de varios factores con credenciales de dominio a través de Citrix Gateway.

Ahora, Citrix Probe Agent para el sondeo de aplicaciones y escritorios permite la autenticación de varios factores con credenciales de dominio a través de Citrix Gateway. Esta función ayuda a ejecutar Probe Agent en máquinas que están conectadas a StoreFront a través de Citrix Gateway. Unos resultados exhaustivos de los sondeos disponibles en Supervisar pueden ayudar a solucionar problemas relacionados con las aplicaciones aprovisionadas, las máquinas de host o las conexiones antes de que los usuarios los experimenten. La compatibilidad de Citrix Gateway con autenticación de varios factores solo está disponible para Citrix Gateway configurado con LDAP y OTP nativo mediante un esquema de inicio de sesión único. Para obtener más información, consulte Sondeo de aplicaciones y escritorios

Se rediseñó la interfaz de usuario de Directiva de acceso para ofrecer mayor flexibilidad en el control de acceso a los recursos. Hemos rediseñado la interfaz de usuario de **Modificar grupo de entrega > Directiva de acceso** para darle mayor flexibilidad a la hora de administrar el acceso a los

recursos de los grupos de entrega. Estas son las principales funciones disponibles con el nuevo diseño:

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

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

Noviembre de 2023

Funciones nuevas y mejoradas

Función para crear catálogos de Citrix Provisioning mediante la interfaz de Configuración completa. Para crear un catálogo de Citrix Provisioning, tenía que usar el asistente de configuración de Citrix Virtual Apps and Desktops. Con esta función, ahora puede crear un catálogo de Citrix Provisioning mediante la interfaz de usuario de Configuración completa y PowerShell.

Esta implementación le ofrece las siguientes ventajas:

- Una única consola unificada para administrar los catálogos de MCS y de Citrix Provisioning.
- Hay nuevas funciones para los catálogos de Citrix Provisioning, como la solución de administración de identidades, el aprovisionamiento bajo demanda, etc.

De momento, esta función solo está disponible para las cargas de trabajo de Azure. Para obtener más información, consulte Crear catálogos de Citrix Provisioning en Citrix Studio.

Presentamos la búsqueda de grupos de aplicaciones. Hemos introducido la función de búsqueda de grupos de aplicaciones en el nodo **Aplicaciones**. Con esta mejora, ahora puede buscar directamente un grupo de aplicaciones dentro de cualquier carpeta de aplicaciones. Para obtener más información, consulte Buscar grupos de aplicaciones.

Límites de configuración modificados. En la siguiente tabla se describen las modificaciones realizadas en los límites de configuración de DaaS para mejorar el rendimiento y ofrecer rentabilidad.

Recurso	Límite anterior	Nuevo límite
Dominios de Active Directory	85	100
Catálogos	1000	2000
Grupos de entrega	1000	2000
Ubicación de recursos	85	100
Ubicación de recursos -> Total de sesiones	20 000	25 000

Para obtener más información, consulte Límites.

Una única opción para conservar la máquina virtual y el disco del sistema durante los ciclos de energía. Iniciar una máquina virtual existente en Azure ahora es más rápido que iniciar una nueva, por lo que retener las máquinas virtuales durante los ciclos de energía es una opción más eficiente. En respuesta a este cambio, hemos combinado las opciones **Conservar las máquinas virtuales durante los ciclos de energía** y **Conservar el disco del sistema durante los ciclos de energía** en una sola opción, **Conservar VM y disco del sistema durante los ciclos de energía**. Esto significa que, al seleccionar esta opción para reducir los tiempos de reinicio de las máquinas virtuales conservando los discos del sistema, también se conservan las máquinas virtuales.

Nueva función en la Configuración completa para filtrar los tamaños de las máquinas en función de la *propiedad Encryption at Host* (Cifrado en el host) en los perfiles de las máquinas (específico de Azure VM). Una vez que elija un perfil de máquina con *Encryption at host* habilitado durante la creación o administración del catálogo de máquinas de Azure, solo se muestran los tamaños de máquina que admiten esta función.

Restringir las acciones de copia de seguridad y restauración al rol Administrador total. Hemos mejorado el control de acceso para las acciones de copia de seguridad y restauración. Ahora, solo los usuarios con el rol Administrador total pueden acceder al nodo **Copia de seguridad + Restauración** para evitar acciones no autorizadas.

Almacenamiento en caché de datos para el nodo de búsqueda. Hemos introducido el almacenamiento en caché de datos para el nodo **Buscar** de Citrix DaaS. Con esta mejora se logra un mejor rendimiento de búsqueda. A continuación se enumeran los casos de uso que facilitan las tareas habituales:

- Visualización rápida de los resultados de la búsqueda después de obtenerlos por primera vez.
- Conservación de los resultados de paginación después de salir y volver al nodo **Buscar**.

Información de las imágenes en la página Catálogos de máquinas. Ahora puede ver la siguiente información de una imagen a través de las **Propiedades de plantilla** del catálogo de máquinas:

- Sistema operativo
- Machine Identity Service
- Almacenamiento de Machine Creation Services
- Ruta de archivo de `pagefile.sys` para implementaciones de Azure.

Esta mejora proporciona una mayor claridad en la información de la imagen y garantiza que los administradores tengan toda la información sobre el catálogo de máquinas en un único lugar.

Función para fijar filtros de búsqueda. Para ofrecer una experiencia de búsqueda rápida, la Configuración completa permite fijar filtros de búsqueda. Al fijar filtros, es posible mantener accesibles en la página los filtros de búsqueda que se utilizan con frecuencia. Esta mejora está disponible en los paneles de búsqueda de los siguientes nodos:

- **Buscar**
- **Catálogos de máquinas**
- **Grupos de entrega**
- **Aplicaciones**

Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Función para asociar metadatos a registros de configuración. Con esta mejora, ahora puede adjuntar metadatos a los registros de configuración asociando un par `name-value` a las operaciones de alto nivel. Para obtener más información, consulte Asociar metadatos a registros de configuración.

Ignorar los recursos huérfanos con una etiqueta específica. En los entornos de Azure, un recurso administrado por el cliente etiquetado con todas las etiquetas de Citrix se detecta como un recurso huérfano. Con esta función, si agrega otra etiqueta `CitrixDetectIgnore` con el valor true para ese recurso, el recurso se omite al detectar los recursos huérfanos.

Solución para el problema de GUID duplicados de SCCM. Tras crear varias máquinas virtuales mediante MCS, System Center Configuration Manager (SCCM) mostraba solo una máquina virtual en su consola debido a duplicación de los GUID. Este problema ahora se resuelve agregando un paso en la preparación de la imagen. Este paso elimina los certificados y la información de GUID existentes en la imagen maestra. El paso está habilitado de forma predeterminada.

Reparar la información de identidad de las cuentas de equipo activas. Con esta función, puede restablecer la información de identidad de las cuentas de equipo activas que tengan problemas relacionados con la identidad. Puede elegir restablecer solo la contraseña de la máquina y las claves de confianza, o bien restablecer toda la configuración del disco de identidad. Esta implementación se aplica tanto a catálogos de máquinas persistentes como no persistentes. En la actualidad, la función

solo es compatible con los entornos de virtualización de Azure y VMware. Para obtener más información, consulte Reparar la información de identidad de las cuentas de equipo activas.

Cifrado en la información de host asociada a un perfil de máquina. En los entornos de Azure, con esta función, ahora puede saber si el cifrado en el host está habilitado para una entrada de perfil de máquina (VM o especificación de plantilla) mediante comandos de PowerShell. Para obtener más información, consulte Recuperar la información de cifrado en el host de un perfil de máquina.

Reparar los certificados de usuario de las identidades de máquinas híbridas unidas a Azure AD. Con esta función, puede usar un comando de PowerShell para reparar los certificados de usuario de las identidades de máquinas híbridas unidas a Azure AD si están dañados o han caducado. Para obtener más información, consulte Crear catálogos unidos a Azure Active Directory híbrido.

Compatibilidad con advertencias de caducidad de certificados para catálogos de máquinas unidas a Hybrid Azure AD. Configuración completa ahora proporciona advertencias con un mes de antelación sobre la caducidad de los certificados de usuario en los catálogos de máquinas unidas a Hybrid Azure AD. Esta mejora tiene como objetivo reducir el riesgo de interrupciones del servicio como resultado de la caducidad del certificado. Para ver los detalles y las acciones recomendadas, vaya al nodo **Catálogos de máquinas**, seleccione el catálogo de máquinas y, a continuación, haga clic en la ficha **Solucionar problemas**.

Puede ejecutar el comando `Get-ProvScheme` para obtener información sobre la fecha de caducidad del certificado de usuario de un catálogo de máquinas unido a Azure AD híbrido.

Compatibilidad con máquinas virtuales confidenciales de Azure (Technical Preview). Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa. Con esta función, ahora puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina. Para obtener más información, consulte Máquinas virtuales confidenciales de Azure (Technical Preview).

Función para convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina en un entorno de AWS. Ahora, en un entorno de AWS, puede utilizar una máquina virtual o una plantilla de inicio como entrada de perfil de máquina para convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina. Las nuevas máquinas virtuales agregadas al catálogo toman los valores de las propiedades del perfil de máquina. Para obtener más información, consulte Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina.

Compatibilidad con el plug-in de HPE Moonshot administrado por Citrix (Technical Preview). Anteriormente, se usaba el plug-in de Moonshot administrado por HPE (HPE Moonshot Machine Manager) mantenido por Hewlett Packard Enterprise (HPE) para realizar las acciones de administración

de energía en el chasis HPE Moonshot. El plug-in se basaba en API antiguas que dificultaban los proyectos de infraestructura de MCS. Con esta función, se presenta un plug-in de HPE Moonshot administrado por Citrix (HPE Moonshot). Con este plug-in, puede crear conexiones a su chasis HPE Moonshot, crear catálogos y administrar la energía de las máquinas del catálogo mediante la interfaz de Configuración completa y los comandos de PowerShell. Para obtener más información, consulte:

- Entornos de virtualización de HPE Moonshot (Technical Preview)
- Conexión a HPE Moonshot (Technical Preview)
- Crear un catálogo de máquinas de HPE Moonshot (Technical Preview)
- Administrar un catálogo de HPE Moonshot (Technical Preview)

Posibilidad de cambiar el tamaño de la memoria y de la caché de disco. Con esta función, ahora puede cambiar el tamaño de la memoria y de la caché de disco de la caché de reescritura (cuando E/S de MCS está habilitada) mediante un comando de PowerShell sin crear un nuevo catálogo de máquinas. Esta implementación le ayuda a tener una configuración de caché optimizada que se adapta a las necesidades de su empresa. Esta función se aplica a:

- Entornos de GCP y Microsoft Azure, y
- un catálogo no persistente con E/S de MCS habilitada

Para obtener más información, consulte Cambiar la configuración de la caché en un catálogo de máquinas existente.

Función para crear un catálogo con claves de cifrado administradas por el cliente. En los entornos de Azure, ahora puede crear un catálogo de Citrix Provisioning habilitado con una clave de cifrado administrada por el cliente (CMEK) mediante la interfaz de Configuración completa y los comandos de PowerShell. Para obtener más información, consulte Crear un catálogo habilitado para claves de cifrado administradas por el cliente.

Posibilidad de copiar etiquetas en todos los recursos de Azure. Con esta función, en el entorno Azure, ahora puede copiar las etiquetas especificadas en un perfil de máquina en todos los recursos, como varias NIC y discos (disco del sistema operativo, disco de identidad y disco de caché de reescritura), de una máquina virtual nueva o existente de un catálogo de máquinas.

La fuente del perfil de máquina puede ser una VM o una especificación de plantilla de Azure Resource Manager. Para obtener más información, consulte Copiar etiquetas en todos los recursos.

El estado de la sesión cambia a desconectado al suspender la máquina. Anteriormente, después de suspender una máquina virtual, la sesión seguía mostrándose como **Activa**. Con esta mejora, después de suspender una máquina virtual, el estado de la sesión asociada ahora se muestra como **Desconectada**.

Posibilidad de crear máquinas virtuales de AWS que admitan la hibernación. Ahora puede crear catálogos de máquinas que admitan la hibernación de máquinas virtuales en sus entornos de AWS, lo que mejora la rentabilidad general de su implementación. También puede modificar un catálogo

para incluir máquinas virtuales con capacidad de hibernación si el perfil de máquina asociado admite esta capacidad. Para obtener más información, consulte Administrar la energía de las VM de AWS.

Función para configurar métodos de equilibrio de carga a nivel de grupo de entrega (Technical Preview). Esta función le permite elegir el método de **equilibrio de carga vertical** a nivel de grupo de entrega. Con esta función, cada máquina se ajusta al índice de carga máximo antes de que se encienda la siguiente máquina. Autoscale y Equilibrio de carga vertical determinan cuándo se enciende la siguiente máquina. Esta función logra la máxima utilización de cada máquina y ahorro de costes en nubes públicas. Esta función ofrece más flexibilidad a la hora de administrar las estrategias de equilibrio de carga de las máquinas.

Puede configurar un grupo de entrega para que herede el método de equilibrio de carga de los parámetros a nivel de sitio o anular el método de equilibrio de carga a nivel de sitio y elegir en su lugar uno de los métodos de equilibrio de carga vertical u horizontal. Para obtener más información, consulte el paso 2. Equilibrio de carga.

Compatibilidad con máquinas virtuales que admiten hibernación en Azure (Technical Preview). En entornos de Azure, puede crear un catálogo de máquinas de MCS que admita la hibernación. Con esta función, puede suspender una máquina virtual y, a continuación, conectarse de nuevo al estado anterior de la misma cuando un usuario vuelva a iniciar sesión. Para obtener más información, consulte Crear VM con capacidad de hibernación (Technical Preview).

Guía de introducción a DaaS. Hemos publicado una nueva guía para optimizar y simplificar la implementación y la configuración de DaaS para administradores nuevos y experimentados. Ofrece estas ventajas clave:

- **Inicio fácil.** Con cuestionarios paso a paso, esta guía ayuda a los nuevos administradores a configurar sus implementaciones rápidamente. La información de ayuda contextual que aparece en la guía ayuda a comprender conceptos y terminología esenciales.
- **Simplifique configuraciones complejas.** Esta guía incluye parámetros preconfigurados donde sea necesario y proporciona acceso a la interfaz de usuario de Configuración completa para configuraciones avanzadas. Los administradores experimentados pueden usarla como base para configuraciones más complejas.

Para obtener más información, consulte Guía de introducción al uso de DaaS.

Asigne letras de unidad a discos de caché de reescritura mediante Configuración completa. Antes, solo podía asignar una letra de unidad específica al disco de memoria caché de reescritura mediante un cmdlet de PowerShell. Ahora puede realizar la misma tarea con Configuración completa. Para obtener más información, consulte Crear catálogos de máquinas.

Función para cambiar varias propiedades de máquinas de Azure mediante Configuración completa. Ahora, para las máquinas Azure aprovisionadas por Machine Creation Services, puede cambiar estos parámetros de propiedades mediante Configuración completa:

- Tipo de almacenamiento
- Grupo de hosts dedicado
- Parámetros de Azure Compute Gallery

Al cambiar cualquiera de estos parámetros, Configuración completa identifica automáticamente parámetros relacionados y proporciona una sincronización automática o mensajes de aviso en los que se le solicita que seleccione de nuevo los parámetros relacionados. Esta prestación garantiza cambios coherentes en los parámetros asociados, lo que evita posibles errores de configuración. Para obtener más información, consulte Modificar un catálogo.

Use agrupaciones de identidades existentes con el fin de crear identidades para máquinas aprovisionadas por MCS. Ahora, al crear catálogos unidos a AD o agregarles máquinas mediante Configuración completa, puede usar un grupo de identidades existente para asignar identidades de máquinas. Esta función le permite aplicar un esquema de nombres de cuentas de máquina coherente en varios catálogos. Para obtener más información, consulte Identidades de las máquinas.

Topología de sesión. La vista Topología de sesión es el siguiente paso para mejorar flujos de trabajo de solución de problemas en Supervisar. La vista Topología de sesión proporciona una representación visual de la ruta de las sesiones de HDX conectadas. Puede acceder a la vista de topología desde **Detalles de usuario > Rendimiento de sesión**.

La vista Topología de sesión de una sesión de HDX conectada muestra los componentes involucrados en la ruta de la sesión con sus metadatos, el enlace entre los componentes y las aplicaciones publicadas en VDA. Además, las mediciones de la latencia de ICA e ICA RTT se muestran para la sesión cuando esta está conectada.

Use la vista Topología de sesión para comprender los componentes a través de los cuales fluyen los datos de la sesión e identificar el salto específico que podría ocasionar problemas de rendimiento. Para obtener más información, consulte Topología de sesión.

Octubre de 2023

Funciones nuevas y mejoradas

Ajuste los parámetros de Autoscale mediante el uso histórico. La nueva ficha de parámetros de Autoscale denominada **Datos detallados de Autoscale** ofrece un gráfico completo que compara visualmente los parámetros de Autoscale y los datos de uso de las máquinas desde la semana anterior. Con este gráfico, puede obtener información sobre la eficacia de los parámetros de Autoscale:

- **No es rentable**. Hay un despilfarro financiero debido al exceso de aprovisionamiento de capacidad.
- **Mala experiencia de usuario**. La experiencia del usuario se ve afectada negativamente debido al insuficiente aprovisionamiento de capacidad.

- **Buen equilibrio entre la experiencia de usuario y el coste**. La capacidad aprovisionada está alineada con el uso histórico.

Para obtener más información, consulte Analizar la eficacia de los parámetros de Autoscale.

Compatibilidad con varias NIC para máquinas virtuales de Azure. Ahora, con Configuración completa, puede crear máquinas virtuales de Azure con varias NIC. El recuento máximo de NIC de una máquina virtual viene determinado por el parámetro del tamaño de la máquina, mientras que el recuento real de NIC permitido lo define el parámetro del perfil de la máquina. Para obtener más información, consulte Crear catálogos de máquinas.

Para crear o actualizar un catálogo con varias NIC por máquina virtual mediante comandos de PowerShell, consulte Crear o actualizar un catálogo con varias NIC por máquina virtual.

Tendencias de las métricas de rendimiento de las sesiones. Supervisar presenta la nueva ficha **Detalles del usuario > Rendimiento de sesión** con flujos de trabajo para la solución de problemas mejorados, empezando por la capacidad de correlacionar métricas en tiempo real para identificar problemas dentro de las sesiones de los usuarios. Ahora, Experiencia de sesión contiene tendencias de métricas de sesión como ICARTT, latencia de ICA, fotogramas por segundo, ancho de banda de salida disponible y ancho de banda de salida consumido. Esta función ayuda a reducir el tiempo medio de resolución al permitirle correlacionar varias métricas de rendimiento en una sola vista. Para obtener más información, consulte el artículo Problemas de usuario.

Compatibilidad con versiones de VDA en la página de parámetros de la directiva de creación/-modificación. Como parte de la creación de directivas y al configurar los parámetros, el sistema ofrece una opción para ver el tipo de parámetros. Puede ver los siguientes tipos de parámetros:

- Todos los parámetros: Ver todos los parámetros de todas las versiones de VDA
- Solo parámetros actuales: Ver solo los parámetros de las versiones actuales de VDA
- Solo parámetros antiguos: Ver solo los parámetros de las versiones retiradas de VDA

Para obtener más información, consulte Crear directivas.

Limitar la visibilidad de las aplicaciones solo para las cuentas de Active Directory. La capacidad de limitar la visibilidad de las aplicaciones solo está disponible para las cuentas de usuario de Active Directory y no para las cuentas de Azure Active Directory y Okta. Para facilitar esta función, en el flujo de trabajo de configuración de la aplicación, en la página Seleccionar usuarios o grupos, las opciones **Azure Active Directory** y **Okta** del campo **Seleccione el tipo de identidad** están inhabilitadas.

Nueva opción de la interfaz de usuario para eliminar los registros de VM únicamente de la base de datos del sitio de Citrix. Cuando se produce un error al eliminar un catálogo y máquinas virtuales debido a un hipervisor no accesible, ahora puede optar por eliminar únicamente los registros de VM de la base de datos del sitio de Citrix, dejando las VM intactas en el host. Para obtener más información, consulte Eliminar un catálogo.

Función para crear catálogos de máquinas vacíos para máquinas no aprovisionadas por MCS. La creación de catálogos de máquinas vacíos ahora se extiende a las máquinas no aprovisionadas por MCS, incluidas las siguientes:

- Máquinas virtuales o blade aprovisionadas mediante tecnologías distintas de Machine Creation Services.
- Máquinas físicas no administradas por Citrix DaaS
- Máquinas de acceso con Remote PC

Con esta función, ahora puede crear catálogos de máquinas sin necesidad de agregarles máquinas durante la creación de dichos catálogos.

Mejoras en la actualización de imágenes. Anteriormente, al actualizar las imágenes, se actualizaban todas las imágenes del árbol, independientemente de si se había seleccionado un nodo específico del árbol. Con la última mejora, si selecciona un nodo, solo se actualizan las imágenes de ese nodo. Esta mejora garantiza un proceso de actualización más selectivo y aumenta significativamente la velocidad de actualización de las imágenes. Además, ahora puede borrar un nodo seleccionado del árbol de imágenes manteniendo presionada la tecla CTRL y haciendo clic en el nodo. Para obtener más información, consulte Imagen maestra.

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

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

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

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

Supervisar varias instancias de Citrix DaaS (Technical Preview). Ahora puede usar Citrix Monitor para supervisar y solucionar problemas en varias instancias de Citrix DaaS. Citrix DaaS permite a los clientes agregar varias instancias de servicio mediante un modelo de tipo centro y radios. Con esta configuración, los administradores pueden realizar una búsqueda en el servicio de asistencia técnica en todas las instancias de DaaS configuradas desde una única consola Supervisar. Para obtener más información sobre la configuración necesaria para agregar las instancias de servicio de tipo radio a un

centro, consulte Agregar varias instancias de servicio de Citrix Virtual Apps and Desktops. Supervisar permite la agregación de hasta cuatro arrendatarios de DaaS (los radios) en un solo arrendatario (el centro).
Para supervisar de manera unificada todos los arrendatarios de DaaS, use la enumeración bidireccional de las instancias de centro y radios. Para obtener más información, consulte Búsqueda agregada en varias instancias de DaaS (Technical Preview).

Compatibilidad con vSAN 8.0. Ahora puede usar MCS para aprovisionar máquinas virtuales en el entorno de vSAN 8.0.

Conservar los parámetros de NIC en máquinas virtuales aprovisionadas. Antes, los parámetros de NIC de la imagen maestra no se conservaban en las máquinas virtuales aprovisionadas. Por ejemplo, si configuró los parámetros de DNS en la imagen maestra, las máquinas virtuales aprovisionadas no conservaban los parámetros de DNS configurados de la imagen maestra. Ahora, con esta función, las máquinas virtuales aprovisionadas pueden conservar los parámetros de NIC de la imagen maestra. Los parámetros se conservan incluso después de actualizaciones de Windows. El controlador de filtros se instala automáticamente si realiza una instalación nueva de la versión 2308 o una posterior de VDA en una máquina implementada con Hyper-V mediante las instalaciones de imágenes maestras de MCS. Sin embargo, actualmente, si actualiza una versión anterior de VDA (versión anterior a 2308) y quiere instalar el controlador de filtros, debe marcar la casilla del **controlador de filtros de Hyper-V de Citrix** de la página **Componentes adicionales** mientras actualiza el VDA. Para obtener más información, consulte Instalar componentes adicionales.

Esta función se aplica a:

- Máquinas virtuales con Hyper-V (incluidos Azure y SCVMM)
- Catálogos de máquinas de MCS persistentes y no persistentes
- Catálogos de máquinas de MCS no persistentes con E/S de MCS
- Imagen maestra con varias NIC

Detectar recursos huérfanos de Azure. Con esta función, ahora puede detectar los recursos huérfanos en su implementación de Azure, lo que permite administrar de manera eficiente los recursos. Una vez identificados los recursos huérfanos, puede adoptar medidas adicionales para aumentar la productividad y reducir los costes. Para obtener más información, consulte Detectar recursos de Azure huérfanos en su implementación.

Nuevo estado de actualización de las imágenes. Al supervisar los estados de actualización de las imágenes de los catálogos en Configuración completa, ahora puede ver un nuevo estado **Preparando la imagen**, además de los existentes **Totalmente actualizada**, **Parcialmente actualizada** y **Pendiente de actualizar**. Para obtener más información, consulte Cambiar la imagen maestra.

Comandos de PowerShell para crear etiquetas automáticas (Technical Preview). Con esta función, ahora puede crear etiquetas automáticamente mediante el comando de PowerShell. Para obtener más información, consulte Etiquetas automáticas.

El signo de notificación se muestra al usuario o al grupo de entrega. Al crear o modificar una directiva y configurar los parámetros, si todos los grupos de entrega están inhabilitados, el sistema muestra una advertencia en la que se indica que ninguno de los elementos de este filtro está habilitado. Si hay al menos un grupo de entrega habilitado, el sistema no muestra la señal de advertencia. Para obtener más información, consulte Configuraciones de directivas

Septiembre de 2023

Funciones nuevas y mejoradas

Comandos de PowerShell para administrar la caché de host local (LHC). Ahora puede usar los comandos de PowerShell para administrar la LHC en Citrix Cloud Connectors. Para obtener más información, consulte Comandos de PowerShell para la memoria caché de host local.

Función para crear catálogos de máquinas vacíos. En Configuración completa, ahora puede crear un catálogo de máquinas sin crear inmediatamente máquinas virtuales. Con esta función, puede posponer la creación de las máquinas virtuales hasta que los hosts de back-end estén completamente preparados o hasta que se complete el aprovisionamiento de las máquinas virtuales, lo que ofrece mayor flexibilidad a la hora de crear catálogos. Actualmente, esta función solo es aplicable a los catálogos aprovisionados por Machine Creation Services. Para obtener más información, consulte Crear catálogos de máquinas.

Almacenamiento en caché de datos para el nodo principal. Hemos introducido el almacenamiento en caché de datos para el nodo **Inicio** de Citrix DaaS. Esta mejora afecta a la experiencia del usuario al reducir el tiempo de carga de página cuando se navega al nodo **Inicio**.

Mejoras en la búsqueda de aplicaciones. Hemos renovado la funcionalidad de búsqueda en el nodo **Aplicaciones** para adaptarla al nuevo diseño introducido en el nodo **Buscar**. Esta nueva función mejora la experiencia de búsqueda de aplicaciones y la hace uniforme en todo DaaS. La palabra clave **Nombre de la aplicación** de la expresión de filtro cambia a **Nombre**, pero conserva su significado original. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Gestión de ámbitos mejorada: Muestra de objetos en una vista de carpetas. En las páginas de creación y administración de ámbitos, los catálogos de máquinas, los grupos de entrega y los grupos de aplicaciones se muestran ahora en estructuras de carpetas que se ajustan a su administración en DaaS. Esta vista de carpetas simplifica el proceso de selección de objetos para la creación y administración de ámbitos y lo hace más sencillo e intuitivo. Para obtener más información, consulte Crear y administrar ámbitos.

Se ha eliminado la opción Dejar a Citrix Cloud la administración de usuarios. Al crear un grupo de entrega en Administrar > Configuración completa, en la página Usuarios, ya no se ofrece esta opción. En el caso de los grupos de entrega en los que las asignaciones de usuarios se gestionaron a través

de Citrix Cloud, se pueden seguir gestionando las asignaciones de usuarios en la biblioteca de Citrix Cloud.

Se ha quitado la opción Azure Alemania. En consonancia con el cierre de Microsoft Cloud Deutschland el 29 de octubre de 2021, hemos quitado la opción **Azure Alemania** de la página de creación de conexiones de host.

Alertas de servicio proactivas en Configuración completa. Las alertas se presentan en dos niveles: Las alertas a nivel de todo el sitio que se muestran en la página de inicio (icono de bandera) y las alertas relacionadas con zonas que se muestran en la ficha Solucionar problemas de cada zona. Actualmente, esta función proporciona advertencias y alertas proactivas para garantizar que la caché de host local y las zonas estén correctamente configuradas, de modo que, cuando se produzca una interrupción, la caché de host local funcione y sus usuarios no se vean afectados. Para obtener más información, consulte Alertas de estado del servicio y Zonas.

Agosto de 2023

Funciones nuevas y mejoradas

Configuración completa: Función para aprovisionar máquinas virtuales de AWS y GCP mediante perfiles de máquina. Ahora, al aprovisionar máquinas virtuales de AWS o GCP mediante Machine Creation Services (MCS), puede seleccionar una máquina virtual existente como perfil de máquina, lo que permite que las máquinas virtuales del catálogo hereden parámetros de la máquina virtual seleccionada.

- Para las máquinas virtuales de GCP, los parámetros antiguos incluyen el ID del conjunto de cifrado de disco, el tamaño de la máquina, el tipo de almacenamiento y la zona.
- En el caso de las máquinas virtuales de AWS, los parámetros antiguos varían en función de la etapa:
  - Durante la creación del catálogo: Tamaño de la máquina, tipo de arrendamiento, grupo de seguridad y cantidad de NIC.
  - Durante la modificación del catálogo: Tamaño de la máquina y grupo de seguridad.

Para obtener más información, consulte Crear un catálogo de máquinas.

Presentamos la funcionalidad de búsqueda en los nodos Catálogos de máquinas y Grupos de entrega. Ahora puede buscar y localizar directamente catálogos de máquinas y grupos de entrega en los nodos **Catálogos de máquinas** y **Grupos de entrega**. La funcionalidad de búsqueda en estos nodos proporciona la misma interfaz que el nodo **Buscar**, lo que proporciona una experiencia de búsqueda nativa en todo DaaS. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Consulte el estado del dispositivo de punto final en Diagnóstico de inicios de sesión mediante Postura del dispositivo. La función de diagnóstico de inicios de sesión de Supervisar ayuda a detectar el componente y la fase exactos en que se produjo un error de sesión. Esto ayuda a identificar el motivo exacto del error en el inicio de una sesión y a adoptar las medidas recomendadas.

Ahora, como siguiente paso para que esta comprobación sea exhaustiva en todos los componentes que participan en la secuencia de inicio de la sesión, puede ver los resultados del escaneo del dispositivo de punto final. Al hacer clic en **Dispositivo de punto final** en la lista de componentes, se muestra el estado del escaneo de Postura del dispositivo. Device Posture Service analiza el dispositivo de punto final para comprobar su conformidad en función de directivas definidas por el administrador.

Asegúrese de que Device Posture Service esté configurado con DaaS tal y como se describe en el artículo Postura de dispositivos. Los errores registrados por Postura de dispositivos se describen en Registros de errores de Postura de dispositivos.

Para obtener más información, consulte Pasos para diagnosticar un error en el inicio de una sesión.

Nuevas opciones en Configuración completa para redirigir solicitudes de API a Azure y GCP a través de Citrix Cloud Connectors. Antes, las solicitudes de API a Azure y GCP solo se podían redirigir a través de dispositivos de punto final públicos. Ahora, con una nueva opción en **Configuración completa > Agregar conexión y recursos**, puede optar por un enfoque más seguro y redirigirlas a través de Citrix Cloud Connectors. Para obtener más información, consulte Crear una entidad principal de servicio y una conexión mediante Configuración completa.

Mejoras en las búsquedas y los filtrados. Hemos hecho estas mejoras en las búsquedas:

- **Búsqueda simplificada**: Ahora, al realizar una búsqueda sin filtros, se quitan las recomendaciones de búsqueda, lo que permite búsquedas claras y sencillas.
- **Actualización del operador AND/OR**: Ahora, las opciones "Hacer coincidir todo (operador AND)"y "Hacer coincidir cualquiera (operador OR)"están disponibles en el panel de filtros, al que se puede acceder con un solo clic en el icono de filtros.
- **Configuración de filtros simplificada**: Ahora puede especificar y aplicar varios filtros directamente desde el panel de filtros.
- **Interfaz más limpia**: Se ha quitado la función para fijar filtros, lo que simplifica la interfaz de usuario y hace que las búsquedas sean más intuitivas.
- **Incorporación rápida de filtros**: Ahora, después de aplicar filtros, puede usar el signo más para agregar rápidamente otro filtro.
- **Eliminar conjuntos de filtros guardados**: Ahora puede eliminar fácilmente conjuntos de filtros guardados directamente en el menú de búsqueda, sin tener que ir a **Administrar conjuntos de filtros**.

Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Función de actualización de versiones de VDA para catálogos de máquinas creados por Distribución rápida de Azure. Ahora, con Configuración completa, puede habilitar la **actualización de versiones de VDA** para catálogos de máquinas creados mediante Distribución rápida de Azure y, a continuación, **actualizar la versión de VDA** en ellos para llevar a cabo actualizaciones inmediatas o programadas. Para obtener más información, consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.

Posibilidad de restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS en SCVMM. Ya puede usar el comando `Reset-ProvVMDisk` de PowerShell para restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. La función automatiza el proceso de restablecimiento de disco del sistema operativo. Por ejemplo, ayuda a restablecer la máquina virtual a su estado inicial de un catálogo de escritorio de desarrollo persistente creado con MCS. Actualmente, esta función se aplica a los entornos de virtualización de Azure, Citrix Hypervisor, SCVMM y VMware. Para obtener más información sobre el uso del comando de PowerShell para restablecer el disco del sistema operativo, consulte Restablecer disco de SO.

Actualice propiedades de máquinas virtuales individuales. Ahora puede actualizar propiedades de máquinas virtuales individuales en catálogos de máquinas de MCS persistentes mediante un comando de PowerShell. Esta implementación le ayuda a administrar máquinas virtuales individuales de manera eficiente sin actualizar todo el catálogo de máquinas. Actualmente, esta función solo se aplica al entorno de Azure. Para obtener más información, consulte Actualizar propiedades de máquinas virtuales individuales.

Restrinja la carga y la descarga de discos administrados. Según la directiva de Azure, no puede cargar ni descargar más de cinco discos o instantáneas al mismo tiempo con el mismo objeto de acceso a disco. Con esta función, el límite de cinco cargas o descargas simultáneas no se aplica si:

- Configura `ProxyHypervisorTrafficThroughConnector` en `CustomProperties`
- Y no configura la directiva de Azure para crear accesos a disco automáticamente para que cada disco nuevo utilice dispositivos de punto final privados.

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

Compatibilidad con perfiles de máquina en Citrix Hypervisor. Ahora, en Citrix Hypervisor, puede crear un catálogo de máquinas de MCS mediante un perfil de máquina. El origen de la entrada del per-

fil de la máquina es una máquina virtual. El perfil de la máquina captura las propiedades del hardware de una plantilla de VM y las aplica a las máquinas virtuales recién aprovisionadas del catálogo. Para obtener más información, consulte Crear un catálogo de máquinas mediante un perfil de máquina.

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

Permiso para administrar conjuntos de configuraciones. Para permitir un control más preciso de la administración de conjuntos de configuraciones de WEM, presentamos un nuevo permiso denominado **Administrar conjuntos de configuraciones** en el conjunto de permisos de **Catálogos de máquinas**. Este permiso otorga acceso exclusivo a los usuarios que pueden realizar tareas como vincular o desvincular conjuntos de configuraciones y cambiar a conjuntos de configuraciones diferentes para los catálogos. Para obtener más información, consulte Administrar el conjunto de configuraciones de un catálogo.

Nueva opción en la Configuración completa para permitir la limpieza de los dispositivos obsoletos unidos a Azure AD. Hemos introducido una opción en Configuración completa para simplificar la limpieza de los dispositivos obsoletos unidos a Azure AD en Citrix DaaS. Anteriormente, tenía que ejecutar un script personalizado de PowerShell para realizar la tarea. Al habilitar esta opción, se concede permiso a las conexiones de host para limpiar automáticamente los dispositivos obsoletos unidos a Azure AD. Para obtener más información, consulte Conexiones de host de Azure.

Supervise el estado de actualización de las imágenes de los catálogos mediante la Configuración completa. Ahora puede supervisar los estados de actualización de las imágenes de los catálogos de máquinas no persistentes mediante una nueva columna, **Actualización de imágenes**. Esta columna indica si las imágenes de un catálogo están **Totalmente actualizadas**, **Parcialmente actualizadas** o **Pendientes de actualización**.

Para mostrar la columna en la tabla **Catálogos de máquinas**, siga estos pasos:

1. En el nodo **Catálogos de máquinas**, seleccione el icono **Columnas que mostrar** en la barra de acciones.
2. Seleccione **Catálogo de máquinas > Estado de la imagen**.
3. Haga clic en **Guardar**.

Al mostrar la columna **Actualización de imágenes**, puede disminuir el rendimiento de la consola. Recomendamos mostrarla solo cuando sea necesario.

Entorno seguro para el tráfico administrado de GCP. Con esta función, ahora puede permitir solo el acceso privado a Google en sus proyectos de Google Cloud. Esta implementación mejora la seguridad

a la hora de gestionar datos confidenciales. Para ello, agregue `ProxyHypervisorTrafficThroughConnect` a `CustomProperties` en el caso de una implementación de Citrix Cloud. Si utiliza una agrupación de trabajadores privados, agregue `UsePrivateWorkerPool` a `CustomProperties`. Para obtener más información, consulte Crear un entorno seguro para el tráfico administrado de GCP.

Julio de 2023

Funciones nuevas y mejoradas

Función para obtener una lista de recursos huérfanos en Azure. En los entornos de Azure, ahora puede obtener una lista de los recursos huérfanos que MCS crea, pero que MCS ya no usa. Esta función ayuda a evitar costes adicionales. Para obtener más información, consulte Obtener una lista de recursos huérfanos.

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

Nueva función en Configuración completa para filtrar el inventario de las AMI de AWS. Al seleccionar plantillas de máquinas durante la creación de catálogos de AWS, ahora puede filtrar el inventario de la AMI de AWS para una plantilla de destino mediante los siguientes criterios de búsqueda:

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

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

Compatibilidad con la eliminación de dispositivos de Azure AD. Con esta función, los dispositivos obsoletos de Azure AD pueden eliminarse sistemáticamente asignando el rol de administrador de dispositivos de la nube a la entidad principal de servicio y modificando la propiedad personalizada de la conexión de host. Si no elimina los dispositivos obsoletos de Azure AD, la VM no persistente correspondiente permanecerá en el estado de inicialización hasta que la elimine manualmente del portal de Azure AD. Para obtener más información, consulte Crear catálogos unidos a Azure Active Directory.

Compatibilidad con el perfil de máquina en el entorno de AWS. Al crear un catálogo para aprovisionar máquinas mediante Machine Creation Services (MCS) en AWS, ahora puede usar un perfil de máquina para capturar las propiedades del hardware de una instancia de EC2 (VM) o versión de plantilla de inicio y aplicarlas a las máquinas aprovisionadas. Las propiedades que se capturan pueden incluir, por ejemplo, las propiedades del volumen de EBS, el tipo de instancia, la optimización de

EBS y otras configuraciones de AWS compatibles. Al modificar el catálogo, se puede cambiar el perfil de máquina de las máquinas aprovisionadas proporcionando una máquina virtual o una plantilla de inicio diferentes. Para obtener más información, consulte Crear un catálogo mediante un perfil de máquina.

El límite de exportación de los resultados de búsqueda se amplió de 10 000 a 30 000. Hemos ampliado el límite de exportación de los resultados de búsqueda. Anteriormente restringido a 10 000 elementos, ahora puede exportar hasta 30 000 elementos a un archivo CSV. Para obtener más información, consulte Exportar resultados de búsqueda en un archivo CSV.

Opción de actualización de imagen. Ahora, al seleccionar imágenes maestras para catálogos de máquinas, puede obtener rápidamente la lista de imágenes maestras más actualizada mediante la opción **Actualizar** de la parte superior derecha. Tenga en cuenta que la opción **Actualizar** no está disponible para los catálogos de AWS. Además, hay una opción de **actualización** disponible para los perfiles de máquinas y los grupos de hosts en los catálogos de Azure.

Junio de 2023

Funciones nuevas y mejoradas

Función para obtener propiedades personalizadas a partir de la entrada del perfil de máquina en GCP. Antes, en entornos de GCP, al crear un catálogo de máquinas de MCS mediante una entrada de perfil de máquina, tenía que especificar de forma explícita las propiedades personalizadas. Esto suponía un esfuerzo adicional. Ahora, con esta función, puede derivar estas propiedades personalizadas sin definirlas explícitamente:

- `ServiceOffering`
- `CryptoKeyId`
- `CatalogZones`
- `Storage`

Al ejecutar los comandos `New-ProvScheme` y `Set-ProvScheme` sin especificar explícitamente las propiedades personalizadas, los valores de las propiedades se derivan de la entrada de perfil de máquina.

Por ejemplo, `New-ProvScheme -MachineProfile` escribe el tipo de máquina del perfil de máquina en la propiedad `ServiceOffering` del esquema de aprovisionamiento, a menos que especifique `ServiceOffering` en el comando `New-ProvScheme`. Si ejecuta `Set-ProvVMScheme` dos veces, se aplicará el comando más reciente.

Quite etiquetas en entornos de AWS. Antes, los comandos `Remove-ProvVM` y `Remove-ProvScheme` de PowerShell con el parámetro `ForgetVM` quitaban las máquinas virtuales y los catálogos de máquinas de la base de datos de Citrix. Sin embargo, los comandos no quitaban las

etiquetas. Había que administrar de forma individual las máquinas virtuales y los catálogos de máquinas que no se quitaban por completo de todos los recursos. Con esta función, puede utilizar:

- `Remove-ProvVM` con el parámetro `ForgetVM` para quitar máquinas virtuales y etiquetas de una sola máquina virtual o una lista de máquinas virtuales de un catálogo de máquinas.
- `Remove-ProvScheme` con el parámetro `ForgetVM` para quitar un catálogo de máquinas de la base de datos de Citrix y recursos de un catálogo de máquinas.

Esta implementación ayuda a:

- Identificar recursos filtrados
- Quitar el coste adicional de mantener recursos que no son necesarios

Esta función solo se puede aplicar a máquinas virtuales persistentes. Para obtener más información, consulte Quitar etiquetas.

Posibilidad de obtener el historial de errores y advertencias asociados a un catálogo de máquinas de MCS. Antes, solo se mostraban las advertencias y los errores más recientes asociados a un catálogo de máquinas. Ahora, con esta función, puede obtener una lista histórica de las advertencias y errores de un catálogo de máquinas de MCS. Esta lista le ayuda a comprender los problemas que pueda haber en su catálogo de máquinas de MCS y a corregirlos.

Para obtener más información, consulte Obtener advertencias y errores asociados a un catálogo.

Mayor capacidad con rendimiento mejorado para Citrix en Google Cloud. Ahora, Citrix admite catálogos que contengan hasta 3000 VDA en un solo proyecto de Google Cloud. Esta actualización aporta mejoras de rendimiento tanto en las operaciones de aprovisionamiento como en las de administración de energía.

Posibilidad de restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS en Google Cloud y el entorno de AWS. Ya puede usar el comando `Reset-ProvVMDisk` de PowerShell para restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. La función automatiza el proceso de restablecimiento de disco del sistema operativo. Por ejemplo, ayuda a restablecer la máquina virtual a su estado inicial de un catálogo de escritorio de desarrollo persistente creado con MCS. Actualmente, esta función se aplica a los entornos de virtualización de AWS, Azure, Citrix Hypervisor, Google Cloud y VMware. Para obtener más información sobre el uso del comando de PowerShell para restablecer el disco del sistema operativo, consulte Restablecer disco de SO.

Función para cambiar propiedades personalizadas relacionadas con el disco de catálogos y máquinas virtuales existentes en GCP. Antes, en entornos de GCP, solo podía agregar las propiedades personalizadas al crear el catálogo de máquinas de MCS. Ahora, con esta función, puede cambiar estas propiedades personalizadas relacionadas con el disco de un catálogo existente y de las máquinas virtuales existentes del catálogo.

- `PersistOSDisk`
- `PersistWBC`
- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

Esta implementación le ayuda a seleccionar diferentes tipos de almacenamiento para diferentes discos incluso después de crear un catálogo y, por lo tanto, a equilibrar los precios asociados a los diferentes tipos de almacenamiento. Para obtener más información, consulte Cambiar las propiedades personalizadas relacionadas con el disco de un catálogo existente.

Se amplió la función de tiempo de espera de sesión dinámico a la versión 2203 LTSR CU3 de VDA y versiones posteriores. Ahora, para los grupos de entrega con SO de sesión única, esta función se aplica a los VDA con la versión 2206 CR o una posterior, o con la 2203 LTSR CU3 o una posterior. Para obtener más información, consulte Tiempos de espera de sesión dinámicos.

Experiencia mejorada en la creación de conexiones de host en Configuración completa. Ahora, tras seleccionar una ubicación de recursos, la lista desplegable **Tipo de conexión** muestra todos los hipervisores y servicios de la nube compatibles con Citrix, y su disponibilidad depende de:

- Para una ubicación de recursos sin Cloud Connectors accesibles, solo están disponibles los hipervisores y los servicios de la nube que permiten implementaciones sin conectores.
- Para una ubicación de recursos con Cloud Connectors accesibles, solo están disponibles los hipervisores y los servicios de la nube que tengan sus plug-ins instalados correctamente en esos conectores.

Para obtener más información, consulte Crear y administrar conexiones.

Selección de componentes adicionales en la actualización de versiones de VDA. Ahora puede seleccionar qué componentes adicionales quiere actualizar o instalar al actualizar la versión de un VDA. Para obtener más información, consulte Configurar la actualización automática de versiones de los VDA.

> **Importante:**
>
> Para utilizar la función de componentes adicionales, asegúrese de que su agente de actualización de versiones de VDA sea la versión 7.34 o una posterior, que se incluye a partir de la versión 2206 del instalador de VDA.

Ahora, Configuración completa preconfigura ciertos parámetros para máquinas de Azure en función de los perfiles de máquina. Ahora, al aprovisionar máquinas virtuales de Azure, Configuración completa preconfigura estos parámetros en función del perfil de máquina seleccionado:

- Grupo de hosts
- Conjunto de cifrado de discos

- Zona de disponibilidad
- Tipo de licencia

Compatibilidad con la hibernación de instancias de AWS. Ahora puede iniciar instancias de AWS, configurarlas como quiera y ponerlas en hibernación. El proceso de hibernación almacena el estado en memoria de la instancia, junto con sus direcciones IP privadas y elásticas, lo que le permite continuar exactamente donde lo dejó. Para obtener más información sobre la creación de máquinas virtuales que permitan la hibernación, consulte Hibernación de instancias.

Función para optimizar la limitación de AWS. Ahora puede encender y apagar una gran cantidad de máquinas en un catálogo de AWS sin problemas de limitación. Los problemas de limitación se producen cuando la cantidad de solicitudes enviadas a AWS supera la cantidad de solicitudes que el servidor puede gestionar. Esta función aumenta la eficiencia al reducir la cantidad de llamadas de AWS para encender y apagar máquinas de forma masiva. También reduce significativamente el tiempo necesario para encender y apagar las máquinas en catálogos persistentes.

Entorno seguro para el tráfico administrado de Azure. Antes, confiaba en la red pública de Internet para permitir que sus dispositivos de punto final de Azure interactuaran con recursos de su entorno. Como resultado, se planteaban problemas de seguridad porque se accedía a la red pública de Internet. Con esta función, MCS permite que el tráfico de red se redirija a través de los Citrix Cloud Connectors de su entorno. Esto hace que el entorno sea seguro, ya que, ahora, todo el tráfico administrado de Azure se origina en su propio entorno. Para ello, agregue `ProxyHypervisorTrafficThroughConnector` en `CustomProperties`. Para obtener más información, consulte Crear un entorno seguro para el tráfico administrado de Azure.

Después de configurar las propiedades personalizadas, puede configurar las directivas de Azure para tener acceso a discos privados con los discos administrados de Azure.

Compatibilidad con el aprovisionamiento de máquinas virtuales de catálogo con el agente de Azure Monitor. El agente de Azure Monitor (AMA) recopila datos de supervisión y los entrega a Azure Monitor. Con esta función, puede aprovisionar máquinas virtuales del catálogo de máquinas de MCS (persistentes y no persistentes) con el AMA instalado como una extensión. Esta implementación permite la supervisión al identificar de forma única las máquinas virtuales en los datos de supervisión. Para obtener más información sobre el AMA, consulte Información general del agente de Azure Monitor.

Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Para obtener más información sobre el aprovisionamiento de máquinas virtuales del catálogo de máquinas con el AMA habilitado, consulte Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado.

Habilite la programación de reinicio de un catálogo de MCS. Antes, para programar actualizaciones de imágenes, tenía que esperar el siguiente reinicio o activar un reinicio inmediato de todas las máquinas virtuales. Ahora, con esta función, puede crear una programación de

reinicio único para que un catálogo se active en la fecha y la hora deseadas a fin de facilitar las actualizaciones de imágenes de MCS. Para crear una programación de reinicio, utilice el comando `BrokerCatalogRebootSchedule`. Para obtener más información, consulte Cambiar la imagen maestra.

Administre los secretos caducados de los clientes en Distribución rápida de Azure. En Distribución rápida de Azure, ahora puede mantenerse informado con alertas cuando caduquen los secretos de los clientes y actualizarlos fácilmente para garantizar un acceso continuo a los recursos de Azure. Para obtener más información, consulte Actualizar los secretos de cliente caducados.

Mayo de 2023

Funciones nuevas y mejoradas

Mejoras en las búsquedas. Esta función mejora el aspecto visual y las interacciones con los filtros, lo que se traduce en una mejor experiencia en las búsquedas. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Nueva directiva de exclusiones de usuarios que permite definir rutas de directorio que no se redirigen a la capa de usuarios. Las exclusiones de usuarios se aplican a la capa de personalización de usuarios (UPL), pero no al host de la sesión. Ahora, logoff.txt contiene todas las exclusiones de usuarios activas. Para obtener más información, consulte Capa de personalización de usuarios.

Función para actualizar la versión del hardware de las nuevas máquinas virtuales agregadas a un catálogo de máquinas de MCS. Ahora, en los entornos de VMware, puede actualizar la versión de hardware de las máquinas virtuales recién agregadas a un catálogo de máquinas de MCS existente mediante un origen de perfil de máquina. No es necesario crear otro catálogo de máquinas para actualizar la versión de hardware de las máquinas virtuales agregadas al catálogo. Debe utilizar el flujo de trabajo del perfil de máquina para utilizar esta función.

Función para filtrar instancias de máquinas virtuales de AWS. Antes, al utilizar una instancia de máquina virtual de AWS como entrada de perfil de máquina para crear un catálogo de máquinas de MCS, a veces, el catálogo no se creaba o no funcionaba correctamente porque la entrada del perfil de máquina no era válida. Ahora, con esta función, puede enumerar las instancias de máquinas virtuales de AWS que se pueden usar como máquinas virtuales de perfil de máquina válidas. Para ello, utilice el comando `Get-HypInventoryItem`. Para obtener más información, consulte Filtrar instancias de VM.

Función para convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina en un entorno de Azure. Ahora, en el entorno de Azure, puede utilizar una máquina virtual o una especificación de plantilla como entrada de perfil de máquina para convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina. Las máquinas virtuales existentes y las máquinas

virtuales nuevas agregadas al catálogo toman los valores de las propiedades del perfil de la máquina a menos que se sobrescriban con propiedades personalizadas explícitas. Para obtener más información, consulte Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina.

Función para el cifrado doble en discos administrados en un entorno de Azure. Ahora, en el entorno de Azure, puede crear un catálogo de máquinas de MCS con doble cifrado. El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado. Para obtener más información, consulte Cifrado doble en discos administrados.

Función para perfiles de máquina en VMware. Ahora, en entornos de VMware, puede crear un catálogo de máquinas de MCS mediante un perfil de máquina. El origen de la entrada del perfil de la máquina es una plantilla de VMware. El perfil de la máquina captura las propiedades del hardware de una plantilla de VMware y las aplica a las máquinas virtuales recién aprovisionadas del catálogo. Para obtener más información, consulte Crear un catálogo de máquinas mediante un perfil de máquina.

Posibilidad de restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS en Azure y Citrix Hypervisor. Ya puede usar el comando `Reset-ProvVMDisk` de PowerShell para restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. La función automatiza el proceso de restablecimiento de disco del sistema operativo. Por ejemplo, ayuda a restablecer la máquina virtual a su estado inicial de un catálogo de escritorio de desarrollo persistente creado con MCS. Actualmente, esta función se aplica a los entornos de virtualización de Azure, Citrix Hypervisor y VMware. Para obtener más información sobre el uso del comando de PowerShell para restablecer el disco del sistema operativo, consulte Restablecer disco de SO.

Experiencia mejorada en la creación de conexiones de host. Ahora puede obtener esta información al crear una conexión de host:

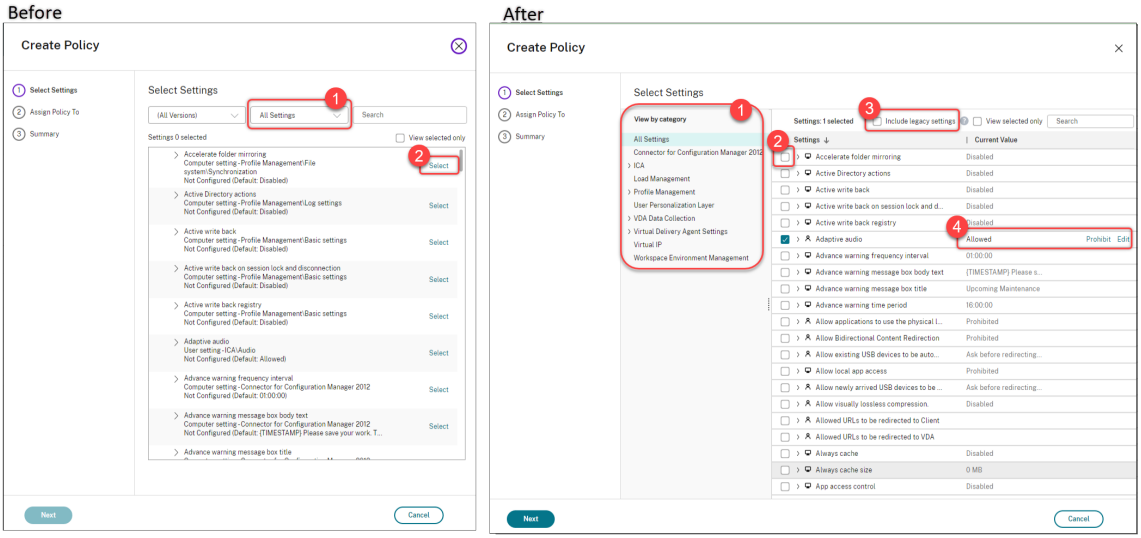
- Lista de todos los plug-ins de hipervisor compatibles con Citrix, incluidos los plug-ins de terceros
- Disponibilidad del plug-in de hipervisor. Si el estado de disponibilidad es false, es posible que sea porque Cloud Connector no esté instalado

Esta función le ayuda a configurar correctamente una ubicación de recursos y, por lo tanto, a crear una conexión de host. Para obtener más información, consulte el Paso 1. Conexión.

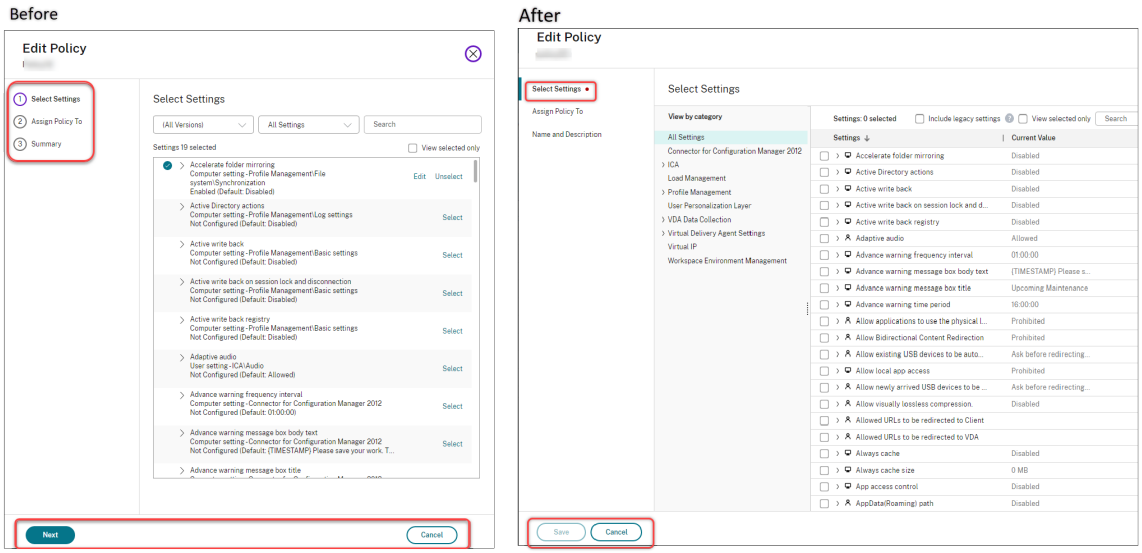
Mejoras en la experiencia de usuario para el nodo Directivas. Para mejorar la experiencia de usuario y hacer que la administración de directivas sea más eficiente, hemos implementado estas mejoras en el nodo **Configuración completa > Directivas**:

- Nuevo diseño de interfaz de usuario para las acciones **Crear directiva** y **Crear plantilla**:

- Vista de carpetas ampliable para la configuración de directivas. En la página **Seleccionar configuraciones**, todas las configuraciones se muestran por categoría en una vista de árbol ampliable, lo que facilita la búsqueda de las configuraciones.
- Para seleccionar una configuración, basta con hacer clic en una casilla en lugar de utilizar el botón **Seleccionar**.
- Las configuraciones antiguas se ocultan de forma predeterminada para que solo se muestren las configuraciones más relevantes. Si se necesita una configuración antigua, seleccione **Incluir configuraciones antiguas**.
- Se agregó un botón de acción junto a un parámetro booleano, lo que permite cambiar su valor directamente en la lista de configuraciones.



- Nuevo diseño de la interfaz de usuario de la acción **Modificar directiva**:
  - El menú de navegación se actualizó a una lista sin orden. Ahora, cada elemento de la lista incluye un botón **Guardar** en su página. Con este nuevo diseño, puede guardar los cambios realizados en un elemento sin tener que navegar por todos los elementos del menú de navegación. Estas mejoras hacen que la administración de directivas sea más eficiente y simplificada.
  - Aparecen puntos rojos junto a los elementos de navegación para indicar errores de configuración.



- Arrastre los elementos para priorizar de nuevo las directivas. Ahora, en la lista de prioridades, para cambiar la prioridad de una directiva, puede arrastrarla a la posición que quiera.

Nueva opción para desactivar el cierre de sesión forzado de los usuarios en Autoscale. Ya está disponible una nueva opción, **No notificar ni forzar el cierre de sesión del usuario**, en la página **Administrar Autoscale > Notificación de cierre de sesión del usuario**. Con la opción seleccionada, Autoscale no forzará a los usuarios a cerrar sesión en las máquinas en estado de purga ni les notificará que cierren sesión e inicien sesión en otra máquina. Para obtener más información, consulte Notificaciones de cierre de sesión del usuario.

Posibilidad de reiniciar los PC en la nube de Windows 365. Ahora puede usar Citrix DaaS para reiniciar los PC en la nube con Windows 365.

Más detalles de las sesiones. Ahora, al ver una sesión en **Configuración completa > Buscar > Sesiones**, la vista de sesión (en el panel inferior) incluye más detalles de la sesión para ayudarle a solucionar e identificar posibles problemas en el cliente:

- **Hora de reconexión.** La hora a la que una sesión se conectó de nuevo después de haberse desconectado.
- **Plataforma cliente.** La plataforma utilizada para iniciar la sesión.
- **Versión del cliente.** La versión de la plataforma cliente utilizada para iniciar la sesión.
- **IP del host remoto.** La dirección IP del host remoto donde se aloja Citrix Workspace.

Función para cambiar el nombre de los grupos de seguridad de Azure AD para máquinas virtuales. Ahora, para las máquinas virtuales agregadas a un grupo de seguridad de Azure AD a través de Citrix DaaS, puede cambiar el nombre del grupo de seguridad mediante **Configuración completa > Modificar catálogo de máquinas**. El cambio de nombre se produce después de guardar el cambio.

Selección de dominio predeterminada para cuentas de máquinas. Al crear un catálogo, el dominio

en el que reside el recurso (conexión) se selecciona de forma predeterminada para las cuentas de máquina.

Posibilidad de mostrar los grupos de seguridad asignados a Azure AD para que las máquinas virtuales se unan. En la Configuración completa, al crear máquinas virtuales unidas a Azure Active Directory, ahora está disponible la opción **Unirse a un grupo de seguridad asignado como miembro**, que le permite agregar el grupo de seguridad de Azure AD en el que residen las máquinas virtuales a un grupo de seguridad asignado. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Opción para cambiar las redes de las conexiones. En Configuración completa, ahora puede cambiar las redes de una conexión. No puede disociar redes de una conexión si están en uso. Para obtener más información, consulte Modificar red.

Posibilidad de quitar etiquetas en entornos de Azure. Antes, los comandos `Remove-ProvVM` y `Remove-ProvScheme` de PowerShell con el parámetro `ForgetVM` quitaban las máquinas virtuales y los catálogos de máquinas de la base de datos de Citrix. Sin embargo, esos comandos no quitaban las etiquetas de los recursos. Había que administrar de forma individual las máquinas virtuales y los catálogos de máquinas que no se eliminaban por completo de todos los recursos. Con esta función, puede utilizar:

- `Remove-ProvVM` con el parámetro `ForgetVM` para quitar máquinas virtuales y etiquetas creadas sobre los recursos de una sola máquina virtual o una lista de máquinas virtuales de un catálogo de máquinas.
- `Remove-ProvScheme` con el parámetro `ForgetVM` para quitar un catálogo de máquinas de la base de datos de Citrix y etiquetas creadas sobre los recursos de todo un catálogo de máquinas.

Esta implementación ayuda a identificar los recursos huérfanos que MCS ha creado, pero que ya no utiliza.

Esta función solo se puede aplicar a máquinas virtuales persistentes. Para obtener más información, consulte Quitar etiquetas.

Alerta de máquinas fallidas. La funcionalidad de notificaciones y alertas proactivas de Director se ha mejorado para incluir una nueva alerta, Máquinas fallidas (en %) basada en el porcentaje de máquinas que fallan en un grupo de entrega. La nueva condición de alerta permite configurar los umbrales de alerta como un porcentaje de las máquinas que han fallado en un grupo de entrega. Para obtener más información, consulte la sección Máquinas fallidas del artículo Alertas.

Abril de 2023

Funciones nuevas y mejoradas

Publicar con plataformas de la nube específicas mediante Citrix Provisioning en Image Portability Service. Ya están disponibles flujos de trabajo específicos para usar Image Portability Service para publicar en AWS, Azure y Google Cloud. Además, se han actualizado los permisos necesarios para Azure y las redes. Para obtener más información detallada, consulte Migrar cargas de trabajo a la nube pública.

Función para identificar por qué una máquina está en modo de mantenimiento. Antes, PowerShell era la única opción para identificar por qué una máquina estaba en modo de mantenimiento. Ahora puede hacerlo en Configuración completa:

1. Utilice Buscar para localizar la máquina.
2. Marque **Motivo del mantenimiento** en la ficha **Detalles** del panel inferior. O coloque el cursor sobre la columna **Modo de mantenimiento**. Puede aparecer esta información:

- Por el administrador: El administrador la puso en modo de mantenimiento.
- Máximo de registros fallidos: Puesta en modo de mantenimiento cuando la máquina supera el máximo de intentos de registro permitido.

Además, ahora está disponible un filtro llamado **Motivo del mantenimiento**. Puede usarlo para identificar las máquinas de destino.

Esta función es útil, al permitir que los administradores solucionen problemas con máquinas en modo de mantenimiento.

Use variables para notificar a los usuarios el tiempo restante antes de que se les cierre la sesión. Ahora, al forzar el cierre de sesión de los usuarios, puede usar `%s%` o `%m%` como variables para indicar la hora especificada en el mensaje de notificación. Para expresar el tiempo en segundos, utilice `%s%`. Para expresar el tiempo en minutos, utilice `%m%`. Para obtener más información, consulte Notificaciones de cierre de sesión del usuario.

Posibilidad de personalizar el comportamiento de encendido en caso de error en el cambio del tipo de almacenamiento. Al encenderse, es posible que el tipo de almacenamiento de un disco administrado no cambie al tipo deseado debido a un error de Azure. Anteriormente, en estos casos, la máquina virtual permanecía apagada y se le enviaba un mensaje de error. Con esta función, puede optar por encender la máquina virtual incluso cuando no se pueda restaurar el almacenamiento al tipo configurado o mantener la máquina virtual apagada. Para obtener más información, consulte Personalizar el comportamiento de encendido en caso de error en el cambio del tipo de almacenamiento.

Compatibilidad con la activación MAK. Ahora puede aprovisionar catálogos de máquinas persistentes y no persistentes con máquinas virtuales activadas mediante la clave de activación múltiple

(MAK). Con esta función, ahora MCS también puede comunicarse con las máquinas virtuales aprovisionadas. Esta implementación ayuda a activar el sistema Windows sin reducir el recuento de activaciones. Para obtener más información, consulte Activación de licencias por volumen.

Función para el cifrado de discos de Azure en el host. Con esta función, ahora puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Puede utilizar una máquina virtual o una especificación de plantilla como entrada para un perfil de máquina. Para obtener más información, consulte Cifrado de discos de Azure en el host.

En este tipo de cifrado, el servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo. Para obtener más información, consulte Encryption at host - End-to-end encryption for your VM data.

Compatibilidad con la plantilla de instancias de GCP como entrada para el perfil de máquina. Con esta función, ahora puede seleccionar una plantilla de instancias de GCP como entrada para el perfil de máquina. Las plantillas de instancias son recursos ligeros de GCP y, por lo tanto, muy rentables. Para hacer esto, utilice los comandos de PowerShell. Para obtener más información sobre el uso de los comandos de PowerShell para crear y actualizar catálogos de máquinas mediante la selección de una plantilla de instancias de GCP, consulte Crear un catálogo de máquinas con el perfil de máquina como plantilla de instancias.

Opción para modificar el nombre del grupo de seguridad dinámico de Azure AD. Puede modificar o eliminar el nombre de un grupo de seguridad dinámico de Azure AD desde Azure Portal. Esto puede hacer que el nombre del grupo de seguridad dinámico de Azure AD no esté sincronizado con el grupo de seguridad dinámico asociado a un catálogo de máquinas. Con esta función, ahora puede modificar el nombre del grupo de seguridad dinámico de Azure AD asociado a un catálogo de máquinas.

Esta modificación hace que la información del grupo de seguridad dinámico de Azure AD almacenada en el objeto del grupo de identidades de Azure AD sea coherente con la información almacenada en Azure Portal. Para obtener más información, consulte Modificar el nombre del grupo de seguridad dinámico de Azure AD.

Se han agregado permisos necesarios en GCP. Ahora se han agregado los permisos necesarios para hacer lo siguiente:

- Crear una conexión de host
- Administrar la energía de las máquinas virtuales
- Aprovisionar catálogos

Para obtener más información, consulte Acerca de los permisos de GCP.

Gestión de credenciales. Para mejorar la seguridad, de forma predeterminada, las credenciales de los usuarios que no se encuentran en el mismo dominio que sus VDA no se reenvían a la nube. Los

intentos de inicio de sesión fallan cuando se cumplen todas las condiciones siguientes:

- El usuario se encuentra en un dominio diferente del VDA
- No existe confianza entre los dominios
- StoreFront está instalado en el mismo dominio que el VDA

Anteriormente, en estas condiciones, no se podía autenticar al usuario en StoreFront. Por este motivo, Cloud Connector reenviaba las credenciales de usuario a la nube para dirigir la solicitud de autenticación al destino correcto para ese usuario. Este comportamiento se puede configurar aún si es necesario. Para obtener más información, consulte el parámetro `CredentialForwardingToCloudAllowed` de Set-Brokersite en el SDK de PowerShell de DaaS.

Marzo de 2023

Funciones nuevas y mejoradas

Posibilidad de configurar el rol y el ámbito de los administradores. Citrix Cloud ahora admite un mayor grado de flexibilidad y personalización al configurar el acceso para un administrador. Anteriormente, solo podían seleccionarse pares predefinidos de roles y ámbitos. Con esta mejora, puede seleccionar un rol y asociarlo después al ámbito que desee.

Para obtener más información, consulte Configurar acceso personalizado para un administrador.

Función para crear un grupo de seguridad dinámico bajo un grupo de seguridad asignado existente. Anteriormente, podía crear grupos de seguridad dinámicos de Azure AD para un catálogo de máquinas. Con esta función, también puede agregar un grupo de seguridad dinámico de Azure AD a un grupo de seguridad asignado de Azure AD existente. Puede realizar lo siguiente:

- Obtener información del grupo de seguridad.
- Obtener todos los grupos de seguridad asignados de Azure AD que se sincronizan desde el servidor de AD local o los grupos de seguridad asignados a los que se pueden asignar roles de Azure AD.
- Obtener todos los grupos de seguridad dinámicos de Azure AD.
- Agregar un grupo de seguridad dinámico de Azure AD como miembro del grupo asignado de Azure AD.
- Eliminar la pertenencia entre el grupo de seguridad dinámico de Azure AD y el grupo de seguridad asignado de Azure AD al eliminar el grupo de seguridad dinámico de Azure AD junto con el catálogo de máquinas.

Para obtener más información, consulte Crear un grupo de seguridad dinámico de Azure AD bajo un grupo de seguridad asignado de Azure AD existente.

Compatibilidad con grupos de seguridad dinámicos de Azure AD para las máquinas virtuales unidas a Azure AD. Citrix ahora admite grupos de seguridad dinámicos para un catálogo al crear un catálogo de máquinas de MCS. Las reglas de los grupos de seguridad dinámicos colocan las máquinas virtuales del catálogo en un grupo de seguridad dinámico según el esquema de nomenclatura del catálogo de máquinas. Esto resulta útil cuando quiere administrar las máquinas virtuales con Azure Active Directory (Azure AD). También es útil cuando quiere aplicar directivas de acceso condicional o distribuir aplicaciones desde Intune filtrando las máquinas virtuales con un grupo de seguridad dinámico de Azure AD. Al eliminar un catálogo, también se elimina el grupo de seguridad dinámico. Para obtener más información, consulte Grupo de seguridad dinámico de Azure Active Directory.

Para obtener más información sobre los requisitos de licencia para usar grupos de seguridad dinámicos, consulte el documento Create or update a dynamic group in Azure Active Directory de Microsoft.

Opción para agregar máquinas virtuales a los grupos de seguridad de Azure AD a través de Configuración completa. Al crear máquinas virtuales unidas a Azure AD, ahora está disponible la opción **Grupo de seguridad de Azure AD**. La opción permite agregar las máquinas virtuales a un grupo de seguridad de Azure AD según su esquema de nomenclatura. Para obtener más información, consulte Crear un catálogo de Microsoft Azure.

Opción para cambiar el tipo de almacenamiento de una máquina virtual a un nivel inferior al apagar en entornos de Azure. En los entornos de Azure, ahora puede ahorrar costes de almacenamiento si cambia el tipo de almacenamiento de las máquinas virtuales existentes a un nivel inferior cuando estas están apagadas. Para ello, utilice la propiedad personalizada StorageTypeAtShutdown. Para obtener más información, consulte Cambiar el tipo de almacenamiento de las máquinas virtuales existentes a un nivel inferior al apagarlas.

Función para permitir los identificadores de seguridad al crear máquinas virtuales. Anteriormente, al crear nuevas máquinas virtuales con la configuración especificada en un esquema de aprovisionamiento, no se podía agregar un identificador de seguridad (`ADAccountSid`) al comando `NewProvVM`. Con esta función, ahora puede agregar el parámetro `ADAccountSid` para identificar de forma unívoca las máquinas al crear máquinas virtuales. Para obtener más información, consulte Agregar SID al crear máquinas virtuales.

Posibilidad de obtener advertencias asociadas a los catálogos de MCS. Anteriormente, no recibía ninguna información que indicara que hubiera problemas con un catálogo de máquinas. Con esta función, ahora puede recibir advertencias para entender los problemas relativos a sus catálogos de MCS y corregirlos.

Las advertencias, a diferencia de los errores, no hacen que falle una tarea de aprovisionamiento iniciada.

Para recibir advertencias, utilice los comandos de PowerShell. Para obtener más información, consulte Recuperar las advertencias asociadas a un catálogo.

Arrendatarios compartidos para conexiones. Ya puede agregar arrendatarios y suscripciones que compartan Azure Compute Gallery con la suscripción de la conexión. Como resultado, al crear o actualizar catálogos, puede seleccionar imágenes compartidas de dichos arrendatarios y suscripciones. Para obtener más información, consulte Modificar los parámetros de conexión.

Se retiró la compatibilidad para cambiar el tipo de sistema operativo de los catálogos de Azure. Al cambiar las imágenes del catálogo, solo se muestran las imágenes con el mismo tipo de sistema operativo que la imagen que se está usando. Con esta mejora, Citrix DaaS ya no permite cambiar el tipo de sistema operativo de los catálogos de Azure, por ejemplo, de Windows a Linux y viceversa, tras la creación del catálogo.

Febrero de 2023

Funciones nuevas y mejoradas

Función para compartir imágenes entre diferentes arrendatarios de Azure. Antes, en entornos de Azure, solo podía compartir imágenes con suscripciones compartidas mediante Azure Compute Gallery. Ahora, con esta función, puede seleccionar una imagen de Azure Compute Gallery que pertenezca a otra suscripción compartida en un arrendatario diferente para crear y actualizar un catálogo de MCS. Para obtener más información, consulte Compartir imágenes entre arrendatarios de Azure.

Modelado de directivas. La función de modelado de directivas ahora está disponible para el público en general. Puede simular directivas con fines de planificación y prueba. Para obtener más información, consulte Usar el asistente de modelado de directivas.

Posibilidad de activar o desactivar las funciones de previsualización. En Configuración completa > Inicio, como administrador de Citrix Cloud con acceso total, puede activar o desactivar las funciones de Tech Preview sin ponerse en contacto con Citrix. Para obtener más información, consulte la página de inicio de la interfaz de Configuración completa.

Buscar diagnósticos de sesión con el nombre de usuario. Esta función permite usar el diagnóstico de inicio de sesión a partir del nombre de usuario si no tiene el ID de transacción. Resulta especialmente útil para que los administradores del servicio de asistencia técnica puedan clasificar una sesión fallida si el usuario final no ha capturado el ID de la transacción.
Puede buscar por un nombre de usuario y seleccionar una sesión para clasificarla entre una lista de sesiones fallidas que el usuario haya intentado iniciar en las últimas 48 horas. La página Diagnóstico de inicio de sesión muestra los detalles de la sesión fallida. Muestra el componente exacto y la etapa en la que se produjo el error. Para obtener más información, consulte el artículo Diagnóstico de inicio de sesión.

Implementar aplicaciones web y SaaS seguras con Secure Private Access. En la ficha **Configuración completa > Aplicaciones > Aplicaciones**, ahora está disponible una nueva opción, **Agregar**

aplicaciones web/SaaS, en la barra de acciones. La opción le permite implementar aplicaciones web y SaaS seguras con Secure Private Access. Citrix Secure Private Access proporciona a los usuarios remotos una manera fácil y flexible de acceder a las aplicaciones web, SaaS y cliente-servidor con un enfoque de confianza cero. Además, habilita el inicio de sesión único (SSO) en aplicaciones web y SaaS, junto con controles de seguridad detallados, como marcas de agua y controles de copiar/pegar, entre otras funciones de seguridad. Con Citrix Secure Private Access, puede combinar todas sus aplicaciones virtualizadas y no virtualizadas en un solo lugar y mejorar la experiencia de los usuarios. Consulte Citrix Secure Private Access.

Filtrar el contenido del registro durante un período de tiempo específico. Ahora hay disponible una nueva opción, **Personalizado**, en la lista de duración de **Configuración completa > Registros > Eventos**. Sirve para especificar un período de eventos para filtrar la búsqueda. Para obtener más información, consulte Registro de configuraciones.

Actualizaciones de Autoscale. Hemos actualizado la opción **Controle cuándo Autoscale comienza a encender máquinas etiquetadas** para facilitar su comprensión. La opción controla cuándo Autoscale comienza a encender las máquinas etiquetadas en función del porcentaje de la capacidad restante de las máquinas sin etiquetar. Cuando el porcentaje cae por debajo del umbral (el valor predeterminado es 10%), Autoscale comienza a encender las máquinas etiquetadas. Cuando el porcentaje supera el umbral, Autoscale pasa al modo de apagado. Para obtener más información, consulte Autoscale de máquinas etiquetadas (ampliación en la nube).

Directivas de App Protection. Ahora puede habilitar App Protection al crear o modificar un grupo de entrega. La función ofrece funciones contra el registro de tecleo y la captura de pantalla en las sesiones de los clientes. Para obtener más información, consulte Crear grupos de entrega y Administrar grupos de entrega.

Utilización de GPU en tiempo real disponible para las GPU de AMD. Ya puede ver la utilización de las GPU de AMD Radeon Instinct MI25 y las CPU de AMD EPYC 7V12 (Rome) en Supervisar. Supervisar ya es compatible con las GPU de NVIDIA Tesla M60. La utilización de la GPU muestra gráficos con el porcentaje de utilización en tiempo real de la GPU, la memoria de la GPU y la memoria del codificador y del decodificador para solucionar problemas relacionados con la GPU en VDA de SO multisesión o de sesión única. Los gráficos de Utilización de GPU de AMD solo están disponibles para los VDA que ejecutan Windows de 64 bits y Citrix Virtual Apps and Desktops 7 2212 o versiones posteriores. Para obtener más información, consulte Utilización de la GPU.

Función para programar actualizaciones de configuración en Azure. Ahora, en entornos de Azure, puede programar una franja horaria para las actualizaciones de configuración de las máquinas aprovisionadas por MCS existentes mediante el comando de PowerShell `Schedule-ProvVMUpdate`. Cualquier encendido o reinicio durante el intervalo de tiempo programado aplica una actualización programada del esquema de aprovisionamiento a una máquina. También puede cancelar la actualización de la configuración antes de la hora programada mediante `Cancel-ProvVMUpdate`.

Puede programar y cancelar la actualización de la configuración de:

- Una o varias máquinas virtuales
- Todo un catálogo

Para obtener más información, consulte Programar actualizaciones de configuración.

Función para usar imágenes preparadas por Citrix directamente desde Google Cloud Marketplace. Ahora puede buscar y seleccionar imágenes que ofrece Citrix en Google Cloud Marketplace para crear catálogos de MCS. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Para obtener más información, consulta Google Cloud Marketplace.

Limitar el ámbito de los grupos de hosts en la conexión de host de SCVMM. Antes, la conexión de host a SCVMM requería que el administrador tuviera configurado un único grupo de hosts de nivel superior. Esto implica que el administrador podía ver todos los grupos, clústeres o hosts de un único grupo de hosts de nivel superior. Ahora, con esta función, en implementaciones grandes en las que un solo SCVMM administra varios clústeres en diferentes centros de datos, puede limitar el ámbito de los grupos de hosts de los administradores. Para ello, puede usar el rol de administrador delegado en la consola de Microsoft System Center Virtual Machine Manager (VMM) para seleccionar los grupos de hosts a los que debe tener acceso un administrador. Para obtener más información, consulte Instalar y configurar un hipervisor.

Función de almacenamiento con redundancia de zonas en Azure. Antes, MCS solo ofrecía almacenamiento con redundancia local. Ahora, con esta función, el almacenamiento con redundancia de zonas es una opción en Azure, lo que le permite seleccionar un tipo de almacenamiento según el tipo de redundancia que quiera utilizar. El almacenamiento con redundancia de zonas replica sincrónicamente su disco administrado de Azure en varias zonas de disponibilidad, lo que le permite recuperarse de un error en una zona al usar la redundancia en otras. Para obtener más información, consulte Habilitar el almacenamiento con redundancia de zonas.

Enero de 2023

Funciones nuevas y mejoradas

Opción de pasar un disco de almacenamiento a disco duro estándar cuando las máquinas virtuales se apaguen. Ahora, hay una nueva opción, **Habilitar el ahorro de costes de almacenamiento**, disponible en la página **Parámetros de disco** al crear o actualizar catálogos de Azure. Esta opción ahorra costes de almacenamiento al revertir un disco de almacenamiento a una unidad de disco duro estándar y el disco de caché de reescritura cuando la máquina virtual se apague. La máquina virtual cambia a sus parámetros originales al reiniciarse. Para obtener más información, consulte Crear un catálogo de Microsoft Azure.

Función para configurar la itinerancia de sesiones en Configuración completa. Antes, PowerShell era la única opción para configurar la itinerancia de sesiones para aplicaciones y escritorios. Ahora

puede hacerlo en **Configuración completa**. Para obtener más información, consulte Administrar grupos de entrega.

Se cambió el nombre de algunas acciones para que se ajusten mejor a sus significados reales. Hemos cambiado el nombre de estas acciones en **Configuración completa > Catálogos de máquinas** y **Configuración completa > Grupos de entrega**. Los flujos de trabajo para realizar esas acciones permanecen sin cambios.

- **Actualizar máquinas** pasa a ser **Cambiar imagen maestra**
- **Revertir actualización de máquina** pasa a ser **Revertir imagen maestra**
- **Actualizar versión de catálogo** pasa a ser **Cambiar nivel funcional**
- **Actualizar versión de grupo de entrega** pasa a ser **Cambiar nivel funcional**
- **Deshacer actualización de versión de catálogo** pasa a ser **Deshacer cambio de nivel funcional**
- **Deshacer actualización de versión de grupo de entrega** pasa a ser **Deshacer cambio de nivel funcional**

Función para organizar grupos de aplicaciones mediante carpetas. Ahora puede crear carpetas anidadas para organizar grupos de aplicaciones y acceder a ellos fácilmente. Para obtener más información, consulte Organizar grupos de aplicaciones mediante carpetas.

Mejoras en las restricciones para los grupos de entrega. Antes, al restringir el uso de aplicaciones o escritorios para un grupo de entrega, solo podía especificar los usuarios y los grupos de usuarios que podían usarlos en un grupo de entrega. Ahora también puede agregar usuarios y grupos de usuarios que quiera bloquear. Esta mejora resulta útil al agregar un grupo de usuarios a una lista de usuarios permitidos y, al mismo tiempo, se quiere bloquear un subconjunto de usuarios de la lista de permitidos. Para obtener más información, consulte Crear grupos de entrega.

Acceso a Citrix Analytics for Performance: Detalles de la sesión desde Supervisar. La página Detalles de la sesión de Citrix Analytics for Performance ahora está integrada en Supervisar. Al hacer clic en **View Session Timeline** en la página Sesiones de Supervisar para ver la página Detalles de sesiones de Citrix Analytics for Performance en Supervisar. Esto requiere que tenga derecho a usar Citrix Analytics for Performance. Los detalles de la sesión están disponibles para las sesiones categorizadas como Excelente, Media o Mala en Citrix Analytics for Performance.

Puede ver una tendencia de la experiencia con respecto a la sesión durante los últimos tres días, junto con los factores que contribuyen a dicha experiencia. Esta información complementa los datos en tiempo real disponibles en Supervisar, que el administrador del servicio de asistencia utiliza para solucionar problemas relacionados con la experiencia de la sesión.

Para obtener más información, consulte el artículo Análisis de sitios.

Las máquinas virtuales no persistentes se eliminan de los hipervisores o servicios de la nube al eliminarlas o al eliminar sus catálogos de máquinas en Configuración completa. Ahora, la opción

de retener las máquinas virtuales en hipervisores o servicios de la nube solo está disponible para máquinas virtuales persistentes. Para obtener más información, consulte Administrar catálogos de máquinas.

Diciembre de 2022

Funciones nuevas y mejoradas

Función para crear catálogos unidos a Azure AD, unidos a Azure AD híbrido y con Microsoft Intune habilitado con máquinas virtuales maestras unidas a Azure AD. Ya puede crear catálogos unidos a Azure AD, unidos a Azure AD híbrido y con Microsoft Intune habilitado con máquinas virtuales maestras unidas a Azure AD, unidas a Azure AD híbrido y no unidas a ningún dominio. Si quiere administrar una máquina virtual maestra con Microsoft Intune, utilice la versión 2212 de VDA o una posterior y no omita la preparación de la imagen al crear o actualizar catálogos de máquinas.

Para obtener más información sobre las identidades de máquinas, consulte Unidos a Azure Active Directory, Microsoft Intune y Unidos a Azure Active Directory híbrido.

Función en MCS para eliminar objetos de VM sin acceder al hipervisor. Ahora puede eliminar objetos de VM en MCS sin tener acceso al hipervisor. Al eliminar una máquina virtual o un esquema de aprovisionamiento, MCS necesita quitar etiquetas para que los recursos ya no se rastreen ni se identifiquen. Antes, si no se podía acceder al hipervisor, se ignoraban los errores de eliminación de etiquetas. Con esta función, si no se puede acceder al hipervisor mientras se utiliza el comando `Remove-ProvVM`, no se podrán quitar las etiquetas, pero si utiliza la opción `PurgeDBOnly`, aún puede eliminar de la base de datos el objeto de recurso de VM. Para obtener más información, consulte Eliminar máquinas sin acceder al hipervisor.

Noviembre de 2022

Funciones nuevas y mejoradas

Compatibilidad con la entrega de aplicaciones en formato MSIX y de conexión de aplicaciones MSIX. En **Configuración completa > Paquetes de aplicaciones**, ahora puede cargar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX en Citrix Cloud para entregarlas a sus usuarios. Para obtener más información, consulte Paquetes de aplicaciones.

Mensaje sobre niveles funcionales y versiones de VDA no compatibles. Ahora, la interfaz de Configuración completa le avisa sobre versiones de VDA y niveles funcionales no compatibles. Para evitar posibles problemas:

- Si una máquina ejecuta una versión de VDA no compatible, se le pedirá que la actualice a una versión compatible.

- Si no se admite el nivel funcional de un catálogo o grupo de entrega, se le pedirá que lo establezca en un nivel superior.

> **Sugerencia:**
>
> Los VDA están cubiertos por los ciclos de vida CR y LTSR de Citrix Virtual Apps and Desktops.

Posibilidad de agregar anotaciones en imágenes maestras ampliada a la creación de catálogos. Ahora, al crear un catálogo de MCS en **Configuración completa**, puede agregar anotaciones en su imagen maestra. Para obtener más información, consulte Imagen maestra.

Función para exportar datos de asignación de escritorios a través de Configuración completa. Ahora, al ver las asignaciones de escritorio de un grupo de entrega con SO de sesión única, puede exportar los datos de la asignación en un archivo CSV con fines de auditoría. Para ello, seleccione dicho grupo de entrega en **Configuración completa > Grupos de entrega**, vaya a la ficha **Escritorios** y, a continuación, haga clic en **Exportar** en la esquina superior izquierda de la ficha.

Las fichas de Todas las aplicaciones y Carpetas de aplicaciones se han consolidado en una sola. En **Configuración completa > Aplicaciones**, las fichas de **Todas las aplicaciones** y **Carpetas de aplicaciones** se han consolidado en una sola ficha: **Aplicaciones**. Este cambio unifica la experiencia de usuario en la administración de vistas de carpetas en los nodos de Configuración completa.

Opción para cambiar el tipo de almacenamiento a un nivel inferior al apagar una máquina virtual en entornos de Azure. Ahora, en entornos de Azure, puede ahorrar costes de almacenamiento al cambiar el tipo de almacenamiento de un disco administrado a un nivel inferior cuando apaga una máquina virtual. Para ello, utilice la propiedad `StorageTypeAtShutdown` personalizada. El tipo de almacenamiento del disco pasa a un nivel inferior (tal y como se especifica en la propiedad personalizada `StorageTypeAtShutdown`) al apagar la máquina virtual. Tras encender la máquina virtual, el tipo de almacenamiento vuelve a ser el original (tal y como se especifica en la propiedad personalizada `StorageType` o `WBCDiskStorageType`). Para obtener más información, consulte Cambio del tipo de almacenamiento a un nivel inferior al apagar una máquina virtual.

Actualizaciones en la vista de filtros. La página Filtros de Supervisar se ha actualizado para incluir listas separadas de filtros guardados y predeterminados a fin de facilitar la visualización y acceso a los filtros. Puede seleccionar una vista entre Máquinas, Sesiones, Conexiones o Instancias de aplicaciones. A continuación, puede seleccionar un filtro de la lista de filtros guardados o filtros predeterminados para ver la lista de datos filtrados. Puede utilizar las listas desplegables para ajustar los criterios de filtrado o modificar los criterios existentes. Puede guardar el filtro en la lista de filtros guardados. Para obtener más información, consulte el artículo Filtros.

Posibilidad de restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. En los entornos de virtualización de VMware, ahora puede usar el comando `Reset-ProvVMDisk` de PowerShell para restablecer el disco del sistema

operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. La función automatiza el proceso de restablecimiento de disco del sistema operativo. Por ejemplo, ayuda a restablecer la máquina virtual a su estado inicial de un catálogo de escritorio de desarrollo persistente creado con MCS.

Para obtener más información sobre el uso del comando de PowerShell para restablecer el disco del sistema operativo, consulte Restablecer disco de SO.

Compatibilidad con la actualización de perfiles de máquinas y propiedades personalizadas adicionales de máquinas aprovisionadas por MCS en entornos de Azure. Anteriormente, en los entornos de Azure, se podía utilizar `Request-ProvVMUpdate` para actualizar la propiedad `ServiceOffering` personalizada de una máquina aprovisionada por MCS. Ahora también puede actualizar el perfil de la máquina y las siguientes propiedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

Para obtener más información, consulte Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento.

Compatibilidad con perfiles de máquina en GCP. Al crear un catálogo para aprovisionar máquinas mediante Machine Creation Services (MCS) en entornos de Google Cloud Platform (GCP), ahora puede usar un perfil de máquina para capturar las propiedades del hardware de una máquina virtual y aplicarlas a las máquinas virtuales recién aprovisionadas del catálogo. Cuando no se utiliza el parámetro `MachineProfile`, las propiedades del hardware se obtienen de la instantánea o la VM de la imagen maestra.

Los perfiles de máquina funcionan con los sistemas operativos Linux y Windows.

Para obtener información sobre cómo crear un catálogo de máquinas con un perfil de máquina, consulte Crear un catálogo de máquinas mediante un perfil de máquina.

Compatibilidad con la actualización de máquinas aprovisionadas por MCS en entornos de GCP. En entornos de GCP, `Set-ProvScheme` cambia la plantilla (esquema de aprovisionamiento) y no afecta a las máquinas existentes. Con el comando `Request-ProvVMUpdate` de PowerShell, ahora puede aplicar el esquema de aprovisionamiento actual a una máquina (o a un conjunto de máquinas). Actualmente, en Google Cloud Platform, la actualización de propiedades que admite esta función es el perfil de máquina. Para obtener más información, consulte Actualizar las máquinas aprovisionadas mediante PowerShell.

Octubre de 2022

Funciones nuevas y mejoradas

Compatibilidad con el uso de perfiles de máquinas y grupos de hosts al mismo tiempo. Ahora, al crear un catálogo con una imagen maestra de Azure Resource Manager, puede usar un perfil de máquina y un grupo de hosts al mismo tiempo. Esto resulta útil en casos en que quiera utilizar el inicio seguro para reforzar la seguridad y, al mismo tiempo, ejecutar las máquinas en hosts dedicados. Para obtener información, consulte Entornos de virtualización para Azure Resource Manager.

Función para organizar grupos de entrega mediante carpetas. Ahora puede crear un árbol de carpetas para organizar el acceso fácil a grupos de entrega. Para obtener más información, consulte Organizar grupos de entrega con carpetas.

Función para programar un reinicio único de máquinas a través de Configuración completa. Ahora hay una nueva opción, **Una vez**, disponible al crear programaciones de reinicio para grupos de entrega. Con esta opción, puede programar que las máquinas de un grupo de entrega se reinicien una sola vez, en una fecha y hora específicas. Para obtener más información, consulte Crear una programación de reinicios.

Programación de sondeo avanzada. Ahora es posible mejorar la programación del sondeo de aplicaciones y escritorios desde Supervisar. Con esta función, se puede configurar Citrix Probe Agent para ejecutar las tareas de sondeo en días específicos de la semana y repetirlas a intervalos específicos durante el día. Esto le permite programar una sola tarea de sondeo para que se repita en momentos específicos del día y de la semana. Ahora puede comprobar de forma proactiva el estado del sitio con sondeos configurados para que se ejecuten con regularidad en los momentos elegidos. Esta función simplifica la configuración y la administración del sondeo en Supervisar. Para obtener más información, consulte Sondeo de aplicaciones y escritorios.

Septiembre de 2022

Funciones nuevas y mejoradas

Las versiones anteriores del SDK de PowerShell remoto se han retirado. Si usa una versión retirada, el SDK deja de funcionar y aparece un mensaje de error que le pide que descargue la versión actual. Si esto ocurre, descargue el SDK de PowerShell remoto más reciente del sitio web de Citrix.

Catálogos de máquinas con inicio seguro en Azure. En los entornos de Azure, puede crear catálogos de máquinas habilitados con inicio seguro y usar la propiedad `SupportsTrustedLaunch` del inventario de máquinas virtuales para determinar los tamaños de las máquinas virtuales que admiten el inicio seguro.

El inicio seguro es una forma integrada de mejorar la seguridad de máquinas virtuales de 2.ª generación. Inicio seguro protege contra técnicas de ataque avanzadas y persistentes. Para obtener más información, consulte Catálogos de máquinas con inicio seguro.

Función para identificar los recursos de Microsoft System Center Virtual Machine Manager creados por MCS. Ahora puede identificar los recursos de Microsoft System Center Virtual Machine Manager (SCVMM) creados por MCS mediante etiquetas. Para obtener más información sobre las etiquetas que MCS agrega a los recursos, consulte Identificar los recursos creados por MCS.

Función para identificar los recursos de VMware creados por MCS. Ahora puede identificar los recursos de VMware creados por MCS mediante etiquetas. Para obtener más información sobre las etiquetas que MCS agrega a los recursos, consulte Identificar los recursos creados por MCS.

Función para optimizar la limitación de AWS WorkSpace. Ahora puede encender y apagar una gran cantidad de máquinas en AWS WorkSpace sin problemas de limitación. Los problemas de limitación se producen cuando la cantidad de solicitudes enviadas a AWS WorkSpace supera la cantidad de solicitudes que el servidor puede gestionar. Por lo tanto, ahora, Citrix agrupa varias solicitudes en una sola antes de enviarla al SDK de AWS WorkSpace.

Posibilidad de comprobar los detalles de la máquina al ver los recuentos de máquinas en Inicio. Al ver los recuentos de máquinas por estado de disponibilidad en **Inicio**, ahora puede hacer clic en un estado para ver los detalles de las máquinas que tienen ese estado. Para obtener más información, consulte la página de inicio de la interfaz de Configuración completa.

Función para crear catálogos de máquinas con una imagen de una suscripción diferente del mismo arrendatario de Azure. Anteriormente, en los entornos de Azure, solo podía seleccionar una imagen dentro de su suscripción para crear un catálogo de máquinas. Con esta función, ahora puede seleccionar una imagen en Azure Compute Gallery (anteriormente conocida como Shared Imaged Gallery) que pertenezca a una suscripción compartida diferente para crear y actualizar catálogos de MCS.

Para obtener más información sobre la creación de un catálogo, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Para obtener información sobre cómo compartir imágenes con otra entidad principal de servicio del mismo arrendatario, consulte Compartir imágenes con otra entidad principal de servicio del mismo arrendatario.

Para obtener información sobre los comandos de PowerShell para seleccionar una imagen de una suscripción diferente, consulte Uso de PowerShell para seleccionar una imagen de una suscripción diferente.

Para obtener más información sobre Azure Compute Gallery, consulte Azure Shared Image Gallery.

Agosto de 2022

Funciones nuevas y mejoradas

Función para identificar todos los recursos de Citrix Hypervisor creados por MCS. Ahora puede identificar los recursos de Citrix Hypervisor creados por MCS mediante etiquetas. Para obtener más información sobre las etiquetas que MCS agrega a los recursos, consulte Identificar los recursos creados por MCS.

Compatibilidad con el uso de grupos de hosts y zonas de disponibilidad de Azure al mismo tiempo. En los entornos de Azure, ahora hay una comprobación previa para evaluar si la creación de un catálogo de máquinas se hará correctamente en función de la zona de disponibilidad de Azure especificada en la propiedad personalizada y la zona del grupo de hosts. La creación del catálogo falla si la zona de disponibilidad especificada en la propiedad personalizada no coincide con la zona del grupo de hosts.

Un grupo de hosts es un recurso que representa un conjunto de hosts dedicados. Un host dedicado es un servicio que proporciona servidores físicos que alojan una o más máquinas virtuales.
Las zonas de disponibilidad de Azure son ubicaciones separadas físicamente dentro de cada región de Azure y toleran los errores locales.

Para obtener más información sobre las distintas combinaciones de zona de disponibilidad y zona de grupos de hosts con las que se crea correctamente o falla la creación del catálogo de máquinas, consulte Usar grupos de hosts y zonas de disponibilidad de Azure al mismo tiempo.

Función para actualizar el ID de carpeta de un catálogo de máquinas en VMware. Ahora, en entornos de virtualización de VMware, puede actualizar el ID de carpeta de un catálogo de máquinas de MCS mediante la propiedad personalizada `FolderID` de `Set-ProvScheme`. Las máquinas virtuales creadas después de actualizar el ID de carpeta se crean bajo este nuevo ID de carpeta. Si esta propiedad no se especifica en `CustomProperties`, las máquinas virtuales se crean en la carpeta en la que se encuentra la imagen maestra. Para obtener más información sobre la actualización del ID de carpeta, consulte Actualizar el ID de carpeta de un catálogo de máquinas.

Configuración de la zona horaria. Ahora puede configurar el formato de fecha y hora de la interfaz para que se adapte a sus preferencias mediante el parámetro **Fecha y hora**. Para obtener más información, consulte Configuración de la zona horaria.

Ahora, Image Portability Service (IPS) admite Amazon Web Services (AWS). Al configurar los permisos y los componentes necesarios para AWS, los flujos de trabajo de IPS se pueden usar con una cuenta de AWS. Consulte Migrar cargas de trabajo a la nube pública para obtener más información detallada.

Configuración del archivo de paginación durante la preparación de imágenes en entornos de Azure. Ahora, en los entornos de Azure, puede evitar posibles confusiones con la ubicación del

archivo de paginación. Con ese fin, MCS ahora determina la ubicación del archivo de paginación al crear el esquema de aprovisionamiento durante la preparación de la imagen. Este cálculo se basa en ciertas reglas. Las funciones como el disco de SO efímero (EOS) y E/S de MCS tienen su propia ubicación prevista de archivo de paginación y son exclusivas entre sí. Además, aunque separe la preparación de la imagen de la creación del esquema de aprovisionamiento, MCS determina correctamente la ubicación del archivo de paginación. Para obtener más información sobre la ubicación del archivo de paginación, consulte Ubicación del archivo de paginación.

Opción para actualizar la configuración del archivo de paginación en entornos de Azure. Ahora, al crear un catálogo en un entorno de Azure, puede especificar el parámetro del archivo de paginación, incluidos la ubicación y el tamaño, mediante comandos de PowerShell. Esto supedita el parámetro del archivo de paginación determinados por MCS. Para ello, ejecute el comando `New-ProvScheme` con estas propiedades personalizadas:

- `PageFileDiskDriveLetterOverride`: Letra de la unidad de disco de la ubicación del archivo de paginación
- `InitialPageFileSizeInMB`: Tamaño del archivo de paginación inicial en MB
- `MaxPageFileSizeInMB`: Tamaño del archivo de paginación máximo en MB

Para obtener más información sobre cómo actualizar el parámetro del archivo de paginación, consulte Actualizar el parámetro del archivo de paginación.

Actualizaciones de la página de inicio. Ahora, el widget Introducción tiene un nuevo aspecto. Otras actualizaciones de la página de inicio incluyen:

- Los iconos Actualizar y Ayuda recién agregados en la esquina superior derecha.
- Recuentos de recursos en los que se puede hacer clic, lo que proporciona un acceso rápido a páginas de recursos relevantes.
- Mejora del icono No me gusta. Si no le gusta una recomendación, esta desaparece. Si no le gusta el widget de recomendaciones, el widget desaparece.

Para obtener más información, consulte Página de inicio.

Función para habilitar extensiones de máquinas virtuales de Azure. Ahora, al usar una especificación de plantillas ARM como perfil de máquina para crear un catálogo de máquinas, puede agregar extensiones de VM de Azure a las máquinas virtuales del catálogo, ver la lista de extensiones compatibles y quitar extensiones que haya agregado. Las extensiones de VM de Azure son pequeñas aplicaciones que proporcionan tareas de configuración y automatización posteriores a la implementación en máquinas virtuales de Azure. Por ejemplo, si una VM requiere la instalación de software, protección antivirus o la capacidad de ejecutar un script dentro de ella, puede usar una extensión de VM. Para obtener más información sobre cómo habilitar las extensiones de VM de Azure, consulte Usar PowerShell para habilitar extensiones de VM de Azure.

Inicio seguro disponible para discos de SO efímero. Ahora puede crear esquemas de aprovision-

amiento mediante un disco de SO efímero en Windows con inicio seguro. El inicio seguro es una forma integrada de mejorar la seguridad de máquinas virtuales de 2.ª generación. Las protege de técnicas de ataque avanzadas y persistentes mediante la combinación de tecnologías que se pueden habilitar de forma independiente, como el arranque seguro y la versión virtualizada del Módulo de plataforma segura (vTPM). Para obtener más información sobre la creación de un catálogo de máquinas, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Julio de 2022

Funciones nuevas y mejoradas

Tiempos de espera de sesión dinámicos para máquinas con SO de sesión única. Ahora, los tiempos de espera de sesión dinámicos están disponibles en máquinas con SO de sesión única. Se necesita un grupo de entrega con al menos un VDA con la versión 2206 o una posterior. Asegúrese de que dichos VDA se hayan registrado en Citrix Cloud al menos una vez. Para obtener más información, vaya a Tiempos de espera de sesión dinámicos.

Envío de recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión en Autoscale. Ahora dispone de una nueva función en **Notificaciones de cierre de sesión del usuario** (antes denominada **Forzar el cierre de sesión del usuario**) en Autoscale. La función le permite enviar recordatorios de cierre de sesión a los usuarios sin forzarlos a cerrar la sesión. Al hacerlo, se evita la posible pérdida de datos causada por forzar a los usuarios a cerrar sus sesiones. Consulte Notificaciones de cierre de sesión del usuario para obtener información detallada.

Capacidad para establecer el tipo de licencia del SO Linux al crear catálogos de máquinas virtuales de Linux en Azure. Ahora, con la interfaz de Configuración completa, puede elegir el tipo de licencia del sistema operativo Linux al crear catálogos de máquinas virtuales Linux en Azure. Tiene dos opciones para sus licencias propias de Linux: Red Hat Enterprise Linux y SUSE Linux Enterprise Server. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Experiencia de búsqueda mejorada en Configuración completa. El nodo de búsqueda proporciona estas funciones y mejoras nuevas:

- **Capacidad para exportar resultados de búsqueda**. Ahora puede exportar resultados de búsqueda. Para ello, haga clic en el icono de exportación de la esquina superior derecha.
- **Nuevo filtro disponible**. El filtro Acción de energía pendiente ya se puede usar. Use el filtro para refinar las búsquedas.
- **Función de búsqueda "No contiene"para ciertos elementos**. Ahora, elementos como los nombres de máquinas y las etiquetas admiten criterios de búsqueda con "No contiene".
- **Función para buscar objetos al agregar filtros**. Ahora, al agregar filtros para estos objetos,

puede buscarlos: conexiones, catálogos de máquinas, grupos de entrega, grupos de aplicaciones y etiquetas.

Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Compatibilidad con perfiles de almacenamiento de VMware. Ahora, al crear un catálogo de máquinas con una imagen maestra en un almacén de datos de vSAN, puede copiar la directiva de almacenamiento, como la información de RAID-1 o RAID-5, de la imagen maestra en los dispositivos de destino creados. Para los catálogos existentes, la directiva de almacenamiento permanece sin cambios aunque actualice el catálogo.

Función para el registro de SPN de RestrictedKrbHost. Ahora, todas las cuentas de equipo creadas por Citrix MCS están registradas en nombres principales de servicio (SPN) de `RestrictedKrbHost`. Esto evita la necesidad de ejecutar el comando `setspn` con el fin de registrar el SPN para las cuentas de equipo después de que MCS las haya creado.

Paquetes de aplicaciones en Configuración completa para entregar aplicaciones empaquetadas de Microsoft. El nodo App-V pasa a llamarse Paquetes de aplicaciones y se ha rediseñado para adaptarse a más tipos de aplicaciones empaquetadas de Microsoft. Antes tenía que usar el módulo de detección para agregar aplicaciones empaquetadas de App-V a su entorno para su entrega. Ahora puede agregar y entregar las aplicaciones en un solo lugar mediante el nodo Paquetes de aplicaciones. Para obtener más información, consulte Paquetes de aplicaciones.

Función para usar especificaciones de plantillas ARM como perfiles de máquinas. Antes solo podía usar máquinas virtuales como perfiles de máquina. Ahora puede usar especificaciones de plantillas ARM como perfiles de máquinas también al crear catálogos de máquinas de Azure. Esta función le permite aprovechar funciones de las plantillas ARM de Azure, como el control de versiones. Para asegurarnos de que la especificación seleccionada está configurada correctamente y contiene las configuraciones necesarias, la validamos nosotros. Si se produce un error en la validación, se le pedirá que seleccione otro perfil de máquina. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Función para validar la especificación de plantillas ARM. Ahora puede validar la especificación de plantilla ARM para asegurarse de que se puede utilizar como perfil de máquina para crear un catálogo de máquinas. Hay dos formas de validar la especificación de la plantilla ARM:

- Usar la interfaz de administración de Configuración completa.
- Usar los comandos de PowerShell.

Para obtener más información sobre la validación de la especificación de la plantilla ARM, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Junio de 2022

Funciones nuevas y mejoradas

Función de programación de reinicios para máquinas con SO de sesión única. Antes, la función de programación de reinicios solo estaba disponible para máquinas con SO multisesión. Ahora también está disponible para máquinas con SO de sesión única. Ya puede crear programaciones de reinicios para grupos de entrega que contengan máquinas con SO de sesión única. Para obtener más información, consulte Crear y administrar programaciones de reinicios para las máquinas de un grupo de entrega.

Opción para realizar precomprobaciones de los nombres de usuario. Ahora, la opción **Comprobar nombre** está disponible al introducir las credenciales de dominio. Con esta opción, puede comprobar si el nombre de usuario es válido o único. La opción es útil, por ejemplo, cuando:

- El mismo nombre de usuario existe en varios dominios. Se le solicita que seleccione el usuario correspondiente.
- No se acuerda del nombre del dominio. Puede introducir el nombre del usuario sin especificar el nombre del dominio. Si la comprobación se realiza correctamente, el nombre del dominio se rellena automáticamente.

Para obtener más información, consulte Credenciales de dominio.

Posibilidad de cambiar el parámetro de red de un esquema de aprovisionamiento existente. Ahora puede cambiar el parámetro de red de un esquema de aprovisionamiento existente para que las nuevas máquinas virtuales se creen en la nueva subred. Utilice el parámetro `-NetworkMapping` del comando `Set-ProvScheme` para cambiar el parámetro de la red. Solo las máquinas virtuales recién aprovisionadas del esquema tendrán los nuevos parámetros de subred. También debe asegurarse de que las subredes estén en la misma unidad de alojamiento. Para obtener más información, consulte Cambiar el parámetro de red de un esquema de aprovisionamiento existente.

Obtener información del nombre de la región de las máquinas virtuales de Azure, los discos administrados, las instantáneas, el VHD de Azure y la plantilla de ARM. Ahora puede mostrar la información del nombre de la región de una VM de Azure, discos administrados, instantáneas, el VHD de Azure y la plantilla de ARM. Esta información se muestra para los recursos de la imagen maestra cuando se asigna un catálogo de máquinas. Para obtener más información, consulte Obtenga la información del nombre de la región de las máquinas virtuales de Azure, los discos administrados, las instantáneas, el VHD de Azure y la plantilla de ARM.

Posibilidad de usar valores de propiedades de perfil de máquina en el entorno de Azure. Ahora, al crear un catálogo de Azure con un perfil de máquina, puede definir los valores de propiedad a partir de la especificación de plantilla de ARM o de la VM, lo que se utilice como perfil de máquina, si los valores no están definidos explícitamente en las propiedades personalizadas. Las propiedades afectadas por esta función son las siguientes:

- Zona de disponibilidad
- ID de grupo de hosts dedicado
- ID del conjunto de cifrado de disco
- Tipo de SO
- Tipo de licencia
- Oferta de servicios
- Tipo de almacenamiento

Si faltan algunas propiedades en el perfil de la máquina (MachineProfile) y no están definidas en las propiedades personalizadas (CustomProperties), se utiliza el valor predeterminado de las propiedades siempre que sea aplicable. Para obtener más información, consulte Usar valores de propiedades de perfil de máquina.

Mayor compatibilidad con la actualización de versiones de VDA. Ahora, con la interfaz de Configuración completa, puede actualizar la versión de las máquinas persistentes aprovisionadas por MCS. Puede actualizarlas por catálogo o por máquina. Para obtener más información, consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.

Citrix Probe Agent en planos de control de Citrix Cloud Japan y Citrix Cloud Government. Ahora, Citrix Probe Agent admite sitios alojados en planos de control de Citrix Cloud Japan y Citrix Cloud Government. Para usar el agente de sondeos en estos planos, establezca el valor del Registro en la ruta "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\region"en 2 para la región Japan y en 3 para la región Government. Citrix Probe Agent automatiza el proceso de comprobación del estado de aplicaciones y escritorios virtuales que se publican en un sitio. Para obtener más información, consulte Sondeo de aplicaciones y escritorios.

Personalizar el puerto utilizado para la comunicación entre los VDA y los Cloud Connectors. Ahora puede personalizar el puerto que el VDA utiliza para comunicar con los Cloud Connectors en función de sus requisitos de seguridad específicos. Esta función es útil si el equipo de seguridad no permite dejar abierto el puerto predeterminado (puerto 80) o si el puerto predeterminado ya está en uso. Para obtener más información, consulte Personalizar el puerto para la comunicación con los Cloud Connectors.

Compatibilidad con la organización de catálogos de máquinas por medio de carpetas. Ahora puede crear carpetas anidadas para organizar los catálogos de máquinas y acceder a ellos fácilmente. Para obtener más información, consulte Organizar los catálogos por medio de carpetas.

Compatibilidad con SCVMM 2022. Ahora Citrix DaaS admite System Center Virtual Machine Manager (SCVMM) 2022 de Microsoft. SCVMM proporciona una gama de servicios que incluyen el mantenimiento de los recursos que necesita para implementar las máquinas virtuales. Para obtener más información sobre las nuevas funciones admitidas en SCVMM 2022, consulte What's new in System Center Virtual Machine Manager.

Función para configurar el parámetro del máximo de operaciones simultáneas de aprovision-

amiento en AWS. Ahora Citrix DaaS admite `MaximumConcurrentProvisioningOperations` como propiedad personalizada configurable para MCS en AWS. `MaximumConcurrentProvisioningOperat` es la propiedad que determina la cantidad de máquinas virtuales que puede crear o eliminar simultáneamente. Si bien MCS admite un máximo de 100 operaciones de aprovisionamiento simultáneas de forma predeterminada, ahora puede introducir comandos de PowerShell para personalizar este valor. Puede introducir un valor comprendido entre 1 y 1000. Al poder establecer esta propiedad en el valor que prefiera, podrá controlar la cantidad de tareas paralelas que puede realizar al crear o eliminar máquinas virtuales. Para obtener más información sobre cómo configurar el máximo de operaciones de aprovisionamiento simultáneas, consulte Valores predeterminados de conexión de host.

Mayo de 2022

Funciones nuevas y mejoradas

Diagnóstico de inicios de sesión mejorado. Citrix DaaS ahora admite un diagnóstico de errores de inicio de sesión detallado. Ahora puede ver los componentes involucrados en la secuencia de inicio de sesión. Se resaltan los componentes que fallaron con los últimos códigos de error generados. Esto ayuda a identificar el motivo exacto del error en el inicio de una sesión y a adoptar las medidas recomendadas.

La página Transacción se amplía con el panel Detalles de la transacción, que contiene una lista de componentes que indican la aparición del error. Al hacer clic en el nombre del componente, se muestran los detalles del componente y los detalles del último error conocido. Se muestran el motivo del fallo y el código de error. Al hacer clic en el enlace Más información, se accede al código específico de Códigos de error que contiene una descripción detallada y la acción recomendada. Para obtener más información, consulte Diagnóstico de la sesión.

Compatibilidad con el uso de Set-ProvServiceConfigurationData en el SDK de PowerShell remoto. Ya puede ejecutar `Set-ProvServiceConfigurationData` con el SDK de PowerShell remoto para configurar todos los parámetros aplicables. También puede omitir la habilitación de DHCP durante la preparación de imágenes con este comando. A continuación, se muestra la lista de parámetros compatibles con `Set-ProvServiceConfigurationData`:

- Cambiar el tiempo de espera de la preparación de imágenes: `Set-ProvServiceConfigurationData -Name "ImageManagementPrep_PreparationTimeout"-value 60`
- Omitir la habilitación de DHCP: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value EnableDHCP`
- Omitir el rearmado del KMS de Microsoft Windows: `Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps -Value OsRearm`

- Omitir el rearmado del KMS de Microsoft Office:
  ```
  Set-ProvServiceConfigurationData -Name ImageManagementPrep_Excluded_Steps
   -Value OfficeRearm
  ```
- Inhabilitar el apagado automático de VM de preparación:
  ```
  Set-ProvServiceConfigurationData –Name ImageManagementPrep_NoAutoShutdown
   –Value true
  ```
- Inhabilitar la inyección de dominios:
  ```
  Set-ProvServiceConfigurationData –Name DisableDomainInjection –
  Value true
  ```

Capacidad para establecer el tipo de licencia de Linux al crear catálogos de máquinas Linux mediante comandos de PowerShell. Con los comandos de PowerShell, puede establecer el tipo de licencia de Linux al crear catálogos de máquinas Linux. Tiene dos opciones para crear sus propias licencias de Linux: RHEL_BYOS y SLES_BYOS. El parámetro se establece de forma predeterminada en licencias de Azure Linux. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Función para identificar todos los recursos de Azure creados por MCS. Ahora puede identificar todos los recursos de Azure creados por MCS, como la imagen, el disco del ID, el disco del SO, la tarjeta NIC, la VM, etc., que estén asociados a un ProvScheme mediante una etiqueta llamada `provschemeID`. Para obtener más información sobre las etiquetas que MCS agrega a los recursos, consulte Identificar los recursos creados por MCS.

Compatibilidad con el aprovisionamiento de Azure Stack HCI mediante SCVMM. Ahora, MCS permite el aprovisionamiento de Azure Stack HCI mediante Microsoft System Center Virtual Machine Manager (SCVMM). Puede administrar el clúster de Azure Stack HCI con las herramientas existentes, incluido SCVMM. Para obtener más información, consulte Entornos de virtualización de Microsoft System Center Virtual Machine Manager.

Función para agregar manualmente usuarios que no son de Active Directory. Ahora, con la interfaz de administración de Configuración completa, puede introducir una lista de nombres de usuario separados por puntos y comas al agregar usuarios que no sean de Active Directory a un catálogo. Tenga en cuenta el formato al agregar usuarios que residen en directorios distintos. Por ejemplo: si los usuarios están en Active Directory, introduzca los nombres directamente. Si no es así, introduzca los nombres en este formato: `<identity provider>:<user name>`. Ejemplo: `AzureAD:username`. Para obtener más información, consulte Crear un catálogo de máquinas.

Abril de 2022

Funciones nuevas y mejoradas

Página de inicio de la interfaz de Configuración completa. Ahora Configuración completa cuenta con una página de inicio, que proporciona una descripción general de la implementación y las cargas de trabajo de Citrix DaaS, junto con información que le ayuda a sacar el máximo rendimiento de su suscripción. La página consta de estas partes:

- **Descripción general del servicio**. Proporciona una descripción general de la implementación y las cargas de trabajo de Citrix DaaS.
- **Recomendaciones**. Recomienda funciones que están disponibles con su suscripción y recopila sus comentarios.
- **Novedades**. Muestra las funciones más recientes.
- **Funciones en Tech Preview**. Muestra las funciones que se hallan en Tech Preview.
- **Introducción**. Muestra los pasos que le guiarán durante la configuración inicial.

Para obtener más información, consulte Página de inicio.

Muestra el progreso de la creación y las actualizaciones de los catálogos. Ahora, Configuración completa le permite mantenerse al día sobre la creación y las actualizaciones de catálogos. Puede obtener una visión general del proceso de creación y actualización, ver el historial de los pasos realizados y supervisar el progreso y el tiempo de ejecución del paso actual. Para obtener más información, consulte Comenzar a crear el catálogo.

Muestra los hipervisores y los servicios de la nube disponibles según la zona seleccionada. En Configuración completa, al crear conexiones de host, debe seleccionar una zona antes de seleccionar un tipo de conexión. La lista desplegable Tipo de conexión muestra los hipervisores y los servicios de la nube disponibles con la zona. Antes, para garantizar que la lista Tipo de conexión mostrara un hipervisor o servicio de la nube necesario, tenía que instalar su plug-in en cada zona. Ahora, con esta nueva secuencia de configuración, puede instalar el plug-in solo en la zona requerida.

También puede usar el comando de PowerShell para obtener la lista de plug-ins de hipervisor disponibles con la zona seleccionada. Para obtener más información, consulte Crear una conexión y recursos.

Compatibilidad con usuarios no unidos a AD local en Configuración completa. Hay un nuevo campo, **Seleccione el tipo de identidad**, disponible en las interfaces en las que se asignan usuarios a escritorios o aplicaciones aprovisionados, grupos de entrega o grupos de aplicaciones. Ahora, con el campo, puede seleccionar cuentas de usuario de cualquiera de estos proveedores de identidades a los que está conectada su cuenta de Citrix Cloud:

- Active Directory
- Azure Active Directory

- Okta

Posibilidad de rechazar propiedades personalizadas no válidas en entornos de Google Cloud Platform (GCP) y Azure. Ahora puede evitar posibles confusiones si las propiedades personalizadas establecidas en `New-ProvScheme` y `Set-ProvScheme` no surten efecto. Si especifica propiedades personalizadas no existentes, recibirá un mensaje de error. Para obtener más información, consulte Consideraciones importantes sobre la configuración de propiedades personalizadas.

Función para crear máquinas unidas a Azure Active Directory. Ahora, en **Configuración completa**, al crear un catálogo, el tipo de identidad **Unido a Azure Active Directory** está disponible en **Identidades de máquina**. Con ese tipo de identidad, puede usar MCS para crear máquinas unidas a Azure Active Directory. También tiene una opción adicional, **Inscribir las máquinas en Microsoft Intune**, para inscribir las máquinas en Microsoft Intune para su administración.

Para obtener información sobre la creación de catálogos unidos a Azure Active Directory, consulte Crear catálogos de máquinas. Para obtener información sobre los requisitos y las consideraciones relacionadas con la unión a Azure Active Directory, consulte Unidos a Azure Active Directory.

Función para crear máquinas unidas a Azure Active Directory híbrido. Ahora, en **Configuración completa**, al crear un catálogo, el tipo de identidad **Unido a Azure Active Directory híbrido** está disponible en **Identidades de máquina**. Con ese tipo de identidad, puede usar MCS para crear máquinas unidas a Azure Active Directory híbrido. Estas máquinas son propiedad de una organización en las que se ha iniciado sesión con una cuenta de Active Directory Domain Services perteneciente a esa organización.

Para obtener información sobre la creación de catálogos unidos a Azure Active Directory híbrido, consulte Crear catálogos de máquinas. Para obtener información sobre los requisitos y las consideraciones relacionadas con la unión a Azure Active Directory híbrido, consulte Unidos a Azure Active Directory híbrido.

Compatibilidad con inicio de confianza de Azure para instantáneas. Ahora, además de las imágenes, el inicio de confianza de Azure también está disponible para instantáneas. Si selecciona una instantánea con el inicio de confianza habilitado, es obligatorio usar un perfil de máquina. Además, debe seleccionar un perfil de máquina con el inicio de confianza habilitado. Para obtener más información, consulte Entornos de nube para Microsoft Azure Resource Manager.

Exportación de máquinas. Ahora puede exportar las máquinas que aparecen en la página **Máquinas** del asistente de **configuración de catálogos de máquinas** en un archivo CSV, que se utilizará como plantilla al agregar máquinas a un catálogo en bloque. Para obtener más información, consulte Exportar máquinas de un catálogo.

Opción para acceder a la consola web de Workspace Environment Management. Ahora, hay una opción, Environment Management (Web), disponible en el menú de la ficha **Administrar**. Esta opción le lleva a la nueva consola web de Workspace Environment Management. Para acceder a la consola

antigua, utilice **Environment Management**. Estamos migrando todo el conjunto de funcionalidades de la antigua consola a la nueva consola web. La consola web normalmente responde más rápido que la antigua consola. Para obtener más información, consulte Workspace Environment Management Service.

Capacidad para administrar los parámetros de ProvScheme. Ahora, al utilizar MCS para crear catálogos, obtendrá un error si establece los parámetros `New-ProvScheme` en hipervisores no compatibles durante la creación del catálogo de máquinas o si actualiza los parámetros `Set-ProvScheme` después de crear el catálogo de máquinas. Para obtener más información, consulte Crear catálogos de máquinas.

Aumento de los límites de ubicación de recursos. Ahora, se han aumentado los límites de ubicación de recursos para los VDA de sesión única y los VDA multisesión a 10 000 y 1000, respectivamente. Para obtener más información, consulte Límites.

Función para reiniciar máquinas sin administración de energía después de purgar todas las sesiones. Ahora Citrix DaaS le permite crear programaciones de reinicio para máquinas cuya energía no se administra después de que todas las sesiones se hayan purgado de las máquinas. En la interfaz de Configuración completa, seleccione **Reiniciar todas las máquinas después de purgar todas las sesiones** como **Duración del reinicio**. Para obtener más información, consulte Crear una programación de reinicios.

Función para actualizar la versión de máquinas VDA (Tech Preview). Ahora, con la interfaz de Configuración completa, puede actualizar la versión de las máquinas VDA para la implementación de Citrix DaaS. Puede actualizarlas por catálogo o por máquina. La función se aplica a las máquinas que no se crean con MCS (por ejemplo, máquinas físicas). Para obtener más información, consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.

Las máquinas no se apagan durante las interrupciones del servicio. Citrix DaaS ahora evita que el intermediario apague las máquinas virtuales cuando la zona en la que se encuentran sufre una interrupción. Las máquinas estarán disponibles automáticamente para las conexiones cuando finalice la interrupción. No tiene que adoptar ninguna medida para que las máquinas estén disponibles después de la interrupción del servicio.

Diagnóstico de inicio de sesión. Citrix DaaS ahora admite un diagnóstico de errores de inicio de sesión mejorado. Use el ID de transacción de 32 dígitos (8-4-4-4-12) generado por la aplicación Citrix Workspace desde Citrix Monitor (es decir, el servicio Citrix Director) para localizar el componente y la etapa exactos en los que se produjo el problema y adoptar las medidas recomendadas para resolverlo. Para obtener más información, consulte Diagnóstico de inicio de sesión.

Opción para acceder al servicio de Grabación de sesiones. Ahora, hay una opción, Grabación de sesiones, disponible en el menú de la ficha **Administrar**. La llegada del servicio de Grabación de sesiones proporciona una administración centralizada de directivas, reproducciones y configuraciones de los servidores. Alivia la carga de los administradores de TI al proporcionar un punto de entrada

unificado para administrar y observar los objetos distribuidos en su organización. Para obtener más información, consulte Servicio de Grabación de sesiones (Tech Preview).

Cambio de nombre de Citrix Virtual Apps and Desktops Service. El nombre de **Citrix Virtual Apps and Desktops Service** ha cambiado a **Citrix DaaS**. Puede obtener más información sobre el cambio de nombre en el anuncio en nuestro blog.

El nombre de las siguientes soluciones Citrix Virtual Apps and Desktops Service ha cambiado.

- **Citrix Virtual Apps Service Advanced** se llama ahora **Citrix DaaS Advanced**.
- **Citrix Virtual Apps Service Premium** se llama ahora **Citrix DaaS Premium**.
- **Citrix Virtual Desktops Service** se llama ahora **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops Service Advanced** se llama ahora **Citrix DaaS Advanced Plus**.
- **Citrix Virtual Apps and Desktops Service Premium** está disponible ahora como **Citrix DaaS Premium y Citrix DaaS Premium Plus**.
- **Citrix Virtual Apps and Desktops Standard para Azure** se llama ahora **Citrix DaaS Standard para Azure**.
- **Citrix Virtual Apps and Desktops Standard para Google Cloud** se llama ahora **Citrix DaaS Standard para Google Cloud**.
- **Citrix Virtual Apps and Desktops Premium para Google Cloud** se llama ahora **Citrix DaaS Premium para Google Cloud**.

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

- La interfaz de usuario del producto, el contenido del producto y las imágenes e instrucciones de la documentación del producto se actualizarán en las próximas semanas.
- Es posible que algunos elementos (como los comandos y los MSI conserven los nombres anteriores para que los scripts existentes de cliente sigan funcionando).
- Asimismo, la documentación de producto y otros recursos relacionados (como vídeos y entradas de blog) que se incluyan como enlaces en la documentación de este producto pueden contener todavía los nombres anteriores.

> **Nota:**
>
> El nombre del producto local, **Citrix Virtual Apps and Desktops**, sigue siendo el mismo.

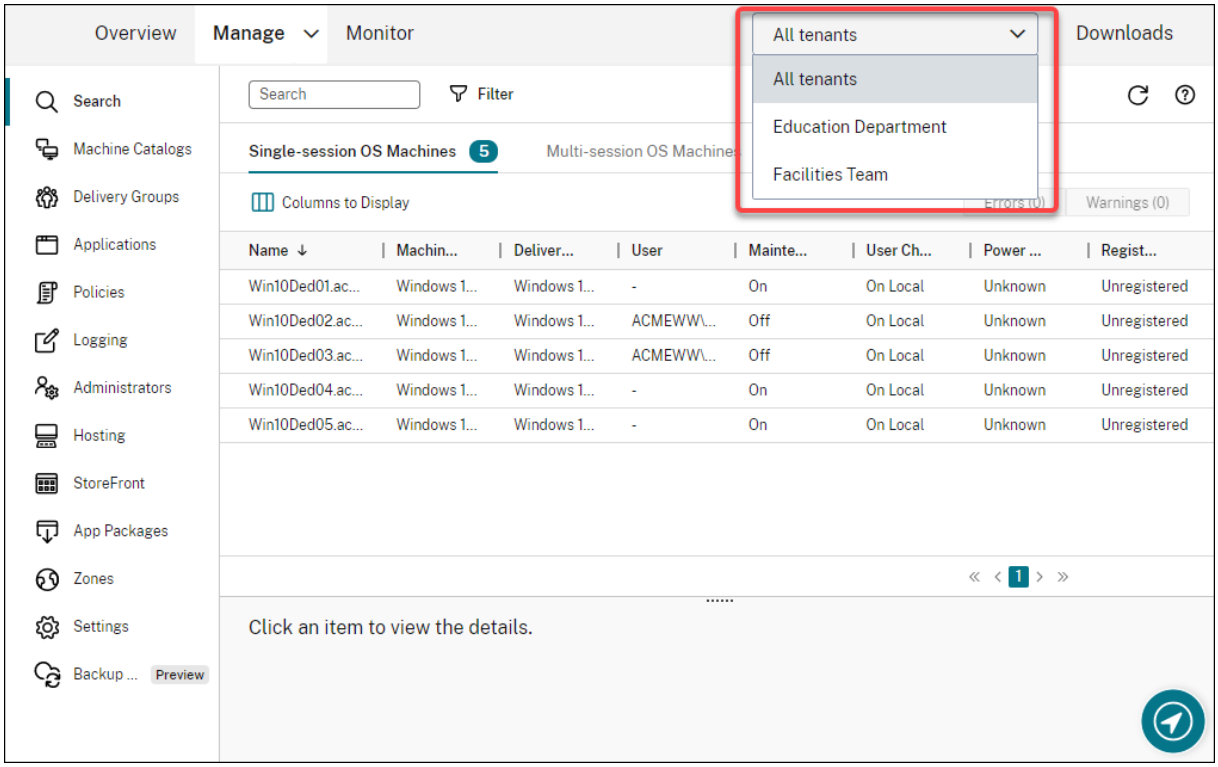
Compatibilidad con arrendatarios en Configuración completa. Ahora puede crear particiones de configuración en una sola instancia de Citrix DaaS. Para ello, cree ámbitos de arrendatario en **Administradores > Ámbitos** y asocie objetos de configuración, como catálogos de máquinas y grupos de entrega, a esos arrendatarios. Como resultado, los administradores con acceso a un arrendatario solo pueden administrar objetos que estén asociados al arrendatario. Esta función es útil, por ejemplo, si su organización:

- Tiene diferentes silos empresariales (divisiones independientes o equipos de administración de TI separados)
- O tiene varios sitios locales y quiere mantener la misma configuración en una sola instancia de Citrix DaaS

Además, la interfaz de Configuración completa le permite filtrar clientes arrendatarios por nombre. De forma predeterminada, la interfaz muestra información sobre todos los arrendatarios.

La función está disponible tanto para proveedores CSP (Citrix Service Provider) como no CSP. La interfaz de un entorno CSP es esencialmente la misma que la de un entorno no CSP, excepto por el método utilizado para crear arrendatarios.

- Los CSP incorporan los clientes arrendatarios a Citrix DaaS y luego configuran el acceso de administrador a Citrix DaaS. Para obtener más información, consulte Citrix DaaS para Citrix Service Providers.
- Para crear clientes arrendatarios, los no CSP crean primero ámbitos y, a continuación, configuran el acceso personalizado para los administradores correspondientes. Para obtener más información, consulte Crear y administrar ámbitos.



Actualizaciones de Autoscale. Hemos actualizado Autoscale con un estilo de hoja para ofrecerle una mejor experiencia de usuario. Los flujos de trabajo para configurar los parámetros siguen siendo iguales. Otras actualizaciones de Autoscale incluyen:

- **Restringir Autoscale** se llama ahora **Autoscale de máquinas etiquetadas** para que sea más

fácil de entender.
- Se agregó una nueva opción: **Controlar cuándo Autoscale comienza a encender máquinas etiquetadas**. Esta opción permite controlar cuándo Autoscale comienza a encender las máquinas etiquetadas en función del uso de máquinas sin etiquetar.

Para obtener más información sobre la función Autoscale de máquinas etiquetadas, consulte Autoscale de máquinas etiquetadas.

Comprobaciones de validez de licencias. La interfaz de Configuración completa ahora comprueba automáticamente la validez de las licencias que usan las conexiones de host. Las conexiones de host cuyas licencias no sean válidas se ponen en modo de mantenimiento. Como resultado, no se pueden realizar ciertas operaciones, como modificar la conexión o desactivar el modo de mantenimiento. Una licencia deja de ser válida, por ejemplo, cuando:

- La licencia ha caducado. En este caso, contacte con un representante de ventas de Citrix para renovarla o comprar nuevas licencias.
- La licencia se ha eliminado del Servidor de licencias.

Estilo de hoja aplicado a los nodos de directivas y catálogos de máquinas. El estilo de hoja se aplica ahora a todos los nodos de Configuración completa.

Compatibilidad con la actualización de máquinas aprovisionadas por MCS en entornos de Azure. `Set-ProvScheme` cambia la plantilla (esquema de aprovisionamiento) y no afecta a las máquinas existentes. Con el comando Request-ProvVMUpdate, ahora puede aplicar el esquema de aprovisionamiento actual a una máquina (o a un conjunto de máquinas). Actualmente, la actualización de propiedades que admite esta función es `ServiceOffering`. Para obtener más información, consulte Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento.

Marzo de 2022

Funciones nuevas y mejoradas

Citrix Virtual Apps and Desktops para Google Cloud está disponible en Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium para Google Cloud ya se puede adquirir en Google Cloud Marketplace. Citrix Virtual Apps and Desktops Premium para Google Cloud ejecuta el plano de control de Citrix Virtual Apps and Desktops Service en Google Cloud.

Compatibilidad con inicio de confianza para Azure. El inicio de confianza de Azure ya está disponible para la interfaz de administración de Configuración completa. Si selecciona una imagen con inicio de confianza habilitado, es obligatorio usar un perfil de máquina. Además, debe seleccionar un perfil de máquina con el inicio de confianza habilitado. Para obtener más información, consulte Entornos de nube para Microsoft Azure Resource Manager.

Se ha aplicado el estilo de hoja a los asistentes en tres nodos más de Configuración completa. Los nodos son **Búsqueda**, **Grupos de entrega** y **Aplicaciones**.

Se ha publicado Image Portability Service (IPS) con disponibilidad generalizada. IPS simplifica la administración de imágenes en distintas plataformas. Esta funcionalidad es útil para administrar imágenes entre una ubicación de recursos local y la nube pública. Las API de REST de Citrix Virtual Apps and Desktops sirven para automatizar la administración de recursos en un sitio de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Migrar cargas de trabajo a la nube pública.

Febrero de 2022

Funciones nuevas y mejoradas

Permisos de Azure. Se requieren dos conjuntos de permisos por motivos de seguridad y para minimizar el riesgo.

- Permisos mínimos: Este conjunto de permisos proporciona un mejor control de la seguridad. Sin embargo, las nuevas funciones que requieren permisos adicionales fallarán debido a que se usan permisos mínimos.
- Permisos generales: Este conjunto de permisos no le impide obtener nuevas mejoras.

Para obtener más información, consulte Acerca de los permisos Azure.

Compatibilidad con el uso del disco temporal de la VM para alojar el disco de caché con reescritura en entornos de Azure. Hemos agregado una opción, **Usar disco no persistente de caché con reescritura**, a la página **Configuración del catálogo de máquinas > Parámetros del disco** de la interfaz **Administrar > Configuración completa**. Seleccione esa opción si no quiere que el disco de caché con reescritura persista para las máquinas virtuales aprovisionadas. Con la opción seleccionada, usamos el disco temporal de la VM para alojar el disco de caché con reescritura si el disco temporal tiene suficiente espacio. Esto reduce los costes. Para obtener más información, consulte Entornos de nube para Microsoft Azure Resource Manager.

Actualizaciones de los parámetros predeterminados de conexión de host de AWS. Los valores de los parámetros predeterminados de conexión de host de AWS se han actualizado a valores más altos y probablemente los mismos para toda la configuración de la plataforma de la nube de AWS. Esto ayuda a crear conexiones de host en entornos de nube de AWS sin evaluar ni configurar los valores de los parámetros predeterminados conforme a la configuración individual. Para obtener más información, consulte Valores predeterminados de conexión de host.

Se agregaron diferentes niveles de almacenamiento en entornos de GCP. Ahora puede proporcionar estas propiedades personalizadas en los entornos de GCP para establecer el tipo de almacenamiento de los discos conectados en la máquina virtual recién creada:

- StorageType

- IdentityDiskStorageType
- WBCDiskStorageType

Para obtener más información, consulte SDK de Citrix Virtual Apps and Desktops Service.

Cambiar ciertos parámetros de VM después de crear catálogos de VM de Azure. Ahora, con la interfaz de administración de Configuración completa, puede cambiar estos parámetros después de crear un catálogo:

- Tamaño de la máquina
- Zonas de disponibilidad
- Perfil de máquina
- Licencias de Windows

Para ello, en el nodo **Catálogos de máquinas**, seleccione el catálogo y, a continuación, seleccione **Modificar catálogo de máquinas** en la barra de acciones. Para obtener más información, consulte Modificar un catálogo.

Función para almacenar el disco del sistema operativo efímero de Azure en el disco de caché o en el disco temporal. Ahora, Citrix Virtual Apps and Desktops Service le permite almacenar el disco del sistema operativo efímero de Azure en un disco de caché o en un disco temporal para máquinas virtuales habilitadas para Azure. Esta funcionalidad es útil en entornos de Azure que requieren un disco SSD de mayor rendimiento, en lugar de un disco HDD estándar. Para obtener más información, consulte Entornos de nube para Microsoft Azure Resource Manager.

Compatibilidad con Nutanix Clusters en AWS. Citrix Virtual Apps and Desktops Service admite Nutanix Clusters en AWS. Nutanix Clusters simplifica la forma en que las aplicaciones se ejecutan en nubes privadas o en varias nubes públicas. Para obtener más información, consulte Nutanix Clusters en AWS.

Disponibilidad de VMware Cloud en Amazon Web Services (AWS). VMware Cloud en Amazon Web Services (AWS) le permite migrar cargas locales de trabajo de Citrix basadas en VMware a la nube de AWS y su entorno principal de Citrix Virtual Apps and Desktops a Citrix Virtual Apps and Desktops Service. Para obtener más información, consulte VMware Cloud en Amazon Web Services (AWS).

Posibilidad de configurar el disco caché de reescritura para máquinas que se ejecutan en Google Cloud Platform (GCP). En la interfaz de administración de Configuración completa, al aprovisionar máquinas en GCP, ahora puede configurar los siguientes parámetros del disco de caché de reescritura:

- Tamaño del disco
- Memoria asignada a la caché
- Tipo de almacenamiento en disco
- Persistencia de disco

Para obtener más información, consulte Crear un catálogo de máquinas en el artículo Entornos de virtualización Google Cloud Platform.

Enero de 2022

Funciones nuevas y mejoradas

Compatibilidad con Nutanix Clusters en AWS. Ahora, Citrix Virtual Apps and Desktops Service admite Nutanix Clusters en AWS. Esto proporciona la misma funcionalidad que un clúster local de Nutanix. Solo se admite un clúster único, *Prism Element*. Para obtener más información, consulte Entornos de virtualización de Nutanix.

Nuevas funciones disponibles en Comprobación de estado de Cloud. Comprobación de estado de Cloud se ha actualizado a una nueva versión, con funciones que incluyen:

- **Corrección automática.** Comprobación de estado de Cloud ahora admite detectar y corregir automáticamente ciertos problemas identificados en las máquinas en las que se está ejecutando. Ahora hay un informe de resultados que le muestra qué medidas específicas se adoptaron. Para obtener más información, consulte Corrección automática.
- **Compatibilidad con línea de comandos.** Comprobación de estado de Cloud ahora se puede ejecutar desde la línea de comandos. Para obtener más información, consulte Ejecución de Comprobación de estado de Cloud en la línea de comandos.
- **Estado del controlador de inyección universal de Citrix.** Comprobación de estado de Cloud ahora muestra el estado del controlador de inyección universal (UVI) de Citrix y tiene asociada una comprobación del registro de eventos para los controladores UVI de Citrix.
- **Comprobación del registro de inicio de sesión.** Comprobación de estado de Cloud comprueba ahora los parámetros del registro de inicio de sesión.
- **Actualizaciones al informe de comprobación.** Para los elementos verificados que tienen varios puntos de control, el informe de comprobación final enumera ahora todos los controles que se han efectuado para mostrar qué acciones se realizaron durante la comprobación de estado.

Para obtener más información, consulte Comprobación de estado de Cloud.

Solucionar problemas de registro de VDA e inicio de sesión con Configuración completa. Con la interfaz de administración de Configuración completa, ahora puede realizar comprobaciones que evalúen el estado de los VDA. Las comprobaciones de estado de los VDA identifican posibles causas de problemas comunes con el registro y el inicio de sesión de los VDA. Puede realizar comprobaciones de estado de forma individual y en lotes. Para obtener más información, consulte Comprobaciones de estado en el VDA.

Posibilidad de especificar la fecha de caducidad del secreto de Azure para las conexiones existentes. Con la interfaz de administración de Configuración completa, ahora puede especificar la fecha en la cual caduca el secreto de la aplicación. Para obtener instrucciones sobre cómo ver la fecha de caducidad del secreto, consulte Entornos en la nube de Microsoft Azure Resource Manager. Al usar esta función, tenga en cuenta las siguientes diferencias:

- Para las entidades de servicio creadas manualmente en Azure, puede modificar directamente la fecha de caducidad en la página **Modificar conexión > Propiedades de la conexión**.
- Para modificar por primera vez la fecha de caducidad de las entidades de servicio creadas a través de Configuración completa en su nombre, vaya a **Modificar conexión > Modificar parámetros > Usar existente**. Puede hacer ulteriores modificaciones en la página **Modificar conexión > Propiedades de la conexión**.

Un botón para agregar administradores. Se agregó un botón, **Agregar administrador**, a la ficha **Configuración completa > Administradores > Administradores**. El botón ofrece una manera rápida de ir a **Administración de acceso e identidad > Administradores**, donde puede agregar (invitar) administradores. Para obtener más información, consulte Agregar un administrador.

Nuevo diseño de los asistentes en Configuración completa. Hemos actualizado los asistentes en los siguientes nodos con un nuevo estilo, incluidos colores, fuentes y otros cambios de formato, para ofrecerle una experiencia de usuario mejor: **Administradores**, **Alojamiento**, **StoreFront**, **Paquetes de aplicaciones**, **Zonas** y **Parámetros**. Los nuevos asistentes aparecen en vistas de hoja con ventanillas más amplias, lo que permite mostrar más contenido. Los flujos de trabajo para configurar los parámetros siguen siendo iguales.

Compatibilidad para retener el disco del sistema cuando la E/S de MCS está habilitada para máquinas que se ejecutan en Google Cloud Platform (GCP). Al aprovisionar máquinas en GCP en la interfaz de administración de Configuración completa, ahora puede conservar el disco del sistema durante los ciclos de energía cuando la optimización del almacenamiento de MCS (E/S de MCS) está habilitada. Para obtener más información, consulte Habilitar actualizaciones de optimización del almacenamiento de MCS.

Compatibilidad con carga o descarga directa desde EBS en Amazon Web Services (AWS). AWS proporciona ahora una API que permite la creación directa de volúmenes de EBS con el contenido deseado. Ahora puede usar la API para eliminar el requisito de trabajador de volumen para la creación de catálogos y la agregación de máquinas virtuales. Para obtener información sobre los permisos de AWS requeridos para esta funcionalidad, consulte Entornos en la nube de Amazon Web Services.

Posibilidad de identificar los recursos de Amazon Web Services (AWS) creados por MCS. Hemos agregado una nueva etiqueta denominada `CitrixProvisioningSchemeID` para identificar los recursos de AWS creados por MCS. Para obtener más información, consulte Identificar los recursos creados por MCS.

Posibilidad de configurar el acceso a Administrar y Supervisar. Ahora, la interfaz de adminis-

tración de Configuración completa le ofrece opciones adicionales para controlar si quiere conceder a los roles personalizados acceso a **Administrar** y **Supervisar**. Para obtener más información, consulte Crear y administrar roles.

Diciembre de 2021

Funciones nuevas y mejoradas

Compatibilidad con Google Cloud VMware Engine. La plataforma le permite ahora migrar cargas de trabajo locales de Citrix basadas en VMware a Google Cloud y su entorno principal de Citrix Virtual Apps and Desktops a Citrix Virtual Apps and Desktops Service. Para obtener más información, consulte Compatibilidad con VMware Engine de Google Cloud Platform (GCP).

Posibilidad de especificar con qué comienzan los nombres de las cuentas al especificar un esquema de nomenclatura. Esta versión presenta una nueva opción en la página **Configuración de catálogo de máquinas > Identidades de las máquinas** de la interfaz de administración de Configuración completa. Dicha opción le permite especificar números o letras con los que comienzan los nombres de las cuentas, ofreciéndole un mayor control sobre la denominación de las cuentas de máquina al crear catálogos. Para obtener más información, consulte Identidades de las máquinas.

Compatibilidad con la creación de conexiones Nutanix AHV XI y Nutanix AHV Prism Central (PC). En la interfaz de gestión de Configuración completa, ahora puede crear conexiones Nutanix AHV XI y Nutanix AHV PC. Para obtener más información, consulte Entornos de virtualización de Nutanix.

Compatibilidad con la selección del tipo de almacenamiento para los discos del sistema operativo al aprovisionar máquinas virtuales en GCP. En la interfaz de administración de Configuración completa, al aprovisionar máquinas virtuales en GCP, ahora puede seleccionar el tipo de almacenamiento para el disco del sistema operativo. Las opciones de almacenamiento disponibles en la página **Configuración de catálogo de máquinas > Almacenamiento** incluyen **Disco persistente estándar**, **Disco persistente equilibrado** y **Disco persistente SSD**. Para obtener más información, consulte Crear un catálogo de máquinas.

La interfaz de administración de Configuración completa admite ahora Disco efímero de Azure. Anteriormente, PowerShell era la única opción para crear máquinas que usen discos de SO efímeros. Ahora agregamos una opción, **Disco de SO efímero de Azure**, a la página **Configuración de catálogo de máquinas > Tipos de licencia y almacenamiento**. Seleccione la opción si quiere usar el disco local de la VM para alojar el disco del sistema operativo. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Proteja los recursos administrados por Machine Creation Services (MCS) contra la eliminación accidental. Ahora puede proteger los recursos administrados por MCS en Google Cloud Platform (GCP) aplicando el indicador `deletionProtection` de GCP habilitado para las VM. Con el permiso

`compute.instances.setDeletionProtection` o el rol de administrador de procesos (Compute Admin) de IAM, puede restablecer el indicador para permitir la eliminación del recurso. Esta funcionalidad se aplica tanto a catálogos persistentes como no persistentes. Para obtener más información, consulte Proteger contra la eliminación accidental de máquinas.

Noviembre de 2021

Funciones nuevas y mejoradas

Agregar anotaciones en una imagen al actualizar las máquinas. Ahora, en la interfaz de administración de Configuración completa, puede agregar anotaciones en una imagen al actualizar un catálogo creado por MCS. Cada vez que actualiza el catálogo, se crea una entrada relacionada con la nota. Si actualiza el catálogo sin agregar una nota, la entrada aparece como nula (-). Para ver el historial de notas de la imagen, seleccione el catálogo, haga clic en **Propiedades de plantilla** en el panel inferior y, a continuación, haga clic en **Ver historial de notas**. Para obtener más información, consulte Actualizar un catálogo.

Compatibilidad con licencias de varios tipos. La interfaz de administración de Configuración completa ahora admite licencias de varios tipos, lo que le permite especificar qué derechos de licencia quiere que utilicen su sitio (la implementación de un producto de Citrix Virtual Apps and Desktops Service) o un grupo de entrega.

- En el nivel de sitio, usted determina qué licencia usar en todo el sitio cuando los usuarios inician una aplicación o un escritorio en sus dispositivos. La licencia seleccionada se aplica a todos los grupos de entrega, excepto a los configurados con una licencia diferente.
- En el nivel de grupo de entrega, usted determina qué licencia quiere que utilice el grupo de entrega, lo que le permite disfrutar de la flexibilidad y las ventajas que ofrecen las licencias de varios tipos.

Para obtener más información, consulte Licencias de varios tipos.

Compatibilidad para mostrar la información del plan de compra de Azure Marketplace. Al crear un catálogo de máquinas en la interfaz de administración de Configuración completa, ahora puede ver la información del plan de compra de imágenes maestras originadas a partir de imágenes de Azure Marketplace.

Octubre de 2021

Funciones nuevas y mejoradas

Posibilidad de actualizar catálogos persistentes de MCS. Hemos introducido la opción **Actualizar máquinas** para catálogos persistentes de MCS en la interfaz de administración de Configuración com-

pleta. La opción permite administrar la imagen o la plantilla que utiliza el catálogo. Al actualizar un catálogo persistente, tenga en cuenta lo siguiente: Solo las máquinas que agregue al catálogo posteriormente se crearán con la nueva imagen o plantilla. No implementamos la actualización en las máquinas ya existentes del catálogo. Para obtener más información, consulte Actualizar un catálogo.

Opción de aprovisionar máquinas virtuales en un host dedicado de Azure. Hemos agregado una opción, **Usar un grupo de hosts**, a la página **Configuración de catálogo de máquinas > Imagen maestra** de la interfaz de administración de Configuración completa. La opción le permite especificar qué grupo de hosts quiere utilizar al aprovisionar máquinas virtuales en entornos Azure. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Mejorar el rendimiento conservando una VM aprovisionada durante los ciclos de energía. Hemos agregado un parámetro, **Conservar las máquinas virtuales durante los ciclos de energía**, a la página **Configuración de catálogo de máquinas > Parámetros del disco** de la interfaz de administración de Configuración completa. La configuración le permite conservar una máquina virtual aprovisionada cuando tiene lugar un ciclo de energía en entornos Azure. Para obtener más información, consulte Optimización del almacenamiento de MCS. De forma alternativa, puede configurar la función mediante PowerShell. Para obtener más información, consulte Conservación de una máquina virtual aprovisionada durante los ciclos de apagado y encendido.

Vincule un catálogo de máquinas a un conjunto de configuraciones de Workspace Environment Management. Ahora, al crear un catálogo de máquinas, puede vincularlo a un conjunto de configuraciones de Workspace Environment Management. De este modo, podrá utilizar Workspace Environment Management Service para ofrecer la mejor experiencia posible en espacios de trabajo a sus usuarios. También puede optar por vincular el catálogo después de crear el catálogo. Para obtener más información, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Septiembre de 2021

Funciones nuevas y mejoradas

Agregue una descripción informativa para las actualizaciones de imágenes. Ahora puede agregar descripciones informativas acerca de los cambios relacionados con las actualizaciones de imágenes de los catálogos de máquinas. Esta funcionalidad resulta útil para los administradores que quieren agregar etiquetas descriptivas al actualizar una imagen utilizada por un catálogo, por ejemplo, *Office 365 instalado*. Con los comandos de PowerShell, puede crear y ver estos mensajes. Para obtener más información, consulte Agregar descripciones a una imagen.

Integración de Azure VMware Solution (AVS). Citrix Virtual Apps and Desktops Service admite AVS, Azure VMware Solution. AVS proporciona una infraestructura de la nube que contiene clústeres de

vSphere creados por Azure. Aproveche Citrix Virtual Apps and Desktops Service para usar AVS en el aprovisionamiento de la carga de trabajo de VDA del mismo modo que utilizaría vSphere en entornos locales. Para obtener más información, consulte Integración de Azure VMware Solution.

El mismo grupo de recursos para varios catálogos. Ahora puede utilizar el mismo grupo de recursos para actualizar y crear catálogos en Citrix Virtual Apps and Desktops Service. Este proceso:

- Se aplica a cualquier grupo de recursos que contenga uno o varios catálogos de máquinas.
- Admite grupos de recursos que Machine Creation Services no crea.
- Crea la máquina virtual y los recursos asociados.
- Elimina recursos del grupo de recursos cuando se quita la máquina virtual o el catálogo.

Para obtener más información, consulte Grupos de recursos de Azure.

Obtenga información de las máquinas virtuales de Azure, instantáneas, el disco del sistema operativo y la definición de imagen de la galería. Puede mostrar información sobre una máquina virtual de Azure, el disco del SO, la instantánea y la definición de imágenes de galería. Esta información se muestra para los recursos de la imagen maestra cuando se asigna un catálogo de máquinas. Utilice esta funcionalidad para ver y seleccionar una imagen de Linux o Windows. Para obtener más información, consulte Obtener información de las máquinas virtuales de Azure, instantáneas, el disco del sistema operativo y la definición de imagen de la galería.

Nueva actualización para la Configuración automatizada. La Configuración automatizada se ha actualizado a una nueva versión, con funciones que incluyen:

- Compatibilidad con Machines Creation Services (MCS): Ahora la Configuración automatizada admite catálogos MCS. Para obtener más información, consulte Descripción de la migración de catálogos aprovisionados de Machine Creation Services.

Otras actualizaciones a la Configuración automatizada incluyen:

- Compatibilidad con zonas mejoradas al prerrellenar el archivo ZoneMapping.yml con los nombres de las zonas locales durante la exportación y ubicaciones de recursos de la nube al realizar la copia de seguridad.
- StoreFront se ha convertido en un componente administrable de alto nivel. Antes de esto, StoreFront se administraba como parte de los grupos de entrega. Esta separación facilita la fusión de sitios.
- Se cambió `AddMachinesOnly` por `MergeMachines` para que coincida con el patrón de las opciones de fusión actuales y nuevas.
- Se agregó el uso del archivo SecurityClient.csv para importar los campos ClientId y Secret al crear y actualizar CustomerInfo.yml cuando se utilizan los cmdlets de compatibilidad.
- Se agregó la migración de preferencias de zona de usuario.
- Se corrigió la función del plano de control japonés.
- Otras correcciones y mejoras.

Descargue la Configuración automatizada en Descargas de Citrix. Para obtener más información sobre la Configuración automatizada, consulte Migrar la configuración a Citrix Cloud.

Hay más opciones de programación disponibles con programaciones de reinicios. Ahora, la interfaz de administración de Configuración completa le ofrece opciones adicionales para controlar el momento en que se producen los reinicios programados. Además de las programaciones de reinicios periódicos diarios, ahora puede establecer patrones de periodicidad semanales y mensuales. Para obtener más información, consulte Crear una programación de reinicios.

Conserve columnas personalizadas que degradan el rendimiento. Antes, en el nodo **Buscar** de la interfaz de administración de Configuración completa, las columnas personalizadas que degradaban el rendimiento desaparecían después de actualizar la ventana del explorador o después de cerrar sesión en la consola y, a continuación, iniciaba sesión de nuevo. Ahora puede controlar si se conservan esas columnas personalizadas. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Use la herramienta de Configuración automatizada para restaurar y hacer copias de seguridad. Agregamos un nodo, **Copia de seguridad y restauración**, a la interfaz de administración de Configuración completa. Ese nodo combina todos los recursos relacionados con la herramienta de Configuración automatizada, incluida información sobre:

- Programar copias de seguridad automatizadas de la configuración de Citrix Virtual Apps and Desktops mediante un solo comando
- Restaurar una copia de seguridad anterior si fuera necesario
- Realizar y restaurar copias de seguridad granularmente
- Otros casos de uso disponibles

Para obtener más información, consulte la documentación de la Configuración automatizada.

Compatibilidad con catálogos que no están unidos a ningún dominio. Agregamos un tipo de identidad, **No unido a un dominio**, a la página **Configuración de catálogo de máquinas > Identidades de las máquinas** de la interfaz de administración de Configuración completa. Con ese tipo de identidad, puede usar MCS para crear máquinas que no estén unidas a ningún dominio. Para obtener más información, consulte Crear catálogos de máquinas.

Compatibilidad con el uso de perfiles de máquina. Agregamos una opción, **Usar un perfil de máquina**, a la página **Configuración de catálogo de máquinas > Imagen maestra** de la interfaz de administración de Configuración completa. Esta opción le permite especificar el perfil de máquina del que quiere que las máquinas virtuales hereden la configuración al crearlas en entornos de Azure. Las máquinas virtuales del catálogo pueden heredar configuraciones del perfil de máquina seleccionado. Entre los ejemplos de configuraciones se incluyen:

- Redes aceleradas
- Diagnóstico de arranque

- Almacenamiento en caché de discos de host (relacionado con discos de SO y de E/S de MCS)
- Tamaño de máquina (a menos que se especifique lo contrario)
- Etiquetas colocadas en la máquina virtual

Para obtener más información, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Compatibilidad con Windows Server 2022. Requiere VDA 2106, como mínimo.

Agosto de 2021

Funciones nuevas y mejoradas

Se ha ampliado el número de elementos que se pueden ordenar, de 500 a 5000. En el nodo **Búsqueda** de la interfaz de administración de Configuración completa, ahora puede ordenar hasta 5000 elementos por cualquier encabezado de columna. Cuando el número de elementos supera los 5000, utilice filtros para reducirlo a 5000 o menos y permitir la ordenación. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Compatibilidad con tipos de almacenamiento de Azure adicionales. Ahora puede seleccionar distintos tipos de almacenamiento para máquinas virtuales en entornos Azure a través de MCS. Para obtener más información, consulte Tipos de almacenamiento.

Compatibilidad con la selección del tipo de almacenamiento para los discos de caché de reescritura. En la interfaz de administración de Configuración completa, al crear un catálogo de MCS, ahora puede seleccionar el tipo de almacenamiento para el disco de caché de reescritura. Los tipos de almacenamiento disponibles incluyen: SSD Premium, SSD estándar y HDD estándar. Para obtener más información, consulte Crear catálogos de máquinas.

Apagado de las máquinas suspendidas. En la interfaz **Administrar > Configuración completa**, hemos agregado una opción, **Al no reconectarse en (minutos)**, a la página **Parámetros por carga** de la interfaz de usuario Administrar Autoscale para grupos de entrega con SO de sesión única. La opción está disponible después de seleccionar **Suspender**, lo que le permite especificar cuándo apagar las máquinas suspendidas. Las máquinas suspendidas permanecen disponibles para los usuarios desconectados cuando se vuelven a conectar, pero no están disponibles para nuevos usuarios. El apagado de las máquinas vuelve a hacerlas disponibles para manejar las cargas de trabajo. Para obtener más información, consulte Autoscale.

Se ha ampliado la compatibilidad para permitir el uso de archivos CSV para agregar máquinas en bloque a un catálogo. En la interfaz **Administrar > Configuración completa**, ahora puede utilizar un archivo CSV para agregar en bloque máquinas ya presentes en su centro de datos a un catálogo con funciones de administración de energía de dichas máquinas. Para obtener más información, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

Julio de 2021

Funciones nuevas y mejoradas

Registros de configuración. La interfaz de usuario de **Registros** en **Administrar > Configuración completa** ha cambiado. Las tres fichas siguientes comprenden la interfaz:

- **Eventos** (anteriormente, registro de configuración). Esta ficha le permite hacer seguimiento de los cambios de configuración y las actividades administrativas.
- **Tareas**. Esta ficha le permite ver las tareas relacionadas con las operaciones de un catálogo de máquinas.
- **API**. Esta ficha le permite ver las solicitudes de API de REST realizadas durante un período de tiempo determinado.

Para obtener más información, consulte Registro de configuraciones.

Autoscale ahora le proporciona opciones de tiempo de espera de sesión dinámico. Esto le permite configurar los tiempos de espera de sesión por desconexión y por inactividad para los tiempos de uso de horas punta y horas normales con el fin de lograr una purga más rápida de las máquinas y ahorrar costes. Para obtener más información, consulte Tiempos de espera de sesión dinámicos.

Compatibilidad con claves de cifrado administradas por el cliente (CMEK) de Google Cloud Platform (GCP). Ahora puede usar CMEK de Google con catálogos de MCS. CMEK proporciona un mayor control sobre las claves utilizadas para cifrar datos dentro de un proyecto de Google Cloud. Para obtener más información, consulte Claves de cifrado administradas por el cliente (CMEK). Para configurar esta función, consulte Uso de claves de cifrado administradas por el cliente (CMEK). La función está disponible en la página **Configuración de catálogo de máquinas > Parámetros del disco** de la interfaz **Administrar > Configuración completa** .

> **Nota:**
>
> Esta funcionalidad está disponible como Tech Preview.

Actualizaciones de la ficha Administrar. Hemos actualizado las opciones del menú de la ficha **Administrar**:

- **Configuración completa**: Antes esta opción le llevaba a la consola antigua. Ahora le lleva a la nueva consola web (Web Studio). La consola web contiene las mismas funciones que la consola antigua e incluye varias mejoras. Le recomendamos empezar a usarla.
- **Configuración antigua**: Esta opción le lleva a la consola antigua, que está programada para retirarse en septiembre de 2021. Después de eso, **Configuración completa** será la única interfaz que ofrezca acceso a toda la gama de acciones de configuración y administración.

Ahora Web Studio permite elegir una conexión de administración de energía para los catálogos de acceso con Remote PC. Antes podía utilizar Studio para crear una conexión de host Wake on LAN

a su ubicación de recursos (al seleccionar **Wake on LAN para Remote PC** como tipo de conexión). Sin embargo, PowerShell era su única opción para asociar esa conexión a un catálogo de acceso con Remote PC. Ahora puede usar Studio para ello. Para obtener más información, consulte Configurar Wake on LAN en la interfaz de Configuración completa.

Junio de 2021

Funciones nuevas y mejoradas

Acceda a imágenes de Shared Image Gallery de Azure. Ahora, al crear un catálogo de máquinas, puede acceder a imágenes de Shared Image Gallery de Azure en la pantalla Imagen maestra. Para obtener más información, consulte Acceder a imágenes desde Shared Image Gallery de Azure.

Máquinas virtuales blindadas en Google Cloud Platform (GCP). Puede aprovisionar máquinas virtuales blindadas en GCP. Una máquina virtual blindada se ve reforzada por un conjunto de controles de seguridad que proporcionan integridad verificable de sus instancias de Compute Engine, con prestaciones avanzadas de seguridad de plataforma como el arranque seguro, un módulo de plataforma virtual de confianza, firmware UEFI y la supervisión de la integridad. Para obtener más información, consulte Shield VMs.

Aplique HTTPS o HTTP. Utilice parámetros de Registro para aplicar el tráfico HTTPS o HTTP a través de XML Service.

Utilice siempre SSD estándar para un disco de identidad a fin de reducir los costes en entornos de Azure. Los catálogos de máquinas utilizan el tipo de almacenamiento SSD estándar para los discos de identidad. Los discos SSD estándar de Azure son una opción de almacenamiento rentable optimizada para cargas de trabajo que necesitan un rendimiento uniforme en niveles más bajos de operaciones IOPS. Para obtener más información sobre los tipos de almacenamiento, consulte Imagen maestra de Azure Resource Manager.

> **Nota:**
>
> Para obtener más información sobre los precios de los discos administrados de Azure, consulte Managed Disks pricing.

Nuevas funciones disponibles en Web Studio. Ahora, están disponibles las siguientes funciones en la consola web:

- **Ahora Studio admite la autenticación en Azure para crear una entidad principal de servicio**. Ahora puede establecer una conexión de host con Azure mediante la autenticación en Azure para crear una entidad principal de servicio. Así, ya no se necesita crear manualmente una entidad principal de servicio en la suscripción de Azure antes de crear una conexión en Studio. Para obtener información, consulte Entornos de virtualización para Azure Resource Manager.

- **Ahora Studio permite clonar catálogos de máquinas existentes**. Esta función le permite clonar un catálogo de máquinas existente para utilizarlo como plantilla para uno nuevo, lo que elimina la necesidad de crear un catálogo similar desde cero. Al clonar un catálogo, no se pueden cambiar los parámetros asociados a la administración de máquinas y del sistema operativo. El catálogo clonado hereda esos parámetros del original. Para obtener más información, consulte Clonar un catálogo.
- **Ya disponible un nuevo nodo denominado Parámetros en el panel de navegación de Studio**. El nodo **Parámetros** le permite configurar los parámetros que se aplican a todo el sitio (la implementación de un producto de Citrix Virtual Apps and Desktops Service). Están disponibles estos parámetros:
  - **Equilibrar la carga de catálogos multisesión**. Seleccione la opción de equilibrio de carga que satisfaga sus necesidades. Este parámetro se aplica a todos los catálogos. Antes, para acceder a esta función, hacía clic en el icono de engranaje situado en la esquina superior derecha de la consola. Para obtener más información, consulte Equilibrar la carga de las máquinas.
- **Experiencia de búsqueda mejorada en Studio**. Esta versión mejora la experiencia de búsqueda en Studio. Al utilizar filtros para realizar una búsqueda avanzada, la ventana Agregar filtros aparece en primer plano sin modificar la vista del fondo. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.
- **Posibilidad de suspender y reanudar las máquinas virtuales de Google Cloud en MCS**. Ahora puede suspender y reanudar las máquinas virtuales de Google Cloud en MCS tal y como lo haría con cualquier máquina virtual. Para obtener más información, consulte Administrar grupos de entrega. Para habilitar esta capacidad, establezca los permisos `compute.instances.suspend` y `compute.instances.resume` en la cuenta de servicio de Google Cloud. La función de administrador de procesos (Compute Admin) incluye estos permisos.

  En Citrix Virtual Apps and Desktops, también puede utilizar el comando `New-BrokerHostingPowerAct` de PowerShell para suspender y reanudar las máquinas virtuales. Para obtener más información, consulte New-Brokerhostingpoweraction.

  Google Cloud aplica algunas limitaciones en el tipo y la configuración de las instancias que se pueden suspender. Para obtener información adicional, consulta Suspending and resuming an instance en el sitio de Google Cloud.

Mayo de 2021

Funciones nuevas y mejoradas

Reconexión de sesiones después de desconectarse de una máquina en modo de mantenimiento. Antes, cuando los usuarios de escritorios de sesión única (VDI) agrupados (aleatorios) se desconectaban de una máquina en modo de mantenimiento, no se permitía la reconexión de sesiones a ninguna máquina del grupo. Las máquinas multisesión y las máquinas estáticas de sesión única siempre permitían la reconexión de sesiones en esa circunstancia.

Ahora, mediante PowerShell, puede controlar al nivel del grupo de entrega si se permite la reconexión de sesiones tras una desconexión en una máquina en modo de mantenimiento. Esto se aplica a todos los VDA del grupo (tanto sesión única como multisesión).

Para obtener información detallada, consulte Reconexión de sesiones de control al desconectarse de la máquina en modo de mantenimiento.

Disponibilidad del sondeo de aplicaciones y del sondeo de escritorios en todas las ediciones de Citrix Virtual Apps and Desktops Service. Además de la disponibilidad existente en la edición **Premium**, el sondeo de aplicaciones y el sondeo de escritorios ya están disponibles en las ediciones de **Citrix Virtual Apps Advanced Service** y **Citrix Virtual Apps and Desktops Advanced Service**.

Nuevas funciones disponibles en Web Studio. Ahora, está disponible la siguiente función en la consola web:

- **Studio ahora admite la selección de Zonas de disponibilidad de Azure**. Anteriormente, PowerShell era la única alternativa para aprovisionar máquinas en una zona de disponibilidad específica en entornos de Azure. Al utilizar Studio para crear un catálogo de máquinas, ahora puede seleccionar una o varias zonas de disponibilidad en las que quiera aprovisionar máquinas. Si no se especifica ninguna zona, Machine Creation Services (MCS) deja que Azure coloque las máquinas dentro de la región. Si se especifica más de una zona, MCS distribuye aleatoriamente las máquinas entre ellas. Para obtener más información, consulte Aprovisionar máquinas en zonas de disponibilidad especificadas.

Disco efímero de Azure. Citrix Virtual Apps and Desktops Service admite discos efímeros de Azure. Un disco efímero le permite reutilizar el disco de caché para almacenar el disco del sistema operativo de una máquina virtual habilitada para Azure. Esta funcionalidad es útil en entornos de Azure que requieren un disco SSD de mayor rendimiento, en lugar de un disco HDD estándar.

> **Nota:**
>
> Los catálogos persistentes no admiten discos de SO efímeros. Además, al utilizar esta funcionalidad, tenga en cuenta que el disco de alto rendimiento representa un coste adicional. Es conveniente reutilizar el disco de caché para almacenar el disco del sistema operativo, en lugar de

> pagar por un disco administrado extra.

Los discos de SO efímeros requieren que el esquema de aprovisionamiento use discos administrados y una Shared Image Gallery. Para obtener más información, consulte Discos efímeros de Azure.

Rendimiento mejorado para los VDA administrados por MCS en Azure. Citrix Virtual Apps and Desktops Service mejora el rendimiento de los VDA administrados con Machine Creation Services (MCS) en Azure. Esta mejora cambia los valores predeterminados de *Acciones simultáneas absolutas* para la conexión de host a 500, y de *Máximo de acciones nuevas por minuto* para la conexión de host a 2000. No se requieren tareas de configuración manual para aprovechar esta mejora. Para obtener más información, consulte Limitación de Azure.

Nuevas funciones disponibles en Comprobación de estado de Cloud. Comprobación de estado de Cloud se ha actualizado a una nueva versión, con funciones que incluyen:

- **Detección automática de máquinas VDA**. Comprobación de estado de Cloud ahora puede detectar y obtener automáticamente los VDA de las implementaciones de Citrix Virtual Apps and Desktops Service. Para obtener más información, consulte Obtener máquinas VDA.
- **Programación de comprobaciones de estado**. Comprobación de estado de Cloud ahora le permite configurar programaciones para realizar comprobaciones de estado periódicas. Para obtener más información, consulte Programador de Comprobación de estado de Cloud.
- **Información de la versión de Comprobación de estado de Cloud** Ahora puede comprobar qué versión de Comprobación de estado de Cloud está utilizando. Para ver la información de la versión, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la ventana principal de Comprobación de estado de Cloud.
- **Corrección automática**. Comprobación de estado de Cloud ahora admite detectar y corregir automáticamente ciertos problemas identificados en las máquinas en las que se está ejecutando. Para obtener más información, consulte Corrección automática.

  > **Nota:**
  >
  > La corrección automática está disponible como Tech Preview.

Abril de 2021

Funciones nuevas y mejoradas

Obtener instancias dinámicas con la API de AWS. Citrix Virtual Apps and Desktops Service ahora consulta a AWS para obtener tipos de instancias dinámicamente. Esta funcionalidad elimina la necesidad de crear un archivo `InstanceTypes.xml` personalizado para aquellos clientes que quieren utilizar tamaños de máquina distintos de los definidos en Citrix Virtual Apps and Desktops Service. Esta información la proporcionaba anteriormente el archivo `InstanceTypes.xml`. Para facilitar este acceso

dinámico a los tipos de instancias de AWS disponibles, los usuarios deben actualizar los permisos de sus entidades principales de servicio para incluir los permisos `ec2:DescribeInstanceTypes`. Para ofrecer compatibilidad con versiones anteriores a los clientes que optan por no actualizar los permisos de sus entidades principales de servicio, se utilizan los tipos de instancias de AWS enumerados en `InstanceTypes.xml`. Este proceso genera un mensaje de advertencia en el registro de CDF de MCS.

> **Nota:**
>
> Citrix Studio no muestra el mensaje de advertencia incluido en el registro de CDF.

Para obtener más información sobre los permisos, consulte Definir permisos de IAM y Acerca de los permisos de AWS.

Nuevas funciones disponibles en Web Studio. Ahora, está disponible la siguiente función en la consola web:

- **Studio ahora muestra la fecha y hora de su zona horaria**. Anteriormente, Studio solo mostraba la fecha y la hora según el reloj del sistema y la zona horaria. Studio ahora admite mostrar la fecha y la hora locales en su zona horaria cuando pasa el puntero del mouse sobre un elemento de evento. El tiempo se expresa en estándar UTC.

Compatibilidad con E/S de MCS en máquinas virtuales de Azure sin almacenamiento temporal. La E/S de MCS ahora admite la creación de catálogos de máquinas para máquinas virtuales que no tienen discos temporales ni almacenamiento conectado. Con esta compatibilidad:

- La instantánea (disco administrado) se obtiene de la máquina virtual de origen *sin* almacenamiento temporal. Las máquinas virtuales del catálogo de máquinas no tienen almacenamiento temporal.
- La instantánea (disco administrado) se obtiene de la máquina virtual de origen *con* almacenamiento temporal. Las máquinas virtuales del catálogo de máquinas tienen almacenamiento temporal.

Para obtener más información, consulte Optimización del almacenamiento de Machine Creation Services (MCS).

Nuevas funciones disponibles en Web Studio. Ahora, está disponible la siguiente función en la consola web:

- **Forzar cierre de sesión**. Autoscale ahora permite forzar el cierre de sesiones en máquinas cuando se alcanza el período de gracia establecido, posibilitando el apagado de la máquina. Esto permite que Autoscale apague las máquinas mucho más rápidamente, lo que reduce los costes. Puede enviar notificaciones a los usuarios antes de que se cierre la sesión. Para obtener más información, consulte Autoscale.

Nueva actualización para la Configuración automatizada. La Configuración automatizada se ha actualizado a una nueva versión, con funciones que incluyen:

- **Fusión de varios sitios**: Puede fusionar varios sitios en uno y evitar conflictos entre nombres mediante prefijos y sufijos. Para obtener más información, consulte Fusionar varios sitios en uno.
- **Activación del sitio**: Puede elegir si es la implementación local o en la nube la que controla recursos, como programaciones de reinicio y esquemas de energía. Para obtener más información, consulte Activar sitios.

Otras actualizaciones a la Configuración automatizada incluyen:

- La capacidad de migrar roles y ámbitos de administrador.
- Un parámetro `Quiet` para seleccionar cmdlets y suprimir el registro de la consola.
- Un parámetro `SecurityFileFolder` que permite colocar el archivo CvadAcSecurity.yml en un recurso compartido de red seguro que requiere autenticación.
- La capacidad de filtrar por nombre de máquina en catálogos de máquinas y grupos de entrega.
- Mejoras en los parámetros de selección de componentes para utilizar el método de parámetro modificador, que elimina la necesidad de agregar `$true` tras el nombre del componente.
- Un nuevo cmdlet (`New-CvadAcZipInfoForSupport`) para comprimir todos los archivos de registro y enviarlos a asistencia técnica de Citrix.

Descargue la Configuración automatizada en Descargas de Citrix. Para obtener más información sobre la Configuración automatizada, consulte Migración a la nube.

Preservación de las instancias de GCP en los ciclos de energía. Las instancias no persistentes de Google Cloud Platform (GCP) ya no se eliminan al apagar las máquinas. En su lugar, las instancias se preservan entre ciclos de energía. Al apagar una instancia no persistente, el disco del SO se desactiva y se elimina. Al encender la instancia, el disco del SO se vuelve a crear desde el disco base y se conecta a la instancia existente.

Compatibilidad con imágenes de Azure Gen2. Ahora puede aprovisionar un catálogo de VM de 2.ª generación mediante una instantánea de 2.ª generación o un disco administrado de 2.ª generación para acortar los tiempos de arranque. Para obtener más información, consulte Crear catálogos de máquinas. Estos sistemas operativos son compatibles con las imágenes de 2.ª generación de Azure:

- Windows Server 2019, 2016, 2012 y 2012 R2
- Windows 10

> **Nota:**
>
> No se pueden crear catálogos de máquinas de 2.ª generación mediante una instantánea o un

> disco administrado de 1.ª generación. Del mismo modo, tampoco se pueden crear catálogos de máquinas de 1.ª generación mediante una instantánea o un disco administrado de 2.ª generación. Para obtener más información, consulte Compatibilidad con máquinas virtuales de 2.ª generación en Azure.

Inhabilitación de cuentas de almacenamiento de tablas. Machine Creation Services (MCS) ya no crea cuentas de almacenamiento de tablas para catálogos que usan discos administrados al aprovisionar agentes VDA en Azure. Para obtener más información, consulte Azure Table Storage.

Eliminación de bloqueos en las cuentas de almacenamiento. Al crear un catálogo en Azure con un disco administrado, ya no se crea una cuenta de almacenamiento. Las cuentas de almacenamiento creadas para catálogos existentes no cambian. Este cambio solo se aplica a los discos administrados. En el caso de los discos no administrados, no hay cambios en su comportamiento existente. Machine Creation Services (MCS) continúa creando bloqueos y cuentas de almacenamiento.

Nuevas funciones disponibles en Web Studio. Ahora, están disponibles las siguientes funciones en la consola web:

- **Utilizar una clave de cifrado administrada por el cliente para cifrar datos en las máquinas**. Ahora Studio agrega un parámetro denominado **Clave de cifrado administrada por el cliente** a la página **Configuración de catálogo de máquinas > Parámetros del disco**. Este parámetro permite elegir si quiere cifrar datos en las máquinas que se aprovisionarán en el catálogo. Para obtener más información, consulte Clave de cifrado administrada por el cliente.
- **Ahora Studio permite restringir Autoscale a máquinas etiquetadas**. Antes tenía que usar PowerShell para restringir Autoscale a determinadas máquinas de un grupo de entrega. Ahora también puede usar Studio. Para obtener más información, consulte Restringir Autoscale a determinadas máquinas en un grupo de entrega.

Marzo de 2021

Funciones nuevas y mejoradas

Hosts dedicados de Azure. Los hosts dedicados de Azure le permiten aprovisionar a un solo cliente máquinas virtuales en hardware dedicado. Al utilizar un host dedicado, Azure garantiza que las máquinas virtuales sean las únicas máquinas activas en ese host. Esto proporciona más control y visibilidad a los clientes, lo que garantiza el cumplimiento de sus normas o requisitos de seguridad interna. Se requiere un grupo de hosts de Azure preconfigurado, en la región de la unidad de alojamiento, al utilizar el parámetro `HostGroupId`. Además, se requiere la ubicación automática de Azure. Para obtener más información, consulte Hosts dedicados de Azure.

> **Sugerencia:**
>
> Al usar hosts dedicados de Azure, la selección de la **zona de disponibilidad de Azure** no tiene ningún efecto. La máquina virtual se ubica mediante el proceso de ubicación automática de Azure.

Compatibilidad con el cifrado del lado del servidor de Azure. Citrix Virtual Apps and Desktops Service admite claves de cifrado administradas por el cliente para los discos administrados por Azure. Gracias a esta compatibilidad, puede satisfacer los requisitos organizativos y de conformidad mediante el cifrado de los discos administrados del catálogo de máquinas con su propia clave de cifrado. Para obtener más información, consulte Cifrado del lado del servidor de Azure.

Aprovisionar máquinas en zonas de disponibilidad especificadas en Azure. Ahora puede aprovisionar máquinas en una zona de disponibilidad específica en entornos de Azure. Con esta funcionalidad:

- Puede especificar una o varias zonas de disponibilidad en Azure. Si se proporciona más de una zona, las máquinas se distribuyen equitativamente entre las zonas proporcionadas.
- La máquina virtual y el disco correspondiente se colocan en la zona (o zonas) especificadas.
- Puede buscar zonas de disponibilidad para una oferta de servicio o región determinadas. Las zonas de disponibilidad válidas se muestran mediante comandos de PowerShell. Los elementos de inventario de las ofertas de servicios se pueden ver con `Get-Item`.

Para obtener más información, consulte Aprovisionamiento de máquinas en zonas de disponibilidad especificadas en Azure.

Nuevas funciones disponibles en Web Studio. Ahora, están disponibles las siguientes funciones en la consola web:

- **Studio ahora admite la asociación de aplicaciones a iconos personalizados**. Antes, se tenía que usar PowerShell para agregar iconos personalizados y utilizarlos con aplicaciones publicadas. Ahora también puede usar Studio para hacer eso. Para obtener más información, consulte Administrar grupos de aplicaciones.
- **Ahora, Studio admite la aplicación de etiquetas a catálogos de máquinas**. Anteriormente, se podía usar Studio para crear o eliminar etiquetas para utilizarlas con un catálogo. Sin embargo, se tenía que usar PowerShell para aplicar etiquetas al catálogo. Ahora también puede usar Studio para aplicar o quitar una etiqueta de un catálogo, de la misma manera que con los grupos de entrega. Para obtener más información, consulte Aplicar etiquetas a catálogos de máquinas.
- **Ahora Studio permite cambiar entre los modos "equilibrio de carga horizontal"y "equilibrio de carga vertical"**. Antes, PowerShell era la única opción para cambiar entre estos modos. Ahora Studio le ofrece más flexibilidad para controlar el equilibrio de la carga de máquinas con SO multisesión. Para obtener más información, consulte Equilibrar la carga de las máquinas.

- **Studio ahora admite la inclusión de máquinas en modo de mantenimiento para las programaciones de reinicios**. Anteriormente, PowerShell era la única opción para configurar reinicios programados para máquinas en modo de mantenimiento. Ahora también puede usar Studio para decidir si incluir esas máquinas en una programación de reinicios. Para obtener más información, consulte Crear una programación de reinicios.
- **Studio ahora admite la configuración de Wake on LAN para el acceso con Remote PC**. Anteriormente, se tenía que usar PowerShell para configurar Wake on LAN para el acceso con Remote PC. Ahora también puede usar Studio para configurar la función. Para obtener más información, consulte Configurar Wake on LAN.
- **Studio ahora admite la aplicación de propiedades de instancias de AWS y el etiquetado de recursos operativos**. Al crear un catálogo para aprovisionar máquinas mediante MCS en AWS, puede decidir si aplicar las propiedades de etiqueta y el rol de IAM a esas máquinas. También puede decidir si aplicar etiquetas de máquina a los recursos operativos. Dispone de estas dos opciones:

  - **Aplicar propiedades de plantilla de máquina a máquinas virtuales**
  - **Aplicar etiquetas de máquina a recursos operativos**

  Para obtener más información, consulte Aplicar propiedades de instancias de AWS y etiquetar recursos operativos.

Shared Image Gallery de Azure. Citrix Virtual Apps and Desktops Service admite Shared Image Gallery de Azure como un repositorio de imágenes publicadas para máquinas aprovisionadas con MCS en Azure. Los administradores tienen la opción de almacenar una imagen maestra en la galería para acelerar la creación e hidratación de discos de SO. Este proceso mejora los tiempos de arranque y de inicio de aplicaciones en las máquinas virtuales no persistentes. Para obtener más información sobre esta función, consulte Shared Image Gallery de Azure.

> **Nota:**
>
> La funcionalidad Shared Image Gallery es compatible con discos administrados. No está disponible para catálogos de máquinas antiguos.

Depósitos de almacenamiento creados en la misma región de Google Cloud Platform que el catálogo de máquinas. En versiones anteriores, MCS creaba depósitos de almacenamiento temporales durante el aprovisionamiento como parte del proceso de carga de discos. Estos depósitos abarcaban varias regiones, las cuales Google define como una gran zona geográfica que contiene dos o más lugares geográficos. Estos depósitos temporales residían en la ubicación geográfica de Estados Unidos, independientemente de dónde se aprovisionara el catálogo. Ahora MCS crea depósitos de almacenamiento en la misma región en la que se aprovisionan los catálogos. Los depósitos de almacenamiento ya no son temporales: permanecen en su proyecto de Google Cloud Platform una vez completado el proceso de aprovisionamiento. Las futuras operaciones de aprovisionamiento utilizan

el depósito de almacenamiento existente, si existe uno en esa región. Se crea otro depósito de almacenamiento si no existe ninguno en la región especificada.

Febrero de 2021

Funciones nuevas y mejoradas

Compatibilidad con imágenes de Azure Gen2. Ahora puede aprovisionar discos administrados mediante máquinas virtuales de 2.ª generación en entornos de Azure para acortar los tiempos de arranque. Están disponibles los siguientes sistemas operativos:

- Windows Server 2019, 2016, 2012 y 2012 R2
- Windows 10

> **Nota:**
>
> Con esta compatibilidad, solo se admite un subconjunto de máquinas virtuales. Por ejemplo, algunas máquinas virtuales pueden ser de 1.ª generación y de 2.ª generación, mientras que otras solo pueden ser de 1.ª generación. Para obtener más información, consulte Compatibilidad con máquinas virtuales de 2.ª generación en Azure.

Programaciones de reinicio de máquinas. Ahora, Citrix Studio contiene una nueva opción denominada **Reiniciar todas las máquinas después de las sesiones de purga** en el menú **Duración del reinicio**. Esta opción permite elegir si reiniciar todas las máquinas después de purgar todas las sesiones. Cuando llega el momento del reinicio, las máquinas se ponen en estado de purga y se reinician tras cerrarse todas las sesiones. Para obtener más información, consulte Crear una programación de reinicios.

Nuevas funciones disponibles en Web Studio. Ahora, están disponibles las siguientes funciones en la consola web:

- **Ahora, Studio admite el uso de archivos CSV para agregar máquinas en bloque a un catálogo**. Esta función permite utilizar un archivo CSV para:
  - Agregar máquinas en bloque a un catálogo de SO multisesión o SO de sesión única cuando la energía de las máquinas no se administra a través de Studio.
  - Agregar máquinas en bloque a un catálogo de acceso con Remote PC. Anteriormente, se tenían que elegir unidades organizativas para agregar máquinas en bloque a un catálogo de acceso con Remote PC. Sin embargo, hacerlo no es fácil en casos con restricciones de estructura de las unidades organizativas. Esta función ofrece más flexibilidad para agregar máquinas en bloque. Puede agregar máquinas solamente (para utilizarlas con asignaciones automáticas de usuarios) o agregar máquinas junto con asignaciones de usuarios.

Para obtener más información, consulte Crear catálogos de máquinas y Administrar catálogos de máquinas.

- **Desarrollo ampliado para Azure administrado por Citrix.** Azure administrado por Citrix ahora está disponible en las siguientes ediciones de Citrix Virtual Apps and Desktops Service: Standard para Azure, Advanced, Premium y Workspace Premium Plus.
- **Colocar imágenes maestras en Shared Image Gallery de Azure**. Ahora, Studio ofrece la opción de colocar imágenes maestras en Shared Image Gallery (SIG) de Azure. SIG es un repositorio para administrar y compartir imágenes. Le permite poner sus imágenes a disposición de toda la organización. Le recomendamos almacenar una imagen maestra en SIG al crear grandes catálogos de máquinas no persistentes, ya que, así, los discos del SO de VDA se pueden restablecer más rápidamente. Para obtener información, consulte Entornos de virtualización para Azure Resource Manager.
- **Conservación de los discos del sistema para catálogos de máquinas de MCS en Azure**. Ahora Studio le permite controlar el hecho de conservar los discos del sistema para los VDA durante los ciclos de energía. Normalmente, el disco del sistema se elimina al apagar la máquina y se vuelve a crear al encenderla. Esto garantiza que el disco esté siempre limpio, pero alarga los reinicios de las máquinas virtuales. Si las escrituras del sistema se redirigen a la caché y se vuelven a escribir en el disco de caché, el disco del sistema no cambia. Para evitar la recreación innecesaria de discos, use la opción **Conservar el disco del sistema durante los ciclos de energía**, disponible en la página **Configuración de catálogo de máquinas > Parámetros del disco**. Al habilitar esta opción, se reducen los tiempos de reinicio de las máquinas virtuales, pero aumenta los costes de almacenamiento. Esta opción puede ser útil en casos donde un entorno contiene cargas de trabajo con tiempos de reinicio que dependen de otros factores. Para obtener más información, consulte Optimización del almacenamiento de MCS.
- **Ahora Studio admite la creación de catálogos de máquinas de MCS con disco persistente de caché con reescritura**. Antes, PowerShell era la única opción para crear un catálogo con disco de caché persistente con reescritura. Ahora puede usar Studio para controlar si el disco de caché con reescritura persiste para las máquinas virtuales aprovisionadas en Azure al crear un catálogo. Si se inhabilita, el disco de caché con reescritura se elimina durante cada ciclo de energía para ahorrar costes de almacenamiento, lo que provoca la pérdida de los datos redirigidos al disco. Para conservar dichos datos, habilite la opción **Usar disco persistente de caché con reescritura**, disponible en la página **Configuración de catálogo de máquinas > Parámetros del disco**. Para obtener más información, consulte Optimización del almacenamiento de MCS.

App Protection para Citrix Virtual Apps and Desktops Service con StoreFront. Para obtener más información, consulte App Protection.

Enero de 2021

Nuevas funciones disponibles en Web Studio. Ahora, están disponibles las siguientes funciones en la consola web:

- **Studio ahora admite la asociación de aplicaciones a iconos personalizados**. Antes, se tenía que usar PowerShell para agregar iconos personalizados y utilizarlos con aplicaciones publicadas. Ahora también puede usar Studio para hacer eso. Para obtener más información, consulte Administrar grupos de aplicaciones.
- **Ahora, Studio admite la aplicación de etiquetas a catálogos de máquinas**. Anteriormente, se podía usar Studio para crear o eliminar etiquetas para utilizarlas con un catálogo. Sin embargo, se tenía que usar PowerShell para aplicar etiquetas al catálogo. Ahora también puede usar Studio para aplicar o quitar una etiqueta de un catálogo, de la misma manera que con los grupos de entrega. Para obtener más información, consulte Aplicar etiquetas a catálogos de máquinas.
- **Ahora Studio permite cambiar entre los modos "equilibrio de carga horizontal"y "equilibrio de carga vertical"**. Antes, PowerShell era la única opción para cambiar entre estos modos. Ahora Studio le ofrece más flexibilidad para controlar el equilibrio de la carga de máquinas con SO multisesión. Para obtener más información, consulte Equilibrar la carga de las máquinas.
- **Studio ahora admite la inclusión de máquinas en modo de mantenimiento para las programaciones de reinicios**. Anteriormente, PowerShell era la única opción para configurar reinicios programados para máquinas en modo de mantenimiento. Ahora también puede usar Studio para decidir si incluir esas máquinas en una programación de reinicios. Para obtener más información, consulte Crear una programación de reinicios.
- **Studio ahora admite la configuración de Wake on LAN para el acceso con Remote PC**. Anteriormente, se tenía que usar PowerShell para configurar Wake on LAN para el acceso con Remote PC. Ahora también puede usar Studio para configurar la función. Para obtener más información, consulte Configurar Wake on LAN.
- **Studio ahora admite la aplicación de propiedades de instancias de AWS y el etiquetado de recursos operativos**. Al crear un catálogo para aprovisionar máquinas mediante MCS en AWS, puede decidir si aplicar las propiedades de etiqueta y el rol de IAM a esas máquinas. También puede decidir si aplicar etiquetas de máquina a los recursos operativos. Dispone de estas dos opciones:

  - **Aplicar propiedades de plantilla de máquina a máquinas virtuales**
  - **Aplicar etiquetas de máquina a recursos operativos**

  Para obtener más información, consulte Aplicar propiedades de instancias de AWS y etiquetar recursos operativos.

- **Host dedicado de AWS**. Ahora Citrix Studio agrega una opción llamada **Usar host dedicado** a la página **Configuración de catálogo de máquinas > Seguridad**. Esta configuración es adecuada para implementaciones con restricciones de licencias o requisitos de seguridad que exigen el uso de un host dedicado. Con un host dedicado, dispone de un host físico completo, y se factura por hora. Al tener ese host, puede poner en marcha tantas instancias de EC2 como permita dicho host sin cargos adicionales. Para obtener más información, consulte Arrendamiento de AWS.
- **Ahora Studio permite ejecutar programaciones de reinicios inmediatamente**. Ahora Studio le permite ejecutar programaciones de reinicios inmediatamente para reiniciar todas las máquinas correspondientes de la programación. Para obtener más información, consulte Ejecutar inmediatamente una programación de reinicios.
- **Autoscale.** Autoscale ofrece las siguientes mejoras y funciones nuevas:
  - **Ahora Studio permite ver máquinas en estado de purga**. Antes, PowerShell era la única opción para identificar máquinas en estado de purga. Ahora puede usar Studio para identificar máquinas que se hallen en estado de purga. Para obtener más información, consulte Mostrar máquinas en estado de purga.
  - **Ahora, Studio admite la definición de horas de máxima actividad con una precisión de 30 minutos para grupos de entrega de VDI**. Antes, se tenía que usar PowerShell para definir las horas de máxima actividad de los días incluidos en una programación con una precisión de 30 minutos para los grupos de entrega de VDI. Ahora también puede usar Studio para hacer eso. Con lo que puede establecer por separado la cantidad mínima de máquinas activas en un grupo de entrega de VDI para cada media hora del día.

Shared Image Gallery de Azure. Citrix Virtual Apps and Desktops Service admite Shared Image Gallery de Azure como un repositorio de imágenes publicadas para máquinas aprovisionadas con MCS en Azure. Los administradores tienen la opción de almacenar una imagen en la galería para acelerar la creación e hidratación de discos de SO a partir de la imagen maestra. Este proceso mejora los tiempos de arranque y de inicio de aplicaciones en las máquinas virtuales no persistentes.

La galería contiene estos tres elementos:

- Galería. Las imágenes se almacenan aquí. MCS crea una galería para cada catálogo de máquinas.
- Definición de imagen de la galería. Esta definición incluye información (el tipo y el estado del sistema operativo, la región de Azure) sobre la imagen maestra. MCS crea una definición de imagen para cada imagen maestra creada para el catálogo.
- Versión de la imagen de la galería. Cada imagen de Shared Image Gallery puede tener varias versiones, y cada versión puede tener varias réplicas en diferentes regiones. Cada réplica es una copia completa de la imagen maestra. Citrix Virtual Apps and Desktops Service siempre crea una versión de imagen Standard_LRS (versión 1.0.0) para cada imagen con la cantidad adecuada de

réplicas en la región del catálogo. Esta configuración se basa en la cantidad de máquinas del catálogo, el índice de réplicas y el máximo de réplicas que se hayan configurado.

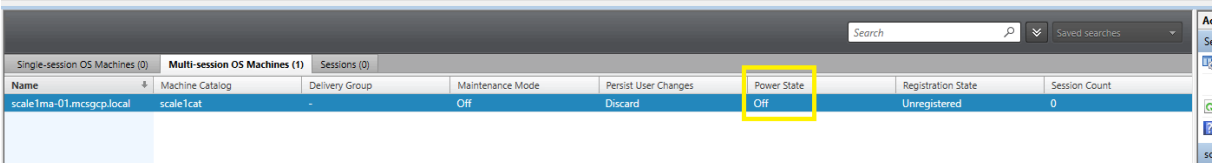
> **Nota:**
>
> La funcionalidad Shared Image Gallery solo funciona con discos administrados. No está disponible para catálogos de máquinas antiguos.

Para obtener más información sobre esta función, consulte Configurar Shared Image Gallery.

Depósitos de almacenamiento creados en la misma región de Google Cloud Platform que el catálogo de máquinas. En versiones anteriores, MCS creaba depósitos de almacenamiento temporales durante el aprovisionamiento como parte del proceso de carga de discos. Estos depósitos abarcaban varias regiones, las cuales Google define como una gran zona geográfica que contiene dos o más lugares geográficos. Estos depósitos temporales residían en la ubicación geográfica de Estados Unidos, independientemente de dónde se aprovisionara el catálogo. Ahora MCS crea depósitos de almacenamiento en la misma región en la que se aprovisionan los catálogos. Los depósitos de almacenamiento ya no son temporales: permanecen en su proyecto de Google Cloud Platform una vez completado el proceso de aprovisionamiento. Las futuras operaciones de aprovisionamiento utilizan el depósito de almacenamiento existente. Si hay alguno en esa región, se crea otro depósito de almacenamiento si no existe ninguno en la región especificada.

Opción de PowerShell que establece la opción predeterminada para reutilizar los VDA agrupados durante una interrupción del servicio. Una nueva opción de comando de PowerShell (`-DefaultReuseMachinesWithoutShutdownInOutage`) amplía, de forma predeterminada, la capacidad de reutilizar los VDA de escritorio agrupados que no se hayan apagado durante una interrupción del servicio. Véase Compatibilidad con aplicaciones y escritorios.

Aprovisionamiento a demanda en Google Cloud Platform. Citrix Virtual Apps and Desktops Service actualiza el modo en que Google Cloud Platform (GCP) aprovisiona catálogos de máquinas. Al crear un catálogo de máquinas, la instancia de máquina correspondiente no se crea en GCP y el estado de energía se establece en **inactiva**. Las máquinas no se aprovisionan en el momento de la creación del catálogo, sino la primera vez que se encienden. Por ejemplo, después de crear un catálogo, el estado de energía de la máquina virtual se establece en **inactiva**:

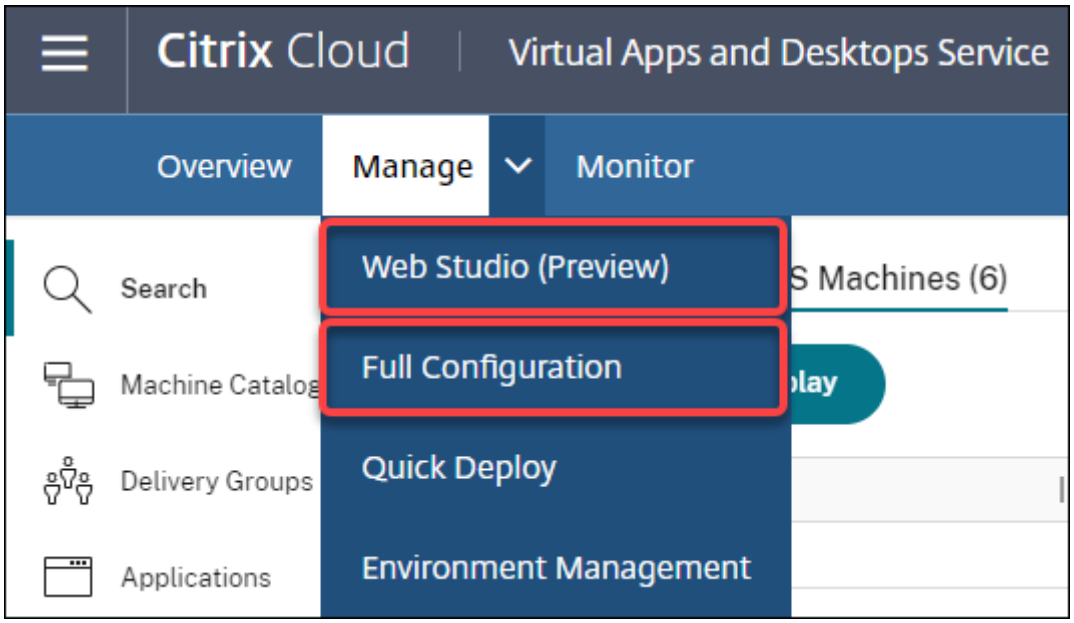


Diciembre de 2020

Funciones nuevas y mejoradas

Web Studio está disponible como Tech Preview. Ya hay disponible una nueva consola web. Estamos en proceso de migrar todo el conjunto de funcionalidades de Studio de la antigua consola a la nueva consola web. La consola web normalmente responde más rápido que la antigua consola. De forma predeterminada, inicia sesión automáticamente en la consola web. Puede cambiar fácilmente entre la consola web y la antigua consola desde la ficha **Administrar** para realizar las tareas de configuración o de administración de sitios. Haga clic en la flecha hacia abajo situada junto a **Administrar** y seleccione una opción:

- **Web Studio (Tech Preview)**. Le lleva a la nueva consola web.
- **Configuración completa**. Le lleva a la antigua consola.



Estas funciones solo están disponibles en la consola web:

- **Compatibilidad con el tipo de disco SSD estándar para Azure**. Ahora Studio es compatible con el tipo de disco SSD estándar. Los discos SSD estándar de Azure son una opción de almacenamiento rentable optimizada para cargas de trabajo que necesitan un rendimiento uniforme en niveles más bajos de operaciones IOPS. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen maestra de Azure Resource Manager.
- **Ahora Studio admite la configuración de la demora del apagado para grupos de entrega estáticos de VDI**. Antes solo podía configurar la demora del apagado de los grupos de entrega estáticos de VDI a través del SDK de PowerShell. Ahora Studio le permite configurar la demora del apagado en la interfaz de usuario de Autoscale para grupos de entrega estáticos de VDI. Para obtener más información, consulte Autoscale.

Octubre de 2020

Funciones nuevas y mejoradas

Descartar múltiples alertas de Hypervisor. Citrix Monitor ahora permite descartar automáticamente las alertas de Hypervisor que tienen más de un día. Para obtener más información, consulte Supervisar alertas de hipervisor.

Elimine la dirección IP externa. Ya no es necesaria una dirección IP externa en una máquina virtual temporal que se utiliza para preparar una imagen aprovisionada en Google Cloud Platform (GCP). Esta dirección IP externa permite que la máquina virtual temporal acceda a la API pública de Google para completar el proceso de aprovisionamiento.

Habilite el Acceso privado a Google para permitir que la máquina virtual acceda a la API pública de Google directamente desde la subred. Para obtener más información, consulte Habilitar el acceso privado a Google.

El nuevo modelo define cómo se administran las identidades de las máquinas. Las identidades de las máquinas utilizadas en los catálogos de máquinas se han administrado y mantenido mediante Active Directory. Todas las máquinas creadas por MCS se unirán ahora a Active Directory. El nuevo modelo de Citrix Virtual Apps and Desktops Service define la forma en que se administran las identidades de las máquinas. Este modelo permite la creación de catálogos de máquinas mediante *grupos de trabajo* o máquinas no unidas a dominios.

> **Sugerencia:**
>
> Esta funcionalidad admite un nuevo servicio de identidad, *FMA trust*, agregado a Citrix Cloud para máquinas no unidas a un dominio.

MCS se comunica con el nuevo servicio de confianza de FMA para administrar las identidades. La información de identidad se almacena en el disco de identidad como una pareja de GUID y clave privada, en lugar del SID de dominio y el paradigma de contraseña de cuenta de equipo que utiliza Active Directory. Los VDA que utilizan máquinas no unidas a un dominio utilizan esta combinación de GUID y clave privada para el registro de intermediarios. Para obtener más información, consulte Configurar la compatibilidad con catálogos no unidos a ningún dominio.

Utilice la carga directa para los discos administrados de Azure. Esta versión le permite usar la carga directa al crear discos administrados en un entorno de Azure. Esta funcionalidad reduce los costes asociados a cuentas de almacenamiento adicionales. Ya no es necesario almacenar el VHD en una cuenta de almacenamiento antes de convertirlo en un disco administrado. Además, la carga directa elimina la necesidad de conectar un disco administrado vacío a una máquina virtual. La carga directa en un disco administrado de Azure simplifica el flujo de trabajo al permitirle copiar directamente un VHD local para utilizarlo como disco administrado. Los discos administrados compatibles incluyen HDD estándar, SSD estándar y SSD Premium.

Para obtener más información sobre esta función, consulte el blog de Microsoft Azure.

Para obtener más información sobre los discos administrados de Azure, consulte la página de documentación.

Grupo de recursos único en Azure. Ahora puede crear y usar un solo grupo de recursos de Azure para actualizar y crear catálogos en Citrix Virtual Apps and Desktops. Esta mejora se aplica tanto a las entidades principales de servicio de ámbito completo como a las de ámbito limitado.
Se eliminó la limitación anterior de 240 VM/800 discos administrados por grupo de recursos de Azure. Ya no hay límite en la cantidad de máquinas virtuales, discos administrados, instantáneas e imágenes por grupo de recursos de Azure.

Para obtener información, consulte Entornos de virtualización para Azure Resource Manager.

Septiembre de 2020

Funciones nuevas y mejoradas

Distribución rápida La nueva función Distribución rápida reemplaza a la Distribución rápida de Azure anterior. La nueva función ofrece una forma rápida de empezar a usar Citrix Virtual Apps and Desktops Service con Microsoft Azure. Puede usar Quick Deploy para entregar escritorios y aplicaciones, y configurar el acceso con Remote PC.

Administrador de sesión (rol integrado). Citrix Studio ahora agrega un nuevo rol integrado denominado **Administrador de sesión**. El rol permite a un administrador ver grupos de entrega y administrar sus sesiones y máquinas asociadas en la página **Filtros** de la ficha **Supervisar**. Con esta función, puede configurar los permisos de acceso de los administradores existentes o los administradores que invite para que puedan desempeñar sus roles en la organización. Para obtener más información sobre el rol integrado, consulte Roles y ámbitos integrados. Para obtener información acerca de cómo asignar el rol integrado a un administrador, consulte Administración delegada y supervisión.

Para obtener un nivel más detallado de control sobre el acceso a la página **Filtros** relacionada con sesiones y máquinas, cree un rol personalizado y seleccione una de las siguientes opciones para el objeto Director: **Página Ver filtros: Solo máquinas**, **página Ver filtros: Solo sesiones**. Para obtener información sobre cómo crear un rol personalizado, consulte Crear y administrar roles.

Compatibilidad con un nuevo tipo de máquina. Esta versión agrega compatibilidad con las series NV v4 y DA v4 de máquinas AMD, al configurar discos premium para un catálogo de máquinas. Para obtener más información, consulte Crear grupos de entrega.

Agosto de 2020

Funciones nuevas y mejoradas

Acceso limitado al SDK remoto de PowerShell durante una interrupción del servicio. Anteriormente, no se podía usar comandos de PowerShell durante una interrupción. Ahora, la Caché de host local permite un acceso limitado al SDK remoto de PowerShell durante una interrupción del servicio. Consulte Elementos no disponibles durante una interrupción del servicio.

Compatibilidad con dos ediciones nuevas de Citrix Virtual Apps and Desktops Service. Ahora Citrix Monitor admite dos nuevas ediciones de Citrix Virtual Apps and Desktops Service: el servicio **Citrix Virtual Apps Advanced** y el servicio **Citrix Virtual Apps and Desktops Advanced**. Para obtener más información, consulte la Tabla de compatibilidad de funciones de Citrix Monitor.

Compatibilidad con Virtual Private Cloud (VPC) compartida en Google Cloud Platform. Citrix Virtual Apps and Desktops Service admite la nube privada virtual compartida en Google Cloud Platform como un recurso de host. Puede utilizar Machine Creation Services (MCS) para aprovisionar máquinas en una nube VPC compartida, y administrarlas desde Citrix Studio. Para obtener información sobre la VPC compartida, consulte Nube privada virtual compartida.

Selección de zonas para Google Cloud Platform. Citrix Virtual Apps and Desktops Service admite la selección de zonas en Google Cloud Platform. Esta función permite a los administradores especificar una o varias zonas dentro de una región para la creación del catálogo.

Para las máquinas virtuales de tipo arrendatario único, la selección de zonas ofrece a los administradores la posibilidad de colocar nodos de arrendatario único en las zonas que deseen. En el caso de las máquinas virtuales que no son de tipo arrendatario único, la selección de zonas ofrece la posibilidad de colocar máquinas virtuales de manera determinante en las zonas deseadas, lo que proporciona una gran flexibilidad en el diseño de la implementación. Para obtener información de configuración, consulte Habilitar selección de zona.

Asimismo:

- El arrendamiento único ofrece acceso exclusivo a un nodo de arrendatario único (un servidor físico de Compute Engine dedicado a alojar solo las máquinas virtuales de un proyecto). Estos nodos permiten agrupar las máquinas virtuales en el mismo hardware, o separar unas máquinas virtuales de las máquinas virtuales de otros proyectos.
- Los nodos de arrendatario único pueden contribuir a cumplir los requisitos de hardware dedicado para casos donde se pide utilizar su propia licencia (Bring Your Own License o BYOL). Además, permiten cumplir con los requisitos de privacidad, seguridad y directivas de control de acceso a la red, como la normativa HIPAA.

> **Nota:**
>
> El arrendamiento único es la única manera de usar implementaciones de VDI con Windows 10 en Google Cloud. VDI de servidor también admite este método. Dispone de una descripción detallada del arrendamiento único en el sitio de documentación de Google.

Rendimiento de arranque mejorado para discos de sistema de Azure. Esta versión admite un rendimiento de arranque mejorado para implementaciones de Citrix Cloud que usan Azure cuando E/S de MCS está habilitado. De esta manera, puede conservar el disco del sistema. Eso ofrece las siguientes ventajas:

- Las máquinas virtuales y las aplicaciones ahora se arrancan y se inician con un rendimiento similar al de la imagen maestra.
- Se reduce el consumo de cuota de API, la eliminación y la creación del disco del sistema, y la demora de transición de estado causada al eliminar una VM.

Por ejemplo, utilice la propiedad personalizada `PersistOSDisk` de PowerShell en el comando `New-ProvScheme` para configurar esta función.

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>'
<!--NeedCopy-->
```

Para obtener más información de configuración, consulte Mejorar el rendimiento del arranque.

July 2020

Funciones nuevas y mejoradas

Compatibilidad con acceso pormenorizado basado en roles a la página Filtros. Citrix Studio proporciona ahora un control más detallado sobre el acceso a la página **Supervisar > Filtros** cuando se crea un rol personalizado. Concretamente, puede asignar permisos para ver cualquier combinación de **máquinas**, **sesiones**, **conexiones**e **instancias de aplicación** en relación con un rol personalizado. A continuación, se indican cuatro opciones adicionales para el objeto **Director** en la ventana **Crear rol**:

- Página Ver Filtros: Solo instancias de aplicación
- Página Ver Filtros: Solo conexiones
- Página Ver Filtros: Solo máquinas
- Página Ver Filtros: Solo sesiones

Para obtener información sobre cómo crear roles, consulte Crear y administrar roles.

Compatibilidad con demora de apagado para máquinas VDI asignadas (solo PowerShell). En versiones anteriores, la demora del apagado solo se aplicaba a máquinas sin asignar. A partir de esta versión, la demora del apagado se aplica tanto a las máquinas asignadas como a las no asignadas. Para obtener más información, consulte Cómo administra Autoscale la energía de las máquinas.

Compatibilidad con licencias de cliente de Windows. Ahora Citrix Virtual Apps and Desktops Service admite el uso de licencias de cliente de Windows para aprovisionar máquinas virtuales en Azure. Para utilizar máquinas virtuales con Windows 10 en Azure, compruebe que el contrato de licencias por volumen con Microsoft cumple los requisitos para este uso. Para obtener más información, consulte Crear un catálogo de máquinas con una imagen maestra de Azure Resource Manager.

Mayo de 2020

Funciones nuevas y mejoradas

Programaciones de reinicio de las máquinas. Ahora puede indicar si una programación de reinicio afecta a las máquinas que se hallan en el modo de mantenimiento. Esta función solo está disponible en PowerShell. Para obtener más información, consulte Reinicios programados para máquinas en modo de mantenimiento.

Disponibilidad de recursos. Ahora puede garantizar la disponibilidad de recursos durante una interrupción del servicio sin tener que publicar recursos en cada zona (ubicación de recursos). Para obtener más información, consulte Disponibilidad de recursos.

Abril de 2020

Funciones nuevas y mejoradas

Granularidad de programación mejorada para grupos de entrega de VDI (solo PowerShell). Autoscale ahora permite definir las horas punta para los días incluidos en una programación a un nivel granular de 30 minutos. Puede establecer por separado la cantidad mínima de máquinas activas en un grupo de entrega de VDI para cada media hora del día. Además, Autoscale ahora puede aumentar o reducir el número de máquinas encendidas en los grupos de entrega de VDI en franjas de media hora, en lugar de una hora. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.

Detección de MTU. El protocolo Citrix Enlightened Data Transport (EDT) ahora incluye prestaciones de detección de MTU. La detección de MTU permite a EDT determinar y establecer automáticamente el tamaño de carga útil para la sesión. Esta función permite que la sesión ICA se ajuste a redes con requisitos de unidad de transmisión máxima (MTU) o tamaño máximo de segmento (MSS) no estándar. La capacidad de ajuste evita la fragmentación de paquetes que puede dar lugar a una degradación del rendimiento o un error al establecer una sesión ICA. Para esta actualización, se requiere la aplicación Citrix Workspace 1911 para Windows como mínimo. Si se utiliza Citrix Gateway, la versión mínima de firmware de Citrix ADC requerida es 13.0.52.24 o 12.1.56.22. Para obtener más información, consulte Detección de MTU en EDT.

Marzo de 2020

Funciones nuevas y mejoradas

Métricas de dispositivo de destino de PVS. Citrix Monitor proporciona ahora un panel de métricas de dispositivos de destino de PVS en la página Detalles de la máquina. Utilice el panel para ver el estado de los dispositivos de destino de Provisioning, tanto en máquinas con sistema operativo de sesión única como multisesión. En este panel, hay disponibles varias métricas de Red, Arranque y Caché. Estas métricas le ayudan a supervisar y solucionar problemas en los dispositivos de destino de PVS para asegurarse de que funcionen correctamente. Para obtener más información, consulte Métricas de dispositivo de destino de PVS.

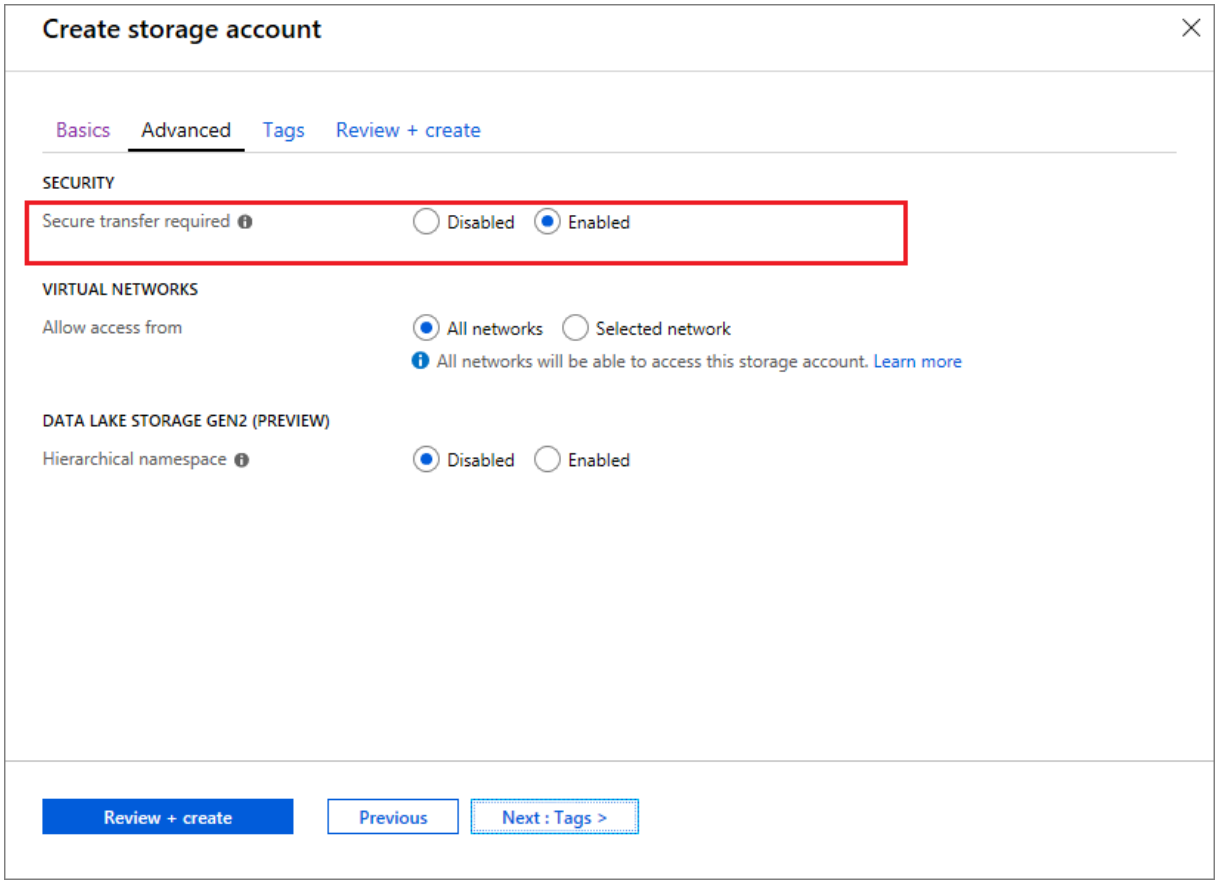
Captura de propiedades de instancia de AWS. MCS lee ahora las propiedades de la instancia de la que se obtuvo la imagen AMI y aplica el rol y etiquetas de IAM (Administración de acceso e identidad) de la máquina a las máquinas aprovisionadas de un catálogo determinado. Cuando se utiliza esta función opcional, el proceso de creación de catálogos busca la instancia AMI de origen seleccionada, leyendo un conjunto limitado de propiedades. Estas propiedades se almacenan en una plantilla de inicio de AWS, que sirve para aprovisionar las máquinas de ese catálogo. Cualquier máquina del catálogo heredará las propiedades de instancia capturadas. Para obtener más información, consulte Captura de propiedades de instancia de AWS.

Etiquetado de recursos operativos de AWS. Esta versión introduce una opción para etiquetar los recursos creados por los componentes de Citrix durante el aprovisionamiento. Cada etiqueta consta de una clave definida por el cliente y un valor opcional que mejora su capacidad para administrar, buscar y filtrar recursos. Para obtener más información, consulte Etiquetado de recursos operativos de AWS.

Transferencia segura en el almacenamiento de Azure. Machine Creation Services (MCS) ofrece una mejora para las cuentas de almacenamiento creadas por catálogos aprovisionados por MCS en entornos de Azure Resource Manager. Esta mejora habilita automáticamente la propiedad requerida de transferencias seguras. Esta opción mejora la seguridad de la cuenta de almacenamiento porque

permite únicamente solicitudes dirigidas a la cuenta desde conexiones seguras. Para obtener más información, consulte Requisito de transferencia segura para garantizar conexiones seguras en el sitio de Microsoft.

Habilite la propiedad **Se requiere transferencia segura** al crear una cuenta de almacenamiento en Azure:



Compatibilidad con discos administrados SSD de Azure. Machine Creation Services (MCS) admite discos administrados SSD estándar para las máquinas virtuales de Azure. Este tipo de disco ofrece un rendimiento constante y una mejor disponibilidad en comparación con los discos HDD. Para obtener más información, consulte Discos SSD estándar para cargas de trabajo de máquinas virtuales de Azure.

Utilice la propiedad personalizada `StorageAccountType` de PowerShell en el comando `New-ProvScheme` o en el comando `Set-ProvScheme` para configurar esta función:

```
1 <Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"
    true`" /><Property xsi:type=`"StringProperty`" Name=`"
    StorageAccountType`" Value=`"StandardSSD_LRS`" /><Property xsi:type
    =`"StringProperty`" Value=`"Windows_Server`" />
2 <!--NeedCopy-->
```


> **Nota:**
>
> Esta función solo está disponible cuando se utilizan discos administrados, es decir, la propiedad personalizada `UseManagedDisks` está establecida en **true**. Para los discos no administrados, solo se admiten HDD estándar y SSD premium.

Enero de 2020

Funciones nuevas y mejoradas

Barra de idioma en Citrix Studio. A partir de esta versión, Citrix Studio ofrece una barra de idioma para facilitar la asignación correcta del teclado.

- Si el idioma de Citrix Cloud o el idioma de presentación de su explorador está establecido en **inglés** o **japonés**, es posible que la barra de idioma no aparezca.
- Si el idioma de Citrix Cloud o el idioma de presentación de su explorador está establecido en **alemán**, **español**o **francés**, la barra de idioma aparece después de iniciar sesión en Citrix Studio. Hay dos opciones de idioma en la lista de la barra de idioma. Seleccione la opción que coincida con el idioma que aparece en primer lugar en su explorador.

  > **Sugerencia:**
  >
  > - Es posible que el parámetro que configure en la barra de idioma no surta efecto. En este caso, cierre la sesión y vuelva a iniciar sesión.
  > - Es posible que no se puedan introducir ciertos símbolos y caracteres traducidos mediante la barra de idioma. Para resolver el problema, debe configurar el idioma de Citrix Cloud, el idioma del explorador web y la distribución del teclado local. Para obtener más información, consulte el artículo CTX310743 de Knowledge Center.

Temporizador de demora máximo de la programación de reinicios (solo para PowerShell). Si una programación de reinicios de las máquinas de un grupo de entrega no comienza debido a una interrupción de la base de datos del sitio, puede especificar cuánto tiempo se debe esperar a partir de la hora de inicio programada. Si la conexión a la base de datos se restaura durante ese intervalo, comienzan los reinicios. Si la conexión no se restablece durante ese intervalo, los reinicios no comienzan. Para obtener más información, consulte Reinicios programados que se retrasan por una interrupción de la base de datos.

Equilibrio de carga vertical (solo PowerShell). Anteriormente, el servicio utilizaba el equilibrio de carga horizontal para todos los inicios de RDS, que asigna la carga entrante a la máquina RDS con menos carga. Ese sigue siendo el valor predeterminado. Ahora, puede usar PowerShell para habilitar el equilibrio de carga vertical como configuración para todo el sitio.

Cuando se habilita el equilibrio de carga vertical, el intermediario asigna la carga entrante a la máquina con más carga que no ha alcanzado una marca de agua alta. De esta forma, se saturan las máquinas existentes antes de pasar a otras máquinas. A medida que los usuarios se desconectan y liberan las máquinas existentes, se asigna nueva carga a esas máquinas.

El equilibrio de carga horizontal está habilitado de forma predeterminada. Para ver, habilitar o inhabilitar el equilibrio de carga vertical, los cmdlets `Get-BrokerSite` y `Set-BrokerSite` ahora admiten el parámetro `UseVerticalScalingForRdsLaunches`. Para obtener más información, consulte Administrar la carga de las máquinas de un grupo de entrega.

Diciembre de 2019

Funciones nuevas y mejoradas

Servicio para Citrix Service Providers (CSP). Los CSP ahora pueden incluir clientes de arrendatarios en Virtual Apps and Desktops Service, configurar el acceso de administrador de clientes al servicio y proporcionar espacios de trabajo compartidos o dedicados a los usuarios de los clientes mediante dominios federados. Para obtener más información, consulte Citrix Virtual Apps and Desktops Service para Citrix Service Providers.

Asistencia para determinar por qué una máquina está en modo de mantenimiento (solo PowerShell). Con PowerShell, ahora puede determinar por qué una máquina está en modo de mantenimiento. Para ello, utilice el parámetro `-MaintenanceModeReason`. Esta función es útil, al permitir que los administradores solucionen problemas con máquinas en modo de mantenimiento. Para obtener información detallada, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/Broker/Get-BrokerMachine/.

Autoscale. Autoscale ofrece ahora la posibilidad de crear máquinas y eliminarlas dinámicamente. Puede hacer uso de esta función a través de un script de PowerShell. El script le ayuda a aumentar o reducir dinámicamente la cantidad de máquinas del grupo de entrega en función de las condiciones de carga actuales. Para obtener más información, consulte Aprovisionar máquinas de forma dinámica con Autoscale.

Noviembre de 2019

Funciones nuevas y mejoradas

GroomStartHour. Ahora Supervisar admite **GroomStartHour**, una nueva configuración que ayuda a los administradores a determinar el momento del día en que la limpieza debe comenzar. Para obtener más información, consulte la documentación del SDK de Citrix Virtual Apps and Desktops.

Paginación OData. Ahora Supervisar admite la **paginación OData**. Todos los dispositivos de punto final de OData 4 devuelven un máximo de 100 registros por página con un enlace a los siguientes 100 registros en la respuesta. Para obtener más información, consulte Accessing Monitor Service data using the OData 4 endpoint in Citrix Cloud.

Octubre de 2019

Funciones nuevas y mejoradas

App-V. La funcionalidad de App-V ya está disponible en Citrix Cloud. Puede agregar paquetes de App-V al Delivery Controller de su configuración de Citrix Cloud, ya sea en modo de administración única o dual. El *módulo de detección de paquetes de Virtual Apps and Desktops Service*, disponible en las Descargas de Citrix, le permite importar paquetes de App-V y registrar servidores de Microsoft App-V. Las aplicaciones que contienen estarán disponibles para los usuarios. Este módulo de PowerShell le permite registrar servidores de publicación y de administración de Microsoft App-V mediante direcciones URL de DNS, lo que evita la necesidad de que los servidores detrás de los mecanismos de equilibrio de carga se registren con la verdadera dirección URL de su máquina. Para obtener más información, consulte Módulo de detección de Citrix Virtual Apps and Desktops Service para paquetes y servidores de App-V.

Google Cloud Platform. Ahora Citrix Virtual Apps and Desktops Service permite utilizar Machine Creation Services (MCS) para aprovisionar máquinas en Google Cloud Platform (GCP). Para obtener más información, consulte Entornos de virtualización Google Cloud Platform.

Septiembre de 2019

Funciones nuevas y mejoradas

Compatibilidad con VDA para Azure Virtual Desktop. Para ver los sistemas operativos y las versiones de VDA compatibles, consulte VDA en un entorno de Azure Virtual Desktop.

Directiva de energía mejorada. En versiones anteriores, las máquinas VDI que pasaban a un período de tiempo en el que se requería una acción (acción de desconexión="**Suspender**"o "**Apagar**") permanecían encendidas. Este caso se producía si la máquina se desconectaba durante un período de tiempo (horas punta u horas normales) donde no se requería ninguna acción (acción de desconexión="**Nada**").

A partir de esta versión, Autoscale suspende o apaga las máquinas cuando transcurre el tiempo de desconexión especificado, en función de la acción de desconexión configurada para el período de tiempo de destino. Para obtener más información, consulte Administrar la energía de máquinas VDI que pasan a otro período de tiempo con sesiones desconectadas.

Catálogos de máquinas: Etiquetas. Ahora puede usar PowerShell para aplicar etiquetas a catálogos de máquinas. Para obtener más información, consulte Aplicar etiquetas a catálogos de máquinas.

Duración de inicio de sesión. Ahora Supervisar muestra la duración de inicio de sesión dividida en períodos de tiempo de inicio de sesión de la aplicación Workspace e inicio de sesión de VDA. Estos datos le ayudan a comprender y solucionar problemas con una duración elevada para iniciar las sesiones. Además, la duración de cada fase involucrada en el inicio de las sesiones ayuda a solucionar problemas asociados a fases individuales. Por ejemplo, si el tiempo de asignación de unidades es elevado, puede comprobar si todas las unidades válidas se asignan correctamente en el objeto de directiva de grupo o en el script. Esta función está disponible en los VDA 1903 o en versiones posteriores. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión.

Agosto de 2019

Funciones nuevas y mejoradas

Reconexión automática de sesión. La página Sesiones de la ficha Tendencias ahora incluye información sobre la cantidad de reconexiones automáticas. Las reconexiones automáticas se intentan cuando las directivas de fiabilidad de la sesión o de reconexión automática del cliente están activas. La información de reconexión automática le ayuda a ver y solucionar problemas de conexión de red que sufren interrupciones, así como a analizar las redes que tienen una experiencia fluida y sin problemas.

El desglose proporciona información adicional, como la fiabilidad de la sesión o la reconexión automática del cliente, las marcas de tiempo, la dirección IP del dispositivo de punto final o el nombre de la máquina de punto final en la que está instalada la aplicación Workspace. Esta función está disponible para la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, Citrix Receiver para Windows y Citrix Receiver para Mac. Esta función requiere agentes VDA con la versión 1906 o una posterior. Para obtener más información, consulte:

- Sesiones
- Configuraciones de directiva de Reconexión automática de clientes
- Configuraciones de directiva de Fiabilidad de sesiones
- Reconexión automática de sesión

Julio de 2019

Funciones nuevas y mejoradas

Registros de configuración. Ahora puede usar el SDK de PowerShell remoto para eliminar periódicamente el contenido de la base de datos de registros de configuración. Para obtener más información,

consulte Programar la eliminación periódica de datos.

Autoscale. Autoscale proporciona ahora la flexibilidad necesaria para administrar la energía solo en un subconjunto de máquinas de un grupo de entrega. Esta función puede ser útil en casos de uso de "cloud bursting"(ampliación en la nube), en los que quiera utilizar los recursos locales para gestionar las cargas de trabajo antes de usar los basados en la nube para hacer frente a la demanda adicional (es decir, cargas de trabajo en ráfagas). Para obtener más información, consulte Restringir Autoscale a determinadas máquinas en un grupo de entrega.

Acceso a aplicaciones locales y redirección de URL. Citrix Studio le permite ahora agregar la opción Agregar aplicación de acceso local a la interfaz de usuario de Studio para su sitio mediante el SDK de PowerShell. Para obtener más información, consulte Proporcionar acceso solo a las aplicaciones publicadas.

Cambios en el nombre del sistema operativo. Los nombres de sistema operativo han cambiado en las páginas **Crear catálogo de máquinas > Configuración del catálogo de máquinas > Sistema operativo** y **Supervisar**:

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

Duración de Citrix Profile Management en la carga de perfil. Ahora, Supervisar incluye la duración del procesamiento del perfil en la barra Carga de perfil del gráfico Duración de inicio de sesión. Esto es lo que tarda Citrix Profile Management en procesar perfiles de usuario. Esta información ayuda a los administradores a solucionar problemas con la duración elevada de cargas de perfil de manera más precisa. Esta mejora está disponible en VDA 1903 y en versiones posteriores. Para obtener más información, consulte Carga de perfil.

Sondeo de escritorios. El sondeo de escritorios es una función de Citrix Virtual Apps and Desktops Service. Automatiza las comprobaciones de estado de los escritorios virtuales publicados en un sitio, lo que mejora la experiencia del usuario. Para iniciar el sondeo de escritorios, instale y configure Citrix Probe Agent en uno o más dispositivos de punto final. El sondeo de escritorios está disponible para los sitios con licencia Premium. Esta función requiere Citrix Probe Agent 1903 o una versión posterior. Para obtener más información, consulte Sondeo de aplicaciones y escritorios.

> **Nota:**
>
> Ahora Citrix Probe Agent admite TLS 1.2.

Junio de 2019

Funciones nuevas y mejoradas

Restringir por etiquetas. Las etiquetas son cadenas que identifican elementos como, por ejemplo, máquinas, aplicaciones, escritorios, grupos de aplicaciones y directivas. Después de crear una etiqueta y agregarla a un elemento, puede adaptar determinadas operaciones para que solo se apliquen a los elementos que tengan esa etiqueta concreta. Para obtener más información, consulte Grupos de aplicaciones y Etiquetas.

Notificaciones por correo electrónico. Citrix Virtual Apps and Desktops Service envía directamente notificaciones por correo electrónico relacionadas con alertas y sondeos. Esto elimina la necesidad de configurar el servidor de correo electrónico SMTP. La casilla **Preferencias de notificación** está marcada de forma predeterminada, y Citrix Cloud envía notificaciones de alerta a las direcciones de correo electrónico proporcionadas en la sección **Preferencias de notificación**. Asegúrese de que la dirección de correo electrónico `donotreplynotifications@citrix.com` aparece en la lista de direcciones permitidas en la configuración del correo electrónico.

Mayo de 2019

Funciones nuevas y mejoradas

Autoscale. Autoscale es una función de Citrix Virtual Apps and Desktops Service que ofrece una solución robusta y de alto rendimiento para administrar de forma proactiva la energía de sus máquinas. Su objetivo es equilibrar los costes y la experiencia de usuario. Autoscale incorpora la antigua tecnología Smart Scale en la solución de administración de energía de Studio. Para obtener más información, consulte Autoscale. Puede supervisar las métricas de las máquinas administradas por Autoscale desde las páginas Tendencias de la ficha **Supervisar**. Para obtener más información, consulte Supervisar máquinas administradas con Autoscale.

Febrero de 2019

Funciones nuevas y mejoradas

Supervisar alertas de hipervisor. Las alertas de Citrix Hypervisor y VMware vSphere ahora se muestran en la ficha **Supervisar** > **Alertas** para ayudar a supervisar los siguientes estados/parámetros del estado del hipervisor:

- Uso de CPU
- Uso de memoria
- Uso de la red

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

Para obtener más información, consulte la sección Supervisar alertas de hipervisor en Alertas y notificaciones.

Comunicaciones a través de versiones de TLS anteriores. Para mejorar la seguridad del servicio, Citrix bloquea toda comunicación a través de Transport Layer Security (TLS) 1.0 y 1.1 desde el 15 de marzo de 2019 y permite únicamente las comunicaciones a través de TLS 1.2. Para obtener más información, consulte Versiones de TLS. Para obtener una guía completa, consulte CTX247067.

Grupos de aplicaciones. Los grupos de aplicaciones permiten administrar colecciones de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega. Para obtener más información, consulte Crear grupos de aplicaciones.

Rendimiento de inicio de sesión: Desglose de perfiles Ahora, el panel **Duración de inicio de sesión** de la página **Detalles del usuario** que se encuentra en la sección **Supervisar**, incluye un desglose sobre la **fase de carga de los perfiles** del proceso de inicio de sesión. Este desglose de perfiles ofrece información útil sobre los perfiles de usuario para la sesión actual, lo que puede ayudar a los administradores a solucionar problemas de carga de perfiles importantes. Se muestra un texto de ayuda con la siguiente información de perfiles de usuario:

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

Un desglose detallado ofrece información sobre las carpetas individuales, su tamaño y la cantidad de archivos. Esta función solamente está disponible en agentes VDA 1811 y versiones posteriores. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

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

Sondeo de aplicaciones. Esta función automatiza la evaluación del estado de las aplicaciones virtuales publicadas en un sitio.

Para iniciar el sondeo de aplicaciones:

- En una o más máquinas de punto final, instale Citrix Application Probe Agent

- Configure Citrix Application Probe Agent con las credenciales de Citrix Workspace y Citrix Virtual Apps and Desktops Service.
- Configure las aplicaciones que se van a sondear, las máquinas de punto final donde se ejecutará el sondeo y la hora programada del sondeo en **Supervisar** > **Configuración** de Citrix Virtual Apps and Desktops Service.

El agente prueba el inicio de las aplicaciones seleccionadas a través de Citrix Workspace e informa de los resultados del sondeo en la ficha **Supervisar** de Citrix Virtual Apps and Desktops Service en:

- La página Aplicaciones: los datos de las últimas 24 horas y la página **Tendencias** > **Resultados del sondeo de aplicaciones**
- Los datos históricos del sondeo junto con la etapa en la que se produjo el error del sondeo: Accesibilidad de Workspace, Autenticación de Workspace, Enumeración de Workspace, Descarga de ICA o Inicio de aplicación.

El informe de fallo se envía por correo electrónico a las direcciones de configuradas. Puede programar sondeos de aplicaciones para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Así, puede utilizar los resultados para solucionar problemas de forma proactiva relacionados con las aplicaciones aprovisionadas, las máquinas de alojamiento o las conexiones antes de que los usuarios los sufran. Para obtener más información, consulte Sondeo de aplicaciones y escritorios.

Enero de 2019

Funciones nuevas y mejoradas

Administración delegada con ámbito personalizado. La supervisión ahora admite el ámbito personalizado para los roles integrados de administrador delegado. Para obtener más información sobre las funciones integradas disponibles para la supervisión y cómo asignarlas, consulte Roles de administrador delegado.

Diciembre de 2018

Funciones nuevas y mejoradas

La fecha a partir de la cual Citrix bloqueará la comunicación por Transport Layer Security (TLS) 1.0 y 1.1 ha cambiado del 31 de diciembre de 2018 al 31 de enero de 2019. Para obtener más detalles, consulte Versiones TLS retiradas.

Noviembre de 2018

Funciones nuevas y mejoradas

Datos históricos de máquinas, disponibles mediante la API de OData: Los siguientes datos históricos que contienen análisis de máquina ahora están disponibles a través de la API de OData. Esta información se recopila cada hora y se acumula para el día.

- Cantidad de máquinas encendidas (para máquinas con administración de energía)
- Cantidad de máquinas registradas
- Cantidad de máquinas en modo de mantenimiento
- Cantidad total de máquinas

Los datos se agregan para el período de tiempo durante el cual se ejecuta Monitor Service. Para obtener más información sobre uso y ejemplos de la OData API, consulte Citrix Monitor Service 7 1808. El esquema de la base de datos está disponible en Esquema de Monitor Service.

Rendimiento de inicio de sesión: Desglose de la sesión interactiva: El panel **Duración de inicio de sesión** en la vista **Detalles del usuario y de la sesión** incluye información sobre la fase de la **sesión interactiva** del proceso de inicio de sesión. El tiempo empleado para cada una de las tres subfases (**Pre-userinit**, **Userinit** y **Shell**) se muestra en la barra de la **sesión interactiva** como texto de ayuda. Así, se ofrece una solución de problemas más precisa a esta fase del inicio de sesión. También se indica el tiempo acumulado de demora entre las subfases, así como un enlace a la documentación correspondiente. Esta función está disponible en Delivery Controller 7 1808 y versiones posteriores. La barra de desglose de la **sesión interactiva** muestra solamente la duración de la sesión actual. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Rendimiento de inicio de sesión: Desglose de GPO: El panel **Duración de inicio de sesión** de la vista **Detalles del usuario y de la sesión** contiene la duración de los GPO (objetos de directiva de grupo). Este es el tiempo total necesario para aplicar los GPO a la máquina virtual durante el proceso de inicio de sesión. Ahora, puede ver el desglose de cada directiva aplicada por cada CSE (extensión del lado del cliente) como texto de ayuda en la barra de GPO. El desglose muestra el estado y el tiempo empleado en aplicar cada directiva. Esta información adicional facilita la solución de problemas que implican una alta duración de GPO. Las duraciones del desglose representan solo el tiempo de procesamiento de CSE, no se suman al tiempo total de GPO. Esta función está disponible en Delivery Controller 7 1808 y versiones posteriores. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Correcciones

Las consultas de informes personalizados guardadas durante la supervisión no están disponibles después de una actualización de Citrix Cloud. [DNA-23420]

Octubre de 2018

Funciones nuevas y mejoradas

Aplicaciones: límite por máquina. Ahora puede limitar la cantidad de instancias de aplicación por máquina. Este límite se aplica a todas las máquinas existentes en el sitio. Este límite se suma al límite de aplicaciones existente para todos los usuarios en el grupo de entrega y al límite por usuario. Esta capacidad solo está disponible a través de PowerShell, no desde Studio. Para obtener más información, consulte Configurar límites de aplicaciones.

Windows Server 2019. Ahora puede instalar agentes VDA para SO multisesión (anteriormente VDA para SO de servidor) en máquinas con Windows Server 2019, como se indica en Requisitos del sistema.

Septiembre de 2018

Funciones nuevas y mejoradas

Administración delegada. Con la administración delegada, puede configurar los permisos de acceso que todos sus administradores necesitarán en función del rol que desempeñan en la organización. Para obtener más información, consulte Administración delegada. La supervisión admite la asignación de roles integrados. Los roles integrados están disponibles en su totalidad. Para obtener más información sobre los roles integrados disponibles para la supervisión y cómo asignarlos, consulte Roles de administrador delegado.

Registros de configuración. La función "Registros de configuración"permite a los administradores realizar un seguimiento de los cambios de configuración y las actividades administrativas. Para obtener información más detallada, consulte Registros de configuración.

Varios cmdlets de PowerShell en el SDK de PowerShell remoto que estaban antes inhabilitados ahora están habilitados, para usar con Registros de configuración:

- Log:GetLowLevelOperation
- Log:GetHighLevelOperation
- Log:GetSummary
- Log:GetDataStore
- Log:ExportReport

Caché de host local. La función Caché de host local ya está disponible. La función Caché de host local (LHC) permite que las operaciones de intermediación de las conexiones continúen cuando un Cloud Connector de una ubicación de recursos no pueda comunicarse con Citrix Cloud. Para obtener más información, consulte Caché de host local.

Citrix Provisioning. Para aprovisionar agentes VDA, ahora puede usar Citrix Provisioning o Machine Creation Services existente. Para obtener información específica sobre Citrix Provisioning en el entorno de nube, consulte Citrix Provisioning administrado por Citrix Cloud.

Correcciones

En versiones anteriores, cuando se usaba el aprovisionamiento a demanda de Azure, todas las máquinas virtuales se eliminaban cuando se apagaban. Ahora, solo se eliminan las máquinas virtuales agrupadas. Las máquinas virtuales persistentes (dedicadas) no se eliminan cuando se apagan.

Agosto de 2018

- **Nuevos nombres de producto**

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

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

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

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

A continuación, dispone de un resumen rápido:

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

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

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

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

Agradecemos su comprensión durante esta transición.

Para obtener más información detallada sobre nuestros nuevos nombres, consulte https://www.citrix.com/about/citrix-product-guide/.

- **Cambios en los números de versión de productos y componentes**

  Citrix instala y administra la mayoría de los componentes de Citrix Virtual Apps and Desktops, por lo que no tendrá que preocuparse por esos números de versión. Sin embargo, es posible que vea números de versión cuando instale Cloud Connectors e instale o actualice la versión de VDA en ubicaciones de recursos.

  Los números de las versiones de componentes y productos de Citrix Virtual Apps and Desktops se muestran en el formato: **AAMM.*c.m.b***

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

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

  En versiones anteriores (7.18 y versiones anteriores), los números de versión se mostraban en el formato: 7.*versión*, donde el valor "versión"aumentaba de uno en uno con cada versión. Por ejemplo, la versión de VDA después de XenApp y XenDesktop 7.17 era 7.18. Las versiones anteriores (7.18 y anteriores) no se actualizarán al nuevo formato de numeración.

- **Versiones TLS retiradas**. Para mejorar la seguridad de Citrix Virtual Apps and Desktops Service, Citrix bloqueará toda comunicación a través de Transport Layer Security (TLS) 1.0 y 1.1; bloqueo efectivo el 31 de diciembre de 2018. Para obtener más detalles, consulte Versiones TLS retiradas.

- **Entorno de virtualización Google Cloud Platform**. Con Citrix Virtual Apps and Desktops Service, puede administrar manualmente la energía de las máquinas virtuales de Citrix Virtual Apps and Desktops en la plataforma de Google Cloud, llamada Google Cloud Platform (GCP). Para obtener más información, consulte Entornos de virtualización Google Cloud Platform.

Julio de 2018

- **Exportar datos de filtros**. Ahora puede exportar datos de supervisión en tiempo real de la ficha **Supervisar** > **Filtros** a archivos en formato CSV. La función de exportación está disponible en las páginas Máquinas, Sesiones, Conexiones y Filtro para instancias de aplicación. Puede seleccionar un filtro personalizado predefinido o seleccionar criterios de filtro adecuados, elegir columnas requeridas en la tabla y exportar los datos. Se pueden exportar datos de hasta 100 000 registros. Los archivos CSV exportados ofrecen una vista completa de los datos en tiempo real y facilitan el análisis de grandes conjuntos de datos.

Junio de 2018

- **Conexiones con Azure Resource Manager**. En el asistente de creación de conexiones de Studio, seleccionar el entorno de Azure en la página **Conexión** equivale a seleccionar todas las nubes de Azure que sean válidas para la suscripción de Azure que usted tiene. La disponibilidad general del servicio gubernamental de la nube de Azure para Estados Unidos y Alemania reemplaza las versiones Tech Preview de esos dos entornos en versiones anteriores.

Mayo de 2018

- **Distribución rápida de Azure**. Si la ubicación de recursos utiliza máquinas de Azure Resource Manager para entregar aplicaciones y escritorios, ahora tiene la opción de elegir el método de implementación que prefiera:
  - Configuración completa: Este método utiliza la consola de administración de Studio, que le guiará durante la creación de un catálogo de máquinas y posteriormente la creación de un grupo de entrega.
  - Distribución rápida de Azure: Esta nueva opción ofrece una interfaz más sencilla, para una implementación más rápida de aplicaciones y escritorios.
- **Enlace de Citrix Health Assistant.** La página "Detalles de la máquina"de una máquina no registrada en la consola de supervisión ahora contiene el botón **Health Assistant**. Actualmente, el botón enlaza con el artículo Solucionar de problemas de máquinas de la documentación de Citrix y con el artículo Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch de Knowledge Center, desde donde puede descargar la herramienta. Citrix Health Assistant

es una herramienta para solucionar problemas técnicos de configuración en VDA no registrados. La herramienta automatiza varias comprobaciones de estado para identificar las posibles causas de los problemas más comunes en el registro de los VDA, el inicio de sesión y la configuración de la redirección de zonas horarias.

- **Desglose de la sesión interactiva** En la consola de supervisión, ahora la vista **Detalles de usuario > Duración del inicio de sesión** incluye información sobre la fase de la **sesión interactiva** del proceso de inicio de sesión. Para ofrecer una solución más detallada de esta fase del inicio de sesión, ahora la **sesión interactiva** cuenta con tres subfases: **Pre-userinit**, **Userinit** y **Shell**. En esta versión, al pasar el mouse sobre la **sesión interactiva**, se muestran las subfases y un enlace a la documentación. Para obtener una descripción de las subfases y cómo mejorar el rendimiento de cada fase, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

Marzo de 2018

- **Predicción de instancias de aplicación (Preview).** Esta es la primera función de supervisión basada en análisis predictivo. La predicción de patrones en el uso de recursos es importante para que los administradores organicen los recursos y la cantidad de licencias que requiera cada recurso. La función "Predicción de instancias de aplicación"indica la cantidad probable de instancias de aplicación alojadas que se lanzarán por sitio o grupo de entrega a lo largo del tiempo. Para hacer la predicción, se utilizan algoritmos de aprendizaje automático basados en modelos creados con datos históricos existentes. El nivel de tolerancia indica la calidad de la predicción.

  Para obtener más información, consulte Predicción de instancias de aplicación en Director. Puede compartir sus comentarios sobre la utilidad y la usabilidad de esta función en el foro de Citrix Cloud.

- **API de grupos de entrega: Tech Preview**

  En la Tech Preview de las API de grupos de entrega, se ofrece un conjunto de interfaces API de REST que puede usar para automatizar la administración de grupos de entrega. Puede ver y probar el conjunto completo de las API disponibles en la documentación de las API de Citrix Cloud, en https://developer.cloud.com/.

- **Autenticación en Web Studio**

  En Citrix Cloud, la consola de administración del servicio ahora usa un token de portador para autenticar a los clientes. El token de portador es necesario para autenticar el acceso a la API de REST de los grupos de entrega.

- **Acceso a los datos de Monitor Service mediante la API de OData 4 (función en fase Preview).**

  Puede crear paneles personalizados de supervisión e informes basados en los datos consultados en Monitor Service mediante el dispositivo de punto final OData 4. OData 4 se basa en la

API web de ASP .NET y admite consultas de agregación. Use su nombre de usuario y su token de portador de Citrix Cloud para acceder a los datos con el dispositivo de punto final de la versión 4. Para obtener más información y ver ejemplos, consulte Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

Puede compartir sus comentarios sobre la utilidad de esta función en el foro de Citrix Cloud.

Correcciones

- Puede mover y eliminar carpetas de aplicaciones, y cambiarles el nombre. [#STUD-2376]

Enero de 2018

- **Verificación de licencias de RDS** La función de crear catálogos que contienen máquinas con SO de servidor Windows ahora incluye una comprobación automática de licencias RDS. Se muestran todas las licencias RDS emitidas que se hayan encontrado, para que se puedan tomar los pasos adecuados para evitar una interrupción del servicio. Para obtener más información, consulte Crear catálogos de máquinas.
- **Acceda a la consola de la máquina desde Supervisar.** El panel Detalles de la máquina de la sección Supervisar ahora proporciona acceso a las consolas de las máquinas alojadas en el hipervisor XenServer 7.3. Ahora puede solucionar problemas en los VDA directamente desde la sección Supervisar. Para obtener más información, consulte Acceder a la consola de la máquina en Solucionar problemas de máquinas.

Diciembre de 2017

Funciones nuevas y mejoradas

- **Citrix Workspace.** Citrix Workspace ahora está disponible para clientes **nuevos** de XenApp y XenDesktop Service. Para obtener más información, consulte Configuración del espacio de trabajo.
- **Análisis de aplicaciones.** Ahora puede analizar y supervisar eficazmente el rendimiento de las aplicaciones gracias a la nueva página Análisis de aplicaciones disponible desde la ficha **Supervisar** > **Aplicaciones**. La página ofrece una vista centralizada del estado y el uso de todas las aplicaciones publicadas en el sitio. Muestra diferentes métricas, como la cantidad de instancias por aplicación y los fallos y errores asociados a las aplicaciones publicadas. Esta función requiere agentes VDA con la versión 7.15 o una posterior.

  Para obtener más información, consulte la sección Analíticas de aplicaciones en Supervisar.

Noviembre de 2017

Funciones nuevas y mejoradas

- **Caché de host local.** La función Caché de host local (LHC) permite que las operaciones de intermediación de las conexiones continúen cuando un Cloud Connector de una ubicación de recursos no pueda comunicarse con Citrix Cloud. Para obtener más información, consulte Caché de host local.
- **Azure Managed Disks.** Los discos administrados de Azure (Azure Managed Disks) se utilizan ahora de manera predeterminada para máquinas virtuales aprovisionadas con MCS en entornos de Azure Resource Manager. Si lo prefiere, puede usar cuentas de almacenamiento convencionales. Para obtener más información, consulte Entornos de virtualización para Microsoft Azure Resource Manager.
- **Administrador de asistencia técnica (Help Desk).** Al administrar los administradores de servicios para una cuenta de cliente de Citrix Cloud, ahora tiene una nueva opción: Administrador de asistencia técnica. Un administrador de asistencia técnica puede acceder a las funciones de Supervisar del servicio. Para obtener más detalles, consulte Administrar.

Correcciones

- Ahora puede usar el asistente de la consola de administración de servicios para crear un catálogo de máquinas de Acceso con Remote PC. En versiones anteriores, era necesario usar un cmdlet de PowerShell para crear un catálogo (como se documenta en CTX220737). Después, había que volver a la consola de administración para crear un grupo de entrega. Ahora, se puede crear el catálogo y el grupo de entrega secuencialmente en la consola de administración.
- Los catálogos creados por MCS pueden usar cuentas de máquinas existentes de Active Directory. [#DNA-24566]
- Cuando se supervisa una implementación, al desplazarse por una tabla ordenada de **Tendencias > Sesiones** se muestran resultados precisos. [DNA-51257]

Más información

- Problemas conocidos.
- Para obtener información sobre el software de terceros que está incluido en el servicio, consulte Avisos de terceros.

Problemas conocidos

May 17, 2024

Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) presenta estos problemas conocidos:

- En un entorno de VMware alojado en AWS, no se pueden crear catálogos de máquinas de MCS si la imagen maestra está habilitada para vTPM. Para obtener asistencia de VMware, consulte Get Support. [PMCS-37603]
- Es posible que las pantallas de los monitores no se carguen si la URL de Pendo `https://citrix-cloud-content.customer.pendo.io/` está bloqueada.
  [DIR-18482]
- Aparecerá un error si ejecuta un comando con `XDHyp:\` en el SDK de PowerShell remoto. Para solucionar este problema:

  1. Ejecute un comando con `Hyp`. Por ejemplo: `Get-HypServiceStatus`
  2. Ejecute un comando con `XDHyp:\`. Por ejemplo: `Get-ChildItem XDHyp:\Connections\`

  [BRK-13723]
- Tras los cambios en la arquitectura de la versión 2209 de Citrix DaaS, los iconos predeterminados de los escritorios de Windows y de las aplicaciones implementadas antes de esta versión cambiaron a iconos genéricos de escritorio de PC. Este cambio solo se aplica a escritorios y aplicaciones que apuntan al icono predeterminado. Si quiere cambiar los iconos de nuevo al icono predeterminado de la aplicación de Windows, ejecute este script con el SDK de PowerShell remoto:
  `Get-BrokerApplication -IconUid 1 | Set-BrokerApplication -IconUid 0`.
- En **Administrar > Configuración completa**, no se puede cambiar el tipo de SO de los catálogos de Azure y se muestra un mensaje de error. Ya no se permite cambiar el tipo de SO de los catálogos de Azure aunque use PowerShell. [STUD-19819]
- En entornos de Microsoft Azure, al habilitar el disco de SO efímero de Azure y la E/S de MCS al mismo tiempo, no se crea un catálogo de máquinas. Sin embargo, para los catálogos de máquinas existentes, aún puede actualizar un catálogo de máquinas, agregar o eliminar máquinas virtuales y eliminar un catálogo de máquinas. [PMCS-21698]
- Es posible que el icono de la flecha desplegable de los botones Promedio de E/S por segundo, Control de sesión y Control de energía no aparezcan en las páginas **Detalles del usuario** y **De-**

talles de máquina. Sin embargo, la funcionalidad opera como es debido. Para ver todos los elementos del menú, haga clic en cualquier lugar del botón. [DIR-11875]

- Si usa servicios de dominio de Azure AD: Los nombres principales de usuario (UPN) de inicio de sesión de Workspace (o StoreFront) 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.
- Al realizar implementaciones en Azure y crear un catálogo de MCS en versión 7.9 o una posterior con caché de reescritura habilitada y la versión del VDA instalado en la imagen maestra es 1811 o una versión anterior, se produce un error. Además, no se puede crear nada relacionado con Personal vDisk para Microsoft Azure. Como solución temporal, seleccione otra versión del catálogo para implementar en Azure o inhabilite la caché de reescritura. Para inhabilitar la caché de reescritura cuando crea un catálogo, desmarque las casillas **Memoria asignada para caché** y **Tamaño de caché de disco** en la página **Máquinas**.
- El enlace **Consola** de **Supervisar > Detalles de la máquina** no inicia la consola de la máquina en los exploradores Microsoft Edge 44 y Firefox 68 ESR. [DIR-8160]
- Cuando intenta usar la opción "Reiniciar"en la versión web o escritorio de la aplicación Workspace, el diálogo "Reiniciando"nunca se cierra ni notifica que la operación se completó correctamente. El hipervisor muestra que la máquina se ha apagado, pero no se ha iniciado. Como solución temporal, pasado algún tiempo, el usuario puede cerrar el cuadro de diálogo "Reiniciando"e iniciar el escritorio. [BRK-5564]

Para problemas relacionados con los VDA actuales, consulte Problemas conocidos.

Elementos retirados

March 6, 2024

En este artículo, se informa con antelación de las funciones de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) que se están retirando gradualmente, para que pueda tomar a tiempo las decisiones empresariales oportunas. Citrix supervisa el uso que hacen los clientes de las funciones que se retirarán y los comentarios que tengan cuando estas se retiran definitivamente. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener información detallada sobre el ciclo de vida útil de los productos, consulte el artículo Product Lifecycle Support Policy.

> **Nota:**
>
> Los elementos retirados y la eliminación de Citrix Virtual Apps and Desktops se describen en su propio artículo Elementos retirados.

Elementos eliminados y obsoletos

En esta lista se muestran las funciones de Citrix DaaS que se han retirado o eliminado.

Los elementos *retirados* no se quitan inmediatamente. Citrix sigue admitiéndolos, pero se quitarán de la siguiente versión.

Los elementos *eliminados* se quitan o ya no se ofrecen ni se desarrollan en Citrix DaaS. Las fechas en **negrita** indican las actualizaciones más recientes.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Función para configurar la caché de reescritura para que incluya solo una caché de disco y ninguna caché de memoria	Febrero de 2024		Use la opción de configuración del tamaño de la memoria caché y asigne un tamaño distinto de cero.
Compatibilidad con los catálogos de Azure creados antes de existir la función de aprovisionamiento bajo demanda (catálogos “antiguos”)	Febrero de 2024		Cree de nuevo las máquinas virtuales del catálogo antiguo de Azure. Los catálogos se aprovisionan bajo demanda y ayudan a ahorrar costes de almacenamiento.
Compatibilidad con Citrix Connector 3.1 para System Center Configuration Manager	Diciembre de 2023		Actualice la imagen o la aplicación manualmente.
Compatibilidad para usar una imagen maestra en una región diferente de la región en la que se creó el catálogo	Diciembre de 2023		Use Azure Compute Gallery para replicar la imagen maestra en la región requerida.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Compatibilidad con trabajador de volumen de AWS	Noviembre de 2023		Use carga y descarga directa en disco. Consulte Carga y descarga directa en disco.
Compatibilidad con `Leave user management to Citrix Cloud` usado en la creación de grupos de entrega.	Septiembre de 2023	Septiembre de 2023	
Compatibilidad con `AwsCaptureInstanceProperties` de uso en entornos de AWS	Agosto de 2023		Usar un perfil de máquina. Consulte Crear un catálogo mediante un perfil de máquina.
Compatibilidad con VMware vSphere 6.7		Junio de 2023	Utilice versiones posteriores para VMware vSphere.
Comando de PowerShell `Schedule-ProvVMUpdate`	Abril de 2023		Use el comando `Set-ProvVMUpdateTimeWindow`.
Comando de PowerShell `Request-ProvVMUpdate`	Abril de 2023		Utilice el comando `Set-ProvVMUpdateTimeWindow` con los parámetros `-StartsNow` y `-DurationInMinutes -1`.
Comando de PowerShell `Cancel-ProvVMUpdate`	Abril de 2023		Use el comando `Clear-ProvVMUpdateTimeWindow`.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Parámetro `DedicatedTenancy` utilizado en el comando `New-ProvScheme`	Marzo de 2023		Utilice el parámetro `TenancyType`.
Disco no administrado para crear máquinas virtuales en el entorno Azure	Junio de 2022		
Compatibilidad con cuatro comandos específicos de AWS: `Revoke-HypSecurityGroupIngress`, `Revoke-HypSecurityGroupEgress`, `Grant-HypSecuritygroupegress` y `Grant-HypSecurityGroupIngress`	Mayo de 2022		
Parámetro `StorageAccountType` utilizado en entornos de Azure	Abril de 2022		Utilice `StorageType`.
Consola antigua (consola basada en MMC)	Julio de 2021	Noviembre de 2021	Utilice **Administrar > Configuración completa** para acceder a toda la gama de acciones de configuración y administración.
Distribución rápida de Azure	Septiembre de 2020		Utilice Distribución rápida.

Elemento	Retirada anunciada en la versión	Eliminado en la versión	Alternativa
Capacidad para importar dispositivos de destino de Citrix Provisioning para crear catálogos en Citrix Studio.	Agosto de 2020	Febrero de 2021	Utilice el asistente para la exportación de dispositivos de Citrix Provisioning para enviar máquinas virtuales de Citrix Provisioning en Delivery Controllers o MCS para la creación de catálogos. Consulte Export Devices Wizard.

Requisitos del sistema

June 12, 2024

Introducción

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

No se pueden ofrecer recomendaciones concretas de tamaño para VM que entregan escritorios y aplicaciones debido a la naturaleza dinámica y compleja del hardware existente en el mercado. Cada implementación tiene necesidades únicas. Por lo general, el tamaño de una máquina virtual se calcula en función del hardware y no se tienen en cuenta las cargas de trabajo del usuario (excepto para la memoria RAM; necesita más memoria RAM para las aplicaciones que consumen más). Citrix Tech Zone contiene las instrucciones más recientes sobre el tamaño de los VDA.

> **Importante:**
>
> Las versiones de VDA mencionadas en este artículo están sujetas al ciclo de vida de los productos Citrix. Para obtener más información, consulte la tabla de productos en el sitio web de Citrix.
>
> Para obtener más información sobre el uso de los VDA LTSR con Citrix DaaS, consulte CTX205549.

Recuerde: En una implementación de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), no se necesita instalar ni administrar los componentes principales (Delivery Controllers,

la base de datos del sitio o las consolas de administración o supervisión). Para obtener instrucciones sobre la instalación de Virtual Delivery Agent (VDA), consulte:

- Instalar VDA
- Instalar los VDA mediante la línea de comandos.

Cloud Connectors

Para obtener más información, consulte Detalles técnicos de Cloud Connector.

VDA en un entorno de Azure

Sistemas operativos compatibles:

- Windows 11 multisesión
- Windows 11 de sesión única
- Windows 10 multisesión
- Windows 10 de sesión única
- Windows Server 2022 (requiere un VDA 2106, como mínimo)
- Windows Server 2019
- Windows Server 2016

Todos los VDA que no hayan llegado al final de su vida útil son compatibles con Citrix DaaS. En el caso de los VDA LTSR, recomendamos usarlos con la actualización acumulativa (CU) más reciente. Para obtener más información sobre el ciclo de vida de los VDA, consulte la tabla de productos de Citrix.

Windows Server 2012 R2 solo es compatible con VDA 1912 (y versiones CU posteriores).

Windows Server necesita licencias de Microsoft RDS.

Para obtener información sobre Azure Virtual Desktop, consulte la documentación de Microsoft.

VDA para SO de sesión única

La siguiente información es aplicable a la última versión de VDA.

Sistemas operativos compatibles:

- Windows 11
- Windows 10
  - Para obtener información sobre las ediciones compatibles, consulte CTX224843. Ese artículo también contiene enlaces a problemas conocidos de Citrix con las versiones compatibles de Windows.

  - La redirección de composición del escritorio y el modo de gráficos antiguo no se admiten en Windows 10.

Requisitos:

- Microsoft .NET Framework 4.8 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Si la máquina contiene una versión anterior de runtime (por ejemplo, 2015-2017), el instalador de Citrix la actualiza.
  - Si la máquina contiene una versión anterior a 2015, Citrix instala la versión más reciente en paralelo.

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

Algunas funciones de aceleración multimedia (como la Redirección de HDX MediaStream para Windows Media) requieren que Microsoft Media Foundation esté instalado en la máquina donde quiere instalar el VDA. Si la máquina no tiene instalado Media Foundation, las funciones de aceleración multimedia no se instalan y no funcionan. No quite Media Foundation de la máquina después de instalar el software de Citrix. De lo contrario, los usuarios no pueden iniciar sesión en la máquina. En la mayoría de las ediciones de SO de escritorio Windows compatibles, la compatibilidad para Media Foundation ya está instalada y no se puede quitar. Sin embargo, las ediciones N no incluyen ciertas tecnologías relacionadas con elementos multimedia. Puede obtener el software de Microsoft o de un tercero.

Más información:

- Para obtener información acerca de Linux VDA, consulte la documentación del producto Linux Virtual Delivery Agent.
- Para usar la función VDI de servidor, puede usar la interfaz de línea de comandos para instalar un VDA de sesión única en una máquina Windows Server compatible. Consulte VDI de servidor para obtener instrucciones.
- Para obtener información sobre cómo instalar un VDA en una máquina más antigua, consulte Sistemas operativos anteriores.
- Consulte también VDA en un entorno de Azure Virtual Desktop.

VDA para SO multisesión

La siguiente información es aplicable a la última versión de VDA.

Sistemas operativos compatibles:

- Windows Server 2022 (requiere un VDA 2106, como mínimo)
- Windows Server 2019, Standard y Datacenter Edition
- Windows Server 2016, Standard y Datacenter Edition
- Windows 11
- Windows 10 (64 bits), todas las versiones compatibles

El instalador implementa automáticamente los siguientes requisitos:

- Microsoft .NET Framework 4.8 (o una versión posterior) se instala automáticamente si no está instalado.
- Microsoft Visual C++ 2015-2019 Redistributable.
  - Si la máquina contiene una versión anterior de runtime (por ejemplo, 2015-2017), el instalador de Citrix la actualiza.
  - Si la máquina contiene una versión anterior a 2015, Citrix instala la versión más reciente en paralelo.

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

Algunas funciones de aceleración multimedia (como la Redirección de HDX MediaStream para Windows Media) requieren que Microsoft Media Foundation esté instalado en la máquina donde quiere instalar el VDA. Si la máquina no tiene instalado Media Foundation, las funciones de aceleración multimedia no se instalan y no funcionan. No quite Media Foundation de la máquina después de instalar el software de Citrix. De lo contrario, los usuarios no pueden iniciar sesión en la máquina. En la mayoría de las versiones de Windows Server, la función Media Foundation se instala a través del Administrador del servidor. Sin embargo, las ediciones N no incluyen ciertas tecnologías relacionadas con elementos multimedia. Puede obtener el software de Microsoft o de un tercero.

Si Media Foundation no está presente en el VDA, estas funciones multimedia no funcionarán:

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

Más información:

- Para obtener más información acerca de Linux VDA, consulte los artículos de Linux Virtual Delivery Agent.
- Para obtener información sobre cómo instalar un VDA en un sistema operativo Windows que ya no es compatible, consulte Sistemas operativos anteriores.
- Consulte también VDA en un entorno de Azure Virtual Desktop.

Hosts o recursos de virtualización

Se admiten los siguientes recursos de host/virtualización (ordenados alfabéticamente). Donde corresponda, se admiten las siguientes versiones *superior.inferior*, incluidas las actualizaciones de esas versiones. CTX131239 contiene la información de versión más reciente de hipervisor, además de enlaces a los problemas conocidos.

- **Amazon Web Services (AWS)**
  - Puede aprovisionar aplicaciones y escritorios en sistemas operativos Windows Server compatibles.
  - No se admite Amazon Relational Database Service (Amazon RDS).

  Para obtener más información, consulte Entornos de nube de AWS.
- **XenServer (anteriormente Citrix Hypervisor)**

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

  Para obtener más información, consulte Entornos de virtualización de XenServer.
- **Google Cloud Platform**

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

  Para obtener más información, consulte Entornos de virtualización de HPE Moonshot.
- **Microsoft Azure Resource Manager**

  Para obtener más información, consulte Entornos de nube para Microsoft Azure Resource Manager.
- **Microsoft System Center Virtual Machine Manager**

  Incluye cualquier versión de Hyper-V que se pueda registrar en las versiones compatibles de System Center Virtual Machine Manager.

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

  Para obtener más información, consulte Entornos de virtualización de Microsoft System Center Virtual Machine Manager.
- **Nutanix Acropolis**

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

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

- **VMware Cloud on AWS**

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

  Para obtener más información, consulte VMware Cloud en Amazon Web Services (AWS).

- **Azure VMware Solution (AVS)**

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

  Para obtener más información, consulte Integración de Azure VMware Solution (AVS).

- **Google Cloud VMware Engine**

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

  Para obtener más información, consulte VMware Engine de Google Cloud.

- **VMware vSphere(vCenter + ESXi)**

  No se admite la operación "Linked Mode"de vSphere vCenter.

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

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

> **Nota:**
>
> No debe instalar el software del VDA en ningún servidor Citrix DDC o StoreFront. El VDA debe ser un sistema independiente. La instalación de varios componentes en una sola máquina virtual solo está permitida cuando se desarrolla una prueba de concepto o cuando se publica la consola de administración de Studio solo para administradores. En este caso, debe asegurarse de que los usuarios que no sean administradores no tengan acceso a las máquinas virtuales de DDC/StoreFront.

Niveles funcionales de Active Directory

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

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

Para obtener más información acerca de Active Directory, consulte Unidos a Active Directory.

Tecnologías HDX

Para conocer la compatibilidad y los requisitos necesarios para la función HDX, consulte HDX.

Universal Print Server

El servidor de impresión universal (Universal Print Server) consta de componentes de cliente y de servidor. El componente UpsClient va incluido en la instalación del VDA. Debe instalar el componente UpsServer en cada servidor de impresión donde residen las impresoras compartidas que se quieren aprovisionar con Citrix Universal Print Driver en las sesiones de usuario.

El componente UpsServer se admite en:

- Windows Server 2019
- Windows Server 2016

Requisitos:

- Microsoft .NET Framework 4.8 (mínimo)
- Microsoft Visual C++ 2015-2022 Redistributable.
  - Si la máquina contiene una versión anterior de runtime (por ejemplo, 2015-2017), el instalador de Citrix la actualiza.
  - Si la máquina contiene una versión anterior a 2015, Citrix instala la versión más reciente en paralelo.

En el caso de los VDA multisesión, la autenticación de usuario durante las operaciones de impresión requiere que el servidor Universal Print Server esté unido al mismo dominio que el VDA.

Los paquetes de componentes de cliente y de servidor independientes también están disponibles para la descarga.

Para obtener más información, consulte Aprovisionar impresoras.

Conectividad del servicio

Consulte Requisitos del sistema y de conectividad para obtener información sobre la conexión a Internet Esta información incluye requisitos comunes a la mayoría de los servicios de Citrix Cloud, además de requisitos específicos de Citrix DaaS.

Otros

- La Consola de administración de directivas de grupo (GPMC) de Microsoft es necesaria si quiere almacenar la información sobre directivas de Citrix en Active Directory, en lugar de la base de datos de configuración del sitio. La máquina donde instale `CitrixGroupPolicyManagement_x64.msi` debe tener Visual Studio 2015 Runtime instalado. Para obtener más información, consulte la documentación de Microsoft.
- Este producto es compatible con las versiones 3 a 5 de PowerShell.
- Para las funciones y los componentes de producto que se pueden instalar en servidores de Windows, no se ofrecen las instalaciones de Server Core y Nano Server a menos que se indique.
- Para obtener información detallada sobre los límites de recursos en una implementación, consulte Límites.
- Para ver las versiones de StoreFront compatibles, consulte los requisitos del sistema para StoreFront.
- Para obtener información sobre la globalización, consulte CTX119253.
- Para obtener información sobre los puertos que utiliza Citrix DaaS, consulte Communication Ports Used by Citrix Technologies.
- Para obtener información sobre los requisitos al utilizar la interfaz de administración de Distribución rápida, consulte Requisitos.

Límites

June 12, 2024

Los valores de este artículo indican los límites de una única instancia de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Citrix ha probado exhaustivamente estos límites y los recomienda para ofrecer la mejor experiencia de usuario final y administrador. Estos límites son flexibles y no se aplican técnicamente (excepto la cantidad total de agentes VDA por ubicación de recursos). Cuando la cantidad de usuarios simultáneos supera los 125 000, Citrix puede adaptarse y combinar varias instancias de Citrix DaaS para ofrecer una experiencia unificada a cualquier escala.

La información de este artículo es dinámica. Vuelva con frecuencia para consultar las novedades. Si tiene actualmente requisitos que los límites publicados no contemplan, contacte a un representante de Citrix para obtener ayuda.

Límites de configuración

Si las directivas superan el límite, Citrix recomienda utilizar Workspace Environment Management Service u Objetos de directiva de grupo (GPO) de Active Directory.

Recurso	Límite
Dominios de Active Directory	100
Carpetas de aplicaciones	1000
Grupos de aplicaciones	250
Aplicaciones	5000
Catálogos	2000
Grupos de entrega	2000
Conexiones de host	200
Ubicaciones de recursos	100
Directivas de la consola Administrar (Configuración completa)	200
Etiquetas	10 000
VDA	100 000

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 ubicaciones de recursos adicionales.

Recurso	Límite
Total de VDA (límite estricto)	10 000
Total de sesiones	25 000
Dominios de Active Directory	1
Conexiones de host	40

Los Citrix Cloud Connectors se asignan a ubicaciones de recursos y vinculan las cargas de trabajo a Citrix DaaS. Para obtener información sobre los límites de los Cloud Connectors, consulte Consideraciones de escala y tamaño para los Cloud Connectors.

Límites de aprovisionamiento

Los límites de aprovisionamiento de esta tabla son los máximos recomendados por Citrix para una sola suscripción de proveedor pública.

Es probable que alcance los límites de cuota de su proveedor de nube pública en niveles inferiores. En tales casos, póngase en contacto con el proveedor para aumentar su cuota de suscripción. Para implementaciones a mayor escala, Citrix recomienda un modelo radial, en el que los agentes VDA se reparten entre varias suscripciones y conexiones de host.

Para obtener más información, consulte las siguientes arquitecturas de referencia:

- Citrix DaaS en AWS
- Virtualización de Citrix en Google Cloud
- Citrix DaaS en Azure

Recurso	Límite
Agentes VDA por cuenta y región de Amazon Web Services	3000
VDA por proyecto de Google Cloud Platform	3000
VDA por suscripción a Microsoft Azure por región	5000

> **Nota:**
>
> Los límites son los recomendados por Citrix.

Límites de uso

Para obtener información sobre los roles de administración y las diferencias entre ellos, consulte:

- Administradores de Administrar (Configuración completa)
- Administradores (Supervisar en Director)

Recurso	Límite
Administradores totales simultáneos (Supervisar en Director)	40
Administradores de asistencia simultáneos (Supervisar en Director)	200
Administradores de sesiones simultáneos (Supervisar en Director)	50

Recurso	Límite
Administradores de la nube simultáneos de Administrar (Configuración completa)	100
Administradores de asistencia simultáneos de Administrar (Configuración completa)	60
Usuarios finales simultáneos	125 000
Recursos publicados para un solo usuario	250
Inicios de sesión por minuto	3000

- Supervisar (Director) permite la agregación de hasta cuatro arrendatarios de Citrix DaaS (los radios) en un solo arrendatario (el centro).
- Los administradores de asistencia técnica de la instancia del hub pueden supervisar y solucionar problemas de usuarios, máquinas, dispositivos de punto final y transacciones de todas las instancias agregadas (centro y radio) en función de la configuración de administración delegada de la instancia específica.
- La cantidad de administradores simultáneos por instancia de Citrix DaaS se indica en la tabla Límites de uso.

Registro de cambios de límites

En la siguiente tabla se hace un seguimiento de la modificación en los límites de configuración:

Fecha	Recurso	Descripción
22 Nov 2023	Dominios de Active Directory	El límite se incrementó de 85 a 100.
	Catálogos	El límite se incrementó de 1000 a 2000.
	Grupos de entrega	El límite se incrementó de 1000 a 2000.
	Ubicaciones de recursos	El límite se incrementó de 85 a 100.
	Ubicación de recursos -> Total de sesiones	El límite se incrementó de 20 000 a 25 000.
07 Dec 2023	Límites de aprovisionamiento -> VDA por suscripción a Microsoft Azure por región	El límite se incrementó de 2500 a 5000.

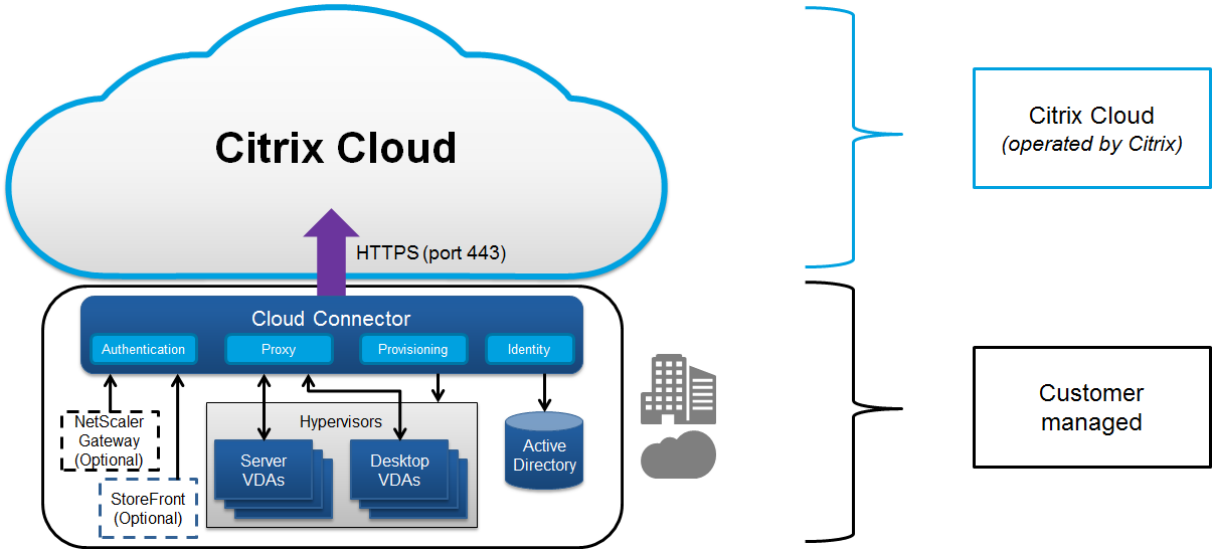
Información técnica general sobre la seguridad

May 17, 2024

Información general sobre la seguridad

Este documento es aplicable a Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) alojado en Citrix Cloud. La información incluye Citrix Virtual Apps Essentials y Citrix Virtual Desktops Essentials.

Citrix Cloud administra el funcionamiento del plano de control para entornos de Citrix DaaS. El plano de control incluye los Delivery Controllers, las consolas de administración, la base de datos SQL, el servidor de licencias y, opcionalmente, StoreFront y Citrix Gateway (antes NetScaler Gateway). Los agentes Virtual Delivery Agent (VDA) que alojan las aplicaciones y los escritorios permanecen bajo el control del cliente en el centro de datos que este elija, ya sea en la nube o local. Estos componentes se conectan con el servicio de nube por medio de un agente llamado el Citrix Cloud Connector. Si los clientes optan por utilizar Citrix Workspace, también pueden utilizar Citrix Gateway Service, en lugar de ejecutar Citrix Gateway en su centro de datos. Este diagrama ilustra Citrix DaaS y sus límites de seguridad.



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.

Flujo de datos

Citrix DaaS no aloja los VDA, por lo que los datos de aplicaciones y las imágenes del cliente necesarias para el aprovisionamiento siempre se alojan en la instalación del cliente. El plano de control tiene acceso a los metadatos (como nombres de usuario, nombres de máquina y accesos directos de aplicaciones), con lo que se restringe el acceso a la propiedad intelectual del cliente desde el plano de control.

Los datos que transitan entre la nube y las instalaciones del cliente utilizan conexiones TLS seguras a través del puerto 443.

Aislamiento de datos

Citrix DaaS solo almacena los metadatos necesarios para la intermediación y la supervisión de escritorios y aplicaciones del cliente. La información confidencial (como imágenes, perfiles de usuario y otros datos de aplicaciones) permanece en las instalaciones del cliente o en su suscripción con un proveedor de nube pública.

Ediciones del servicio

Las prestaciones de Citrix DaaS varían según la edición. Por ejemplo, Citrix Virtual Apps Essentials solo admite Citrix Gateway Service y Citrix Workspace. Consulte la documentación de ese producto para obtener más información sobre las funciones compatibles.

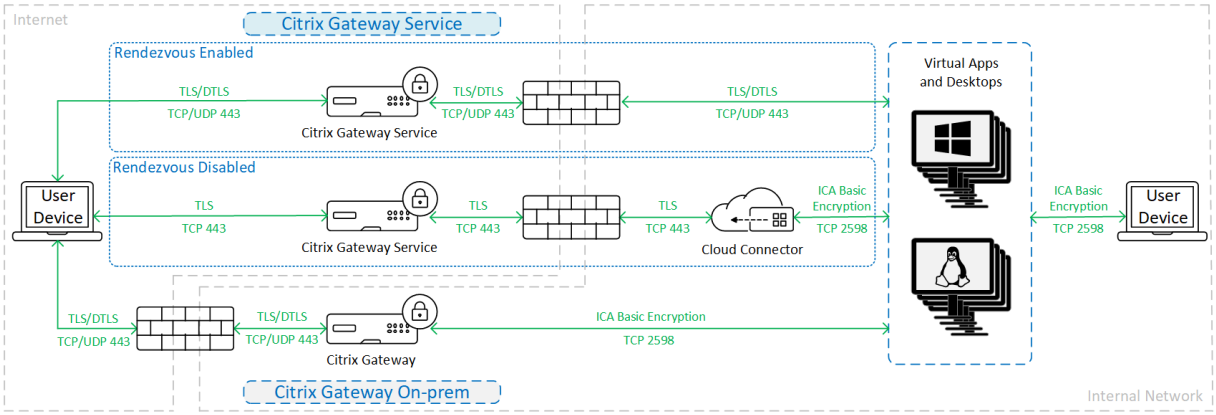
Seguridad ICA

Citrix DaaS proporciona varias opciones para proteger el tráfico ICA en tránsito. Estas son las opciones disponibles:

- **Cifrado básico:** La configuración predeterminada.
- **SecureICA:** Permite cifrar los datos de sesión mediante cifrado RC5 (128 bits).
- **TLS/DTLS de VDA:** Permite utilizar cifrado a nivel de red mediante TLS/DTLS.
- **Protocolo Rendezvous:** Disponible solo cuando se utiliza Citrix Gateway Service. Cuando se utiliza el protocolo Rendezvous, las sesiones ICA se cifran de extremo a extremo mediante TLS/DTLS.

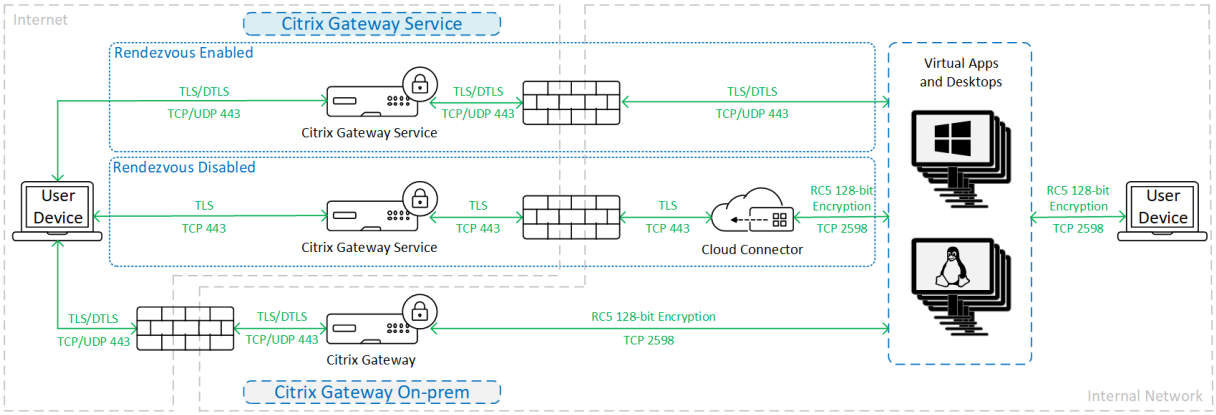
Cifrado básico

Cuando se utiliza el cifrado básico, el tráfico se cifra como se muestra en el gráfico siguiente.



SecureICA

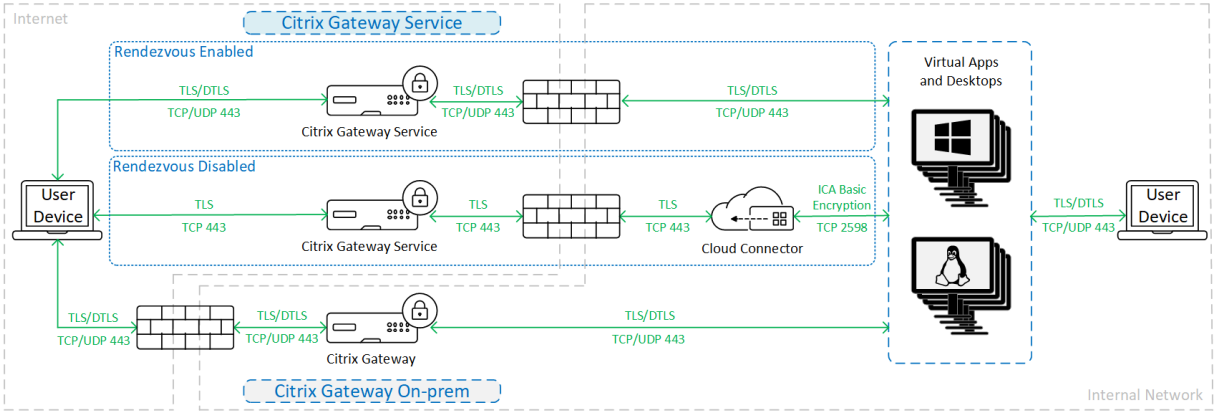
Cuando se utiliza SecureICA, el tráfico se cifra como se muestra en el gráfico siguiente.



> **Nota:**
>
> SecureICA no se admite cuando se utiliza la aplicación Workspace para HTML5.

TLS/DTLS de VDA

Cuando se utiliza el cifrado TLS/DTLS de VDA, el tráfico se cifra como se muestra en el gráfico siguiente.



Nota:

Cuando se utiliza Gateway Service sin Rendezvous, el tráfico entre el VDA y el Cloud Connector no está cifrado con TLS, puesto que Cloud Connector no admite la conexión al VDA con cifrado a nivel de red.

Más recursos

Para obtener más información sobre las opciones de seguridad ICA y cómo configurarlas, consulte:

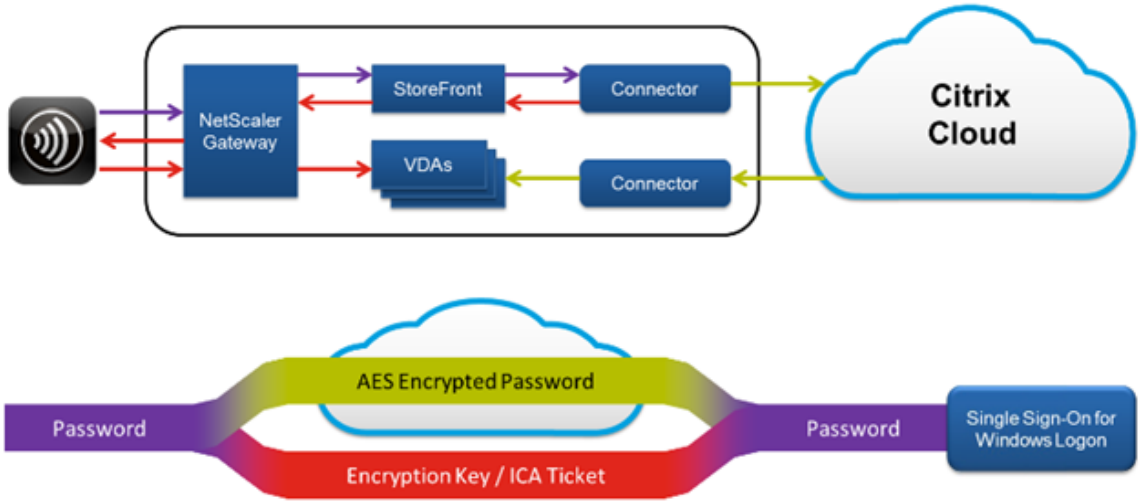
- SecureICA: Configuraciones de directiva de Seguridad
- TLS/DTLS de VDA: Transport Layer Security (TLS)
- Protocolo Rendezvous: Protocolo Rendezvous

Gestión de credenciales

Citrix DaaS gestiona cuatro tipos de credenciales:

- Credenciales de usuario. Cuando se usa un servidor StoreFront administrado por el cliente, Citrix Cloud Connector cifra las credenciales de usuario con el cifrado AES-256 y una clave aleatoria de un solo uso generada para cada inicio. La clave nunca se transfiere a la nube, y solo se devuelve a la aplicación Citrix Workspace. Esta aplicación pasa esta clave directamente al VDA para descifrar la contraseña del usuario durante el inicio de sesión para una experiencia de inicio Single Sign-On. El flujo se muestra en la siguiente figura.

  De forma predeterminada, las credenciales de usuario no se reenvían a través de límites de dominios que no son de confianza. Si hay un VDA y StoreFront instalados en un dominio y un usuario de otro dominio intenta conectarse al VDA, se produce un error en el intento de inicio de sesión, a menos que se establezca una confianza entre los dominios. Puede inhabilitar este comportamiento y permitir que las credenciales se reenvíen entre dominios que no son de confianza mediante el SDK de PowerShell de DaaS. Para obtener más información, consulte Set-Brokersite.



- Credenciales de administrador. Los administradores se autentican en Citrix Cloud. La autenticación genera un token web JSON (JWT) firmado y de un solo uso, lo que permite que el administrador acceda a Citrix DaaS.
- Contraseñas del hipervisor. Los hipervisores locales que requieren una contraseña para autenticarse tienen una contraseña generada por el administrador que se guarda cifrada directamente en la base de datos SQL en la nube. Citrix administra las claves de homólogos. De esta manera, se asegura de que las credenciales de hipervisor solo estén disponibles para los procesos autenticados.
- Credenciales de Active Directory (AD). Machine Creation Services utiliza el Cloud Connector para crear cuentas de máquina en un Active Directory del cliente. Dado que la cuenta de máquina del Cloud Connector tiene el acceso de solo lectura en AD, se piden las credenciales al administrador para cada operación de creación o eliminación de máquinas. Estas credenciales se almacenan solo en la memoria y solamente se conservan durante un evento de aprovisionamiento.

Consideraciones sobre la implementación

Citrix recomienda que los usuarios consulten la documentación publicada sobre las prácticas recomendadas para implementar agentes VDA y aplicaciones Citrix Gateway en sus entornos.

Requisitos de acceso de red del Citrix Cloud Connector

Los Citrix Cloud Connectors solo necesitan el puerto 443 para el tráfico saliente a Internet, y se pueden alojar detrás de un proxy HTTP.

- La comunicación que se usa en Citrix Cloud para HTTPS es TLS. (Consulte Versiones TLS retiradas).

- En la red interna, el Cloud Connector necesita acceso a lo siguiente para Citrix DaaS:
  - VDA. Puerto 80, para tráfico de entrada y de salida. Además de 1494 y 2598 de entrada si se usa Citrix Gateway Service.
  - Servidores StoreFront. Puerto 80 de entrada.
  - Citrix Gateways, si se configuran como STA. Puerto 80 de entrada.
  - Controladores de dominio de Active Directory
  - Hipervisores. Solo tráfico de salida. Consulte Communication Ports Used by Citrix Technologies para puertos específicos.

El tráfico entre los VDA y los Cloud Connectors se cifra con la seguridad a nivel de mensaje Kerberos.

StoreFront administrado por el cliente

Un servidor StoreFront administrado por el cliente ofrece más opciones de configuración de seguridad y flexibilidad para la arquitectura de la implementación, incluida la capacidad de mantener las credenciales del usuario en la infraestructura local ("on-premises"). El servidor StoreFront puede alojarse detrás de Citrix Gateway para proporcionar acceso remoto seguro, aplicar la autenticación de varios factores y agregar otras funciones de seguridad.

Citrix Gateway Service

Con Citrix Gateway Service, ya no es necesario implementar Citrix Gateway en los centros de datos del cliente.

Para obtener más información, consulte Citrix Gateway Service.

Todas las conexiones TLS entre el Cloud Connector y Citrix Cloud se inician desde el Cloud Connector a Citrix Cloud. No se requiere asignar puertos de firewall para el tráfico entrante.

Confianza en XML

Esta opción está disponible en **Configuración completa > Parámetros > Habilitar confianza en XML** y está inhabilitada de forma predeterminada. Como alternativa, puede utilizar Citrix DaaS Remote Powershell SDK para administrar la confianza en XML.

La confianza en XML se aplica a las implementaciones que utilizan:

- Un StoreFront local.
- Tecnología de autenticación de suscriptor (usuario) que no requiere contraseñas. Ejemplos de tales tecnologías son las soluciones de PassThrough de dominio, tarjetas inteligentes, SAML y Veridium.

Habilitar la confianza en XML permite a los usuarios autenticarse correctamente y, a continuación, iniciar las aplicaciones. El Cloud Connector confía en las credenciales enviadas desde StoreFront. Habilite la confianza en XML solo cuando haya protegido las comunicaciones entre los Citrix Cloud Connectors y StoreFront (mediante firewalls, IPSec u otras recomendaciones de seguridad).

Este parámetro está inhabilitado de forma predeterminada.

Use el SDK de PowerShell remoto de Citrix DaaS para administrar la confianza en XML.

- Para comprobar el valor actual de confianza en XML, ejecute `Get-BrokerSite` e inspeccione el valor de `TrustRequestsSentToTheXMLServicePort`.
- Para habilitar la confianza en XML, ejecute `Set-BrokerSite -TrustRequestsSentToTheXmlServ $true`
- Para inhabilitar la confianza en XML, ejecute `Set-BrokerSite -TrustRequestsSentToTheXmlSer $false`

Aplicar tráfico HTTPS o HTTP

Para aplicar tráfico HTTPS o HTTP a través de XML Service, configure uno de estos conjuntos de valores del Registro en cada uno de sus Cloud Connectors.

Después de configurar los parámetros, reinicie Remote Broker Provider Service en cada Cloud Connector.

En `HKLM\Software\Citrix\DesktopServer\`:

- Para aplicar el tráfico HTTPS (e ignorar HTTP): Establezca `XmlServicesEnableSsl` en `1` y `XmlServicesEnableNonSsl` en `0`.
- Para aplicar el tráfico HTTP (e ignorar HTTPS): Establezca `XmlServicesEnableNonSsl` en `1` y `XmlServicesEnableSsl` en `0`.

Versiones TLS retiradas

Para mejorar la seguridad de Citrix DaaS, Citrix empezó a bloquear toda comunicación a través de Transport Layer Security (TLS) 1.0 y 1.1 desde el 15 de marzo de 2019.

Todas las conexiones a los servicios de Citrix Cloud procedentes de Citrix Cloud Connector requieren TLS 1.2.

Para garantizar la conexión a Citrix Workspace desde los dispositivos de los usuarios, la versión instalada de Citrix Receiver debe ser igual o más reciente que las siguientes.

Receiver	Versión
Windows	4.2.1000
Mac	12.0
Linux	13.2
Android	3.7
iOS	7.0
Chrome/HTML5	La más reciente (el explorador web debe admitir TLS 1.2).

Para actualizar la versión de Citrix Receiver a la más reciente, vaya a https://www.citrix.com/products/receiver/.

Como alternativa, actualice a la aplicación Citrix Workspace, que utiliza TLS 1.2. Para descargar la aplicación Citrix Workspace, vaya a https://www.citrix.com/downloads/workspace-app/.

Si necesita seguir usando TLS 1.0 o 1.1 (por ejemplo, si tiene un cliente ligero basado en una versión anterior de Receiver para Linux), instale un almacén de StoreFront en su ubicación de recursos. A continuación, haga que todos los Citrix Receivers apunten a él.

Más información

Los siguientes recursos contienen información de seguridad:

- Información técnica general sobre la seguridad para Azure administrado por Citrix.
- Sitio de seguridad de Citrix.
- Información de seguridad y cumplimiento: El centro de seguridad y cumplimiento contiene boletines de seguridad que pueden ayudarle a mantenerse informado. El centro también cuenta con documentación sobre estándares y certificaciones que son importantes para mantener un entorno de TI seguro y conforme.
- Guía de implementación segura para la plataforma Citrix Cloud: Esta guía ofrece una visión general de las prácticas recomendadas al utilizar Citrix Cloud, y describe la información que Citrix Cloud recopila y administra. Esta guía también contiene enlaces a información completa sobre Citrix Cloud Connector.
- Requisitos del sistema y de conectividad.
- Recomendaciones y consideraciones de seguridad.
- Tarjetas inteligentes.

- Transport Layer Security (TLS).

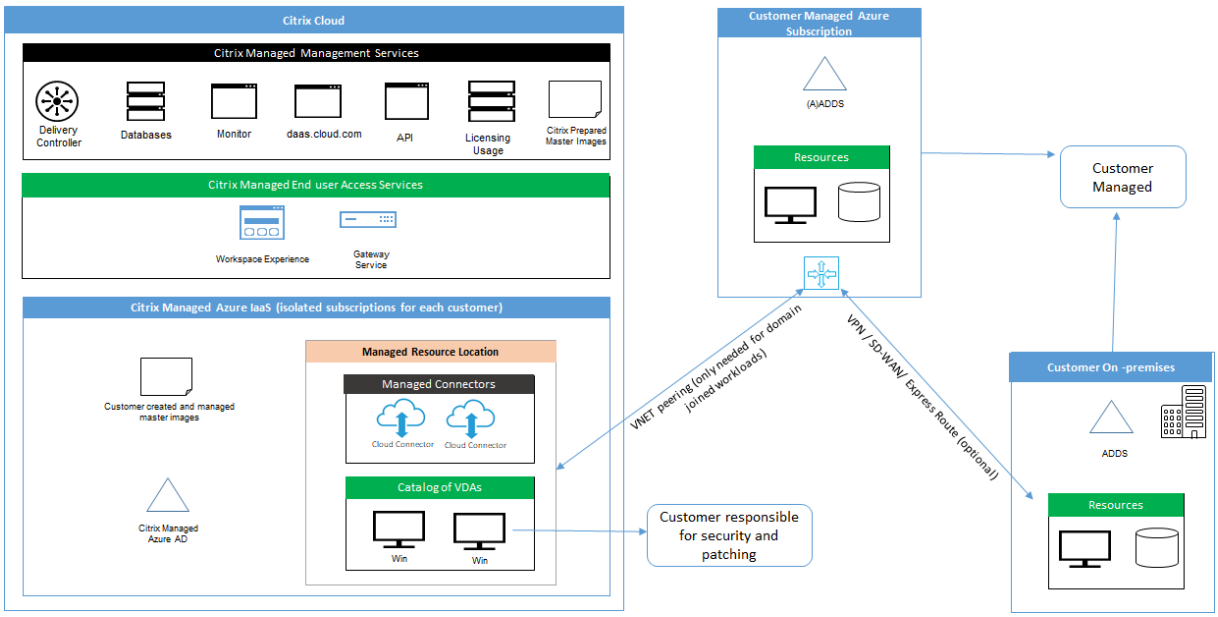
> **Nota:**
>
> Este documento es una introducción y una descripción general de la funcionalidad de seguridad de Citrix Cloud. Asimismo, este documento tiene por finalidad definir la división de responsabilidades entre Citrix y los clientes cuando se trata de proteger la implementación de Citrix Cloud. No está pensado para ser una guía de configuración o administración de Citrix Cloud ni de ninguno de sus componentes o servicios.

Información técnica general sobre la seguridad para Azure administrado por Citrix

May 17, 2024

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

En el siguiente diagrama, se muestran los componentes de una implementación de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) que utiliza Citrix Managed Azure. En este ejemplo, se utiliza una conexión de emparejamiento de redes virtuales.



Con Azure administrado por Citrix, los agentes Virtual Delivery Agent (VDA) del cliente que proporcionan escritorios y aplicaciones, además de Citrix Cloud Connectors, se implementan en modalidad de arrendatario y suscripción de Azure que Citrix administra.

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

Al utilizar una suscripción a Azure administrado por Citrix, Citrix DaaS 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 además restringe el acceso a AAD y a Citrix DaaS al personal de operaciones de Citrix únicamente. 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.

Cuando se utiliza el generador de imágenes de Citrix DaaS para crear y personalizar una nueva imagen de máquina, los puertos 3389-3390 se abren temporalmente en la red virtual administrada por Citrix, de modo que el cliente pueda conectar con RDP con 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 se pongan en contacto con los controladores de dominio locales, recursos compartidos de archivos u otros recursos de intranet, Citrix DaaS proporciona un flujo de emparejamiento de redes virtuales 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 a través de

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

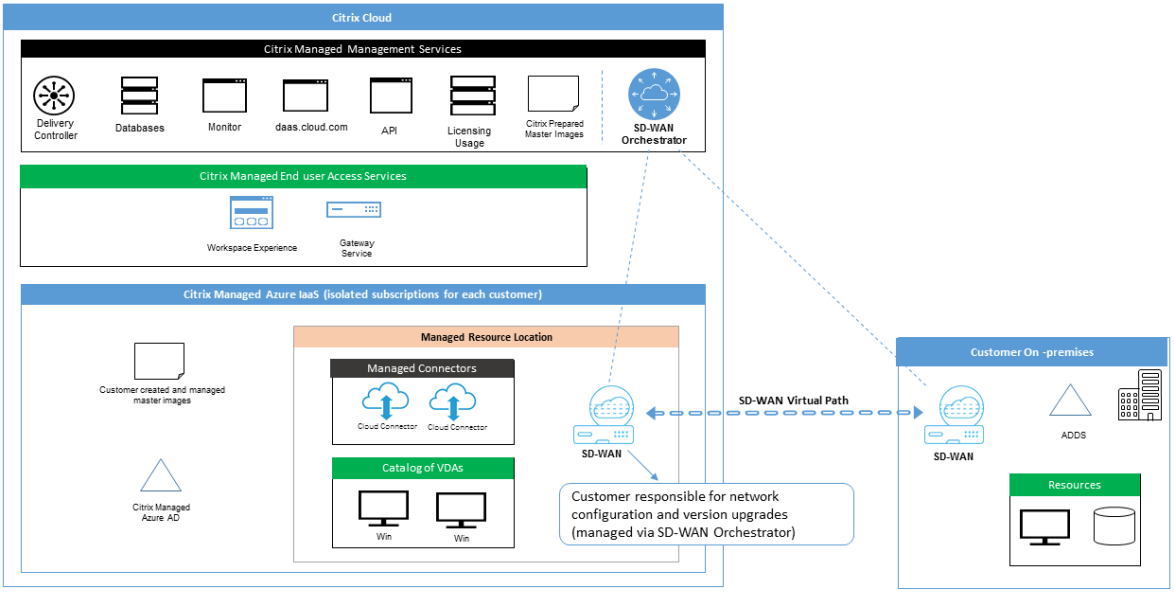
Citrix admite una forma totalmente automatizada de implementar instancias virtuales de Citrix SD-WAN para habilitar la conectividad entre Citrix DaaS y los recursos locales. La conectividad de Citrix SD-WAN tiene una serie de ventajas con respecto al emparejamiento de redes virtuales, entre ellas:

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 requiere que los clientes que quieren aprovechar la conectividad SD-WAN para Citrix DaaS usen SD-WAN Orchestrator para administrar sus redes Citrix SD-WAN.

En el siguiente diagrama, se muestran los componentes agregados en una implementación de Citrix DaaS cuando se utiliza una suscripción a de Azure administrado por Citrix y conectividad SD-WAN.



La implementación de Citrix SD-WAN para Citrix DaaS 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 de salida de la red virtual, 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 instancias SD-WAN virtuales utilizadas con Citrix DaaS , mantiene los recursos subyacentes de Azure (máquinas virtuales, equilibradores de carga, etc.), proporciona parámetros predeterminados de uso inmediato seguros y eficientes para la configuración inicial de instancias virtuales SD-WAN y habilita el mantenimiento y la solución de problemas continuos 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 hacer copia de seguridad de todas las imágenes de máquina cargadas en Citrix DaaS, 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:

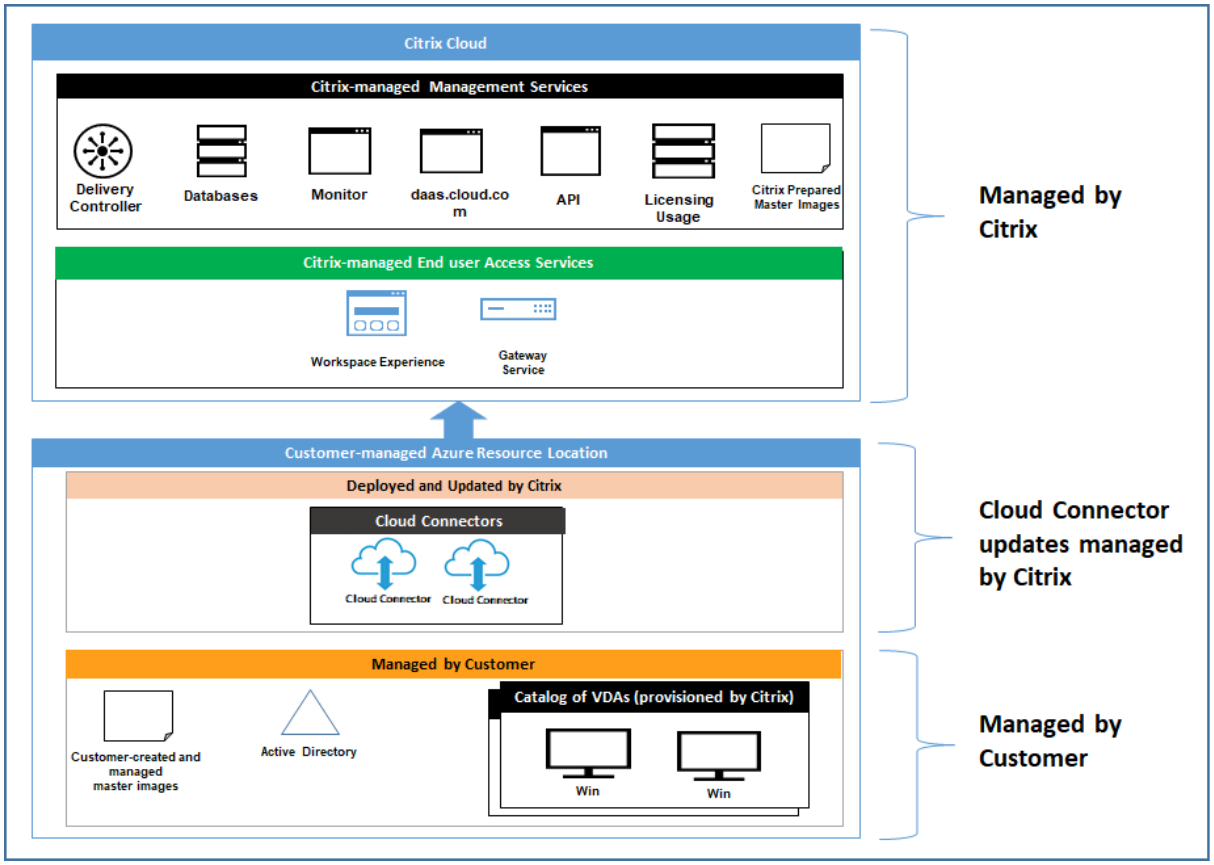
- Se permite temporalmente el tráfico de entrada por el puerto 3389 desde el intervalo de direcciones IP especificado por el cliente al bastión.
- Se permite temporalmente el tráfico de entrada por el puerto 3389 desde la dirección IP del bastión a cualquier dirección de la red virtual (VDA y Cloud Connectors).
- 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 de acuerdo con sus requisitos de red, con la excepción de algunos elementos necesarios para garantizar el correcto funcionamiento de SD-WAN en la red virtual 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 de una red de cliente deben ejecutar

la misma versión del software SD-WAN, los clientes deben administrar las implementaciones de versiones de software actualizadas en las instancias SD-WAN de Citrix DaaS conforme a sus programaciones y restricciones de mantenimiento de la red.

La incorrecta configuración de las reglas de redirección y firewall de SD-WAN, o una mala gestión de las contraseñas de administración de SD-WAN, pueden generar riesgos de seguridad tanto para los recursos virtuales de Citrix DaaS como para los recursos locales a los que se puede acceder a través de 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 crear un nuevo emparejamiento de redes virtuales o una nueva instancia de SD-WAN dentro de Citrix DaaS.

Responsabilidades compartidas de Citrix y del cliente

Citrix Cloud Connector para catálogos unidos a dominios

Citrix DaaS 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 experimente problemas con el catálogo de Citrix DaaS, existen 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 una vez que el cliente deseche el bastión o finalice el acceso RDP a través de Citrix DaaS.

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

- **Auditable:** La cuenta debe crearse específicamente para uso por parte de Citrix DaaS, de modo que el uso de la cuenta sea fácil auditar.
- **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

Lista de canales virtuales permitidos

May 17, 2024

La lista de canales virtuales permitidos es una función que le permite controlar qué canales virtuales que no son de Citrix están permitidos en su entorno. De forma predeterminada, la funcionalidad de lista de canales virtuales permitidos está habilitada. Como resultado, solo se pueden abrir los canales virtuales de Citrix en las sesiones de Citrix Virtual Apps and Desktops. Si hay necesidad de utilizar canales virtuales personalizados, ya sean internos o de un tercero, deben agregarse explícitamente a la lista de permitidos.

Configuración

La lista de canales virtuales permitidos está habilitada de forma predeterminada. Puede configurar esta función mediante los siguientes parámetros de la directiva de Citrix:

- **Lista de canales virtuales permitidos**: Para habilitar o inhabilitar la función y agregar canales virtuales a la lista.
- **Limitación de los registros de la lista de canales virtuales permitidos**: Establece el período de limitación para el registro de eventos de la lista de canales virtuales permitidos.
- **Registros de la lista de canales virtuales permitidos**: Establece el nivel de registro de la lista de canales virtuales permitidos.

Agregar canales virtuales a la lista de permitidos

Para agregar un canal virtual a la lista de permitidos, necesita la siguiente información:

1. El nombre del canal virtual tal y como se define en el código, que puede tener hasta 7 caracteres. Por ejemplo, `CTXCVC1`.
2. Las rutas a los procesos que abren el canal virtual en la máquina VDA. Por ejemplo, `C:\Program Files\Application\run.exe`.

Una vez que tenga la información necesaria, deberá agregar el canal virtual a la lista de permitidos mediante la configuración de la directiva Lista de canales virtuales permitidos. Para agregar un canal virtual a la lista, escriba el nombre del canal virtual seguido de una coma y, a continuación, la ruta del proceso que accede al canal virtual. Si hay varios procesos, puede agregarlos separando cada proceso con comas.

Para procesos individuales

Con los ejemplos anteriores, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

Para varios procesos

Si hay varios procesos, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

Uso de comodines

Se admite el uso de comodines (*). Puede usar caracteres comodín cuando los nombres de los directorios o ejecutables cambian en función de la versión de la aplicación o si el componente de terceros está instalado en los perfiles de los usuarios.

Puede usar caracteres comodín en los siguientes casos:

- Para reemplazar el nombre completo del directorio.
  Por ejemplo: `C:\Program Files\Application\*\run1.exe`
- Para reemplazar parte del nombre del directorio.
  Por ejemplo: `C:\Program Files\Application\v*\run1.exe`
- Para reemplazar el nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\*.exe`
- Para reemplazar parte del nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\run*.exe`

Se aplican las siguientes restricciones:

- El comodín solo se puede usar para reemplazar un único directorio. Por ejemplo: si el ejecutable se encuentra en `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application\*\run1.exe`
  - No permitido: `C:\Program Files\*\run1.exe`
- Las entradas deben contener la extensión de archivo.
  - Permitido: `C:\Program Files\Application\v1.2\*.exe`
  - No permitido: `C:\Program Files\Application\v1.2\*`
- Todas las rutas deben ser locales.

> **Nota:**
>
> - No se permiten las rutas de red.
> - La compatibilidad con caracteres comodín está disponible a partir de Citrix Virtual Apps and Desktops 2206.
> - La compatibilidad con caracteres comodín está disponible en Citrix Virtual Apps and Desktops 2203 LTSR a partir de la CU2.

Uso de variables de entorno del sistema

Puede usar variables de entorno del sistema para simplificar la definición de los procesos de confianza en su lista de permitidos. Puede usar cualquiera de las variables listas para usar, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` y `%systemroot%`.

También puede usar variables de entorno personalizadas siempre que estén definidas a nivel del sistema.

En los siguientes ejemplos se muestran variables de entorno listas para usar:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

En el siguiente ejemplo se muestra una variable de entorno del sistema personalizada:

- Nombre de variable personalizada: `app`
- Valor de variable personalizada: `%programfiles%\Application\`
- Entrada en la lista de permitidos: `CTXCVC1,%app%\run.exe`

> **Nota:**
>
> No se admiten variables de entorno de usuario.
>
> La compatibilidad con variables de entorno está disponible a partir de la versión 2209 de Citrix

> Virtual Apps and Desktops.

Obtener nombres y procesos de canales virtuales

La forma más sencilla de obtener el nombre del canal virtual y el proceso que lo abre en la máquina VDA es obtener la información del desarrollador o del proveedor tercero que proporcionó el canal virtual.

También puede obtener esta información aplicando los registros de la funcionalidad y siguiendo estos pasos:

1. Una vez establecidos los componentes del cliente y del servidor del canal virtual personalizado, inicie una aplicación virtual o un escritorio virtual.
2. En el registro de eventos del sistema de la máquina VDA, busque el nombre del canal virtual personalizado y el proceso que lo intentó abrir. Para obtener más información sobre los eventos disponibles, consulte Registros de eventos.
3. Cierre la sesión.
4. Agregue una entrada a la configuración de directiva Lista de canales virtuales permitidos para el canal virtual y el proceso identificados.
5. Reinicie la máquina.
6. Una vez registrado el VDA, ejecute la aplicación virtual o el escritorio virtual para comprobar que los canales virtuales personalizados se abren correctamente.

Consideraciones sobre canales virtuales Citrix

Todos los canales virtuales Citrix integrados son de confianza y se permite abrirlos sin ninguna configuración adicional. Sin embargo, las dos funcionalidades siguientes requieren entradas explícitas en la lista de permitidos debido a dependencias externas:

- Redirección multimedia
- HDX RealTime Optimization Pack para Skype for Business

Redirección multimedia

Si usa un reproductor multimedia distinto de Windows Media Player como reproductor multimedia del sistema, debe agregarlo a la lista de permitidos como proceso de confianza. Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: `CTXMM`
- Proceso: Ruta al reproductor multimedia utilizado en la máquina VDA. Por ejemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.

- Entrada en la lista de permitidos: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

HDX RealTime Optimization Pack para Skype for Business

Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: `CTXRMEP`
- Proceso: Ruta al archivo ejecutable de Skype for Business en la máquina VDA, que puede variar según la versión de Skype for Business o si se ha usado una ruta de instalación personalizada. Por ejemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.
- Entrada en la lista de permitidos: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

Métodos de entrega

May 22, 2022

Es probable que un único método de entrega no cubra todas sus necesidades.

Por eso, puede plantearse varios métodos de entrega de aplicaciones. Elegir el método adecuado ayuda a mejorar la escalabilidad, la administración y la experiencia de los usuarios.

- **Aplicación instalada:** La aplicación es parte de la imagen base del escritorio. El proceso de instalación implica realizar modificaciones en el Registro y copiar archivos DLL y EXE, entre otros, a la unidad de la imagen. Para obtener más información, consulte Crear catálogos de máquinas.
- **Aplicación distribuida por streaming (Microsoft App-V):** La aplicación se incluye en un perfil y se entrega a demanda a los escritorios de toda la red. Los archivos de aplicación y los parámetros de Registro se colocan en un contenedor del escritorio virtual, aislados del sistema operativo base y entre ellos. Este aislamiento ayuda a solucionar los problemas de compatibilidad. Para obtener más información, consulte App-V.
- **Aplicación por capas (Citrix App Layering):** Cada capa contiene una sola aplicación, agente o sistema operativo. Al integrar una capa de sistema operativo, una capa de plataforma (por ejemplo, VDA) y muchas capas de aplicaciones, un administrador puede crear fácilmente nuevas imágenes a implementar. La distribución en capas facilita el mantenimiento cotidiano, ya que el sistema operativo, el agente y la aplicación se encuentran en una capa cada uno. Cuando actualiza una capa, todas las imágenes implementadas que contienen esa capa se actualizan. Consulte Citrix App Layering.

- **Aplicación alojada en Windows:** Una aplicación se instala en un host multiusuario de Citrix Virtual Apps y se implementa como una aplicación, no como un escritorio. Un usuario accede a la aplicación Windows alojada en servidores directamente desde el dispositivo de punto final o un escritorio VDI, con lo que se oculta el hecho de que la aplicación se ejecuta de forma remota. Para obtener información detallada, consulte Crear grupos de entrega.
- **Aplicación local:** Una aplicación se implementa en el dispositivo de punto final. La interfaz de la aplicación aparece en la sesión de usuario alojada en el VDI, aunque se ejecute en el dispositivo de punto final. Para obtener más información, consulte Acceso a aplicaciones locales y redirección de URL.

Para los escritorios, puede utilizar los escritorios VDI o los escritorios publicados de Citrix Virtual Apps.

Aplicaciones y escritorios publicados de Citrix Virtual Apps

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

Caso de uso:

- Quiere una entrega de recursos basada en servidores, que no sea muy costosa, para minimizar el coste de entregar aplicaciones a muchos usuarios, al tiempo que les ofrece una experiencia de usuario segura y de alta definición.
- Sus usuarios realizan tareas bien definidas y no requieren personalización ni acceso sin conexión a las aplicaciones. Los usuarios pueden ser trabajadores de tareas, como operadores de centros de llamadas o trabajadores del sector comercial, o usuarios que comparten estaciones de trabajo.
- Tipos de aplicaciones: cualquier aplicación.

Ventajas y consideraciones:

- Una solución fácilmente administrable y ampliable dentro del centro de datos.
- La solución de entrega de aplicaciones más rentable.
- Las aplicaciones alojadas se administran de manera centralizada y los usuarios no pueden modificar la aplicación, lo que proporciona una experiencia de usuario coherente, segura y fiable.
- Los usuarios deben estar conectados a la red para acceder a sus aplicaciones.

Experiencia de usuario:

- El usuario solicita una o varias aplicaciones desde StoreFront, desde su menú Inicio, o con una dirección URL que le ha sido suministrada.
- Las aplicaciones se entregan virtualmente y se muestran en alta definición en los dispositivos de usuario.

- Los cambios que haga el usuario se guardan cuando se cierra la sesión de aplicación, siempre que así lo indiquen los parámetros del perfil. Si no es así, los cambios se eliminan.

Procesamiento, alojamiento y entrega de aplicaciones:

- El procesamiento de las aplicaciones tiene lugar en las máquinas que las alojan (hosts), en lugar de procesarse en los dispositivos de usuario. Estas máquinas host pueden ser físicas o virtuales.
- Las aplicaciones y los escritorios residen en una máquina con SO multisesión.
- Las máquinas están disponibles a través de los catálogos de máquinas.
- Las máquinas incluidas en catálogos se organizan en grupos de entrega que se encargan de entregar un mismo conjunto de aplicaciones a grupos de usuarios.
- Las máquinas con SO multisesión admiten grupos de entrega que alojan o aplicaciones o escritorios, o ambos.

Administración de sesiones y asignación:

- Las máquinas de SO multisesión ejecutan varias sesiones desde una sola máquina para entregar varias aplicaciones y escritorios a varios usuarios conectados simultáneamente. Cada usuario requiere una sola sesión desde la que puede ejecutar todas sus aplicaciones alojadas.

  Por ejemplo, un usuario inicia una sesión y solicita una aplicación. Una sesión en esa máquina deja de estar disponible para otros usuarios. Un segundo usuario inicia una sesión y solicita una aplicación alojada en esa máquina. Ahora, hay una segunda sesión que ya no está disponible para otros usuarios. Si ambos usuarios solicitan aplicaciones adicionales, no se necesitarán sesiones adicionales porque un usuario puede ejecutar varias aplicaciones en la misma sesión. Si otros dos usuarios inician sesiones y solicitan escritorios, y hay dos sesiones disponibles en esa misma máquina, esa máquina usará cuatro sesiones para alojar a cuatro usuarios diferentes.
- Dentro del grupo de entrega al que esté asignado el usuario, se selecciona una máquina del servidor que tenga la menor carga. Se asigna, de forma aleatoria, una máquina con disponibilidad de la sesión para entregar aplicaciones a un usuario cuando este inicia sesión.

Aplicaciones alojadas en VM

Usar máquinas con SO de sesión única para entregar aplicaciones alojadas en VM

Caso de uso:

- Quiere una solución de entrega de aplicaciones basada en clientes que sea segura, que permita una administración centralizada y que admita muchos usuarios por servidor host. Quiere ofrecer a los usuarios unas aplicaciones que se muestran perfectamente en alta definición.
- Sus usuarios son contratistas externos o internos, colaboradores de terceros y otros miembros de equipo de carácter provisional. Los usuarios no necesitan acceso sin conexión a las aplicaciones alojadas.

- Tipos de aplicaciones: Aplicaciones que podrían no funcionar correctamente con otras aplicaciones o que podrían interactuar con el sistema operativo, como Microsoft .NET Framework. Estos tipos de aplicaciones son ideales para alojarlos en máquinas virtuales.

Ventajas y consideraciones:

- Las aplicaciones y los escritorios incluidos en la imagen se administran, alojan y ejecutan de forma segura dentro del centro de datos, con lo que se ofrece una solución de entrega de aplicaciones más rentable.
- Cuando el usuario inicia sesión, se le puede asignar aleatoriamente una máquina del grupo de entrega que está configurado para alojar una misma aplicación. También se puede asignar estáticamente una única máquina para entregar la aplicación a un único usuario cada vez que éste inicia una sesión. Las máquinas asignadas de forma estática permiten a los usuarios instalar y administrar sus propias aplicaciones en la máquina virtual.
- La ejecución de sesiones múltiples no se admite en máquinas de SO de sesión única. Por lo tanto, cada usuario que inicia una sesión consume una máquina dentro del grupo de entrega, y los usuarios deben estar conectados a la red para acceder a sus aplicaciones.
- Este método puede aumentar la cantidad de recursos de servidor necesarios para el procesamiento de las aplicaciones y aumentar la cantidad de almacenamiento necesaria para los discos Personal vDisk de los usuarios.

Experiencia de usuario:

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

Procesamiento, alojamiento y entrega de aplicaciones:

- Lo mismo que las máquinas con SO multisesión, excepto que son máquinas virtuales con SO de sesión única.

Administración de sesiones y asignación:

- Las máquinas con SO de sesión única ejecutan una única sesión de escritorio desde una única máquina. Al acceder únicamente a aplicaciones, un usuario puede usar varias aplicaciones (y no se limita a una sola aplicación). El sistema operativo percibe cada aplicación como una nueva sesión.
- En un grupo de entrega, cuando los usuarios inician sesión, pueden acceder a una máquina asignada estáticamente (el usuario siempre inicia sesión en la misma máquina), o bien, acceden una máquina asignada aleatoriamente que se selecciona en función de la disponibilidad de la sesión.

Escritorios VDI

Utilice máquinas con SO de sesión única para entregar escritorios VDI de Citrix Virtual Desktops.

Los escritorios VDI se alojan en máquinas virtuales y entregan a cada usuario un sistema operativo de escritorio.

Los escritorios VDI necesitan más recursos que los escritorios publicados de Citrix Virtual Apps, pero no es necesario que las aplicaciones instaladas en ellos sean compatibles con sistemas operativos de servidor. Además, según el tipo de escritorio VDI que elija, estos escritorios se pueden asignar a usuarios individuales. Esto permite a los usuarios un alto grado de personalización.

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

- **Escritorio aleatorio no persistente, también conocido como escritorio de VDI agrupado:** Cada vez que un usuario inicia sesión en uno de estos escritorios, se conecta a un escritorio seleccionado de un grupo de escritorios. Este grupo se basa en una sola imagen. Todos los cambios realizados en el escritorio se pierden tras reiniciarse la máquina.
- **Escritorio estático no persistente:** Durante el primer inicio de sesión, a un usuario se le asigna un escritorio proveniente de un grupo de escritorios (Todas las máquinas del grupo se basan en una sola imagen.) Después del primer uso, cada vez que el usuario inicie sesión para usar uno de estos escritorios, se conectará al mismo escritorio que le fue asignado la primera vez. Todos los cambios realizados en el escritorio se pierden tras reiniciarse la máquina.
- **Escritorio estático persistente:** A diferencia de otros tipos de escritorios VDI, los usuarios pueden personalizar completamente estos escritorios. Durante el primer inicio de sesión, a un usuario se le asigna un escritorio proveniente de un grupo de escritorios. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez. Los cambios realizados en el escritorio se conservan tras reiniciarse la máquina.

Acceso con Remote PC

Acceso con Remote PC es una funcionalidad de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), gracias a la cual las organizaciones pueden hacer que sus empleados accedan fácilmente a los recursos corporativos de forma remota y segura. La plataforma Citrix hace posible este acceso seguro al proporcionar a los usuarios acceso a sus PC físicos de oficina. Si los usuarios pueden acceder a sus PC de oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para hacer su trabajo. Acceso con Remote PC elimina la necesidad de introducir y proporcionar otras herramientas para adaptarse al teletrabajo. Por ejemplo, aplicaciones o escritorios virtuales y su infraestructura asociada.

Acceso con Remote PC utiliza los mismos componentes de Citrix DaaS que facilitan aplicaciones y escritorios virtuales. Como resultado, los requisitos y el proceso de implementación y configuración

de Acceso con Remote PC son los mismos que los necesarios para implementar Citrix DaaS para la entrega de recursos virtuales. Esta uniformidad ofrece una experiencia de administración homogénea y unificada. Los usuarios disfrutan de la mejor experiencia posible al utilizar Citrix HDX para la entrega de sesiones de PC de oficina.

Para obtener más información, consulte Acceso con Remote PC.

Introducción: Planificar y crear una implementación

May 17, 2024

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

Si no conoce los componentes, la terminología y los objetos utilizados en Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), consulte Citrix DaaS.

Para obtener una guía desde el punto de vista del cliente, vaya a Citrix Success Center. Success Center le ofrece una guía para las cinco etapas clave de lo que puede hacer con Citrix: planificación, construcción, implementación, administración y optimización.

- La información que contiene Success Center complementa a esta documentación de producto.
- Los artículos y las guías de Success Center ofrecen un panorama general de las soluciones disponibles. También contienen enlaces a detalles específicos de cada servicio de esta documentación de producto.

Si va a migrar desde una implementación de Citrix Virtual Apps and Desktops, consulte Migrar a la nube.

> **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.
>
> 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**.

Cómo utilizar este artículo

Para configurar la implementación de Citrix DaaS, complete las tareas que se resumen a continuación. Se proporcionan enlaces a los detalles de cada tarea.

Revise todo el proceso antes de comenzar la implementación, para familiarizarse con él. Este artículo también contiene enlaces a otras fuentes de información útiles.

> **Nota:**
>
> Si va a utilizar la interfaz de Distribución rápida para aprovisionar máquinas de Microsoft Azure, siga las instrucciones de instalación de Introducción a Distribución rápida.

Planificación y preparación

Puede utilizar la guía Plan de Success Center para establecer objetivos, definir casos de uso y metas empresariales, identificar riesgos potenciales y crear un plan de proyecto.

En la documentación de Citrix Tech Zone, consulte una guía de prueba de concepto paso a paso para este servicio.

Registrarse

Regístrese para obtener una cuenta de Citrix y solicite una demo de Citrix DaaS.

Configurar una ubicación de recursos

Una ubicación de recursos contiene los recursos necesarios para entregar aplicaciones y escritorios a los usuarios. La creación de ubicaciones de recursos permite a DaaS utilizar esos recursos. Para obtener más información sobre las ubicaciones de recursos, consulte Conectarse a Citrix Cloud.

Antes de crear máquinas, debe conectar una ubicación de recursos a DaaS:

- Las máquinas unidas a un dominio requieren que tenga Cloud Connectors instalados en la ubicación de recursos. En este caso, puede hacer lo siguiente:
  - Crear catálogos unidos a Active Directory locales
  - Crear catálogos unidos a Azure Active Directory
  - Crear catálogos unidos a Azure Active Directory híbrido

  Para tener alta disponibilidad, se recomienda instalar dos Cloud Connectors en cada ubicación de recursos. Consulte Instalar el Cloud Connector.

  Más información:

  - ¿Qué son las ubicaciones de recursos y los Cloud Connectors?
  - Vídeo sobre la instalación de Cloud Connectors:

- Las máquinas que no están unidas a un dominio no requieren Cloud Connectors, pero requieren que Rendezvous V2 esté habilitado. El protocolo Rendezvous permite a los VDA eludir los Cloud Connectors para conectarse de forma directa y segura con DaaS. Consulte Rendezvous V2. En este caso, puede hacer lo siguiente:
  - Crear catálogos que no estén unidos a ningún dominio

Si utiliza la interfaz de Distribución rápida para aprovisionar máquinas virtuales de Azure, Citrix crea la ubicación de recursos y Cloud Connectors por usted.

Crear una conexión a la ubicación de recursos

Después de agregar una ubicación de recursos y Cloud Connectors, cree una conexión con la ubicación de recursos mediante la interfaz de Configuración completa de Citrix DaaS.

Este paso no es necesario en ninguno de los siguientes casos:

- Construye una implementación simple de prueba de concepto
- Utiliza la interfaz de Distribución rápida para aprovisionar máquinas virtuales de Azure.

Más información:

- ¿Qué son los hosts?
- ¿Qué son las conexiones de host?

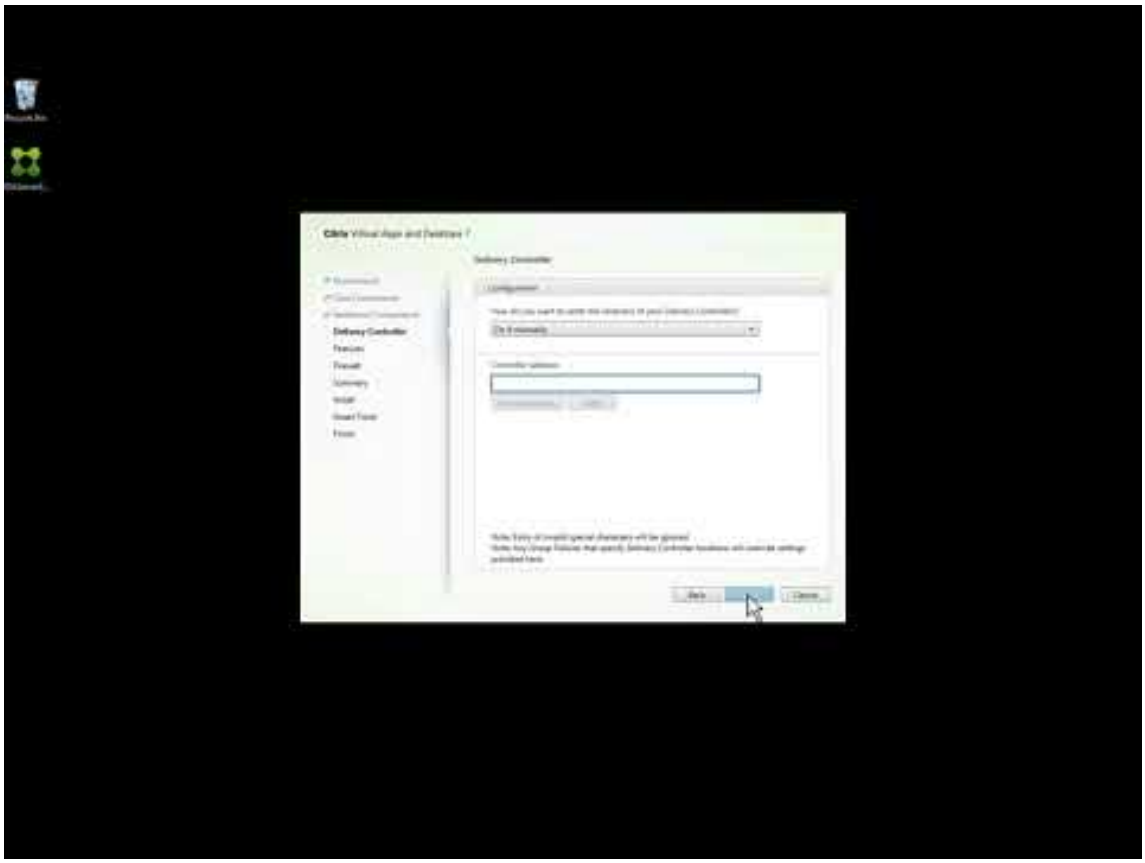
Instalar VDA

Cada máquina que entrega aplicaciones y escritorios a los usuarios debe tener instalado un Virtual Delivery Agent (VDA) de Citrix.

- Para una implementación simple de prueba de concepto, descargue e instale un VDA en una máquina.
- Si utiliza una imagen para aprovisionar las VM, instale un VDA en ella.
- Para implementaciones de acceso con Remote PC, instale la versión básica de VDA para SO de sesión única en cada PC físico de la oficina.

Manuales y más información:

- ¿Qué son los VDA?
- Preparación de la instalación e instrucciones
- Instalación de VDA mediante la línea de comandos
- Vídeo sobre la descarga e instalación de un VDA:

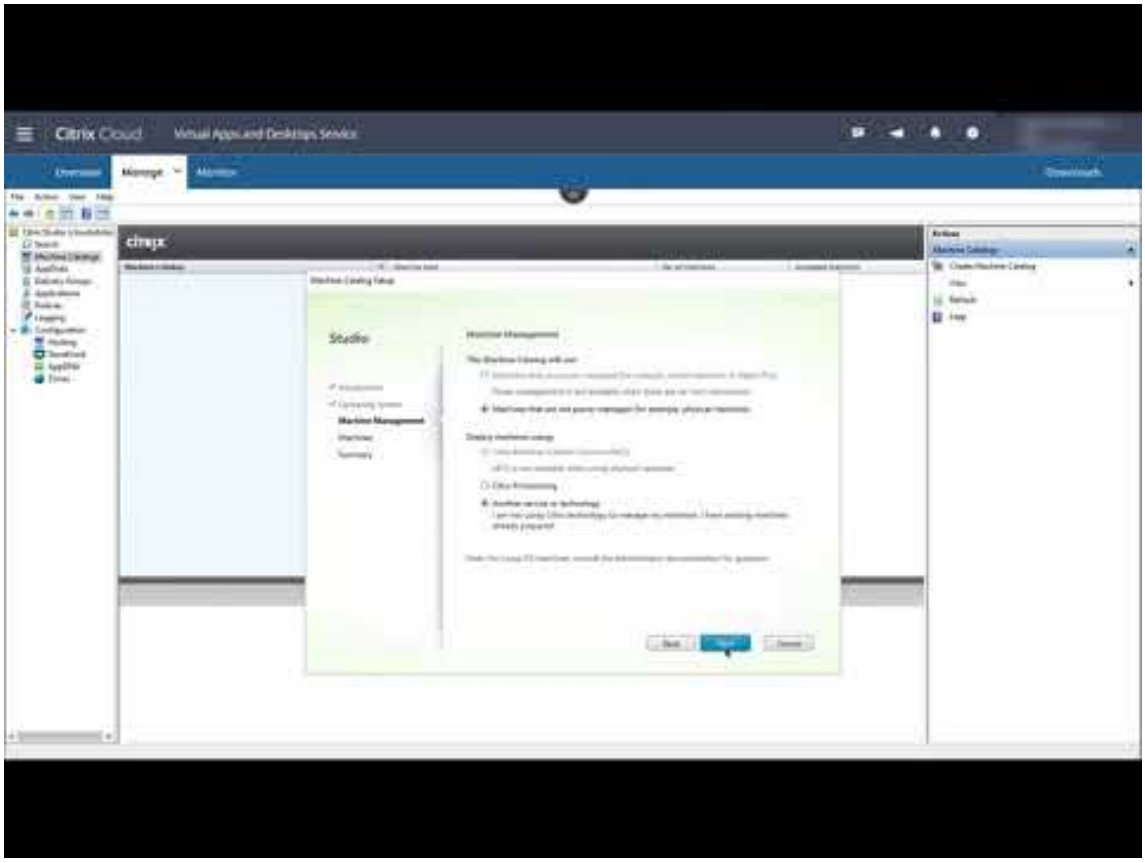


Crear un catálogo

Después de crear una conexión a la ubicación de recursos (si fuera necesario), cree un catálogo. Si utiliza la interfaz de Configuración completa, el flujo de trabajo le guiará automáticamente a este paso.

Manuales y más información:

- ¿Qué son los catálogos?
- Crear un catálogo
- Utilice la interfaz de Distribución rápida para implementar un catálogo que contenga máquinas virtuales de Azure.
- Vídeo sobre la creación de un catálogo mediante la interfaz de configuración completa para la administración:



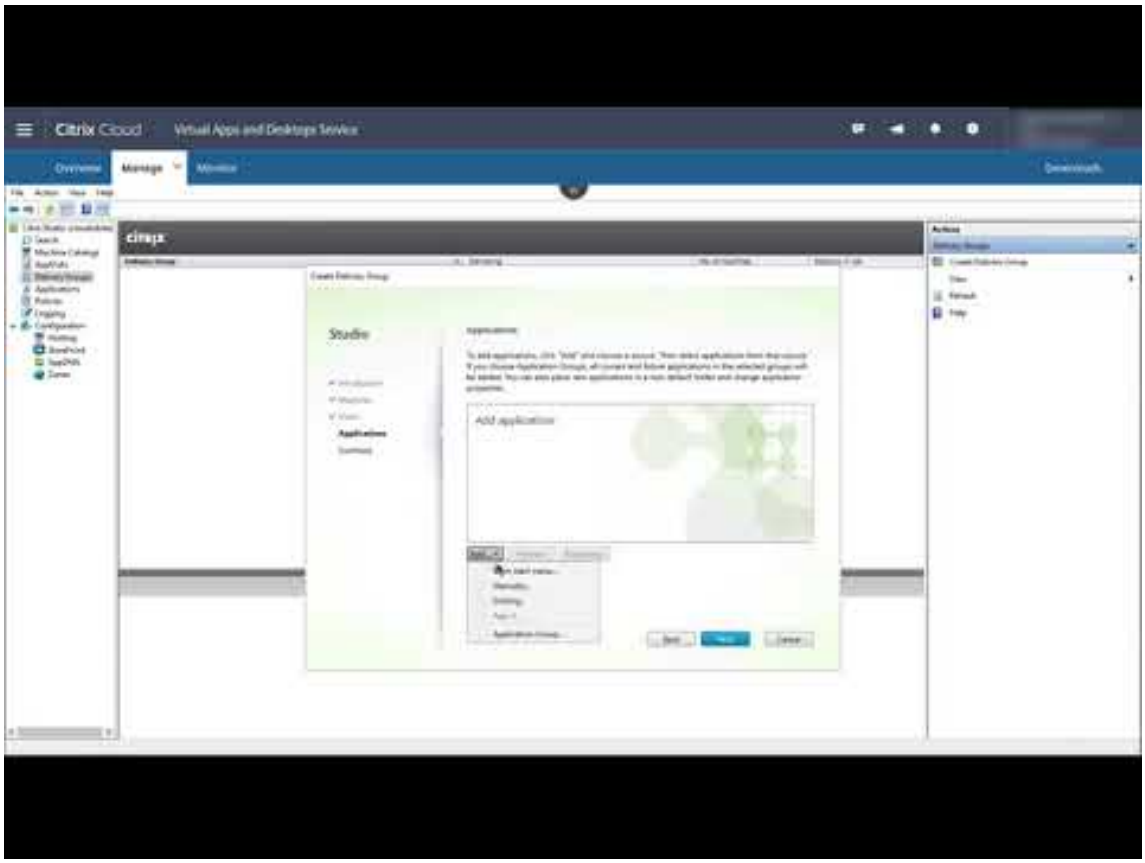
Crear un grupo de entrega

Después de crear el primer catálogo, el flujo de trabajo de **Administrar** le guiará para crear un grupo de entrega.

Este paso no es necesario si utiliza la interfaz de Distribución rápida para aprovisionar máquinas virtuales de Azure.

Manuales y más información:

- ¿Qué son los grupos de entrega?
- Crear un grupo de entrega
- Vídeo sobre cómo crear un grupo de entrega:



Implementar otros componentes y tecnologías

Después de completar las tareas anteriores para configurar la implementación de Citrix DaaS, siga las instrucciones del área Build de Citrix Success Center. Encontrará información sobre el aprovisionamiento y la configuración de otros componentes y tecnologías en la solución de Citrix, por ejemplo:

- directivas de Citrix
- StoreFront
- App Layering
- Workspace Environment Management (WEM) Service
- Citrix Gateway Service
- Zonas

- Servicio de autenticación federada (FAS)

Complete otras tareas que se aplican a su configuración. Por ejemplo, si piensa entregar cargas de trabajo de Windows Server, configure un servidor de licencias de Microsoft RDS.

Iniciar aplicaciones y escritorios

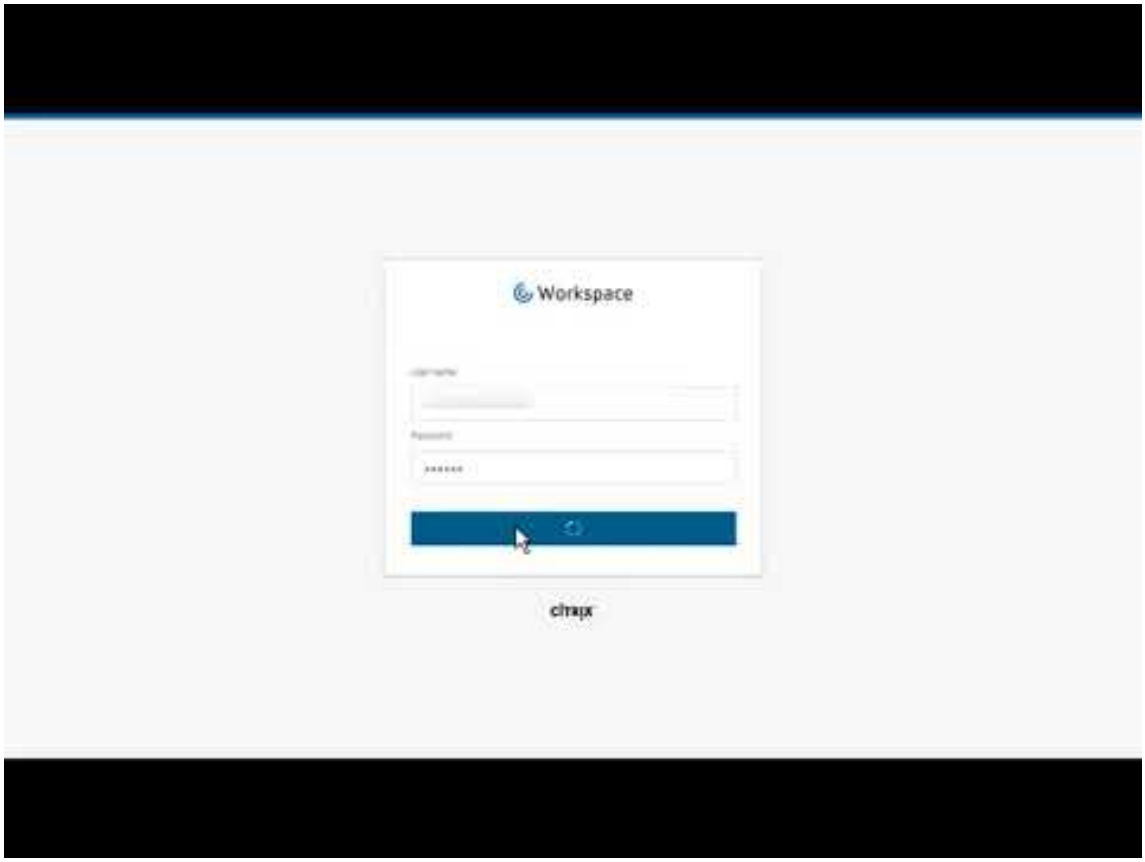
Después de configurar la implementación, la publicación se produce automáticamente. Las aplicaciones y escritorios configurados están disponibles para los usuarios en su Citrix Workspace. Un usuario no tiene más que ir hacia la URL de Workspace y seleccionar una aplicación o escritorio para que se inicien inmediatamente.

Envíe la URL del espacio de trabajo a los usuarios. Puede encontrar la URL del espacio de trabajo en dos ubicaciones:

- En la consola de Citrix Cloud, seleccione **Configuración de Workspace** en el menú de la esquina superior izquierda. La ficha **Acceso** contiene la URL del espacio de trabajo.
- En la página **Vista general** de Citrix DaaS, la URL del espacio de trabajo aparece cerca de la parte inferior de la página.

Más información:

- Vídeo sobre cómo los usuarios inician aplicaciones y escritorios desde Workspace:



Más información

La serie Citrix Cloud Learning ofrece cursos educativos organizados según su ruta:

- Si es la primera vez que usa Citrix DaaS, consulte New to Citrix DaaS Learning Path.
- Si va a migrar desde una implementación de Citrix Virtual Apps and Desktops, consulte Migrating Citrix DaaS to Citrix Cloud Learning Path.

Registrarse en Citrix DaaS

May 23, 2022

Introducción

Puede suscribirse a Citrix DaaS a través de Citrix o a través de Azure Marketplace.

Si piensa usar Azure administrado por Citrix, también puede realizar un pedido de Citrix Azure Consumption Fund a través de Citrix o a través de Azure Marketplace.

- Al realizar un pedido a través de Citrix, puede realizar un pedido de Citrix DaaS y Citrix Azure Consumption Fund al mismo tiempo.
- Al hacerlo a través de Azure Marketplace, primero se realiza un pedido de Citrix DaaS. A continuación, puede realizar otro pedido para Citrix Azure Consumption Fund.

Si ahora realiza un pedido de Citrix DaaS solamente, puede realizar un pedido de Citrix Azure Consumption Fund más tarde, ya sea a través de Azure Marketplace o de su representante de cuenta de Citrix.

Demostraciones y pruebas

Puede probar Citrix DaaS mediante una solicitud a través de Citrix. Desde una prueba puede pasarse a una suscripción de servicio de pago.

Durante una prueba, puede utilizar, si quiere, una suscripción a Azure administrado por Citrix para catálogos, imágenes y conexiones de red. Si tiene recursos administrados por Citrix en el momento de pasarse a una suscripción de pago, debe adquirir fondos de consumo o eliminar dichos recursos administrados por Citrix. Si no adquiere fondos de consumo, esos recursos se eliminan automáticamente, lo que podría afectar a los usuarios.

Si actualmente está suscrito a un servicio de Citrix DaaS

En general, una cuenta de Citrix Cloud le permite suscribirse a solo uno de los servicios de Citrix DaaS (o a una edición) por OrgID de Citrix. Por ejemplo, puede suscribirse a la edición Premium de Citrix DaaS O a Citrix DaaS para Azure, pero no a ambas.

Si se ha suscrito a Citrix DaaS y quiere suscribirse a este servicio, tiene dos opciones:

- Suscribirse a este servicio con otra cuenta de Citrix Cloud (OrgID).
- Cancelar la instancia de Citrix DaaS que ya tiene y, a continuación, realizar un pedido de este servicio. Para obtener instrucciones sobre la cancelación de servicios, consulte CTX239027.

Realizar pedidos a través de Citrix

Puede realizar un pedido de este servicio (y Citrix Azure Consumption Fund) a través de Citrix Cloud o a través de su representante de cuenta de Citrix.

A través de Citrix Cloud:

- Siga las instrucciones indicadas en Registrarse en Citrix Cloud para obtener una cuenta de Citrix Cloud y un ID de organización.

- Puede solicitar una demo de Citrix DaaS. En el mosaico de Citrix DaaS, haga clic en **Solicitar demostración**. Proporcione la información solicitada.

  Un representante de Citrix se pondrá en contacto con usted para analizar sus requisitos, su entorno y sus planes. Según la evaluación de nuestro representante, tendrá autorización para participar en una demostración de administrador o en una evaluación de prueba de concepto. Para obtener más información, consulte Pruebas de servicio de Citrix Cloud.

Cuando obtenga la autorización para realizar una prueba, el texto del mosaico de Citrix DaaS de la consola de Citrix Cloud cambia a **Administrar**.

Realizar pedidos a través de Azure Marketplace

Puede realizar un pedido de estas ofertas de Citrix a través de Azure Marketplace:

- Citrix DaaS para Azure
- Citrix DaaS edición Advanced
- Citrix DaaS edición Premium
- Workspace Premium Plus

Si piensa alojar las cargas de trabajo de Citrix Virtual Apps and Desktops en Microsoft Azure y quiere utilizar una suscripción de Azure administrado por Citrix, solicite Citrix Azure Consumption Fund después de realizar un pedido de Citrix DaaS o Workspace Premium Plus.

Con Citrix Azure Consumption Fund, se le cobra cada mes por su consumo, que puede variar según los recursos de alojamiento que elija y las horas de uso. Puede revisar el uso de los fondos de consumo a través de Citrix Cloud.

Desde Azure Marketplace:

- No se puede combinar Citrix DaaS y los fondos de consumo en un mismo pedido.
- El proceso de los pedidos de Citrix Azure Consumption Fund es esencialmente el mismo que el de Citrix DaaS, pero antes debe haber realizado un pedido de este último.

Requisitos para realizar pedidos a través de Azure Marketplace

- 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 ninguna cuenta de Citrix Cloud, siga las instrucciones indicadas en Registrarse en Citrix Cloud.
- Una cuenta de Azure y al menos una suscripción a Azure en esa cuenta.

Procedimiento para realizar pedidos a través de Azure Marketplace

Siga este procedimiento para realizar el pedido de Citrix DaaS o Workspace Premium Plus a través de Azure Marketplace (si quiere utilizar Azure administrado por Citrix, realice otro pedido de Citrix Azure Consumption Fund después de realizar el pedido de Citrix DaaS).

1. Inicie sesión en Azure Marketplace con las credenciales de su cuenta de Azure.
2. Busque la oferta de Citrix para la que quiere realizar un pedido y vaya hasta ella.
3. Seleccione **Get it now**.
4. En el mensaje **One more thing**, rellene la información requerida, marque la casilla de consentimiento y, a continuación, seleccione **Continue**.
5. Revise las fichas que contienen información sobre el producto, los planes, los precios y el uso. Cuando tenga todo listo, seleccione un plan (si hay más de uno disponible) y, a continuación, seleccione **Set up + subscribe**.
6. En la ficha **Basics**:
   - **Subscription:** Indica el plan seleccionado.
   - **Resource group:** Seleccione o cree un grupo de recursos.
   - **Name:** Introduzca un nombre para el pedido de suscripción, de modo que pueda identificarlo fácilmente más adelante.
   - La información indicada en **Plan** muestra el precio del plan seleccionado según el plazo de facturación. Para cambiar el plazo del plan, seleccione **Change plan**. Seleccione el plazo que quiera y seleccione **Change plan**.
7. En la ficha **Review + subscribe**, revise la información de contacto y actualícela si es necesario. Revise la información básica de la suscripción. Seleccione **Subscribe**.
8. En la página **Subscription in progress**, seleccione **Configure account now** (si el botón no está habilitado, espere un momento). Se le llevará a una página de activación de Citrix.
9. En la página de activación:
   - Use el enlace **Sign in** 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.
   - Acepte los términos y condiciones y, a continuación, seleccione **Activate Order**.

Después de realizar el pedido a través de Azure Marketplace

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 utilizar Citrix DaaS.

Gestionar un pedido de Citrix Azure Consume Fund no lleva mucho tiempo. Cuando se notifica a Citrix del pedido, aparece una pancarta en la consola de Citrix DaaS que indica que se le preparará una suscripción a Azure administrado por Citrix.

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

Realizar pedidos a través de Google Cloud Marketplace

Puede realizar pedidos de estas ofertas de Citrix a través de Google Cloud Marketplace:

- Citrix DaaS Standard para Google Cloud
- Citrix DaaS Premium para Google Cloud

Necesita lo siguiente para realizar pedidos a través de Google Cloud Marketplace:

- 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 ninguna cuenta de Citrix Cloud, siga las instrucciones indicadas en Registrarse en Citrix Cloud.
- Una cuenta de Google Cloud y al menos una suscripción de Google Cloud en esa cuenta.

Para realizar su pedido:

1. Iniciar sesión en Google Cloud Marketplace
2. Siga las instrucciones de la página Citrix DaaS para Google Cloud para realizar la compra.

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 utilizar Citrix DaaS.

No elimine el recurso de Citrix DaaS en Google Cloud. Al eliminar ese recurso, se cancela la suscripción.

A continuación

Una vez que se haya gestionado el pedido, continúe con los pasos siguientes indicados en Planificar y crear una implementación.

Por ejemplo:

- Si aún no ha configurado su hipervisor o servicio de nube, o Active Directory, consulte Configurar ubicaciones de recursos.
- Si su entorno de host y Active Directory ya están configurados, consulte Crear una conexión.

Citrix HDX Plus para Windows 365

April 18, 2024

Citrix HDX Plus para Windows 365 le permite integrar Citrix Cloud en Windows 365 para utilizar las tecnologías de Citrix HDX y ofrecer una experiencia mejorada y más segura en PC en la nube Windows 365, además de otros servicios de Citrix Cloud para mejorar la capacidad de administración.

Para obtener más información, consulte Citrix HDX Plus para Windows 365.

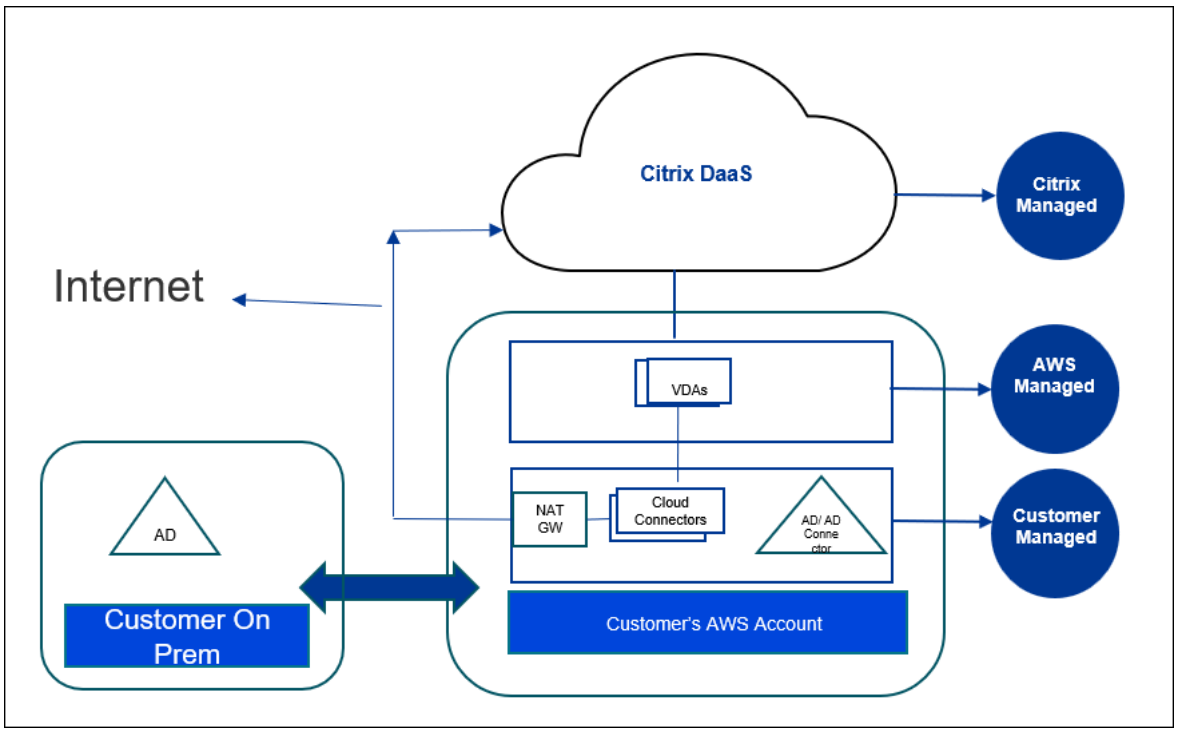
Citrix DaaS for Amazon WorkSpaces Core (Tech Preview)

May 17, 2024

Introducción

En este artículo se describe cómo preparar y crear una implementación con Citrix for Amazon WorkSpaces Core. Amazon WorkSpaces Core está ubicado en Amazon Web Services (AWS).

A continuación se muestra una representación de la implementación de AWS y su administración con Citrix DaaS:



Acerca de esta Tech Preview

- Para obtener asistencia durante esta Technical Preview, contacte con AWS Support o Citrix Support.
- Para administrar el entorno Citrix durante esta Tech Preview, utilice únicamente la consola **Administrar** de Citrix DaaS. No se admite ninguna API de Citrix o AWS durante esta Tech Preview. (Citrix agradece sus comentarios sobre las API que quiera utilizar en el futuro).

Preparar y crear una implementación

La lista de verificación de distribuciones de la interfaz de **Distribución rápida** contiene enlaces a los procedimientos 1 a 5.

1. Antes de empezar, complete los requisitos previos en Citrix Cloud y AWS.
2. Crear una ubicación de recursos en Citrix Cloud. (Este procedimiento también se incluye como requisito previo).
3. Conecte su cuenta de AWS. Este procedimiento habilita los permisos para que Citrix DaaS pueda conectarse a AWS.
4. Cree una conexión de directorio. Este procedimiento configura una conexión que permite el acceso al Active Directory de su organización.
5. Importe una imagen. Este procedimiento le permite crear una experiencia de escritorio para sus usuarios.

6. Cree una implementación. Este procedimiento especifica las máquinas que se van a implementar y los usuarios que pueden acceder a ellas a través de Citrix Workspace.

Antes de comenzar

Asegúrese de haber completado las siguientes tareas antes de empezar a preparar y crear la implementación.

Hay una excepción: la creación de una ubicación de recursos en Citrix Cloud se muestra como requisito previo. También es el primer procedimiento de la lista de verificación de implementación. Por lo tanto, si crea la ubicación de recursos como parte de los requisitos previos, omita ese procedimiento en la secuencia de la lista de verificación. Del mismo modo, complete ese procedimiento de la lista de verificación si no lo hizo antes.

Requisitos previos para completar en Citrix Cloud

- Cree una cuenta de Citrix Cloud y suscríbase a Citrix DaaS. Su representante de Citrix puede ayudarle con esto. Su representante también habilita esta función de Tech Preview para usted.
- Cree una ubicación de recursos de Citrix Cloud. (Este procedimiento también está vinculado en la interfaz de Distribución rápida).

Requisitos previos para completar en AWS

- Cree una cuenta de usuario de AWS. La cuenta debe tener:
  - Permisos de rol para el cliente API de Citrix.
  - Permisos de acceso programático. Para obtener más información, consulte Permisos de acceso programático a la cuenta de AWS.
  - Cree el rol Workspaces_DefaultRole. Para obtener más información, consulte Crear el rol Workspaces_DefaultRole.
- En su Active Directory:
  - Use la opción AD Connector para almacenar y administrar información. Para obtener más información, consulte AD Connector.
  - Cree una unidad organizativa en la que se crearán las máquinas virtuales. Esa unidad organizativa debe tener una directiva de Citrix para la comunicación con los Cloud Connector y Citrix Cloud. Consulte la sección Referencia para obtener información detallada.
  - Establezca una directiva de grupo para la configuración de Citrix Cloud Connector:

1. Descargue la consola de administración de directivas de grupo más reciente proporcionada por Citrix (CitrixGroupPolicyManagement_64.msi) desde el sitio de descargas de Citrix.
2. Instale el MSI (esa máquina debe tener Visual Studio 2015 runtime instalado). A continuación, cree una directiva de Citrix que contenga la configuración de la directiva Controllers. Ese parámetro especifica las direcciones de Cloud Connector.

- Cree una puerta de enlace NAT o utilice una ya existente. Para obtener más información, consulte NAT Gateway.
- Cree o use uno o más grupos de seguridad existentes que permitan a los Citrix Cloud Connector comunicarse con las máquinas virtuales implementadas. Para obtener más información, consulte Controlar el tráfico a los recursos de AWS mediante grupos de seguridad
- Abra un tíquet de AWS Support para habilitar BYOL en su cuenta. Para empezar, póngase en contacto con su administrador de cuentas o representante de ventas de AWS, o contacte con el Centro de asistencia de AWS. Su contacto verificará y habilitará BYOL. Para obtener más información, consulte Habilitar BYOL en su cuenta para BYOL mediante la consola de Amazon WorkSpaces.

  > **Nota:**
  >
  > Actualmente, las versiones Windows 10 N y Windows 11 N no son compatibles con BYOL.

  - El uso de la función Citrix DaaS for Amazon WorkSpaces Core habilitará automáticamente la función Bring Your Own Protocol (BYOP) en AWS WorkSpaces Core.
  - Tenga suficientes licencias de Windows 10 para los escritorios que se crearán. Para obtener más información, consulte Traiga sus propias licencias (BYOL) de escritorio de Windows.

Preparación general

Revise cada procedimiento antes de empezar. Ventaja: esto ayudará a completar fácilmente los procesos.

Crear una ubicación de recursos

Cree una ubicación de recursos en Citrix Cloud.

- Una ubicación de recursos contiene dos o más Cloud Connector que se comunican con Citrix Cloud. Los servidores en los que instale los Cloud Connector deben estar en una VPC EC2, unidos a un dominio y deben tener conectividad a Internet. Los Cloud Connector deben estar en la misma VPC que el directorio que planea usar.

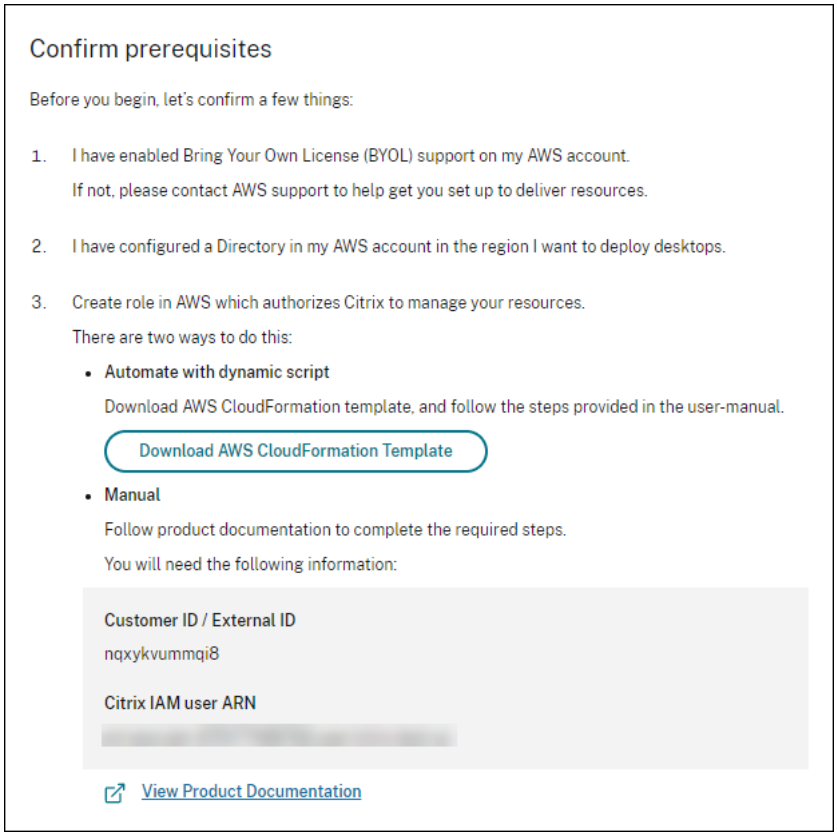
- Para obtener más información sobre los Cloud Connector, consulte Citrix Cloud Connector y cómo aprovisionarlos.
- La ubicación de recursos también puede contener sus servidores de Active Directory. Para obtener más información, consulte Conectar Active Directory a Citrix Cloud.

Conectar la cuenta de AWS

Este procedimiento habilita los permisos para que Citrix DaaS se conecte a AWS.

Para crear AssumeRole para AWS WorkSpaces Core, siga estos pasos:

1. En Citrix DaaS, en **Administrar > Distribución rápida > Cuentas**, haga clic en **Conectar cuenta**.
2. En la página de la **cuenta de Connect AWS**, en **Confirmar requisitos previos**, haga clic en **Descargar la plantilla de AWS CloudFormation**. Después de descargar la plantilla, haga clic en **Siguiente**.



1. Para cargar la plantilla, consulte Crear AssumeRole para la integración de AWS Workspace Core.
2. En la página **Autenticar cuenta**, agregue el **nombre de recurso de Amazon** (ARN) generado en el campo **ID de rol**, introduzca un nombre en el campo **Nombre** y haga clic en **Siguiente**. Se abre la página **Seleccionar región**.

El **ID de rol** corresponde al ARN del rol que autorizará a Citrix a administrar los recursos. El ID de rol se encuentra en la consola de administración de AWS. Para acceder al mismo, vaya a **IAM > Roles**.

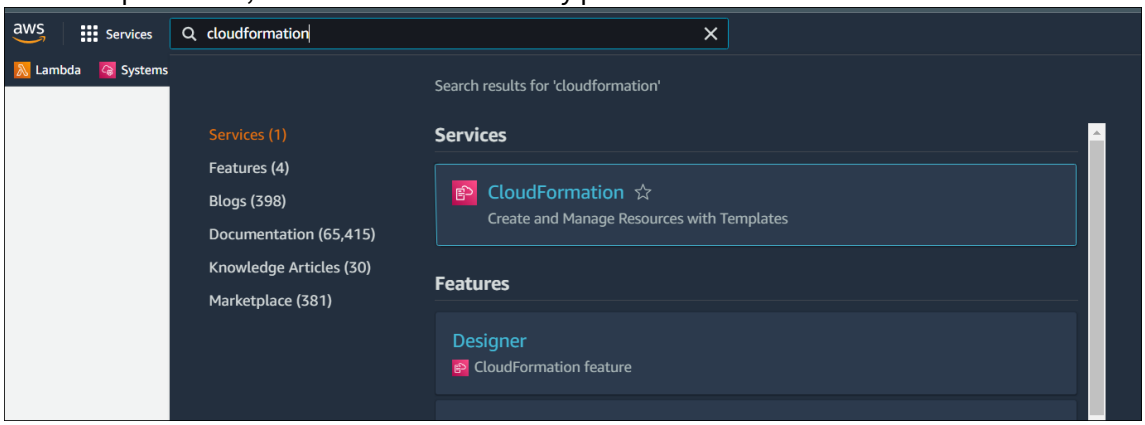
Si está utilizando el script `CloudFormation`, vaya a CloudFormation y haga clic en la pila correspondiente que se utilizó para crear el rol. Navegue hasta la ficha **Recursos** y haga clic en el recurso con LogicalID `CitrixAssumeRole`.

> **Nota:**
>
> No es posible conectar dos cuentas de la misma región para la misma cuenta de AWS.

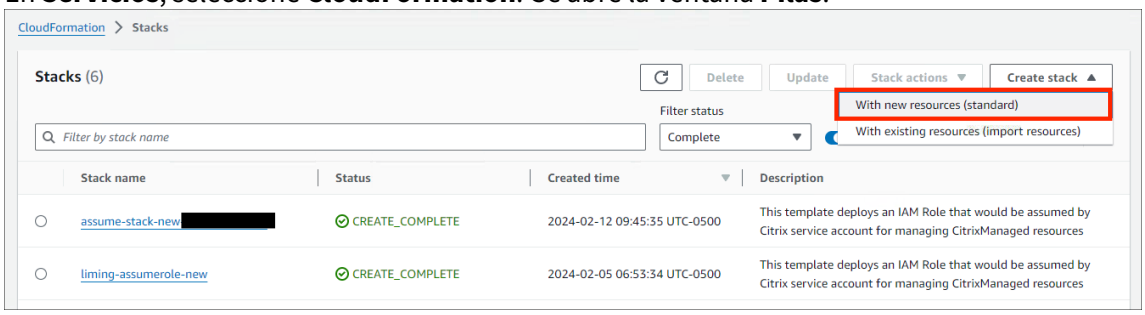
3. En la página **Elegir región**, seleccione la región en la que quiere implementar sus escritorios y haga clic en **Siguiente**.
4. En la página **Configurar compatibilidad con BYOL**, para configurar la disponibilidad de BYOL, se requiere una interfaz de red de administración que esté conectada a una red segura de Amazon. Seleccione un rango de direcciones IP en las que buscar para usarlas como esa interfaz. A continuación, seleccione Mostrar bloques de CIDR disponibles. Si los bloques CIDR están disponibles en el rango de búsqueda seleccionado, seleccione un bloque de CIDR disponible. Cuando se selecciona correctamente un intervalo de direcciones de búsqueda y un bloque de CIDR disponible, se muestra un mensaje de confirmación. Haga clic en **Siguiente**.
5. En la página **Resumen**, revise la información que haya especificado. Puede regresar a las páginas anteriores. Cuando haya terminado, haga clic en **Finalizar**.
   El proceso de conexión puede tardar varias horas en completarse.

Crear AssumeRole para la integración de AWS Workspace Core

1. En la ventana del explorador web, abra el sitio web de **Amazon Web Services** e inicie sesión.
2. En el campo **Buscar**, escriba **cloudformation** y presione **Entrar**.



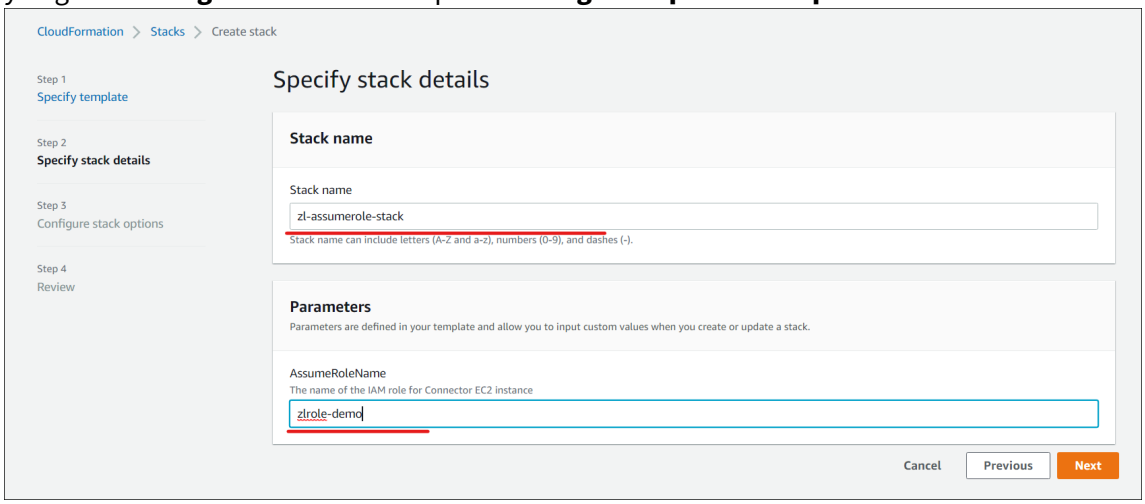
3. En **Servicios**, seleccione **CloudFormation**. Se abre la ventana **Pilas**.



4. Haga clic en **Crear pila > Con nuevos recursos (estándar)** en la esquina superior derecha. Se abre la ventana **Crear pila**.

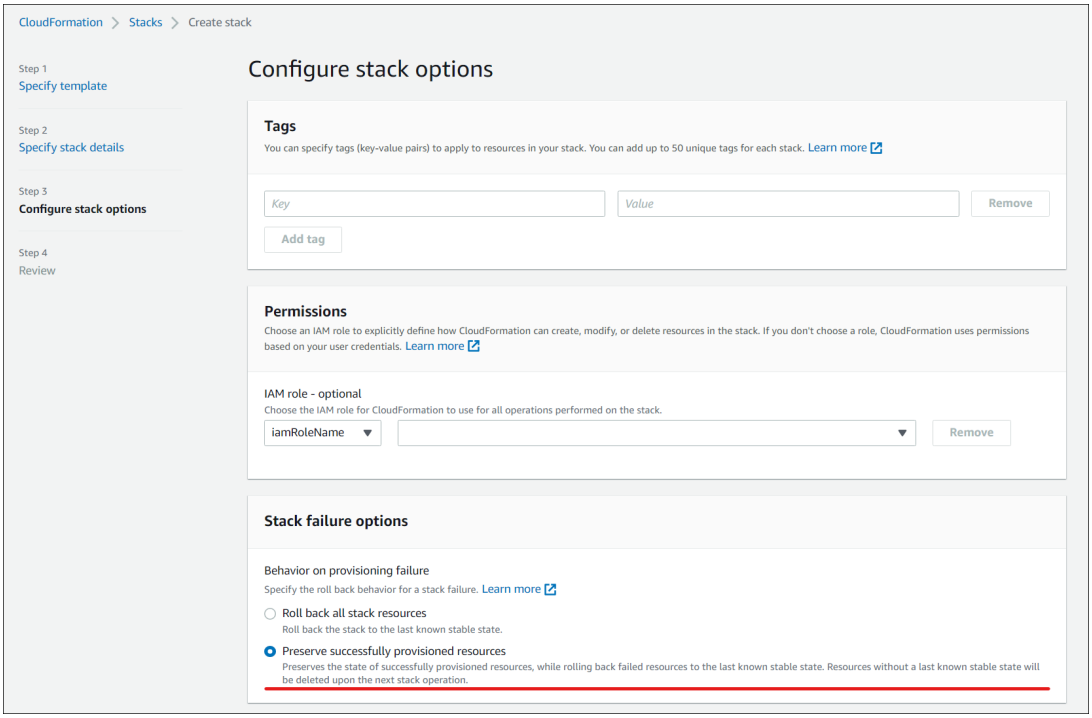
   a) En **Requisito previo: preparar plantilla**, seleccione **La plantilla está lista**.
   b) En **Especificar plantilla**, haga clic en **Cargar un archivo de plantilla > Elegir archivo** y después haga clic en **Siguiente**. Se abre el panel **Especificar detalles de la pila**.

5. En el panel **Especificar detalles de la pila**, introduzca un **Nombre de pila** y **AssumeRoleName**, y haga clic en **Siguiente**. Se abre el panel **Configurar opciones de pila**.

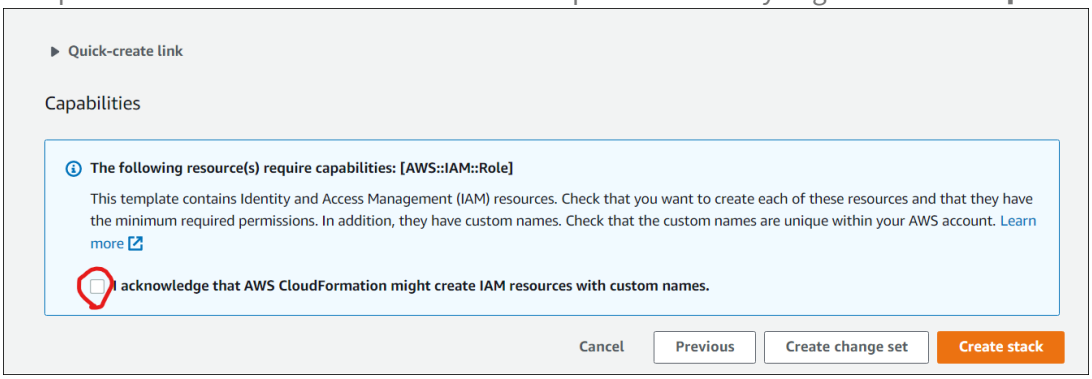


Nota:

- En el panel **Configurar opciones de pila**, seleccione la opción **Conservar los recursos aprovisionados correctamente**. Esta opción conserva el estado de los recursos aprovisionados correctamente. Los recursos sin un último estado estable conocido se eliminan en la siguiente operación de pila.

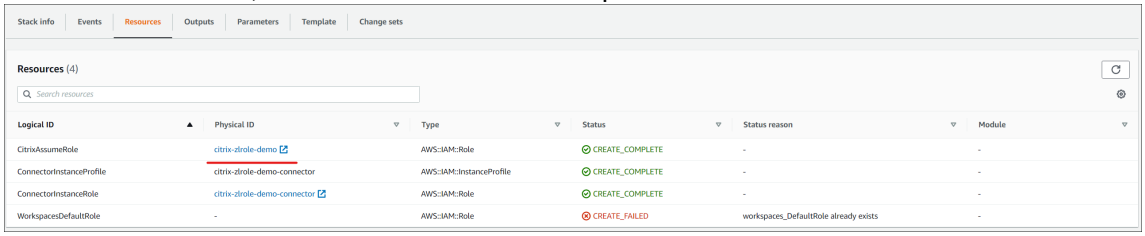


- En la ventana emergente **Capacidades**, seleccione la casilla **Reconozco que AWS CloudFormation podría crear recursos de IAM con nombres personalizados** y haga clic en la ventana emergente Capacidades, seleccione la casilla Reconozco que AWS CloudFormation podría crear recursos de IAM con nombres personalizados y haga clic en **Crear pila**.

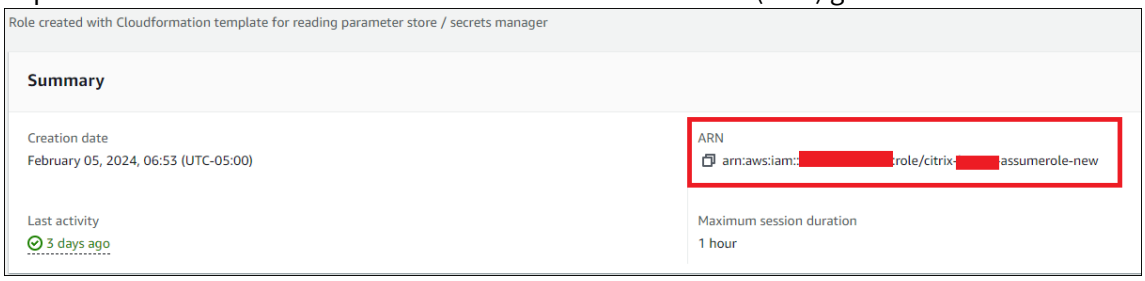


La creación de la pila puede fallar al final porque **Workspace_DefaultRole** ya se había creado. Esto no afecta a la creación de **AssumeRole**.

1. La ficha **Eventos** muestra el estado de la pila creada.
2. En la ficha **Recursos**, seleccione el ID físico correspondiente al **AssumeRole** creado.



3. El panel Resumen muestra el **nombre de recurso de Amazon** (ARN) generado.



4. Reanude el procedimiento desde el paso 4 de Conectar su cuenta de AWS

Crear una conexión de directorio

> **Nota:**
>
> Anule el registro de su directorio de AWS al principio de este paso. Tras crear una conexión de directorio con Citrix DaaS, el directorio seleccionado se registra para crear Amazon WorkSpaces con Citrix DaaS.

Este procedimiento crea una conexión que permite el acceso al Active Directory de su organización.

Requisitos previos:

- Una ubicación de recursos que contiene dos Cloud Connector.
- Un grupo de seguridad.
- Una unidad organizativa en su Active Directory.

Para obtener información sobre los requisitos previos, consulte Antes de empezar.

Puede iniciar este procedimiento desde uno de estos dos lugares:

- Un enlace en la lista de verificación para empezar.
- En la consola **Administrar** de DaaS, seleccione **Distribución rápida** en el panel izquierdo y **Conexiones de directorio** en la sección **Amazon WorkSpaces Core**. Después seleccione **Crear conexión de directorio**.

Siga la secuencia de **Crear conexión de directorio**:

1. **Confirme los requisitos previos:**si ha completado los requisitos previos, haga clic en **Siguiente**.
2. **Conectar directorio:** seleccione la ubicación del recurso, la cuenta y el directorio. (La cuenta seleccionada debe tener al menos un directorio).
    - Seleccione dos subredes en las que se implementarán las máquinas de escritorio. Las subredes deben estar en las zonas de disponibilidad adecuadas.
    - Especifique un nombre descriptivo para esta conexión.

- Cuando haya terminado, haga clic en **Siguiente**.

3. **Parámetros de la máquina virtual:** los parámetros que seleccione se aplican a todas las máquinas virtuales que usan esta conexión de directorio.
   - La unidad organizativa seleccionada debe coincidir con la unidad organizativa a la que se dirigen las Directivas de grupo Citrix.
   - Seleccione un grupo de seguridad.
   - Indique si quiere conceder privilegios de administrador a cada usuario asignado a máquinas virtuales.

Importar una imagen

Este procedimiento le permite crear una experiencia de escritorio para sus usuarios.

Requisitos previos para importar la imagen:

- Debe ser una imagen de EC2.
- Debe tener instalado un Citrix Virtual Delivery Agent (VDA).
- Debe estar preparado para BYOL. Hay un script de BYOL disponible en: BYOLChecker.zip.

Para importar la imagen, siga estos pasos:

1. **Confirme los requisitos previos:** después de los pasos de los requisitos previos, haga clic en **Siguiente**. (Si no ha preparado la imagen para BYOL, puede descargar el script desde esta página). Para obtener más información, consulte Requisitos.
2. **Elija una imagen** e introduzca un nombre descriptivo para esa imagen. Seleccione la cuenta, la AMI y agregue una descripción. Haga clic en **Siguiente**. Se abre la página **Resumen**.
3. En la página **Resumen**, revise la información que ha proporcionado. Tras la verificación, seleccione **Importar imagen**.

   > **Nota:**
   >
   > La importación de una imagen podría tardar varias horas.

Integrar la imagen de Microsoft Office 2019 al importar una imagen

Para integrar la imagen de Microsoft Office 2019 al importar una imagen:

1. En **Web Studio > Distribución rápida**, haga clic en **Imágenes**.
2. En **Mis imágenes**, haga clic en **Importar imagen**.
3. En **Importar imagen > Requisitos previos**, haga clic en **Siguiente: elegir imagen**.
4. En **Importar imagen > Elegir imagen:**

- Seleccione una cuenta en el menú desplegable **Cuenta**.
- Seleccione una AMI en el menú desplegable **AMI**.
- Introduzca el nombre de la imagen en el campo **Nombre**.
- Seleccione **Incluir Microsoft Office 2019 Professional Plus** en la imagen.
- Introduzca una descripción en el campo **Descripción**.

5. En **Importar imagen > Elegir imagen**, haga clic en **Siguiente: Resumen**.
6. En **Elegir imagen > Resumen**, asegúrese de que aparezca **Seleccionado** para **Microsoft Office 2019**.
7. En **Mis imágenes**, haga clic en **Importar imagen**.
   El estado de la imagen implementada recientemente muestra **importando** hasta que finalice la operación de importación.
8. En **Mis imágenes**, seleccione la imagen implementada recientemente y haga clic en **Ver detalles**.
9. En el panel de **detalles**, el campo **Microsoft Office 2019** muestra **Incluido**.

> **Nota:**
>
> Solo son compatibles las siguientes versiones del sistema operativo:
>
> - Windows 10 versión 21H2 (actualización de diciembre de 2021)
> - Windows 10 versión 22H2 (actualización de noviembre de 2022)
> - Windows 10 Enterprise LTSC 2019 (1809) (1809)
> - Windows 10 Enterprise LTSC 2021 (21H2) (21H2)
> - Windows 11 versión 22H2 (versión de octubre de 2022)

Cree una implementación

Una implementación es un grupo de escritorios a los que los usuarios pueden acceder desde su Citrix Workspace. Este procedimiento especifica las características de las máquinas virtuales que se van a implementar como escritorios y qué usuarios de AD pueden usarlas.

Requisitos previos

Complete todos los pasos que se indican en Preparar y crear una implementación.

1. En **Web Studio > Distribución rápida**, haga clic en **Implementaciones** en la columna **Amazon Web Services**. Haga clic en **Crear una implementación**.
2. **Nombre y conexión:** introduzca un nombre descriptivo para este grupo de máquinas. El nombre debe ser único. Seleccione una conexión de directorio y haga clic en **Siguiente: imagen y rendimiento**.
3. **Imagen y rendimiento:** seleccione el sistema operativo y el rendimiento de máquina para las máquinas. Especifique el tamaño predeterminado para el volumen raíz y el volumen de usuario.

No es posible cambiar el tamaño del volumen después de iniciar un escritorio en este grupo. Por lo tanto, especifique el tamaño máximo que piensa que necesitará. También puede especificar estos tamaños por usuario en la página siguiente. Haga clic en **Siguiente**: Usuarios.

4. **Usuarios:** busque y seleccione los usuarios a los que se les permitirá acceder a los escritorios. Si quiere personalizar los tamaños de los volúmenes para un usuario, seleccione **Modificar tamaños de volumen de usuario y raíz** y después especifique los tamaños. Haga clic en **Siguiente: Resumen**.
5. **Resumen:** revise la información proporcionada y haga clic en **Crear implementación**.

Integrar las aplicaciones de Microsoft 365 Windows

Para integrar las aplicaciones de Microsoft 365, consulte Microsoft 365 Apps para empresas, ahora disponibles en los servicios de Amazon WorkSpaces y Traiga sus propias licencias (BYOL) de Microsoft 365.

Administrar máquinas en una implementación

Además de las funciones de administración de máquinas que se describen en Administrar catálogos de máquinas, para algunas acciones, puede seleccionar las máquinas que quiere administrar desde una implementación.

Para administrar las máquinas de una implementación:

1. En **Web Studio > Distribución rápida**, seleccione **Implementaciones**.
2. En el panel **Implementaciones**, seleccione la implementación que contiene las máquinas que quiere administrar.
3. Haga clic en **Ver detalles**.
4. En el panel de **Detalles de implementación**, seleccione la máquina que quiere administrar.
5. Entre las acciones que se muestran, seleccione la acción que quiere realizar en la máquina:

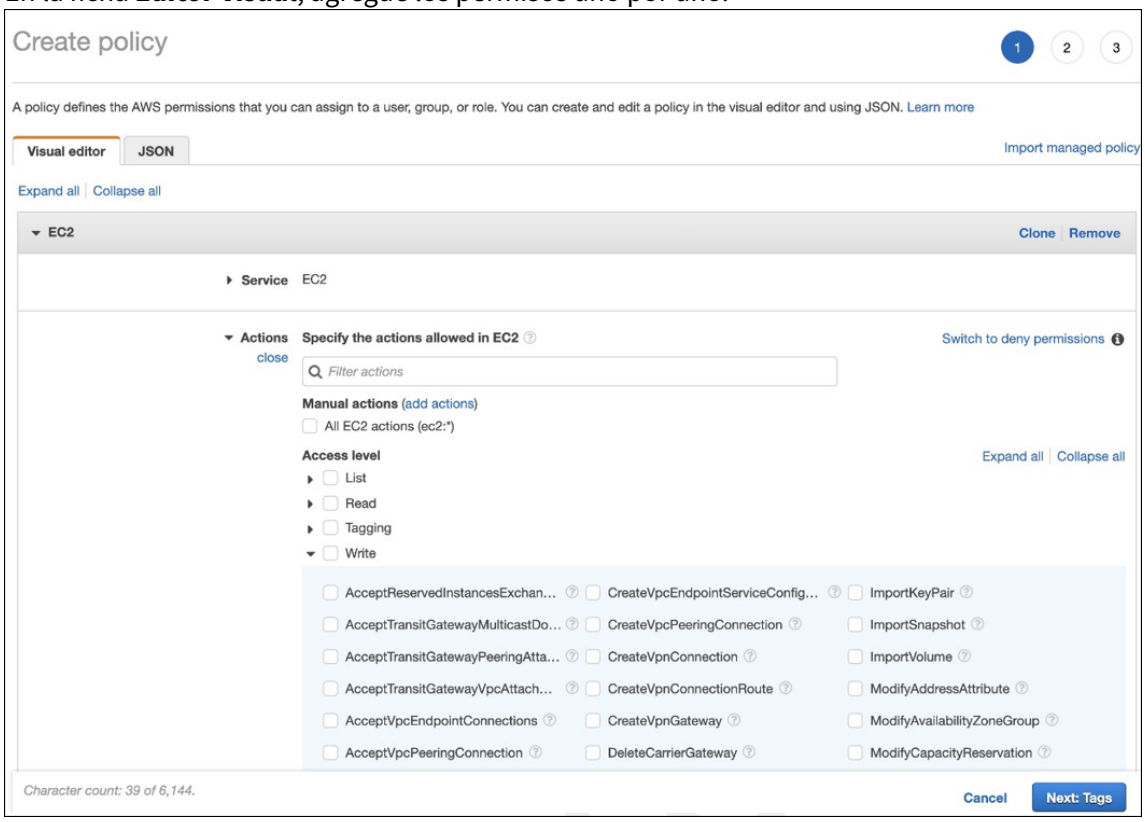
- Haga clic en **Modificar tamaño de volumen** para cambiar el tamaño del volumen de la máquina.
- Haga clic en **Eliminar** para eliminar la máquina de la implementación y de AWS. Si una máquina está en un grupo de entrega, solo se puede eliminar si está en modo de mantenimiento.
- Haga clic en **Activar/desactivar el modo de mantenimiento** para activar el modo de mantenimiento (si está desactivado) o lo desactivarlo (si está activado) para la máquina.

Referencia

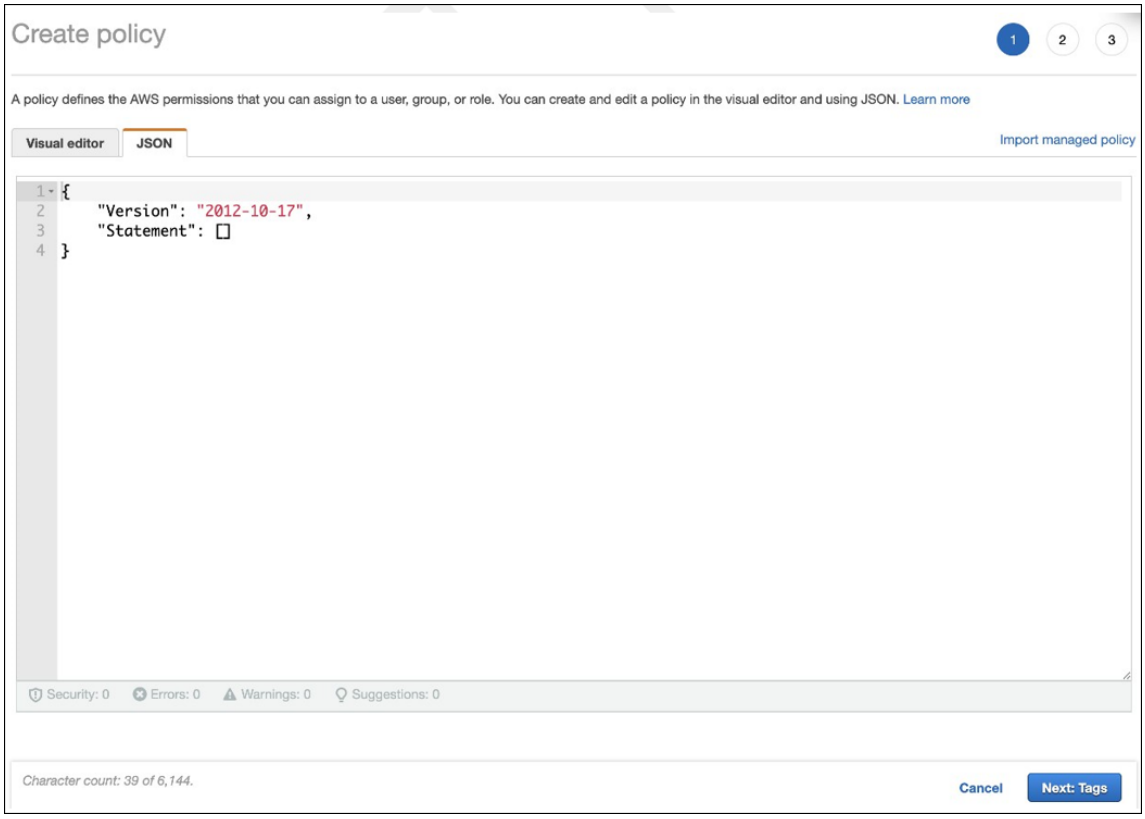
Permisos de acceso programático a la cuenta de AWS

La cuenta de usuario de AWS debe tener ciertos permisos de acceso programático para realizar llamadas de API a la capa de recursos de AWS. El acceso programático crea un ID de clave de acceso y una clave de acceso secreta.
Puede crear una directiva que contenga estos permisos en la consola de IAM. Como se muestra en los siguientes gráficos, puede usar el editor visual (añadiendo los permisos uno por uno) o el JSON (añadiendo el fragmento de código que se muestra a continuación).
Para obtener más información, consulte Creación de un usuario de IAM en su cuenta de AWS.

- En la ficha **Editor visual**, agregue los permisos uno por uno.



- En la ficha **JSON**, agregue el fragmento que se muestra después del siguiente gráfico.



Permisos requeridos

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                    "workdocs:DeregisterDirectory",
                    "workdocs:RegisterDirectory",
                    "workdocs:AddUserToGroup",
                    "ec2:ImportInstance",
                    "ec2:DescribeImages",
                    "ec2:DescribeImageAttribute"
                    "ec2:CreateKeyPair",
                    "ec2:DescribeKeyPairs",
                    "ec2:ModifyImageAttribute",
                    "ec2:DescribeVpcs",
                    "ec2:DescribeSubnets",
                    "ec2:RunInstances",
                    "ec2:DescribeSecurityGroups",
                    "ec2:CreateTags",
                    "ec2:DescribeRouteTables",
                    "ec2:DescribeInternetGateways",
```



```
                    "ec2:CreateSecurityGroup",
                    "ec2:DescribeInstanceTypes",
                    "servicequotas:ListServices",
                    "servicequotas:GetRequestedServiceQuotaChange",
                    "servicequotas:ListTagsForResource",
                    "servicequotas:GetServiceQuota",
                    "servicequotas:
                       GetAssociationForServiceQuotaTemplate",
                    "servicequotas:ListAWSDefaultServiceQuotas",
                    "servicequotas:ListServiceQuotas",
                    "servicequotas:GetAWSDefaultServiceQuota",
                    "servicequotas:
                       GetServiceQuotaIncreaseRequestFromTemplate",
                    "servicequotas:
                       ListServiceQuotaIncreaseRequestsInTemplate",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistory",
                    "servicequotas:
                       ListRequestedServiceQuotaChangeHistoryByQuota",
                    "sts:DecodeAuthorizationMessage",
                    "ds:*",
                    "workspaces:*",
                    "iam:GetRole",
                    "iam:GetContextKeysForPrincipalPolicy",
                    "iam:SimulatePrincipalPolicy"

                ],
                "Resource": "*"
            }

        ]
 }

<!--NeedCopy-->
```

Citrix DaaS para Google Cloud

November 17, 2022

Citrix DaaS para Google Cloud le permite implementar escritorios y aplicaciones de Google Cloud mediante la interfaz de administración de Configuración completa de Citrix DaaS. Citrix DaaS para Google Cloud está disponible en las ediciones Standard y Premium.

Para obtener información sobre las funciones disponibles, consulte la tabla de funciones de Citrix Virtual Apps and Desktops.

Puede adquirir Citrix DaaS para Google Cloud en Google Cloud Marketplace.

Después de adquirir Citrix DaaS, inicie sesión en Citrix Cloud. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.

Siga las instrucciones de instalación indicadas en esta documentación del producto. Mediante la interfaz de Configuración completa, puede crear conexiones, catálogos y grupos de entrega, del mismo modo que lo haría al utilizar esa interfaz con otras ediciones de productos (por ahora estas ediciones no tienen una interfaz de administración de Distribución rápida).

Es posible que algunas pantallas de la interfaz de Configuración completa sean distintas de las de la documentación. Por ejemplo, al crear una conexión en una edición de Citrix Virtual Apps and Desktops para Google Cloud, los tipos de conexión disponibles incluyen los hipervisores compatibles y Google Cloud. Los demás servicios de la nube no están disponibles.

Del mismo modo, use la información de la documentación del producto que se aplica a los hipervisores compatibles y a Google Cloud.

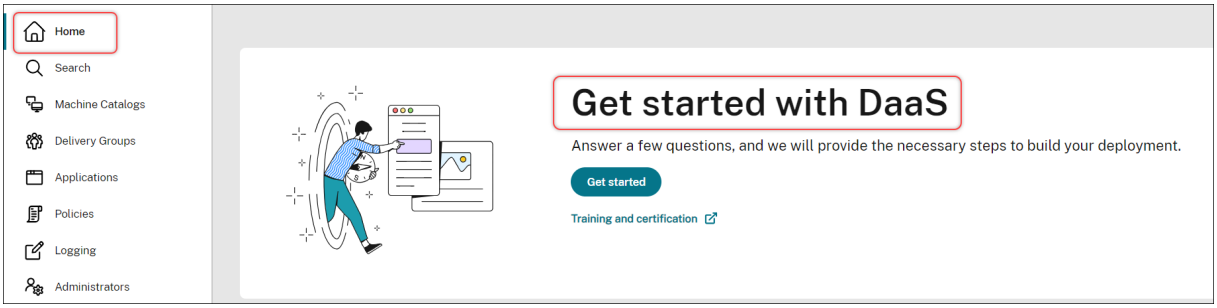
Para obtener instrucciones detalladas sobre la implementación y la configuración de Citrix DaaS en Google Cloud, consulte este artículo de Citrix Tech Zone: Citrix virtualization on Google Cloud. En este artículo se explica cómo definir la arquitectura de la implementación, preparar el proyecto de Google Cloud, configurar los servicios de red e implementar Active Directory.

Guía de introducción a DaaS (Tech Preview)

May 17, 2024

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

La guía de introducción a DaaS agiliza y simplifica el proceso de implementación de DaaS tanto para los administradores nuevos como para los experimentados. Con esta guía, puede configurar rápidamente sus implementaciones de DaaS al responder una serie de preguntas.



Este artículo detalla los procesos de configuración de cinco casos típicos de implementación de DaaS.

Ventajas

Las ventajas de esta guía incluyen:

- **Inicio fácil**. Esta guía conecta los pasos de implementación esenciales a través de un flujo de trabajo detallado basado en cuestionarios. Si tiene poca experiencia como administrador, puede configurar rápidamente su implementación mientras aprende conceptos y terminología a través de la ayuda contextual.
- **Simplifique configuraciones complejas**. Esta guía proporciona parámetros preconfigurados siempre que sea necesario y acceso a la interfaz de usuario de Configuración completa para configuraciones avanzadas. Si tiene experiencia como administrador, puede utilizar la guía como punto de partida para configuraciones complejas.

Casos de implementación admitidos

Esta guía proporciona implementaciones rápidas para estos casos:

¿Qué entregar?	¿Ya existen máquinas?	Tipo de máquina	Comentario
Escritorios y aplicaciones virtuales	No	Máquinas virtuales (aprovisionadas por DaaS)	Energía administrada
Escritorios y aplicaciones virtuales	Sí	Máquinas virtuales o PC blade	Energía administrada
Escritorios y aplicaciones virtuales	Sí	Máquinas físicas o virtuales	Energía no administrada
Equipos de oficina	Sí	Máquinas físicas	Energía administrada
Equipos de oficina	Sí	Máquinas físicas	Energía no administrada

Consulte estas secciones para obtener instrucciones detalladas:

- Entregar aplicaciones y escritorios desde cero (con administración de energía)
- Entregar aplicaciones y escritorios mediante máquinas existentes (con administración de energía)

- Entregar aplicaciones y escritorios mediante máquinas existentes (sin administración de energía)
- Entregar PC de oficina (con administración de energía)
- Entregar PC de oficina (sin administración de energía)

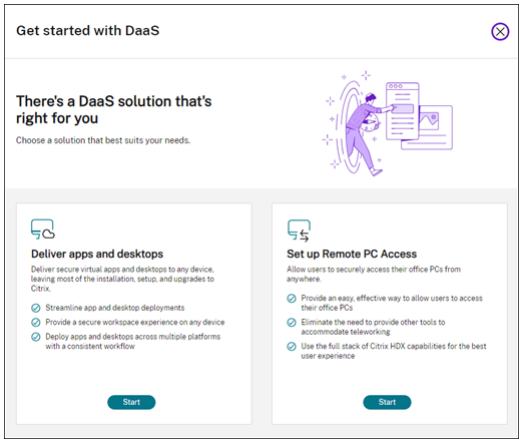
Terminología

Estas son las condiciones específicas de DaaS:

- **Ubicación de recursos** Contiene los recursos necesarios para entregar aplicaciones y escritorios a los usuarios.
- **Conexión de host** Conecta DaaS a un host (hipervisor o servicio de la nube) en una ubicación de recursos. La creación de conexiones de host es necesaria para crear y administrar máquinas en hosts o para administrar la energía de máquinas existentes.
- **Imagen maestra.** Sirve de plantilla para replicar máquinas virtuales en el host. Incluye el sistema operativo, las aplicaciones, Virtual Delivery Agent (VDA) y otro software.
- **Catálogo de máquinas.** Colección de máquinas idénticas. Pueden ser virtuales o físicas, según sus necesidades. Puede crear un catálogo de máquinas para crear máquinas configuradas de forma idéntica en un host o importar máquinas a DaaS para administrarlas.
- **Grupo de entrega.** Contiene máquinas de catálogos de máquinas. Además, especifica los usuarios que pueden usar esas máquinas y las aplicaciones y escritorios que hay disponibles para esos usuarios.
- **Perfil de máquina** Especifica las propiedades de las máquinas virtuales. Las máquinas virtuales de un catálogo pueden heredar las propiedades de un perfil de máquina.

Acceder a la guía

1. Vaya a la página **DaaS > Inicio**.
2. Buscar **Introducción a DaaS**.
3. Haga clic en **Comenzar** para iniciar el proceso de implementación.



> **Nota:**
>
> Puede salir del proceso en cualquier momento al hacer clic en **Cerrar**, y la guía guardará los parámetros automáticamente. Para continuar con la configuración, haga clic en **Continuar**. Para empezar de cero, haga clic en **Volver a empezar**.

Entregar aplicaciones y escritorios desde cero (con administración de energía)

Esta sección le guía a través del proceso de implementación para crear máquinas virtuales y entregar aplicaciones y escritorios con ellas.

Requisitos previos

Antes de empezar, necesita:

- Conectividad desde Citrix Cloud con el proveedor de identidades de destino

  Para obtener más información, consulta la sección correspondiente en Proveedores de identidades.

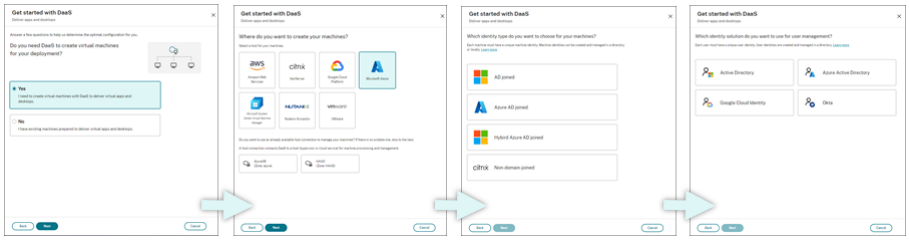
- Rol: Administrador total o administrador de Cloud
- Permisos necesarios en el hipervisor o servicio de la nube de destino.

  Para obtener más información, consulte las secciones correspondientes en Crear y administrar conexiones.

- Credenciales de administrador para la creación de cuentas de VM

Preparar

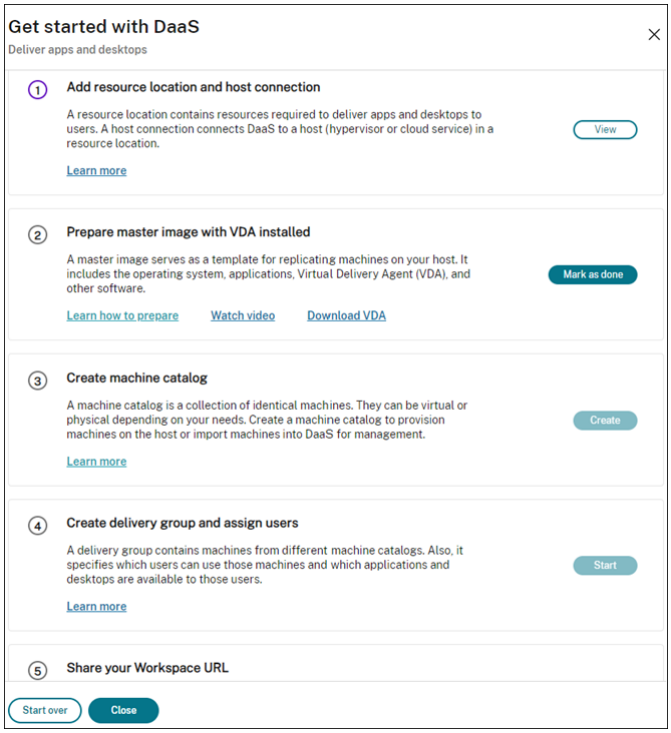
Responda las preguntas que aparecen en pantalla para completar estos parámetros al nivel de la infraestructura. Consulte esta tabla para obtener detalles.



#	Parámetro	Descripción
1	Especifique si se necesitan crear máquinas virtuales	Seleccione **Sí**.
2	Seleccionar el tipo de host	Seleccione un tipo de host para la implementación. Opciones: AWS, XenServer (antes denominado Citrix Hypervisor), Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis y VMware
3	Seleccionar el tipo de identidad de la máquina	Seleccione un tipo de identidad para la administración de máquinas. Opciones: Unida a AD, Unida a Azure AD, Unida a Azure AD híbrido y No unida a ningún dominio
4	Seleccione el tipo de identidad del usuario	Seleccione un tipo de identidad para la administración de usuarios. Opciones: Active Directory, Azure Active Directory, Google Cloud Identity y Okta

Pasos de implementación

Tras completar los parámetros al nivel de la infraestructura, aparecen los pasos específicos de este caso de implementación como se indica a continuación.



Siga las instrucciones que aparecen en pantalla para completar los parámetros.

Paso 1: Agregue una ubicación de recursos y conexiones de host Para configurar su ubicación de recursos, instale Cloud Connectors y configure conexiones a hipervisores o servicios de la nube en la ubicación.

1. Asigne un nombre a la ubicación de recursos.
2. Descargue e instale Cloud Connectors en al menos dos máquinas con Windows Server.
3. Detecte los Cloud Connectors instalados.
4. Agregue y configure conexiones de host para la ubicación de recursos. Los parámetros detallados de una conexión incluyen:
    - Detalles de conexión, como la dirección de la conexión, el nombre de usuario y la contraseña.
    - Recursos de almacenamiento
    - Recursos de red

    > **Nota:**
    >
    > DaaS crea y administra máquinas virtuales en hosts a través de esas conexiones. Debe especificar las conexiones al crear catálogos de máquinas.

Paso 2: Prepare imágenes maestras para sus máquinas Prepare imágenes maestras en las máquinas virtuales de su ubicación de recursos. Para obtener más información, consulte Preparar una imagen maestra en el hipervisor o servicio de nube.

Paso 3: Cree catálogos de máquinas Cree un catálogo de máquinas para crear un grupo de máquinas configuradas de forma idéntica en un host. Estos son los pasos detallados:

1. Asigne un nombre al catálogo.
2. Seleccione el tipo de máquina.

   Opciones: Multisesión, sesión única estática (escritorios personales) y sesión única aleatoria (escritorios agrupados).
3. Seleccione una conexión de host.

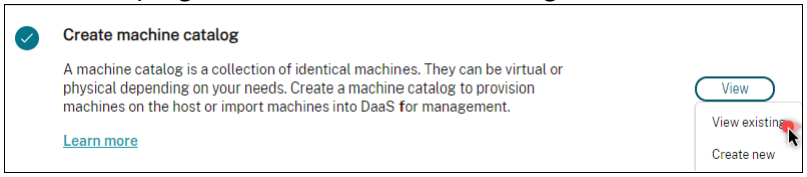
   Las opciones se originan en todas las conexiones de host que configuró para las ubicaciones de recursos en el paso 1.
4. Seleccione una imagen maestra.
5. Seleccione un perfil de máquina.

   > **Nota:**
   >
   > Ahora mismo puede usar perfiles de máquina para los servicios de la nube de Azure, GCP y AWS, y el uso de perfiles de máquina es opcional para GCP.
6. Defina la cantidad de máquinas que quiere crear.
7. Configure las identidades de las máquinas.

   De forma predeterminada, se muestra el tipo de identidad de máquina que seleccionó en la fase de preparación. Proporcione los parámetros de identidad requeridos para las máquinas virtuales, como el dominio, la unidad organizativa y el esquema de nombres.
8. Introduzca las credenciales de administrador necesarias para la creación de máquinas.
9. Haga clic en **Crear**.

   > **Sugerencia:**
   >
   > El botón **Crear** solo está disponible después de proporcionar todos los parámetros necesarios.

   Para ver el progreso de la creación del catálogo, seleccione **Ver > Ver existentes**.



Paso 4: Cree grupos de entrega y asigne usuarios

> **Sugerencia:**
>
> Antes de crear grupos de entrega, consulte los catálogos existentes para asegurarse de que al menos un catálogo se haya creado correctamente. De lo contrario, no podrá crear grupos de entrega.

La creación de un grupo de entrega incluye estas subtareas:

- Agregar máquinas virtuales al grupo
- Asignar usuarios al grupo
- Especificar qué aplicaciones y escritorios quiere poner a disposición de los usuarios asignados

1. Asigne un nombre al grupo.
2. Para agregar máquinas al grupo, seleccione un catálogo de máquinas y especifique cuántas máquinas virtuales hay disponibles para el grupo.
3. Especifique las aplicaciones y escritorios disponibles para este grupo:
    - Para agregar aplicaciones de una máquina en ejecución al catálogo seleccionado, haga clic en **Agregar > Desde el menú Inicio**.
    - Para agregar aplicaciones implementadas en recursos compartidos de red, haga clic en **Agregar > Manualmente** y, a continuación, proporcione los parámetros necesarios, como la ruta, el directorio de trabajo, etc.
    - (Solo es visible con máquinas con SO multisesión) Para la entrega de escritorios, mantenga seleccionado **Habilitar entrega de escritorios**.
4. Agregue usuarios que puedan acceder a aplicaciones y escritorios de este grupo.

Paso 5: Comparta la URL de Workspace con sus usuarios Vaya a **Configuración de Workspace > Acceso** y, a continuación, comparta la URL de Workspace con sus usuarios.

Entregar aplicaciones y escritorios mediante máquinas existentes (con administración de energía)

Esta sección le guía a través del proceso de implementación de la entrega de aplicaciones y escritorios mediante máquinas existentes (con administración de energía).

Requisitos previos

Antes de empezar, necesita:

- Conectividad desde Citrix Cloud con el proveedor de identidades de destino

  Para obtener más información, consulta la sección correspondiente en Proveedores de identidades.

- Rol: Administrador total o administrador de Cloud

Preparar

Responda las preguntas que aparecen en pantalla para completar estos parámetros al nivel de la infraestructura.

#	Parámetro	Descripción
1	Especifique si se necesitan crear máquinas virtuales	Seleccione **No**.
2	Seleccione si se requiere la administración de energía	Selecciones **Máquinas con administración de energía (por ejemplo, máquinas virtuales o PC blade)**.
3	Seleccionar la plataforma de host	Seleccione la plataforma de host en la que residen sus máquinas existentes. Opciones: AWS, Citrix, Google Cloud Platform, Microsoft Azure, Microsoft System Center Virtual Machine Manager, Nutanix Acropolis y VMware
4	Seleccione el tipo de identidad del usuario	Seleccione un tipo de identidad para la administración de usuarios. Opciones: Active Directory, Azure Active Directory, Google Cloud Identity y Okta

Pasos de implementación

Tras completar los parámetros al nivel de la infraestructura, aparecen los pasos específicos de este caso de implementación. Siga las instrucciones que aparecen en pantalla para completar los parámetros.

Paso 1: Agregue una ubicación de recursos y conexiones de host Para configurar su ubicación de recursos, instale Cloud Connectors y configure conexiones a hipervisores o servicios de la nube en su ubicación.

1. Asigne un nombre a la ubicación de recursos.
2. Descargue e instale Cloud Connectors en al menos dos máquinas con Windows Server.
3. Detecte los Cloud Connectors instalados.
4. Agregue y configure conexiones de host para la ubicación de recursos. Entre los parámetros de configuración de conexión se incluyen la dirección de conexión, el nombre de usuario y la contraseña.

> **Nota:**
>
> DaaS administra la energía de las máquinas en ubicaciones de recursos a través de conexiones. Debe especificar una conexión al importar sus máquinas a un catálogo.

Paso 2: Cree catálogos de máquinas Cree un catálogo de máquinas e importe sus máquinas en él.

1. Asignar un nombre al catálogo
2. Seleccione el tipo de máquina.

   Opciones: Multisesión, sesión única estática (escritorios personales) y sesión única aleatoria (escritorios agrupados).
3. Seleccione una ubicación de recursos.
4. Importe máquinas al catálogo.
   Las máquinas se organizan por conexión de host. Elija una conexión de host para importar las máquinas asociadas.
5. Haga clic en **Crear**.

Paso 3: Cree grupos de entrega y asigne usuarios Para crear un grupo de entrega, debe:

- Agregar máquinas virtuales al grupo
- Asignar usuarios al grupo
- Especificar qué aplicaciones y escritorios quiere poner a disposición de los usuarios asignados

1. Asigne un nombre al grupo.
2. Seleccione un catálogo de máquinas según sea necesario y, a continuación, especifique cuántas máquinas están disponibles para el grupo de entrega.
3. Especifique las aplicaciones y escritorios disponibles para este grupo:

- Para agregar aplicaciones de una máquina en ejecución al catálogo seleccionado, haga clic en **Agregar > Desde el menú Inicio**.
- Para agregar aplicaciones implementadas en recursos compartidos de red, haga clic en **Agregar > Manualmente** y, a continuación, proporcione los parámetros necesarios, como la ruta, el directorio de trabajo, etc.
- (Solo es visible con máquinas con SO multisesión) Para la entrega de escritorios, mantenga seleccionado **Habilitar entrega de escritorios**.

4. Agregue usuarios al grupo.

Paso 4: Comparta la URL de Workspace con sus usuarios Vaya a **Configuración de Workspace > Acceso** y, a continuación, comparta la URL de Workspace con sus usuarios.

Entregar aplicaciones y escritorios mediante máquinas existentes (sin administración de energía)

Esta sección le guía a través del proceso de implementación de la entrega de aplicaciones y escritorios mediante máquinas existentes (sin administración de energía).

Requisitos previos

Antes de empezar, necesita:

- Conectividad desde Citrix Cloud con el proveedor de identidades de destino

  Para obtener más información, consulte la sección correspondiente en Proveedores de identidades

- Rol: Administrador total o administrador de Cloud

Preparar

Responda las preguntas que aparecen en pantalla para completar estos parámetros al nivel de la infraestructura.

#	Parámetro	Descripción
1	Especifique si se necesitan crear máquinas virtuales	Seleccione **No**.

#	Parámetro	Descripción
2	Seleccione si se requiere la administración de energía	Seleccione **Máquinas sin administración de energía (por ejemplo, máquinas físicas)**.
3	Seleccione el tipo de identidad del usuario	Seleccione un tipo de identidad para la administración de usuarios. Opciones: Active Directory, Azure Active Directory, Google Cloud Identity y Okta

Pasos de implementación

Tras completar los parámetros al nivel de la infraestructura, aparecen los pasos específicos de este caso de implementación. Siga las instrucciones que aparecen en pantalla para completar los parámetros.

Paso 1: Agregue una ubicación de recursos Instale Cloud Connectors para configurar la ubicación de sus recursos.

1. Asigne un nombre a la ubicación de recursos.
2. Descargue e instale Cloud Connectors en al menos dos máquinas con Windows Server.
3. Detecte los Cloud Connectors instalados.

> **Nota:**
>
> La creación de conexiones de host solo es necesaria cuando se quiere administrar la energía de las máquinas.

Paso 2: Cree un catálogo de máquinas Cree un catálogo de máquinas e importe sus máquinas en él.

1. Asignar un nombre al catálogo
2. Seleccione el tipo de máquina.

   Opciones: Multisesión, sesión única estática (escritorios personales) y sesión única aleatoria (escritorios agrupados).
3. Seleccione una ubicación de recursos.

4. Importe máquinas al catálogo.

   Para facilitar la búsqueda automática, utilice nombres de equipo parciales y una selección de directorios.

5. Haga clic en **Crear**.

Paso 3: Cree grupos de entrega y asigne usuarios Para crear un grupo de entrega, debe:

- Agregar máquinas virtuales al grupo
- Asignar usuarios al grupo
- Especificar qué aplicaciones y escritorios quiere poner a disposición de los usuarios asignados

1. Asigne un nombre al grupo.
2. Seleccione un catálogo de máquinas según sea necesario y, a continuación, especifique cuántas máquinas están disponibles para el grupo de entrega.
3. Especifique las aplicaciones y escritorios disponibles para este grupo:
   - Para agregar aplicaciones de una máquina en ejecución al catálogo seleccionado, haga clic en **Agregar > Desde el menú Inicio**.
   - Para agregar aplicaciones implementadas en recursos compartidos de red, haga clic en **Agregar > Manualmente** y, a continuación, proporcione los parámetros necesarios, como la ruta, el directorio de trabajo, etc.
   - (Solo es visible con máquinas con SO multisesión) Para la entrega de escritorios, mantenga seleccionado **Habilitar entrega de escritorios**.
4. Agregue usuarios al grupo.

Paso 4: Comparta la URL de Workspace con sus usuarios Vaya a **Configuración de Workspace > Acceso** y, a continuación, comparta la URL de Workspace con sus usuarios.

Entregar PC de oficina (con administración de energía)

Esta sección le guía a través del proceso de implementación de la entrega de PC de oficina (con administración de energía).

Requisitos previos

Antes de empezar, necesita:

- Los nombres de máquina de los PC.

- Que Citrix Virtual Delivery Agent (VDA) esté instalado en cada PC (este paso se puede realizar después de crear el catálogo).

  Para obtener más información, consulte Descargar VDA.

Preparar

Responda las preguntas que aparecen en pantalla para completar estos parámetros al nivel de la infraestructura.

#	Paso	Descripción
1	Seleccione el tipo de asignación de máquinas.	Seleccione cómo se asignan las máquinas. Opciones: Asignación estática automática, Preasignación estática y Grupo aleatorio sin asignar
2	Determinar si se permite a los usuarios encender las máquinas	Seleccione **Quiero que los usuarios remotos enciendan las máquinas ellos solos**.
3	Seleccione el tipo de identidad del usuario	Seleccione un tipo de identidad para la administración de usuarios. Opciones: Active Directory, Azure Active Directory, Google Cloud Identity y Okta

Pasos de implementación

Tras completar los parámetros al nivel de la infraestructura, aparecen los pasos específicos de este caso de implementación. Siga las instrucciones que aparecen en pantalla para completar los parámetros.

Paso 1: Agregue una ubicación de recursos y conexiones de host Para configurar su ubicación de recursos, instale Cloud Connectors y agregue una conexión del tipo **Wake on LAN para Remote PC**.

1. Asigne un nombre a la ubicación de recursos.
2. Descargue e instale Cloud Connectors en al menos dos máquinas con Windows Server.

3. Detecte los Cloud Connectors instalados.
4. Haga clic en **Agregar** para agregar una conexión:

    a) Seleccione una ubicación de recursos (zona).
    b) Seleccione **Wake on LAN para Remote PC** para **Tipo de conexión**.
    c) Introduzca un nombre para la conexión.

> **Nota:**
>
> DaaS administra la energía de las máquinas a través de las conexiones configuradas. Debe configurar conexiones del tipo **Wake on LAN para Remote PC** al crear catálogos de acceso con Remote PC para máquinas con administración de energía.

Paso 2: Cree un catálogo de acceso con Remote PC Cree un catálogo de máquinas e importe en él sus PC de oficina.

1. Asignar un nombre al catálogo
2. Seleccione una ubicación de recursos.
3. Seleccione un tipo de asignación de máquinas. De forma predeterminada, se muestra el tipo que seleccionó en la fase de preparación.
4. Seleccione **Conexión Wake on LAN**. Las opciones son las conexiones del tipo **Wake on LAN para Remote PC** que configuró para la ubicación seleccionada.
5. Importe sus máquinas.
6. Haga clic en **Crear**.

Paso 3: Cree grupos de entrega y asigne usuarios Cree un grupo de entrega para agrupar máquinas que quiera entregar y especifique quién puede acceder a ellas.

1. Asigne un nombre al grupo.
2. Seleccione un catálogo de máquinas según lo que necesite. Solo aparecen los catálogos de **Acceso con Remote PC**.
3. Asigne usuarios al grupo.

Paso 4: Comparta la URL de Workspace con sus usuarios Vaya a **Configuración de Workspace > Acceso** y, a continuación, comparta la URL de Workspace con sus usuarios.

Entregar PC de oficina (sin administración de energía)

Esta sección le guía a través del proceso de implementación de la entrega de PC de oficina (sin administración de energía).

Requisitos previos

Antes de empezar, necesita:

- Los nombres de máquina de los PC.
- Que Citrix Virtual Delivery Agent (VDA) esté instalado en cada PC (este paso se puede realizar después de crear el catálogo).

  Para obtener más información, consulte Descargar VDA.

Preparar

Responda las preguntas que aparecen en pantalla para completar estos parámetros al nivel de la infraestructura.

#	Parámetro	Descripción
1	Seleccione el tipo de asignación de máquinas.	Seleccione cómo se asignan las máquinas. Opciones: Asignación estática automática, Preasignación estática y Grupo aleatorio sin asignar
2	Determinar si se permite a los usuarios encender las máquinas	No marque **Quiero que los usuarios remotos enciendan las máquinas ellos solos**.
3	Seleccione el tipo de identidad del usuario	Seleccione un tipo de identidad para la administración de usuarios. Opciones: Active Directory, Azure Active Directory, Google Cloud Identity y Okta

Pasos de implementación

Tras completar los parámetros al nivel de la infraestructura, aparecen los pasos específicos de este caso de implementación. Siga las instrucciones que aparecen en pantalla para completar los parámetros.

Paso 1: Agregue una ubicación de recursos Instale Cloud Connectors para configurar la ubicación de sus recursos.

1. Asigne un nombre a la ubicación de recursos.
2. Descargue e instale Cloud Connectors en al menos dos máquinas con Windows Server.
3. Detecte los Cloud Connectors instalados.

> **Nota:**
>
> La creación de conexiones de host solo es necesaria cuando se quiere administrar la energía de las máquinas.

Paso 2: Cree un catálogo de acceso con Remote PC Cree un catálogo e importe en él sus PC de oficina.

1. Asignar un nombre al catálogo
2. Seleccione una ubicación de recursos.
3. Seleccione un tipo de asignación. De forma predeterminada, se muestra el tipo que seleccionó en la fase de preparación.
4. Importe sus máquinas.
5. Haga clic en **Crear**.

Paso 3: Cree grupos de entrega y asigne usuarios Cree un grupo de entrega para máquinas que quiera entregar y especifique quién puede acceder a ellas.

1. Asigne un nombre al grupo.
2. Seleccione un catálogo de máquinas según lo que necesite. Solo aparecen los catálogos de **Acceso con Remote PC**.
3. Asigne usuarios para el grupo.

Paso 4: Comparta la URL de Workspace con sus usuarios Vaya a **Configuración de Workspace > Acceso** y, a continuación, comparta la URL de Workspace con sus usuarios.

Identidades de las máquinas

October 30, 2023

Cada máquina debe tener una identidad de máquina única, también conocida como cuenta de equipo. Las identidades de máquina se pueden crear y administrar en las máquinas de forma local o en un directorio, como Active Directory (AD) local o Azure AD. Citrix permite alojar aplicaciones y

escritorios virtuales en máquinas que estén unidas a Active Directory, Azure Active Directory, Azure Active Directory híbrido o que no estén unidas a ningún dominio.

Tipos de identidad de máquinas

Se admiten estos tipos de identidad de máquina.

Tipo de identidad de máquina	Descripción
Unida a AD	Las identidades se crean y se administran en Active Directory local. Las máquinas aprovisionadas se unen a Active Directory local mediante las identidades de máquina asignadas.
Unida a Azure AD	Las identidades se crean y se administran en Azure AD. Las máquinas aprovisionadas se unen a Azure AD mediante las identidades de máquina asignadas. No se permite importar máquinas virtuales en Citrix DaaS.
Unida a Azure AD híbrido	Las identidades se crean en Active Directory local y se sincronizan con Azure AD a través de Azure AD Connect. Las máquinas aprovisionadas se unen a Active Directory y a Azure AD local. Luego, las máquinas se unen a Azure AD híbrido. Para importar una máquina virtual unida a Azure AD híbrido, Citrix DaaS la trata como una máquina virtual unida a Active Directory.
No unido a un dominio	Las identidades se crean y se administran en las máquinas de forma local. No se permite importar máquinas virtuales en Citrix DaaS.

Configuraciones compatibles

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

Infraestructura admitida

Identidad de la máquina	Citrix DaaS	Citrix Workspace	Citrix StoreFront	Citrix Gateway Service	Citrix Gateway
Unida a AD	Sí	Sí	Sí	Sí	Sí
Unida a Azure AD	Sí	Sí	No	Sí	No
Unida a Azure AD híbrido	Sí	Sí	Sí	Sí	Sí
No unida a ningún dominio	Sí	Sí	Sí	Sí	Sí

> **Nota**
>
> Cuando se utiliza StoreFront, ni la caché de host local ni la continuidad del servicio están disponibles para los hosts de sesión que no están unidos a un dominio.

Proveedores de identidades para autenticación en espacios de trabajo admitidos

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

Unidos a Azure Active Directory

July 3, 2023

Las identidades se crean y se administran en Active Directory local. Las máquinas aprovisionadas se unen a Active Directory local mediante las identidades de máquina asignadas. Para obtener más información sobre los niveles funcionales admitidos para el bosque y el dominio, consulte Niveles funcionales de Active Directory.

Para obtener información sobre cómo crear catálogos unidos a Active Directory (AD) mediante Citrix DaaS, consulte Crear catálogos de máquinas.

Unidos a Azure Active Directory

May 17, 2024

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

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

Requisitos

- Plano de control: Consulte Configuraciones compatibles
- Tipo de VDA: Sesión única (solo escritorios) o multisesión (aplicaciones y escritorios)
- Versión del VDA: 2203 o una posterior
- Tipo de aprovisionamiento: Persistente y No persistente de Machine Creation Services (MCS) con flujo de trabajo de perfil de máquina
- Tipo de asignación: Dedicada y agrupada
- Plataforma de alojamiento: Solo Azure
- Rendezvous V2 debe estar habilitado

Limitaciones

- No se admite la continuidad del servicio.
- No se admite Single Sign-On para escritorios virtuales. Los usuarios deben introducir manualmente las credenciales al iniciar sesión en sus escritorios.

- No se admite el inicio de sesión con Windows Hello en el escritorio virtual. Por el momento, solo se admiten el nombre de usuario y la contraseña. Si los usuarios intentan iniciar sesión con algún método de Windows Hello, reciben un error que indica que no son el usuario intermediario, y la sesión se desconecta. Los métodos asociados incluyen el PIN, la clave FIDO2, la autenticación MFA, etc.
- Compatibilidad solamente con entornos en la nube de Microsoft Azure Resource Manager
- La primera vez que se inicia una sesión de escritorio virtual, es posible que la pantalla de inicio de sesión de Windows muestre el mensaje de inicio de sesión del último usuario que inició sesión sin la opción de cambiar a otro usuario. El usuario debe esperar a que se agote el tiempo de espera del inicio de sesión y aparezca la pantalla de bloqueo del escritorio, y, a continuación, hacer clic en la pantalla de bloqueo para mostrar de nuevo la pantalla de inicio de sesión. En ese momento, el usuario puede seleccionar **Otros usuarios** e introducir sus credenciales. Este es el comportamiento de cada sesión nueva cuando las máquinas no son persistentes.

Consideraciones

Configuración de imágenes

- Considere la posibilidad de optimizar la imagen de Windows con la herramienta Citrix Optimizer.

Unida a Azure AD

- Considere la posibilidad de inhabilitar Windows Hello para que los usuarios no tengan que configurarlo cuando inicien sesión en su escritorio virtual. Si utiliza VDA 2209 o una versión posterior, esto se hace automáticamente. Para las versiones anteriores, puede hacerlo de dos maneras:
  - Directiva de grupo o directiva local
    - Vaya a **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Windows Hello empresarial**.
    - Configure **Usar Windows Hello empresarial** en:
      - **Deshabilitado**
      - O en **Habilitado** y seleccione **No iniciar el aprovisionamiento de Windows Hello después de iniciar sesión**.
  - Microsoft Intune
    - Cree un perfil de dispositivo que inhabilite Windows Hello empresarial. Consulte la documentación de Microsoft para obtener información detallada.

    - Actualmente, Microsoft solo admite la inscripción en Intune de máquinas persistentes, lo que significa que no puede administrar máquinas no persistentes con Intune.

- Los usuarios deben tener acceso explícito en Azure para iniciar sesión en las máquinas con sus credenciales de AAD. Esto se puede facilitar al agregar asignación de roles a nivel de grupo de recursos:

    1. Inicie sesión en Azure Portal.
    2. Seleccione **Grupos de recursos**.
    3. Haga clic en el grupo de recursos donde residen las cargas de trabajo de los escritorios virtuales.
    4. Seleccione **Control de acceso (IAM)**.
    5. Haga clic en **Agregar asignación de funciones**.
    6. Busque **Inicio de sesión de usuario para máquinas virtuales**, selecciónelo en la lista y haga clic en **Siguiente**.
    7. Seleccione **Usuario, grupo o entidad de servicio**.
    8. Haga clic en **Seleccionar miembros** y seleccione los usuarios y grupos a los que quiere proporcionar acceso a los escritorios virtuales.
    9. Haga clic en **Seleccionar**.
    10. Haga clic en **Revisar + asignar**.
    11. Haga clic en **Revisar + asignar** una vez más.

> **Nota:**
>
> Si decide dejar que MCS cree el grupo de recursos para los escritorios virtuales, agregue esta asignación de roles después de crear el catálogo de máquinas.

- Las máquinas virtuales principales pueden estar unidas a Azure AD o no estar unidas a ningún dominio. Esta funcionalidad requiere la versión 2212 de VDA o una posterior.

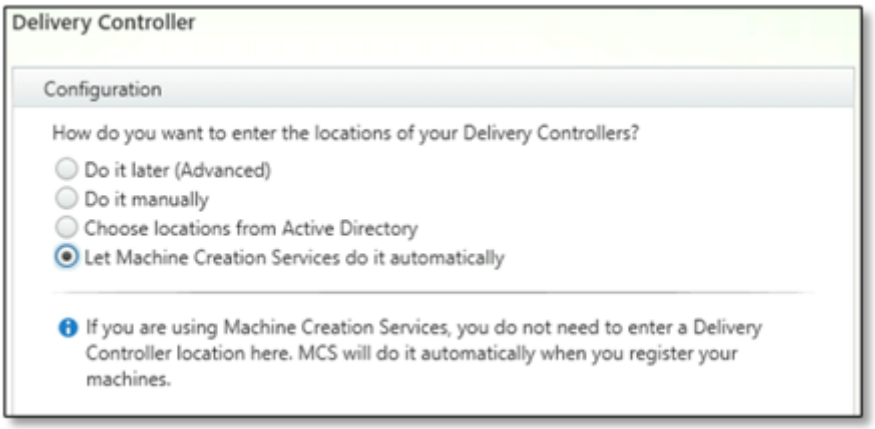
Instalación y configuración de VDA

Siga estos pasos para instalar el VDA:

1. Asegúrese de seleccionar estas opciones en el asistente de instalación:

    - En la página Entorno, seleccione **Crear una imagen maestra de MCS**.

- En la página Delivery Controller, seleccione **Dejar que Machine Creation Services lo haga automáticamente**.



2. Una vez instalado el VDA, agregue el siguiente valor de Registro:

   - Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo de valor: DWORD
   - Nombre del valor: GctRegistration
   - Información del valor: 1

3. Para la VM maestra basada en Windows 11 22H2, cree una tarea programada en la VM maestra que ejecute el siguiente comando al iniciarse el sistema con la cuenta SYSTEM. Esta actividad de programar una tarea en la VM maestra solo es necesaria para los VDA de la versión 2212 o anterior.

```
1 reg ADD HKLM\Software\AzureAD\VirtualDesktop /v Provider /t REG_SZ
      /d Citrix /f
2 <!--NeedCopy-->
```


4. Si une la máquina virtual maestra a Azure AD y, a continuación, elimina manualmente la unión con la utilidad `dsregcmd`, asegúrese de que el valor de `AADLoginForWindowsExtensionJoined` en HKLM\ Software\ Microsoft\ Windows Azure\ CurrentVersion\ AADLoginForWindowsExtension sea cero.

Qué hacer a continuación

Cuando la ubicación de recursos y la conexión de host estén disponibles, proceda a crear el catálogo de máquinas. Para obtener más información sobre la creación de catálogos de máquinas unidas a Azure Active Directory, consulte Crear catálogos unidos a Azure Active Directory.

Microsoft Intune

March 6, 2024

Este artículo describe los requisitos para crear catálogos con Microsoft Intune habilitado mediante Citrix DaaS, además de los requisitos descritos en la sección de requisitos del sistema de Citrix DaaS.

Microsoft Intune es un servicio basado en la nube que se centra en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Usted controla cómo se utilizan los dispositivos de su organización, incluidos los teléfonos móviles, las tabletas y los equipos portátiles. Para obtener más información, consulte Microsoft Intune. Los dispositivos deben cumplir con los requisitos mínimos del sistema. Para obtener más información, consulte la documentación de Microsoft Sistemas operativos y navegadores compatibles en Intune.

Microsoft Intune opera con la funcionalidad de Azure AD.

> **Importante:**
>
> Antes de habilitar esta función, compruebe que su entorno de Azure cumpla con los requisitos de licencias para usar Microsoft Intune. Para obtener más información, consulte la documentación de Microsoft: https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses. No habilite la función si no tiene la licencia de Intune adecuada.

Requisitos

- Plano de control: Citrix DaaS
- Tipo de VDA: VDA con SO de sesión única
- Versión del VDA: 2203 o una posterior
- Tipo de aprovisionamiento: Persistente de Machine Creation Services (MCS) con el flujo de trabajo de perfil de máquina solamente

- Tipo de tarea: Dedicada

Limitaciones

- Admitir solamente máquinas virtuales persistentes unidas a Azure AD de sesión única.
- Admitir solo máquinas virtuales persistentes unidas a Azure AD híbrido de sesión única que empleen credenciales de usuario o credenciales de dispositivo con capacidad de coadministración. Para obtener más información, consulte Inscripción automática de un dispositivo Windows mediante directiva de grupo.
- No omita la preparación de imágenes al crear o actualizar catálogos de máquinas.

Consideraciones

- Cree un perfil de dispositivo que inhabilite Windows Hello empresarial.
- Utilice la versión 2212 del VDA o una versión posterior si Microsoft Intune debe administrar una máquina virtual principal.

Qué hacer a continuación

Para obtener información sobre la creación de catálogos con Microsoft Intune habilitado, consulte Crear catálogos con Microsoft Intune habilitado.

Unidos a Azure Active Directory híbrido

May 17, 2024

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

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

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

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

Requisitos

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

Limitaciones

- Si se utiliza Servicio de autenticación federada (FAS) de Citrix, el inicio de sesión único (SSO) se dirige a AD local en lugar de Azure AD. En este caso, se recomienda configurar la autenticación basada en certificados de Azure AD para que el token de actualización principal (PRT) se genere al iniciar sesión el usuario, lo que facilita el inicio Single Sign-On en recursos de Azure AD dentro de la sesión. De lo contrario, el token PRT no estará presente, y el inicio SSO en recursos de Azure AD no funcionará. Para obtener información sobre cómo implementar el inicio de sesión único (SSO) de Azure AD en los VDA unidos de forma híbrida mediante el Servicio de autenticación federada (FAS) de Citrix, consulte VDA unidos de forma híbrida.
- No omita la preparación de imágenes al crear o actualizar catálogos de máquinas. Si quiere omitir la preparación de la imagen, asegúrese de que las máquinas virtuales maestras no estén unidas a Azure AD ni a Azure AD híbrido.

Consideraciones

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

  1. Ejecute `gpedit.msc`.

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

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

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

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

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

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

        break;
     }


    if ($provider -eq 1)
    {

        Set-ItemProperty -Path $VirtualDesktopKeyPath -Name "
           Provider" -Value "Citrix" -Force
        Set-ItemProperty -Path $WorkplaceJoinKeyPath -Name "
           autoWorkplaceJoin" -Value 1 -Force
        Start-Sleep 5
        dsregcmd /join
        break
     }

   }


  Start-Sleep 1
 }

<!--NeedCopy-->
```


Qué hacer a continuación

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

No unida a ningún dominio

November 17, 2023

Este artículo describe los requisitos para crear catálogos que no están unidos a ningún dominio mediante Citrix DaaS, además de los requisitos descritos en la sección de requisitos del sistema de Citrix DaaS.

Requisitos

- Plano de control: Consulte Configuraciones compatibles
- Tipo de VDA: Sesión única (solo escritorios) o multisesión (aplicaciones y escritorios)
- Versión del VDA: 2203 o una posterior
- Tipo de aprovisionamiento: Persistente y No persistente de Machine Creation Services (MCS)
- Tipo de asignación: Dedicada y agrupada
- Plataforma de alojamiento: Todas las plataformas compatibles con MCS
- Rendezvous V2 debe estar habilitado
- Cloud Connectors: Solo es necesario si planea aprovisionar máquinas en hipervisores locales o si quiere utilizar Active Directory como proveedor de identidades en Workspace.

Limitaciones

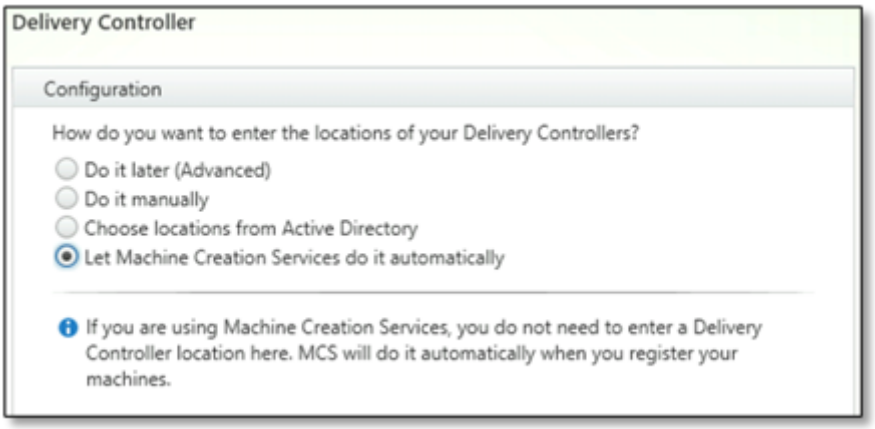
- No se admite la continuidad del servicio.
- Siempre que utilizamos un VDA multisesión que no está unido a ningún dominio, los datos del perfil del usuario local no se conservan y se eliminan al cerrar la sesión.

Instalación y configuración de VDA

Siga estos pasos para instalar el VDA:

1. Asegúrese de seleccionar estas opciones en el asistente de instalación:
    - En la página Entorno, seleccione **Crear una imagen maestra de MCS**.

- En la página Delivery Controller, seleccione **Dejar que Machine Creation Services lo haga automáticamente**.



2. Una vez instalado el VDA, agregue el siguiente valor de Registro:

   - Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
   - Tipo de valor: DWORD
   - Nombre del valor: GctRegistration
   - Información del valor: 1

Qué hacer a continuación

Cuando la ubicación de recursos y la conexión de host estén disponibles, proceda a crear el catálogo de máquinas. Para obtener más información sobre la creación de catálogos de máquinas no unidos a un dominio, consulte Crear catálogos que no estén unidos a ningún dominio.

Configurar ubicaciones de recursos

June 12, 2024

Las ubicaciones de recursos contienen los recursos necesarios para entregar aplicaciones y escritorios a los usuarios. Los recursos se administran desde Citrix Cloud. Entre los recursos típicos se incluyen los siguientes:

- Hipervisores o servicios de nube, conocidos como *hosts*, que incluyen:
  - Controladores de dominio de Active Directory.
  - Virtual Delivery Agents (VDA): Los VDA se instalan en una máquina que entrega las aplicaciones y los escritorios a los usuarios.
  - Citrix Gateway (optativo): Para habilitar el acceso externo seguro a las aplicaciones y los escritorios que se ofrecerán a los usuarios, agregue un dispositivo Citrix Gateway VPX a la ubicación de recursos. A continuación, configure Citrix Gateway.
  - Servidores Citrix StoreFront.
  - Para comunicarse con Citrix Cloud, cada ubicación de recursos debe contener un Citrix Cloud Connector. Se recomienda un mínimo de dos Cloud Connectors por ubicación de recursos.

Una zona equivale a una ubicación de recursos. Cuando se crea una ubicación de recursos y se instala un Cloud Connector, se crea automáticamente una zona para usted. Para obtener más información, consulte Zonas.

Para obtener más información sobre los tipos de recursos, consulte Conectarse a Citrix Cloud.

Requisitos del host

El hipervisor o el servicio de nube, donde se aprovisionan las máquinas virtuales, necesita permisos o una configuración únicos.

- Si el hipervisor o el servicio de nube requiere redes virtuales, siga las instrucciones proporcionadas en la documentación correspondiente.
- Cree la nube privada virtual (VPC) (para AWS o GCP) o la red virtual (VNET) (para Azure) adecuadas para las máquinas que agregará a la ubicación de recursos.
- Cree las reglas apropiadas para proteger el tráfico entrante y saliente entre las máquinas en la red virtual. Por ejemplo, si utiliza AWS, asegúrese de que el grupo de seguridad de la nube VPC tiene configuradas las reglas apropiadas para que las máquinas en la nube VPC sean accesibles solamente desde las direcciones IP que usted especifique.

Se admiten los siguientes tipos de host:

- Entornos de virtualización de Amazon Web Services (AWS)
- Entornos de virtualización de XenServer
- Entornos de virtualización Google Cloud Platform
- Entornos de virtualización de HPE Moonshot
- Entornos de virtualización de Microsoft Azure Resource Manager
- Entornos de virtualización de Microsoft System Center Virtual Machine Manager
- Entornos de virtualización de Nutanix
- Soluciones de Nutanix Cloud y de partners
- Entornos de virtualización de VMware
- Soluciones de VMware Cloud y de partners

Active Directory

Aprovisione un servidor Windows, instale los servicios de dominio de Active Directory (AD DS) y promuévalo a un controlador de dominio. Para obtener instrucciones, consulte el documento de Microsoft Introducción a Active Directory Domain Services.

Estas son algunas consideraciones importantes:

- Debe tener al menos un controlador de dominio que ejecute los Servicios de dominio de Active Directory.
- No instale ningún componente Citrix en un controlador de dominio.

Para obtener más información, consulte:

- Niveles funcionales de Active Directory
- Administración de acceso e identidad en Citrix Cloud.
- Conectar Active Directory con Citrix Cloud
- Casos de implementación para usar el Connector Appliance con Active Directory

Cloud Connectors

Cloud Connector es un grupo de servicios de Citrix Cloud que permite la comunicación entre los VDA, StoreFront y el Delivery Controller basado en la nube. Puede instalar Cloud Connectors interactivamente o desde la línea de comandos.

Para obtener más información sobre los Cloud Connectors, consulte:

- Citrix Cloud Connector
- Detalles técnicos
- Configuración del proxy y del firewall
- Instalación
- Actualizaciones de los Connectors

Consideraciones sobre el tamaño y la escala

- Cuando evalúe Citrix DaaS para determinar la dimensión y la escalabilidad, tenga en cuenta todos los componentes.
- Investigue y pruebe la configuración de los Cloud Connectors y el StoreFront para sus requisitos específicos.
- Un tamaño insuficiente de las máquinas puede afectar negativamente al rendimiento del sistema.

El artículo Consideraciones sobre el tamaño y la escala para los Cloud Connectors incluye lo siguiente:

- Información sobre pruebas de tamaño y escala
- Capacidades máximas probadas
- Prácticas recomendadas para la configuración de máquinas de Cloud Connector

Agregar un tipo de recursos

1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Ubicaciones de recursos**.
3. Seleccione **+ Ubicaciones de recursos** para agregar una nueva ubicación de recursos.
4. Escriba un nombre para la ubicación de recursos y, a continuación, haga clic en **Guardar**. Para obtener información sobre las consideraciones de nomenclatura, consulte Restricciones de nombres.
5. En la nueva ubicación de recursos, seleccione **+ Cloud Connectors**.
6. Descargue e instale el software del Cloud Connector en al menos dos servidores del dominio donde tenga sus recursos de Citrix DaaS.
    - Durante la instalación, seleccione la ubicación de recursos que creó en los pasos anteriores.
    - Tras la instalación, Citrix Cloud agrega los servidores a la ubicación de recursos y registra los dominios en los que ha instalado los Cloud Connectors.
7. Compruebe que los dominios registrados estén activos:
    - Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
    - Seleccione **Dominios**. Aparecerá una lista de los dominios en que se han implementado Cloud Connectors.

- Busque los dominios que utiliza con Citrix DaaS. Los dominios activos se muestran con una barra verde en el lado izquierdo de la entrada del dominio.

Si algún dominio no tiene el indicador visual descrito, significa que el dominio **no está utilizado**. Si especifica un dominio no utilizado durante la configuración del catálogo de máquinas, no se puede crear el catálogo. Para garantizar que la configuración del catálogo de máquinas se realice sin errores, siga los pasos que se indican en Activar un dominio no utilizado.

Para obtener más información, consulte CTX473009: DaaS Catalog Creation Wizard: "Internal Server Error"when creating adding new machine accounts.

Activar un dominio no utilizado

1. En la ficha **Dominio**, en **Administración de acceso e identidad**, seleccione **Mostrar dominios no utilizados**. Tras seleccionar esta opción, la etiqueta cambia a **Ocultar dominios no utilizados**.
2. Busque el dominio no utilizado en la lista. Los dominios no utilizados muestran una barra gris en el lado izquierdo de la entrada de dominio y un menú de tres puntos con una sola opción en el lado derecho.
3. Seleccione el menú de tres puntos y, a continuación, seleccione **Usar dominio**. La barra gris pasa a ser verde y el menú de tres puntos cambia a **Inhabilitar**.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para configurar una ubicación de recursos para tipos de host específicos:
  - Entornos de virtualización de AWS
  - Entornos de virtualización de Google Cloud
  - Entornos de virtualización de HPE Moonshot
  - Entornos de virtualización de Microsoft Azure Resource Manager
  - Entornos de virtualización de Microsoft System Center Virtual Machine Manager
  - Entornos de virtualización de Nutanix
  - Soluciones de Nutanix Cloud y de partners
  - Entornos de virtualización de VMware
  - Soluciones de VMware Cloud y de partners
  - Entornos de virtualización de XenServer
- Para una implementación completa, cree y administre conexiones y recursos asociados a una ubicación de recursos.

- Revisar todos los pasos del proceso de instalación y configuración

Entornos de virtualización de AWS

March 30, 2024

En este artículo se describe cómo configurar su cuenta de AWS como ubicación de recursos que puede usar con Citrix DaaS.

La ubicación de recursos contiene un conjunto básico de componentes; es ideal para una prueba de concepto u otra implementación que no requiera recursos repartidos por varias zonas de disponibilidad.

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

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

Después de completar las tareas, puede instalar agentes VDA, aprovisionar máquinas, crear catálogos de máquinas y crear grupos de entrega.

Descripción general de tareas

Configurar una nube privada virtual (VPC) con subredes públicas y privadas. Una vez completada esta tarea, AWS implementa puertas de enlace NAT con una dirección IP elástica en la subred pública. Esto permite que las instancias de la subred privada accedan a Internet. Las instancias en la subred pública están accesibles para el tráfico público entrante, mientras que las instancias en la subred privada no lo están.

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

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

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

Tarea 1: Configurar la nube VPC

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

> **Nota:**
>
> Al cambiar el nombre de una nube privada virtual (VPC) de AWS en la consola de AWS, se rompe la unidad de alojamiento existente en Citrix Cloud. Si la unidad de alojamiento se rompe, no se pueden crear catálogos nuevos ni agregar máquinas a catálogos existentes. Del problema conocido: PMCS-7701

Tarea 2: Configurar grupos de seguridad

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

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

Para crear los grupos de seguridad:

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

Configurar el grupo de seguridad público

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

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

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

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

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

Configurar el grupo de seguridad privado

1. En la lista de grupos de seguridad, seleccione el grupo de seguridad privado.
2. Si aún no ha configurado el tráfico del grupo de seguridad público, debe configurar los puertos TCP. Seleccione la ficha **Inbound Rules** y seleccione **Edit** para crear estas reglas:

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

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

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

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

Tarea 3: Iniciar instancias

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

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

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

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

- Una instancia de host bastión en la subred pública
- Tres instancias en la subred privada para usarlas de la siguiente manera:
  - Una como controlador de dominio
  - Dos como Cloud Connectors

Tarea 4: Crear un conjunto de opciones de DHCP

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

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

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

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

Tarea 5: Configurar las instancias

1. A través de un cliente RDP, conéctese a la dirección IP pública de la instancia del host bastión. Cuando se le solicite, introduzca las credenciales de la cuenta de administrador.

2. Desde la instancia del host bastión, inicie una **Conexión a Escritorio remoto** (RDC) y conéctese a la dirección IP privada de la instancia que quiere configurar. Cuando se le solicite, introduzca las credenciales del administrador de la instancia.
3. Configure los parámetros de DNS para todas las instancias en la subred privada:
    a) Seleccione **Inicio > Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Cambiar configuración del adaptador**. Haga doble clic en la conexión de red que aparece.
    b) Seleccione **Propiedades > Protocolo de Internet versión 4 (TCP/IPv4) > Propiedades**.
    c) Seleccione **Avanzado > DNS**. Compruebe que los siguientes parámetros están habilitados y seleccione **Aceptar**:
        - **Registrar en DNS las direcciones de esta conexión**
        - **Use el sufijo DNS de esta conexión en el registro de DNS**
4. Configure el controlador de dominio:
    a) Mediante el Administrador de servidores, agregue el rol Servicios de dominio de Active Directory con todas las funciones predeterminadas.
    b) Promueva la instancia a un controlador de dominio. Durante la promoción, habilite el DNS y use el nombre de dominio que especificó al crear el conjunto de opciones de DHCP. Reinicie la instancia cuando lo pida el sistema.
5. Configure el primer Cloud Connector:
    a) Una la instancia al dominio y reinicie cuando lo pida el sistema. Desde la instancia del host bastión, vuelva a conectarse a la instancia mediante RDP.
    b) Inicie sesión en Citrix Cloud. Seleccione **Ubicaciones de recursos** en el menú superior de la izquierda.
    c) Descargue el Cloud Connector.
    d) Cuando se le solicite, ejecute el archivo `cwcconnector.exe` y suministre las credenciales de Citrix Cloud. Siga las instrucciones del asistente.
    e) Cuando haya terminado, seleccione **Actualizar** para ver la página **Ubicaciones de recursos**. Una vez que el Cloud Connector está registrado, la instancia aparece en la página.
6. Para configurar el segundo Cloud Connector, repita los pasos correspondientes.
7. Adjunte una directiva de IAM a los Cloud Connectors para compatibilizar las conexiones de alojamiento de AWS con la autorización basada en roles. Debe tener la misma directiva de IAM adjunta a todos los Cloud Connectors de una ubicación de recursos. Para obtener información sobre los permisos de AWS, consulte Permisos requeridos por AWS.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con AWS.
- Revisar todos los pasos del proceso de instalación y configuración

Más información

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

Entornos de virtualización de Google Cloud

May 17, 2024

Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) le permite aprovisionar y administrar máquinas en Google Cloud.

Requisitos previos

Antes de empezar a aprovisionar las máquinas virtuales en Google Cloud Platform (GCP), debe asegurarse de que se cumplen los siguientes requisitos previos.

1. La suscripción a Citrix debe incluir compatibilidad con cargas de trabajo multinube híbridas. Para obtener más información, consulte la comparativa de funciones en las suscripciones a Citrix.
2. La cuenta de administrador debe tener los permisos suficientes para crear conexiones de host, catálogos de máquinas y grupos de entrega. Para obtener más información, consulte Configurar la administración delegada.
3. Identifique un proyecto de Google Cloud en el que se almacenen todos los recursos informáticos asociados al catálogo de máquinas. Puede ser un proyecto existente o uno nuevo. Para obtener más información, consulte Proyectos de Google Cloud.
4. Habilite las API de Google Cloud necesarias para la integración con Citrix DaaS. Para obtener más información, consulte Habilitar las API de Google Cloud.
5. Cree las cuentas de servicio en Google Cloud y conceda los permisos correspondientes. Para obtener más información, consulte Configurar y actualizar cuentas de servicio.

6. Descargue el archivo de claves de la cuenta de servicio de Citrix Cloud. Para obtener más información, consulte Clave de cuenta de Citrix Cloud Service.
7. Las máquinas virtuales deben tener acceso a las API de Google sin una dirección IP pública. Para obtener más información, consulte Habilitar el acceso privado a Google.

Proyectos de Google Cloud

Existen básicamente dos tipos de proyectos de Google Cloud:

- Proyecto de Provisioning: En este caso, la cuenta de administrador actual es propietaria de las máquinas aprovisionadas del proyecto. Este tipo de proyecto se conoce también como proyecto local.
- Proyecto de nube privada virtual (VPC) compartida: Proyecto en el que las máquinas creadas en el proyecto de aprovisionamiento utilizan la VPC del proyecto de VPC compartida. La cuenta de administrador utilizada para los proyectos de aprovisionamiento tiene permisos limitados en este proyecto, específicamente, solo permisos para usar la nube VPC.

URL de dispositivo de punto final del servicio

Debe tener acceso a las siguientes URL:

- `https://oauth2.googleapis.com`
- `https://cloudresourcemanager.googleapis.com`
- `https://compute.googleapis.com`
- `https://storage.googleapis.com`
- `https://cloudbuild.googleapis.com`

Habilitar las API de Google Cloud

Para utilizar la funcionalidad de Google Cloud a través de la interfaz de Configuración completa de Citrix DaaS, habilite estas API en su proyecto de Google Cloud:

- API de Compute Engine
- API de Cloud Resource Manager
- API de Identity and Access Management (IAM)
- API de Cloud Build

En la consola de Google Cloud, siga estos pasos:

1. En el menú superior izquierdo, seleccione **APIs and Services > Enabled APIs & services**.

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

    a) Vaya a **APIs and Services > Library**.
    b) En el cuadro de búsqueda, escriba *Compute Engine*.
    c) En los resultados de la búsqueda, seleccione **Compute Engine API**.
    d) En la página **Compute Engine API**, seleccione **Enable**.

3. Habilite la API de Cloud Resource Manager.

    a) Vaya a **APIs and Services > Library**.
    b) En el cuadro de búsqueda, escriba *Cloud Resource Manager*.
    c) En los resultados de búsqueda, seleccione **Cloud Resource Manager API**.
    d) En la página **Cloud Resource Manager API**, seleccione **Enable**. Aparece el estado de la API.

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

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

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

    - gcloud services enable compute.googleapis.com
    - gcloud services enable cloudresourcemanager.googleapis.com
    - gcloud services enable iam.googleapis.com
    - gcloud services enable cloudbuild.googleapis.com
    - gcloud services enable cloudkms.googleapis.com

3. Haga clic en **Authorize** cuando Cloud Shell se lo indique.

Configurar y actualizar cuentas de servicio

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

> nueva directiva de la organización, vaya a la sección Antes del 29 de abril de 2024.

Antes del 29 de abril de 2024

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   El operador criptográfico de Cloud KMS requiere los siguientes permisos:

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

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

5. Haga clic en **CONTINUE**
6. En la página **Grant users access to this service account**, agregue usuarios o grupos para permitirles realizar acciones en esta cuenta de servicio.
7. Haga clic en **DONE**.

8. Vaya a la consola principal de IAM.
9. Identifique la cuenta de servicio creada.
10. Compruebe que los roles se hayan asignado correctamente.

Consideraciones:

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

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

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

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

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

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

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

   Por ejemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`
3. Seleccione el icono del lápiz para modificar el acceso a la entidad principal de la cuenta de servicio.

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

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

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

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

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

A partir del 29 de abril de 2024

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

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

  Debe crear esta cuenta de servicio manualmente.

  Puede identificar esta cuenta de servicio con una dirección de correo electrónico. Por ejemplo, `<my-service-account>@<project-id>.iam.gserviceaccount.com`.
- *Cuenta de servicio de Cloud Compute*: Esta cuenta de servicio se aprovisiona automáticamente después de habilitar todas las API mencionadas en Habilitar las API de Google Cloud. Para ver todas las cuentas de servicio creadas automáticamente, vaya a **IAM y Admin > IAM** en la consola de **Google Cloud** y seleccione la casilla de verificación **Incluir asignaciones de funciones proporcionadas por Google**. Esta cuenta tiene el rol de editor básico de IAM para realizar las operaciones. Sin embargo, si elimina el permiso predeterminado para tener un control más granular, deberá agregar el rol **Administrador de almacenamiento** que requiere los siguientes permisos:

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

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

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

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

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

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

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

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

   El operador criptográfico de Cloud KMS requiere los siguientes permisos:

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

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

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

Consideraciones:

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

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

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

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

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

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

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

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

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

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

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

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

Permisos de almacenamiento y administración de depósitos

Citrix DaaS mejora el proceso de notificación de errores de compilación en la nube para el servicio de Google Cloud. Este servicio ejecuta compilaciones en Google Cloud. Citrix DaaS crea un depósito de almacenamiento denominado `citrix-mcs-cloud-build-logs-{ region } -{ 5 random characters }` donde los servicios de Google Cloud capturan la información del registro de compilación. Se establece una opción en este depósito que elimina el contenido tras un período de 30 días. Este proceso requiere que la cuenta de servicio utilizada para la conexión

tenga establecidos los permisos `storage.buckets.update` en Google Cloud. Si la cuenta de servicio no tiene este permiso, Citrix DaaS ignora los errores y continúa con el proceso de creación del catálogo. Sin este permiso, el tamaño de los registros de compilación aumenta y se requiere una limpieza manual.

Habilitar el acceso privado a Google

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

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

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

1. En Google Cloud, acceda a la **configuración de red de VPC**.
2. Identifique las subredes usadas o el entorno de Citrix en la ficha **Subredes del proyecto actual**.
3. Haga clic en el nombre de las subredes y habilite el **Acceso privado a Google**.

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

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

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con entornos de Google Cloud.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

- Crear y administrar conexiones y recursos

- Crear catálogos de máquinas

Entornos de virtualización de HPE Moonshot

June 12, 2024

Citrix DaaS administra sus cargas de trabajo de HPE Moonshot a través de un plug-in de HPE Moonshot administrado por Citrix presente en el plano de control de DaaS. Con este plug-in, puede crear conexiones a su chasis HPE Moonshot, crear catálogos y administrar la energía de las máquinas del catálogo.

Pasos clave

1. Configure sus entornos de HPE.
2. Cree una conexión con el chasis HPE Moonshot.

   > **Nota:**
   >
   > Tras habilitar la función, el plug-in de HPE Moonshot administrado por Citrix se instala automáticamente. Por lo tanto, puede seguir usando el catálogo de máquinas existente con el plug-in de Moonshot administrado por Citrix en lugar del plug-in de HPE Moonshot administrado por HPE.

3. Cree un catálogo de máquinas.

   > **Nota:**
   >
   > Antes de crear un catálogo, asegúrese de tener uno o más nodos de cartuchos HPE Moonshot e instale los VDA en esos nodos. Puede considerar el chasis HPE Moonshot como el hipervisor y los nodos de cartuchos como máquinas virtuales.

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

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina que vaya a entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con HPE Moonshot.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

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

Entornos de virtualización de Microsoft Azure Resource Manager

May 17, 2024

Cuando use Azure Resource Manager para aprovisionar máquinas virtuales en la implementación de Citrix DaaS, familiarícese con lo siguiente:

- ¿Qué es Microsoft Entra ID?
- Guía de introducción a la integración de Microsoft Entra ID con las aplicaciones
- Objetos de aplicación y de entidad de servicio en Microsoft Entra ID

Para configurar el Administrador de recursos de Microsoft Azure, consulte Configurar la ubicación de recursos.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con Microsoft Azure.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

- Crear y administrar conexiones y recursos
- Crear catálogos de máquinas
- CTX219211: Set up a Microsoft Entra ID account
- CTX219243: Grant XenApp and XenDesktop access to your Azure subscription
- CTX219271: Deploy hybrid cloud using site-to-site VPN

Entornos de virtualización de Microsoft System Center Virtual Machine Manager

January 24, 2024

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

Consulte Requisitos del sistema para ver una lista de las versiones de VMM compatibles.

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

- Máquinas virtuales de SO de servidor o escritorio de 1.ª generación
- Máquinas virtuales con Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 10 y Windows 11 (con o sin Secure Boot) de 2.ª generación

Instalar y configurar un hipervisor

Instale el rol Microsoft Hyper-V Server y VMM en los servidores.

Compruebe la siguiente información de cuenta:

En **Administrar > Configuración completa**, la cuenta que indique cuando cree una conexión debe ser un administrador de VMM o administrador delegado de VMM para las máquinas Hyper-V en cuestión. Si esta cuenta solo tiene el rol de administrador delegado en VMM, los datos de almacenamiento no aparecen en la interfaz de **Configuración completa** durante el proceso de creación de la conexión.

La cuenta de usuario también debe ser un miembro del grupo de seguridad local de administradores en cada uno de los servidores de Hyper-V para permitir la administración del ciclo de vida de las VM (creación, actualización y eliminación de VM).

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

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

1. En el **asistente para crear roles de usuario**, seleccione **Fabric Administrator** (administrador delegado) como rol de usuario.
2. En **Miembros**, agregue la cuenta de usuario en Active Directory que quiera usar como administrador delegado.
3. En **Ámbito**, seleccione los grupos de hosts a los que quiere que tenga acceso el administrador delegado.

4. Cree otra **cuenta de ejecución** con las credenciales de usuario del administrador delegado. Use estas credenciales para crear una conexión de hipervisor más adelante. No use las cuentas del rol de administrador principal.

Instalar la consola de VMM

Instale una consola de System Center Virtual Machine Manager en cada servidor que tenga un Citrix Cloud Connector.

La versión de la consola debe coincidir con la versión del servidor de administración. Aunque es posible conectar una consola anterior al servidor de administración, se produce un error al aprovisionar los agentes VDA si las versiones son distintas.

Aprovisionamiento de Azure Stack HCI mediante SCVMM

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

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

Integrar Azure Stack HCI en SCVMM

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

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

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

   > **Nota:**
   >
   > Instale la consola de administrador de SCVMM 2019 UR3 o una versión posterior en las VM de Cloud Connector.

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

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


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

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

e) Cree la conexión de host de SCVMM en la interfaz de **Configuración completa**.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con Microsoft System Center Virtual Machine Manager.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

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

Entornos de virtualización de Nutanix

February 12, 2024

Siga estas instrucciones si usa Nutanix Acropolis para ofrecer máquinas virtuales en su entorno de Citrix DaaS. El proceso de configuración incluye la tarea de instalar y registrar el plug-in de Nutanix en su entorno de Citrix DaaS.

Para obtener más información, consulte la guía de instalación de plug-ins MCS de Nutanix Acropolis, disponible en el portal de asistencia de Nutanix.

> **Importante:**
>
> Instale el plug-in de Nutanix en todos los Cloud Connectors en los que Citrix DaaS deba crear una

> conexión de host a la ubicación de recursos que incluya un hipervisor de Nutanix.

Instalar y registrar el plug-in de Nutanix

Complete el procedimiento para instalar y registrar el plug-in de Nutanix en todos sus Cloud Connectors. Use las funciones disponibles en **Administrar > Configuración completa** en Citrix Cloud para crear una conexión con Nutanix.

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

Para obtener más información sobre cómo configurar los entornos de virtualización de Nutanix, consulte Agregar un tipo de recurso o activar un dominio no utilizado en Citrix Cloud.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con Nutanix.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

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

Soluciones de Nutanix Cloud y de partners

January 24, 2024

Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) admite estas soluciones de Nutanix Cloud y de partners:

- Nutanix Cloud Clusters en AWS

Nutanix Cloud Clusters en AWS

Citrix DaaS admite Nutanix Cloud Clusters en AWS. Los clústeres de Nutanix simplifican la forma en que las aplicaciones se ejecutan en nubes privadas o en varias nubes públicas. Para obtener más in-

formación sobre Nutanix Cloud Clusters en AWS, consulte Nutanix Cloud Clusters on AWS Deployment and User Guide.

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

Requisitos

Necesita estas cuentas para utilizar Nutanix Clusters en AWS:

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

Crear un Nutanix Cluster

Para crear un Nutanix Cluster:

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

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

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

Si el clúster no se crea:

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

Además de otros recursos, Nutanix CFS crea:

- 1 nube VPC denominada *Nutanix Cluster xxxxxxxxxxxx* 10.0.0.0/16
- 2 subredes: 10.0.128.0/24 y 10.0.129.0/24

- 1 puerta de enlace de Internet
- 1 puerta de enlace NAT

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

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

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con soluciones de Nutanix Cloud y de partners.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

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

Entornos de virtualización de VMware

January 24, 2024

Si quiere utilizar VMware para proporcionar máquinas virtuales, siga estas instrucciones.

Instale vCenter Server y las herramientas de administración adecuadas. (No se admite la operación "Linked Mode"de vSphere vCenter.)

> **Nota:**
>
> No se admite la operación "Linked Mode"de vSphere vCenter.

Si piensa usar Machine Creation Services (MCS), no inhabilite la función de explorador del almacén de datos (Datastore Browser) en el servidor vCenter, como se describe en Disabling the vCenter Server Datastore Browser. Si inhabilita esta función, MCS no funciona correctamente.

Para configurar los entornos de virtualización de VMware, consulte Agregar un tipo de recurso o activar un dominio no utilizado en Citrix Cloud.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con VMware.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

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

Soluciones de VMware Cloud y de partners

January 24, 2024

Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) admite estas soluciones de VMware Cloud y de partners:

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

Utilice Citrix DaaS para migrar cargas locales de trabajo de Citrix basadas en VMware a las soluciones de partners de VMware correspondientes.

Integración de Azure VMware Solution (AVS)

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

Configurar el clúster de AVS

Para permitir que Citrix DaaS use AVS, siga estos pasos en Azure:

- Solicitar una cuota del host
- Registrar el proveedor de recursos `Microsoft.AVS`

- Verificar la lista de comprobación de planificación de redes
- Lista de comprobación para la red
- Crear una nube privada de AVS
- Acceder a la nube privada de AVS
- Configurar redes para la nube privada de VMware en Azure
- Configurar DHCP para AVS
- Agregar un segmento de red en AVS
- Verificar el entorno de AVS

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

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

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

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

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

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

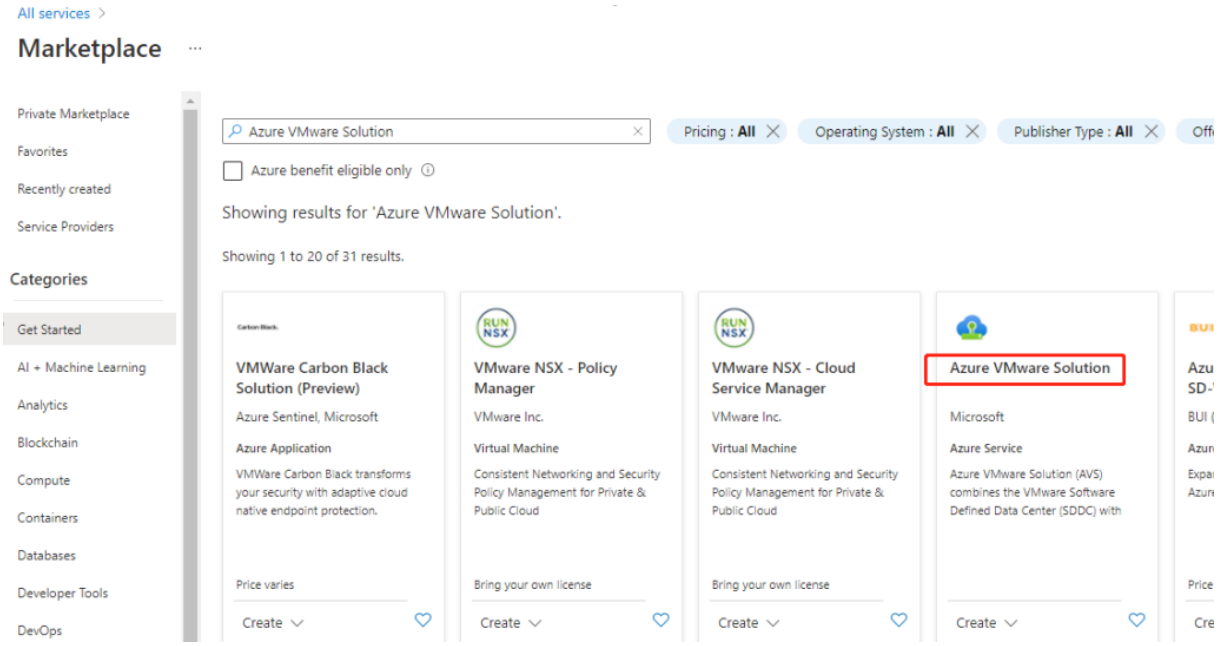
Registrar el proveedor de recursos Microsoft.AVS Después de solicitar la cuota del host, registre el proveedor de recursos:

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

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

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

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



En la ventana **Azure VMware Solution**:

1. Seleccione **Create**.
2. Vaya a la ficha **Basics**.
3. Introduzca valores para los campos con la información de esta tabla:

Campo	Valor
Subscription	Seleccione la suscripción que piensa utilizar para la implementación. Todos los recursos de una suscripción de Azure se facturan juntos.

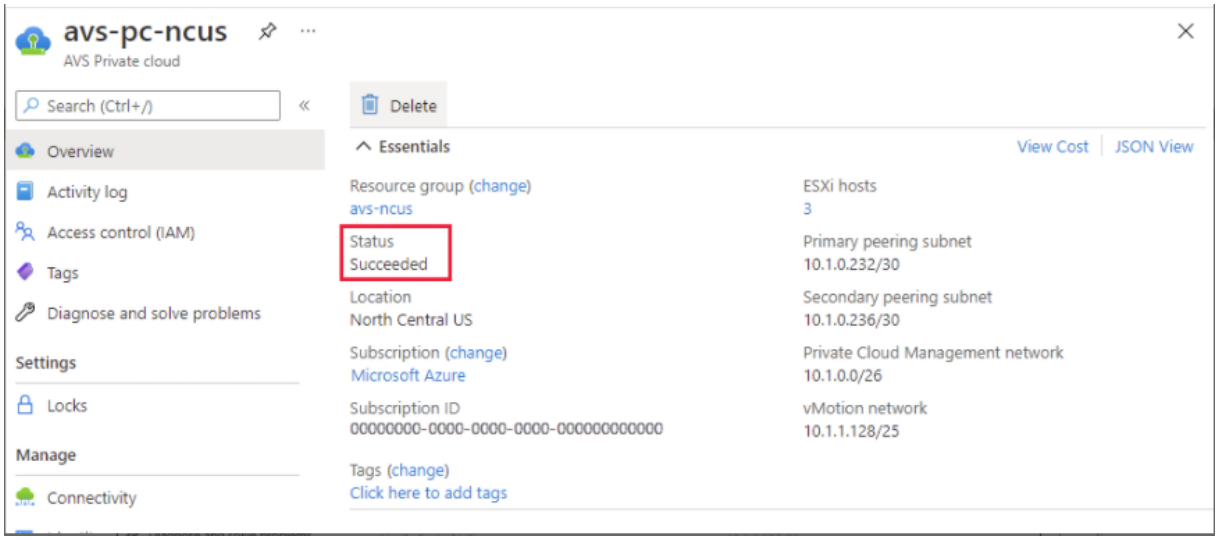
Campo	Valor
Resource group	Seleccione el grupo de recursos de su nube privada. Un grupo de recursos de Azure es un contenedor lógico en el que se implementan y administran recursos de Azure. Si no, también puede crear otro grupo de recursos para su nube privada.
Location	Seleccione una ubicación, como East US. Esta es la región definida durante la fase de planificación.
Resource name	Proporcione el nombre de su nube privada de Azure VMware Solution.
Size of host	Seleccione el tamaño que necesite.
Number of hosts	Muestra la cantidad de hosts asignados al clúster de nubes privadas. El valor predeterminado es 3, que se puede aumentar o reducir después de la implementación.
Address block for private cloud	Proporciona un bloque de direcciones IP para la nube privada. La redirección CIDR representa la red de administración de nubes privadas y se utilizará para los servicios de administración de clústeres, como vCenter Server y NSX-T Manager. Utilice el espacio de direcciones /22; por ejemplo, 10.175.0.0/22. La dirección debe ser única y no solaparse con otras redes virtuales de Azure ni con redes locales.

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

1. En el campo **Location**, seleccione la región que tiene el servicio AVS. La región del grupo de recursos es la misma que la región de AVS.
2. En el campo **Size of host**, seleccione el tamaño que necesite.
3. Especifique una dirección IP en el campo **Address Block for private cloud**. Por ejemplo, 10.15.0.0/22.
4. Seleccione **Review + Create**.
5. Tras revisar la información, haga clic en **Create**.

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

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



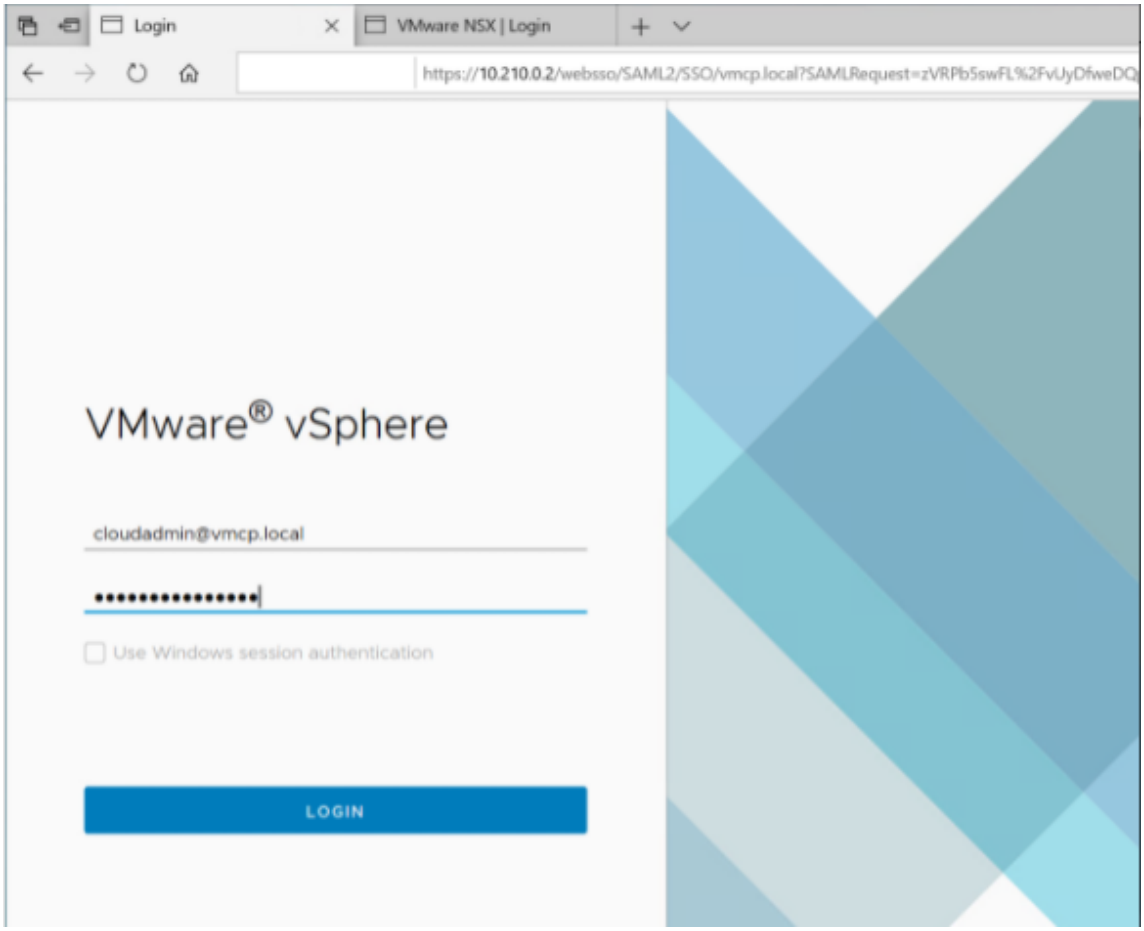
Acceder a la nube privada de AVS Una vez que haya creado una nube privada, cree una máquina virtual de Windows y conéctese al vCenter local de su nube privada.

Crear una máquina virtual de Windows

1. En el grupo de recursos, seleccione **+ Add**, busque **Microsoft Windows 10/11 o Windows Server 2016/2019** y seleccione esa opción.
2. Introduzca la información necesaria y, a continuación, seleccione **Review + Create**.
3. Una vez superada la validación, seleccione **Create** para iniciar el proceso de creación de máquinas virtuales.

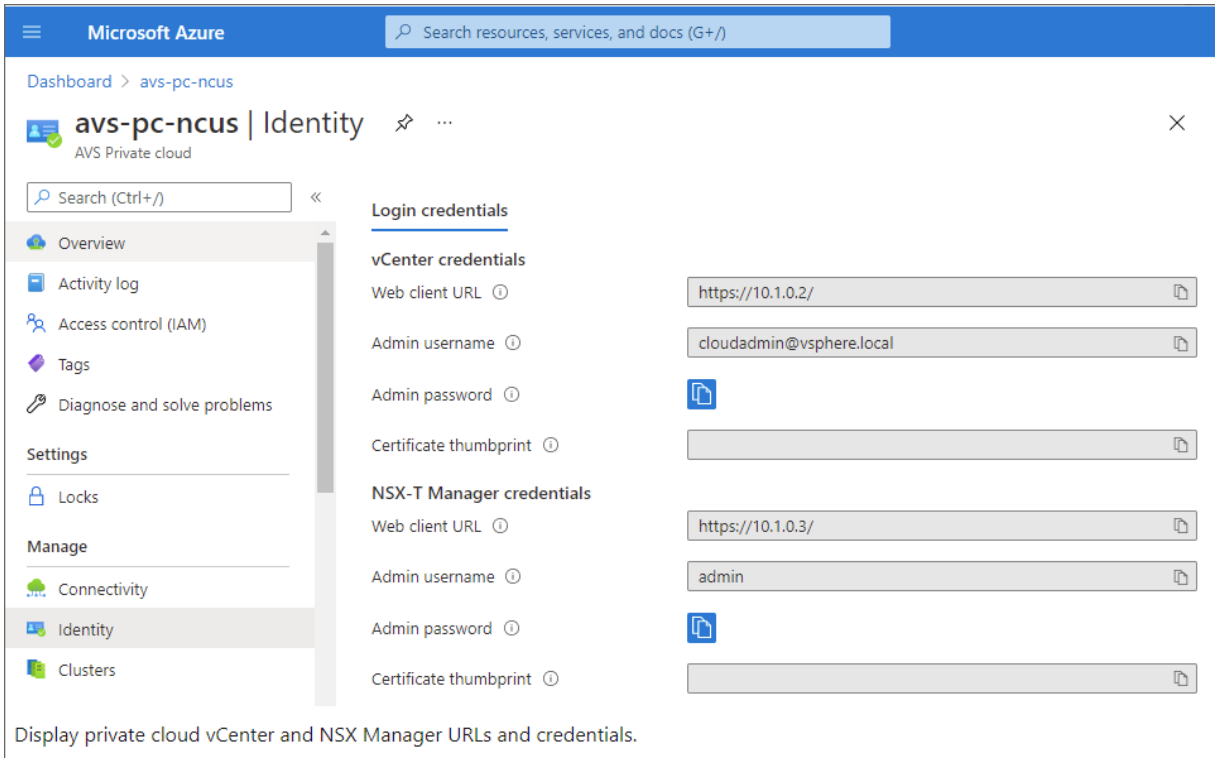
Conectarse al vCenter local de su nube privada

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



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

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



Display private cloud vCenter and NSX Manager URLs and credentials.

Tras confirmar las URL y las credenciales de usuario:

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

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

Crear una red virtual

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

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

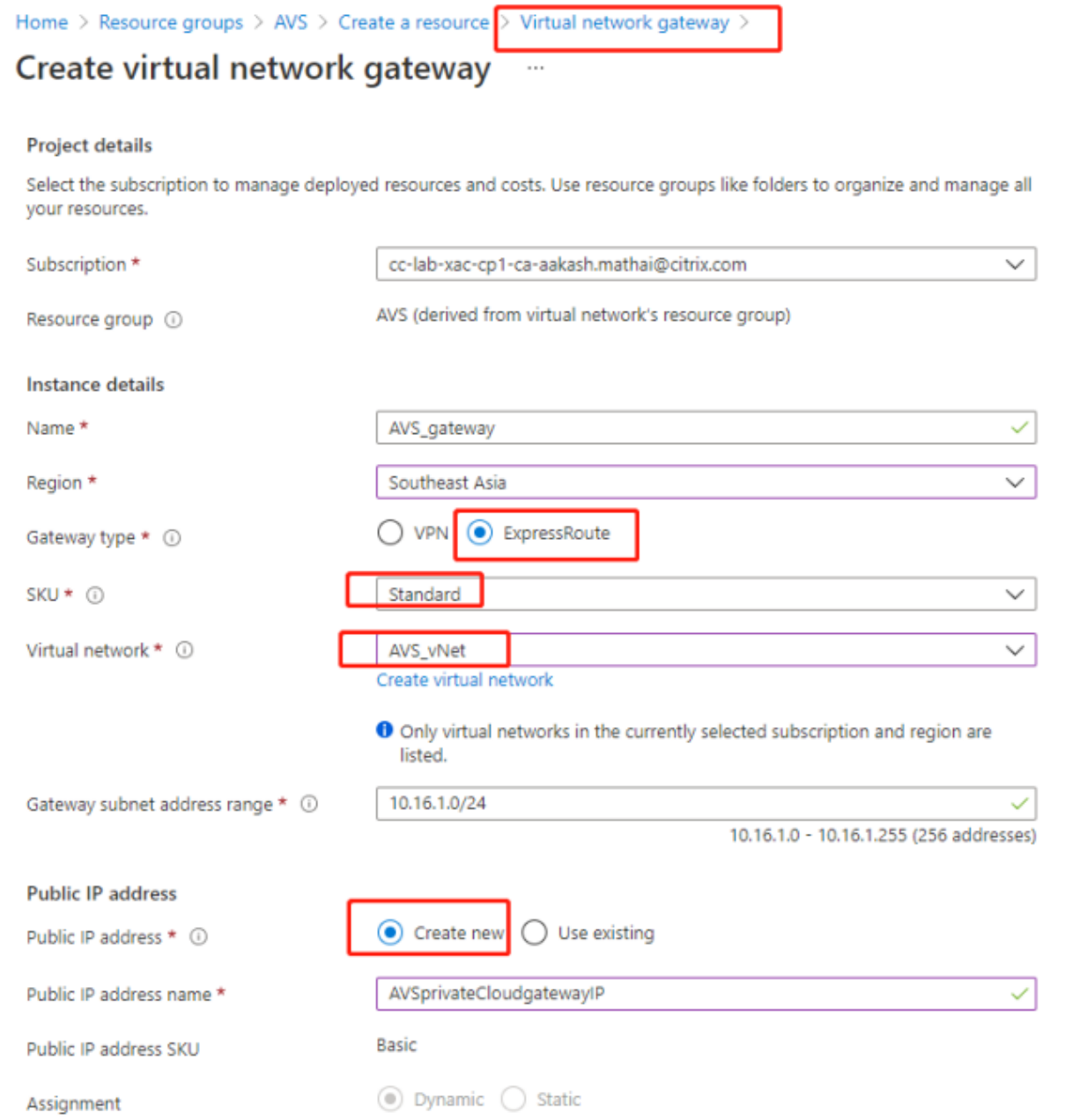
> **Importante:**
>
> Utilice una dirección que no se superponga con el espacio de direcciones que utilizó al crear su nube privada.

Después de introducir el espacio de direcciones:

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

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

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

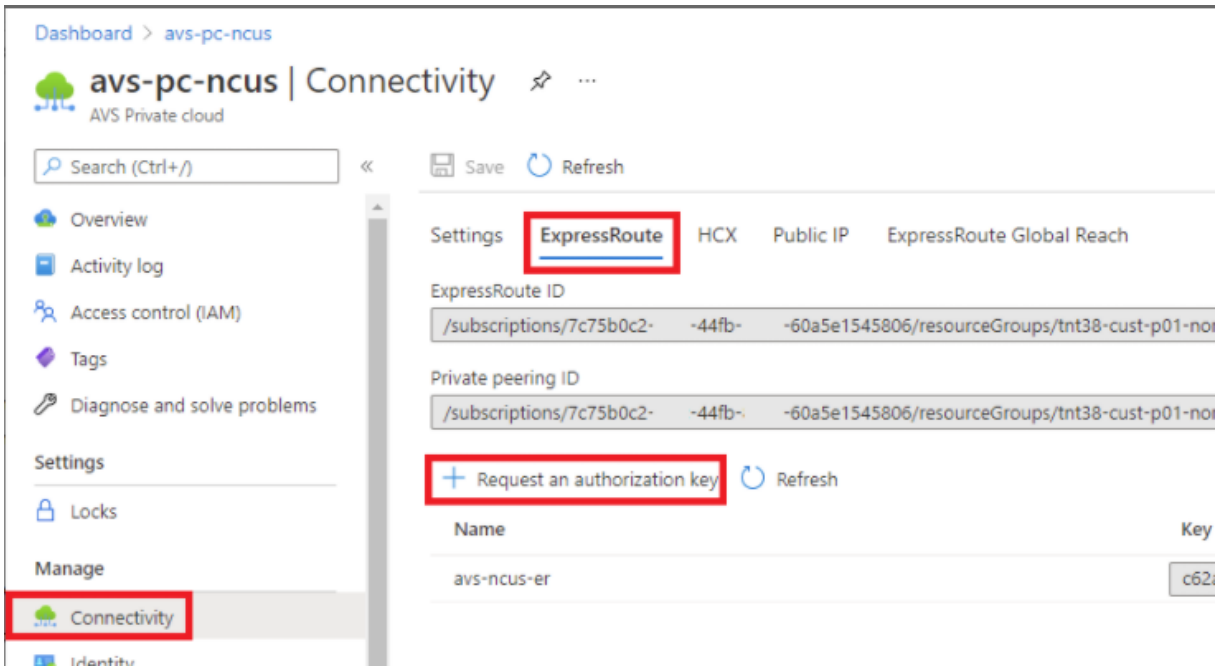


Tras revisar la configuración de la puerta de enlace de red virtual, haga clic en **Create** para implementar la puerta de enlace de red virtual.
Una vez finalizada la implementación, conecte su conexión de **ExpressRoute** a la puerta de enlace de red virtual que contiene la nube privada de AVS.

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

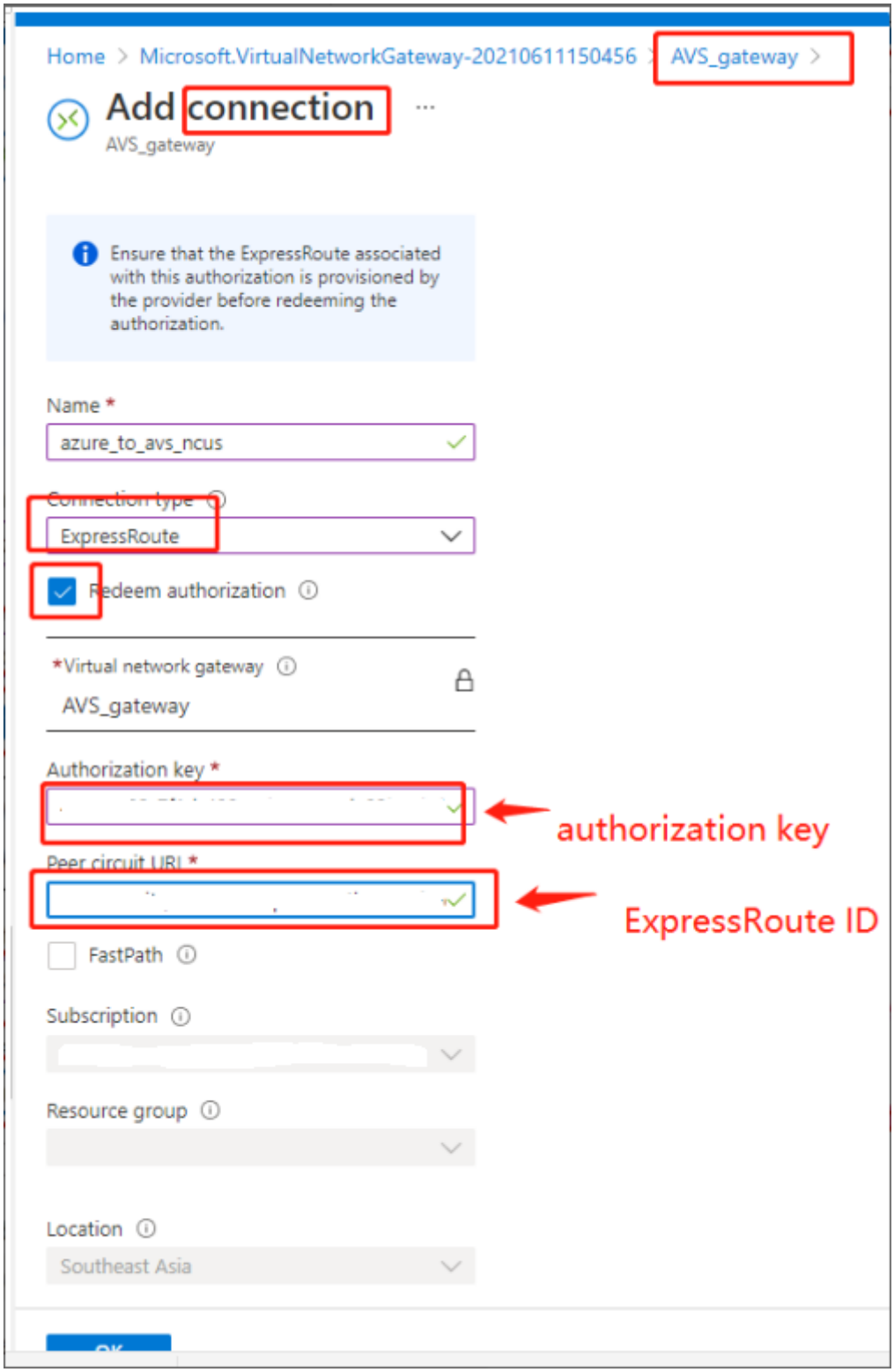
1. Solicite una clave de autorización de ExpressRoute.

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

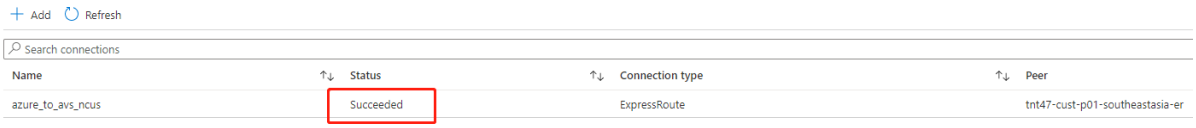


Después de solicitar una clave de autorización:

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



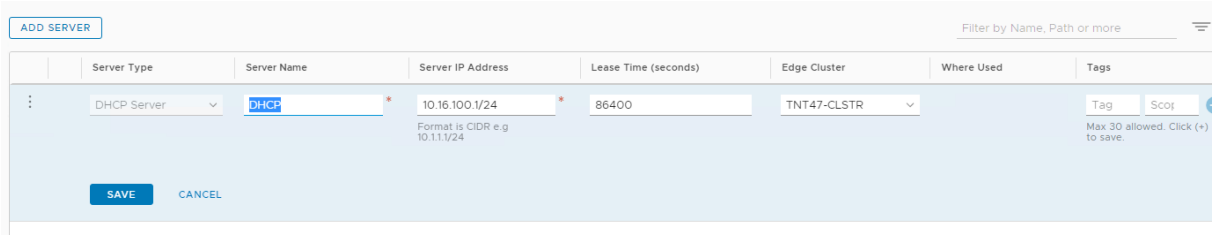
La conexión se establece entre el circuito de ExpressRoute y la red virtual:



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

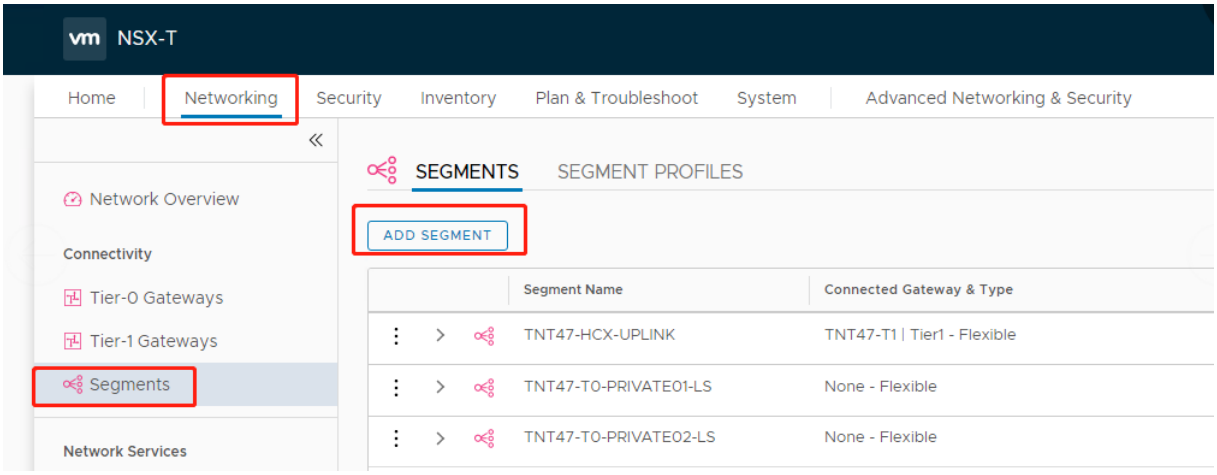
Usar NSX-T para alojar el servidor DHCP En NSX-T Manager:

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



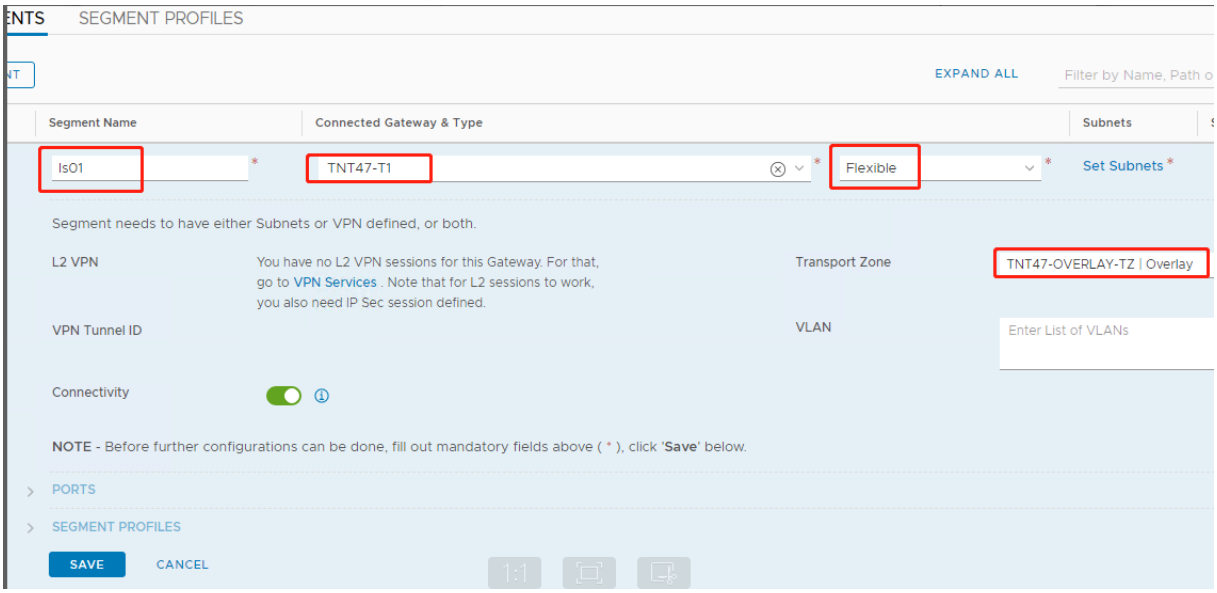
Agregar un segmento de red en Azure VMware Solution Después de configurar DHCP, agregue un segmento de red.

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



En la pantalla **Segments profile**:

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



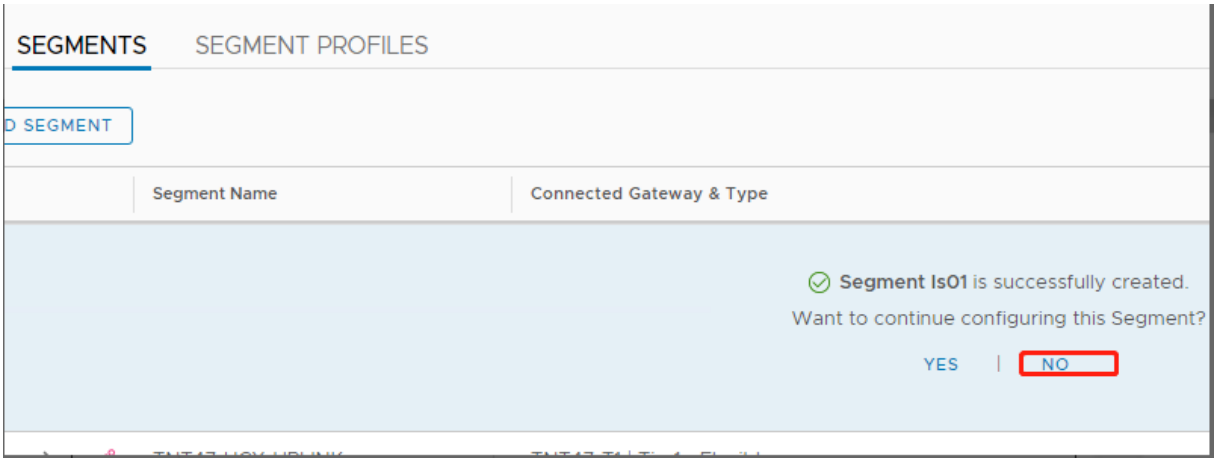
En la sección **Subnets**:

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

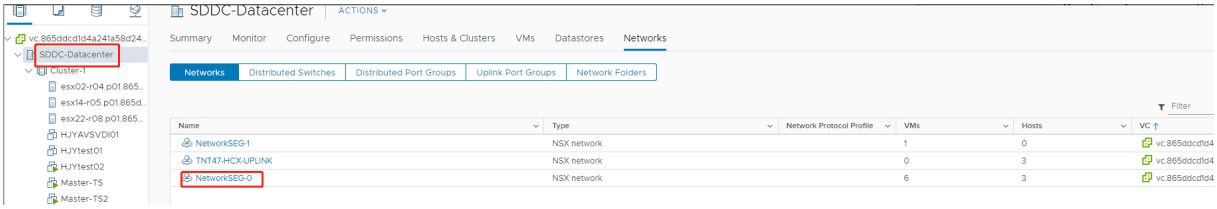
> **Importante:**
>
> La dirección IP de este segmento debe pertenecer a la dirección IP de la puerta de enlace de Azure, 10.15.0.0/22.

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

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



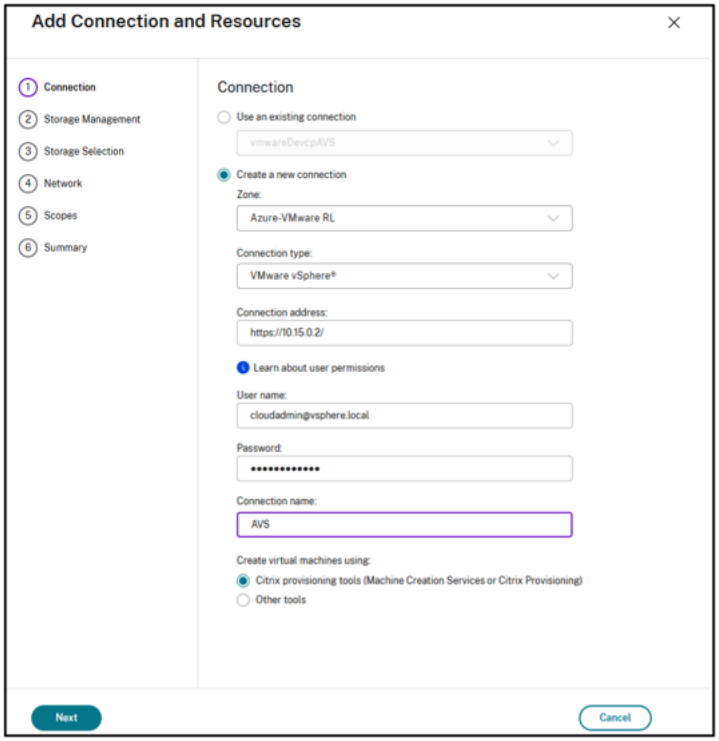
En vCenter, seleccione **Networking > SDDC-Datacenter**:



Verificar el entorno de AVS Configure la ubicación de recursos para la nube privada de AVS e instale un par de Cloud Connectors.

Crear la conexión de AVS en Citrix Studio

1. Cree una máquina en vCenter e instale un par de Cloud Connectors en la máquina. Consulte Configurar las instancias.
2. En **Administrar > Configuración completa**, seleccione Alojamiento en el panel de la izquierda.
3. Seleccione el nodo de alojamiento y haga clic en **Agregar conexión y recursos**.
4. En la pantalla **Conexión**, seleccione **Crear una nueva conexión** y los siguientes detalles:



a) Seleccione el **Tipo de conexión VMware vSphere**.
b) En **Dirección de la conexión**, introduzca la dirección IP privada de vCenter.
c) Introduzca las credenciales de vCenter.
d) Escriba un nombre para la conexión.
e) Elija la herramienta para crear máquinas virtuales.

5. En la pantalla **Red**, seleccione la subred creada en el servidor NSX-T.
6. Complete el asistente.

Google Cloud VMware Engine

Citrix DaaS le permite migrar cargas de trabajo de Citrix locales basadas en VMware a VMware Engine de Google Cloud.

Configurar Google Cloud VMware Engine

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

Acceder al portal de VMware Engine

1. En la **consola de Google Cloud**, haga clic en el menú de navegación.

2. En la sección **Compute**, haga clic en **VMware Engine** para abrir VMware Engine en una nueva ficha de explorador.

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

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

   > **Nota:**
   >
   > La implementación de HCX solo se aplica a IP Plan versión 1.0.

3. Obtenga el rol de "administrador de servicios de VMware Engine"de IAM.

Crear la primera nube privada

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

   > **Importante:**
   >
   > - El rango de enrutamiento CIDR no debe superponerse con ninguna de sus subredes locales o en la nube. El rango de enrutamiento CIDR debe ser /27 o superior.
   > - La implementación de HCX solo se aplica a IP Plan versión 1.0.

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

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

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

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

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

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

Implementar una puerta de enlace de VPN

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

Conectar la VPN

1. Establezca una conexión de punto a sitio entre su red local y la nube privada mediante la configuración de VPN Gateway. Consulte Configurar la puerta de enlace de VPN de Google Cloud VMware Engine.
2. Cargue la configuración de VPN descargada en Configurar la puerta de enlace de VPN de Google Cloud VMware Engine.
3. Importe a su cliente VPN, por ejemplo, OpenVPN Connect.

Para obtener más información, consulte Connecting using VPN.

Crear la primera subred

Acceder a NSX-T Manager desde el portal de VMware Engine El proceso de creación de una subred se produce en NSX-T, al que se accede a través de VMware Engine. Haga lo siguiente para acceder a NSX-T Manager.

1. Inicie sesión en el portal de **Google Cloud VMware Engine**.
2. En el menú de navegación principal, vaya a **Resources**.
3. Haga clic en el **nombre de la nube privada** en la que desea crear la subred.
4. En la página de detalles de la nube privada, haga clic en la ficha **vSphere Management Network**.
5. Haga clic en el **nombre de dominio completo** correspondiente a NSX-T Manager.
6. Cuando se le indique, introduzca sus credenciales de inicio de sesión. Si ha configurado vIDM y lo ha conectado a un origen de identidad, como Active Directory, use sus credenciales de origen de identidad en su lugar.

   > **Aviso:**
   >
   > Puede recuperar las credenciales generadas en la página de detalles de la nube privada.

Configurar el servicio DHCP para la subred Antes de crear una subred, configure un servicio DHCP:

En NSX-T Manager:

1. Vaya a **Networking > DHCP**. El panel de mandos de redes muestra que el servicio DHCP crea una puerta de enlace de nivel 0 y una de nivel 1.
2. Para comenzar a aprovisionar un servidor DHCP, haga clic en **Add Server**.
3. Seleccione **DHCP** para **Server Type**, proporcione el nombre del servidor y la dirección IP.
4. Haga clic en **Save** para crear el servicio DHCP.

Haga lo siguiente para conectar este servicio DHCP a la puerta de enlace de nivel 1 correspondiente. El servicio DHCP ya ha aprovisionado una puerta de enlace de nivel 1 predeterminada:

1. Seleccione **Tier 1 Gateways**, seleccione los puntos suspensivos en vertical de la puerta de enlace de nivel 1 y, a continuación, seleccione **Edit**.
2. En el campo **IP Address Management**, seleccione **No IP Allocation Set**.
3. Seleccione **DHCP Local Server** para **Type**.
4. Seleccione el servidor DHCP que creó para **DHCP Server**.
5. Haga clic en **Guardar**.
6. Haga clic en **Close Editing**.

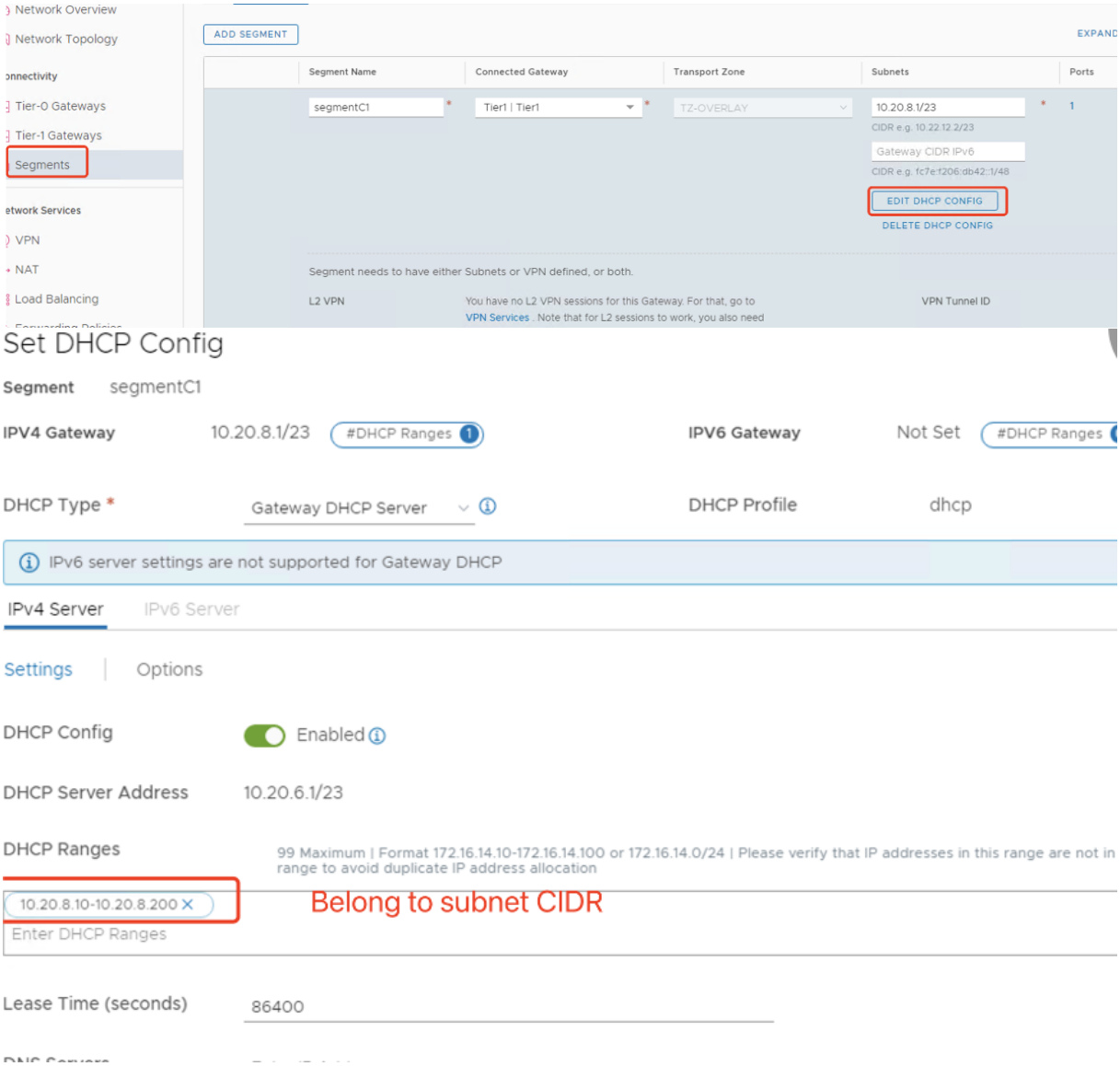
Ahora puede crear un segmento de red en NSX-T. Para obtener más información sobre DHCP en NSX-T, consulte la documentación de VMware para DHCP.

Crear un segmento de red en NSX-T Para las VM de carga de trabajo, cree subredes como segmentos de red de NSX-T para su nube privada:

1. En NSX-T Manager, vaya a **Networking > Segments**.
2. Haga clic en **Add Segment**.
3. Introduzca un nombre para el segmento en Name.
4. Seleccione **Tier -1** como **Connected Gateway** y deje Type como **Flexible**.
5. Haga clic en **Set Subnets**.
6. Haga clic en **Add Subnets**.
7. En **Gateway IP/Prefix Length**, introduzca el rango de subredes. Especifique el rango de subredes con **.1** como último octeto. Por ejemplo, **10.12.2.1/24**.
8. Especifique los rangos de DHCP y haga clic en **ADD**.
9. En **Transport Zone**, seleccione **TZ-OVERLAY** en la lista desplegable.
10. Haga clic en **Guardar**. Ahora puede seleccionar este segmento de red en vCenter al crear una VM.

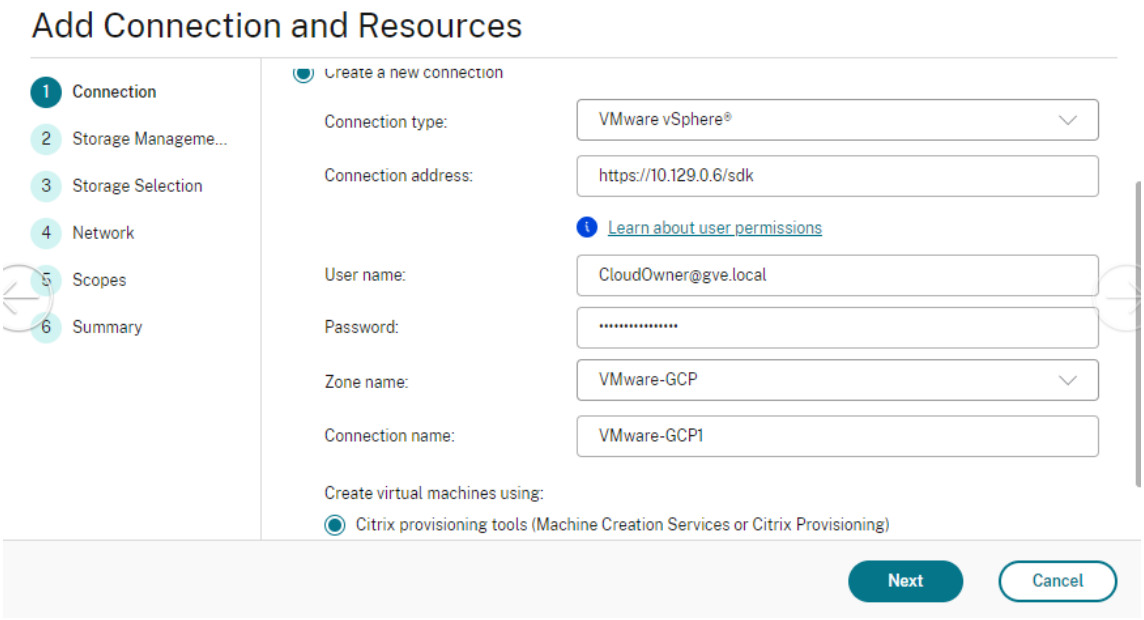
En una región determinada, puede configurar como máximo 100 rutas únicas desde VMware Engine a su red de VPC mediante el acceso a servicios privados. Esto incluye, por ejemplo, rangos de direcciones IP de administración de nube privada, segmentos de red de carga de trabajo de NSX-T y rangos de direcciones IP de red HCX. Este límite incluye todas las nubes privadas de la región.

> **Nota:**
>
> Existe un problema de configuración de Google Cloud por el que debe configurar el rango DHCP varias veces. Por lo tanto, asegúrese de configurar el rango DHCP después de la configuración de Google Cloud. Haga clic en **EDIT DHCP CONFIG** para configurar los rangos DHCP.



Crear la conexión de VMware de Google Cloud en Citrix Studio

1. Cree una máquina en vCenter e instale un par de Cloud Connectors en la máquina. Consulte Configurar las instancias.
2. Abra Citrix Studio.
3. Seleccione el nodo de alojamiento y haga clic en **Agregar conexión y recursos**.
4. En la pantalla **Conexión**, seleccione **Crear una nueva conexión** y los siguientes detalles:



a) Seleccione el **Tipo de conexión VMware vSphere**.
b) En **Dirección de la conexión**, introduzca la dirección IP privada de vCenter.
c) Introduzca las credenciales de vCenter.
d) Escriba un nombre para la conexión.
e) Elija la herramienta para crear máquinas virtuales.

5. En la pantalla **Red**, seleccione la subred creada en el servidor NSX-T.
6. Complete el asistente.

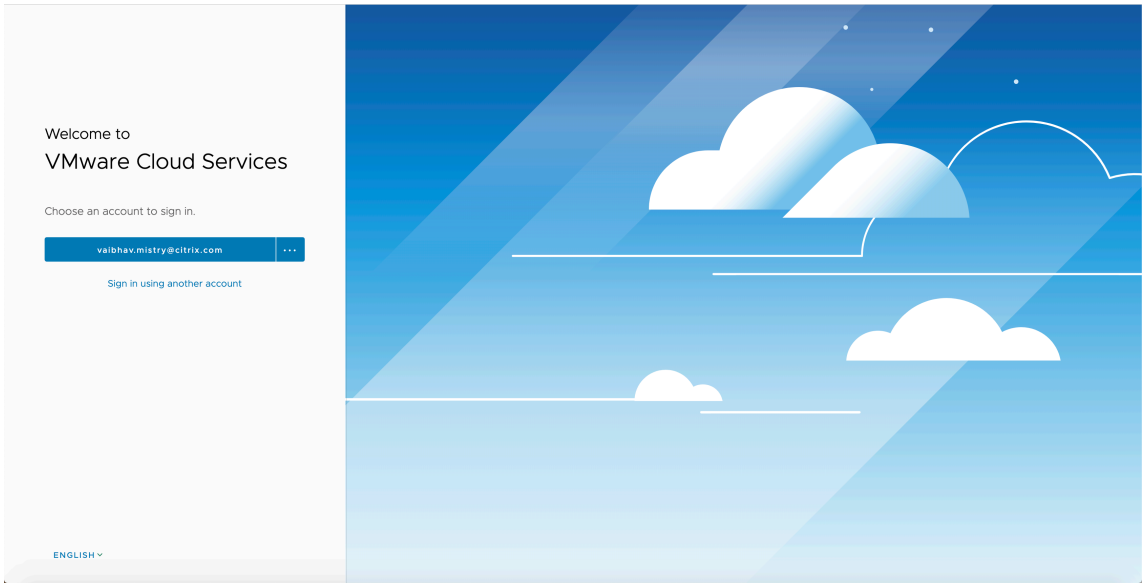
VMware Cloud en Amazon Web Services (AWS)

VMware Cloud en Amazon Web Services (AWS) le permite migrar cargas locales de trabajo de Citrix basadas en VMware a AWS Cloud y su entorno principal de Citrix Virtual Apps and Desktops a Citrix DaaS.

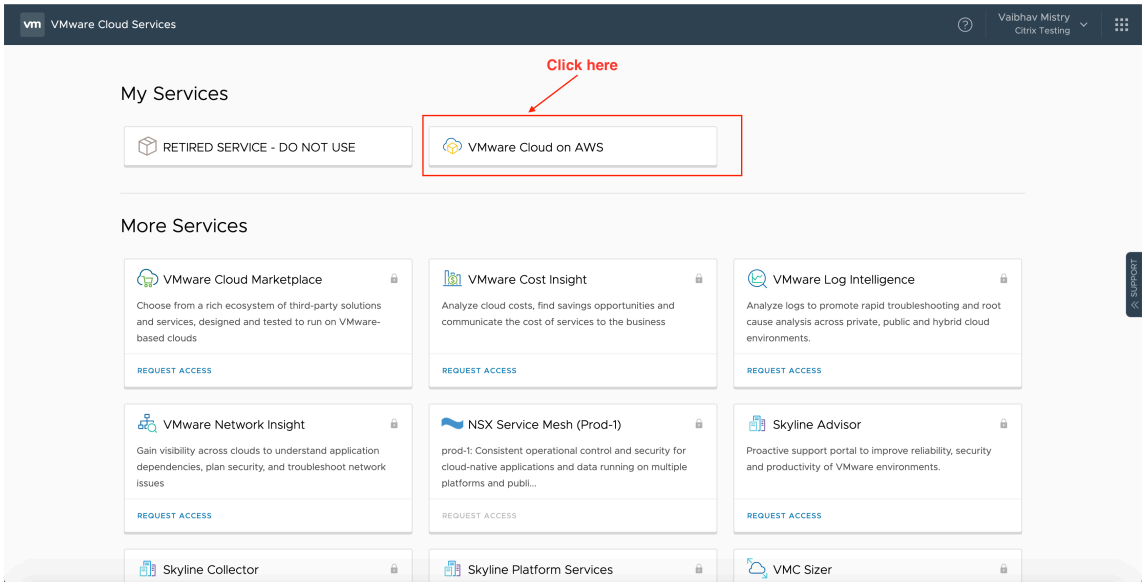
En este artículo se describe el procedimiento para configurar VMware Cloud en AWS.

Acceder al entorno de VMware Cloud

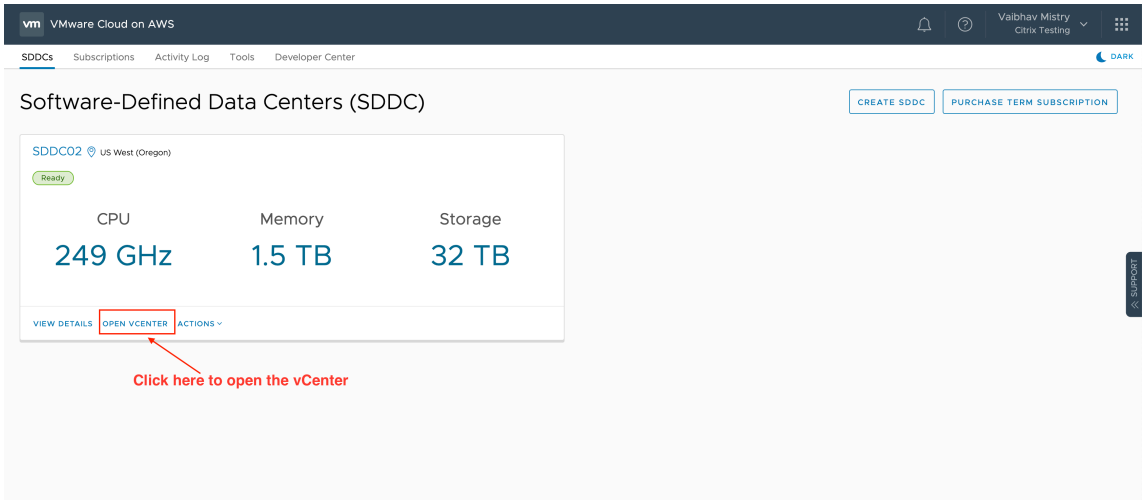
1. Inicie sesión en los servicios de VMware Cloud mediante la URL https://console.cloud.vmware.com/.

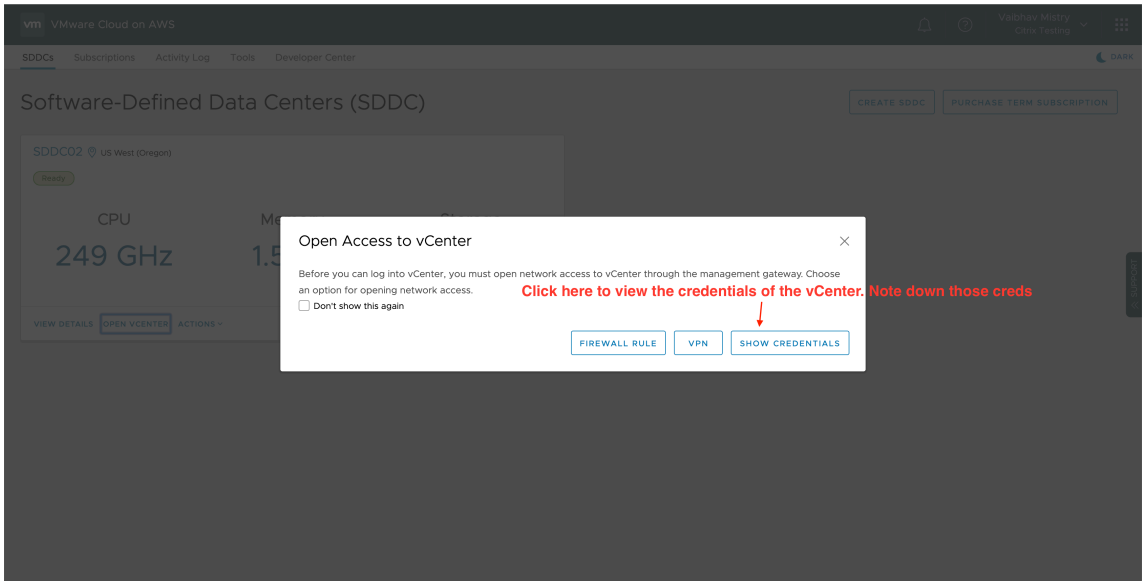


2. Haga clic en **VMware Cloud on AWS**. Aparecerá la página Software-Defined Data Centers (SDDC).

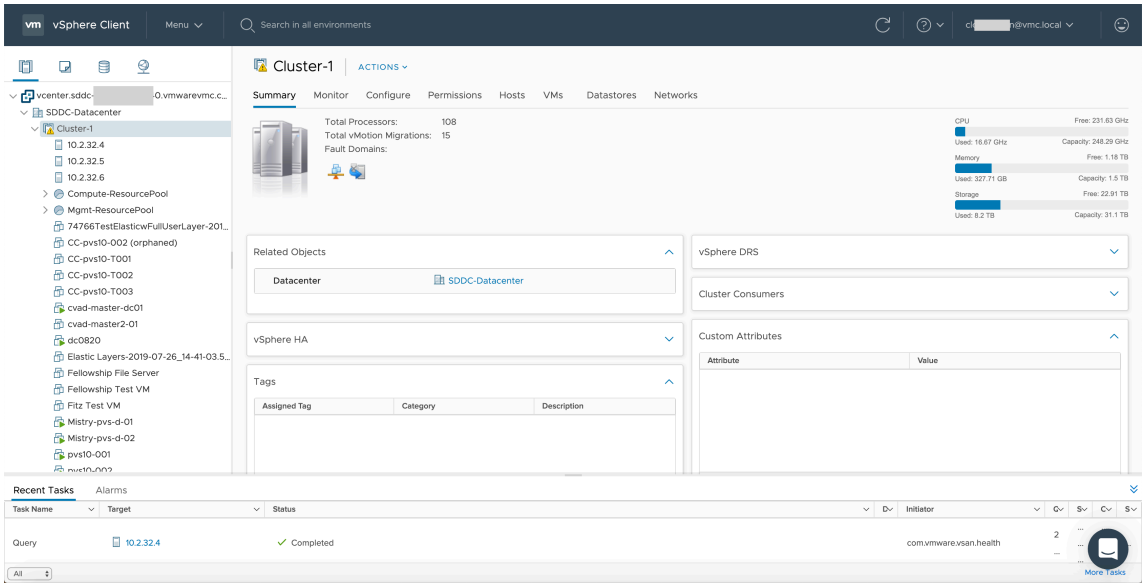


3. Haga clic en **OPEN VCENTER** y, a continuación, en **SHOW CREDENTIALS**. Anote las credenciales para usarlas más adelante.





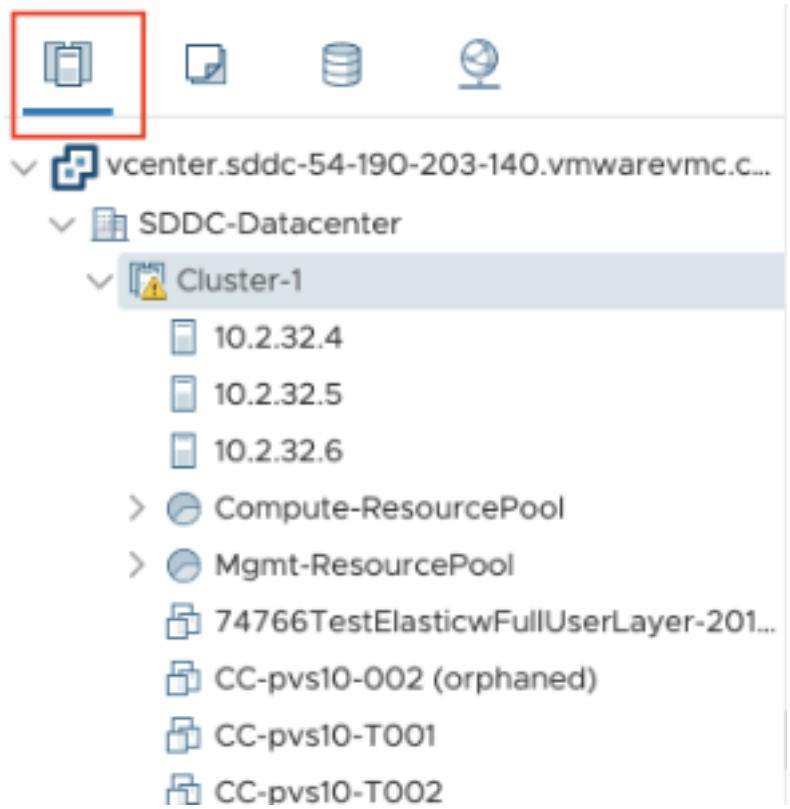
4. Abra un explorador web e introduzca la URL de vSphere Web Client.
5. Introduzca las credenciales anotadas y haga clic en **Login**. La página web del cliente de vSphere es similar al entorno local.



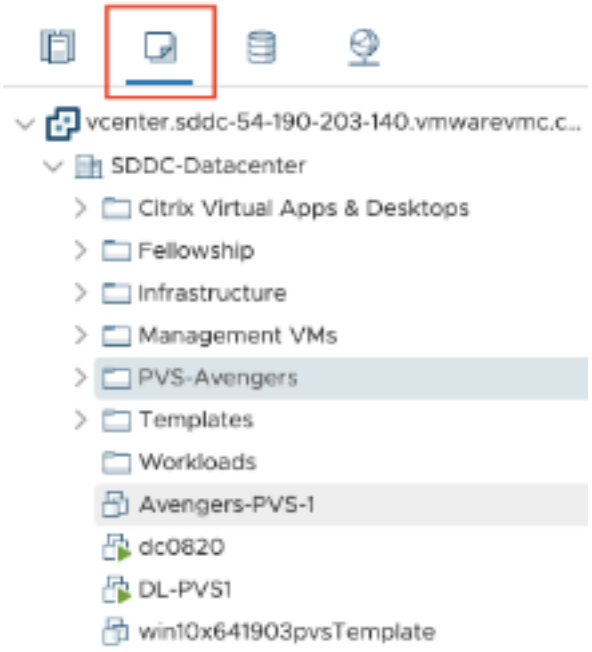
Acerca del entorno de VMware Cloud

Hay cuatro vistas en la página web del cliente de vSphere.

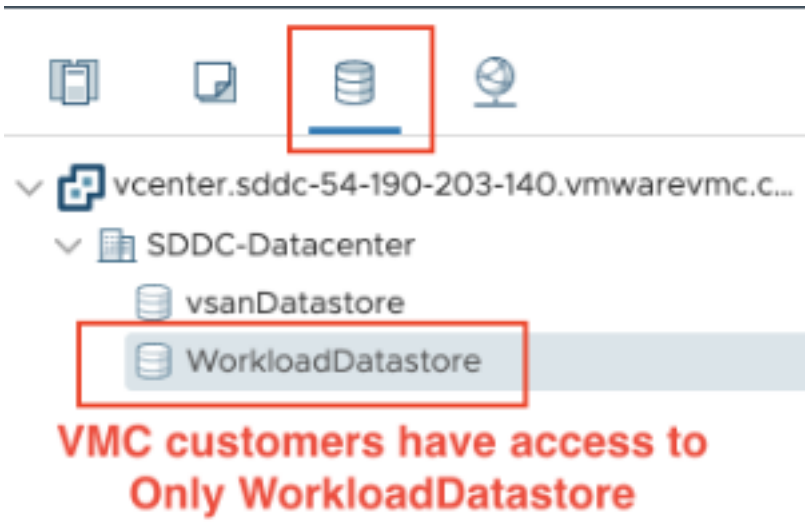
- Vista Host y Cluster: No puede crear clústeres, pero el administrador de la nube puede crear varios grupos de recursos.



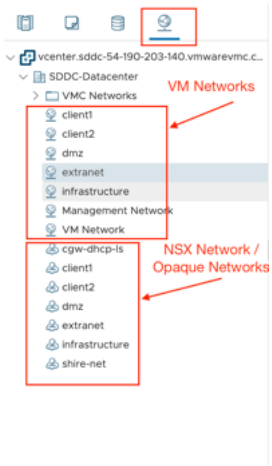
- Vista VM y Template: El administrador de la nube puede crear muchas carpetas.



- Vista Storage: Seleccione el almacenamiento **WorkloadDatastore** cuando agregue la unidad de alojamiento en Citrix Studio porque tiene acceso a Workload Datastore solamente.



- Vista Network: Los iconos son diferentes para las redes de la nube de VMware y las redes opacas.



Después de configurar el clúster, consulte Entornos de virtualización de VMware para agregar conexiones y recursos.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.

- Para crear y administrar una conexión, consulte Conexión con soluciones de VMware Cloud y de partners.
- Revisar todos los pasos del proceso de instalación y configuración

Más información

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

Entornos de virtualización de XenServer

January 24, 2024

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

Para configurar XenServer, consulte Agregar un tipo de recursos.

Qué hacer a continuación

- Para una implementación sencilla de prueba de concepto, instale un VDA en una máquina designada para entregar aplicaciones o un escritorio a los usuarios.
- Para crear y administrar conexiones, consulte Conexión con XenServer.
- Revisar todos los pasos del proceso de instalación y configuración.

Más información

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

Consideraciones de tamaño y escala para los Cloud Connectors

January 24, 2024

Cuando evalúe Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) para determinar la dimensión y la escalabilidad, tenga en cuenta todos los componentes. Investigue y pruebe la configuración

de los Citrix Cloud Connectors y el StoreFront para sus requisitos específicos. Proporcionar recursos insuficientes para dimensionamiento y escalabilidad afecta negativamente al rendimiento de la implementación.

> **Nota:**
>
> - Estas recomendaciones se aplican a Citrix DaaS Standard para Azure, además de aplicarse a Citrix DaaS.
> - Las pruebas y recomendaciones que figuran en este artículo son pautas que le servirán para comenzar con las pruebas. Le recomendamos que realice las pruebas en su entorno para validar el tamaño de conector correcto.

En este artículo encontrará detalles sobre las capacidades máximas probadas, además de recomendaciones de mejores prácticas para la configuración de la máquina de Cloud Connector. Las pruebas se realizaron en implementaciones configuradas con StoreFront y la caché de host local (LHC).

La información proporcionada es aplicable a las implementaciones en las que cada ubicación de recursos contiene cargas de trabajo de VDI o cargas de trabajo de RDS. Para las ubicaciones de recursos que contienen cargas de trabajo mixtas de VDI y RDS, póngase en contacto con Citrix Consulting Services.

Cloud Connector enlaza sus cargas de trabajo a Citrix DaaS de las siguientes formas:

- Proporciona un proxy para la comunicación entre los VDA y Citrix DaaS
- Proporciona un proxy para la comunicación entre Citrix DaaS y su instancia de Active Directory (AD) e hipervisores
- En las implementaciones que incluyen servidores de StoreFront, el Cloud Connector actúa como intermediario de sesión temporal durante las interrupciones de la nube, proporcionando a los usuarios acceso continuo a los recursos

Es importante que sus Cloud Connectors tengan el tamaño y la configuración adecuados para satisfacer sus necesidades específicas.

Cada conjunto de Cloud Connectors se asigna a una ubicación de recursos (también conocida como zona). Una ubicación de recursos es una separación lógica que especifica qué recursos se comunican con ese conjunto de Cloud Connectors. Se necesita al menos una ubicación de recursos por dominio para comunicar con Active Directory (AD).

Cada catálogo de máquinas y conexión de host se asigna a una ubicación de recursos.

En el caso de las implementaciones con más de una ubicación de recursos, asigne catálogos de máquinas y VDA a las ubicaciones de recursos a fin de optimizar la capacidad de la LHC de intermediar en las conexiones durante las interrupciones. Para obtener más información sobre la creación y administración de ubicaciones de recursos, consulte Conectarse a Citrix Cloud. Para obtener un rendimiento óptimo, configure los Cloud Connectors en conexiones de baja latencia a los VDA, los servidores de AD y los hipervisores.

Procesadores y almacenamiento recomendados

Para obtener un rendimiento similar al observado en estas pruebas, utilice procesadores modernos compatibles con extensiones SHA. Las extensiones SHA reducen la carga criptográfica en la CPU. Los procesadores recomendados incluyen:

- Procesadores Zen y más recientes de Advanced Micro Devices (AMD)
- Procesadores Intel Ice Lake y más modernos

Los procesadores recomendados funcionan de manera eficiente. Puede utilizar procesadores más antiguos; sin embargo, podría aumentar la carga de la CPU. Recomendamos aumentar la cantidad de vCPU para compensar esta situación.

Las pruebas descritas en este artículo se realizaron con procesadores AMD EPYC e Intel Cascade Lake.

Los Cloud Connectors tienen una gran carga criptográfica mientras se comunican con la nube. Los Cloud Connectors que utilizan procesadores con extensiones SHA tienen una carga de CPU menor, lo que se expresa en un menor uso de CPU por parte del Servicio de Subsistema de Autoridad de Seguridad Local de Windows (LSASS).

Citrix recomienda usar almacenamiento moderno con operaciones de E/S por segundo (IOPS) adecuadas, especialmente en las implementaciones que utilizan LHC. Se recomiendan las unidades de estado sólido (SSD), pero no se necesitan niveles de almacenamiento en la nube premium. Se necesitan niveles de IOPS más altos en los entornos con LHC en los que Cloud Connector ejecuta una pequeña copia de la base de datos. Esta base de datos se actualiza periódicamente con cambios en la configuración del sitio y proporciona funciones de intermediación en la ubicación de recursos en momentos de interrupción de Citrix Cloud.

Configuración de procesamiento recomendada para la caché de host local

La caché de host local (LHC) proporciona alta disponibilidad al permitir que la intermediación de las conexiones de una implementación continúen cuando un Cloud Connector no puede comunicarse con Citrix Cloud.

Los Cloud Connectors ejecutan Microsoft SQL Express Server LocalDB, que se instala automáticamente al instalar Cloud Connector. La configuración de CPU de Cloud Connector, especialmente la cantidad de núcleos disponibles para SQL Express Server LocalDB, afecta directamente al rendimiento de la LHC. La cantidad de núcleos de CPU disponibles para SQL Server Express Server LocalDB afecta al rendimiento de la caché de host local, incluso más que la asignación de memoria. Esta sobrecarga de CPU solo se observa en modo LHC cuando no se puede acceder a Citrix DaaS y el intermediario de LHC está activo. Para cualquier implementación que utilice LHC, Citrix recomienda cuatro núcleos por socket, con un mínimo de cuatro núcleos de CPU por Cloud Connector. Para

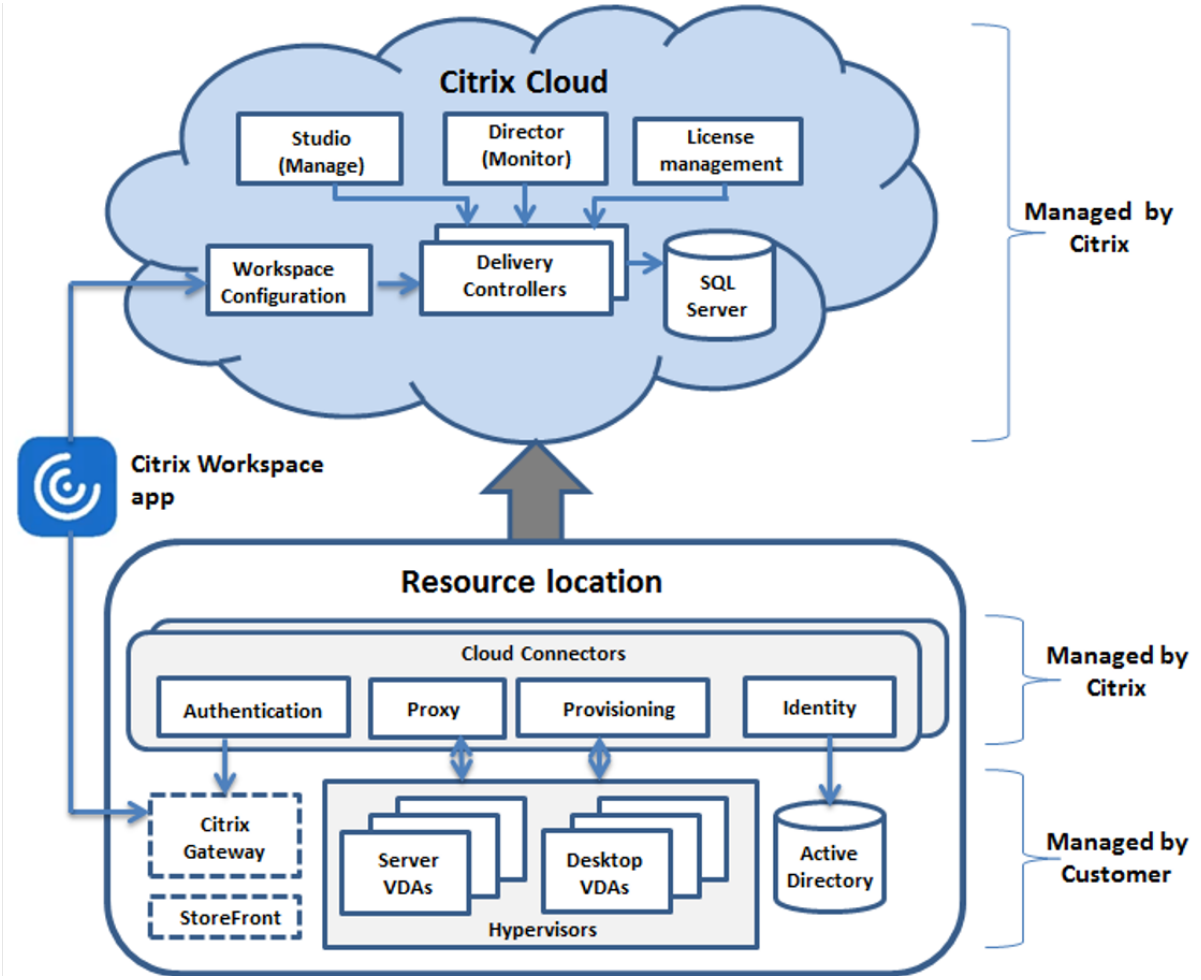
obtener información sobre la configuración de recursos de procesamiento para SQL Express Server LocalDB, consulte Compute capacity limits by edition of SQL Server.

Si los recursos de procesamiento disponibles para SQL Express Server LocalDB están mal configurados, los tiempos de sincronización de la configuración podrían aumentar y el rendimiento durante las interrupciones podría reducirse. En algunos entornos virtualizados, la capacidad de procesamiento puede depender de la cantidad de procesadores lógicos, y no de los núcleos de CPU.

Resumen de los resultados de las pruebas

Todos los resultados de este resumen se basan en los resultados obtenidos de un entorno de prueba según lo configurado en las secciones detalladas de este artículo. Los resultados que se muestran aquí son para una única ubicación de recursos. Las diferentes configuraciones del sistema pueden dar lugar a resultados diferentes.

En esta ilustración, se ofrece una descripción gráfica de la configuración probada.



Esta tabla proporciona una guía rápida para determinar el tamaño de la ubicación de recursos. 10 000

es el máximo para una sola ubicación de recursos. Consulte Límites para obtener información sobre los límites de una ubicación de los recursos.

> **Nota:**
>
> Superar el límite puede provocar problemas de conectividad y de rendimiento durante una interrupción del servicio. Por lo tanto, no debe superar el límite recomendado, ya que esto puede provocar que los VDA no se registren.

Los resultados se basan en pruebas internas de Citrix. Las configuraciones descritas se probaron con diferentes cargas de trabajo, incluidas pruebas de inicio de sesiones de alta velocidad y avalanchas de registros.

	Medio	Grande	Máximo
VDA	1000 VDI o 250 RDS	5000 VDI o 500 RDS	10 000 VDI o 1000 RDS
Conexiones de host	20	40	40
CPU para conectores	4 CPU virtuales	4 CPU virtuales	8 vCPU
Memoria para conectores	6 GB	8 GB	10 GB

Metodología de las pruebas

Se realizaron pruebas para agregar carga y medir el rendimiento de los componentes del entorno. Los componentes se supervisan mediante la recopilación de datos de rendimiento y el tiempo del procedimiento (como el tiempo de inicio de sesión o el tiempo de registro). En algunos casos, se utilizaron herramientas de simulación de Citrix para simular VDA y sesiones. Estas herramientas están diseñadas para utilizar los componentes de Citrix de la misma manera que lo hacen los VDA y las sesiones tradicionales, sin los mismos requisitos de recursos para alojar sesiones reales y VDA. Las pruebas se realizaron tanto en el modo de intermediación (broker) en la nube como en el modo de LHC para entornos con Citrix StoreFront.

Las recomendaciones para el dimensionamiento de Cloud Connector de este artículo se basan en los datos recopilados durante estas pruebas.

Se realizaron las siguientes pruebas:

- **Avalancha de inicios/inicios de sesión:** Una prueba que simula periodos de picos repentinos de inicios de sesión
- **Avalancha de registros de VDA:** Una prueba que simula periodos de picos repentinos de registros de VDA Por ejemplo, tras un ciclo de actualización o al realizar la transición entre el modo de intermediación en la nube y el modo de caché de host local.

- **Avalancha de acciones de energía de VDA:** Una prueba que simula un gran volumen de acciones de energía de VDA.

Casos y condiciones de las pruebas

Estas pruebas se realizaron con LHC configurada. Para obtener más información sobre el uso de LHC, consulte el artículo Caché de host local. LHC requiere un servidor StoreFront local. Para obtener información detallada sobre StoreFront, consulte la documentación de producto de StoreFront.

Recomendaciones para las configuraciones de StoreFront:

- Si tiene varias ubicaciones de recursos con un solo servidor o grupo de servidores de StoreFront, habilite la opción de verificación de estado avanzada para el almacén de StoreFront. Consulte los requisitos de StoreFront en el artículo Caché de host local.
- Para obtener tasas de inicio de sesiones más altas, utilice un grupo de servidores StoreFront. Consulte Configurar grupos de servidores en la documentación de producto de StoreFront.

Condiciones de prueba:

- Los requisitos de CPU y memoria son solo para el SO base y los servicios Citrix. Las aplicaciones y los servicios de terceros pueden requerir recursos adicionales.
- Los VDA son cualquier máquina virtual o física que ejecute Citrix Virtual Delivery Agent.
- Las pruebas se realizan únicamente con agentes VDA de Windows.
- En todos los VDA probados, se administraba la energía con Citrix DaaS.
- Se probaron cargas de trabajo de entre 1000 y 10 000 servidores VDI y entre 250 y 1000 servidores RDS con entre 1000 y 20 000 sesiones.
- Las sesiones RDS se probaron con hasta 20 000 por ubicación de recursos.
- Las pruebas se realizaron con un Cloud Connector tanto durante un funcionamiento normal como durante una interrupción del servicio. Citrix recomienda utilizar al menos dos Cloud Connectors para tener alta disponibilidad. En el modo de interrupción, solo se utiliza uno de los conectores para la intermediación y registro de VDA.
- Las pruebas se realizaron con el Cloud Connector configurado con procesadores Intel Cascade Lake.
- Las sesiones se iniciaron a través de un único servidor Citrix StoreFront.
- Las pruebas de inicio de sesiones con caché de host local durante las interrupciones tuvieron lugar después de volverse a registrar las máquinas.

Los recuentos de sesiones de RDS son una recomendación y no un límite. Pruebe su propio límite de sesiones de RDS en su entorno.

> **Nota:**

> El recuento de sesiones y la tasa de inicio son más importantes para RDS que el recuento de VDA.

Cargas de trabajo medias

Estas cargas de trabajo se probaron con 4 CPU virtuales y 6 GB de memoria.

Cargas de trabajo de prueba	Condición del sitio	Tiempo de registro de VDA	Uso de memoria y CPU de registro	Duración de la prueba de inicio	Uso de CPU y memoria de inicio de sesión	Tasa de inicio
1000 VDI	En línea	5 minutos	Máximo de CPU = 36%, promedio de CPU = 33%, máximo de memoria = 5,3 GB	2 minutos	Máximo de CPU = 29%, promedio de CPU = 27%, máximo de memoria = 3,7 GB	500 por minuto
1000 VDI	Interrupción	4 minutos	Máximo de CPU = 11%, promedio de CPU = 10%, máximo de memoria = 4,5 GB	2 minutos	Máximo de CPU = 42%, promedio de CPU = 28%, máximo de memoria = 4,0 GB	500 por minuto
250 RDS, 5000 sesiones	En línea	3 minutos	Máximo de CPU = 14%, promedio de CPU = 4%, máximo de memoria = 3,5 GB	9 minutos	Máximo de CPU = 46%, promedio de CPU = 21%, máximo de memoria = 3,7 GB	555 por minuto

Cargas de trabajo de prueba	Condición del sitio	Tiempo de registro de VDA	Uso de memoria y CPU de registro	Duración de la prueba de inicio	Uso de CPU y memoria de inicio de sesión	Tasa de inicio
250 RDS, 5000 sesiones	Interrupción	3 minutos	Máximo de CPU = 15%, promedio de CPU = 5%, máximo de memoria = 3,7	9 minutos	Máximo de CPU = 51%, promedio de CPU = 32%, máximo de memoria = 4,2 GB	555 por minuto

Cargas de trabajo grandes

Estas cargas de trabajo se probaron con 4 CPU virtuales y 8 GB de memoria.

Cargas de trabajo de prueba	Condición del sitio	Tiempo de registro de VDA	Uso de memoria y CPU de registro	Duración de la prueba de inicio	Uso de CPU y memoria de inicio de sesión	Tasa de inicio
5000 VDI	En línea	3-4 minutos	Máximo de CPU = 45%, promedio de CPU = 25%, máximo de memoria = 7,0 GB	5 minutos	Máximo de CPU = 75%, promedio de CPU = 55%, máximo de memoria = 7,0 GB	1000 por minuto
5000 VDI	Interrupción	4-6 minutos	Máximo de CPU = 15%, promedio de CPU = 5%, máximo de memoria = 7,5 GB	5 minutos	Máximo de CPU = 45%, promedio de CPU = 40%, máximo de memoria = 7,5 GB	1000 por minuto

Cargas de trabajo de prueba	Condición del sitio	Tiempo de registro de VDA	Uso de memoria y CPU de registro	Duración de la prueba de inicio	Uso de CPU y memoria de inicio de sesión	Tasa de inicio
500 RDS, 10 000 sesiones	En línea	3 minutos	Máximo de CPU = 45%, promedio de CPU = 25%, máximo de memoria = 7,0 GB	10 minutos	Máximo de CPU = 75%, promedio de CPU = 55%, máximo de memoria = 7,0 GB	1000 por minuto
500 RDS, 10 000 sesiones	Interrupción	3 minutos	Máximo de CPU = 15%, promedio de CPU = 5%, máximo de memoria = 7,5	10 minutos	Máximo de CPU = 45%, promedio de CPU = 40%, máximo de memoria = 7,5 GB	1000 por minuto

Cargas de trabajo máximas

Estas cargas de trabajo se probaron con 8 CPU virtuales y 10 GB de memoria.

Cargas de trabajo de prueba	Condición del sitio	Tiempo de registro de VDA	Uso de memoria y CPU de registro	Duración de la prueba de inicio	Uso de CPU y memoria de inicio de sesión	Tasa de inicio
10 000 VDI	En línea	3-4 minutos	Máximo de CPU = 85%, promedio de CPU = 10%, máximo de memoria = 8,5 GB	7 minutos	Máximo de CPU = 66%, promedio de CPU = 28%, máximo de memoria = 7,0 GB	1400 por minuto

Cargas de trabajo de prueba	Condición del sitio	Tiempo de registro de VDA	Uso de memoria y CPU de registro	Duración de la prueba de inicio	Uso de CPU y memoria de inicio de sesión	Tasa de inicio
10 000 VDI	Interrupción	4-5 minutos	Máximo de CPU = 90%, promedio de CPU = 17%, máximo de memoria = 8,2 GB	5 minutos	Máximo de CPU = 90%, promedio de CPU = 45%, máximo de memoria = 8,5 GB	2000 por minuto
1000 RDS, 20 000 sesiones	En línea	1-2 minutos	Máximo de CPU = 60%, promedio de CPU = 20%, máximo de memoria = 8,6 GB	17 minutos	Máximo de CPU = 66%, promedio de CPU = 25%, máximo de memoria = 6,8 GB	1200 por minuto
1000 RDS, 20 000 sesiones	Interrupción	3-4 minutos	Máximo de CPU = 22%, promedio de CPU = 10%, máximo de memoria = 8,5	21 minutos	Máximo de CPU = 90%, promedio de CPU = 50%, máximo de memoria = 7,5 GB	1000 por minuto

> **Nota:**
>
> Las cargas de trabajo que aparecen aquí son las máximas recomendadas para una ubicación de recursos. Para admitir cargas de trabajo más grandes, agregue más ubicaciones de recursos.

Uso de recursos para sincronización de la configuración

El proceso de sincronización de la configuración mantiene los Cloud Connectors actualizados con Citrix DaaS. Las actualizaciones se envían automáticamente a los Cloud Connectors para garantizar que los estos estén preparados para hacerse cargo de la intermediación en caso de que se produzca

una interrupción. La sincronización de la configuración actualiza la base de datos de la caché de host local, SQL Express Server LocalDB. Durante el proceso, los datos se importan a una base de datos temporal y, a continuación, se cambia a esa base de datos una vez importados. Esto garantiza que siempre haya una base de datos de caché de host local lista para tomar el control.

El uso de CPU, memoria y disco aumenta temporalmente mientras los datos se importan a la base de datos temporal.

Resultados de la prueba:

- **Tiempo de importación de datos:** 7-10 minutos
- **Uso de CPU:**
  - máximo = 25%
  - promedio = 15%
- **Uso de memoria:**
  - máximo = 9 GB
  - aumento de aproximadamente 2 GB a 3 GB
- **Uso del disco:**
  - Pico de lectura de disco de 4 MB/s
  - Pico de escritura en disco de 18 MB/s
  - Pico de escritura en disco de 70 MB/s durante la descarga y escritura de los archivos de configuración XML
  - Pico de lectura de disco de 4 MB/s al finalizar la importación
- **Tamaño de base de datos de caché de host local**
  - Archivo de base de datos 400-500 MB
  - Base de datos de registros de 200-300 MB

Condiciones de prueba:

- Prueba en un AMD EPYC con 8 CPU virtuales
- La base de datos de configuración del sitio importada era para un entorno con un total de 80 000 VDA y 300 000 usuarios en todo el sitio (tres turnos de 100 000 usuarios)
- El tiempo de importación de datos se probó en una ubicación de recursos con 10 000 VDI

Consideraciones de uso de recursos adicionales:

- Durante la importación, se descargan todos los datos de configuración del sitio. Esta descarga puede provocar un pico de memoria, según el tamaño del sitio.
- El sitio probado utilizaba aproximadamente 800 MB para la base de datos y los archivos de registros de la base de datos combinados. Durante una sincronización de la configuración, estos archivos se duplican con un tamaño máximo combinado de aproximadamente 1600 MB.

Asegúrese de que su Cloud Connector tenga suficiente espacio en disco para los archivos duplicados. El proceso de sincronización de la configuración falla si el disco está lleno.

Instalar VDA

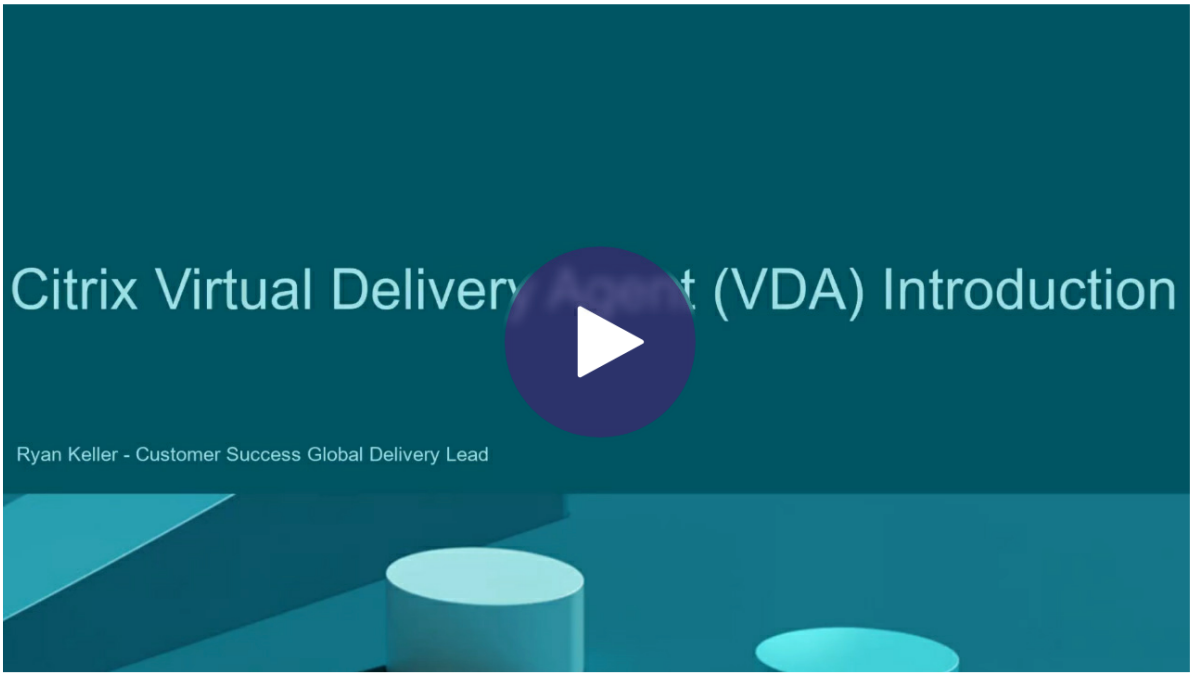
May 17, 2024

Introducción

Este artículo comienza con una descripción de los VDA de Windows y los instaladores de VDA disponibles. El resto del artículo describe los pasos en el asistente de instalación de VDA. Se ofrecen asimismo los equivalentes de línea de comandos. Para obtener información detallada, consulte Instalar los VDA mediante la línea de comandos.

Para obtener información sobre Linux VDA, consulte Linux Virtual Delivery Agent.

Aquí dispone de una introducción a los agentes VDA.



Consideraciones sobre la instalación

El artículo Citrix DaaS describe qué son los VDA y para qué sirven. Aquí hay más información.

- **Recopilación de datos de análisis:** Los datos de análisis se recopilan automáticamente cuando se instalan o actualizan la versión de componentes. De forma predeterminada, los datos se cargan en Citrix automáticamente cuando se completa la instalación. Además, cuando se instalan los componentes, se inscribe automáticamente en el programa Citrix Customer Experience Improvement Program (CEIP), que carga datos anónimos. Igualmente, durante una instalación o la actualización de una versión, se le ofrece la oportunidad de inscribirse en Call Home.

  Si falla la instalación del VDA, un analizador MSI revisa el registro MSI del fallo, y muestra el código de error exacto. El analizador sugiere un artículo CTX si se trata de un problema conocido. El analizador también recopila datos anónimos sobre el código del error. Estos datos se incluyen con otros recopilados por el programa CEIP. Si finaliza la inscripción en CEIP, los datos del analizador MSI recopilados ya no se envían a Citrix.

  Para obtener información acerca de estos programas, consulte Citrix Insight Services.

- **Aplicación Citrix Workspace:** La aplicación Citrix Workspace para Windows no se instala de manera predeterminada cuando instala un VDA. Puede descargar e instalar o actualizar la versión de la aplicación Citrix Workspace para Windows y otras aplicaciones Citrix Workspace desde el sitio web de Citrix. También puede poner esas aplicaciones Citrix Workspace a disposición de los usuarios desde Workspace o el servidor StoreFront.

- **Print Spooler Service:** El servicio Microsoft Print Spooler Service debe estar habilitado. No se puede instalar correctamente un VDA si ese servicio está inhabilitado.

- **Microsoft Media Foundation:** La mayoría de las ediciones Windows admitidas vienen con Microsoft Media Foundation ya instalado. Si la máquina donde quiere instalar el VDA no tiene instalado Microsoft Media Foundation (como las ediciones N), algunas funciones multimedia no se instalan ni funcionan.

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

  Puede aceptar la limitación o finalizar la instalación del VDA y reiniciar la máquina más tarde, después de instalar Media Foundation. En la interfaz gráfica, se presenta esta opción en un mensaje. En la línea de comandos, puede usar la opción `/no_mediafoundation_ack` para aceptar la limitación.

- **Grupo de usuarios locales:** Cuando se instala el VDA, se crea automáticamente un nuevo grupo de usuarios locales llamado Usuarios con acceso directo. Para VDA con SO de sesión única, este grupo solo se aplica a las conexiones RDP. Para VDA con SO multisesión, este grupo se aplica a conexiones ICA y RDP.

- **Dirección requerida para Cloud Connector:** El VDA debe tener al menos una dirección válida de Cloud Connector (en la misma ubicación de recursos) con la que comunicarse. De lo contrario, las sesiones no se pueden establecer. Debe especificar direcciones de Cloud Connector en el momento de instalar el VDA. Para obtener información sobre otros modos de especificar direcciones de Cloud Connector donde puedan registrarse agentes VDA, consulte Registro de VDA.
- **Consideraciones del sistema operativo:**
  - Revise Requisitos del sistema para conocer las versiones, las plataformas y los sistemas operativos compatibles.
  - Compruebe que cada sistema operativo mantiene las actualizaciones más recientes.
  - Compruebe que todos los VDA tengan los relojes del sistema sincronizados. La infraestructura Kerberos que protege la comunicación entre las máquinas requiere sincronización.
  - Dispone de directrices de optimización para máquinas con Windows 10 en CTX216252.
  - Si intenta instalar (o actualizar) un VDA de Windows en un sistema operativo que no admite esta versión del VDA, aparece un mensaje que describe las opciones de que dispone. Por ejemplo, si intenta instalar el VDA más reciente en una máquina con una versión de Windows antigua, un mensaje le llevará a CTX139030. Para obtener más información, consulte Sistemas operativos anteriores.
- **MSI instalados:** Varios MSI se instalan automáticamente al instalar un VDA. Puede evitar la instalación de algunos MSI en la página **Componentes adicionales** de la interfaz gráfica o con la opción `/exclude` de la interfaz de la línea de comandos. Para otros, la única forma de impedir su instalación es con la opción `/exclude` de la interfaz de la línea de comandos.
- **Unida a un dominio:** Compruebe que la máquina esté unida a un dominio antes de instalar el software de VDA.

Herramientas de compatibilidad para VDA

Todos los instaladores de VDA incluyen un MSI de compatibilidad. Este MSI contiene herramientas de Citrix para verificar el rendimiento del VDA (es decir, su estado general y la calidad de las conexiones). Puede habilitar o inhabilitar la instalación de ese MSI desde la página **Componentes adicionales** de la interfaz gráfica del instalador de VDA. Desde la línea de comandos, inhabilite la instalación con la opción `/exclude "Citrix Supportability Tools"`.

De forma predeterminada, el MSI de compatibilidad se instala en `C:\Program Files (x86)\Citrix\Supportability Tools\`. Puede cambiar esta ubicación desde la página **Componentes** de la interfaz gráfica del instalador de VDA o con la opción `/installdir` desde la línea de comandos. Tenga en cuenta que, si cambia esta ubicación, se cambiará la ubicación de todos los componentes de VDA instalados, no solo de las herramientas de compatibilidad.

Herramientas disponibles actualmente en el MSI de compatibilidad:

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

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

Reinicios durante la instalación del VDA

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

Para minimizar los demás reinicios necesarios durante la instalación de VDA:

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

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

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

Después de cada reinicio, la instalación del VDA continúa. Si va a realizar la instalación desde la línea de comandos, puede evitar la reanudación automática con la opción `/noresume`.

Se produce un reinicio durante la actualización de un VDA a la versión 7.17 (o una versión posterior compatible). Este reinicio no se puede evitar.

Restaurar en caso de error al instalar o actualizar

> **Nota:**
>
> Esta funcionalidad solo está disponible para los VDA de sesión única.

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

Cuando se inicia una instalación o actualización de VDA de sesión única con esta funcionalidad habilitada, el instalador crea un punto de restauración del sistema anterior al comienzo del proceso

de instalación o actualización. Si el proceso de instalación o actualización del VDA falla, la máquina vuelve al estado del punto de restauración. La carpeta `%temp%/Citrix` contiene registros de implementación y otra información acerca de la restauración.

De forma predeterminada, esta función está inhabilitada.

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

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

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

  Si la instalación o actualización se completa correctamente, el punto de restauración no se utiliza, pero se conserva.

- Ejecute un instalador de VDA con la opción `/enablerestore` o `/enablerestorecleanup`.

  - Si utiliza la opción `/enablerestorecleanup` y la instalación o actualización se completa correctamente, el punto de restauración se elimina automáticamente.
  - Si utiliza la opción `/enablerestore` y la instalación o actualización se completa correctamente, el punto de restauración no se utiliza, pero se conserva.

Instaladores de VDA

Los programas de instalación de los VDA se pueden descargar directamente desde la consola de Citrix Cloud.

De forma predeterminada, los archivos que contiene el instalador autoextraíble se extraen en la carpeta `Temp`. Los archivos que se extraen en la carpeta `Temp` se eliminan automáticamente una vez completada la instalación. También puede usar el comando `/extract` con una ruta de acceso absoluta.

Dispone de tres instaladores independientes de VDA para la descarga.

VDAServerSetup.exe instala un VDA de SO multisesión.

VDAWorkstationSetup.exe instala un VDA de SO de sesión única.

VDAWorkstationCoreSetup.exe instala un VDA de SO de sesión única, optimizado para implementaciones del acceso con Remote PC o instalaciones básicas de VDI. El acceso con Remote PC usa

máquinas físicas. Las instalaciones básicas de VDI son máquinas virtuales que no se utilizan como imagen. Este instalador solo instala los servicios básicos necesarios para las conexiones de VDA. Por lo tanto, solo permite el uso de un subconjunto de las opciones que son válidas con el instalador VDAWorkstationSetup.

Este instalador para la versión actual no instala ni contiene los componentes utilizados para:

- App-V.
- Profile Management. Excluir Citrix Profile Management de la instalación afecta a las pantallas de Supervisar.
- Machine Identity Service.
- Aplicación Citrix Workspace para Windows
- Citrix Supportability Tools.
- Citrix Files para Windows.
- Citrix Files para Outlook.
- Memoria caché de escritura de E/S de MCS para optimizar el almacenamiento.

Este instalador no instala ni contiene una aplicación Citrix Workspace para Windows.

Este instalador instala automáticamente el MSI de redirección de contenido del explorador. La instalación automática es aplicable a la versión 2003 y versiones posteriores compatibles de VDA.

Utilizar `VDAWorkstationCoreSetup.exe` equivale a usar el instalador `VDAWorkstationSetup.exe` para instalar un VDA de SO de sesión única y una de las siguientes opciones:

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

Si instala un VDA con el instalador `VDAWorkstationCoreSetup.exe` y más tarde actualiza la versión de ese VDA con el instalador `VDAWorkstationSetup.exe`, tiene la opción de instalar las funciones y los componentes omitidos.

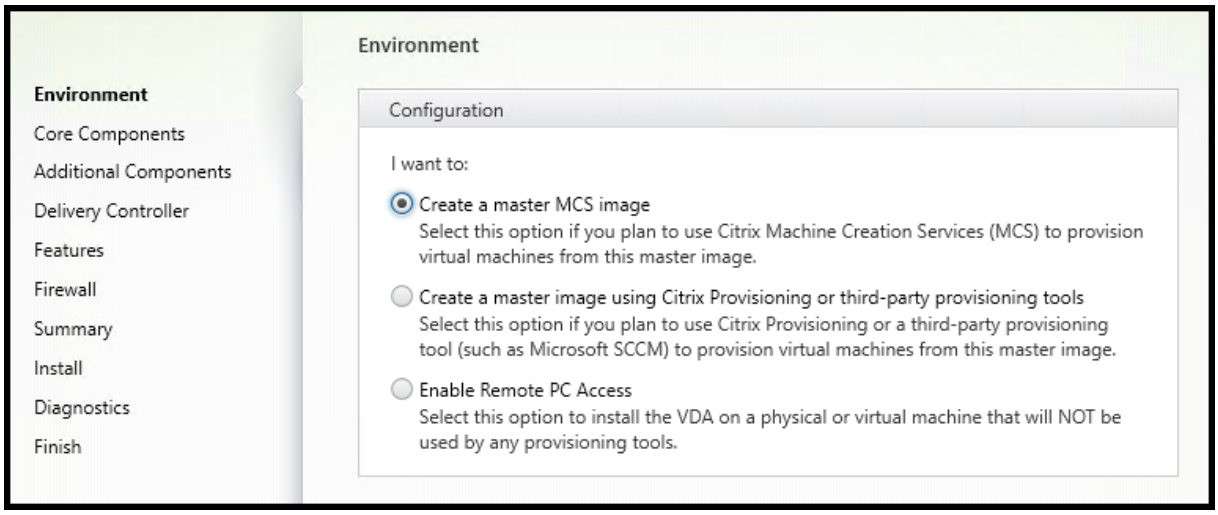
Paso 1. Descargue el software del producto e inicie el asistente

1. En la máquina donde va a instalar el VDA, inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione Citrix DaaS en la lista **Mis servicios**.
3. A la derecha, haga clic en **Descargas** y seleccione **Descargar VDA**. Se le redirigirá a la página de descargas de VDA. Busque el instalador de VDA que quiera utilizar y seleccione **Descargar archivo**.

4. Una vez completada la descarga, haga clic con el botón secundario en el archivo y seleccione **Ejecutar como administrador**. Se iniciará el asistente de instalación.

Como alternativa a los pasos del 1 al 3, puede descargar el VDA directamente desde la página de descargas de Citrix.

Paso 2. Especifique cómo se usará el VDA



En la página **Entorno**, especifique cómo va a usar el VDA e indique si usará esta máquina como imagen para aprovisionar máquinas. La opción que elija afecta a las herramientas de aprovisionamiento de Citrix que se instalan automáticamente (si las hay) y a los valores predeterminados de la página **Componentes adicionales** del instalador de VDA.

Elija una de las siguientes opciones:

- **Crear una imagen maestra de MCS:** Seleccione esta opción para instalar un VDA en la imagen de una VM si va a usar Machine Creation Services para aprovisionar máquinas virtuales. Esta opción instala Machine Identity Service. Esta es la opción predeterminada.

  Opción de la línea de comandos: `/mastermcsimage` o `/masterimage`

- **Crear una imagen maestra con Citrix Provisioning o herramientas de aprovisionamiento de terceros:** Seleccione esta opción para instalar un VDA en la imagen de una VM o si va a usar Citrix Provisioning o herramientas de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager). Utilice esta opción para máquinas virtuales previamente aprovisionadas que se iniciaron desde un disco de lectura/escritura de Citrix Provisioning.

  Opción de línea de comandos: `/masterpvsimage`

- (Aparece solo en las máquinas con SO multisesión) **Habilitar conexiones de broker con servidores:** Seleccione esta opción para instalar un VDA en una máquina física o virtual que no se utilizará como imagen.

Opción de línea de comandos: `/remotepc`

- (Aparece solo en las máquinas con SO multisesión) **Habilitar el acceso con Remote PC:** Seleccione esta opción para instalar un VDA en una máquina física que se usará para acceso con Remote PC.

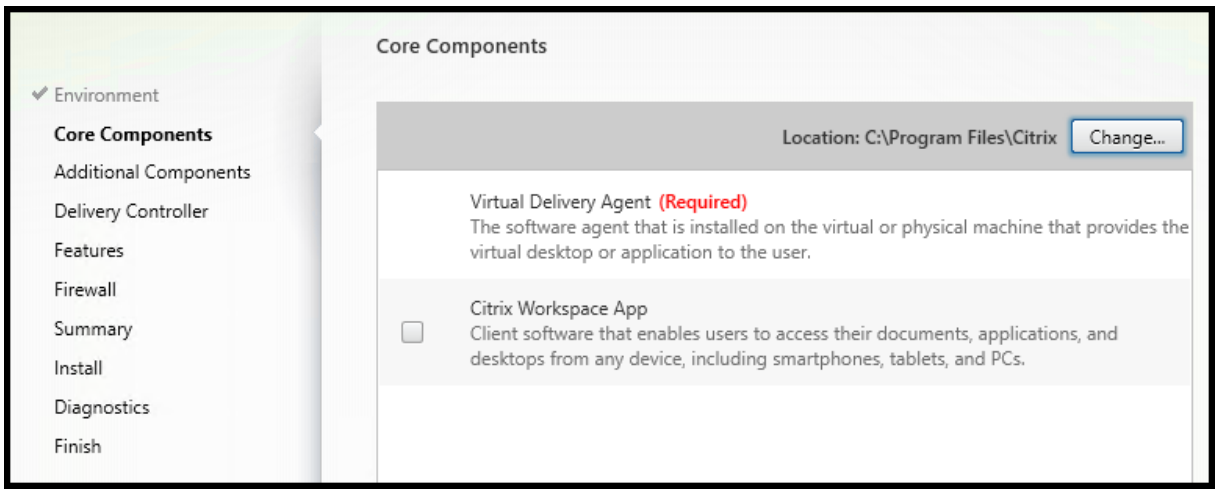
  Opción de línea de comandos: `/remotepc`

Seleccione **Siguiente**.

Esta página no aparecerá:

- Al actualizar la versión de un VDA.
- Al utilizar el instalador `VDAWorkstationCoreSetup.exe`.

Paso 3. Seleccionar los componentes que instalar y la ubicación de la instalación



En la página **Componentes principales**:

- **Ubicación:** De forma predeterminada, los componentes se instalan en `C:\Program Files\Citrix`. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones. Si indica otra ubicación, esta debe tener permisos de ejecución para el servicio de red.

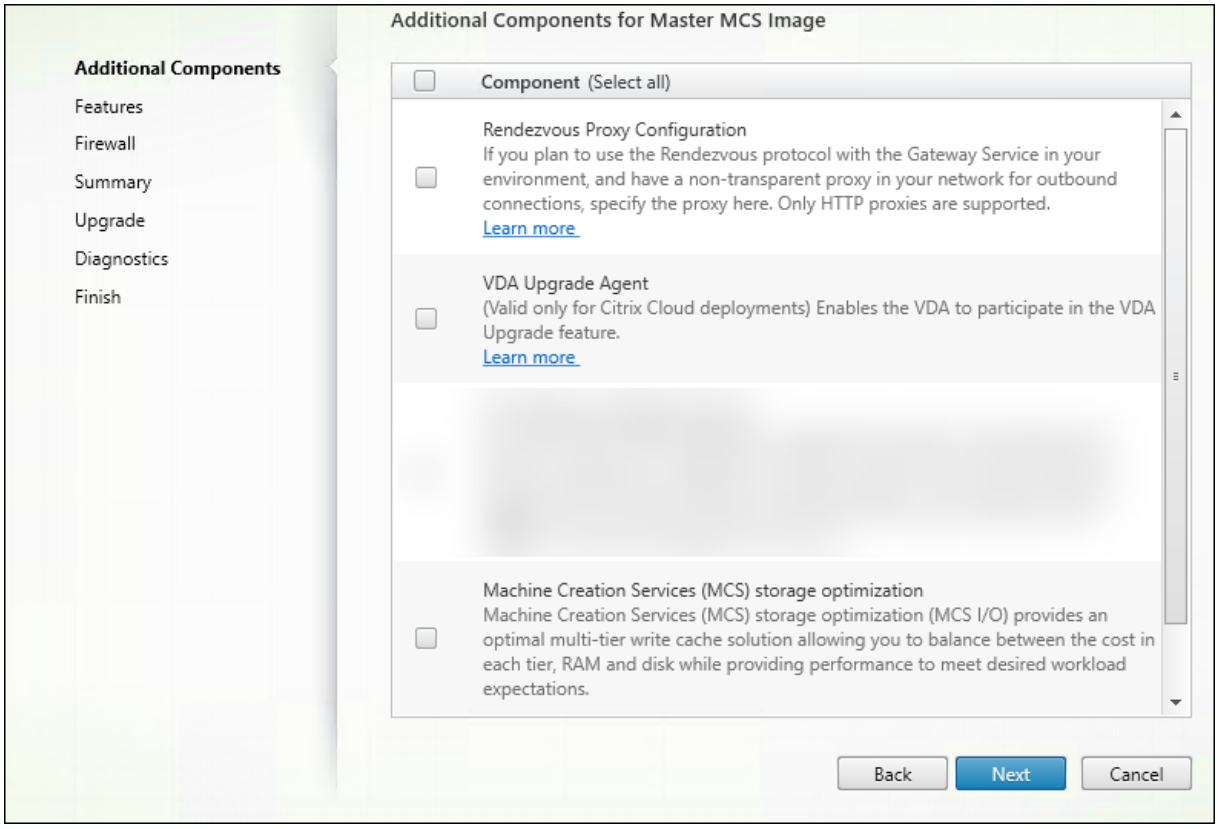
  Opción de línea de comandos: `/installdir`

- **Componentes:** De forma predeterminada, no se instala la aplicación Citrix Workspace para Windows con el VDA. Si utiliza el instalador `VDAWorkstationCoreSetup.exe`, la aplicación Citrix Workspace para Windows no se instala nunca, así que esta casilla no aparece.

  Opción de línea de comandos: `/components vda,plugin` para instalar el VDA y la aplicación Citrix Workspace para Windows

Seleccione **Siguiente**.

Paso 4. Instale componentes adicionales



La página **Componentes adicionales** contiene casillas de verificación para habilitar o inhabilitar la instalación de otras funcionalidades y tecnologías con el VDA. En una instalación de la línea de comandos, puede usar las opciones `/exclude` o `/includeadditional` para omitir o incluir uno o varios de los componentes disponibles.

En la siguiente tabla se indica el parámetro predeterminado de los elementos en esta página. El parámetro predeterminado depende de la opción que seleccione en la página **Entorno**.

Página Componentes adicionales	Página Entorno: "Imagen maestra con MCS"o "Imagen maestra con Citrix Provisioning …"seleccionado	Página Entorno: "Habilitar conexiones de broker con servidores"(para SO multisesión) o "Acceso con Remote PC"(para SO de sesión única) seleccionado
Citrix Personalization for App-V	No seleccionado	No seleccionado
Capa de personalización de usuarios	No seleccionado	No se muestra porque no es válido para este caso de uso.
Citrix Supportability Tools	Seleccionado	No seleccionado

Página Componentes adicionales	Página Entorno: “Imagen maestra con MCS”o “Imagen maestra con Citrix Provisioning …”seleccionado	Página Entorno: “Habilitar conexiones de broker con servidores”(para SO multisesión) o “Acceso con Remote PC”(para SO de sesión única) seleccionado
Citrix Profile Management	Seleccionado	No seleccionado
Citrix Profile Management WMI Plug-in	Seleccionado	No seleccionado
Citrix VDA Upgrade Agent	No seleccionado	No seleccionado
Copia de seguridad y restauración de Citrix	No seleccionado	No seleccionado
Citrix Files para Windows	No seleccionado	No seleccionado
Citrix Files para Outlook	No seleccionado	No seleccionado
Optimización del almacenamiento de Machine Creation Services (MCS)	No seleccionado	No seleccionado
Configuración del protocolo Rendezvous	No seleccionado	No seleccionado

Esta página no aparecerá:

- Al usar el instalador `VDAWorkstationCoreSetup.exe`. Además, las opciones de la línea de comandos para los componentes adicionales no son válidas cuando se utilizan junto con ese instalador.
- Al actualizar la versión de un VDA y todos los componentes adicionales ya están instalados. Si alguno de los componentes adicionales ya está instalado, la página muestra solo aquellos que no están instalados.

La lista de componentes puede incluir:

- **Personalización de Citrix para App-V:** Instale este componente si va a usar aplicaciones provenientes de paquetes de Microsoft App-V. Para obtener más información, consulte App-V.

  Opción de línea de comandos: `/includeadditional "Citrix Personalization for App-V – VDA"` para habilitar la instalación del componente, `/exclude "Citrix Personalization for App-V – VDA"` para impedir la instalación del componente

- **Capa de personalización de usuarios de Citrix:** Instala el MSI para la capa de personalización de usuarios. Para obtener más información, consulte Capa de personalización de usuarios.

Este componente aparece solo cuando se instala un VDA en una máquina Windows 10 de sesión única.

Opción de línea de comandos: `/includeadditional "User Personalization Layer"` para habilitar la instalación del componente, `/exclude "User Personalization Layer"` para impedir la instalación del componente

- **Citrix Supportability Tools:** Instala el MSI que contiene las herramientas de compatibilidad de Citrix.

  Opción de línea de comandos: `/includeadditional "Citrix Supportability Tools"` para habilitar la instalación del componente, `/exclude "Citrix Supportability Tools"` para impedir la instalación del componente

- **Citrix Profile Management:** Este componente administra los parámetros de personalización de usuario en los perfiles de usuario. Para obtener más detalles, consulte Profile Management.

  Excluir Citrix Profile Management de la instalación afecta a la supervisión y la solución de problemas de los agentes VDA en Citrix Cloud.

  - En las páginas **Detalles del usuario** y **Punto final** de la ficha **Supervisar**, el panel **Personalización** y el panel **Duración de inicio de sesión** fallan.
  - En las páginas **Panel de mandos** y **Tendencias**, el panel **Duración media de inicios de sesión** solo mostrará datos para máquinas que tengan Profile Management instalado.

  Aunque use una solución de terceros para la administración de perfiles de usuario, Citrix recomienda instalar y ejecutar el servicio Citrix Profile Management. No es necesario habilitar el servicio Citrix Profile Management.

  Opción de línea de comandos: `/includeadditional "Citrix Profile Management "` para habilitar la instalación del componente, `/exclude "Citrix Profile Management"` para impedir la instalación del componente

- **Plug-in WMI de Citrix Profile Management:** Este plug-in ofrece información del tiempo de ejecución de Profile Management en objetos WMI (Windows Management Instrumentation); por ejemplo, el proveedor del perfil, el tipo de perfil, el tamaño y el uso del disco. Los objetos WMI proporcionan información acerca de las sesiones a Citrix Director.

  Opción de línea de comandos: `/includeadditional "Citrix Profile Management WMI Plugin"` para habilitar la instalación del componente, `/exclude "Citrix Profile Management WMI Plugin"` para impedir la instalación del componente

- **Agente de actualización de VDA** (aplicable solamente a implementaciones de Citrix DaaS): Permite que los VDA participen en la función de actualización de VDA. Puede utilizar esta función para actualizar la versión de los VDA de un catálogo desde la consola de administración de forma inmediata o a una hora programada. Si este agente no está instalado, puede actualizar un VDA mediante el instalador de VDA en la máquina.

Opciones de línea de comandos: `/includeadditional "Citrix VDA Upgrade Agent"` para habilitar la instalación del componente, `/exclude "Citrix VDA Upgrade Agent"` para impedir la instalación del componente

- **Citrix Files para Windows:** Este componente permite a los usuarios conectarse a su cuenta de Citrix Files. Una vez conectados, pueden interactuar con Citrix Files a través de una unidad asignada en el sistema de archivos de Windows sin requerir una sincronización completa de su contenido.

  Opciones de línea de comandos: `/includeadditional "Citrix Files for Windows"` para habilitar la instalación del componente, `/exclude "Citrix Files for Windows"` para impedir la instalación del componente

- **Citrix Files para Outlook:** El componente le permite hacer envíos a través de Citrix Files para omitir las restricciones de tamaño de archivo y agregar seguridad a sus archivos adjuntos o correos electrónicos. Puede proporcionar una solicitud de carga de archivos segura directamente en su correo electrónico. Para obtener más información, consulte Citrix Files para Outlook.

  Opciones de línea de comandos: `/includeadditional "Citrix Files for Outlook"` para habilitar la instalación del componente, `/exclude "Citrix Files for Outlook"` para impedir la instalación del componente

- **Optimización del almacenamiento de Machine Creation Services (MCS):** Instala el controlador E/S de Citrix MCS. Para obtener más información, consulte Almacenamiento compartido por los hipervisores y Configurar caché para datos temporales.

  Opciones de línea de comandos: `/includeadditional "Citrix MCS IODriver"` para habilitar la instalación del componente, `/exclude "Citrix MCS IODriver"` para impedir la instalación del componente

- **Configuración del proxy:** Instale este componente si piensa utilizar el protocolo Rendezvous con Citrix Gateway Service en su entorno y tiene un proxy no transparente en la red para las conexiones salientes. Solo se admiten proxies HTTP.

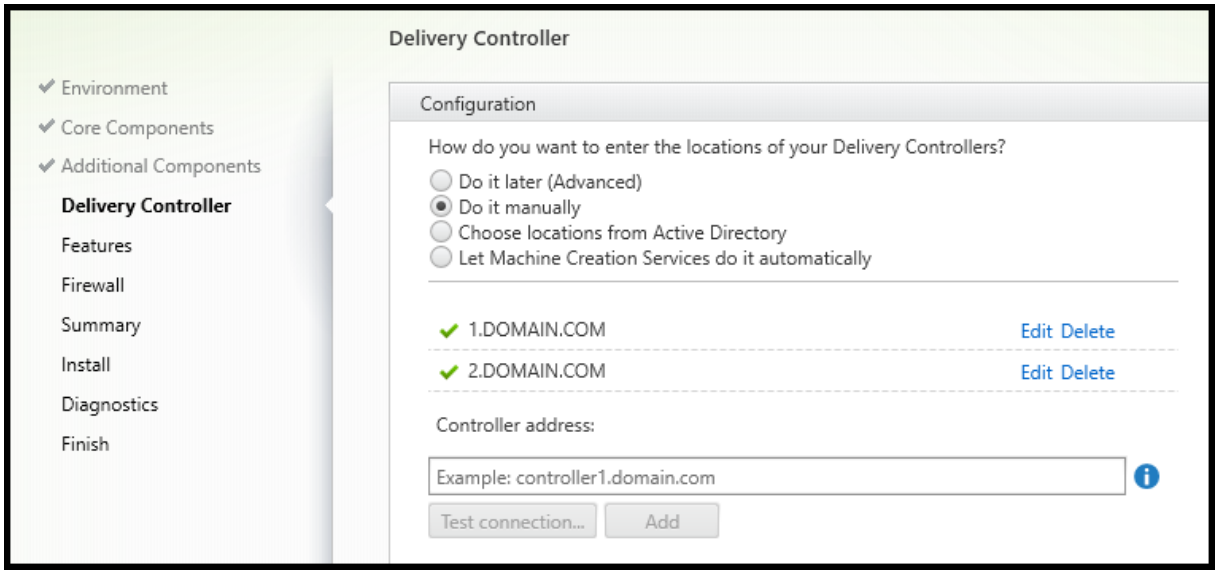
  Si instala este componente, especifique la dirección del proxy o la ruta del archivo PAC en la página **Configuración del proxy de Rendezvous**. Para obtener más información sobre la funcionalidad, consulte Protocolo Rendezvous.

  Opción de línea de comandos: `/includeadditional "Citrix Rendezvous V2"` para habilitar la instalación del componente, `/exclude "Citrix Rendezvous V2"` para impedir la instalación del componente

- **Copia de seguridad y restauración de Citrix:** Si se produce un error al instalar o actualizar la versión de un VDA, este componente puede devolver la máquina a una copia de seguridad que se realizó antes de la instalación o la actualización.

Opción de línea de comandos: `/includeadditional "Citrix Backup and Restore"` para habilitar la instalación del componente, `/exclude "Citrix Backup and Restore"` para impedir la instalación del componente.

Paso 5. Direcciones de Cloud Connector



En la página **Delivery Controller**, seleccione **Hacerlo manualmente**. Introduzca el nombre DNS de un Cloud Connector instalado y luego seleccione **Agregar**. Si ha instalado Cloud Connectors adicionales en la ubicación de recursos, agregue sus nombres DNS.

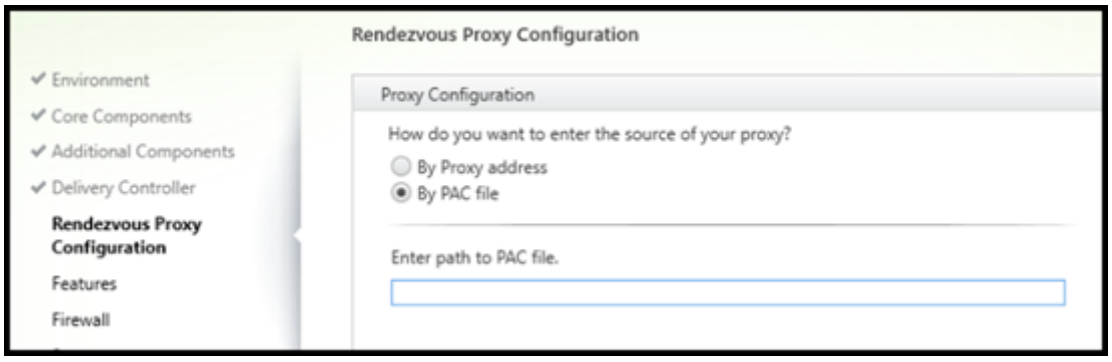
Seleccione **Siguiente**.

Consideraciones:

- La dirección solo puede contener caracteres alfanuméricos.
- Un registro correcto de VDA también requiere que los puertos del firewall que se utilizan para la comunicación con el Cloud Connector estén abiertos. Se habilitan de forma predeterminada en la página **Firewall** del asistente.

Opción de línea de comandos: `/controllers`

Paso 6. Configuración de proxy



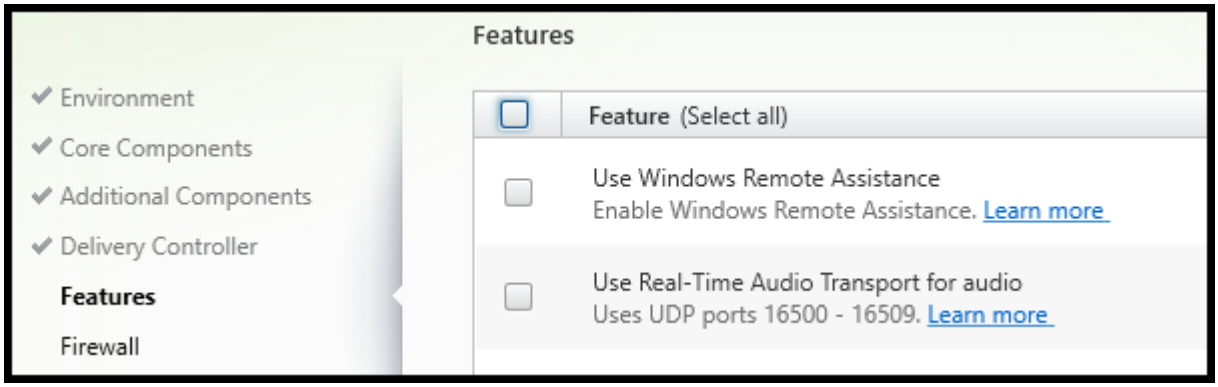
La página **Configuración del proxy de Rendezvous** aparece solo si ha habilitado la casilla de verificación **Configuración del proxy de Rendezvous** en la página **Componentes adicionales**.

1. Seleccione si va a especificar el origen de proxy por dirección de proxy o por ruta de archivo PAC.
2. Especifique la dirección del proxy o la ruta del archivo PAC.
   - Formato de dirección de proxy: `http://<url-or-ip>:<port>`
   - Formato de archivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

El firewall del puerto de proxy debe estar abierto para que la prueba de conexión se haga correctamente. Si no se puede establecer una conexión con el proxy, puede elegir si quiere continuar con la instalación del VDA.

Opción de línea de comandos: `/proxyconfig`

Paso 7. Habilite o inhabilite las funciones



En la página **Funciones**, marque o desmarque las casillas de verificación para habilitar o inhabilitar respectivamente las funcionalidades que quiera utilizar.

- **Usar Asistencia remota de Windows:** Si esta opción está habilitada, la Asistencia remota de Windows se usa con la función de remedo de usuarios del componente Director en Citrix Cloud. La Asistencia remota de Windows abre los puertos dinámicos en el firewall. Opción inhabilitada de forma predeterminada.

  Opción de línea de comandos: `/enable_remote_assistance`

- **Usar transporte de audio Real-Time:** Habilite esta función si en su red se utiliza ampliamente voz sobre IP. Esta función reduce la latencia y mejora la resistencia del audio en redes con pérdida. Lo que permite que los datos de audio se transmitan mediante RTP sobre UDP. Opción inhabilitada de forma predeterminada.

  Opción de línea de comandos: `/enable_real_time_transport`

- **Usar la pantalla compartida:** Cuando está habilitada, los puertos usados para compartir pantalla se abren en el firewall de Windows. Opción inhabilitada de forma predeterminada.

  Opción de línea de comandos: `/enable_ss_ports`

- **¿El VDA está instalado en una máquina virtual en una nube?** Este parámetro ayuda a Citrix a identificar correctamente ubicaciones de recursos para implementaciones de VDA locales y de servicio (Citrix Cloud) con el fin de obtener telemetría. Esta función no afecta a la utilización por parte del cliente. Habilite este parámetro si la implementación usa Citrix DaaS. Opción inhabilitada de forma predeterminada.

  Opción de línea de comandos: `/xendesktopcloud`

Seleccione **Siguiente**.

Si esta página contiene una funcionalidad denominada **E/S de MCS**, no la utilice. La funcionalidad E/S de MCS se configura en la página **Componentes adicionales**.

Paso 8. Puertos de firewall

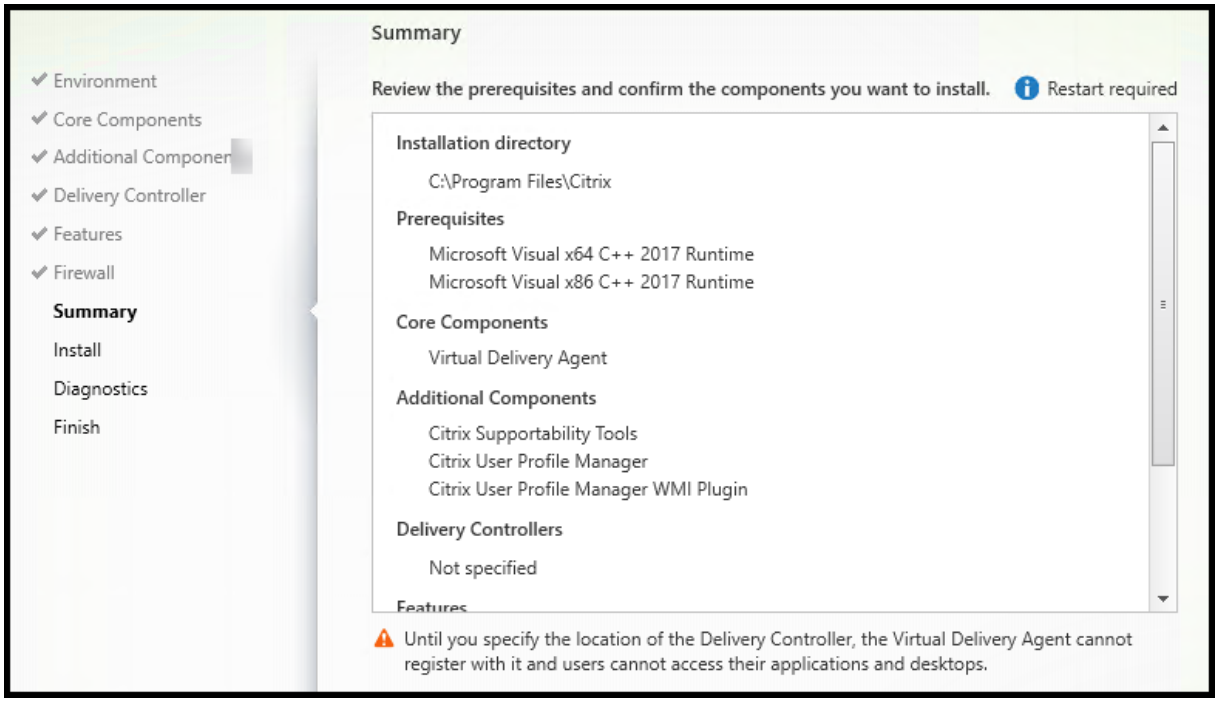
La página **Firewall** indica los puertos que utiliza el VDA y los Cloud Connectors para comunicarse entre sí. De forma predeterminada, estos puertos se abren automáticamente si el servicio Firewall de Windows se está ejecutando, incluso aunque el firewall no esté habilitado. Esta opción predeterminada no presenta problemas para la mayoría de las implementaciones.

Para obtener información acerca de los puertos, consulte Puertos de red.

Seleccione **Siguiente**.

Opción de línea de comandos: `/enable_hdx_ports`

Paso 9. Revise los requisitos previos y confirme la instalación

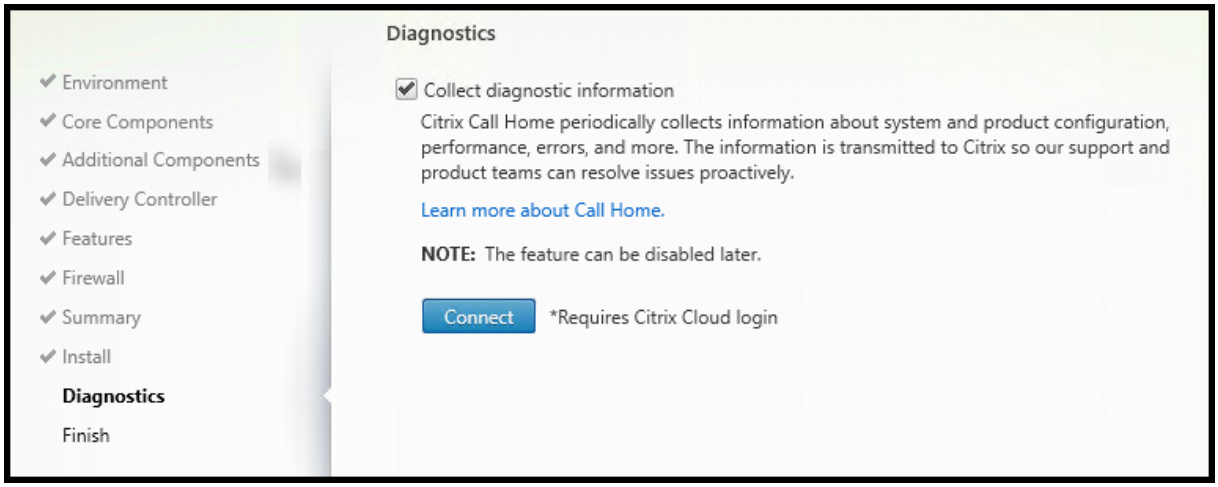


La página **Resumen** muestra lo que se instalará. Si lo necesita, puede volver a las páginas anteriores del asistente y cambiar las opciones.

(Solo VDA de sesión única) Active la casilla de verificación para **habilitar la restauración automática si falla la actualización falla** por si se produjera un error. Para obtener información más detallada, consulte Restaurar en caso de error al instalar o actualizar.

Cuando tenga todo listo, seleccione **Instalar**.

Paso 10. Diagnosticar

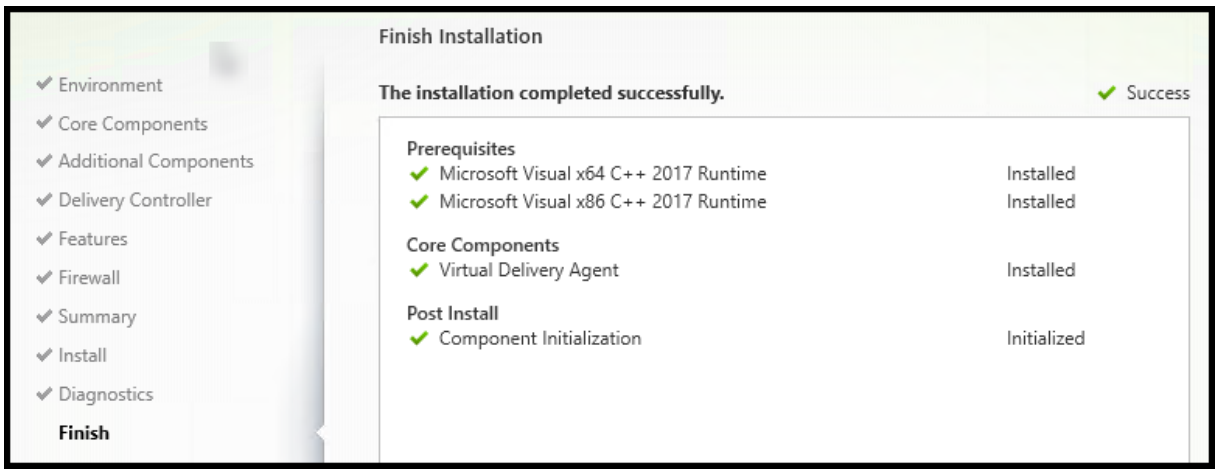


En la página **Diagnósticos**, elija si quiere participar en Citrix Call Home. Si elige participar (opción predeterminada), seleccione **Conectar**. Cuando se le solicite, introduzca las credenciales de su cuenta de Citrix

Una vez validadas las credenciales (o si elige no participar), seleccione **Siguiente**.

Para obtener más información, consulte Call Home.

Paso 11. Finalice la instalación



La página **Finalizar** presenta marcas de verificación verdes para todos los requisitos previos y los componentes que se hayan instalado e inicializado correctamente.

Seleccione **Finish**. De forma predeterminada, la máquina se reinicia automáticamente. Aunque puede inhabilitar este reinicio automático, el VDA no se podrá utilizar hasta que se reinicie la máquina.

Si va a instalar un VDA en máquinas individuales (en lugar de una imagen), repita según sea necesario los pasos anteriores para instalar un VDA en otras máquinas.

Solucionar problemas técnicos

En la pantalla **Administrar > Configuración completa**, la **versión instalada de VDA** en el panel de detalles referente al grupo de entrega puede no ser la versión real instalada en las máquinas. La pantalla Programas y funciones de la máquina Windows muestra la versión real del VDA.

Citrix Optimizer

Citrix Optimizer es una herramienta para el sistema operativo Windows que ayuda a los administradores de Citrix a eliminar y mejorar varios componentes para optimizar los VDA.

Una vez instalado un VDA y completado el reinicio final, descargue e instale Citrix Optimizer. Consulte CTX224676. El artículo de CTX contiene el paquete de descarga e instrucciones sobre la instalación y el uso de Citrix Optimizer.

Personalizar un VDA

Más tarde, para personalizar (cambiar la información de) un VDA instalado:

1. Desde la función de Windows para quitar o cambiar programas, seleccione **Citrix Virtual Delivery Agent** o **Citrix Remote PC Access/VDI Core Services VDA**. A continuación, haga clic con el botón secundario y seleccione **Cambiar**.
2. Seleccione **Personalizar configuración de Virtual Delivery Agent**.

Cuando se inicie el instalador, cambie los parámetros disponibles.

Personalizar el puerto para la comunicación con los Cloud Connectors

En función de sus requisitos de seguridad específicos, puede personalizar el puerto que los VDA utilizan para comunicar con los Cloud Connectors. Esta función es útil si el equipo de seguridad no permite dejar abierto el puerto predeterminado (puerto 80) o si el puerto predeterminado ya está en uso.

Para personalizar el puerto, siga estos pasos:

1. Agregue el número de puerto de Controller en los Citrix Cloud Connectors.
2. Agregue el número de puerto de VDA a los VDA.

Agregar el número de puerto de Controller en los Citrix Cloud Connectors

Vaya a Citrix Cloud Connector y ejecute los dos comandos de PowerShell siguientes:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort <port number>`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort <port number> -ConfigureFirewall`

Ejemplo:

- `PS C:\> & 'C:\Program Files\Citrix\XaXdCloudProxy\XaXdCloudProxy.exe'-VdaPort 18000`
- `PS C:\> & 'C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe'-VdaPort 18000 -ConfigureFirewall`

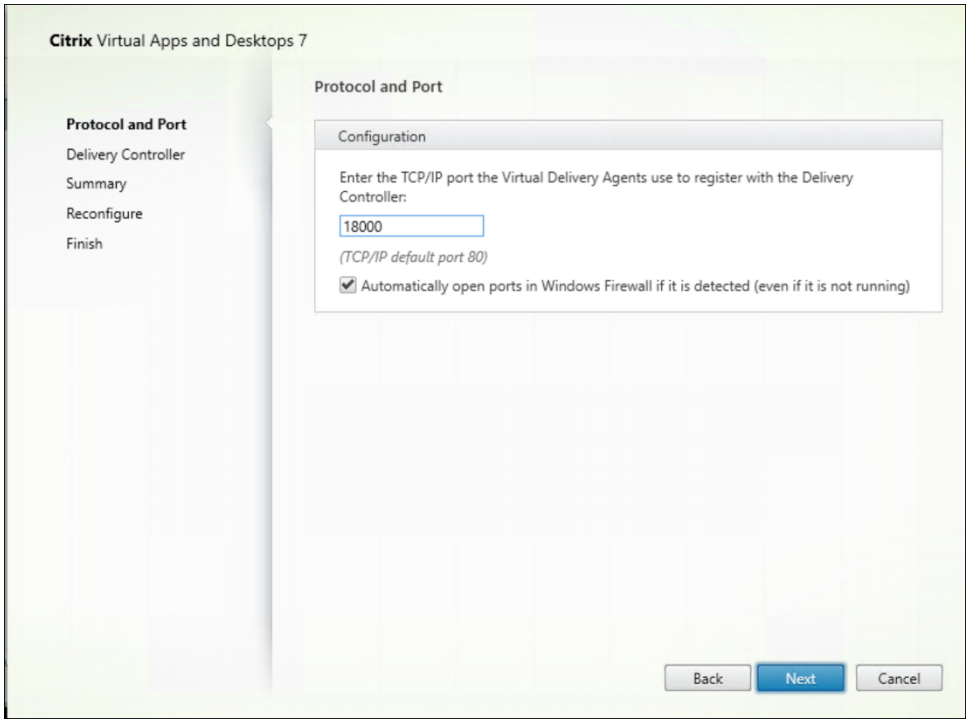
Al personalizar el puerto, tenga en cuenta lo siguiente:

- Debe usar el mismo número de puerto en ambos comandos.
- Debe ejecutar ambos comandos *en todos los Cloud Connectors*.
- Para comunicar correctamente con los Cloud Connectors, asegúrese de que todos los VDA usan el mismo número de puerto.
- El puerto que configure persiste en las actualizaciones del conector.

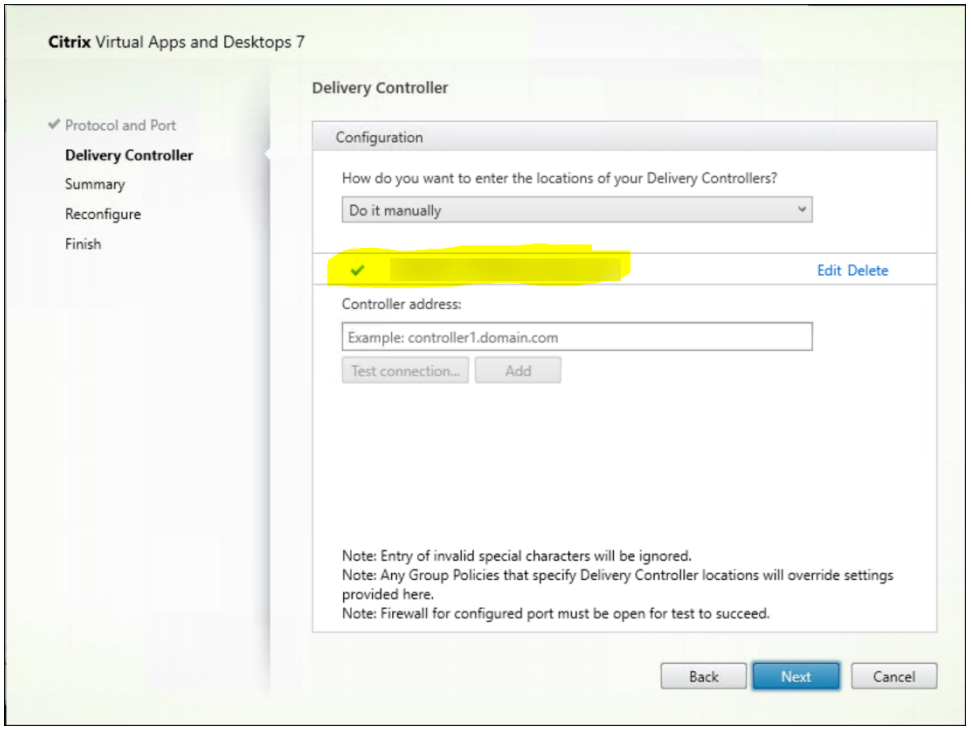
Agregar el número de puerto de VDA a los VDA

Instale el VDA con los valores predeterminados y configure del siguiente modo. Si el VDA ya está instalado, continúe con los pasos que se indican a continuación.

1. En el VDA, abra **XenDesktopVdaSetup.exe**, que se encuentra en `C:\Program Files\Citrix\XenDesktopVdaSetup\XenDesktopVdaSetup.exe`.
2. En la página **Protocolo y puerto**, agregue el número de puerto personalizado.



3. En la página **Delivery Controller**, introduzca el FQDN del Controller.



4. Haga clic en **Siguiente** para continuar con el asistente y completar la configuración.

Los números de puerto se reconfiguran correctamente.

> **Nota:**
>
> Es posible que aparezca el siguiente mensaje de error al probar una conexión de Controller: No se encontró ninguna instancia de Controller en ejecución en < la dirección de Controller introducida >. Si la dirección es correcta, puedes descartar el mensaje.

Solución de problemas

Para comprobar si los puertos personalizados están configurados correctamente, vaya a Cloud Connector y siga estos pasos de solución de problemas:

1. Compruebe que existen las dos claves de Registro siguientes.

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Nombre: CustomVDAPortNumber
   Tipo: REG_DWORD
   Datos: 18000

   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XaXdCloudProxyPersist
   Nombre: CustomVDAPortNumberHA
   Tipo: REG_DWORD
   Datos: 18000

2. Ejecute el siguiente comando para crear un archivo TXT.

   - `netsh http show urlacl > <filepath>.txt`

   Ejemplo:

   - `netsh http show urlacl > c:\reservations.txt`

3. Abra el archivo TXT y compruebe las cuatro URL siguientes para verificar que se utiliza el puerto correcto.

   - `http://+:18000/Citrix/CdsController/IRegistrar/`
   - `http://+:18000/Citrix/CdsController/ITicketing/`
   - `http://+:18000/Citrix/CdsController/IDynamicDataSink/`
   - `http://+:18000/Citrix/CdsController/INotifyBroker/`

4. Compruebe que se hayan creado las dos reglas de firewall siguientes y que los puertos necesarios estén abiertos.

   - Citrix XaXdProxy
   - Citrix Broker Service (TCP-In)

Otra información

- Después de instalar un VDA, puede comprobar el estado y la disponibilidad del sitio y sus componentes con una comprobación de estado de Cloud.

Qué hacer a continuación

Cree catálogos de máquinas.

Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.

Instalar los VDA mediante la línea de comandos

June 19, 2023

Introducción

Este artículo se aplica en caso de instalar, actualizar y personalizar los agentes de Virtual Delivery Agent (VDA) en máquinas con sistemas operativos Windows.

En este artículo, se describe cómo emitir comandos de instalación del VDA. Antes de comenzar una instalación, revise la sección Instalar los VDA para conocer aspectos a tener en cuenta durante la instalación, cuáles son los programas de instalación, y qué información debe especificarse durante el proceso.

Instalar un VDA desde la línea de comandos

Para instalar un VDA (y ver el progreso de ejecución del comando y los valores de retorno), debe tener permisos administrativos elevados, o bien, debe usar la opción **Ejecutar como administrador**.

1. En la máquina donde va a instalar el VDA, inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
3. En la parte superior derecha, haga clic en **Descargas** y seleccione **Descargar VDA**. Se le redirigirá a la página de descargas de VDA. Busque el instalador de VDA que quiera utilizar y haga clic en **Descargar archivo**.
4. Una vez completada la descarga, ejecútelo. Use las opciones descritas en este artículo.
    - Para el componente Virtual Delivery Agent para SO multisesión, ejecute `VDAServerSetup.exe`
    - Para el componente Virtual Delivery Agent para SO de sesión única, ejecute `VDAWorkstationSetup.exe`
    - Para el componente de servicios principales de Virtual Delivery Agent para SO de sesión única, ejecute `VDAWorkstationCoreSetup.exe`.

Para extraer los archivos antes de la instalación, use la opción `/extract` con la ruta de acceso absoluta, por ejemplo: `.\VDAWorkstationCoreSetup.exe /extract %temp%\CitrixVDAInstallMedia` (el directorio debe existir; de lo contrario, la extracción falla). A continuación, en un comando aparte, ejecute el comando correspondiente con las opciones válidas que se indican en este artículo.

- Para `VDAServerSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`
- Para `VDAWorkstationCoreSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopRemotePCSetup.exe`
- Para `VDAWorkstationSetup_XXXX.exe`, ejecute `<extract folder>\Extract\Image-Full\x64\XenDesktop Setup\XenDesktopVDASetup.exe`

Opciones de línea de comandos para instalar un VDA

Las siguientes opciones son válidas con uno o más de los comandos: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe`, y `VDAWorkstationCoreSetup.exe`.

- **/components** *componente*[,*componente*]

  Lista de los componentes, separados por comas, para instalar o quitar. Los valores válidos son:

  - **VDA:** Virtual Delivery Agent
  - **PLUGINS:** Aplicación Citrix Workspace para Windows

  Para instalar el VDA y la aplicación Citrix Workspace, especifique `/components vda,plugins`.

  Si se omite la opción `plugins`, solo se instala el VDA (la aplicación Citrix Workspace no).

  Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. Ese instalador no puede instalar la aplicación Citrix Workspace.

- **/controllers** "*controller* [*controller*]…"

  Lista de nombres de dominio completos (FQDN) de Citrix Cloud Connectors, escritos entre comillas rectas, con los que se puede comunicar el VDA. No especifique ambas opciones, `/site_guid` y `/controllers`.

- **/disableexperiencemetrics**

  Impide que los análisis recopilados durante la instalación, la actualización o la eliminación se carguen automáticamente en Citrix.

- **/enable_hdx_ports**

  Abre los puertos del Firewall de Windows requeridos por el VDA y por las funciones especificadas (excepto la Asistencia remota de Windows) si se detecta el servicio del Firewall de Windows, incluso aunque el firewall no esté habilitado. Si se utiliza un firewall distinto o no se utiliza ninguno, es necesario configurar el firewall manualmente. Para obtener información acerca de los puertos, consulte Puertos de red.

  Para abrir los puertos UDP que usa el transporte adaptable HDX, especifique la opción `/enable_hdx_udp_ports`, además de la opción `/enable_hdx_ports`.

- **/enable_hdx_udp_ports**

  Abre los puertos UDP en el firewall de Windows que requiere el transporte adaptable HDX, si se detecta el servicio Firewall de Windows (incluso aunque el firewall no esté habilitado). Si se utiliza un firewall distinto o no se utiliza ninguno, es necesario configurar el firewall manualmente. Para obtener información acerca de los puertos, consulte Puertos de red.

Para abrir los puertos que utiliza el VDA, especifique la opción `/enable_hdx_ports`, además de la opción `/enable_hdx_udp_ports`.

- **/enable_real_time_transport**

  Habilita o inhabilita el uso de UDP para los paquetes de audio (Transferencia de audio RealTime para audio). Habilitar esta función puede mejorar el rendimiento del audio. Incluya la opción `/enable_hdx_ports` si quiere que los puertos UDP se abran automáticamente si se detecta el servicio de Firewall de Windows.

- **/enable_remote_assistance**

  Habilita la función de remedo en la Asistencia remota de Windows para utilizarla con las funciones de **Supervisar**. Si especifica esta opción, la Asistencia remota de Windows abrirá los puertos dinámicos en el firewall.

- **/enablerestore** o **/enablerestorecleanup**

  (Válido solo para VDA de sesión única) Habilita el retorno automático al punto de restauración si falla la instalación o actualización del VDA.

  Si la instalación/actualización se completa correctamente:

  - `/enablerestorecleanup` indica al instalador que quite el punto de restauración.
  - `/enablerestore` indica al instalador que conserve el punto de restauración, aunque no se haya utilizado.

  Para obtener información más detallada, consulte Restaurar en caso de error al instalar o actualizar.

- **/enable_ss_ports**

  Abre los puertos del firewall de Windows que se requieren para compartir la pantalla, si se detecta el servicio Firewall de Windows, incluso si el firewall no está habilitado. Si se utiliza un firewall distinto o no se utiliza ninguno, es necesario configurar el firewall manualmente.

- **/exclude** "*componente*"[,"*componente*"]

  Impide la instalación de uno o varios componentes opcionales, separados por comas y escritos entre comillas rectas. Por ejemplo, para instalar o actualizar un VDA en una imagen que se administra mediante Machine Creation Services, se necesita el componente Machine Identity Service. Los valores válidos son:

  - Machine Identity Service
  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools

  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2

  Excluir Citrix Profile Management de la instalación (`/exclude "Citrix Profile Management"`) afecta a la supervisión y la solución de problemas de los agentes VDA en la ficha **Supervisar**. En las páginas **Detalles del usuario** y **Punto final**, el panel "Personalización" y el panel "Duración de inicio de sesión"fallan. En las páginas **Panel de mandos** y **Tendencias**, el panel Duración media de inicios de sesión solo mostrará datos para máquinas que tengan Profile Management instalado.

  Aunque use una solución de terceros para la administración de perfiles, Citrix recomienda instalar y ejecutar el servicio Citrix Profile Management. No es necesario habilitar el servicio Citrix Profile Management.

  Si va a usar MCS para aprovisionar máquinas virtuales, no excluya Machine Identity Service.

  Si especifica `/exclude` e `/includeadditional` con el mismo nombre de componente adicional, ese componente no se instala.

  Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. El instalador excluye automáticamente muchos de los elementos.

- **/h** o **/help**

  Muestra la ayuda del comando.

- **/includeadditional** "*componente*"[,"*componente*"] …

  Incluye la instalación de uno o varios componentes opcionales, separados por comas y escritos entre comillas. Los nombres de los componentes distinguen entre mayúsculas y minúsculas.

  Esta opción puede ser útil cuando está creando una implementación de acceso con Remote PC y quiere instalar componentes que no están incluidos de manera predeterminada. Los valores válidos son:

  - Citrix Profile Management
  - Citrix Profile Management WMI Plug-in
  - Citrix Personalization for App-V - VDA
  - Citrix Supportability Tools
  - Citrix MCS IODriver
  - Citrix VDA Upgrade Agent
  - Citrix Rendezvous V2
  - Capa de personalización de usuarios
  - Citrix Web Socket VDA Registration Tool

Si especifica /exclude e /includeadditional con el mismo nombre de componente, ese componente no se instala.

- **/installdir** *directorio*

  Directorio vacío existente donde se instalarán los componentes. Valor predeterminado = C:\Archivos de programa\Citrix.

- **/install_mcsio_driver**

  No usar. En su lugar, use /includeadditional "Citrix MCS IODriver" o /exclude "Citrix MCS IODriver"

- **/logpath** *path*

  Ubicación del archivo de registro. La carpeta especificada debe existir. El instalador no puede crearla. Predeterminado = "%TEMP%\Citrix\XenDesktop Installer"

  Esta opción no está disponible en la interfaz gráfica.

- **/masterimage**

  Válido solamente cuando se instala un VDA en una VM. Establece el VDA como imagen. Esta opción equivale a /mastermcsimage.

  Esta opción no es válida cuando se utiliza el instalador VDAWorkstationCoreSetup.exe.

- **/mastermcsimage**

  Especifica que esta máquina se utilizará como imagen con Machine Creation Services. Esta opción equivale a /masterimage.

- **/masterpvsimage**

  Especifica que esta máquina se utilizará como imagen con Citrix Provisioning o una herramienta de aprovisionamiento de terceros (como Microsoft System Center Configuration Manager).

- **/no_mediafoundation_ack**

  Comprueba que Microsoft Media Foundation no está instalado, y algunas funciones multimedia de HDX no se instalan ni funcionan. Si se omite esta opción y Media Foundation no está instalado, falla la instalación de VDA. La mayoría de las ediciones Windows admitidas vienen con Media Foundation ya instalado, a excepción de las ediciones N.

- **/nodesktopexperience**

  Válido solo cuando se instala un VDA para SO multisesión. Impide la habilitación de la función Enhanced Desktop Experience. Esta función también se controla con la configuración de directiva de Citrix Enhanced Desktop Experience.

- **/noreboot**

Impide que se reinicie el sistema después de la instalación. El VDA no se puede usar hasta después de reiniciarse.

- **/noresume**

  De forma predeterminada, cuando se necesita reiniciar la máquina durante una instalación, el instalador se reanuda automáticamente después de que se complete el reinicio. Para anular el valor predeterminado, especifique `/noresume`. Puede ser útil si debe volver a montar el medio o quiere capturar información durante una instalación automatizada.

- **/portnumber** *puerto*

  Válido solamente si se especifica la opción `/reconfig`. Número de puerto para habilitar las comunicaciones entre VDA y Controller. El puerto previamente configurado queda inhabilitado a menos que sea el puerto 80.

- **/proxyconfig** "*dirección o ruta del archivo PAC*"

  Válido solo si el comando contiene `/includeadditional "Citrix Rendezvous V2"`. La dirección o la ruta del archivo PAC del proxy para uso con el protocolo Rendezvous. Para obtener más información sobre la funcionalidad, consulte Protocolo Rendezvous.

  - Formato de dirección de proxy: `http://<url-or-ip>:<port>`
  - Formato de archivo PAC: `http://<url-or-ip>:<port>/<path>/<filename>.pac`

- **/quiet** o **/passive**

  No aparece ninguna interfaz de usuario durante la instalación. La única prueba de que está teniendo lugar el proceso de instalación y configuración aparece en el Administrador de tareas de Windows. Si se omite esta opción, se abre la interfaz gráfica.

- **/reconfigure**

  Personaliza los parámetros de VDA configurados anteriormente cuando se usa con las opciones `/portnumber`, `/controllers` o `/enable_hdx_ports`. Si se especifica esta opción sin especificar también la opción `/quiet`, se abrirá la interfaz gráfica para personalizar VDA.

- **/remotepc**

  Válido solo para implementaciones de acceso con Remote PC (SO de sesión única) o conexiones intermediadas (SO multisesión).

  Esta opción no es válida cuando se utiliza el instalador `VDAWorkstationCoreSetup.exe`. El instalador excluye la instalación de estos componentes.

- **/remove_appdisk_ack**

  Autoriza al instalador de VDA a desinstalar el plug-in de VDA para AppDisks si está instalado.

- **/remove_pvd_ack**

  Autoriza al instalador de VDA a desinstalar el disco Personal vDisk si está instalado.

- **/remove**

  Quita los componentes especificados con la opción /`components`.

- **/removeall**

  Quita el VDA. No quita la aplicación Citrix Workspace (si está instalada).

- **/sendexperiencemetrics**

  Envía automáticamente a Citrix los análisis recopilados durante la instalación, la actualización o la eliminación. Si se omite esta opción (o se indica la opción /`disableexperiencemetrics`), los análisis se recopilan localmente, pero no se envían automáticamente.

- **/servervdi**

  Instala un VDA para SO de sesión única en un servidor Windows compatible. Omita esta opción cuando instale un VDA multisesión en un servidor Windows. Antes de usar esta opción, consulte VDI de servidor.

- **/site_guid** *guid*

  Identificador único global de la unidad organizativa (OU) de Active Directory para el sitio. Esto asocia un escritorio virtual con un sitio cuando se usa Active Directory para la detección (el método de detección predeterminado y recomendado es la actualización automática). El GUID del sitio es una de las propiedades del sitio que se muestra en **Administrar > Configuración completa**. No especifique ambas opciones, /`site_guid` y /`controllers`.

- **/tempdir** *directorio*

  Directorio que contiene los archivos temporales durante la instalación. Valor predeterminado = c:\Windows\Temp.

  Esta opción no está disponible en la interfaz gráfica.

- **/virtualmachine**

  Válido solamente cuando se instala un VDA en una VM. Invalida la detección de un equipo físico por parte del instalador, donde la información de BIOS que se pasa a las VM las hace aparecer como equipos físicos.

  Esta opción no está disponible en la interfaz gráfica.

- **/xendesktopcloud**

  Indica que el VDA está instalado en una implementación de Citrix DaaS (Citrix Cloud).

Ejemplos: Instalar un agente VDA

- **Instale un VDA en un SO multisesión.** El siguiente comando instala un VDA en un sistema operativo multisesión.

  ```
  VDAServerSetup.exe /quiet /controllers "Contr-East.domain.com"/
  enable_hdx_ports /masterimage
  ```

  El VDA se usará como imagen.

- **Instale un VDA con SO multisesión o un VDA con SO de sesión única.** Este comando instala un VDA con SO multisesión o un VDA con SO de sesión única.

  ```
  VDAServerSetup_XXXX.exe /quiet /controllers "ddc1.abc.com",
  "ddc2.abc.com"/enable_hdx_ports /enable_Remote_Assistance /
  enable_real_time_transport /enable_ss_ports /noreboot
  ```

  Separe cada FQDN del Delivery Controller con una coma. Tenga en cuenta que `XXXX` representa la versión del VDA.

- **Instale un VDA de los servicios principales en un SO de sesión única.** El siguiente comando instala un VDA con los servicios principales en un SO de sesión única para utilizarlo en una implementación de VDA o de acceso con Remote PC.

  ```
  VDAWorkstationCoreSetup.exe /quiet /controllers "Contr-East.
  domain.com"/enable_hdx_ports /noreboot
  ```

  La aplicación Citrix Workspace y otros servicios no principales no se instalan. Se especifica la dirección de un Cloud Connector, y los puertos del Firewall de Windows se abren automáticamente. El administrador gestiona los reinicios.

Personalizar un VDA mediante línea de comandos

Después de instalar un VDA, puede personalizar varios parámetros. Ejecute `XenDesktopVDASetup.exe` mediante una o varias de las siguientes opciones.

- `/reconfigure` (opción necesaria para personalizar un VDA)
- `/h` o `/help`
- `/quiet`
- `/noreboot`
- `/controllers`
- `/portnumber port`
- `/enable_hdx_ports`

Qué hacer a continuación

- Crear catálogos de máquinas
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.

Crear y administrar conexiones y recursos

February 21, 2024

Introducción

La configuración de una conexión implica seleccionar el tipo de conexión en la lista de hipervisores y servicios de nube compatibles, así como elegir los recursos de red y almacenamiento adecuados para esa conexión.

> **Nota:**
>
> Para poder realizar tareas de administración de recursos y conexiones, debe tener privilegios de administrador total.

Dónde encontrar información acerca de los tipos de conexión

En los requisitos del sistema, se ofrece una lista de las versiones de hipervisores y servicios de nube compatibles, junto con enlaces a artículos para cada host en cuestión.

Almacenamiento de host

Se admite un producto de almacenamiento si puede administrarse a través de un hipervisor compatible. Citrix Support solo ayuda a los proveedores de productos de almacenamiento a resolver problemas y a documentar estos problemas y soluciones en el Knowledge Center, según sea necesario.

Cuando se aprovisionan máquinas, los datos se clasifican por tipo:

- Sistema operativo (OS): Incluye imágenes
- Datos temporales: Incluyen todos los datos no persistentes escritos en las máquinas aprovisionadas por MCS, archivos de paginación de Windows y todos los datos que se sincronicen con ShareFile. Estos datos se descartan cada vez que la máquina se reinicia. Si la imagen base incluye datos de perfil de usuario, estos datos permanecen persistentes. Si se usa una solución de perfiles de usuario centralizada, los datos del perfil de usuario se sincronizan con el almacén

de perfiles externo. Los datos del perfil de usuario almacenados en la caché local se descartan cada vez que se reinicia la máquina.

La asignación de distintos recursos de almacenamiento a diferentes tipos de datos puede minimizar la carga del sistema y mejorar el rendimiento en términos de IOPS (operaciones de entrada/salida por segundo) en cada dispositivo de almacenamiento. Esta asignación estratégica hace un uso óptimo de los recursos disponibles del host. Además, permite seleccionar el medio de almacenamiento más adecuado en función de las necesidades específicas de cada tipo de datos, como una mayor persistencia o resistencia para ciertos tipos de datos.

- Opciones de almacenamiento local y compartido: Los recursos de almacenamiento pueden estar centralizados, es decir, separados de cualquier host en particular y utilizados por todos los hosts, o localizados en un hipervisor específico. Las opciones centralizadas incluyen los volúmenes compartidos de clústeres de Windows, que pueden o no tener almacenamiento adjunto adicional, o los dispositivos de los proveedores de almacenamiento. Las soluciones de almacenamiento centralizado pueden ofrecer funciones de optimización avanzadas, como rutas de control de almacenamiento específicas del hipervisor y acceso directo a los plug-ins.
- Ventajas y desventajas del almacenamiento local: El almacenamiento local de los datos temporales evita la necesidad de ir a la red para acceder al almacenamiento compartido y, por tanto, reduce la carga en términos de IOPS en los recursos compartidos. Puesto que el almacenamiento centralizado puede resultar más caro, el uso de almacenamiento local puede ser una alternativa rentable. Sin embargo, estas ventajas deben considerarse junto con la disponibilidad de almacenamiento suficiente en los servidores del hipervisor.

Almacenamiento compartido por los hipervisores

El método de almacenamiento compartido por los hipervisores guarda los datos que necesitan persistencia a largo plazo en una ubicación central, lo que proporciona una copia de seguridad y una administración centralizadas. Ese almacenamiento contiene los discos del sistema operativo.

Cuando se selecciona este método, se puede elegir si usar almacenamiento local (en servidores de la misma agrupación de hipervisores) para datos de máquina temporales. Estos datos no requieren persistencia ni tanta resistencia como los datos del almacenamiento compartido. Esto se denomina *caché de datos temporales*. El disco local ayuda a reducir el tráfico hacia el almacenamiento de SO principal. Este disco se borra cada vez que se reinicia la máquina. Se accede al disco a través de una memoria caché de escritura. Tenga en cuenta que, si usa almacenamiento local para datos temporales, el VDA aprovisionado queda asociado a un host de hipervisor específico. Si ese host falla, la máquina virtual no se puede iniciar.

Excepción: Si usa volúmenes de almacenamiento en clúster o CSV (Clustered Storage Volumes), Microsoft System Center Virtual Machine Manager no permite la creación de discos caché de datos temporales en el almacenamiento local.

Si almacena datos temporales localmente, puede habilitar y configurar valores no predeterminados para el tamaño de la memoria y del disco de caché de cada VM al crear un catálogo de máquinas que usa esa conexión. No obstante, los valores predeterminados se ajustan al tipo de conexión y son suficientes en la mayoría de los casos.

El hipervisor también puede ofrecer tecnologías de optimización a través de la caché en memoria local de lectura de las imágenes de los discos. Por ejemplo, XenServer ofrece IntelliCache. Esto también puede reducir el tráfico de red hacia el almacenamiento central.

Almacenamiento local en el hipervisor

El método de almacenamiento local en el hipervisor almacena datos localmente en el hipervisor. Con este método, las imágenes y otros datos del SO se transfieren a todos los hipervisores utilizados en el sitio, tanto para la creación inicial de las máquinas como para las futuras actualizaciones de las imágenes. Esto da como resultado un tráfico importante en la red de administración. La transferencia de imágenes consume también mucho tiempo y las imágenes no llegan a todos los hosts al mismo tiempo.

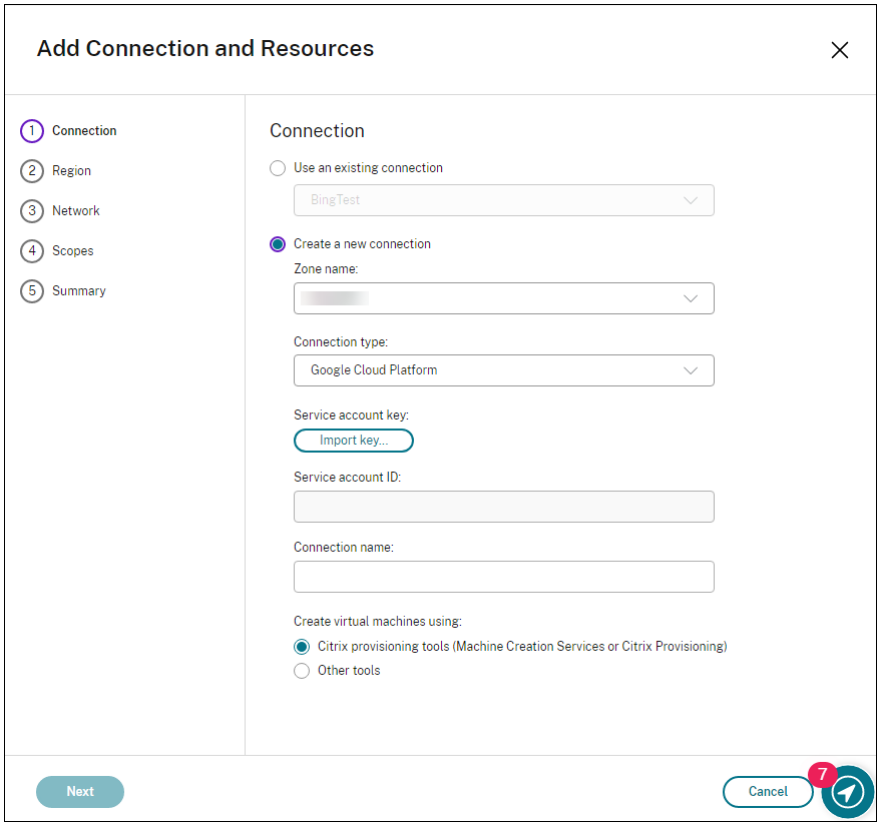
Crear una conexión y recursos

> **Importante:**
>
> Los recursos de host (almacenamiento y red) de la ubicación de recursos deben estar disponibles antes de crear la conexión.

1. Inicie sesión en Citrix Cloud.
2. Vaya al menú superior izquierdo y seleccione **Mis servicios > DaaS**.
3. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
4. Seleccione **Agregar conexiones y recursos** en la barra de acciones.
5. El asistente le guiará en el proceso de configuración que se describe en los pasos siguientes. El contenido específico de cada página depende del tipo de conexión seleccionado. Después de completar los pasos de cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**.

> **Nota:**
>
> El contenido de cada página del asistente varía según el tipo de conexión que haya seleccionado.

Paso 1. Conexión



En la página **Conexión**:

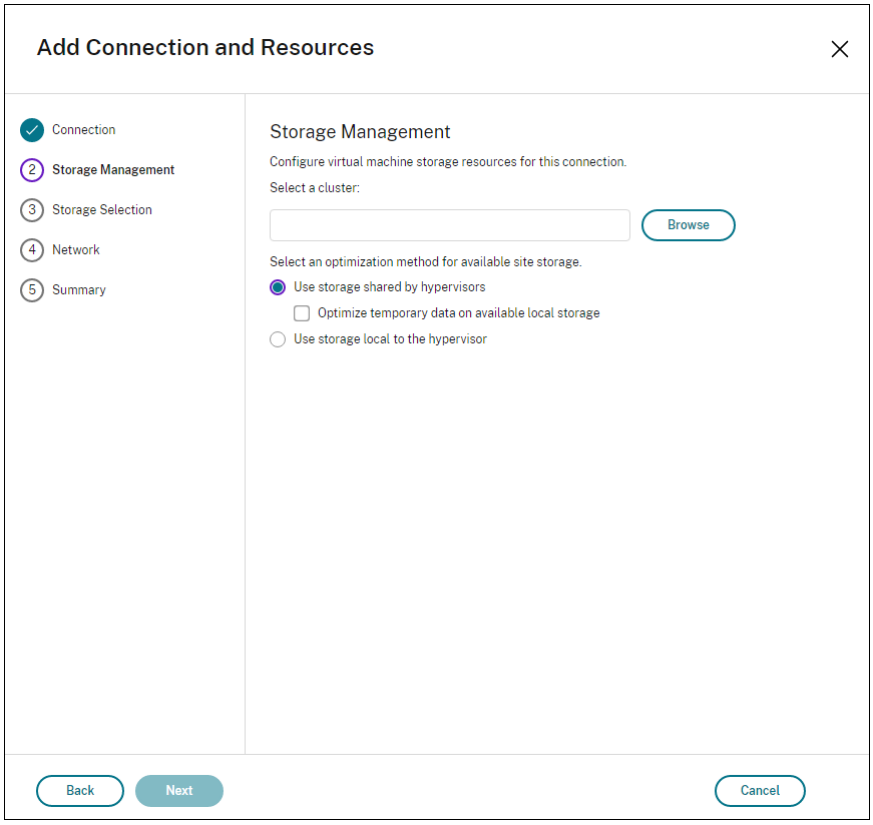
- Para crear otra conexión, seleccione **Crear una conexión**. Para crear una conexión basada en la misma configuración de host que una conexión existente, seleccione **Usar una conexión existente** y, a continuación, seleccione la conexión correspondiente.
- Seleccione una zona en el campo **Nombre de zona**. Las opciones son todas las ubicaciones de recursos que configuró.
- Seleccione un hipervisor o servicio de la nube en el campo **Tipo de conexión**. Las opciones incluyen todos los hipervisores y servicios de la nube compatibles con Citrix:
  - Para una ubicación de recursos sin Cloud Connectors accesibles, solo están disponibles los hipervisores y los servicios de la nube que permiten implementaciones sin conectores.
  - Para una ubicación de recursos con Cloud Connectors accesibles, solo están disponibles los hipervisores y los servicios de la nube que tengan sus plug-ins instalados correctamente en esos conectores.

  También puede utilizar el comando `Get-HypHypervisorPlugin [-ZoneUid] $rluid [-IncludeUnavailable]` false o true de PowerShell para obtener la lista de hipervisores y servicios de la nube disponibles.

- Escriba un nombre para la conexión. Este nombre aparece en la pantalla **Alojamiento**.
- Elija una herramienta para crear máquinas virtuales.

> **Nota:**
>
> La información de la página **Conexión** varía según el host o tipo de conexión que se utilice. Por ejemplo, cuando se usa Azure Resource Manager, puede utilizar una entidad de servicio existente o crear una nueva. Para obtener información detallada, consulte Conexión con Microsoft Azure.

Paso 2. Administración del almacenamiento



Para obtener más información sobre los tipos y métodos de administración de almacenamiento, consulte Almacenamiento de host.

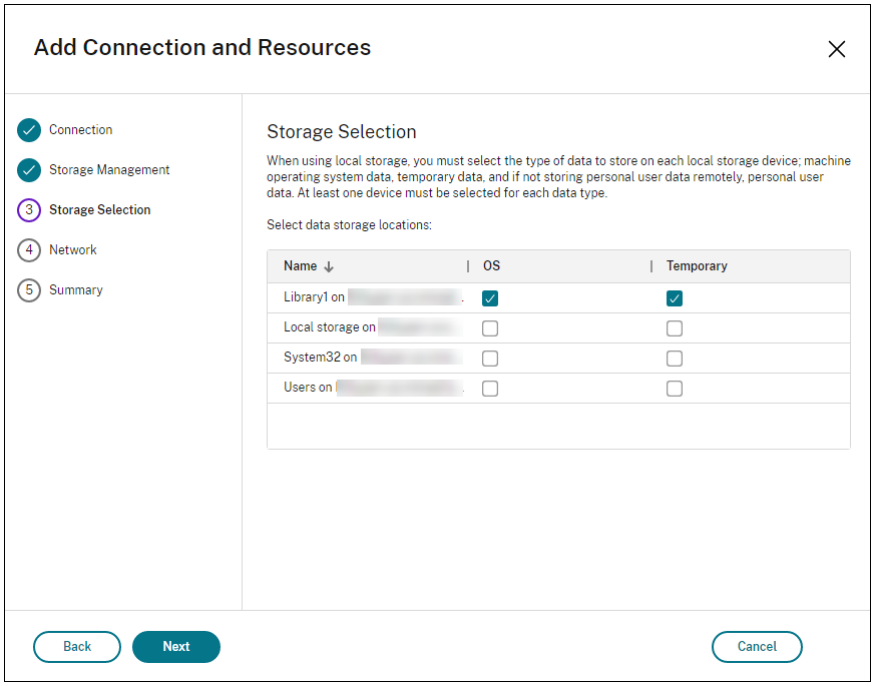
Si está configurando una conexión con un host de Hyper-V o VMware, busque y seleccione el nombre del clúster. Otros tipos de conexión no requieren un nombre de clúster.

Seleccione un método de administración del almacenamiento: puede ser almacenamiento compartido por los hipervisores o almacenamiento local en cada hipervisor.

Para obtener más información, consulte Almacenamiento compartido por los hipervisores y Almacenamiento local en el hipervisor.

Si usa almacenamiento compartido en una agrupación de XenServer, indique si quiere usar IntelliCache para reducir la carga en el dispositivo de almacenamiento compartido. Consulte Uso de IntelliCache para conexiones XenServer.

Paso 3. Selección del almacenamiento



Para obtener más información sobre la selección del almacenamiento, consulte Almacenamiento de hosts.

Seleccione al menos un dispositivo de almacenamiento en el host para cada tipo de datos. El método de administración de almacenamiento seleccionado en la página anterior afecta a qué tipos de datos estarán disponibles para seleccionar en esta página. Es necesario seleccionar al menos un dispositivo de almacenamiento para cada tipo de datos admitido antes de pasar a la página siguiente del asistente.

Puede obtener más opciones de configuración en la página **Selección de almacenamiento** si eligió **Usar almacenamiento compartido por hipervisores** y selecciona **Optimizar datos temporales en el almacenamiento local disponible** en la página **Administración del almacenamiento**. Puede seleccionar, por ejemplo, los dispositivos de almacenamiento local (en la misma agrupación de hipervisores) que quiere usar para los datos temporales.

Se mostrará la cantidad de dispositivos de almacenamiento seleccionados en ese momento (en el gráfico "1 storage device selected"). Al pasar el puntero sobre ese texto, aparecen los nombres de los dispositivos seleccionados (a menos que no haya ninguno configurado).

1. Seleccione **Seleccionar** para cambiar los dispositivos de almacenamiento que quiere usar.

2. En el cuadro de diálogo **Seleccionar almacenamiento**, seleccione o deje sin seleccionar las casillas de cada dispositivo de almacenamiento y, a continuación, seleccione **Aceptar**.

Paso 4. Region

> **Nota:**
>
> La página **Región** solo aparece para algunos tipos de host.

La selección de región indica dónde se implementarán las máquinas virtuales. Preferiblemente, elija una región cercana a donde los usuarios accederán a sus aplicaciones.

Paso 5. Red

Introduzca un nombre para los recursos. Este es el nombre que aparece en la consola Administrar para identificar la combinación de almacenamiento y red asociada a la conexión.

Seleccione una o varias redes que usarán las VM.

Algunos tipos de conexión (como Azure Resource Manager) también muestran las subredes que utilizarán las máquinas virtuales. Seleccione una o varias subredes.

Paso 6. Resumen

Revise las opciones seleccionadas. Si quiere hacer cambios, vuelva a las páginas anteriores del asistente. Una vez revisado, seleccione **Finalizar**.

> **Nota:**
>
> - Si guarda los datos temporales localmente, puede configurar valores no predeterminados para el almacenamiento de datos temporales cuando cree el catálogo que contendrá las máquinas que usen esta conexión.
> - El ámbito no se muestra a los administradores de acceso total. Para obtener más información, consulte Administradores, roles y ámbitos.

Modificar parámetros de conexión

No puede utilizar este procedimiento para lo siguiente:

- Cambiar el nombre de una conexión o crear una conexión.
- Cambiar los parámetros de GPU de una conexión. Los catálogos que accedan a este recurso deben usar una imagen adecuada específica de la GPU. Por lo tanto, si quiere cambiar los parámetros de GCP, cree una conexión en lugar de modificar una conexión existente.

Cómo modificar una conexión

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en la barra de acciones.
3. Utilice la página **Propiedades de la conexión** para cambiar la dirección y las credenciales de la conexión. Cambie la dirección solo si la máquina host actual tiene una nueva dirección. Al introducir una dirección a otra máquina, se desconfiguran los catálogos de máquinas de la conexión.
   - Seleccione **Modificar parámetros…** y, a continuación, introduzca la nueva información.
   - Si quiere especificar los servidores de alta disponibilidad para una conexión de XenServer, seleccione **Modificar servidores…** y seleccione los servidores. Citrix recomienda seleccionar todos los servidores en la agrupación para permitir la comunicación con XenServer en caso de que falle el servidor principal de la agrupación.

     > **Nota:**
     >
     > Si utiliza HTTPS y quiere configurar servidores de alta disponibilidad, no instale un certificado comodín para todos los servidores de una agrupación. Se requiere un certificado individual para cada servidor. Para obtener más información, consulte Crear una conexión con XenServer.

4. Utilice la página **Avanzados** para modificar los parámetros y especificar una cantidad máxima de acciones simultáneas (o máquinas simultáneas) por conexión de alojamiento. Estos parámetros pueden resultar útiles si los parámetros de administración de energía permiten que se inicien demasiadas o demasiado pocas máquinas al mismo tiempo. Todos los tipos de conexión tienen valores predeterminados concretos que son adecuados en la mayoría de los casos. Por lo general, no es necesario cambiarlos.
   - En las opciones **Acciones simultáneas (de cualquier tipo)** y **Actualizaciones de inventario de Personal vDisk simultáneas**, se especifican dos valores: el número máximo absoluto que se puede dar de forma simultánea en esta conexión y un porcentaje máximo de todas las máquinas que utilizan esta conexión. Debe especificar valores absolutos y porcentuales. El límite real aplicado es el valor más bajo.

     Por ejemplo: en una implementación con 34 máquinas, si **Acciones simultáneas (de cualquier tipo)** está establecido en un valor absoluto de 10 y un valor de porcentaje de 10, el límite real aplicado es 3 (es decir, 10 por ciento de 34, redondeado al número entero más cercano que sea menor que el valor absoluto de 10 máquinas).
   - La opción **Máximo de acciones nuevas por minuto** es un número absoluto. No hay ningún valor porcentual.

- Introduzca la información en el campo **Opciones de conexión** únicamente con la ayuda de un representante de asistencia técnica de Citrix Support.

5. Utilice la página **Ámbitos** para seleccionar uno o más ámbitos para este host.

   > **Nota:**
   >
   > El ámbito no se muestra a los administradores de acceso total. Por definición, esos administradores pueden acceder a todos los objetos de Citrix Cloud y servicios suscritos que gestione el cliente.

   Para obtener más información, consulte Administradores, roles y ámbitos.

6. Utilice la página **Arrendatarios compartidos** para agregar arrendatarios y suscripciones que compartan Azure Compute Gallery con la suscripción de esta conexión.

   a) Introduzca el **secreto** de la aplicación asociada a esta conexión. Con esta información, puede autenticarse en Azure. Le recomendamos que cambie las claves con regularidad para garantizar la seguridad.
   b) Agregue suscripciones y arrendatarios compartidos. Puede agregar hasta ocho arrendatarios compartidos. Para cada arrendatario, puede agregar hasta ocho suscripciones.

7. Haga clic en **Guardar** y **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Activar o desactivar el modo de mantenimiento de una conexión

Si activa el modo de mantenimiento de una conexión, impide que cualquier otra acción de energía nueva afecte a las máquinas almacenadas en la conexión. Los usuarios no se pueden conectar a una máquina mientras está en modo de mantenimiento. Si los usuarios ya están conectados, los cambios del modo de mantenimiento se efectúan cuando se cierra la sesión.

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión. Para activar el modo de mantenimiento, seleccione **Activar modo de mantenimiento** en la barra de acciones. Para desactivar el modo de mantenimiento, seleccione **Desactivar modo de mantenimiento**.

También puede activar o desactivar el modo de mantenimiento en máquinas individuales. Puede activar o desactivar el modo de mantenimiento en las máquinas de los catálogos de máquinas o grupos de entrega.

Eliminar una conexión

> **Precaución:**
>
> La eliminación de una conexión puede provocar la eliminación de una gran cantidad de máquinas y la pérdida de datos. Compruebe que se haya hecho copia de seguridad de los datos de usuario en las máquinas afectadas, si fueran útiles.

Antes de eliminar una conexión, compruebe que:

- Todos los usuarios hayan cerrado la sesión en las máquinas almacenadas en la conexión.
- No existan sesiones de usuario desconectadas en ejecución.
- El modo de mantenimiento está activo para máquinas agrupadas y dedicadas.
- Todas las máquinas de los catálogos que usan la conexión están apagadas.

Un catálogo de máquinas se vuelve inutilizable al eliminar una conexión a la que se hace referencia en ese catálogo. Si se hace referencia a esta conexión en un catálogo, puede eliminar el catálogo. Antes de eliminar un catálogo, compruebe que no haya otras conexiones que lo estén utilizando.

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Eliminar conexión** en la barra de acciones.
3. Si esta conexión contiene máquinas almacenadas, se le preguntará si quiere eliminar las máquinas. Si debieran eliminarse, especifique qué debe hacerse con las cuentas de equipo de Active Directory asociadas.

Cambiar el nombre de una conexión

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Cambiar nombre de conexión**.

Probar una conexión

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Probar conexión**.

Ver detalles de máquinas en una conexión

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Ver máquinas** en la barra de acciones.

El panel superior ofrece una lista de las máquinas a las que se accede a través de la conexión. Seleccione una máquina para ver información detallada sobre ella en el panel inferior. También se proporcionan detalles de sesión para las sesiones abiertas.

Utilice la función de búsqueda para encontrar máquinas rápidamente. Seleccione una búsqueda guardada en la lista que aparece en la parte superior de la ventana o cree una búsqueda nueva. Puede realizar la búsqueda con todo o parte del nombre de la máquina o puede crear una expresión y usarla para una búsqueda avanzada. Para crear una expresión, seleccione **Expandir** y, a continuación, seleccione elementos de las listas de propiedades y operadores.

Administrar máquinas en una conexión

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione una conexión y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Seleccione una de estas opciones en la barra de acciones. Es posible que algunas acciones no estén disponibles según el estado de la máquina y el tipo de host de la conexión.

    - **Iniciar:** Inicia la máquina si está apagada o suspendida.
    - **Suspender:** Pausa la máquina sin apagarla y actualiza la lista de máquinas.
    - **Apagar:** Solicita al sistema operativo de la máquina que se apague.
    - **Forzar apagado:** Apaga la máquina y actualiza la lista de máquinas.
    - **Reiniciar:** Solicita al sistema operativo que se apague y que, a continuación, vuelva a iniciar la máquina. Si el sistema operativo no puede hacerlo, el escritorio se mantiene en su estado actual.
    - **Habilitar modo de mantenimiento:** Detiene temporalmente las conexiones a una máquina. Los usuarios no pueden conectarse a una máquina en este estado. Si los usuarios están conectados, los cambios del modo de mantenimiento se efectúan cuando se cierra la sesión (también puede activar o desactivar el modo de mantenimiento en todas las máquinas a las que se accede a través de una conexión, tal y como se describe anteriormente).
    - **Quitar del grupo de entrega:** Quitar una máquina de un grupo de entrega no la elimina del catálogo de máquinas que utiliza ese grupo de entrega. Puede quitar una máquina solamente cuando no haya ningún usuario conectado a ella. Active el modo de mantenimiento para evitar temporalmente la conexión de usuarios mientras la quita.
    - **Eliminar:** Cuando se elimina una máquina, los usuarios dejan de tener acceso a ella y esta se elimina del catálogo de máquinas. Antes de eliminar una máquina, asegúrese de contar con una copia de seguridad de todos los datos del usuario o de que esos datos ya no sean necesarios. Puede eliminar una máquina solamente cuando no haya ningún usuario conectado a ella. Active el modo de mantenimiento para impedir temporalmente la conexión de usuarios mientras la elimina.

Para acciones que implican el apagado de una máquina, si la máquina no se apaga en 10 minutos, se desconecta. Si Windows intenta instalar actualizaciones durante el cierre, existe el riesgo de que el equipo se apague antes de que se completen las actualizaciones.

Modificar la opción de almacenamiento

Puede mostrar el estado de los servidores que se usan para almacenar datos del sistema operativo, datos temporales y datos personales (PvD) para las VM que usan esa conexión. También puede especificar qué servidores usar para el almacenamiento de cada tipo de datos.

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Modificar almacenamiento** en la barra de acciones.
3. En el panel de la izquierda, seleccione el tipo de datos: sistema operativo o datos temporales.
4. Seleccione o deje sin seleccionar las casillas de los dispositivos de almacenamiento para el tipo de datos seleccionado.
5. Seleccione **OK**.

Cada dispositivo de almacenamiento en la lista incluye su nombre y su estado. Los valores del estado de almacenamiento son:

- **En uso**: El almacenamiento se está usando para crear máquinas.
- **Reemplazado**: El almacenamiento se usa solo para máquinas existentes. No se agregan nuevas máquinas a este almacenamiento.
- **Sin usar:** El almacenamiento no se está utilizando para crear máquinas.

Si deja sin marcar la casilla de un dispositivo que está actualmente **En uso**, su estado cambia a **Reemplazado**. Las máquinas existentes seguirán utilizando ese dispositivo de almacenamiento (y podrán escribir datos en él). Por lo tanto, esa ubicación puede llenarse incluso cuando ya no se utiliza para crear máquinas.

Detectar recursos huérfanos de Azure

Los recursos huérfanos son recursos no utilizados presentes en el sistema que pueden generar un gasto innecesario.

Esta función le permite detectar los recursos de Azure huérfanos en los hosts de su sitio en la nube.

Siga los pasos en Citrix DaaS:

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione una conexión y, a continuación, seleccione **Detectar recursos huérfanos** en la barra de acciones. El cuadro de diálogo **Detectar recursos huérfanos** muestra el informe de recursos huérfanos.
3. Para ver el informe de recursos huérfanos, seleccione **Ver informe**.

Como alternativa, puede detectar recursos huérfanos de Azure mediante PowerShell. Para obtener más información, consulte Obtener una lista de recursos huérfanos.

Para entender los motivos de los recursos huérfanos y saber cómo proceder, consulte Efficiently manage Orphaned Azure resources with Citrix.

Temporizadores de conexión

Puede usar configuraciones de directiva Citrix para configurar tres temporizadores de conexión:

- **Temporizador de duración máxima de conexión:** Determina la duración máxima de una conexión sin interrupciones entre un dispositivo de usuario y un escritorio virtual. Use las configuraciones de directiva **Temporizador de conexión de sesión** e **Intervalo de temporizador de conexión de sesiones**.
- **Temporizador de conexión inactiva:** Este parámetro determina la cantidad de tiempo que se mantiene la conexión sin interrupciones entre un dispositivo de usuario y un escritorio virtual, si el usuario no realiza entradas. Use las configuraciones de directiva **Temporizador de sesión inactiva** e **Intervalo de temporizador de sesiones inactivas**.
- **Temporizador de desconexión**: Determina la cantidad de tiempo que un escritorio virtual desconectado y bloqueado puede permanecer bloqueado antes de que se cierre la sesión. Use las configuraciones de directiva **Temporizador de sesión desconectada** e **Intervalo de temporizador de sesiones desconectadas**.

Al actualizar estos parámetros, compruebe que son coherentes en toda la implementación.

Consulte la documentación de configuraciones de directivas para obtener más información.

Modificar redes de recursos

Es posible cambiar redes con una conexión. Haga lo siguiente:

1. Vaya a **Administrar > Configuración completa > Alojamiento**.
2. Seleccione los recursos de destino en la conexión y, a continuación, seleccione **Modificar red** en la barra de acciones.
3. Seleccione una o varias redes que usarán las nuevas máquinas virtuales.
4. Haga clic en **Guardar** para guardar los cambios y salir.

Eliminar, cambiar el nombre o probar recursos

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione los recursos de destino en la conexión y, a continuación, seleccione la entrada correspondiente en la barra de acciones:
    - **Eliminar recursos**

- **Cambiar nombre de recursos**
- **Probar recursos**

Obtener una lista de recursos huérfanos

Puede obtener una lista de los recursos huérfanos que MCS ha creado, pero de los que ya hace seguimiento. Esto se aplica actualmente a los entornos de Azure. Para obtener la lista, puede usar los comandos de PowerShell. Puede filtrar mediante conexiones.

> **Nota:**
>
> El comando de PowerShell se rechaza si hay algún aprovisionamiento o actualización de imagen en curso.

Limitaciones

- Solo un usuario con el rol de administrador de Cloud o administrador total integrado puede ejecutar el comando de PowerShell y obtener la lista de recursos huérfanos.
- Para evitar el reconocimiento incorrecto de los recursos huérfanos, no encienda las máquinas virtuales mientras filtra los recursos huérfanos.
- Alrededor de 2000 registros se muestran como huérfanos en caso de una posible carga de trabajo grande.

Mostrar la lista de recursos huérfanos

Para mostrar la lista de recursos huérfanos:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Ejecute los comandos siguientes:

   a) Obtenga el identificador de conexión. El uid de conexión es el valor del atributo HypervisorConnectionUID.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.PluginId -like 'Azure*'  }
    "
   <!--NeedCopy-->
   ```

   b) Obtenga la lista de recursos huérfanos.

   ```
   get-provorphanedresource
   -HypervisorConnectionUid <connection uid>
   <!--NeedCopy-->
   ```


Mostrar la lista de recursos huérfanos de un ID de suscripción

Para mostrar la lista de recursos huérfanos de un ID de suscripción:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Ejecute los comandos siguientes:

   a) Busque el identificador de conexión mediante el identificador de suscripción. El uid de conexión es el valor del atributo HypervisorConnectionUID.

   ```
   Get-ChildItem xdhyp:\connections | where {
     $_.CustomProperties -match '<subscriptionId>'  }

   <!--NeedCopy-->
   ```

   b) Obtenga la lista de recursos huérfanos.

   ```
   get-provorphanedresource -HypervisorConnectionUid <connection
       uid>
   <!--NeedCopy-->
   ```

> **Nota:**
>
> Compruebe los recursos detenidamente antes de eliminarlos.

Qué hacer a continuación

- Para obtener información sobre la conexión con tipos de host específicos, consulte:
  - Conexión con AWS
  - Conexión con entornos de Google Cloud
  - Conexión con Microsoft Azure
  - Conexión con Microsoft System Center Virtual Machine Manager
  - Conexión con Nutanix
  - Conexión con soluciones de Nutanix Cloud y de partners
  - Conexión con VMware
  - Conexión con soluciones de VMware Cloud y de partners
  - Conexión a XenServer

Si está en el proceso de implementación inicial, cree un catálogo de máquinas.

Conexión con AWS

May 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de nube de AWS.

> **Nota:**
>
> Antes de crear una conexión con AWS, debe terminar de configurar su instancia de AWS como ubicación de recursos. Consulte Entornos de virtualización de AWS.

Crear una conexión

Al crear una conexión desde la interfaz de Configuración completa:

- Debe proporcionar la clave de API y los valores de clave secreta. Puede exportar el archivo de claves que contiene esos valores de AWS y, a continuación, importarlos. También debe proporcionar la región, la zona de disponibilidad, el nombre de la nube VPC, las direcciones de subred, el nombre de dominio, los nombres de los grupos de seguridad y las credenciales.
- El archivo de credenciales para la cuenta raíz de AWS, (que se puede obtener de la consola de AWS), no está en el mismo formato que los archivos de credenciales descargados para los usuarios estándar de AWS. Por lo tanto, Citrix DaaS no puede usar el archivo para rellenar los campos de la clave de API y la clave secreta. Debe utilizar archivos de credenciales de Identity Access Management (IAM) de AWS.

> **Nota:**
>
> Después de crear una conexión, los intentos de actualizar la clave de API y la clave secreta podrían fallar. Para resolver el problema, compruebe las restricciones del servidor proxy o del firewall y asegúrese de que se puede contactar con la siguiente dirección: `https://*.amazonaws.com`.

Limitación

Si cambia el nombre de una nube privada virtual (VPC) de AWS en la consola de AWS, se desconfigura la unidad de alojamiento existente en Citrix Cloud. Si la unidad de alojamiento se rompe, no se pueden crear catálogos nuevos ni agregar máquinas a catálogos existentes. Para resolver este problema, cambie el nombre de la VPC de AWS al nombre original.

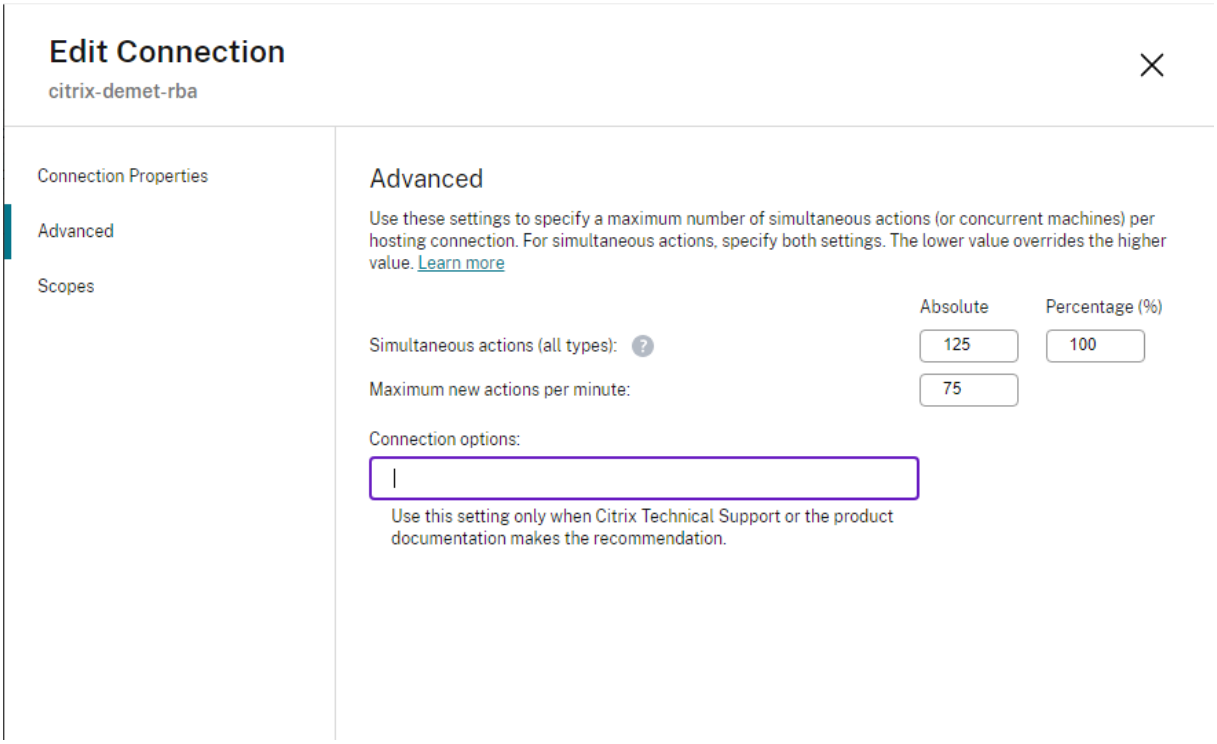
Valores predeterminados de conexión de host

Cuando crea conexiones de host en la interfaz de Configuración completa del entorno de nube de AWS, se muestran estos valores predeterminados:

Opción	Absoluta	Porcentaje
Acciones simultáneas (de cualquier tipo)	125	100
Máximo de acciones nuevas por minuto	150	n/d
Máximo de operaciones de aprovisionamiento simultáneas	100	n/d

MCS admite un máximo de 100 operaciones simultáneas de aprovisionamiento de forma predeterminada.

Para configurar estos valores, vaya a la sección **Avanzado** de Citrix Studio, en la pantalla **Modificar conexión**:



También puede usar el SDK de PowerShell remoto y, así, definir el máximo de operaciones simultáneas para establecer una configuración óptima según su entorno.

Utilice la propiedad personalizada de PowerShell, `MaximumConcurrentProvisioningOperations`, para especificar el máximo de operaciones simultáneas de aprovisionamiento de AWS.

Antes de la configuración:

- Asegúrese de haber instalado el SDK de PowerShell para Cloud.
- Debe comprender que el valor predeterminado de `MaximumConcurrentProvisioningOperations` es 100.

Siga estos pasos para personalizar el valor de `MaximumConcurrentProvisioningOperations`:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Escriba `cd xdhyp:\Connections\`.
4. Escriba `dir` para enumerar las conexiones.
5. Cambie o inicialice la cadena CustomProperties:
   - Si la cadena CustomProperties tiene un valor, copie las CustomProperties en el Bloc de notas. A continuación, cambie la propiedad `MaximumConcurrentProvisioningOperations` por el valor que prefiera. Puede introducir un valor comprendido entre 1 y 1000. Por ejemplo, `<Property xsi:type="IntProperty"Name="MaximumConcurrentProvis "Value="xyz"/>`.
   - Si la cadena CustomProperties está vacía o es nula, debe inicializar la cadena. Para ello, introduzca la sintaxis apropiada tanto para el esquema como para la propiedad `MaximumConcurrentProvisioningOperations`.
6. En la ventana de **PowerShell**, pegue las CustomProperties modificadas del Bloc de notas y asigne una variable a las CustomProperties modificadas. Si inicializó las Custom Properties, agregue estas líneas después de la sintaxis:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
   citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
   org/2001/XMLSchema-instance"><Property xsi:type="IntProperty"
   Name="MaximumConcurrentProvisioningOperations" Value="100"/></
   CustomProperties>'.
   ```

   Esta cadena establece la propiedad `MaximumConcurrentProvisioningOperations` en 100. En la cadena CustomProperties, debe establecer la propiedad `MaximumConcurrentProvision` en un valor que se ajuste a sus necesidades.
7. Introduzca `Get-XDAuthentication`, lo que le solicitará sus credenciales.

8. Ejecute `$cred = Get-Credential`, lo que es posible que le solicite únicamente una contraseña (o un nombre y una contraseña). También es posible que se le pida el ID de la aplicación y el secreto asociado. Para las conexiones que utilizan la autenticación basada en roles, **role_based_auth** es el nombre y la contraseña a la vez. De lo contrario, introduzca el secreto y el ID de la API de AWS.
9. Ejecute `set-item -PSPath 'XDHyp:\Connections<connection-name>' -CustomProperties $customProperties -username $cred.username -Securepassword $cred.password`. Debe definir *<connection-name>* como el nombre de la conexión.
10. Introduzca `dir` para verificar la cadena CustomProperties actualizada.

Configurar grupos de seguridad por interfaz de red

Al modificar una conexión de host, ahora puede configurar la cantidad máxima de grupos de seguridad permitidos por interfaz de red elástica (ENI) mediante un comando de PowerShell. Para obtener información sobre los valores de cuota de los grupos de seguridad de AWS, consulte Grupos de seguridad.

Para configurar grupos de seguridad por interfaz de red:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute `cd xdhyp:\Connections\`.
4. Ejecute `dir` para enumerar las conexiones.
5. Ejecute el siguiente comando de PowerShell para configurar los grupos de seguridad por interfaz de red:

```
Set-HypHypervisorConnectionMetadata -HypervisorConnectionName aws
    -Name "Citrix_MachineManagement_Options" -Value "
    AwsMaxENISecurityGroupLimit=<number>"
<!--NeedCopy-->
```

> **Nota:**
>
> Si no establece un valor para `AwsMaxENISecurityGroupLimit`, tomará 5 como valor predeterminado.

URL de “punto de enlace”de servicio

URL de “punto de enlace”de servicio de zona estándar

Cuando utiliza MCS, se agrega una nueva conexión de AWS con una clave de API y un secreto de API. Con esta información, junto con la cuenta autenticada, MCS consulta a AWS las zonas admitidas mediante la llamada a la API de EC2 con la acción de AWS DescribeRegions. Para la consulta, se utiliza una URL de dispositivo de punto final de servicio (punto de enlace de servicio, como se conoce en AWS) de EC2 genérica `https://ec2.amazonaws.com/`. Use MCS para seleccionar la zona de la conexión en la lista de zonas admitidas. La URL de punto de enlace del servicio de AWS preferida se selecciona automáticamente para la zona. Sin embargo, después de crear la URL de punto de enlace de servicio, ya no podrá establecerla ni modificarla.

URL de “punto de enlace”de servicio no estándar

Puede haber situaciones en las que no necesite la URL de punto de enlace de servicio de AWS elegida automáticamente para la conexión. En estos casos, puede usar el SDK de Citrix Cloud y PowerShell para crear una conexión con una URL de punto de enlace de servicio no estándar. Por ejemplo: para crear una conexión mediante la URL de punto de enlace de servicio `https://ec2.cn-north-1.amazonaws.com.cn`:

1. Configure el Cloud Connector alojado en AWS y compruebe que tiene conectividad.
2. Ejecute los siguientes comandos de PowerShell para ver la lista de Cloud Connectors.

```
1  PS C:> asnp citrix.*
2  PS C:> Get-XDAuthentication
3  PS C:> Get-ConfigEdgeServer
4 <!--NeedCopy-->
```

3. Busque el UID de zona del Cloud Connector recién creado e introdúzcalo en los siguientes comandos de PowerShell. Sustituya los elementos en cursiva por los valores respectivos.

```
PS C:\> $hyp= New-Item -Path xdhyp:\Connections -ZoneUidUID_de_Zona-
Name“Mi_Nueva_Conexión”-ConnectionType "AWS"-HypervisorAddress @
("https://ec2.cn-north-1.amazonaws.com.cn")-UserName“Clave_API”
-Password“Secreto de API” -Persist
PS C:\> New-BrokerHypervisorConnection -HypHypervisorConnectionUid
 $hyp. HypervisorConnectionUid
```

4. Actualice la ficha **Configuración completa > Alojamiento** para comprobar que se ha creado la conexión de EC2.
5. Agregue una ubicación de recursos mediante la nueva conexión.

Definir permisos de IAM

Utilice la información de esta sección para definir los permisos de IAM para Citrix DaaS en AWS. El servicio IAM de Amazon permite cuentas con varios usuarios que se pueden organizar en grupos. Estos usuarios pueden tener diferentes permisos para controlar su capacidad de realizar operaciones asociadas con la cuenta. Para obtener más información acerca de los permisos de IAM, consulte Referencia de directivas JSON de IAM.

Para aplicar la directiva de permisos de IAM a un nuevo grupo de usuarios:

1. Inicie sesión en la consola de administración de AWS y seleccione el **servicio IAM** en la lista desplegable.
2. Seleccione **Create a New Group of Users**.
3. Escriba un nombre para el nuevo grupo de usuarios y seleccione **Continue**.
4. En la página **Permissions**, elija **Custom Policy** y, luego, **Select**.
5. Escriba un nombre para la **directiva de permisos** (Permissions policy).
6. En la sección **Policy Document**, introduzca los permisos correspondientes.

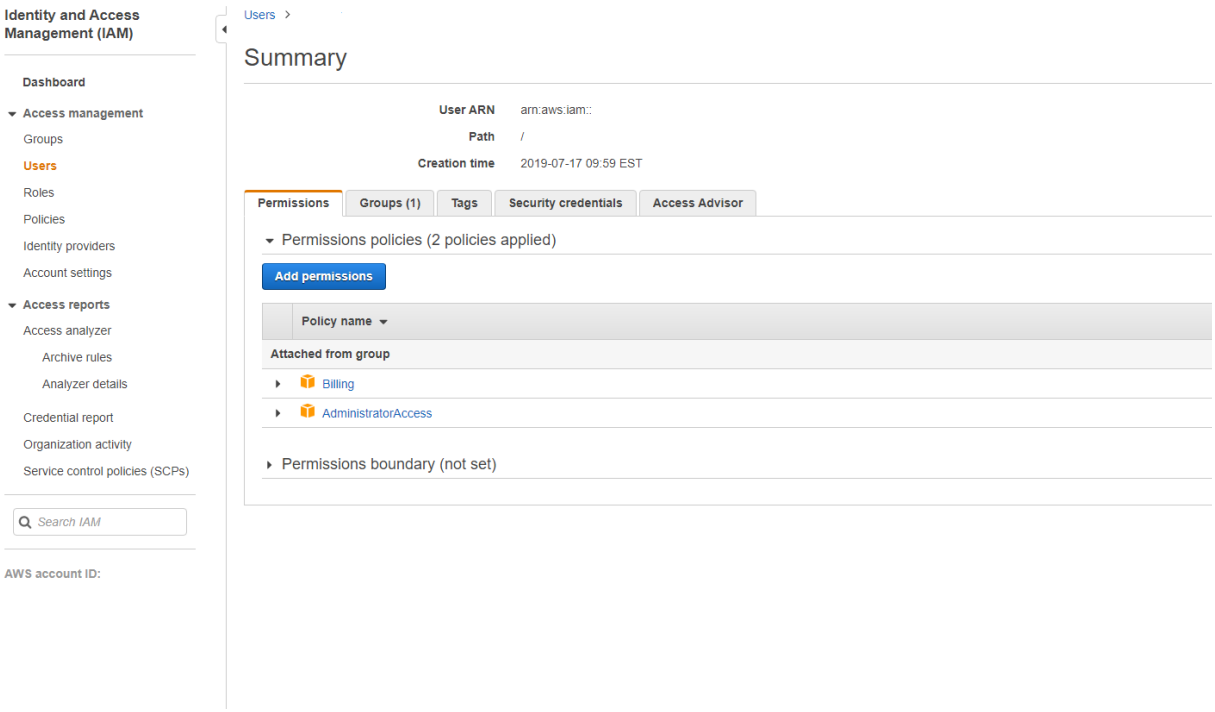
Después de indicar información sobre la directiva, seleccione **Continue** para completar la aplicación de la directiva de permisos de IAM al grupo de usuarios. A los usuarios del grupo se les conceden permisos para realizar solo aquellas acciones que son necesarias para Citrix DaaS.

> **Importante:**
>
> Utilice el texto de directiva proporcionado en el ejemplo siguiente para indicar las acciones que Citrix DaaS utiliza para realizar operaciones en una cuenta de AWS sin restringir esas operaciones a recursos específicos. Citrix recomienda utilizar el ejemplo como prueba. Para entornos de producción, puede optar por agregar más restricciones a los recursos.

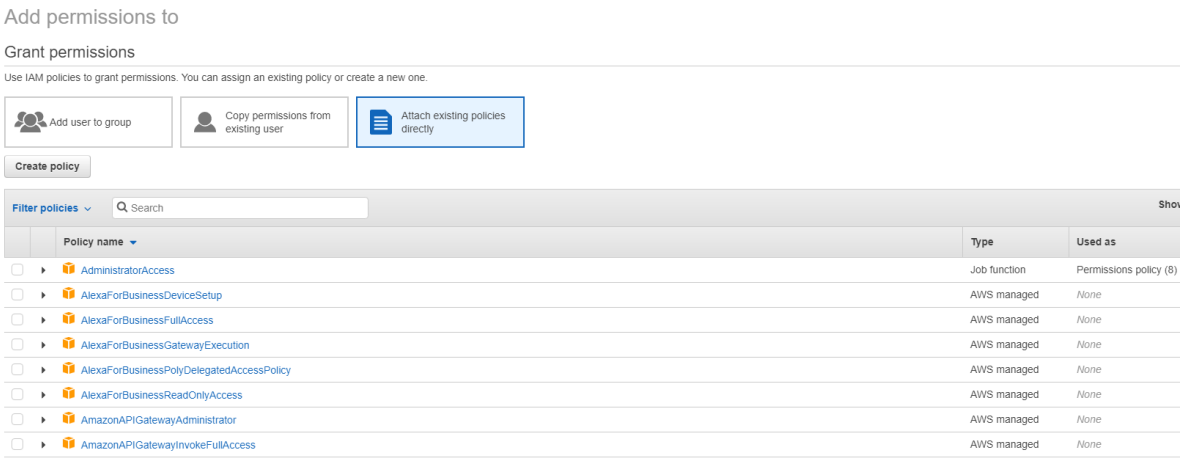
Agregar permisos de IAM

Agregue los permisos en la sección **IAM** de la consola de administración de AWS (AWS Management Console):

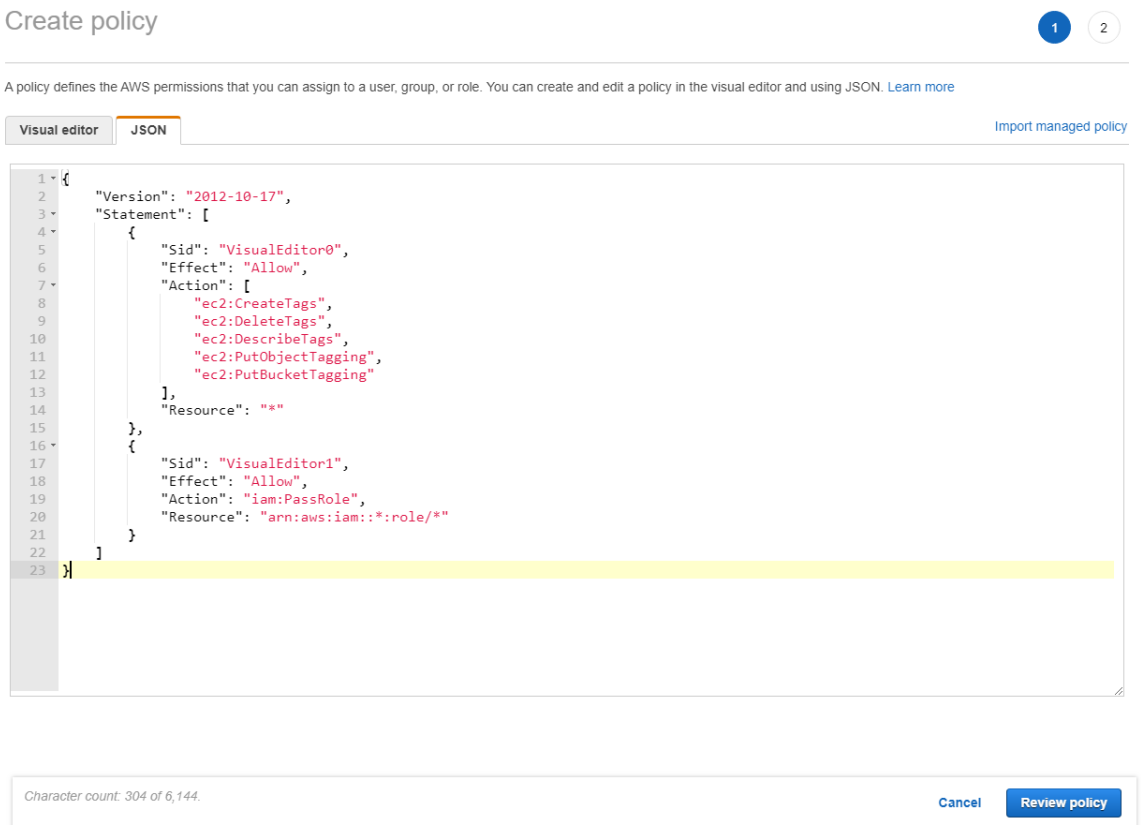
1. En el panel **Summary**, seleccione la ficha **Permissions**.
2. Seleccione **Add permissions**.



En la pantalla **Add Permissions to**, conceda los permisos:



Utilice lo siguiente como ejemplo en la ficha **JSON**:



> **Sugerencia:**
>
> Es posible que el ejemplo sobre JSON indicado no incluya todos los permisos necesarios para su entorno. Para obtener más información, consulte Acerca de los permisos de AWS.

Permisos de AWS requeridos

Esta sección contiene la lista completa de permisos de AWS. Utilice el conjunto completo de permisos que se indica en la sección para que la funcionalidad opere correctamente.

> **Nota:**
>
> El permiso *iam:PassRole* solo es necesario para **role_based_auth**.

Crear una conexión de host

Se agrega una nueva conexión de host con la información obtenida de AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {
```



```
6
7               "Action": [
8                   "ec2:DescribeAvailabilityZones",
9                   "ec2:DescribeImages",
10                  "ec2:DescribeInstances",
11                  "ec2:DescribeInstanceTypes",
12                  "ec2:DescribeSecurityGroups",
13                  "ec2:DescribeSubnets",
14                  "ec2:DescribeVpcs"
15              ],
16              "Effect": "Allow",
17              "Resource": "*"
18          }
19
20      ]
21  }
22
23  <!--NeedCopy-->
```

Administración de energía de las máquinas virtuales

Las instancias de máquina están encendidas o apagadas.

```
1  {
2
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6
7              "Action": [
8                  "ec2:AttachVolume",
9                  "ec2:CreateVolume",
10                 "ec2:DeleteVolume",
11                 "ec2:DescribeInstances",
12                 "ec2:DescribeVolumes",
13                 "ec2:DetachVolume",
14                 "ec2:StartInstances",
15                 "ec2:StopInstances"
16             ],
17             "Effect": "Allow",
18             "Resource": "*"
19         }
20
21     ]
22  }
23
24  <!--NeedCopy-->
```


Creación, actualización o eliminación de máquinas virtuales

Se crea, actualiza o elimina un catálogo de máquinas con las máquinas virtuales aprovisionadas como instancias de AWS.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteVolume",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",

                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
```



```
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:PutBucketAcl",
                "s3:PutBucketTagging",
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
}

<!--NeedCopy-->
```


> **Nota:**
>
> - La sección EC2 relacionada con SecurityGroups solo es necesaria si se debe crear un grupo de seguridad de aislamiento para la máquina virtual de preparación durante la creación del catálogo. Una vez hecho esto, no se requieren estos permisos.

Carga y descarga directa en disco La carga directa en disco elimina el requisito de trabajador de volumen para el aprovisionamiento de catálogos de máquinas y, en su lugar, utiliza las API públicas que proporciona AWS. Esta funcionalidad reduce el coste asociado a las cuentas de almacenamiento adicionales y la complejidad para mantener las operaciones de trabajador de volumen.

> **Nota:**
>
> Se ha retirado la función de trabajador de volumen.

Se deben agregar los siguientes permisos a la directiva:

- `ebs:StartSnapshot`
- `ebs:GetSnapshotBlock`
- `ebs:PutSnapshotBlock`
- `ebs:CompleteSnapshot`
- `ebs:ListSnapshotBlocks`
- `ebs:ListChangedBlocks`
- `ec2:CreateSnapshot`
- `ec2:DeleteSnapshot`
- `ec2:DescribeLaunchTemplates`

> **Importante:**
>
> - Puede agregar una nueva máquina virtual a los catálogos de máquinas existentes sin ningún recurso de trabajador de volumen, como AMI de trabajador de volumen y VM de trabajador de volumen.
> - Si elimina un catálogo que utilizaba cualquier trabajador de volumen anteriormente, se eliminan todos los artefactos relacionados con el trabajador de volumen.

Cifrado de EBS de volúmenes creados

EBS puede cifrar automáticamente los volúmenes recién creados si la imagen AMI está cifrada o si EBS está configurado para cifrar todos los volúmenes nuevos. Sin embargo, para implementar la funcionalidad, se deben incluir los siguientes permisos en la directiva de IAM.

```
1 {
```



```
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": [
9                   "kms:CreateGrant",
10                  "kms:Decrypt",
11                  "kms:DescribeKey",
12                  "kms:GenerateDataKeyWithoutPlainText",
13                  "kms:GenerateDataKey",
14                  "kms:ReEncryptTo",
15                  "kms:ReEncryptFrom"
16             ],
17             "Resource": "*"
18          }
19
20     ]
21  }
22
23  <!--NeedCopy-->
```

> **Nota:**
>
> Los permisos se pueden limitar a claves específicas si se incluye un recurso y bloque de condición, a discreción del usuario. Por ejemplo: **Permisos de KMS con condición**:

```
1  {
2
3       "Version": "2012-10-17",
4       "Statement": [
5          {
6
7              "Effect": "Allow",
8              "Action": [
9                   "kms:CreateGrant",
10                  "kms:Decrypt",
11                  "kms:DescribeKey",
12                  "kms:GenerateDataKeyWithoutPlainText",
13                  "kms:GenerateDataKey",
14                  "kms:ReEncryptTo",
15                  "kms:ReEncryptFrom"
16             ],
17             "Resource": [
18                 "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123
                      -456d-a12b-a123b4cd56ef"
19             ],
20             "Condition": {
21
22                 "Bool": {
23
24                     "kms:GrantIsForAWSResource": true
```



```
                    }

                }

            }

    ]
 }

<!--NeedCopy-->
```

La siguiente instrucción de directiva de claves es la predeterminada para las claves KMS, que es necesaria para permitir que la cuenta utilice las directivas de IAM para delegar el permiso para todas las acciones (kms:*) en la clave KMS.

```
{

"Sid": "Enable IAM policies",
"Effect": "Allow",
"Principal": {

"AWS": "arn:aws:iam::111122223333:root"
 }
 ,
"Action": "kms:",
"Resource": ""
 }

<!--NeedCopy-->
```

Para obtener más información, consulte la documentación oficial de AWS Key Management Service.

Autenticación basada en roles de IAM

Estos permisos se agregan para admitir la autenticación basada en roles.

```
{

     "Version": "2012-10-17",
     "Statement": [
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
 }

<!--NeedCopy-->
```


Directiva de permisos mínimos de IAM

El siguiente código JSON puede utilizarse para todas las funciones compatibles actualmente. Mediante esta directiva, puede crear conexiones de host, crear, actualizar o eliminar máquinas virtuales y administrar la energía.
La directiva se puede aplicar a los usuarios como se explica en las secciones Definir permisos de IAM o también puede usar la autenticación basada en roles mediante la clave de seguridad y la clave secreta de **role_based_auth** .

> **Importante:**
>
> Para usar **role_based_auth**, configure en primer lugar la funcionalidad de IAM deseada en la instancia ec2 del Cloud Connector al configurar este último. Con Citrix Studio, agregue la conexión de host y suministre "role_based_auth"para la clave de autenticación y el secreto. Una conexión de host con estos parámetros utiliza la autenticación basada en roles.

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ec2:AttachVolume",
                "ec2:AssociateIamInstanceProfile",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateImage",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DeleteLaunchTemplate",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeLaunchTemplates",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
```



```
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeSpotInstanceRequests",
                "ec2:DescribeInstanceCreditSpecifications",
                "ec2:DescribeInstanceAttribute",
                "ec2:GetLaunchTemplateData",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcs",
                "ec2:DetachVolume",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:RebootInstances",
                "ec2:RunInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
,
        {

            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::citrix*"
         }
,
        {

```



```
            "Action": [
                "ebs:StartSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ec2:CreateSnapshot"
            ],
            "Effect": "Allow",
            "Resource": "*"
         }
 ,
        {

            "Effect": "Allow",
            "Action": [
                 "kms:CreateGrant",
                 "kms:Decrypt",
                 "kms:DescribeKey",
                 "kms:GenerateDataKeyWithoutPlainText",
                 "kms:GenerateDataKey",
                 "kms:ReEncryptTo",
                 "kms:ReEncryptFrom"
            ],
            "Resource": "*"
         }
 ,
        {

            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/*"
         }

    ]
 }

<!--NeedCopy-->
```

Nota:

- La sección EC2 relacionada con SecurityGroups solo es necesaria si se debe crear un grupo de seguridad de aislamiento para la máquina virtual de preparación durante la creación del catálogo. Una vez hecho esto, no se requieren estos permisos.
- La sección KMS solo es necesaria cuando se utiliza el cifrado de volúmenes de EBS.
- La sección de permisos `iam:PassRole` solo es necesaria para **role_based_auth**.
- Se pueden agregar permisos específicos a nivel de recursos, en lugar de pleno acceso, en función de los requisitos y el entorno. Para obtener más información, consulte los documentos de AWS Demystifying EC2 Resource-Level Permissions y Access management for

> AWS resources.
> - Utilice los permisos `ec2:CreateNetworkInterface` y `ec2:DeleteNetworkInterface` solo si utiliza el método de trabajador de volumen.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica de AWS, consulte Crear un catálogo de AWS.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de AWS

Conexión con entornos de Google Cloud

April 18, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de Google Cloud.

> **Nota:**
>
> Antes de crear una conexión con Google Cloud, debe terminar de configurar su cuenta de Google Cloud como ubicación de recursos. Consulte Entornos de virtualización de Google Cloud.

Agregar una conexión

En la interfaz de Configuración completa, siga las instrucciones de Crear y administrar conexiones y recursos. Esta descripción es una guía para configurar una conexión de alojamiento:

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione **Agregar conexión y recursos** en la barra de acciones.
3. En la página **Conexión**, seleccione **Crear una conexión** y **Herramientas de aprovisionamiento de Citrix** y, a continuación, seleccione **Siguiente**.
    - **Nombre de zona**. Seleccione una zona (equivalente a una ubicación de recursos) en la que quiere que residan los recursos del host. Las zonas se crean automáticamente cuando

se crea una ubicación de recursos y se le agrega un Cloud Connector. Para obtener más información, consulte Zonas.

- **Tipo de conexión**. Seleccione **Google Cloud Platform** en el menú.
- **Clave de cuenta de servicio**. Importe la clave contenida en el archivo de credenciales de Google (JSON). Puede pegar la clave del archivo de credenciales o buscar el archivo de credenciales. Para pegar la clave:

  a) Localice su archivo de credenciales
  b) Abra el archivo con el Bloc de notas (o cualquier editor de texto)
  c) Copie el contenido.
  d) Vuelva a la página **Conexión**, seleccione **Agregar clave**, pegue el contenido y, a continuación, seleccione **Listo**.

- **ID de cuenta de servicio**. El campo se completa automáticamente con la información de la clave de la cuenta de servicio.
- **Nombre de la conexión**. Escriba un nombre para la conexión.
- **Redirigir tráfico a través de Citrix Cloud Connectors**. Para redirigir solicitudes de API a través de un Citrix Cloud Connector disponible, marque esta casilla. También puede marcar la casilla **Habilitar Google Cloud Build para usar agrupaciones privadas** para obtener un nivel de seguridad adicional.

  Como alternativa, puede habilitar esta función mediante PowerShell. Para obtener más información, consulte Crear un entorno seguro para el tráfico administrado de GCP.

> **Nota:**
>
> Esta opción solo está disponible cuando hay Citrix Cloud Connectors activos en la implementación. Actualmente, esta función no es compatible con Connector Appliances.

- **Crear máquinas virtuales usando**. Seleccione un método para crear máquinas virtuales.

4. En la página **Región**, seleccione un nombre de proyecto en el menú, seleccione una región que contenga los recursos que quiere utilizar y, a continuación, seleccione **Siguiente**.
5. En la página **Red**, escriba un nombre para los recursos, seleccione una red virtual en el menú, seleccione un subconjunto y, a continuación, seleccione **Siguiente**. El nombre de los recursos ayuda a identificar esta combinación de región y red. Las redes virtuales con el sufijo *(Shared)* (Compartida) anexado a su nombre representan VPC compartidas. Si configura un rol de IAM a nivel de subred para una VPC compartida, solo aparecerán subredes específicas de la VPC compartida en la lista de subredes.

> **Nota:**
>
> - El nombre de conexión puede contener entre 1 y 64 caracteres, y no puede contener solo espacios en blanco o los caracteres `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

6. En la página **Resumen**, confirme la información y seleccione **Finalizar** para salir de la ventana **Agregar conexión y recursos**.

Después de crear la conexión y los recursos, podrá verlos. Para configurar la conexión, selecciónela y, a continuación, seleccione la opción correspondiente en la barra de acciones.

Del mismo modo, puede eliminar, cambiar el nombre o probar los recursos creados en la conexión. Para ello, seleccione el recurso de la conexión y, a continuación, seleccione la opción correspondiente de la barra de acciones.

Crear un entorno seguro para el tráfico administrado de GCP

Puede permitir solo el acceso privado a Google en sus proyectos de Google Cloud. Esta implementación mejora la seguridad a la hora de gestionar datos confidenciales. Para hacerlo:

1. Instale Cloud Connectors en la VPC donde quiera aplicar los controles de servicio de la VPC. Consulte VPC Service Controls para obtener más información.
2. Agregue `ProxyHypervisorTrafficThroughConnector` a `CustomProperties` en el caso de una implementación de Citrix Cloud. Si utiliza una agrupación de trabajadores privados, agregue `UsePrivateWorkerPool` a `CustomProperties`. Para obtener información sobre la agrupación de trabajadores privados, consulte Private pools overview.

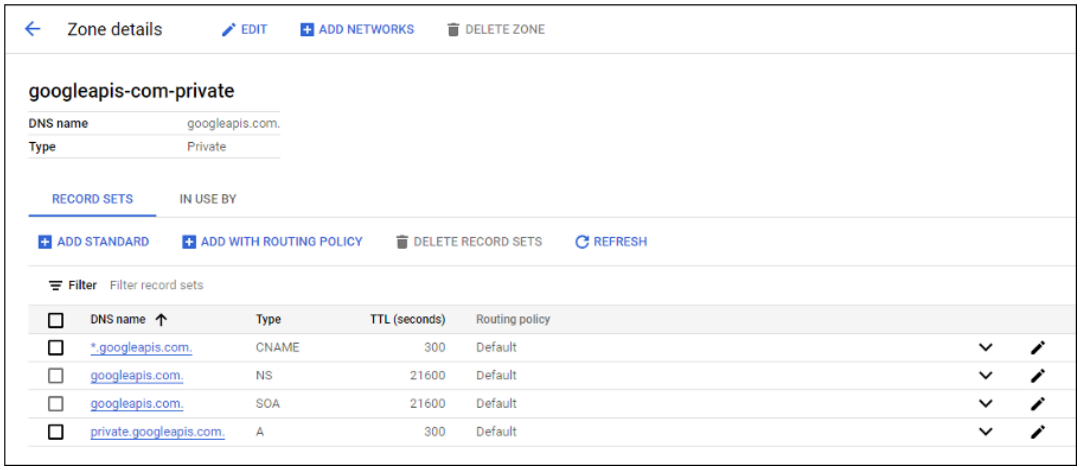
> **Nota:**
>
> Actualmente, esta función no es compatible con Connector Appliance.

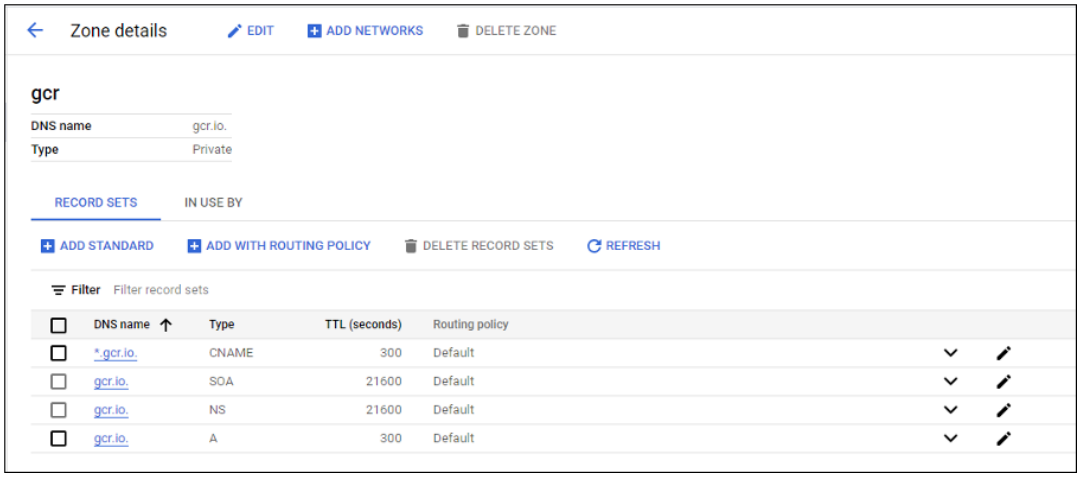
Requisitos para crear un entorno seguro para el tráfico administrado de GCP

Los requisitos para crear un entorno seguro para el tráfico administrado de GCP son los siguientes:

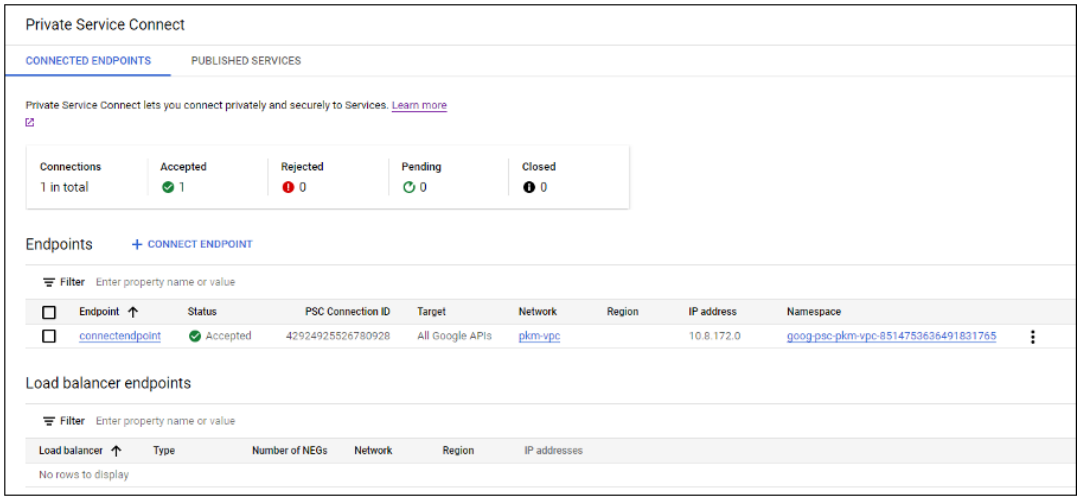
- Asegúrese de que la conexión de alojamiento esté en modo de mantenimiento al actualizar las propiedades personalizadas.
- Para usar agrupaciones de trabajadores privados, se requieren los siguientes cambios:
  - Para la cuenta de servicio de Citrix Cloud, agregue los siguientes roles de IAM:
    - Cuenta de servicio de Cloud Build
    - Administrador de instancias de proceso

    * Usuario de cuenta de servicio
    * Creador de tokens de cuentas de servicio
    * Propietario de agrupación de trabajadores de Cloud Build
- Cree la cuenta de servicio de Citrix Cloud en el mismo proyecto que usa para crear una conexión de alojamiento.
- Configure las zonas DNS para `private.googleapis.com` y `gcr.io` como se describe en la Configuración de DNS.

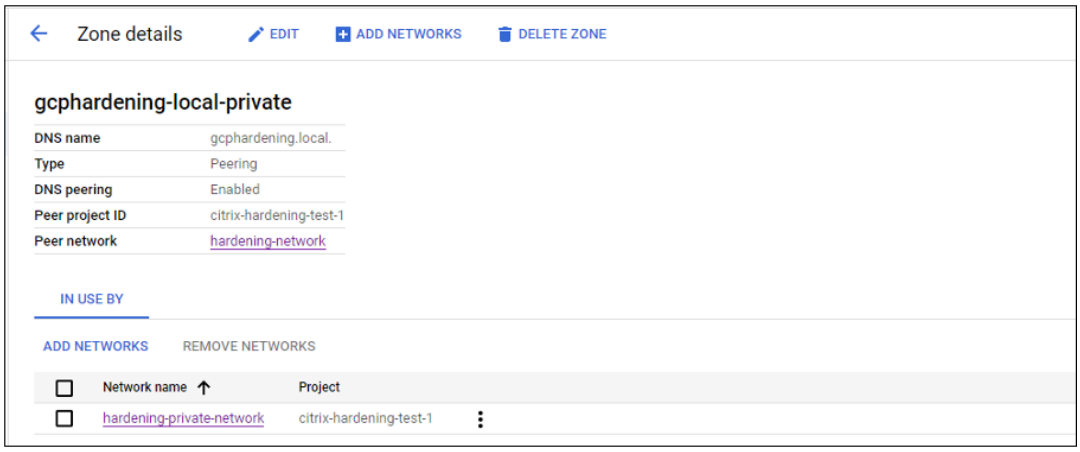




- Configure la traducción de direcciones de red (NAT) privada o utilice una conexión de servicio privada. Para obtener más información, consulte Access Google APIs through endpoints.



- Si usa una VPC emparejada, cree una zona de Cloud DNS que conecte a la VPC emparejada. Para obtener más información, consulte Create a peering zone.



- En los controles de servicio de VPC, configure las reglas de salida para que las API y las máquinas virtuales puedan comunicarse con Internet. Las reglas de entrada son opcionales. Por ejemplo:

```
Egress Rule 1
From:
Identities:ANY_IDENTITY
To:
Projects =
All projects
Service =
Service name: All services
<!--NeedCopy-->
```


Habilitar el proxy

Para habilitar el proxy, defina las propiedades personalizadas de esta manera en la conexión de host:

1. Abra una ventana de PowerShell desde el host del Delivery Controller o utilice el SDK de PowerShell remoto. Para obtener más información sobre el SDK de PowerShell remoto, consulte SDK y API.
2. Ejecute los comandos siguientes:

   a) `Add-PSSnapin citrix*`
   b) `cd XDHyp:\Connections\`
   c) `dir`

3. Copie `CustomProperties` de la conexión a un bloc de notas.
4. Anexe la configuración de la propiedad de la siguiente manera:

   - En caso de implementación en la nube (con agrupaciones públicas): Anexe la configuración de la propiedad `<Property xsi:type="StringProperty"Name ="ProxyHypervisorTrafficThroughConnector"Value="True"/>` a `CustomProperties` para habilitar el proxy. Por ejemplo:

     ```
     <CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
        -instance" xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation">
     <Property xsi:type="StringProperty" Name="
        ProxyHypervisorTrafficThroughConnector" Value="True"/>
     </CustomProperties>
     <!--NeedCopy-->
     ```

     Permita la regla de entrada de la cuenta de servicio de Cloud Build en el perímetro de servicio de la VPC. Por ejemplo:

     ```
     Ingress Rule 1
     From:
     Identities:
     <ProjectID>@cloudbuild.gserviceaccount.com
     Source > All sources allowed
     To:
     Projects =
     All projects
     Services =
     Service name: All services
     <!--NeedCopy-->
     ```

     Para obtener información sobre el perímetro de servicio de la VPC, consulte Service perimeter details and configuration.

- En el caso de una agrupación de trabajadores privados en una implementación en la nube, anexe la configuración de propiedad `<Property xsi:type="StringProperty" Name="ProxyHypervisorTrafficThroughConnector"Value="True"/>` y `<Property xsi:type="StringProperty"Name="UsePrivateWorkerPool "Value="True"/>` a `CustomProperties` para habilitar el proxy. Por ejemplo:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema
   -instance" xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation">
<Property xsi:type="StringProperty" Name="
   ProxyHypervisorTrafficThroughConnector" Value="True"/>
<Property xsi:type="StringProperty" Name="
   UsePrivateWorkerPool" Value="True"/>
</CustomProperties>
<!--NeedCopy-->
```

5. En la ventana de PowerShell, asigne una variable a las propiedades personalizadas modificadas. Por ejemplo:
   `$customProperty = '<CustomProperties...</CustomProperties>'`.
6. Ejecute `$gcpServiceAccount = "<ENTER YOUR SERVICE ACCOUNT EMAIL HERE>"`.
7. Ejecute `$gcpPrivateKey = "<ENTER YOUR SERVICE ACCOUNT PRIVATE KEY HERE AFTER REMOVING ALL INSTANCES OF \n >"`.
8. Ejecute `$securePassword = ConvertTo-SecureString $gcpPrivateKey -AsPlainText -Force`.
9. Ejecute lo siguiente para actualizar una conexión de host existente:

```
Set-Item -PassThru -Path @('XDHyp:\Connections\<ENTER YOUR
   CONNECTION NAME HERE>') -SecurePassword $securePassword -
   UserName $gcpServiceAccount -CustomProperties $customProperty
<!--NeedCopy-->
```

Permisos de GCP requeridos

En esta sección, se incluye la lista completa de permisos de GCP. Utilice el conjunto completo de permisos que se indica en la sección para que la funcionalidad opere correctamente.

> **Nota:**
>
> GCP presentará cambios en el comportamiento predeterminado de los servicios de Cloud Build y en el uso de las cuentas de servicio a partir del 29 de abril de 2024. Para obtener más información, consulte Cambio de la cuenta de servicio de Cloud Build. Los proyectos de Google existentes con la API de Cloud Build habilitada antes del 29 de abril de 2024 no se ven afectados por este cambio.

> No obstante, si quiere mantener el comportamiento actual del servicio de Cloud Build a partir del 29 de abril, puede crear o aplicar una directiva de organización para inhabilitar la aplicación de restricciones antes de habilitar la API. Si establece la nueva directiva de organización, puede seguir usando los permisos existentes en esta sección y los elementos marcados en **Antes del cambio de la cuenta de servicio de Cloud Build**. De lo contrario, sigue los permisos y elementos existentes que están marcados en **Después del cambio de cuenta de servicio de Cloud Build**.

Crear una conexión de host

- Permisos mínimos requeridos para la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning:

```
compute.instanceTemplates.list
compute.instances.list
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Administrador de procesos
  - Usuario de Cloud Datastore

- Permisos adicionales requeridos para la nube VPC compartida con la cuenta de servicio de Citrix Cloud en el proyecto de nube VPC compartida:

```
compute.networks.list
compute.subnetworks.list
resourcemanager.projects.get
<!--NeedCopy-->
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute Network User

Administración avanzada de máquinas virtuales

Permisos mínimos requeridos para la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning en el caso de catálogos solo con administración de energía:

```
compute.instanceTemplates.list
compute.instances.list
```



```
compute.instances.get
compute.instances.reset
compute.instances.resume
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.networks.list
compute.projects.get
compute.regions.list
compute.subnetworks.list
compute.zones.list
resourcemanager.projects.get
compute.zoneOperations.get
<!--NeedCopy-->
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Administrador de procesos
- Usuario de Cloud Datastore

Crear, actualizar o eliminar máquinas virtuales

- Permisos mínimos requeridos para la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
```



```
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
iam.serviceAccounts.actAs
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
compute.networks.get
compute.resourcePolicies.use
```



```
80
81  <!--NeedCopy-->
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Administrador de procesos
- Administrador de almacenamiento
- Editor de compilaciones en la nube
- Usuario de cuenta de servicio
- Usuario de Cloud Datastore

- Permisos adicionales requeridos para la nube VPC compartida con la cuenta de servicio de Citrix Cloud en el proyecto de nube VPC compartida a fin de crear una unidad de alojamiento mediante la VPC y la subred del proyecto de VPC compartida:

```
1  compute.firewalls.list
2  compute.networks.list
3  compute.projects.get
4  compute.regions.list
5  compute.subnetworks.get
6  compute.subnetworks.list
7  compute.subnetworks.use
8  compute.zones.list
9  resourcemanager.projects.get
10 <!--NeedCopy-->
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Compute Network User
- Usuario de Cloud Datastore

- (Antes del cambio de la cuenta de servicio de Cloud Build): Permisos mínimos requeridos por el servicio Google Cloud Build para la cuenta de servicio de Cloud Build en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:
- (Después del cambio de la cuenta de servicio de Cloud Build): Permisos mínimos requeridos por el servicio Google Cloud Compute para la cuenta de servicio de Cloud Compute en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

```
1  compute.disks.create
2  compute.disks.delete
3  compute.disks.get
4  compute.disks.list
5  compute.disks.setLabels
6  compute.disks.use
7  compute.disks.useReadOnly
8  compute.images.get
9  compute.images.list
10 compute.images.useReadOnly
```



```
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.getSerialPortOutput
compute.instances.list
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
logging.logEntries.create
pubsub.topics.publish
resourcemanager.projects.get
source.repos.get
source.repos.list
storage.buckets.create
storage.buckets.get
storage.buckets.list
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Cuenta de servicio de Cloud Build (después del cambio de la cuenta de servicio de Cloud Build, es una cuenta de servicio de Cloud Compute)
- Administrador de instancias de proceso
- Usuario de cuenta de servicio

- Permisos mínimos requeridos por el servicio Google Cloud Build para la cuenta de servicio de Cloud Compute en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

```
resourcemanager.projects.get
storage.objects.create
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

Estos roles definidos por Google tienen los permisos que se indican anteriormente:

- Compute Network User

  - Storage Account User
  - Usuario de Cloud Datastore

- (Antes del cambio de la cuenta de servicio de Cloud Build): Permisos adicionales requeridos por el servicio Google Cloud Build para la nube VPC compartida con la cuenta de servicio de Cloud Build en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

- (Después del cambio de la cuenta de servicio de Cloud Build): Permisos adicionales requeridos por el servicio Google Cloud Compute para la nube VPC compartida con la cuenta de servicio de Cloud Compute en el proyecto de Provisioning al descargar el disco de instrucciones de preparación en MCS:

```
compute.firewalls.list
compute.networks.list
compute.subnetworks.list
compute.subnetworks.use
resourcemanager.projects.get
<!--NeedCopy-->
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute Network User
  - Storage Account User
  - Usuario de Cloud Datastore

- Permisos adicionales requeridos para Cloud Key Management Service (KMS) con la cuenta de servicio de Citrix Cloud en el proyecto de Provisioning:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
<!--NeedCopy-->
```

  Estos roles definidos por Google tienen los permisos que se indican anteriormente:

  - Compute KMS Viewer

Permisos generales

Estos son los permisos de la cuenta de servicio de Citrix Cloud en el proyecto Provisioning para todas las funciones disponibles en MCS. Estos permisos ofrecen la mejor compatibilidad en el futuro:

```
resourcemanager.projects.get
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
```



```
compute.acceleratorTypes.list
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.setLabels
compute.disks.use
compute.disks.useReadOnly
compute.firewalls.create
compute.firewalls.delete
compute.firewalls.list
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instanceTemplates.create
compute.instanceTemplates.delete
compute.instanceTemplates.get
compute.instanceTemplates.list
compute.instanceTemplates.useReadOnly
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.reset
compute.instances.resume
compute.instances.setDeletionProtection
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.suspend
compute.instances.update
compute.instances.updateAccessConfig
compute.instances.updateDisplayDevice
compute.instances.updateSecurity
compute.instances.updateShieldedInstanceConfig
compute.instances.updateShieldedVmConfig
compute.machineTypes.get
compute.machineTypes.list
compute.networks.list
compute.networks.updatePolicy
compute.nodeGroups.list
compute.nodeTemplates.get
compute.projects.get
```



```
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.list
compute.snapshots.get
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.list
cloudkms.keyRings.get
cloudkms.keyRings.list
compute.disks.list
compute.instances.setServiceAccount
compute.networks.get
compute.networks.use
compute.networks.useExternalIp
iam.serviceAccounts.actAs
compute.resourcePolicies.use
<!--NeedCopy-->
```

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica de Google Cloud Platform (GCP), consulte Crear un catálogo de Google Cloud Platform.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de Google Cloud.

Conexión a HPE Moonshot

May 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos sobre HPE Moonshot.

> **Nota:**
>
> Antes de crear una conexión con HPE Moonshot, debe terminar de configurar su cuenta de HPE. Consulte Entornos de virtualización de HPE Moonshot.

Crear una conexión

Puede crear una conexión a HPE Moonshot mediante:

- Interfaz de Configuración completa
- Comandos de PowerShell

Crear una conexión mediante la interfaz de Configuración completa

1. En la página **Agregar conexión y recursos**, seleccione **HPE Moonshot** como tipo de conexión.
2. Introduzca la dirección de conexión de su Moonshot iLO Chassis Manager. Puede usar una dirección IP, un nombre de host o un nombre de dominio completo (FQDN) para la dirección.
3. Introduzca las credenciales administrativas del chasis y un nombre de conexión descriptivo.

La configuración de la conexión se detiene cuando se produce una de las siguientes situaciones:

- DaaS recibe un certificado firmado por una entidad de certificación pública con errores: Aparece un mensaje de error. Siga las instrucciones que aparecen en la pantalla para solucionar el problema. De lo contrario, no podrá continuar con la creación de la conexión.
- DaaS recibe un certificado firmado por una entidad de certificación privada. Aparece una página de advertencia. Compare la huella digital recibida con la del servidor para determinar la validez del certificado. Si es válido, seleccione **Confiar en el certificado** y haga clic en **Aceptar** para continuar con la creación de la conexión. A continuación, DaaS confiará en el certificado y almacenará la huella digital para su futura validación.

Crear una conexión mediante comandos de PowerShell

Al crear una conexión mediante comandos de PowerShell, proporcione la siguiente información:

- IP: Dirección IP del servidor HPE

- Username: Nombre de usuario de HPE
- Password: Contraseña de HPE

Por ejemplo:

```
New-Item -ConnectionType "Custom" -HypervisorAddress $IP -Metadata @{
 "Citrix_Orchestration_Hypervisor_Secret_Allow_Edit"="false" }
  -Path @("XDHyp:\Connections$connectionName") -Persist -PluginId "
     HPMoonshotFactory" -Scope @() -SecurePassword $Password -UserName
     $UserName -sslthumbprint $SslThumbprint New-
     BrokerHypervisorConnection -HypHypervisorConnectionUid
     $HypervisorConnectionID
<!--NeedCopy-->
```

> **Nota:**
>
> El parámetro `sslthumbprint` solo es obligatorio para los certificados firmados por una entidad de certificación privada.

Validación de certificados y huellas digitales

Para crear una conexión con **HPE Moonshot**, el certificado no debe contener errores y la huella digital debe tener un valor correcto. A continuación, se indican los casos de uso relacionados con la validación de certificados y huellas digitales:

- Certificado firmado por una entidad de certificación pública con errores. La conexión no se crea correctamente. Consulte los detalles del error y resuelva el problema.
- Certificado firmado por una entidad de certificación pública sin errores. La conexión se crea correctamente y el valor de `SslThumbprints` es **Null**.
- Certificado firmado por una entidad de certificación privada sin errores y un valor de `sslthumbprint`. La conexión se crea correctamente con un valor de `SslThumbprints` correcto.
- Certificado firmado por una entidad de certificación privada con un valor de huella digital incorrecto. La conexión no se crea correctamente.
- Certificado firmado por una entidad de certificación privada sin errores. La conexión se crea correctamente. El valor de `SSlThumbprints` es **Null** al crear la conexión. El servicio del sitio actualiza el valor de `SSlThumbprints` con un valor.

Administrar conexiones

En esta sección se detalla cómo puede administrar las conexiones:

- Corregir problemas de certificados mediante la interfaz de Configuración completa
- Actualizar el valor de la huella digital mediante un comando de PowerShell

Corregir problemas de certificados

DaaS bloquea una conexión a HPE Moonshot cuando surgen problemas con los certificados, lo que le impide entregar y administrar cargas de trabajo en los nodos de HPE Moonshot asociados. Aparecerá un icono de error junto a la conexión en la lista de **conexiones de host**. Consulte la siguiente tabla para ver problemas específicos y soluciones.

Problema	Solución
Hay un error en el certificado firmado por una entidad de certificación pública	Haga clic en la conexión y seleccione la ficha **Solucionar problemas**. Consulte los detalles del error y resuelva el problema.
El certificado recibido está firmado por una entidad de certificación privada o ha caducado.	Modifique la conexión del host para actualizar la huella digital del certificado. Pasos detallados 1. Seleccione la conexión y haga clic en **Modificar conexión**. 1. En la página **Propiedades de la conexión**, haga clic en **Modificar parámetros**. 1. Introduzca la contraseña para conectarse al chasis HPE Moonshot y, a continuación, haga clic en **Guardar**. 1. En la página de **advertencia** que aparece, compare la huella digital recibida con la del servidor para comprobar la validez del certificado. 1. Si son iguales, seleccione **Confiar en el certificado** y, a continuación, haga clic en **Aceptar**.

Actualizar el valor de la huella digital

Después de crear la conexión, puede actualizar el valor de su huella digital mediante el comando `Set-Item` de PowerShell. Por ejemplo, ejecute estos comandos:

1. Obtenga los detalles de una conexión. Por ejemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```


2. Actualice el valor de la huella digital. Por ejemplo:

```
Set-Item -LiteralPath xdhyp:\connections\SinMoonshot-101 -Username
    Administrator -SslThumbprint
   xxxxxxxxxxx12AD048480631BB7AB10D69xxxxx
<!--NeedCopy-->
```

3. Compruebe el valor actualizado de la huella digital. Por ejemplo:

```
Get-Item -LiteralPath xdhyp:\connections\SinMoonshot-101
<!--NeedCopy-->
```

> **Nota:**
>
> La actualización falla si se proporciona un valor de huella digital incorrecto en el comando `Set-Item`.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica sobre HPE Moonshot, consulte Crear un catálogo de máquinas de HPE Moonshot.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de HPE Moonshot

Conexión con Microsoft Azure

May 17, 2024

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

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de nube de Azure Resource Manager.

> **Nota:**
>
> Antes de crear una conexión con Microsoft Azure, debe terminar de configurar su cuenta de Azure como ubicación de recursos. Consulte Entornos de virtualización de Microsoft Azure Resource Manager.

Crear conexiones y entidades principales de servicio

Antes de crear conexiones, debe configurar entidades principales de servicio que las conexiones utilizan para acceder a recursos de Azure. Puede crear una conexión de dos maneras:

- Crear una entidad principal de servicio y una conexión juntos mediante Configuración completa
- Crear una conexión mediante una entidad principal de servicio creada previamente

En esta sección se muestra cómo completar estas tareas:

- Crear una entidad principal de servicio y una conexión mediante Configuración completa
- Crear una entidad principal de servicio con PowerShell
- Obtener el secreto de la aplicación en Azure
- Crear una conexión mediante una entidad principal de servicio existente

Consideraciones

Antes de empezar, tenga en cuenta lo siguiente:

- Citrix recomienda usar la entidad principal de servicio con un rol *Colaborador*. Sin embargo, consulte la sección Permisos mínimos para obtener la lista de permisos mínimos correspondientes.
- Al crear la primera conexión, Azure pide conceder a ese rol los permisos necesarios. Para conexiones futuras, aún deberá autenticarse, pero Azure recuerda su consentimiento anterior y no vuelve a mostrar la solicitud.
- Tras autenticarse en Azure por primera vez, se invita a una aplicación multiarrendatario propiedad de Citrix (ID: `08b70dc3-76c5-4611-ba7d-3312ba36cb2b`) a su instancia de Azure Active Directory en nombre de la cuenta autenticada. Si selecciona **Habilitar la administración de dispositivos unidos a Azure AD** en la página **Detalles de conexión**, Citrix usa esta aplicación para crear nuevas entidades principales de servicio y conceder los permisos adecuados para el aprovisionamiento de cargas de trabajo y para la administración de dispositivos de Azure AD.
- Las cuentas utilizadas para la autenticación deben ser de un coadministrador de la suscripción.

- La cuenta utilizada para la autenticación debe ser un miembro del directorio de suscripción. Hay dos tipos de cuentas que tener en cuenta: "cuenta profesional o educativa"y "cuenta personal de Microsoft"Para más información, consulte CTX219211.
- Puede usar una cuenta existente de Microsoft si la agrega como miembro del directorio de suscripción. Sin embargo, puede haber complicaciones si el usuario antes tenía acceso como invitado a uno de los recursos del directorio. En ese caso, puede tener una entrada de marcador de posición en el directorio que no le concederá los permisos necesarios, y se producirá un error.

  Para rectificarlo, quite los recursos del directorio y agréguelos de nuevo explícitamente. Sin embargo, use esta opción con cuidado, ya que tiene efectos no deseados para otros recursos a los que pueda acceder esta cuenta.
- Hay un problema conocido que consiste en que algunas cuentas se detectan como invitados del directorio cuando en realidad son miembros. Por regla general, configuraciones como esta se producen con las cuentas de directorio antiguas establecidas. Solución temporal: Agregue una cuenta al directorio, con el valor correcto de membresía.
- Los grupos de recursos son simplemente contenedores de recursos, y pueden contener recursos de regiones distintas a su propia región. Eso puede ser confuso si cree que los recursos que se muestran en la región de un grupo de recursos están disponibles.
- Su red y subred deben ser lo suficientemente grandes como para alojar la cantidad de máquinas que necesita. Eso requiere previsión, pero Microsoft le ayuda a especificar los valores correctos, con orientación sobre la capacidad del espacio de direcciones.

Crear una entidad principal de servicio y una conexión mediante Configuración completa

> **Importante:**
>
> Esta función aún no está disponible para las suscripciones de Azure China.

Con Configuración completa, puede crear una entidad principal de servicio y una conexión en un único flujo de trabajo. Las entidades principales de servicio permiten a las conexiones acceder a recursos de Azure. Al autenticarse en Azure para crear una entidad principal de servicio, se registra una aplicación en Azure. Se crea una clave secreta (denominada *secreto de cliente* o *secreto de aplicación*) para la aplicación registrada. La aplicación registrada (una *conexión* en este caso) usa el secreto de cliente para autenticarse en Azure AD.

Antes de empezar, asegúrese de cumplir estos requisitos previos:

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

- Tiene permisos de administrador global, administrador de aplicaciones o desarrollador de aplicaciones para la autenticación. Los permisos se pueden revocar después de crear una conexión de host. Para obtener más información sobre los roles, consulte Roles integrados de Azure AD.

Utilice el asistente **Agregar conexiones y recursos** para crear una entidad principal de servicio y una conexión juntos:

1. En la página **Conexión**, seleccione **Crear una conexión**, el tipo de conexión **Microsoft Azure** y su entorno de Azure.
2. Seleccione las herramientas a utilizar para crear las máquinas virtuales y, a continuación, seleccione **Siguiente**.
3. En la página **Detalles de la conexión**, cree una entidad principal de servicio y defina el nombre de la conexión de la siguiente manera:

   a) Para conceder el permiso de conexión para limpiar automáticamente los dispositivos obsoletos unidos a Azure AD, seleccione **Habilitar la administración de dispositivos unidos a Azure AD**. Le recomendamos que seleccione esta opción si quiere crear máquinas unidas a Azure AD a través de esta conexión. Para obtener más información, consulte Habilitar la administración de dispositivos unidos a Azure AD.

   b) Introduzca el ID de suscripción de Azure y un nombre para la conexión. Después de introducir el ID de suscripción, se habilita el botón **Crear**.

   > **Nota:**
   >
   > El nombre de conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco o los caracteres `\/;:#.*?=<>|[]{ } "'()'`.

   a) Seleccione **Crear** e introduzca el nombre de usuario y la contraseña de la cuenta de Azure Active Directory.

   b) Seleccione **Iniciar sesión**.

   c) Seleccione **Aceptar** para conceder a Citrix DaaS los permisos mostrados. Azure crea una entidad principal de servicio que permite a Citrix DaaS administrar recursos de Azure en nombre del usuario especificado.

   d) Tras seleccionar **Aceptar**, volverá a la página **Detalles de la conexión**.

   > **Nota:**
   >
   > Después de autenticarse correctamente en Azure, desaparecen los botones **Crear** y **Usar existente**. Aparece el texto **Conexión correcta**, con una marca de verificación verde que indica la conexión correcta a su suscripción de Azure.

e) Para redirigir solicitudes de API a Azure a través de Citrix Cloud Connectors, marque la casilla **Redirigir tráfico a través de Citrix Cloud Connectors**.

Como alternativa, puede habilitar esta función mediante PowerShell. Para obtener más información, consulte Crear un entorno seguro para el tráfico administrado de Azure.

> **Nota:**
>
> Esta opción solo está disponible cuando hay Citrix Cloud Connectors activos en la implementación. Actualmente, esta función no es compatible con Connector Appliances.

f) Seleccione **Siguiente**.

> **Nota:**
>
> No puede pasar a la página siguiente hasta que se haya autenticado correctamente en Azure y haya dado su consentimiento para otorgar los permisos necesarios.

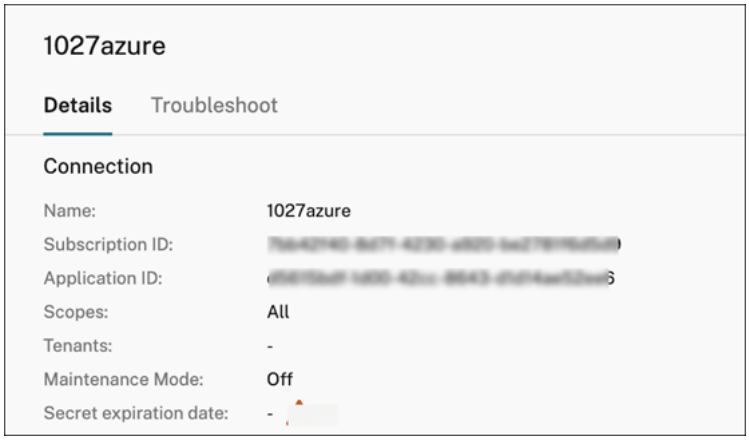
4. Configure los recursos para la conexión de la siguiente manera:

   - En la página **Región**, seleccione una región.
   - En la página **Red**, haga lo siguiente:
     - Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red. El nombre de un recurso no puede contener solo espacios en blanco ni los caracteres `\/;:#.*?=<>|[]{ } "'()'`.
     - Seleccione un par de red virtual y grupo de recursos (si tiene más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas). Si en la página anterior seleccionó una región que no tiene redes virtuales, vuelva a esa página y seleccione una región que las tenga.

5. En la página **Resumen**, verá un resumen de los parámetros. Seleccione **Finalizar** para completar la configuración.

Ver el ID de la aplicación Después de crear una conexión, puede ver el ID de aplicación que la conexión usa para acceder a los recursos de Azure.

En la lista **Agregar conexión y recursos**, seleccione la conexión para ver los detalles. La ficha **Detalles** muestra el ID de la aplicación.



Crear una entidad principal de servicio con PowerShell

Para crear una entidad principal de servicio con PowerShell, conéctese a su suscripción de Azure Resource Manager y use los siguientes cmdlets de PowerShell que se proporcionan en las siguientes secciones.

Asegúrese de tener preparados estos elementos:

- **SubscriptionId:** `SubscriptionID` de Azure Resource Manager perteneciente a la suscripción donde quiere aprovisionar los agentes VDA.
- **ActiveDirectoryID**: ID de arrendatario de la aplicación que registró en Azure AD.
- **ApplicationName:** Nombre de la aplicación que se va a crear en Azure AD.

Estos son los pasos detallados:

1. Conéctese a su suscripción de Azure Resource Manager.

   ```
   Connect-AzAccount
   ```

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

   ```
   Get-AzSubscription -SubscriptionId $subscriptionId | Select-
   AzSubscription
   ```

3. Cree la aplicación en su arrendatario de AD.

   ```
   $AzureADApplication = New-AzADApplication -DisplayName $ApplicationName
   ```

4. Cree una entidad principal de servicio.

   ```
   New-AzADServicePrincipal -ApplicationId $AzureADApplication.AppId
   ```

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


```
New-AzRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName
 $AzureADApplication.AppId –scope /subscriptions/$SubscriptionId
```

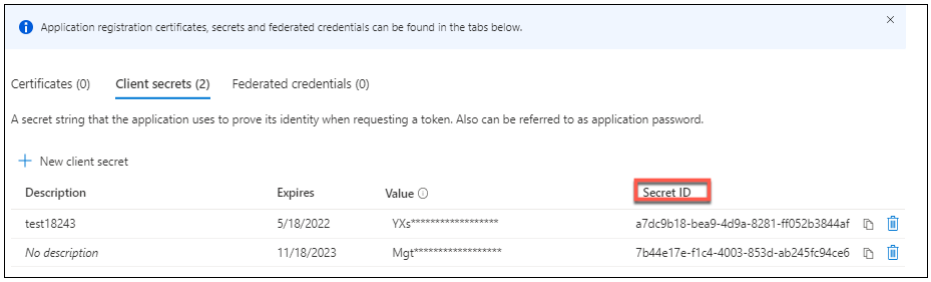
6. En la ventana de resultados de la consola de PowerShell, anote el ID de aplicación (ApplicationId). Debe proporcionar ese ID cuando cree la conexión de host.

Obtener el secreto de la aplicación en Azure

Para crear una conexión mediante una entidad principal de servicio existente, primero debe obtener el ID de la aplicación y el secreto de la entidad principal del servicio en Azure Portal.

Estos son los pasos detallados:

1. Obtenga el **ID de aplicación** desde la interfaz de Configuración completa o mediante PowerShell.
2. Inicie sesión en Azure Portal.
3. En Azure, seleccione **Azure Active Directory**.
4. En **Registros de aplicaciones**, en Azure AD, seleccione su aplicación.
5. Vaya a **Certificados y secretos**.
6. Haga clic en **Secretos del cliente**.



Crear una conexión mediante una entidad principal de servicio existente

Si ya tiene una entidad principal de servicio, puede usarla para crear una conexión mediante Configuración completa.

Asegúrese de tener estos elementos listos:

- SubscriptionId
- ActiveDirectoryID (ID de arrendatario).
- ID de aplicación
- Secreto de la aplicación

  Para obtener más información, consulte Obtener el secreto de la aplicación.

- Fecha de caducidad del secreto

Estos son los pasos detallados:

En el asistente **Agregar conexión y recursos**:

1. En la página **Conexión**, seleccione **Crear una conexión**, el tipo de conexión **Microsoft Azure** y su entorno de Azure.
2. Seleccione las herramientas a utilizar para crear las máquinas virtuales y, a continuación, seleccione **Siguiente**.
3. En la página **Detalles de conexión**, escriba su ID de suscripción de Azure y un nombre para la conexión.

   > **Nota:**
   >
   > El nombre de conexión puede contener de 1 a 64 caracteres, y no puede contener solo espacios en blanco o los caracteres `\/;:#.*?=<>|[]{ } "'()'`.

4. Seleccione **Usar existente**. En la ventana **Detalles de entidad principal de servicio existente**, introduzca estos parámetros para la entidad principal de servicio existente. Después de introducir la información, se habilitará el botón **Guardar**. Seleccione **Guardar**. No puede avanzar más allá de esta página hasta que haya proporcionado detalles válidos.

   - **ID de suscripción**. Introduzca el ID de su suscripción de Azure. Para obtener su ID de suscripción, inicie sesión en Azure Portal y vaya a **Suscripciones > Vista general**.
   - **ID de Active Directory** (ID de arrendatario). Escriba el ID del directorio (arrendatario) de la aplicación con la que se registró en Azure AD.
   - **ID de la aplicación**. Escriba el ID de la aplicación (cliente) con la que se registró en Azure AD.
   - **Secreto de la aplicación**. Introduzca una clave secreta (secreto de cliente). La aplicación registrada utiliza la clave para autenticarse en Azure AD. Le recomendamos cambiar las claves con frecuencia por motivos de seguridad. Asegúrese de guardar la clave porque no podrá recuperarla más tarde.
   - **Fecha de caducidad del secreto**. Introduzca la fecha en la cual caduca el secreto de la aplicación. Recibirá una alerta en la consola antes de que caduque la clave secreta. Sin embargo, si la clave secreta caduca, recibirá errores.

     > **Nota:**
     >
     > Por motivos de seguridad, el período de caducidad no puede ser superior a dos años a partir de ahora.

   - **URL de autenticación**. Este campo se rellena automáticamente y no se puede modificar.

- **URL de administración**. Este campo se rellena automáticamente y no se puede modificar.
- **Sufijo de almacenamiento**. Este campo se rellena automáticamente y no se puede modificar.

  Se requiere acceso a los siguientes dispositivos de punto final para crear un catálogo de MCS en Azure. El acceso a estos dispositivos de punto final optimiza la conectividad entre la red local y Azure Portal y sus servicios.

  - URL de autenticación: https://login.microsoftonline.com/
  - URL de administración: https://management.azure.com/ Esta es una URL de solicitud para las API del proveedor de Azure Resource Manager. El dispositivo de punto final para la administración depende del entorno. Por ejemplo: para Azure Global es https://management.azure.com/ y, para Azure US Government, https://management.usgovcloudapi.net/.
  - Sufijo de almacenamiento: https://*.core.windows.net./ Este (*) es un carácter comodín para el sufijo de almacenamiento. Por ejemplo, https://demo.table.core.windows.net/.

5. Tras seleccionar **Guardar**, volverá a la página **Detalles de conexión**. Seleccione **Siguiente** para pasar a la página siguiente.
6. Configure los recursos para la conexión de la siguiente manera:

   - En la página **Región**, seleccione una región.
   - En la página **Red**, haga lo siguiente:
     - Escriba un nombre de recurso de 1 a 64 caracteres para identificar más fácilmente la combinación de región y red. El nombre de un recurso no puede contener solo espacios en blanco ni los caracteres `\/;:#.*?=<>|[]{ } "'()'`.
     - Seleccione un par de red virtual y grupo de recursos (si tiene más de una red virtual con el mismo nombre, emparejar un nombre de red con un grupo de recursos ofrece combinaciones únicas). Si en la página anterior seleccionó una región que no tiene redes virtuales, vuelva a esa página y seleccione una región que las tenga.
7. En la página **Resumen**, verá un resumen de los parámetros. Seleccione **Finalizar** para completar la configuración.

Administrar entidades principales de servicio y conexiones

En esta sección se detalla cómo puede administrar entidades principales de servicio y conexiones:

- Configurar parámetros de limitación de Azure
- Habilitar la administración de dispositivos unidos a Azure AD
- Administrar la entidad principal de servicio de una conexión de host existente

- Habilitar el uso compartido de imágenes en Azure
- Agregar arrendatarios compartidos a una conexión mediante la Configuración completa
- Implementar el uso compartido de imágenes con PowerShell
- Crear un entorno seguro para el tráfico administrado de Azure
- Administrar el secreto de aplicación y la fecha de caducidad del secreto

Configurar parámetros de limitación de Azure

Azure Resource Manager limita las solicitudes de suscripciones y arrendatarios mediante la redirección del tráfico en función de límites definidos y adaptada a las necesidades específicas del proveedor. Consulte Limitación de solicitudes de Resource Manager en el sitio de Microsoft para obtener más información. Existen límites para las suscripciones y los arrendatarios, donde administrar muchas máquinas podría resultar problemático. Por ejemplo: es posible que una suscripción que contenga muchas máquinas sufra problemas de rendimiento relacionados con las operaciones de energía.

> **Sugerencia:**
>
> Para obtener más información, consulte Mejora del rendimiento de Azure con Machine Creation Services.

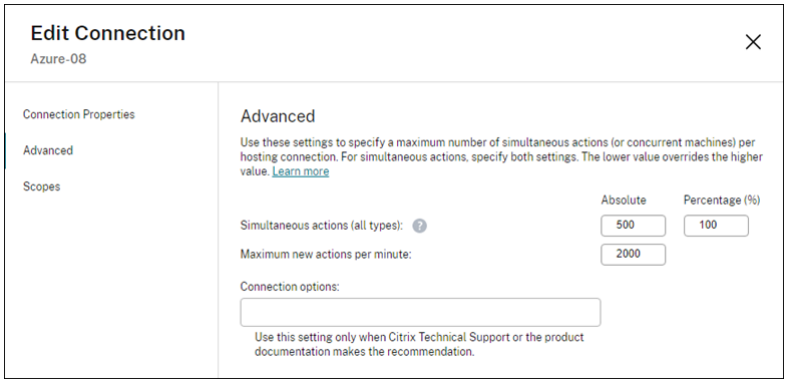
Para ayudar a mitigar estos problemas, Citrix DaaS permite quitar la limitación interna de MCS para usar más cuota de solicitudes disponible de Azure.

Le recomendamos la siguiente configuración óptima al encender o apagar máquinas virtuales en suscripciones grandes, como, por ejemplo, aquellas que contengan 1000 máquinas virtuales:

- Operaciones simultáneas absolutas: 500
- Máximo de nuevas operaciones por minuto: 2000
- Máximo de operaciones simultáneas: 500

Para usar la interfaz de Configuración completa en la configuración de operaciones de Azure para una conexión de host determinada:

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione una conexión relacionada con Azure para modificarla.
3. En el asistente **Modificar conexión**, seleccione **Avanzado**.
4. En la página **Avanzado**, utilice las opciones de configuración para especificar la cantidad de acciones simultáneas y el máximo de acciones nuevas por minuto y las opciones de conexión adicionales.



MCS admite un máximo de 500 operaciones simultáneas de forma predeterminada. De forma alternativa, puede utilizar el SDK de PowerShell remoto para establecer el máximo de operaciones simultáneas.

Utilice la propiedad de **PowerShell** `MaximumConcurrentProvisioningOperations` para especificar el máximo de operaciones simultáneas de aprovisionamiento de Azure. Al usar esta propiedad, tenga en cuenta lo siguiente:

- El valor predeterminado de `MaximumConcurrentProvisioningOperations` es 500.
- Configure el parámetro `MaximumConcurrentProvisioningOperations` mediante el comando `Set-item` de PowerShell.

Habilitar la administración de dispositivos unidos a Azure AD

Los dispositivos obsoletos unidos a Azure AD en Azure pueden impedir que se unan nuevas máquinas y que no funcionen correctamente. Para evitar posibles problemas, puede conceder el permiso de conexión para administrar los dispositivos unidos a Azure AD. Con este permiso, las conexiones pueden limpiar automáticamente los dispositivos obsoletos unidos a Azure AD.

> **Nota:**
>
> Los dispositivos unidos a Azure AD no se pueden eliminar de Azure AD al eliminar máquinas o catálogos de máquinas.

1. En **Administrar > Configuración completa**, seleccione Alojamiento en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en la barra de acciones.
3. Seleccione **Propiedades de la conexión** en el panel izquierdo.
4. En la página **Propiedades de la conexión** que aparece, siga estos pasos:
    a) Seleccione **Habilitar la administración de dispositivos unidos a Azure AD**.
    b) Haga clic en **Guardar**.

c) En la ventana de inicio de sesión de Azure que aparece, introduzca la contraseña de la suscripción y, a continuación, haga clic en **Iniciar sesión**.

Una vez completado el inicio de sesión, volverá a aparecer la lista de conexiones y recursos de alojamiento. Haga clic en la conexión de la lista y, a continuación, haga clic en la ficha **Detalles** del panel inferior. Podrá ver que, en el campo **Administración de dispositivos unidos de Azure AD**, se muestra **Habilitado**.

Al habilitar la administración de dispositivos unidos a Azure AD con Configuración completa, debe autenticarse con Azure AD, independientemente del método de creación de conexiones de host que elija (crear una nueva o usar la existente). El rol **Administrador de dispositivos en la nube** integrado en Azure AD se asigna a la entidad principal de servicio. Para adoptar los permisos mínimos para la administración de dispositivos unidos a Azure AD, puede quitar manualmente la asignación del rol **Administrador de dispositivos en la nube** a la entidad principal de servicio y crear un rol personalizado de Azure AD que solo incluya los permisos mínimos y asignarlo a la entidad principal de servicio.

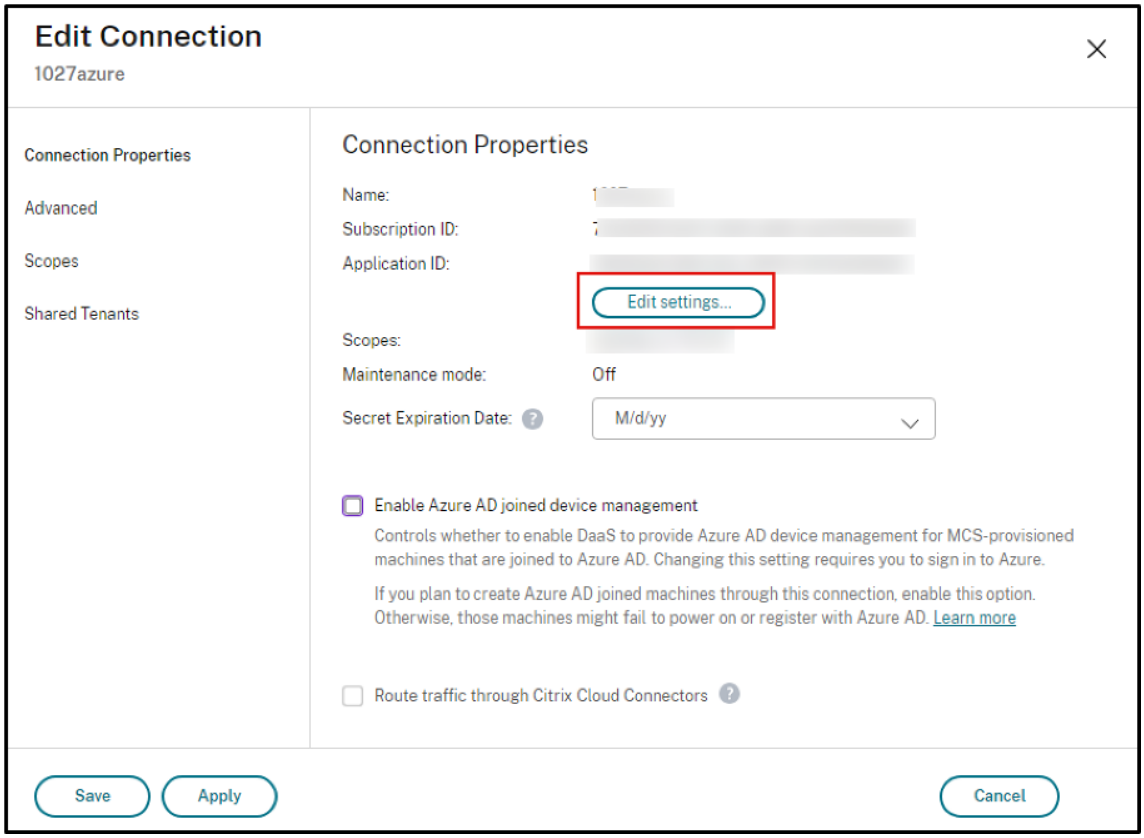
> **Nota:**
>
> - Los permisos mínimos para la administración de dispositivos unidos a Azure AD son los permisos de Azure AD y no los permisos de Azure Resource Manager. No se pueden asignar explícitamente a una entidad principal de servicio. Debe crear un rol personalizado en Azure AD que incluya esos permisos y asignarlo a la entidad principal de servicio. Para obtener más información, consulte Create and assign a custom role in Azure Active Directory.
> - Para crear un rol personalizado en Azure AD, necesita una licencia Premium P1 o P2 de Azure AD.

Administrar la entidad principal de servicio de una conexión de host existente

Después de crear una conexión de host mediante una entidad principal de servicio, puede modificar dicha conexión para que:

- Tenga una nueva entidad principal de servicio
- Use otra entidad principal de servicio

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en la barra de acciones.
3. Seleccione **Propiedades de la conexión** en el panel izquierdo.
4. En la página **Propiedades de la conexión**, haga clic en **Modificar parámetros**. Ahora puede optar por crear una nueva entidad principal de servicio o por usar otra entidad principal de servicio existente.



- Haga clic en **Crear entidad principal de servicio** para crear una. Siga las instrucciones para iniciar sesión en su cuenta de usuario de Azure AD. Citrix usa el ID de la aplicación multiarrendatario `08b70dc3-76c5-4611-ba7d-3312ba36cb2b` para crear una nueva entidad principal de servicio para la conexión de host existente y conceder los permisos adecuados.

  Si selecciona **Habilitar la administración de dispositivos unidos a Azure AD** en la página **Propiedades de la conexión**, se asigna el rol de administrador de dispositivos en la nube integrado de Azure AD a la entidad principal de servicio recién creada.

- Haga clic en **Usar existente** para usar otra entidad principal de servicio para esa conexión de host. Sin embargo, hay dos supuestos:

  - Si selecciona **Habilitar la administración de dispositivos unidos a Azure AD**, se le pedirá que inicie sesión en su cuenta de usuario de Azure AD. Citrix usa el ID de la aplicación multiarrendatario `08b70dc3-76c5-4611-ba7d-3312ba36cb2b` para asignar el rol de administrador de dispositivos en la nube integrado de Azure AD a la entidad principal de servicio existente.
  - Si no selecciona **Habilitar la administración de dispositivos unidos a Azure AD**, no se le pedirá que inicie sesión en su cuenta de usuario de Azure AD. Introduzca el ID y el secreto de la aplicación para la entidad principal de servicio existente.

Para obtener información sobre cómo habilitar la administración de dispositivos unidos a Azure AD, consulte Habilitar la administración de dispositivos unidos a Azure AD.

Habilitar el uso compartido de imágenes en Azure

Al crear o actualizar catálogos de máquinas, puede seleccionar imágenes compartidas de diferentes suscripciones y arrendatarios de Azure (compartidas a través de Azure Compute Gallery). Para habilitar el uso compartido de imágenes con o entre arrendatarios, debe hacer los ajustes necesarios en Azure:

- Compartir imágenes con un arrendatario (entre suscripciones)
- Compartir imágenes entre arrendatarios

Compartir imágenes con un arrendatario (entre suscripciones) Para seleccionar una imagen de Azure Compute Gallery que pertenezca a una suscripción diferente, la imagen debe compartirse con la entidad principal de servicio (SPN) de esa suscripción.

Por ejemplo: si hay una entidad principal de servicio (SPN 1) que está configurada en Studio como:

Entidad principal de servicio: SPN 1

Suscripción: suscripción 1

Arrendatario: arrendatario 1

La imagen está en una suscripción diferente, que está configurada en Studio como:

Suscripción: suscripción 2

Arrendatario: arrendatario 1

Si quiere compartir la imagen de la suscripción 2 con la suscripción 1 (SPN 1), vaya a la suscripción 2 y comparta el grupo de recursos con SPN 1.

La imagen debe compartirse con otro SPN mediante control de acceso por roles (RBAC) de Azure. Azure RBAC es el sistema de autorización que se utiliza para administrar el acceso a los recursos de Azure. Para obtener más información sobre Azure RBAC, consulte el documento de Microsoft What is Azure role-based access control (Azure RBAC). Para conceder acceso, asigne roles a las entidades principales de servicio en el ámbito del grupo de recursos con el rol Colaborador. Para asignar roles de Azure, debe tener el permiso `Microsoft.Authorization/roleAssignments/write`, como administrador de acceso de usuario o propietario. Para obtener más información sobre cómo compartir imágenes con otro SPN, consulte el documento de Microsoft Assign Azure roles using the Azure portal.

Compartir imágenes entre arrendatarios Para compartir imágenes entre arrendatarios con Azure Compute Gallery, cree un registro de aplicaciones.

Por ejemplo, si hay dos arrendatarios (arrendatario 1 y arrendatario 2) y quiere compartir su galería de imágenes con el arrendatario 1, entonces:

1. Cree un registro de aplicaciones para el arrendatario 1. Para obtener más información, consulte Create the app registration.
2. Permita que el arrendatario 2 acceda a la aplicación mediante una solicitud de inicio de sesión con explorador web. Sustituya `Tenant2 ID` por el ID del arrendatario 1. Sustituya `Application (client)ID` por el ID de la aplicación del registro de aplicaciones que creó. Cuando haya terminado con las sustituciones, pegue la URL en un explorador web y siga las instrucciones de inicio de sesión para iniciar sesión en el arrendatario 2. Por ejemplo:

   ```
   https://login.microsoftonline.com/<Tenant 2 ID>/oauth2/authorize?
      client_id=<Application (client) ID>&response_type=code&
      redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F
   <!--NeedCopy-->
   ```

   Para obtener más información, consulte Give Tenant 2 access.
3. Permita a la aplicación acceder al grupo de recursos del arrendatario 2. Inicie sesión como el arrendatario 2 y otorgue acceso al registro de aplicaciones para el grupo de recursos que contiene la imagen de la galería. Para obtener más información, consulte Authenticate requests across tenants.

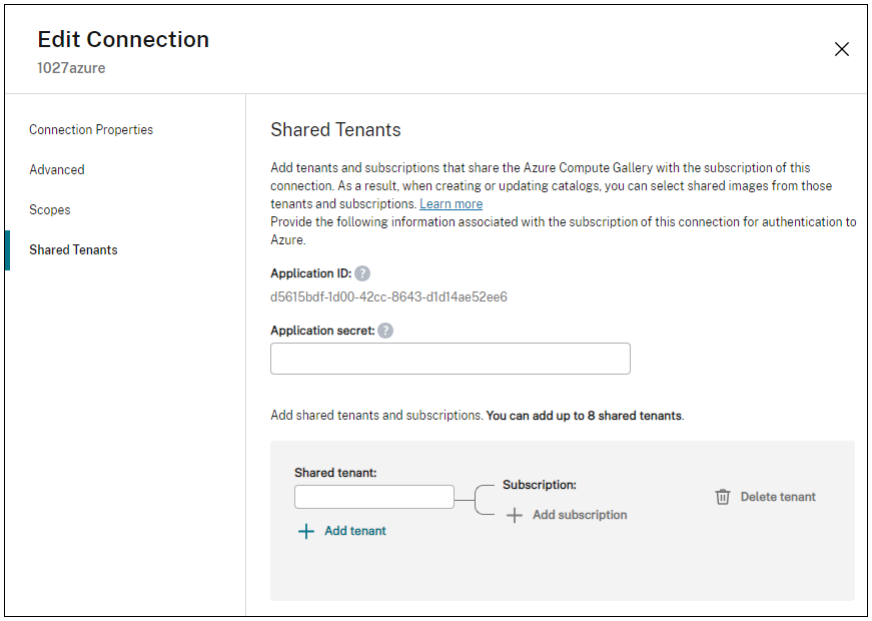
Agregar arrendatarios compartidos a una conexión mediante la Configuración completa

Al crear o actualizar catálogos de máquinas en la interfaz Configuración completa, puede seleccionar imágenes compartidas de diferentes suscripciones y arrendatarios de Azure (compartidas a través de Azure Compute Gallery). La función requiere que proporcione información compartida sobre la suscripción y los arrendatarios compartidos para las conexiones de host asociadas.

> **Nota:**
>
> Asegúrese de haber configurado los ajustes necesarios en Azure para permitir el uso compartido de imágenes entre arrendatarios. Para obtener más información, consulte Compartir imágenes entre arrendatarios.

Complete estos pasos para establecer una conexión:

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Seleccione la conexión y, a continuación, seleccione **Modificar conexión** en la barra de acciones.



3. En **Shared Tenants**, haga lo siguiente:

   a) Proporcione el ID de la aplicación y el secreto de la aplicación asociados a la suscripción de la conexión. DaaS usa esta información para autenticarse en Azure AD.
   b) Agregue arrendatarios y suscripciones que compartan Azure Compute Gallery con la suscripción de la conexión. Puede agregar hasta ocho arrendatarios compartidos y ocho suscripciones por cada arrendatario.

4. Cuando haya terminado, seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

Implementar el uso compartido de imágenes con PowerShell

Esta sección le guiará a través de los procesos para compartir imágenes con PowerShell:

- Seleccionar una imagen de una suscripción diferente
- Actualizar las propiedades personalizadas de la conexión de host con identificadores de arrendatarios compartidos
- Seleccionar una imagen de otro arrendatario

Seleccionar una imagen de una suscripción diferente Puede seleccionar una imagen en Azure Compute Gallery que pertenezca a una suscripción compartida diferente del mismo arrendatario de Azure para crear y actualizar catálogos de MCS mediante los comandos de PowerShell.

1. En la carpeta raíz de la unidad de alojamiento, Citrix crea una nueva carpeta de suscripción compartida llamada `sharedsubscription`.

2. Enumere todas las suscripciones compartidas de un arrendatario.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\sharedsubscription.
    folder"
<!--NeedCopy-->
```

3. Seleccione una suscripción compartida y, a continuación, enumere todos los grupos de recursos compartidos de esa suscripción compartida.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription"
<!--NeedCopy-->
```

4. Seleccione un grupo de recursos y, a continuación, enumere todas las galerías de ese grupo de recursos.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\ xyz.resourcegroup"
<!--NeedCopy-->
```

5. Seleccione una galería y, a continuación, enumere todas las definiciones de imágenes de esa galería.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\testgallery.gallery"
<!--NeedCopy-->
```

6. Seleccione una definición de imagen y, a continuación, enumere todas las versiones de imagen de esa definición de imagen.

```
Get-ChildItem -Path "XDhyp:\HostingUnits\azres\image.folder\abc123
    .sharedsubscription\xyz.resourcegroup\sigtestdef.
    imagedefinition"
<!--NeedCopy-->
```

7. Cree y actualice un catálogo de MCS con los siguientes elementos:

   - Resource group
   - Galería
   - Definición de imagen de la galería
   - Versión de la imagen de la galería

   Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Actualizar las propiedades personalizadas de la conexión de host con identificadores de arrendatarios compartidos Use `Set-Item` para actualizar las propiedades personalizadas de la conex-

ión de host con un ID de arrendatario y un ID de suscripción compartidos. Agregue una propiedad `SharedTenants` en `CustomProperties`. El formato de `Shared Tenants` es:

```
[{
 "Tenant":"94367291-119e-457c-bc10-25337231f7bd","Subscriptions":["7
    bb42f40-8d7f-4230-a920-be2781f6d5d9"] }
 ,{
 "Tenant":"50e83564-c4e5-4209-b43d-815c45659564","Subscriptions":["06
    ab8944-6a88-47ee-a975-43dd491a37d0"] }
 ]
<!--NeedCopy-->
```

Por ejemplo:

```
Set-Item -CustomProperties "<CustomProperties xmlns=`"http://schemas.
   citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
   /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`" Value=`"
   123`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`" Value
   =`"https://management.azure.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"AuthenticationAuthority`"
   Value=`"https://login.microsoftonline.com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value=`"
   core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"123abc`
   " />
<Property xsi:type=`"StringProperty`" Name=`"SharedTenants`" Value=`"`[
    {
  'Tenant':'123abc', 'Subscriptions':['345', '567']  }
  ]`"` />
</CustomProperties>"
-LiteralPath @("XDHyp:\Connections\aazure") -PassThru -UserName "
   advc345" -SecurePassword
$psd
<!--NeedCopy-->
```

> **Nota:**
>
> Puede agregar más de un arrendatario. Cada arrendatario puede tener más de una suscripción.

Seleccionar una imagen de otro arrendatario Puede seleccionar una imagen en Azure Compute Gallery que pertenezca a otro arrendatario de Azure para crear y actualizar catálogos de MCS mediante comandos de PowerShell.

1. En la carpeta raíz de la unidad de alojamiento, Citrix crea una nueva carpeta de suscripción compartida llamada `sharedsubscription`.
2. Enumere todas las suscripciones compartidas.

```
Get-ChildItem XDHyp:\HostingUnits\azres\sharedsubscription.folder
```



```
<!--NeedCopy-->
```

3. Seleccione una suscripción compartida y, a continuación, enumere todos los grupos de recursos compartidos de esa suscripción compartida.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
   sharedsubscription
<!--NeedCopy-->
```

4. Seleccione un grupo de recursos y, a continuación, enumere todas las galerías de ese grupo de recursos.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
   sharedsubscription\ xyz.resourcegroup
<!--NeedCopy-->
```

5. Seleccione una galería y, a continuación, enumere todas las definiciones de imágenes de esa galería.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
   sharedsubscription\xyz.resourcegroup\efg.gallery
<!--NeedCopy-->
```

6. Seleccione una definición de imagen y, a continuación, enumere todas las versiones de imagen de esa definición de imagen.

```
Get-ChildItem XDHyp:\HostingUnits\azres\image.folder\abc123.
   sharedsubscription\xyz.resourcegroup\efg.gallery\hij.
   imagedefinition
<!--NeedCopy-->
```

7. Cree y actualice un catálogo de MCS con los siguientes elementos:

   - Resource group
   - Galería
   - Definición de imagen de la galería
   - Versión de la imagen de la galería

   Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Crear un entorno seguro para el tráfico administrado de Azure

MCS permite que el tráfico de red (llamadas de API desde Citrix Cloud al hipervisor de Azure) se redirija a través de los Cloud Connectors de su entorno. Esta implementación le ayuda a bloquear su suscripción de Azure para permitir el tráfico de red desde direcciones IP específicas. Para ello, agregue

`ProxyHypervisorTrafficThroughConnector` en `CustomProperties`. Después de configurar las propiedades personalizadas, puede configurar las directivas de Azure para tener acceso a discos privados con los discos administrados de Azure.

Si configura la directiva de Azure para crear accesos a disco automáticamente para que cada disco nuevo utilice dispositivos de punto final privados, no podrá cargar ni descargar más de cinco discos o instantáneas al mismo tiempo con el mismo objeto de acceso a disco que exige Azure. Este límite es para cada catálogo de máquinas si configura la directiva de Azure al nivel de grupo de recursos, y para todos los catálogos de máquinas si configura la directiva de Azure al nivel de suscripción.
Si no configura la directiva de Azure para crear accesos a disco automáticamente para que cada disco nuevo utilice dispositivos de punto final privados, no se aplicará el límite de cinco operaciones simultáneas.

> **Nota:**
>
> Actualmente, esta función no es compatible con Connector Appliance. Para conocer las limitaciones de Azure relacionadas con esta función, consulte Restrict import/export access for managed disks using Azure Private Link.

Habilitar el proxy Para habilitar el proxy, defina las propiedades personalizadas de esta manera en la conexión de host:

1. Abra una ventana de PowerShell con Remote PowerShell SDK. Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-daas/sdk-api.html#citrix-virtual-apps-and-desktops-remote-powershell-sdk/.
2. Ejecute los comandos siguientes:

```
Add-PSSnapin citrix*.
cd XDHyp:\Connections\
dir
<!--NeedCopy-->
```

3. Copie `CustomProperties` de la conexión a un bloc de notas y agréguele el parámetro de propiedad `<Property xsi:type="StringProperty"Name="ProxyHypervisorTrafficThr "Value="True"/>` a `CustomProperties` para habilitar el proxy. Por ejemplo:

```
<CustomProperties xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance" xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value="
    4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
```



```
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>
<!--NeedCopy-->
```

4. En la ventana de PowerShell, asigne una variable a las propiedades personalizadas modificadas. Por ejemplo:

```
$customProperty = '<CustomProperties xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance" xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation">
<Property xsi:type="StringProperty" Name="SubscriptionId" Value
    ="4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx" />
<Property xsi:type="StringProperty" Name="ManagementEndpoint"
    Value="https://management.azure.com/" />
<Property xsi:type="StringProperty" Name="AuthenticationAuthority"
     Value="https://login.microsoftonline.com/" />
<Property xsi:type="StringProperty" Name="StorageSuffix" Value="
    core.windows.net" />
<Property xsi:type="StringProperty" Name="TenantId" Value="5cxxxxx
    -9xxx-4xxx-8xxx-dffe3efdxxxx" />
<Property xsi:type="StringProperty" Name="
    ProxyHypervisorTrafficThroughConnector" Value="True" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Ejecute `$cred = Get-Credential`. Si se le solicita, proporcione las credenciales de conexión. Las credenciales son el ID de aplicación y el secreto de Azure.

6. Ejecute `Set-Item -PSPath XDHyp:\Connections\<Connection_Name> -CustomProperties $customProperty -username $cred.username -Securepassword $cred.password`.

> **Importante:**
>
> Si recibe un mensaje que indica que falta `SubscriptionId`, sustituya todas las comillas dobles (“) por comillas simples invertidas seguidas de comillas dobles (“”) en la propiedad personalizada. Por ejemplo:

```
<CustomProperties xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
    instance`" xmlns=`"http://schemas.citrix.com/2014/xd/
    machinecreation`">
<Property xsi:type=`"StringProperty`" Name=`"SubscriptionId`"
    Value=`"4991xxxx-2xxx-4xxx-8xxx-ff59a830xxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"ManagementEndpoint`"
    Value=`"https://management.azure.com/`" />
```



```
<Property xsi:type=`"StringProperty`" Name=`"
    AuthenticationAuthority`" Value=`"https://login.microsoftonline
    .com/`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageSuffix`" Value
    =`"core.windows.net`" />
<Property xsi:type=`"StringProperty`" Name=`"TenantId`" Value=`"5
    cxxxxx-9xxx-4xxx-8xxx-dffe3efdxxxx`" />
<Property xsi:type=`"StringProperty`" Name=`"
    ProxyHypervisorTrafficThroughConnector`" Value=`"True`" />
</CustomProperties>
<!--NeedCopy-->
```

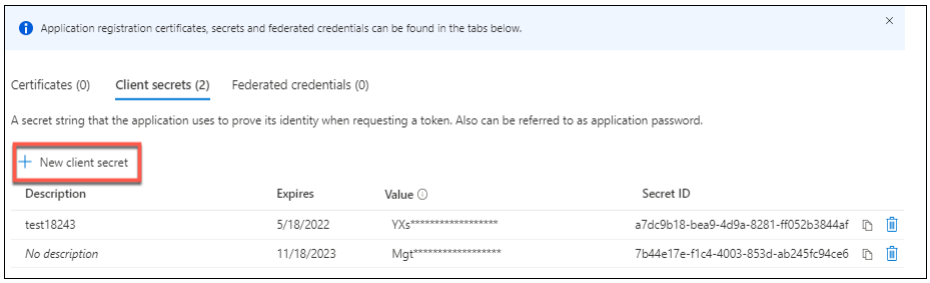
7. Ejecute `dir` para comprobar los parámetros actualizados de `CustomProperties`.

Administrar el secreto de aplicación y la fecha de caducidad del secreto

Asegúrese de cambiar el secreto de aplicación para una conexión antes de que caduque. Recibirá una alerta en la interfaz de Configuración completa antes de que caduque la clave secreta.

Crear un secreto de aplicación en Azure Puede crear un secreto de aplicación para una conexión a través de Azure Portal.

1. Seleccione **Azure Active Directory**.
2. En **Registros de aplicaciones**, en Azure AD, seleccione su aplicación.
3. Vaya a **Certificados y secretos**.
4. Haga clic en **Secretos de cliente > Nuevo secreto de cliente**.



5. Proporcione una descripción del secreto y especifique una duración. Cuando haya terminado, seleccione **Agregar**.

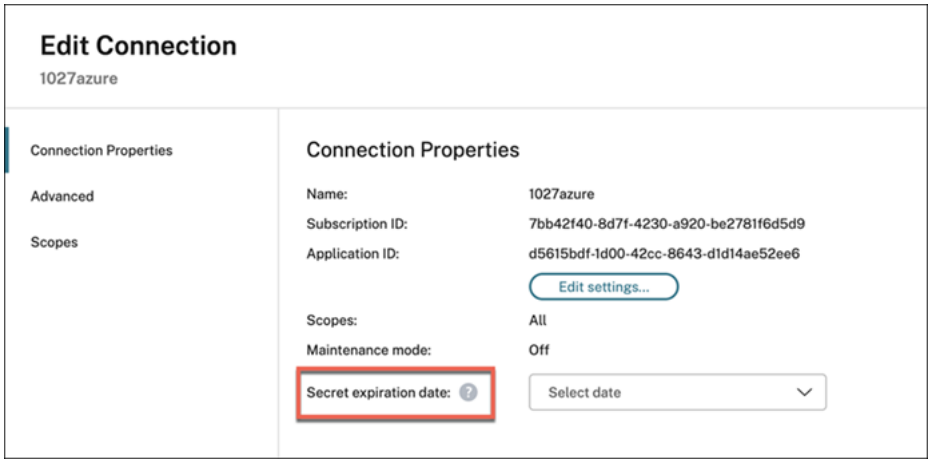
> **Nota:**
>
> Guarde el secreto de cliente porque no podrá recuperarlo más tarde.

6. Copie el valor del secreto del cliente y la fecha de caducidad.

7. En la interfaz de Configuración completa, modifique la conexión correspondiente y sustituya el contenido de los campos **Secreto de la aplicación** y **Fecha de caducidad del secreto** por los valores copiados.

Cambiar la fecha de caducidad del secreto Puede usar la interfaz de Configuración completa para agregar o modificar la fecha de caducidad del secreto de la aplicación en uso.

1. En el asistente **Agregar conexión y recursos**, haga clic con el botón secundario en una conexión y haga clic en **Modificar conexión**.
2. En la página **Propiedades de conexión**, haga clic en **Fecha de caducidad del secreto** para agregar o modificar la fecha de caducidad del secreto de la aplicación en uso.



Permisos de Azure requeridos

En esta sección se detallan los permisos mínimos y los permisos generales necesarios para Azure.

Permisos mínimos

Los permisos mínimos ofrecen un mejor control de la seguridad. Sin embargo, las nuevas funciones que requieren permisos adicionales fallan si solo se otorgan los permisos mínimos. En esta sección se enumeran los permisos mínimos por acción.

Crear una conexión de host Agregue una conexión de host con la información obtenida de Azure.

```
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/disks/read",
"Microsoft.Resources/providers/read",
"Microsoft.Resources/subscriptions/locations/read",
```



```
"Microsoft.Resources/tenants/read"
<!--NeedCopy-->
```

Administración de energía de las máquinas virtuales Encienda o apague las instancias de máquina.

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Creación, actualización o eliminación de máquinas virtuales Cree un catálogo de máquinas y, a continuación, agregue, elimine y actualice máquinas, y elimine el catálogo de máquinas.

A continuación, se muestra la lista de permisos mínimos requeridos cuando las imágenes maestras son discos administrados o instantáneas que se encuentran en la misma región que la conexión de host.

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Compute/snapshots/beginGetAccess/action",
"Microsoft.Compute/snapshots/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
   read",
"Microsoft.Compute/skus/read",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Features/providers/features/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
```



```
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

Necesita los siguientes permisos adicionales, en función de los permisos mínimos, para las siguientes funciones:

- Si la imagen maestra es un disco duro virtual de una cuenta de almacenamiento ubicada en la misma región que la conexión de host:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
<!--NeedCopy-->
```

- Si la imagen maestra es una versión de imagen de Azure Compute Gallery (anteriormente, Shared Image Gallery):

```
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
<!--NeedCopy-->
```

- Si la imagen maestra es un disco administrado, una instantánea o un VHD que se encuentra en una región diferente de la región de la conexión de host:

```
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
<!--NeedCopy-->
```

- Si usa el grupo de recursos administrado por Citrix:

```
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
<!--NeedCopy-->
```

- Si coloca la imagen maestra en Azure Compute Gallery (anteriormente, Shared Image Gallery) en un arrendatario o en una suscripción compartidos:


```
"Microsoft.Compute/galleries/write",
"Microsoft.Compute/galleries/images/write",
"Microsoft.Compute/galleries/images/versions/write",
"Microsoft.Compute/galleries/read",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Resources/subscriptions/read",
<!--NeedCopy-->
```

- Si usa compatibilidad con hosts dedicados de Azure:

```
"Microsoft.Compute/hostGroups/read",
"Microsoft.Compute/hostGroups/write",
"Microsoft.Compute/hostGroups/hosts/read",
<!--NeedCopy-->
```

- Si utiliza cifrado del lado del servidor (SSE) con claves administradas por el cliente (CMK):

```
"Microsoft.Compute/diskEncryptionSets/read",
<!--NeedCopy-->
```

- Si implementa máquinas virtuales mediante plantillas ARM (perfil de máquina):

```
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/deployments/operationstatuses/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
<!--NeedCopy-->
```

- Si usa la especificación de plantilla de Azure como perfil de máquina:

```
"Microsoft.Resources/templateSpecs/read",
"Microsoft.Resources/templateSpecs/versions/read",
<!--NeedCopy-->
```

Crear, actualizar y eliminar máquinas con discos no administrados A continuación, se muestra la lista de permisos mínimos requeridos cuando la imagen maestra es un disco duro virtual (VHD) y se utiliza el grupo de recursos proporcionado por el administrador:

```
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/listKeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
```



```
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/locations/usages/read",
<!--NeedCopy-->
```

Administración de dispositivos unidos a Azure AD A continuación, se muestra la lista de permisos mínimos necesarios para administrar los dispositivos unidos a Azure AD:

```
microsoft.directory/devices/standard/read
microsoft.directory/devices/delete
<!--NeedCopy-->
```

Permisos generales

El rol de colaborador tiene pleno acceso para administrar todos los recursos. Este conjunto de permisos no le impide obtener nuevas funcionalidades.

El siguiente conjunto de permisos proporciona la mejor compatibilidad de cara al futuro, aunque incluye más permisos de los necesarios con el conjunto de funciones actual:

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
"Microsoft.Compute/disks/delete",
"Microsoft.Compute/disks/endGetAccess/action",
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/galleries/delete",
"Microsoft.Compute/galleries/images/delete",
"Microsoft.Compute/galleries/images/read",
"Microsoft.Compute/galleries/images/versions/delete",
"Microsoft.Compute/galleries/images/versions/read",
"Microsoft.Compute/galleries/images/versions/write",
```



```
13 "Microsoft.Compute/galleries/images/write",
14 "Microsoft.Compute/galleries/read",
15 "Microsoft.Compute/galleries/write",
16 "Microsoft.Compute/hostGroups/hosts/read",
17 "Microsoft.Compute/hostGroups/read",
18 "Microsoft.Compute/hostGroups/write",
19 "Microsoft.Compute/snapshots/beginGetAccess/action",
20 "Microsoft.Compute/snapshots/delete",
21 "Microsoft.Compute/snapshots/endGetAccess/action",
22 "Microsoft.Compute/snapshots/read",
23 "Microsoft.Compute/snapshots/write",
24 "Microsoft.Compute/virtualMachines/deallocate/action",
25 "Microsoft.Compute/virtualMachines/delete",
26 "Microsoft.Compute/virtualMachines/read",
27 "Microsoft.Compute/virtualMachines/restart/action",
28 "Microsoft.Compute/virtualMachines/start/action",
29 "Microsoft.Compute/virtualMachines/write",
30 "Microsoft.Compute/locations/publishers/artifacttypes/types/versions/
      read",
31 "Microsoft.Compute/skus/read",
32 "Microsoft.Compute/virtualMachines/extensions/read",
33 "Microsoft.Compute/virtualMachines/extensions/write",
34 "Microsoft.Network/networkInterfaces/delete",
35 "Microsoft.Network/networkInterfaces/join/action",
36 "Microsoft.Network/networkInterfaces/read",
37 "Microsoft.Network/networkInterfaces/write",
38 "Microsoft.Network/networkSecurityGroups/delete",
39 "Microsoft.Network/networkSecurityGroups/join/action",
40 "Microsoft.Network/networkSecurityGroups/read",
41 "Microsoft.Network/networkSecurityGroups/write",
42 "Microsoft.Network/virtualNetworks/subnets/read",
43 "Microsoft.Network/virtualNetworks/read",
44 "Microsoft.Network/virtualNetworks/subnets/join/action",
45 "Microsoft.Network/locations/usages/read",
46 "Microsoft.Resources/deployments/operationstatuses/read",
47 "Microsoft.Resources/deployments/read",
48 "Microsoft.Resources/deployments/validate/action",
49 "Microsoft.Resources/deployments/write",
50 "Microsoft.Resources/deployments/delete",
51 "Microsoft.Resources/subscriptions/resourceGroups/read",
52 "Microsoft.Resources/subscriptions/resourceGroups/write",
53 "Microsoft.Resources/subscriptions/resourceGroups/delete",
54 "Microsoft.Resources/providers/read",
55 "Microsoft.Resources/subscriptions/locations/read",
56 "Microsoft.Resources/subscriptions/read",
57 "Microsoft.Resources/tags/read",
58 "Microsoft.Resources/tags/write",
59 "Microsoft.Resources/tenants/read",
60 "Microsoft.Resources/templateSpecs/read",
61 "Microsoft.Resources/templateSpecs/versions/read",
62 "Microsoft.Storage/storageAccounts/delete",
63 "Microsoft.Storage/storageAccounts/listKeys/action",
64 "Microsoft.Storage/storageAccounts/read",
```



```
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/locations/usages/read",
"Microsoft.Storage/skus/read",
"Microsoft.Features/providers/features/read",
"Microsoft.Insights/DataCollectionRuleAssociations/Read",
"Microsoft.Insights/dataCollectionRules/read",
"Microsoft.Insights/diagnosticsettings/delete",
"Microsoft.Insights/diagnosticsettings/read",
"Microsoft.Insights/diagnosticsettings/write",
<!--NeedCopy-->
```

Permiso de Azure AD Si crea catálogos de máquinas unidas a Azure AD, MCS será responsable de administrar los dispositivos de Azure AD cuando habilite la administración de dispositivos unidos a Azure AD. El rol **Administrador de dispositivos en la nube** integrado en Azure AD ofrece la mejor compatibilidad de cara al futuro, aunque incluye más permisos de los necesarios con el conjunto de funciones actual.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica de Azure, consulte Crear un catálogo de Microsoft Azure.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de Microsoft Azure Resource Manager

Conexión con Microsoft System Center Virtual Machine Manager

January 24, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de crear una conexión con VMM, debe terminar de configurar su instancia de VMM como ubicación de recursos. Consulte Entornos de virtualización de Microsoft System Center Virtual

> Machine Manager.

Crear una conexión

Si utiliza MCS para aprovisionar las VM, haga esto en el asistente de creación de conexiones:

- Escriba la dirección como el nombre de dominio completo del servidor host.
- Introduzca las credenciales de la cuenta del administrador que configuró. Esa cuenta debe tener permisos para crear nuevas máquinas virtuales.
- En el cuadro de diálogo Detalles del host, seleccione el clúster o el host independiente a utilizar para crear las VM.

  > **Importante**
  >
  > Busque un clúster o un host independiente aunque utilice una implementación de host de Hyper-V único.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para crear catálogos de máquinas con MCS en un recurso compartido de archivos de SMB 3, consulte Crear un catálogo de Microsoft System Center Virtual Machine Manager.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de Microsoft System Center Virtual Machine Manager.

Conexión con Nutanix

January 24, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos sobre Nutanix.

> **Nota:**
>
> Antes de crear una conexión con Nutanix, debe terminar de configurar su cuenta de Nutanix como ubicación de recursos. Consulte Entornos de virtualización de Nutanix.

Crear una conexión con Nutanix

La información siguiente es un complemento de las instrucciones que aparecen en Crear y administrar conexiones. Para crear una conexión Nutanix, siga las instrucciones generales de ese artículo, teniendo en cuenta los detalles específicos de Nutanix.

En el asistente **Agregar conexión y recursos**, seleccione el tipo de conexión **Nutanix** en la página **Conexión** y luego especifique la dirección y las credenciales, además de un nombre para la conexión. En la página **Red**, seleccione una red para la unidad de alojamiento.

Es posible seleccionar los siguientes tipos de conexión: **Nutanix AHV**, **Nutanix AHV Xi** y **Nutanix AHV PC**.

- Para **Nutanix AHV**, especifique la dirección y las credenciales del clúster de Prism Element (PE).
- Para **Nutanix AHV PC**, especifique la dirección y las credenciales del hipervisor.

  > **Nota:**
  >
  > Actualmente, el tipo de conexión **Nutanix AHV PC** solo se usa para crear una conexión a Nutanix Cloud Cluster (NC2) en Azure. Además, un catálogo de máquinas solo se puede hospedar en un solo clúster en una conexión de NC2 en Azure.

- Para **Nutanix AHV DRaaS**, especifique su dirección y nombre de usuario y, a continuación, importe las claves públicas y privadas incluidas en sus archivos de credenciales de Nutanix DRaaS (`.pem`). (Los administradores de Nutanix DRaaS generan claves públicas y privadas en la nube de Nutanix DRaaS.)

  - Para importar la clave, busque el archivo de credenciales, ábralo con Bloc de notas (o cualquier editor de texto) y, a continuación, copie el contenido. Después, vuelva a la página **Conexión**, seleccione **Importar clave**, pegue el contenido y, a continuación, seleccione **Guardar**.

  Precaución: No cambie el contenido de las credenciales ni su formato.

> **Sugerencia:**
>
> Si implementa máquinas que utilizan Nutanix AHV (Prism Element) como recurso, seleccione el contenedor en el que reside el disco de la VM.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica de Nutanix, consulte Crear un catálogo de Nutanix.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de Nutanix
- Soluciones de Nutanix Cloud y de partners

Conexión con soluciones de Nutanix Cloud y de partners

January 24, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de las soluciones de Nutanix Cloud y de partners.

Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) admite estas soluciones de Nutanix Cloud y de partners:

- Nutanix Cloud Clusters en AWS

> **Nota:**
>
> - Antes de crear una conexión con una solución de Nutanix Cloud y de partners, debe terminar de configurar su cuenta correspondiente como ubicación de recursos. Consulte Soluciones de Nutanix Cloud y de partners.
> - Para obtener la información más reciente sobre cómo configurar Nutanix en la nube, consulte la guía más reciente de Nutanix.

Conectarse a Nutanix Prism

Después de crear un clúster de Nutanix, conéctese a Nutanix Prism.
Para conectarse a Nutanix Prism:

1. Cree una máquina virtual bastión en la subred 10.0.129.0/24.
2. Conéctese por RDP a la VM bastión, vaya a la URL de **Prism Element** que copió en la sección anterior.
3. Inicie sesión con las credenciales predeterminadas: `admin`:`nutanix`/`4u`. Recuerde cambiar la contraseña.

Crear una VM en el clúster de Nutanix

Después de conectarse a **Nutanix Prism**, cree máquinas virtuales en el clúster de Nutanix.

Si la VM necesita acceder a Internet

1. Vaya a la consola de AWS.
2. Cree otra subred 10.0.130.0/24 en la misma VPC que la creada por Nutanix CFS.
3. Agregue una ruta a la tabla de rutas de esta subred para dirigir todo el tráfico que no sea local a la puerta de enlace NAT mencionada.
4. Conéctese por RDP a la VM bastión, vaya a la URL de **Prism Element** que copió en la sección anterior e inicie sesión.
5. Agregue una nueva red. Vaya a **Parámetros > Configuración de red > Crear subred**. Use la misma subred 10.0.130.0/24 que se usa en AWS.
6. Cree todas las máquinas virtuales (AD, CC, VDA, etc.) en esa nueva subred.

Si la VM no necesita acceder a Internet

1. Conéctese por RDP a la VM bastión, vaya a la URL de **Prism Element** que copió en la sección anterior e inicie sesión.
2. Agregue una nueva red. Vaya a **Parámetros > Configuración de red > Crear subred**. Use la subred 10.0.129.0/24.
3. Cree todas las máquinas virtuales (AD, CC, VDA, etc.) en esa subred.

> **Sugerencia:**
>
> Asegúrese de que la información sobre la hora y la zona horaria de las VM esté configurada correctamente. Sobre todo para AD.

Crear una conexión de host

1. En **Administrar > Configuración completa**, seleccione **Alojamiento** en el panel de la izquierda.
2. Haga clic en **Agregar conexión y recursos**.
3. En la pantalla **Conexión**, seleccione **Crear una conexión** y, en la **Dirección de la conexión**, introduzca `https://xxx.xxx.xxx.xxx:9440`.
4. Siga las instrucciones de la interfaz de usuario para completar el asistente.

> **Nota:**
>
> Todas las máquinas virtuales con conector deben tener el plug-in de Nutanix instalado para que la opción Nutanix esté disponible en Citrix Studio aunque los plug-ins no se utilicen en la zona de Nutanix.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.

- Para obtener información específica de Nutanix, consulte Crear un catálogo de Nutanix.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de Nutanix
- Soluciones de Nutanix Cloud y de partners

Conexión con VMware

May 17, 2024

Crear y administrar conexiones y recursos describe los asistentes que crean una conexión. La siguiente información incluye detalles específicos de los entornos de virtualización de VMware.

> **Nota:**
>
> Antes de crear una conexión con VMware, debe terminar de configurar su cuenta de VMware como ubicación de recursos. Consulte Entornos de virtualización de VMware.

Permisos requeridos

Cree una cuenta de usuario de VMware y uno o varios roles de VMware con un conjunto de los permisos que se describen en este artículo. Base la creación de roles en un nivel específico de granularidad necesaria sobre los permisos del usuario para solicitar las distintas operaciones de Citrix DaaS en cualquier momento. Para conceder los permisos específicos al usuario en cualquier momento, asócielos al rol correspondiente, en el nivel de centro de datos como mínimo, con la opción **Propagar a elementos secundarios** seleccionada.

En estas tablas, se muestran las asignaciones entre las operaciones de Citrix DaaS y los permisos mínimos requeridos de VMware.

Agregar conexiones y recursos

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

Administración de energía

SDK	Interfaz de usuario
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
Datastore.Browse	Datastore > Browse datastore

Aprovisionar máquinas (Machine Creation Services)

Para aprovisionar máquinas mediante MCS, son obligatorios los siguientes permisos:

SDK	Interfaz de usuario
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
Virtual machine.Config.Add or remove device	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Change memory
VirtualMachine.Config.Settings	Virtual machine > Configuration > Change settings

SDK	Interfaz de usuario
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Interact.Suspend	Virtual machine > Interaction > Suspend
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine
VirtualMachine.State.CreateSnapshot	vSphere 5.0, Update 2, vSphere 5.1, Update 1, and vSphere 6.x, Update 1: Virtual machine > State > Create snapshot; vSphere 5.5: Virtual machine > Snapshot management > Create snapshot; vSphere 8.0: Virtual machine > Snapshot management > Create snapshot

Actualizar y revertir imagen

SDK	Interfaz de usuario
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk

SDK	Interfaz de usuario
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Interact.PowerOn	Virtual machine > Interaction > Power On
VirtualMachine.Interact.Reset	Virtual machine > Interaction > Reset
VirtualMachine.Inventory.CreateFromExisting	Virtual machine > Inventory > Create from existing
VirtualMachine.Inventory.Create	Virtual machine > Inventory > Create new
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove
VirtualMachine.Provisioning.Clone	Virtual machine > Provisioning > Clone virtual machine

Eliminar máquinas aprovisionadas

SDK	Interfaz de usuario
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
VirtualMachine.Config.RemoveDisk	Virtual machine > Configuration > Remove disk
VirtualMachine.Interact.PowerOff	Virtual machine > Interaction > Power Off
VirtualMachine.Inventory.Delete	Virtual machine > Inventory > Remove

Perfil de almacenamiento (vSAN)

Para ver, crear o eliminar directivas de almacenamiento durante la creación de catálogos en un almacén de datos de vSAN, son obligatorios los siguientes permisos:

SDK	Interfaz de usuario
StorageProfile.Update	PROFILE-DRIVEN STORAGE > Profile-driven storage update. Para vSphere 8: VM storage policies > Update VM storage policies
StorageProfile.View	PROFILE-DRIVEN STORAGE > Profile-driven storage view. Para vSphere 8: VM storage policies > View VM storage policies

Etiquetas y atributos personalizados

Las etiquetas y los atributos personalizados permiten adjuntar metadatos a las máquinas virtuales creadas en el inventario de vSphere y facilitan la búsqueda y el filtrado de estos objetos. Para crear, modificar, asignar y eliminar etiquetas o categorías, son obligatorios los siguientes permisos:

SDK	Interfaz de usuario
InventoryService.Tagging.CreateTag	vSphere Tagging > Create vSphere Tag
InventoryService.Tagging.CreateCategory	vSphere Tagging > Create vSphere Tag Category
InventoryService.Tagging.EditTag	vSphere Tagging > Edit vSphere Tag
InventoryService.Tagging.EditCategory	vSphere Tagging > Edit vSphere Tag Category
InventoryService.Tagging.DeleteTag	vSphere Tagging > Delete vSphere Tag
InventoryService.Tagging.DeleteCategory	vSphere Tagging > Delete vSphere Tag Category
InventoryService.Tagging.AttachTag	vSphere Tagging > Assign or Unassign vSphere Tag
InventoryService.Tagging.ObjectAttachable	vSphere Tagging > Assign or Unassign vSphere Tag on Object
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

> **Nota:**
>
> Cuando MCS crea un catálogo de máquinas, etiqueta las máquinas virtuales de destino con etiquetas con nombres especiales. Estas etiquetas diferencian la imagen maestra de las máquinas virtuales creadas por MCS e impiden el uso de máquinas virtuales creadas por MCS para la preparación de imágenes. Puede identificar la diferencia por el valor del atributo `XdProvisioned` en vCenter. El atributo se establece en **True** si MCS crea las máquinas virtuales.

Operaciones de cifrado

Los privilegios relativos a las operaciones de cifrado determinan quién puede realizar los distintos tipos de operaciones de cifrado en los diferentes tipos de objetos. El proveedor de claves nativas de vSphere usa los privilegios de `Cryptographer.*`. Para las operaciones de cifrado, se requieren los siguientes permisos mínimos:

> **Nota:**
>
> Estos permisos son necesarios para crear catálogos de máquinas de MCS con una máquina virtual equipada con vTPM.

SDK	Interfaz de usuario
Cryptographic operations.Direct Access	Privileges > All Privileges > Cryptographic operations > Direct Access
Cryptographic operations.Add disk	Privileges > All Privileges > Cryptographic operations > Add disk
Cryptographic operations.Clone	Privileges > All Privileges > Cryptographic operations > Clone
Cryptographic operations.Encrypt	Privileges > All Privileges > Cryptographic operations > Encrypt
Cryptographic operations.Encrypt new	Privileges > All Privileges > Cryptographic operations > Encrypt new
Cryptographic operations.Decrypt	Privileges > All Privileges > Cryptographic operations > Decrypt
Cryptographic operations.Migrate	Privileges > All Privileges > Cryptographic operations > Migrate
Cryptographic operations.Read KMS information	Privileges > All Privileges > Cryptographic operations > Read KMS information

Aprovisionar máquinas (Citrix Provisioning)

Estos permisos para clonar e implementar una plantilla son necesarios para aprovisionar máquinas virtuales mediante el asistente Citrix Virtual Apps and Desktops Setup Wizard y el asistente Export Devices Wizard a través de la consola de Citrix Provisioning. Establezca los permisos al crear una conexión de alojamiento.
Necesita todos los permisos de Aprovisionar máquinas (Machine Creation Services) y lo siguiente:

SDK	Interfaz de usuario
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory

SDK	Interfaz de usuario
VirtualMachine.Config.Settings	Virtual machine > Configuration > Settings
VirtualMachine.Provisioning.CloneTemplate	Virtual machine > Provisioning > Clone template
VirtualMachine.Provisioning.DeployTemplate	Virtual machine > Provisioning > Deploy template
vApp.Export	vApp > Export

> **Nota:**
>
> `vApp.Export` es necesario para crear catálogos de máquinas de MCS mediante perfiles de máquina.

Protección de las conexiones con el entorno VMware

El uso de conexiones `HTTPS` / `SSL` con vCenter requiere que Citrix DaaS confíe en la conexión.

Existen dos opciones:

- (Recomendada) La base de datos Citrix DaaS tiene instalada la huella digital SSL. Citrix DaaS utiliza esta huella digital en cada Cloud Connector para establecer la confianza en las conexiones a vCenter.
- (Alternativa) Cada Cloud Connector confía en el certificado de vCenter y los servicios del Cloud Connector reutilizan esta confianza. Esta confianza puede proceder de un:
  - Certificado de vCenter emitido por una CA en la que confía Windows, lo que establece la confianza entre Windows y vCenter.
  - Certificado de vCenter instalado en Windows, lo que establece la confianza entre Windows y vCenter

> **Nota:**
>
> El certificado de vCenter y la huella digital SSL de VMware no son necesarios para las soluciones de VMware Cloud ni de sus partners.

Huella digital SSL de VMware

La funcionalidad de la huella digital SSL de VMware resuelve un error frecuente que se daba al crear una conexión de host a un hipervisor VMware vSphere. Anteriormente, los administradores tenían que crear manualmente una relación de confianza entre los Delivery Controllers administrados por Citrix que hubiera en el sitio y el certificado del hipervisor antes de crear una conexión. La función

huella digital SSL de VMware elimina ese requisito manual: la huella digital del certificado que no es de confianza se almacena en la base de datos del sitio, de modo que el hipervisor puede identificarse continuamente como hipervisor de confianza por Citrix DaaS o, incluso si no es por esta, por los Controllers.

Al crear una conexión de host de vSphere, un cuadro de diálogo le permite ver el certificado de la máquina a la que se está conectando. Por lo que puede elegir si quiere confiar en ella.

La huella digital SSL de VMware se puede actualizar posteriormente con el SDK de PowerShell `Set-Item -LiteralPath "<FullPath_to_connection>"-username $cred.username -Securepassword $cred.password -SslThumbprint "<New ThumbPrint>"-hypervisorAddress <vcenter URL>`.

> **Sugerencia:**
>
> La huella digital del certificado debe escribirse en mayúsculas.

Obtener e importar un certificado

Para proteger las comunicaciones de vSphere, Citrix recomienda utilizar HTTPS en lugar de HTTP. HTTPS requiere certificados digitales. Citrix recomienda utilizar un certificado digital emitido por una entidad de certificación conforme a la directiva de seguridad de la organización.

Si no puede utilizar un certificado digital emitido por una entidad de certificación y las directivas de seguridad de la organización lo permiten, puede utilizar el certificado autofirmado instalado por VMware. Agregue el certificado de VMware vCenter a cada Cloud Connector.

1. Agregue el nombre de dominio completo (FQDN) del equipo que ejecuta vCenter Server al archivo hosts de ese servidor, ubicado en %SystemRoot%/WINDOWS/system32/Drivers/etc/. Este paso solo es necesario si el nombre FQDN del equipo que ejecuta vCenter Server aún no está presente en el sistema de nombres de dominio.
2. Obtenga el certificado de vCenter con alguno de los tres métodos siguientes:

   Desde el servidor vCenter:

   a) Copie el archivo rui.crt desde el servidor vCenter a una ubicación accesible en los Cloud Connectors.
   b) En el Cloud Connector, vaya a la ubicación donde está el certificado exportado y abra el archivo rui.crt.

   Descargue el certificado mediante un explorador web: Si utiliza Internet Explorer, en función de la cuenta de usuario, deberá hacer clic con el botón secundario en Internet Explorer y elegir **Ejecutar como administrador** para descargar o instalar el certificado.

a) Abra el explorador web y establezca una conexión web segura con el servidor vCenter (por ejemplo https://server1.domain1.com).
b) Acepte las advertencias de seguridad.
c) Haga clic en la barra de dirección donde aparece el error de certificado.
d) Haga clic en **Certificate is not valid** y, a continuación, en la ficha **Details**.
e) Haga clic en **Export.**
f) Guarde el certificado exportado.
g) Vaya a la ubicación del certificado exportado y abra el archivo CER.

Impórtelo directamente desde Internet Explorer ejecutado como administrador:

a) Abra el explorador web y establezca una conexión web segura con el servidor vCenter (por ejemplo https://server1.domain1.com).
b) Acepte las advertencias de seguridad.
c) Haga clic en la barra de dirección donde aparece el error de certificado.
d) Vea el certificado.

3. Importe el certificado en el almacén de certificados de cada Cloud Connector.

a) Haga clic en **Instalar certificado**, seleccione **Máquina local** y, a continuación, haga clic en **Siguiente**.
b) Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, haga clic en **Examinar**. En una versión posterior compatible, seleccione **Personas de confianza** y, a continuación, haga clic en **Aceptar**. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

> **Importante:**
>
> Si cambia el nombre del servidor vSphere después de la instalación, debe generar un certificado autofirmado nuevo en ese servidor antes de importar el certificado nuevo.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica de VMware, consulte Crear un catálogo de VMware.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización VMware.
- Soluciones de VMware Cloud y de partners

Conexión con soluciones de VMware Cloud y de partners

January 24, 2024

Tras configurar el clúster de Azure VMware Solution (AVS), Google Cloud VMware Engine y VMware Cloud en AWS, cree las conexiones. Para crear conexiones, consulte Conexión con entornos de virtualización de VMware.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica de VMware, consulte Crear un catálogo de VMware.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización VMware.
- Soluciones de VMware Cloud y de partners

Conexión a XenServer

April 18, 2024

Crear y administrar conexiones y recursos proporciona instrucciones detalladas sobre cómo usar el asistente para crear una conexión. Antes de establecer una conexión con XenServer (antes denominado Citrix Hypervisor), debe terminar de configurar su instancia de XenServer como host. Consulte Agregar un tipo de recurso o activar un dominio no utilizado en Citrix Cloud.

Crear una conexión a XenServer

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

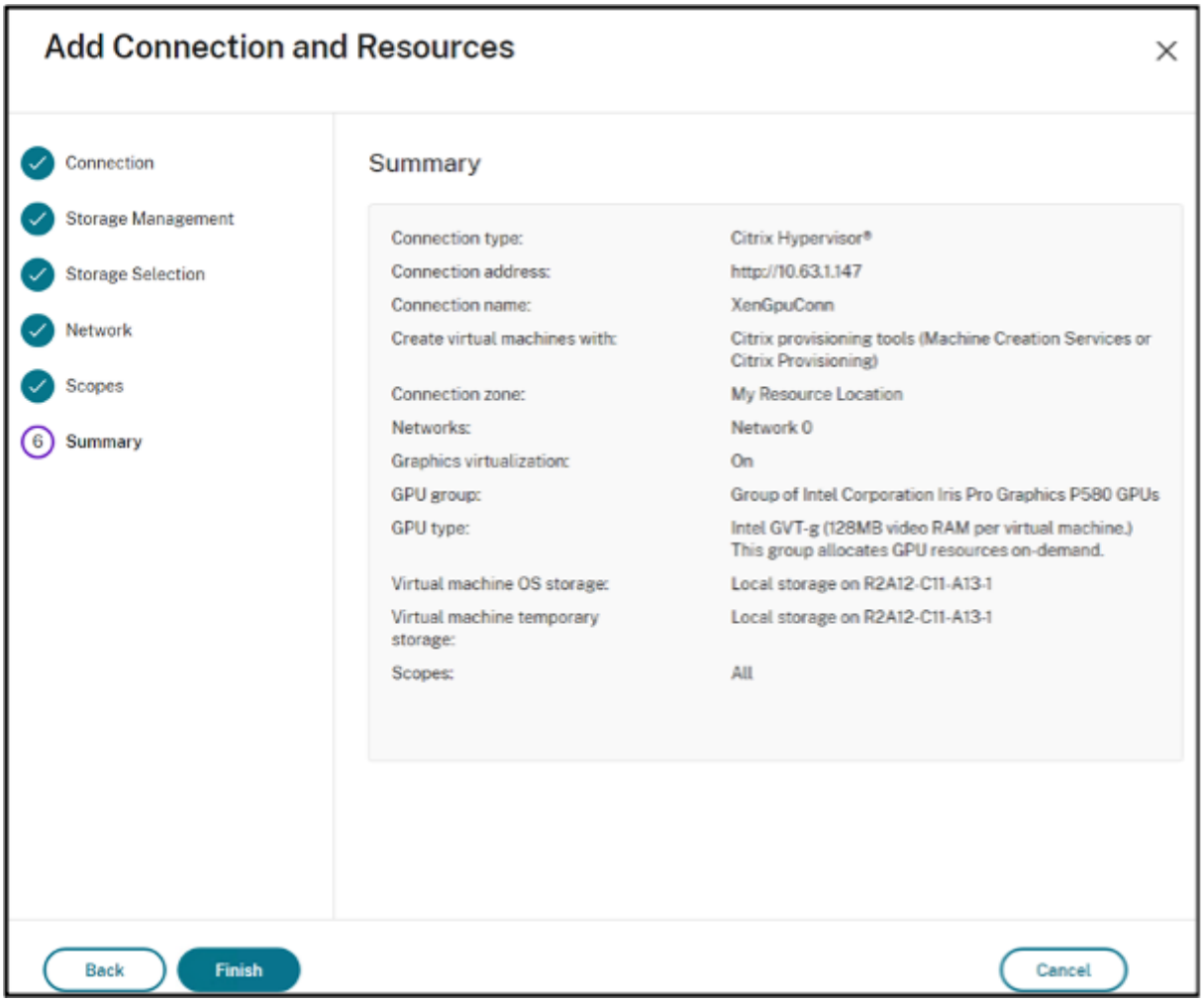
Citrix recomienda utilizar HTTPS para proteger las comunicaciones con XenServer. Para utilizar HTTPS, debe reemplazar el certificado TLS predeterminado que se instaló en XenServer. Para obtener más información, consulte Install a TLS certificate on your server.

Es posible configurar la alta disponibilidad si esta función está habilitada en el servidor XenServer. Citrix recomienda seleccionar todos los servidores de la agrupación (en **Edit High Availability**) para permitir la comunicación con el servidor XenServer en caso de que falle el servidor principal de la agrupación.

> **Nota:**
>
> Si utiliza HTTPS y quiere configurar servidores de alta disponibilidad, no instale un certificado comodín para todos los servidores de una agrupación. Se requiere un certificado individual para cada servidor.

Cuando se usa el almacenamiento local en uno o varios hosts de XenServer para el almacenamiento de datos temporales, compruebe que cada ubicación de almacenamiento que forma parte de la agrupación tenga un nombre único. (Para modificar un nombre en XenCenter, haga clic con el botón secundario en el espacio de almacenamiento y modifique la propiedad de nombre.)

Si se conecta a la instancia de XenServer compatible con vGPU, puede verificar el grupo de la GPU y el tipo de la GPU en la página **Resumen** del asistente para crear una conexión.



Usar IntelliCache para conexiones XenServer

Con IntelliCache, las implementaciones de VDI alojadas son más rentables porque le permiten usar una combinación de almacenamiento compartido y almacenamiento local. Esto mejora el rendimiento y reduce el tráfico de red. El almacenamiento local almacena en caché la imagen maestra proveniente del almacenamiento compartido, lo que reduce la cantidad de lecturas en el almacenamiento compartido. Para los escritorios compartidos, las escrituras en los discos de diferenciación se realizan en el almacenamiento local del host y no en el almacenamiento compartido.

Estas son algunas consideraciones importantes:

- Cuando utiliza IntelliCache, el almacenamiento compartido debe ser NFS.
- Citrix recomienda utilizar un dispositivo de almacenamiento local de alto rendimiento para garantizar la transferencia de datos más rápida que sea posible.

Para usar IntelliCache, habilite IntelliCache tal y como se detalla:

- Al instalar XenServer, seleccione **Enable thin provisioning**. Consulte Install the XenServer host para obtener información sobre la instalación del host de XenServer desde un medio local. Citrix no admite agrupaciones mixtas de servidores, donde algunos servidores tienen el componente IntelliCache habilitado y otros servidores no tienen dicho componente habilitado.
- En Citrix DaaS, IntelliCache está inhabilitado de forma predeterminada. Puede cambiar la configuración únicamente al crear una conexión con XenServer. No podrá inhabilitar IntelliCache más adelante. Al crear una conexión con XenServer:
  - Seleccione el tipo de almacenamiento **compartido**.
  - Marque la casilla **Usar IntelliCache**.

Para obtener más información, consulte IntelliCache.

Permisos de XenServer necesarios

Los permisos de XenServer se basan en roles (RBAC). La función de control de acceso basado en roles (RBAC) de XenServer le permite asignar usuarios, roles y permisos para controlar quién tiene acceso a su XenServer y qué acciones pueden realizar. El sistema RBAC de XenServer asigna un usuario (o un grupo de usuarios) a roles definidos (un conjunto de permisos con nombre). Los roles tienen permisos de XenServer asociados para realizar determinadas operaciones.

Para obtener más información, consulte Control de acceso basado en roles.

La jerarquía de roles, en orden de aumento de los permisos, es: Solo lectura → Operador de VM → Administrador de VM → Administrador avanzado de VM → Operador de agrupaciones → Administrador de agrupaciones.

En la siguiente sección se resume el rol mínimo requerido para cada tarea de aprovisionamiento.

Crear una conexión de host

Tarea	Rol mínimo requerido
Agregue una conexión de host con la información obtenida de XenServer	Solo lectura
Ver los usuarios y sus roles asignados	Solo lectura

Administración avanzada de máquinas virtuales

Tarea	Rol mínimo requerido
Encender o apagar las máquinas virtuales	Operador de VM

Crear, actualizar o eliminar máquinas virtuales

Tarea	Rol mínimo requerido
Agregar máquinas virtuales a las programaciones de instantáneas existentes o quitarlas de las mismas	Administrador avanzado de VM
Agregar, modificar y eliminar programaciones de instantáneas	Operador de agrupaciones
Publicar imagen maestra	Operador de agrupaciones (requiere bloqueo de puertos de conmutador)
Crear un catálogo de máquinas	Operador de agrupaciones: requiere bloqueo de puertos de conmutador
Agregar o quitar máquinas virtuales (no incluye máquinas virtuales habilitadas para GPU)	Administrador de máquinas virtuales
Agregar o quitar máquinas virtuales (máquinas virtuales habilitadas para GPU)	Operador de agrupaciones
Agregar, quitar o configurar dispositivos de CD o discos virtuales	Administrador de máquinas virtuales
Administrar etiquetas	Operador de VM

Para obtener más información sobre los roles y los permisos de RBAC, consulte Roles y permisos de RBAC.

Para obtener información sobre el bloqueo de puertos de conmutador, consulte Usar bloqueo de puertos de conmutador.

Qué hacer a continuación

- Si está en el proceso de implementación inicial, consulte Crear catálogos de máquinas.
- Para obtener información específica sobre XenServer, consulte Crear un catálogo de XenServer.

Más información

- Crear y administrar conexiones y recursos
- Entornos de virtualización de XenServer

Crear catálogos de máquinas

June 13, 2024

> **Nota:**
>
> En este artículo, se describe cómo crear catálogos con la interfaz Configuración completa. Si utiliza Distribución rápida para crear recursos de Azure, siga las instrucciones que se indican en Crear catálogos con Distribución rápida.

Las colecciones de máquinas físicas o virtuales se administran como una entidad única, llamada catálogo de máquinas. Dentro de un catálogo de máquinas, todas las máquinas comparten un tipo de sistema operativo común, que puede ser un sistema operativo multisesión o un sistema operativo de sesión única, como los sistemas basados en Windows o Linux.

La interfaz **Administrar > Configuración completa** le guía para crear el primer catálogo de máquinas. Después de crear el primer catálogo de máquinas, creará su primer grupo de entrega. Posteriormente, puede cambiar el catálogo que haya creado y crear más catálogos.

Información general

Cuando crea un catálogo de máquinas virtuales, debe indicar cómo aprovisionarlas. Puede utilizar Machine Creation Services (MCS). O bien, puede utilizar sus propias herramientas para aprovisionar máquinas.

- Si elige Machine Creation Services para aprovisionar las máquinas, debe proporcionar una imagen (o instantánea) para crear máquinas virtuales idénticas en el catálogo. Antes de crear el catálogo, debe comenzar por configurar una conexión de alojamiento con el hipervisor o servicio de nube que elija y, a continuación, crear y configurar la imagen maestra en el mismo. La configuración de la imagen maestra requiere tareas como la unión a un dominio cuando sea necesario, instalar los controladores necesarios, publicar las aplicaciones e implementar el Virtual Delivery Agent (VDA) en la imagen.
- Después de crear la imagen maestra, cree el catálogo de máquinas en la interfaz **Administrar > Configuración completa**. Debe seleccionar esa imagen (o una instantánea de ella), especificar la cantidad de máquinas virtuales que se van a crear en el catálogo y configurar información adicional.
- Aun si las máquinas ya están disponibles, debe crear igualmente uno o varios catálogos para poder importar estas máquinas virtuales al catálogo.

Si utiliza MCS para crear el primer catálogo, especifique una unidad host que haya creado anteriormente. La unidad host proporciona la configuración de recursos para que pueda crear una máquina virtual. Más adelante (después de crear el primer catálogo y el grupo de entrega), podrá cambiar la información sobre esa unidad de alojamiento o su conexión de host principal o crear más conexiones y unidades de alojamiento.

Si un Cloud Connector no funciona correctamente, las operaciones de aprovisionamiento de MCS (como las actualizaciones de catálogos) tardan más de lo habitual, y el rendimiento de la interfaz de administración se degrada significativamente.

Verificar licencias RDS

La creación de un catálogo que contenga máquinas con SO Windows multisesión incluye una comprobación automática de las licencias RDS de Microsoft válidas. En el catálogo, se busca una máquina encendida y registrada para llevar a cabo la comprobación.

- Si no encuentra ninguna máquina encendida y registrada, muestra un mensaje de advertencia, donde explica que la comprobación de licencias RDS no se puede realizar.
- Si encuentra una máquina y detecta un error, **Administrar > Configuración completa** muestra un mensaje de advertencia sobre el catálogo que contiene el problema detectado. Para quitar una advertencia de licencias de RDS de un catálogo (para que ya no aparezca en la pantalla), seleccione el catálogo. Seleccione **Quitar advertencia de licencias de RDS**. Cuando se le solicite, confirme la acción.

Registro de VDA

El agente VDA debe registrarse en un Cloud Connector para que se le tenga en cuenta cuando se inicien sesiones con intermediario. Los VDA no registrados pueden derivar en una infrautilización de los recursos disponibles. Existen varios motivos por los que un VDA podría no estar registrado y es posible solucionar muchos de ellos. Se proporciona información para la solución de problemas en el Asistente para la creación de catálogos y después de agregar el catálogo a un grupo de entrega.

En el Asistente para la creación de catálogos de máquinas, después de agregar las máquinas existentes, la lista de nombres de cuenta de equipo indicará si cada máquina es adecuada para agregarla al catálogo. Pase el puntero sobre el icono situado junto a cada máquina para ver un mensaje informativo sobre esa máquina.

Si el mensaje indica una máquina problemática, puede quitarla (mediante el botón **Quitar**) o agregarla. Por ejemplo, si un mensaje indica que no se puede obtener información acerca de una máquina (posiblemente porque nunca se registró), puede optar por agregarla de todos modos.

Para obtener más información sobre la solución de problemas de registro de VDA, consulte CTX136668.

Resumen de la creación de catálogos con MCS

A continuación, se ofrece un breve resumen de las acciones de MCS predeterminadas después de proporcionar información en el Asistente para la creación de catálogos de máquinas.

- Si selecciona una imagen (en lugar de una instantánea), MCS crea una instantánea.
- MCS crea una copia completa de la instantánea y la coloca en cada ubicación de almacenamiento definida en la conexión de host.
- MCS agrega las máquinas a Active Directory, lo que crea identidades únicas.
- MCS crea la cantidad de máquinas virtuales especificadas en el asistente, con dos discos definidos para cada máquina virtual. Además de los dos discos por máquina virtual, también se almacena en la misma ubicación de almacenamiento una copia completa de la instantánea o la imagen maestra. Si ha definido varias ubicaciones de almacenamiento, cada una obtiene los siguientes tipos de disco:
  - La copia completa de la instantánea (indicada anteriormente), que es de solo lectura, y se comparte entre las máquinas virtuales que se acaban de crear.
  - Un disco de identidad único de 16 MB que proporciona a cada máquina virtual una identidad única. Cada máquina virtual obtiene un disco de identidad.
  - Un disco de diferenciación único para almacenar las escrituras realizadas en la máquina virtual. Este disco es de aprovisionamiento ligero (si el almacenamiento del host lo admite) y aumenta al tamaño máximo de la imagen maestra, si fuera necesario. Cada máquina

virtual obtiene un disco de diferenciación. El disco de diferenciación contiene los cambios realizados durante las sesiones. Es permanente para los escritorios dedicados. Para los escritorios agrupados, se elimina y se crea uno nuevo después de cada reinicio.

Como alternativa, al crear máquinas virtuales para entregar escritorios estáticos, puede especificar (en la página **Máquinas** del Asistente para la creación del catálogo de máquinas) que se creen clones de máquinas virtuales pesados (de copia completa). Los clones completos no necesitan retener la imagen maestra en cada almacén de datos. Cada máquina virtual tiene su propio archivo.

Consideraciones sobre el almacenamiento de Machine Creation Services

Hay muchos factores al tomar una decisión sobre las soluciones de almacenamiento, las configuraciones y las prestaciones para MCS. La siguiente información proporciona consideraciones adecuadas para la capacidad de almacenamiento:

Consideraciones de capacidad:

- Discos

  Los discos Delta o de diferenciación (Diff) consumen la mayor cantidad de espacio en la mayoría de las implementaciones de MCS para cada máquina virtual. Cada máquina virtual creada por MCS se da en un mínimo de 2 discos tras la creación.

  - Disco0 = Disco de diferenciación: Contiene el sistema operativo cuando se copia de la imagen base maestra.
  - Disk1 = Disco de identidad: 16 MB. Contiene datos de Active Directory para cada máquina virtual.

  A medida que el producto evoluciona, es posible que tenga que agregar más discos para satisfacer determinados casos de uso y el consumo de funciones. Por ejemplo:

  - Optimización de almacenamiento de MCS crea un disco de estilo de caché de escritura para cada máquina virtual.
  - MCS agregó la capacidad de usar clones completos, en lugar del caso de uso del disco Delta descrito en la sección anterior.

  Las funciones del hipervisor también pueden entrar en la ecuación. Por ejemplo:

  - XenServer IntelliCache crea un disco de lectura en el almacenamiento local para cada XenServer. Esta opción ahorra en IOPS en la imagen que podría mantenerse en la ubicación de almacenamiento compartido.

- Sobrecarga del hipervisor

Cada hipervisor usa archivos específicos que crean sobrecarga para las máquinas virtuales. Los hipervisores también usan el almacenamiento para operaciones de administración y registro general. Calcular el espacio para incluir la sobrecarga de:

  - Archivos de registros
  - Archivos específicos del hipervisor. Por ejemplo:
    * VMware agrega más archivos a la carpeta de **almacenamiento de VM**. Consulte Prácticas recomendadas de VMware.
    * Calcule los requisitos del tamaño total de máquinas virtuales. Tome como ejemplo una máquina virtual con 20 GB para el disco virtual, 16 GB para el archivo de intercambio de máquina virtual y 100 MB para los archivos de registros; 36,1 GB en total.
  - Instantáneas para XenServer; Instantáneas para VMware.

- Sobrecarga del proceso

  Crear un catálogo, agregar una máquina y actualizar un catálogo tienen implicaciones únicas en el almacenamiento. Por ejemplo:

  - La creación inicial de catálogos requiere que se copie una copia del disco base en cada ubicación de almacenamiento.
    * También requiere que cree una máquina virtual de preparación temporalmente.
  - Agregar una máquina a un catálogo no requiere copiar el disco base en cada ubicación de almacenamiento. La creación del catálogo varía en función de las funcionalidades seleccionadas.
  - Actualizar el catálogo para crear un disco base adicional en cada ubicación de almacenamiento. Las actualizaciones de catálogos también experimentan un pico temporal de almacenamiento donde cada máquina virtual en el catálogo tiene 2 discos de diferenciación (Diff) durante un cierto período de tiempo.

Más consideraciones:

- **Tamaño de la RAM:** Afecta al tamaño de ciertos archivos y discos de hipervisor, incluidos los discos de optimización de E/S, la memoria caché de escritura, y archivos de instantáneas.
- **Aprovisionamiento fijo/dinámico:** se prefiere el almacenamiento NFS debido a las prestaciones del aprovisionamiento dinámico.

Optimización del almacenamiento de Machine Creation Services (MCS)

La función de optimización del almacenamiento de Machine Creation Services (MCS) también se conoce como E/S de MCS. Esta función solo está disponible en Azure, GCP, XenServer, VMware y SCVMM.

- El contenedor de la memoria caché de escritura *se basa en los archivos*; es la misma funcionalidad que se encuentra en Citrix Provisioning. Por ejemplo, el nombre de archivo en la memoria caché de escritura de Citrix Provisioning es `D:\vdiskdif.vhdx`, y el nombre de archivo en la memoria caché de escritura de E/S de MCS es `D:\mcsdif.vhdx`.
- Para obtener mejoras en los diagnósticos, incluya un archivo de volcado de errores de Windows escrito en el disco de la memoria caché de escritura.
- E/S de MCS conserva la tecnología de *memoria caché en la RAM con desbordamiento al disco duro* para proporcionar la mejor solución de memoria caché de escritura a varios niveles. Esta funcionalidad permite a los administradores equilibrar el coste en cada nivel, RAM y disco, y también el rendimiento para satisfacer las expectativas deseadas de carga de trabajo.

Actualizar el método de memoria caché de escritura de la opción *por disco* a la opción *por archivo* requiere los siguientes cambios:

1. E/S de MCS ya no admite la memoria caché solo en RAM. Especifique un tamaño de disco durante la creación del catálogo de máquinas.
2. El disco de la memoria caché de escritura de una VM se crea y se formatea automáticamente al arrancar la VM por primera vez. Cuando la VM ya está activa, el archivo de la memoria caché de escritura `mcsdif.vhdx` se escribe en el volumen formateado `MCSWCDisk`.
3. El archivo de paginación se redirige a este volumen con formato, `MCSWCDisk`. Como resultado, este tamaño de disco tiene en cuenta la cantidad total de espacio en disco. Incluye el delta entre el tamaño del disco y la carga de trabajo generada, más el tamaño del archivo de paginación. Normalmente, esto se asocia al tamaño de la RAM de la VM.

Habilitar actualizaciones de optimización del almacenamiento de MCS Para habilitar esta función de optimización del almacenamiento de E/S de MCS, actualice la versión del Delivery Controller y de los VDA a la versión más reciente de Citrix DaaS.

> **Nota:**
>
> Si actualiza una implementación existente que tiene habilitada E/S de MCS, no se necesita ninguna configuración adicional. El VDA y la actualización de Delivery Controller gestionan la actualización de E/S de MCS.

Para obtener información sobre cómo asignar una letra de unidad a un disco de caché con reescritura, consulte Asignar una letra de unidad específica al disco de la memoria caché de reescritura de E/S de MCS.

Preparar una imagen maestra en el hipervisor o servicio de nube

La imagen maestra contiene el sistema operativo, las aplicaciones no virtualizadas, el VDA y otro software.

Información útil:

- Una imagen maestra también se conoce como imagen clon, imagen dorada, VM base o imagen base. Los proveedores de host y los proveedores de servicios en la nube pueden usar otros nombres.
- Compruebe que el hipervisor o el servicio de nube tienen procesadores, memoria y capacidad de almacenamiento suficientes para admitir la cantidad de máquinas creadas.
- Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo de la máquina.
- Los catálogos de máquinas de acceso con Remote PC no utilizan imágenes maestras.
- Consideraciones acerca de la activación de KMS de Microsoft al utilizar Machine Creation Services: Si la implementación incluye agentes VDA con la versión 7.x y un host de XenServer 6.1 o 6.2, vSphere o Microsoft System Center Virtual Machine Manager, no tendrá que rearmar manualmente Microsoft Windows ni Microsoft Office.

Instale y configure el siguiente software en la imagen maestra:

- Herramientas de integración para el hipervisor (como Citrix VM Tools, Servicios de integración de Hyper-V o VMware Tools). Si omite este paso, es posible que las aplicaciones y los escritorios no funcionen correctamente.
- Un agente VDA. Citrix recomienda instalar la última versión de VDA para poder disponer de las funciones más recientes. Un error en la instalación del VDA en la imagen maestra provoca un error en la creación de catálogos.
- Si fuera necesario, herramientas de terceros, como el software antivirus o agentes de distribución electrónica de software. Configure los servicios con los parámetros adecuados para los usuarios y el tipo de máquina (como, por ejemplo, la actualización de las funciones).
- Aplicaciones de terceros que no va a virtualizar. Citrix recomienda virtualizar las aplicaciones. La virtualización reduce costes, ya que desaparece la necesidad de actualizar la imagen maestra después de agregar o volver a configurar una aplicación. Además, al tener menos aplicaciones instaladas, se reduce el tamaño de los discos duros de la imagen maestra, lo que ahorra costes de almacenamiento.
- Clientes App-V con la configuración recomendada, si se van a publicar aplicaciones de App-V. El cliente de App-V está disponible en Microsoft.
- Si utiliza Machine Creation Services y va a localizar Microsoft Windows, instale las configuraciones regionales y los paquetes de idioma. Durante el aprovisionamiento, cuando se crea una instantánea, las máquinas virtuales aprovisionadas usan las configuraciones regionales y los paquetes de idioma instalados.

> **Importante:**
>
> Si utiliza Machine Creation Services, no ejecute Sysprep en imágenes maestras.

Para preparar una imagen maestra:

1. Con la herramienta de administración del hipervisor, cree una imagen maestra y, a continuación, instale el sistema operativo, además de todos los Service Pack y las actualizaciones. Especifique la cantidad de CPU virtuales. También puede especificar el valor de la CPU virtual si crea el catálogo de máquinas mediante PowerShell. No se puede especificar la cantidad de CPU virtuales si crea el catálogo desde **Administrar > Configuración completa**. Configure la cantidad necesaria de espacio en disco duro para los escritorios y las aplicaciones. Ese valor no se puede cambiar más adelante o en el catálogo.
2. Compruebe que el disco duro está conectado a la ubicación de dispositivo 0. La mayoría de las plantillas de imagen maestra estándar configuran esta ubicación de manera predeterminada, pero es posible que no suceda lo mismo con algunas plantillas personalizadas.
3. Instale y configure el software anterior en la imagen maestra.
4. Si no utiliza Machine Creation Services, debe unir la imagen maestra al dominio al que pertenecen las aplicaciones y los escritorios. Compruebe que la imagen maestra está disponible en el host donde se crearán las máquinas. Si utiliza Machine Creation Services, no es necesario unir la imagen maestra a un dominio. Las máquinas aprovisionadas se unen al dominio especificado en el Asistente para la creación de catálogos.
5. Citrix recomienda que cree y dé nombre a una instantánea de la imagen maestra, para que se pueda identificar más tarde. Si especifica una imagen maestra en lugar de una instantánea al crear un catálogo de máquinas, la interfaz de administración crea una instantánea, pero no se le podrá asignar ningún nombre.

Activación de licencias por volumen

MCS admite la activación de licencias por volumen para automatizar y administrar la activación de los sistemas operativos Windows y Microsoft Office. Los tres modelos que admite MCS para la activación de licencias por volumen son:

- Servicio de administración de claves KMS (Key Management Service)
- Activación basada en Active Directory (ADBA)
- Multiple Activation Key (MAK)

Puede cambiar la configuración de activación después de crear el catálogo de máquinas.

Servicio de administración de claves KMS (Key Management Service)

KMS es un servicio ligero que no requiere un sistema dedicado y se puede alojar fácilmente y de manera conjunta en un sistema que proporcione otros servicios. Esta funcionalidad se admite en todas las versiones de Windows compatibles con Citrix. Durante la preparación de la imagen, MCS realiza el rearmado de Microsoft Windows y Microsoft Office KMS. Puede omitir el rearmado ejecutando el comando `Set-Provserviceconfigurationdata`. Para obtener más información sobre el rearmado de

Microsoft Windows KMS y Microsoft Office KMS durante la preparación de imágenes, consulte Machine Creation Services: Image Preparation Overview and Fault-Finding. Para obtener más información sobre la activación de KMS, consulte Activate using Key Management Service.

> **Nota:**
>
> Todos los catálogos de máquinas creados después de ejecutar el comando `Set-Provserviceconfigurat` tienen la misma configuración que se proporciona en el comando.

Activación basada en Active Directory (ADBA)

ADBA le permite activar máquinas a través de sus conexiones de dominio. Las máquinas se activan inmediatamente cuando se unen al dominio. Estas máquinas permanecen activadas mientras sigan unidas al dominio y en contacto con él. Esta funcionalidad se admite en todas las versiones de Windows compatibles con Citrix, excepto en Windows Server 2022. Para obtener más información sobre la activación basada en Active Directory, consulte Activate using Active Directory-based activation.

Multiple Activation Key (MAK)

MAK es una modalidad de activación por volumen y de autenticación del sistema Windows con la ayuda del servidor de Microsoft. Es necesario comprar la clave MAK de Microsoft, a la que se le asigna una cantidad fija de recuentos de activación. Cada vez que se activa un sistema Windows, el recuento de activaciones se reduce. Hay dos maneras de activar el sistema:

- Activación con conexión: Si el sistema Windows que quiere activar tiene acceso a Internet, el sistema activa Windows automáticamente al instalar la clave de producto. Este proceso reduce el recuento de activaciones en 1 para la instancia MAK correspondiente.
- Activación sin conexión: Si el sistema Windows no puede conectarse a Internet para la activación en línea, MCS obtiene un ID de confirmación y un ID de instalación del servidor de Microsoft para activar el sistema Windows. Esta forma de activación es útil para catálogos de máquinas no persistentes.

> **Nota:**
>
> - MCS no admite la activación de Microsoft Office mediante MAK.
> - La versión mínima de VDA requerida es 2303.

Requisitos clave

- El Delivery Controller debe tener acceso a Internet.
- Crear un nuevo catálogo si la nueva imagen que va a actualizarse tiene una clave MAK distinta de la original.

- Instalar la clave MAK en la imagen maestra. Consulte Deploy MAK Activation para conocer los pasos para instalar la clave MAK en un sistema Windows.
- Si no está utilizando la preparación de imágenes:

  1. Agregue el valor de registro de DWORD `Manual` en `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
  2. Defina el valor en `1`.

Recuentos de activación Para ver el número de activaciones restantes para la clave MAK o para comprobar si una máquina virtual consume dos o más activaciones, utilice la herramienta de gestión de activación por volumen (Volume Activation Management Tool, VAMT). Consulte Install VAMT.

Activar el sistema Windows mediante MAK Para activar el sistema Windows mediante MAK:

1. Instale la clave de producto en la imagen maestra. Este paso consume un recuento de activación.
2. Cree un catálogo de máquinas de MCS.
3. Si no utiliza la preparación de imágenes:

   a) Agregue el valor de registro de DWORD `Manual` en `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatfo\Activation`.
   b) Defina el valor en `1`.

   Este método inhabilita la opción de activación con conexión.
4. Agregue máquinas virtuales al catálogo de máquinas.
5. Encienda las máquinas virtuales.
6. Dependiendo de si se trata de una activación con o sin conexión, se activa el sistema Windows.

   - Si se trata de una activación con conexión, el sistema Windows se activa después de instalar la clave del producto.
   - Si se trata de una activación si conexión, MCS se comunica con las máquinas virtuales aprovisionadas para obtener el estado de activación del sistema Windows. A continuación, MCS obtiene un ID de confirmación y un ID de instalación del servidor de Microsoft. Estos identificadores se utilizan para activar el sistema Windows.

Solución de problemas Si la máquina virtual aprovisionada no está activada con la clave MAK instalada, ejecute el comando `Get-ProvVM` o `Get-ProvScheme` en una ventana de PowerShell.

- El comando `Get-ProvScheme`: Consulte el parámetro `WindowsActivationType` asociado al catálogo de máquinas de MCS en la imagen maestra más reciente.
- El comando `Get-ProvVM`. Consulte los parámetros `WindowsActivationType`, `WindowsActivationStatus`, `WindowsActivationStatusErrorCode` y `WindowsActivation` .

Puede comprobar el error y comprobar los pasos para resolver el problema.

Crear un catálogo de máquinas mediante la interfaz de Configuración completa

Antes de crear un catálogo:

- Compruebe que ha creado una conexión con el hipervisor, servicio de nube u otro recurso que aloja las máquinas.
- Si ha creado una imagen maestra para aprovisionar máquinas. asegúrese de haber instalado un VDA en esa imagen maestra.

> **Nota:**
>
> Si utiliza un hipervisor o un servicio de nube para alojar las VM, el asistente para la creación de catálogos puede contener páginas específicas adicionales para el host en cuestión. Por ejemplo, cuando se utiliza una imagen maestra de Azure Resource Manager, el asistente de creación de catálogos contiene una página de **Tipos de licencia y almacenamiento**. Para obtener información específica sobre el host, consulte los artículos correspondientes que se mencionan en Qué hacer a continuación.

Iniciar el asistente de creación de catálogos

1. Inicie sesión en Citrix Cloud. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
2. Seleccione **Administrar**.
3. Si este es el primer catálogo que se crea, se le guiará para la selección correcta (como "Configure las máquinas y cree catálogos de máquinas para ejecutar aplicaciones y escritorios"). Se abrirá el asistente para la creación de catálogos.
4. Si ya creó un catálogo y quiere crear otro, siga estos pasos:
    a) En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.

b) Para organizar los catálogos por medio de carpetas, cree carpetas en la carpeta **Catálogos de máquinas** predeterminada. Para obtener más información, consulte Crear una carpeta de catálogo.
c) Seleccione la carpeta en la que quiere crear el catálogo y, a continuación, haga clic en **Crear catálogo de máquinas**. Se abrirá el asistente para la creación de catálogos.

El asistente le guiará a través de las páginas que se describen en las secciones siguientes. Las páginas que verá pueden variar según las opciones que escoja y la conexión (con un host) que utilice. Hosts o recursos de virtualización indica las fuentes de información de los tipos de host compatibles.

Seleccionar un tipo de máquina

Cada catálogo debe contener máquinas de un solo tipo de sistema operativo. Seleccione una de las siguientes opciones en la página **Tipo de máquina**:

- **SO multisesión:** Un catálogo de SO multisesión proporciona escritorios compartidos alojados. Las máquinas pueden ejecutar versiones compatibles de los sistemas operativos Windows o Linux, pero el catálogo no puede contener ambos sistemas a la vez.
- **SO de sesión única:** Un catálogo de SO de sesión única ofrece escritorios VDI que se pueden asignar a diferentes usuarios.
- **Acceso con Remote PC:** Un catálogo de acceso con Remote PC ofrece a los usuarios acceso remoto a sus escritorios físicos de oficina. El acceso con Remote PC no requiere una VPN para proporcionar seguridad.

Seleccionar opciones de administración de máquinas

> **Nota:**
>
> La página **Administración de máquinas** no aparece si selecciona **Acceso con Remote PC** en la página **Tipo de máquina**.

La página **Administración de máquinas** indica cómo se administran las máquinas y con qué herramienta se implementan.

Seleccione una de las opciones para indicar cómo debe administrarse la energía de las máquinas a través de la interfaz de Configuración completa:

- **Máquinas con administración de energía (por ejemplo, máquinas virtuales o PC blade)**: Esta opción solo está disponible si ya configuró una conexión con un hipervisor o un servicio de nube.
- **Máquinas sin administración de energía (por ejemplo, máquinas físicas)**

Si selecciona la opción **Máquinas con administración de energía (por ejemplo, máquinas virtuales o PC blade)**, seleccione una herramienta para crear máquinas virtuales:

- **Citrix Machine Creation Services (MCS):** Utiliza una imagen maestra para crear y administrar máquinas virtuales. Los catálogos de máquinas en entornos de nube usan MCS. MCS no está disponible para máquinas físicas.
- **Otro servicio o tecnología:** Una herramienta que administra las máquinas que ya se encuentran en el centro de datos. Citrix recomienda usar Microsoft System Center Configuration Manager u otra aplicación de terceros para una mayor uniformidad entre las máquinas del catálogo.

> **Nota:**
>
> Para máquinas con sistema operativo Linux, consulte Crear Linux VDA con Machine Creation Services (MCS).

Seleccionar una experiencia de escritorio

> **Nota:**
>
> Las opciones de la página **Experiencia de escritorio** varían según el tipo de máquina que seleccione en la página **Tipo de máquina**.

- En las máquinas con **sistema operativo multisesión**, a los usuarios se les asigna un escritorio aleatorio cada vez que inician sesión. En la página **Experiencia de escritorio**, están disponibles las siguientes opciones:
  - Guardar los cambios en el disco local de la máquina que aloja los escritorios virtuales: Persistente
  - Descartar todos los cambios y eliminar el escritorio virtual cuando el usuario cierre la sesión: No persistente

  > **Nota:**
  >
  > En el caso de las máquinas multisesión persistentes, los cambios que hagan los usuarios en los escritorios se guardarán y podrán acceder a ellos todos los usuarios autorizados.

- En el caso de las máquinas con sistema operativo de sesión única, tiene disponibles las siguientes opciones en la página **Experiencia de escritorio**:
  - Los usuarios se conectarán a un escritorio nuevo (aleatorio) cada vez que inicien sesión.
  - Los usuarios se conectarán al mismo escritorio (estático) cada vez que inicien sesión.

  Además, puede decidir si los cambios realizados por los usuarios se guardarán o se descartarán después de cerrar sesión.

Seleccionar una imagen

> **Nota:**
>
> - Esta página solo aparece si selecciona **Citrix Machine Creation Services (MCS)** en la página **Administración de máquinas**.
> - Las opciones disponibles en esta página varían en función del hipervisor o el servicio de nube.

Siga estos pasos para completar los parámetros de la página:

1. Seleccione un tipo de imagen para el catálogo de máquinas y, a continuación, seleccione una imagen. Hay dos tipos de imágenes disponibles:

   - **Imagen maestra**: Una instantánea o una máquina virtual creada como imagen maestra. Se somete a una preparación automática de imágenes al inicio de la creación del catálogo. Si es necesario, puede agregar una nota a la imagen seleccionada.

     > **Nota:**
     >
     > – Si utiliza Machine Creation Services, no debe ejecutar Sysprep en las imágenes maestras.
     > – Si especifica una imagen maestra en lugar de una instantánea, la interfaz de administración crea una instantánea, pero no se le podrá asignar ningún nombre.
     > – Aparecerá un mensaje de error si selecciona una instantánea o máquina virtual que no sea compatible con la tecnología de administración de la máquina que haya seleccionado antes en el asistente.
     > – Para actualizar las imágenes de un nodo, selecciónelo en el árbol y, a continuación, haga clic en la opción **Actualizar** en la esquina superior derecha. Si no selecciona ningún nodo de imágenes, al hacer clic en **Actualizar** se actualizan todas las imágenes del árbol. Para borrar un nodo seleccionado del árbol, mantenga presionada la tecla **CTRL** y, a continuación, haga clic en el nodo.

   - **Imagen preparada**: Una imagen que se ha sometido al proceso de preparación de imágenes y está lista para usarse directamente en la creación de máquinas virtuales. Al optar por imágenes preparadas en lugar de imágenes maestras, el proceso de creación de catálogos es más rápido y fiable, a la vez que se optimiza la administración de las imágenes durante todo el ciclo de vida.

   Para obtener más información sobre la preparación de imágenes, consulte Machine Creation Services: Image Preparation Overview and Fault-Finding.

2. Para heredar los parámetros de máquina virtual de un perfil de máquina, seleccione **Usar un perfil de máquina** y, a continuación, seleccione una especificación de plantilla de VM o ARM (específica de Azure) para usarla como perfil de máquina.

> **Nota:**
>
> Actualmente, el uso de perfiles de máquina está restringido a máquinas virtuales de Azure, AWS y GCP.

3. Seleccione el nivel funcional mínimo para el catálogo. Para que pueda utilizar las funciones más recientes del producto, compruebe que la imagen maestra tiene instalada la versión más reciente de VDA.

Configurar las máquinas

> **Nota:**
>
> - El título de esta página depende de lo seleccionado en la página **Administración de máquinas**: **Máquinas**, **Máquinas virtuales** o **Máquinas y usuarios**.
> - Esta página no aparece si selecciona **Acceso con Remote PC** en la página **Tipo de máquina**.
> - Puede crear un catálogo vacío, lo que significa que el catálogo no contiene máquinas.

- **Si utiliza MCS para crear máquinas:**
  - Especifique la cantidad de máquinas virtuales que se van a crear. Introduzca **0** (cero) si no quiere crear ninguna. Más adelante, para crear máquinas virtuales para un catálogo vacío, puede usar la opción **Agregar máquinas**.
  - Seleccione la cantidad de memoria (en MB) que tendrá cada máquina virtual.

    > **Importante:**
    >
    > Cada máquina virtual creada tendrá un disco duro. El tamaño está establecido en la imagen maestra y no se puede cambiar el tamaño del disco duro en el catálogo.

  - Si indica en la página **Experiencia de escritorio** que los cambios que los usuarios efectúen en los escritorios estáticos se deben guardar en un disco Personal vDisk aparte, especifique el tamaño del disco virtual en GB y la letra de su unidad.
  - Si la implementación utiliza más de una zona (ubicación de recursos), puede seleccionar una zona para el catálogo.
  - Si quiere crear máquinas virtuales de escritorio estático, seleccione un modo de copia para la máquina virtual. Consulte Modo de copia para la máquina virtual.
  - Si piensa crear máquinas virtuales de escritorio no persistentes aleatorias, puede habilitar y configurar la memoria caché de reescritura para los datos temporales de las máquinas a fin de mejorar el rendimiento de E/S. Para obtener más información, consulte Configurar la caché de datos temporales.

- **Si utiliza otras herramientas para proporcionar las máquinas:**

  Agregue (o importe una lista de) nombres de cuentas de máquinas. Puede cambiar el nombre de la cuenta de una VM después de agregarla o importarla. Si especificó máquinas estáticas en la página **Experiencia de escritorio**, puede especificar el nombre de usuario de Active Directory para cada máquina virtual que agregue.

  > **Sugerencia:**
  >
  > Para agregar usuarios, puede buscarlos o introducir manualmente una lista de nombres de usuario separados por puntos y comas. Si los usuarios están en Active Directory, introduzca los nombres directamente. Si no es así, introduzca los nombres en este formato: `<identity provider>:<user name>`. Ejemplo: `AzureAD:username`.

  Después de agregar o importar los nombres, puede hacer clic en el botón **Quitar** para eliminar nombres de la lista sin salir de esa página del asistente.

- **Si utiliza otras herramientas (no MCS):**

  Un icono y un cuadro de información emergente acerca de cada máquina agregada (o importada) pueden ayudarle a identificar aquellas máquinas que no sean aptas para ser agregadas al catálogo o no puedan registrarse en un Cloud Connector.

Modo de copia para la máquina virtual El modo de copia que especifique en la página **Máquinas** determina si MCS crea clones ligeros (copia rápida) o pesados (copia completa) a partir de la imagen maestra. (La opción predeterminada es clones ligeros.)

- Puede optar por los clones de copia rápida para un uso más eficiente del almacenamiento y una creación de máquinas más rápida.
- En cambio, puede utilizar los clones de copia completa para mejorar la recuperación de datos y la asistencia a la migración de datos, con IOPS potencialmente reducidas una vez creadas las máquinas.

Configurar la caché de datos temporales Al usar MCS para administrar máquinas aleatorias no persistentes en un catálogo, puede habilitar la memoria caché de reescritura para las máquinas a fin de mejorar el rendimiento de E/S.

La memoria caché de reescritura se denomina E/S de MCS. Para obtener más información, consulte este artículo del blog.

Requisitos previos Para habilitar la memoria caché de reescritura, el catálogo debe cumplir estos requisitos:

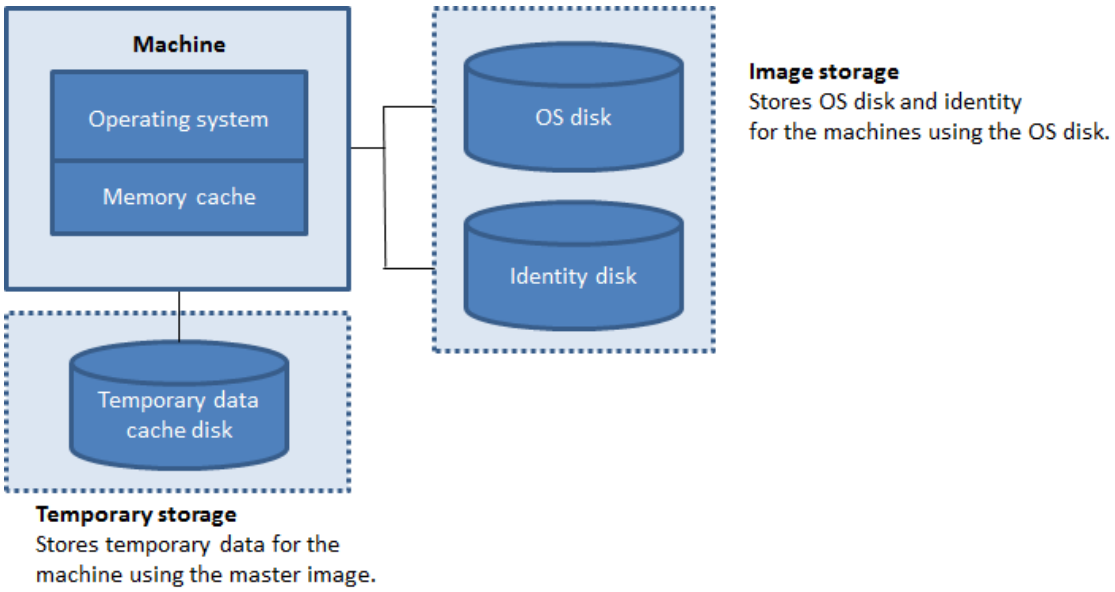
- Debe usar una conexión que especifique el almacenamiento de datos temporales. Para obtener más información, consulte Conexiones y recursos.
- Los VDA deben tener al menos la versión 7.9 e instalarse con un controlador de E/S de MCS actual.

  > **Nota:**
  >
  > La instalación de este controlador es una opción cuando instala o actualiza un VDA. De forma predeterminada, ese controlador no se instala.

- Para habilitar la asignación de letras de unidad para las cachés de disco, las máquinas virtuales deben cumplir estos requisitos adicionales:
  - Sistema operativo: Windows
  - Versión de VDA: 2305 o una posterior

Consideraciones

- Las memorias cachés de reescritura vienen en caché de *memoria* y en caché de *disco*. De forma predeterminada, sus valores predeterminados varían según el tipo de conexión. Por lo general, los valores predeterminados son suficientes para la mayoría de los casos, sin embargo, considere el espacio necesario para:
  - Archivos de datos temporales creados por Windows, incluido el archivo de paginación de Windows.
  - Datos de perfil de usuario.
  - Datos de ShareFile que se sincronizan en las sesiones de usuario.
  - Datos que pueden crear o copiar los usuarios de las sesiones, o aplicaciones que los usuarios pueden instalar dentro de la sesión.



- La configuración de la caché de reescritura con solo una memoria caché de disco y sin memoria caché ha quedado obsoleta. Para habilitar una caché para datos temporales, recomendamos seleccionar **Tamaño de caché de disco (GB)** y **Memoria asignada para caché (MB)** y especificar un tamaño superior a 0 para la memoria caché. Los datos temporales se escriben inicialmente en la memoria caché. Cuando la memoria caché alcanza su límite configurado, los datos más antiguos se trasfieren al disco de caché de datos temporales.
- La memoria caché es parte de la memoria total de cada máquina. Por lo tanto, si habilita la casilla **Tamaño de memoria caché (MB) (recomendado)**, considere aumentar la cantidad total de memoria en cada máquina.
- Cambiar el valor predeterminado del **tamaño de la caché del disco (GB)** puede afectar al rendimiento. El tamaño debe coincidir con los requisitos de los usuarios y la carga que se coloca en la máquina.

  > **Importante:**
  >
  > Si la memoria caché de disco se queda sin espacio, la sesión del usuario se vuelve inutilizable.

- Si desmarca la casilla **Tamaño de caché de disco**, no se creará ninguna caché de disco. En este caso, especifique un valor de **Memoria asignada para caché** que sea suficiente para contener todos los datos temporales. Esto es factible solo si hay grandes cantidades de RAM disponibles para asignarse a cada VM.
- Si deja sin marcar ambas casillas, los datos temporales no se almacenan en caché. Se escriben en el disco de diferenciación (ubicado en el almacenamiento de SO) para cada VM. (esta es la acción de aprovisionamiento en las versiones anteriores a la 7.9).

- No habilite el almacenamiento en caché si va a usar este catálogo para crear AppDisks.
- No puede cambiar los valores de caché en un catálogo de máquinas después de haberlo creado.

Usar archivos CSV para agregar máquinas en bloque Si utiliza la interfaz de administración **Configuración completa**, puede agregar máquinas en bloque a través de archivos CSV. La funcionalidad está disponible para todos los catálogos, excepto los creados a través de MCS.

A continuación, dispone de un flujo de trabajo general para utilizar archivos CSV y agregar máquinas en bloque:

1. En la página **Máquinas**, seleccione **Agregar archivo CSV**. Aparecerá la ventana **Agregar máquinas en bloque**.
2. Seleccione **Descargar plantilla CSV**.
3. Rellene el archivo de la plantilla.
4. Busque el archivo o arrástrelo hasta aquí para cargarlo.
5. Haga clic en **Validar** para comprobar la validación de la importación.
6. Seleccione **Importar** para completar el proceso.

Para obtener información sobre las consideraciones con respecto a los archivos CSV, consulte Aspectos que tener en cuenta al usar archivos CSV para agregar máquinas.

También puede exportar máquinas de un catálogo en la misma página Máquinas. El CSV exportado de máquinas se puede utilizar como plantilla al agregar máquinas en bloque. Para exportar máquinas:

1. En la página **Máquinas**, seleccione **Exportar en archivo CSV**. Se descarga un archivo CSV que contiene una lista de las máquinas.
2. Abra el archivo CSV para agregar o modificar máquinas según sea necesario. Para agregar máquinas en bloque mediante el archivo CSV guardado, consulte la sección anterior, Usar archivos CSV para agregar máquinas en bloque.

> **Nota:**
>
> - Esta función no está disponible para los catálogos de acceso con Remote PC.
> - La exportación e importación de máquinas en archivos CSV solo se permite entre catálogos del mismo tipo.

Configurar NIC para las máquinas

La página **Tarjetas NIC** no aparece si selecciona **Acceso con Remote PC** en la página **Tipo de máquina**.

Si quiere utilizar varias tarjetas de interfaz de red (NIC), asocie una red virtual a cada tarjeta. Por ejemplo, puede asignar una tarjeta para el acceso a una red segura concreta y otra para el acceso a una red más habitual. También puede agregar o quitar tarjetas NIC desde esta página.

Agregar cuentas de máquina

> **Nota:**
>
> Esta página **Cuentas de máquina** solo aparece cuando selecciona **Acceso con Remote PC** en la página **Tipo de máquina**.

Agregue las unidades organizativas (OU) o las cuentas de máquina de Active Directory. No use barras diagonales (/) en el nombre de una unidad organizativa.

Puede elegir una conexión de administración de energía que haya configurado previamente u optar por no usar la administración de energía. Si quiere usar la administración de energía, pero aún no se ha configurado la conexión correspondiente, puede crear dicha conexión más tarde y luego modificar el catálogo de máquinas para actualizar la configuración de la administración de energía.

También puede agregar máquinas en bloque mediante archivos CSV. A continuación, dispone de un flujo de trabajo general para ello:

1. En la página **Cuentas de máquina**, seleccione **Agregar archivo CSV**. Aparecerá la ventana **Agregar máquinas en bloque**.
2. Seleccione **Descargar plantilla CSV**.
3. Rellene el archivo de la plantilla.
4. Busque el archivo o arrástrelo hasta aquí para cargarlo.
5. Haga clic en **Validar** para comprobar la validación de la importación.
6. Seleccione **Importar** para completar el proceso.

Para obtener información sobre las consideraciones con respecto a los archivos CSV, consulte Aspectos que tener en cuenta al usar archivos CSV para agregar máquinas.

Configurar las identidades de las máquinas del catálogo

> **Nota:**
>
> - La página **Identidades de las máquinas** solo aparece cuando no selecciona **Acceso con Rermote PC** en la página **Tipo de máquina** y selecciona **Citrix Machine Creation Services (MCS)** en la página **Administración de máquinas**.

Cada máquina del catálogo debe tener una identidad única. Esta página le permite configurar las identidades de las máquinas del catálogo. Las máquinas se unen a la identidad después de aprovisionarse. No se puede cambiar el tipo de identidad después de crear el catálogo.

Un flujo de trabajo general para configurar los parámetros de esta página es el siguiente:

1. Seleccione una identidad de la lista.
2. Indique si se van a crear cuentas o si se van a utilizar cuentas existentes, además de la ubicación (dominio) de estas.

Se pueden seleccionar una de las siguientes opciones:

- **Active Directory local**: Máquinas de las que es propietaria una organización en las que se ha iniciado sesión con una cuenta de Active Directory perteneciente a esa organización. Están presentes en instancias locales.

  > **Nota:**
  >
  > De forma predeterminada, se selecciona el dominio en el que reside el recurso (conexión).

- **Unido a Azure AD**: Máquinas de las que es propietaria una organización en las que se ha iniciado sesión con una cuenta de Azure Active Directory perteneciente a esa organización. Solo existen en la nube. Para obtener información sobre los requisitos, las limitaciones y los aspectos a tener en cuenta, consulte Unido a Azure Active Directory.

  > **Nota:**
  >
  > Esta opción requiere que la imagen maestra cumpla los requisitos del sistema operativo. Para obtener más información, consulte Dispositivos unidos a Microsoft Entra en la documentación de Microsoft.

- **Unido a Azure Active Directory híbrido**. Máquinas propiedad de una organización en las que se ha iniciado sesión con una cuenta de Active Directory Domain Services perteneciente a esa organización. Existen en la nube y en instancias locales. Para obtener información sobre los requisitos, las limitaciones y los aspectos a tener en cuenta, consulte Unido a Azure Active Directory híbrido.

  > **Nota:**
  >
  > - Antes de poder usar la opción de unido a Azure Active Directory híbrido, asegúrese de que su entorno de Azure cumpla con los requisitos previos. Consulte Configurar la unión híbrida de Microsoft Entra.
  > - Esta opción requiere que la imagen maestra cumpla los requisitos del sistema operativo. Para obtener más información, consulte Dispositivos unidos a Microsoft Entra.

- **No unido a un dominio**. Máquinas que no están unidas a ningún dominio. Para obtener información sobre los requisitos y las limitaciones, consulte No unidos a ningún dominio.

> **Importante:**
>
> - Si selecciona **Active Directory local** o **Unido a Azure Active Directory híbrido** como el tipo de identidad, cada máquina del catálogo debe tener una cuenta de equipo de Active Directory correspondiente.
> - El tipo de identidad **No unido a un dominio** requiere la versión 1811 o una posterior del VDA como el nivel funcional mínimo para el catálogo. Para que esté disponible, actualice el nivel funcional mínimo.
> - Los tipos de identidad **Unido a Azure Active Directory** y **Unido a Azure Active Directory híbrido** requieren la versión 2203 o una posterior del VDA como nivel funcional mínimo para el catálogo. Para que estén disponibles, actualice el nivel funcional mínimo.

Si crea cuentas, debe tener permiso para crear cuentas de equipo en la unidad organizativa donde residen las máquinas. Cada máquina del catálogo debe tener un nombre exclusivo. Especifique el esquema de denominación de cuentas para las máquinas que quiere crear. Para obtener más información, consulte Esquema de nomenclatura de cuentas de máquina.

> **Nota:**
>
> Asegúrese de que en los nombres de las unidades organizativas no se utilizan barras inclinadas hacia delante (`/`).

Si usa cuentas existentes, vaya a esas cuentas o haga clic en **Importar** y especifique un archivo `.csv` que contenga los nombres de cuenta. El contenido del archivo importado debe tener el formato: `[ADComputerAccount] ADcomputeraccountname.domain`

Compruebe que hay cuentas suficientes para las máquinas que está agregando. La interfaz de Configuración completa administra esas cuentas. Por eso, permita que dicha interfaz restablezca las contraseñas de todas las cuentas, o bien, especifique la contraseña de la cuenta (que debe ser la misma para todas las cuentas).

Para catálogos que contienen máquinas físicas o máquinas existentes, seleccione o importe las cuentas existentes y asigne cada máquina a una cuenta de equipo de Active Directory y a una cuenta de usuario.

Esquema de nomenclatura de cuentas de máquina Cada máquina de un catálogo debe tener un nombre único. Debe especificar un esquema de nomenclatura de cuentas de máquina al crear un catálogo. Use comodines (marcas hash) como marcadores de posición para los números o letras secuenciales que aparecen en el nombre.

Al especificar un esquema de nomenclatura, tenga en cuenta lo siguiente:

- La cantidad máxima de caracteres permitida es 15.

- El esquema de nomenclatura debe contener, al menos, un carácter comodín. Debe poner todos los comodines juntos.
- El nombre completo, incluidos los comodines, debe contener al menos 2 caracteres, pero no más de 15. Debe incluir al menos un carácter no numérico y un carácter # (comodín).
- El nombre no debe incluir espacios ni ninguno de estos caracteres: `,~!@'$%^&.()} {\/*?"<>|=+[];:_".`.
- El nombre no puede terminar con un guion (-).
- La cantidad de caracteres aumenta a medida que aumenta la cantidad de cuentas de máquinas. Por ejemplo, si crea 1000 cuentas de máquina con el esquema "granlongitud#", el último nombre de cuenta creado (granlongitud1000) contiene 16 caracteres, lo que supera la cantidad máxima de caracteres permitida.

Puede indicar si los valores secuenciales son números (0-9) o letras (A-Z):

- **0-9**. Si se selecciona, los comodines especificados se traducen a números secuenciales.

  > **Nota:**
  >
  > Si solo hay un comodín (#), los nombres de las cuentas comienzan por 1. Si hay dos, los nombres de las cuentas comienzan por 01. Si hay tres, los nombres de las cuentas comienzan por 001, y así sucesivamente.

- **A-Z**. Si se selecciona, los comodines especificados se traducen a letras secuenciales.

Por ejemplo, un esquema de denominación PC-Ventas-## (con números del **0 al 9** seleccionados) da como resultado cuentas llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.

Si lo quiere, puede especificar con qué empiezan los nombres de las cuentas.

- Si selecciona **0-9**, las cuentas se designan secuencialmente, empezando por los números especificados. Introduzca uno o más dígitos, según el número de comodines que utilice en el campo anterior. Por ejemplo, si usa dos comodines, introduzca dos dígitos o más.
- Si selecciona **A-Z**, las cuentas se designan secuencialmente, empezando por las letras especificadas. Introduzca una o más letras, según el número de comodines que utilice en el campo anterior. Por ejemplo, si usa dos comodines, introduzca dos letras o más.

Agregar credenciales de dominio

Seleccione **Introducir credenciales** e introduzca las credenciales de un administrador con permiso para realizar operaciones de cuentas en el dominio de Active Directory de destino.

Utilice la opción **Comprobar nombre** para comprobar si el nombre de usuario es válido o único. La opción es útil, por ejemplo, cuando:

- El mismo nombre de usuario existe en varios dominios. Se le solicita que seleccione el usuario correspondiente.
- No se acuerda del nombre del dominio. Puede introducir el nombre del usuario sin especificar el nombre del dominio. Si la comprobación se realiza correctamente, el nombre del dominio se rellena automáticamente.

> **Nota:**
>
> Si el tipo de identidad que seleccionó en **Identidades de máquina** es **Unido a Azure Active Directory híbrido**, las credenciales que introduzca deben tener el permiso `Write userCertificate`.

Seleccionar un conjunto de configuraciones de Workspace Environment Management (opcional)

La página **WEM** aparece solamente cuando utiliza la edición Advanced o Premium de Citrix DaaS.

Seleccione un conjunto de configuraciones de Workspace Environment Management (WEM) al que quiera vincular el catálogo. Un conjunto de configuraciones es un contenedor lógico que se utiliza para organizar un conjunto de configuraciones de WEM. La vinculación de un catálogo a un conjunto de configuraciones le permite utilizar WEM para ofrecer la mejor experiencia posible en espacios de trabajo a sus usuarios.

> **Importante:**
>
> - Para poder vincular un catálogo a un conjunto de configuraciones, debe configurar la implementación de WEM Service. Inicie sesión en Citrix Cloud y, a continuación, inicie WEM Service. Para obtener más información, consulte Introducción a Workspace Environment Management Service.
> - Si ya utiliza WEM, es posible que las máquinas del catálogo que va a aprovisionar ya estén presentes en un conjunto de configuraciones. Por ejemplo, a través de Active Directory. En ese caso, le recomendamos que utilice Active Directory de principio a fin para realizar la configuración y omitir esta configuración.

Si el conjunto de configuraciones seleccionado no contiene parámetros relacionados con la configuración básica de WEM, aparece esta opción:

- **Aplicar parámetros básicos al conjunto de configuraciones**. Esta opción le permite empezar rápidamente a utilizar WEM mediante la aplicación de parámetros básicos al conjunto de configuraciones. Los parámetros básicos incluyen la protección contra picos de CPU, la prevención automática de picos de CPU y la optimización inteligente de la CPU. Para ver los parámetros básicos, haga clic en el enlace *Aquí*. Para modificarlos, use la consola de WEM.

Actualizar la versión de los VDA (opcional)

> **Importante:**
>
> - Para garantizar una actualización de versión fluida, asegúrese de cumplir los requisitos previos y de revisar los problemas conocidos antes de actualizar los VDA a las versiones CR o LTSR CU. Consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.
> - Al actualizar los VDA LTSR a las versiones LTSR CU (actualización acumulativa), asegúrese de que la versión de los agentes de actualización de VDA que se ejecutan en los VDA sea 7.36.0.7 o posterior. Para obtener más información, consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.

Esta función se aplica a estos tipos de máquinas:

- Máquinas persistentes aprovisionadas por MCS. Se implementan mediante **Citrix Machine Creation Services** en la página **Administración de máquinas** durante la creación del catálogo.
- Máquinas que no se crean con MCS (por ejemplo, máquinas físicas). Se implementan mediante **Otro servicio o tecnología** en la página **Administración de máquinas** durante la creación del catálogo.

Para obtener más información sobre las dos opciones, consulte Administración de máquinas.

En la página **Actualización de versión de VDA**, seleccione la versión del VDA a la que quiere actualizarse. Si se especifica, los VDA del catálogo que tienen instalado el agente de actualización de versiones de VDA pueden actualizarse a la versión seleccionada: de forma inmediata o a una hora programada.

> **Nota:**
>
> - Esta función solo permite la actualización a la versión más reciente del VDA. La hora a la que se crea un programa de actualización de un VDA o a la que se actualiza la versión de un VDA determina la versión más reciente del VDA.
> - Después de configurar los parámetros de actualización de versión del VDA, es posible que el campo **Actualización de versión del VDA** tarde hasta 15 minutos en reflejar el estado más reciente. Para mostrar la columna **Actualización de versión de VDA**, haga clic en el icono Columnas que mostrar de la esquina superior derecha, seleccione **Catálogo de máquinas > Actualización de versión de VDA** y haga clic en **Guardar**.

Elija una opción de VDA que se adapte a su implementación:

> **Importante:**
>
> Puede cambiar entre VDA CR (Current Release) y VDA LTSR (Long Term Service Release) siempre

> que cambie de una versión anterior a una versión posterior. No puede cambiar de una versión posterior a una anterior porque se considera una reversión. Por ejemplo, no puede cambiar de la versión 2212 CR a 2203 LTSR (cualquier CU), pero puede actualizar la versión 2112 CR a 2203 LTSR (cualquier CU).

- **La versión CR más reciente de VDA**. Las versiones Current Release (CR) ofrecen las funciones más recientes e innovadoras sobre virtualización de aplicaciones, escritorios y servidores.
- **La versión LTSR más reciente de VDA**. Se recomiendan las versiones Long Term Service Releases (LTSR) para entornos de producción de grandes empresas que prefieren conservar la misma versión base durante un período prolongado.

Tras la creación del catálogo, puede actualizar la versión de los VDA según sea necesario. Para obtener más información, consulte Actualizar la versión de los VDA.

Si quiere habilitar la actualización de versión de los VDA más adelante, puede modificar el catálogo después de crearlo para volver a esta página. Para obtener más información, consulte Configurar los parámetros de actualización de versión del VDA mediante la modificación de un catálogo.

Revisar los parámetros

En la página **Resumen**, revise la configuración especificada. Introduzca un nombre y una descripción para el catálogo. Esta información aparece en la interfaz de administración de Configuración completa.

Cuando haya terminado, seleccione **Finalizar** para iniciar la creación del catálogo.

En **Catálogos de máquinas**, el nuevo catálogo aparece con una barra de progreso integrado.

Para ver los detalles del progreso de la creación:

1. Pase el mouse por encima del catálogo de máquinas.
2. En el texto de ayuda que aparece, haga clic en **Ver detalles**.

   Aparece un gráfico de progreso detallado en el que puede ver lo siguiente:

   - Historial de los pasos
   - Progreso y tiempo de ejecución del paso actual
   - Pasos restantes

Crear un catálogo de máquinas de MCS mediante comandos de PowerShell

También puede crear un catálogo de máquinas de MCS mediante comandos de PowerShell. Para obtener más información, consulte:

- SDK y API
- Administrar Citrix DaaS mediante Remote PowerShell SDK
- New-ProvScheme

Asignar una letra de unidad específica a un disco de la memoria caché de reescritura de E/S de MCS

Puede asignar una letra de unidad específica a un disco de la memoria caché de reescritura de E/S de MCS. Esta implementación le ayuda a evitar conflictos entre la letra de la unidad de cualquier aplicación que utilice y la letra de la unidad del disco de la memoria caché de reescritura de E/S de MCS. Para hacer esto, puede ser comandos de PowerShell. Los hipervisores compatibles son Azure, GCP, VMware, SCVMM y XenServer.

> **Nota:**
>
> Esta función requiere la versión 2305 de VDA o una posterior.

Limitaciones

- Aplicable solo al sistema operativo Windows
- Letra de unidad aplicable al disco de la memoria caché de reescritura: De E a Z
- No se aplica cuando el disco temporal de Azure se utiliza como disco de la memoria caché de reescritura
- Aplicable solo cuando al crear otros catálogos de máquinas

Asignar una letra de unidad a un disco de la memoria caché de reescritura Para asignar una letra de unidad al disco de la memoria caché de reescritura:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Cree un grupo de identidades si aún no se ha creado. Para obtener más información, consulte Creación de un catálogo.
4. Cree un esquema de aprovisionamiento mediante el comando `New-ProvScheme` con la propiedad `WriteBackCacheDriveLetter`. Por ejemplo:

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "<name>" `
-IdentityPoolName $schemeName `
-ProvisioningSchemeName $schemeName `
-InitialBatchSizeHint 1 `
-UseWriteBackCache -WriteBackCacheDiskSize 127 -
    WriteBackCacheMemorySize 256 -WriteBackCacheDriveLetter E `
```



```
-MasterImageVM "XDHyp:\HostingUnits<name>\image.folder\abcd-resources.resourcegroup\MCSIOMasterVm_OsDisk_1_d3e2d6352xxxxxxxxx2130aa145ec77.manageddisk" `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\name\virtualprivatecloud.folder\East US. region\virtualprivatecloud.folder\abcd-resources.resourcegroup\abcd-resources-vnet.virtualprivatecloud\default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\<name>\serviceoffering.folder\Standard_D2s_v5.serviceoffering" `
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS"/>
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false" />
<Property xsi:type="StringProperty" Name="PersistVm" Value="false" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value="false" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="abcd-group1" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Termine de crear el catálogo.

Consideraciones importantes sobre la configuración de propiedades personalizadas

Las propiedades personalizadas se deben establecer correctamente en `New-ProvScheme` y `Set-ProvScheme` en entornos de GCP y Azure. Si especifica propiedades personalizadas que no existen, aparece este mensaje de error y los comandos no se ejecutan.

```
Invalid property found: <invalid property>. Ensure that the CustomProperties parameter supports the property.
```


Consideración importante sobre la configuración de parámetros de ProvScheme

Cuando utiliza MCS para crear un catálogo, se produce un error si:

- Establece estos parámetros `New-ProvScheme` en hipervisores no compatibles al crear un catálogo de máquinas:

Parámetro	Hipervisor compatible
`UseWriteBackCache`	VMware
	Hyper-V
	XenServer
	Azure
	GCP
`DedicatedTenancy`	Azure
	GCP
	AWS
`TenancyType`	Azure
	GCP
	AWS
`UseFullDiskCloneProvisioning`	VMware
	Hyper-V
	XenServer

- Actualiza estos parámetros `Set-ProvScheme` después de crear el catálogo de máquinas:
  - `CleanOnBoot`
  - `UseWriteBackCache`
  - `DedicatedTenancy`
  - `TenancyType`
  - `UseFullDiskCloneProvisioning`

Agregar SID al crear máquinas virtuales

Puede agregar el parámetro `ADAccountSid` para identificar unívocamente las máquinas al crear nuevas máquinas virtuales.

Para hacerlo:

1. Cree un catálogo con el tipo de identidad admitido.
2. Agregue máquinas al catálogo mediante `NewProvVM`. Por ejemplo:

```
New-ProvVM  -ProvisioningSchemeName "name"  -ADAccountSid @("SID "
    )  -RunAsynchronously
<!--NeedCopy-->
```

Sin embargo, no puede aprovisionar una máquina con:

- Una cuenta de AD que no esté en el grupo de identidades del catálogo
- Una cuenta de AD que no esté disponible

Validar la configuración antes de crear un catálogo de máquinas MCS

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

> **Nota:**
>
> Durante la validación, no debe crear un catálogo de máquinas MCS real. Debe usar el resultado del comando para corregir los errores y después crear un catálogo correcto. Por lo tanto, mientras ejecuta el comando `New-ProvScheme`, use un nombre de grupo de identidades falso.

Para validar la configuración, lleve a cabo los siguientes pasos:

1. Abra una ventana de PowerShell desde el host del Delivery Controller.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute el comando `New-ProvScheme` y use el parámetro `-validate`. Proporcione un nombre de grupo de identidades falso para que el comando funcione. Por ejemplo,

```
$result =New-ProvScheme  -CleanOnBoot -HostingUnitName "vSanRg" -
    IdentityPoolName "mptmpcatalogdemo" -InitialBatchSizeHint 1  -
    MasterImageVM "XDHyp:\HostingUnits\vSanRg\Windows19MasterImage.
    vm\Citrix_XD_NonMachineProfileWin19Machines.snapshot" -
    NetworkMapping @{
 "0"="XDHyp:\HostingUnits\vSanRg\VM Network.network" }
  -ProvisioningSchemeName "MachineProfileW10Machines"  -Scope @()
-VMCpuCount 2  -VM
MemoryMB 6143 -MachineProfile "XDHyp:\HostingUnits\vSanRg\TRW-
    Win11-tpm-BL-TEMPLATE.template" -TenancyType Shared  -
    FunctionalLevel "L7_20" -Validate
```



```
$result.TerminatingError | Format-List -Property *
<!--NeedCopy-->
```

Mensaje de error:

```
ErrorData    : {
 [[ValidationFailureCount, xxx], [InvalidMemoryValue, The memory
    size provided 6143 must be a multiple of 4 MB and must be
    greater than or equal to 4 MB.], [InconsistentGuestOsSetting,
    The GuestOs setting - windows9_64Guest of the selected machine
     profile does not match with the setting -
    windows2019srv_64Guest of master image. Please select a
    machine profile that matches the GuestOs setting of the master
     image.], [InconsistentVtpmSetting, The vTPM setting of the
    selected machine profile does not match with the selected
    master image. Please select a machine profile that matches the
     vTPM setting of the master image.], [
    InconsistentFirmwareSetting, The firmware setting - efi of the
     selected machine profile does not match with the setting -
    bios of master image. Please select a machine profile that
    matches the firmware setting of the master image ErrorId
    : ValidationFailure
ErrorMessage : ValidationFailure
Operation    : ValidatingInputs
<!--NeedCopy-->
```

4. Tras validar los parámetros de configuración, puede crear un catálogo de máquinas MCS con un nombre real del grupo de identidades y los parámetros correctos.

Qué hacer a continuación

Para obtener información sobre la creación de catálogos de hipervisores específicos, consulte:

- Crear un catálogo de AWS
- Crear un catálogo de Google Cloud Platform
- Crear un catálogo de Microsoft Azure
- Crear un catálogo de Microsoft System Center Virtual Machine Manager
- Crear un catálogo de Nutanix
- Crear un catálogo de VMware
- Crear un catálogo de XenServer

Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.

Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.

Ahora puede crear un catálogo de Citrix Provisioning mediante la interfaz de usuario de Configuración completa y PowerShell.
Esta implementación le ofrece las siguientes ventajas:

- Una única consola unificada para administrar los catálogos de MCS y de Citrix Provisioning.
- Hay nuevas funciones para los catálogos de Citrix Provisioning, como la solución de administración de identidades, el aprovisionamiento bajo demanda, etc.

Actualmente, esta función solo está disponible para las cargas de trabajo de Azure y VMware. Sin embargo, en los entornos VMware, actualmente puede crear los catálogos utilizando únicamente comandos de PowerShell. Para obtener más información, consulte Crear catálogos de Citrix Provisioning en Citrix Studio.

Más información

- Administración de imágenes de Citrix Virtual Apps and Desktops
- Crear y administrar conexiones y recursos
- Crear catálogos unidos a identidades de máquinas
- Administrar catálogos de máquinas

Crear un catálogo de AWS

May 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de AWS.

> **Nota:**
>
> Antes de crear un catálogo de AWS, debe terminar de crear una conexión con AWS. Consulte Conexión con AWS.

Configuración de la red durante la preparación de imágenes

Durante la preparación de la imagen, se crea una máquina virtual (VM) de preparación basada en la máquina virtual original. Esta máquina virtual de preparación está desconectada de la red. Para desconectar la red de la máquina virtual de preparación, se crea un grupo de seguridad de red para denegar todo el tráfico entrante y saliente. Este grupo de seguridad de red persiste y se reutiliza. El nombre del grupo de seguridad de red es `Citrix.XenDesktop.IsolationGroup-GUID`, donde el GUID se genera aleatoriamente.

Arrendamiento de AWS

AWS ofrece estas opciones de arrendamiento: arrendamiento compartido (el tipo predeterminado) y arrendamiento dedicado. El arrendamiento compartido significa que es posible que varias instancias de Amazon EC2 de diferentes clientes residan en el mismo hardware físico. El arrendamiento dedicado significa que las instancias de EC2 se ejecutan únicamente en hardware con otras instancias que haya implementado. Los demás clientes no utilizan el mismo hardware.

Puede usar MCS para aprovisionar hosts dedicados de AWS mediante la interfaz de Configuración completa o PowerShell.

Requisitos para el aprovisionamiento a los hosts de AWS

- Una imagen (AMI) importada de BYOL (bring your own license). Con hosts dedicados, puede usar y administrar sus licencias existentes.
- Una asignación de hosts dedicados con suficiente utilización para abarcar las solicitudes de aprovisionamiento.
- Habilitar el **emplazamiento automático**.

Configurar el arrendamiento de host dedicado de AWS mediante la interfaz de Configuración completa

Al utilizar MCS para crear un catálogo y, así, aprovisionar máquinas en AWS, la página **Configuración de catálogo de máquinas > Seguridad** presenta estas opciones:

- **Usar un hardware compartido**. Esta configuración es adecuada para la mayoría de las implementaciones. Varios clientes comparten componentes de hardware aunque no interactúen entre sí. El uso de hardware compartido es la opción menos costosa para utilizar instancias de Amazon EC2.
- **Usar host dedicado**. Un host dedicado de Amazon EC2 es un servidor físico con una capacidad de instancias de EC2 totalmente dedicada, lo que le permite utilizar licencias de software por socket o máquina virtual existentes. Los hosts dedicados tienen una utilización predeterminada basada en el tipo de instancia. Por ejemplo: un único host dedicado asignado de los tipos de instancia C4 Large está limitado a ejecutar 16 instancias. Consulte el sitio de AWS para obtener más información.
- **Usar instancia dedicada**. Este parámetro es más adecuado para implementaciones con requisitos específicos de seguridad o de cumplimiento de normas. Con una instancia dedicada, seguirá disfrutando de las ventajas de tener un host separado de los demás clientes de AWS, pero sin pagar por todo el host. No es necesario preocuparse por la capacidad del host, pero se le cobrará una tarifa más alta por las instancias.

Esta configuración es adecuada para implementaciones con restricciones de licencias o requisitos de seguridad que exigen el uso de un host dedicado. Con un host dedicado, dispone de un host físico completo, y se factura por hora. Al tener ese host, puede poner en marcha tantas instancias de EC2 como permita dicho host sin cargos adicionales.

> **Nota:**
>
> Puede eliminar discos de identidad de preparación disponibles si no hay ninguna tarea en curso de creación de catálogos o actualización de imágenes.

Configurar el arrendamiento de host dedicado de AWS mediante PowerShell

También puede aprovisionar hosts dedicados de AWS a través de PowerShell. Use el cmdlet `New-ProvScheme` con el parámetro `TenancyType` establecido en `Host`.

Capturar la propiedad de instancia de AWS

Cuando crea un catálogo para aprovisionar máquinas con Machine Creation Services (MCS) en AWS, selecciona una imagen AMI que represente la imagen maestra de ese catálogo. A partir de esa imagen AMI, MCS utiliza una instantánea del disco.

> **Sugerencia:**
>
> Para utilizar la captura de propiedades de instancias de AWS, debe tener una máquina virtual asociada a la imagen AMI.

MCS lee las propiedades de la instancia de la que se obtuvo la imagen AMI y aplica el rol y etiquetas de IAM (Administración de acceso e identidad) de la máquina a las máquinas aprovisionadas de un catálogo determinado. Cuando se utiliza esta función opcional, el proceso de creación de catálogos busca la instancia AMI de origen seleccionada, leyendo un conjunto limitado de propiedades. Estas propiedades se almacenan en una plantilla de inicio de AWS, que sirve para aprovisionar las máquinas de ese catálogo. Cualquier máquina del catálogo heredará las propiedades de instancia capturadas.

Las propiedades capturadas incluyen:

- Roles de IAM: Aplicados a las instancias aprovisionadas.
- Etiquetas: Aplicadas a las instancias aprovisionadas, sus discos y sus NIC. Estas etiquetas se aplican a los recursos transitorios de Citrix, incluidos: el depósito y objetos de S3, imágenes AMI, instantáneas y plantillas de inicio.

> **Sugerencia:**
>
> El etiquetado de los recursos transitorios de Citrix es optativo y se puede configurar mediante la propiedad personalizada `AwsOperationalResourcesTagging`. Para aplicar etiquetas correctamente y crear un catálogo de AWS con etiquetado de recursos operativos, no elimine la instancia de EC2 que se utilizó para crear la imagen AMI.

Capturar la propiedad de instancia de AWS

Puede utilizar esta funcionalidad especificando una propiedad personalizada, `AwsCaptureInstancePropert`, al crear un esquema de aprovisionamiento para una conexión de host de AWS:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true"
...<standard provscheme parameters
```

Consulte el New-ProvScheme para obtener más información.

> **Nota:**
>
> `AwsCaptureInstanceProperties` se ha retirado. En su lugar, recomendamos usar perfiles de máquina para especificar las propiedades de las máquinas virtuales.

Etiquetar un recurso operativo de AWS

Una imagen AMI (Amazon Machine Image) representa un tipo de dispositivo virtual utilizado para crear una máquina virtual dentro del entorno de Amazon Cloud, conocido comúnmente como EC2. Puede utilizar una imagen AMI para implementar servicios que utilicen el entorno EC2. Cuando crea un catálogo para aprovisionar máquinas con MCS en AWS, selecciona una imagen **AMI** que sirve de imagen maestra para ese catálogo.

> **Importante:**
>
> La creación de catálogos mediante la captura de una propiedad de instancia y una plantilla de inicio es necesaria para utilizar el etiquetado de recursos operativos.

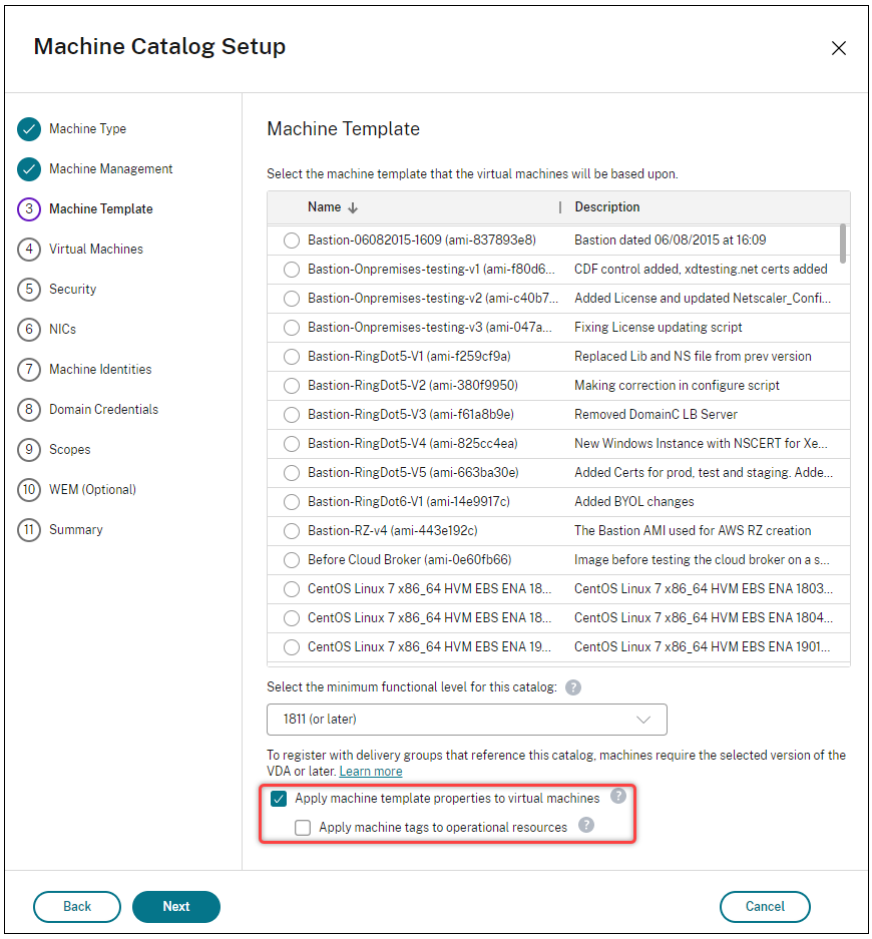
Para crear un catálogo de AWS, primero debe crear una imagen AMI de la instancia que quiere que sirva de imagen maestra. MCS lee las etiquetas de esa instancia y las incorpora a la plantilla de inicio. A continuación, las etiquetas de la plantilla de inicio se aplican a todos los recursos de Citrix creados en su entorno de AWS, incluidos:

- Máquinas virtuales
- Discos de VM
- Interfaces de red de VM
- Depósitos de S3

- Objetos de S3
- Plantillas de lanzamiento
- Imágenes AMI

Aplicar propiedades de instancias de AWS y etiquetar recursos operativos en la interfaz de Configuración completa

Al crear un catálogo para aprovisionar máquinas mediante MCS en AWS, puede decidir si aplicar las propiedades de etiqueta y el rol de IAM a esas máquinas. También puede decidir si aplicar etiquetas de máquina a los recursos operativos. Dispone de estas dos opciones:



- **Aplicar propiedades de plantilla de máquina a máquinas virtuales**
  - Controla si se aplican a las máquinas virtuales de este catálogo las propiedades de etiqueta y rol de IAM asociadas a la plantilla de máquina seleccionada.
- **Aplicar etiquetas de máquina a recursos operativos**
  - Controla si aplicar etiquetas de máquina a cada elemento creado en el entorno de AWS que facilite el aprovisionamiento de máquinas. Los recursos operativos se crean como

subproductos de la creación de catálogos. Constan de recursos temporales y persistentes, como la instancia de VM de preparación y Amazon Machine Image.

Etiquetar un recurso operativo con PowerShell

Para usar PowerShell para etiquetar recursos:

1. Abra una ventana de PowerShell desde el host de DDC (Desktop Delivery Controller).
2. Ejecute el comando `asnp citrix` para cargar módulos de PowerShell específicos de Citrix.

Para etiquetar un recurso para una máquina virtual aprovisionada, utilice la propiedad personalizada `AwsOperationalResourcesTagging`. La sintaxis de esta propiedad es:

```
New-ProvScheme -CustomProperties "AwsCaptureInstanceProperties,true;
AwsOperationalResourcesTagging,true" ...<standard provscheme parameters
>
```

Crear un catálogo de máquinas basado en perfiles de máquina con PowerShell

Puede usar un perfil de máquina para capturar las propiedades de hardware de una instancia de EC2 (VM) o versión de plantilla de inicio y aplicarlas a las máquinas aprovisionadas. Las propiedades que se capturan pueden incluir, por ejemplo, las propiedades del volumen de EBS, el tipo de instancia, la optimización de EBS, opciones de CPU, tipo de arrendamiento, capacidad de hibernación y otras configuraciones de AWS compatibles.

Puede usar una instancia (VM) de AWS EC2 o una versión de plantilla de inicio de AWS como entrada del perfil de máquina.

> **Nota:**
>
> Las propiedades del volumen de EBS se derivan únicamente de un perfil de máquina.

Consideraciones importantes

Consideraciones importantes a la hora de crear un catálogo de máquinas de MCS:

- Si agrega parámetros de propiedades de hardware de máquina en los comandos `New-ProvScheme` y `Set-ProvScheme`, los valores proporcionados en los parámetros sobrescriben los valores del perfil de máquina.
- Si asigna a `AwsCaptureInstanceProperties` el valor **`true`** y no establece la propiedad `MachineProfile`, solo se capturarán los roles y etiquetas de IAM.

- No puede establecer `AwsCaptureInstanceProperties` y `MachineProfile` al mismo tiempo.

  > **Nota:
  >
  > `AwsCaptureInstanceProperties` se ha retirado.

- Si no se proporciona un perfil de máquina, debe proporcionar explícitamente los valores de las siguientes propiedades:
  - Grupo de seguridad
  - ENI o red virtual
- Solo puede habilitar `AwsOperationalResourcesTagging` si habilita `AwsCaptureInstancePrope` o especifica un perfil de máquina.

Una consideración importante después de crear un catálogo de máquinas de MCS es:

- No se puede cambiar un catálogo basado en perfiles de máquina a un catálogo no basado en perfiles de máquina.

Crear un catálogo de máquinas mediante un perfil de máquina

Para crear un catálogo de máquinas mediante un perfil de máquina

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Cree un grupo de identidades si aún no se ha creado. Por ejemplo,

```
1 New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
     Domain abcdf -NamingSchemeType Numeric
2 <!--NeedCopy-->
```

4. Ejecute el comando New-ProvScheme. Por ejemplo:

```
1 New-ProvScheme -ProvisioningSchemeName demet-test-1
2 -HostingUnitUid aa633238-9xxd-4cf6-80e8-232a758a1xx1
3 -IdentityPoolUid 34d5b088-e312-416f-907d-16573xxxxxc4
4 -CleanOnBoot
5 -MasterImageVM 'XDHyp:\HostingUnits\cvad-test-scalestress\citrix-
     demet-ami.0 (ami-0ca813xxxxxx061ef).template'
6 -MachineProfile 'XdHyp:\HostingUnits\cvad-test-scalestress\us-east
     -1a.availabilityzone\machine-profile-instance i (i-0xxxxxxxx).
     vm'
7 <!--NeedCopy-->
```

5. Complete la creación del catálogo.

Actualizar el perfil de las máquinas

Para actualizar el perfil de máquina en un catálogo al que inicialmente se aprovisionó un perfil de máquina, haga lo siguiente. También puede cambiar el tipo de arrendamiento y la capacidad de hibernación del origen del perfil de máquina mientras modifica un catálogo de máquinas de MCS.

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo,

```
Set-ProvScheme `
-ProvisioningSchemeUid "<ID" `
-MachineProfile "XDHyp:\HostingUnits\abc\us-east-1a.
   availabilityzone\citrix-cvad-machineprofile-instance (i-0
   xxxxxxxx).vm"
<!--NeedCopy-->
```

Crear un catálogo con la versión de la plantilla de inicio mediante PowerShell

Puede crear un catálogo de máquinas de MCS con una versión de plantilla de inicio como entrada del perfil de máquina. También puede actualizar la entrada de un catálogo de perfiles de máquina de una máquina virtual a una versión de plantilla de inicio y de una versión de plantilla de inicio a una máquina virtual.

En la consola EC2 de AWS, puede proporcionar la información de configuración de instancia de una plantilla de inicio junto con el número de versión. Cuando se especifica la versión de la plantilla de inicio como entrada del perfil de máquina al crear o actualizar un catálogo de máquinas, las propiedades de esa versión de la plantilla de inicio se copian en las máquinas virtuales con VDA aprovisionadas.

Las siguientes propiedades se pueden proporcionar mediante la entrada del perfil de máquina o de forma explícita como parámetros en los comandos `New-ProvScheme` y `Set-ProvScheme`. Si se proporcionan en los comandos `New-ProvScheme` o `Set-ProvScheme`, tienen prioridad sobre los valores de estas propiedades del perfil de máquina.

- Oferta de servicios
- Redes
- Grupos de seguridad
- Tipo de arrendamiento

> **Nota:**
>
> Si la oferta de servicios no se proporciona en la plantilla de inicio del perfil de la máquina o como parámetro del comando `New-ProvScheme`, aparecerá el error correspondiente.

Para crear un catálogo con la versión de la plantilla de inicio como entrada del perfil de máquina:

1. Abra una ventana de **PowerShell**.

2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Obtenga la lista de versiones de una plantilla de inicio. Por ejemplo:

```
XDHyp:\HostingUnits\test\test-mp-sard (lt-01xxxxx).launchtemplate>
    ls | Select FullPath
<!--NeedCopy-->
```

4. Cree un grupo de identidades si no se ha creado. Por ejemplo:

```
New-AcctIdentityPool `
-IdentityPoolName "abc11" `
-NamingScheme "abc1-##" `
-NamingSchemeType Numeric `
-Domain "citrix-xxxxxx.local" `
-ZoneUid "xxxxxxxx" `
<!--NeedCopy-->
```

5. Cree un esquema de aprovisionamiento con una versión de plantilla de inicio como entrada del perfil de máquina. Por ejemplo:

```
New-ProvScheme `
-ProvisioningSchemeName "MPLT1" `
-HostingUnitUid "c7f71f6a-3f45-4xxx-xxxx-xxxxxxxxxx" `
-IdentityPoolUid "bf3a6ba2-1f80-4xxx-xxxx-xxxxxxxxx" `
-MasterImageVM "XDHyp:\HostingUnits\xxxd-ue1a\apollo-non-
   persistent-vda-win2022 (ami-0axxxxxxxxxx).template" `
-CleanOnBoot `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
   (lt-01xxxxx).launchtemplate\lt-01xxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

6. Registre un esquema de aprovisionamiento como un catálogo de broker. Por ejemplo:

```
New-BrokerCatalog -Name "MPLT1" `
-AllocationType Random `
-Description "Machine profile catalog" `
-ProvisioningSchemeId fe7df345-244e-4xxxx-xxxxxxxxx `
-ProvisioningType Mcs `
-SessionSupport MultiSession `
-PersistUserChanges Discard
<!--NeedCopy-->
```

7. Complete la creación del catálogo.

Actualizar el origen del perfil de máquina

También puede actualizar la entrada de un catálogo de perfiles de máquina de una máquina virtual a una versión de plantilla de inicio y de una versión de plantilla de inicio a una máquina virtual. Por ejemplo:

- Para actualizar la entrada de un catálogo de perfiles de máquina de una VM a una versión de plantilla de inicio:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\xxxx-ue1a\machineprofiletest
    (lt-0bxxxxxxxxxxxx).launchtemplate\lt-0bxxxxxxxxxxx (1).
   launchtemplateversion"
<!--NeedCopy-->
```

- Para actualizar la entrada de un catálogo de perfiles de máquina de una versión de plantilla de inicio a una VM:

```
Set-ProvScheme -ProvisioningSchemeName "CloudServiceOfferingTest"
    `
-MachineProfile "XDHyp:\HostingUnits\sard-ue1a\us-east-1a.
   availabilityzone\apollo-non-persistent-vda-win2022-2 (i-08
   xxxxxxxxx).vm"
<!--NeedCopy-->
```

Cifrar los discos de ID y sistema operativo

Puede crear un catálogo persistente y no persistente de máquinas virtuales con claves de AWS KMS (clave administrada por el cliente y clave administrada por AWS) que se puede usar para cifrar el disco del sistema operativo y el disco de identidad (ID).

- Las claves administradas por AWS se rotan automáticamente cada año.
- La rotación automática de las claves administradas por el cliente es opcional y se puede administrar manualmente.

Puede consultar los siguientes documentos de AWS para obtener más información sobre las claves de KMS:

- Conceptos de AWS KMS
- Cómo funciona la rotación automática de claves

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

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

Limitaciones

Tenga en cuenta las siguientes limitaciones:

- Actualmente, MCS solo admite un disco en la AMI de imagen maestra.
- No puede cifrar directamente los volúmenes o las instantáneas de EBS sin cifrar existentes, ni modificar la clave de KMS de un volumen cifrado existente. Para ello, debe:

  1. Cree una nueva instantánea de ese volumen.
  2. Crear un volumen nuevo a partir de esa instantánea
  3. Cifrar el nuevo volumen.

Consulte los siguientes documentos de AWS:

- Cifrar recursos no cifrados
- Limitaciones del cifrado automático o predeterminado de los volúmenes de EBS: Cifrar automáticamente volúmenes de Amazon EBS nuevos y existentes.

Crear un catálogo con cifrado de disco

Puede crear un catálogo de máquinas de MCS con cifrado de disco mediante:

- Imagen maestra
- Perfil de máquina

Consideraciones al usar la entrada de perfil de máquina:

- La clave de KMS de la entrada del perfil de máquina tiene prioridad sobre la clave de KMS de la imagen maestra.
- Si no se proporciona ninguna entrada de perfil de máquina, se usa la clave de KMS de la AMI de la imagen maestra para cifrar los discos de las máquinas virtuales del catálogo.
- Si el perfil de máquina contiene asignaciones de dispositivos de bloques, los dispositivos de bloques presentes en la plantilla de imagen maestra (AMI) y el perfil de máquina deben coincidir. Por ejemplo, si la AMI tiene un dispositivo definido en `/dev/sda1`, el perfil de la máquina también debe tener un dispositivo definido en `/dev/sda1`.
- Si no hay ninguna clave en el origen del perfil de máquina y la imagen maestra no está cifrada, los discos de las máquinas virtuales del catálogo no se cifran.
- Cuando la imagen maestra está cifrada, una plantilla de inicio o VM de origen de perfil de máquina debe tener un volumen raíz cifrado para que se considere una entrada válida.

Modificar un catálogo existente

Puede modificar un catálogo existente mediante el comando `Set-ProvScheme` de PowerShell para tener:

- Una entrada de perfil de máquina con un volumen que contiene una nueva clave de KMS.

- Una AMI de plantilla de imagen maestra cifrada con una nueva clave de KMS.

Consideraciones importantes:

- Los volúmenes de nuevas máquinas virtuales que se agregan al catálogo se cifran con la nueva clave de KMS.
- Para actualizar los parámetros de cifrado cuando hay un perfil de máquina existente, ejecute `Set-ProvScheme` con un nuevo perfil de máquina.
- No puede modificar un catálogo existente para que pase de tener volúmenes cifrados a volúmenes no cifrados.
  No puede actualizar la imagen de una AMI maestra cifrada a una AMI maestra no cifrada.

Copiar etiquetas en máquinas virtuales

Puede copiar las etiquetas de las NIC y los discos (disco de identidad, disco de caché de reescritura y disco de sistema operativo) que se especifican en el perfil de la máquina a las máquinas virtuales recién creadas en un catálogo de máquinas de MCS. Puede especificar estas etiquetas en cualquiera de las fuentes de perfiles de máquinas (instancia de máquina virtual de AWS o versión de plantilla de lanzamiento de AWS). Esta función se aplica a máquinas virtuales y catálogos de máquinas persistentes y no persistentes.

> **Nota:**
>
> - En la consola AWS EC2, no puede ver los valores de **Etiquetar interfaces de red** en las **etiquetas de recursos de versión de la plantilla de inicio**. No obstante, puede ejecutar el comando de PowerShell `aws ec2 describe-launch-template-versions --launch-template-id lt-0bb652503d45dcbcd --versions 12` para ver las especificaciones de las etiquetas.
> - Si un origen de perfil de máquina (máquina virtual o versión de plantilla de inicio) tiene dos interfaces de red (eni-1 y eni-2), y eni-1 tiene la etiqueta t1 y eni-2 tiene la etiqueta t2, la VM obtiene las etiquetas de las dos interfaces de red.

Filtrar instancias de VM con PowerShell

Una instancia de máquina virtual de AWS que utilice como máquina virtual de perfil de máquina debe ser compatible para que el catálogo de máquinas se cree y funcione correctamente. Para enumerar las instancias de máquinas virtuales de AWS que se pueden usar como máquinas virtuales de entrada de perfil de máquina, puede usar el comando `Get-HypInventoryItem`. El comando puede buscar en páginas y filtrar el inventario de máquinas virtuales disponibles en una unidad de alojamiento.

Paginación:

Get-HypInventoryItem admite dos modos de paginación:

- El modo de paginación utiliza los parámetros `-MaxRecords` y `-Skip` para devolver conjuntos de elementos:
  - `-MaxRecords`: El valor predeterminado es **1**. Esto controla la cantidad de elementos que devolverán.
  - `-Skip`: El valor predeterminado es **0**. Esto controla la cantidad de elementos que se deben omitir desde el principio absoluto (o el final absoluto) de la lista en el hipervisor.
- El modo de desplazamiento utiliza los parámetros `-MaxRecords`, `-ForwardDirection` y `-ContinuationToken` para permitir el desplazamiento por los registros:
  - `-ForwardDirection`: El valor predeterminado es **True**. Esto se usa junto con `-MaxRecords` para devolver el siguiente conjunto de registros coincidentes o el conjunto anterior de registros coincidentes.
  - `-ContinuationToken`: Devuelve los elementos inmediatamente después (o antes si `ForwardDirection` es **false**), pero sin incluir el elemento indicado en `ContinuationToken`.

Ejemplos de paginación:

- Para devolver un solo registro de la plantilla de máquina con el nombre más bajo. El campo `AdditionalData` tiene `TotalItemsCount` y `TotalFilteredItemsCount`:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template
<!--NeedCopy-->
```

- Para devolver diez registros de la plantilla de máquina con el nombre más bajo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 10 | select Name
<!--NeedCopy-->
```

- Para devolver una matriz de registros que termine con el nombre más alto:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ForwardDirection $False -MaxRecords 10
     | select Name
<!--NeedCopy-->
```

- Para devolver una matriz de registros que comience en la plantilla de máquina asociada al `ContinuationToken` correspondiente:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -ContinuationToken "ami-07xxxxxxxxx" -
    MaxRecords 10
<!--NeedCopy-->
```

Filtros:

Se admiten estos parámetros opcionales adicionales para el filtrado. Puede combinar estos parámetros con las opciones de paginación.

- `-ContainsName "my_name"`: Si la cadena dada coincide con parte del nombre de una AMI, la AMI se incluye en el resultado de `Get`. Por ejemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -ContainName ‘apollo’
     | select Name
<!--NeedCopy-->
```

- `-Tags '{ "Key0": "Value0", "Key1": "Value1", "Key2": "Value2" } '`: Si una AMI tiene al menos una de estas etiquetas, se incluye en el resultado de `Get` . Por ejemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -MaxRecords 100 -Tags '{
"opex owner": "Not tagged" }
' | select Name
<!--NeedCopy-->
```

> **Nota:**
>
> Se admiten dos valores de etiqueta. El valor de la etiqueta **Not Tagged** coincide con elementos que no tienen la etiqueta especificada en su lista de etiquetas. El valor de la etiqueta **All values** coincide con elementos que tienen la etiqueta, independientemente del valor de la etiqueta. De lo contrario, la coincidencia solo se produce si el elemento tiene la etiqueta y el valor es igual al indicado en el filtro.

- `-Id "ami-0a2d913927e0352f3"`: Si la AMI coincide con el ID proporcionado, se incluye en el resultado de `Get`. Por ejemplo:

```
Get-HypInventoryItem -LiteralPath "XDHyp:\HostingUnits\ctx-test"
    -ResourceType template -Id ami-xxxxxxxxxxxx
<!--NeedCopy-->
```

Filtrado en el parámetro AdditionalData:

El parámetro de filtrado `AdditionalData` muestra plantillas o máquinas virtuales en función de su capacidad, oferta de servicio o cualquier propiedad que se encuentre en AdditionalData. Por ejemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200).
   AdditionalData
<!--NeedCopy-->
```

También puede agregar un parámetro `-Warn` para indicar las máquinas virtuales incompatibles. Las

máquinas virtuales se incluyen en un campo de `AdditionalData` denominado **Warning**. Por ejemplo:

```
(Get-HypInventoryItem -ResourceType "launchtemplateversion" -
   LiteralPath "XDHyp:\HostingUnits\aws" -MaxRecords 200 -Template "ami
   -015xxxxxxxx" -Warn $true).AdditionalData
<!--NeedCopy-->
```

Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de AWS.

Más información

- Crear y administrar conexiones y recursos
- Conexión con AWS
- Crear catálogos de máquinas

Crear un catálogo de Google Cloud Platform

May 22, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de Google Cloud.

> **Nota:**
>
> Antes de crear un catálogo de Google Cloud Platform (GCP), debe terminar de crear una conexión con GCP. Consulte Conexión con entornos de Google Cloud.

Preparar la instancia de una VM maestra y un disco persistente

> **Sugerencia:**
>
> "Disco persistente"es el término de Google Cloud para "disco virtual".

Para preparar la instancia de una VM maestra, cree y configure una instancia de VM con propiedades que coincidan con la configuración que quiera para las instancias de VDA clonadas en el catálogo

de máquinas planificado. La configuración no se aplica solamente al tamaño y al tipo de instancia. También incluye atributos de instancia como metadatos, etiquetas, asignaciones de GPU, etiquetas de red y propiedades de cuenta de servicio.

Como parte del proceso, MCS utiliza la instancia de VM maestra para crear la *plantilla de instancias* de Google Cloud. A continuación, la plantilla de instancias se utiliza para crear las instancias de VDA clonadas que componen el catálogo de máquinas. Las instancias clonadas heredan las propiedades (excepto las propiedades de VPC, subred y disco persistente) de la instancia de VM maestra a partir de la cual se creó la plantilla de instancias.

Después de configurar las propiedades de la instancia de VM maestra según sus especificaciones, inicie la instancia y, a continuación, prepare el disco persistente para la instancia.

Le recomendamos crear manualmente una instantánea del disco. Esto le permite utilizar una convención de nomenclatura útil para realizar un seguimiento de las versiones, le ofrece más opciones para administrar versiones anteriores de la imagen maestra y le ahorra tiempo en la creación de catálogos de máquinas. Si no crea su propia instantánea, MCS crea una instantánea temporal (que se elimina al final del proceso de aprovisionamiento).

Habilitar selección de zona

Citrix DaaS admite la selección de zonas. Con la selección de zonas, puede especificar las zonas en las que quiere crear máquinas virtuales. Con la selección de zonas, los administradores pueden colocar nodos de arrendatario único en las zonas de su elección. Para configurar el arrendamiento único, debe completar lo siguiente en Google Cloud:

- Reservar un nodo de arrendatario único de Google Cloud
- Crear la imagen maestra del VDA

Reservar un nodo de arrendatario único de Google Cloud

Para reservar un nodo de arrendatario único de Google Cloud, consulte la documentación de Google Cloud.

> **Importante:**
>
> Una plantilla de nodos se utiliza para indicar las características de rendimiento del sistema que se reserva al grupo de nodos. Estas características incluyen la cantidad de vGPU, la cantidad de memoria asignada al nodo y el tipo de máquina utilizado para las máquinas creadas en el nodo. Para obtener más información, consulte la documentación de Google Cloud.

Crear la imagen maestra del VDA

Para implementar máquinas en el nodo de arrendatario único, debe realizar pasos adicionales al crear una imagen de máquina virtual maestra. Las instancias de máquina en Google Cloud tienen una propiedad llamada *node affinity labels* (etiquetas de afinidad de nodos). Las instancias utilizadas como imágenes maestras para catálogos implementados en el nodo de arrendatario único requieren una *etiqueta de afinidad de nodos* que coincida con el nombre del **grupo de nodos de destino**. Para lograr esto, tenga en cuenta lo siguiente:

- Establezca la etiqueta en la consola de Google Cloud cuando cree la instancia. Para obtener información detallada, consulte Establecer una etiqueta de afinidad de nodos al crear una instancia.
- En el caso de una instancia existente, establezca la etiqueta desde la línea de comandos de **gcloud**. Para obtener información detallada, consulte Configurar una etiqueta de afinidad de nodos para una instancia existente.

> **Nota:**
>
> Si quiere utilizar el arrendamiento único con una VPC compartida, consulte Nube privada virtual compartida.

Establecer una etiqueta de afinidad de nodos al crear una instancia Para configurar la etiqueta de afinidad de nodos:

1. En la consola de Google Cloud, vaya a **Compute Engine > VM instances**.
2. En la página **VM instances**, seleccione **Create instance**.
3. En la página **Instance creation**, escriba o configure la información necesaria y, a continuación, seleccione **management, security, disks, networking, sole tenancy** para abrir el panel de parámetros.
4. En la ficha **Sole Tenancy**, seleccione **Browse** para ver los grupos de nodos disponibles en el proyecto actual. Aparecerá la página **Sole-tenant node**, que muestra una lista de los grupos de nodos disponibles.
5. En la página **Sole-tenant node**, seleccione el grupo de nodos correspondiente de la lista y, a continuación, seleccione **Select** para volver a la ficha **Sole tenancy**. El campo de las etiquetas de afinidad de nodos se rellena con la información seleccionada. Esta configuración garantiza que los catálogos de máquinas creados a partir de la instancia se implementarán en el grupo de nodos seleccionado.
6. Seleccione **Create** para crear la instancia.

Configurar una etiqueta de afinidad de nodos para una instancia existente Para configurar la etiqueta de afinidad de nodos:

1. En la ventana del terminal de Google Cloud Shell, utilice el comando *gcloud compute instances* para establecer una etiqueta de afinidad de nodos. Incluya la siguiente información en el comando **gcloud**:

   - **Nombre de la VM**. Por ejemplo, utilice una máquina virtual existente denominada `s*2019-vda-base`.*
   - **Nombre del grupo de nodos**. Utilice el nombre de grupo de nodos creado anteriormente. Por ejemplo, `mh-sole-tenant-node-group-1`.
   - **La zona en la que reside la instancia**. Por ejemplo, la máquina virtual reside en `*us-east-1b* zone`.

   Por ejemplo, escriba el siguiente comando en la ventana de terminal:

   - `gcloud compute instances set-scheduling "s2019-vda-base"--node-group="mh-sole-tenant-node-group-1"--zone="us-east1-b"`

   Para obtener más información sobre el comando *gcloud compute instances*, consulte la documentación de Google Developer Tools en https://cloud.google.com/sdk/gcloud/reference/beta/compute/instances/set-scheduling.

2. Vaya a la página **VM instance details** de la instancia y verifique que el campo **Node Affinities** se rellenó con la etiqueta.

Creación de un catálogo de máquinas

> **Nota:**
>
> Cree los recursos antes de crear los catálogos de máquinas. Al configurar catálogos de máquinas, utilice las convenciones de nomenclatura establecidas por Google Cloud. Consulte Lineamientos para asignar nombres a buckets para obtener más información.

Puede crear un catálogo de máquinas de dos maneras:

- Interfaz de Configuración completa
- PowerShell. Consulte Administrar Citrix DaaS mediante Remote PowerShell SDK. Para obtener información sobre cómo implementar funciones específicas con PowerShell, consulte Usar PowerShell

Crear un catálogo de máquinas mediante la interfaz de Configuración completa

Siga las instrucciones que se indican en Crear catálogos de máquinas. La siguiente descripción se aplica exclusivamente a los catálogos de Google Cloud.

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione **Crear catálogo de máquinas** en la barra de acciones.
3. En la página **Tipo de máquina**, seleccione **SO multisesión** y, a continuación, seleccione **Siguiente**. Citrix DaaS también admite sistemas operativos de sesión única.
4. En la página **Administración de máquinas**, seleccione las opciones **Máquinas con administración de energía** y **Citrix Machine Creation Services** y, a continuación, seleccione **Siguiente**. Si hay varios recursos, seleccione uno en el menú.
5. En la página **Imagen**, complete estos pasos según sea necesario y, a continuación, haga clic en **Siguiente**.

   a) Seleccione una instantánea o una máquina virtual como imagen maestra. Si quiere utilizar la funcionalidad de arrendamiento único, debe seleccionar una imagen cuya propiedad de grupo de nodos esté configurada correctamente. Consulte Habilitar selección de zona.

   b) Para usar una máquina virtual existente como perfil de máquina, seleccione **Usar un perfil de máquina** y después seleccione la máquina virtual.

   > **Nota:**
   >
   > Actualmente, las máquinas virtuales de este catálogo heredan el ID del conjunto de cifrado del disco, el tamaño de la máquina, el tipo de almacenamiento y los parámetros de zona del perfil de máquina.

   c) Seleccione el nivel funcional mínimo para el catálogo.

6. En la página **Almacenamiento**, seleccione el tipo de almacenamiento utilizado para contener el sistema operativo con este catálogo de máquinas. Cada una de las siguientes opciones de almacenamiento tiene características de precio y rendimiento únicas. Se crea siempre un disco de identidad con el disco persistente estándar zonal.

   - Disco persistente estándar
   - Disco persistente equilibrado
   - Disco persistente SSD

   Para obtener información detallada sobre las opciones de almacenamiento de Google Cloud, consulte Storage options.

7. En la página **Máquinas virtuales**, especifique cuántas máquinas virtuales quiere crear, revise la especificación detallada de dichas máquinas, seleccione el tipo de máquina de Google Cloud y, a continuación, seleccione **Siguiente**. Si utiliza grupos de nodos de arrendatario único para catálogos de máquinas, deberá seleccionar **solo** las zonas en las que están disponibles los nodos de arrendatario único reservados. Consulte Habilitar selección de zona.

8. En la página **Parámetros del disco**, puede configurar los siguientes parámetros:

   - Elija si quiere habilitar la caché de reescritura. Después de habilitar la caché de reescritura, puede hacer lo siguiente:

     - Puede configurar la RAM y el tamaño del disco utilizados para almacenar en caché datos temporales. Para obtener más información, consulte Configurar la caché de datos temporales.

     - Seleccione el tipo de almacenamiento del disco de caché con reescritura. Están disponibles las siguientes opciones de almacenamiento para uso con el disco de caché con reescritura:

       * Disco persistente estándar
       * Disco persistente equilibrado
       * Disco persistente SSD

       Para obtener información detallada sobre las opciones de almacenamiento de Google Cloud, consulte Storage options.

     - Seleccione el tipo de disco de caché con reescritura.

       * **Usar disco no persistente de caché con reescritura**. Si se selecciona, el disco de caché con reescritura no persiste en las máquinas virtuales aprovisionadas. El disco se borra durante los ciclos de energía y se pierden todos los datos redirigidos al disco.
       * **Usar disco persistente de caché con reescritura**. Si se selecciona, el disco de caché con reescritura persiste en las máquinas virtuales aprovisionadas. Habilitar esta opción aumenta los costes de almacenamiento.

   - Cuando la optimización del almacenamiento de MCS (E/S de MCS) está habilitada, puede elegir si quiere conservar los discos del sistema para los VDA durante los ciclos de energía. Para obtener más información, consulte Habilitar actualizaciones de optimización del almacenamiento de MCS.

   - Elija si quiere usar su propia clave para proteger el contenido del disco. Para utilizar esta función, primero debe crear sus propias claves de cifrado administradas por el cliente (CMEK). Para obtener más información, consulte Uso de claves de cifrado administradas por el cliente (CMEK).

     > **Nota:**
     >
     > Solo está disponible en la interfaz **Administrar > Configuración completa**.

     Después de crear las claves, puede seleccionar una de esas claves de la lista. No se puede cambiar la clave después de crear el catálogo. Google Cloud no admite claves de rotación

en discos o imágenes persistentes existentes. Por lo tanto, después de aprovisionar un catálogo, el catálogo está asociado a una versión específica de la clave. Si esa clave se inhabilita o destruye, las instancias y los discos cifrados con ella quedan inutilizables hasta que la clave se rehabilita o restaura.

9. En la página **Identidades de las máquinas**, seleccione una cuenta de Active Directory y, a continuación, seleccione **Siguiente**.
   - Si selecciona **Crear nuevas cuentas de Active Directory**, seleccione un dominio y, a continuación, introduzca la secuencia de caracteres que representa el esquema de nomenclatura para las cuentas de equipo de VM aprovisionadas creadas en Active Directory. El esquema de nomenclatura de cuentas puede contener de 1 a 64 caracteres y no puede contener espacios en blanco, ni caracteres no ASCII o especiales.
   - Si selecciona **Usar cuentas de Active Directory existentes**, seleccione **Examinar** para desplazarse a las cuentas de equipo de Active Directory existentes de las máquinas seleccionadas.
10. En la página **Credenciales de dominio**, seleccione **Introducir credenciales**, escriba el nombre de usuario y la contraseña, seleccione **Guardar** y, a continuación, seleccione **Siguiente**.
    - Las credenciales que escriba deben tener permisos para realizar operaciones en cuentas de Active Directory.
11. En la página **Ámbitos**, seleccione ámbitos para el catálogo de máquinas y, a continuación, seleccione **Siguiente**.
    - Puede seleccionar ámbitos opcionales o seleccione **Ámbito personalizado** para personalizarlos según sea necesario.
12. En la página **Resumen**, confirme la información, especifique un nombre para el catálogo y seleccione **Finalizar**.

    > **Nota:**
    >
    > El nombre del catálogo puede contener entre 1 y 39 caracteres, y no puede contener solo espacios en blanco o los caracteres `\ / ; : # . * ? = < > | [ ] { } "' ( )' )`.

La creación del catálogo de máquinas puede tardar mucho tiempo en completarse. Una vez finalizada, aparece el catálogo. Desde la consola de Google Cloud, puede comprobar que las máquinas se hayan creado en los grupos de nodos de destino.

Importar máquinas de Google Cloud creadas manualmente

Con esta función, puede:

- Importar máquinas con sistema operativo multisesión de Google Cloud creadas manualmente en un catálogo de Citrix DaaS.
- Eliminar las máquinas con sistema operativo multisesión de Google Cloud creadas manualmente de un catálogo de Citrix DaaS.
- Utilizar las prestaciones de administración de energía existentes en Citrix DaaS para administrar la energía de las máquinas con SO multisesión Windows en Google Cloud. Por ejemplo, establecer una programación de reinicio para dichas máquinas.

Esta funcionalidad no requiere cambios en el flujo de aprovisionamiento de Citrix DaaS; tampoco se necesita eliminar ninguna función existente.

Se recomienda utilizar MCS para aprovisionar máquinas en la interfaz de Configuración completa de Citrix DaaS, en lugar de importar máquinas de Google Cloud creadas manualmente.

Nube privada virtual compartida

Las nubes VPC compartidas constan de un proyecto host (desde el que están disponibles las subredes compartidas) y uno o varios proyectos de servicios que utilizan el recurso. Las nubes VPC compartidas son las opciones idóneas para instalaciones grandes, ya que ofrecen control, uso y administración centralizados de los recursos de empresa compartidos de Google Cloud. Para obtener más información, consulte el sitio de documentación de Google.

Con esta función, Machine Creation Services (MCS) admite el aprovisionamiento y la administración de catálogos de máquinas implementados en las nubes VPC compartidas. Esta compatibilidad, equivalente en funcionalidad a la compatibilidad que se ofrece en nubes VPC locales, difiere en dos áreas:

- Debe conceder permisos adicionales a la cuenta de servicio utilizada para crear la conexión de host. Este proceso permite a MCS acceder a los recursos de VPC compartida y utilizarlos. Consulte Se necesitan nuevos permisos.
- Debe crear dos reglas de firewall, una para la entrada y otra para la salida. Estas reglas de firewall se utilizan durante el proceso de creación de imágenes maestras. Consulte Reglas de firewall.

Para obtener información sobre cómo configurar una nube privada virtual compartida, consulte Configurar la nube VPC compartida.

Se necesitan nuevos permisos

Se requiere una cuenta de servicio de Google Cloud con permisos específicos cuando se crea la conexión de host. Estos permisos adicionales se deben conceder a todas las cuentas de servicio utilizadas para crear conexiones de host basadas en VPC compartidas.

> **Sugerencia:**
>
> Estos permisos adicionales no son nuevos en Citrix DaaS. Se utilizan para facilitar la implementación de VPC locales. Con las VPC compartidas, estos permisos adicionales permiten el acceso a otros recursos de VPC compartidas.

Se debe conceder un máximo de cuatro permisos adicionales a la cuenta de servicio asociada a la conexión de host para admitir una nube VPC compartida:

- **compute.firewalls.list**: Este permiso es obligatorio. Permite a MCS recuperar la lista de reglas de firewall presentes en la nube VPC compartida.
- **compute.networks.list**: Este permiso es obligatorio. Permite a MCS identificar las redes de nubes VPC compartidas disponibles para la cuenta de servicio.
- **compute.subnetworks.list**: Este permiso es opcional, en función de cómo utilice las nubes VPC. Permite a MCS identificar las subredes dentro de las nubles VPC compartidas que sean visibles. Este permiso ya es necesario para utilizar nubes VPC locales, pero también debe asignarse en el proyecto host de nubes VPC compartidas.
- **compute.subnetworks.use**: Este permiso es opcional, en función de cómo utilice las nubes VPC. Es necesario utilizar recursos de subred en los catálogos de máquinas aprovisionadas. Este permiso ya es necesario para utilizar nubes VPC locales, pero también debe asignarse en el proyecto host de nubes VPC compartidas.

Al utilizar estos permisos, tenga en cuenta que existen diferentes enfoques basados en el tipo de permiso utilizado para crear el catálogo de máquinas:

- Permiso a nivel de proyecto:
  - Permite el acceso a todas las nubes VPC compartidas dentro del proyecto host.
  - Requiere que se asignen los permisos `compute.subnetworks.list` y `compute.subnetworks.use` a la cuenta de servicio.
- Permiso a nivel de subred:
  - Permite el acceso a subredes específicas dentro de la nube VPC compartida.
  - Los permisos `compute.subnetworks.list` y `compute.subnetworks.use` son intrínsecos a la asignación a nivel de subred y, por lo tanto, no es necesario asignarlos directamente a la cuenta de servicio.

Seleccione el enfoque que se adapte a las necesidades y los estándares de seguridad de su organización.

> **Sugerencia:**

> Para obtener más información sobre las diferencias entre los permisos a nivel de proyecto y a nivel de subred, consulte Service Project Admins.

Reglas de firewall

Durante la preparación de un catálogo de máquinas, se prepara una imagen de máquina para que sirva como disco del sistema de la imagen maestra del catálogo. Cuando se produce este proceso, el disco se conecta temporalmente a una máquina virtual. Esta máquina virtual debe ejecutarse en un entorno aislado que impida todo el tráfico de red entrante y saliente. Este aislamiento se logra gracias a un par de reglas de firewall "deny-all"(denegar todo): una para el tráfico de entrada y otra para el tráfico de salida. Al utilizar nubes VPC locales de Google Cloud, MCS crea este firewall en la red local y lo aplica a la máquina para la creación de imagen maestra. Una vez finalizada la creación de la imagen maestra, la regla de firewall se elimina de la imagen.

Se recomienda mantener al mínimo la cantidad de nuevos permisos necesarios para usar nubes VPC compartidas. Las nubes VPC compartidas son recursos de empresa de alto nivel y suelen tener protocolos de seguridad más rígidos. Por este motivo, cree un par de reglas de firewall en el proyecto host en los recursos de VPC compartida, una para la entrada y otra para la salida. Asígneles la máxima prioridad. Aplique una nueva etiqueta de destino a cada una de estas reglas, con el siguiente valor:

```
citrix-provisioning-quarantine-firewall
```

Cuando MCS crea o actualiza un catálogo de máquinas, busca reglas de firewall que contengan esta etiqueta de destino. A continuación, comprueba que las reglas sean correctas y las aplica a la máquina utilizada para preparar la imagen maestra del catálogo. Si no se encuentran reglas de firewall o se encuentran, pero son incorrectas o ellas o sus prioridades, aparecerá un mensaje similar al siguiente:

```
"Unable to find valid INGRESS and EGRESS quarantine firewall rules
for VPC <name> in project <project>. "Please ensure you have created
 'deny all'firewall rules with the network tag ‘citrix-provisioning-
quarantine-firewall'and proper priority." "Refer to Citrix Documentation
 for details."
```

Configurar la nube VPC compartida

Antes de agregar la VPC compartida como conexión de host en la interfaz de Configuración completa de Citrix DaaS, siga estos pasos para agregar cuentas de servicio desde el proyecto que aprovisionará:

1. Crear un rol de IAM.
2. Agregar una cuenta de servicio al rol de IAM del proyecto host.
3. Agregar la cuenta de servicio de Cloud Build a la VPC compartida.
4. Crear reglas de firewall.

Crear un rol de IAM Determine el nivel de acceso del rol:

- *Acceso a nivel de proyecto* o
- Un modelo más restringido que utiliza el *acceso a nivel de subred*.

Acceso a nivel de proyecto para el rol de IAM. Para el rol de IAM a nivel de proyecto, incluya los siguientes permisos:

- compute.firewalls.list
- compute.networks.list
- compute.subnetworks.list
- compute.subnetworks.use

Para crear un rol de IAM a nivel de proyecto:

1. En la consola de Google Cloud, vaya a **IAM & Admin > Roles**.
2. En la página **Roles**, seleccione **CREATE ROLE**.
3. En la página **Create Role**, especifique el nombre del rol. Seleccione **ADD PERMISSIONS**.
    a) En la página **Add permissions**, agregue permisos al rol de forma individual. Para agregar un permiso, escriba el nombre del permiso en el campo **Filter table**. Seleccione el permiso y, a continuación, seleccione **ADD**.
    b) Seleccione **CREATE**.

Subnet-level IAM role. Este rol omite la adición de los permisos `compute.subnetworks.list` y `compute.subnetworks.use` después de seleccionar **CREATE ROLE**. Para este nivel de acceso de IAM, los permisos `compute.firewalls.list` y `compute.networks.list` deben aplicarse al nuevo rol.

Para crear un rol de IAM a nivel de subred:

1. En la consola de Google Cloud, vaya a **VPC network** > **Shared VPC**. Aparecerá la página **Shared VPC**, que muestra las subredes de las redes de VPC compartidas que contiene el proyecto host.
2. En la página **Shared VPC**, seleccione la subred a la que quiere acceder.
3. En la esquina superior derecha, seleccione **ADD MEMBER** para agregar una cuenta de servicio.
4. En la página **Add members**, siga estos pasos:
    a) En el campo **New members**, escriba el nombre de su cuenta de servicio y, a continuación, selecciónela en el menú.
    b) Seleccione el campo **Select a role** y, a continuación, **Compute Network User**.
    c) Seleccione **SAVE**.
5. En la consola de Google Cloud, vaya a **IAM & Admin** > **Roles**.
6. En la página **Roles**, seleccione **CREATE ROLE**.
7. En la página **Create Role**, especifique el nombre del rol. Seleccione **ADD PERMISSIONS**.

a) En la página **Add permissions**, agregue permisos al rol de forma individual. Para agregar un permiso, escriba el nombre del permiso en el campo **Filter table**. Seleccione el permiso y, a continuación, seleccione **ADD**.
b) Seleccione **CREATE**.

Agregar una cuenta de servicio al rol de IAM del proyecto host Después de crear un rol de IAM, siga estos pasos para agregar una cuenta de servicio para el proyecto host:

1. En la consola de Google Cloud, vaya al proyecto host y, a continuación, a **IAM & Admin > IAM**.
2. En la página **IAM**, seleccione **ADD** para agregar una cuenta de servicio.
3. En la página **Add members**:

   a) En el campo **New members**, escriba el nombre de su cuenta de servicio y, a continuación, selecciónela en el menú.
   b) En el campo Select a role, introduzca el rol de IAM que creó y, a continuación, seleccione el rol en el menú.
   c) Seleccione **SAVE**.

Ahora la cuenta de servicio está configurada para el proyecto host.

Agregar la cuenta de servicio de Cloud Build a la VPC compartida Cada suscripción a Google Cloud tiene una cuenta de servicio que tiene, como nombre, el número de identificación del proyecto, seguido de `cloudbuild.gserviceaccount`. Por ejemplo: `705794712345@cloudbuild.gserviceaccount`.

Para determinar el número de ID del proyecto, vaya a **Cloud overview > Dashboard** en la consola de Google Cloud. El ID y el número de proyecto se muestran en la tarjeta de información Dashboard Project del proyecto:

Siga estos pasos para agregar la cuenta de servicio de Cloud Build a la VPC compartida:

1. En la consola de Google Cloud, vaya al proyecto host y, a continuación, a **IAM & Admin** > **IAM**.
2. En la página **Permissions**, seleccione **ADD** para agregar una cuenta.
3. En la página **Add members**, siga estos pasos:

   a) En el campo **New members**, escriba el nombre de la cuenta de servicio de Cloud Build y, a continuación, selecciónela en el menú.
   b) Seleccione el campo **Select a role**, escriba `Computer Network User` y, a continuación, seleccione el rol en el menú.
   c) Seleccione **SAVE**.

Crear reglas de firewall Como parte del proceso de masterización, MCS copia la imagen de máquina seleccionada y la utiliza para preparar el disco del sistema de la imagen maestra para el catálogo. Durante la masterización, MCS conecta el disco a una máquina virtual temporal, que luego ejecuta scripts de preparación. Esta máquina virtual debe ejecutarse en un entorno aislado que prohíba todo el tráfico de red entrante y saliente.

Para crear un entorno aislado, MCS requiere dos reglas "*deny all*"en el firewall (una regla de entrada y una regla de salida). Por lo tanto, cree dos reglas de firewall (entrada y salida) en el *proyecto host* de la siguiente manera:

1. En la consola de Google Cloud, vaya al proyecto host y, a continuación, a **VPC Network > Firewall**.
2. En la página **Firewall**, seleccione **CREATE FIREWALL RULE**.
3. En la página **Create a firewall rule**, complete lo siguiente:
    - **Nombre**. Escriba el nombre de la regla.
    - **Network**. Seleccione la red de VPC compartida a la que se aplica la regla de firewall de entrada.
    - **Priority**. Cuanto menor sea el valor, mayor será la prioridad de la regla. Recomendamos un valor pequeño (por ejemplo, 10).
    - **Direction of traffic**. Seleccione **Ingress**.
    - **Action on match**. Seleccione **Deny**.
    - **Targets**. Utilice el valor predeterminado, **Specified target tags**.
    - **Target tags**. Escriba `citrix-provisioning-quarantine-firewall`.
    - **Source filter**. Utilice el valor predeterminado, **IP ranges**.
    - **Source IP ranges**. Escriba un intervalo que tenga en cuenta todo el tráfico. Escriba `0.0.0.0/0`.
    - **Protocols and ports**. Seleccione **Deny all**.
4. Seleccione **CREATE** para crear la regla.
5. Repita los pasos para crear otra regla. En **Direction of traffic**, seleccione **Egress**.

Usar claves de cifrado administradas por el cliente (CMEK)

Puede utilizar claves de cifrado administradas por el cliente (CMEK) para catálogos de MCS. Al utilizar esta funcionalidad, asigna el rol `CryptoKey Encrypter/Decrypter` del servicio Key Management Service (KMS) de Google Cloud al agente de servicio de Compute Engine. La cuenta de Citrix DaaS debe tener los permisos correctos en el proyecto en el que se almacena la clave. Consulte Asignar permisos a la cuenta de Citrix DaaS. Consulte Ayuda a proteger los recursos con claves de Cloud KMS para obtener más información.

El agente de servicio de Compute Engine tiene el siguiente formato: `service-<Project_Number>@compute-system.iam.gserviceaccount.com`. Este formato es distinto de la

cuenta de servicio predeterminada de Compute Engine.

> **Nota:**
>
> Puede que esta cuenta de servicio de Compute Engine no aparezca en la pantalla **IAM Permissions** de Google Console. En tales casos, use el comando `gcloud` como se describe en Ayuda a proteger los recursos con claves de Cloud KMS.

Asignar permisos a la cuenta de Citrix DaaS

Los permisos de Google Cloud KMS se pueden configurar de varias formas. Puede proporcionar permisos de KMS a *nivel de proyecto* o a *nivel de recursos*. Consulte Permisos y funciones para obtener más información.

Permisos de KMS a nivel de proyecto Una opción es proporcionar a la cuenta de Citrix DaaS permisos a nivel de proyecto para explorar los recursos de Cloud KMS. Para ello, cree un rol personalizado y agregue los siguientes permisos:

- `cloudkms.keyRings.list`
- `cloudkms.keyRings.get`
- `cloudkms.cryptokeys.list`
- `cloudkms.cryptokeys.get`

Asigne este rol personalizado a su cuenta de Citrix DaaS. Esto le permite examinar las claves regionales del proyecto correspondiente del inventario.

Permisos de KMS a nivel de recursos Para la otra opción, los permisos a nivel de recursos, en la consola de Google Cloud, vaya a la `cryptoKey` que utiliza para aprovisionamiento de MCS. Agregue la cuenta de Citrix DaaS a un llavero o a una clave que utilice para aprovisionamiento de catálogos.

> **Sugerencia:**
>
> Con esta opción, no puede examinar las claves regionales de su proyecto en el inventario, puesto que la cuenta de Citrix DaaS no tiene permisos de lista a nivel de proyecto sobre los recursos de Cloud KMS. Sin embargo, aún podrá aprovisionar un catálogo con CMEK especificando el `cryptoKeyId` correcto en las propiedades personalizadas de `ProvScheme`. Consulte Crear un catálogo con CMEK mediante propiedades personalizadas.

Rotar claves administradas por el cliente

Google Cloud no admite claves de rotación en discos o imágenes persistentes existentes. Una vez que se aprovisiona una máquina, se asocia a la versión de clave en uso en el momento de su creación. Sin

embargo, se puede crear una nueva versión de la clave y esa nueva clave se utilizará con las máquinas o recursos recién aprovisionados creados al actualizar un catálogo con una nueva imagen maestra.

Consideraciones importantes acerca de los llaveros Los llaveros no se pueden cambiar de nombre ni eliminar. Además, podría incurrir en cargos imprevistos al configurarlos. Al eliminar o quitar un llavero, Google Cloud muestra un mensaje de error:

```
Sorry, you can't delete or rename keys or key rings. We were concerned about the security implications of allowing multiple keys or key versions over time to have the same resource name, so we decided to make names immutable. (And you can't delete them, because we wouldn't be able to do a true deletion--there would still have to be a tombstone tracking that this name had been used and couldn't be reused).
We're aware that this can make things untidy, but we have no immediate plans to change this.
If you want to avoid getting billed for a key or otherwise make it unavailable, you can do so by deleting all the key versions; neither keys nor key rings are billed for, just the active key versions within the keys.
<!--NeedCopy-->
```

> **Sugerencia:**
>
> Para obtener más información, consulte Editing or deleting a key ring from the console.

Compatibilidad con "Acceso uniforme a nivel de bucket"

Citrix DaaS es compatible con la directiva de acceso uniforme a nivel de depósito de Google Cloud. Esta funcionalidad amplía el uso de la directiva de IAM que concede permisos a una cuenta de servicio para permitir la manipulación de recursos, incluidos los depósitos de almacenamiento. Con control de acceso uniforme a nivel de depósito, Citrix DaaS le permite utilizar una lista de control de acceso (ACL) para controlar el acceso a los depósitos de almacenamiento o a los objetos almacenados en ellos. Para obtener información general acerca del acceso uniforme a nivel de depósito de Google Cloud, consulte Acceso uniforme a nivel de bucket. Para obtener información sobre la configuración, consulte Requerir acceso uniforme a nivel de bucket.

Usar PowerShell

En esta sección se detalla cómo realizar las siguientes tareas con PowerShell:

- Crear un catálogo con un disco persistente de caché con reescritura
- Mejorar el rendimiento del arranque con E/S de MCS
- Crear un catálogo con CMEK mediante propiedades personalizadas

- Crear un catálogo de máquinas mediante un perfil de máquina
- Crear un catálogo de máquinas con el perfil de máquina como plantilla de instancias
- Crear un catálogo con máquinas virtuales blindadas
- Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único

Crear un catálogo con un disco persistente de caché con reescritura

Para configurar un catálogo con un disco persistente de caché con reescritura, use el comando `New-ProvScheme CustomProperties` de PowerShell.

> **Sugerencia:**
>
> Use el parámetro de PowerShell `New-ProvScheme CustomProperties` solo para conexiones de alojamiento basadas en la nube. Si quiere aprovisionar máquinas con un disco persistente de caché con reescritura para una solución local (por ejemplo, XenServer), PowerShell no es necesario porque el disco conserva automáticamente los datos.

Este comando ofrece una propiedad adicional, `PersistWBC`, que se utiliza para determinar cómo el disco de caché con reescritura persiste en máquinas aprovisionadas con MCS. La propiedad `PersistWBC` solo se utiliza cuando se especifica el parámetro `UseWriteBackCache` y cuando se establece el parámetro `WriteBackCacheDiskSize` para indicar que se ha creado un disco.

> **Nota:**
>
> Este comportamiento se aplica tanto a Azure como a GCP, donde los datos del disco de caché con reescritura predeterminado de E/S de MCS se eliminan y se vuelven a crear cuando se apaga o se enciende la máquina. Puede optar por conservar los datos del disco para evitar la eliminación y la recreación de los datos del disco caché con reescritura de E/S de MCS.

He aquí unos cuantos ejemplos de propiedades que se encuentran en el parámetro `CustomProperties` antes de optar por la propiedad `PersistWBC`:

```
1 <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageAccountType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="ResourceGroups" Value="
     benvaldev5RG3" />
5 </CustomProperties>
6 <!--NeedCopy-->
```


> **Nota:**
>
> Este ejemplo solo se aplica a Azure. Las propiedades son diferentes en el entorno de GCP.

Al utilizar estas propiedades, tenga en cuenta que contienen valores predeterminados si las propiedades se omiten del parámetro `CustomProperties`. La propiedad `PersistWBC` tiene dos valores posibles: **true** o **false**.

Cuando la propiedad `PersistWBC` es **true**, el disco de caché con reescritura no se elimina cuando el administrador de Citrix DaaS apaga la máquina desde la interfaz de administración.

Cuando la propiedad `PersistWBC` es **false**, el disco de caché con reescritura se elimina cuando el administrador de Citrix DaaS apaga la máquina desde la interfaz de administración.

> **Nota:**
>
> Si se omite la propiedad `PersistWBC`, su valor predeterminado es **false**, y la memoria caché de reescritura se elimina cuando la máquina se apaga desde la interfaz de administración.

Por ejemplo, así se usa el parámetro `CustomProperties` para configurar `PersistWBC` en "true" :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
   benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Importante:**
>
> La propiedad `PersistWBC` solo se puede configurar mediante el cmdlet de PowerShell `New-ProvScheme`. Si se intenta modificar `CustomProperties` de un esquema de aprovisionamiento después de la creación, esto no afecta al catálogo de máquinas ni a la persistencia del disco de caché con reescritura cuando se apaga una máquina.

Por ejemplo, configure `New-ProvScheme` para utilizar la memoria caché de reescritura mientras configura la propiedad `PersistWBC` en "true":

```
New-ProvScheme
-CleanOnBoot
```



```
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistWBC`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

Mejorar el rendimiento del arranque con E/S de MCS

Puede mejorar el rendimiento de arranque de los discos administrados de Azure y GCP cuando E/S de MCS está habilitada. Utilice la propiedad personalizada `PersistOSDisk` de PowerShell en el comando `New-ProvScheme` para configurar esta función. Las opciones asociadas a `New-ProvScheme` son:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
   Premium_LRS" />
<Property xsi:type="StringProperty" Name="Resource<!--NeedCopy-->
``````<!--NeedCopy-->
````````Groups" Value="benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
</CustomProperties>
<!--NeedCopy-->
```

Para habilitar esta función, establezca la propiedad personalizada `PersistOSDisk` en **true**. Por ejemplo:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
   /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
   Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
   =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
   GoldImages.resourcegroup\W10MCSIO-01
   _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
    CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
    adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
   folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

**Crear un catálogo con CMEK mediante propiedades personalizadas**

Al crear el esquema de aprovisionamiento a través de PowerShell, especifique una propiedad `CryptoKeyId` en `ProvScheme CustomProperties`. Por ejemplo:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="<
       yourCryptoKeyId>" />
</CustomProperties>'
<!--NeedCopy-->
```

`cryptoKeyId` debe especificarse en el siguiente formato:

`projectId:location:keyRingName:cryptoKeyName`

Por ejemplo, si quiere usar la clave `my-example-key` en el llavero `my-example-key-ring` de la región `us-east1` y el proyecto con ID `my-example-project-1`, su configuración personalizada de `ProvScheme` se asemejaría a:

```
'<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
    <Property xsi:type="StringProperty" Name="CryptoKeyId" Value="my-
       example-project-1:us-east1:my-example-key-ring:my-example-key"
       />
</CustomProperties>'
<!--NeedCopy-->
```

Todas las imágenes y discos aprovisionados de MCS relacionados con este esquema de aprovisionamiento utilizan esta clave de cifrado administrada por el cliente.

> **Sugerencia:**
>
> Si utiliza claves globales, la ubicación de las propiedades del cliente debe indicar `global`, y no el nombre de la **región**, que en el ejemplo anterior es **us-east1**. Por ejemplo: `<Property xsi:type="StringProperty"Name="CryptoKeyId"Value="my-example-project-1:global:my-example-key-ring:my-example-key"/>`.

### Crear un catálogo de máquinas mediante un perfil de máquina

Al crear un catálogo para aprovisionar máquinas mediante Machine Creation Services (MCS), puede usar un perfil de máquina para capturar las propiedades del hardware de una máquina virtual y aplicarlas a las máquinas virtuales recién aprovisionadas del catálogo. Cuando no se utiliza el parámetro `MachineProfile`, las propiedades del hardware se obtienen de la instantánea o la VM de la imagen maestra.
Algunas propiedades se definen de forma explícita; por ejemplo `StorageType`, `CatalogZones` y `CryptoKeyId` se omiten en el perfil de la máquina.

- Para crear un catálogo con un perfil de máquina, utilice el comando `New-ProvScheme`. Por ejemplo, `New-ProvScheme –MachineProfile "path to VM"`. Si no especifica el parámetro `MachineProfile`, las propiedades del hardware se capturan de la máquina virtual de la imagen maestra.
- Para actualizar un catálogo con un nuevo perfil de máquina, utilice el comando `Set-ProvScheme`. Por ejemplo, `Set-ProvScheme –MachineProfile "path to` **`new`** `VM"`. Este comando no cambia el perfil de máquina de las máquinas virtuales existentes del catálogo. Solo las nuevas máquinas virtuales que se agregan al catálogo tienen el nuevo perfil de máquina.
- También puede actualizar la imagen maestra; sin embargo, al actualizar la imagen maestra, las propiedades del hardware no se actualizan. Si quiere actualizar las propiedades del hardware, debe actualizar el perfil de la máquina con el comando `Set-ProvScheme`. Estos cambios solo se aplicarán a las nuevas máquinas del catálogo. Para actualizar las propiedades de hardware

de una máquina existente, puede utilizar el comando `Set-ProvVMUpdateTimeWindow` mediante los parámetros `-StartsNow` y `-DurationInMinutes -1`.

> **Nota:**
>
> - `StartsNow` indica que la hora de inicio programada es la hora actual.
> - `DurationInMinutes` con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

### Crear un catálogo de máquinas con el perfil de máquina como plantilla de instancias

Puede seleccionar una plantilla de instancias de GCP como entrada para el perfil de la máquina. Las plantillas de instancias son recursos ligeros de GCP y, por lo tanto, muy rentables.

#### Crear un nuevo catálogo de máquinas con el perfil de máquina como plantilla de instancias

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Utilice el siguiente comando para encontrar una plantilla de instancias en su proyecto de GCP:

```
cd XDHyp:\HostingUnits<HostingUnitName>\instanceTemplates.folder
<!--NeedCopy-->
```

4. Cree un nuevo catálogo de máquinas con el perfil de máquina como plantilla de instancias mediante el comando NewProvScheme:

```
New-ProvScheme -ProvisioningSchemeName <CatalogName>  -
    HostingUnitName <HostingUnitName> -IdentityPoolName <identity
    pool name> -MasterImageVM
XDHyp:\HostingUnits<HostingUnitName>\Base.vm\Base.snapshot -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder\mytemplate.template
<!--NeedCopy-->
```

   Para obtener más información sobre el comando New-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/New-ProvScheme/.

5. Utilice los comandos de PowerShell para terminar de crear el catálogo de máquinas.

#### Actualizar un catálogo de máquinas para tener una plantilla de instancias como perfil de máquina

1. Abra una ventana de PowerShell.

2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute este comando:

```
Set-ProvScheme -ProvisioningSchemeName  <CatalogName> -
    MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
    instanceTemplates.folder<TemplateName>.template
<!--NeedCopy-->
```

Para obtener información sobre el comando Set-ProvScheme, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/MachineCreation/Set-ProvScheme/.

### Crear un catálogo con máquinas virtuales blindadas

Puede crear un catálogo de máquinas de MCS con propiedades de VM blindada. Una máquina virtual blindada se ve reforzada por un conjunto de controles de seguridad que proporcionan integridad verificable de sus instancias de Compute Engine, con prestaciones avanzadas de seguridad de plataforma como el arranque seguro, un módulo de plataforma virtual de confianza, firmware UEFI y la supervisión de la integridad.

MCS admite la creación del catálogo mediante el flujo de trabajo del perfil de máquina. Si utiliza un flujo de trabajo de perfil de máquina, debe habilitar las propiedades de máquina virtual blindad de una instancia de máquina virtual. A continuación, puede utilizar esta instancia de máquina virtual como entrada del perfil de máquina.

#### Crear un catálogo de máquinas de MCS con máquinas virtuales blindadas

1. Habilite las opciones de máquina virtual blindada de una instancia de máquina virtual en la consola de Google Cloud. Consulte Quickstart: Enable Shielded VM options.
2. Cree un catálogo de máquinas de MCS con un flujo de trabajo de perfil de máquina mediante la instancia de máquina virtual.
   a) Abra una ventana de PowerShell.
   b) Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
   c) Cree un grupo de identidades si aún no se ha creado.
   d) Ejecute el comando `New-ProvScheme`. Por ejemplo:

```
New-ProvScheme -ProvisioningSchemeName <catalog-name>
-HostingUnitName gcp-hostint-unit
-MasterImageVM XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    vda.vm
-MachineProfile XDHyp:\HostingUnits\gcp-hostint-unit\catalog-
    machine.vm
<!--NeedCopy-->
```

3. Termine de crear el catálogo de máquinas.

#### Actualizar un catálogo de máquinas con un nuevo perfil de máquina

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName <catalog-name>
-MasterImageVM XDHyp:\HostingUnits<hostin-unit>\catalog-vda.vm
-MachineProfile "DHyp:\HostingUnits<hostin-unit>\catalog-machine.
    vm
<!--NeedCopy-->
```

Para aplicar el cambio realizado en `Set-ProvScheme` a las máquinas virtuales existentes, ejecute el comando `Set-ProvVMUpdateTimeWindow`.

1. Ejecute el comando `Set-ProvVMUpdateTimeWindow`. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

2. Reinicie las máquinas virtuales.

### Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único

Puede crear máquinas virtuales de Windows 11 en GCP. Sin embargo, si instala Windows 11 en la imagen maestra, debe habilitar vTPM durante el proceso de creación de la imagen maestra. Además, debe habilitar vTPM en el origen del perfil de máquina (plantilla de instancia o máquina virtual).

Los pasos clave para crear máquinas virtuales de Windows 11 en el nodo de arrendatario único son:

1. Configurar los entornos de virtualización de Google Cloud. Para obtener información, consulte Entornos de Google Cloud.
2. Instalar un VDA. Consulte Instalar VDA.
3. Crear una conexión con entornos de Google Cloud. Para obtener más información, consulte Conexión con entornos de nube de Google.
4. Crear una imagen maestra de Bring Your Own License (BYOL) de Windows 11 e importarla en Google Cloud. Consulte Crear una imagen maestra de BYOL para Windows 11.
5. Crear el origen del perfil de la máquina: aprovisione la máquina virtual en el nodo de arrendatario único y habilite el vTPM del perfil de máquina de origen. Consulte Aprovisionar una máquina virtual en un nodo de arrendatario único.
6. Crear un catálogo de máquinas de MCS con el origen del perfil de máquina de Windows 11 habilitado con vTPM. El origen del perfil de máquina debe tener el mismo tipo de instancia que se describe en el nodo de arrendatario único. Consulte Crear un catálogo de máquinas de MCS con el origen del perfil de máquina de Windows 11.

### Crear una imagen maestra de BYOL para Windows 11

Hay dos opciones para crear una imagen maestra de BYOL para Windows 11 e importar la imagen maestra en Google Cloud:

- Usar las herramientas de Cloud Build de Google Cloud
- Crear la imagen maestra en cualquier otro hipervisor

### Usar las herramientas de Cloud Build de Google Cloud

1. Cargue los archivos de instalación ISO de Windows 11, SDK de GCP, .NET Framework y PowerShell en el depósito de almacenamiento de GCP.
2. Proporcione la ubicación del archivo en el archivo `.yaml` de Cloud Build como parámetro.
3. Ejecute el siguiente Cloud Build desde la línea de comandos para compilar la imagen final de Windows 11. GCP arranca y crea la imagen maestra en el proyecto seleccionado mediante un flujo de trabajo de Daisy en GCP, y la imagen maestra se importa a GCP.

```
gcloud compute instances import INSTANCE-NAME--source-uri=gs://
   BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
   --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Nota:**
>
> Sustituya todo el texto en mayúscula por los detalles reales del recurso.

Para obtener la información completa, consulte Crear imágenes de BYOL de Windows personalizadas.

### Crear la imagen maestra en cualquier otro hipervisor

1. Cree la imagen maestra de Windows 11 con cualquier otro hipervisor.
2. Exporte la imagen maestra en formato OVF a la máquina local.
3. Cargue los archivos OVF en el depósito de almacenamiento de GCP mediante la CLI de gcloud local.

```
gsutil cp LOCAL_IMAGE_PATH_OVF_FILES gs://BUCKET_NAME/
<!--NeedCopy-->
```

4. Ejecute el siguiente Cloud Build desde la línea de comandos para compilar la imagen final de Windows 11. GCP arranca y crea la imagen maestra en el proyecto seleccionado mediante un flujo de trabajo de Daisy en GCP, y la imagen maestra se importa a GCP.

```
gcloud compute instances import INSTANCE-NAME --source-uri=gs://
    BUCKET/IMAGE-OVF-FILE.ovf --guest-os-features=UEFI_COMPATIBLE
    --byol --machine-type=MACHINE-TYPE --zone=ZONE
<!--NeedCopy-->
```

> **Nota:**
>
> Sustituya todo el texto en mayúscula por los detalles reales del recurso.

#### Aprovisionar una máquina virtual en un nodo de arrendatario único

Use los nodos de arrendatario único para mantener sus máquinas virtuales separadas físicamente de las máquinas virtuales de otros proyectos, o para agruparlas en el mismo hardware de host. Para obtener información sobre el nodo de arrendatario único, consulte el documento de GCP Descripción general de los usuarios únicos.

Para aprovisionar una máquina virtual (origen del perfil de máquina) en el nodo de arrendatario único, consulte el documento de GCP Aprovisionar VM en nodos de usuario único.

> **Nota:**
>
> - Seleccione el mismo tipo de instancia y región que el grupo de nodos.
> - Habilite vTPM en la sección de VM protegida. Para obtener más información, consulte Guía de inicio rápido: Habilita las opciones de VM protegida.
> - Inhabilite Bitlocker en la máquina virtual de origen.

#### Crear un catálogo de máquinas de MCS con el origen del perfil de máquina de Windows 11

Puede crear un catálogo de máquinas de MCS para crear máquinas virtuales de Windows 11 mediante la interfaz de Configuración completa o los comandos de PowerShell.

> **Nota:**
>
> - Para la imagen maestra, seleccione instantánea o VM de Windows 11.
> - Para el origen del perfil de la máquina, seleccione VM de Windows 11 como perfil de máquina. El origen del perfil de máquina debe tener el mismo tipo de instancia que se describe en el nodo de arrendatario único.

Para obtener información sobre el uso de la interfaz de Configuración completa, consulte Crear un catálogo de máquinas mediante la interfaz de Configuración completa.

Para obtener información sobre los comandos de PowerShell, consulte Crear un catálogo de máquinas mediante un perfil de máquina.

Después de crear el catálogo y encender las máquinas virtuales, puede ver las máquinas virtuales de Windows 11 que se ejecutan en el nodo de arrendatario único en la consola de Google Cloud.

### Google Cloud Marketplace

Puede buscar y seleccionar imágenes que ofrece Citrix en Google Cloud Marketplace para crear catálogos de máquinas. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función.

Para buscar el producto de VM Citrix VDA en Google Cloud Marketplace, vaya a https://console.cloud.google.com/marketplace/.

Puede usar una imagen personalizada o una imagen preparada por Citrix en Google Cloud Marketplace para actualizar una imagen de un catálogo de máquinas.

> **Nota:**
>
> Si el perfil de la máquina no contiene información sobre el tipo de almacenamiento, el valor se deriva de las propiedades personalizadas.

Las imágenes compatibles de Google Cloud Marketplace son:

- Windows 2019 de sesión única
- Windows 2019 multisesión
- Ubuntu

Ejemplo de uso de una imagen preparada por Citrix como origen para crear un catálogo de máquinas:

```
New-ProvScheme -ProvisioningSchemeName GCPCatalog \
-HostingUnitName GcpHu -IdentityPoolName gcpPool -CleanOnBoot \
-MasterImageVM XDHyp:\HostingUnits\GcpHu\images.folder\citrix-daas-
   win2019-single-vda-v20220819.publicimage \
-MachineProfile XDHyp:\HostingUnits\GcpHu\Base.vm
<!--NeedCopy-->
```

### Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de Google Cloud Platform.

### Más información

- Crear y administrar conexiones y recursos
- Conexión con entornos de Google Cloud
- Crear catálogos de máquinas

## Crear un catálogo de máquinas de HPE Moonshot

May 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de HPE Moonshot.

> **Nota:**
>
> - Crear una conexión con HPE Moonshot
> - Compruebe que tiene uno o más nodos de HPE Moonshot disponibles e instale los VDA en esos nodos.
> - Para obtener información sobre cómo crear la imagen de cartucho inicial de HPE Moonshot, consulte el documento OS Deployment on Moonshot User Guide.

Puede crear un catálogo de máquinas de HPE Moonshot con:

- Interfaz de Configuración completa
- Comandos de PowerShell

### Crear un catálogo de máquinas mediante la interfaz de Configuración completa

En el asistente de **Configuración de catálogo de máquinas**:

1. En la página **Sistema operativo**, seleccione **SO multisesión** o **SO de sesión única**.
2. En la página **Administración de máquinas**, seleccione **Máquinas con administración de energía** y **Otro servicio o tecnología**.
3. En la página **Máquinas virtuales**, agregue máquinas y sus cuentas de máquinas de Active Directory. Puede realizar una de las siguientes acciones:
    - Haga clic en **Agregar máquinas** para agregar máquinas manualmente. Aparecerá la ventana **Seleccionar VM**. Expanda la conexión de chasis HPE Moonshot que creó anteriormente y seleccione los nodos (VM) que quiere agregar. A continuación, agregue los nombres de las cuentas de máquina asociadas.

- Haga clic en **Agregar archivo CSV** para agregar máquinas en bloque. Para obtener información sobre el uso de archivos CSV para agregar máquinas, consulte Usar archivos CSV para agregar máquinas en bloque a un catálogo.

Las páginas **Ámbitos** y **Resumen** no contienen información específica de HPE Moonshot.

### Crear un catálogo de máquinas mediante comandos de PowerShell

Ejecute los comandos `New-BrokerCatalog` y `New-BrokerMachine` de PowerShell para crear un catálogo de brokers e importar máquinas a dicho catálogo.

Por ejemplo:

```
1 New-BrokerCatalog -AllocationType "Random" -IsRemotePC $False -
    MachinesArePhysical $False -MinimumFunctionalLevel "L7_20" -Name "
    BurMC" -PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
    Scope @() -SessionSupport "MultiSession" -ZoneUid "e166e2cb-25dc
    -4578-bc07-bcf2a82d1463"
2 New-BrokerMachine -CatalogUid 3 -HostedMachineId "c10n1" -
    HypervisorConnectionUid 4 -IsReserved $False -MachineName "S
    -1-5-21-2589939477-3963209805-1860259709-1121"
3 <!--NeedCopy-->
```

### Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de HPE Moonshot.

### Más información

- Crear y administrar conexiones y recursos
- Conexión a HPE Moonshot
- Crear catálogos de máquinas

## Crear un catálogo de Microsoft Azure

June 13, 2024

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

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de crear un catálogo de Microsoft Azure, debe terminar de crear una conexión con Microsoft Azure. Consulte Conexión con Microsoft Azure.

### Creación de un catálogo de máquinas

Puede crear un catálogo de máquinas de dos maneras:

- Interfaz de Configuración completa.
- PowerShell. Consulte Administrar Citrix DaaS mediante Remote PowerShell SDK. Para obtener información sobre cómo implementar funciones específicas con PowerShell, consulte Usar PowerShell.

### Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa

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

Una imagen puede ser un disco, una instantánea o la versión de una imagen de una definición de imagen en Azure Compute Gallery que se usa para crear las máquinas virtuales en un catálogo de máquinas.

Antes de crear el catálogo de máquinas, cree una imagen en Azure Resource Manager.

> **Nota:**
>
> - Se ha retirado el uso de discos no administrados para aprovisionar máquinas virtuales.
> - Se retiró la compatibilidad con el uso de una imagen maestra de una región diferente a la configurada en la conexión del host. Use Azure Compute Gallery para replicar la imagen maestra en la región deseada.

Durante la preparación de la imagen, se crea una máquina virtual (VM) de preparación basada en la máquina virtual original. Esta máquina virtual de preparación está desconectada de la red. Para

desconectar la red de la máquina virtual de preparación, se crea un grupo de seguridad de red para denegar todo el tráfico entrante y saliente. El grupo de seguridad de red se crea automáticamente una vez por catálogo. El nombre del grupo de seguridad de red es `Citrix-Deny-All-a3pgu-GUID`, donde el GUID se genera aleatoriamente. Por ejemplo, `Citrix-Deny-All-a3pgu-3f161981-28e2-4223-b797-88b04d336dd1`.

En el asistente para la creación de catálogos de máquinas:

1. Las páginas **Tipo de máquina** y **Administración de máquinas** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
2. En la página **Imagen**, seleccione la imagen que quiera utilizar como imagen maestra para todas las máquinas del catálogo. Aparecerá el asistente para **seleccionar una imagen**. Siga estos pasos para seleccionar una imagen:

   a) (Aplicable solo a las conexiones configuradas con imágenes compartidas en o entre arrendatarios). Seleccione una suscripción en la que resida la imagen.
   b) Seleccione un grupo de recursos.
   c) Vaya a la versión de imagen de Azure, disco administrado de Azure o Azure Compute Gallery.

   Al seleccionar una imagen, tenga en cuenta lo siguiente:

   - Compruebe que hay un VDA de Citrix instalado en la imagen.
   - Si selecciona un disco conectado a una máquina virtual, debe apagar esta antes de continuar con el siguiente paso.

   > **Nota:**
   >
   > - La suscripción correspondiente a la conexión (host) que creó las máquinas del catálogo se indica con un punto verde. Las demás suscripciones son aquellas en las que se comparte Azure Compute Gallery con esa suscripción. En esas suscripciones, solo se muestran las galerías compartidas. Para obtener información sobre cómo configurar las suscripciones compartidas, consulte Compartir imágenes con un arrendatario (entre suscripciones) y Compartir imágenes entre arrendatarios.
   > - Puede crear un esquema de aprovisionamiento mediante un disco de SO efímero en Windows con inicio seguro. Al seleccionar una imagen con inicio seguro, debe seleccionar un perfil de máquina con inicio seguro que esté habilitado con vTPM. Para crear catálogos de máquinas con un disco de SO efímero, consulte Cómo crear máquinas con discos de SO efímeros.
   > - Durante la replicación de imágenes, puede continuar y seleccionar la imagen como imagen maestra y completar la configuración. Sin embargo, es posible que la creación de catálogos tarde más tiempo en completarse mientras se replica la imagen. MCS

> necesita que la replicación se complete en una hora a partir de la creación de catálogos. Si la replicación tarda más, no se crean los catálogos. Puede verificar el estado de la replicación en Azure. Inténtelo de nuevo si la replicación sigue pendiente o después de que se haya completado.
> - Puede aprovisionar un catálogo de máquinas virtuales de 2.ª generación mediante una imagen de 2.ª generación para mejorar el rendimiento del tiempo de arranque. Sin embargo, no se admite la creación de catálogos de máquinas de 2.ª generación con una imagen de 1.ª generación. Del mismo modo, tampoco se admite la creación de catálogos de máquinas de 1.ª generación con una imagen de 2.ª generación. Además, cualquier imagen antigua que no tenga información de generación es una imagen de 1.ª generación.

Elija si quiere que las máquinas virtuales del catálogo hereden configuraciones de un perfil de máquina. De forma predeterminada, está marcada la casilla **Usar un perfil de máquina (obligatorio para Azure Active Directory)**. Haga clic en **Seleccione un perfil de máquina** para buscar una VM o una especificación de plantilla de ARM en una lista de grupos de recursos.

Algunos ejemplos de configuraciones que las máquinas virtuales pueden heredar de un perfil de máquina incluyen:

- Redes aceleradas
- Diagnóstico de arranque
- Almacenamiento en caché de discos de host (relacionado con discos de SO y de E/S de MCS)
- Tamaño de máquina (a menos que se especifique lo contrario)
- Etiquetas colocadas en la máquina virtual

> **Nota:**
>
> - Al seleccionar una imagen maestra para los catálogos de máquinas en Azure, el perfil de máquina se filtra en función de la imagen maestra que seleccione. Por ejemplo, el perfil de la máquina se filtra en función del sistema operativo Windows, el tipo de seguridad, la compatibilidad con la hibernación y el ID del conjunto de cifrado de discos de la imagen maestra.
> - Es obligatorio usar un perfil de máquina con Inicio seguro como **Tipo de seguridad** al seleccionar una imagen o una instantánea que tenga habilitado el inicio seguro. A continuación, para habilitar o inhabilitar SecureBoot y vTPM, especifique sus valores en el perfil de la máquina. Para obtener información sobre el inicio de confianza de Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Valide la especificación de plantilla ARM para asegurarse de que se puede utilizar como perfil de

máquina para crear un catálogo de máquinas. Para obtener información sobre cómo crear una especificación de plantilla de Azure, consulte Crear una especificación de plantilla de Azure.

Hay dos formas de validar la especificación de la plantilla ARM:

- Después de seleccionar la especificación de plantilla ARM en la lista de grupos de recursos, haga clic en **Siguiente**. Aparecen mensajes de error si la especificación de plantilla ARM contiene errores.
- Ejecute uno de estos comandos de PowerShell:
  - `Test-ProvInventoryItem -HostingUnitName <string> -InventoryPath <string>`
  - `Test-ProvInventoryItem -HostingUnitUid <Guid> -InventoryPath <string>`

  Por ejemplo:

```
1  Test-ProvInventoryItem -HostingUnitName "we-vdi0101-d-vnet" -
      InventoryPath machineprofile.folder/vdi01-d-rg.
      resourcegroup/VDD-templ-spec.templatespec/1.5.
      templatespecversion
2  <!--NeedCopy-->
```

Tras crear el catálogo, podrá ver las configuraciones que la imagen hereda del perfil de máquina. En el nodo **Catálogos de máquinas**, seleccione el catálogo para ver sus detalles en el panel inferior. A continuación, haga clic en la ficha **Propiedades de plantilla** para ver las propiedades del perfil de máquina. La sección **Etiquetas** muestra hasta tres etiquetas. Para ver todas las etiquetas colocadas en la máquina virtual, haga clic en **Ver todo**.

Si quiere que MCS aprovisione máquinas virtuales en un host dedicado de Azure, active la casilla de verificación **Usar un grupo de hosts** y, a continuación, seleccione un grupo de hosts de la lista. Un grupo de hosts es un recurso que representa un conjunto de hosts dedicados. Un host dedicado es un servicio que proporciona servidores físicos que alojan una o más máquinas virtuales. Su servidor está dedicado a su suscripción de Azure, no se comparte con otros suscriptores. Cuando utiliza un host dedicado, Azure garantiza que sus máquinas virtuales sean las únicas máquinas activas en ese host. Esta función es adecuada para situaciones en las que debe cumplir con requisitos normativos o de seguridad interna. Para obtener más información sobre los grupos de hosts y las consideraciones para usarlos, consulte Aprovisionar VM en hosts dedicados de Azure.

> **Importante:**
>
> - Solo se muestran los grupos de hosts que tienen habilitada la ubicación automática de Azure.
> - El uso de un grupo de hosts cambia la página **Máquinas virtuales** que se ofrece más

> adelante en el asistente. En esa página, solo se muestran los tamaños de máquina que contiene el grupo de hosts seleccionado. Además, las zonas de disponibilidad se seleccionan automáticamente y no están disponibles para selección manual.

3. La página **Tipos de licencia y almacenamiento** solo aparece cuando se usa una imagen de Azure Resource Manager.

   Puede utilizar los siguientes tipos de almacenamiento para el catálogo de máquinas:

   - **SSD Premium**. Ofrece una opción de almacenamiento en disco de alto rendimiento y baja latencia, adecuada para máquinas virtuales con cargas de trabajo intensivas de E/S.
   - **SSD estándar**. Ofrece una opción de almacenamiento rentable, adecuada para cargas de trabajo que necesitan un rendimiento uniforme a niveles de IOPS más bajos.
   - **HDD estándar**. Ofrece una opción de almacenamiento en disco fiable y de bajo coste, adecuada para máquinas virtuales que ejecutan cargas de trabajo donde no importa la latencia.
   - **Disco de SO efímero de Azure**. Ofrece una opción de almacenamiento rentable que reutiliza el disco local de las VM para alojar el disco del sistema operativo. Como alternativa, puede usar PowerShell para crear máquinas que usen discos de SO efímeros. Para obtener más información, consulte Discos efímeros de Azure. Tenga en cuenta lo siguiente cuando utilice un disco de SO efímero:
     - El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.
     - Para actualizar máquinas que usan discos de SO efímeros, debe seleccionar una imagen cuyo tamaño no exceda el tamaño del disco de caché o el disco temporal de la VM.
     - No puede usar la opción **Conservar VM y disco del sistema durante los ciclos de energía** que se ofrece más adelante en el asistente.

   > **Nota:**
   >
   > El disco de identidad siempre se crea con un SSD estándar, independientemente del tipo de almacenamiento que elija.

   El tipo de almacenamiento determina el tamaño de las máquinas que se ofrecen en la página **Máquinas virtuales** del asistente. MCS configura discos premium y estándar para uso de almacenamiento con redundancia local (LRS). LRS hace varias copias sincrónicas de los datos en un único centro de datos. Los discos de SO efímeros de Azure usan el disco local de las VM para almacenar el sistema operativo. Para obtener más información acerca de los tipos de almacenamiento y la replicación de almacenamiento de Azure, consulte lo siguiente:

   - Introducción a Azure Storage

- Azure Premium Storage: diseño para un alto rendimiento
- Redundancia de Azure Storage

Seleccione si utilizar licencias de Windows o de Linux existentes:

- Licencias de Windows: El uso de licencias de Windows junto con imágenes de Windows (imágenes que admita la plataforma Azure o imágenes personalizadas) permite ejecutar máquinas virtuales de Windows en Azure a un coste reducido. Existen dos tipos de licencias:
  - **Licencia de Windows Server**. Le permite utilizar sus licencias de Windows Server o Azure Windows Server, con lo que puede usar las ventajas híbridas de Azure. Para obtener información detallada, consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Las ventajas híbridas de Azure reducen los costes de ejecución de máquinas virtuales en Azure a la tarifa básica de procesamiento, lo que elimina el gasto en licencias de Windows Server adicionales desde la galería de Azure.
  - **Licencia de cliente de Windows**. Le permite llevar sus licencias de Windows 10 y Windows 11 a Azure, con lo que puede usar máquinas virtuales con Windows 10 y Windows 11 en Azure sin necesidad de licencias adicionales. Para obtener más información, consulte Licencias de acceso de cliente y licencias de administración.
- Licencias de Linux: Con las licencias de Linux de su propia suscripción (BYOS), no tiene que pagar por el software. El cargo de las licencias BYOS solo incluye la tarifa de hardware del procesamiento. Existen dos tipos de licencias:
  - **RHEL_BYOS**: Para usar correctamente el tipo RHEL_BYOS, habilite Red Hat Cloud Access en su suscripción de Azure.
  - **SLES_BYOS**: Las versiones de BYOS de SLES permiten el uso de SUSE.

Observe a continuación:

- Verificar la licencia de Windows
- Configurar la licencia de Linux

Consulte estos documentos para comprender los tipos de licencias y sus beneficios:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery es un repositorio que sirve para administrar y compartir imágenes. Le permite poner sus imágenes a disposición de toda la organización. Le recomendamos almacenar una imagen en Azure Compute Gallery al crear grandes catálogos de máquinas no persistentes, ya que, así, los discos del SO de VDA se pueden restablecer más rápidamente. Después

de seleccionar **Colocar la imagen preparada en Azure Compute Gallery**, aparece la sección de **configuración de Azure Compute Gallery**, que le permite especificar más parámetros de Azure Computer Gallery:

- **Índice de máquinas virtuales por réplica de imagen**. Permite especificar la ratio de máquinas virtuales y réplicas de imagen que mantendrá Azure. De forma predeterminada, Azure mantiene una única réplica de imagen por cada 40 máquinas no persistentes. En el caso de máquinas persistentes, la cantidad predeterminada es de 1000 máquinas.
- **Máximo de réplicas**. Permite especificar el máximo de réplicas de imagen que conservará Azure. El valor predeterminado es 10.

Para obtener información sobre Azure Compute Gallery, consulte Azure Compute Gallery.

4. En la página **Máquinas virtuales**, indique la cantidad de máquinas virtuales que quiere crear y su tamaño. Después de crear el catálogo, puede modificar el catálogo para cambiar el tamaño de la máquina.
5. La página **Tarjetas NIC** no contiene información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
6. En la página **Parámetros del disco**, elija si quiere habilitar la caché de reescritura. Con la función de optimización del almacenamiento de MCS habilitada, puede configurar los siguientes parámetros al crear un catálogo: Esta configuración se aplica tanto a los entornos de Azure como a los de GCP.

   Después de habilitar la caché de reescritura, puede hacer lo siguiente:

   - Puede configurar la RAM y el tamaño del disco utilizados para almacenar en caché datos temporales. Para obtener más información, consulte Configurar la caché de datos temporales.
   - Seleccione el tipo de almacenamiento del disco de caché con reescritura. Están disponibles las siguientes opciones de almacenamiento para uso con el disco de caché con reescritura:
     - SSD Premium
     - SSD estándar
     - HDD estándar
   - Elija si prefiere que el disco de caché de reescritura sea persistente para las máquinas virtuales aprovisionadas. Seleccione **Habilitar caché con reescritura** para que estas opciones estén disponibles. De forma predeterminada, se selecciona **Usar disco no persistente de caché con reescritura**.
   - Seleccione el tipo de disco de caché con reescritura.

  - **Usar disco no persistente de caché con reescritura**. Si se selecciona, el disco de caché con reescritura se elimina durante los ciclos de energía. Se perderán todos los datos redirigidos a él. Si el disco temporal de la VM tiene suficiente espacio, se usa para alojar el disco de caché con reescritura para reducir los costes. Tras la creación del catálogo, puede comprobar si las máquinas aprovisionadas utilizan el disco temporal. Para ello, haga clic en el catálogo y verifique la información de la ficha **Propiedades de plantilla**. Si se usa el disco temporal, verá **Disco no persistente de caché con reescritura**, y su valor es **Sí (con el disco temporal de la máquina virtual)**. De lo contrario, verá **Disco no persistente de caché con reescritura**, y su valor es **No (sin usar el disco temporal de la VM)**.
  - **Usar disco persistente de caché con reescritura**. Si se selecciona, el disco de caché con reescritura persiste en las máquinas virtuales aprovisionadas. Habilitar esta opción aumenta los costes de almacenamiento.

- Elija si quiere conservar las VM y los discos del sistema para los VDA durante los ciclos de energía.

  **Conservar VM y disco del sistema durante los ciclos de energía.** Disponible al seleccionar **Habilitar caché con reescritura**. De forma predeterminada, las VM y los discos del sistema se eliminan al apagar la máquina y se crean de nuevo al iniciarla. Si quiere reducir los tiempos de reinicio de las máquinas virtuales, seleccione esta opción. Recuerde que habilitar esta opción también aumenta los costes de almacenamiento.

- Elija si quiere **habilitar el ahorro de costes de almacenamiento**. Si se habilita, para ahorrar costes de almacenamiento, revierta el disco de almacenamiento a un disco duro estándar cuando la máquina virtual se apague. La máquina virtual cambia a sus parámetros originales al reiniciarse. La opción se aplica tanto a los discos de almacenamiento como a los discos de caché de reescritura. También puede usar PowerShell. Consulte Cambiar el tipo de almacenamiento a un nivel inferior al apagar una máquina virtual.

  > **Nota:**
  >
  > Microsoft impone restricciones al cambiar el tipo de almacenamiento durante el apagado de máquinas virtuales. También es posible que, en el futuro, Microsoft bloquee cambios en el tipo de almacenamiento. Para obtener más información, consulte este artículo de Microsoft.

- Elija si quiere cifrar los datos de las máquinas de este catálogo y qué clave de cifrado usar. El cifrado del lado del servidor con una clave administrada por el cliente (CMK) permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Los parámetros predeterminados se heredan del perfil de máquina o de la imagen maestra, y el perfil tiene prioridad:

- Si usa un *perfil de máquina* con una clave *CMK*, se selecciona automáticamente la opción **Utilice esta clave para cifrar datos en cada máquina** y se establece de forma predeterminada en la clave del *perfil de máquina*.
- Si usa un *perfil de máquina* con una clave administrada por la plataforma (PMK) y la *imagen maestra* está cifrada con *CMK*, se selecciona automáticamente la opción **Utilice esta clave para cifrar datos en cada máquina** y se establece de forma predeterminada en la clave de la imagen maestra.
- Si *no* usa un *perfil de máquina* y la *imagen maestra* está cifrada con *CMK*, se selecciona automáticamente la opción **Utilice esta clave para cifrar datos en cada máquina** y se establece de forma predeterminada en la clave de la *imagen maestra*.

Para obtener más información, consulte Cifrado del lado del servidor de Azure.

7. En la página **Grupo de recursos**, elija si quiere crear grupos de recursos o usar los grupos existentes.

   - Si opta por crear grupos de recursos, seleccione **Siguiente**.
   - Si decide utilizar los grupos de recursos existentes, seleccione esos grupos en la lista **Grupos de recursos de aprovisionamiento disponibles**.

   > **Nota:**
   >
   > Debe seleccionar grupos suficientes para las máquinas que está creando en el catálogo. Si no elige suficientes, aparecerá un mensaje. Puede seleccionar más del mínimo requerido de máquinas si va a agregar más máquinas al catálogo más tarde. No se puede agregar más grupos de recursos a un catálogo una vez creado el catálogo.

   Para obtener más información, consulte Grupos de recursos de Azure.

8. En la página **Identidades de las máquinas**, elija un tipo de identidad y configure las identidades de las máquinas de este catálogo. Si selecciona las máquinas virtuales como **unidas a Azure Active Directory**, puede agregarlas a un grupo de seguridad de Azure AD. Estos son los pasos detallados:

   a) En el campo **Tipo de identidad**, seleccione **Unido a Azure Active Directory**. Aparecerá la opción **Grupo de seguridad de Azure AD (opcional)**.
   b) Haga clic en **Grupo de seguridad de Azure AD: Crear nuevo**.
   c) Introduzca un nombre de grupo y, a continuación, haga clic en **Crear**.
   d) Siga las instrucciones que aparecen en pantalla para iniciar sesión en Azure.
   Si el nombre del grupo no existe en Azure, aparecerá un icono verde. De lo contrario, aparecerá un mensaje de error en el que se le pide que introduzca un nombre nuevo.
   e) Para agregar el grupo de seguridad a un grupo de seguridad asignado, seleccione **Unirse a un grupo de seguridad asignado como miembro** y, a continuación, haga clic en **Seleccione un grupo** para elegir un grupo asignado al que unirse.

f) Introduzca el esquema de nomenclatura de las cuentas de máquina para las máquinas virtuales.

Tras la creación del catálogo, Citrix DaaS accede a Azure en su nombre y crea el grupo de seguridad y una regla de pertenencia dinámica para el grupo. Según la regla, las máquinas virtuales con el esquema de nomenclatura especificado en este catálogo se agregan automáticamente al grupo de seguridad.

Para agregar a este catálogo máquinas virtuales con un esquema de nomenclatura diferente, debe iniciar sesión en Azure. A continuación, Citrix DaaS puede acceder a Azure y crear una regla de pertenencia dinámica basada en el nuevo esquema de nomenclatura.

Para poder eliminar el grupo de seguridad de Azure al eliminar este catálogo, también es necesario iniciar sesión en Azure.

> **Nota:**
>
> Para cambiar el nombre del grupo de seguridad de Azure AD tras la creación del catálogo, modifique el catálogo y vaya a **Grupo de seguridad de Azure AD** en el menú de navegación de la izquierda. Los nombres de los grupos de seguridad de Azure AD no deben contener estos caracteres: `@ "\ / ; : # . * ? = < > | [ ] ( )'`.

- Las páginas **Credenciales de dominio** y **Resumen** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.

Complete el asistente.

### Crear una especificación de plantilla de Azure

Puede crear una especificación de plantilla de Azure en Azure Portal y utilizarla en la interfaz de Configuración completa y en los comandos de PowerShell para crear o actualizar catálogos de máquinas de MCS.

Para crear una especificación de plantilla de Azure para una máquina virtual existente:

1. Vaya a Azure Portal. Seleccione un grupo de recursos y, a continuación, seleccione la VM y la interfaz de red. En el menú **...** de la parte superior, haga clic en **Export template**.
2. Desmarque la casilla **Include parameters** si quiere crear una especificación de plantilla para el aprovisionamiento de catálogos.
3. Haga clic en **Add to library** para modificar la especificación de la plantilla más adelante.
4. En la página **Importing template**, introduzca la información requerida, como **Name**, **Subscription**, **Resource Group**, **Location** y **Version**. Haga clic en **Next: Edit Template**.

5. También necesita una interfaz de red como recurso independiente si quiere aprovisionar catálogos. Por lo tanto, debe quitar cualquier `dependsOn` especificado en la especificación de la plantilla. Por ejemplo:

```
"dependsOn": [
"[resourceId('Microsoft.Network/networkInterfaces', 'tnic937')]"
],
<!--NeedCopy-->
```

6. Haga clic en **Review+Create** y cree la especificación de la plantilla.
7. En la página **Template Specs**, compruebe la especificación de plantilla que creó. Haga clic en la especificación de la plantilla. En el panel de la izquierda, haga clic en **Versions**.
8. Para crear otra versión, haga clic en **Create new version**. Especifique un nuevo número de versión, modifique la especificación de la plantilla actual y haga clic en **Review+Create** para crear la otra versión de la especificación de plantilla.

Puede obtener información sobre la especificación y la versión de la plantilla mediante estos comandos de PowerShell:

- Para obtener información sobre la especificación de la plantilla, ejecute:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec
<!--NeedCopy-->
```

- Para obtener información sobre la versión de la especificación de la plantilla, ejecute:

```
get-item XDHyp:\HostingUnits\East\machineprofile.folder\abc.
    resourcegroup\bggTemplateSpec.templatespec\bgg1.0.
    templatespecversion
<!--NeedCopy-->
```

#### Usar una especificación de plantilla para crear o actualizar un catálogo

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar la interfaz de Configuración completa o los comandos de PowerShell.

- Mediante la interfaz de **Configuración completa**: Consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.
- Para PowerShell: Consulte Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

## Aprovisionar máquinas en zonas de disponibilidad especificadas

En entornos de Azure, es posible aprovisionar máquinas en zonas de disponibilidad específicas. Para ello, use la interfaz de Configuración completa o PowerShell

> **Nota:**
>
> Si no se especifica ninguna zona, MCS permite a Azure colocar las máquinas dentro de la región. Si se especifica más de una zona, MCS distribuye aleatoriamente las máquinas entre ellas.

### Configurar zonas de disponibilidad en la interfaz de Configuración completa

Al crear un catálogo de máquinas, puede especificar las zonas de disponibilidad en las que quiere aprovisionar máquinas. En la página **Máquinas virtuales**, seleccione una o varias zonas de disponibilidad donde quiera crear máquinas.

Hay dos razones por las que podría no haber zonas de disponibilidad disponibles: La región no tiene zonas de disponibilidad o el tamaño de máquina seleccionado no está disponible.

Para obtener información sobre cómo configurar mediante un comando de PowerShell, consulte Configurar zonas de disponibilidad con PowerShell.

## Discos efímeros de Azure

Un disco efímero de Azure le permite reutilizar el disco de caché o el disco temporal para almacenar el disco del sistema operativo de una máquina virtual habilitada para Azure. Esta funcionalidad es útil en entornos de Azure que requieren un disco SSD de mayor rendimiento, en lugar de un disco HDD estándar. Para obtener información sobre cómo crear un catálogo con un disco efímero de Azure, consulte Crear un catálogo con un disco efímero de Azure.

> **Nota:**
>
> Los catálogos persistentes no admiten discos de SO efímeros.

Los discos de SO efímeros requieren que el esquema de aprovisionamiento use discos administrados y una Azure Compute Gallery. Para obtener más información, consulte Shared Image Gallery de Azure.

### Almacenamiento de un disco de SO efímero temporal

Tiene la posibilidad de almacenar un disco de SO efímero en el disco temporal de la VM o en un disco de recursos. Esta funcionalidad le permite usar un disco de SO efímero con una máquina virtual que

no tenga caché o que no tenga suficiente caché. Estas VM tienen un disco temporal o de recursos para almacenar un disco de SO efímero, como Ddv4.

Se deben tener en cuenta las siguientes cuestiones:

- Un disco efímero se almacena en el disco de caché o en el disco temporal (de recursos) de las VM. Se prefiere el disco de caché antes que el disco temporal, a menos que el disco de caché no sea lo suficientemente grande como para albergar el contenido del disco del sistema operativo.
- En el caso de las actualizaciones, si una nueva imagen es más grande que el disco de caché, pero más pequeña que el disco temporal, el disco de SO efímero se sustituye por el disco temporal de la VM.

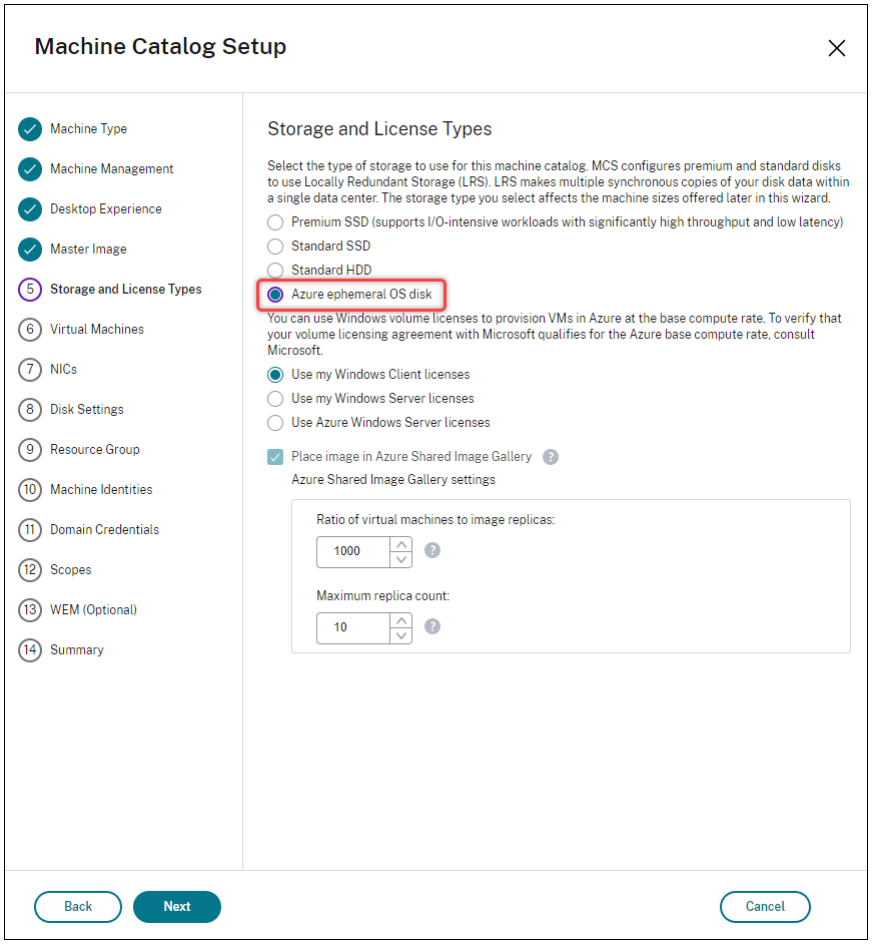
### Optimización del almacenamiento (E/S de MCS) con discos efímeros de Azure y Machine Creation Services (MCS)

El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.

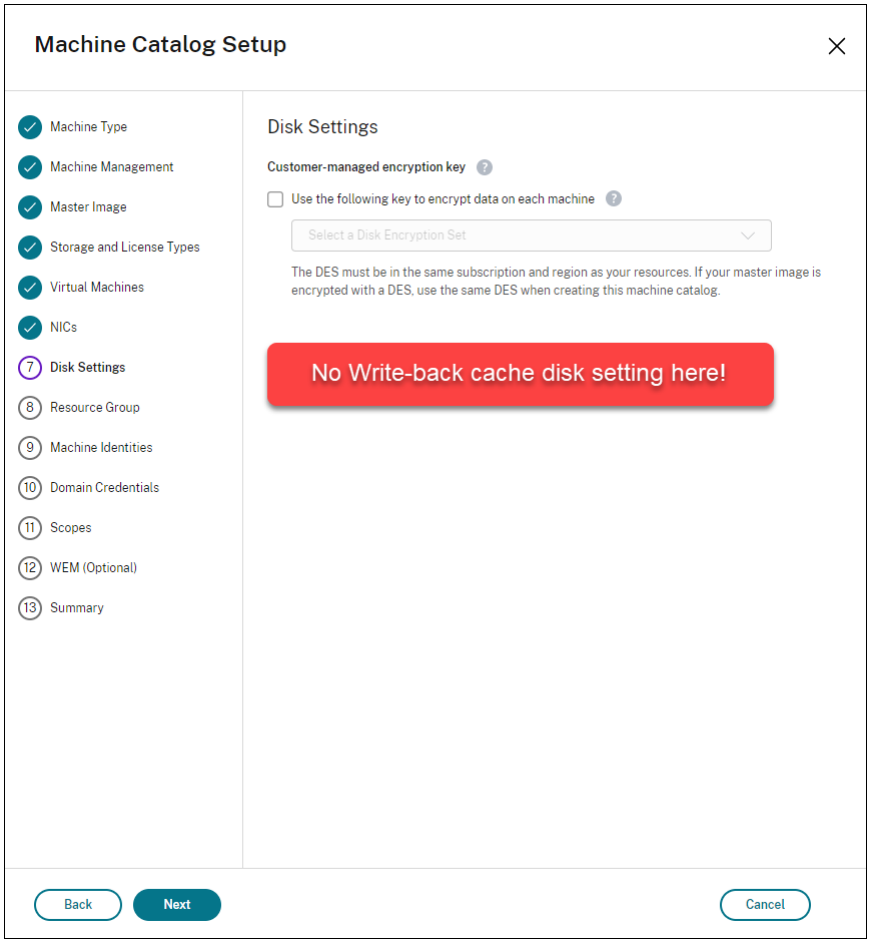
Las consideraciones importantes son las siguientes:

- No puede crear un catálogo de máquinas con el disco de SO efímero y la E/S de MCS habilitados al mismo tiempo.
- En el asistente de **Configuración del catálogo de máquinas**, si selecciona **Disco de SO efímero de Azure** en la página **Tipos de licencia y almacenamiento**, no obtiene la opción de configuración del disco de caché de reescritura en la página **Parámetros del disco**.






- Los parámetros de PowerShell (`UseWriteBackCache` y `UseEphemeralOsDisk`) establecidos en **true** en `New-ProvScheme` o `Set-ProvScheme` fallan con el mensaje de error correspondiente.
- Para catálogos de máquinas existentes creados con ambas funciones habilitadas, aún puede:
  - actualizar un catálogo de máquinas;
  - agregar o eliminar máquinas virtuales;
  - eliminar un catálogo de máquinas.

### Azure Compute Gallery

Utilice Azure Compute Gallery (antes, Shared Image Gallery) como repositorio de imágenes publicadas para máquinas aprovisionadas por MCS en Azure. Puede almacenar una imagen publicada en la galería para acelerar la creación e hidratación de discos de SO, mejorando los tiempos de inicio y lanzamiento de aplicaciones en máquinas virtuales no persistentes. Azure Compute Gallery contiene los tres elementos siguientes:

- Galería: El lugar donde se almacenan las imágenes. MCS crea una galería para cada catálogo de máquinas.
- Definición de imagen de la galería: Esta definición incluye información (el tipo y el estado del sistema operativo, la región de Azure) sobre la imagen publicada. MCS crea una definición de imagen para cada imagen creada para el catálogo.
- Versión de la imagen de la galería: Cada imagen de Azure Compute Gallery puede tener varias versiones, y cada versión puede tener varias réplicas en diferentes regiones. Cada réplica es una copia completa de la imagen publicada. Citrix DaaS crea una versión de imagen Standard_LRS (versión 1.0.0) para cada imagen con la cantidad adecuada de réplicas en la región del catálogo en función de la cantidad de máquinas del catálogo, el índice de réplicas configurado y el máximo de réplicas configurado.

> **Nota:**
>
> La funcionalidad de Azure Compute Gallery solo es compatible con los discos administrados. No está disponible para catálogos de máquinas antiguos.

Para obtener más información, consulte Introducción a Shared Image Gallery de Azure.

#### Acceder a imágenes desde Azure Compute Gallery

Al seleccionar una imagen para utilizarla para crear un catálogo de máquinas, puede seleccionar las imágenes que haya creado en Azure Compute Gallery. Estas imágenes aparecen en la lista de imágenes de la página **Imagen** del asistente de configuración del catálogo de máquinas.

Para que aparezcan estas imágenes, haga lo siguiente:

1. Configure Citrix DaaS.
2. Conéctese a Azure Resource Manager.
3. En Azure Portal, cree un grupo de recursos. Para obtener información detallada, consulte Crear una galería Shared Image Gallery de Azure mediante el portal.
4. En el grupo de recursos, cree una galería Azure Compute Gallery.
5. En Azure Compute Gallery, cree una definición de imagen.
6. En la definición de imagen, cree una versión de imagen.

Para obtener información sobre cómo configurar Azure Compute Gallery, consulte Configurar Azure Compute Gallery.

### Condiciones para que el disco temporal de Azure sea apto como disco de caché con reescritura

Solamente puede usar el disco temporal de Azure como disco de caché con reescritura si se cumplen todas las condiciones siguientes:

- El disco de caché con escritura no debe persistir, ya que el disco temporal de Azure no es adecuado para datos persistentes.
- El tamaño de VM de Azure elegido debe incluir un disco temporal.
- No es necesario que el disco de SO efímero esté habilitado.
- Aceptar colocar el archivo de caché con escritura en el disco temporal de Azure.
- El tamaño del disco temporal de Azure debe ser mayor que el tamaño total de (tamaño del disco de caché con reescritura + espacio reservado para el archivo de paginación + 1 GB de espacio de búfer).

#### Casos de disco no persistente de caché con reescritura

En la siguiente tabla se describen tres casos diferentes en los que se utiliza un disco temporal para la caché con reescritura al crear un catálogo de máquinas.

| Caso | Resultado |
| --- | --- |
| Se cumplen todas las condiciones para usar un disco temporal para la caché con reescritura. | El archivo WBC `mcsdif.vhdx` se coloca en el disco temporal. |
| El disco temporal no tiene suficiente espacio para uso de caché con reescritura. | Se crea un disco VHD "MCSWCDisk"y se coloca un archivo WBC `mcsdif.vhdx` en este disco. |
| El disco temporal tiene espacio suficiente para usar caché de reescritura, pero `UseTempDiskForWBC` está configurado como false. | Se crea un disco VHD "MCSWCDisk"y se coloca un archivo WBC `mcsdif.vhdx` en este disco. |

Consulte los siguientes temas de PowerShell:

- Crear un catálogo de máquinas con un disco no persistente de caché con reescritura
- Crear un catálogo de máquinas con un disco persistente de caché con reescritura

### Cifrado del lado del servidor de Azure

Citrix DaaS admite claves de cifrado administradas por el cliente para los discos administrados por Azure a través de Azure Key Vault. Gracias a esta compatibilidad, puede satisfacer los requisitos organizativos y de conformidad mediante el cifrado de los discos administrados del catálogo de máquinas con su propia clave de cifrado. Para obtener más información, consulte Cifrado del lado del servidor de Azure Disk Storage.

Al utilizar esta función para discos administrados:

- Para cambiar la clave con la que está cifrado actualmente el disco, cámbiela en `DiskEncryptionSet`. Todos los recursos asociados a ese `DiskEncryptionSet` se cifrarán con la nueva clave.
- Cuando inhabilite o elimine la clave, todas las máquinas virtuales con discos que utilicen esa clave se apagarán automáticamente. Después de apagarse, las máquinas virtuales no se podrán utilizar, a menos que la clave se vuelva a habilitar o se asigne una nueva clave. Ningún catálogo que utilice la clave se podrá encender ni se le podrán agregar máquinas virtuales.

#### Consideraciones importantes al utilizar claves de cifrado administradas por el cliente

Tenga en cuenta lo siguiente al usar esta funcionalidad:

- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben residir en la misma suscripción y región.
- Los discos, las instantáneas y las imágenes cifradas con claves administradas por el cliente no pueden transferirse a otro grupo de recursos y suscripción.
- Consulte el sitio de Microsoft para conocer las limitaciones de los conjuntos de cifrado de disco por región.

> **Nota:**
>
> Para obtener información acerca de la configuración del cifrado del lado del servidor de Azure, consulte Inicio rápido: Creación de un almacén de claves mediante Azure Portal.

#### Clave de cifrado administrada por el cliente de Azure

Al crear un catálogo de máquinas, puede elegir si cifrar los datos presentes en las máquinas aprovisionadas en el catálogo. El cifrado del lado del servidor con una clave de cifrado administrada por el cliente permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Un conjunto de cifrado de disco (Disk Encryption Set o DES) representa una clave administrada por el cliente. Para utilizar esta función, primero debe crear el DES en Azure. Un DES tiene este formato:

- `/subscriptions/12345678-1234-1234-1234-123456789012/resourceGroups/Sample-RG/providers/Microsoft.Compute/diskEncryptionSets/SampleEncryption`

Seleccione un DES de la lista. El DES que seleccione debe estar en la misma suscripción y región que los recursos.

Si crea un catálogo con una clave de cifrado y posteriormente inhabilita el DES correspondiente en Azure, ya no podrá encender las máquinas del catálogo ni agregarle máquinas.

Consulte Crear un catálogo de máquinas con una clave administrada por el cliente.

### Cifrado de discos de Azure en el host

Puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Puede utilizar una máquina virtual o una especificación de plantilla como entrada para un perfil de máquina.

Este método de cifrado no cifra los datos a través del almacenamiento de Azure. El servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo.

**Restricciones:**

El cifrado de discos de Azure en el host:

- No se admite con todos los tamaños de máquina de Azure
- Es incompatible con el cifrado de discos de Azure

Para obtener más información, consulte:

- Crear un catálogo de máquinas con capacidad de cifrado en el host.
- Obtener la información de cifrado en el host desde un perfil de máquina

### Cifrado doble en disco administrado

Puede crear un catálogo de máquinas con doble cifrado. Todos los catálogos creados con esta función tienen todos los discos cifrados del lado del servidor con claves administradas por la plataforma y por el cliente. Usted posee y mantiene el Azure Key Vault, la clave de cifrado y los conjuntos de cifrado de disco (DES).

El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado.

> **Nota:**
>
> - Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante la interfaz de Configuración completa y los comandos de PowerShell.
> - Puede utilizar un flujo de trabajo no basado en perfiles de máquina o un flujo de trabajo basado en perfiles de máquina para crear o actualizar un catálogo de máquinas con doble cifrado.

> - Si utiliza un flujo de trabajo no basado en perfiles de máquina para crear un catálogo de máquinas, puede reutilizar el `DiskEncryptionSetId` almacenado.
> - Si usa un perfil de máquina, puede usar una máquina virtual o una especificación de plantilla como entrada de perfil de máquina.

#### Limitaciones

- No se admite el cifrado doble en los discos Ultra Disk ni en los discos Premium SSD v2.
- El cifrado doble no se admite en discos no administrados.
- Si inhabilita una clave de un conjunto de cifrado de disco asociados a un catálogo, se inhabilitan las máquinas virtuales del catálogo.
- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben estar en la misma suscripción y región.
- Solo puede crear un máximo de 50 conjuntos de cifrado de disco por región y suscripción.

Consulte los siguientes temas de PowerShell:

- Crear un catálogo de máquinas con doble cifrado
- Convertir un catálogo sin cifrar para usar el cifrado doble
- Verificar que el catálogo tenga un cifrado doble

### Grupos de recursos de Azure

Los grupos de recursos de aprovisionamiento de Azure ofrecen una manera de aprovisionar las VM que proporcionan escritorios y aplicaciones a los usuarios. Puede agregar los grupos de recursos de Azure vacíos existentes cuando cree un catálogo de máquinas con MCS. También puede decidir que se creen nuevos grupos de recursos para usted. Para obtener información acerca de los grupos de recursos de Azure, consulte la documentación de Microsoft.

#### Uso del grupo de recursos de Azure

No hay límite en el número de máquinas virtuales, discos administrados, instantáneas e imágenes por grupo de recursos de Azure (se eliminó la limitación de 240 VM/800 discos administrados por grupo de recursos de Azure).

- Al utilizar la entidad de servicio de ámbito completo para crear un catálogo de máquinas, MCS crea solo un grupo de recursos de Azure y utiliza ese grupo para el catálogo.
- Al utilizar la entidad de servicio de ámbito restringido para crear un catálogo de máquinas, debe proporcionar un grupo de recursos de Azure vacío y creado previamente para el catálogo.

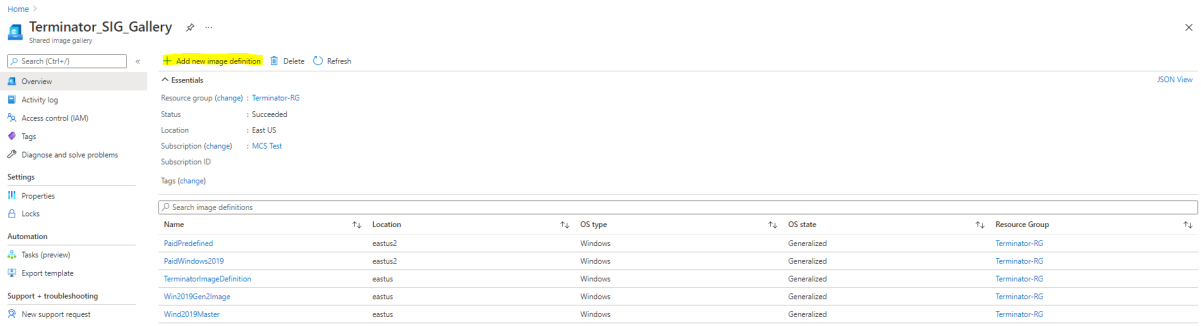
### Azure Marketplace

Citrix DaaS admite el uso de una imagen maestra en Azure que contenga información del plan para crear un catálogo de máquinas. Para obtener más información, consulte Microsoft Azure Marketplace.

> **Sugerencia:**
>
> Algunas imágenes que se encuentran en Azure Marketplace, como la imagen estándar de Windows Server, no llevan anexa información del plan. La funcionalidad Citrix DaaS es para imágenes de pago.

### Compruebe que la imagen creada en Azure Compute Gallery contiene información del plan de Azure

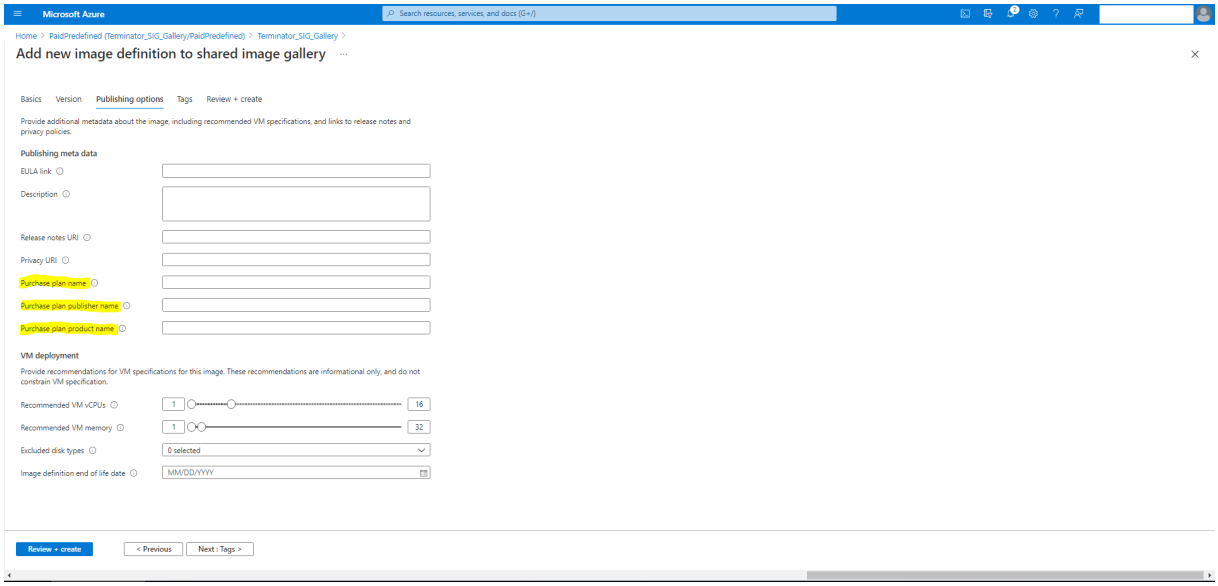
Use el procedimiento descrito en esta sección para ver las imágenes de Azure Compute Gallery en la interfaz de Configuración completa. Estas imágenes se pueden usar, opcionalmente, para una imagen maestra. Para colocar la imagen en una Azure Compute Gallery, cree una definición de imagen en una galería.



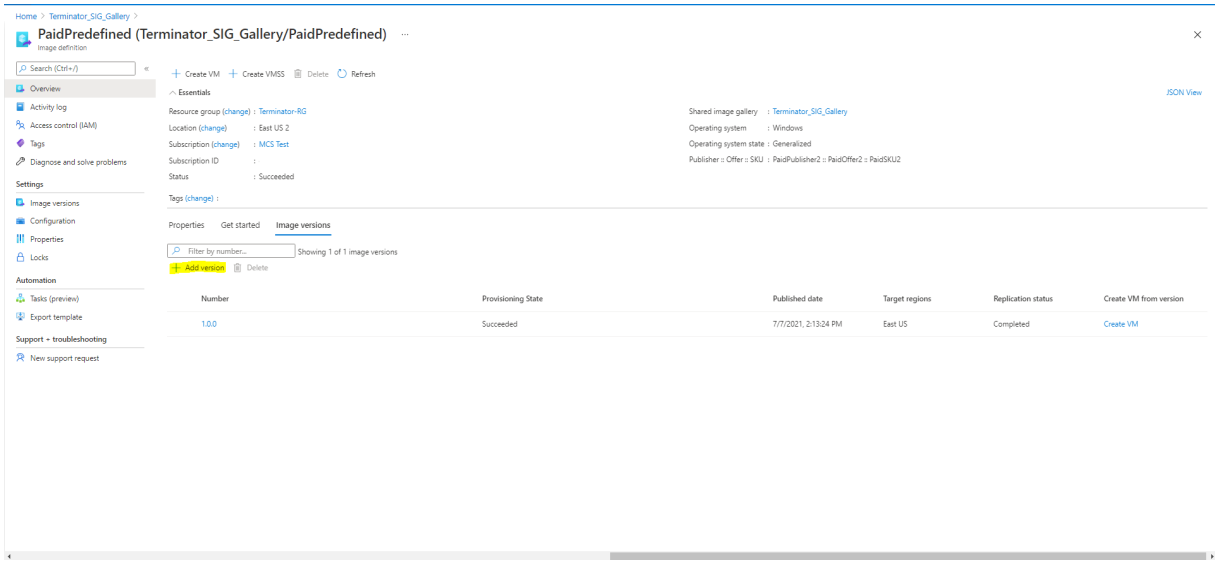

En la página **Publishing options**, verifique la información del plan de compra.

Los campos de información del plan de compra están vacíos inicialmente. Rellene esos campos con la información del plan de compra utilizada para la imagen. Si no se rellena la información del plan de compra, puede ocurrir un error en el procesamiento del catálogo de máquinas.

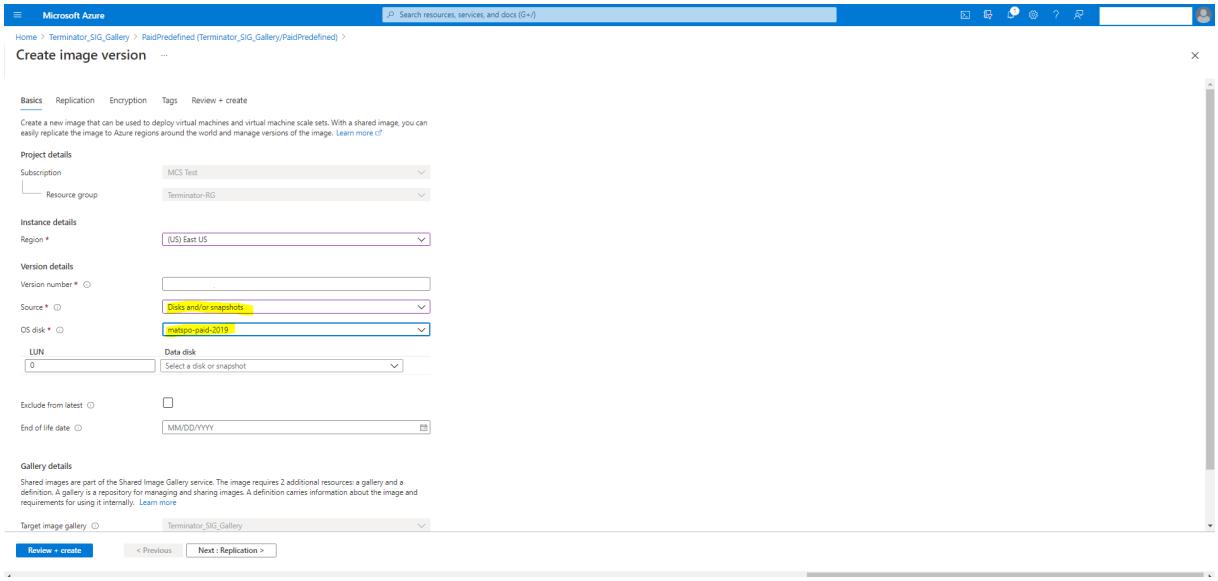



Después de verificar la información del plan de compra, cree una versión de la imagen dentro de la definición. Sirve de imagen maestra. Haga clic en **Add version**:




En la sección **Version details**, seleccione la instantánea de la imagen o el disco administrado como origen:




## Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado

La supervisión de Azure es un servicio que puede utilizar para recopilar, analizar y responder a datos de telemetría de sus entornos locales y de Azure.

El agente de Azure Monitor (AMA) recopila datos de supervisión de recursos de procesamiento, como máquinas virtuales, y los entrega a Azure Monitor. Actualmente, permite la recopilación de registros de eventos y métricas de Syslog y rendimiento, y los envía a los orígenes de datos de las Métricas de Azure Monitor y los Registros de Azure Monitor.

Para habilitar la supervisión mediante la identificación exclusiva de las máquinas virtuales en los datos de supervisión, puede aprovisionar las máquinas virtuales de un catálogo de máquinas de MCS con AMA instalado como extensión.

### Requisitos

- Permisos: Asegúrese de tener los permisos mínimos de Azure especificados en Acerca de los permisos de Azure y estos permisos para usar Azure Monitor:
  - `Microsoft.Compute/virtualMachines/extensions/read`
  - `Microsoft.Compute/virtualMachines/extensions/write`
  - `Microsoft.Insights/DataCollectionRuleAssociations/Read`
  - `Microsoft.Insights/dataCollectionRuleAssociations/write`
  - `Microsoft.Insights/DataCollectionRules/Read`
- Regla de recopilación de datos: Configure una regla de recopilación de datos (DCR) en Azure Portal. Para obtener información sobre cómo configurar una DCR, consulte Creación de una

regla de recopilación de datos. Las DCR son específicas de cada plataforma (Windows o Linux). Asegúrese de crear una DCR según la plataforma requerida.
El AMA utiliza las reglas de recopilación de datos (DCR) para administrar la asignación entre los recursos, como las máquinas virtuales, y los orígenes de datos, como las Métricas de Azure Monitor y los Registros de Azure Monitor.

- Espacio de trabajo predeterminado: Cree un espacio de trabajo en Azure Portal. Para obtener información sobre cómo crear un espacio de trabajo, consulte Creación de un área de trabajo de Log Analytics. Al recopilar registros y datos, la información se almacena en un espacio de trabajo. Un espacio de trabajo tiene un ID de espacio de trabajo y un ID de recurso únicos. El nombre del espacio de trabajo debe ser único para un grupo de recursos determinado. Después de crear un espacio de trabajo, configure los orígenes de datos y las soluciones para almacenar sus datos en el espacio de trabajo.
- Extensión de supervisión en la lista de permitidos: Las extensiones `AzureMonitorWindowsAgent` y `AzureMonitorLinuxAgent` son extensiones de la lista de permitidos definida por Citrix. Para ver la lista de extensiones incluidas en la lista de permitidos, utilice el comando `Get-ProvMetadataConfiguration` de PowerShell.
- Imagen maestra: Microsoft recomienda quitar extensiones de una máquina existente antes de crear otra máquina a partir de ella. Si no se quitan las extensiones, es posible que queden archivos sobrantes y que se produzca un comportamiento inesperado. Para obtener más información, consulte Si la máquina virtual se vuelve a crear a partir de una máquina virtual existente.

Para obtener información sobre cómo crear un catálogo con AMA habilitado mediante PowerShell, consulte Aprovisionar VM de catálogo con AMA habilitado.

### Máquinas virtuales confidenciales de Azure

Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa.

Puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina.

#### Consideraciones importantes acerca de las máquinas virtuales confidenciales

Las consideraciones importantes relativas a los tamaños de máquina virtual compatibles y la creación de catálogos de máquinas con VM confidenciales son las siguientes:

- Tamaños de VM compatibles: Las máquinas virtuales confidenciales admiten los siguientes tamaños:
  - Serie DCasv5
  - Serie DCadsv5
  - Serie ECasv5
  - Serie ECadsv5
- Crear catálogos de máquinas con VM confidenciales.
  - Puede crear un catálogo de máquinas con VM confidenciales de Azure mediante la interfaz de Configuración completa y los comandos de PowerShell.
  - Para crear un catálogo de máquinas con VM confidenciales de Azure, debe usar un flujo de trabajo basado en perfiles de máquina. Puede usar una máquina virtual o una especificación de plantilla como entrada del perfil de máquina.
  - La imagen maestra y la entrada del perfil de máquina deben estar habilitadas con el mismo tipo de seguridad confidencial. Los tipos de seguridad son:
    * VMGuestStateOnly: VM confidencial con solo el estado de invitado de VM cifrado
    * DiskWithVMGuestState: VM confidencial con disco de SO y estado de invitado de máquina virtual cifrados con una clave administrada por la plataforma o una clave administrada por el cliente. Se pueden cifrar tanto los discos de SO normales como los efímeros.
  - Con el parámetro AdditionalData, puede obtener información de VM confidencial de varios tipos de recursos, como discos administrados, instantáneas, imágenes de Azure Compute Gallery, máquinas virtuales y especificaciones de plantilla de Azure Resource Manager. Por ejemplo:

    ```
    PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork
       \image.folder\username-dev-testing-rg.resourcegroup\
       username-dev-tsvda.vm).AdditionalData
    <!--NeedCopy-->
    ```

    Los campos de datos adicionales son:
    * DiskSecurityType
    * ConfidentialVMDiskEncryptionSetId
    * DiskSecurityProfiles

    Para obtener la propiedad de computación confidencial de un tamaño de una máquina, ejecute el siguiente comando: `(Get-Item -path "XDHyp:\Connections\my-connection-name\East US.region\serviceoffering.folder\abc.serviceoffering").AdditionalData`

    El campo de datos adicional es `ConfidentialComputingType`.

- No puede cambiar la imagen maestra ni el perfil de máquina de un tipo de seguridad confidencial a un tipo de seguridad no confidencial ni de un tipo de seguridad no confidencial a uno confidencial.
- Aparecerán los mensajes de error correspondientes a cualquier configuración incorrecta.

#### Preparar imágenes maestras y perfiles de máquina

Antes de crear un conjunto de máquinas virtuales confidenciales, siga estos pasos para preparar una imagen maestra y un perfil de máquina para ellas:

1. En el portal de Azure, cree una máquina virtual confidencial con parámetros específicos, como:
   - **Tipo de seguridad**: Máquinas virtuales confidenciales
   - **Cifrado de disco de SO confidencial**: Habilitado.
   - **Administración de claves**: Cifrado de disco confidencial con una clave administrada por la plataforma
     Para obtener más información sobre la creación de máquinas virtuales confidenciales, consulte este artículo de Microsoft.
2. Prepare la imagen maestra en la máquina virtual creada. Instale las aplicaciones y VDA necesarios en la máquina virtual creada.

   > **Nota:**
   >
   > No se admite la creación de máquinas virtuales confidenciales mediante VHD. En su lugar, use Azure Compute Gallery, discos administrados o instantáneas para este fin.

3. Cree el perfil de la máquina de una de estas maneras:
   - Use la máquina virtual existente creada en el paso 1 si tiene las propiedades de máquina necesarias.
   - Si opta por una especificación de plantilla de ARM como perfil de máquina, cree la especificación de plantilla según sea necesario. En concreto, configure parámetros que cumplan con los requisitos de VM confidencial, como *SecurityEncryptionType* y *diskEncryptionSet* (para la clave administrada por el cliente). Para obtener más información, consulte Crear una especificación de plantilla de Azure.

     > **Nota:**
     >
     > - Asegúrese de que la imagen maestra y el perfil de la máquina tengan el mismo tipo de clave de seguridad.
     > - Para crear máquinas virtuales confidenciales que requieran cifrado de disco de SO confidencial con una clave administrada por el cliente, asegúrese de que los

> ID del conjunto de cifrado de disco tanto en la imagen maestra como en el perfil de la máquina sean idénticos.

### Crear máquinas virtuales confidenciales mediante Configuración completa o comandos de PowerShell

Para crear un conjunto de máquinas virtuales confidenciales, cree un catálogo de máquinas con una imagen maestra y un perfil de máquina derivados de la máquina virtual confidencial deseada.

Para crear el catálogo mediante la Configuración completa, siga los pasos descritos en Crear catálogos de máquinas. Tenga en cuenta las siguientes consideraciones:

- En la página **Imagen**, seleccione una imagen maestra y un perfil de máquina que haya preparado para la creación de la máquina virtual confidencial. La selección del perfil de la máquina es obligatoria y solo están disponibles para selección los perfiles cuyo tipo de cifrado de seguridad coincida con el de la imagen maestra seleccionada.
- En la página **Máquinas virtuales**, solo aparecen para selección los tamaños de máquina compatibles con máquinas virtuales confidenciales.
- En la página **Parámetros del disco**, no puede especificar el conjunto de cifrado del disco porque se hereda del perfil de máquina seleccionado.

### Usar PowerShell

En esta sección se detalla cómo realizar las siguientes tareas con PowerShell:

- Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell
- Habilitar las extensiones de VM de Azure
- Catálogos de máquinas con inicio seguro
- Usar valores de propiedades de perfil de máquina
- Configurar zonas de disponibilidad con PowerShell
- Aprovisionar VM en hosts dedicados de Azure
- Configurar los tipos de almacenamiento
- Habilitar el almacenamiento con redundancia de zonas
- Capture la configuración de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina
- Verificar la licencia de Windows
- Configurar la licencia de Linux
- Crear un catálogo de máquinas con un disco efímero de Azure
- Configurar Azure Compute Gallery
- Crear o actualizar un catálogo con varias NIC por máquina virtual
- Crear un catálogo de máquinas con un disco no persistente de caché con reescritura
- Crear un catálogo de máquinas con un disco persistente de caché con reescritura

- Mejorar el rendimiento del arranque con E/S de MCS
- Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente
- Crear un catálogo de máquinas con capacidad de cifrado en el host
- Crear un catálogo de máquinas con doble cifrado
- Determinación de la ubicación del archivo de paginación
- Casos de configuración de archivos de paginación
- Especificar los parámetros del archivo de páginación
- Modificar los parámetros del archivo de páginación
- Aprovisionar VM de catálogo con AMA habilitado
- Crear un catálogo con máquinas virtuales de Azure Spot
- Copiar etiquetas en todos los recursos

### Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar la interfaz de Configuración completa o los comandos de PowerShell.

Para la interfaz de Configuración completa, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.

Mediante los comandos de PowerShell:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Cree o actualice un catálogo.

    - Para crear un catálogo:

        a) Utilice el comando `New-ProvScheme` con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

```
New-ProvScheme -MasterImageVM "XDHyp:/HostingUnits/azure/
    image.folder/fgthj.resourcegroup/nab-ws-
    vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
    folder/fgthj.resourcegroup/test.templatespec/V1.
    templatespecversion"
-ProvisioningSchemeName <String>
-HostingUnitName <String>
-IdentityPoolName <String>
[-ServiceOffering <String>][-CustomProperties <String>]
[<CommonParameters>]
<!--NeedCopy-->
```

        b) Termine de crear el catálogo.

- Para actualizar un catálogo, utilice el comando `Set-ProvScheme` con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

```
Set-ProvScheme -MasterImageVm 'XDHyp://Connections/Azure/East
    Us.region/vm.folder/MasterDisk.vm'
MachineProfile 'XDHyp:/HostingUnits/azure/machineprofile.
   folder/fgthj.resourcegroup/testing.templatespec/V1.
   templatespecversion'
[-ProvisioningSchemeName] <String>
[-CustomProperties <String>][-ServiceOffering <String>] [-
   PassThru]
[<CommonParameters>]
<!--NeedCopy-->
```

### Habilitar las extensiones de VM de Azure

Después de seleccionar la especificación de la plantilla ARM, ejecute estos comandos de PowerShell para operar con extensiones de Azure VM:

- Para ver la lista de extensiones de VM de Azure compatibles: `Get-ProvMetadataConfiguration`
- Para agregar más extensiones de VM: `Add-ProvMetadataConfiguration`. Por ejemplo, `Add-ProvMetadataConfiguration -PluginType "AzureRM"-ConfigurationName "Extension"-ConfigurationValue "CustomScriptExtension"`

  Si intenta agregar uno de estos elementos, el comando no se ejecuta y aparece un mensaje de error:

  - Extensión definida por Citrix.
  - Extensión existente definida por el usuario.
  - Claves de configuración no admitidas. Por ahora, la clave de configuración admitida es `Extension`.
- Para quitar extensiones de la lista: `Remove-ProvMetadataConfiguration`. Puede quitar las extensiones que agregó.

### Catálogos de máquinas con inicio seguro

Para crear correctamente un catálogo de máquinas con inicio seguro, utilice:

- Un perfil de máquina con inicio seguro
- Un tamaño de máquina virtual compatible con el inicio seguro
- Una versión de máquina virtual Windows que admita inicio seguro. En la actualidad, Windows 10, Windows 11 y Windows Server 2016, 2019 y 2022 admiten el inicio seguro.

> **Importante:**
>
> MCS admite la creación de un catálogo con máquinas virtuales habilitadas para inicio seguro. Sin embargo, para actualizar un catálogo persistente y las máquinas virtuales ya existentes, debe usar el portal de Azure. No puede actualizar el inicio seguro de un catálogo no persistente. Para obtener más información, consulte el documento de Microsoft Enable Trusted launch on existing Azure VMs.

Para ver los elementos de inventario que ofrecen Citrix DaaS y determinar si el tamaño de máquina virtual admite el inicio seguro, ejecute el siguiente comando:

1. Abra una ventana de PowerShell.
2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute este comando:

```
$s = (ls XDHyp:\HostingUnits<name of hosting unit>\serviceoffering
    .folder"<VM size>".serviceoffering)
<!--NeedCopy-->
```

4. Ejecute `$s | select -ExpandProperty Additionaldata`
5. Compruebe el valor del atributo `SupportsTrustedLaunch`.
   - Si `SupportsTrustedLaunch` es **True**, el tamaño de máquina virtual admite el inicio seguro.
   - Si `SupportsTrustedLaunch` es **False**, el tamaño de máquina virtual no admite el inicio seguro.

Según la instancia de PowerShell de Azure, puede usar este comando para determinar los tamaños de máquina virtual que admiten el inicio seguro:

```
(Get-AzComputeResourceSku | where {
 $_.Locations.Contains($region) -and ($_.Name -eq "<VM size>")  }
 )[0].Capabilities
<!--NeedCopy-->
```

A continuación, se muestran ejemplos que describen si el tamaño de máquina virtual admite el inicio seguro después de ejecutar el comando de Azure PowerShell.

- *Ejemplo 1*: Si la máquina virtual de Azure solo admite la generación 1, esa máquina virtual no admite el inicio seguro. Por lo tanto, la funcionalidad `TrustedLaunchDisabled` no se muestra después de ejecutar el comando de Azure PowerShell.
- *Ejemplo 2*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad `TrustedLaunchDisabled` es **True**, el tamaño de máquina virtual de la generación 2 no se admite para el inicio seguro.

- *Ejemplo 3*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad `TrustedLaunchDisabled` no se muestra después de ejecutar el comando de PowerShell, se admite el tamaño de máquina virtual de generación 2 para el inicio seguro.

Para obtener más información sobre el inicio seguro para máquinas virtuales de Azure, consulte el documento Trusted Launch for Azure Virtual Machines de Microsoft.

#### Crear un catálogo de máquinas con inicio seguro

1. Cree una imagen maestra habilitada para inicio seguro. Consulte la documentación Trusted Launch VM Images de Microsoft.
2. Cree una especificación de plantilla o máquina virtual con el tipo de seguridad **máquinas virtuales con inicio seguro**. Para obtener más información sobre cómo crear una especificación de plantilla o VM, consulte el documento Deploy a Trusted Launch VM de Microsoft.
3. Cree un catálogo de máquinas mediante la interfaz de Configuración completa o los comandos de PowerShell.

   - Si quiere usar la interfaz de Configuración completa, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.
   - Si quiere usar los comandos de PowerShell, utilice el comando `New-ProvScheme` con la especificación de plantilla o VM como entrada de perfil de máquina. Para ver la lista completa de comandos para crear un catálogo, consulte Creación de un catálogo.

     Ejemplo de `New-ProvScheme` con VM como entrada del perfil de máquina:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
     -MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.
        folder<def.resourcegroup><machine profile vm.vm>"
     -ProvisioningSchemeName <String>
     -HostingUnitName <String>
     -IdentityPoolName <String>
     [-ServiceOffering <String>][-CustomProperties <String>]
     [<CommonParameters>]
     <!--NeedCopy-->
     ```

     Ejemplo de `New-ProvScheme` con especificación de plantilla como entrada del perfil de máquina:

     ```
     New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
        IdentityPoolName "name" -InitialBatchSizeHint 1
     ```

```
2   -MasterImageVM "XDHyp:/HostingUnits/azure/image.folder/fgthj.
        resourcegroup/nab-ws-vda_OsDisk_1_xxxxxxxxxxa.manageddisk"
3   MachineProfile "XDHyp:/HostingUnits/azure/machineprofile.
        folder/fgthj.resourcegroup/test.templatespec/V1.
        templatespecversion"
4   -ProvisioningSchemeName <String>
5   -HostingUnitName <String>
6   -IdentityPoolName <String>
7   [-ServiceOffering <String>][-CustomProperties <String>]
8   [<CommonParameters>]
9   <!--NeedCopy-->
```

#### Errores al crear catálogos de máquinas con inicio seguro

Al crear un catálogo de máquinas con inicio seguro en los siguientes casos, se obtienen los errores correspondientes:

| Caso | Error |
| --- | --- |
| Si selecciona un perfil de máquina al crear un catálogo no administrado | `MachineProfileNotSupportedForUnmanagedCata` |
| Si selecciona un perfil de máquina que admite el inicio seguro al crear un catálogo con un disco no administrado como imagen maestra | `SecurityTypeNotSupportedForUnmanagedDisk` |
| Si no selecciona un perfil de máquina al crear un catálogo administrado con una imagen maestra de origen que tenga inicio seguro como tipo de seguridad | `MachineProfileNotFoundForTrustedLaunchMaste` |
| Si selecciona un perfil de máquina con un tipo de seguridad diferente del tipo de seguridad de la imagen maestra | `SecurityTypeConflictBetweenMasterImageAndMa` |
| Si selecciona un tamaño de máquina virtual que no admite el inicio seguro, pero usa una imagen maestra que sí admite el inicio seguro al crear un catálogo | `MachineSizeNotSupportTrustedLaunch` |

### Usar valores de propiedades de perfil de máquina

El catálogo de máquinas utiliza las siguientes propiedades que se definen en las propiedades personalizadas:

- Zona de disponibilidad

- ID de grupo de hosts dedicado
- ID del conjunto de cifrado de disco
- Tipo de SO
- Tipo de licencia
- Tipo de almacenamiento

Si estas propiedades personalizadas no se definen explícitamente, los valores de propiedad se establecen a partir de la especificación de plantilla de ARM o de la VM, lo que se utilice como perfil de máquina. Además, si no se especifica `ServiceOffering`, se establecerá a partir del perfil de máquina.

> **Nota:**
>
> Si faltan algunas propiedades en el perfil de la máquina (MachineProfile) y no están definidas en las propiedades personalizadas (CustomProperties), se utilizan los valores por defecto de las propiedades siempre que sea aplicable.

En la siguiente sección se describen algunos casos de `New-ProvScheme` y `Set-ProvScheme` en los que `CustomProperties` tiene definidas todas las propiedades o los valores se derivan de MachineProfile.

- Casos de New-ProvScheme
  - MachineProfile tiene todas las propiedades y CustomProperties no está definido. Ejemplo:

    ```
    New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
    \machineprofile.folder\azure.resourcegroup\mpA.vm"
    ```

    Estos valores se definen como propiedades personalizadas del catálogo:

    ```
    1  Get-ProvScheme | select CustomProperties
    2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
           machinecreation" xmlns:xsi="http://www.w3.org/2001/
           XMLSchema-instance">
    3  <Property xsi:type="StringProperty" Name="StorageAccountType"
           Value="<mpA-value>"/>
    4  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
           -value>"/>
    5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
           "<mpA-value>"/>
    6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
           " Value="<mpA-value>"/>
    7  <Property xsi:type="StringProperty" Name="
           DedicatedHostGroupId" Value="<mpA-value>"/>
    8  <Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
           value>"/>
    9  </CustomProperties>
    10 <!--NeedCopy-->
    ```

- MachineProfile tiene algunas propiedades y CustomProperties no está definido. Ejemplo: MachineProfile solo tiene LicenseType y OsType.

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"
  ```

  Estos valores se definen como propiedades personalizadas del catálogo:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="OSType" Value="<mpA
        -value>"/>
  4  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<mpA-value>"/>
  5  </CustomProperties>
  6  <!--NeedCopy-->
  ```

- Tanto MachineProfile como CustomProperties definen todas las propiedades. Ejemplo:

  ```
  New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
  \machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
   $CustomPropertiesA
  ```

  Las propiedades personalizadas tienen prioridad. Estos valores se definen como propiedades personalizadas del catálogo:

  ```
  1  Get-ProvScheme | select CustomProperties
  2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
        machinecreation" xmlns:xsi="http://www.w3.org/2001/
        XMLSchema-instance">
  3  <Property xsi:type="StringProperty" Name="StorageAccountType"
         Value="<CustomPropertiesA-value>"/>
  4  <Property xsi:type="StringProperty" Name="OSType" Value="<
        CustomPropertiesA-value>"/>
  5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
        "<CustomPropertiesA-value>"/>
  6  <Property xsi:type="StringProperty" Name="DiskEncryptionSetId
        " Value="<CustomPropertiesA-value>"/>
  7  <Property xsi:type="StringProperty" Name="
        DedicatedHostGroupId" Value="<CustomPropertiesA-value>"/>
  8  <Property xsi:type="StringProperty" Name="Zones" Value="<
        CustomPropertiesA-value>"/>
  9  </CustomProperties>
  10 <!--NeedCopy-->
  ```

- Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Ejemplo:

  * CustomProperties define LicenseType y StorageAccountType
  * MachineProfile define LicenseType, OsType y Zones

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-CustomProperties
 $CustomPropertiesA
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="OSType" Value="<mpA
   -value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "<CustomPropertiesA-value>"/>
<Property xsi:type="StringProperty" Name="Zones" Value="<mpA-
   value>"/>
</CustomProperties>
<!--NeedCopy-->
```

- Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Además, ServiceOffering no está definido. Ejemplo:
  - CustomProperties define StorageType
  - MachineProfile define LicenseType

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
   \machineprofile.folder\azure.resourcegroup\mp.vm"
-ServiceOffering "XDHyp:\HostingUnits\azureunit\
   serviceoffering.folder<explicit-machine-size>.
   serviceoffering"
<!--NeedCopy-->
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
Get-ProvScheme | select ServiceOffering
serviceoffering.folder<explicit-machine-size>.serviceoffering

Get-ProvScheme | select CustomProperties
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageAccountType"
    Value="explicit-storage-type"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
   "value-from-machineprofile"/>
</CustomProperties>
<!--NeedCopy-->
```

- Si OsType no está ni en CustomProperties ni en MachineProfile, entonces:
  - El valor se lee de la imagen maestra.

* Si la imagen maestra es un disco no administrado, OsType se establece en Windows. Ejemplo:

```
New-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpA.vm"-MasterImageVM
 "XDHyp:\HostingUnits\azureunit\image.folder\linux-master-
image.manageddisk"
```

El valor de la imagen maestra se escribe en las propiedades personalizadas, en este caso Linux.

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="OSType" Value="
      Linux"/>
4  </CustomProperties>
5  <!--NeedCopy-->
```

- Casos de Set-ProvScheme
  - Un catálogo con:
    * CustomProperties para `StorageAccountType` y OsType
    * MachineProfile `mpA.vm` que define zonas
  - Actualizaciones:
    * MachineProfile mpB.vm que define StorageAccountType
    * Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define LicenseType y OsType

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"-CustomProperties
 $CustomPropertiesB
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
      machinecreation" xmlns:xsi="http://www.w3.org/2001/
      XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
       Value="<mpB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
      CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
      "<CustomPropertiesB-value>"/>
6      </CustomProperties>
7  <!--NeedCopy-->
```

- Un catálogo con:
  - CustomProperties para `StorageAccountType` y OsType
  - MachineProfile `mpA.vm` que define StorageAccountType y LicenseType
- Actualizaciones:
  - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define StorageAccountType y OsType.

```
Set-ProvScheme -CustomProperties $CustomPropertiesB
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
1  Get-ProvScheme | select CustomProperties
2  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
3  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<CustomPropertiesB-value>"/>
4  <Property xsi:type="StringProperty" Name="OSType" Value="<
       CustomPropertiesB-value>"/>
5  <Property xsi:type="StringProperty" Name="LicenseType" Value=
       "<mp-A-value>"/>
6  </CustomProperties>
7  <!--NeedCopy-->
```

- Un catálogo con:
  - CustomProperties para `StorageAccountType` y OsType
  - MachineProfile `mpA.vm` que define Zones
- Actualizaciones:
  - MachineProfile mpB.vm que define StorageAccountType y LicenseType
  - `ServiceOffering` está sin especificar

```
Set-ProvScheme -MachineProfile "XDHyp:\HostingUnits\azureunit
\machineprofile.folder\azure.resourcegroup\mpB.vm"
```

Estos valores se definen como propiedades personalizadas del catálogo:

```
1  Get-ProvScheme | select ServiceOffering
2  serviceoffering.folder<value-from-machineprofile>.
       serviceoffering
3
4  Get-ProvScheme | select CustomProperties
5  <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
       machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
6  <Property xsi:type="StringProperty" Name="StorageAccountType"
        Value="<mpB-value>"/>
```

```
<Property xsi:type="StringProperty" Name="OSType" Value="<
    prior-CustomProperties-value>"/>
<Property xsi:type="StringProperty" Name="LicenseType" Value=
    "<mpB-value>"/>
</CustomProperties>
<!--NeedCopy-->
```

### Configurar zonas de disponibilidad con PowerShell

Con PowerShell, puede ver Citrix DaaS que ofrece elementos de inventario mediante `Get-Item`. Por ejemplo, para ver la oferta de servicio de la *región oriental de EE. UU.* `Standard_B1ls`:

```
$serviceOffering = Get-Item -path "XDHyp:\Connections\my-connection-
    name\East US.region\serviceoffering.folder\Standard_B1ls.
    serviceoffering"
<!--NeedCopy-->
```

Para ver las zonas, utilice el parámetro `AdditionalData` para el elemento:

`$serviceOffering.AdditionalData`

Si no se especifican zonas de disponibilidad, no hay ningún cambio en la forma en que se aprovisionan las máquinas.

Para configurar las zonas de disponibilidad a través de PowerShell, utilice la propiedad personalizada **Zonas** disponible con la operación `New-ProvScheme`. La propiedad **Zonas** define una lista de zonas de disponibilidad en las que aprovisionar máquinas. Esas zonas pueden incluir una o más zonas de disponibilidad. Por ejemplo, `<Property xsi:type="StringProperty"Name="Zones" Value="1, 3"/>` para las zonas 1 y 3.

Utilice el comando `Set-ProvScheme` para actualizar las zonas de un esquema de aprovisionamiento.

Si se proporciona una zona no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error con instrucciones sobre cómo corregir el comando no válido.

> **Sugerencia:**
>
> Si especifica una propiedad personalizada no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error al respecto.

#### Resultado de usar grupos de hosts y zonas de disponibilidad de Azure al mismo tiempo

Hay una comprobación previa para evaluar si la creación de un catálogo de máquinas se hará correctamente en función de la zona de disponibilidad especificada en la propiedad personalizada y la

zona del grupo de hosts. La creación del catálogo falla si la zona de disponibilidad especificada en la propiedad personalizada no coincide con la zona del grupo de hosts.

Para obtener información sobre cómo configurar zonas de disponibilidad a través de PowerShell, consulte Configurar zonas de disponibilidad a través de PowerShell.

Para obtener información sobre los hosts dedicados de Azure, consulte Hosts dedicados de Azure.

En la siguiente tabla se describen las distintas combinaciones de zona de disponibilidad y zona de grupo de hosts, y con cuáles se crea correctamente o falla la creación de un catálogo de máquinas.

| Zona de grupo de hosts | Zona de disponibilidad en la propiedad personalizada | Resultado de la creación del catálogo de máquinas |
|---|---|---|
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | No especificada | Correcto. Las máquinas se crean en la zona del grupo de hosts |
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | La misma zona que la del grupo de hosts. Por ejemplo, la zona de la propiedad personalizada se establece en 1 | Correcto. Las máquinas se crean en la Zona 1 |
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | Distinta de la zona del grupo de hosts. Por ejemplo, la zona de la propiedad personalizada se establece en 2 | Como la zona de disponibilidad especificada y la zona del grupo de hosts no coinciden, la creación del catálogo falla con un error relevante durante las comprobaciones previas |
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | Se especificaron varias zonas. Por ejemplo, las zonas de las propiedades personalizadas se establecen en 1,2 o 2,3 | Como la zona de disponibilidad especificada y la zona del grupo de hosts no coinciden, la creación del catálogo falla con un error relevante durante las comprobaciones previas |
| No especificada. Por ejemplo, la zona del grupo de hosts es None | No especificada | Como la zona de disponibilidad especificada y la zona del grupo de hosts coinciden (es decir, no hay zona), la creación del catálogo se realiza correctamente. No se crean máquinas en ninguna zona |

| Zona de grupo de hosts | Zona de disponibilidad en la propiedad personalizada | Resultado de la creación del catálogo de máquinas |
|---|---|---|
| No especificada. Por ejemplo, la zona del grupo de hosts es None | Especificada. Por ejemplo, las zonas de la propiedad personalizada se establecen en una o varias zonas | Como la zona de disponibilidad especificada y la zona del grupo de hosts no coinciden, la creación del catálogo falla con un error relevante durante las comprobaciones previas |

### Aprovisionar VM en hosts dedicados de Azure

Puede usar MCS para aprovisionar VM en los hosts dedicados de Azure. Antes de aprovisionar VM en hosts dedicados de Azure:

- Cree un grupo de hosts.
- Cree hosts en ese grupo de hosts.
- Compruebe que haya suficiente capacidad de host reservada para crear catálogos y máquinas virtuales.

Puede crear un catálogo de máquinas con arrendamiento de hosts definido a través del siguiente script de PowerShell:

```
1 New-ProvScheme <otherParameters> -CustomProperties '<CustomProperties
     xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi
     ="http://www.w3.org/2001/XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="HostGroupId" Value="
      myResourceGroup/myHostGroup" />
3  ...other Custom Properties...
4  </CustomProperties>
5 <!--NeedCopy-->
```

Cuando utilice MCS para aprovisionar máquinas virtuales en hosts dedicados de Azure, tenga en cuenta que:

- Un *host dedicado* es una propiedad del catálogo y no se puede cambiar una vez creado dicho catálogo. Actualmente, el arrendamiento dedicado no está disponible en Azure.
- Se requiere un grupo de hosts de Azure preconfigurado, en la región de la unidad de alojamiento, al utilizar el parámetro `HostGroupId`.
- Se requiere la ubicación automática de Azure. Esta funcionalidad realiza una solicitud para incorporar la suscripción asociada al grupo de hosts. Para obtener más información, consulte VM Scale Set on Azure Dedicated Hosts - Public Preview. Si la ubicación automática no está habilitada, MCS genera un error durante la creación del catálogo.

### Configurar los tipos de almacenamiento

Seleccione distintos tipos de almacenamiento para máquinas virtuales en entornos Azure que utilizan MCS. Para las máquinas virtuales de destino, MCS admite:

- Disco de SO: SSD Premium, SSD o HDD
- Disco de memoria caché con escritura: SSD Premium, SSD o HDD

Al utilizar estos tipos de almacenamiento, tenga en cuenta lo siguiente:

- Asegúrese de que su máquina virtual sea compatible con el tipo de almacenamiento seleccionado.
- Si su configuración usa un disco efímero de Azure, no tiene la posibilidad de configurar el disco de caché de reescritura.

> **Sugerencia:**
>
> `StorageType` está configurado para un tipo de SO y una cuenta de almacenamiento. `WBCDiskStorageType` está configurado para el tipo de almacenamiento de memoria caché de escritura. Para un catálogo normal, se requiere `StorageType`. Si `WBCDiskStorageType` no está configurado, `StorageType` se utiliza como predeterminado para `WBCDiskStorageType` .

Si WBCDiskStorageType no está configurado, StorageType se utiliza como predeterminado para WBCDiskStorageType.

#### Configurar los tipos de almacenamiento de las máquinas virtuales

Para configurar los tipos de almacenamiento para VM, use el parámetro `StorageType` en `New-ProvScheme`. Para actualizar el valor del parámetro `StorageType` en un catálogo existente a uno de los tipos de almacenamiento compatibles, use el comando `Set-ProvScheme`.

A continuación, se muestra un conjunto de ejemplo del parámetro `CustomProperties` en un esquema de aprovisionamiento:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance">
2 <Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
      />
3 <Property xsi:type="StringProperty" Name="StorageType" Value="
     Premium_LRS" />
4 <Property xsi:type="StringProperty" Name="LicenseType" Value="
     Windows_Client" />
5 </CustomProperties>'
6 <!--NeedCopy-->
```

### Habilitar el almacenamiento con redundancia de zonas

Puede seleccionar almacenamiento con redundancia de zonas durante la creación de catálogos. Replica sincrónicamente su disco administrado de Azure en varias zonas de disponibilidad, lo que le permite recuperarse de un error en una zona al usar la redundancia en otras.

Puede especificar **Premium_ZRS** y **StandardSSD_ZRS** en las propiedades personalizadas del tipo de almacenamiento. El almacenamiento ZRS se puede configurar mediante propiedades personalizadas existentes o mediante la plantilla **MachineProfile**. El almacenamiento ZRS también está disponible con el comando `Set-ProvVMUpdateTimeWindow` mediante los parámetros `-StartsNow` y `-DurationInMinutes -1`. Puede cambiar el almacenamiento de VM existente de LRS a ZRS.

> **Nota:**
>
> - `StartsNow` indica que la hora de inicio programada es la hora actual.
> - `DurationInMinutes` con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

**Limitaciones:**

- Compatible solo para discos administrados
- Compatible únicamente con unidades de estado sólido (SSD) estándar y premium
- No es compatible con `StorageTypeAtShutdown`
- Disponible solo en determinadas regiones.
- El rendimiento de Azure disminuye al crear discos ZRS a escala. Por lo tanto, al encenderlas por primera vez, encienda las máquinas en lotes más pequeños (menos de 300 máquinas a la vez)

#### Definir el almacenamiento con redundancia de zonas como tipo de almacenamiento en disco

Puede seleccionar un almacenamiento con redundancia de zonas durante la creación de catálogos inicial o puede actualizar el tipo de almacenamiento en un catálogo existente.

#### Seleccionar el almacenamiento con redundancia de zonas mediante los comandos de PowerShell

Al crear un catálogo en Azure mediante el comando `New-ProvScheme` de PowerShell, use `Standard_ZRS` como valor en `StorageAccountType`.
Por ejemplo:

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    StandardSSD_ZRS" />
<!--NeedCopy-->
```

Al definir este valor, se valida mediante una API dinámica que determina si se puede utilizar correctamente. Se pueden producir estas excepciones si el uso de ZRS no es válido para su catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: La propiedad personalizada StorageTypeAtShutdown no se puede utilizar con el almacenamiento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Esta excepción se produce si intenta utilizar el almacenamiento ZRS en una región de Azure que no admite ZRS.
- **ZrsRequiresManagedDisks**: Solo puede utilizar el almacenamiento con redundancia de zonas con discos administrados.

Puede configurar el tipo de almacenamiento en disco mediante estas propiedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`

> **Nota:**
>
> Durante la creación de catálogos, se utiliza el `StorageType` del disco del sistema operativo del perfil de máquina si las propiedades personalizadas no están configuradas.

## Capture la configuración de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina

Puede capturar la configuración de diagnóstico de las máquinas virtuales y las NIC desde un perfil de máquina mientras crea un catálogo de máquinas, actualiza un catálogo de máquinas existente y actualiza las máquinas virtuales existentes.

Puede crear una máquina virtual o una especificación de plantilla como fuente del perfil de máquina.

### Pasos clave

1. Configure los ID necesarios en Azure. Debe proporcionar estos ID en la especificación de la plantilla.
    - Cuenta de almacenamiento
    - Espacio de trabajo de analíticas de registros
    - Espacio de nombres del centro de eventos con el precio del nivel estándar
2. Cree un origen de perfil de máquina.
3. Cree un nuevo catálogo de máquinas, actualice un catálogo existente o actualice las máquinas virtuales existentes.

### Configurar los ID necesarios en Azure

Configure una de las siguientes opciones en Azure:

- Cuenta de almacenamiento
- Espacio de trabajo de analíticas de registros
- Espacio de nombres del centro de eventos con el precio del nivel estándar

**Configurar una cuenta de almacenamiento** Cree una cuenta de almacenamiento estándar en Azure. En la especificación de la plantilla, indique el resourceId completo de la cuenta de almacenamiento como el `storageAccountId`.

Una vez que las máquinas virtuales estén configuradas para registrar los datos en la cuenta de almacenamiento, los datos se pueden encontrar en el contenedor `insights-metrics-pt1m`.

**Configurar un espacio de trabajo de análisis de registros** Cree un espacio de trabajo de análisis de registros. En la especificación de la plantilla, indique el resourceId completo para el espacio de trabajo de análisis de registros como workspaceId.

Una vez que las máquinas virtuales estén configuradas para registrar datos en el espacio de trabajo, los datos se pueden consultar en Registros en Azure. Puede ejecutar el siguiente comando en Azure en Registros para mostrar un recuento de todas las métricas registradas por un recurso:

‘AzureMetrics
| summarize Count=count() by ResourceId# Crear un catálogo de Microsoft Azure

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

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de crear un catálogo de Microsoft Azure, debe terminar de crear una conexión con Microsoft Azure. Consulte Conexión con Microsoft Azure.

### Creación de un catálogo de máquinas

Puede crear un catálogo de máquinas de dos maneras:

- Interfaz de Configuración completa.
- PowerShell. Consulte Administrar Citrix DaaS mediante Remote PowerShell SDK. Para obtener información sobre cómo implementar funciones específicas con PowerShell, consulte Usar PowerShell.

### Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa

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

Una imagen puede ser un disco, una instantánea o la versión de una imagen de una definición de imagen en Azure Compute Gallery que se usa para crear las máquinas virtuales en un catálogo de máquinas.

Antes de crear el catálogo de máquinas, cree una imagen en Azure Resource Manager.

> **Nota:**
>
> - Se ha retirado el uso de discos no administrados para aprovisionar máquinas virtuales.
> - Se retiró la compatibilidad con el uso de una imagen maestra de una región diferente a la configurada en la conexión del host. Use Azure Compute Gallery para replicar la imagen maestra en la región deseada.

Durante la preparación de la imagen, se crea una máquina virtual (VM) de preparación basada en la máquina virtual original. Esta máquina virtual de preparación está desconectada de la red. Para desconectar la red de la máquina virtual de preparación, se crea un grupo de seguridad de red para denegar todo el tráfico entrante y saliente. El grupo de seguridad de red se crea automáticamente una vez por catálogo. El nombre del grupo de seguridad de red es <!JEKYLL@5180@0>, donde el GUID se genera aleatoriamente. Por ejemplo, <!JEKYLL@5180@1>.

En el asistente para la creación de catálogos de máquinas:

1. Las páginas **Tipo de máquina** y **Administración de máquinas** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
2. En la página **Imagen**, seleccione la imagen que quiera utilizar como imagen maestra para todas las máquinas del catálogo. Aparecerá el asistente para **seleccionar una imagen**. Siga estos pasos para seleccionar una imagen:

    a) (Aplicable solo a las conexiones configuradas con imágenes compartidas en o entre arrendatarios). Seleccione una suscripción en la que resida la imagen.
    b) Seleccione un grupo de recursos.
    c) Vaya a la versión de imagen de Azure, disco administrado de Azure o Azure Compute Gallery.

Al seleccionar una imagen, tenga en cuenta lo siguiente:

- Compruebe que hay un VDA de Citrix instalado en la imagen.
- Si selecciona un disco conectado a una máquina virtual, debe apagar esta antes de continuar con el siguiente paso.

> **Nota:**
>
> - La suscripción correspondiente a la conexión (host) que creó las máquinas del catálogo se indica con un punto verde. Las demás suscripciones son aquellas en las que se comparte Azure Compute Gallery con esa suscripción. En esas suscripciones, solo se muestran las galerías compartidas. Para obtener información sobre cómo configurar las suscripciones compartidas, consulte Compartir imágenes con un arrendatario (entre suscripciones) y Compartir imágenes entre arrendatarios.
> - Puede crear un esquema de aprovisionamiento mediante un disco de SO efímero en Windows con inicio seguro. Al seleccionar una imagen con inicio seguro, debe seleccionar un perfil de máquina con inicio seguro que esté habilitado con vTPM. Para crear catálogos de máquinas con un disco de SO efímero, consulte Cómo crear máquinas con discos de SO efímeros.
> - Durante la replicación de imágenes, puede continuar y seleccionar la imagen como imagen maestra y completar la configuración. Sin embargo, es posible que la creación de catálogos tarde más tiempo en completarse mientras se replica la imagen. MCS necesita que la replicación se complete en una hora a partir de la creación de catálogos. Si la replicación tarda más, no se crean los catálogos. Puede verificar el estado de la replicación en Azure. Inténtelo de nuevo si la replicación sigue pendiente o después de que se haya completado.
> - Puede aprovisionar un catálogo de máquinas virtuales de 2.ª generación mediante una imagen de 2.ª generación para mejorar el rendimiento del tiempo de arranque. Sin embargo, no se admite la creación de catálogos de máquinas de 2.ª generación con una imagen de 1.ª generación. Del mismo modo, tampoco se admite la creación de catálogos de máquinas de 1.ª generación con una imagen de 2.ª generación. Además, cualquier imagen antigua que no tenga información de generación es una imagen de 1.ª generación.

Elija si quiere que las máquinas virtuales del catálogo hereden configuraciones de un perfil de máquina. De forma predeterminada, está marcada la casilla **Usar un perfil de máquina (obligatorio para Azure Active Directory)**. Haga clic en **Seleccione un perfil de máquina** para buscar una VM o una especificación de plantilla de ARM en una lista de grupos de recursos.

Algunos ejemplos de configuraciones que las máquinas virtuales pueden heredar de un perfil de máquina incluyen:

- Redes aceleradas

- Diagnóstico de arranque
- Almacenamiento en caché de discos de host (relacionado con discos de SO y de E/S de MCS)
- Tamaño de máquina (a menos que se especifique lo contrario)
- Etiquetas colocadas en la máquina virtual

> **Nota:**
>
> - Al seleccionar una imagen maestra para los catálogos de máquinas en Azure, el perfil de máquina se filtra en función de la imagen maestra que seleccione. Por ejemplo, el perfil de la máquina se filtra en función del sistema operativo Windows, el tipo de seguridad, la compatibilidad con la hibernación y el ID del conjunto de cifrado de discos de la imagen maestra.
> - Es obligatorio usar un perfil de máquina con Inicio seguro como **Tipo de seguridad** al seleccionar una imagen o una instantánea que tenga habilitado el inicio seguro. A continuación, para habilitar o inhabilitar SecureBoot y vTPM, especifique sus valores en el perfil de la máquina. Para obtener información sobre el inicio de confianza de Azure, consulte https://docs.microsoft.com/en-us/azure/virtual-machines/trusted-launch.

Valide la especificación de plantilla ARM para asegurarse de que se puede utilizar como perfil de máquina para crear un catálogo de máquinas. Para obtener información sobre cómo crear una especificación de plantilla de Azure, consulte Crear una especificación de plantilla de Azure.

Hay dos formas de validar la especificación de la plantilla ARM:

- Después de seleccionar la especificación de plantilla ARM en la lista de grupos de recursos, haga clic en **Siguiente**. Aparecen mensajes de error si la especificación de plantilla ARM contiene errores.
- Ejecute uno de estos comandos de PowerShell:
  - <!JEKYLL@5180@2>
  - <!JEKYLL@5180@3>

  Por ejemplo:

  <!JEKYLL@5180@4>

Tras crear el catálogo, podrá ver las configuraciones que la imagen hereda del perfil de máquina. En el nodo **Catálogos de máquinas**, seleccione el catálogo para ver sus detalles en el panel inferior. A continuación, haga clic en la ficha **Propiedades de plantilla** para ver las propiedades del perfil de máquina. La sección **Etiquetas** muestra hasta tres etiquetas. Para ver todas las etiquetas colocadas en la máquina virtual, haga clic en **Ver todo**.

Si quiere que MCS aprovisione máquinas virtuales en un host dedicado de Azure, active la casilla de verificación **Usar un grupo de hosts** y, a continuación, seleccione un grupo de hosts de la lista. Un grupo de hosts es un recurso que representa un conjunto de hosts dedicados. Un host dedicado es un servicio que proporciona servidores físicos que alojan una o más máquinas virtuales. Su servidor está dedicado a su suscripción de Azure, no se comparte con otros suscriptores. Cuando utiliza un host dedicado, Azure garantiza que sus máquinas virtuales sean las únicas máquinas activas en ese host. Esta función es adecuada para situaciones en las que debe cumplir con requisitos normativos o de seguridad interna. Para obtener más información sobre los grupos de hosts y las consideraciones para usarlos, consulte Aprovisionar VM en hosts dedicados de Azure.

> **Importante:**
>
> - Solo se muestran los grupos de hosts que tienen habilitada la ubicación automática de Azure.
> - El uso de un grupo de hosts cambia la página **Máquinas virtuales** que se ofrece más adelante en el asistente. En esa página, solo se muestran los tamaños de máquina que contiene el grupo de hosts seleccionado. Además, las zonas de disponibilidad se seleccionan automáticamente y no están disponibles para selección manual.

3. La página **Tipos de licencia y almacenamiento** solo aparece cuando se usa una imagen de Azure Resource Manager.

   Puede utilizar los siguientes tipos de almacenamiento para el catálogo de máquinas:

   - **SSD Premium**. Ofrece una opción de almacenamiento en disco de alto rendimiento y baja latencia, adecuada para máquinas virtuales con cargas de trabajo intensivas de E/S.
   - **SSD estándar**. Ofrece una opción de almacenamiento rentable, adecuada para cargas de trabajo que necesitan un rendimiento uniforme a niveles de IOPS más bajos.
   - **HDD estándar**. Ofrece una opción de almacenamiento en disco fiable y de bajo coste, adecuada para máquinas virtuales que ejecutan cargas de trabajo donde no importa la latencia.
   - **Disco de SO efímero de Azure**. Ofrece una opción de almacenamiento rentable que reutiliza el disco local de las VM para alojar el disco del sistema operativo. Como alternativa, puede usar PowerShell para crear máquinas que usen discos de SO efímeros. Para obtener más información, consulte Discos efímeros de Azure. Tenga en cuenta lo siguiente cuando utilice un disco de SO efímero:
     - El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.
     - Para actualizar máquinas que usan discos de SO efímeros, debe seleccionar una imagen cuyo tamaño no exceda el tamaño del disco de caché o el disco temporal de la VM.

- No puede usar la opción **Conservar VM y disco del sistema durante los ciclos de energía** que se ofrece más adelante en el asistente.

> **Nota:**
>
> El disco de identidad siempre se crea con un SSD estándar, independientemente del tipo de almacenamiento que elija.

El tipo de almacenamiento determina el tamaño de las máquinas que se ofrecen en la página **Máquinas virtuales** del asistente. MCS configura discos premium y estándar para uso de almacenamiento con redundancia local (LRS). LRS hace varias copias sincrónicas de los datos en un único centro de datos. Los discos de SO efímeros de Azure usan el disco local de las VM para almacenar el sistema operativo. Para obtener más información acerca de los tipos de almacenamiento y la replicación de almacenamiento de Azure, consulte lo siguiente:

- Introducción a Azure Storage
- Azure Premium Storage: diseño para un alto rendimiento
- Redundancia de Azure Storage

Seleccione si utilizar licencias de Windows o de Linux existentes:

- Licencias de Windows: El uso de licencias de Windows junto con imágenes de Windows (imágenes que admita la plataforma Azure o imágenes personalizadas) permite ejecutar máquinas virtuales de Windows en Azure a un coste reducido. Existen dos tipos de licencias:
  - **Licencia de Windows Server**. Le permite utilizar sus licencias de Windows Server o Azure Windows Server, con lo que puede usar las ventajas híbridas de Azure. Para obtener información detallada, consulte https://azure.microsoft.com/en-us/pricing/hybrid-benefit/. Las ventajas híbridas de Azure reducen los costes de ejecución de máquinas virtuales en Azure a la tarifa básica de procesamiento, lo que elimina el gasto en licencias de Windows Server adicionales desde la galería de Azure.
  - **Licencia de cliente de Windows**. Le permite llevar sus licencias de Windows 10 y Windows 11 a Azure, con lo que puede usar máquinas virtuales con Windows 10 y Windows 11 en Azure sin necesidad de licencias adicionales. Para obtener más información, consulte Licencias de acceso de cliente y licencias de administración.
- Licencias de Linux: Con las licencias de Linux de su propia suscripción (BYOS), no tiene que pagar por el software. El cargo de las licencias BYOS solo incluye la tarifa de hardware del procesamiento. Existen dos tipos de licencias:
  - **RHEL_BYOS**: Para usar correctamente el tipo RHEL_BYOS, habilite Red Hat Cloud Access en su suscripción de Azure.
  - **SLES_BYOS**: Las versiones de BYOS de SLES permiten el uso de SUSE.

Observe a continuación:

- Verificar la licencia de Windows
- Configurar la licencia de Linux

Consulte estos documentos para comprender los tipos de licencias y sus beneficios:

- https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.management.compute.models.virtualmachine.licensetype?view=azure-dotnet
- https://docs.microsoft.com/en-us/azure/virtual-machines/linux/azure-hybrid-benefit-linux

Azure Compute Gallery es un repositorio que sirve para administrar y compartir imágenes. Le permite poner sus imágenes a disposición de toda la organización. Le recomendamos almacenar una imagen en Azure Compute Gallery al crear grandes catálogos de máquinas no persistentes, ya que, así, los discos del SO de VDA se pueden restablecer más rápidamente. Después de seleccionar **Colocar la imagen preparada en Azure Compute Gallery**, aparece la sección de **configuración de Azure Compute Gallery**, que le permite especificar más parámetros de Azure Computer Gallery:

- **Índice de máquinas virtuales por réplica de imagen**. Permite especificar la ratio de máquinas virtuales y réplicas de imagen que mantendrá Azure. De forma predeterminada, Azure mantiene una única réplica de imagen por cada 40 máquinas no persistentes. En el caso de máquinas persistentes, la cantidad predeterminada es de 1000 máquinas.
- **Máximo de réplicas**. Permite especificar el máximo de réplicas de imagen que conservará Azure. El valor predeterminado es 10.

Para obtener información sobre Azure Compute Gallery, consulte Azure Compute Gallery.

4. En la página **Máquinas virtuales**, indique la cantidad de máquinas virtuales que quiere crear y su tamaño. Después de crear el catálogo, puede modificar el catálogo para cambiar el tamaño de la máquina.
5. La página **Tarjetas NIC** no contiene información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.
6. En la página **Parámetros del disco**, elija si quiere habilitar la caché de reescritura. Con la función de optimización del almacenamiento de MCS habilitada, puede configurar los siguientes parámetros al crear un catálogo: Esta configuración se aplica tanto a los entornos de Azure como a los de GCP.

   Después de habilitar la caché de reescritura, puede hacer lo siguiente:

   - Puede configurar la RAM y el tamaño del disco utilizados para almacenar en caché datos temporales. Para obtener más información, consulte Configurar la caché de datos temporales.

- Seleccione el tipo de almacenamiento del disco de caché con reescritura. Están disponibles las siguientes opciones de almacenamiento para uso con el disco de caché con reescritura:
  - SSD Premium
  - SSD estándar
  - HDD estándar
- Elija si prefiere que el disco de caché de reescritura sea persistente para las máquinas virtuales aprovisionadas. Seleccione **Habilitar caché con reescritura** para que estas opciones estén disponibles. De forma predeterminada, se selecciona **Usar disco no persistente de caché con reescritura**.
- Seleccione el tipo de disco de caché con reescritura.
  - **Usar disco no persistente de caché con reescritura**. Si se selecciona, el disco de caché con reescritura se elimina durante los ciclos de energía. Se perderán todos los datos redirigidos a él. Si el disco temporal de la VM tiene suficiente espacio, se usa para alojar el disco de caché con reescritura para reducir los costes. Tras la creación del catálogo, puede comprobar si las máquinas aprovisionadas utilizan el disco temporal. Para ello, haga clic en el catálogo y verifique la información de la ficha **Propiedades de plantilla**. Si se usa el disco temporal, verá **Disco no persistente de caché con reescritura**, y su valor es **Sí (con el disco temporal de la máquina virtual)**. De lo contrario, verá **Disco no persistente de caché con reescritura**, y su valor es **No (sin usar el disco temporal de la VM)**.
  - **Usar disco persistente de caché con reescritura**. Si se selecciona, el disco de caché con reescritura persiste en las máquinas virtuales aprovisionadas. Habilitar esta opción aumenta los costes de almacenamiento.
- Elija si quiere conservar las VM y los discos del sistema para los VDA durante los ciclos de energía.

  **Conservar VM y disco del sistema durante los ciclos de energía.** Disponible al seleccionar **Habilitar caché con reescritura**. De forma predeterminada, las VM y los discos del sistema se eliminan al apagar la máquina y se crean de nuevo al iniciarla. Si quiere reducir los tiempos de reinicio de las máquinas virtuales, seleccione esta opción. Recuerde que habilitar esta opción también aumenta los costes de almacenamiento.
- Elija si quiere **habilitar el ahorro de costes de almacenamiento**. Si se habilita, para ahorrar costes de almacenamiento, revierta el disco de almacenamiento a un disco duro estándar cuando la máquina virtual se apague. La máquina virtual cambia a sus parámetros originales al reiniciarse. La opción se aplica tanto a los discos de almacenamiento como a los discos de caché de reescritura. También puede usar PowerShell. Consulte Cambiar el tipo de almacenamiento a un nivel inferior al apagar una máquina virtual.

> **Nota:**
>
> Microsoft impone restricciones al cambiar el tipo de almacenamiento durante el apagado de máquinas virtuales. También es posible que, en el futuro, Microsoft bloquee cambios en el tipo de almacenamiento. Para obtener más información, consulte este artículo de Microsoft.

- Elija si quiere cifrar los datos de las máquinas de este catálogo y qué clave de cifrado usar. El cifrado del lado del servidor con una clave administrada por el cliente (CMK) permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Los parámetros predeterminados se heredan del perfil de máquina o de la imagen maestra, y el perfil tiene prioridad:
  - Si usa un *perfil de máquina* con una clave *CMK*, se selecciona automáticamente la opción **Utilice esta clave para cifrar datos en cada máquina** y se establece de forma predeterminada en la clave del *perfil de máquina*.
  - Si usa un *perfil de máquina* con una clave administrada por la plataforma (PMK) y la *imagen maestra* está cifrada con *CMK*, se selecciona automáticamente la opción **Utilice esta clave para cifrar datos en cada máquina** y se establece de forma predeterminada en la clave de la imagen maestra.
  - Si *no* usa un *perfil de máquina* y la *imagen maestra* está cifrada con *CMK*, se selecciona automáticamente la opción **Utilice esta clave para cifrar datos en cada máquina** y se establece de forma predeterminada en la clave de la *imagen maestra*.

Para obtener más información, consulte Cifrado del lado del servidor de Azure.

7. En la página **Grupo de recursos**, elija si quiere crear grupos de recursos o usar los grupos existentes.
   - Si opta por crear grupos de recursos, seleccione **Siguiente**.
   - Si decide utilizar los grupos de recursos existentes, seleccione esos grupos en la lista **Grupos de recursos de aprovisionamiento disponibles**.

   > **Nota:**
   >
   > Debe seleccionar grupos suficientes para las máquinas que está creando en el catálogo. Si no elige suficientes, aparecerá un mensaje. Puede seleccionar más del mínimo requerido de máquinas si va a agregar más máquinas al catálogo más tarde. No se puede agregar más grupos de recursos a un catálogo una vez creado el catálogo.

   Para obtener más información, consulte Grupos de recursos de Azure.

8. En la página **Identidades de las máquinas**, elija un tipo de identidad y configure las identidades de las máquinas de este catálogo. Si selecciona las máquinas virtuales como **unidas a**

**Azure Active Directory**, puede agregarlas a un grupo de seguridad de Azure AD. Estos son los pasos detallados:

a) En el campo **Tipo de identidad**, seleccione **Unido a Azure Active Directory**. Aparecerá la opción **Grupo de seguridad de Azure AD (opcional)**.
b) Haga clic en **Grupo de seguridad de Azure AD: Crear nuevo**.
c) Introduzca un nombre de grupo y, a continuación, haga clic en **Crear**.
d) Siga las instrucciones que aparecen en pantalla para iniciar sesión en Azure.
Si el nombre del grupo no existe en Azure, aparecerá un icono verde. De lo contrario, aparecerá un mensaje de error en el que se le pide que introduzca un nombre nuevo.
e) Para agregar el grupo de seguridad a un grupo de seguridad asignado, seleccione **Unirse a un grupo de seguridad asignado como miembro** y, a continuación, haga clic en **Seleccione un grupo** para elegir un grupo asignado al que unirse.
f) Introduzca el esquema de nomenclatura de las cuentas de máquina para las máquinas virtuales.

Tras la creación del catálogo, Citrix DaaS accede a Azure en su nombre y crea el grupo de seguridad y una regla de pertenencia dinámica para el grupo. Según la regla, las máquinas virtuales con el esquema de nomenclatura especificado en este catálogo se agregan automáticamente al grupo de seguridad.

Para agregar a este catálogo máquinas virtuales con un esquema de nomenclatura diferente, debe iniciar sesión en Azure. A continuación, Citrix DaaS puede acceder a Azure y crear una regla de pertenencia dinámica basada en el nuevo esquema de nomenclatura.

Para poder eliminar el grupo de seguridad de Azure al eliminar este catálogo, también es necesario iniciar sesión en Azure.

> **Nota:**
>
> Para cambiar el nombre del grupo de seguridad de Azure AD tras la creación del catálogo, modifique el catálogo y vaya a **Grupo de seguridad de Azure AD** en el menú de navegación de la izquierda. Los nombres de los grupos de seguridad de Azure AD no deben contener estos caracteres: <!JEKYLL@5180@5>.

- Las páginas **Credenciales de dominio** y **Resumen** no contienen información específica de Azure. Siga las instrucciones indicadas en el artículo Crear catálogos de máquinas.

Complete el asistente.

### Crear una especificación de plantilla de Azure

Puede crear una especificación de plantilla de Azure en Azure Portal y utilizarla en la interfaz de Configuración completa y en los comandos de PowerShell para crear o actualizar catálogos de máquinas de MCS.

Para crear una especificación de plantilla de Azure para una máquina virtual existente:

1. Vaya a Azure Portal. Seleccione un grupo de recursos y, a continuación, seleccione la VM y la interfaz de red. En el menú **...** de la parte superior, haga clic en **Export template**.
2. Desmarque la casilla **Include parameters** si quiere crear una especificación de plantilla para el aprovisionamiento de catálogos.
3. Haga clic en **Add to library** para modificar la especificación de la plantilla más adelante.
4. En la página **Importing template**, introduzca la información requerida, como **Name**, **Subscription**, **Resource Group**, **Location** y **Version**. Haga clic en **Next: Edit Template**.
5. También necesita una interfaz de red como recurso independiente si quiere aprovisionar catálogos. Por lo tanto, debe quitar cualquier <!JEKYLL@5180@6> especificado en la especificación de la plantilla. Por ejemplo:

   <!JEKYLL@5180@7>
6. Haga clic en **Review+Create** y cree la especificación de la plantilla.
7. En la página **Template Specs**, compruebe la especificación de plantilla que creó. Haga clic en la especificación de la plantilla. En el panel de la izquierda, haga clic en **Versions**.
8. Para crear otra versión, haga clic en **Create new version**. Especifique un nuevo número de versión, modifique la especificación de la plantilla actual y haga clic en **Review+Create** para crear la otra versión de la especificación de plantilla.

Puede obtener información sobre la especificación y la versión de la plantilla mediante estos comandos de PowerShell:

- Para obtener información sobre la especificación de la plantilla, ejecute:

  <!JEKYLL@5180@8>
- Para obtener información sobre la versión de la especificación de la plantilla, ejecute:

  <!JEKYLL@5180@9>

#### Usar una especificación de plantilla para crear o actualizar un catálogo

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar la interfaz de Configuración completa o los comandos de PowerShell.

- Mediante la interfaz de **Configuración completa**: Consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.
- Para PowerShell: Consulte Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

## Aprovisionar máquinas en zonas de disponibilidad especificadas

En entornos de Azure, es posible aprovisionar máquinas en zonas de disponibilidad específicas. Para ello, use la interfaz de Configuración completa o PowerShell

> **Nota:**
>
> Si no se especifica ninguna zona, MCS permite a Azure colocar las máquinas dentro de la región. Si se especifica más de una zona, MCS distribuye aleatoriamente las máquinas entre ellas.

### Configurar zonas de disponibilidad en la interfaz de Configuración completa

Al crear un catálogo de máquinas, puede especificar las zonas de disponibilidad en las que quiere aprovisionar máquinas. En la página **Máquinas virtuales**, seleccione una o varias zonas de disponibilidad donde quiera crear máquinas.

Hay dos razones por las que podría no haber zonas de disponibilidad disponibles: La región no tiene zonas de disponibilidad o el tamaño de máquina seleccionado no está disponible.

Para obtener información sobre cómo configurar mediante un comando de PowerShell, consulte Configurar zonas de disponibilidad con PowerShell.

## Discos efímeros de Azure

Un disco efímero de Azure le permite reutilizar el disco de caché o el disco temporal para almacenar el disco del sistema operativo de una máquina virtual habilitada para Azure. Esta funcionalidad es útil en entornos de Azure que requieren un disco SSD de mayor rendimiento, en lugar de un disco HDD estándar. Para obtener información sobre cómo crear un catálogo con un disco efímero de Azure, consulte Crear un catálogo con un disco efímero de Azure.

> **Nota:**
>
> Los catálogos persistentes no admiten discos de SO efímeros.

Los discos de SO efímeros requieren que el esquema de aprovisionamiento use discos administrados y una Azure Compute Gallery. Para obtener más información, consulte Shared Image Gallery de Azure.

### Almacenamiento de un disco de SO efímero temporal

Tiene la posibilidad de almacenar un disco de SO efímero en el disco temporal de la VM o en un disco de recursos. Esta funcionalidad le permite usar un disco de SO efímero con una máquina virtual que

no tenga caché o que no tenga suficiente caché. Estas VM tienen un disco temporal o de recursos para almacenar un disco de SO efímero, como <!JEKYLL@5180@10>.

Se deben tener en cuenta las siguientes cuestiones:

- Un disco efímero se almacena en el disco de caché o en el disco temporal (de recursos) de las VM. Se prefiere el disco de caché antes que el disco temporal, a menos que el disco de caché no sea lo suficientemente grande como para albergar el contenido del disco del sistema operativo.
- En el caso de las actualizaciones, si una nueva imagen es más grande que el disco de caché, pero más pequeña que el disco temporal, el disco de SO efímero se sustituye por el disco temporal de la VM.

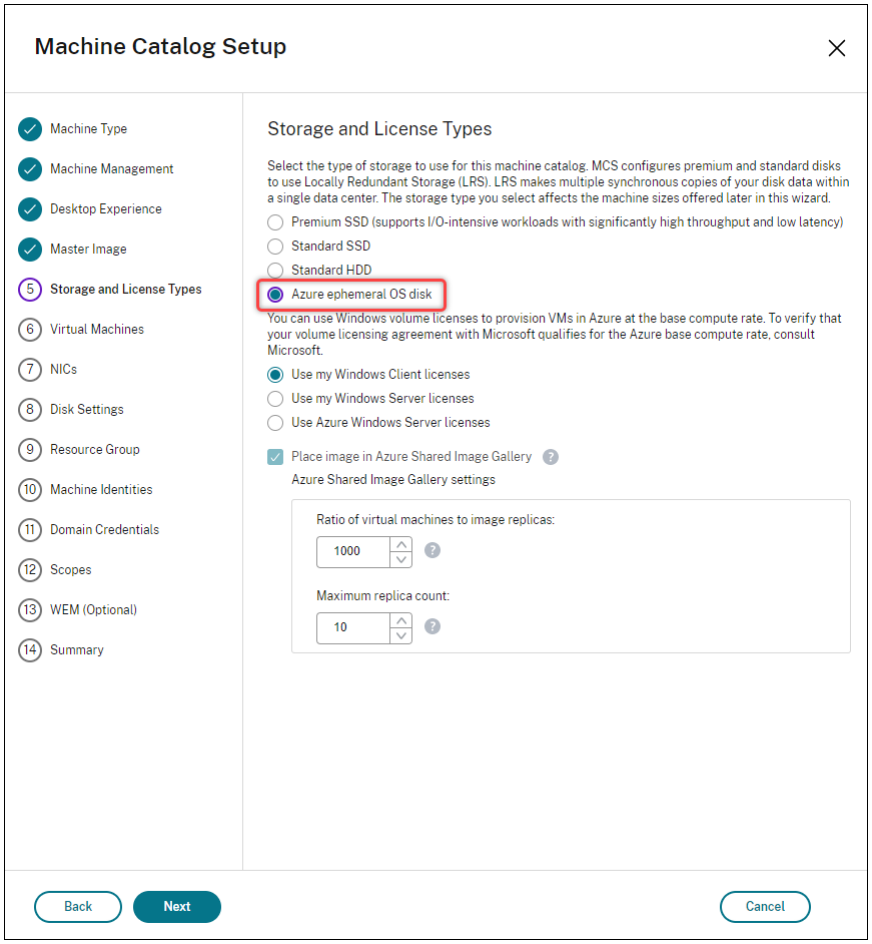
### Optimización del almacenamiento (E/S de MCS) con discos efímeros de Azure y Machine Creation Services (MCS)

El disco de SO efímero de Azure y la E/S de MCS no se pueden habilitar al mismo tiempo.

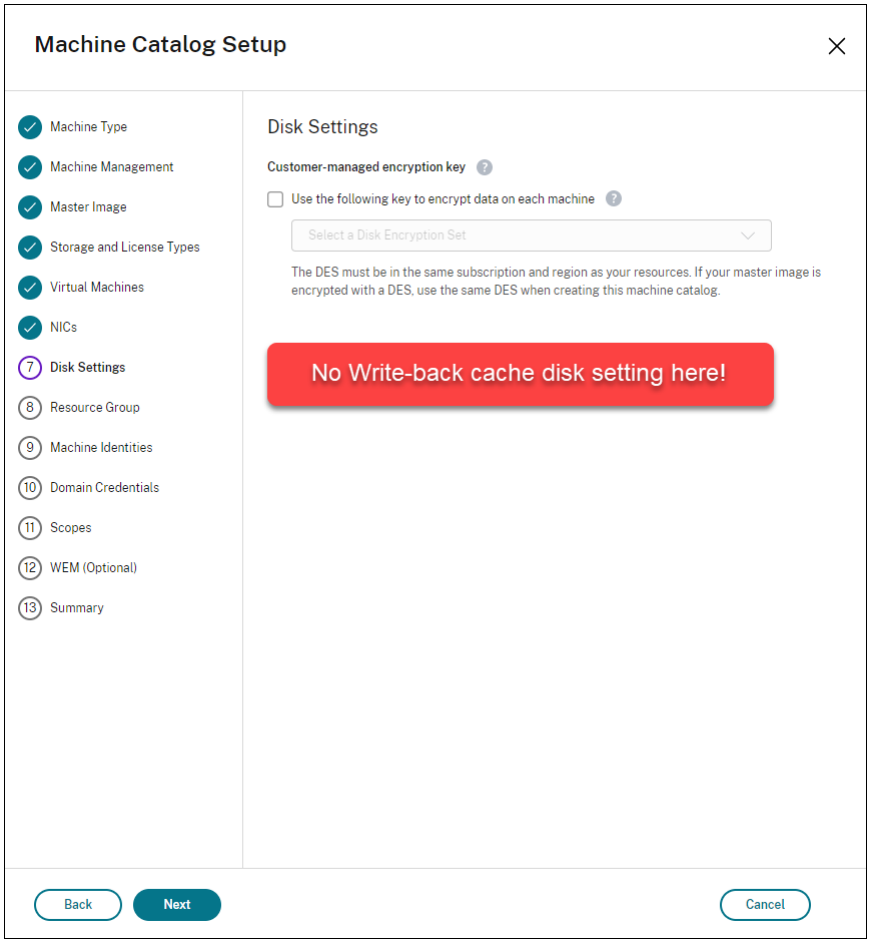
Las consideraciones importantes son las siguientes:

- No puede crear un catálogo de máquinas con el disco de SO efímero y la E/S de MCS habilitados al mismo tiempo.
- En el asistente de **Configuración del catálogo de máquinas**, si selecciona **Disco de SO efímero de Azure** en la página **Tipos de licencia y almacenamiento**, no obtiene la opción de configuración del disco de caché de reescritura en la página **Parámetros del disco**.






- Los parámetros de PowerShell (<!JEKYLL@5180@11> y <!JEKYLL@5180@12>) establecidos en **true** en <!JEKYLL@5180@13> o <!JEKYLL@5180@14> fallan con el mensaje de error correspondiente.
- Para catálogos de máquinas existentes creados con ambas funciones habilitadas, aún puede:
  - actualizar un catálogo de máquinas;
  - agregar o eliminar máquinas virtuales;
  - eliminar un catálogo de máquinas.

### Azure Compute Gallery

Utilice Azure Compute Gallery (antes, Shared Image Gallery) como repositorio de imágenes publicadas para máquinas aprovisionadas por MCS en Azure. Puede almacenar una imagen publicada en la galería para acelerar la creación e hidratación de discos de SO, mejorando los tiempos de inicio y lanzamiento de aplicaciones en máquinas virtuales no persistentes. Azure Compute Gallery contiene los tres elementos siguientes:

- Galería: El lugar donde se almacenan las imágenes. MCS crea una galería para cada catálogo de máquinas.
- Definición de imagen de la galería: Esta definición incluye información (el tipo y el estado del sistema operativo, la región de Azure) sobre la imagen publicada. MCS crea una definición de imagen para cada imagen creada para el catálogo.
- Versión de la imagen de la galería: Cada imagen de Azure Compute Gallery puede tener varias versiones, y cada versión puede tener varias réplicas en diferentes regiones. Cada réplica es una copia completa de la imagen publicada. Citrix DaaS crea una versión de imagen Standard_LRS (versión 1.0.0) para cada imagen con la cantidad adecuada de réplicas en la región del catálogo en función de la cantidad de máquinas del catálogo, el índice de réplicas configurado y el máximo de réplicas configurado.

> **Nota:**
>
> La funcionalidad de Azure Compute Gallery solo es compatible con los discos administrados. No está disponible para catálogos de máquinas antiguos.

Para obtener más información, consulte Introducción a Shared Image Gallery de Azure.

#### Acceder a imágenes desde Azure Compute Gallery

Al seleccionar una imagen para utilizarla para crear un catálogo de máquinas, puede seleccionar las imágenes que haya creado en Azure Compute Gallery. Estas imágenes aparecen en la lista de imágenes de la página **Imagen** del asistente de configuración del catálogo de máquinas.

Para que aparezcan estas imágenes, haga lo siguiente:

1. Configure Citrix DaaS.
2. Conéctese a Azure Resource Manager.
3. En Azure Portal, cree un grupo de recursos. Para obtener información detallada, consulte Crear una galería Shared Image Gallery de Azure mediante el portal.
4. En el grupo de recursos, cree una galería Azure Compute Gallery.
5. En Azure Compute Gallery, cree una definición de imagen.
6. En la definición de imagen, cree una versión de imagen.

Para obtener información sobre cómo configurar Azure Compute Gallery, consulte Configurar Azure Compute Gallery.

### Condiciones para que el disco temporal de Azure sea apto como disco de caché con reescritura

Solamente puede usar el disco temporal de Azure como disco de caché con reescritura si se cumplen todas las condiciones siguientes:

- El disco de caché con escritura no debe persistir, ya que el disco temporal de Azure no es adecuado para datos persistentes.
- El tamaño de VM de Azure elegido debe incluir un disco temporal.
- No es necesario que el disco de SO efímero esté habilitado.
- Aceptar colocar el archivo de caché con escritura en el disco temporal de Azure.
- El tamaño del disco temporal de Azure debe ser mayor que el tamaño total de (tamaño del disco de caché con reescritura + espacio reservado para el archivo de paginación + 1 GB de espacio de búfer).

#### Casos de disco no persistente de caché con reescritura

En la siguiente tabla se describen tres casos diferentes en los que se utiliza un disco temporal para la caché con reescritura al crear un catálogo de máquinas.

| Caso | Resultado |
| --- | --- |
| Se cumplen todas las condiciones para usar un disco temporal para la caché con reescritura. | El archivo WBC <!JEKYLL@5180@15> se coloca en el disco temporal. |
| El disco temporal no tiene suficiente espacio para uso de caché con reescritura. | Se crea un disco VHD “MCSWCDisk”y se coloca un archivo WBC <!JEKYLL@5180@16> en este disco. |
| El disco temporal tiene espacio suficiente para usar caché de reescritura, pero <!JEKYLL@5180@17> está configurado como false. | Se crea un disco VHD “MCSWCDisk”y se coloca un archivo WBC <!JEKYLL@5180@18> en este disco. |

Consulte los siguientes temas de PowerShell:

- Crear un catálogo de máquinas con un disco no persistente de caché con reescritura
- Crear un catálogo de máquinas con un disco persistente de caché con reescritura

### Cifrado del lado del servidor de Azure

Citrix DaaS admite claves de cifrado administradas por el cliente para los discos administrados por Azure a través de Azure Key Vault. Gracias a esta compatibilidad, puede satisfacer los requisitos organizativos y de conformidad mediante el cifrado de los discos administrados del catálogo de máquinas con su propia clave de cifrado. Para obtener más información, consulte Cifrado del lado del servidor de Azure Disk Storage.

Al utilizar esta función para discos administrados:

- Para cambiar la clave con la que está cifrado actualmente el disco, cámbiela en <!JEKYLL@5180@19>. Todos los recursos asociados a ese <!JEKYLL@5180@20> se cifrarán con la nueva clave.
- Cuando inhabilite o elimine la clave, todas las máquinas virtuales con discos que utilicen esa clave se apagarán automáticamente. Después de apagarse, las máquinas virtuales no se podrán utilizar, a menos que la clave se vuelva a habilitar o se asigne una nueva clave. Ningún catálogo que utilice la clave se podrá encender ni se le podrán agregar máquinas virtuales.

#### Consideraciones importantes al utilizar claves de cifrado administradas por el cliente

Tenga en cuenta lo siguiente al usar esta funcionalidad:

- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben residir en la misma suscripción y región.
- Los discos, las instantáneas y las imágenes cifradas con claves administradas por el cliente no pueden transferirse a otro grupo de recursos y suscripción.
- Consulte el sitio de Microsoft para conocer las limitaciones de los conjuntos de cifrado de disco por región.

> **Nota:**
>
> Para obtener información acerca de la configuración del cifrado del lado del servidor de Azure, consulte Inicio rápido: Creación de un almacén de claves mediante Azure Portal.

#### Clave de cifrado administrada por el cliente de Azure

Al crear un catálogo de máquinas, puede elegir si cifrar los datos presentes en las máquinas aprovisionadas en el catálogo. El cifrado del lado del servidor con una clave de cifrado administrada por el cliente permite administrar el cifrado a nivel de disco administrado y proteger los datos que contengan las máquinas del catálogo. Un conjunto de cifrado de disco (Disk Encryption Set o DES) representa una clave administrada por el cliente. Para utilizar esta función, primero debe crear el DES en Azure. Un DES tiene este formato:

- <!JEKYLL@5180@21>

Seleccione un DES de la lista. El DES que seleccione debe estar en la misma suscripción y región que los recursos.

Si crea un catálogo con una clave de cifrado y posteriormente inhabilita el DES correspondiente en Azure, ya no podrá encender las máquinas del catálogo ni agregarle máquinas.

Consulte Crear un catálogo de máquinas con una clave administrada por el cliente.

### Cifrado de discos de Azure en el host

Puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host. Actualmente, MCS solo admite el flujo de trabajo de perfiles de máquina para esta función. Puede utilizar una máquina virtual o una especificación de plantilla como entrada para un perfil de máquina.

Este método de cifrado no cifra los datos a través del almacenamiento de Azure. El servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo.

**Restricciones:**

El cifrado de discos de Azure en el host:

- No se admite con todos los tamaños de máquina de Azure
- Es incompatible con el cifrado de discos de Azure

Para obtener más información, consulte:

- Crear un catálogo de máquinas con capacidad de cifrado en el host.
- Obtener la información de cifrado en el host desde un perfil de máquina

### Cifrado doble en disco administrado

Puede crear un catálogo de máquinas con doble cifrado. Todos los catálogos creados con esta función tienen todos los discos cifrados del lado del servidor con claves administradas por la plataforma y por el cliente. Usted posee y mantiene el Azure Key Vault, la clave de cifrado y los conjuntos de cifrado de disco (DES).

El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado.

> **Nota:**
>
> - Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante la interfaz de Configuración completa y los comandos de PowerShell.
> - Puede utilizar un flujo de trabajo no basado en perfiles de máquina o un flujo de trabajo basado en perfiles de máquina para crear o actualizar un catálogo de máquinas con doble cifrado.
> - Si utiliza un flujo de trabajo no basado en perfiles de máquina para crear un catálogo de máquinas, puede reutilizar el <!JEKYLL@5180@22> almacenado.

> • Si usa un perfil de máquina, puede usar una máquina virtual o una especificación de plantilla como entrada de perfil de máquina.

#### Limitaciones

- No se admite el cifrado doble en los discos Ultra Disk ni en los discos Premium SSD v2.
- El cifrado doble no se admite en discos no administrados.
- Si inhabilita una clave de un conjunto de cifrado de disco asociados a un catálogo, se inhabilitan las máquinas virtuales del catálogo.
- Todos los recursos relacionados con las claves administradas por el cliente (instancias de Azure Key Vault, conjuntos de cifrado de disco, máquinas virtuales, discos e instantáneas) deben estar en la misma suscripción y región.
- Solo puede crear un máximo de 50 conjuntos de cifrado de disco por región y suscripción.

Consulte los siguientes temas de PowerShell:

- Crear un catálogo de máquinas con doble cifrado
- Convertir un catálogo sin cifrar para usar el cifrado doble
- Verificar que el catálogo tenga un cifrado doble

### Grupos de recursos de Azure

Los grupos de recursos de aprovisionamiento de Azure ofrecen una manera de aprovisionar las VM que proporcionan escritorios y aplicaciones a los usuarios. Puede agregar los grupos de recursos de Azure vacíos existentes cuando cree un catálogo de máquinas con MCS. También puede decidir que se creen nuevos grupos de recursos para usted. Para obtener información acerca de los grupos de recursos de Azure, consulte la documentación de Microsoft.

#### Uso del grupo de recursos de Azure

No hay límite en el número de máquinas virtuales, discos administrados, instantáneas e imágenes por grupo de recursos de Azure (se eliminó la limitación de 240 VM/800 discos administrados por grupo de recursos de Azure).

- Al utilizar la entidad de servicio de ámbito completo para crear un catálogo de máquinas, MCS crea solo un grupo de recursos de Azure y utiliza ese grupo para el catálogo.
- Al utilizar la entidad de servicio de ámbito restringido para crear un catálogo de máquinas, debe proporcionar un grupo de recursos de Azure vacío y creado previamente para el catálogo.

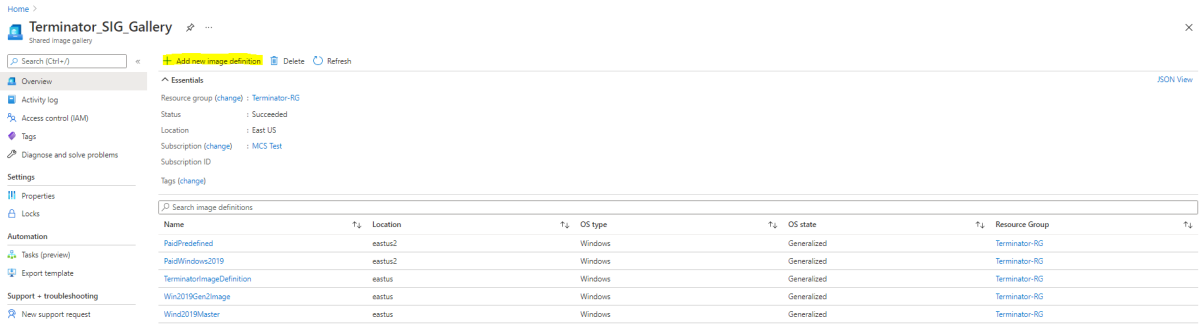
### Azure Marketplace

Citrix DaaS admite el uso de una imagen maestra en Azure que contenga información del plan para crear un catálogo de máquinas. Para obtener más información, consulte Microsoft Azure Marketplace.

> **Sugerencia:**
>
> Algunas imágenes que se encuentran en Azure Marketplace, como la imagen estándar de Windows Server, no llevan anexa información del plan. La funcionalidad Citrix DaaS es para imágenes de pago.

### Compruebe que la imagen creada en Azure Compute Gallery contiene información del plan de Azure

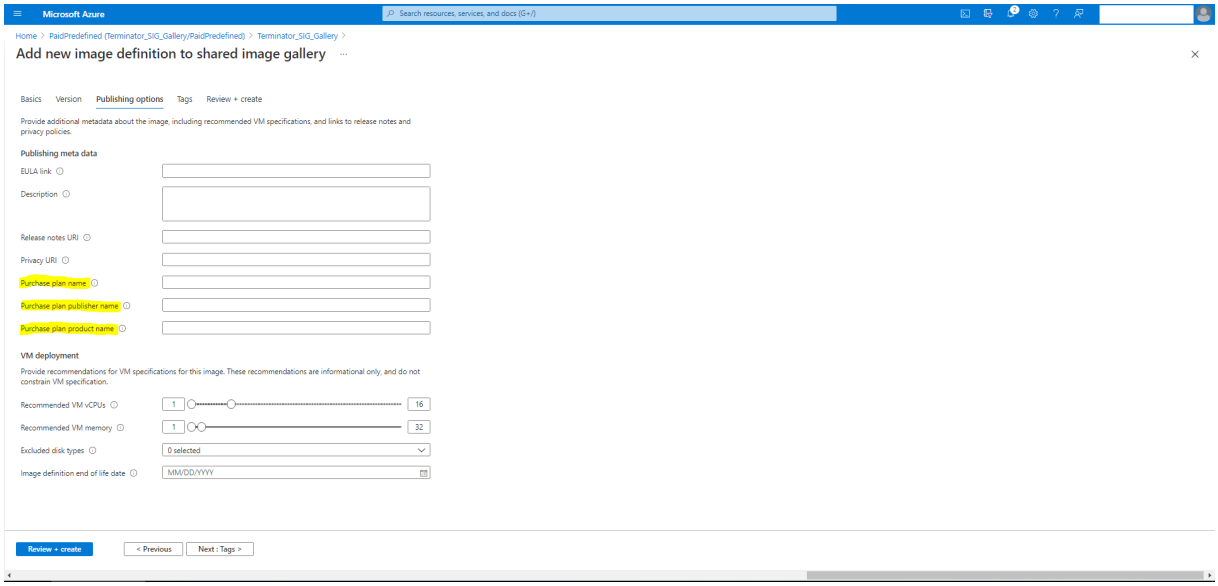
Use el procedimiento descrito en esta sección para ver las imágenes de Azure Compute Gallery en la interfaz de Configuración completa. Estas imágenes se pueden usar, opcionalmente, para una imagen maestra. Para colocar la imagen en una Azure Compute Gallery, cree una definición de imagen en una galería.



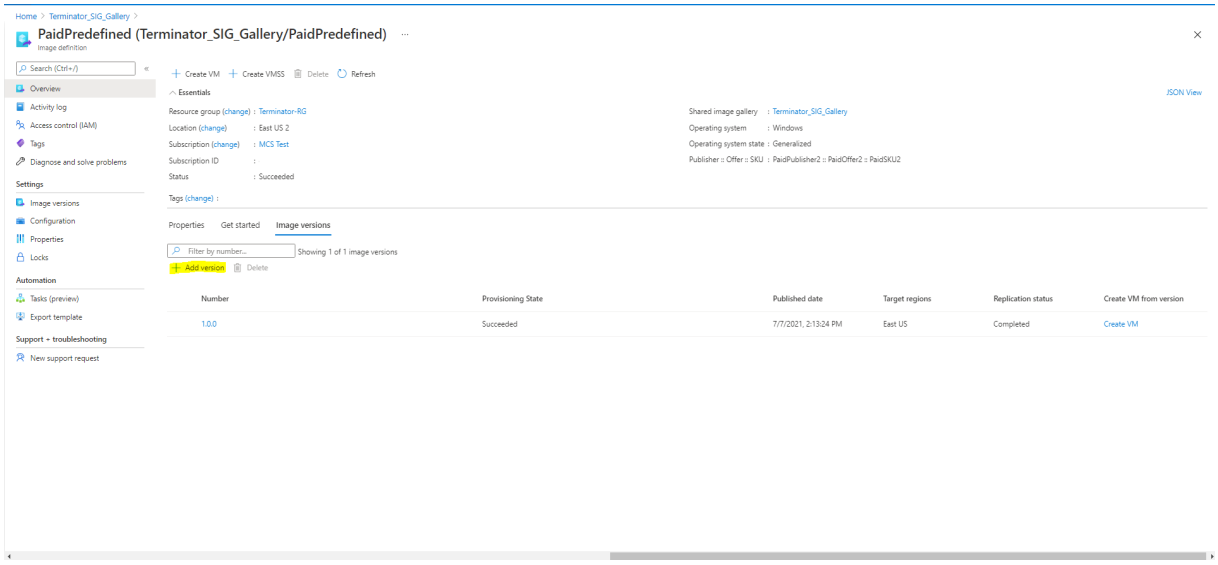

En la página **Publishing options**, verifique la información del plan de compra.

Los campos de información del plan de compra están vacíos inicialmente. Rellene esos campos con la información del plan de compra utilizada para la imagen. Si no se rellena la información del plan de compra, puede ocurrir un error en el procesamiento del catálogo de máquinas.

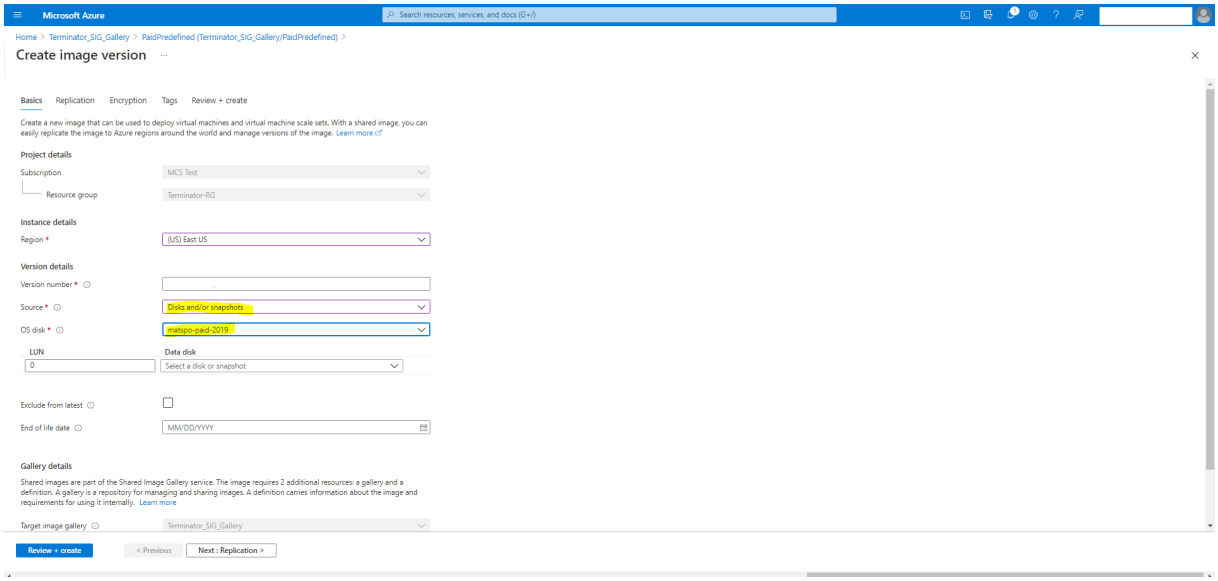



Después de verificar la información del plan de compra, cree una versión de la imagen dentro de la definición. Sirve de imagen maestra. Haga clic en **Add version**:




En la sección **Version details**, seleccione la instantánea de la imagen o el disco administrado como origen:




## Aprovisionar máquinas virtuales del catálogo con el agente de Azure Monitor instalado

La supervisión de Azure es un servicio que puede utilizar para recopilar, analizar y responder a datos de telemetría de sus entornos locales y de Azure.

El agente de Azure Monitor (AMA) recopila datos de supervisión de recursos de procesamiento, como máquinas virtuales, y los entrega a Azure Monitor. Actualmente, permite la recopilación de registros de eventos y métricas de Syslog y rendimiento, y los envía a los orígenes de datos de las Métricas de Azure Monitor y los Registros de Azure Monitor.

Para habilitar la supervisión mediante la identificación exclusiva de las máquinas virtuales en los datos de supervisión, puede aprovisionar las máquinas virtuales de un catálogo de máquinas de MCS con AMA instalado como extensión.

### Requisitos

- Permisos: Asegúrese de tener los permisos mínimos de Azure especificados en Acerca de los permisos de Azure y estos permisos para usar Azure Monitor:
  - <!JEKYLL@5180@23>
  - <!JEKYLL@5180@24>
  - <!JEKYLL@5180@25>
  - <!JEKYLL@5180@26>
  - <!JEKYLL@5180@27>
- Regla de recopilación de datos: Configure una regla de recopilación de datos (DCR) en Azure Portal. Para obtener información sobre cómo configurar una DCR, consulte Creación de una

regla de recopilación de datos. Las DCR son específicas de cada plataforma (Windows o Linux). Asegúrese de crear una DCR según la plataforma requerida.
El AMA utiliza las reglas de recopilación de datos (DCR) para administrar la asignación entre los recursos, como las máquinas virtuales, y los orígenes de datos, como las Métricas de Azure Monitor y los Registros de Azure Monitor.

- Espacio de trabajo predeterminado: Cree un espacio de trabajo en Azure Portal. Para obtener información sobre cómo crear un espacio de trabajo, consulte Creación de un área de trabajo de Log Analytics. Al recopilar registros y datos, la información se almacena en un espacio de trabajo. Un espacio de trabajo tiene un ID de espacio de trabajo y un ID de recurso únicos. El nombre del espacio de trabajo debe ser único para un grupo de recursos determinado. Después de crear un espacio de trabajo, configure los orígenes de datos y las soluciones para almacenar sus datos en el espacio de trabajo.
- Extensión de supervisión en la lista de permitidos: Las extensiones <!JEKYLL@5180@28> y <!JEKYLL@5180@29> son extensiones de la lista de permitidos definida por Citrix. Para ver la lista de extensiones incluidas en la lista de permitidos, utilice el comando <!JEKYLL@5180@30> de PowerShell.
- Imagen maestra: Microsoft recomienda quitar extensiones de una máquina existente antes de crear otra máquina a partir de ella. Si no se quitan las extensiones, es posible que queden archivos sobrantes y que se produzca un comportamiento inesperado. Para obtener más información, consulte Si la máquina virtual se vuelve a crear a partir de una máquina virtual existente.

Para obtener información sobre cómo crear un catálogo con AMA habilitado mediante PowerShell, consulte Aprovisionar VM de catálogo con AMA habilitado.

### Máquinas virtuales confidenciales de Azure

Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa.

Puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina.

#### Consideraciones importantes acerca de las máquinas virtuales confidenciales

Las consideraciones importantes relativas a los tamaños de máquina virtual compatibles y la creación de catálogos de máquinas con VM confidenciales son las siguientes:

- Tamaños de VM compatibles: Las máquinas virtuales confidenciales admiten los siguientes tamaños:
  - Serie DCasv5
  - Serie DCadsv5
  - Serie ECasv5
  - Serie ECadsv5
- Crear catálogos de máquinas con VM confidenciales.
  - Puede crear un catálogo de máquinas con VM confidenciales de Azure mediante la interfaz de Configuración completa y los comandos de PowerShell.
  - Para crear un catálogo de máquinas con VM confidenciales de Azure, debe usar un flujo de trabajo basado en perfiles de máquina. Puede usar una máquina virtual o una especificación de plantilla como entrada del perfil de máquina.
  - La imagen maestra y la entrada del perfil de máquina deben estar habilitadas con el mismo tipo de seguridad confidencial. Los tipos de seguridad son:
    - VMGuestStateOnly: VM confidencial con solo el estado de invitado de VM cifrado
    - DiskWithVMGuestState: VM confidencial con disco de SO y estado de invitado de máquina virtual cifrados con una clave administrada por la plataforma o una clave administrada por el cliente. Se pueden cifrar tanto los discos de SO normales como los efímeros.
  - Con el parámetro AdditionalData, puede obtener información de VM confidencial de varios tipos de recursos, como discos administrados, instantáneas, imágenes de Azure Compute Gallery, máquinas virtuales y especificaciones de plantilla de Azure Resource Manager. Por ejemplo:

    <!JEKYLL@5180@31>

    Los campos de datos adicionales son:

    - DiskSecurityType
    - ConfidentialVMDiskEncryptionSetId
    - DiskSecurityProfiles

    Para obtener la propiedad de computación confidencial de un tamaño de una máquina, ejecute el siguiente comando: <!JEKYLL@5180@32>

    El campo de datos adicional es <!JEKYLL@5180@33>.
  - No puede cambiar la imagen maestra ni el perfil de máquina de un tipo de seguridad confidencial a un tipo de seguridad no confidencial ni de un tipo de seguridad no confidencial a uno confidencial.
  - Aparecerán los mensajes de error correspondientes a cualquier configuración incorrecta.

### Preparar imágenes maestras y perfiles de máquina

Antes de crear un conjunto de máquinas virtuales confidenciales, siga estos pasos para preparar una imagen maestra y un perfil de máquina para ellas:

1. En el portal de Azure, cree una máquina virtual confidencial con parámetros específicos, como:
   - **Tipo de seguridad**: Máquinas virtuales confidenciales
   - **Cifrado de disco de SO confidencial**: Habilitado.
   - **Administración de claves**: Cifrado de disco confidencial con una clave administrada por la plataforma
     Para obtener más información sobre la creación de máquinas virtuales confidenciales, consulte este artículo de Microsoft.
2. Prepare la imagen maestra en la máquina virtual creada. Instale las aplicaciones y VDA necesarios en la máquina virtual creada.

   > **Nota:**
   >
   > No se admite la creación de máquinas virtuales confidenciales mediante VHD. En su lugar, use Azure Compute Gallery, discos administrados o instantáneas para este fin.

3. Cree el perfil de la máquina de una de estas maneras:
   - Use la máquina virtual existente creada en el paso 1 si tiene las propiedades de máquina necesarias.
   - Si opta por una especificación de plantilla de ARM como perfil de máquina, cree la especificación de plantilla según sea necesario. En concreto, configure parámetros que cumplan con los requisitos de VM confidencial, como *SecurityEncryptionType* y *diskEncryptionSet* (para la clave administrada por el cliente). Para obtener más información, consulte Crear una especificación de plantilla de Azure.

     > **Nota:**
     >
     > - Asegúrese de que la imagen maestra y el perfil de la máquina tengan el mismo tipo de clave de seguridad.
     > - Para crear máquinas virtuales confidenciales que requieran cifrado de disco de SO confidencial con una clave administrada por el cliente, asegúrese de que los ID del conjunto de cifrado de disco tanto en la imagen maestra como en el perfil de la máquina sean idénticos.

### Crear máquinas virtuales confidenciales mediante Configuración completa o comandos de PowerShell

Para crear un conjunto de máquinas virtuales confidenciales, cree un catálogo de máquinas con una imagen maestra y un perfil de máquina derivados de la máquina virtual confidencial deseada.

Para crear el catálogo mediante la Configuración completa, siga los pasos descritos en Crear catálogos de máquinas. Tenga en cuenta las siguientes consideraciones:

- En la página **Imagen**, seleccione una imagen maestra y un perfil de máquina que haya preparado para la creación de la máquina virtual confidencial. La selección del perfil de la máquina es obligatoria y solo están disponibles para selección los perfiles cuyo tipo de cifrado de seguridad coincida con el de la imagen maestra seleccionada.
- En la página **Máquinas virtuales**, solo aparecen para selección los tamaños de máquina compatibles con máquinas virtuales confidenciales.
- En la página **Parámetros del disco**, no puede especificar el conjunto de cifrado del disco porque se hereda del perfil de máquina seleccionado.

### Usar PowerShell

En esta sección se detalla cómo realizar las siguientes tareas con PowerShell:

- Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell
- Habilitar las extensiones de VM de Azure
- Catálogos de máquinas con inicio seguro
- Usar valores de propiedades de perfil de máquina
- Configurar zonas de disponibilidad con PowerShell
- Aprovisionar VM en hosts dedicados de Azure
- Configurar los tipos de almacenamiento
- Habilitar el almacenamiento con redundancia de zonas
- Capture la configuración de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina
- Verificar la licencia de Windows
- Configurar la licencia de Linux
- Crear un catálogo de máquinas con un disco efímero de Azure
- Configurar Azure Compute Gallery
- Crear o actualizar un catálogo con varias NIC por máquina virtual
- Crear un catálogo de máquinas con un disco no persistente de caché con reescritura
- Crear un catálogo de máquinas con un disco persistente de caché con reescritura
- Mejorar el rendimiento del arranque con E/S de MCS
- Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente
- Crear un catálogo de máquinas con capacidad de cifrado en el host

- Crear un catálogo de máquinas con doble cifrado
- Determinación de la ubicación del archivo de paginación
- Casos de configuración de archivos de paginación
- Especificar los parámetros del archivo de páginación
- Modificar los parámetros del archivo de páginación
- Aprovisionar VM de catálogo con AMA habilitado
- Crear un catálogo con máquinas virtuales de Azure Spot
- Copiar etiquetas en todos los recursos

### Usar la especificación de la plantilla para crear o actualizar un catálogo con PowerShell

Puede crear o actualizar un catálogo de máquinas de MCS mediante una especificación de plantilla como entrada de datos de un perfil de máquina. Para ello, puede utilizar la interfaz de Configuración completa o los comandos de PowerShell.

Para la interfaz de Configuración completa, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.

Mediante los comandos de PowerShell:

1. Abra la ventana de **PowerShell**.
2. Ejecute <!JEKYLL@5180@34>.
3. Cree o actualice un catálogo.
    - Para crear un catálogo:
        a) Utilice el comando <!JEKYLL@5180@35> con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

        <!JEKYLL@5180@36>

        b) Termine de crear el catálogo.
    - Para actualizar un catálogo, utilice el comando <!JEKYLL@5180@37> con una especificación de plantilla como entrada de datos de un perfil de máquina. Por ejemplo:

    <!JEKYLL@5180@38>

### Habilitar las extensiones de VM de Azure

Después de seleccionar la especificación de la plantilla ARM, ejecute estos comandos de PowerShell para operar con extensiones de Azure VM:

- Para ver la lista de extensiones de VM de Azure compatibles: <!JEKYLL@5180@39>

- Para agregar más extensiones de VM: <!JEKYLL@5180@40>. Por ejemplo, <!JEKYLL@5180@41>

  Si intenta agregar uno de estos elementos, el comando no se ejecuta y aparece un mensaje de error:

  - Extensión definida por Citrix.
  - Extensión existente definida por el usuario.
  - Claves de configuración no admitidas. Por ahora, la clave de configuración admitida es <!JEKYLL@5180@42>.

- Para quitar extensiones de la lista: <!JEKYLL@5180@43>. Puede quitar las extensiones que agregó.

### Catálogos de máquinas con inicio seguro

Para crear correctamente un catálogo de máquinas con inicio seguro, utilice:

- Un perfil de máquina con inicio seguro
- Un tamaño de máquina virtual compatible con el inicio seguro
- Una versión de máquina virtual Windows que admita inicio seguro. En la actualidad, Windows 10, Windows 11 y Windows Server 2016, 2019 y 2022 admiten el inicio seguro.

> **Importante:**
>
> MCS admite la creación de un catálogo con máquinas virtuales habilitadas para inicio seguro. Sin embargo, para actualizar un catálogo persistente y las máquinas virtuales ya existentes, debe usar el portal de Azure. No puede actualizar el inicio seguro de un catálogo no persistente. Para obtener más información, consulte el documento de Microsoft Enable Trusted launch on existing Azure VMs.

Para ver los elementos de inventario que ofrecen Citrix DaaS y determinar si el tamaño de máquina virtual admite el inicio seguro, ejecute el siguiente comando:

1. Abra una ventana de PowerShell.
2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute este comando:

   <!JEKYLL@5180@44>

4. Ejecute <!JEKYLL@5180@45>
5. Compruebe el valor del atributo <!JEKYLL@5180@46>.

   - Si <!JEKYLL@5180@47> es **True**, el tamaño de máquina virtual admite el inicio seguro.
   - Si <!JEKYLL@5180@48> es **False**, el tamaño de máquina virtual no admite el inicio seguro.

Según la instancia de PowerShell de Azure, puede usar este comando para determinar los tamaños de máquina virtual que admiten el inicio seguro:

<!JEKYLL@5180@49>

A continuación, se muestran ejemplos que describen si el tamaño de máquina virtual admite el inicio seguro después de ejecutar el comando de Azure PowerShell.

- *Ejemplo 1*: Si la máquina virtual de Azure solo admite la generación 1, esa máquina virtual no admite el inicio seguro. Por lo tanto, la funcionalidad <!JEKYLL@5180@50> no se muestra después de ejecutar el comando de Azure PowerShell.
- *Ejemplo 2*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad <!JEKYLL@5180@51> es **True**, el tamaño de máquina virtual de la generación 2 no se admite para el inicio seguro.
- *Ejemplo 3*: Si la máquina virtual de Azure solo admite la generación 2 y la funcionalidad <!JEKYLL@5180@52> no se muestra después de ejecutar el comando de PowerShell, se admite el tamaño de máquina virtual de generación 2 para el inicio seguro.

Para obtener más información sobre el inicio seguro para máquinas virtuales de Azure, consulte el documento Trusted Launch for Azure Virtual Machines de Microsoft.

#### Crear un catálogo de máquinas con inicio seguro

1. Cree una imagen maestra habilitada para inicio seguro. Consulte la documentación Trusted Launch VM Images de Microsoft.
2. Cree una especificación de plantilla o máquina virtual con el tipo de seguridad **máquinas virtuales con inicio seguro**. Para obtener más información sobre cómo crear una especificación de plantilla o VM, consulte el documento Deploy a Trusted Launch VM de Microsoft.
3. Cree un catálogo de máquinas mediante la interfaz de Configuración completa o los comandos de PowerShell.

    - Si quiere usar la interfaz de Configuración completa, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager en la interfaz de Configuración completa.
    - Si quiere usar los comandos de PowerShell, utilice el comando <!JEKYLL@5180@53> con la especificación de plantilla o VM como entrada de perfil de máquina. Para ver la lista completa de comandos para crear un catálogo, consulte Creación de un catálogo.

      Ejemplo de <!JEKYLL@5180@54> con VM como entrada del perfil de máquina:

      <!JEKYLL@5180@55>

Ejemplo de <!JEKYLL@5180@56> con especificación de plantilla como entrada del perfil de máquina:

<!JEKYLL@5180@57>

#### Errores al crear catálogos de máquinas con inicio seguro

Al crear un catálogo de máquinas con inicio seguro en los siguientes casos, se obtienen los errores correspondientes:

| Caso | Error |
| --- | --- |
| Si selecciona un perfil de máquina al crear un catálogo no administrado | <!JEKYLL@5180@58> |
| Si selecciona un perfil de máquina que admite el inicio seguro al crear un catálogo con un disco no administrado como imagen maestra | <!JEKYLL@5180@59> |
| Si no selecciona un perfil de máquina al crear un catálogo administrado con una imagen maestra de origen que tenga inicio seguro como tipo de seguridad | <!JEKYLL@5180@60> |
| Si selecciona un perfil de máquina con un tipo de seguridad diferente del tipo de seguridad de la imagen maestra | <!JEKYLL@5180@61> |
| Si selecciona un tamaño de máquina virtual que no admite el inicio seguro, pero usa una imagen maestra que sí admite el inicio seguro al crear un catálogo | <!JEKYLL@5180@62> |

### Usar valores de propiedades de perfil de máquina

El catálogo de máquinas utiliza las siguientes propiedades que se definen en las propiedades personalizadas:

- Zona de disponibilidad
- ID de grupo de hosts dedicado
- ID del conjunto de cifrado de disco
- Tipo de SO
- Tipo de licencia
- Tipo de almacenamiento

Si estas propiedades personalizadas no se definen explícitamente, los valores de propiedad se establecen a partir de la especificación de plantilla de ARM o de la VM, lo que se utilice como perfil de máquina. Además, si no se especifica <!JEKYLL@5180@63>, se establecerá a partir del perfil de máquina.

> **Nota:**
>
> Si faltan algunas propiedades en el perfil de la máquina (MachineProfile) y no están definidas en las propiedades personalizadas (CustomProperties), se utilizan los valores por defecto de las propiedades siempre que sea aplicable.

En la siguiente sección se describen algunos casos de <!JEKYLL@5180@64> y <!JEKYLL@5180@65> en los que <!JEKYLL@5180@66> tiene definidas todas las propiedades o los valores se derivan de MachineProfile.

- Casos de New-ProvScheme
  - MachineProfile tiene todas las propiedades y CustomProperties no está definido. Ejemplo:

    <!JEKYLL@5180@67>

    Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5180@68>
  - MachineProfile tiene algunas propiedades y CustomProperties no está definido. Ejemplo: MachineProfile solo tiene LicenseType y OsType.

    <!JEKYLL@5180@69>

    Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5180@70>
  - Tanto MachineProfile como CustomProperties definen todas las propiedades. Ejemplo:

    <!JEKYLL@5180@71>

    Las propiedades personalizadas tienen prioridad. Estos valores se definen como propiedades personalizadas del catálogo:

    <!JEKYLL@5180@72>
  - Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Ejemplo:
    - CustomProperties define LicenseType y StorageAccountType
    - MachineProfile define LicenseType, OsType y Zones

    <!JEKYLL@5180@73>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5180@74>

- Algunas propiedades se definen en MachineProfile y otras se definen en CustomProperties. Además, ServiceOffering no está definido. Ejemplo:
  - CustomProperties define StorageType
  - MachineProfile define LicenseType

<!JEKYLL@5180@75>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5180@76>

- Si OsType no está ni en CustomProperties ni en MachineProfile, entonces:
  - El valor se lee de la imagen maestra.
  - Si la imagen maestra es un disco no administrado, OsType se establece en Windows. Ejemplo:

<!JEKYLL@5180@77>

El valor de la imagen maestra se escribe en las propiedades personalizadas, en este caso Linux.

<!JEKYLL@5180@78>

- Casos de Set-ProvScheme
  - Un catálogo con:
    - CustomProperties para <!JEKYLL@5180@79> y OsType
    - MachineProfile <!JEKYLL@5180@80> que define zonas
  - Actualizaciones:
    - MachineProfile mpB.vm que define StorageAccountType
    - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define LicenseType y OsType

<!JEKYLL@5180@81>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5180@82>

- Un catálogo con:
  - CustomProperties para <!JEKYLL@5180@83> y OsType
  - MachineProfile <!JEKYLL@5180@84> que define StorageAccountType y LicenseType

- Actualizaciones:
  - Un nuevo conjunto de propiedades personalizadas $CustomPropertiesB que define StorageAccountType y OsType.

<!JEKYLL@5180@85>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5180@86>

- Un catálogo con:
  - CustomProperties para <!JEKYLL@5180@87> y OsType
  - MachineProfile <!JEKYLL@5180@88> que define Zones
- Actualizaciones:
  - MachineProfile mpB.vm que define StorageAccountType y LicenseType
  - <!JEKYLL@5180@89> está sin especificar

<!JEKYLL@5180@90>

Estos valores se definen como propiedades personalizadas del catálogo:

<!JEKYLL@5180@91>

### Configurar zonas de disponibilidad con PowerShell

Con PowerShell, puede ver Citrix DaaS que ofrece elementos de inventario mediante <!JEKYLL@5180@92>. Por ejemplo, para ver la oferta de servicio de la *región oriental de EE. UU.* <!JEKYLL@5180@93>:

<!JEKYLL@5180@94>

Para ver las zonas, utilice el parámetro <!JEKYLL@5180@95> para el elemento:

<!JEKYLL@5180@96>

Si no se especifican zonas de disponibilidad, no hay ningún cambio en la forma en que se aprovisionan las máquinas.

Para configurar las zonas de disponibilidad a través de PowerShell, utilice la propiedad personalizada **Zonas** disponible con la operación <!JEKYLL@5180@97>. La propiedad **Zonas** define una lista de zonas de disponibilidad en las que aprovisionar máquinas. Esas zonas pueden incluir una o más zonas de disponibilidad. Por ejemplo, <!JEKYLL@5180@98> para las zonas 1 y 3.

Utilice el comando <!JEKYLL@5180@99> para actualizar las zonas de un esquema de aprovisionamiento.

Si se proporciona una zona no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error con instrucciones sobre cómo corregir el comando no válido.

> **Sugerencia:**
>
> Si especifica una propiedad personalizada no válida, el esquema de aprovisionamiento no se actualiza y aparece un mensaje de error al respecto.

**Resultado de usar grupos de hosts y zonas de disponibilidad de Azure al mismo tiempo**

Hay una comprobación previa para evaluar si la creación de un catálogo de máquinas se hará correctamente en función de la zona de disponibilidad especificada en la propiedad personalizada y la zona del grupo de hosts. La creación del catálogo falla si la zona de disponibilidad especificada en la propiedad personalizada no coincide con la zona del grupo de hosts.

Para obtener información sobre cómo configurar zonas de disponibilidad a través de PowerShell, consulte Configurar zonas de disponibilidad a través de PowerShell.

Para obtener información sobre los hosts dedicados de Azure, consulte Hosts dedicados de Azure.

En la siguiente tabla se describen las distintas combinaciones de zona de disponibilidad y zona de grupo de hosts, y con cuáles se crea correctamente o falla la creación de un catálogo de máquinas.

| Zona de grupo de hosts | Zona de disponibilidad en la propiedad personalizada | Resultado de la creación del catálogo de máquinas |
|---|---|---|
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | No especificada | Correcto. Las máquinas se crean en la zona del grupo de hosts |
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | La misma zona que la del grupo de hosts. Por ejemplo, la zona de la propiedad personalizada se establece en 1 | Correcto. Las máquinas se crean en la Zona 1 |
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | Distinta de la zona del grupo de hosts. Por ejemplo, la zona de la propiedad personalizada se establece en 2 | Como la zona de disponibilidad especificada y la zona del grupo de hosts no coinciden, la creación del catálogo falla con un error relevante durante las comprobaciones previas |
| Especificada. Por ejemplo, el grupo de hosts está en la Zona 1 | Se especificaron varias zonas. Por ejemplo, las zonas de las propiedades personalizadas se establecen en 1,2 o 2,3 | Como la zona de disponibilidad especificada y la zona del grupo de hosts no coinciden, la creación del catálogo falla con un error relevante durante las comprobaciones previas |

| Zona de grupo de hosts | Zona de disponibilidad en la propiedad personalizada | Resultado de la creación del catálogo de máquinas |
|---|---|---|
| No especificada. Por ejemplo, la zona del grupo de hosts es <!JEKYLL@5180@100> | No especificada | Como la zona de disponibilidad especificada y la zona del grupo de hosts coinciden (es decir, no hay zona), la creación del catálogo se realiza correctamente. No se crean máquinas en ninguna zona |
| No especificada. Por ejemplo, la zona del grupo de hosts es <!JEKYLL@5180@101> | Especificada. Por ejemplo, las zonas de la propiedad personalizada se establecen en una o varias zonas | Como la zona de disponibilidad especificada y la zona del grupo de hosts no coinciden, la creación del catálogo falla con un error relevante durante las comprobaciones previas |

### Aprovisionar VM en hosts dedicados de Azure

Puede usar MCS para aprovisionar VM en los hosts dedicados de Azure. Antes de aprovisionar VM en hosts dedicados de Azure:

- Cree un grupo de hosts.
- Cree hosts en ese grupo de hosts.
- Compruebe que haya suficiente capacidad de host reservada para crear catálogos y máquinas virtuales.

Puede crear un catálogo de máquinas con arrendamiento de hosts definido a través del siguiente script de PowerShell:

<!JEKYLL@5180@102>

Cuando utilice MCS para aprovisionar máquinas virtuales en hosts dedicados de Azure, tenga en cuenta que:

- Un *host dedicado* es una propiedad del catálogo y no se puede cambiar una vez creado dicho catálogo. Actualmente, el arrendamiento dedicado no está disponible en Azure.
- Se requiere un grupo de hosts de Azure preconfigurado, en la región de la unidad de alojamiento, al utilizar el parámetro <!JEKYLL@5180@103>.
- Se requiere la ubicación automática de Azure. Esta funcionalidad realiza una solicitud para incorporar la suscripción asociada al grupo de hosts. Para obtener más información, consulte VM

Scale Set on Azure Dedicated Hosts - Public Preview. Si la ubicación automática no está habilitada, MCS genera un error durante la creación del catálogo.

### Configurar los tipos de almacenamiento

Seleccione distintos tipos de almacenamiento para máquinas virtuales en entornos Azure que utilizan MCS. Para las máquinas virtuales de destino, MCS admite:

- Disco de SO: SSD Premium, SSD o HDD
- Disco de memoria caché con escritura: SSD Premium, SSD o HDD

Al utilizar estos tipos de almacenamiento, tenga en cuenta lo siguiente:

- Asegúrese de que su máquina virtual sea compatible con el tipo de almacenamiento seleccionado.
- Si su configuración usa un disco efímero de Azure, no tiene la posibilidad de configurar el disco de caché de reescritura.

> **Sugerencia:**
>
> <!JEKYLL@5180@104> está configurado para un tipo de SO y una cuenta de almacenamiento. <!JEKYLL@5180@105> está configurado para el tipo de almacenamiento de memoria caché de escritura. Para un catálogo normal, se requiere <!JEKYLL@5180@106>. Si <!JEKYLL@5180@107> no está configurado, <!JEKYLL@5180@108> se utiliza como predeterminado para <!JEKYLL@5180@109>.

Si WBCDiskStorageType no está configurado, StorageType se utiliza como predeterminado para WBCDiskStorageType.

#### Configurar los tipos de almacenamiento de las máquinas virtuales

Para configurar los tipos de almacenamiento para VM, use el parámetro <!JEKYLL@5180@110> en <!JEKYLL@5180@111>. Para actualizar el valor del parámetro <!JEKYLL@5180@112> en un catálogo existente a uno de los tipos de almacenamiento compatibles, use el comando <!JEKYLL@5180@113>.

A continuación, se muestra un conjunto de ejemplo del parámetro <!JEKYLL@5180@114> en un esquema de aprovisionamiento:

<!JEKYLL@5180@115>

### Habilitar el almacenamiento con redundancia de zonas

Puede seleccionar almacenamiento con redundancia de zonas durante la creación de catálogos. Replica sincrónicamente su disco administrado de Azure en varias zonas de disponibilidad, lo que le permite recuperarse de un error en una zona al usar la redundancia en otras.

Puede especificar **Premium_ZRS** y **StandardSSD_ZRS** en las propiedades personalizadas del tipo de almacenamiento. El almacenamiento ZRS se puede configurar mediante propiedades personalizadas existentes o mediante la plantilla **MachineProfile**. El almacenamiento ZRS también está disponible con el comando <!JEKYLL@5180@116> mediante los parámetros <!JEKYLL@5180@117> y <!JEKYLL@5180@118>. Puede cambiar el almacenamiento de VM existente de LRS a ZRS.

> **Nota:**
>
> - <!JEKYLL@5180@119> indica que la hora de inicio programada es la hora actual.
> - <!JEKYLL@5180@120> con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

**Limitaciones:**

- Compatible solo para discos administrados
- Compatible únicamente con unidades de estado sólido (SSD) estándar y premium
- No es compatible con <!JEKYLL@5180@121>
- Disponible solo en determinadas regiones.
- El rendimiento de Azure disminuye al crear discos ZRS a escala. Por lo tanto, al encenderlas por primera vez, encienda las máquinas en lotes más pequeños (menos de 300 máquinas a la vez)

#### Definir el almacenamiento con redundancia de zonas como tipo de almacenamiento en disco

Puede seleccionar un almacenamiento con redundancia de zonas durante la creación de catálogos inicial o puede actualizar el tipo de almacenamiento en un catálogo existente.

#### Seleccionar el almacenamiento con redundancia de zonas mediante los comandos de PowerShell

Al crear un catálogo en Azure mediante el comando <!JEKYLL@5180@122> de PowerShell, use <!JEKYLL@5180@123> como valor en <!JEKYLL@5180@124>.
Por ejemplo:

<!JEKYLL@5180@125>

Al definir este valor, se valida mediante una API dinámica que determina si se puede utilizar correctamente. Se pueden producir estas excepciones si el uso de ZRS no es válido para su catálogo:

- **StorageTypeAtShutdownNotSupportedForZrsDisks**: La propiedad personalizada StorageTypeAtShutdown no se puede utilizar con el almacenamiento ZRS.
- **StorageAccountTypeNotSupportedInRegion**: Esta excepción se produce si intenta utilizar el almacenamiento ZRS en una región de Azure que no admite ZRS.
- **ZrsRequiresManagedDisks**: Solo puede utilizar el almacenamiento con redundancia de zonas con discos administrados.

Puede configurar el tipo de almacenamiento en disco mediante estas propiedades personalizadas:

- <!JEKYLL@5180@126>
- <!JEKYLL@5180@127>
- <!JEKYLL@5180@128>

> **Nota:**
>
> Durante la creación de catálogos, se utiliza el <!JEKYLL@5180@129> del disco del sistema operativo del perfil de máquina si las propiedades personalizadas no están configuradas.

## Capture la configuración de diagnóstico en máquinas virtuales y NIC desde un perfil de máquina

Puede capturar la configuración de diagnóstico de las máquinas virtuales y las NIC desde un perfil de máquina mientras crea un catálogo de máquinas, actualiza un catálogo de máquinas existente y actualiza las máquinas virtuales existentes.

Puede crear una máquina virtual o una especificación de plantilla como fuente del perfil de máquina.

### Pasos clave

1. Configure los ID necesarios en Azure. Debe proporcionar estos ID en la especificación de la plantilla.
    - Cuenta de almacenamiento
    - Espacio de trabajo de analíticas de registros
    - Espacio de nombres del centro de eventos con el precio del nivel estándar
2. Cree un origen de perfil de máquina.
3. Cree un nuevo catálogo de máquinas, actualice un catálogo existente o actualice las máquinas virtuales existentes.

### Configurar los ID necesarios en Azure

Configure una de las siguientes opciones en Azure:

- Cuenta de almacenamiento
- Espacio de trabajo de analíticas de registros
- Espacio de nombres del centro de eventos con el precio del nivel estándar

**Configurar una cuenta de almacenamiento** Cree una cuenta de almacenamiento estándar en Azure. En la especificación de la plantilla, indique el resourceId completo de la cuenta de almacenamiento como el <!JEKYLL@5180@130>.

Una vez que las máquinas virtuales estén configuradas para registrar los datos en la cuenta de almacenamiento, los datos se pueden encontrar en el contenedor <!JEKYLL@5180@131>.

**Configurar un espacio de trabajo de análisis de registros** Cree un espacio de trabajo de análisis de registros. En la especificación de la plantilla, indique el resourceId completo para el espacio de trabajo de análisis de registros como workspaceId.

Una vez que las máquinas virtuales estén configuradas para registrar datos en el espacio de trabajo, los datos se pueden consultar en Registros en Azure. Puede ejecutar el siguiente comando en Azure en Registros para mostrar un recuento de todas las métricas registradas por un recurso:

‘AzureMetrics

**Configurar un centro de eventos** Haga lo siguiente para configurar un centro de eventos en Azure Portal:

1. Crea un espacio de nombres para centros de eventos con los precios del nivel estándar.
2. Cree un centro de eventos debajo del espacio de nombres.
3. Vaya a **Capturar** en el centro de eventos. Encienda el interruptor para capturar con el tipo de salida Avro.
4. Cree un contenedor nuevo en una cuenta de almacenamiento existente para capturar los registros.
5. En la especificación de la plantilla, especifique el `eventHubAuthorizationRuleId` en el siguiente formato: `/subscriptions/093f4c12-704b-4b1d-8339-f339e7557f60/resourcegroups/matspo/providers/Microsoft.EventHub/namespaces/matspoeventhub/authorizationrules/RootManageSharedAccessKey`
6. Especifique el nombre del centro de eventos.

Una vez que las máquinas virtuales están configuradas para registrar datos en el centro de eventos, los datos se capturan en el contenedor de almacenamiento configurado.

### Crear una fuente de perfil de máquina

Puede crear una máquina virtual o una especificación de plantilla como fuente del perfil de máquina.

**Cree un perfil de máquina basado en máquinas virtuales con parámetros de diagnóstico** Si quiere crear una máquina virtual como perfil de máquina, primero configure los parámetros de diagnóstico en la propia máquina virtual de plantilla. Puede consultar las instrucciones detalladas que se proporcionan en la documentación de Microsoft Parámetros de diagnóstico en Azure Monitor.

Puede ejecutar los siguientes comandos para verificar que ahora hay una configuración de diagnóstico asociada a la máquina virtual o a la NIC:

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2659 --resource-type microsoft.network/
    networkInterfaces
<!--NeedCopy-->
```

```
az monitor diagnostic-settings list --resource-group matspo --resource
    matspo-tog-cc2 --resource-type microsoft.compute/virtualMachines
<!--NeedCopy-->
```

**Cree una plantilla de perfil de máquina basada en especificaciones con parámetros de diagnóstico** Si quiere usar una máquina virtual que ya tenga habilitada la configuración de diagnóstico y exportarla a una especificación de plantilla ARM, esta configuración no se incluirá automáticamente en la plantilla. Debe agregar o modificar manualmente la configuración de diagnóstico en la plantilla ARM.

Sin embargo, si quiere una máquina virtual como perfil de máquina, MCS se asegura de que la configuración de diagnóstico crítica se capture y aplique con precisión a los recursos de su catálogo de MCS.

1. Cree una especificación de plantilla estándar que defina una máquina virtual y tarjetas NIC.
2. Agregue recursos adicionales para implementar la configuración de diagnóstico de acuerdo con la especificación: Microsoft.Insights diagnosticSettings. Para conocer el ámbito, haga referencia a una máquina virtual o NIC que esté en la plantilla por su nombre con un identificador parcial. Por ejemplo, para crear una configuración de diagnóstico adjunta a una máquina virtual denominada Test-VM en la especificación de la plantilla, especifique el ámbito de la siguiente manera:

   ```
   "scope": "microsoft.compute/virtualMachines/test-VM",
   <!--NeedCopy-->
   ```

3. Use la especificación de la plantilla como fuente del perfil de máquina.

#### Crear o actualizar un catálogo con parámetros de diagnóstico

Después de crear un origen de perfiles de máquinas, ahora puede crear un catálogo de máquinas mediante un comando `New-ProvScheme`, actualizar un catálogo de máquinas existente mediante un comando `Set-ProvScheme` y actualizar las máquinas virtuales existentes mediante un comando `Request-ProvVMUpdate`.

### Verificar la licencia de Windows

Para comprobar que la máquina virtual aprovisionada aprovecha los beneficios de las licencias, ejecute este comando de PowerShell: `Get-AzVM -ResourceGroup MyResourceGroup -Name MyVM`.

- Para el tipo de licencia de Windows Server, compruebe que el tipo de licencia es **Windows_Server**. Encontrará instrucciones adicionales en https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing/.
- Para el tipo de licencia de cliente de Windows, compruebe que el tipo de licencia es **Windows_Client**. Encontrará instrucciones adicionales en https://docs.microsoft.com/en-us/azure/virtual-machines/windows/windows-desktop-multitenant-hosting-deployment/.

También puede usar el SDK de PowerShell `Get-Provscheme` para hacer la verificación. Por ejemplo: `Get-Provscheme -ProvisioningSchemeName "My Azure Catalog"`. Para obtener más información sobre este cmdlet, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Get-ProvScheme/.

### Configurar la licencia de Linux

Con las licencias de Linux de su propia suscripción (BYOS), no tiene que pagar por el software. El cargo de las licencias BYOS solo incluye la tarifa de hardware del procesamiento. Existen dos tipos de licencias:

- **RHEL_BYOS**: Para usar correctamente el tipo RHEL_BYOS, habilite Red Hat Cloud Access en su suscripción de Azure.
- **SLES_BYOS**: Las versiones de BYOS de SLES permiten el uso de SUSE.

Puede establecer el valor de LicenseType en opciones de Linux con `New-ProvScheme` y `Set-ProvScheme`.

Ejemplo de configuración de LicenseType en RHEL_BYOS con `New-ProvScheme`:

```
New-ProvScheme -CleanOnBoot -ProvisioningSchemeName "azureCatalog" -
    RunAsynchronously -Scope @() -SecurityGroup @() -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
    xsi:type="StringProperty" Name="LicenseType" Value="RHEL_BYOS" /></
    CustomProperties>'
<!--NeedCopy-->
```

Ejemplo de configuración de LicenseType en SLES_BYOS con `Set-ProvScheme`:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
     '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /><Property
    xsi:type="StringProperty" Name="LicenseType" Value="SLES_BYOS" /></
    CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Si el valor `LicenseType` está vacío, los valores predeterminados son Azure Windows Server License o Azure Linux License, según el valor de OsType.

Ejemplo de configuración de LicenseType vacío:

```
Set-ProvScheme -ProvisioningSchemeName "azureCatalog" -CustomProperties
     '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"><Property xsi:type="StringProperty" Name="UseManagedDisks"
     Value="true" /><Property xsi:type="StringProperty" Name="
    StorageAccountType" Value="StandardSSD_LRS" /><Property xsi:type="
    StringProperty" Name="ResourceGroups" Value="hu-dev-mcs" /><Property
     xsi:type="StringProperty" Name="OsType" Value="Linux" /></
    CustomProperties>'
<!--NeedCopy-->
```

### Crear un catálogo de máquinas con un disco efímero de Azure

Para aprovisionar discos de SO efímeros con `New-ProvScheme`, tenga en cuenta las siguientes restricciones:

- El tamaño de VM utilizado para el catálogo debe admitir discos de SO efímeros.
- El tamaño de la memoria caché o del disco temporal asociado al tamaño de la máquina virtual debe ser mayor o igual que el tamaño del disco del sistema operativo.
- El tamaño del disco temporal debe ser mayor que el tamaño del disco de la memoria caché.

Tenga en cuenta también estas restricciones al:

- Crear el esquema de aprovisionamiento
- Modificar el esquema de aprovisionamiento
- Actualizar la imagen

Para utilizar discos efímeros, debe establecer la propiedad personalizada `UseEphemeralOsDisk` en **true** al ejecutar `New-ProvScheme`.

> **Nota:**
>
> Si la propiedad personalizada `UseEphemeralOsDisk` se establece en **false** o no se especifica un valor, todos los VDA aprovisionados seguirán utilizando un disco de SO aprovisionado.

A continuación, se muestra un conjunto de ejemplo de propiedades personalizadas para uso en el esquema de aprovisionamiento:

```
"CustomProperties": [
            {

                "Name": "UseManagedDisks",
                "Value": "true"
             }
 ,
            {

                "Name": "StorageType",
                "Value": "Standard_LRS"
             }
 ,
            {

                "Name": "UseSharedImageGallery",
                "Value": "true"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaRatio",
                "Value": "40"
             }
 ,
            {

                "Name": "SharedImageGalleryReplicaMaximum",
```

```
                    "Value": "10"
                }
    ,
                {

                    "Name": "LicenseType",
                    "Value": "Windows_Server"
                }
    ,
                {

                    "Name": "UseEphemeralOsDisk",
                    "Value": "true"
                }

            ],
<!--NeedCopy-->
```

### Configurar un disco efímero para un catálogo existente

Para configurar un disco de SO efímero de Azure para un catálogo existente, utilice el parámetro `UseEphemeralOsDisk` de `Set-ProvScheme`. Establezca el valor del parámetro `UseEphemeralOsDisk` en **true**.

> **Nota:**
>
> Para utilizar esta función, también debe habilitar los parámetros `UseManagedDisks` y `UseSharedImageGallery`.

Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties <
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="UseSharedImageGallery" Value=
    "true" />
<Property xsi:type="StringProperty" Name="UseEphemeralOsDisk" Value="
    true" />
</CustomProperties>'
<!--NeedCopy-->
```

### Configurar Azure Compute Gallery

Utilice el comando `New-ProvScheme` para crear un esquema de aprovisionamiento que permita usar Azure Compute Gallery. Utilice el comando `Set-ProvScheme` para habilitar o inhabilitar esta

función en los esquemas de aprovisionamiento y para cambiar el índice de réplicas y los valores máximos de las réplicas.

Se agregaron tres propiedades personalizadas a los esquemas de aprovisionamiento para admitir la función Azure Compute Gallery:

`UseSharedImageGallery`

- Define si se debe usar Azure Compute Gallery para almacenar las imágenes publicadas. Si se establece en **True**, la imagen se almacena como una imagen de Azure Compute Gallery; de lo contrario, la imagen se almacena como una instantánea.
- Los valores válidos son **True** y **False**.
- Si la propiedad no está definida, el valor predeterminado es **False**.

`SharedImageGalleryReplicaRatio`

- Define el índice entre máquinas y réplicas de versiones de imágenes de la galería.
- Los valores válidos son números enteros mayores que 0.
- Si la propiedad no está definida, se utilizan los valores predeterminados. El valor predeterminado para los discos de SO persistentes es 1000, y el valor predeterminado para los discos de SO no persistentes es 40.

`SharedImageGalleryReplicaMaximum`

- Define el máximo de réplicas para cada versión de imagen de la galería.
- Los valores válidos son números enteros mayores que 0.
- Si la propiedad no está definida, el valor predeterminado es 10.
- Azure admite actualmente hasta 10 réplicas por versión de imagen de la galería. Si la propiedad se establece en un valor mayor que el admitido por Azure, MCS intenta utilizar el valor especificado. Azure genera un error, el cual MCS registra. Luego, MCS deja el recuento de réplicas actual sin cambiar.

> **Sugerencia:**
>
> Al utilizar Azure Compute Gallery para almacenar una imagen publicada de catálogos aprovisionados con MCS, MCS establece el recuento de réplicas de versiones de imágenes de la galería en función de la cantidad de máquinas del catálogo, el índice de réplicas y el máximo de réplicas. El recuento de réplicas se calcula al dividir la cantidad de máquinas del catálogo entre el índice de réplicas (se redondea al valor entero más cercano). A continuación, se limita el valor al recuento máximo de réplicas. Por ejemplo, con un índice de réplicas de 20 y un máximo de 5, entre 0 y 20 máquinas tienen una réplica creada, entre 21 y 40 tienen 2 réplicas, entre 41 y 60 tienen 3 réplicas, entre 61 y 80 tienen 4 réplicas, y más de 81 tienen 5 réplicas.

**Caso de uso: Actualizar el índice de réplicas y el máximo de réplicas de Azure Compute Gallery**

El catálogo de máquinas existente usa Azure Compute Gallery. Utilice el comando `Set-ProvScheme` para actualizar las propiedades personalizadas de todas las máquinas existentes del catálogo y de futuras máquinas:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

**Caso de uso: Convertir un catálogo de instantáneas en un catálogo de Azure Compute Gallery**

Para este caso de uso:

1. Ejecute `Set-ProvScheme` con el indicador `UseSharedImageGallery` establecido en **True**. Si quiere, incluya las propiedades `SharedImageGalleryReplicaRatio` y `SharedImageGalleryReplicaMaximum`.
2. Actualice el catálogo.
3. Apague y encienda las máquinas para forzar una actualización.

Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
    <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance"> <Property xsi:type="StringProperty" Name="StorageType"
    Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
    UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
    Name="UseSharedImageGallery" Value="True"/> <Property xsi:type="
    IntProperty" Name="SharedImageGalleryReplicaRatio" Value="30"/> <
    Property xsi:type="IntProperty" Name="
    SharedImageGalleryReplicaMaximum" Value="20"/></CustomProperties>'
<!--NeedCopy-->
```

> **Sugerencia:**
>
> Los parámetros `SharedImageGalleryReplicaRatio` y `SharedImageGalleryReplicaMaximum` no son necesarios. Una vez completado el comando `Set-ProvScheme`, aún no se ha creado la imagen de Azure Compute Gallery. Una vez configurado el catálogo para utilizar la galería,

> la siguiente operación de actualización del catálogo almacena la imagen publicada en la galería. El comando de actualización del catálogo crea la galería, la imagen de la galería y la versión de la imagen. Apagar y encender las máquinas las actualiza, momento en el que se actualiza el recuento de réplicas, si procede. A partir de ese momento, todas las máquinas no persistentes existentes se restablecen mediante la imagen de Azure Compute Gallery, y todas las máquinas recién aprovisionadas se crean mediante la imagen. La antigua instantánea se borra automáticamente en unas horas.

**Caso de uso: Convertir un catálogo de Azure Compute Gallery en un catálogo de instantáneas**

Para este caso de uso:

1. Ejecute `Set-ProvScheme` con el indicador `UseSharedImageGallery` establecido en **False** o sin definir.
2. Actualice el catálogo.
3. Apague y encienda las máquinas para forzar una actualización.

Por ejemplo:

```
1 Set-ProvScheme -ProvisioningSchemeName catalog-name -CustomProperties '
     <CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
     machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
     instance"> <Property xsi:type="StringProperty" Name="StorageType"
     Value="Standard_LRS"/> <Property xsi:type="StringProperty" Name="
     UseManagedDisks" Value="True"/> <Property xsi:type="StringProperty"
     Name="UseSharedImageGallery" Value="False"/></CustomProperties>'
2 <!--NeedCopy-->
```

> **Sugerencia:**
>
> A diferencia de actualizar una instantánea a un catálogo de Azure Compute Gallery, los datos personalizados de cada máquina aún no se actualizan para reflejar las nuevas propiedades personalizadas. Ejecute el siguiente comando para ver las propiedades personalizadas originales de Azure Compute Gallery: `Get-ProvVm -ProvisioningSchemeName catalog-name`. Una vez finalizado el comando `Set-ProvScheme`, aún no se ha creado la instantánea de la imagen publicada. Una vez configurado el catálogo para que no utilice la galería, la siguiente operación de actualización del catálogo almacena la imagen publicada como una instantánea. A partir de ese momento, todas las máquinas no persistentes existentes se restablecen mediante la instantánea, y todas las máquinas recién aprovisionadas se crean a partir de la instantánea. Apagar y encender las máquinas las actualiza, momento en el que los datos personalizados de las máquinas se actualizan para reflejar que `UseSharedImageGallery` está establecido en **False**. Los antiguos elementos de Azure Compute Gallery (la galería, la imagen y la versión) se borran automáticamente en unas horas.

### Crear o actualizar un catálogo con varias NIC por máquina virtual

MCS admite varias NIC por máquina virtual. Puede asociar varias NIC de una máquina virtual a varias subredes. Sin embargo, esas subredes deben estar en la misma red virtual (VNet). Puede usar los comandos de PowerShell para:

- Crear un catálogo con varias NIC en una máquina virtual
- Actualizar la configuración de un catálogo existente para tener varias NIC en una máquina virtual, de modo que las máquinas virtuales recién creadas tengan varias NIC
- Actualizar una máquina virtual existente para que tenga varias NIC

Puede crear o actualizar un catálogo de máquinas no basado en perfiles de máquina y un catálogo de máquinas basado en perfiles de máquina para tener varias NIC en una máquina virtual. Actualmente, para un catálogo de máquinas basado en perfiles de máquina, solo puede tener la misma cantidad de NIC que la especificada en el origen del perfil de máquina.

Las propiedades como las redes aceleradas y el grupo de seguridad de red se derivan del origen del perfil de la máquina.

> **Nota:**
>
> El tamaño de la máquina virtual debe admitir la misma cantidad de NIC y las redes aceleradas correspondientes. De lo contrario, se producirá un error.

Puede obtener la cantidad máxima de NIC asociadas a un tamaño de máquina virtual seleccionado. Una propiedad de PowerShell denominada `MaxNetworkInterfaces` muestra el recuento máximo de NIC al ejecutar el comando `get-item` de PowerShell con el parámetro `AdditionalData` .

#### Obtener el recuento máximo de NIC

Para obtener el recuento máximo de NIC:

1. Abra una ventana de **PowerShell** desde el host del Delivery Controller.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute `Get-ChildItem -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder"` para enumerar todos los tamaños de máquinas virtuales disponibles.
4. Ejecute `get-item -Path "XDHyp:\Connections\abc-connection\East US.region\serviceoffering.folder\Standard_M416ms_v2.serviceoffering").AdditionalData`
5. Compruebe `MaxNetworkInterfaces` para saber el máximo de NIC.

### Crear un catálogo con varias NIC en una máquina virtual

Para crear un catálogo con varias NIC en una máquina virtual, haga lo siguiente:

1. Abra una ventana de PowerShell desde el host del Delivery Controller.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Cree un grupo de identidades si aún no se ha creado.
4. Cree el esquema de aprovisionamiento.
    - Si crea un catálogo de máquinas no basado en perfiles de máquinas, ejecute el comando `New-ProvScheme` con el parámetro `NetworkMappings`. Puede agregar varias subredes al parámetro `NetworkMappings`. Por ejemplo:

      ```
      New-Provscheme -NetworkMappings @{
      "0"="subnetpath1";"1"="subnetpath1" }

      <!--NeedCopy-->
      ```

    - Si crea un catálogo de máquinas basado en perfiles de máquinas:
        a) Cree una máquina virtual en Azure para tener varias NIC. Para obtener información, consulte Crear y administrar una máquina virtual con Windows que tiene varias NIC. También puede crear otra máquina virtual y, a continuación, conectar una interfaz de red en la página Redes de Azure Portal.
        b) Ejecute el comando `New-ProvScheme` con la máquina virtual como entrada de perfil de máquina.

      > **Nota:**
      >
      > Al crear un catálogo de máquinas basado en perfiles de máquina, el recuento de `NetworkMappings` debe ser el mismo que el recuento de `NetworkInterfaceCount` del perfil de máquina. `NetworkInterfaceCount` puede obtenerse de `AdditionalData` de `Get-item -Path "machine profile path"`.

5. Termine de crear el catálogo.

### Actualizar un catálogo para tener varias NIC en una máquina virtual

Para actualizar un catálogo de modo que tenga varias NIC en una máquina virtual, haga lo siguiente:

1. Abra una ventana de **PowerShell** desde el host del Delivery Controller.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Actualice el esquema de aprovisionamiento:
    - Si crea un catálogo de máquinas no basado en perfiles de máquinas, ejecute el comando `Set-ProvScheme` con el parámetro `NetworkMappings`. Puede agregar varias subredes al parámetro `NetworkMappings`. Por ejemplo:

```
Set-Provscheme -NetworkMappings @{
"0"="subnetpath1";"1"="subnetpath1" }

<!--NeedCopy-->
```

- Si crea un catálogo de máquinas basado en un perfil de máquina:

  a) Cree una máquina virtual en Azure para tener varias NIC. Para obtener información, consulte Crear y administrar una máquina virtual con Windows que tiene varias NIC.
  b) Ejecute el comando `Set-ProvScheme` con la máquina virtual como entrada de perfil de máquina.

#### Actualizar una máquina virtual existente para tener varias NIC en una máquina virtual

También puede actualizar una máquina virtual existente mediante `Set-ProvVMUpdateTimeWindow` y llevar a cabo un ciclo de energía en la máquina virtual existente durante el período de actualización. Para obtener más información sobre cómo actualizar una VM existente, consulte Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento.

### Crear un catálogo de máquinas con un disco no persistente de caché con reescritura

Para configurar un catálogo con disco no persistente de caché con reescritura, utilice el parámetro de PowerShell `New-ProvScheme CustomProperties`. Las propiedades personalizadas son:

- `UseTempDiskForWBC`. Esta propiedad indica si acepta usar el almacenamiento temporal de Azure para almacenar el archivo de caché con reescritura. Esto debe establecerse en "true" cuando se ejecuta `New-ProvScheme` si quiere usar el disco temporal como disco de caché con reescritura. Si no se especifica esta propiedad, el parámetro se establece en false de forma predeterminada.

Por ejemplo, así se usa el parámetro `CustomProperties` para configurar `UseTempDiskForWBC` en "true":

```
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.
    com/2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
    XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="
    false"/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false
    "/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value
    ="Premium_LRS"/> `
```

```
    <Property xsi:type="StringProperty" Name="WBCDiskStorageType" Value
       ="Premium_LRS"/> `
    <Property xsi:type="StringProperty" Name="LicenseType" Value="
       Windows_Client"/> `
    <Property xsi:type="StringProperty" Name="UseTempDiskForWBC" Value
       ="true"/> `
    </CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Después de confirmar que el catálogo de máquinas use el almacenamiento temporal local de Azure para el archivo de caché con reescritura, no se puede cambiar para que use VHD más adelante.

### Crear un catálogo de máquinas con un disco persistente de caché con reescritura

Para configurar un catálogo con disco persistente de caché de reescritura, use el parámetro `New-ProvScheme CustomProperties` de PowerShell.

> **Sugerencia:**
>
> Use el parámetro de PowerShell `New-ProvScheme CustomProperties` solo para conexiones de alojamiento basadas en la nube. Si quiere aprovisionar máquinas con un disco persistente de caché con reescritura para una solución local (por ejemplo, XenServer), PowerShell no es necesario porque el disco conserva automáticamente los datos.

Este parámetro ofrece una propiedad adicional, `PersistWBC`, que se utiliza para determinar cómo el disco de caché con reescritura persiste en máquinas aprovisionadas con MCS. La propiedad `PersistWBC` solo se utiliza cuando se especifica el parámetro `UseWriteBackCache` y cuando se establece el parámetro `WriteBackCacheDiskSize` para indicar que se ha creado un disco.

> **Nota:**
>
> Este comportamiento se aplica tanto a Azure como a GCP, donde los datos del disco de caché con reescritura predeterminado de E/S de MCS se eliminan y se vuelven a crear cuando se apaga o se enciende la máquina. Puede optar por conservar los datos del disco para evitar la eliminación y la recreación de los datos del disco caché con reescritura de E/S de MCS.

He aquí unos cuantos ejemplos de propiedades que se encuentran en el parámetro `CustomProperties` antes de optar por la propiedad `PersistWBC`:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
```

```
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
</CustomProperties>
<!--NeedCopy-->
```

> **Nota:**
>
> Este ejemplo solo se aplica a Azure. Las propiedades son diferentes en el entorno de GCP.

Al utilizar estas propiedades, tenga en cuenta que contienen valores predeterminados si las propiedades se omiten del parámetro `CustomProperties`. La propiedad `PersistWBC` tiene dos valores posibles: **true** o **false**.

Cuando la propiedad `PersistWBC` es **true**, el disco de caché con reescritura no se elimina cuando el administrador de Citrix DaaS apaga la máquina desde la interfaz de administración.

Cuando la propiedad `PersistWBC` es **false**, el disco de caché con reescritura se elimina cuando el administrador de Citrix DaaS apaga la máquina desde la interfaz de administración.

> **Nota:**
>
> Si se omite la propiedad `PersistWBC`, su valor predeterminado es **false**, y la memoria caché de reescritura se elimina cuando la máquina se apaga desde la interfaz de administración.

Por ejemplo, así se usa el parámetro `CustomProperties` para configurar `PersistWBC` en “true” :

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="true" />
</CustomProperties>
<!--NeedCopy-->
```

> **Importante:**
>
> La propiedad `PersistWBC` solo se puede configurar mediante el cmdlet de PowerShell `New-ProvScheme`. Si se intenta modificar `CustomProperties` de un esquema de aprovisionamiento después de la creación, esto no afecta al catálogo de máquinas ni a la persistencia del disco de caché con reescritura cuando se apaga una máquina.

Por ejemplo, configure `New-ProvScheme` para utilizar la memoria caché de reescritura mientras configura la propiedad `PersistWBC` en "true":

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`" Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"benvaldev5RG3`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"true`" />
</CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\GoldImages.resourcegroup\W10MCSIO-01_OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\CloudScale02.resourcegroup\adVNET.virtualprivatecloud\adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Mejorar el rendimiento del arranque con E/S de MCS

Puede mejorar el rendimiento de arranque de los discos administrados de Azure y GCP cuando E/S de MCS está habilitada. Utilice la propiedad personalizada `PersistOSDisk` de PowerShell en el comando `New-ProvScheme` para configurar esta función. Las opciones asociadas a `New-ProvScheme` son:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="Premium_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="
```

```
    benvaldev5RG3" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
    />
</CustomProperties>
<!--NeedCopy-->
```

Para habilitar esta función, establezca la propiedad personalizada `PersistOSDisk` en **true**. Por ejemplo:

```
New-ProvScheme
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
    /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
    XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
    UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
    StringProperty`" Name=`"StorageAccountType`" Value=`"Premium_LRS`"
    /><Property xsi:type=`"StringProperty`" Name=`"ResourceGroups`"
    Value=`"benvaldev5RG3`" /><Property xsi:type=`"StringProperty`" Name
    =`"PersistOsDisk`" Value=`"true`" /></CustomProperties>"
-HostingUnitName "adSubnetScale1"
-IdentityPoolName "BV-WBC1-CAT1"
-MasterImageVM "XDHyp:\HostingUnits\adSubnetScale1\image.folder\
    GoldImages.resourcegroup\W10MCSIO-01
    _OsDisk_1_a940e6f5bab349019d57ccef65d2c7e3.manageddisk"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\adSubnetScale1\virtualprivatecloud.folder\
     CloudScale02.resourcegroup\adVNET.virtualprivatecloud\
     adSubnetScale1.network" }

-ProvisioningSchemeName "BV-WBC1-CAT1"
-ServiceOffering "XDHyp:\HostingUnits\adSubnetScale1\serviceoffering.
    folder\Standard_D2s_v3.serviceoffering"
-UseWriteBackCache
-WriteBackCacheDiskSize 127
-WriteBackCacheMemorySize 256
<!--NeedCopy-->
```

### Crear un catálogo de máquinas con una clave de cifrado administrada por el cliente

Si quiere crear un catálogo de máquinas mediante los comandos de PowerShell, donde la clave de cifrado sea una clave administrada por el cliente, haga lo siguiente:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Escriba `cd xdhyp:/`.
4. Escriba `cd .\HostingUnits\(your hosting unit)`.
5. Escriba cd diskencryptionset.folder.

6. Escriba dir para obtener la lista de conjuntos de cifrado de disco.
7. Copie el ID de un conjunto de cifrado de disco.
8. Cree una cadena de propiedades personalizada para incluir el ID del conjunto de cifrado de disco. Por ejemplo:

```
$customProperties = "<CustomProperties xmlns=`"http://schemas.
    citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.
    org/2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"persistWBC`" Value=`"
    False`" />
<Property xsi:type=`"StringProperty`" Name=`"PersistOsDisk`" Value
    =`"false`" />
<Property xsi:type=`"StringProperty`" Name=`"UseManagedDisks`"
    Value=`"true`" />
<Property xsi:type=`"StringProperty`" Name=`"DiskEncryptionSetId`"
     Value=`"/subscriptions/0xxx4xxx-xxb-4bxx-xxxx-xxxxxxxx/
    resourceGroups/abc/providers/Microsoft.Compute/
    diskEncryptionSets/abc-des`"/>
</CustomProperties>
<!--NeedCopy-->
```

9. Cree un grupo de identidades si aún no se ha creado. Por ejemplo:

```
New-AcctIdentityPool -IdentityPoolName idPool -NamingScheme ms## -
    Domain def.local -NamingSchemeType Numeric
<!--NeedCopy-->
```

10. Ejecute el comando New-ProvScheme. Por ejemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "name" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\azure-res2\image.folder\def.
    resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\azure-res2\virtualprivatecloud.folder\
     def.resourcegroup\def-vnet.virtualprivatecloud\subnet1.network
     " }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\azure-res2\serviceoffering.
    folder\Standard_DS2_v2.serviceoffering"
-MachineProfile "XDHyp:\HostingUnits<adnet>\machineprofile.folder<
    def.resourcegroup><machine profile vm.vm>"
-CustomProperties $customProperties
<!--NeedCopy-->
```

11. Termine de crear el catálogo de máquinas.

### Crear un catálogo de máquinas con capacidad de cifrado en el host

Para crear un catálogo de máquinas con capacidad de cifrado en el host

1. Compruebe si la suscripción tiene habilitada la funcionalidad de cifrado en el host o no. Para ello, consulte https://learn.microsoft.com/en-us/rest/api/resources/features/get?tabs=HTTP/. Si no está habilitada, debe habilitar la funcionalidad para la suscripción. Para obtener información sobre cómo habilitar la funcionalidad para su suscripción, consulte https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-host-based-encryption-portal?tabs=azure-powershell#prerequisites/.

2. Compruebe si un tamaño de máquina virtual de Azure determinado admite el cifrado en el host o no. Para ello, en una ventana de PowerShell, ejecute uno de los siguientes comandos:

```
PS XDHyp:\Connections<your connection>\east us.region\
   serviceoffering.folder>
<!--NeedCopy-->
```

```
PS XDHyp:\HostingUnits<your hosting unit>\serviceoffering.folder>
<!--NeedCopy-->
```

3. Cree una máquina virtual o una especificación de plantilla, como entrada para el perfil de máquina, en Azure Portal con el cifrado en el host habilitado.

   - Si quiere crear una máquina virtual, seleccione un tamaño de máquina virtual que admita el cifrado en el host. Tras crear la máquina virtual, se habilita la propiedad **Encryption at host** (Cifrado en el host).
   - Si quiere utilizar una especificación de plantilla, asigne al parámetro `Encryption at Host` el valor **true** en `securityProfile`.

4. Cree un catálogo de máquinas de MCS con un flujo de trabajo de perfil de máquina. Para ello, seleccione una máquina virtual o una especificación de plantilla.

   - Disco del sistema operativo/disco de datos: Se cifra mediante una clave gestionada por el cliente y una clave gestionada por la plataforma
   - Disco de SO efímero: Se cifra solo mediante una clave administrada por la plataforma
   - Disco de caché: Se cifra mediante una clave administrada por el cliente y una clave administrada por la plataforma

   Puede crear el catálogo de máquinas a través de la interfaz de Configuración completa o ejecutando los comandos de PowerShell.

#### Obtener la información de cifrado en el host desde un perfil de máquina

Puede recuperar la información de cifrado en el host desde un perfil de máquina al ejecutar el comando de PowerShell con el parámetro `AdditionalData`. Si el parámetro `EncryptionAtHost` es **True**, indica que el cifrado en el host está habilitado para el perfil de máquina.

Por ejemplo: Cuando la entrada del perfil de máquina sea una VM, ejecute el siguiente comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def.vm).AdditionalData
<!--NeedCopy-->
```

Por ejemplo: Cuando la entrada del perfil de máquina sea una especificación de plantilla, ejecute el siguiente comando:

```
(get-item XDHyp:\HostingUnits\myAzureNetwork\machineprofile.folder\abc.
   resourcegroup\def_templatespec.templatespec\EncryptionAtHost.
   templatespecversion).AdditionalData
<!--NeedCopy-->
```

### Crear un catálogo de máquinas con doble cifrado

Puede crear y actualizar un catálogo de máquinas con doble cifrado mediante la interfaz de Configuración completa y los comandos de PowerShell.

Los pasos detallados para crear un catálogo de máquinas con doble cifrado son:

1. Cree un Azure Key Vault y un DES con claves administradas por la plataforma y por el cliente. Para obtener información sobre cómo crear un Azure Key Vault y un DES, consulte Uso de Azure Portal para habilitar el cifrado doble en reposo para discos administrados.
2. Para buscar conjuntos de cifrado de disco disponibles en su conexión de host:
   a) Abra una ventana de **PowerShell**.
   b) Ejecute los siguientes comandos de PowerShell:
      i. `asnp citrix*`
      ii. `cd xdhyp:`
      iii. `cd HostingUnits`
      iv. `cd YourHostingUnitName (ex. azure-east)`
      v. `cd diskencryptionset.folder`
      vi. `dir`

   Puede usar un ID del `DiskEncryptionSet` para crear o actualizar un catálogo mediante propiedades personalizadas.

3. Si quiere utilizar el flujo de trabajo del perfil de máquina, cree una especificación de máquina virtual o plantilla como entrada de perfil de máquina.

   - Si quiere utilizar una máquina virtual como entrada de perfil de máquina:
     a) Cree una máquina virtual en Azure Portal.
     b) Vaya a **Disks > Key Management** para cifrar la máquina virtual directamente con cualquier otro `DiskEncryptionSetID`.
   - Si quiere utilizar una especificación de plantilla como entrada de perfil de máquina:
     a) En la plantilla, en `properties>storageProfile>osDisk>managedDisk`, agregue el parámetro `diskEncryptionSet` y agregue el ID del DES de doble cifrado.

4. Cree el catálogo de máquinas

   - Si usa la interfaz de Configuración completa, realice una de estas acciones, además de seguir los pasos que se indican en Crear catálogos de máquinas.
     - Si no utiliza un flujo de trabajo basado en perfiles de máquina, en la página **Parámetros de disco**, seleccione **Utilice esta clave para cifrar datos en cada máquina**. A continuación, seleccione su DES de doble cifrado en la lista desplegable. Siga con la creación del catálogo.
     - Si utiliza un flujo de trabajo de perfil de máquina, en la página **Imagen**, seleccione una imagen maestra (o imagen preparada) y un perfil de máquina. Asegúrese de que el perfil de la máquina tenga un ID de conjunto de cifrado de disco en sus propiedades.

     Todas las máquinas creadas en el catálogo se cifran con doble cifrado mediante la clave asociada al DES que haya seleccionado.
   - Si usa comandos de PowerShell, realice una de estas acciones:
     - Si no utiliza un flujo de trabajo basado en perfiles de máquina, agregue la propiedad personalizada `DiskEncryptionSetId` en el comando `New-ProvScheme`. Por ejemplo:

```
1  New-ProvScheme -CleanOnBoot -CustomProperties '<
       CustomProperties xmlns="http://schemas.citrix.com/2014/
       xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/
       XMLSchema-instance">
2  <Property xsi:type="StringProperty" Name="UseManagedDisks"
        Value="true" />
3  <Property xsi:type="StringProperty" Name="
       StorageAccountType" Value="Premium_LRS" />
4  <Property xsi:type="StringProperty" Name="
       DiskEncryptionSetId" Value="/subscriptions/12345678-
       xxxx-1234-1234-123456789012/resourceGroups/Sample-RG/
       providers/Microsoft.Compute/diskEncryptionSets/
       SampleEncryptionSet" />
```

```
5   </CustomProperties>'
6   -HostingUnitName "Redacted"
7   -IdentityPoolName "Redacted"
8   -InitialBatchSizeHint 1
9   -MasterImageVM "Redacted"
10  -NetworkMapping @{
11  "0"="Redacted" }
12
13  -ProvisioningSchemeName "Redacted"
14  -ServiceOffering "Redacted"
15  <!--NeedCopy-->
```

- Si utiliza un flujo de trabajo basado en perfiles de máquina, utilice una entrada de perfil de máquina en el comando `New-ProvScheme`. Por ejemplo:

```
1   New-ProvScheme -CleanOnBoot
2   -HostingUnitName azure-east
3   -IdentityPoolName aio-ip
4   -InitialBatchSizeHint 1
5   -MasterImageVM XDHyp:\HostingUnits\azure-east\image.folder
       \abc.resourcegroup\fgb-vda-snapshot.snapshot
6   -NetworkMapping @{
7   "0"="XDHyp:\HostingUnits\azure-east\virtualprivatecloud.
       folder\apa-resourceGroup.resourcegroup\apa-
       resourceGroup-vnet.virtualprivatecloud\default.network"
        }
8
9   -ProvisioningSchemeName aio-test
10  -MachineProfile XDHyp:\HostingUnits\azure-east\
       machineprofile.folder\abc.resourcegroup\abx-mp.
       templatespec\1.0.0.templatespecversion
11  <!--NeedCopy-->
```

Termine de crear un catálogo mediante el SDK de PowerShell remoto. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/. Todas las máquinas creadas en el catálogo se cifran con doble cifrado mediante la clave asociada al DES que haya seleccionado.

#### Convertir un catálogo sin cifrar para usar el cifrado doble

Puede actualizar el tipo de cifrado de un catálogo de máquinas (mediante propiedades personalizadas o un perfil de la máquina).

- Si no utiliza un flujo de trabajo basado en perfiles de máquina, agregue la propiedad personalizada DiskEncryptionSetId en el comando `Set-ProvScheme`. Por ejemplo:

```
1   Set-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
```

```
-CustomProperties '<CustomProperties xmlns="http://schemas.citrix
    .com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org
    /2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/12345678-xxxx-1234-1234-123456789012/
    resourceGroups/Sample-RG/providers/Microsoft.Compute/
    diskEncryptionSets/SampleEncryptionSet" />
</CustomProperties>'
<!--NeedCopy-->
```

- Si utiliza un flujo de trabajo basado en perfiles de máquina, utilice una entrada de perfil de máquina en el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName mxiao-test -MachineProfile
    XDHyp:\HostingUnits\azure-east\machineprofile.folder\aelx.
    resourcegroup\elx-mp.templatespec\1.0.0.templatespecversion
<!--NeedCopy-->
```

Cuando se haya completado correctamente, todas las máquinas virtuales nuevas que agregue al catálogo se cifrarán con cifrado doble con la clave asociada al DES que haya seleccionado.

#### Verificar que el catálogo tenga un cifrado doble

- En la interfaz de Configuración completa:
  1. Vaya a **Catálogos de máquinas**.
  2. Seleccione el catálogo que quiere verificar. Haga clic en la ficha **Propiedades de plantilla** situada cerca de la parte inferior de la pantalla.
  3. En **Detalles de Azure**, verifique el ID del conjunto de cifrado de disco en **Conjunto de cifrado de disco**. Si el ID del DES del catálogo está vacío, el catálogo no está cifrado.
  4. En Azure Portal, compruebe que el tipo de cifrado del DES asociado al ID del DES sean claves administradas por la plataforma y por el cliente.
- Usar el comando de PowerShell:
  1. Abra la ventana de **PowerShell**.
  2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
  3. Use `Get-ProvScheme` para obtener la información de su catálogo de máquinas. Por ejemplo:

     ```
     Get-ProvScheme -ProvisioningSchemeName "SampleProvSchemeName"
     <!--NeedCopy-->
     ```

  4. Obtenga la propiedad personalizada del ID del DES del catálogo de máquinas. Por ejemplo:

```
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
     Value="/subscriptions
    /12345678-1234-1234-1234-123456789012/resourceGroups/Sample
    -RG/providers/Microsoft.Compute/diskEncryptionSets/
    SampleEncryptionSet" />
<!--NeedCopy-->
```

5. En Azure Portal, compruebe que el tipo de cifrado del DES asociado al ID del DES sean claves administradas por la plataforma y por el cliente.

### Determinación de la ubicación del archivo de paginación

La ubicación del archivo de paginación se determina según el siguiente supuesto:

> **Nota:**
>
> La ubicación predeterminada del archivo de paginación está en el disco del SO.

| Caso | Ubicación |
|---|---|
| La configuración del archivo de paginación se especifica en las propiedades personalizadas | Según se especifica en las propiedades personalizadas |
| El disco de SO efímero o la hibernación están habilitados | Disco de SO |
| La máquina virtual tiene un disco temporal | Disco temporal |
| E/S de MCS está habilitada | Disco WBC |

### Casos de configuración de archivos de paginación

En esta tabla se describen algunos casos posibles de configuración de archivos de paginación durante la preparación de imágenes y la actualización del esquema de aprovisionamiento:

| Durante | Caso | Resultado |
| --- | --- | --- |
| Preparación de imágenes | El archivo de paginación de la imagen de origen se establece en el disco temporal, mientras que el tamaño de la máquina virtual que especifique en el esquema de aprovisionamiento no tiene disco temporal | El archivo de paginación se coloca en el SO |
| Preparación de imágenes | El archivo de paginación de la imagen de origen se establece en el disco de SO, mientras que el tamaño de la máquina virtual que se especifica en el esquema de aprovisionamiento tiene un disco temporal | El archivo de paginación se coloca en el disco temporal |
| Preparación de imágenes | Establezca el archivo de paginación de la imagen de origen en el disco temporal y habilite el disco de SO efímero en el esquema de aprovisionamiento. | El archivo de paginación se coloca en el disco del sistema operativo |
| Actualización del esquema de aprovisionamiento | Intenta actualizar el esquema de aprovisionamiento cuando la versión del VDA es anterior a la 2311 | Modifica la configuración del archivo de paginación con una advertencia |
| Actualización del esquema de aprovisionamiento | Intenta actualizar el esquema de aprovisionamiento cuando la versión del VDA es 2311 o posterior | Determina la ubicación del archivo de paginación según la determinación de la ubicación del archivo de paginación |

### Especificar los parámetros del archivo de páginación

Con los comandos de PowerShell, puede especificar los parámetros del archivo de paginación, incluidos la ubicación y el tamaño. Esto supedita los parámetros del archivo de paginación determinados por MCS según la determinación de la ubicación del archivo de paginación. Para ello, ejecute este comando `New-ProvScheme` durante la creación del catálogo de máquinas.

### Consideraciones importantes

Tenga en cuenta lo siguiente antes de continuar con la creación del catálogo:

- Debe proporcionar todas las propiedades personalizadas (“PageFileDiskDriveLetterOverride” , “InitialPageFileSizeInMB”y “MaxPageFileSizeInMB”) en el comando `New-ProvScheme` o ninguna de ellas.
- Esta función no está disponible a través de Citrix Studio.
- El tamaño del archivo de paginación inicial debe estar entre 16 MB y 16777216 MB.
- El tamaño del archivo de paginación máximo debe ser superior o igual al tamaño del archivo de paginación inicial e inferior a 16777216 MB.
- Puede establecer el tamaño inicial del archivo de paginación y el tamaño máximo del archivo de paginación en cero al mismo tiempo.

> **Nota:**
>
> Puede modificar los parámetros del archivo de paginación de las máquinas virtuales recién agregadas de un catálogo existente sin actualizar la imagen maestra. Para modificar los parámetros del archivo de paginación, necesita la versión 2311 o posterior del VDA. Puede modificar los parámetros del archivo de paginación mediante los comandos de PowerShell. Para obtener más información, consulte Modificar los parámetros del archivo de paginación.

```
New-ProvScheme -CleanOnBoot `
-HostingUnitName "zijinnet" `
-IdentityPoolName "PageFileSettingExample" `
-ProvisioningSchemeName "PageFileSettingExample" `
-InitialBatchSizeHint 1 `
-MasterImageVM "XDHyp:\HostingUnits\zijinnet\image.folder\neal-
   zijincloud-resources.resourcegroup\
   CustomWin10VDA_OsDisk_1_9473d7c8a6174b2c8284c7d3efeea88f.manageddisk
   " `
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\zijinnet\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\neal-zijincloud-resources.
    resourcegroup\neal-zijincloud-resources-vnet.virtualprivatecloud\
    default.network" }
  `
-ServiceOffering "XDHyp:\HostingUnits\zijinnet\serviceoffering.folder\
   Standard_B2ms.serviceoffering" `
-CustomProperties '<CustomProperties xmlns=" http://schemas.citrix.com
   /2014/xd/machinecreation" xmlns:xsi=" http://www.w3.org/2001/
   XMLSchema-instance"> `
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="false
   "/> `
<Property xsi:type="StringProperty" Name="PersistVm" Value="false"/> `
<Property xsi:type="StringProperty" Name="
   PageFileDiskDriveLetterOverride" Value="d"/> `
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
   Value="2048"/> `
```

```
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196"/> `
<Property xsi:type="StringProperty" Name="StorageAccountType" Value="
    Premium_LRS"/> `
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client"/> `
</CustomProperties>'
<!--NeedCopy-->
```

### Modificar los parámetros del archivo de páginación

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

Para modificar los parámetros del archivo de paginación, necesita la versión 2311 o posterior del VDA. Puede modificar los parámetros del archivo de paginación mediante los comandos de PowerShell.

A continuación se muestran los distintos parámetros del archivo de paginación que puede modificar en el entorno de Azure:

- `PageFileDiskDriveLetterOverride`
- `InitialPageFileSizeInMB`
- `MaxPageFileSizeInMB`

#### Modificar los parámetros del archivo de paginación de un catálogo existente

Para modificar los parámetros del archivo de paginación de un catálogo de máquinas existente, ejecute el comando `Set-ProvScheme`. En este caso, las actualizaciones se aplican solo a las nuevas máquinas virtuales agregadas al catálogo. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName $schemeName -CustomProperties '<
    CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
    machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
    instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    StandardSSD_LRS" />
<Property xsi:type="StringProperty" Name="
    PageFileDiskDriveLetterOverride" Value="D" />
<Property xsi:type="StringProperty" Name="InitialPageFileSizeInMB"
    Value="2048" />
<Property xsi:type="StringProperty" Name="MaxPageFileSizeInMB" Value
    ="8196" />
```

```
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property  xsi:type="StringProperty" Name="Zones" Value="1" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="neal-
    test-group1" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
</CustomProperties>'
<!--NeedCopy-->
```

> **Nota:**
>
> Si habilita la caché de reescritura e intenta asignar a `PageFileDiskDriveLetterOverride` el valor `C:` con el comando de PowerShell, el controlador de E/S de MCS redirige automáticamente el archivo de paginación a la unidad de disco correcta, en vez de a `C:`.

### Aprovisionar VM de catálogo con AMA habilitado

1. Configure una plantilla de perfil de máquina.
   - Si quiere usar una máquina virtual como plantilla de perfil de máquina:
     a) Cree una máquina virtual en Azure Portal.
     b) Encienda la máquina virtual.
     c) Agregue la máquina virtual a la regla de recopilación de datos en **Recursos**. Esto invoca la instalación del agente en la máquina virtual de la plantilla.

     > **Nota:**
     >
     > Si debe crear un catálogo de Linux, configure una máquina Linux.

   - Si quiere utilizar la especificación de plantilla como plantilla de perfil de máquina:
     a) Configure una especificación de plantilla.
     b) Agregue esta asociación de extensiones y reglas de recopilación de datos a la especificación de plantilla generada:

```
{

"type": "Microsoft.Compute/virtualMachines/extensions",
"apiVersion": "2022-03-01",
"name": "<vm-name>/AzureMonitorWindowsAgent",
"dependsOn": [
    "Microsoft.Compute/virtualMachines/<vm-name>"
],
"location": "<azure-region>",
"properties": {

    "publisher": "Microsoft.Azure.Monitor",
    "type": "AzureMonitorWindowsAgent",
```

```
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "enableAutomaticUpgrade": true
}

}
,
{

    "type": "Microsoft.Insights/
       dataCollectionRuleAssociations",
    "apiVersion": "2021-11-01",
    "name": "<associatio-name>",
    "scope": "Microsoft.Compute/virtualMachines/<vm-name>",
    "dependsOn": [
     "Microsoft.Compute/virtualMachines/<vm-name>",
    "Microsoft.Compute/virtualMachines/<vm-name>/extensions
       /AzureMonitorWindowsAgent"
    ],
    "properties": {

       "description": "Association of data collection rule.
           Deleting this association will break the data
          collection for this Arc server.",
     "dataCollectionRuleId": "/subscriptions/<azure-
        subscription>/resourcegroups/<azure-resource-group
        >/providers/microsoft.insights/datacollectionrules
        /<azure-data-collection-rule>"
      }

     }

<!--NeedCopy-->
```

> **Nota:**
>
> Si tiene una regla de recopilación de datos configurada con un conector de datos de Microsoft Sentinel, simplemente puede agregar `dataCollectionRuleAssociation` en la especificación de plantilla de la misma manera que una asociación DCR normal. Las máquinas virtuales del catálogo pueden aparecer entonces en el DCR de Sentinel y Azure Monitor Agent (AMA) se instalará en esas máquinas virtuales. Para obtener información sobre las prácticas recomendadas para la creación de reglas de recopilación de datos, consulte Procedimientos recomendados para la creación y administración de reglas de recopilación de datos en Azure Monitor.

2. Cree o actualice un catálogo de máquinas de MCS existente.
   - Para crear otro catálogo de MCS:
     a) Seleccione esa especificación de máquina virtual o plantilla como perfil de máquina en la interfaz de Configuración completa.

b) Continúe con los pasos siguientes para crear el catálogo.

- Para actualizar un catálogo de MCS existente, utilice estos comandos de PowerShell. En este caso, solo las máquinas virtuales nuevas obtienen la plantilla de perfil de máquina actualizada.

```
1 Set-ProvScheme -ProvisioningSchemeName "name"
2 -MachineProfile "XDHyp:\HostingUnits\Unit1\machineprofile.
     folder\abc.resourcegroup\ab-machine-profile.vm"
3 <!--NeedCopy-->
```

- Para actualizar máquinas virtuales existentes con la plantilla de perfil de máquina actualizada, ejecute `Set-ProvScheme` y, a continuación, `Set-ProvVMUpdateTimeWindow`:

```
1 Set-ProvScheme -ProvisioningSchemeName "name" -MachineProfile
      "XDHyp:\HostingUnits\Unit1\machineprofile.folder\abc.
     resourcegroup\ab-machine-profile.vm"
2 Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
      -StartsNow -DurationInMinutes -1
3 <!--NeedCopy-->
```

3. Encienda las máquinas virtuales del catálogo.
4. Vaya a Azure Portal y compruebe si la extensión de supervisión está instalada en la máquina virtual y si la máquina virtual aparece en los recursos de la DCR. Después de unos minutos, los datos de supervisión se muestran en Azure Monitor.

#### Solución de problemas

Para obtener información sobre la guía de solución de problemas del agente de Azure Monitor, consulte lo siguiente:

- https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-troubleshoot-windows-vm/
- https://learn.microsoft.com/en-us/azure/azure-resource-manager/troubleshooting/create-troubleshooting-template/

### Crear un catálogo con máquinas virtuales de Azure Spot

Las máquinas virtuales Azure Spot le permiten aprovechar la capacidad informática no usada de Azure con un importante ahorro de costes. Sin embargo, la capacidad de asignar una máquina virtual Azure Spot depende de la capacidad y los precios actuales. Por lo tanto, Azure podría desalojar la máquina virtual en ejecución, no crear la máquina virtual o no encenderla según la directiva de desalojo. Por

lo tanto, las máquinas virtuales de Azure Spot son buenas para algunas aplicaciones y escritorios no son críticos. Para obtener más información, consulte Usar máquinas virtuales de Azure Spot.

### Limitaciones

- Las máquinas virtuales de Azure Spot no presentan compatibilidad con todos los tamaños de máquinas virtuales. Para obtener más información, consulte Limitaciones.

  Puede ejecutar el siguiente comando de PowerShell para comprobar si el tamaño de una máquina virtual es compatible con máquinas virtuales puntuales o no. Si el tamaño de una máquina virtual es compatible con máquinas virtuales Spot, entonces `SupportsSpotVM` es **True**.

  ```
  (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\serviceoffering.
     folder\Standard_D2ds_v4.serviceoffering"). AdditionalData
  <!--NeedCopy-->
  ```

- Actualmente, las máquinas virtuales de Azure Spot no tienen disponible la función de hibernación.

### Requisito

Al crear el origen del perfil de máquina (especificación de máquina virtual o plantilla) para el catálogo de máquinas virtuales de Azure Spot, debe seleccionar Azure Spot Instance (si usa una máquina virtual) o configurar `priority` como `Spot` (si usa una especificación de plantilla).

### Pasos para crear un catálogo con máquinas virtuales de Azure Spot

1. Cree un origen de perfil de máquina (máquina virtual o plantilla de inicio).
   - Para crear una máquina virtual con Azure Portal, consulte Implementar máquinas virtuales Azure Spot con Azure Portal.
   - Para crear una especificación de plantilla, agregue las siguientes propiedades en **recursos > tipo: Microsoft.Compute/virtualMachines > propiedades** en la especificación de plantilla. Por ejemplo:

     ```
     "priority": "Spot",
     "evictionPolicy": "Deallocate",
     "billingProfile": {

     "maxPrice": 0.01
      }

     <!--NeedCopy-->
     ```

> **Nota:**
>
> - La directiva de desalojo puede **desasignarse** o **eliminarse**.
>   - Para las máquinas virtuales no persistentes, MCS siempre establece la directiva de desalojo como **Eliminar**. Si se desaloja la máquina virtual, se elimina junto con todos los discos no persistentes (por ejemplo, el disco del sistema operativo). No se elimina ningún disco persistente (por ejemplo, el disco de identidad). Sin embargo, un disco del sistema operativo es persistente si el tipo de catálogo es persistente o si la propiedad personalizada `PersistOsDisk` está establecida en True. Del mismo modo, un disco WBC es persistente si la propiedad personalizada `PersistWbc` se establece en **True**.
>   - Para las máquinas virtuales persistentes, MCS siempre establece la directiva de desalojo como Desasignar. Si se desaloja la máquina virtual, se desasigna. No se realizan cambios en los discos.
> - El precio máximo es el precio que está dispuesto a pagar por hora. Si está usando **Solo capacity** , entonces es **-1**. El precio máximo solo puede ser nulo, -1 o un decimal mayor que cero. Para obtener más información, consulte Precios.

2. Puede ejecutar el siguiente comando de PowerShell para comprobar si un perfil de máquina está habilitado para Azure Spot VM o no. Si el parámetro `SpotEnabled` es **True** y `SpotEvictionPolicy` está establecido en **Desasignar** o **Eliminar**, el perfil de la máquina está habilitado para Azure Spot VM. Por ejemplo,

   - Si la fuente del perfil de la máquina es una máquina virtual, ejecute el siguiente comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
      .folder\fifthcolumn.resourcegroup\kb-spot-delete.vm").
      AdditionalData
   <!--NeedCopy-->
   ```

   - Si el origen del perfil de la máquina es una especificación de plantilla, ejecute el siguiente comando:

   ```
   (Get-Item "XDHyp:\HostingUnits\azure-res-conn2\machineprofile
      .folder\fifthcolumn.resourcegroup\fc-aeh-templatespec.
      templatespec\14.0.0-spot-delete.templatespecversion").
      AdditionalData
   <!--NeedCopy-->
   ```

3. Cree un catálogo de máquinas mediante un perfil de máquina con el comando `New-ProvScheme` PowerShell.

Puede actualizar un catálogo mediante el comando `Set-ProvScheme`. También puede actualizar las máquinas virtuales existentes mediante el comando PowerShell `Set-ProvVmUpdateTimeWindow` . El perfil de la máquina se actualiza la próxima vez que se enciende.

#### Desalojos en una máquina virtual Azure Spot en ejecución

Si la capacidad de procesamiento no está disponible o el precio por hora es superior al precio máximo configurado, Azure desaloja una máquina virtual de Spot en ejecución. De forma predeterminada, no se le notifica ningún desalojo. La máquina virtual simplemente se congela y se desaloja. Microsoft recomienda usar eventos programados para supervisar los desalojos. Consulte Supervisar continuamente el desalojo. También puede ejecutar scripts desde una máquina virtual para recibir una notificación antes del desalojo. Por ejemplo, Microsoft tiene un script de sondeo en Python ScheduledEvents.cs.

#### Solución de problemas

- Puede ver las propiedades de la máquina virtual Spot en customMachineData de la máquina virtual aprovisionada mediante el comando `Get-ProvVM`. Si el campo de prioridad está establecido en **Spot**, significa que Spot está en uso.
- Puede comprobar si una máquina virtual usa Spot en Azure Portal:

  1. Busque la máquina virtual en Azure Portal.
  2. Vaya a la página **Descripción general**.
  3. Desplácese hacia abajo y localice la sección **Azure Spot**.
     - Si Spot no está en uso, este campo está vacío.
     - Si se está usando, se establecen los campos de **directiva de desalojo de Azure Spot** y **Azure Spot**.

1. Puede comprobar el perfil de facturación o el precio máximo por hora de la máquina virtual en la página de configuración.

### Copiar etiquetas en todos los recursos

Puede copiar las etiquetas especificadas en un perfil de máquina en todos los recursos, como varias NIC y discos (disco del sistema operativo, disco de identidad y disco de caché de reescritura), de una máquina virtual nueva o existente de un catálogo de máquinas. La fuente del perfil de máquina puede ser una VM o una especificación de plantilla de Azure Resource Manager.

> **Nota:**
>
> Debe agregar la directiva a las etiquetas (consulte Assign policy definitions for tag compliance) o agregar las etiquetas en un origen de perfil de máquina para conservar las etiquetas en los recursos.

### Requisitos previos

Cree el origen del perfil de máquina (VM o especificación de plantilla de Azure Resource Manager) para tener etiquetas en la VM, los discos y las tarjetas NIC de esa VM.

- Si quiere usar una VM como entrada del perfil de máquina, aplique etiquetas a VM y a todos los recursos de Azure Portal. Consulte Apply tags with Azure portal.
- Si quiere usar una especificación de plantilla de Azure Resource Manager como entrada del perfil de la máquina, agregue el siguiente bloque de etiquetas bajo cada recurso.

```
1   "tags": {
2
3  "TagC": "Value3"
4   }
5  ,
6  <!--NeedCopy-->
```

> **Nota:**
>
> Puede tener un máximo de un disco y al menos una tarjeta NIC en la especificación de plantilla.

### Copie las etiquetas en los recursos de una VM de un nuevo catálogo de máquinas

1. Cree un catálogo persistente o no persistente con una VM o una especificación de plantilla de Azure Resource Manager como entrada del perfil de máquina.
2. Agregue una VM al catálogo y enciéndala. Debería poder ver que las etiquetas especificadas en el perfil de máquina se han copiado en los recursos correspondientes de esa VM.

   > **Nota:**
   >
   > Aparecerá un error si la cantidad de tarjetas NIC proporcionadas en el perfil de máquina no coincide con la cantidad de tarjetas NIC que quiere que usen las VM.

### Modificar las etiquetas de los recursos de una VM existente

1. Cree un perfil de máquina con las etiquetas de todos los recursos.
2. Actualice el catálogo de máquinas existente con el perfil de máquina actualizado. Por ejemplo:

```
1  Set-ProvScheme -ProvisioningSchemeName <YourCatalogName> -
       MachineProfile <PathToYourMachineProfile>
2  <!--NeedCopy-->
```

3. Apague la máquina virtual en la que quiera aplicar las actualizaciones.
4. Solicite una actualización programada para la máquina virtual. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName <
    YourCatalogName>  -VMName machine1 -StartsNow -
    DurationInMinutes -1
<!--NeedCopy-->
```

5. Encienda la máquina virtual.
6. Debería poder ver que las etiquetas especificadas en el perfil de máquina se han copiado en los recursos correspondientes.

> **Nota:**
>
> Aparecerá un error si la cantidad de tarjetas NIC proporcionadas en el perfil de máquina no coincide con la cantidad de tarjetas NIC proporcionadas en `Set-ProvScheme`.

### Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de Microsoft Azure.

### Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft Azure Resource Manager
- Crear catálogos de máquinas

## Crear un catálogo de Microsoft System Center Virtual Machine Manager

February 21, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de crear un catálogo de VMM, debe terminar de crear una conexión con VMM. Consulte Conexión con Microsoft System Center Virtual Machine Manager.

### Crear una VM maestra

- Instale un agente Virtual Desktop Agent en la VM maestra y seleccione la opción de optimizar el escritorio. Esto mejora el rendimiento.
- Tome una instantánea de la VM maestra para usarla como copia de seguridad.
- Cree escritorios virtuales.

### MCS en recursos compartidos de archivos SMB 3

En caso de catálogos de máquinas creados a través de MCS en recursos compartidos SMB 3 para el almacenamiento de VM, las credenciales deben cumplir los siguientes requisitos para que las llamadas desde la biblioteca de comunicaciones de XenServer (HCL) puedan conectarse al almacenamiento SMB.

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

Para obtener más información sobre SMB 3, consulte Información general sobre el uso compartido de archivos mediante el protocolo SMB 3 en Windows Server.

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

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

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

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

ConvertVirtualHardDisk en el espacio de nombres root\virtualization\v2

Ejemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdastext)
$result
<!--NeedCopy-->
```

**Crear disco de diferenciación:** Consolida una imagen para crear un disco de diferenciación a partir de la imagen generada. A continuación, el disco de diferenciación se adjunta a una nueva VM.

CreateVirtualHardDisk en el espacio de nombres root\virtualization\v2

Ejemplo:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdastext);
$result
<!--NeedCopy-->
```

**Cargar discos de identidad:** La biblioteca HCL no puede cargar directamente el disco de identidad en el almacenamiento de SMB. Por lo tanto, la máquina Hyper-V debe cargar y copiar el disco de identidad en el almacenamiento. Debido a que la máquina Hyper-V no puede leer el disco desde el Cloud Connector, la HCL debe copiar primero el disco de identidad mediante la máquina Hyper-V tal y como se indica.

1. La HCL carga la identidad en la máquina Hyper-V mediante el recurso compartido de administrador.
2. La máquina Hyper-V copia el disco en el almacenamiento de SMB a través de un script de PowerShell que se ejecuta en la sesión remota de PowerShell.

   Se crea una carpeta en la máquina Hyper-V y los permisos de la carpeta están bloqueados únicamente para el usuario de VMM (a través de la conexión remota de PowerShell).
3. La biblioteca HCL elimina el archivo del recurso compartido de administrador.
4. Cuando la biblioteca HCL completa la carga del disco de identidad en la máquina Hyper-V, la sesión remota de PowerShell copia los discos de identidad al almacenamiento de SMB y, después, los elimina de la máquina Hyper-V.

La carpeta del disco de identidad se crea de nuevo si se elimina para que pueda reutilizarse.

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

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

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

## Crear un catálogo con un perfil de máquina

Puede usar un perfil de máquina para crear y actualizar un catálogo de máquinas MCS en entornos de System Center Virtual Machine Manager (SCVMM). También puede habilitar la virtualización anidada y el vTPM.

### Consideraciones importantes

- La imagen maestra solo puede ser una instantánea y no una máquina virtual.
- Solo puede usar una máquina virtual como origen de perfil de máquina.
- Puede configurar VTPM desde la consola de Hyper-V y no desde la consola SCVMM.
- Si la imagen maestra tiene el vTPM habilitado, debe habilitar el vTPM en el origen del perfil de la máquina.
- vTPM solo es compatible en máquinas de 2.ª generación.
- Los siguientes parámetros sobrescriben los valores capturados en un perfil de máquina si se proporcionan por separado:
  - VMCpuCount
  - VMMemoryMB
  - Almacenamiento en disco
- Puede actualizar un catálogo existente mediante el comando `Set-ProvScheme`.

### Pasos para crear un catálogo mediante un perfil de máquina

1. Cree una máquina virtual para que sea un origen de perfiles de máquina. Para obtener más información, consulte Aprovisionar máquinas virtuales en el tejido de VMM. No puede cambiar la **generación** después de seleccionarla.
   - Si quiere habilitar la virtualización anidada, seleccione la casilla de verificación **Habilitar la virtualización anidada** en la página **Seleccionar origen**.
   - Si quiere habilitar vTPM, después de crear la máquina virtual, inicie sesión en el host de Hyper-V y busque su máquina virtual en el **administrador de Hyper-V**. Haga clic con el botón derecho en la máquina virtual y, a continuación, vaya a **Parámetros**. En **Seguridad**, seleccione la casilla **Habilitar el módulo de plataforma segura**.

2. Abra una ventana de **PowerShell**.
3. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
4. Cree un catálogo de brokers. Este catálogo contiene máquinas que están a punto de crearse.
5. Cree un grupo de identidades. Se convierte en un contenedor para las cuentas de AD creadas para las máquinas que se van a crear.
6. Cree un esquema de aprovisionamiento con el perfil de la máquina. Por ejemplo:

```
New-ProvScheme -HostingUnitName "<hostingunit name>"
-IdentityPoolName "ID1" -MasterImageVM "XDHyp:\HostingUnits\HU1<
    path to the checkpoint/snapshot>"
-ProvisioningSchemeName "<catalogname>"  -MachineProfile "XDHyp:<
    path to the machine profile VM>"
<!--NeedCopy-->
```

7. Actualiza el catálogo de Broker con el identificador único del esquema de aprovisionamiento.
8. Cree máquinas virtuales y agréguelas al catálogo.

Puede actualizar un catálogo existente mediante el comando Set-ProvScheme. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName "<catalogname>" -MachineProfile
    "XDHyp:<path to the machine profile VM>"
<!--NeedCopy-->
```

### Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de Microsoft System Center Virtual Machine Manager.

### Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft System Center Virtual Machine Manager
- Crear catálogos de máquinas

## Crear un catálogo de Nutanix

February 12, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de Nutanix.

> **Nota:**
>
> Antes de crear un catálogo de Nutanix, debe terminar de crear una conexión con Nutanix. Consulte Conexión con Nutanix.

### Crear un catálogo de máquinas mediante una instantánea de Nutanix

La instantánea que seleccione es la plantilla que se utiliza para crear las máquinas virtuales del catálogo. Antes de crear el catálogo de máquinas, cree las imágenes y las instantáneas en Nutanix. Para obtener más información, consulte la documentación de Nutanix.

En el asistente para la creación de catálogos:

- Las páginas **Sistema operativo** y **Administración de máquinas** no contienen información específica de Nutanix.
- La página **Contenedor** o **Cluster and Container** es exclusiva de Nutanix.
  - Si implementa máquinas mediante Nutanix AHV XI como recursos, en la página **Contenedor**, seleccione un contenedor donde colocar los discos de identidad de las VM.
  - Si implementa máquinas mediante Nutanix AHV Prism Central (PC) como recursos, aparecerá la página **Cluster and Container**. Seleccione el clúster que se utilizará para la implementación de las máquinas virtuales y, a continuación, un contenedor.
- En la página **Imagen**, seleccione la instantánea de la imagen. Utilice la consola de Acropolis para cambiar el nombre de las instantáneas, si es necesario. Si cambia el nombre de las instantáneas, reinicie el asistente de creación de catálogos para ver una lista con los nombres actualizados.
- En la página **Máquinas virtuales**, indique la cantidad de unidades CPU virtuales y la cantidad de núcleos por cada CPU virtual.
- En la página **Tarjetas NIC**, seleccione el tipo de tarjeta de interfaz de red (NIC) para filtrar las redes asociadas. Esta opción solo está disponible para conexiones de Nutanix AHV PC. Hay dos tipos de NIC: **VLAN** y **SUPERPOSICIÓN**. Seleccione una o varias NIC que contengan la imagen maestra y, a continuación, seleccione una red virtual asociada para cada NIC.
- Las páginas **Identidades de las máquinas**, **Credenciales de dominio**, **Ámbitos** y **Resumen** no contienen información específica de Nutanix.

### Limitación

Al crear un catálogo de MCS con una conexión de host de Nutanix (específicamente, el plug-in 2.7.1 de Nutanix AHV y el plug-in 2.5.1 de Nutanix AHV), el tamaño del disco duro de las máquinas virtuales aprovisionadas no se muestra correctamente en la interfaz de Configuración completa.

- Plug-in 2.7.1 de Nutanix AHV: El tamaño que se muestra es mucho más pequeño (1 GB) que el tamaño de almacenamiento real.
- Plug-in 2.5.1 de Nutanix AHV: El tamaño que se muestra es mucho más pequeño (32 GB) que el tamaño de almacenamiento real.

Sin embargo, esto funciona según lo diseñado si la VM de la imagen maestra es una instantánea en la VM.

### Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas.

### Más información

- Crear y administrar conexiones y recursos
- Conexión con Nutanix
- Conexión con soluciones de Nutanix Cloud y de partners
- Crear catálogos de máquinas

## Crear un catálogo de VMware

May 17, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas.

> **Nota:**
>
> Antes de crear un catálogo de VMware, debe terminar de crear una conexión con VMware. Consulte Conexión con VMware.

### Crear un catálogo de máquinas mediante un perfil de máquina

Puede crear un catálogo de máquinas de MCS mediante un perfil de máquina. El origen de la entrada del perfil de la máquina es una plantilla de VMware. El perfil de la máquina captura las propiedades del hardware de una plantilla de VMware y las aplica a las máquinas virtuales recién aprovisionadas del catálogo.

> **Nota:**
>
> - La entrada de la imagen maestra (instantánea) y la entrada del perfil de la máquina (plantilla de VMware) deben tener las dos vTPM habilitado o inhabilitado. Esta regla se aplica tanto a `New-ProvScheme` como a `Set-ProvScheme`.
> - Si la imagen maestra tiene vTPM habilitado, la plantilla de VMware solo puede provenir del mismo origen de máquina virtual que la imagen maestra.
> - La directiva de almacenamiento cifrado solo admite la clonación completa.

La plantilla de VMware en el perfil de máquina debe existir durante el ciclo de vida del catálogo para permitir el aprovisionamiento de máquinas virtuales en el catálogo. Sin una plantilla de VMware, no puede aprovisionar nuevas máquinas virtuales. Al eliminar una plantilla de VMware, debe proporcionar una plantilla nueva mediante el comando `Set-ProvScheme`.

- MCS captura las propiedades de las plantillas de VMware. Puede crear otra plantilla de VMware que haga referencia a las propiedades almacenadas de la plantilla de VMware mediante el comando `Get-Provscheme`.
- Igualmente, si existen el catálogo de máquinas y las máquinas virtuales aprovisionadas, se puede usar una máquina aprovisionada de MCS para crear otra plantilla de VMware.

En función de cada sistema operativo, puede crear un catálogo de máquinas con diferentes configuraciones:

- Si Windows 11 está instalado en la imagen maestra, es necesario tener habilitado vTPM para la imagen maestra. Por lo tanto, la plantilla de VMware, que es el origen del perfil de la máquina, debe tener el vTPM conectado.
- Si Windows 10 está instalado en la imagen maestra sin ningún vTPM conectado, puede crear un catálogo de máquinas con una plantilla de VMware que no sea vTPM como origen para el perfil de la máquina.

Hay otra configuración en la que puede crear un catálogo de máquinas mediante el modo de disco de copia completa con una plantilla de perfil de máquina aplicada con una directiva de almacenamiento cifrado.

Para crear un catálogo de máquinas mediante los comandos de PowerShell con el perfil de la máquina como entrada:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute los comandos siguientes:

   - Para crear un catálogo de máquinas con una plantilla de VMware con un vTPM conectado como origen para la entrada del perfil de la máquina y la imagen maestra instalada en Windows 11:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "vSanRg"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<network name>.
   network" }

-ProvisioningSchemeName "<string>"
-Scope @() -VMCpuCount 4  -VMMemoryMB 6144
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared
-FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"  -IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<catalog name>" -
   ProvisioningType 'MCS'
-Scope @()  -SessionSupport "SingleSession"
-ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

   - Para crear un catálogo de máquinas con una plantilla de VMware sin un vTPM como origen para el perfil de la máquina y la imagen maestra instalada en Windows 10:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme  -CleanOnBoot
-HostingUnitName "<string>"
-IdentityPoolName "<string>"
-InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"  -Description "<string>"  -
   IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()  -SessionSupport "
   SingleSession" -ZoneUid "<Uid"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Para crear un catálogo de máquinas mediante el modo de disco de copia completa con una plantilla de perfil de máquina aplicada con una directiva de almacenamiento cifrado:

```
$identityPool = New-AcctIdentityPool
-IdentityPoolName "<string>"
-NamingScheme "<string>-###"
-NamingSchemeType Numeric
-Domain "<domain name>"
-ZoneUid "<Uid>"  -Scope @()
<!--NeedCopy-->
```

```
$provScheme =New-ProvScheme
-HostingUnitName "<string>"
```

```
-IdentityPoolName "<string>" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits<hosting unit name><
   snapshot name>.snapshot"
-NetworkMapping @{
"0"="XDHyp:\HostingUnits<hosting unit name>\<string>.network"
    }

-ProvisioningSchemeName "<string>"  -Scope @() -VMCpuCount 4
    -VMMemoryMB 8192
-MachineProfile "XDHyp:\HostingUnits<hosting unit name><
   template name>.template"
-TenancyType Shared  -FunctionalLevel "L7_20"
-UseFullDiskCloneProvisioning
<!--NeedCopy-->
```

```
$catalog = New-BrokerCatalog
-AllocationType "Static"
-PersistUserChanges  "OnLocal"
-Description "<string>"
-IsRemotePC $False
-MinimumFunctionalLevel 'L7_9' -Name "<string>" -
   ProvisioningType 'MCS' -Scope @()
-SessionSupport "SingleSession" -ZoneUid "<Uid>"
<!--NeedCopy-->
```

```
Set-BrokerCatalog -Name "<string>"
-ProvisioningSchemeId $provScheme.ProvisioningSchemeUid.Guid
<!--NeedCopy-->
```

- Para actualizar un perfil de máquina, utilice el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName 'name' -
   IdentityPoolName 'name' -MachineProfile 'XDHyp:\
   HostingUnits<hosting unit name><template name>.template
<!--NeedCopy-->
```

### Comprobar la presencia de varias tarjetas NIC

Aparecen diversos mensajes de error durante las comprobaciones preliminares sobre presencia de varias tarjetas NIC cuando se usa un perfil de máquina y el parámetro `NetworkMapping` en los comandos `New-ProvScheme` y `Set-ProvScheme`.

La lista de verificación preliminar para detectar la presencia de varias tarjetas NIC es la siguiente:

- Solo se usa y valida el recuento de tarjetas NIC de la plantilla de perfil de la máquina. La red a la que apuntan estas tarjetas NIC no se usa ni se valida con respecto a las redes de la unidad de alojamiento.

- Si el recuento de tarjetas NIC en la plantilla de perfil de la máquina es mayor que el número de redes de la unidad de alojamiento, aparecerá un mensaje de error.
- Si el recuento de tarjetas NIC en la plantilla de perfil de la máquina es cero, aparecerá un mensaje de error.
  Cuando el recuento de tarjetas NIC en la plantilla de perfil de la máquina es uno, entonces:
  - If no network mapping is specified in the `New-ProvScheme` or `Set-ProvScheme` command, and the hosting unit network is one, then the hosting unit network is used.
  - If network mapping is specified, then the specified network mapping is used if it is valid.
- Cuando el recuento de tarjetas NIC en la plantilla de perfil de la máquina es superior a 1 o el recuento de redes de la unidad de alojamiento es superior a 1, entonces:
  - El comando requiere una asignación de red válida y debe proporcionar una asignación para cada tarjeta NIC (es decir, el recuento de NetworkMapping debe ser el mismo que el recuento de tarjetas NIC del perfil de máquina).
  - No se pueden asignar varias tarjetas NIC a la misma red en la unidad de alojamiento.
  - El recuento de `NetworkMapping` y el recuento de tarjetas NIC del perfil de máquina debe ser inferior o igual al recuento de redes de la unidad de alojamiento.
  - Se debe proporcionar `NetworkMapping` para cada ID comprendido entre 0 y n-1, donde n es el número de adaptadores de red de la plantilla del perfil de máquina.

### Solución de problemas

Si no se puede crear el catálogo, consulte CTX294978.

### Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de VMware.

### Más información

- Crear y administrar conexiones y recursos
- Conexión con VMware
- Conexión con soluciones de VMware Cloud y de partners
- Crear catálogos de máquinas

# Crear un catálogo de XenServer

March 6, 2024

Crear catálogos de máquinas describe los asistentes con los que se crea un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de XenServer (antes denominado Citrix Hypervisor).

> **Nota:**
>
> Antes de crear un catálogo de XenServer, debe terminar de crear una conexión a XenServer. Consulte Conexión a XenServer.

## Crear un catálogo de máquinas con un XenServer compatible con GPU

Las máquinas que pueden usar GPU requieren una imagen maestra dedicada. Esas máquinas virtuales requieren controladores de tarjeta de vídeo compatibles con GPU. Configure máquinas que pueden usar GPU para que la máquina virtual funcione con el software que usa la GPU para las operaciones.

1. En XenCenter, cree una VM con VGA estándar, redes y vCPU.
2. Actualice la configuración de la máquina virtual para habilitar el uso de GPU (PassThrough o vGPU).
3. Instale un sistema operativo compatible y habilite el protocolo RDP.
4. Instale Citrix VM Tools y los controladores de NVIDIA.
5. Desactive la consola de administración de Virtual Network Computing (VNC) para optimizar el rendimiento y, a continuación, reinicie la VM.
6. Se le solicitará que use RDP. Mediante RDP, instale el VDA y, a continuación, reinicie la VM.
7. Si quiere, puede crear una instantánea de la VM para establecer un punto de referencia para otras imágenes maestras de GPU.
8. Mediante RDP, instale las aplicaciones específicas del usuario que están configuradas en XenCenter y funcionan con GPU.

## Crear un catálogo de máquinas basado en perfiles de máquina con PowerShell

Al crear un catálogo para aprovisionar máquinas mediante MCS, puede usar un perfil de máquina para capturar las propiedades del hardware de una máquina virtual y aplicarlas a las máquinas virtuales recién aprovisionadas del catálogo. Si no se utiliza el parámetro `MachineProfile`, las propiedades del hardware se obtienen de la instantánea o la VM de la imagen maestra.

> **Nota:**
>
> Actualmente, solo puede usar una instantánea como entrada de perfil de máquina.

Puede configurar explícitamente estos parámetros para sobrescribir los valores de los parámetros en la entrada del perfil de máquina:

- `VMCpuCount`
- `VMMemory`
- `NetworkMapping`

### Crear un catálogo con un perfil de máquina

1. Abra la ventana de PowerShell.
2. Ejecute `asnp citrix*`.
3. Cree un grupo de identidades. El grupo de identidades es un contenedor para las cuentas de Active Directory (AD) de las máquinas virtuales que se crearán. Por ejemplo:

```
New-AcctIdentityPool -Domain "citrix-xxxxxx.local" -
    IdentityPoolName "ExampleIdentityPool" -NamingScheme "abc1-##"
    -NamingSchemeType "Numeric" -Scope @() -ZoneUid "xxxxxxxx"
<!--NeedCopy-->
```

4. Cree las cuentas de equipo de AD necesarias en Active Directory.

```
$password = "password123" | ConvertTo-SecureString -AsPlainText -
    Force
New-AcctADAccount -IdentityPoolName "ExampleIdentityPool" -Count
    10 -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
Set-AcctAdAccountUserCert -IdentityPoolName "ExampleIdentityPool"
    -ADUserName "citrix-xxxxxx\admin1" -ADPassword $password
<!--NeedCopy-->
```

5. Ejecute el comando `New-ProvScheme` para crear un catálogo. Por ejemplo:

```
New-ProvScheme -CleanOnBoot -HostingUnitName "ExampleHostingUnit"
    -IdentityPoolName "ExampleIdentityPool" -InitialBatchSizeHint 2
     -CustomProperties '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
</CustomProperties>'
-MasterImageVM "XDHyp:\HostingUnits\ExampleHostingUnit\ExampleVDA.
    vm\ExampleVDA.snapshot" -ProvisioningSchemeName "ExampleCatalog
    " -Scope @() -SecurityGroup @()
-MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfile.vm\ExampleSnapshot.snapshot"
```

```
<!--NeedCopy-->
```

6. Registre el esquema de aprovisionamiento como un catálogo de broker. Por ejemplo:

```
$ConfigZone = Get-ConfigZone | Where-Object {
  $_.Name -eq "xxxxxx"  }

New-BrokerCatalog -Name "MPLT1" -AllocationType Random -
    Description "Machine profile catalog" -ProvisioningSchemeId
    fe7df345-244e-4xxxx-xxxxxxxxx -ProvisioningType Mcs -
    SessionSupport MultiSession -PersistUserChanges Discard -
    ZoneUid ($ConfigZone.Uid)
<!--NeedCopy-->
```

7. Agregue las VM al catálogo.

### Actualizar un catálogo con un nuevo perfil de máquina

> **Nota:**
>
> - En este caso, el comando `Set-ProvScheme` no cambia el perfil de máquina de las máquinas virtuales existentes del catálogo. Solo las nuevas máquinas virtuales que se agregan al catálogo tienen el nuevo perfil de máquina.
> - No puede convertir catálogos de máquinas basado en perfiles de máquina en catálogos de máquinas no basados en perfiles de máquina.

Para actualizar el catálogo con un nuevo perfil de máquina:

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName "ExampleCatalog" -
    MachineProfile "XDHyp:\HostingUnits\ExampleHostingUnit\
    ExampleMachineProfileVm.vm\ExampleMachineProfileSnapshot.
    snapshot"
<!--NeedCopy-->
```

   Para obtener más información sobre el comando Set-ProvScheme, consulte Set-ProvScheme.

## Qué hacer a continuación

- Si este es el primer catálogo creado, Studio le guiará para crear un grupo de entrega.
- Para revisar todo el proceso de configuración, consulte Planificar y crear una implementación.
- Para administrar catálogos, consulte Administrar catálogos de máquinas y Administrar un catálogo de XenServer.

### Más información

- Crear y administrar conexiones y recursos
- Conexión a XenServer
- Crear catálogos de máquinas

## Crear catálogos de diferentes tipos de unión

July 3, 2023

Con MCS, puede aprovisionar máquinas como máquinas que no estén unidas a un dominio, que estén unidas a AD en instancias locales, que estén unidas a Azure AD o que estén unidas a Azure AD híbrido.

Para obtener información sobre cómo configurar identidades de máquinas en la interfaz de Configuración completa, consulte Crear catálogos de máquinas.

Para obtener información específica sobre cómo crear catálogos unidos de identidades de máquinas, consulte lo siguiente:

- Crear catálogos unidos a Azure Active Directory
- Crear catálogos con Microsoft Intune habilitado
- Crear catálogos unidos a Azure Active Directory híbrido
- Crear catálogos que no estén unidos a ningún dominio

## Crear catálogos unidos a Azure Active Directory

February 12, 2024

En este artículo se describe cómo crear catálogos unidos a Azure Active Directory (AD) mediante Citrix DaaS.

Para obtener información sobre los requisitos, las limitaciones y los aspectos a tener en cuenta, consulte Unidos a Azure Active Directory.

Antes de crear el catálogo de máquinas, necesita lo siguiente:

1. Nueva ubicación de recursos
    - Vaya a la interfaz de usuario de la administración de Citrix Cloud > menú de tres líneas de la parte superior izquierda > **Ubicaciones de recursos**.

- Haga clic en **+ Ubicación de recursos**.
- Escriba un nombre para nueva la ubicación de recursos y haga clic en **Guardar**.

2. Cree una conexión de host. Consulte la sección Crear y administrar conexiones para obtener información detallada. Al implementar máquinas en Azure, consulte Conexión con Azure Resource Manager.

3. Para eliminar sistemáticamente los dispositivos obsoletos de Azure AD y permitir que se le unan nuevos dispositivos, puede asignar el rol de administrador de dispositivos en la nube a la entidad principal de servicio de aprovisionamiento. Si no elimina los dispositivos obsoletos de Azure AD, la VM no persistente correspondiente permanecerá en el estado de inicialización hasta que la elimine manualmente del portal de Azure AD. Para ello, habilite la administración de conexiones de host en dispositivos unidos a Azure AD mediante la interfaz de Configuración completa o siga estos pasos:

   a) Inicie sesión en Azure Portal y vaya a **Azure Active Directory > Roles and administrators**.

   b) Busque el rol integrado **Cloud Device Administrator** y haga clic en **Add assignments** para asignar el rol a la entidad principal de servicio de la aplicación utilizada por la conexión de host.

   c) Utilice el SDK de PowerShell remoto de Citrix para ejecutar los siguientes comandos a fin de obtener las `CustomProperties` de la conexión de host existente. `${HostingConnectionName}` hace referencia al nombre de la conexión de host.

      i. Abra una ventana de **PowerShell**.

      ii. Ejecute `asnp citrix*` para cargar los módulos de **PowerShell** específicos de Citrix.

      iii. Ejecute el siguiente comando para obtener las propiedades personalizadas existentes de la conexión de host.

```
(Get-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
 ).CustomProperties
<!--NeedCopy-->
```

      iv. Copie las propiedades personalizadas de la conexión en un bloc de notas y añada la configuración de propiedad `<Property xsi:type="StringProperty"Name="AzureAdDeviceManagement"Value="true"/>`.

      v. En la ventana de **PowerShell**, asigne una variable a las propiedades personalizadas modificadas. Por ejemplo, `$UpdatedCustomProperties='<CustomProperties ...</CustomProperties>'`.

      vi. Vuelva a establecer la propiedad personalizada en la conexión de host:

```
Set-Item -LiteralPath XDHyp:\Connections${
 HostingConnectionName }
  -CustomProperties ${
 UpdatedCustomProperties }
  -ZoneUid ${
 ZoneUid }

<!--NeedCopy-->
```

vii. Ejecute el comando `(Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName } ).CustomProperties` para verificar la configuración actualizada de las propiedades personalizadas.

Puede crear catálogos unidos a Azure AD mediante la interfaz de Configuración completa o **PowerShell**.

### Usar la interfaz de Configuración completa

La información siguiente complementa a las instrucciones del artículo Crear catálogos de máquinas. Para crear catálogos unidos a Azure AD, siga las instrucciones generales de ese artículo y tenga en cuenta los detalles específicos sobre los catálogos unidos a Azure AD.

En el asistente para la creación de catálogos:

1. En la página **Imagen**:
   - Seleccione 2106 o una versión posterior como nivel funcional.
   - Seleccione **Usar un perfil de máquina** y seleccione la máquina correspondiente de la lista.
2. En la página **Identidades de las máquinas**, seleccione **Unido a Azure Active Directory**. Las máquinas creadas son propiedad de una organización, en las que se ha iniciado sesión con una cuenta de Azure AD que pertenece a esa organización. Solo existen en la nube.

   > **Nota:**
   >
   > - El tipo de identidad **Unido a Azure Active Directory** requiere la versión 2106 o una posterior como nivel funcional mínimo para el catálogo.
   > - Las máquinas se unen al dominio de Azure AD asociado al arrendatario al que está vinculada la conexión de host.

3. Los usuarios deben tener acceso explícito en Azure para iniciar sesión en las máquinas con sus credenciales de AAD. Consulte la sección Unidos a Azure Active Directory para obtener más detalles.

### Mediante PowerShell

He aquí los pasos de **PowerShell** equivalentes a las operaciones de Configuración completa. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La diferencia entre los catálogos unidos a AD local y los unidos a Azure AD radica en la creación del grupo de identidades y el esquema de aprovisionamiento.

Para crear un grupo de identidades para los catálogos unidos a Azure AD:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType="AzureAD" -
     WorkgroupMachine -IdentityPoolName "AzureADJoinedCatalog" -
     NamingScheme "AzureAD-VM-##" -NamingSchemeType "Numeric" -Scope @()
     -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

Para crear un esquema de aprovisionamiento para los catálogos unidos a Azure AD, se requiere el parámetro **MachineProfile** en New-ProvScheme:

```
1 New-ProvScheme -CustomProperties "<CustomProperties xmlns=`"http://
     schemas.citrix.com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.
     w3.org/2001/XMLSchema-instance`"><Property xsi:type=`"StringProperty
     `" Name=`"UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
     StringProperty`" Name=`"StorageType`" Value=`"StandardSSD_LRS`" /><
     Property xsi:type=`"StringProperty`" Name=`"LicenseType`" Value=`"
     Windows_Server`" /></CustomProperties>" -HostingUnitName "
     AzureResource" -IdentityPoolName "AzureADJoinedCatalog" -
     InitialBatchSizeHint 1 -MachineProfile "XDHyp:\HostingUnits\
     AzureResource\image.folder\azuread-rg.resourcegroup\MasterVDA.vm" -
     MasterImageVM "XDHyp:\HostingUnits\AzureResource\image.folder\
     azuread-rg.resourcegroup\azuread-
     small_OsDisk_1_5fb42fadf7ff460bb301ee0d56ea30da.manageddisk" -
     NetworkMapping @{
2  "0"="XDHyp:\HostingUnits\AzureResource\virtualprivatecloud.folder\East
       US.region\virtualprivatecloud.folder\azuread-rg.resourcegroup\
      azuread-vnet.virtualprivatecloud\Test_VNET.network" }
3   -ProvisioningSchemeName "AzureADJoinedCatalog" -RunAsynchronously -
       Scope @() -SecurityGroup @() -ServiceOffering "XDHyp:\HostingUnits
       \AzureResource\serviceoffering.folder\Standard_DS1_v2.
       serviceoffering"
4 <!--NeedCopy-->
```

Todos los demás comandos que se utilizan para crear catálogos unidos a Azure AD son los mismos que se usan para los catálogos tradicionales unidos a AD local.

### Ver el estado del proceso de unión a Azure AD

En la interfaz de Configuración completa, el estado del proceso de unión a Azure AD es visible cuando las máquinas unidas a Azure AD de un grupo de entrega están encendidas. Para ver el estado, utilice Buscar para identificar esas máquinas y, a continuación, para cada una de ellas, compruebe la **identidad de la máquina** en la ficha **Detalles** del panel inferior. Esta información puede aparecer en **Identidad de la máquina**:

- Unida a Azure AD
- Aún no se ha unido a Azure AD

> **Nota:**
>
> Si las máquinas no se hallan unidas a Azure AD, no se registran en el Delivery Controller. Su estado de registro aparece como **Inicialización.**

Además, mediante la interfaz de Configuración completa, puede averiguar por qué las máquinas no están disponibles. Para ello, haga clic en una máquina del nodo **Buscar**, marque **Registro** en la ficha **Detalles** del panel inferior y, a continuación, lea el texto de ayuda para obtener información adicional.

### Grupo de entrega

Consulte la sección Crear grupos de entrega para obtener información detallada.

### Habilitar Rendezvous

Una vez creado el grupo de entrega, puede habilitar Rendezvous. Consulte Rendezvous V2 para obtener información detallada.

### Solución de problemas

Si las máquinas no logran unirse a Azure AD, haga lo siguiente:

- Compruebe si la identidad administrada asignada del sistema está habilitada para las máquinas. Las máquinas aprovisionadas por MCS deben tener esta opción habilitada automáticamente. El proceso de unión a Azure AD falla sin una identidad administrada asignada del sistema. Si la identidad administrada asignada del sistema no está habilitada para máquinas aprovisionadas por MCS, es posible que se deba a lo siguiente:
  - `IdentityType` del grupo de identidades asociado al esquema de aprovisionamiento no está configurado en `AzureAD`. Para comprobarlo, ejecute `Get-AcctIdentityPool`.

- En el caso de los catálogos que usan imágenes maestras con la versión 2206 de VDA o anterior, compruebe el estado de aprovisionamiento de la extensión **AADLoginForWindows** para las máquinas. Si la extensión **AADLoginForWindows** no existe, los posibles motivos son:
  - `IdentityType` del grupo de identidades asociado al esquema de aprovisionamiento no está configurado en `AzureAD`. Para comprobarlo, ejecute `Get-AcctIdentityPool`.
  - La directiva de Azure bloquea la instalación de la extensión **AADLoginForWindows**.
- Para solucionar problemas de aprovisionamiento de la extensión **AADLoginForWindows**, puede comprobar los registros en `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` de la máquina aprovisionada por MCS.

  > **Nota:**
  >
  > MCS no se basa en la extensión `AADLoginForWindows` para unir una máquina virtual a Azure AD cuando se usa una imagen maestra con la versión 2209 de VDA o una posterior. En este caso, la extensión `AADLoginForWindows` no se instalará en la máquina aprovisionada por MCS. Por consiguiente, no se pueden recopilar los registros de aprovisionamiento de la extensión `AADLoginForWindows`.

- Para comprobar el estado de la unión a Azure AD y los registros de depuración, ejecute el comando `dsregcmd /status` en la máquina aprovisionada por MCS.
- Consulte los registros de eventos de Windows en **Registros de aplicaciones y servicios > Microsoft > Windows > Registro de dispositivos de usuario**.
- Ejecute `Get-Item -LiteralPath XDHyp:\Connections\${ HostingConnectionName }` para comprobar si la administración de dispositivos de Azure AD está configurada correctamente.

  Compruebe que el valor de:
  - La propiedad `AzureAdDeviceManagement` en `CustomProperties` es **true**
  - La propiedad `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` en los metadatos es **true**

  Si el valor de `Citrix_MCS_AzureAdDeviceManagement_PermissionGranted` es **false**, indica que la `ServicePrincipal` de la aplicación utilizada por la conexión de host no cuenta con permisos suficientes para la administración de dispositivos de Azure AD. Para resolver esto, asigne a la `ServicePrincipal` el rol **Cloud Device Administrator** .

### Grupo de seguridad dinámico de Azure Active Directory

Las reglas de los grupos dinámicos colocan las máquinas virtuales del catálogo en un grupo de seguridad dinámico según el esquema de nomenclatura del catálogo de máquinas.

Si el esquema de nomenclatura del catálogo de máquinas es Test### (donde # representa un número), Citrix crea la regla de pertenencia dinámica *^Test[0-9]{3}$* en el grupo de seguridad dinámico. Si el nombre de la máquina virtual creada por Citrix está entre Test001 y Test999, la máquina virtual se incluye en el grupo de seguridad dinámico.

> **Nota:**
>
> Si el nombre de la máquina virtual que creó manualmente está entre Test001 y Test999, la máquina virtual también se incluye en el grupo de seguridad dinámico. Esta es una de las limitaciones del grupo de seguridad dinámico.

La funcionalidad de grupo de seguridad dinámico es útil cuando quiere administrar las máquinas virtuales con Azure Active Directory (Azure AD). También es útil cuando quiere aplicar directivas de acceso condicional o distribuir aplicaciones desde Intune filtrando las máquinas virtuales con un grupo de seguridad dinámico de Azure AD.

Puede usar los comandos de **PowerShell** para:

- Crear un catálogo de máquinas con un grupo de seguridad dinámico de Azure AD
- Habilitar la funcionalidad de grupo de seguridad para un catálogo de Azure AD
- Eliminar un catálogo de máquinas con un grupo de seguridad de dispositivos unido a Azure AD

> **Importante:**
>
> - Para crear un catálogo de máquinas con el grupo de seguridad dinámico de Azure AD, agregar máquinas al catálogo y eliminar el catálogo de máquinas, debe tener un token de acceso a Azure AD. Para obtener información sobre cómo obtener el token de acceso a Azure AD, consulte https://docs.microsoft.com/en-us/graph/graph-explorer/graph-explorer-features#consent-to-permissions/.
> - Para solicitar un token de acceso en Azure AD, Citrix solicita el permiso **Group.ReadWrite.All** para la API de Microsoft Graph. Un usuario de Azure AD que tenga el permiso de consentimiento del administrador para todo el arrendatario puede conceder el permiso **Group.ReadWrite.All** para la API de Microsoft Graph. Para obtener información sobre cómo conceder el "consentimiento del administrador para todo el arrendatario" a una solicitud en Azure Active Directory (Azure AD), consulte el documento https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent/ de Microsoft.

### Crear un catálogo de máquinas con un grupo de seguridad dinámico de Azure AD

1. En la interfaz de usuario para configuración del catálogo de máquinas de la consola web, en la página **Identidades de las máquinas**, seleccione **Unido a Azure Active Directory**.
2. Inicie sesión en Azure AD.
3. Obtenga el token de acceso a la API de MS Graph. Utilice este token de acceso como valor del parámetro `$AzureADAccessToken` cuando ejecute los comandos de **PowerShell**.
4. Ejecute el siguiente comando para comprobar si el nombre del grupo de seguridad dinámico existe en el arrendatario.

```
Get-AcctAzureADSecurityGroup
 –AccessToken  $AzureADAccessToken
 –Name "SecurityGroupName"
<!--NeedCopy-->
```

5. Cree un catálogo de máquinas con el ID de arrendatario, el token de acceso y el grupo de seguridad dinámico. Ejecute el siguiente comando para crear un grupo de identidades (IdentityPool) con `IdentityType=AzureAD` y crear un grupo de seguridad dinámico en Azure.

```
New-AcctIdentityPool
-AllowUnicode
-IdentityPoolName "SecurityGroupCatalog"
-NamingScheme "SG-VM-###"
-NamingSchemeType "Numeric" -Scope @()
-ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
-WorkgroupMachine
-IdentityType "AzureAD"
-DeviceManagementType "None"
-AzureADTenantId  620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupName "SecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Habilitar la funcionalidad de grupo de seguridad para un catálogo de Azure AD

Puede habilitar la funcionalidad de seguridad dinámica para un catálogo de Azure AD que se haya creado sin la funcionalidad grupo de seguridad dinámico habilitada. Para hacerlo:

1. Cree manualmente un nuevo grupo de seguridad dinámico. También puede reutilizar un grupo de seguridad dinámico existente.
2. Inicie sesión en Azure AD y obtenga el token de acceso a la API de MS Graph. Utilice este token de acceso como valor del parámetro `$AzureADAccessToken` cuando ejecute los comandos de **PowerShell**.

> **Nota:**
>
> Para obtener información sobre los permisos que requiere el usuario de Azure AD, consulte https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent#prerequisites/.

3. Ejecute el siguiente comando para conectar el grupo de identidades al grupo de seguridad dinámico de Azure AD creado.

```
Set-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADTenantId 620387bb-9167-4bdd-8435-e3dccc58369e
-AzureADSecurityGroupNam "ExistingSecurityGroupName"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

Si actualiza el esquema de nomenclatura, Citrix lo actualizará con una nueva regla de pertenencia. Si elimina el catálogo, se eliminará la regla de pertenencia, y no el grupo de seguridad.

#### Eliminar un catálogo de máquinas con un grupo de seguridad de dispositivos unido a Azure AD

Al eliminar un catálogo de máquinas, también se elimina el grupo de seguridad de dispositivos unido a Azure AD.

Para eliminar el grupo de seguridad dinámico de Azure AD, haga lo siguiente:

1. Inicie sesión en Azure AD.
2. Obtenga el token de acceso a la API de MS Graph. Utilice este token de acceso como valor del parámetro `$AzureADAccessToken` cuando ejecute los comandos de **PowerShell**.
3. Ejecute este comando:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Crear un grupo de seguridad dinámico de Azure AD bajo un grupo de seguridad asignado de Azure AD existente

Puede crear un grupo de seguridad dinámico de Azure AD bajo un grupo de seguridad asignado de Azure AD existente. Puede realizar lo siguiente:

- Obtener información del grupo de seguridad.

- Obtener todos los grupos de seguridad asignados de Azure AD que se sincronizan desde el servidor de AD local o los grupos de seguridad asignados a los que se pueden asignar roles de Azure AD.
- Obtener todos los grupos de seguridad dinámicos de Azure AD.
- Agregar un grupo de seguridad dinámico de Azure AD como miembro del grupo asignado de Azure AD.
- Eliminar la pertenencia entre el grupo de seguridad dinámico de Azure AD y el grupo de seguridad asignado de Azure AD al eliminar el grupo de seguridad dinámico de Azure AD junto con el catálogo de máquinas.

También puede ver mensajes de error explícitos cuando se produce un error en alguna de las operaciones.

**Requisito:**

Debe tener el token de acceso a la API de MS Graph al ejecutar los comandos de **PowerShell**.

Para obtener el token de acceso:

1. Abra el explorador de Microsoft Graph e inicie sesión en Azure AD.
2. Debe contar con los permisos **Group.ReadWrite.all** y **GroupMember.ReadWrite.all**.
3. Obtenga el token de acceso del explorador de Microsoft Graph. Utilice este token de acceso cuando ejecute los comandos de **PowerShell**.

Para obtener información del grupo de seguridad por ID de grupo:

1. Obtenga el token de acceso.
2. Busque el ID del objeto de grupo en el portal de Azure.
3. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token> -GroupId <GroupUid>
<!--NeedCopy-->
```

Para obtener grupos de seguridad por nombre simplificado del grupo:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Name <TargetGroupDisplayName>
<!--NeedCopy-->
```

Para obtener grupos de seguridad cuyo nombre simplificado contiene una subcadena:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-SearchString <displayNameSubString>
<!--NeedCopy-->
```

Para obtener todos los grupos de seguridad asignados de Azure AD que se sincronizan desde el servidor de AD local o los grupos de seguridad asignados a los que se pueden asignar roles de Azure AD:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
<!--NeedCopy-->
```

Para obtener todos los grupos de seguridad dinámicos de Azure AD:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Dynamic true
<!--NeedCopy-->
```

Para obtener los grupos de seguridad asignados de Azure AD con un recuento máximo de registros:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroup
-AccessToken <token>
-Assigned true
-MaxRecordCount 10
<!--NeedCopy-->
```

Para agregar un grupo de seguridad dinámico de Azure AD como miembro del grupo de seguridad asignado de Azure AD:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Add-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
-RefGroupId <DSG-Id>
<!--NeedCopy-->
```

Para obtener los miembros del grupo de seguridad asignado de Azure AD:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Get-AcctAzureADSecurityGroupMember
-AccessToken <token>
-GroupId <ASG-Id>
<!--NeedCopy-->
```

> **Nota:**
>
> `Get-AcctAzureADSecurityGroupMember` le proporciona únicamente los miembros directos del grupo de seguridad situado bajo el grupo de seguridad asignado de Azure AD.

Para eliminar la pertenencia entre el grupo de seguridad dinámico de Azure AD y el grupo de seguridad asignado de Azure AD al eliminar el grupo de seguridad dinámico de Azure AD junto con el catálogo de máquinas:

1. Obtenga el token de acceso.
2. Ejecute el siguiente comando de **PowerShell** en la consola de **PowerShell**:

```
Remove-AcctIdentityPool
-IdentityPoolName "SecurityGroupCatalog"
-AzureADAccessToken $AzureADAccessToken
<!--NeedCopy-->
```

### Modificar el nombre del grupo de seguridad dinámico de Azure AD

Se puede modificar el nombre del grupo de seguridad dinámico de Azure AD asociado a un catálogo de máquinas. Esta modificación hace que la información del grupo de seguridad almacenada en el objeto del grupo de identidades de Azure AD sea coherente con la información almacenada en Azure Portal.

> **Nota:**

> Los grupos de seguridad dinámicos de Azure AD no incluyen los grupos de seguridad sincronizados desde instancias de AD locales ni otros tipos de grupos, como el grupo de Office 365.

El nombre del grupo de seguridad dinámico de Azure AD se puede modificar mediante la interfaz de Configuración completa y los comandos de **PowerShell**.

Para modificar el nombre del grupo de seguridad dinámico de Azure AD mediante **PowerShell**:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de **PowerShell** específicos de Citrix.
3. Ejecute el comando `Set-AcctIdentityPool -AzureAdSeurityGroupName [DSG-Name]`.

Si no se puede modificar el nombre del grupo de seguridad dinámico de Azure AD, recibirá los mensajes de error correspondientes.

## Crear catálogos con Microsoft Intune habilitado

May 17, 2024

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

Este artículo describe cómo crear catálogos habilitados para Microsoft Intune mediante Citrix DaaS. Puede habilitar Microsoft Intune mediante la interfaz de Configuración completa o PowerShell.

Para obtener información sobre los requisitos, las limitaciones y las consideraciones, consulte Microsoft Intune.

### Usar la interfaz de Configuración completa

La información siguiente complementa a las instrucciones del artículo Crear catálogos de máquinas. Esta función requiere la selección de **Unido a Azure Active Directory** en **Identidades de las máquinas** durante la creación del catálogo. Siga las instrucciones generales de ese artículo y tenga en cuenta los detalles específicos de esta función.

En el asistente para la creación de catálogos:

- En la página **Identidades de las máquinas**, seleccione **Unido a Azure Active Directory** y, a continuación, **Inscribir las máquinas en Microsoft Intune**. Si está habilitada, inscriba las máquinas en Microsoft Intune para su administración.

### Usar PowerShell

He aquí los pasos de PowerShell equivalentes a las operaciones de Configuración completa.

Para inscribir máquinas en Microsoft Intune mediante el SDK de PowerShell remoto, utilice el parámetro `DeviceManagementType` en `New-AcctIdentityPool`. Esta función requiere que el catálogo esté unido a Azure AD y que Azure AD posea la licencia correcta de Microsoft Intune. Por ejemplo:

```
1 New-AcctIdentityPool -AllowUnicode -DeviceManagementType "Intune"
     IdentityType="AzureAD" -WorkgroupMachine -IdentityPoolName "
     AzureADJoinedCatalog" -NamingScheme "AzureAD-VM-##" -
     NamingSchemeType "Numeric" -Scope @() -ZoneUid "81291221-d2f2-49d2-
     ab12-bae5bbd0df05"
2 <!--NeedCopy-->
```

### Solucionar problemas técnicos

Si las máquinas no logran inscribirse en Microsoft Intune, haga lo siguiente:

- Compruebe si las máquinas aprovisionadas por MCS están unidas a Azure AD. Las máquinas no logran inscribirse en Microsoft Intune si no están unidas a Azure AD. Consulte https://docs.citrix.com/en-us/citrix-daas/install-configure/create-machine-identities-joined-catalogs/create-azure-ad-joined-catalogs.html para solucionar problemas de unión a Azure AD.
- Compruebe si a su arrendatario de Azure AD se le ha asignado la licencia de Intune adecuada. Consulte https://learn.microsoft.com/en-us/mem/intune/fundamentals/licenses para ver los requisitos de licencias de Microsoft Intune.
- En el caso de los catálogos que usan imágenes maestras con la versión 2206 de VDA o anterior, compruebe el estado de aprovisionamiento de la extensión **AADLoginForWindows** para las máquinas. Si la extensión **AADLoginForWindows** no existe, los posibles motivos son:
  - `IdentityType` del grupo de identidades asociado al esquema de aprovisionamiento no está configurado en `AzureAD` o `DeviceManagementType` no está configurado en `Intune`. Para comprobarlo, ejecute `Get-AcctIdentityPool`.
  - La directiva de Azure bloquea la instalación de la extensión **AADLoginForWindows**.
- Para solucionar problemas de aprovisionamiento de la extensión **AADLoginForWindows**, puede comprobar los registros en `C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.ActiveDirectory.AADLoginForWindows` de la máquina aprovisionada por MCS.

> **Nota:**
>
> MCS no se basa en la extensión `AADLoginForWindows` para unir una máquina virtual a Azure AD y realizar la inscripción en Microsoft Intune cuando se usa una imagen maestra con la versión 2209 de VDA o una posterior. En este caso, la extensión `AADLoginForWindows` no se instalará en la máquina aprovisionada por MCS. Por consiguiente, no se pueden recopilar los registros de aprovisionamiento de la extensión `AADLoginForWindows`.

- Consulte los registros de eventos de Windows en **Registros de aplicaciones y servicios > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider**.

## Crear catálogos unidos a Azure Active Directory híbrido

May 17, 2024

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

En este artículo se describe cómo crear catálogos unidos a Azure Active Directory (AD) híbrido mediante Citrix DaaS.

Puede crear catálogos unidos a Azure AD mediante la interfaz de Configuración completa o PowerShell.

Para obtener información sobre los requisitos, las limitaciones y los aspectos a tener en cuenta, consulte Unidos a Azure Active Directory híbrido.

### Usar la interfaz de Configuración completa

La información siguiente complementa a las instrucciones del artículo Crear catálogos de máquinas. Para crear catálogos unidos a Azure AD híbrido, siga las instrucciones generales de ese artículo y tenga en cuenta los detalles específicos sobre los catálogos unidos a Azure AD híbrido.

En el asistente para la creación de catálogos:

- En la página **Identidades de máquinas**, seleccione **Unido a Azure Active Directory híbrido**. Las máquinas creadas son propiedad de una organización en las que se ha iniciado sesión con

una cuenta de Active Directory Dominio Services perteneciente a esa organización. Existen en la nube y en instancias locales.

> **Nota:**
>
> Si selecciona **Unido a Azure Active Directory híbrido** como el tipo de identidad, cada máquina del catálogo debe tener una cuenta de equipo de AD correspondiente.

### Usar PowerShell

He aquí los pasos de PowerShell equivalentes a las operaciones de Configuración completa. Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

La diferencia entre los catálogos unidos a AD local y los unidos a Azure AD híbrido radica en la creación del grupo de identidades y las cuentas de máquina.

Para crear un grupo de identidades junto con las cuentas de los catálogos unidos a Azure AD híbrido:

```
1 New-AcctIdentityPool -AllowUnicode -IdentityType "HybridAzureAD" -
    Domain "corp.local" -IdentityPoolName "HybridAADJoinedCatalog" -
    NamingScheme "HybridAAD-VM-##" -NamingSchemeType "Numeric" -OU "CN=
    AADComputers,DC=corp,DC=local" -Scope @() -ZoneUid "81291221-d2f2-49
    d2-ab12-bae5bbd0df05"
2 New-AcctADAccount -IdentityPoolName "HybridAADJoinedCatalog" -Count 10
    -ADUserName "corp\admin1" -ADPassword $password
3 Set-AcctAdAccountUserCert -IdentityPoolName "HybridAADJoinedCatalog" -
    All -ADUserName "corp\admin1" -ADPassword $password
4 <!--NeedCopy-->
```

> **Nota:**
>
> `$password` es la contraseña correspondiente de una cuenta de usuario de AD con permisos de escritura.

Todos los demás comandos que se utilizan para crear catálogos unidos a Azure AD híbrido son los mismos que se usan para los catálogos tradicionales unidos a AD local.

### Ver el estado del proceso de unión a Azure AD híbrido

En la interfaz de Configuración completa, el estado del proceso de unión a Azure AD híbrido es visible cuando las máquinas unidas a Azure AD híbrido de un grupo de entrega están encendidas. Para ver el estado, utilice Buscar para identificar esas máquinas y, a continuación, para cada una de ellas, compruebe la **identidad de la máquina** en la ficha **Detalles** del panel inferior. Esta información puede aparecer en **Identidad de la máquina**:

- Unida a Azure AD híbrido
- Aún no se ha unido a Azure AD

> **Nota:**
>
> - Es posible que se produzca una demora en la unión a Azure AD híbrido cuando la máquina se enciende por primera vez. Esto se debe al intervalo de sincronización de identidad de máquina predeterminado (30 minutos de Azure AD Connect). La máquina se halla en estado unido a Azure AD híbrido solamente después de que las identidades de máquina se hayan sincronizado con Azure AD a través de Azure AD Connect.
> - Si las máquinas no están unidas a Azure AD híbrido, no se registran en el Delivery Controller. Su estado de registro aparece como **Inicialización**.

Además, mediante la interfaz de Configuración completa, puede averiguar por qué las máquinas no están disponibles. Para ello, haga clic en una máquina del nodo **Buscar**, marque **Registro** en la ficha **Detalles** del panel inferior y, a continuación, lea el texto de ayuda para obtener información adicional.

### Solucionar problemas técnicos

Si las máquinas no logran unirse a Azure AD híbrido, haga lo siguiente:

- Compruebe si la cuenta de máquina se ha sincronizado con Azure AD a través del portal de Microsoft Azure AD. Si se ha sincronizado, aparece **Aún no se ha unido a Azure AD**, que indica que el estado de registro está pendiente.

  Para sincronizar las cuentas de máquina con Azure AD, asegúrese de lo siguiente:

  - La cuenta de máquina está en la OU configurada para sincronizarse con Azure AD. Las cuentas de máquina sin el atributo **userCertificate** no se sincronizan con Azure AD aunque estén en la OU configurada para sincronizarse.
  - El atributo **userCertificate** se rellena en la cuenta de la máquina. Utilice Active Directory Explorer para ver el atributo.
  - Azure AD Connect debe haberse sincronizado al menos una vez después de haber creado la cuenta de máquina. Si no es el caso, ejecute manualmente el comando `Start-ADSyncSyncCycle -PolicyType Delta` en la consola de PowerShell de la máquina de Azure AD Connect para activar una sincronización inmediata.

- Para comprobar si el par de claves de dispositivos administrados por Citrix para la unión a Azure AD híbrido se ha insertado correctamente en la máquina, consulte el valor de **DeviceKeyPairRestored** en **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix**.

  Verifique que el valor sea 1. Si no es así, he aquí una serie de posibles razones:

  - `IdentityType` del grupo de identidades asociado al esquema de aprovisionamiento no está configurado en `HybridAzureAD`. Para comprobarlo, ejecute `Get-AcctIdentityPool`.
  - La máquina no se aprovisiona con el mismo esquema de aprovisionamiento del catálogo de máquinas.
  - La máquina no está unida al dominio local. La unión al dominio local es un requisito previo para la unión a Azure AD híbrido.

- Para comprobar los mensajes de diagnóstico, ejecute el comando `dsregcmd /status /debug` en la máquina aprovisionada por MCS.

  - Si la unión a Azure AD híbrido se realiza correctamente, **AzureAdJoined** y **DomainJoined** son **YES** en el resultado de la línea de comandos.
  - Si no es así, consulte la documentación de Microsoft para solucionar los problemas: https://docs.microsoft.com/en-us/azure/active-directory/devices/troubleshoot-hybrid-join-windows-current.
  - Si recibe el mensaje de error **Server Message: The user certificate is not found on the device with id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx**, ejecute el siguiente comando de PowerShell para reparar el certificado de usuario:

```
1  Repair-AcctIdentity -IdentityAccountName TEST\VM1 -Target
      UserCertificate
2  <!--NeedCopy-->
```

Para obtener más información sobre el problema del certificado de usuario, consulte CTX566696.

## Crear catálogos que no estén unidos a ningún dominio

November 4, 2022

En este artículo se describe cómo crear catálogos que no estén unidos a un dominio mediante Citrix DaaS.

Para obtener información sobre los requisitos, las limitaciones y las consideraciones, consulte No unidos a ningún dominio.

Antes de crear el catálogo de máquinas, necesita lo siguiente:

1. Nueva ubicación de recursos

   - Vaya a la interfaz de usuario de la administración de Citrix Cloud > menú de tres líneas de la parte superior izquierda > **Ubicaciones de recursos**.

- Haga clic en **+ Ubicación de recursos**.
- Escriba un nombre para nueva la ubicación de recursos y haga clic en **Guardar**.

2. Cree una conexión de host. Consulte la sección Crear y administrar conexiones para obtener información detallada.

Mediante Citrix DaaS, puede crear catálogos basados en grupos de trabajo o máquinas no unidas a dominios. La creación de máquinas no unidas a un dominio depende de cómo se cree la agrupación de identidades de cuenta. La agrupación de identidades de cuenta es el mecanismo utilizado por MCS para crear y realizar un seguimiento de nombres de máquinas durante el aprovisionamiento del catálogo.

Puede crear catálogos no unidos a ningún dominio mediante la interfaz de Configuración completa o PowerShell.

### Usar la interfaz de Configuración completa

La información siguiente complementa a las instrucciones del artículo Crear catálogos de máquinas. Para crear catálogos que no estén unidos a ningún dominio, siga las instrucciones generales de ese artículo y tenga en cuenta los detalles específicos de los catálogos que no están unidos a ningún dominio.

En el asistente para la creación de catálogos:

- En la página **Identidades de máquina**, seleccione **No unido a un dominio**. Las máquinas creadas no están unidas a ningún dominio.

> **Nota:**
>
> El tipo de identidad **No unido a un dominio** requiere la versión 1811 o una posterior del VDA como el nivel funcional mínimo para el catálogo. Para que esté disponible, actualice el nivel funcional mínimo si es necesario.

### Mediante PowerShell

He aquí los pasos de PowerShell equivalentes a las operaciones de Configuración completa.

Puede crear un grupo de identidades para catálogos que no estén unidos a ningún dominio mediante el SDK de PowerShell remoto.

Por ejemplo, en versiones anteriores todos los campos de Active Directory se proporcionaban en una sola instancia:

```
New-AcctIdentityPool -AllowUnicode -Domain "corp.local" -
    IdentityPoolName "NonDomainJoinedCatalog" -NamingScheme "NDJ-VM-##"
    -NamingSchemeType "Numeric" -OU "CN=Computers,DC=corp,DC=local"* -
    Scope @() -ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
<!--NeedCopy-->
```

Ahora, MCS usa los nuevos parámetros de PowerShell, **WorkgroupMachine** e **IdentityType**, para crear un grupo de identidades para catálogos que no están unidos a ningún dominio. Con el mismo ejemplo anterior, los parámetros eliminan la necesidad de especificar todos los parámetros específicos de AD, incluidas las credenciales de administrador de dominio:

```
New-AcctIdentityPool -AllowUnicode -IdentityType "Workgroup" -
    WorkgroupMachine -IdentityPoolName "NonDomainJoinedCatalog" -
    NamingScheme "NDJ-VM-##" -NamingSchemeType "Numeric" -Scope @() -
    ZoneUid "81291221-d2f2-49d2-ab12-bae5bbd0df05"
<!--NeedCopy-->
```

Todos los demás comandos que se utilizan para crear catálogos no unidos a ningún dominio son los mismos que para los catálogos tradicionales unidos a Active Directory local.

## Administrar catálogos de máquinas

June 13, 2024

> **Nota:**
>
> En este artículo, se describe cómo administrar catálogos con la interfaz de Configuración completa y los comandos de PowerShell. Si ha creado el catálogo con la interfaz de Distribución rápida y sigue utilizando esa interfaz para administrarlo, consulte las instrucciones de Administrar catálogos en Distribución rápida.

### Introducción

Puede agregar o quitar máquinas de un catálogo de máquinas, además de cambiarlo de nombre, modificar su descripción o administrar sus cuentas de equipo de Active Directory.

Asimismo, el mantenimiento de catálogos puede incluir las tareas de comprobar que cada máquina tenga los últimos cambios de configuración y las actualizaciones más recientes del sistema operativo o del software antivirus.

- Los catálogos que contienen máquinas agrupadas aleatorias que se han creado con Machine Creation Services (MCS) pueden mantener las máquinas mediante la actualización de la imagen utilizada en el catálogo y, luego, de las máquinas en sí. Este método permite actualizar de forma eficiente una gran cantidad de máquinas de usuario.

- En el caso de los catálogos que contienen máquinas estáticas asignadas permanentemente, puede administrar la imagen o la plantilla que utilizan actualmente esos catálogos, pero solo las máquinas que agregue a los catálogos posteriormente se crearán con la nueva imagen o plantilla.
- En el caso de los catálogos de acceso con Remote PC, las actualizaciones de las máquinas de los usuarios se administran fuera de la interfaz de administración de Configuración completa. Puede realizar esta tarea de forma individual o colectiva mediante herramientas de distribución de software de terceros.

Para obtener información sobre la creación y la administración de conexiones con hosts de hipervisores y servicios de nube, consulte Crear y administrar conexiones y recursos.

> **Nota:**
>
> MCS no es compatible con Windows 10 IoT Core ni Windows 10 IoT Enterprise. Consulte el sitio de Microsoft para obtener más información.

### Acerca de las instancias persistentes

Al actualizar la imagen maestra de un catálogo de MCS que contiene máquinas persistentes, cualquier máquina nueva que se agregue al catálogo utilizará la imagen actualizada. Las máquinas existentes siguen utilizando la imagen maestra original. El proceso de actualización de una imagen se realiza de la misma manera que cuando se trata de cualquier otro tipo de catálogo. Se deben tener en cuenta las siguientes cuestiones:

- Con catálogos de discos persistentes, las máquinas preexistentes no se actualizan a la nueva imagen. Sin embargo, todas las máquinas nuevas que se agreguen al catálogo utilizan la nueva imagen.
- Para catálogos de discos no persistentes, la imagen de la máquina se actualiza la próxima vez solo si la máquina se reinicia en Studio o PowerShell. Si la máquina se reinicia desde el hipervisor fuera de Studio, el disco no se restablece.
- En el caso de catálogos no persistentes, si quiere utilizar imágenes diferentes para máquinas diferentes, las imágenes deben residir en catálogos separados.

### Administrar catálogos de máquinas

Puede administrar un catálogo de máquinas de dos maneras:

- Mediante la interfaz de Configuración completa
- Mediante PowerShell

### Usar la interfaz de Configuración completa

En esta sección se detalla cómo puede administrar los catálogos mediante la interfaz de Configuración completa:

- Ver detalles de un catálogo
- Agregar máquinas a un catálogo
- Eliminar máquinas de un catálogo
- Modificar un catálogo
- Cambiar el nombre de un catálogo
- Eliminar un catálogo
- Administrar cuentas de equipo de Active Directory en un catálogo
- Cambiar la imagen maestra de un catálogo
- Cambiar el nivel funcional o deshacer el cambio
- Clonar un catálogo
- Organizar los catálogos por medio de carpetas
- Configurar la actualización automática de versiones de los VDA
- Administrar el conjunto de configuraciones de un catálogo
- Reintentar la creación de catálogos
- (Solo agentes VDA no aprovisionados por Citrix) Generar y administrar los tokens de inscripción

### Ver detalles de un catálogo

1. Use la función de búsqueda para localizar un catálogo de máquinas específico. Para obtener instrucciones, consulte Buscar instancias.
2. En los resultados de la búsqueda, seleccione un catálogo según sea necesario.
3. Consulte la siguiente tabla para ver las descripciones de las columnas del catálogo.
4. Haga clic en una ficha del panel de detalles inferior para obtener más información sobre este catálogo.

| Columna | Descripción |
|---|---|
| Catálogo de máquinas | El nombre y el tipo de asignación del catálogo. Los tipos de asignación incluyen Aleatoria: Las máquinas del catálogo se asignan a un usuario de forma aleatoria. Permanente: Las máquinas del catálogo se asignan a un usuario de forma permanente. |
| Tipo de máquina | El tipo de sesión admitido de las máquinas del catálogo. Los posibles valores incluyen Tipo de sistema operativo: SO multisesión (virtual); Datos de usuario: Descartar. Tipo de sistema operativo: SO multisesión (virtual); Datos de usuario: En disco local Tipo de sistema operativo: SO de sesión única (acceso con Remote PC) Tipo de sistema operativo: SO de sesión única (virtual); Datos de usuario: Descartar Tipo de sistema operativo: SO de sesión única |

| Columna | Descripción |
| --- | --- |
| Recuento de máquinas | El recuento de máquinas en el catálogo y el método de aprovisionamiento. Los métodos de aprovisionamiento posibles incluyen: Machine Creation Services (máquina de MCS), Manual y Citrix Provisioning Services. |
| Recuento asignado | La cantidad de máquinas del catálogo asignadas a un grupo de entrega. |
| Carpeta | La ubicación del catálogo en el árbol de **Catálogos de máquinas**. Muestra el nombre de la carpeta en la que se encuentra el catálogo (incluida la barra invertida al final) o − si el catálogo está en el nivel raíz. |
| Actualización de versión de VDA | Estado de la actualización de versión de VDA. Entre los valores posibles se incluyen: No configurado, Programado, Disponible y Actualizado. |
| Estado de la imagen | El estado de actualización de la imagen del catálogo. Solo se aplica a los catálogos de máquinas no persistentes. Los valores posibles incluyen: Totalmente actualizada, Parcialmente actualizada, Actualizaciones pendientes y En preparación |

## Agregar máquinas a un catálogo

Antes de comenzar:

- Compruebe que el host de virtualización (hipervisor o proveedor de servicios en la nube) contenga procesadores, memoria y capacidad de almacenamiento suficientes para dar cabida a las máquinas adicionales.
- Compruebe que tiene suficientes cuentas de equipo de Active Directory sin usar. Si utiliza cuentas existentes, tenga en cuenta que la cantidad de máquinas que puede agregar se limita a la cantidad de cuentas disponibles.

- Si usa la interfaz de administración de Configuración completa con el fin de crear cuentas de equipo de Active Directory para las máquinas adicionales, debe tener los permisos de administrador de dominio apropiados.

> **Sugerencia:**
>
> Si la cuenta de Citrix DaaS utilizada para agregar máquinas al catálogo de máquinas tiene permisos de AD restringidos, agregue todos los Cloud Connectors que quiera usar en la pantalla **Iniciar sesión en**.

Para agregar máquinas a un catálogo:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en la barra de acciones.
3. En la página **Máquinas virtuales**, seleccione la cantidad de máquinas virtuales que quiere agregar.
4. En la página **Identidades de las máquinas**, configure los parámetros de la siguiente manera:
    - Seleccione una identidad de la lista.
    - Si procede, indique si se van a crear cuentas o si se van a utilizar cuentas existentes, además de la ubicación (dominio) de estas.

      Si no hay suficientes cuentas existentes de Active Directory para la cantidad de máquinas virtuales que quiere agregar, seleccione el dominio y la ubicación donde se crearán las cuentas.

      Si usa cuentas existentes de Active Directory, vaya a esas cuentas o seleccione **Importar** y especifique un archivo `.csv` que contenga los nombres de cuenta. Compruebe que hay cuentas suficientes para las máquinas que está agregando. La interfaz de Configuración completa administra estas cuentas. Permita que dicha interfaz restablezca las contraseñas de todas las cuentas, o bien, especifique la contraseña de la cuenta (que debe ser la misma para todas las cuentas).
    - Si otros catálogos utilizan esta agrupación de identidades, no puede cambiarla por otra agrupación mediante Configuración completa. En su lugar, utilice el cmdlet **Set-ProvScheme** de PowerShell. Para obtener más información, consulte la documentación del SDK de Citrix Virtual Apps and Desktops.
    - Especifique un esquema de nombres de cuenta con marcas hash para indicar dónde aparecerán los números o las letras secuenciales. Por ejemplo, un esquema de denominación PC-Ventas-## (con números del 0 al 9 seleccionados) da como resultado cuentas de equipo llamadas PC-Ventas-01, PC-Ventas-02, PC-Ventas-03, etc.

- Si lo quiere, puede especificar con qué empiezan los nombres de las cuentas.

  Al especificar con qué comienzan los nombres de las cuentas, tenga en cuenta este caso: Si los números o las letras iniciales ya están en uso, la primera cuenta creada se designa con los números o letras sin utilizar más próximos a partir de entonces.

  Consulte Administrar el número de secuencia del nombre de máquina para personalizar los números de secuencia de las máquinas que se implementan con MCS, a través de los comandos de PowerShell.

5. En la página **Credenciales de dominio**, seleccione **Introducir credenciales** e introduzca credenciales de usuario con permisos suficientes para crear cuentas de máquina.

Las máquinas se crean en un proceso en segundo plano, que puede tardar mucho tiempo si se crea una gran cantidad de máquinas. La creación de máquinas continúa aunque cierre la interfaz de administración de Configuración completa.

#### Usar archivos CSV para agregar máquinas en bloque a un catálogo

Puede agregar máquinas en bloque mediante archivos CSV. La función está disponible para todos los catálogos, excepto los catálogos aprovisionados a través de MCS.

Para agregar máquinas en bloque a un catálogo, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en la barra de acciones. Aparecerá la ventana **Agregar máquinas**.
3. Seleccione **Agregar archivo CSV**. Aparecerá la ventana **Agregar máquinas en bloque**.
4. Seleccione **Descargar plantilla CSV**.
5. Rellene el archivo de la plantilla.
6. Busque el archivo o arrástrelo hasta aquí para cargarlo.
7. Seleccione **Validar** para comprobar la validación de la importación.
8. Seleccione **Importar** para completar el proceso.

#### Aspectos que tener en cuenta al usar archivos CSV para agregar máquinas

> **Nota:**
>
> - Para los usuarios que no son de Active Directory, debe escribir sus nombres en este formato: `<identity provider>:<user name>`. Ejemplo: `AzureAD:username`.
> - Los nombres de las VM distinguen mayúsculas de minúsculas. Al introducir las rutas de las VM, asegúrese de introducir los nombres de las VM correctamente.

Cuando modifique el archivo de plantilla de CSV, tenga en cuenta lo siguiente:

- La función ofrece mayor flexibilidad para agregar máquinas en bloque a partir de un archivo CSV. En el archivo, puede agregar solo máquinas (para utilizarlas con asignaciones automáticas de usuario), o bien, agregar máquinas junto con asignaciones de usuario. Escriba los datos en el siguiente formato:
  - Para pares de cuenta de máquina y nombre de usuario (samName):
    * Dominio\NombreDeEquipo1, Dominio\NombreDeUsuario1
    * Dominio\NombreDeEquipo2, Dominio\NombreDeUsuario1;Dominio\NombreDeUsuario2
    * Dominio\NombreDeEquipo3, AzureAD:NombreDeUsuario
  - Solo para cuentas de máquina:
    * Dominio\NombreDeEquipo1
    * Dominio\NombreDeEquipo2
  - Para pares de nombres de usuario y VM:
    * XDHyp:\Conexiones\NombreDeConexión\NombreDeRegión\carpeta.vm\NombreDeVM1.vm,Dom
    * XDHyp:\Conexiones\NombreDeConexión\NombreDeRegión\carpeta.vm\NombreDeVM2.vm,Dom
  - Solo para máquinas virtuales:
    * XDHyp:\Conexiones\NombreDeConexión\NombreDeRegión\carpeta.vm\NombreDeVM1.vm,Dom
    * XDHyp:\Conexiones\NombreDeConexión\NombreDeRegión\carpeta.vm\NombreDeVM2.vm,Dom

    Por ejemplo:
    `XDHyp:\Connections\xpace-scale\East US.region\vm.folder\wsvdaV3-2.vm`

    donde,
    * `xpace-scale` es el NombreDeConexión: el nombre de la conexión que introdujo en **Configuración completa > Alojamiento > Agregar conexiones y recursos**. Para obtener más información, consulte Crear una conexión y recursos.
    * `East US.region` es la Región: el nombre de la región con una extensión `.region` .
    * `wsvdaV3-2.vm` es el NombreDeVM: el nombre de la máquina virtual con una extensión `.vm`.
- La cantidad máxima de máquinas que puede contener un archivo es 1000. Para importar más de 1000 máquinas, distribúyalas en diferentes archivos y, a continuación, importe esos archivos uno por uno. No se recomienda importar más de 1000 máquinas. De lo contrario, la creación del catálogo puede tardar mucho tiempo en completarse.

También puede exportar máquinas de un catálogo en la misma página **Agregar máquinas**. El CSV exportado de máquinas se puede utilizar como plantilla al agregar máquinas en bloque. Para exportar máquinas:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo de máquinas y, a continuación, seleccione **Agregar máquinas** en la barra de acciones. Aparecerá la ventana **Agregar máquinas**.
3. Seleccione **Exportar en un archivo CSV**. Se descarga un archivo CSV que contiene una lista de las máquinas.
4. Abra el archivo CSV para agregar o modificar máquinas según sea necesario. Para agregar máquinas en bloque mediante el archivo CSV guardado, consulte la sección anterior, Usar archivos CSV para agregar máquinas en bloque a un catálogo.

> **Nota:**
>
> - Esta función no está disponible para los catálogos de acceso con Remote PC y aprovisionados por MCS.
> - La exportación e importación de máquinas en archivos CSV solo se permite entre catálogos del mismo tipo.

#### Inscribir máquinas en catálogos mediante la herramienta de inscripción de VDA de WebSocket

La herramienta de inscripción de VDA de WebSocket facilita la inscripción basada en tokens para máquinas VDA. Esta herramienta le ayuda a convertir una conexión en una conexión de WebSocket agregando el VDA al catálogo de máquinas mediante el token de inscripción.

> **Nota:**
>
> Esta herramienta está diseñada para inscribir máquinas VDA que no se han inscrito en ningún catálogo de máquinas.

Siga las instrucciones para ejecutar la herramienta de inscripción:

1. Inicie sesión en el VDA.
2. Localice la herramienta `EnrollMachine.exe`, en `C:\Program Files\Citrix\Virtual Desktop Agent\Web Socket Vda Enrollment Tool`.
3. Ejecute la herramienta con los parámetros de entrada apropiados. Por ejemplo, `EnrollMachine.exe -websocket_token_string:xxxxxxxxx`

En la siguiente tabla se describen los parámetros de entrada de la herramienta de inscripción:

| Nombre del parámetro | Si son necesarias | Descripción | Ejemplo |
|---|---|---|---|
| -websocket_token_stdin | Sí | Lee el token de inscripción. | .\EnrollMachine.exe -websocket_token_stdin |
| -websocket_token_string | | Lee el token de inscripción directamente desde el parámetro de la línea de comandos. | .\EnrollMachine.exe -websocket_token_string:<token> |
| -websocket_token_file:[token-file-path] | | Lee el token de inscripción de la ruta proporcionada. | .\EnrollMachine.exe -websocket_token_file:C:\token\test2.txt |
| log:[log-file-path] | No | Muestra los registros de la herramienta de inscripción. | .\EnrollMachine.exe log:[C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt] |
| -help | No | Muestra un breve texto de ayuda. | .\EnrollMachine.exe -help |

Una vez que se haya inscrito correctamente, recibirá un mensaje de confirmación en la herramienta y en los registros. Asegúrese de iniciar sesión en la configuración completa para verificar que la máquina VDA se ha agregado al catálogo y que el estado de la máquina está registrado.

**Solución de problemas** De forma predeterminada, puede encontrar los registros de la herramienta de inscripción en:

`C:\ProgramData\Citrix\EnrollMachine\EnrollMachine.txt`

Si ha especificado una ruta diferente para los registros, puede usar `log:[log-file-path]` para recuperarlos.

En la siguiente tabla se enumeran los códigos devueltos por la herramienta de inscripción:

| Código | Cadena | Descripción |
|---|---|---|
| 0 | Success | Un VDA se agregó correctamente al catálogo de máquinas. |
| -1 | InvalidArgument | El parámetro de entrada del token de inscripción no es válido. |
| -2 | BrokerAgentNotFound | No se encuentra el servicio de agente intermediario. |
| -3 | TokenInvalid | El token introducido no es válido. |
| -4 | TokenMissingRequiredClaims | Faltan las notificaciones necesarias para el token, por ejemplo, CustomerId o los URI de inscripción. |
| -5 | InternalError | Se ha producido un error general. |
| -6 | TimedOut | Se ha agotado el tiempo de espera de la tarea. |
| -7 | FailedToDetermineMachineADJoinStatus | El servicio que devuelve el estado de unión al AD de la máquina falló. |
| -8 | ADMachineFailedToFindSid | El servicio que devuelve el Sid de la máquina de AD falló. |
| -9 | EnrollRequestFailed | La solicitud falló debido a un error de HTTP. |
| -10 | EnrollResponseMissingRequiredFields | A la respuesta de la herramienta de inscripción le falta el parámetro `VirtualSiteId`. |
| -11 | InsufficientPermission | No tiene los permisos necesarios para ejecutar la tarea. |
| -12 | FailedToDetermineMachineAadJoinStatus | El servicio que comprueba el estado de unión al AD de la máquina devuelve un error. |

| Código | Cadena | Descripción |
|---|---|---|
| -13 | AadMachineFailedToFindDeviceId | El parámetro adicional `AAD device id` agregado por el sistema está vacío. |
| -14 | AadDeviceIdNotValid | El parámetro adicional `AAD device id` agregado por el sistema no es un GUID válido. |
| -15 | NoValidMacAddress | Dirección MAC no válida. |
| -16 | FailedToGetComputerHostNameForVdaInstanceName | No se pudo obtener el nombre de host del equipo para establecer el parámetro adicional `VdaInstanceName`. |
| -17 | VirtualDesktopAgentRegistryKeyFailedToOpen | No se pudo abrir la clave de registro del VDA para escribir la lista de los Delivery Controller. |
| -18 | Se alcanzó el recuento máximo de token fallidos | Se alcanzó el recuento máximo de token fallidos. |

### Eliminar máquinas de un catálogo

Después de eliminar una máquina de un catálogo, los usuarios ya no podrán acceder a ella. Por eso, antes de eliminar una máquina, compruebe que:

- Existe una copia de seguridad de los datos del usuario, si fueran útiles.
- Todos los usuarios han cerrado la sesión. La activación del modo de mantenimiento impide nuevas conexiones a una máquina.
- Las máquinas se apagan.

Para eliminar máquinas de un catálogo:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Seleccione una o varias máquinas y, a continuación, seleccione **Eliminar** en la barra de acciones.
4. Si piensa eliminar máquinas persistentes del catálogo, elija si quiere eliminarlas también del hipervisor o del servicio de la nube. Si decide eliminarlas, indique si quiere conservar, inhabili-

tar o eliminar sus cuentas de Active Directory.

Al eliminar máquinas persistentes de un catálogo de Azure Resource Manager, las máquinas y los grupos de recursos asociados se eliminan de Azure aunque decida conservarlos.

Al eliminar máquinas no persistentes de un catálogo, estas se eliminan automáticamente del hipervisor o del servicio de la nube.

### Modificar un catálogo

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Modificar catálogo de máquinas** en la barra de acciones.
3. En la página **Ámbitos**, cambie los ámbitos.
4. En la página de tarjetas **NIC**, haga lo siguiente:

   - Para cambiar la asignación de subredes de una NIC, seleccione una red en el campo **Red asociada**.
   - Para agregar una asignación de subred, seleccione **Agregar NIC**, seleccione una red en el campo **Red asociada** y seleccione **Guardar**.

   Solo las subredes presentes en el host asociado al catálogo aparecen en el campo **Red asociada**.

   Solo se puede agregar NIC a los catálogos de máquinas de Azure sin perfiles de máquina.

   > **Nota:**
   >
   > - En el caso de los catálogos de máquinas de AWS, no se puede asignar la misma subred a más de una NIC.
   > - En el caso de los catálogos de máquinas con perfiles de máquina, la cantidad de NIC del catálogo debe ser igual a la cantidad de NIC del perfil de la máquina.
   > - Esta función no es compatible con los hipervisores de IBM Cloud.
   > - Esta función solo es compatible con Nutanix Prism Element en el caso de los hipervisores Nutanix.

5. En la página **Actualización de versión de VDA**, cambie o seleccione la versión del VDA a la que quiere actualizarse. Para obtener más información, consulte Actualización de versión de VDA.
6. Es posible que aparezcan otras páginas, según el tipo de catálogo.

   Para los catálogos creados con una imagen de Azure Resource Manager, se ven las siguientes páginas. Tenga en cuenta que los cambios que haga se aplican solo a las máquinas que agregue al catálogo más adelante. Las máquinas existentes permanecen sin cambios.

- En la página **Máquinas virtuales**, cambie el tamaño de la máquina y las zonas de disponibilidad donde quiera crear máquinas.

  > **Nota:**
  >
  > – Solo se muestran los tamaños de máquina que admite el catálogo.
  > – Si es necesario, seleccione **Mostrar solo los tamaños de máquinas utilizados en otros catálogos de máquinas** para filtrar la lista de tamaños de máquinas.

- En la página **Perfil de máquina**, elija si quiere usar o cambiar un perfil de máquina.
- (Solo cuando el catálogo está configurado con un host de grupo dedicado) En la página **Grupo de hosts dedicado**, elija si quiere cambiar un grupo de hosts.
- En la página **Tipos de almacenamiento y licencias**, elija si quiere cambiar el tipo de almacenamiento, el tipo de licencia y los parámetros de Azure Computer Gallery (disponibles solo cuando se usa **Colocar la imagen preparada en Azure Gallery**).

  > **Nota:**
  >
  > Si el parámetro recién seleccionado no es compatible con el tamaño actual de la máquina, aparece un cuadro de diálogo de advertencia que le informa de que, al cambiar el parámetro, se restablecerá el parámetro de tamaño de la máquina. Si decide continuar, aparecerá un punto rojo junto al menú **Máquinas virtuales** que le pedirá que seleccione un nuevo tamaño de máquina.

Para obtener más información sobre los parámetros disponibles en las páginas, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

Para los catálogos de acceso con Remote PC, se muestran las siguientes páginas:

- En la página **Administración de energía**, cambie los parámetros de administración de energía y seleccione una conexión de administración de energía.
- En la página **Unidades organizativas**, agregue o quite unidades organizativas de Active Directory.

7. En la página **Descripción**, cambie la descripción del catálogo.
8. Haga clic en **Aplicar** para aplicar los cambios realizados y haga clic en **Guardar** para salir.

### Cambiar el nombre de un catálogo

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Cambiar nombre de catálogo de máquinas** en la barra de acciones.

3. Introduzca el nuevo nombre.

### Eliminar un catálogo

Antes de eliminar un catálogo, asegúrese de que:

- Todos los usuarios han cerrado sesión y no hay sesiones desconectadas en ejecución.
- El modo de mantenimiento se activa para todas las máquinas del catálogo, de modo que no se pueden establecer conexiones nuevas.
- Todas las máquinas del catálogo se apagan.
- El catálogo no está asociado a ningún grupo de entrega. Es decir, que el grupo de entrega no contiene máquinas procedentes del catálogo.

Para eliminar un catálogo:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Eliminar catálogo de máquinas** en la barra de acciones.
3. Si el catálogo contiene máquinas persistentes, indique si quiere eliminarlas también del hipervisor o del servicio de la nube. Si decide hacerlo, elija si quiere conservar, inhabilitar o eliminar sus cuentas de equipo de Active Directory.
4. Si es necesario, seleccione **Ocultar progreso** para realizar la eliminación en segundo plano.

> **Nota:**
>
> - Al eliminar un catálogo de Azure Resource Manager, las máquinas y los grupos de recursos asociados se eliminan de Azure aunque decida conservarlos.
> - Al eliminar un catálogo que contiene máquinas no persistentes, esas máquinas se eliminan del hipervisor o del servicio de la nube.
> - Si no se puede acceder al hipervisor o al servicio de nube durante la eliminación del catálogo, se produce un error al eliminar el catálogo y las máquinas virtuales. Si es necesario, puede optar por eliminar los registros de máquinas virtuales únicamente de la base de datos del sitio de Citrix. Para ello, seleccione el catálogo de máquinas en el nodo **Catálogos de máquinas** y, a continuación, realice la eliminación que se muestra en la ficha **Solucionar problemas**. Tenga en cuenta que esta acción deja las máquinas virtuales intactas en el host.

### Administrar cuentas de equipo de Active Directory en un catálogo

Para administrar cuentas de Active Directory en un catálogo de máquinas, puede:

- Liberar cuentas de máquina sin utilizar al quitar cuentas de equipo de Active Directory que haya en catálogos de máquinas con SO de sesión única y con SO multisesión. Estas cuentas se pueden usar para otras máquinas.
- Agregar cuentas de modo que, cuando se agreguen más máquinas al catálogo, las cuentas de equipo ya estén listas. No use barras diagonales (/) en el nombre de una unidad organizativa.

Para administrar cuentas de Active Directory:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Administrar cuentas de AD** en la barra de acciones.
3. Elija si quiere agregar o eliminar las cuentas de equipo. Si agrega cuentas, deberá especificar qué hacer con las contraseñas de cuenta: restablecerlas todas o escribir una contraseña para todas ellas.

   Puede restablecer contraseñas si no conoce las contraseñas de cuenta actuales. Debe tener permisos específicos para realizar el restablecimiento de contraseñas. Si introduce una contraseña, se cambiará la contraseña en las cuentas a medida que se importan. Si elimina una cuenta, elija si la cuenta de Active Directory debe mantenerse, inhabilitarse o eliminarse.

También puede indicar si las cuentas de Active Directory se deben conservar, inhabilitar o eliminar cuando quite máquinas de un catálogo o elimine un catálogo.

### Cambiar la imagen maestra de un catálogo

Se recomienda guardar copias o instantáneas de imágenes antes de cambiar la imagen maestra de un catálogo. La base de datos conserva un registro histórico de las imágenes utilizadas con cada catálogo de máquinas. Si los usuarios tienen problemas con la nueva imagen que implementó en sus escritorios, puede revertirla a la versión anterior para minimizar el tiempo de inactividad de los usuarios. No elimine, mueva ni cambie el nombre de las imágenes. De lo contrario, no podrá revertir la imagen maestra.

> **Importante:**
>
> Al cambiar la imagen maestra de un catálogo persistente, tenga en cuenta lo siguiente: solo las máquinas que agregue al catálogo posteriormente se crearán con la nueva imagen. No implantamos la nueva imagen en las máquinas ya existentes del catálogo.

Una vez actualizada la máquina, se reinicia automáticamente.

### Actualizar o crear una imagen

Antes de cambiar la imagen maestra de un catálogo, para preparar una nueva imagen en el hipervisor de host, actualice una imagen existente o cree otra.

1. En el hipervisor o proveedor del servicio de nube, tome una instantánea de la VM actual y dele un nombre significativo. Esta instantánea se puede utilizar para revertir la imagen maestra.
2. Si es necesario, encienda la máquina virtual de la imagen e inicie sesión.
3. Instale las actualizaciones o realice los cambios necesarios en la imagen.
4. Si la imagen usa un disco Personal vDisk, actualice el inventario.
5. Apague la máquina virtual.
6. Tome una instantánea de la VM y dele un nombre significativo fácilmente reconocible cuando cambie la imagen maestra.

> **Nota:**
>
> Aunque puede crear una instantánea mediante la interfaz de administración, se recomienda crear la instantánea desde la consola de administración del hipervisor y, a continuación, seleccionar la instantánea en la interfaz de administración de Configuración completa. Este método le permite asignar un nombre y una descripción significativos para la instantánea, en lugar de recibir un nombre generado automáticamente. Para imágenes de GPU, puede cambiar la imagen solo a través de la consola XenCenter de XenServer.

### Cambiar la imagen maestra

Para implantar una nueva imagen maestra en todas las máquinas de un catálogo:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Cambiar imagen maestra** en la barra de acciones.
3. En la página **Imagen**, seleccione el host y la imagen que quiere implantar.

   > **Sugerencia:**
   >
   > Para un catálogo creado con MCS, puede anotar su imagen agregando una nota para la imagen. Una nota puede contener hasta 500 caracteres. Cada vez que cambia la imagen maestra, se crea una entrada con una nota relacionada, independientemente de si agrega o no una nota. Si actualiza un catálogo sin agregar una nota, la entrada aparece como nula (-). Para ver el historial de notas de la imagen, seleccione el catálogo, haga clic en

> **Propiedades de plantilla** en el panel inferior y, a continuación, haga clic en **Ver historial de notas**.

4. En la página **Estrategia de implantación**, elija cuándo se cambian las máquinas del catálogo con la nueva imagen (en el siguiente apagado o inmediatamente).

   > **Nota:**
   >
   > La página **Estrategia de implementación** no está disponible para las máquinas virtuales persistentes porque la implementación solo se aplica a las máquinas virtuales no persistentes.

5. En la página **Resumen**, revise la información y seleccione **Finalizar**. Cada máquina se reiniciará automáticamente después de actualizarse.

   Para hacer un seguimiento del progreso de la actualización, busque el catálogo en **Catálogos de máquinas** para ver la barra de progreso integrada y el gráfico de progreso detallado. En el caso de un catálogo no persistente, puede hacer un seguimiento de los estados de actualización de las imágenes a través de la columna **Actualización de imagen**, que incluye **Totalmente actualizada**, **Parcialmente actualizada**, **Actualización pendiente** y **Preparando imagen**.

   > **Sugerencia:**
   >
   > Para mostrar la columna **Actualización de imagen**, seleccione el icono **Columnas que mostrar** en la barra de acciones, seleccione **Catálogo de máquinas > Estado de la imagen** y, a continuación, haga clic en **Guardar**.

Si va a actualizar un catálogo directamente mediante el SDK de PowerShell, puede especificar una plantilla de hipervisor (`VMTemplates`) como alternativa a una imagen o una instantánea de la imagen.

#### Estrategia de implantación

El cambio de la imagen la próxima vez que se apague la máquina afectará inmediatamente a las máquinas que no estén en uso en ese momento, es decir, a las máquinas que no tengan una sesión de usuario activa. Un sistema que está en uso recibe la actualización cuando finaliza la sesión activa actual.

> **Nota:**
>
> La estrategia de implementación solo se aplica a las máquinas virtuales no persistentes.

Se deben tener en cuenta las siguientes cuestiones:

- Las sesiones nuevas no se pueden iniciar hasta que la actualización se haya completado en las máquinas correspondientes.
- Las máquinas de sesión única se actualizan inmediatamente cuando no se están usando o cuando los usuarios no han iniciado sesión en ellas.
- Para un SO multisesión con máquinas secundarias, los reinicios no se producen automáticamente. Deben apagarse y reiniciarse manualmente.

> **Sugerencia:**
>
> Limite la cantidad de máquinas que se reinician mediante la configuración avanzada de una conexión de host. Utilice esta configuración para modificar las acciones realizadas para un catálogo determinado; la configuración avanzada varía en función del hipervisor.

#### Revertir la imagen maestra

Después de aplicar una imagen nueva o actualizada, puede revertirla. Puede ser necesario si surgen problemas con las máquinas recién actualizadas. Cuando revierte una actualización, las máquinas del catálogo vuelven a la última imagen funcional. Las nuevas funciones que requieran la nueva imagen ya no están disponibles. Al igual que en la implantación, la reversión de una máquina implica un reinicio.

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo y, a continuación, seleccione **Revertir imagen maestra** en la barra de acciones.
3. Puede especificar cuándo se aplicará la versión anterior de la imagen a las máquinas tal y como se describe en la operación de implantación.

La reversión solo se aplica a máquinas que deben revertirse. En caso de máquinas que no se hayan cambiado a la imagen nueva o actualizada (por ejemplo, máquinas con usuarios que no han cerrado sesión), los usuarios no reciben mensajes de notificación y no se ven obligados a cerrar la sesión.

Para hacer un seguimiento del progreso de la reversión, busque el catálogo en **Catálogos de máquinas** para ver la barra de progreso integrada y el gráfico de progreso detallado.

La reversión no es posible en ciertos casos, como estos (la opción **Revertir imagen maestra** no se ve).

- No tiene permiso para revertir.
- El catálogo no se creó con MCS.
- El catálogo se creó con una imagen del disco del SO.
- La instantánea utilizada para crear el catálogo está dañada.
- Los cambios de los usuarios en las máquinas del catálogo no se conservan.

- Hay máquinas del catálogo que se están ejecutando.

### Cambiar el nivel funcional o deshacer el cambio

Cambie el nivel funcional del catálogo de máquinas después de actualizar la versión de los VDA de las máquinas a una versión más reciente. Se recomienda actualizar todos los VDA a la versión más reciente para permitir el acceso a todas las funciones nuevas.

Antes de cambiar el nivel funcional de un catálogo de máquinas:

- Inicie las máquinas actualizadas para que se registren en Citrix DaaS. Esto permite a la interfaz de administración determinar si las máquinas del catálogo necesitan actualizarse de versión.

Para cambiar el nivel funcional de un catálogo:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo. En la ficha **Detalles** del panel inferior, se muestra la información de versión.
3. Seleccione **Cambiar nivel funcional**. Si la interfaz de administración detecta que el catálogo necesita cambiar el nivel funcional, muestra un mensaje. Siga las indicaciones. Si una o varias máquinas no se pueden cambiar, aparecerá un mensaje en el que se le explicará el motivo. Para garantizar que todas las máquinas funcionen correctamente. le recomendamos que resuelva esos problemas antes de hacer clic en **Cambiar**.

Después de completar la actualización del catálogo, puede revertir las máquinas a sus versiones anteriores de VDA. Para ello, seleccione el catálogo y, a continuación, seleccione **Deshacer cambio de nivel funcional** en la barra de acciones.

### Clonar un catálogo

Antes de clonar un catálogo, tenga en cuenta esto:

- No se pueden cambiar los parámetros asociados a la administración de máquinas y al sistema operativo. El catálogo clonado hereda esos parámetros del original.
- La clonación de un catálogo puede tardar en completarse. Si es necesario, selecciona **Ocultar progreso** para realizar la clonación en segundo plano.
- El catálogo clonado hereda el nombre del original y tiene el sufijo `Copy`. Puede cambiarle el nombre. Consulte Cambiar el nombre de un catálogo.
- Una vez finalizada la clonación, asegúrese de asignar el catálogo clonado a un grupo de entrega.
- Puede crear un catálogo vacío mediante clonación. Durante la clonación de catálogos, puede establecer el número de máquinas en cero para los catálogos aprovisionados por MCS y no agregar máquinas para los catálogos no aprovisionados por MCS.

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione un catálogo y, a continuación, seleccione **Clonar** en la barra de acciones.
3. En la ventana **Clonar catálogo de máquinas seleccionado**, consulte los parámetros del catálogo clonado y configúrelos según corresponda. Seleccione **Siguiente** para pasar a la página siguiente.
4. En la página **Resumen**, verá un resumen de los parámetros. Seleccione **Finalizar** para iniciar la clonación.
5. Si es necesario, selecciona **Ocultar progreso** para realizar la clonación en segundo plano.

## Organizar los catálogos por medio de carpetas

Puede crear carpetas para organizar los catálogos y acceder a ellos fácilmente. Por ejemplo, puede organizar los catálogos por tipo de imagen o por estructura organizativa.

### Roles obligatorios

De forma predeterminada, debe tener uno de estos roles integrados para crear y administrar carpetas de catálogos: administrador de nube, administrador total o administrador de catálogos de máquinas. Si es necesario, puede personalizar roles para crear y administrar carpetas de catálogos. Para obtener más información, consulte Permisos requeridos.

### Crear una carpeta de catálogo

Antes de empezar, planifique cómo organizar sus catálogos. Se deben tener en cuenta las siguientes cuestiones:

- Puede anidar carpetas con hasta cinco niveles de profundidad (excluyendo la carpeta raíz predeterminada).
- Una carpeta de catálogo puede contener catálogos y subcarpetas.
- Todos los nodos de **Configuración completa** (como los nodos **Catálogos de máquinas** y **Aplicaciones** ) comparten un árbol de carpetas en el back-end. Para evitar conflictos de nombres con otros nodos al cambiar el nombre de las carpetas o moverlas, le recomendamos que asigne nombres diferentes a las carpetas de primer nivel de los distintos nodos.

Para crear una carpeta de catálogo, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.

2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione **Crear carpeta** en la barra de **acciones**.
3. Introduzca un nombre para la nueva carpeta y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Si crea una carpeta en una ubicación no deseada, puede arrastrarla a la ubicación correcta.

#### Mover un catálogo

Puede mover un catálogo entre carpetas. Estos son los pasos detallados:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Ver los catálogos por carpeta. También puede activar **Ver todo** por encima de la jerarquía de carpetas para ver todos los catálogos a la vez.
3. Haga clic con el botón secundario en un catálogo y, a continuación, seleccione **Mover catálogo de máquinas**.
4. Seleccione la carpeta a la que quiere mover el catálogo y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Puede arrastrar un catálogo a una carpeta.

#### Administrar carpetas de catálogos

Puede eliminar, cambiar el nombre y mover las carpetas de catálogos.

Solo puede eliminar una carpeta si esta y sus subcarpetas no contienen catálogos.

Para administrar una carpeta, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione una acción en la barra de **acciones**:
   - Para cambiar el nombre de la carpeta, seleccione **Cambiar nombre de carpeta**.
   - Para eliminar la carpeta, seleccione **Eliminar carpeta**.
   - Para mover la carpeta, seleccione **Mover carpeta**.
3. Siga las instrucciones que aparecen en pantalla para completar los pasos restantes.

**Permisos requeridos**

En la siguiente tabla, se enumeran los permisos necesarios para realizar acciones en las carpetas de catálogos.

| Acción | Permisos requeridos |
|---|---|
| Crear carpetas de catálogos | Crear carpeta de catálogos de máquinas |
| Eliminar carpetas de catálogos | Quitar carpeta de catálogos de máquinas |
| Mover carpetas de catálogos | Mover carpeta de catálogos de máquinas |
| Cambiar nombre de carpetas de catálogos | Modificar carpeta de catálogos de máquinas |
| Mover catálogos a carpetas | Modificar carpeta de catálogos de máquinas y Modificar propiedades de catálogos de máquinas |

## Configurar la actualización automática de versiones de los VDA

> **Importante:**
>
> - Para garantizar una actualización de versión fluida, asegúrese de cumplir los requisitos previos y de revisar los problemas conocidos antes de actualizar los VDA a las versiones CR o LTSR CU. Consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.
> - Al actualizar los VDA LTSR a las versiones LTSR CU (actualización acumulativa), asegúrese de que la versión de los agentes de actualización de VDA que se ejecutan en los VDA sea 7.36.0.7 o posterior. Para obtener más información, consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.
> - Puede cambiar entre VDA CR (Current Release) y VDA LTSR (Long Term Service Release) siempre que cambie de una versión anterior a una versión posterior. No puede cambiar de una versión posterior a una anterior porque se considera una reversión. Por ejemplo, no puede cambiar de la versión 2212 CR a 2203 LTSR (cualquier CU), pero puede actualizar la versión 2112 CR a 2203 LTSR (cualquier CU).
> - También puede actualizar la versión de los VDA mediante PowerShell. Consulte Actualizar la versión de los VDA mediante PowerShell.

Con la función, puede hacer lo siguiente:

- Actualizar la versión de VDA por catálogo
- Modificar o cancelar la actualización de versión programada de un VDA

- Configurar los parámetros de actualización de versión del VDA después de la creación de catálogos
- Actualizar la versión de VDA por máquina

> **Nota:**
>
> - Al programar actualizaciones de versión de VDA para un catálogo, solo se pueden actualizar los VDA del catálogo que tengan instalado el agente de actualización de versiones de VDA.
> - La actualización de versión de un VDA falla cuando la máquina se halla en modo de mantenimiento o cuando hay una sesión activa en la máquina.

### Tipos de máquinas admitidas

Esta función se aplica a estos tipos de máquinas:

- Máquinas persistentes aprovisionadas por MCS (unidas a AD, unidas a Azure AD y no unidas aun dominio). Se implementan mediante **Citrix Machine Creation Services** en la página **Administración de máquinas** durante la creación del catálogo.
- Máquinas de acceso con Remote PC
- Máquinas con Citrix HDX Plus para Windows 365
- Otras máquinas persistentes aprovisionadas mediante tecnologías o servicios de aprovisionamiento que no son de Citrix. Agregue esas máquinas a DaaS para su administración mediante **Otro servicio o tecnología** en la página **Administración de máquinas** durante la creación del catálogo.

Para obtener más información sobre **Citrix Machine Creation Services** y **otras opciones de servicios o tecnologías**, consulte Administración de máquinas.

> **Nota:**
>
> Para las máquinas aprovisionadas con MCS, solo se admiten máquinas persistentes estáticas. No se admiten máquinas aleatorias aunque sean persistentes.

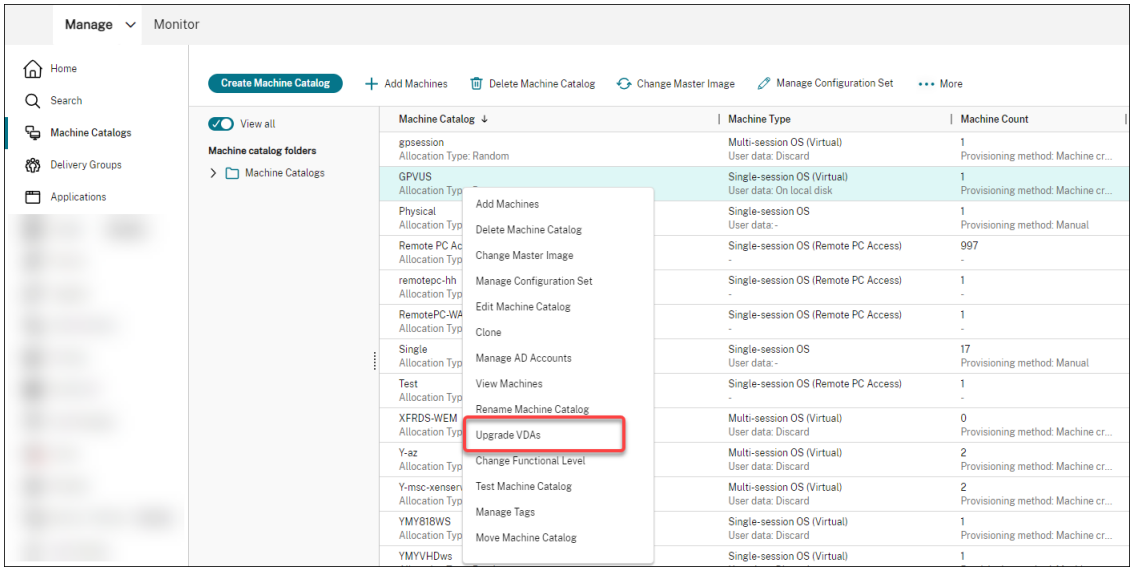
### Actualizar la versión de VDA por catálogo

> **Nota:**
>
> Al programar la actualización de versiones de VDA para un catálogo, tenga en cuenta que se incluirán todas las máquinas del catálogo en el ámbito de la actualización. Por lo tanto, se recomienda hacer una copia de seguridad de esas máquinas antes de iniciar la actualización.

Después de habilitar la actualización de versión de VDA para un catálogo, puede actualizar los VDA del catálogo inmediatamente o programar actualizaciones para el catálogo. Para ello, siga estos pasos:

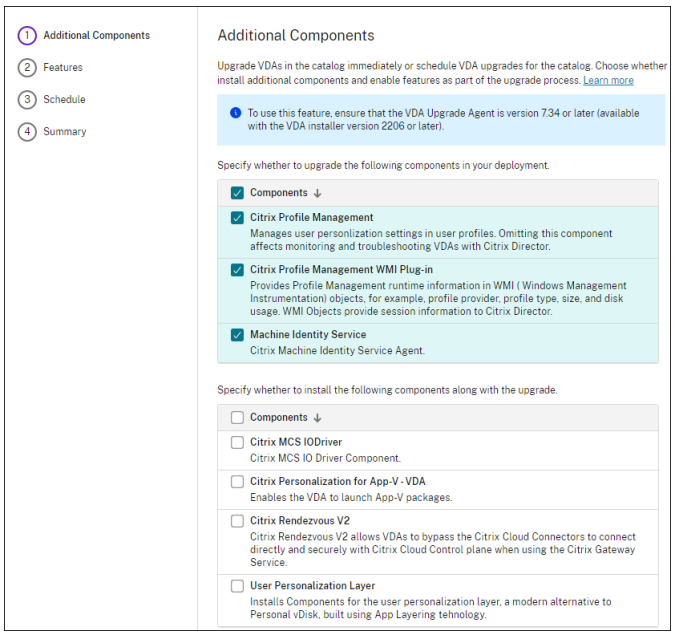
1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.
2. Seleccione el catálogo y, a continuación, **Actualizar versión de VDA** en el menú contextual o la barra de acciones (haga clic con el botón secundario para mostrar el menú contextual). Aparecerá la ventana Actualizar versión de VDA.




3. Elija si quiere actualizar la versión de componentes adicionales de su implementación. También puede optar por instalar ciertos componentes, además de la actualización. Si un componente requiere configuración, debe hacer clic en el botón **Configurar** y definir los parámetros del componente para continuar. Tras la configuración, puede hacer clic en **Modificar** para cambiar la configuración.

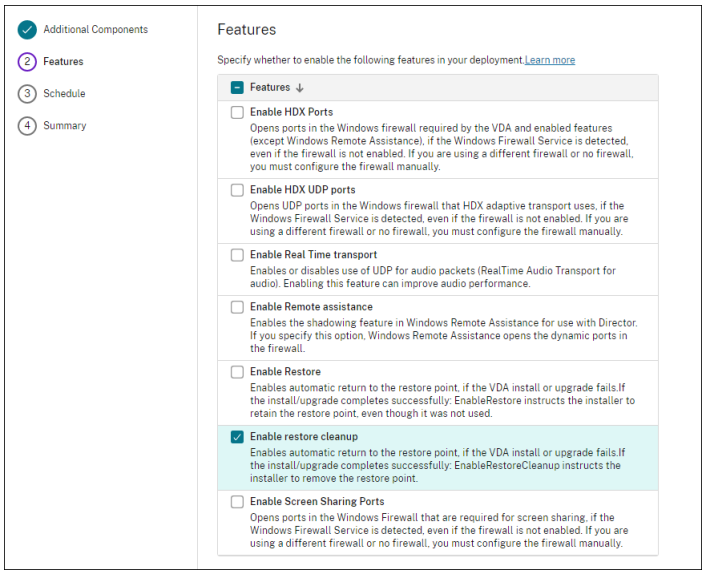
> **Importante:**
>
> - Para utilizar la función de componentes adicionales, asegúrese de que su agente de actualización de versiones de VDA sea la versión 7.34 o una posterior, que se incluye a partir de la versión 2206 del instalador de VDA.
>
> **Nota:**
>
> - Si decide no actualizar la versión de un componente, el componente permanece intacto en la implementación.
> - Para obtener una lista completa de componentes adicionales, consulte Instalar VDA.




4. Haga clic en **Siguiente**.
5. Elija si quiere habilitar alguna de las funciones de la lista. Haga clic en **Siguiente**.

> **Nota:**
>
> De forma predeterminada, la casilla **Habilitar limpieza de restauración** está marcada. Recomendamos habilitar la función de restauración. Con esta función habilitada, se crea un punto de restauración del sistema antes de que comience la actualización de la versión. El punto de restauración se elimina tras la instalación correcta del VDA. Para obtener más información, consulte Restaurar en caso de error al instalar o actualizar.




6. Elija si quiere actualizar la versión de los VDA de forma inmediata o a una hora programada.

- Para actualizar los VDA inmediatamente, seleccione **Actualizar versión** y, a continuación, especifique una duración.

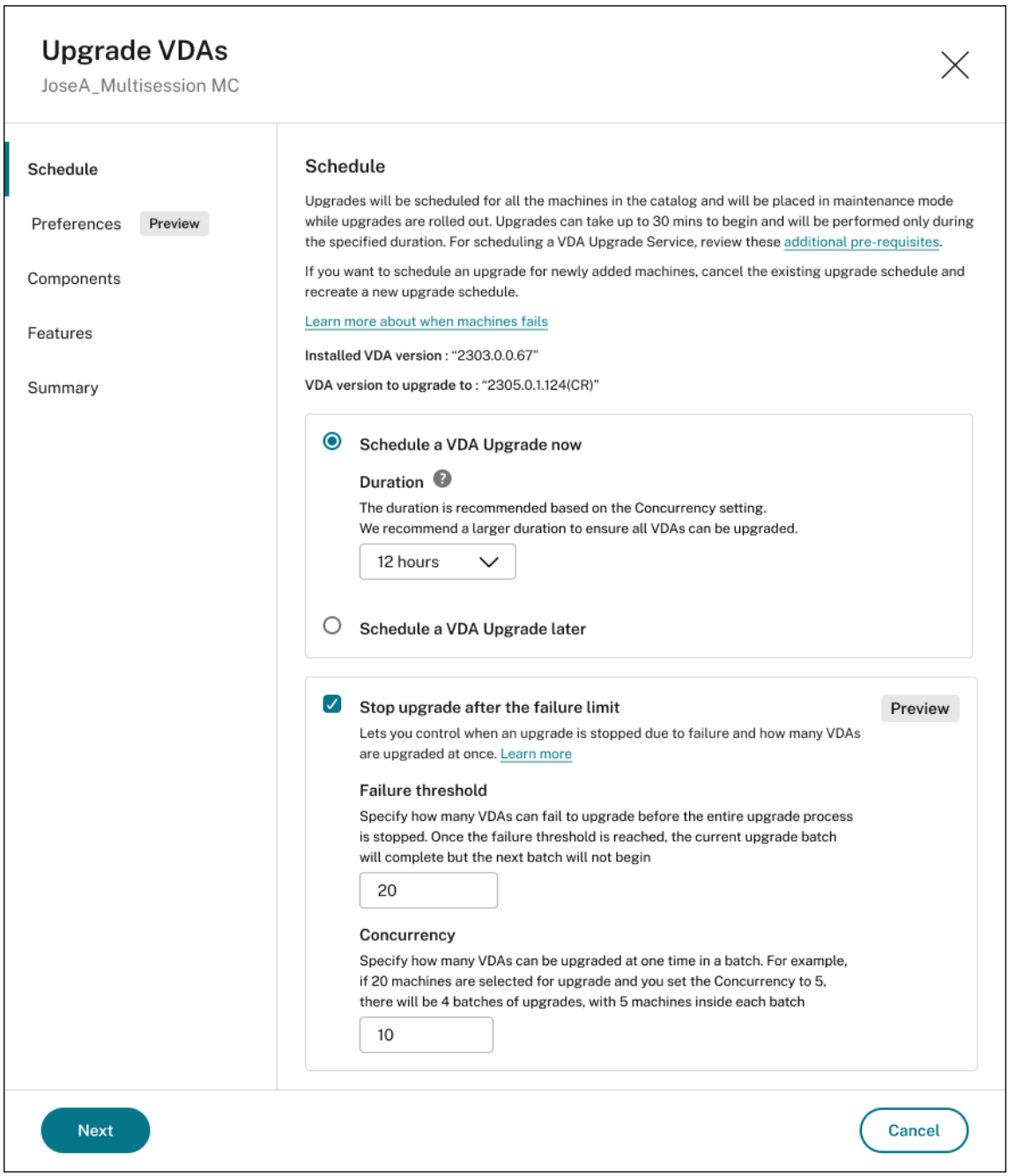
  La duración es la cantidad de tiempo, en horas, tras la cual el servicio de actualización de versión de VDA deja de iniciar nuevas actualizaciones. Las actualizaciones en curso continuarán ejecutándose hasta el final. Durante ese tiempo, DaaS comienza a actualizar los VDA cuando se cumplen los requisitos correspondientes (por ejemplo, si ya no hay sesiones activas).

  Cuantos más VDA deban actualizarse, mayor será esta duración. Recomendamos seleccionar un valor grande (por ejemplo, 12 horas). De lo contrario, según la cantidad de VDA que haya, es posible que DaaS no pueda actualizar algunos en esta ventana.

- Para programar las actualizaciones, seleccione **Actualizar más tarde** y, a continuación, especifique cuándo quieren que se realicen las actualizaciones.

  Solo puede programar las actualizaciones para los próximos siete días. Las actualizaciones que programe solo se aplican a las máquinas que están actualmente en el catálogo. Si agrega máquinas al catálogo más adelante, pero también quiere actualizar su versión, cancele la actualización programada y, a continuación, cree otra programación.




7. Seleccione la opción **Detener actualización de versión después del límite de errores**.

> **Nota:**
>
> De forma predeterminada, esta función está inhabilitada, pero está disponible para los administradores.

**Ilustración de comportamiento**

- El umbral de fallo y el nivel de simultaneidad deben ser superiores a cero.

- El umbral de fallo y el nivel de simultaneidad deben ser inferiores o iguales al número total de máquinas cuya actualización de versión está programada

| Umbral de fallo | Nivel de simultaneidad | Comportamiento |
|---|---|---|
| Proporcionado | No proporcionado o entrada 0 | Se aplica FailureThreshold y el balanceador de cargas decide ConcucrrencyLevel como antes. |
| No proporcionado o entrada 0 | Proporcionado | El valor predeterminado de FailureThreshold es 10 000 (número máximo de máquinas por catálogo) y se utiliza ConcucrrencyLevel para procesamiento por lotes. |
| No proporcionado o entrada 0 | No proporcionado o entrada 0 | El comportamiento predeterminado se aplica a los niveles de simultaneidad actualizados por el balanceador de cargas. |

8. Introduzca el umbral **FailureThreshold**.

   > **Nota:**
   >
   > El umbral de fallo es el número de errores después de los cuales el VUS detiene todas las instalaciones de actualización de versión pendientes de los lotes posteriores que no hayan sido captados por el agente de actualización de versión.

9. Introduzca la **Simultaneidad**.

   > **Nota:**
   >
   > La actualización de versión simultánea es la cantidad de máquinas virtuales que se pueden actualizar simultáneamente en cualquier momento de la ventana de actualización.

10. Haga clic en **Siguiente**.
11. Revise sus opciones en la página **Resumen** y, a continuación, haga clic en **Finalizar** para aplicar los parámetros y salir de la ventana.

> **Nota:**
>
> - La opción **Actualizar versión de VDA** solo está disponible después de habilitar la actualización de VDA para el catálogo. Para habilitar la actualización de VDA, modifique el catálogo.
> - Todas las máquinas del catálogo se colocan en modo de mantenimiento mientras se implementan las actualizaciones. Las actualizaciones pueden tardar hasta 30 minutos en comenzar y solo se llevarán a cabo durante el período de tiempo especificado.

En el nodo **Catálogos de máquinas**, la columna **Actualización de versión de VDA** proporciona información sobre la actualización de versión de VDA para el catálogo. Puede aparecer esta información:

> **Sugerencia:**
>
> Para mostrar la columna **Actualización de versión de VDA**, seleccione **Columnas que mostrar** en la barra de acciones, seleccione **Catálogo de máquinas > Actualización de versión de VDA** y, a continuación, haga clic en **Guardar**.

- **Disponible**: Hay una nueva versión disponible del VDA.
- **Programado**: Se ha programado la actualización de versión del VDA.
- **Sin configurar**: Aparece cuando no se ha habilitado la actualización de versión de VDA para el catálogo.
- **Actualizado**: Los VDA del catálogo están actualizados.
- **Desconocido**: No se puede obtener la información necesaria para la actualización de versión del VDA. Hay varias razones posibles:
  - El VDA estaba en uso en el momento en que tenía lugar la actualización.
  - El número de actualizaciones de versión en curso alcanzó el límite máximo de 500.
  - El agente de actualización de versiones de VDA no respondió en el momento en que tenía lugar la actualización. Asegúrese de que el agente se está ejecutando en el VDA y puede comunicarse con Citrix DaaS.
  - No se pueden realizar las comprobaciones de validación de la actualización de versión. Consulte Requisito de actualización de versiones de VDA.

También puede ver el estado de las actualizaciones de versión de VDA de un catálogo. Para ello, haga clic en el catálogo y, a continuación, compruebe la información del **Estado de la actualización de versión de VDA**, en la ficha **Detalles**. Puede aparecer esta información:

- **Sin programar**: Habilitó la actualización de versión de VDA para el catálogo, pero no configuró ninguna programación para la actualización.
- **Programado**: Creó una programación para la actualización de versión del catálogo. Por ejemplo, si configura la programación para que comience a las `09:00 PM, December 14, 2030`, la información aparecerá de esta manera: Programado para `December 14, 2030 09:00 PM UTC`.

- **En curso**: Se han iniciado las actualizaciones de versión del VDA.
- **Cancelado**: Canceló la actualización programada.
- **Error**: El catálogo contiene al menos una máquina cuya actualización de versión de VDA no se realizó correctamente.
- **Correcto**: La versión de todos los VDA del catálogo se actualizó correctamente.

También puede solucionar problemas de actualización de versión de VDA con acciones recomendadas para un catálogo. Para ello, haga clic en el catálogo y, a continuación, vaya a la ficha **Solucionar problemas**.

Para desglosar rápidamente los catálogos que tienen un estado de actualización de versión de VDA específico, puede usar filtros. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa.

Tenga en cuenta las siguientes consideraciones:

- Los filtros **Actualización de versión de VDA** o **Estado de la actualización de versión de VDA** solo se pueden usar con estos filtros: **Nombre** y **Catálogo de máquinas**.
- Al utilizar los filtros **Actualización de versión de VDA** o **Estado de la actualización de versión de VDA**, los **errores** y las **advertencias** de la esquina superior derecha dejan de estar disponibles.

#### Modificar o cancelar la actualización de versión programada de un VDA

Después de programar las actualizaciones de un catálogo, es posible que quiera modificar o cancelar la actualización programada. Para ello, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.
2. Seleccione el catálogo y, a continuación, **Modificar actualización de versión programada de VDA** en la barra de acciones. Aparece la ventana Modificar actualización de VDA, que muestra información sobre la versión del VDA instalado y la versión del VDA a la que se actualizará.
3. Elija si quiere modificar o cancelar la actualización programada.
    - Para cancelar la actualización, haga clic en **Cancelar actualización de versión programada**. Recuerde: La cancelación de la actualización programada no fuerza la detención de la actualización en curso.
4. Haga clic en **Listo** para salir de la ventana.

### Configurar los parámetros de actualización de versión del VDA mediante la modificación de un catálogo

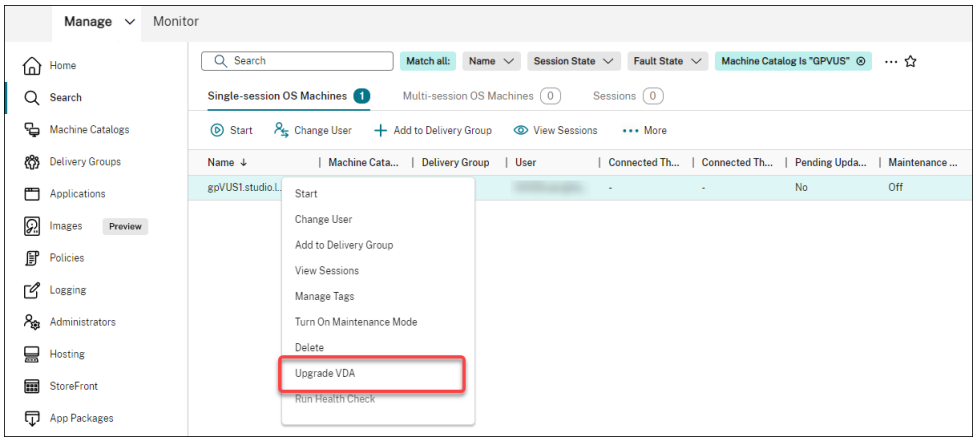
Tras la creación del catálogo, puede configurar los parámetros de actualización de versión del VDA mediante la modificación del catálogo. Antes de empezar a modificarlo, tenga en cuenta lo siguiente:

- Compruebe que todas las máquinas del catálogo tengan la misma opción de VDA (CR o LTSR). De lo contrario, algunas actualizaciones de VDA fallarán. Por ejemplo, si selecciona **La versión LTSR más reciente de VDA**, las actualizaciones CR de VDA fallarán.
- Es posible que se hayan iniciado las actualizaciones de algunas de las máquinas del catálogo. No puede modificar las actualizaciones que ya estén en curso. Las actualizaciones en curso continúan. Las que aún no se hayan iniciado pasarán a la versión especificada.

### Actualizar la versión de VDA por máquina

Después de habilitar la actualización de versión de VDA de un catálogo, puede actualizar los VDA del catálogo uno por uno o en bloque. Para ello, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Buscar**.
2. Seleccione una o más máquinas y, a continuación, **Actualizar versión de VDA** en el menú contextual o la barra de acciones (haga clic con el botón secundario para mostrar el menú contextual).




> **Nota:**
>
> - Para que esté disponible la opción **Actualizar versión de VDA**, asegúrese de haber habilitado la actualización de versión de VDA para el catálogo en el que residen las máquinas seleccionadas y de que esas máquinas tengan instalado el agente de actualización de versiones de VDA. Para habilitar la actualización de versión de VDA, modifique el catálogo.

> - Las máquinas se colocarán en modo de mantenimiento mientras se implementan las actualizaciones. Las actualizaciones pueden tardar hasta 30 minutos en comenzar.
> - Si su selección contiene máquinas para las que las actualizaciones de versión de VDA no están disponibles o cuyas actualizaciones están pendientes (programadas, en curso o a la espera de actualización), omitiremos las actualizaciones de esas máquinas.

En el nodo **Buscar**, puede agregar la columna **Actualización de versión de VDA**. Para obtener información sobre cómo agregar una columna personalizada, consulte Personalizar columnas que mostrar. La columna es útil. Proporciona información sobre la actualización de versión de VDA de la máquina. Puede aparecer esta información:

- **Disponible**: Hay una nueva versión disponible del VDA.
- **Programado**: Se ha programado la actualización de versión del VDA.
- **Sin configurar**: Aparece cuando no se ha habilitado la actualización de versión de VDA para la máquina.
- **Actualizado**: El VDA está actualizado.
- **Desconocido**: La información sobre la actualización de versión del VDA aún no está disponible.

También puede ver el estado de la actualización de versión del VDA de una máquina. Para ello, haga clic en la máquina y, a continuación, compruebe la información del **Estado de la actualización de versión de VDA**, en la ficha **Detalles**. Puede aparecer esta información:

- **Desconocido**: No se puede obtener la información necesaria para la actualización de versión del VDA. Hay varias razones posibles:
  - El VDA estaba en uso en el momento en que tenía lugar la actualización.
  - El número de actualizaciones de versión en curso alcanzó el límite máximo de 500.
  - El agente de actualización de versiones de VDA no respondió en el momento en que tenía lugar la actualización. Asegúrese de que el agente se está ejecutando en el VDA y puede comunicarse con Citrix DaaS.
  - No se pueden realizar las comprobaciones de validación de la actualización de versión. Consulte Requisito de actualización de versiones de VDA.
- **Programado**: Ha configurado un programa de actualización de versión. Por ejemplo, si configura la programación para que comience a las `09:00 PM, December 14, 2030`, la información aparecerá de esta manera: Programado para `December 14, 2030 09:00 PM UTC`.
- **Esperando actualización**: La máquina se coloca en modo de mantenimiento, a la espera de la actualización (asegúrese de que los usuarios hayan cerrado sesión para que la actualización pueda continuar).
- **En curso**: Se ha iniciado la actualización de versión del VDA.

- **Falló la actualización**: No se pudo actualizar la versión del VDA.
- **La validación falló**: No se pudieron validar los parámetros de la actualización de versión de VDA.
- **Cancelado**: La actualización de versión de la máquina se ha cancelado.
- **Correcto**: La versión del VDA se actualizó correctamente.

También puede solucionar problemas de actualización de versión de VDA con acciones recomendadas para una máquina. Para ello, haga clic en la máquina y, a continuación, vaya a la ficha **Solucionar problemas**.

Para desglosar rápidamente las máquinas que tienen un estado de actualización de versión de VDA específico, puede usar filtros. Para obtener más información, consulte Utilizar la búsqueda en la interfaz de administración de Configuración completa. Tenga en cuenta las siguientes consideraciones:

- Los filtros **Actualización de versión de VDA** o **Estado de la actualización de versión de VDA** solo se pueden usar con estos filtros: **Nombre** y **Catálogo de máquinas**.
- Al utilizar los filtros **Actualización de versión de VDA** o **Estado de la actualización de versión de VDA**, los **errores** y las **advertencias** de la esquina superior derecha dejan de estar disponibles.

## Administrar el conjunto de configuraciones de un catálogo

Antes de empezar, asegúrese de haber configurado la implementación de WEM Service. Para obtener más información, consulte Introducción a Workspace Environment Management Service.

> **Nota:**
>
> De forma predeterminada, si tiene el rol de administrador de la nube, administrador de acceso total o administrador de catálogos de máquinas, puede administrar conjuntos de configuraciones para los catálogos. Si es necesario, para permitir que los roles administren conjuntos de configuraciones, puede otorgarles el permiso **Administrar conjuntos de configuraciones**.

### Vincular un catálogo a un conjunto de configuraciones

> **Importante:**
>
> Si sus instancias de Citrix DaaS y WEM Service no residen en la misma región, no podrá vincular un catálogo a un conjunto de configuraciones. En ese caso, migre WEM Service a la misma región que Citrix DaaS.

Para vincular un catálogo a un conjunto de configuraciones, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.

2. Seleccione el catálogo de máquinas y, a continuación, **Administrar conjunto de configuraciones** en la barra de acciones. Aparece la ventana **Administrar conjunto de configuraciones**.
3. Seleccione un conjunto de configuraciones de WEM al que quiera vincular el catálogo.

   > **Nota:**
   >
   > Si el conjunto de configuraciones seleccionado no contiene parámetros relacionados con la configuración básica de WEM, aparece la opción **Aplicar parámetros básicos al conjunto de configuraciones**: Le recomendamos seleccionar la opción para aplicar los parámetros básicos al conjunto de configuraciones.

4. Haga clic en **Guardar** para guardar los cambios.

#### Cambiar a otro conjunto de configuraciones

Para cambiar a otro conjunto de configuraciones de un catálogo, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.
2. Seleccione el catálogo de máquinas y, a continuación, **Administrar conjunto de configuraciones** en la barra de acciones. Aparece la ventana **Administrar conjunto de configuraciones**.
3. Seleccione otro conjunto de configuraciones de WEM al que quiera vincular el catálogo.
4. Haga clic en **Guardar** para guardar los cambios.

#### Desvincular un catálogo del conjunto de configuraciones

Para desvincular un catálogo del conjunto de configuraciones, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas**.
2. Seleccione el catálogo de máquinas y, a continuación, **Administrar conjunto de configuraciones** en la barra de acciones. Aparece la ventana **Administrar conjunto de configuraciones**.
3. Haga clic en el icono X situado a la derecha del conjunto de configuraciones seleccionado.
4. Haga clic en **Guardar** para guardar los cambios.

### Reintentar la creación de catálogos

> **Nota:**
>
> Esta función solo se aplica a catálogos de MCS.

Los catálogos con errores se marcan con un icono de error. Para ver los detalles, vaya a la ficha **Solucionar problemas** de cada catálogo. Antes de reintentar la creación de catálogos, tenga en cuenta estas consideraciones:

- Compruebe primero la información sobre la solución de problemas y resuelva los problemas. La información describe los problemas encontrados y proporciona recomendaciones para resolverlos.
- No se pueden cambiar los parámetros asociados a la administración de máquinas y al sistema operativo. El catálogo hereda esos parámetros del original.
- La creación puede tardar un tiempo en completarse. Si es necesario, seleccione **Ocultar progreso** para realizar la creación en segundo plano.

Para intentar de nuevo la creación de un catálogo, haga lo siguiente:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo y, a continuación, vaya a la ficha **Solucionar problemas**.
3. Haga clic en el hipervínculo Reintentar para intentar crear el catálogo de nuevo.
4. En el asistente que aparece, cambie los parámetros donde sea necesario. Si no necesita realizar ningún cambio, puede ir directamente a la página **Resumen**.
5. Cuando termine, seleccione **Finalizar** para iniciar la creación.

### (Solo agentes VDA no aprovisionados por Citrix) Generar y administrar los tokens de inscripción

Cuando decida adoptar la inscripción basada en tokens para máquinas aprovisionadas que no sean de Citrix, genere tokens por catálogo de máquinas y después compártalos con los administradores de instalación de VDA.

Un token de inscripción incluye:

- Rango de registro: de 1 a 100 máquinas VDA
- Período de validez: de 1 hora a 14 días

Para generar un token para un catálogo mediante la Configuración completa, siga estos pasos:

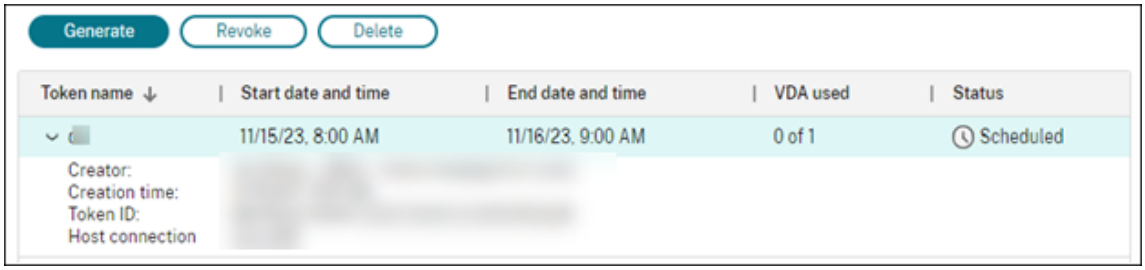
1. En **Configuración completa > Catálogos de máquinas**, busque un catálogo que no esté aprovisionado por MCS y que muestre **Método de aprovisionamiento: Manual** en la columna **Recuento de máquinas**.
2. Haga clic con el botón secundario en el catálogo y después seleccione **Administrar tokens de inscripción**.
3. En la página **Generar token de inscripción** que se muestra, introduzca la siguiente información sobre el token:
    - Escriba un nombre para el token.

- Introduzca su período de validez. El período debe ser de una hora a 14 días. El token solo es válido durante el período especificado.
- (Opcional) Seleccione una conexión de host para administrar la energía de los VDA inscritos con el token. Las opciones incluyen todas las conexiones de host de la zona de este catálogo.
- Introduzca los límites de uso del token (entre 1 y 100).

4. Haga clic en **Generar**.
5. En la ventana **Token generado correctamente** que se muestra, cópielo y guárdelo en un lugar seguro, o haga clic en **Descargar** para descargarlo en la carpeta **Descargas**.

   Se muestra un registro de token en la lista de tokens.




6. Comparta el token con los administradores de instalación del VDA.

   Para obtener más información sobre cómo instalar un VDA y un token en las máquinas, consulte Instalar agentes VDA.

#### Administrar tokens

Tiene dos opciones para revocar un token y hacer que no esté disponible para la inscripción de VDA:

- Revocar: revoca el token pero lo conserva en la lista para fines de registro.
- Eliminar: revoca el token y lo elimina de la lista.

> **Nota:**
>
> Los tokens caducados se eliminan automáticamente en 14 días.

### Usar PowerShell

En esta sección se detalla cómo puede administrar catálogos con PowerShell:

- Usar PowerShell para comprobar el estado de actualización y la versión de los VDA
- Administrar el número de secuencia del nombre de máquina
- Habilitar la programación de reinicios únicos
- Agregar descripciones a una imagen

- Restablecer disco de SO
- Reparar la información de identidad de las cuentas de equipo activas
- Cambiar el parámetro de red de un catálogo de máquinas existente
- Administrar versiones de un catálogo de máquinas
- Cambiar la configuración de caché de un catálogo de máquinas existente
- Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina
- Recuperar advertencias y errores asociados a un catálogo
- Eliminar máquinas sin acceder al hipervisor
- Compatibilidad con la actualización de VDA mediante acceso a recursos compartidos de archivos locales

#### Usar PowerShell para comprobar el estado de actualización y la versión de los VDA

Use el comando `Get-VusCatalog` de PowerShell para comprobar el estado de la actualización de versión de los VDA. Pongamos como ejemplo que el nombre del catálogo es `wuhanTestMC1`. Puede escribir lo siguiente en el símbolo del sistema:

- `PS C:\> Get-VusCatalog -Name wuhanTestMC1`

```
PS C:\Users\hanw> Get-VusCatalog -Name  wuhanTestMC1


CancelledUpgrades           : 0
DurationInHours             : 8
FailedUpgrades              : 0
InProgressUpgrades          : 0
LastStateChangeInUtc        : 4/22/2022 7:52:51 AM
MaxConcurrentUpgrades       : 100
Name                        : wuhanTestMC1
ProvisioningType            : MCS
ScheduledTimeInUtc          : 4/22/2022 7:20:56 AM
SecurityCheckFailedUpgrades : 0
SessionSupport              : SingleSession
StateId                     : UpgradeSuccessful
SuccessfulUpgrades          : 1
TotalMachines               : 1
Uid                         : 12
UpgradeState                : UpgradeAvailable
UpgradeType                 : CR
UpgradeVersion              : 2112.0.0.32068
Uuid                        : 339e7bce-271b-4c37-9a1c-bce287008b65
```

En este ejemplo, `UpgradeState` es `UpgradeAvailable`, lo que significa que la actualización de versión del VDA está habilitada para el catálogo. `StateId` es `UpgradeSuccessful`, lo que significa que la versión del catálogo se actualizó correctamente a 2112.0.0.32068 (`UpgradeVersion`).

Use el comando `Get-BrokerMachine` de PowerShell para obtener la versión actual del VDA.

```
SessionProtocol              :
SessionSecureIcaActive       :
SessionSmartAccessTags       :
SessionStartTime             :
SessionState                 :
SessionStateChangeTime       :
SessionSupport               : MultiSession
SessionType                  :
SessionUid                   :
SessionUserName              :
SessionUserSID               :
SessionsEstablished          : 0
SessionsPending              : 0
SummaryState                 : Unregistered
SupportedPowerActions        : {}
Tags                         : {}
UUID                         : 9c0c4623-a4dc-44f9-ae4b-54c86cc76a7f
Uid                          : 4
VMToolsState                 : NotPresent
WillShutdownAfterUse         : False
WillShutdownAfterUseReason   : None
WindowsConnectionSetting     : LogonEnabled
ZoneHealthy                  : False
ZoneName                     : My Resource Location
ZoneUid                      : ae0366c2-3001-459d-89ff-0b159c9d436d

AgentVersion                 : 2112.0.0.32068
AllocationType               : Static
ApplicationsInUse            : {}
AssignedClientName           :
AssignedIPAddress            :
AssignedUserSIDs             : {}
AssociatedTenantId           :
AssociatedUserFullNames      : {}
AssociatedUserNames          : {}
AssociatedUserSIDs           : {}
AssociatedUserUPNs           : {}
AzureADJoinedMode            : NotAadJoined
BrowserName                  :
Capabilities                 : {}
CatalogName                  : wuhanTestMC1
CatalogUUID                  : 339e7bce-271b-4c37-9a1c-bce287008b65
CatalogUid                   : 12
CbpVersion                   :
ColorDepth                   :
ControllerDNSName            :
DNSName                      : wuhanVUSTest02.WHCloud.Internal
DeliveryType                 :
Description                  :
DesktopConditions            : {}
```

Use el comando `Get-VusAvailableVdaVersion` de PowerShell para obtener la versión más reciente del VDA.

```
PS C:\Users\hanw> Get-VusAvailableVdaVersion

UpgradeType Version
----------- -------
         CR 2203.0.0.33220
       LTSR 2203.0.0.33220
```

### Administrar el número de secuencia del nombre de máquina

Para personalizar el número de secuencia de las máquinas que se implementan con MCS, a través de los comandos de PowerShell, haga lo siguiente:

1. Abra Powershell como administrador en el Delivery Controller.
2. Ejecute el comando `asnp citrix*` para cargar los módulos de Citrix.
3. Ejecute este comando para comprobar el recuento inicial del grupo de identidades del catálogo:

   ```
   Get-AcctIdentityPool -IdentityPoolName xxx
   <!--NeedCopy-->
   ```

   `IdentityPoolName` es el nombre del catálogo.
4. Si quiere establecer este recuento en un valor diferente, ejecute el siguiente comando y especifique StartCount como X:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount X
   <!--NeedCopy-->
   ```
5. Agregue las máquinas al catálogo para que se creen con el recuento requerido.
6. Tras crear las máquinas, ejecute este comando para restablecerlas al valor Y original:

   ```
   Set-AcctIdentityPool -IdentityPoolName xxx -StartCount Y
   <!--NeedCopy-->
   ```

### Habilitar una programación de reinicios únicos

Si quiere habilitar la programación de reinicio único con PowerShell, use estos comandos `BrokerCatalogRebootSchedule` de PowerShell para crear, modificar y eliminar una programación de reinicio:

- `Get-BrokerCatalogRebootSchedule`
- `New-BrokerCatalogRebootSchedule`
- `Set-BrokerCatalogRebootSchedule`
- `Remove-BrokerCatalogRebootSchedule`

- `Rename-BrokerCatalogRebootSchedule`

Ejemplo:

- Para crear una programación de reinicio de las máquinas virtuales del catálogo denominado **Cajeros** que comience el 3 de febrero de 2022, entre las 2:00 y las 4:00.

```
New-BrokerCatalogRebootSchedule -Name BankTellers
-CatalogName BankTellers
-StartDate "2022-02-03"
-StartTime "02:00"
-Enabled $true
-RebootDuration 120
<!--NeedCopy-->
```

- Para crear una programación de reinicio de las máquinas virtuales del catálogo con el UID 17 que comience el 3 de febrero de 2022, entre la 1:00 y las 5:00. 10 minutos antes del reinicio, cada máquina virtual está configurada para mostrar un cuadro de mensaje con el título **ADVERTENCIA: Reinicio pendiente** y el mensaje **Guarde su trabajo** en cada sesión de usuario.

```
New-BrokerCatalogRebootSchedule
-Name 'Update reboot'
-CatalogUid 17
-StartDate "2022-02-03"
-StartTime "01:00" -Enabled $true -RebootDuration 240
-WarningTitle "WARNING: Reboot pending"
-WarningMessage "Save your work" -WarningDuration 10
<!--NeedCopy-->
```

- Para cambiar el nombre de la programación de reinicio del catálogo **Nombre antiguo** a **Nombre nuevo**.

```
Rename-BrokerCatalogRebootSchedule -Name "Old Name" -NewName "New
    Name"
<!--NeedCopy-->
```

- Para mostrar todas las programaciones de reinicio del catálogo con el UID 1 y, a continuación, cambiar el nombre de la programación de reinicio del catálogo con el UID 1 a **Nuevo nombre**.

```
Get-BrokerCatalogRebootSchedule -Uid 1 | Rename-
   BrokerCatalogRebootSchedule -NewName "New Name" -PassThru
<!--NeedCopy-->
```

- Para configurar la programación de reinicios del catálogo denominado **Contabilidad**, se mostrará un mensaje con el título **ADVERTENCIA: Reinicio pendiente y el mensaje Guarde su trabajo** 10 minutos antes del reinicio de cada máquina virtual. El mensaje aparece en todas las sesiones de usuario de esa máquina virtual.

```
Set-BrokerCatalogRebootSchedule -Name Accounting
-WarningMessage "Save your work"
```

```
-WarningDuration 10 -WarningTitle "WARNING: Reboot pending"
<!--NeedCopy-->
```

- Para mostrar todas las programaciones de reinicio que están inhabilitadas y, a continuación, habilitar todas las programaciones de reinicio inhabilitadas.

```
Get-BrokerCatalogRebootSchedule -Enabled $false | Set-
    BrokerCatalogRebootSchedule -Enabled $true
<!--NeedCopy-->
```

- Para configurar la programación de reinicio del catálogo con UID 17, muestre el mensaje **Reiniciando en %m% min** 15, 10 y 5 minutos antes del reinicio de cada máquina virtual.

```
Set-BrokerCatalogRebootSchedule 17 -WarningMessage "Rebooting in
    %m% minutes." -WarningDuration 15 -WarningRepeatInterval 5
<!--NeedCopy-->
```

- Para configurar la zona horaria del catálogo denominado **MiCatálogo**.

```
Set-BrokerCatalog -Name "MyCatalog" -TimeZone <TimeZone>
<!--NeedCopy-->
```

### Agregar descripciones a una imagen

Puede agregar descripciones informativas acerca de los cambios relacionados con las actualizaciones de imágenes de los catálogos de máquinas. Utilice esta función para agregar una descripción al crear un catálogo o al actualizar una imagen maestra existente de un catálogo. También puede mostrar información de cada imagen maestra del catálogo. Esta funcionalidad resulta útil para los administradores que quieren agregar etiquetas descriptivas al actualizar una imagen maestra utilizada por un catálogo, por ejemplo, *Office 365 instalado*. Utilice los siguientes comandos para agregar o ver descripciones de imágenes:

- `NewProvScheme`. Un nuevo parámetro, `masterImageNote`, permite agregar una nota a una imagen. Por ejemplo:

```
C:\PS>New-ProvScheme -ProvisioningSchemeName XenPS -HostingUnitName
    XenHu -IdentityPoolName idPool1 -MasterImageVM XDHyp:\HostingUnits\
    XenHU\Base.vm\Base.snapshot -MasterImageNote "Office365 installed"
<!--NeedCopy-->
```

- `Publish-ProvMasterVMImage`. Utilice este parámetro para publicar la nota. Por ejemplo:

```
C:\PS>Publish-ProvMasterVMImage -ProvisioningSchemeName MyScheme -
    MasterImageVM XDHyp:\HostingUnits\HostUnit1\RhoneCC_baseXP.vm\base.
    snapshot -MasterImageNote "Visual Studio 2019 installed"
<!--NeedCopy-->
```

- `Get-ProvSchemeMasterVMImageHistory`. Mostrar información de cada imagen. Por ejemplo:

```
C:\PS>Get-ProvSchemeMasterVMImageHistory -ProvisioningSchemeName
    MyScheme -Showall

VMImageHistoryUid : 3cba3a75-89cd-4868-989b-27feb378fec5

ProvisioningSchemeUid : 7585f0de-192e-4847-a6d8-22713c3a2f42

ProvisioningSchemeName : MyScheme

MasterImageVM : /Base.vm/base.snapshot

Date : 17/05/2021 09:27:50

MasterImageNote : Office365 installed
<!--NeedCopy-->
```

### Restablecer disco de SO

Utilice el comando `Reset-ProvVMDisk` de PowerShell para restablecer el disco del sistema operativo de una máquina virtual persistente en un catálogo de máquinas creado con MCS. Actualmente, esta función se aplica a los entornos de virtualización de Azure, Google Cloud, SCVMM, VMware y XenServer.

Para ejecutar correctamente el comando de PowerShell, asegúrese de que:

- Las máquinas virtuales de destino están en un catálogo de MCS persistente.
- El catálogo de máquinas MCS funciona correctamente. Esto implica que el esquema de aprovisionamiento y el host existen y que el esquema de aprovisionamiento tiene las entradas correctas.
- El hipervisor no está en modo de mantenimiento.
- Las máquinas virtuales de destino están apagadas y en modo de mantenimiento.

Siga estos pasos para restablecer el disco del sistema operativo:

1. Abra una ventana de **PowerShell**.
2. Ejecute asnp citrix* para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute el comando `Reset-ProvVMDisk` de PowerShell de cualquiera de las siguientes maneras:
    - Especifique la lista de máquinas virtuales en forma de lista separada por comas y efectúe el restablecimiento en cada máquina virtual:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName ("abc"
    ,"def") -OS
<!--NeedCopy-->
```

- Especifique la lista de máquinas virtuales como resultado del comando `Get-ProvVM` y efectúe el restablecimiento en cada máquina virtual:

```
(Get-ProvVM -ProvisioningSchemeName "xxx") | Reset-ProvVMDisk
    "abc" -OS
<!--NeedCopy-->
```

- Especifique una sola máquina virtual por nombre:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS
<!--NeedCopy-->
```

- Cree tareas de restablecimiento independientes para cada una de las máquinas virtuales que devuelva el comando `Get-ProvVM`. Este método es menos eficiente, ya que cada tarea realizará las mismas comprobaciones redundantes, como la comprobación de la capacidad del hipervisor o la comprobación de la conexión para cada máquina virtual.

```
Get-ProvVM -ProvisioningSchemeName "xxx" | Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -OS
<!--NeedCopy-->
```

4. Aparecerá un mensaje de confirmación con una lista de las máquinas virtuales que se restablecerán, junto con un mensaje de advertencia que indica que se trata de una operación irrecuperable. Si no proporciona una respuesta y pulsa **Intro**, no tendrá lugar ninguna otra acción.

   Puede ejecutar el comando `-WhatIf` de PowerShell para imprimir la acción que tendría lugar y salir sin realizar dicha acción.

   También puede omitir el mensaje de confirmación mediante uno de los siguientes métodos:

   - Indique el parámetro `-Force`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Force
<!--NeedCopy-->
```

   - Indique el parámetro `-Confirm:$false`:

```
Reset-ProvVMDisk -ProvisioningSchemeName "xxx" -VMName "abc"
    -OS -Confirm:$false
<!--NeedCopy-->
```

   - Antes de ejecutar `Reset-ProvVMDisk`, cambie `$ConfirmPreference` a “None”:

```
PS C:\Windows\system32> $ConfirmPreference='None'
```

```
PS C:\Windows\system32> $ConfirmPreference
None
PS C:\Windows\system32> Reset-ProvVMDisk -
    ProvisioningSchemeName "xxx" -VMName "abc" -OS
<!--NeedCopy-->
```

> **Nota:**
>
> No saque las máquinas virtuales del modo de mantenimiento ni las encienda hasta que finalice el proceso de restablecimiento.

5. Ejecute `Get-ProvTask` para obtener el estado de las tareas devueltas por el comando `Reset-ProvVMDisk`.

### Reparar la información de identidad de las cuentas de equipo activas

Puede restablecer la información de identidad de las cuentas de equipo activas que tengan problemas relacionados con la identidad. Puede elegir restablecer solo la contraseña de la máquina y las claves de confianza, o bien restablecer toda la configuración del disco de identidad. Esta implementación se aplica tanto a catálogos de máquinas de MCS persistentes como no persistentes.

> **Nota:**
>
> En la actualidad, la función solo es compatible con los entornos de virtualización de Azure y VMware.

#### Condiciones

Para restablecer correctamente el disco de identidad:

- Apague y ponga la VM en modo de mantenimiento
- No incluya el parámetro -OS en el comando de PowerShell

#### Restablecer la información de identidad

Para restablecer la información de identidad:

1. Abra la ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Restablezca la información de identidad.
    - Para restablecer únicamente la contraseña de la máquina y las claves de confianza, ejecute los siguientes comandos en este orden:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

La descripción de los parámetros usados en el comando es la siguiente:

- `IdentityAccountName`: El nombre de la cuenta de identidad que se debe reparar.
- `PrivilegedUserName`: La cuenta de usuario que tiene permiso de escritura en el proveedor de identidades (AD o Azure AD).
- `PrivilegedUserPassword`: Contraseña para PrivilegedUserName.
- `Target`: Objetivo de la acción de reparación. Puede ser IdentityInfo para reparar la contraseña o la clave de confianza de la cuenta y UserCertificate para reparar los atributos del certificado de usuario de las identidades de máquinas híbridas unidas a Azure AD.

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMname <name
    > -Identity -ResetIdentityInfo
<!--NeedCopy-->
```

El parámetro `ResetIdentityInfo` restablece lo siguiente:

- Contraseña y claves de confianza: Si la VM está unida a un dominio de AD (solo para Citrix DaaS)
- Solo claves de confianza: Si la máquina virtual no está unida a un dominio de AD (solo para Citrix DaaS)
- Solo contraseña: Si la máquina virtual está unida a un dominio de AD (solo para Citrix Virtual Apps and Desktops)

- Para restablecer toda la configuración del disco de identidad, ejecute los siguientes comandos en este orden:

```
Repair-AcctIdentity -IdentityAccountName TEST\VM1 -
    PrivilegedUserName TEST\admin1 -PrivilegedUserPassword
    $password -Target IdentityInfo
<!--NeedCopy-->
```

```
Reset-ProvVMDisk ProvisioningSchemeName <name> -VMName <name>
     -Identity
<!--NeedCopy-->
```

4. Escriba **y** para confirmar la acción. También puede omitir el mensaje de confirmación mediante el parámetro `-Force`. Por ejemplo:

```
Reset-ProvVMDisk -ProvisioningSchemeName <name> -VMName <name> -
    Identity -Force
<!--NeedCopy-->
```

5. Ejecute `Get-ProvVM -ProvisioningSchemeName <name -VMName <name>` para comprobar la configuración actualizada del disco de identidad. Los atributos del disco de identidad (por ejemplo, `IdentityDiskId`) deben actualizarse. `StorageId` y `IdentityDiskIndex` no deben cambiar.

### Cambiar el parámetro de red de un catálogo de máquinas existente

Puede cambiar el parámetro de red de un catálogo de máquinas existente para que las nuevas máquinas virtuales se creen en la nueva subred. Utilice el parámetro `-NetworkMapping` del comando `Set-ProvScheme` para cambiar el parámetro de la red.

Para cambiar el parámetro de red de un esquema de aprovisionamiento existente, haga lo siguiente:

1. En la ventana de PowerShell, ejecute el comando `asnp citrix*` para cargar los módulos de PowerShell.
2. Ejecute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para ir a la ruta de red que quiere cambiar.
3. Asigne una variable al nuevo parámetro de red. Por ejemplo:

```
$NewNetworkMap = @{
 "0"= "XDHYP:\HostingUnits\MyNetworks\Network 0.network" }

<!--NeedCopy-->
```

4. Ejecute `Set-ProvScheme -ProvisioningSchemeName "name"-NetworkMapping $NewNetworkMap`.
5. Ejecute `(Get-Provscheme -ProvisioningSchemeName "name").NetworkMaps` para verificar el nuevo parámetro de red para el esquema de aprovisionamiento existente.

### Administrar versiones de un catálogo de máquinas

Cuando se actualiza un catálogo de máquinas de MCS con el comando `Set-ProvScheme`, la configuración actual se guarda como una versión. A continuación, puede administrar las distintas versiones del catálogo de máquinas mediante los comandos de PowerShell. Puede hacer lo siguiente:

- Consulte la lista de versiones de un catálogo de máquinas
- Use cualquier versión anterior para actualizar el catálogo de máquinas
- Eliminar manualmente una versión si no la usa una máquina virtual de ese catálogo de máquinas
- Cambiar el número máximo de versiones que debe conservar el catálogo de máquinas (el valor predeterminado es 99)

Una versión incluye la siguiente información de un catálogo de máquinas:

- VMCpuCount
- VMMemoryMB
- CustomProperties
- ServiceOffering
- MachineProfile
- NetworkMapping
- SecurityGroup

Ejecute los siguientes comandos (se indican como ejemplos) para administrar las distintas versiones de un catálogo de máquinas.

- Para ver los detalles de configuración de las distintas versiones de un catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

- Para ver los detalles de configuración de una versión concreta de un catálogo de máquinas:

```
Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 2
<!--NeedCopy-->
```

- Para ver el número total de versiones asociadas a un catálogo de máquinas:

  “‘

  (Get-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog).Count

- Para usar cualquier versión anterior para actualizar el catálogo de máquinas:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -Version 2
<!--NeedCopy-->
```

- Para eliminar manualmente una versión si no la usa una máquina virtual de ese catálogo de máquinas

```
Remove-ProvSchemeVersion -ProvisioningSchemeName AzureCatalog -
    Version 3
<!--NeedCopy-->
```

- Para cambiar el número máximo de versiones que debe conservar el catálogo de máquinas (el valor predeterminado es 99). Esta configuración se aplica en todos los catálogos. Por ejemplo, en este caso, se conservará un máximo de 15 versiones para todos los catálogos aprovisionados por MCS.

```
Set-ProvServiceConfigurationData -Name "MaxProvSchemeVersions" -
    Value 15
<!--NeedCopy-->
```

Si el número de versiones alcanza el número máximo de versiones, no se puede crear una nueva versión si alguna de las máquinas virtuales del catálogo de máquinas está usando versiones anteriores. En ese caso, realice una de las siguientes acciones:

- Aumente el límite del número máximo de versiones que debe conservar el catálogo de máquinas.
- Actualice algunas máquinas virtuales que están en versiones anteriores para que ninguna máquina virtual deje de hacer referencia a esas versiones anteriores y pueda eliminarlas.

### Cambiar la configuración de caché de un catálogo de máquinas existente

Después de crear un catálogo no persistente con E/S de MCS habilitada, puede usar el comando `Set-ProvScheme` para modificar los siguientes parámetros:

- WriteBackCacheMemorySize
- WriteBackCacheDiskSize

Esta función se aplica actualmente a:

- Entornos de GCP y Microsoft Azure, y
- un catálogo no persistente con E/S de MCS habilitada

#### Requisitos

Los requisitos para modificar la configuración de caché son:

- Actualizar a la versión más reciente de VDA (2308 o posterior).
- Habilitar el parámetro `UseWriteBackCache` para el catálogo de máquinas existente. Use `New-ProvScheme` para crear un catálogo de máquinas con la opción `UseWriteBackCache` habilitada. Por ejemplo:

```
New-ProvScheme -ProvisioningSchemeName $CatalogName -
   HostingUnitUid $HostingUnitUid `
-IdentityPoolUid $acctPool.IdentityPoolUid -CleanOnBoot `
-MasterImageVM $MasterImage `
-ServiceOffering $ServiceOffering `
-NetworkMap $NetworkMap `
-SecurityGroup $SecurityGroup `
-UseWriteBackCache -WriteBackCacheDiskSize 8
<!--NeedCopy-->
```

#### Cambiar la configuración de caché

Ejecute el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName $provScheme.
    ProvisioningSchemeName -WriteBackCacheDisk32 -
    WriteBackCacheMemorySize 128
<!--NeedCopy-->
```

> **Nota:**
>
> - El valor de `WriteBackCacheDiskSize` debe ser mayor que cero porque se requiere al menos 1 GB de almacenamiento en disco de caché.
> - El valor de `WriteBackCacheMemorySize` debe ser menor que el tamaño de la memoria del catálogo de máquinas.
> - Estos cambios solo afectan a las nuevas VM que se agreguen al catálogo después de realizar el cambio. Estos cambios no afectan a las VM existentes.

### Convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina

Puede usar una VM, una especificación de plantilla (en el caso de Azure) o una plantilla de inicio (en el caso de AWS) como entrada del perfil de máquina para convertir un catálogo de máquinas no basado en perfiles de máquina en un catálogo de máquinas basado en perfiles de máquina. Las nuevas máquinas virtuales agregadas al catálogo toman los valores de las propiedades del perfil de máquina.

> **Nota:**
>
> Un catálogo de máquinas existente basado en perfiles de máquina no se puede cambiar a un catálogo de máquinas no basado en perfiles de máquina.

Para hacerlo:

1. Cree un catálogo de máquinas persistente o no persistente con máquinas virtuales y sin un perfil de máquina.
2. Abra la ventana de **PowerShell**.
3. Ejecute el comando `Set-ProvScheme` para aplicar los valores de las propiedades del perfil de la máquina a las nuevas máquinas virtuales agregadas al catálogo de máquinas. Por ejemplo:
   - En el caso de Azure:

     ```
     Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
         -MachineProfile XDHyp:\HostingUnits<HostingUnitName>\
         machineprofile.folder<ResourceGroupName><TemplateSpecName
         ><VersionName>
     <!--NeedCopy-->
     ```

- En el caso de AWS:

```
Set-ProvScheme = Set-ProvScheme -ProvisioningSchemeName xxxx
    -MachineProfile "XDHyp:\HostingUnits<hosting-unit><launch-
    template>.launchtemplate<launch-template-version>.
    launchtemplateversion"
<!--NeedCopy-->
```

### Recuperar advertencias y errores asociados a un catálogo

Puede obtener advertencias y errores históricos para comprender los problemas de su catálogo de máquinas de MCS y corregirlos.

Con los comandos de PowerShell, puede:

- Obtener una lista de errores o advertencias
- Cambiar el estado de una advertencia de **New** a **Acknowledged**
- Eliminar los errores o las advertencias

Para ejecutar los comandos de PowerShell:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.

Para obtener una lista de errores y advertencias:

Ejecute el comando `Get-ProvOperationEvent`.

- Sin parámetros: Obtiene todas las advertencias.
- Con los parámetros `LinkedObjectType` y `LinkedObjectUid`: Obtiene todos los errores y advertencias asociados a un esquema de aprovisionamiento específico.
- Con el parámetro `EventId`: Obtiene errores o advertencias específicos que coinciden con este ID de evento.
- Con el parámetro `Filter`: Obtiene errores o advertencias mediante un filtro personalizado

Para cambiar el estado de los errores o advertencias de **New** a **Acknowledged**:

Ejecute el comando `Confirm-ProvOperationEvent`.

- Con el parámetro `EventId`: Configura el estado de errores o advertencias específicos que coinciden con este ID de evento. Puede obtener el `EventId` de un error o advertencia específico como resultado del comando `Get-ProvOperationEvent`
- Con los parámetros `LinkedObjectType` y `LinkedObjectUid`: Configura el estado de todos los errores y advertencias asociados a un esquema de aprovisionamiento específico.
- Con el parámetro `All`: Configura el estado de todos los errores y advertencias como **Acknowledged**.

Para eliminar los errores o advertencias:

Ejecute el comando `Remove-ProvOperationEvent`.

- Con el parámetro `EventId`: Quita errores o advertencias específicos que coinciden con este ID de evento Puede obtener el `EventId` de un error o advertencia específico como resultado del comando `Get-ProvOperationEvent`
- Con los parámetros `LinkedObjectType` y `LinkedObjectUid`: Quita todos los errores y advertencias asociados a un esquema de aprovisionamiento específico.
- Con el parámetro `All`: Quita todas las advertencias.

Para obtener más información, consulte SDK de PowerShell de Citrix.

## Eliminar máquinas sin acceder al hipervisor

Al eliminar una máquina virtual o un esquema de aprovisionamiento, MCS necesita quitar etiquetas de la máquina virtual y, a veces, también del disco base, para que MCS deje de rastrear o identificar los recursos incluidos en las opciones de eliminación. Sin embargo, algunos de estos recursos solo son accesibles a través del hipervisor. Utilice la opción `PurgeDBOnly` de PowerShell `Remove-ProvVM` para eliminar de la base de datos objetos de recursos de VM, como la máquina virtual, el disco base o la imagen en ACG incluso cuando no se pueda acceder al hipervisor.

Esta opción está habilitada en:

- Todos los hipervisores compatibles
- Máquinas virtuales persistentes y no persistentes

### Limitaciones

No puede usar los comandos -PurgeDBOnly y -ForgetVM al mismo tiempo.

### Usar el comando PurgeDBOnly

Al ejecutar el comando de PowerShell `Remove-ProvVM -ProvisioningSchemeName SCVMM -MC -VMName SCVMM01 -ForgetVM`, es posible que la operación de eliminación falle en estos casos:

- La conexión de host está en modo de mantenimiento
- Credenciales no válidas
- Fallo de autenticación
- Operación no autorizada
- No se puede contactar con el hipervisor

> **Nota:**
>
> Remove-provVM -ForgetVM se dirige solamente a máquinas virtuales persistentes. Si una de las máquinas virtuales de la lista no es persistente, se produce un error en la operación.

Cuando la operación falla porque no se puede contactar con el hipervisor, aparece este mensaje:

```
Try to use -PurgeDBOnly option to clean DDC database.
```

Utilice la opción `-PurgeDBOnly` del comando `Remove-ProvVM` de PowerShell para eliminar de la base de datos de MCS referencias de máquinas virtuales. Por ejemplo,

```
Remove-ProvVM -ProvisioningSchemeName SCVMM-MC -VMName SCVMM01 -
PurgeDBOnly
```

## Compatibilidad con la actualización de VDA mediante acceso a recursos compartidos de archivos locales

Especifique la ubicación del instalador del VDA mediante los cmdlets de PowerShell, lo que reduce la necesidad de proporcionar reglas de red para permitir que cada VDA obtenga el nuevo instalador de VDA en la CDN de Azure administrada por Citrix.

### Cmdlets de PowerShell

Se han agregado dos nuevos parámetros opcionales a los cmdlets **New-VusCatalogSchedule** y **New-VusMachineUpgrade** que permiten usar instaladores desde un recurso compartido de archivos local

- **VdaWorkstationPackageUri**: para especificar la ruta UNC al instalador de VDA del sistema operativo de la estación de trabajo
- **VdaServerPackageUri**: para especificar la ruta UNC al instalador de VDA del sistema operativo del servidor

### Requisitos previos

- Agente de actualización de VDA a la versión 7.40.0.35 o posterior (con la versión 2311 o posterior del instalador de VDA)
- Virtual Apps and Desktops Remote PowerShell SDK versión 7.40 o posterior (publicada el 10 de enero de 2024 o posterior)
- SDK de PowerShell remoto versión 7.42 o posterior (publicado después del 16 de febrero de 2024)

**Cómo configurar los permisos de los recursos compartidos de archivos**

Los recursos compartidos de red que contienen los paquetes de instalación de VDA deben tener acceso de lectura para el servicio Agente de actualización de VDA, que se ejecuta como sistema local (entidad principal NT AUTHORITY\SYSTEM).

- **Permiso para recursos compartidos de archivos con unión a un dominio**

  Cuando la máquina VDA está unida a un dominio, la cuenta del **sistema local** (VUA se ejecuta como sistema local) usa las credenciales del equipo al acceder a los recursos compartidos de red.

  El permiso de privilegio mínimo se puede establecer concediendo acceso de **lectura** a los equipos del dominio.

  1. Elija a las personas de su red con las que quiere compartir el archivo.
  2. Haga clic en **Advanced Sharing Settings** y active **File and Printer Sharing**.

- **Permiso para recursos compartidos de archivos sin unión a un dominio**

  Cuando la máquina VDA no está unida a un dominio, la cuenta **Local System** (VUA se ejecuta como Local System) usa **ANONYMOUS LOGON** al acceder a los recursos compartidos de red.

  1. Seleccione una carpeta compartida.
  2. Inhabilite la protección con contraseña.
     a) Vaya a la ficha **Properties** de la carpeta.
     b) Seleccione **Network and Sharing Center**.
     c) Desactive **Password Protected Sharing**.
  3. Haga clic en **Advanced Sharing** para conceder un permiso para compartir.
     a) Seleccione **Permissions**.
     b) Conceda un permiso de lectura (**Read**) para el recurso compartido a **ANONYMOUS LOGON**.
  4. Seleccione la ficha **Security** para conceder permisos a la carpeta
     a) Haga clic en **Edit** para agregar permisos a la carpeta compartida
     b) Seleccione la carpeta compartida para conceder permisos de carpeta a **ANONYMOUS LOGON**.
  5. Haga clic en **Advanced** para activar **File and Printer Sharing**.
  6. Agregue el nombre de la carpeta compartida a **Network Access Security Policy**.

  > **Nota:**
  >
  > Reinicie el equipo para que el cambio surta efecto inmediatamente.

**Actualizaciones de VDA desde un recurso compartido de archivos local**

1. Descargue el instalador del VDA y colóquelo en el recurso compartido de archivos.

   > **Nota:**
   >
   > Con el servicio Virtual Upgrade Service, puede seleccionar entre la pista Current Release o la pista LTSR.
   >
   > **Por ejemplo:** Si el catálogo de máquinas está establecido en la versión Current Release, es decir, 2311, y la versión del VDA es 2305, debe actualizar el VDA a la versión 2311.

   a) Vaya a la página **Descargas** de nuestro sitio web.
   b) Seleccione **Citrix Virtual Apps and Desktops** como producto.
   c) Seleccione **Citrix Virtual Apps and Desktops 7 2311, All Editions**.
   d) Seleccione el instalador del VDA en el nodo **Components that are on the product ISO but also packaged separately**.

2. Seleccione el instalador de VDA correspondiente según el tipo de catálogo.

   - Descargue el **instalador de VDA para SO multisesión** si el tipo de catálogo es **multisesión**
   - Descargue el **instalador de VDA para SO de sesión única** si el tipo de catálogo es de **sesión única**
   - Descargue el **instalador de VDA de servicios básicos para SO de sesión única** si el tipo de catálogo es **Acceso con Remote PC**

> **Nota:**
>
> La versión del instalador de recursos compartidos de archivos debe coincidir **exactamente** con la versión del instalador más reciente publicada por VUS en la nube.

## Solucionar problemas técnicos

- Para las máquinas con estado `Power State Unknown`, consulte CTX131267 para obtener instrucciones.
- Para reparar máquinas virtuales que muestran continuamente un estado de energía desconocido, consulte How to fix VMs that continuously show an unknown power state.
- Si un Cloud Connector no funciona correctamente, las operaciones de aprovisionamiento de MCS (como las actualizaciones de catálogos) tardan más de lo habitual, y el rendimiento de la consola de administración se degrada significativamente.

### Qué hacer a continuación

Para obtener información sobre la administración de catálogos de hipervisores específicos, consulte:

- Administrar un catálogo de AWS
- Administrar un catálogo de Google Cloud Platform
- Administrar un catálogo de Microsoft Azure
- Administrar un catálogo de Microsoft System Center Virtual Machine Manager
- Administrar un catálogo de VMware
- Administrar un catálogo de XenServer

## Administrar un catálogo de AWS

January 24, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de AWS.

> **Nota:**
>
> Antes de administrar un catálogo de AWS, debe terminar de crear un catálogo de AWS. Consulte Crear un catálogo de AWS.

### Quitar etiquetas

Al crear un catálogo o una máquina virtual, se crean etiquetas en estos recursos:

- Máquina virtual
- Volumen del disco raíz
- Volumen del disco de identidad
- Interfaz de red elástica (ENI)
- Imagen del disco raíz (AMI)
- Plantilla de inicio
- Instantánea de la AMI o del disco raíz

Puede quitar máquinas virtuales y catálogos de máquinas de la base de datos de Citrix y quitar etiquetas creadas por Citrix. Puede usar:

- `Remove-ProvVM` con el parámetro `ForgetVM` para quitar máquinas virtuales y etiquetas creadas por Citrix de una sola máquina virtual o una lista de máquinas virtuales de un catálogo de máquinas.

> **Nota:**
>
> Con el parámetro `ForgetVM`, las máquinas virtuales se quitan de la base de datos del esquema de aprovisionamiento de Citrix; sin embargo, las máquinas virtuales permanecen en el hipervisor.

- `Remove-ProvScheme` con el parámetro `ForgetVM` para quitar un catálogo de máquinas de la base de datos de Citrix y recursos de un catálogo de máquinas.

Para hacerlo:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Desbloquee la máquina virtual antes de quitarlas. Por ejemplo:

```
Unlock-ProvVM -ProvisioningSchemeName "<name>" -VMID "<id"
<!--NeedCopy-->
```

4. Ejecute uno de estos comandos para quitar máquinas virtuales, el catálogo de máquinas y las etiquetas creadas por Citrix de los recursos.

   - Ejecute `Remove-ProvVM` con `ForgetVM` para quitar máquinas virtuales de la base de datos de Citrix y las etiquetas creadas por Citrix de las máquinas virtuales. Por ejemplo:

   ```
   Remove-ProvVM -ProvisioningSchemeName "<name>" -VMName "<name
       >" -ForgetVM
   <!--NeedCopy-->
   ```

   - Ejecute `Remove-ProvScheme` para quitar un catálogo de máquinas de la base de datos de Citrix y los recursos de dicho catálogo de máquinas. Por ejemplo:

   ```
   Run Remove-ProvScheme -ProvisioningSchemeName "<name>" -
       ForgetVM
   <!--NeedCopy-->
   ```

5. Verifique que la máquina virtual se haya quitado del Delivery Controller, pero no del hipervisor.

   a) Ejecute `Get-ProvVM -ProvisioningSchemeName "<name>"-VMName "<name>"`. Esto no debe devolver nada.

   b) Vaya a la consola de Amazon EC2. Debería ver las máquinas virtuales. Ahora, sin embargo, las etiquetas creadas por Citrix se han quitado. Se quitan las etiquetas creadas por Citrix de los siguientes recursos:

      - Máquina virtual
      - Volumen del disco raíz
      - Volumen del disco de identidad

- ENI

6. Si quita el catálogo de máquinas, verifique que el catálogo se haya quitado del Delivery Controller.

   a) Ejecute `Get-ProvScheme -ProvisioningSchemeName "forgetvmdemo"`. Esto debe devolver un error.

   b) Verifique en la consola de Amazon EC2 que se hayan quitado estos recursos.

      - Imagen del disco raíz (AMI)
      - Plantilla de inicio
      - Instantánea de la AMI o del disco raíz

### Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos de la plataforma AWS. Las etiquetas de la tabla se representan como "clave": "valor".

| Resource name | Etiqueta |
|---|---|
| Disco de ID | "Name": "VMName_IdentityDisk"<br>"XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Imagen | "XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| ENI | "Description": "XD Nic"<br>"XdConfig": "XdProvisioned=true"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco de SO | "Name": "VMName_rootDisk"<br>"XdConfig": "XdProvisioned=True"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"<br>[cuando AwsCaptureInstanceProperties = true]<br>"Citrix Resource": "" |

| Resource name | Etiqueta |
| --- | --- |
| PrepVM | [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” “Name”: “Preparation - CatalogName - xxxxxxxxxx” “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “Citrix Resource”: “” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| Instantánea publicada | “XdConfig”: “XdProvisioned=true” Si no se trata de una instantánea para la AMI de Volume Worker, “CitrixProvisioningSchemeId”es: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Plantilla | [cuando AwsCaptureInstanceProperties = true] “XdConfig”: “XdProvisioned=true” [cuando AwsCaptureInstanceProperties = true] “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true] “CitrixOperationalResource”: “” |
| VM en catálogo | “XdConfig”: “XdProvisioned=true” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” [cuando AwsCaptureInstanceProperties = true] “CitrixResource”: “” [cuando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:id”:”lt-xxxx” [cuando AwsCaptureInstanceProperties = true] “aws:ec2launchtemplate:version”: “n” |

| Resource name | Etiqueta |
| --- | --- |
| AMI de trabajador de volumen | [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true]<br>“CitrixOperationalResource”: “”<br>“XdConfig”: “XdProvisioned=true” |
| Programa previo (bootstrapper) de trabajador por volumen | “Name”: “XenDesktop Temp”<br>“XdConfig”: “XdProvisioned=true”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Instancia de trabajador de volumen | [cuando AwsCaptureInstanceProperties = true y AwsOperationalResourcesTagging = true]<br>“CitrixVolumeWorkerBootstrapper”: “”<br>“Name”: “Citrix.XD.Volumeworker-xxxx-xx-xx-xx-xxxx”<br>“XdConfig”: “XdProvisioned=true” |

### Más información

- Crear y administrar conexiones y recursos
- Conexión con AWS
- Crear catálogos de máquinas
- Crear un catálogo de AWS
- Administrar catálogos de máquinas

## Administrar un catálogo de Google Cloud Platform

February 12, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de Google Cloud.

> **Nota:**
>
> Antes de administrar un catálogo de Google Cloud Platform, debe terminar de crear un catálogo de Google Cloud Platform. Consulte Crear un catálogo de Google Cloud Platform.

### Agregar máquinas a un catálogo

Para agregar máquinas a un catálogo, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo de máquinas al que quiere agregar máquinas.
3. Seleccione **Agregar máquinas** en la barra de acciones.
4. En la página **Máquinas virtuales**, especifique la cantidad de máquinas que quiere agregar y, a continuación, seleccione **Siguiente**.
5. En la página **Identidades de las máquinas**, seleccione una cuenta de Active Directory y, a continuación, seleccione **Siguiente**.
6. En la página **Credenciales de dominio**, seleccione **Introducir credenciales**, escriba el nombre de usuario y la contraseña, seleccione **Guardar** y, a continuación, seleccione **Siguiente**.
7. En la página **Resumen**, confirme la información y seleccione **Finalizar**.

### Actualizar máquinas

Esta función puede ser útil en los casos en que quiera actualizar su imagen maestra o el nivel funcional mínimo.

Para actualizar las máquinas, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo de máquinas que contenga las máquinas que quiere actualizar.
3. Seleccione **Cambiar imagen maestra** en la barra de acciones.
4. En la página **Imagen**, seleccione una máquina virtual y el nivel funcional mínimo del catálogo y, a continuación, seleccione **Siguiente**.
5. En la página **Estrategia de implantación**, indique cuándo quiere actualizar las máquinas y, a continuación, seleccione **Siguiente**.
6. En la página **Resumen**, confirme la información y seleccione **Finalizar**.

### Revertir una actualización de máquina

Para revertir la actualización de una máquina, siga estos pasos:

> **Importante:**
>
> No elimine ni mueva ni cambie el nombre de las imágenes maestras. De lo contrario, no podrá revertir la actualización.

1. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
2. Seleccione el catálogo de máquinas en el que quiere revertir la actualización de la máquina.
3. Seleccione **Revertir imagen maestra** en la barra de acciones.
4. En la página **Vista general**, confirme la información y, a continuación, seleccione **Siguiente**.
5. En la página **Estrategia de implantación**, configure la estrategia de implantación y, a continuación, seleccione **Siguiente**.
6. En la página **Resumen**, confirme la información y seleccione **Finalizar**.

### Administración de energía

Citrix DaaS le permite administrar la energía de las máquinas de Google Cloud. Utilice el nodo **Buscar** del panel de navegación para localizar la máquina que quiere administrar. Estas son las acciones de energía que hay disponibles:

- Suprimir
- Iniciar
- Reiniciar
- Forzar reinicio
- Apagar
- Forzar apagado
- Agregar a grupo de entrega
- Administrar etiquetas
- Activar modo de mantenimiento

También puede administrar la energía de las máquinas de Google Cloud mediante Autoscale. Para ello, agregue las máquinas de Google Cloud a un grupo de entrega y, a continuación, habilite Autoscale para dicho grupo de entrega. Para obtener más información sobre Autoscale, consulte Autoscale.

### Actualizar las máquinas aprovisionadas mediante PowerShell

El comando `Set-ProvScheme` cambia el esquema de aprovisionamiento. Sin embargo, no afecta a las máquinas existentes. Ahora, con el comando `Set-ProvVMUpdateTimeWindow` de PowerShell, puede aplicar el esquema de aprovisionamiento actual a una máquina o un conjunto de máquinas persistentes o no persistentes. Actualmente, en GCP, las actualizaciones de propiedades que admite esta función son el perfil de máquina, la oferta de servicios y los parámetros de catálogo personalizados.

Puede actualizar:

- Una sola máquina virtual
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un ID de esquema de aprovisionamiento
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un nombre de esquema de aprovisionamiento

Para actualizar las máquinas virtuales:

1. Compruebe la configuración de las máquinas. Por ejemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Actualice el esquema de aprovisionamiento. Por ejemplo,

   - Actualización del perfil de máquina

```
`Set-ProvScheme –ProvisioningSchemeName "my-catalog" –
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofileinstance.vm"
<!--NeedCopy-->
```

   - Actualización de la oferta de servicios

```
 Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
     ServiceOffering “ XDHyp:\HostingUnits<hosting-unit>\
     serviceoffering.folder<service-offering>.serviceoffering"
 <!--NeedCopy-->
```

3. Compruebe si la propiedad actual de la máquina virtual coincide con el esquema de aprovisionamiento actual y si hay alguna acción de actualización pendiente en la máquina virtual. Por ejemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

   También puede encontrar máquinas con una versión en particular. Por ejemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
    VMName, ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Actualice las máquinas existentes.

   - Para actualizar todas las máquinas:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Para actualizar una lista de máquinas específicas:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
    -1
<!--NeedCopy-->
```

- Para actualizar las máquinas según el resultado de `Get-ProvVM`:

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
    ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Nota:**
>
> - `StartsNow` indica que la hora de inicio programada es la hora actual.
> - `DurationInMinutes` con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

5. Busque las máquinas que tienen una actualización programada. Por ejemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
    , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

6. Reinicie las máquinas. En el siguiente encendido, los cambios en las propiedades se aplicarán a las máquinas existentes. Puede comprobar el estado de la actualización con el siguiente comando:

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

### Cambiar las propiedades personalizadas relacionadas con el disco de un catálogo existente

Puede cambiar estas propiedades personalizadas relacionadas con el disco de un catálogo existente y de máquinas virtuales existentes del catálogo:

- `PersistOSDisk`
- `PersistWBC`

- `StorageType`
- `IdentityDiskStorageType`
- `WbcDiskStorageType`

> **Nota:**
>
> - La propiedad `StorageType` es para el disco del sistema operativo
> - La propiedad `PersistOsDisk` solo se puede configurar para catálogos no persistentes con caché de reescritura habilitada

Esta implementación le ayuda a seleccionar diferentes tipos de almacenamiento para diferentes discos incluso después de crear un catálogo y, por lo tanto, equilibra los precios asociados a los diferentes tipos de almacenamiento.

Para hacer esto, utilice los comandos de PowerShell `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow` .

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*`.
3. Ejecute `Get-ProvVM -VMName <VM name>` para obtener las propiedades personalizadas.
4. Cambie la cadena de propiedades personalizada:
   a) Copie las propiedades personalizadas en un bloc de notas y cámbieles las propiedades personalizadas.
   b) En la ventana de **PowerShell**, pegue las propiedades personalizadas modificadas del Bloc de notas y asigne una variable a las propiedades personalizadas modificadas. Por ejemplo:

```
$cp =  '<CustomProperties xmlns=http://schemas.citrix.com
   /2014/xd/machinecreation xmlns:xsi="http://www.w3.org/2001/
   XMLSchema-instance">
<Property xsi:type="StringProperty" Name="CatalogZones" Value
   ="" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="
   true" />
<Property xsi:type="StringProperty" Name="PersistOSDisk" Value
   ="true" />
<Property xsi:type="StringProperty" Name="WBCDiskStorageType"
   Value="pd-standard" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   pd-standard" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Actualice el catálogo existente. Por ejemplo:

```
Set-ProvScheme -ProvisioningSchemeName <yourCatalogName> -
    CustomProperties $cp
<!--NeedCopy-->
```

6. Actualice las máquinas virtuales existentes. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Reinicie las máquinas virtuales. En el siguiente encendido, los cambios en las propiedades personalizadas se aplicarán a las máquinas virtuales existentes.

### Proteger contra la eliminación accidental de máquinas

Citrix DaaS le permite proteger los recursos de MCS en Google Cloud para evitar la eliminación accidental. Configure la máquina virtual aprovisionada estableciendo el indicador `deletionProtection` en TRUE.

De forma predeterminada, las VM aprovisionadas a través del plug-in de Google Cloud o MCS se crean con "InstanceProtection"habilitada. La implementación se aplica tanto a catálogos persistentes como no persistentes. Los catálogos no persistentes se actualizan cuando las instancias se vuelven a crear a partir de la plantilla. Para las máquinas persistentes, se puede establecer el indicador en la consola de Google Cloud. Para obtener más información sobre cómo establecer el indicador, consulte el sitio de documentación de Google. Las nuevas máquinas que se agregan a catálogos persistentes se crean con la opción `deletionProtection` habilitada.

Si intenta eliminar una instancia de VM para la que estableció el indicador `deletionProtection`, la solicitud falla. Sin embargo, si se le concede el permiso `compute.instances.setDeletionProtection` o se le asigna el rol de **administrador de procesos** (Compute Admin) de IAM, puede restablecer el indicador para permitir la eliminación del recurso.

### Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos de la plataforma GCP. Las etiquetas de la tabla se representan como "clave": "valor".

| Resource name | Etiqueta |
|---|---|
| Disco de ID | "CitrixResource": "internal"<br>"CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

| Resource name | Etiqueta |
| --- | --- |
| Imagen | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Disco de SO | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| máquina virtual de preparación | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |
| Instantánea publicada | “CitrixResource”: “internal” |
| Depósito de almacenamiento | “CitrixResource”: “internal” |
| Plantilla | “CitrixResource”: “internal” |
| VM en catálogo | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”<br>“CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx”. El plug-in también agrega esta etiqueta para las VM aprovisionadas con MCS: “citrix-provisioning-scheme-id”: “provSchemeId”. Puede usar esta etiqueta para filtrar por catálogo en la consola de GCP. |
| Disco WBC | “CitrixResource”: “internal”<br>“CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

> **Nota:**
>
> Una máquina virtual no está visible en el inventario de Citrix si se agrega una etiqueta **CitrixResource** para identificarla como un recurso creado por MCS. Puede quitar la etiqueta o cambiarle el nombre para que sea visible.

## Más información

- Crear y administrar conexiones y recursos
- Conexión con entornos de Google Cloud

- Crear catálogos de máquinas
- Crear un catálogo de Google Cloud Platform
- Administrar catálogos de máquinas

## Administrar un catálogo de HPE Moonshot

May 17, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos del catálogo de HPE Moonshot.

> **Nota:**
>
> Antes de administrar un catálogo de HPE Moonshot, debe terminar de un catálogo de HPE Moonshot. Consulte Crear un catálogo de máquinas de HPE Moonshot.

### Administración de energía

Citrix DaaS le permite administrar la energía de las máquinas de HPE Moonshot. Utilice el nodo **Buscar** del panel de navegación para localizar la máquina que quiere administrar. Estas son las acciones de energía que hay disponibles:

- Iniciar
- Apagar
- Forzar apagado
- Reiniciar
- Restablecer

> **Nota:**
>
> No se admiten las acciones de energía **Suspender** y **Reanudar**.

### Más información

- Crear y administrar conexiones y recursos
- Conexión a HPE Moonshot
- Crear catálogos de máquinas
- Crear un catálogo de máquinas de HPE Moonshot
- Administrar catálogos de máquinas

# Administrar un catálogo de Microsoft Azure

May 17, 2024

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

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de nube de Microsoft Azure Resource Manager.

> **Nota:**
>
> Antes de administrar un catálogo de Microsoft Azure, debe terminar de crear un catálogo de Microsoft Azure. Consulte Crear un catálogo de Microsoft Azure.

## Cambio del tipo de almacenamiento a un nivel inferior al apagar una máquina virtual

Puede ahorrar costes de almacenamiento al cambiar el tipo de almacenamiento de un disco administrado a un nivel inferior cuando apaga una máquina virtual. Para ello, utilice la propiedad `StorageTypeAtShutdown` personalizada.

El tipo de almacenamiento del disco pasa a un nivel inferior (tal y como se especifica en la propiedad personalizada `StorageTypeAtShutdown`) al apagar la máquina virtual. Tras encender la máquina virtual, el tipo de almacenamiento vuelve a ser el original (tal y como se especifica en la propiedad `StorageType` personalizada o en la propiedad `WBCDiskStorageType` personalizada).

> **Importante:**
>
> - El disco no existe hasta que la máquina virtual se encienda al menos una vez. Por lo tanto, no puede cambiar el tipo de almacenamiento la primera vez que enciende la máquina virtual.
> - Es posible que las máquinas virtuales tarden un poco más en iniciarse después de cambiar el tipo de almacenamiento a un nivel inferior.

### Requisitos

- Aplicable a un disco administrado. Esto implica establecer la propiedad personalizada `UseManagedDisks` en true.

- Aplicable a un catálogo persistente y no persistente con un disco de sistema operativo persistente. Esto implica establecer la propiedad personalizada `persistOsDisk` en true.
- Aplicable a un catálogo no persistente con un disco WBC persistente. Esto implica establecer la propiedad personalizada `persistWBC` en true.

#### Restricción

- Según informa Microsoft, solo se puede cambiar el tipo de disco dos veces al día. Consulte el documento de Microsoft. Según informa Citrix, la actualización de `StorageType` tiene lugar cada vez que hay una acción de inicio o desasignación para la máquina virtual. Por lo tanto, limite la cantidad de acciones de energía por máquina virtual a dos veces al día. Por ejemplo, una acción de energía por la mañana para iniciar la máquina virtual y otra por la noche para desasignarla.

#### Cambiar el tipo de almacenamiento a un nivel inferior

Antes de continuar con los pasos, consulte los Requisitos y Restricciones.

1. Agregue la propiedad personalizada `StorageTypeAtShutdown`, establezca el valor en Standard_LRS (HDD) y cree un catálogo mediante `New-ProvScheme`. Para obtener información sobre la creación de catálogos mediante PowerShell, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

   > **Nota:**
   >
   > Si `StorageTypeAtShutdown` tiene algún valor que no esté vacío o no sea Standard_LRS (HDD), la operación fallará.

   Ejemplo de configuración de propiedades personalizadas al crear un catálogo persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="Premium_LRS “ />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
```

```
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> '
<!--NeedCopy-->
```

Ejemplo de configuración de propiedades personalizadas al crear un catálogo no persistente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.
    com/2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="
    true" />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType"
    Value="Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value=""
    />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2"
    />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows"
    />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true
    />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=
    true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties> '
<!--NeedCopy-->
```

> **Nota:**
>
> Al utilizar un perfil de máquina, la propiedad personalizada tiene prioridad sobre la propiedad definida en `MachineProfile`.

2. Apague la máquina virtual y compruebe el tipo de almacenamiento de la máquina virtual en Azure Portal. El tipo de almacenamiento del disco pasa a un nivel inferior, tal y como se especifica en la propiedad `StorageTypeAtShutdown` personalizada.
3. Encienda la máquina virtual. El tipo de almacenamiento del disco vuelve al tipo de almacenamiento mencionado en:

   - Propiedad `StorageType` personalizada para el disco del sistema operativo
   - Propiedad `WBCDiskStorageType` personalizada para el disco WBC solo si la especifica en `CustomProperties`. De lo contrario, vuelve al tipo de almacenamiento mencionado en `StorageType`.

### Aplicar `StorageTypeAtShutdown` a un catálogo existente

Antes de continuar con los pasos, consulte los Requisitos y Restricciones.

Use `Set-ProvScheme` para aplicar `StorageTypeAtShutdown` a las nuevas máquinas virtuales agregadas a un catálogo existente.

Ejemplo de configuración de propiedades personalizadas al agregar una máquina virtual a un catálogo existente:

```
$customProperties='<CustomProperties xmlns="http://schemas.citrix.com
    /2014/xd/machinecreation"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
     />
<Property xsi:type="StringProperty" Name="StorageType" Value="
    Premium_LRS" />
<Property xsi:type="StringProperty" Name="WbcDiskStorageType" Value="
    Standard_SSD_LRS" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
    Windows_Client" />
<Property xsi:type="StringProperty" Name="SchemaVersion" Value="2" />
<Property xsi:type="StringProperty" Name="OsType" Value="Windows" />
<Property xsi:type="BooleanProperty" Name="persistWBC" Value=true />
<Property xsi:type="BooleanProperty" Name="persistOsDisk" Value=true />
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown" Value
    ="Standard_LRS" />
</CustomProperties> '

$ProvScheme = Get-Provscheme -ProvisioningSchemeName $CatalogName

Set-ProvScheme -ProvisioningSchemeName $ProvScheme.
    ProvisioningSchemeName -CustomProperties $customProperties
<!--NeedCopy-->
```

### Cambiar el tipo de almacenamiento de las máquinas virtuales existentes a un nivel inferior al apagarlas

Antes de continuar con los pasos, consulte los Requisitos y Restricciones.

Puede ahorrar costes de almacenamiento si cambia el tipo de almacenamiento de las máquinas virtuales existentes a un nivel inferior cuando estas están apagadas.

Para cambiar el tipo de almacenamiento de las máquinas de un catálogo a un nivel inferior cuando las VM estén apagadas:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.

3. Ejecute `Get-Provscheme -ProvisioningSchemeName $CatalogName`.
4. Cambie la cadena de propiedades personalizada.

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="StorageTypeAtShutdown"
    Value="Standard_LRS" />
</CustomProperties>'
<!--NeedCopy-->
```

5. Actualice el esquema de aprovisionamiento del catálogo existente. La actualización se aplica a las nuevas máquinas virtuales que se agregan después de ejecutar `Set-ProvScheme`.

```
Set-ProvScheme -ProvisioningSchemeName $CatalogName -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Actualice las máquinas virtuales existentes para habilitar `StorageTypeAtShutdown`.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. La próxima vez que encienda las máquinas, se actualizará la propiedad `StorageTypeAtShutdown` de las máquinas. El tipo de almacenamiento cambiará la próxima vez que se apague.
8. Ejecute el siguiente comando para ver el valor `StorageTypeAtShutdown` de cada máquina virtual de un catálogo.

```
Get-ProvVM -ProvisioningSchemeName <catalog-name> | foreach {
  $vmName = $_.VMName; $storageTypeAtShutdown = ($_.CustomVmData |
       ConvertFrom-Json).StorageTypeAtShutdown.
      DiskStorageAccountType; return New-Object psobject -Property
      @{
  "VMName" = $vmName; "StorageTypeAtShutdown" =
      $storageTypeAtShutdown  }
   }

<!--NeedCopy-->
```

### Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento

El comando `Set-ProvScheme` cambia el esquema de aprovisionamiento. Sin embargo, no afecta a las máquinas existentes. Con el comando `Set-ProvVMUpdateTimeWindow` de PowerShell, puede aplicar el esquema de aprovisionamiento actual a una máquina o un conjunto de máquinas persistentes o no persistentes. También puede programar un intervalo de tiempo para

las actualizaciones de configuración de las máquinas aprovisionadas por MCS existentes. Cualquier encendido o reinicio durante el intervalo de tiempo programado aplica una actualización programada del esquema de aprovisionamiento a una máquina. Actualmente, en Azure, puede actualizar `ServiceOffering`, `MachineProfile` y estas propiedades personalizadas:

- `StorageType`
- `WBCDiskStorageType`
- `IdentityDiskStorageType`
- `LicenseType`
- `DedicatedHostGroupId`
- `PersistWBC`
- `PersistOsDisk`
- `PersistVm`

> **Nota:**
>
> - Solo puede actualizar las propiedades personalizadas `StorageType`, `WBCDiskStorageType` y `IdentityDiskStorageType` de un catálogo mediante un disco administrado en entornos de Azure.
> - Si ejecuta `Set-ProvVMUpdateTimeWindow` dos veces, se aplicará el comando más reciente.

Puede actualizar:

- Una sola máquina virtual
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un ID de esquema de aprovisionamiento
- Una lista de máquinas virtuales específicas o todas las máquinas virtuales asociadas a un nombre de esquema de aprovisionamiento (nombre del catálogo de máquinas)

Tras realizar los siguientes cambios en el esquema de aprovisionamiento, la instancia de máquina virtual se vuelve a crear para los catálogos persistentes en Azure:

- Cambiar `MachineProfile`
- Quitar `LicenseType`
- Quitar `DedicatedHostGroupId`

> **Nota:**
>
> El disco del sistema operativo de las máquinas existentes, junto con todos sus datos, permanecen tal cual y una nueva máquina virtual se conecta al disco.

Antes de actualizar las máquinas virtuales existentes:

1. Compruebe la configuración de las máquinas. Por ejemplo,

```
Get-ProvScheme | select ProvisioningSchemeName,
    ProvisioningSchemeVersion
<!--NeedCopy-->
```

2. Actualice el esquema de aprovisionamiento. Por ejemplo,

   - Con VM como entrada de perfil de máquina:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
         MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
         machineprofile.folder<resource-group>.resourcegroup<
         virtual-machine>.vm"
     <!--NeedCopy-->
     ```

   - Con la especificación de plantilla como entrada del perfil de la máquina:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog"
     -MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
         machineprofile.folder<resource-group>.resourcegroup<
         template-spec>.templatespec<template-spec-version>.
         templatespecversion"
     -ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
         serviceoffering.folder<service-offering>.serviceoffering"
     <!--NeedCopy-->
     ```

   - Con solo oferta de servicios:

     ```
     Set-ProvScheme -ProvisioningSchemeName "my-catalog" -
         ServiceOffering "XDHyp:\HostingUnits<hosting-unit>\
         serviceoffering.folder<service-offering>.serviceoffering"
     <!--NeedCopy-->
     ```

3. Compruebe si la propiedad actual de la máquina virtual coincide con el esquema de aprovisionamiento actual y si hay alguna acción de actualización pendiente en la máquina virtual. Por ejemplo,

   ```
   Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
       ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

   También puede encontrar máquinas con una versión en particular. Por ejemplo,

   ```
   Get-ProvVM -Filter "ProvisioningSchemeVersion -eq 1" | select
       VMName, ProvisioningSchemeVersion
   <!--NeedCopy-->
   ```

Para solicitar que las actualizaciones de las máquinas existentes se apliquen en el próximo reinicio:

1. Ejecute estos comandos para actualizar las máquinas existentes y hacer que las actualizaciones se apliquen en el próximo reinicio.

- Para actualizar todas las máquinas. Por ejemplo,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Para actualizar una lista de máquinas específicas. Por ejemplo,

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName <List-Of-Vm-Names> -StartsNow -DurationInMinutes
   -1
<!--NeedCopy-->
```

- Para actualizar las máquinas según el resultado de Get-ProvVM. Por ejemplo,

```
Get-ProvVM -ProvisioningSchemeName "my-catalog" | Set-
   ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
   -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

> **Nota:**
>
> - `StartsNow` indica que la hora de inicio programada es la hora actual.
> - `DurationInMinutes` con un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

2. Busque las máquinas que tienen una actualización programada. Por ejemplo,

```
Get-ProvVM -Filter "ProvisioningSchemeUpdateAfter" | select VMName
   , ProvisioningSchemeUpdateAfter
<!--NeedCopy-->
```

3. Reinicie las máquinas. En el siguiente encendido, los cambios en las propiedades se aplicarán a las máquinas existentes. Puede comprobar el estado de la actualización con el siguiente comando. Por ejemplo,

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

Para programar la actualización de una máquina virtual a los parámetros de aprovisionamiento más recientes la próxima vez que se inicie en la franja horaria programada:

1. Ejecute los comandos siguientes:

- Para programar una actualización con la hora de inicio como la hora actual:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName my-catalog
    -VMName vm1 -StartsNow -DurationInMinutes 120
<!--NeedCopy-->
```

- Para programar una actualización en un fin de semana

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1" -StartTimeInUTC "10/15/2022 9:00am" -DurationInMinutes (New-TimeSpan -Days 2).TotalMinutes
<!--NeedCopy-->
```

> **Nota:**
>
> - `VMName` es opcional. Si no se especifica, la actualización se programa para todo el catálogo.
> - En lugar de `StartTimeInUTC`, use `StartsNow` para indicar que la hora de inicio de la programación es la hora actual.
> - `DurationInMinutes` es opcional. El valor predeterminado es de 120 minutos. Un número negativo (por ejemplo, -1) indica que no hay ningún límite superior en la ventana de tiempo de la programación.

2. Compruebe el estado de la actualización.

```
Get-ProvVM | select VMName, ProvisioningSchemeUpdateRequested, ProvisioningSchemeUpdateUntil, ProvisioningSchemeVersion
<!--NeedCopy-->
```

3. Encienda la máquina virtual. Si enciende la máquina después de la franja horaria programada, no se aplica la actualización de la configuración. Si enciende la máquina durante la franja horaria programada

   - Si la máquina está apagada y:
     - No enciende la máquina, no se aplica la actualización de la configuración
     - Enciende la máquina, se aplica la actualización de la configuración
   - Si la máquina está encendida y:
     - No reinicia la máquina, no se aplica la actualización de la configuración
     - Reinicia la máquina, se aplica la actualización de la configuración

Para cancelar la actualización de configuración:

También puede cancelar una actualización de configuración de una sola máquina virtual, varias máquinas virtuales o todo un catálogo. Para cancelar una actualización de configuración:

1. Ejecute `Clear-ProvVMUpdateTimeWindow`. Por ejemplo:

   - Para cancelar la actualización de configuración programada para una sola máquina virtual:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-catalog" -VMName "vm1"
```

```
<!--NeedCopy-->
```

- Para cancelar la actualización de configuración programada para varias máquinas virtuales:

```
Clear-ProvVMUpdateTimeWindow -ProvisioningSchemeName "my-
    catalog" -VMName "vm1","vm2"
<!--NeedCopy-->
```

> **Nota:**
>
> Las máquinas virtuales deben ser del mismo catálogo.

### Actualizar propiedades de máquinas virtuales individuales

Puede actualizar propiedades de máquinas virtuales individuales en catálogos de máquinas de MCS persistentes mediante el comando de PowerShell `Set-ProvVM`. Sin embargo, las actualizaciones no se aplican de forma inmediata. Debe configurar el intervalo de tiempo mediante el comando de PowerShell `Set-ProvVMUpdateTimeWindow` para que se apliquen las actualizaciones.

Esta implementación le ayuda a administrar máquinas virtuales individuales de manera eficiente sin actualizar todo el catálogo de máquinas. Actualmente, esta función solo se aplica al entorno de Azure.

Actualmente, las propiedades que puede actualizar son:

- `CustomProperties`
- `ServiceOffering`
- `MachineProfile`

Con esta función, puede:

- Actualizar las propiedades de una máquina virtual
- Conservar las propiedades actualizadas en una máquina virtual después de actualizar el catálogo de máquinas
- Revertir las actualizaciones de configuración aplicadas a una máquina virtual

Antes de actualizar las propiedades de una máquina virtual:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Compruebe la configuración del catálogo de máquinas existente. Por ejemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

4. Compruebe la configuración de la máquina virtual en la que quiere aplicar las actualizaciones. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

#### Actualizar propiedades de una máquina virtual

Haga lo siguiente para actualizar las propiedades de una máquina virtual:

1. Apague la máquina virtual en la que quiera aplicar las actualizaciones.
2. Actualice las propiedades de la máquina virtual. Por ejemplo, si quiere actualizar la propiedad personalizada de tipo de almacenamiento (`StorageType`) de la máquina virtual, ejecute lo siguiente:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

   Puede actualizar propiedades de dos máquinas virtuales de un catálogo de máquinas simultáneamente. Por ejemplo:

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    CustomProperties "...<Property Name='StorageType' Value='
    Premium_LRS' />..."
<!--NeedCopy-->
```

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine2 -
    CustomProperties "...<Property Name='StorageType' Value='
    StandardSSD_LRS' />..."
<!--NeedCopy-->
```

   > **Nota:**
   >
   > Las actualizaciones no se aplican de forma inmediata.

3. Obtenga la lista de propiedades que se especificaron para actualizarse y la versión de configuración. Por ejemplo:

```
Get-ProvVMConfiguration -ProvisioningSchemeName AzureCatalog -
    VMName machine1
<!--NeedCopy-->
```

   Compruebe el valor de la propiedad `Version` y las propiedades que se actualizarán (en este caso, `StorageType`).

4. Compruebe la versión de la configuración. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Compruebe el valor de la propiedad `ProvVMConfigurationVersion`. La actualización aún no se ha aplicado. La máquina virtual aún tiene la configuración anterior.

5. Solicite una actualización programada. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

Para obtener más información sobre las actualizaciones programadas, consulte Actualizar las máquinas aprovisionadas al estado actual del esquema de aprovisionamiento.

> **Nota:**
>
> También se aplica cualquier actualización pendiente de esquemas de aprovisionamiento.

6. Reinicie la VM. Por ejemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

7. Compruebe la versión de la configuración. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Compruebe el valor de la propiedad `ProvVMConfigurationVersion`. Ahora la actualización sí se aplica. La máquina virtual ya tiene la nueva configuración.

8. Para aplicar más actualizaciones de configuración en la máquina virtual, apáguela y repita los pasos.

### Conservar las propiedades actualizadas en una máquina virtual después de actualizar el catálogo de máquinas

Haga lo siguiente para mantener las propiedades actualizadas en una máquina virtual:

1. Apague la máquina virtual en la que quiera aplicar las actualizaciones.
2. Actualice el catálogo de máquinas. Por ejemplo, si quiere cambiar el tamaño de la máquina virtual (`ServiceOffering`) y el tipo de almacenamiento (`StorageType`), ejecute lo siguiente:

```
Set-ProvScheme -ProvisioningSchemeName AzureCatalog -
    ServiceOffering Standard_E4_v3 -CustomProperties "...<Property
    Name='StorageType' Value='StandardSSD_LRS' />..."
```

```
<!--NeedCopy-->
```

3. Obtener los detalles de configuración del catálogo de máquinas. Por ejemplo:

```
Get-ProvScheme -ProvisioningSchemeName AzureCatalog
<!--NeedCopy-->
```

Ahora el valor de `ProvisioningSchemeVersion` se incrementa en uno. También se actualizan el tamaño y el tipo de almacenamiento de la máquina virtual.

4. Actualice las propiedades de la máquina virtual. Por ejemplo, proporcione un perfil de máquina a la máquina virtual.

```
Set-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1 -
    MachineProfile "XDHyp:\HostingUnits<hosting-unit>\
    machineprofile.folder<resource-group>.resourcegroup<template-
    spec>.templatespec<template-spec-version>.templatespecversion"
<!--NeedCopy-->
```

> **Nota:**
>
> La entrada del perfil de máquina tiene especificados una etiqueta y un tamaño de máquina virtual diferentes (`ServiceOffering`).

5. Obtenga la lista de propiedades que tendrá la máquina virtual después de combinar las actualizaciones de configuración de la máquina virtual con las actualizaciones del catálogo de máquinas. Por ejemplo:

```
Get-ProvVMConfigurationResultantSet -ProvisioningSchemeName
    AzureCatalog -VMName machine1
<!--NeedCopy-->
```

> **Nota:**
>
> Cualquier actualización de la máquina virtual supeditará las actualizaciones realizadas en el catálogo de máquinas.

6. Solicite una actualización programada para la máquina virtual. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

7. Reinicie la VM. Por ejemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

La máquina virtual mantiene su tamaño de máquina virtual actualizado tal y como se deriva del perfil de máquina. Los valores de etiqueta especificados en el perfil de máquina también se

aplican a la máquina virtual. Sin embargo, el tipo de almacenamiento se deriva del esquema de aprovisionamiento más reciente.

8. Obtenga la versión de configuración de la máquina virtual. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Ahora, `ProvisioningSchemeVersion` y `ProvVMConfigurationVersion` muestra la versión más reciente.

#### Revertir las actualizaciones de configuración aplicadas a una máquina virtual

1. Después de aplicar las actualizaciones a una máquina virtual, apáguela.
2. Ejecute el siguiente comando para quitar las actualizaciones que se aplican en la máquina virtual. Por ejemplo:

```
Set-ProvVM -RevertToProvSchemeConfiguration -
    ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

3. Solicite una actualización programada para la máquina virtual. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName AzureCatalog -
    VMName machine1 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Reinicie la VM. Por ejemplo:

```
New-BrokerHostingPowerAction -MachineName machine1 -Action TurnOn
<!--NeedCopy-->
```

5. Compruebe la versión de configuración de la máquina virtual. Por ejemplo:

```
Get-ProvVM -ProvisioningSchemeName AzureCatalog -VMName machine1
<!--NeedCopy-->
```

Ahora, el valor de `ProvVMConfigurationVersion` es la versión de configuración del catálogo de máquinas.

### Cambiar el cifrado del disco

Puede cambiar el cifrado del disco en los entornos de virtualización de Azure y hacer lo siguiente:

- Crear un catálogo de máquinas MCS con un conjunto de cifrado de disco (DES) distinto del DES de la imagen maestra mediante el comando `New-ProvScheme`. Por ejemplo:

```
$customProperties = @"
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="DiskEncryptionSetId" Name="Zones" Value="/subscriptions/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX/resourceGroups/testrsg/providers/Microsoft.Compute/diskEncryptionSets/test-diskEncryptionSet"/>
</CustomProperties>
"@
New-ProvScheme -CleanOnBoot `
-ProvisioningSchemeName $provisioningSchemeName `
-HostingUnitName $hostingUnitName `
-IdentityPoolName $identityPoolName `
-InitialBatchSizeHint $numberOfVms `
-masterImagePath $masterImagePath `
-NetworkMapping $networkMapping `
-CustomProperties $customProperties
<!--NeedCopy-->
```

- Cambiar el tipo de cifrado del disco de una clave DES a otra clave DES de un catálogo de máquinas de MCS existente y de las máquinas virtuales existentes mediante los comandos `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`. Después de reiniciar las máquinas virtuales, puede ver la clave DES actualizada. Por ejemplo:

```
$customProperties = '<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId" Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/providers/Microsoft.Compute/diskEncryptionSets/diskEncryptionSet1" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Actualizar una máquina virtual y un catálogo de máquinas de MCS que antes no estuvieran habilitados para CMEK para que tengan cifrado (DES) con clave de cifrado administrada por el cliente (CMEK), cifrado de disco en el host o el doble cifrado mediante los comandos `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`. Para obtener información sobre los diferentes tipos de cifrado, consulte Cifrado del lado del servidor de Azure, Cifrado de discos de Azure en el host y Cifrado doble en disco administrado.
- Actualizar máquinas virtuales y un catálogo de máquinas de MCS existentes para que no estén cifrados y que anteriormente estuvieran cifrados mediante los comandos `Set-ProvScheme` y `Set-ProvVMUpdateTimeWindow`. Por ejemplo:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog
    -VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

- Habilitar el cifrado de discos con un dispositivo de punto final privado (un catálogo de máquinas MCS que use una conexión de host habilitada con `ProxyHypervisorTrafficThroughConnector`). Para obtener más información sobre `ProxyHypervisorTrafficThroughConnector`, consulte Crear un entorno seguro para el tráfico administrado de Azure. Para obtener información sobre cómo habilitar el cifrado de disco con dispositivos de punto final privados, consulte Habilitar el cifrado de disco con dispositivos de punto final privados.

#### Habilitar el cifrado de disco con dispositivos de punto final privados

Según la limitación de Azure, actualmente no se puede usar el cifrado del lado del servidor con claves administradas por el cliente para dispositivos de punto final privados. Sin embargo, puede actualizar máquinas virtuales y un catálogo de máquinas de MCS con dispositivos de punto final privados para cifrarlos con la clave DES.

**Actualizar un catálogo de máquinas existente con dispositivos de punto final privados** Estos son los pasos detallados para actualizar un catálogo de máquinas existente con dispositivos de punto final privados:

1. Cree un catálogo sin cifrado de disco mediante `ProxyHypervisorTrafficThroughConnector`. Para obtener más información sobre `ProxyHypervisorTrafficThroughConnector`, consulte Crear un entorno seguro para el tráfico administrado de Azure.
2. Ejecute `Set-ProvScheme` para actualizar el catálogo con `DiskEncryptionSetId`.

   > **Nota:**
   >
   > `DiskEcryptionSetId` se puede configurar mediante `CustomProperties` o `MachineProfile`. Cuando se define tanto en `CustomProperties` como en `MachineProfile`, se aplican las propiedades definidas en `CustomProperties`.

   Ejemplo al usar `CustomProperties`:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
    providers/Microsoft.Compute/diskEncryptionSets/
    diskEncryptionSet1"/>
</CustomProperties>'
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
<!--NeedCopy-->
```

Ejemplo al usar MachineProfile: Use una máquina virtual que tenga habilitado el cifrado de disco o una especificación de plantilla con parámetros de cifrado de disco:

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
    folder\testrg.resourcegroup\new-template.vm"
<!--NeedCopy-->
```

Como alternativa, puede actualizar el perfil de una máquina mediante la interfaz de Configuración completa.

3. Ejecute `Set-ProvVMUpdateTimeWindow` para actualizar las máquinas virtuales del catálogo existentes. Por ejemplo:

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
    VMName azu01, azu02 -StartsNow -DurationInMinutes -1
<!--NeedCopy-->
```

4. Después de reiniciar las máquinas virtuales, puede ver el cifrado de disco actualizado en los discos de las máquinas virtuales en Azure Portal.

5. Ejecute `Set-ProvScheme` para anular el cifrado de disco antes de agregar nuevas máquinas virtuales de catálogo.

   > **Nota:**
   >
   > Este paso es obligatorio porque está actualizando un catálogo de dispositivos de punto final privados. Si no sigue este paso, aparecerán errores al intentar agregar nuevas máquinas virtuales al catálogo.

   Por ejemplo:

```
$customProperties = '<CustomProperties xmlns="http://schemas.
    citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
    org/2001/XMLSchema-instance">
<Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
    Value="" />
</CustomProperties>'
```

```
Set-ProvScheme -ProvisioningSchemeName azure-catalog -
    CustomProperties $customProperties
<!--NeedCopy-->
```

6. Agregue nuevas VM al catálogo.

**Actualizar máquinas virtuales de catálogo individuales** Los pasos detallados para actualizar las máquinas virtuales de catálogo individuales son los siguientes:

1. Cree un catálogo sin cifrado de disco mediante `ProxyHypervisorTrafficThroughConnector`. Para obtener más información sobre `ProxyHypervisorTrafficThroughConnector`, consulte Crear un entorno seguro para el tráfico administrado de Azure.
2. Ejecute `Set-ProvVM` para actualizar la máquina virtual del catálogo con `DiskEncryptionSetId`.

   > **Nota:**
   >
   > `DiskEcryptionSetId` se puede configurar mediante `CustomProperties` o `MachineProfile`.

   Ejemplo al usar `CustomProperties`:

   ```
   $customProperties = '<CustomProperties xmlns="http://schemas.
       citrix.com/2014/xd/machinecreation" xmlns:xsi="http://www.w3.
       org/2001/XMLSchema-instance">
   <Property xsi:type="StringProperty" Name="DiskEncryptionSetId"
       Value="/subscriptions/456c683e2ed7/resourceGroups/testrg/
       providers/Microsoft.Compute/diskEncryptionSets/
       diskEncryptionSet1" />
   </CustomProperties>'
   Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
       CustomProperties $customProperties
   <!--NeedCopy-->
   ```

   Ejemplo al usar MachineProfile:

   ```
   Set-ProvVM -ProvisioningSchemeName azure-catalog  -VMName azu01 -
       MachineProfile "XDHyp:\HostingUnits\azureunit\machineprofile.
       folder\testrg.resourcegroup\new-template.vm"
   <!--NeedCopy-->
   ```

3. Ejecute `Set-ProvVMUpdateTimeWindow` para actualizar las máquinas virtuales del catálogo existentes. Por ejemplo:

   ```
   Set-ProvVMUpdateTimeWindow -ProvisioningSchemeName azure-catalog -
       VMName azu01 -StartsNow -DurationInMinutes -1
   <!--NeedCopy-->
   ```

4. Después de reiniciar las máquinas virtuales, puede ver el cifrado de disco actualizado en los discos de las máquinas virtuales en Azure Portal.
5. Agregue nuevas VM al catálogo.

### Obtener información de las máquinas virtuales de Azure, instantáneas, el disco del sistema operativo y la definición de imagen de la galería

Puede mostrar información de una máquina virtual de Azure, incluidos el disco y el tipo del sistema operativo, la instantánea y la definición de imágenes de galería. Esta información se muestra para los recursos de la imagen maestra cuando se asigna un catálogo de máquinas. Utilice esta funcionalidad para ver y seleccionar una imagen de Linux o Windows. Se agregó una propiedad de PowerShell, `TemplateIsWindowsTemplate`, al parámetro `AdditionDatafield`. Este campo contiene información específica de Azure: el tipo de máquina virtual, el disco del sistema operativo, la información de la imagen de la galería y la información sobre el tipo de SO. Al establecer `TemplateIsWindowsTemplate` en **True**, significa que el tipo de sistema operativo es Windows; al establecer `TemplateIsWindowsTemplate` en **False**, significa que el tipo de sistema operativo es Linux.

> **Sugerencia:**
>
> La información que muestra la propiedad `TemplateIsWindowsTemplate` de PowerShell se deriva de la API de Azure. A veces, es posible que este campo esté vacío. Por ejemplo, una instantánea de un disco de datos no contiene el campo `TemplateIsWindowsTemplate` porque el tipo de sistema operativo no se puede obtener de una instantánea.

Por ejemplo, establezca el parámetro `AdditionData` de la máquina virtual de Azure en **True** para el tipo de sistema operativo Windows mediante PowerShell:

```
PS C:\Users\username> (get-item XDHyp:\HostingUnits\mynetwork\image.
    folder\username-dev-testing-rg.resourcegroup\username-dev-tsvda.vm).
    AdditionalData
Key Value
ServiceOfferingDescription Standard_B2ms
HardDiskSizeGB 127
ResourceGroupName FENGHUAJ-DEV-TESTING-RG
ServiceOfferingMemory 8192
ServiceOfferingCores 2
TemplateIsWindowsTemplate True
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SupportedMachineGenerations Gen1,Gen2
<!--NeedCopy-->
```

### Obtener información del nombre de la región de las máquinas virtuales de Azure, los discos administrados, las instantáneas, el VHD de Azure y las plantillas de ARM

Puede mostrar la información del nombre de la región de una VM de Azure, discos administrados, instantáneas, el VHD de Azure y plantillas de ARM. Esta información se muestra para los recursos de la imagen maestra cuando se asigna un catálogo de máquinas. Una propiedad de PowerShell llamada `RegionName` muestra la información del nombre de la región cuando ejecuta el comando de PowerShell con el parámetro `AdditionalData`.

Por ejemplo, use este comando de PowerShell para obtener información de una VM en Azure.

```
PS C:\Windows\system32> (get-item XDHyp:\HostingUnits\myAzureNetwork\
    image.folder\hu-dev-testing-rg.resourcegroup\hu-dev-tsvda.vm).
    AdditionalData
Key Value
HardDiskSizeGB 127
ResourceGroupName HU-DEV-TESTING-RG
RegionName East US
TemplateIsWindowsTemplate True
LicenseType
ServiceOfferingDescription Standard_B2ms
ServiceOfferingMemory 8192
ServiceOfferingCores 2
SupportedMachineGenerations Gen1,Gen2
ServiceOfferingWithTemporaryDiskSizeInMb 16384
SecurityType
SecureBootEnabled
VTpmEnabled
<!--NeedCopy-->
```

### Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos de la plataforma Azure. Las etiquetas de la tabla se representan como “clave”: “valor”.

| Resource name | Etiqueta |
|---|---|
| Disco de ID | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Imagen | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| NIC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” |

| Resource name | Etiqueta |
| --- | --- |
| | “CitrixResource”: “Internal” |
| Disco de SO | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| VM de preparación | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Instantánea publicada | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Resource group | “CitrixResource”: “Internal” CitrixSchemaVersion: 2.0 |
| Cuenta de almacenamiento | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| VM en catálogo | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |
| Disco WBC | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “CitrixResource”: “Internal” |

> **Nota:**
>
> Una máquina virtual no está visible en el inventario de Citrix si se agrega una etiqueta **CitrixResource** para identificarla como un recurso creado por MCS. Puede quitar la etiqueta o cambiarle el nombre para que sea visible.

## Quitar etiquetas

Al crear un catálogo o una máquina virtual, se crean etiquetas en estos recursos:

- Resource group
- Máquina virtual

- Disco de SO
- Disco de identidad
- Interfaz de red
- Cuenta de almacenamiento

Puede quitar máquinas virtuales y catálogos de máquinas de la base de datos de Citrix y quitar etiquetas. Puede usar:

- `Remove-ProvVM` con el parámetro `ForgetVM` para quitar máquinas virtuales y etiquetas de una sola máquina virtual o una lista de máquinas virtuales de un catálogo de máquinas.
- `Remove-ProvScheme` con el parámetro `ForgetVM` para quitar un catálogo de máquinas de la base de datos de Citrix y etiquetas de todo un catálogo de máquinas.

Esta función solo se puede aplicar a máquinas virtuales persistentes.

Para hacerlo:

1. Abra una ventana de **PowerShell**.
2. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
3. Ejecute `Remove-ProvVM` para eliminar máquinas virtuales de la base de datos de Citrix y etiquetas de máquinas virtuales.
   Por ejemplo:

```
Remove-ProvVM -ProvisioningSchemeName “ProvisioningSchemeName” -VMName “vmname” -ForgetVM
<!--NeedCopy-->
```

4. Ejecute `Remove-ProvScheme` para eliminar el catálogo de máquinas de la base de datos de Citrix y etiquetas de catálogos de máquinas. Por ejemplo:

```
Remove-ProvScheme -ProvisioningSchemeName “ProvisioningSchemeName” -ForgetVM
<!--NeedCopy-->
```

> **Nota:**
>
> Después de usar el parámetro `ForgetVM` en `Remove-ProvScheme`, MCS elimina todas las instantáneas, incluida la instantánea del disco base, si el esquema de aprovisionamiento está presente en su propio grupo de recursos (BYORG) o en el grupo de recursos administrado por Citrix.

## Más información

- Crear y administrar conexiones y recursos
- Conexión con Microsoft Azure

- Crear catálogos de máquinas
- Crear un catálogo de Microsoft Azure
- Administrar catálogos de máquinas

# Administrar un catálogo de Microsoft System Center Virtual Machine Manager

January 24, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de Microsoft System Center Virtual Machine Manager (VMM).

> **Nota:**
>
> Antes de administrar un catálogo de VMM, debe terminar de crear un catálogo de VMM. Consulte Crear un catálogo de Microsoft System Center Virtual Machine Manager.

## Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos de la plataforma SCVMM. Las etiquetas de la tabla se representan como "clave": "valor".

| Resource name | Etiqueta |
| --- | --- |
| máquina virtual de preparación | Cadena de etiqueta: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" Entrada de propiedad personalizada: "XdConfig:"XdProvisioned=True" |
| VM en catálogo | Cadena de etiqueta: "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" Entrada de propiedad personalizada: "XdConfig:"XdProvisioned=True" |

## Más información

- Crear y administrar conexiones y recursos

- Conexión con Microsoft System Center Virtual Machine Manager
- Crear catálogos de máquinas
- Crear un catálogo de Microsoft System Center Virtual Machine Manager
- Administrar catálogos de máquinas

## Administrar un catálogo de VMware

June 12, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de VMware.

> **Nota:**
>
> Antes de administrar un catálogo de VMware, debe terminar de crear un catálogo de VMware. Consulte Crear un catálogo de VMware.

### Actualizar el ID de carpeta de un catálogo de máquinas

Para actualizar el ID de carpeta de un catálogo de máquinas de MCS, especifique `FolderId` en las propiedades personalizadas del comando `Set-ProvScheme`. Las máquinas virtuales creadas después de actualizar el ID de carpeta se crean bajo este nuevo ID de carpeta. Si esta propiedad no se especifica en `CustomProperties`, las máquinas virtuales se crean en la carpeta en la que se encuentra la imagen maestra.

Siga estos pasos para actualizar el ID de carpeta de un catálogo de máquinas.

1. Abra un explorador web e introduzca la URL de **vSphere Web Client**.
2. Introduzca las credenciales y haga clic en **Login**.
3. Cree una carpeta de ubicación de máquinas virtuales en **vSphere Web Client**.
4. Abra una ventana de PowerShell.
5. Ejecute **asnp citrix*** para cargar los módulos de PowerShell específicos de Citrix.
6. Especifique `FolderID` en el campo `CustomProperties` de `Set-ProvScheme`. En este ejemplo, el valor del ID de la carpeta es`group-v2406`.

```
1 Set-ProvScheme -ProvisioningSchemeUid "50bb319c-2e83-4a37-9ea1-94
    f630687372" -CustomProperties "<CustomProperties xmlns=""http
    ://schemas.citrix.com/2014/xd/machinecreation"" xmlns:xsi=""
    http://www.w3.org/2001/XMLSchema-instance""><Property xsi:type=
```

```
    ""StringProperty"" Name=""FolderId"" Value=""group-v2406"" /></
    CustomProperties>"
<!--NeedCopy-->
```

7. Agregue una VM al catálogo de máquinas mediante Studio.
8. Compruebe la nueva VM en vSphere Web Client. La nueva máquina virtual se crea en la nueva carpeta.

#### Buscar el ID de carpeta mediante los comandos de PowerShell

Use el comando `Get-HypConfigurationDataForItem` de Powershell para buscar el ID de una carpeta existente en el Hypervisor de VMware.

Cree una conexión de alojamiento y un grupo de recursos para un Hypervisor de VMware. A continuación, siga estos pasos para buscar el ID de una carpeta en ese Hypervisor.

1. Determine la ruta de `XDHyp` a la raíz del árbol de carpetas de la VM. Por ejemplo:

```
XDHyp:\Connections\VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

2. Use `Get-HypConfigurationDataForItem` para obtener la estructura del árbol. Por ejemplo:

```
Get-HypConfigurationDataForItem -LiteralPath XDHyp:\Connections\
    VMwareConn\Datacenter.datacenter
<!--NeedCopy-->
```

3. Ejecute el siguiente comando para identificar el ID de carpeta en el XML de salida. En este ejemplo, busque el ID de carpeta de `ExampleFolder`en la salida XML.

```
$result = Get-HypConfigurationDataForItem -LiteralPath XDHyp:\
    Connections\VMwareConn\Datacenter.datacenter
$result.VmPlacementFolder
<!--NeedCopy-->
```

**Salida XML:**

```
<?xml version="1.0" encoding="utf-16"?>
<CtxVmPlacementFolder xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Name>vm</Name>
<Id>group-v4</Id>
<SubFolder>
<CtxVmPlacementFolder>
  <Name>vCLS</Name>
  <Id>group-v75</Id>
  <SubFolder />
</CtxVmPlacementFolder>
```

```
<CtxVmPlacementFolder>
  <Name>MyOtherFolder</Name>
  <Id>group-v1110</Id>
  <SubFolder />
</CtxVmPlacementFolder>
<CtxVmPlacementFolder>
  <Name>ExampleFolder</Name>
  <Id>group-v4658</Id>
  <SubFolder />
</CtxVmPlacementFolder>
</SubFolder>
</CtxVmPlacementFolder>
<!--NeedCopy-->
```

#### Buscar el ID de carpeta en vSphere

Acceda al MOB en cualquier sistema ESXi o vCenter Server para buscar el ID de carpeta de las máquinas virtuales.

El explorador de objetos administrados (MOB) es una aplicación de servidor basada en web que está integrada en todos los sistemas ESX/ESXi y vCenter Server. Esta utilidad vSphere le permite ver información detallada sobre objetos como máquinas virtuales, almacenes de datos y grupos de recursos.

1. Abra un explorador web e introduzca `http://x.x.x.x/mob`, donde x.x.x.x es la dirección IP del host de vCenter Server o ESX/ESXi. Por ejemplo, https://10.60.4.70/mob.
2. En la página de **inicio** de MOB, haga clic en el valor del **contenido** de la propiedad.
3. Haga clic en el valor de **rootFolder**.
4. Haga clic en el valor de **childEntity**.
5. Haga clic en el valor de **vmFolder**.
6. Puede encontrar el ID de la carpeta en el valor de **childEntity**.

### Migración del almacenamiento de máquinas virtuales

Puede mover el almacenamiento en disco de las máquinas virtuales existentes de un almacenamiento antiguo a uno nuevo. Durante la migración, MCS conserva las capacidades de la máquina virtual, como la administración de energía, el restablecimiento del disco del sistema operativo, etc. También puede agregar nuevas máquinas virtuales al catálogo de máquinas mediante el nuevo almacenamiento en disco. Para hacer esto, use el comando de PowerShell `Move-ProvVMDisk`.

Actualmente, solo puede migrar máquinas virtuales persistentes de clonación completa.

El nuevo almacenamiento debe cumplir las siguientes condiciones:

- Debe estar dentro del mismo clúster del antiguo almacenamiento.

- El host en el que se ejecuta la máquina virtual debe tener acceso a los almacenes de datos antiguos y nuevos.

Puede realizar las siguientes tareas:

- Migre el almacenamiento en disco
- Retirar el almacenamiento anterior

#### Migre el almacenamiento en disco

Para migrar el almacenamiento en disco:

1. Agregue un nuevo almacenamiento a una unidad de alojamiento existente. Cambie el antiguo almacenamiento a **Reemplazado**. Puede usar la interfaz de Configuración completa o los comandos de PowerShell.
   - Si usa la interfaz de configuración completa, consulte Modificar almacenamiento.
   - Si usa los comandos de PowerShell:
     - Ejecute `Add-Hyphostingunitstorage` para agregar el nuevo almacenamiento a la unidad de alojamiento existente.
     - Ejecute `Set-Hyphostingunitstorage` con **Reemplazado** como true para inhabilitar la creación de nuevas máquinas virtuales en el antiguo almacenamiento.
2. Apague las máquinas virtuales y active el **modo de mantenimiento**.
3. Mueva el almacenamiento en disco de las máquinas virtuales al nuevo almacenamiento y actualice la información de almacenamiento. Por ejemplo:

```
Move-ProvVMDisk -ProvisioningSchemeName "myFullCloneProvScheme" -
    VMName ("VMware-TestVM01", "VMware-TestVM02") -DiskType OS,
    Identity -DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

4. Obtenga el identificador de la tarea de la migración. Por ejemplo:

```
,(Get-ProvVM -ProvisioningSchemeName xxxxx) | Move-ProvVMDisk -
    ProvisioningSchemeName xxxxx -DiskType OS,Identity -
    DestinationStorageId datastore1,datastore1
<!--NeedCopy-->
```

5. Compruebe el estado de la migración.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMovedVirtualMachines`: Proporciona la lista de máquinas virtuales que migraron correctamente los discos, incluidas las máquinas virtuales que ya migraron al nuevo almacenamiento.
   - `(Get-ProvTask -TaskID xxxxxxxxx).DiskMoveFailedVirtualMachines` : proporciona la lista de máquinas virtuales con una migración fallida.

- `(Get-ProvTask -TaskID xxxxxxxxx).NotStartedVirtualMachines`: proporciona la lista de máquinas virtuales cuya migración aún no comenzó.
- `Get-ProvVM -ProvisioningSchemeName xxxxx -VMName "VMware-TestVM01`: proporciona las propiedades de las máquinas virtuales actualizadas después de la migración. Compruebe las propiedades como `StorageId`, `AssignedImage`, `BootedImage`, `IdentityDiskId`, `IdentityDiskStorage` y `LastBootTime`.

Después de migrar los discos de las máquinas virtuales creadas por MCS con instantáneas, es posible que aparezca la advertencia **Se requiere consolidación en VSphere Client**. Para consolidar y evitar la pérdida de datos:

1. Realice una copia de seguridad de VMware VM. Por ejemplo, transfiera todos los archivos de máquina virtual a otra carpeta de un almacén de datos.
2. Cuando aparezca la advertencia, haga clic en **Consolidar** y, a continuación, en **Aceptar** para confirmar la consolidación.

#### Retirar el almacenamiento anterior

Para dejar de usar el antiguo almacenamiento después de la migración de discos de las máquinas virtuales:

1. Obtenga la información sobre los discos base y el número de máquinas en cada almacenamiento en disco de la unidad de alojamiento. Por ejemplo:

   ```
   $result=Get-ProvSchemeResourceInStorage -ProvisioningSchemeName
       xxxxx
   $result
   $result.ProvResourceInStorage | Format-List -Property *
   <!--NeedCopy-->
   ```

   Tras una correcta migración, MCS elimina automáticamente el disco base obsoleto y no hay máquinas en el antiguo almacenamiento. Por lo tanto, después de ejecutar el comando, asegúrese de que no haya máquinas ni discos base en el antiguo almacenamiento.

2. Ejecute `Remove-Hyphostingunitstorage` para eliminar por completo el antiguo almacenamiento de la unidad de alojamiento. También puede usar la interfaz de Configuración completa para eliminar el almacenamiento anterior.

### Identificar los recursos creados por MCS

A continuación, se muestran las etiquetas que MCS agrega a los recursos de la plataforma VMware. Las etiquetas de la tabla se representan como “clave”: “valor”.

| Resource name | Etiqueta |
| --- | --- |
| máquina virtual de preparación | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True” |
| VM en catálogo | “CitrixProvisioningSchemeId”: “xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx” “XdConfig:”XdProvisioned=True” |

### Más información

- Crear y administrar conexiones y recursos
- Conexión con VMware
- Crear catálogos de máquinas
- Crear un catálogo de VMware
- Administrar catálogos de máquinas

## Administrar un catálogo de XenServer

January 24, 2024

Administrar catálogos de máquinas describe los asistentes con los que se administra un catálogo de máquinas. La siguiente información incluye detalles específicos de los entornos de virtualización de XenServer.

> **Nota:**
>
> Antes de administrar un catálogo de XenServer, debe terminar de crear dicho catálogo. Consulte Crear un catálogo de XenServer.

### Identificar los recursos creados por MCS

Cuando Machine Creation Services (MCS) genera recursos, como discos, asigna una etiqueta ID de ProvisioningScheme para un mejor uso de esos recursos.

Las etiquetas son útiles para los administradores, ya que les permiten administrar y organizar mejor los recursos. Por ejemplo, si los recursos, como los discos sin utilizar, están etiquetados, los administradores pueden identificar fácilmente dónde se creó el recurso, lo que hace eficiente el proceso de limpieza.

A continuación, se muestran las etiquetas que MCS agrega a los recursos de la plataforma XenServer. Las etiquetas de la tabla se representan como "clave": "valor".

| Resource name | Etiqueta |
| --- | --- |
| Copia del disco en cada red o almacenamiento local (solo en las instalaciones locales) | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco de ID | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco de SO | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| máquina virtual de preparación | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| VM en catálogo | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |
| Disco WBC | "CitrixProvisioningSchemeId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx" |

### Obtener información sobre un esquema de aprovisionamiento

Para obtener información detallada sobre el esquema de aprovisionamiento, puede ejecutar los siguientes comandos de PowerShell. Sustituya `xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx` por el ID real del esquema de aprovisionamiento:

1. Sustituya el ID del marcador de posición por el ID real del esquema de aprovisionamiento

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Obtenga información detallada sobre el esquema de aprovisionamiento:

```
Get-ProvisioningScheme -Id $provisioningSchemeId
<!--NeedCopy-->
```

### Obtener una lista de recursos creados por MCS

Ejecute los siguientes comandos para obtener una lista completa de los recursos creados por MCS.

1. Sustituya el ID del marcador de posición por el ID real del esquema de aprovisionamiento.

```
$provisioningSchemeId = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
<!--NeedCopy-->
```

2. Obtenga la lista completa de recursos creados por MCS.

```
Get-ProvResource -ProvisioningSchemeUid $provisioningSchemeId |
    ConvertTo-JSON -Depth 6
<!--NeedCopy-->
```

Tras la ejecución, se obtiene el siguiente resultado:

- El nombre y el ID del esquema de aprovisionamiento.
- Una lista de versiones de imágenes de aprovisionamiento incluidas en el esquema de aprovisionamiento. Cada entrada incluye:
  - El nombre y el ID de la imagen.
  - El ID de disco y el ID de almacenamiento del disco.
- Una lista de VM de aprovisionamiento. Cada entrada incluye:
  - El ID del disco de SO y el ID del disco principal del disco de SO.
  - El ID de almacenamiento del disco de SO.
  - El disco de identidad y su ID de almacenamiento.

### Más información

- Crear y administrar conexiones y recursos
- Conexión con XenServer
- Crear catálogos de máquinas
- Crear un catálogo de XenServer
- Administrar catálogos de máquinas

## Administración de energía

December 5, 2023

Con Citrix DaaS, puede administrar la energía de las VM aprovisionadas por MCS en varios hipervisores y servicios de nube compatibles. La operación de administración de energía le proporciona:

- Una experiencia de usuario óptima
- Administración de costes y ahorro de energía

Las acciones de energía disponibles son:

- Iniciar
- Apagar
- Reiniciar
- Suspender

- Reanudar
- Forzar reinicio
- Forzar apagado

> **Nota:**
>
> - En el caso de una VM no persistente, el ciclo de energía (apagado/inicio y reinicio) hace que se restablezca el disco del sistema operativo.
> - Las capacidades y los comportamientos de la acción de energía varían según los hipervisores o los servicios de nube.

En este artículo se describen las principales funciones de administración de energía asociadas a determinados hipervisores compatibles.

- Administrar la energía de las VM de AWS
- Administrar la energía de las VM de Azure

## Administrar la energía de las VM de AWS

May 17, 2024

Para obtener información sobre los permisos necesarios, consulte Acerca de los permisos de AWS.

### Hibernación de instancias

El proceso de hibernación almacena el estado en memoria de la instancia, junto con sus direcciones IP privadas y elásticas, lo que le permite continuar exactamente donde lo dejó.

Cuando se indica a una instancia que hiberne, esta escribe el estado en memoria en un archivo del volumen raíz de EBS y, a continuación, se apaga sola. Un volumen de Amazon EBS es un dispositivo de almacenamiento duradero a nivel de bloques que usted puede conectar a sus instancias. Después de conectar un volumen a una instancia, puede usarlo como si fuera un disco duro físico. Cifre el volumen de EBS raíz de la instancia. El cifrado garantiza la protección adecuada de los datos confidenciales cuando se copian de la memoria al volumen de EBS. Para obtener información sobre el cifrado de EBS, consulte Cifrado de Amazon EBS.

Estas son las limitaciones de la hibernación de instancias admitida:

- Se admite una memoria de instancia (RAM) de solo 150 GB
- No se admite el modo de arranque UEFI
- El SSD de uso general y el SSD de E/S por segundo aprovisionado solo se admiten como tipos de volumen de EBS.

### Crear máquinas virtuales compatibles con la hibernación

Para crear máquinas virtuales compatibles con la hibernación:

1. Cree una conexión de host. Consulte Conexión con AWS.
2. Inicie una instancia con la raíz de EBS cifrada y la propiedad **Stop-Hibernate** habilitada. Para obtener más información, consulte:
   - Ciclo de vida de la instancia
   - Cifrado de Amazon EBS
   - Requisitos previos de la hibernación
   - Habilitar la hibernación de una instancia
   - Hibernación de una instancia bajo demanda o instancia de spot
3. Utilice esta instancia como imagen maestra para crear una AMI.
4. Prepare la imagen maestra:
   a) Instale un VDA en la imagen maestra. Citrix recomienda instalar la última versión para poder disponer de las funciones más recientes. Un error en la instalación del VDA en la imagen maestra provoca un error en la creación de catálogos. Para obtener más información sobre cómo instalar un VDA, consulte Instalar VDA.
   b) Una la imagen maestra al dominio al que pertenecen las aplicaciones y los escritorios. Compruebe que la imagen maestra está disponible en el host donde se crearán las máquinas.
5. Cree una AMI a partir de esa instancia. Para obtener información sobre cómo crear una AMI a partir de una instancia, consulte Crear una AMI a partir de una instancia de Amazon EC2.
6. Cree un catálogo de máquinas mediante el comando `New-ProvScheme`. Defina la propiedad personalizada `AwsCaptureInstanceProperties` en **True**. Para obtener información sobre cómo habilitar propiedades de las instancias de AWS en la interfaz de Configuración completa, consulte Aplicar propiedades de instancias de AWS y etiquetar recursos operativos en la interfaz de Configuración completa.

```
New-ProvScheme  -AdminAddress "xxx" -CleanOnBoot
-CustomProperties "AwsCaptureInstanceProperties,true;"
-HostingUnitName "xxx" -IdentityPoolName $catalog_name -
   InitialBatchSizeHint 1
-MasterImageVM "xyz.template" -NetworkMapping @{
 "0"="XDHyp:\HostingUnits\MyConn\us-east-2a.availabilityzone
    \10.0.0.0``/24 (vpc-0f1771e45671aedcd).network" }

-ProvisioningSchemeName $catalog_name
-RunAsynchronously -Scope @() -SecurityGroup @("xxx") -
   ServiceOffering "xxx"
<!--NeedCopy-->
```

Para obtener información sobre la creación de catálogos de máquinas mediante los comandos de PowerShell, consulte https://developer-docs.citrix.com/projects/citrix-daas-sdk/en/latest/.

Las máquinas virtuales que se pueden hibernar se crean si:

- Selecciona una AMI creada a partir de una imagen maestra que tenga habilitada la propiedad **Stop-Hibernate**.
- La máquina virtual principal está unida a un dominio y tiene el VDA instalado.
- Selecciona el tamaño de máquina virtual correcto (oferta de servicios) que pueda gestionar la hibernación.

El comando **New-ProvScheme** falla y muestra el mensaje de error correspondiente si:

- La máquina virtual principal está habilitada para la hibernación, pero la oferta de servicios no puede gestionar la hibernación.
- Si la máquina virtual principal no está unida a un dominio y no tiene ningún VDA instalado.

#### Estado de hibernación de las ofertas de servicios y AMI

Para obtener el estado de hibernación de las ofertas de servicios y las AMI (plantillas), ejecute estos comandos:

- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\WIN2016-ADDC-2021.09.10.145334-a1968709-10c4-47d5-9642-21e743159a7b(ami-0e6c5b33a52d2a6b6).template'`
- `Get-HypConfigurationObjectForItem 'XDHyp:\HostingUnits\MyConn\R6i Sixteen Extra Large Instance.serviceoffering'`

#### Actualizar la oferta de servicios de un esquema de aprovisionamiento compatible con la hibernación existente

1. Ejecute el comando `Set-ProvScheme`. Por ejemplo,

```
Set-ProvScheme -ProvisioningSchemeName <String> -ServiceOffering <String>
<!--NeedCopy-->
```

El sistema muestra un mensaje de excepción si la oferta de servicios no es compatible.

#### Cree un catálogo de máquinas compatible con hibernación

Al crear catálogos de máquinas, puede utilizar un perfil de máquina que admita la hibernación.

1. En el asistente para la creación de catálogos, siga las instrucciones hasta seleccionar el perfil de la máquina.
2. En la página **Plantilla de máquina**, haga clic en **Seleccione un perfil de máquina** y seleccione un perfil de máquina.
3. En la página **Máquina virtual**, haga clic en el icono **Modificar** y seleccione una máquina virtual.

   > **Nota:**
   >
   > Si el perfil de la máquina está habilitado para hibernación, el sistema muestra solo las VM que se pueden hibernar.

4. Siga las instrucciones que aparecen en pantalla para completar todos los parámetros. La página **Resumen** muestra el estado de hibernación del catálogo.

   > **Nota:**
   >
   > En Modificar el catálogo de máquinas, al cambiar el perfil de máquina a uno con hibernación habilitada, se le pide que reconfigure las VM en consecuencia.

#### Actualizar el catálogo de máquinas que admite la hibernación

Si intenta actualizar un catálogo de máquinas existente con un catálogo de máquinas que no admite la hibernación, la actualización fallará y aparecerá el mensaje de error correspondiente.

#### Administración de energía de máquinas virtuales en hibernación

Puede realizar estas operaciones de administración de energía en las máquinas virtuales hibernadas:

1. Suspender la VM desde el estado de ejecución.
2. Reanudar la máquina virtual desde el estado suspendido.
3. Reiniciar la máquina virtual desde el estado suspendido.

Para ver las opciones de administración de energía, en la interfaz **Administrar > Configuración completa**, haga clic con el botón secundario en las máquinas virtuales en hibernación.

También puede ver el estado de energía como **Suspendiendo** y **Suspendido** para cada máquina virtual según las operaciones de energía que realice en las máquinas virtuales.

## Administrar la energía de las VM de Azure

June 12, 2024

Para obtener información sobre los permisos necesarios, consulte Permisos de Azure requeridos.

### Aprovisionamiento a demanda de Azure

Con el aprovisionamiento a demanda de Azure, las máquinas virtuales se crean solo cuando Citrix DaaS inicia una acción de encendido, después de completarse el aprovisionamiento.

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

- Reduce los costes de almacenamiento
- Proporciona una creación de catálogos más rápida

Al crear un catálogo con MCS, Azure Portal muestra los grupos de seguridad de red, las interfaces de red, las imágenes base y los discos de identidad de los grupos de recursos.

Azure Portal no muestra ninguna máquina virtual hasta que Citrix DaaS inicie una acción de encendido en ella. A continuación, el estado de la máquina virtual en la interfaz de Configuración completa pasa a **Activado**. Existen dos tipos de máquinas con estas diferencias:

- Para una máquina agrupada, el disco del sistema operativo y la caché de reescritura solo existen cuando existe la máquina virtual. Al apagar una máquina agrupada en la consola, la VM no se ve en Azure Portal. Si apaga máquinas de forma rutinaria (por ejemplo, fuera del horario laboral), hay un ahorro significativo en los costes de almacenamiento.
- Para una máquina dedicada, el disco del sistema operativo se crea la primera vez que se encienda la máquina virtual. La VM de Azure Portal permanece almacenada hasta que se elimina la identidad de la máquina. Al apagar una máquina dedicada en la consola, la VM sigue viéndose en Azure Portal.

> **Nota:**
>
> La compatibilidad con los catálogos de Azure creados antes de existir la función de aprovisionamiento bajo demanda (catálogos "antiguos") ha quedado obsoleta. Por lo tanto, cree de nuevo las máquinas virtuales del catálogo antiguo de Azure. Después, los catálogos se aprovisionan bajo demanda, lo que ahorra costes de almacenamiento.

### Conservación de una máquina virtual aprovisionada durante los ciclos de apagado y encendido

Elija si quiere conservar una máquina virtual aprovisionada al apagar y encender. Utilice el parámetro `New-ProvScheme CustomProperties` de PowerShell. Este parámetro admite una propiedad adicional, `PersistVm`, que sirve para determinar si una máquina virtual aprovisionada persiste durante los ciclos de energía. Establezca la propiedad `PersistVm` en **true** para conservar una máquina

virtual cuando se apague, o bien establezca la propiedad en **false** para asegurarse de que la máquina virtual no se conserve al apagarse.

> **Nota:**
>
> La propiedad `PersistVm` solo se aplica a los esquemas de aprovisionamiento con las propiedades `CleanOnBoot` y `UseWriteBackCache` habilitadas. Si no se especifica la propiedad `PersistVm` para máquinas virtuales no persistentes, se eliminan del entorno de Azure al apagarse.

En el ejemplo siguiente, el parámetro `New-ProvScheme CustomProperties` establece la propiedad `PersistVm` en **true**:

```
<CustomProperties xmlns="http://schemas.citrix.com/2014/xd/
   machinecreation" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
   instance">
<Property xsi:type="StringProperty" Name="UseManagedDisks" Value="true"
    />
<Property xsi:type="StringProperty" Name="StorageType" Value="
   Standard_LRS" />
<Property xsi:type="StringProperty" Name="PersistWBC" Value="false" />
<Property xsi:type="StringProperty" Name="PersistOsDisk" Value="true"
   />
<Property xsi:type="StringProperty" Name="PersistVm" Value="true" />
<Property xsi:type="StringProperty" Name="ResourceGroups" Value="demo-
   resourcegroup" />
<Property xsi:type="StringProperty" Name="LicenseType" Value="
   Windows_Client" />
</CustomProperties>
<!--NeedCopy-->
```

En el siguiente ejemplo, el parámetro `New-ProvScheme CustomProperties` conserva la caché de reescritura estableciendo `PersistVM` en **true**:

```
New-ProvScheme
-AzureAdJoinType "None"
-CleanOnBoot
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix.com
   /2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/
   XMLSchema-instance`"><Property xsi:type=`"StringProperty`" Name=`"
   UseManagedDisks`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"StorageType`" Value=`"Standard_LRS`" /><
   Property xsi:type=`"StringProperty`" Name=`"PersistWBC`" Value=`"
   false`" /><Property xsi:type=`"StringProperty`" Name=`"
   PersistOsDisk`" Value=`"true`" /><Property xsi:type=`"
   StringProperty`" Name=`"PersistVm`" Value=`"true`" /><Property xsi:
   type=`"StringProperty`" Name=`"ResourceGroups`" Value=`"demo-
   resourcegroup`" /><Property xsi:type=`"StringProperty`" Name=`"
   LicenseType`" Value=`"Windows_Client`" /></CustomProperties>"
-HostingUnitName "demo"
-IdentityPoolName "NonPersistent-MCSIO-PersistVM"
```

```
 -MasterImageVM "XDHyp:\HostingUnits\demo\image.folder\scale-test.
    resourcegroup\demo-snapshot.snapshot"
 -NetworkMapping @ {
 "0"="XDHyp:\HostingUnits\demo\virtualprivatecloud.folder\East US.
    region\virtualprivatecloud.folder\ji-test.resourcegroup\jitest-vnet
    .virtualprivatecloud\default.network" }

-ProvisioningSchemeName "NonPersistent-MCSIO-PersistVM"
 -ServiceOffering "XDHyp:\HostingUnits\demo\serviceoffering.folder\
    Standard_B2ms.serviceoffering" -UseWriteBackCache
 -WriteBackCacheDiskSize 127
 -WriteBackCacheMemorySize 256
 <!--NeedCopy-->
```

> **Sugerencia:**
>
> La propiedad `PersistVm` determina si se debe conservar una máquina virtual aprovisionada. La propiedad `PersistOsdisk` determina si se debe conservar el disco del sistema operativo. Para conservar una máquina virtual aprovisionada, conserve primero el disco del sistema operativo. No se puede eliminar el disco del sistema operativo sin eliminar antes la máquina virtual. Puede utilizar la propiedad `PersistOsdisk` sin especificar el parámetro `PersistVm`.

### Personalizar el comportamiento de encendido en caso de error en el cambio del tipo de almacenamiento

Al encenderse, el tipo de almacenamiento de un disco administrado puede no cambiar al tipo deseado debido a un error de Azure. En estos casos, la máquina virtual permanecería apagada y se le enviaría un mensaje de error. Sin embargo, puede optar por encender la máquina virtual incluso cuando no se pueda restaurar el almacenamiento al tipo configurado o mantener la máquina virtual apagada.

- Si configura la propiedad personalizada `FailSafeStorageType` como **verdadera** (configuración predeterminada) o no la especifica en los comandos `New-ProvScheme` y `Set-ProvScheme`:
  - Al encenderla, la máquina virtual se enciende con un tipo de almacenamiento incorrecto.
  - Al apagarla, la máquina virtual permanece apagada con un tipo de almacenamiento incorrecto.
- Si configura la propiedad personalizada `FailSafeStorageType` como **falsa** en los comandos `New-ProvScheme` o `Set-ProvScheme`:
  - Al encenderla, la máquina virtual permanece apagada con un tipo de almacenamiento incorrecto.
  - Al apagarla, la máquina virtual permanece apagada con un tipo de almacenamiento incorrecto.

Para crear un catálogo de máquinas que incluya la propiedad personalizada `FailSafeStorageType`:

1. Abra una ventana de PowerShell.
2. Ejecute `asnp citrix*` para cargar los módulos de PowerShell específicos de Citrix.
3. Cree un grupo de identidades si aún no se ha creado.
4. Agregue la propiedad personalizada en `New-ProvScheme`. Por ejemplo:

```
New-ProvScheme -HostingUnitName "Azure-Resources-1" -
    IdentityPoolName "name" -InitialBatchSizeHint 1
-MasterImageVM "XDHyp:\HostingUnits\Azure-Resources-1\image.folder
    \abc.resourcegroup\def.snapshot"
-NetworkMapping @{
 "0"="XDHyp:\HostingUnits\Azure-Resources-1\ght.folder\abc.
     resourcegroup\abc-vnet.virtualprivatecloud\default.network" }

-ProvisioningSchemeName "name"
-ServiceOffering "XDHyp:\HostingUnits\Azure-Resources-1\
    serviceoffering.folder\Standard_DS2_v2.serviceoffering"
-CustomProperties "<CustomProperties xmlns=`"http://schemas.citrix
    .com/2014/xd/machinecreation`" xmlns:xsi=`"http://www.w3.org
    /2001/XMLSchema-instance`">
<Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`
    "Premium_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"StorageTypeAtShutdown
    `" Value=`"Standard_LRS`" />
<Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
     Value=`"true`" />
</CustomProperties>"
<!--NeedCopy-->
```

5. Cree el catálogo de máquinas Para obtener información sobre cómo crear un catálogo con el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/creating-a-catalog/.

Para actualizar un catálogo de máquinas e incluir la propiedad personalizada `FailSafeStorageType`. Esta actualización no afecta a las máquinas virtuales existentes.

1. Actualice la propiedad personalizada en el comando `Set-ProvScheme`. Por ejemplo:

```
    Set-ProvScheme -ProvisioningSchemeName <String> -CustomProperties "
    <CustomProperties xmlns=`"http://schemas.citrix.com/2014/xd/
        machinecreation`" xmlns:xsi=`"http://www.w3.org/2001/XMLSchema-
        instance`">
    <Property xsi:type=`"StringProperty`" Name=`"StorageType`" Value=`"
        Premium_LRS`" />
    <Property xsi:type=`"StringProperty`" Name=`"IdentityDiskStorageType
        `" Value=`"Premium_LRS`" />
    <Property xsi:type=`"StringProperty`" Name=`"FailSafeStorageType`"
        Value=`"false`" />
```

```
6     </CustomProperties>"
7     <!--NeedCopy-->
```

Para aplicar el cambio realizado en Set-ProvScheme a las máquinas virtuales existentes, ejecute el comando `Request-ProvVMUpdate`.

1. Ejecute el comando Request-ProvVMUpdate. Por ejemplo:

```
1 Request-ProvVMUpdate -ProvisioningSchemeName <String> -VMName <
     List-Of-Vm-Names>
2 <!--NeedCopy-->
```

2. Reinicie las máquinas virtuales.

## Crear máquinas virtuales con capacidad de hibernación

En entornos de Azure, puede crear un catálogo de máquinas de MCS que admita la hibernación. Con esta función, puede suspender una máquina virtual y, a continuación, conectarse de nuevo al estado anterior de la misma cuando un usuario vuelva a iniciar sesión.

La capacidad de hibernación se aplica a lo siguiente:

- SO de sesión única
- Máquinas virtuales persistentes y no persistentes
- Escritorios VDI estáticos y aleatorios (agrupados)

Puede reanudar la misma sesión después de hibernar una máquina virtual, independientemente de si el escritorio VDI es estático o aleatorio.

En esta sección, consulte lo siguiente:

- Requisitos previos
- Limitaciones
- Crear y administrar un catálogo de máquinas con capacidad de hibernación
- Crear un catálogo de máquinas para VM con capacidad de hibernación existentes
- Habilitar la hibernación en VM aprovisionadas por MCS existentes
- Comprobar la propiedad de hibernación
- Administración de energía de VM (manual y automatizada)

### Requisitos previos para usar la hibernación

Para usar la hibernación, complete las siguientes tareas:

- Instale Azure VM Agent en la imagen maestra para Windows y Linux. El archivo de paginación de la imagen de Windows puede estar en el disco temporal. MCS establece la ubicación del

archivo de paginación en la unidad C: del disco base cuando la hibernación está habilitada en el catálogo de máquinas.

- MCS establece automáticamente la propiedad de hibernación para los recursos generados. No es necesario configurar propiedades de los recursos maestros para admitir la hibernación.
- Use un tamaño de máquina virtual en su suscripción compatible con la hibernación.
- Cree un perfil de máquina con capacidad de hibernación (VM o especificación de plantilla) para que las máquinas virtuales hereden la capacidad de hibernación. Para crear la máquina virtual, consulte Getting started with hibernation.

> **Nota:**
>
> Según Microsoft, puede implementar máquinas virtuales con hibernación habilitada desde un disco de sistema operativo. Actualmente, esta función se admite en determinadas regiones y pronto estará disponible en todas ellas. Para obtener más información, consulte Implementar máquinas virtuales con hibernación habilitada desde un disco de sistema operativo.

Para crear la especificación de plantilla, haga lo siguiente:

1. Abra Azure Portal. Elija una máquina virtual cuya configuración quiera usar en la plantilla. Seleccione **Export template** en el panel izquierdo.
2. Desactive la casilla de verificación **Include parameters**. Copie el contexto y guárdelo como archivo JSON, por ejemplo, `VMExportTemplate.json`.
3. Asegúrese de que el parámetro `hibernationEnabled` tiene el valor **`true`** en la plantilla. Si el valor del parámetro no es **`true`**, compruebe la configuración de máquina virtual que utilizó. Puede especificar un tamaño de máquina virtual compatible en el archivo de plantilla. Sin embargo, también puede especificar el tamaño de la máquina al crear el catálogo.
4. Agregue la plantilla del recurso de interfaz de red al archivo JSON `VMExportTemplate.json`. Como resultado, tiene un archivo de plantilla de Azure Resource Manager con dos recursos.
5. Seleccione **Azure Portal > Template specs > Import template > Choose local template file** para importar este archivo de plantilla como una especificación de plantilla de Azure Resource Manager.
6. Una vez creada la especificación de plantilla de Azure Resource Manager, puede usarla como perfil de máquina.

> **Nota:**
>
> La sincronización con Citrix Studio puede tardar unos minutos.

Para obtener más información, consulte el documento de Microsoft Prerequisites to use hibernation.

#### Limitaciones

- Solo se admiten los catálogos de máquinas con sistema operativo de sesión única (persistentes y no persistentes).
- Los discos de SO efímeros y las funciones de E/S de MCS no admiten la hibernación de Azure.
- La hibernación puede fallar durante las actualizaciones automáticas de Windows.

Para obtener más información, consulte el documento de Microsoft.

#### Crear y administrar un catálogo de máquinas con capacidad de hibernación

Para crear máquinas virtuales con capacidad de hibernación, puede crear y administrar un catálogo de máquinas con capacidad de hibernación mediante:

- Interfaz de Configuración completa, o
- Comandos de PowerShell

#### Crear un catálogo mediante la interfaz de Configuración completa

1. Inicie sesión en Citrix Cloud. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
2. En **Administrar > Configuración completa**, seleccione **Catálogos de máquinas** en el panel de la izquierda.
3. Seleccione **Crear catálogo de máquinas**. Se abrirá el asistente para la creación de catálogos.
4. En la página **Tipo de máquina**, seleccione el tipo de máquina con **SO de sesión única** para este catálogo.
5. En la página **Administración de máquinas**, seleccione la configuración de la siguiente manera:
   a) Selecciones **Máquinas con administración de energía (por ejemplo, máquinas virtuales o PC blade)**.
   b) Seleccione **Citrix Machine Creation Services (MCS)**.
6. En la página **Experiencia de escritorio**, seleccione la experiencia de escritorio aleatoria o estática según sea necesario.
7. En la página **Imagen**, seleccione una imagen maestra. Seleccione la casilla **Usar un perfil de máquina** y seleccione un perfil de máquina que admita la hibernación. Haga clic en el texto de ayuda para saber si un perfil de máquina admite la hibernación.

8. En la página **Tipos de licencia y almacenamiento**, seleccione el almacenamiento y la licencia que se usarán en este catálogo.
9. En la página **Máquinas virtuales**, seleccione el número de máquinas virtuales, el tamaño de las máquinas virtuales y la zona de disponibilidad.

   > **Nota:**
   >
   > Solo se muestran los tamaños de máquina que admiten hibernación para que seleccione. La serie GPU VM está en Tech Preview.

10. En la página **NIC**, agregue las tarjetas de interfaz de red que quiere que usen las máquinas virtuales.
11. En la página **Parámetros del disco**, seleccione el tipo de almacenamiento y el tamaño del disco de caché de reescritura.
12. En la página **Grupo de recursos**, seleccione el grupo de recursos para aprovisionar las máquinas virtuales.
13. En la página **Identidades de máquinas**, seleccione **Crear nuevas cuentas de Active Directory**. A continuación, especifique un esquema de nomenclatura de las cuentas.
14. En la página **Credenciales de dominio**, haga clic en **Introducir credenciales**. Introduzca las credenciales de su dominio para la creación de cuentas en el dominio de Active Directory de destino.
15. En la página **Resumen**, introduzca un nombre para el catálogo de máquinas y, a continuación, haga clic en **Finalizar**.

Cuando termine de crear el catálogo de máquinas de MCS, búsquelo en la lista de catálogos y, a continuación, haga clic en la ficha **Propiedades de plantilla**. El valor del parámetro **Hibernación** debe ser **Admitido**.

Si quiere modificar un catálogo de máquinas, tenga en cuenta las siguientes restricciones:

- Si el catálogo de máquinas actual admite la hibernación, no podrá:
  - Cambiar el tamaño de máquina virtual a uno no compatible con hibernación.
  - Cambiar el perfil de máquina a uno no compatible con hibernación.
- Si el catálogo de máquinas actual no admite la hibernación, no podrá:
  - En la actualidad, cambiar el perfil de máquina a uno con capacidad de hibernación mediante la interfaz de Configuración completa. Sin embargo, puede hacerlo mediante los comandos de PowerShell. Consulte Habilitar la hibernación en VM aprovisionadas por MCS existentes.

**Crear un catálogo de máquinas para administrar VM con capacidad de hibernación existentes**
Si ya tiene máquinas virtuales con capacidad de hibernación y quiere suspenderlas y reanudarlas, cree un catálogo de máquinas para importar esas máquinas virtuales para la administración de energía.

> **Nota:**
>
> Puede crear un catálogo de máquinas que contenga máquinas virtuales compatibles y no compatibles con hibernación. Sin embargo, si quiere usar funcionalidad relacionada con la hibernación, debe crear el catálogo de máquinas solo con VM compatibles con la hibernación.

Para crear un catálogo con las VM con capacidad de hibernación existentes mediante la interfaz de Configuración completa, siga las instrucciones que aparecen en pantalla y preste atención a los siguientes parámetros clave:

1. En la página **Administración de máquinas**, seleccione **Máquinas con administración de energía** y, a continuación, seleccione **Otro servicio o tecnología** como forma de implementar las máquinas.
2. En la página **Máquinas virtuales**, agregue o importe solo máquinas virtuales con capacidad de hibernación.

**Crear un catálogo de máquinas mediante comandos de PowerShell** Una vez que cumpla con todos los requisitos para usar la hibernación, puede crear un catálogo de máquinas compatible con hibernación mediante el comando `New-ProvScheme`. Para obtener información sobre cómo crear un catálogo mediante el SDK de PowerShell remoto, consulte Administrar Citrix DaaS mediante Remote PowerShell SDK.

Al crear el catálogo, puede comprobar si un tamaño de máquina virtual y un perfil de máquina admiten la hibernación o no con los siguientes comandos de PowerShell:

- Para el tamaño de VM, ejecute el siguiente comando y compruebe si la propiedad `supportsHibernation` tiene el valor **True**. Por ejemplo,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
    VirtualNetwork> \serviceoffering.folder") | select Name,
    AdditionalData | ConvertTo-Json
<!--NeedCopy-->
```

- Para el perfil de máquina, ejecute el siguiente comando y compruebe si la propiedad `supportsHibernation` tiene el valor **True**. Por ejemplo,

```
Get-ChildItem -LiteralPath @("XDHyp:\HostingUnits\ <
    VirtualNetwork> \machineprofile.folder\abc.resourcegroup")|
    select Name, AdditionalData|ConvertTo-Json
<!--NeedCopy-->
```

Si quiere modificar un catálogo de máquinas, tenga en cuenta las siguientes restricciones:

- Si el catálogo de máquinas actual admite la hibernación, no podrá:
  - Cambiar el tamaño de máquina virtual a uno no compatible con hibernación
  - Cambiar el perfil de máquina a uno no compatible con hibernación
- Si el catálogo de máquinas actual no admite la hibernación, no podrá:
  - En la actualidad, cambiar el perfil de máquina a uno con capacidad de hibernación mediante la interfaz de Configuración completa. Sin embargo, puede hacerlo mediante los comandos de PowerShell. Consulte Habilitar la hibernación en VM aprovisionadas por MCS existentes.

Para obtener información sobre cómo modificar el tamaño de máquina virtual y el perfil de máquina de un catálogo mediante el SDK de PowerShell remoto, consulte https://developer-docs.citrix.com/projects/citrix-virtual-apps-desktops-sdk/en/latest/MachineCreation/Set-ProvScheme/.

#### Habilitar la hibernación en VM aprovisionadas por MCS existentes

Puede habilitar la hibernación de Azure en:

- VM aprovisionadas por MCS con Windows de un catálogo de máquinas creado sin un disco temporal.
- VM aprovisionadas por MCS con Linux de un catálogo de máquinas creado con y sin un disco temporal.

> **Nota:**
>
> - Las máquinas virtuales aprovisionadas por MCS existentes deben tener instalado un agente de VM de Azure.
> - Actualmente, solo puede usar el comando de PowerShell para habilitar esta función.

Para hacerlo:

1. Abra una ventana de **PowerShell**.
2. Ejecute `asnp citrix*` para cargar módulos de PowerShell específicos de Citrix.
3. Compruebe la configuración de las máquinas. Por ejemplo:

```
Get-ProvScheme | select ProvisioningSchemeName,
   ProvisioningSchemeVersion
<!--NeedCopy-->
```

4. Habilite la hibernación en este catálogo de máquinas mediante el comando `Set-ProvScheme`. Por ejemplo:

```
Set-ProvScheme -provisioningSchemeName xxxx
-machineprofile <path-to-machineprofile-with-hibernation-enabled>
-serviceoffering "XDHyp:\HostingUnits\msc-dev\serviceoffering.
   folder\Standard_D4as_v5.serviceoffering"
<!--NeedCopy-->
```

5. Solicite la actualización de las máquinas virtuales existentes de un catálogo de máquinas.

```
Set-ProvVMUpdateTimeWindow -ProvisioningSchemeUid xxxx -VMName <
   String[]
<!--NeedCopy-->
```

6. Reinicie las máquinas virtuales para desencadenar las actualizaciones en las máquinas virtuales existentes. Por ejemplo:

```
New-BrokerHostingPowerAction -machinename "<name>" -Action Restart
<!--NeedCopy-->
```

#### Comprobar la propiedad de hibernación

Puede comprobar la propiedad de hibernación de un catálogo de máquinas, una máquina virtual y una máquina de broker mediante los comandos de PowerShell:

- Para comprobar la propiedad de hibernación de un esquema de aprovisionamiento, ejecute los siguientes comandos de PowerShell. El valor del parámetro `HibernationEnabled` debe ser `True`.

```
(Get-ProvScheme -provisioningSchemeName <YourSchemeName>).
   VMMetadata -join "" |  ConvertFrom-Json | Select
   HibernationEnabled
<!--NeedCopy-->
```

- Para comprobar la propiedad de hibernación de una VM de aprovisionamiento, ejecute los siguientes comandos de PowerShell. El valor del parámetro `SupportsHibernation` debe ser `True`.

```
(Get-ProvVM -VMName <YourVMName>).CustomVmData | ConvertFrom-Json
    | Select SupportsHibernation
<!--NeedCopy-->
```

- Para comprobar la capacidad de hibernación de una máquina de broker, ejecute los siguientes comandos de PowerShell. Las acciones de energía **Suspender** y **Reanudar** indican la capacidad de hibernación.

```
(Get-BrokerMachine -MachineName <YourMachineName>).
   SupportedPowerActions
<!--NeedCopy-->
```

### Administración de energía de VM con capacidad de hibernación

Puede realizar estas operaciones de administración de energía en las máquinas virtuales con capacidad de hibernación:

- **Suspender** la VM desde el estado de ejecución
- **Reanudar** la VM desde el estado suspendido
- **Forzar el apagado** de la VM desde un estado suspendido
- **Forzar el reinicio** de la VM desde el estado suspendido

Consulte los siguientes apartados para obtener más información:

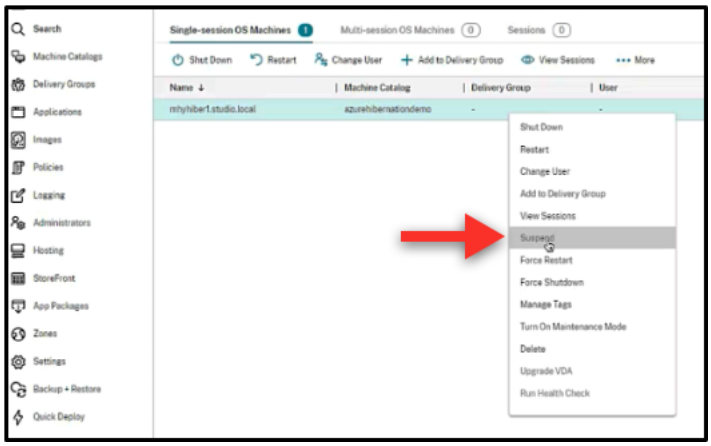
- Suspender
- Reanudar

**Suspender** Puede suspender una máquina virtual de una de las siguientes maneras:

- **Manualmente** desde la interfaz de Configuración completa
- **Automáticamente** mediante la directiva de tiempo de espera: Para obtener más información, consulte Otros parámetros.

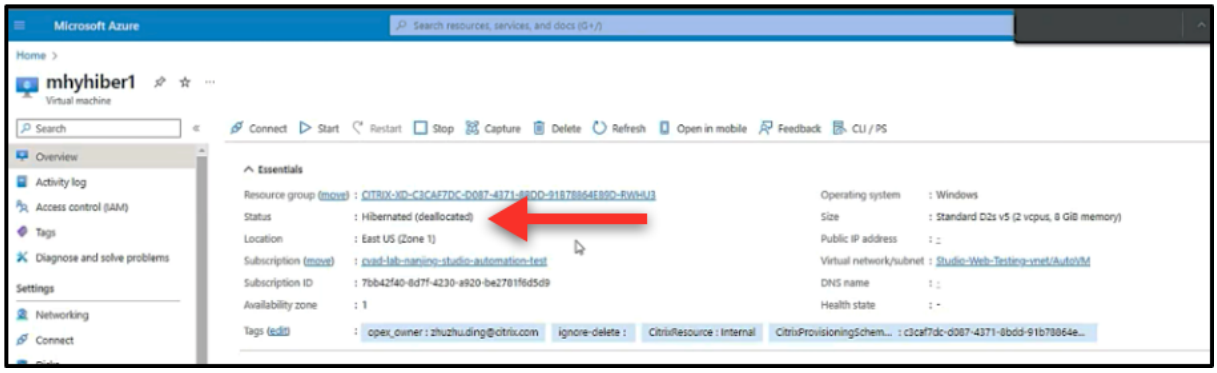
Para suspender manualmente una VM:

1. Haga clic con el botón secundario en la máquina virtual y seleccione **Suspender**. Haga clic en **Sí** para confirmar la acción. El **Estado de energía** cambia de **Suspendiendo** a **Suspendido**.



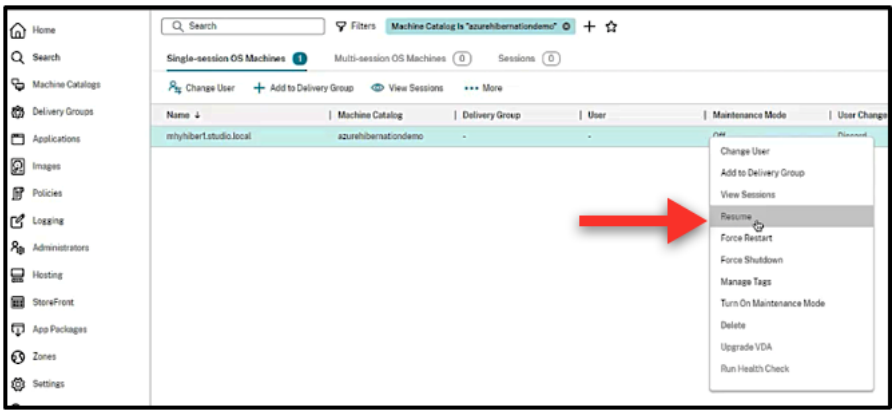

Puede comprobar el estado de la máquina virtual en Azure Portal.

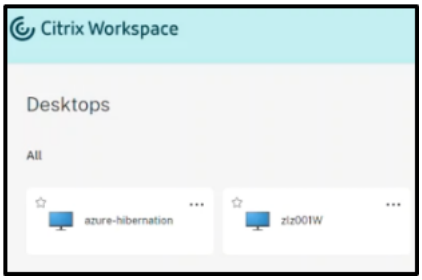



**Reanudar** Puede reanudar una máquina virtual hibernada de una de las siguientes formas:

- **Manualmente**:
  - Los administradores pueden reanudar la VM mediante la interfaz de Configuración completa.




  - Los usuarios finales pueden iniciar la máquina virtual mediante el menú de Citrix Workspace una vez que hacen clic en el icono del escritorio.

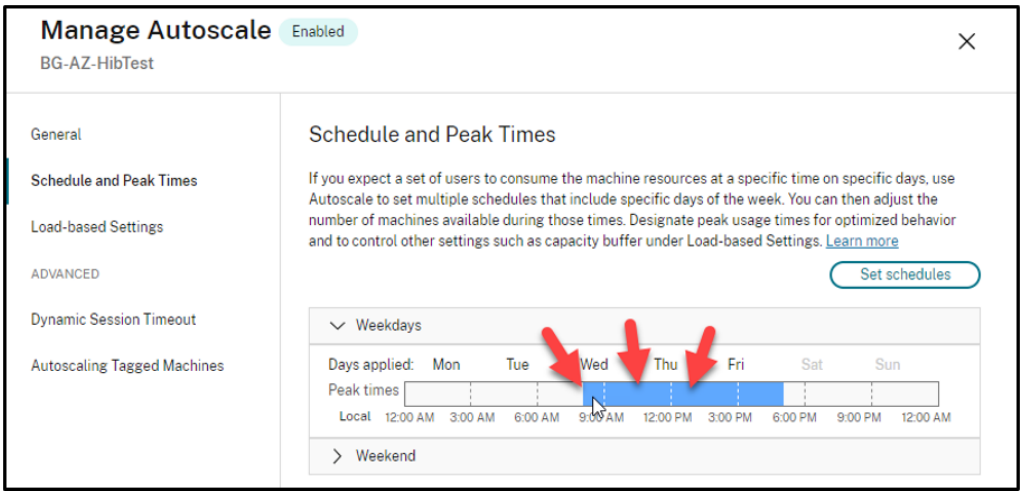



- **Automáticamente**:
  - Autoscale puede encender automáticamente las máquinas hibernadas si configura correctamente las horas punta. Puede establecer las horas punta en intervalos de 30 minutos haciendo clic en el horario. Cada marco azul representa una franja horaria marcada como

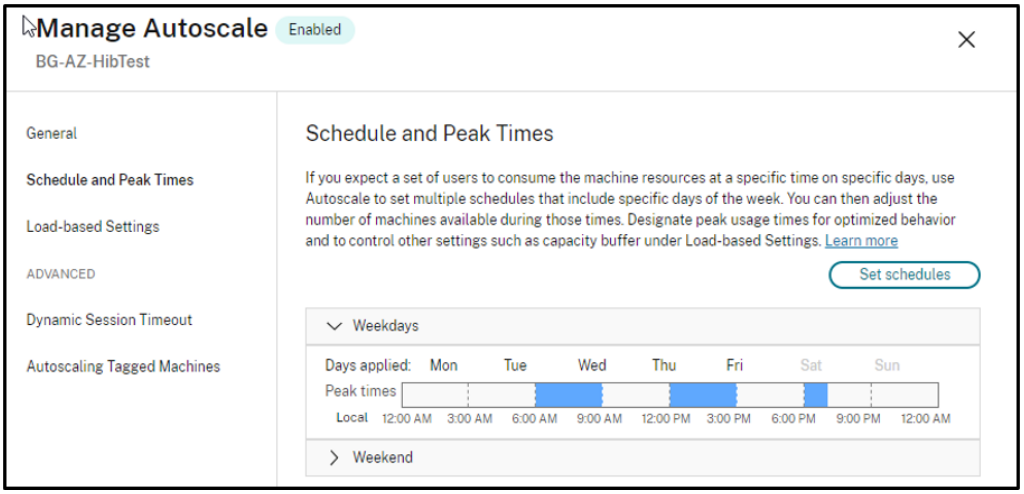
 

hora punta. Las horas punta pueden tener franjas horarias consecutivas y no consecutivas.

* Franjas horarias consecutivas

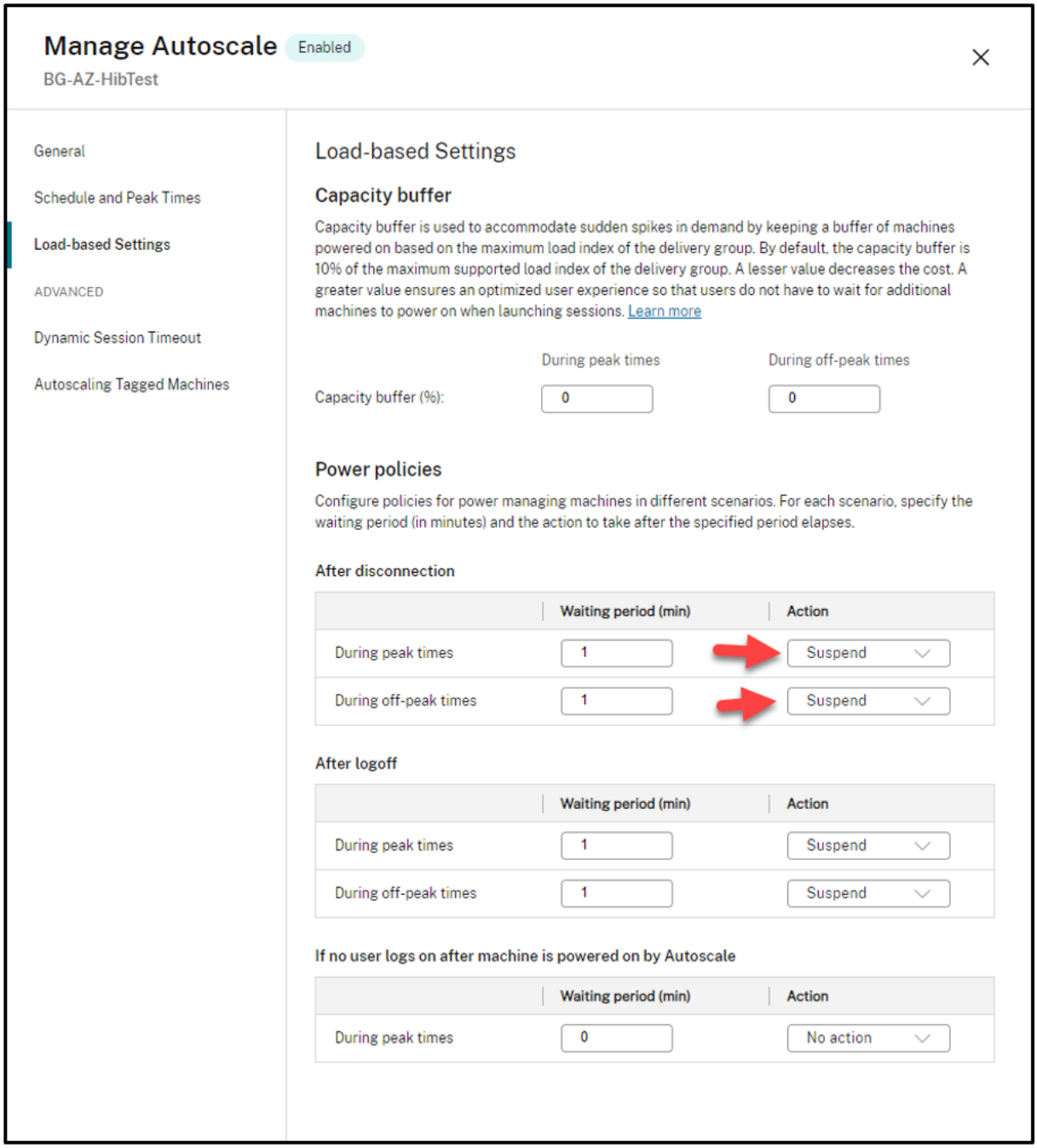



* Franjas horarias no consecutivas




> **Nota:**
>
> En **Administrar Autoscale > Parámetros por carga**, si la **Acción** está configurada como **Suspender**, asegúrese de que todas las VM de ese grupo de entrega tengan capacidad de hibernación. De lo contrario, las máquinas virtuales que no se pueden hibernar seguirán funcionando.




## Más información

Para obtener más información sobre la hibernación de Citrix Azure, consulte el artículo de Citrix Tech Zone.

# Directivas de seguridad

April 12, 2023

En este artículo se describen las funciones de seguridad de varios hipervisores compatibles. Las funciones de seguridad incluyen:

- Grupo de seguridad
- Arranque seguro
- Prestaciones de cifrado

# Grupo de seguridad

April 12, 2023

Un grupo de seguridad es un grupo de reglas de seguridad para filtrar el tráfico de red entre los recursos de una red virtual. Las reglas de seguridad permiten o deniegan el tráfico de red entrante o saliente hacia o desde varios tipos de recursos. Cada regla especifica las siguientes propiedades:

- Nombre: Un nombre único dentro del grupo de seguridad de red
- Prioridad: Las reglas se procesan por orden de prioridad, procesándose los números más bajos antes que los más altos, ya que los números más bajos tienen una prioridad más alta
- Origen o destino: Cualquier dirección IP individual, bloque de enrutamiento entre dominios sin clases (CIDR - por ejemplo, 10.0.0.0/24), etiqueta de servicio o grupo de seguridad de aplicaciones
- Protocolo: Los protocolos en función de los cuales se agregan reglas para cada grupo de seguridad
- Dirección: Si la regla se aplica al tráfico entrante o saliente
- Intervalo de puertos: Puede especificar un puerto individual o un rango de puertos
- Acción: Permitir o denegar

Para obtener más información sobre los hipervisores compatibles, consulte lo siguiente:

- Grupo de seguridad en AWS
- Grupo de seguridad en Microsoft Azure
- Grupo de seguridad en Google Cloud Platform

### Grupo de seguridad en AWS

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

Para obtener más información sobre la configuración de red durante la preparación de la imagen, consulte Configuración de red durante la preparación imágenes.

Al iniciar una instancia, puede especificar uno o más grupos de seguridad. Para configurar grupos de seguridad, consulte Configurar grupos de seguridad.

### Grupo de seguridad en Microsoft Azure

Citrix DaaS admite grupos de seguridad de red en Azure. Se presupone que los grupos de seguridad de red estén asociados a subredes. Para obtener más información, consulte Grupos de seguridad de red.

Para obtener más información sobre el grupo de seguridad de red creado durante la preparación de la imagen, consulte Crear un catálogo de máquinas con una imagen de Azure Resource Manager.

### Grupo de seguridad en Google Cloud Platform

Durante la preparación de un catálogo de máquinas, se prepara una imagen de máquina para que sirva como disco del sistema de la imagen maestra del catálogo. Cuando se produce este proceso, el disco se conecta temporalmente a una máquina virtual. Esta máquina virtual debe ejecutarse en un entorno aislado que impida todo el tráfico de red entrante y saliente. Esto se logra mediante un par de reglas de firewall "deny-all"(denegar todo). Para obtener más información, consulte Reglas de firewall.

## Arranque seguro

May 17, 2024

El arranque seguro está diseñado para garantizar que solo se utilice software de confianza para arrancar el sistema. El firmware tiene una base de datos de certificados de confianza y verifica que la imagen que carga esté firmada por uno de tales certificados. Si esa imagen carga más imágenes, la imagen también debe verificarse de la misma manera.

vTPM es una instancia de software virtualizada de un módulo TPM físico tradicional. vTPM habilita la atestación midiendo toda la cadena de arranque de la máquina virtual (UEFI, SO, sistema y controladores).

Para obtener más información sobre los hipervisores compatibles, consulte lo siguiente:

- Arranque seguro en Google Cloud Platform
- Arranque seguro en Microsoft Azure
- Arranque seguro en VMware

### Arranque seguro en Google Cloud Platform

Puede aprovisionar máquinas virtuales blindadas en GCP. Una máquina virtual blindada está reforzada mediante un conjunto de controles de seguridad que proporcionan integridad verificable de sus instancias de Compute Engine, con prestaciones avanzadas de seguridad de plataforma como el arranque seguro, un módulo de plataforma virtual segura, firmware UEFI y supervisión de la integridad.

Para obtener más información sobre el uso de PowerShell para crear un catálogo con máquinas virtuales blindadas, consulte Uso de PowerShell para crear un catálogo con máquinas virtuales blindadas.

> **Nota:**
>
> Si instala Windows 11 en la imagen maestra, debe habilitar vTPM durante el proceso de creación de la imagen maestra. Además, debe habilitar vTPM en el origen del perfil de máquina (plantilla de instancia o máquina virtual). Para obtener información sobre la creación de máquinas virtuales de Windows 11 en el nodo de arrendatario único, consulte Crear máquinas virtuales de Windows 11 en el nodo de arrendatario único.

### Arranque seguro en Microsoft Azure

En los entornos de Azure, puede crear catálogos de máquinas habilitados con inicio seguro. Azure ofrece el inicio seguro como una forma integrada de mejorar la seguridad de las máquinas virtuales de 2.ª generación. Inicio seguro protege contra técnicas de ataque avanzadas y persistentes. En la base del inicio seguro está el arranque seguro de la máquina virtual. El inicio seguro también utiliza el vTPM para realizar la atestación remota por parte de la nube. Se utiliza para comprobar el estado de la plataforma y para tomar decisiones basadas en la confianza. Puede habilitar el arranque seguro y el vTPM de forma individual.
Para obtener más información sobre cómo crear un catálogo de máquinas con inicio seguro, consulte Catálogos de máquinas con inicio seguro.

### Arranque seguro en VMware

MCS permite crear catálogos de máquinas con una plantilla de VMware con un vTPM conectado como origen para la entrada del perfil de la máquina. Si Windows 11 está instalado en la imagen maestra, es necesario tener habilitado vTPM para la imagen maestra. Por lo tanto, la plantilla de VMware, que es el origen del perfil de la máquina, debe tener el vTPM conectado. Para obtener más información, consulte Crear un catálogo de máquinas mediante un perfil de máquina.

## Prestaciones de cifrado

June 12, 2024

Las prestaciones de cifrado protegen el contenido de las máquinas virtuales de los ataques de invitados malintencionados en un host de máquina virtual compartido y de los ataques lanzados por el software de control del hipervisor que administra todas las máquinas virtuales del host.

Para obtener más información sobre los hipervisores compatibles, consulte lo siguiente:

- Prestaciones de cifrado en AWS
- Prestaciones de cifrado en Google Cloud Platform
- Prestaciones de cifrado en Microsoft Azure)

### Prestaciones de cifrado en AWS

En esta sección se describen las prestaciones de cifrado en los entornos de virtualización de AWS.

#### Cifrado automático

Puede activar el cifrado automático de los nuevos volúmenes de Amazon EBS y de las copias de instantáneas creadas en su cuenta. Para obtener más información, consulte Cifrado automático.

### Prestaciones de cifrado en Google Cloud Platform

En esta sección se describen las prestaciones de cifrado de los entornos de virtualización de Google Cloud Platform (GCP).

Si necesita más control sobre las operaciones con claves del que permiten las claves de cifrado gestionadas por Google, puede utilizar claves de cifrado gestionadas por el cliente. Cuando se utiliza una clave de cifrado administrada por el cliente, Cloud Storage cifra un objeto con la clave en el momento

en que se almacena en un depósito y lo descifra automáticamente cuando el objeto se entrega a los solicitantes. Para obtener más información, consulte Claves de cifrado administradas por el cliente.

Puede utilizar claves de cifrado administradas por el cliente (CMEK) para catálogos de MCS. Para obtener más información, consulte Uso de claves de cifrado administradas por el cliente (CMEK).

## Prestaciones de cifrado en Microsoft Azure

En esta sección se describen las prestaciones de cifrado en los entornos de virtualización de Azure.

### Cifrado del lado del servidor de Azure

La mayoría de los discos administrados de Azure se cifran mediante el cifrado de Azure Storage, que utiliza el cifrado del lado del servidor (SSE) para proteger sus datos y para ayudarle a satisfacer sus exigencias en materia de seguridad y cumplimiento. Citrix DaaS admite claves de cifrado administradas por el cliente para los discos administrados por Azure a través de Azure Key Vault. Para obtener más información, consulte Cifrado del lado del servidor de Azure.

### Cifrado de discos de Azure en el host

Puede crear un catálogo de máquinas de MCS con capacidad de cifrado en el host.

Este método de cifrado no cifra los datos a través del almacenamiento de Azure. El servidor que aloja la máquina virtual cifra los datos y, a continuación, los datos cifrados fluyen a través del servidor de almacenamiento de Azure. Por lo tanto, este método de cifrado cifra los datos de extremo a extremo.

Para obtener más información sobre cómo crear un catálogo de máquinas de MCS con capacidad de cifrado en el host, consulte Cifrado de discos de Azure en el host.

### Cifrado doble de Azure

El cifrado doble es el cifrado del lado de la plataforma (predeterminado) y el cifrado administrado por el cliente (CMEK). Por lo tanto, si usted es un cliente altamente confidencial al que le preocupa el riesgo asociado a cualquier algoritmo de cifrado, implementación o claves comprometidas, puede optar por este doble cifrado. Los discos de datos y del SO persistentes, las instantáneas y las imágenes se cifran en REST con doble cifrado. Para obtener más información, consulte Cifrado doble en discos administrados.

#### Máquinas virtuales confidenciales de Azure

Las máquinas virtuales de computación confidencial de Azure garantizan que su escritorio virtual esté cifrado en memoria y protegido mientras se usa.

Puede usar MCS para crear un catálogo con máquinas virtuales confidenciales de Azure. Para crear dicho catálogo, debe usar el flujo de trabajo del perfil de máquina. Puede usar una máquina virtual o una especificación de plantilla de Azure Resource Manager como entrada para un perfil de máquina.

Para obtener más información, consulte Máquinas virtuales confidenciales de Azure.

## Distribución rápida

November 17, 2023

### Introducción

En Citrix DaaS, la interfaz **Administrar > Distribución rápida** ofrece una implementación rápida de aplicaciones y escritorios cuando se utiliza Microsoft Azure para alojar escritorios y aplicaciones. Esta interfaz ofrece configuración básica, sin funciones avanzadas.

Use Distribución rápida para:

- Aprovisionar máquinas virtuales y catálogos que entregan escritorios y aplicaciones alojados en Microsoft Azure.
- Crear catálogos de acceso con Remote PC para máquinas existentes.

Con Distribución rápida, puede utilizar una suscripción a Azure administrado por Citrix o su propia suscripción a Azure.

(Aunque los nombres son parecidos, Distribución rápida no es lo mismo que el método Creación rápida utilizado para crear catálogos en la interfaz de Distribución rápida).

Como alternativa a Distribución rápida, la interfaz de **Configuración completa** ofrece funciones de configuración avanzadas. Para obtener información sobre las opciones de la ficha **Administrar**, consulte Interfaces de administración.

### Diferencias entre interfaces de administración

En la tabla siguiente, se comparan las interfaces Configuración completa y Distribución rápida.

| Función | Distribución rápida | Configuración completa |
|---|---|---|
| Implementar con Azure | Sí | Sí * |
| Implementar con otros servicios en la nube | No | Sí |
| Implementar con hipervisores locales | No | Sí |
| Imágenes preparadas por Citrix disponibles | Sí | No |
| Experiencia de usuario simplificada | Sí | No |

* Cuando se utiliza una suscripción a Azure administrado por Citrix, se debe utilizar Distribución rápida al crear una imagen o un catálogo.

Si conoce el uso de Configuración completa para crear y administrar catálogos, la Distribución rápida tiene estas diferencias.

- Terminología diferente.
  - En Distribución rápida, se crea un catálogo.
  - En Configuración completa, se crea un catálogo de máquinas. En la práctica, a menudo se conoce simplemente como catálogo.
- Ubicaciones de recursos y Cloud Connectors
  - Distribución rápida crea automáticamente una ubicación de recursos que contiene dos Cloud Connectors al crear el primer catálogo.
  - En Configuración completa, crear una ubicación de recursos y agregar Cloud Connectors son pasos distintos que hay que completar en Citrix Cloud antes de crear un catálogo.
- Imágenes utilizadas para crear catálogos.
  - Distribución rápida ofrece varias imágenes preparadas por Citrix de máquinas con Windows o Linux. Puede utilizar estas imágenes para crear catálogos.

    También puede usar estas imágenes para crear otras imágenes y, a continuación, personalizar las nuevas imágenes para que se adapten a sus necesidades de implementación únicas. Esta funcionalidad se conoce como generador de imágenes. También puede importar imágenes desde su propia suscripción de Azure.
  - En Configuración completa, puede personalizar las imágenes del host compatible que utiliza. Las imágenes preparadas por Citrix no están disponibles.
- Presentación de los catálogos:

  - Los catálogos creados con Distribución rápida se ven tanto en la pantalla de Distribución rápida como en Configuración completa.
  - Los catálogos creados en Configuración completa no se ven en la pantalla de Distribución rápida.

- Grupos de entrega:

  - En Distribución rápida, no se crean grupos de entrega. En Distribución rápida, se especifican las máquinas, las aplicaciones, los escritorios y los usuarios (suscriptores) del catálogo.

    Citrix crea automáticamente un grupo de entrega para cada catálogo de Distribución rápida, con el mismo nombre que el catálogo. Esa acción ocurre en segundo plano. No es necesario hacer nada para crear el grupo de entrega. El grupo de entrega solo aparece en la interfaz de Configuración completa, no en la de Distribución rápida.
  - En Configuración completa, se crea un grupo de entrega y se indica qué máquinas contiene. Opcionalmente, también puede especificar las aplicaciones, los escritorios y los usuarios. También puede crear grupos de aplicaciones.

- Diseño e interfaz de usuario.

  - La interfaz de Distribución rápida tiene un diseño y estilo diferentes a los de Configuración completa. Distribución rápida contiene más instrucciones en pantalla.

Las interfaces no son mutuamente excluyentes. Puede utilizar Distribución rápida para crear algunos catálogos y, a continuación, utilizar Configuración completa para crear otros catálogos.

### 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 en Distribución rápida. 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 > Distribución rápida**, 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.

#### Sustitución de la interfaz anterior de Distribución rápida de Azure

Distribución rápida reemplaza una interfaz anterior denominada Distribución rápida de Azure. La pantalla de Distribución rápida incluye todos los catálogos que creó con Distribución rápida de Azure.

Si comenzó a crear un catálogo en Distribución rápida de Azure, pero no lo terminó, ese catálogo aparece en la lista de catálogos de Distribución rápida. Sin embargo, la única acción disponible en Distribución rápida es eliminarlo.

### Requisitos

- Distribución rápida solo admite cargas de trabajo de Azure. No está disponible con ningún otro tipo de host en la nube, servicios o hipervisores.
- Distribución rápida solo está disponible en las ediciones para Azure, Premium y Advanced de Citrix DaaS y en Workspace Premium Plus.
- Debe tener una cuenta de Citrix Cloud y una suscripción a Citrix DaaS.

- Si solicitó el Consumption Fund de Azure administrado por Citrix, puede usar la suscripción de Azure administrada por Citrix al crear catálogos e imágenes.

  Si no solicitó el Consumption Fund (o prefiere usar su propia suscripción de Azure), debe tener una suscripción a Azure.

- Debe tener los permisos adecuados en Citrix DaaS para ver la ficha **Administrar**. Para obtener más información, consulte Administración delegada.

> **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**.

#### Aspecto a tener en cuenta de Citrix Gateway

Si usa su propio dispositivo Citrix Gateway, este debe tener acceso a la red virtual especificada en el asistente de creación de catálogos. Una VPN puede proporcionar ese acceso.

Citrix Gateway Service funciona automáticamente con los catálogos de Distribución rápida.

## A continuación

Siga las instrucciones de configuración de Distribución rápida de la Introducción.

Después de configurar la implementación con Distribución rápida, puede seguir utilizando esa interfaz para las siguientes tareas de administración.

- Administrar el catálogo. La administración de catálogos incluye agregar o eliminar máquinas, la gestión de aplicaciones y la gestión de programaciones de administración de energía.
- Administrar imágenes. La administración de imágenes incluye la preparación o importación de imágenes, la actualización de catálogos con una nueva imagen, el cambio de nombre o la eliminación de imágenes, y la instalación o actualización de la versión de agentes VDA en una imagen.
- Agregar o quitar usuarios de los catálogos.
- Administrar ubicaciones de recursos.

# Introducción a Distribución rápida

May 23, 2023

En este artículo, se resumen las tareas de configuración para entregar escritorios y aplicaciones mediante la interfaz Distribución rápida de Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service). Le recomendamos que revise cada procedimiento antes de hacerlo realmente, para saber lo que puede esperar.

Para utilizar Distribución rápida para configurar una implementación de Acceso con Remote PC, consulte Acceso con Remote PC.

## Resumen de tareas de configuración

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

1. Revise y complete tareas necesarias en Requisitos del sistema y preparación.
2. Configure una implementación rápida de prueba de concepto o una implementación de producción.
3. Proporcione la URL del espacio de trabajo a los usuarios.

## Requisitos del sistema y preparación

- Registrarse en Citrix Cloud y Citrix DaaS.

  Además, si piensa utilizar Azure administrado por Citrix, deberá solicitar Citrix Azure Consumption Fund (además de Citrix DaaS), ya sea a través de Citrix o de Azure Marketplace.

- **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. Para obtener más información, consulte Configurar un servidor de licencias de Microsoft RDS.
- Si piensa utilizar una suscripción a Azure administrado por Citrix y quiere unir agentes VDA a un dominio mediante la directiva de grupo de Active Directory, debe ser 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 piensa utilizar sus propias imágenes de Azure al crear un catálogo, esas imágenes deben cumplir ciertos requisitos.
- Requisitos de conectividad a Internet: Requisitos del sistema y de conectividad.
- Límites de recursos en una implementación de Citrix DaaS: Límites.

#### Sistemas operativos compatibles

Al utilizar Distribución rápida con una suscripción a Azure administrado por Citrix:

- Windows 10 de sesión única
- Windows 10 multisesión
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux y Ubuntu

Al utilizar Distribución rápida con una suscripción a Azure administrado por el cliente:

- 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
- Red Hat Enterprise Linux y Ubuntu

### 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 utiliza su propia suscripción a Azure (en lugar de una suscripción a Azure administrado por Citrix), agregue 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, utilice el panel de mandos **Distribución rápida > Supervisar** para ver el uso de escritorios, sesiones y máquinas.

### 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.

La URL del espacio de trabajo está disponible en dos ubicaciones:

- En **Administrar > Distribución rápida**, en Citrix DaaS, expanda **Acceso y autenticación de usuarios** a la derecha para ver la URL.
- En la consola de Citrix Cloud, seleccione **Configuración de Workspace** en el menú superior izquierdo. La **ficha Acceso** contiene la URL del espacio de trabajo.

Para obtener información sobre cómo personalizar la URL del espacio de trabajo, consulte Personalizar la URL del espacio de trabajo.

Una vez que los usuarios vayan a la URL del espacio de trabajo y se autentiquen, podrán iniciar sus escritorios y aplicaciones.

### Obtener ayuda

- Revise el artículo Solución de problemas.
- Si sigue teniendo problemas con Citrix DaaS, siga las instrucciones que aparecen en Cómo obtener ayuda y asistencia técnica para abrir un tíquet.

## Crear catálogos con Distribución rápida

May 17, 2024

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

Siga los procedimientos que se indican en este artículo para crear un catálogo de máquinas de Microsoft Azure con la interfaz de administración Distribución rápida.

Revise todo el procedimiento antes de crear un catálogo para saber qué esperar.

Para crear un catálogo con la interfaz de Configuración completa, consulte Crear catálogos de máquinas.

### Tipos de máquina

Un catálogo de Distribución rápida 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. Introduzca la cantidad de máquinas y sesiones por máquina, que representa la cantidad total de sesiones que el catálogo admite.

Al implementar escritorios, los tipos de máquina estática y aleatoria a veces se denominan "tipos de escritorio".

### Formas de crear un catálogo con Distribución rápida

Existen varias formas de crear y configurar un catálogo:

- **Creación rápida** es la forma más rápida de ponerse en marcha. Se proporciona un mínimo de información y Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service) 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. |

| Creación rápida | Creación personalizada |
| --- | --- |
| 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. | Selección de: Imágenes preparadas por Citrix, imágenes que importa de Azure o imágenes que ha integrado en Citrix DaaS a partir de una imagen importada o preparada 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 un programa de administración de energía durante la creación. (Un programa de administración de energía de Distribución rápida difiere de un programa de administración de energía creado con la interfaz de administración Configuración completa). |
| Debe utilizar una suscripción de Azure administrado por Citrix. | Puede utilizar la suscripción de Azure administrado por Citrix o su propia suscripción a Azure. |

Para obtener más información sobre el procedimiento, consulte:

- Crear un catálogo de Distribución rápida con Creación rápida
- Crear un catálogo de Distribución rápida con Creación personalizada

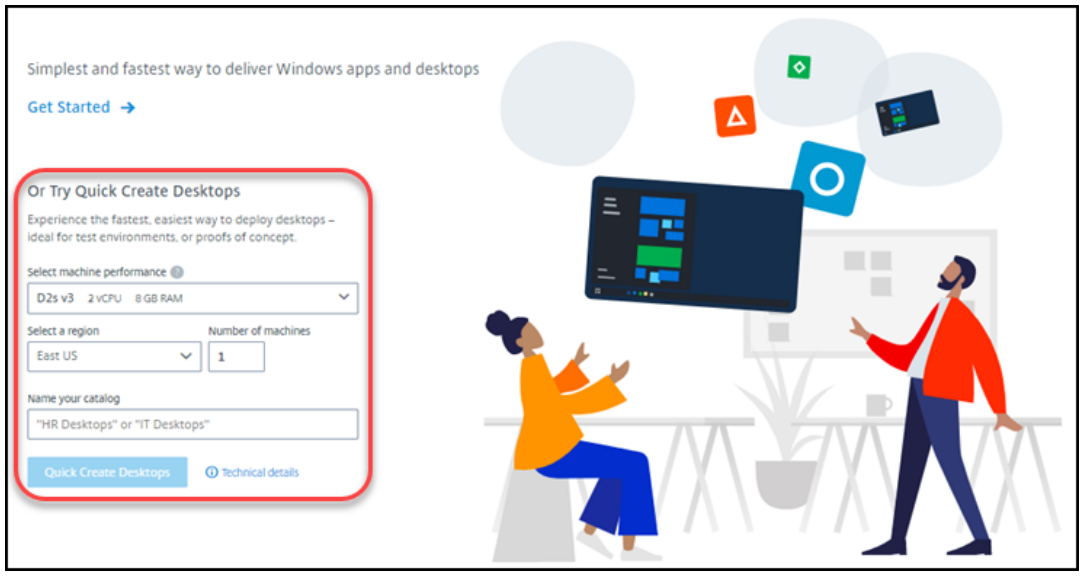
> **Importante:**
>
> Al crear un catálogo (o una imagen) mediante una suscripción a Azure administrado por Citrix por primera vez, se le pide que confirme y acepte su responsabilidad por los cargos incurridos. Recordatorios de ese consentimiento pueden aparecer también al crear otros catálogos o imágenes mediante la suscripción a Azure administrado por Citrix.

### Crear un catálogo de Distribución rápida con Creación rápida

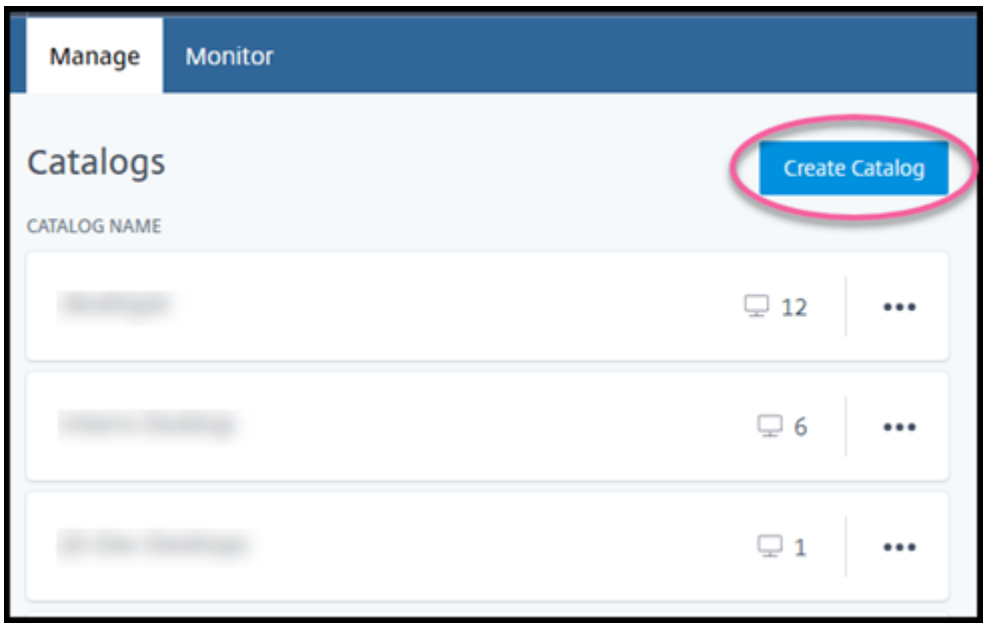
El método de creación rápida utiliza una suscripción a Azure administrado por Citrix y una imagen de Windows 10 preparada por Citrix para crear un catálogo que contiene máquinas estáticas. La configuración de administración de energía utiliza los valores de Ahorro de costes predefinidos. No hay conexión con su red corporativa. Los usuarios deben agregarse mediante Azure AD administrado por Citrix.

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

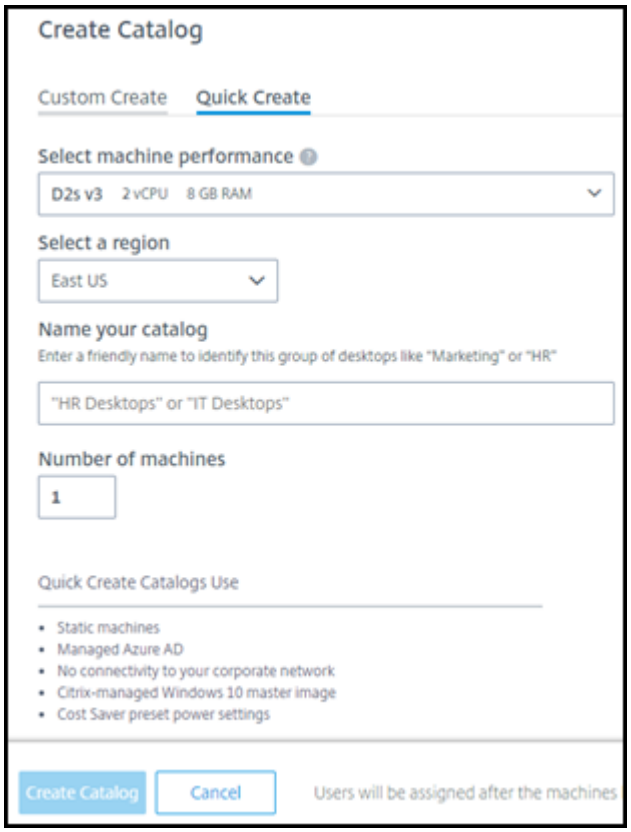



   - Seleccione **Empiece aquí**. Aparecerá el panel de mandos **Administrar > Distribución rápida**. Seleccione **Crear catálogo**.
5. Si ya se ha creado un catálogo (y va a crear otro), se le dirige al panel de mandos **Administrar > Distribución rápida**. Seleccione **Crear catálogo**.




6. Seleccione **Creación rápida** en la parte superior de la página, si la opción 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.

7. Cuando haya terminado, seleccione **Crear catálogo**. (Si va a crear el primer catálogo desde la página de **bienvenida**, seleccione **Escritorios de creación rápida**).
8. Si este es el primer catálogo que va a crear mediante una suscripción a Azure administrado por Citrix, cuando se le solicite, confirme su responsabilidad por los cargos asociados.

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

Qué hacer a continuación:

- Puede agregar usuarios al directorio de Azure AD administrado mientras se crea el catálogo.
- Una vez creado el catálogo, agregue usuarios al catálogo.

### Crear un catálogo de Distribución rápida con Creación 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 Azure administrado por Citrix, puede:

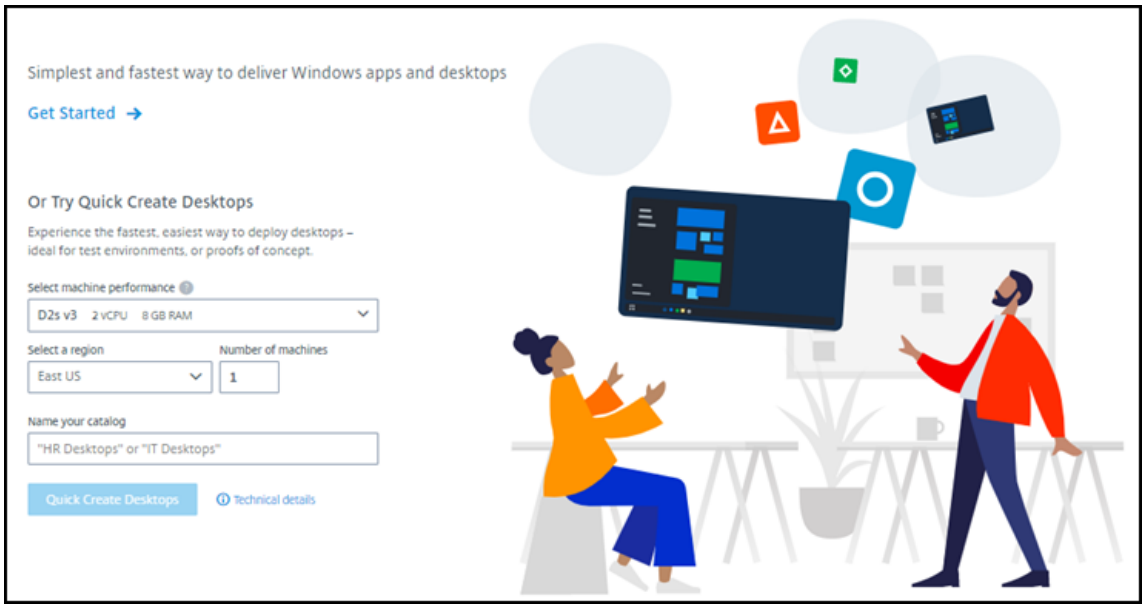
- Solicite Azure Consumption Fund a través de Azure Marketplace, que le proporciona una suscripción a Azure administrado por Citrix.
- Importe (agregue) una o varias de sus suscripciones de Azure a Citrix DaaS antes de crear un catálogo.

Para crear un catálogo:

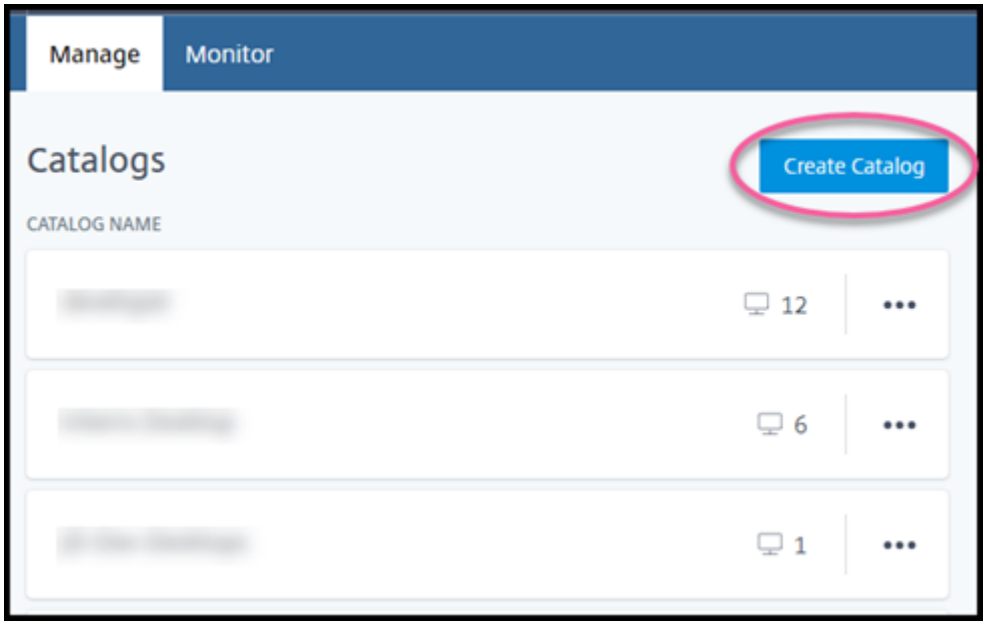
1. Inicie sesión en Citrix Cloud.
2. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
3. Seleccione **Administrar > Distribución rápida**.

4. Si aún no se ha creado un catálogo, se le dirigirá a la página de **bienvenida**. Seleccione **Empiece aquí**. Al final de la página de introducción, se le dirige al panel de mandos **Administrar > Distribución rápida** . Seleccione **Crear catálogo**.

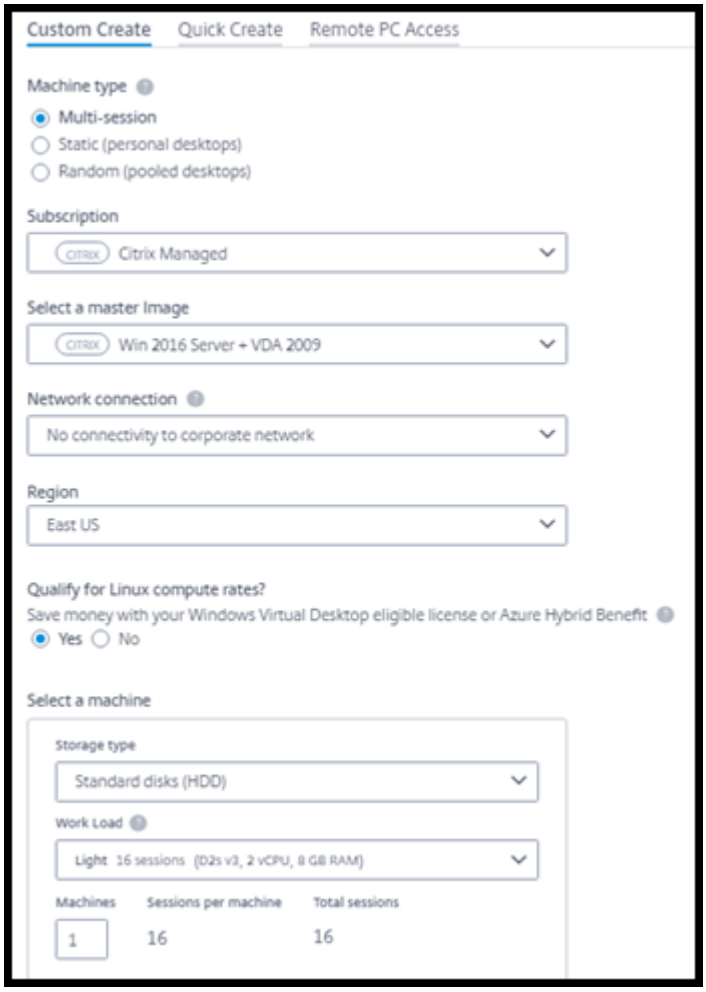



Si ya se ha creado un catálogo, se le dirige al panel **Administrar > Distribución rápida**. Seleccione **Crear catálogo**.




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




6. Complete los siguientes campos. (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.
   - **Imagen maestra:** Seleccione una imagen de sistema operativo que se utilizará para las máquinas del catálogo.
   - **Conexión de red:** Seleccione la conexión de red que quiere utilizar para acceder a los recursos de la red.

     Si ha seleccionado 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 creada anteriormente, como un emparejamiento de redes virtuales o una conexión SD-WAN.

Si ha seleccionado una suscripción a Azure administrada por el cliente, seleccione el grupo de recursos, la red virtual y la subred correspondientes.

- **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 ha seleccionado una 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 Windows Virtual Desktop:** Licencias de Windows 10 o Windows 7 aptas 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**. HDD o SSD.
  - **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 nomenclatura de máquinas.

- **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 (este programa de administración de energía difiere de las funcionalidades de administración de energía disponibles en la interfaz Configuración completa de Citrix DaaS).
- **Unirse a un dominio local (Active Directory):** (Disponible solo si ha seleccionado una conexión de emparejamiento de redes virtuales de Azure en **Conexión de red**) Seleccione **Sí** o **No**. Si selecciona **Sí**, introduzca:
  - Nombre de dominio completo (FQDN) del dominio (por ejemplo, Contoso.com).
  - Unidad organizativa: Para utilizar la unidad organizativa predeterminada (equipos), deje este campo en blanco.
  - Nombre de la cuenta de Citrix DaaS: Debe ser un administrador de dominio o empresa con el formato nombre@dominio o dominio\nombre.
  - Contraseña del nombre de cuenta de Citrix DaaS
- **Parámetros avanzados:** Consulte Parámetros de ubicación de recursos al crear un catálogo.

7. Cuando haya terminado, seleccione **Crear catálogo**.
8. Si este es el primer catálogo que va a crear mediante una suscripción a Azure administrado por Citrix, cuando se le solicite, confirme su responsabilidad por los cargos asociados.

El panel de mandos **Administrar > Distribución rápida** indica cuándo se crea el catálogo. Citrix DaaS también crea automáticamente una ubicación de recursos y agrega dos Citrix 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).

### 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 seleccionar **Parámetros avanzados** en el cuadro de diálogo de creación de catálogos, Citrix DaaS obtiene información de la 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 desea, 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 los parámetros avanzados, seleccione **Guardar** para volver al cuadro de diálogo de creación de catálogos.

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, 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. Citrix DaaS 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 nomenclatura de máquinas, Citrix DaaS utiliza el esquema 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

- Catálogos de acceso con Remote PC
- Crear un catálogo en una red que utilice un servidor proxy
- Mostrar información de catálogo
- Administrar catálogos en Distribución rápida

## Administrar catálogos en Distribución rápida

April 14, 2022

En este artículo se describen las tareas para la administración de los catálogos creados en Distribución rápida.

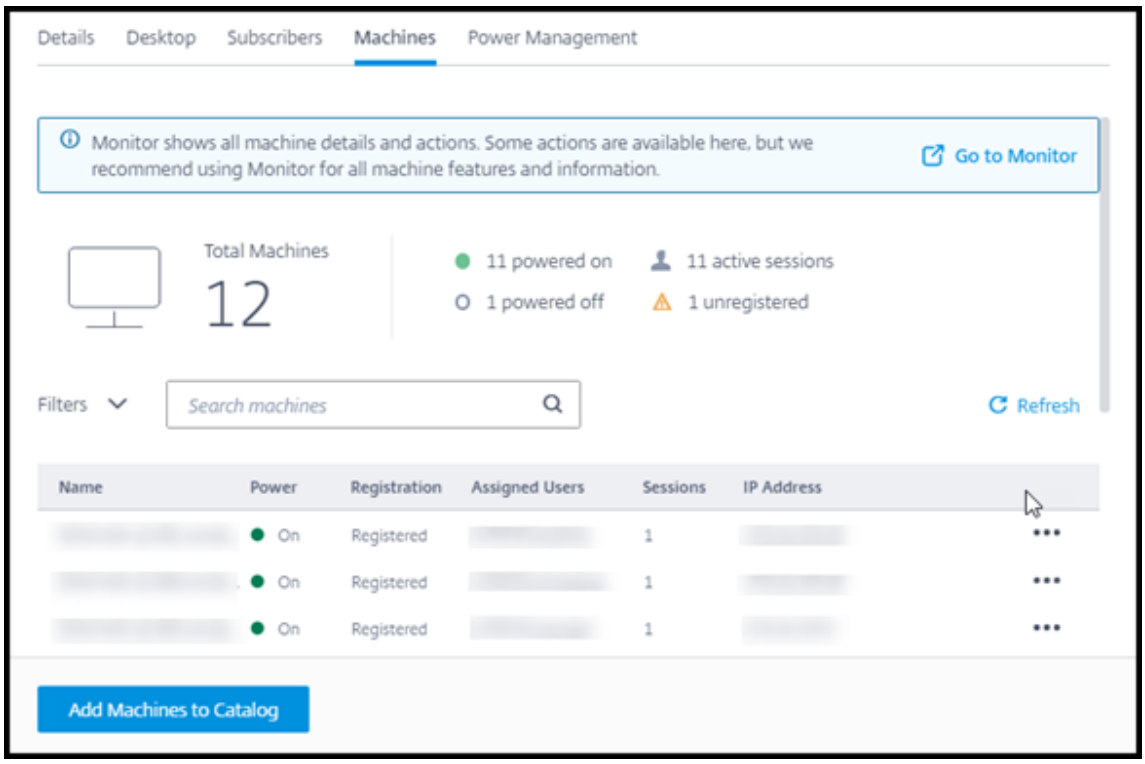
Recuerde: Si utilizó Distribución rápida para crear un catálogo y, a continuación, utiliza la interfaz de Configuración completa para realizar cualquier tarea de administración de ese catálogo, ya no podrá volver a utilizar la interfaz de Distribución rápida con dicho catálogo.

(Para obtener información sobre la administración de catálogos con la interfaz de administración de Configuración completa, consulte Administrar catálogos de máquinas.)

## Agregar máquinas a un catálogo

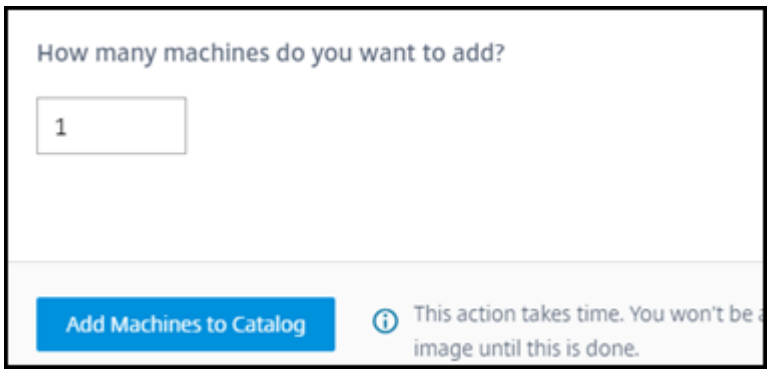
Mientras se agregan máquinas a un catálogo de Distribución rápida, no puede realizar ningún otro cambio en ese catálogo.

1. En **Administrar > Distribución rápida**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Máquinas**, seleccione **Agregar máquinas a 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 Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service).
5. Seleccione **Agregar máquinas a 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 **Administrar > Distribución rápida**, seleccione un catálogo que contenga máquinas multisesión.
2. En la ficha **Detalles**, seleccione **Modificar** junto a **Sesiones por máquina**.
3. Introduzca un nuevo número de sesiones por máquina
4. Seleccione **Actualizar cantidad 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 disponibles en **Administrar > Distribución rápida** también están disponibles en la ficha **Supervisar** de Distribución rápida.

Para seleccionar acciones en **Administrar > Distribución rápida**:

1. En **Administrar > Distribución rápida**, 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:** Reinicia la máquina seleccionada.
   - **Iniciar:** Inicia 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:** Activa el modo de mantenimiento (si está desactivado) o lo desactiva (si está activado) para la máquina seleccionada. De forma predeterminada, el modo de mantenimiento de una máquina está desactivado.

     Activar el modo de mantenimiento impide que se realicen nuevas conexiones a la máquina. Los usuarios pueden conectarse a las sesiones existentes de esa máquina, pero no pueden iniciar nuevas sesiones en la misma.

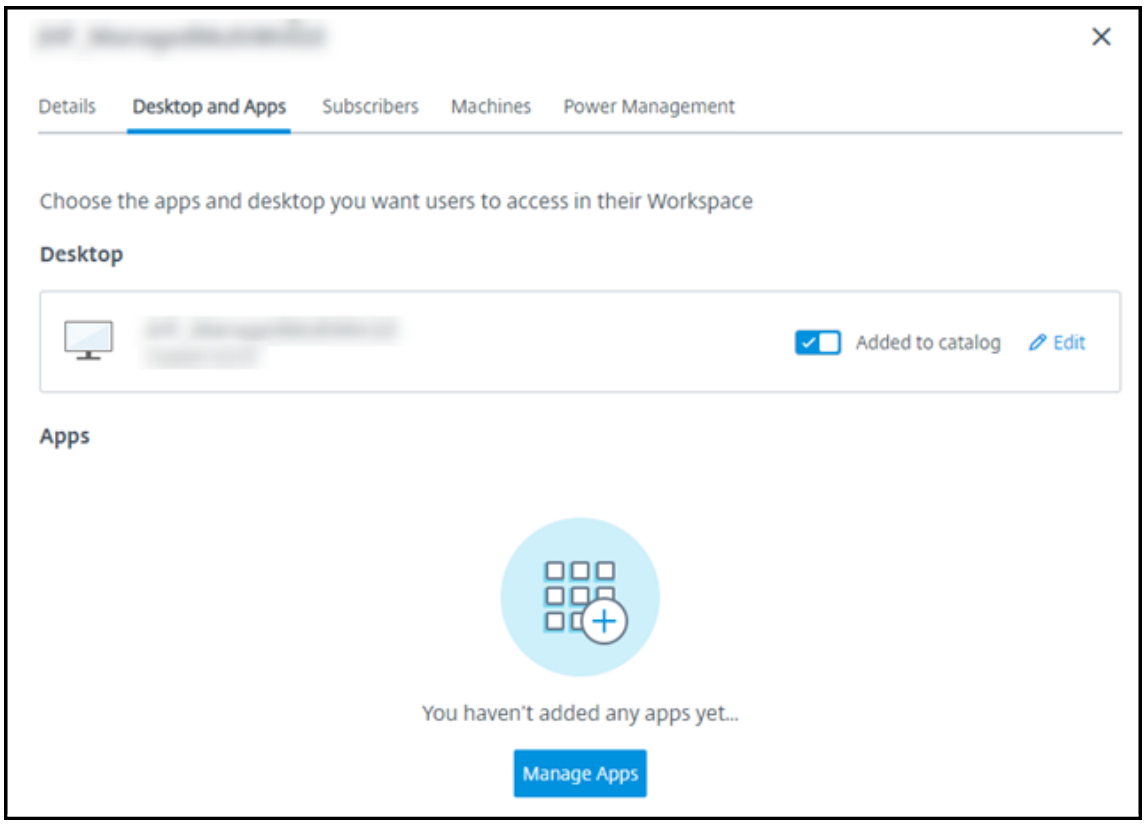
     Puede poner una máquina en modo de mantenimiento antes de aplicar parches o para solucionar problemas.
   - **Eliminar:** Elimina la máquina seleccionada. Esta acción solo está disponible cuando el recuento de sesiones de la máquina es cero. Confirme la eliminación.

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

## Agregar aplicaciones a un catálogo

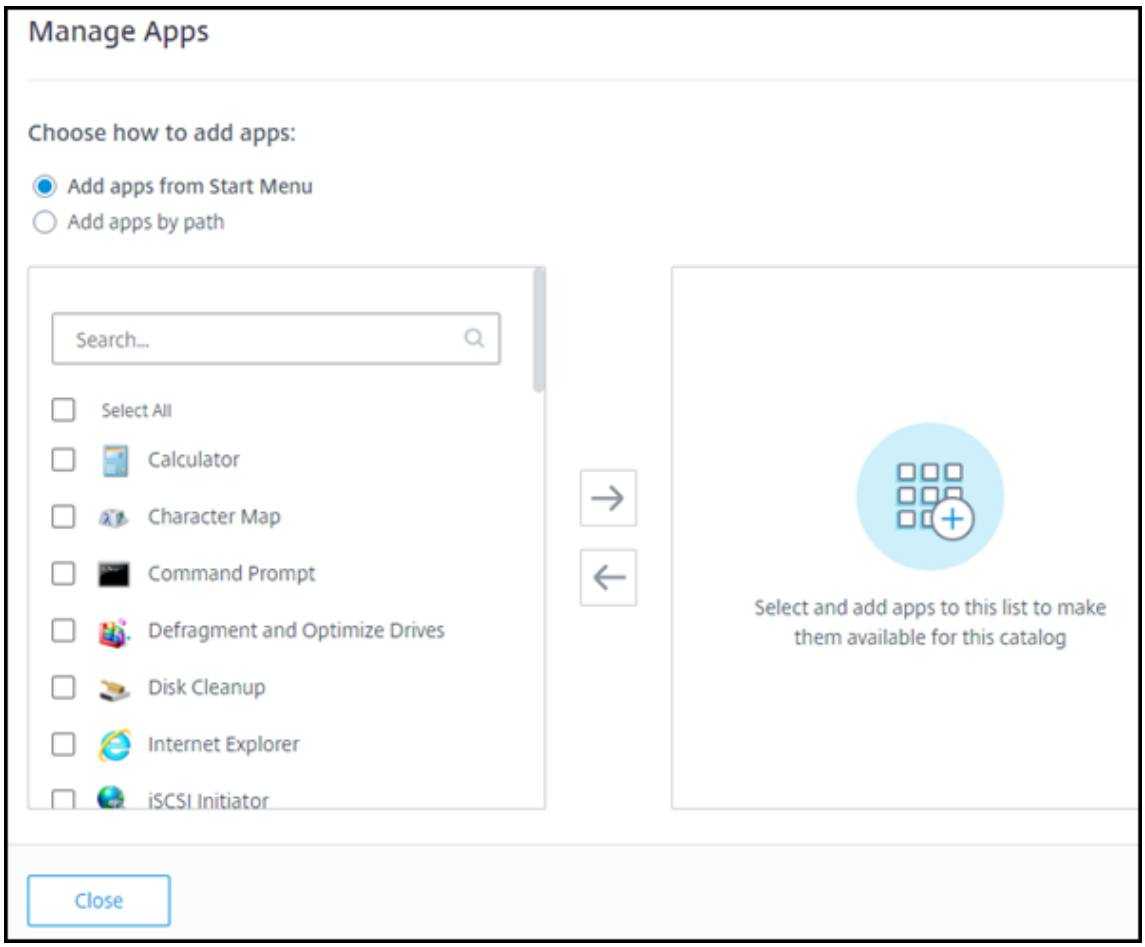
1. En **Administrar > Distribución rápida**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Escritorio y aplicaciones**, seleccione **Administrar aplicaciones**.




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**:

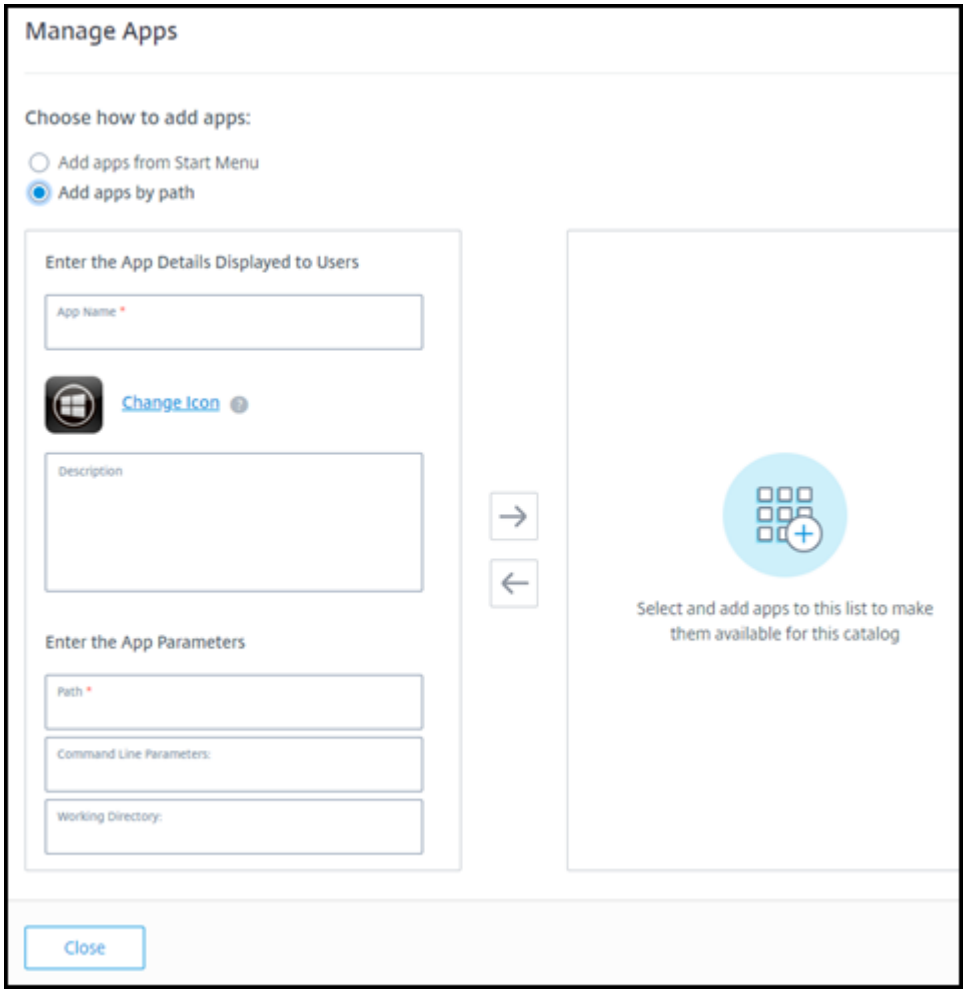
 




- Seleccione las aplicaciones disponibles en la columna de la izquierda. (Utilice **Buscar** para adaptar la lista de aplicaciones.) Seleccione la flecha derecha entre las columnas. Las aplicaciones seleccionadas se desplazan a la columna derecha.
- Del mismo modo, para quitar aplicaciones, selecciónelas en la columna derecha. Seleccione la flecha izquierda entre 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, seleccione **Cambiar icono** y desplácese hasta el icono que quiera 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 línea de comandos, consulte Transferir parámetros a aplicaciones publicadas.

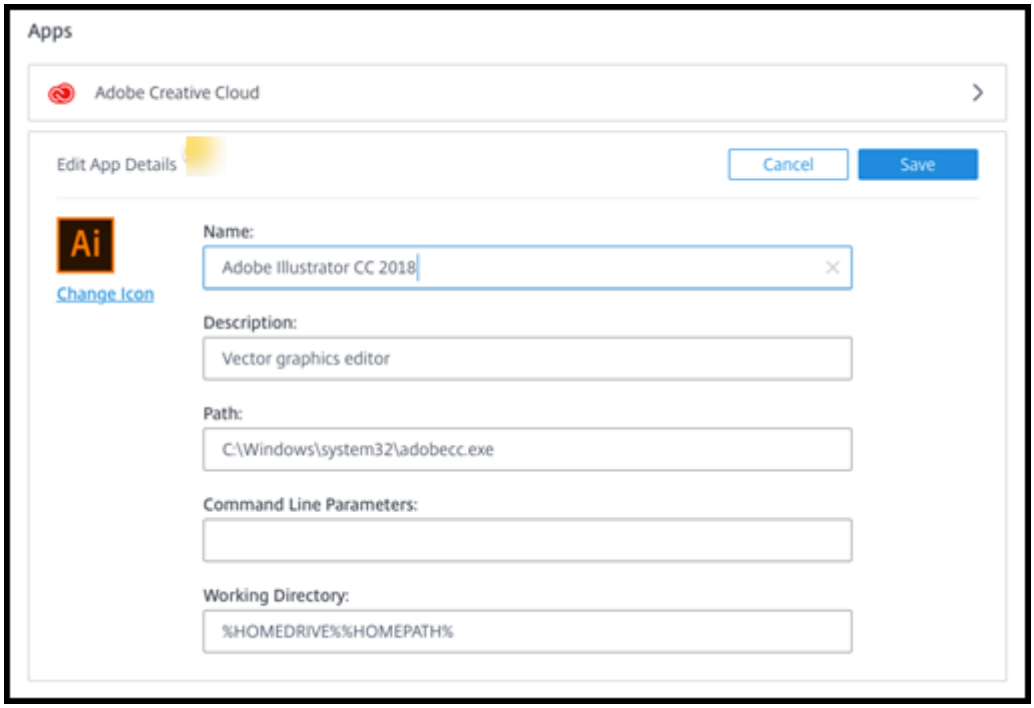
6. Cuando haya terminado, seleccione **Cerrar**.

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 **Administrar > Distribución rápida**, 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. Seleccione 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 ven los usuarios en su instancia de Citrix Workspace, seleccione **Cambiar icono** y vaya al icono que quiere mostrar.
6. Cuando haya terminado, seleccione **Guardar**.

#### 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:\Program Files"`), 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 **Administrar > Distribución rápida**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Escritorio y aplicaciones**, seleccione el icono de la papelera situado junto a las aplicaciones que quiere 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 **Administrar > Distribución rápida**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Detalles**, seleccione **Eliminar catálogo**.
3. Confirme la eliminación.

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 ofrece varias programaciones preestablecidas. 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 desea 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 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 **Administrar > Distribución rápida**, 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 desea 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. Seleccione **Personalizado** en la parte superior y, a continuación, guarde la configuración actual como nuevo parámetro preestablecido. Introduzca un nombre para el nuevo parámetro preestablecido y seleccione la marca de verificación.
6. Cuando haya terminado, seleccione **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.

### Información relacionada

- Actualizar un catálogo con una nueva imagen
- Agregar y quitar usuarios de los catálogos

## Suscripciones a Azure en Distribución rápida

May 17, 2024

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

### Introducción

Al crear un catálogo o crear una imagen en Distribución rápida, elige entre las suscripciones de Azure disponibles. Distribución rápida admite tanto suscripciones de Azure administrado por Citrix como

sus propias suscripciones de Azure administrado por el cliente.

- Para utilizar su propia suscripción a Azure, primero debe importar (agregar) una o más de esas suscripciones a Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Esta acción permite a Citrix DaaS acceder a sus suscripciones de Azure.
- El uso de una suscripción de Azure administrado por Citrix no requiere ninguna configuración de suscripción. Sin embargo, una suscripción de Azure administrado por Citrix solo está disponible cuando solicita Citrix Azure Consumption Fund, además de Citrix DaaS.

Algunas funciones de Citrix DaaS varían en función de si el catálogo utiliza una suscripción a Azure administrado por Citrix o su propia suscripción a 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. | Compatible solo con catálogos de creación personalizada. |
| Siempre disponible al crear catálogos e imágenes. | Debe agregar la suscripción de Azure a Citrix DaaS 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 utilizar el emparejamiento de redes virtuales de Azure para conectarse a los recursos, debe crear una conexión de pares de redes virtuales en Citrix DaaS. | 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 bastión porque ya puede acceder a las máquinas de la suscripción. |

### Ver suscripciones de Azure

Para ver los detalles de la suscripción a Azure, en **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha. A continuación, seleccione una entrada de suscripción.

- La página **Detalles** incluye la cantidad de máquinas, además de los números y nombres de catálogos e imágenes que utilizan 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 utilizar una suscripción de Azure administrada por el cliente, debe agregarla a Citrix DaaS antes de crear un catálogo o crear una imagen que utilice esa suscripción. Tiene dos opciones al agregar las suscripciones de Azure:

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

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

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

1. En **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha.
2. Seleccione **Agregar suscripción de Azure**.
3. En la página **Agregar suscripciones**, seleccione **Agregar las suscripciones de Azure**.
4. Seleccione el botón que permite a Citrix DaaS acceder a sus suscripciones de Azure en su nombre.
5. Seleccione **Autenticar cuenta de Azure**. Vaya a la página de inicio de sesión de Azure.
6. Introduzca sus credenciales de Azure.
7. Regresará automáticamente a Citrix DaaS. 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, seleccione **Agregar suscripciones**.
8. Confirme que desea 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.

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

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

- Antes de agregar una suscripción a Citrix DaaS, cree una aplicación en Azure AD y, a continuación, agréguela como colaborador de la suscripción.
- Agregue la suscripción a Citrix DaaS con la 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**, seleccione **Registros de aplicaciones**.
   d) Seleccione **+ 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) Seleccione **Create**.
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**. Le servirá más adelante al agregar la suscripción a Citrix DaaS.
   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, selecciona **Agregar**.
   f) Anote el valor del secreto de cliente. Le servirá más adelante al agregar la suscripción a Citrix DaaS.
   g) Seleccione la suscripción de Azure que quiere vincular (agregar) a Citrix DaaS y, a continuación, seleccione **Control de acceso (IAM)**.
   h) En el cuadro **Agregar una asignación de roles**, seleccione **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) Seleccione **Guardar**.

**Agregar la suscripción a Citrix DaaS** Necesitará el ID de aplicación, el ID de directorio y el valor secreto de cliente de la aplicación que creó en Azure AD.

1. En **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha.
2. Seleccione **Agregar suscripción de Azure**.
3. En la página **Agregar suscripciones**, seleccione **Agregar las suscripciones a 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. Elija **Seleccione su suscripción** y, a continuación, seleccione la suscripción que quiera.

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

Si Citrix DaaS no puede acceder a una suscripción de Azure después de agregarla, no se admiten algunas acciones de administración de energía del 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 de Azure administrado por Citrix admite un cierto número de máquinas. (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 se puede crear un catálogo (ni agregar máquinas a un catálogo) si el número total de máquinas de todos los catálogos que utilizan esa suscripción a Azure administrado por Citrix supera el límite.

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. En **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha.
3. Seleccione **Agregar suscripción de Azure**.
4. En la página **Agregar suscripciones**, seleccione **Agregue una suscripción de Azure administrada por Citrix**.
5. En la página **Agregue una suscripción de Azure administrada por Citrix**, seleccione **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

Antes de poder quitar una suscripción a Azure, 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. En **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha.
2. Seleccione la entrada de la suscripción.
3. En la ficha **Detalles**, seleccione **Quitar suscripción**.
4. Seleccione **Autenticar cuenta de Azure**. Vaya a la página de inicio de sesión de Azure.
5. Introduzca sus credenciales de Azure.
6. Regresará automáticamente a Citrix DaaS. Confirme la eliminación y, a continuación, seleccione **Sí, eliminar suscripción**.

### Actualizar los secretos de cliente caducados

Cuando caduca el secreto de cliente de una suscripción, no puede crear catálogos de máquinas para ella y aparece una alerta en la entrada de la suscripción. Para resolver este problema, tiene dos opciones:

- Actualizar el secreto de cliente de la aplicación de Azure en uso
- Cambiar a una aplicación de Azure con una fecha de caducidad válida

#### Actualizar el secreto de cliente de la aplicación de Azure en uso

Para seguir usando la aplicación de Azure existente para acceder a los recursos de Azure, siga estos pasos:

1. En Azure, cree un secreto de cliente para la aplicación de Azure en uso. Anote el nuevo secreto y la fecha de caducidad para usarlos en el futuro. Para obtener más información, consulte Crear un secreto de aplicación en Azure.
2. En DaaS, proporcione la información secreta recién creada a la suscripción. Estos son los pasos detallados:

    a) En el panel **Administrar > Distribución rápida de Azure** de Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha.
    b) Haga clic en la suscripción en la que es necesario actualizar el secreto.
    c) En la página de suscripción que aparece, haga clic en el menú de puntos suspensivos del panel **Detalles de la aplicación de Azure** y, a continuación, seleccione **Actualizar secreto de cliente**.

d) En la página **Actualizar secreto de cliente**, escriba el nuevo **secreto de cliente** y la **fecha de caducidad del secreto**.
e) Haz clic en **Actualizar secreto**.

#### Cambiar a una aplicación de Azure con una fecha de caducidad válida

Para cambiar a una aplicación de Azure válida para acceder a los recursos de Azure, obtenga la información de la aplicación necesaria y envíela a la suscripción siguiendo estos pasos:

1. En Azure, obtenga una aplicación de Azure válida y anote sus detalles. Asegúrese de que la nueva aplicación de Azure tenga asignado el rol de *colaborador*. Para obtener más información, consulte Crear una aplicación en Azure AD y agregarla como colaborador.
2. En DaaS, proporcione detalles de la aplicación de Azure a la suscripción. Estos son los pasos detallados:

   a) En el panel **Administrar > Distribución rápida de Azure** de Citrix DaaS para Azure, expanda **Suscripciones a la nube** a la derecha.
   b) Haga clic en la suscripción en la que es necesario actualizar el secreto.
   c) En la página de suscripción que aparece, haga clic en el menú de puntos suspensivos del panel **Detalles de la aplicación de Azure** y, a continuación, seleccione **Sustituir aplicación de Azure**.
   d) En la página **Sustituir aplicación de Azure**, introduzca los detalles de la nueva aplicación de Azure en los campos correspondientes a **ID de directorio (arrendatario)**, **Aplicación (cliente)**, **Secreto del cliente** y **Fecha de caducidad del secreto de la entidad principal de servicio**.
   e) Haz clic en **Sustituir aplicación**.

## Imágenes en Distribución rápida

June 12, 2024

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

Distribución rápida proporciona un conjunto de imágenes preparadas entre las que puede elegir para crear y personalizar una imagen. También puede importar (agregar) imágenes desde su propia suscripción de Azure.

### imágenes preparadas por Citrix

Distribución rápida proporciona varias imágenes preparadas por Citrix:

- Windows 11 (sesión única)
- Windows 11 Enterprise Virtual Desktop (multisesión)
- Windows 11 Enterprise Virtual Desktop (multisesión) con Office 365 ProPlus
- Windows 10 (sesión única)
- Windows 10 Enterprise Virtual Desktop (multisesión)
- Windows 10 Enterprise Virtual Desktop (multisesión) con Office 365 ProPlus
- Windows Server 2022 (multisesión)
- Windows Server 2019 (multisesión)
- Windows Server 2016 (multisesión)
- Linux Ubuntu 22.04 LTS (sesión única)
- Linux Ubuntu 22.04 LTS (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 (anteriormente, Citrix Virtual Apps and Desktops Service). Las imágenes proporcionadas por Citrix tienen una notación **CITRIX**.

Las imágenes preparadas por Citrix no están disponibles en la interfaz Configuración completa de Citrix DaaS.

También puede importar y utilizar su propia imagen de Azure.

### Formas de utilizar imágenes en Distribución rápida

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.

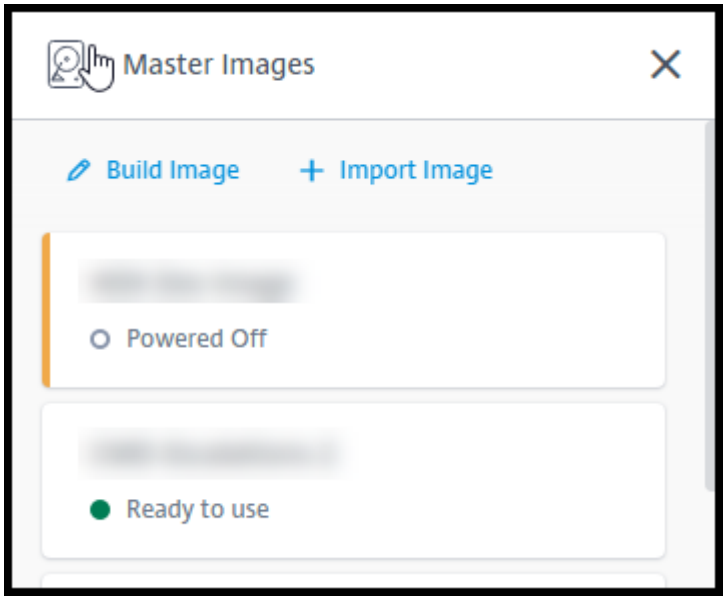
  O bien, puede usar esa imagen para crear una nueva imagen y, a continuación, personalizarla agregando aplicaciones. A continuación, puede utilizar esa imagen personalizada al crear un catálogo.

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

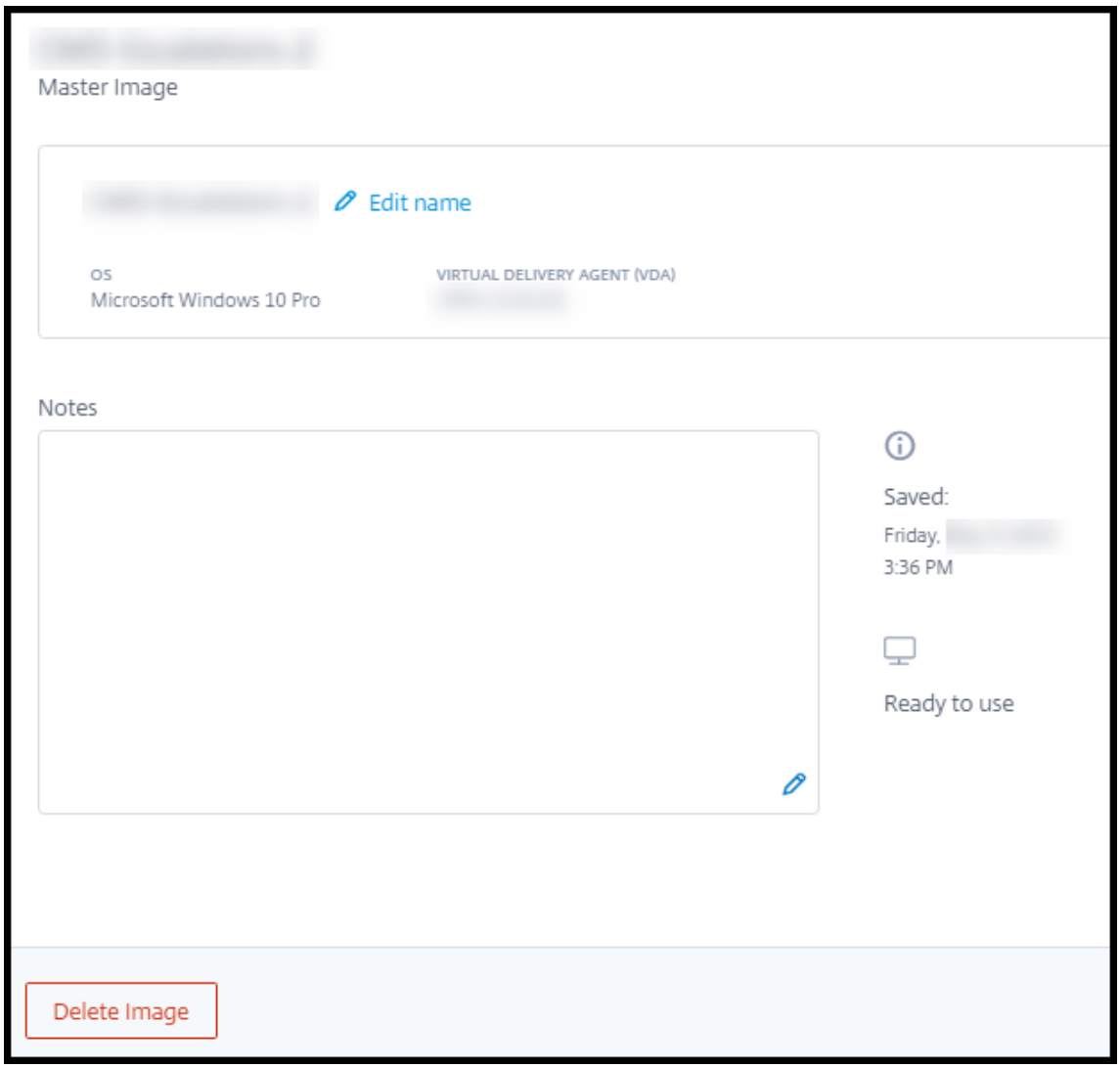
### Mostrar información de imagen

1. En **Administrar > Distribución rápida**, expanda **Imágenes maestras** a la derecha. En la pantalla se enumeran las imágenes preparadas por Citrix y las imágenes que haya importado.




2. Seleccione 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 imágenes que ha preparado o importado, no para imágenes preparadas 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 características 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.

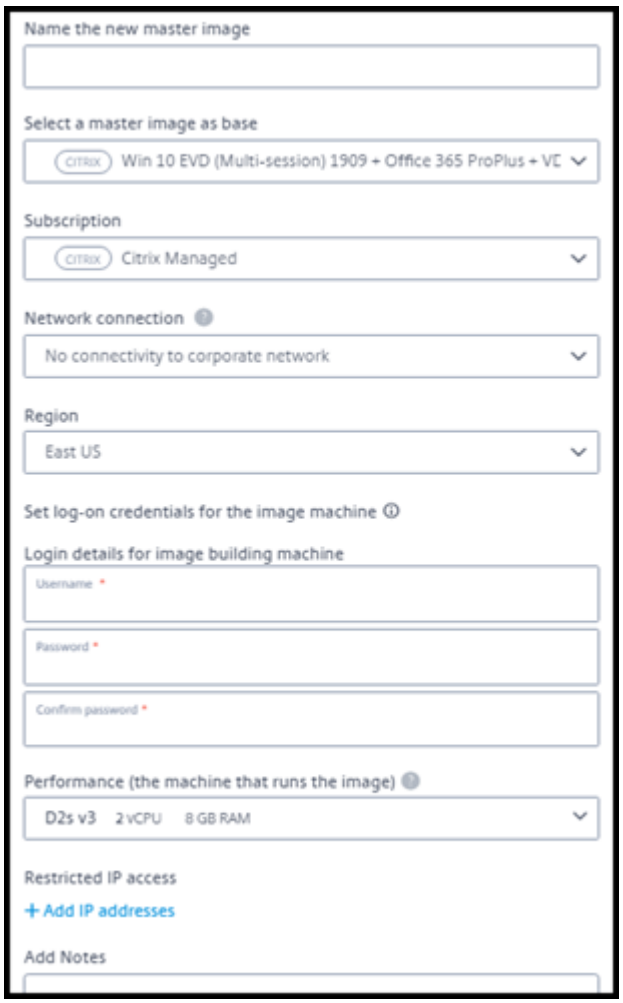
Cuando se utiliza una imagen de Ubuntu preparada por Citrix para crear una nueva imagen, se crea una contraseña raíz para la nueva imagen. Puede cambiar esa contraseña raíz, pero solo durante el proceso de creación y personalización de la imagen. (No se puede cambiar la contraseña raíz después de utilizar 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 **Administrar > Distribución rápida**, expanda **Imágenes maestras** a la derecha.
2. Seleccione **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.
   - **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 Citrix DaaS y credenciales.
   - **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, seleccione **Listo** para volver a la tarjeta de **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 el FQDN, la unidad organizativa, el nombre de la cuenta de Citrix DaaS y las credenciales.
  - Si selecciona **No**, introduzca las credenciales de la máquina host.

4. Cuando haya terminado, seleccione **Crear imagen**.

Una imagen puede tardar hasta 30 minutos en crearse. En **Administrar > Distribución rápida**, expanda **Imágenes maestras** a la derecha para ver el estado actual (como `Building image` o `Ready to customize`).

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 un estado `Ready to customize` (o un 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 **Administrar > Distribución rápida**, expanda **Imágenes maestras** a la derecha. Seleccione la imagen con la que quiere conectar.
2. Seleccione **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, seleccione **Encender**.
3. Inicie 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 seleccione **Finalizar compilación**. 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 **Administrar > Distribución rápida**, la imagen de la derecha indica cuántos catálogos y máquinas utilizan cada imagen.

> **Nota:**
>
> Después de finalizar una imagen, no podrá modificarla. Deberá crear otra imagen (si quiere, con 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

Citrix ejecuta pruebas de validación en la imagen importada. Asegúrese de que se cumplen los siguientes requisitos al preparar la imagen que importará a Citrix DaaS.

- **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:** Las máquinas virtuales de primera generación admiten la mayoría de los sistemas operativos invitados. Las máquinas virtuales de segunda generación admiten la mayoría de las versiones de 64 bits de Windows y las versiones más actuales de los sistemas operativos Linux.
- **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`

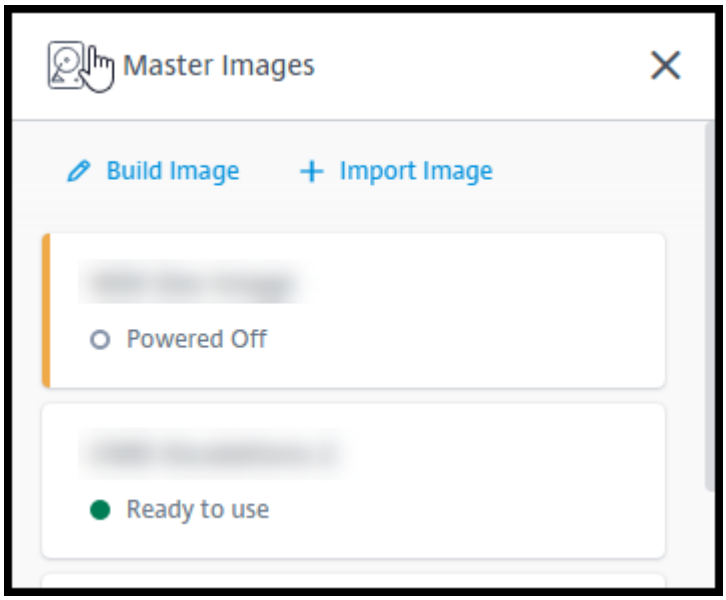
 

  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\ListOfDDCs`
  - `HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\FarmGUID`
  - `HKLM:\SOFTWARE\Policies\Citrix\VirtualDesktopAgent\FarmGUID`

- **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 Azure Virtual Machine Agent overview.

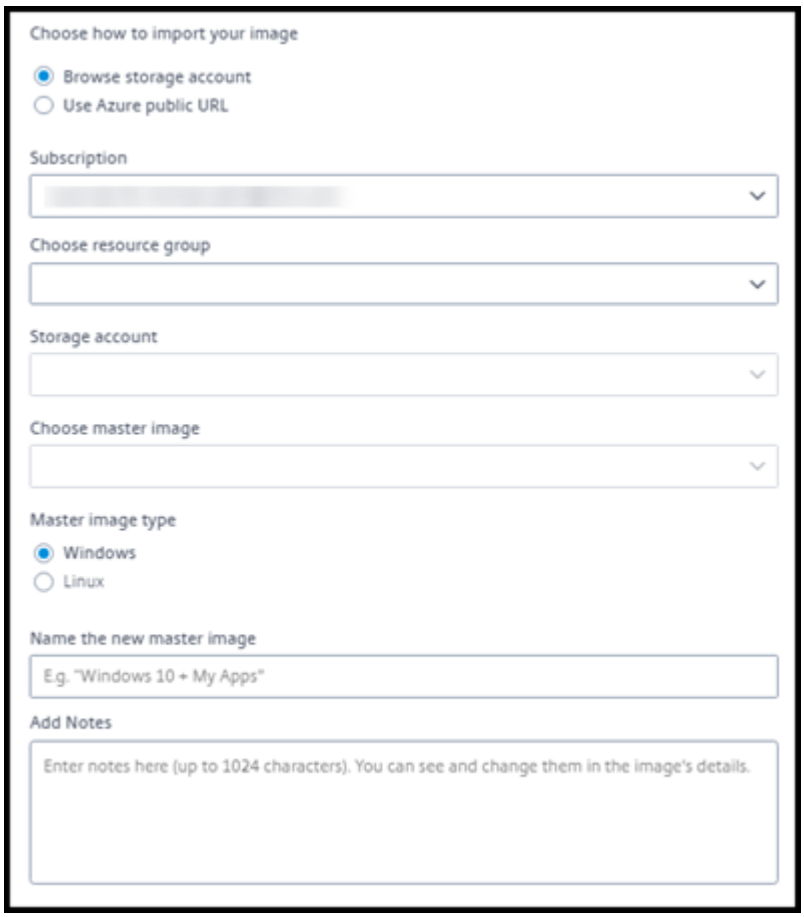
#### Importar la imagen con Distribución rápida

1. En **Administrar > Distribución rápida**, expanda **Imágenes maestras** a la derecha.




2. Seleccione **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 instrucciones, seleccione el enlace al documento Download a Windows VHD from Azure de Microsoft.

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, seleccione **Importar imagen**.

### Actualizar un catálogo de Distribución rápida con una nueva imagen

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

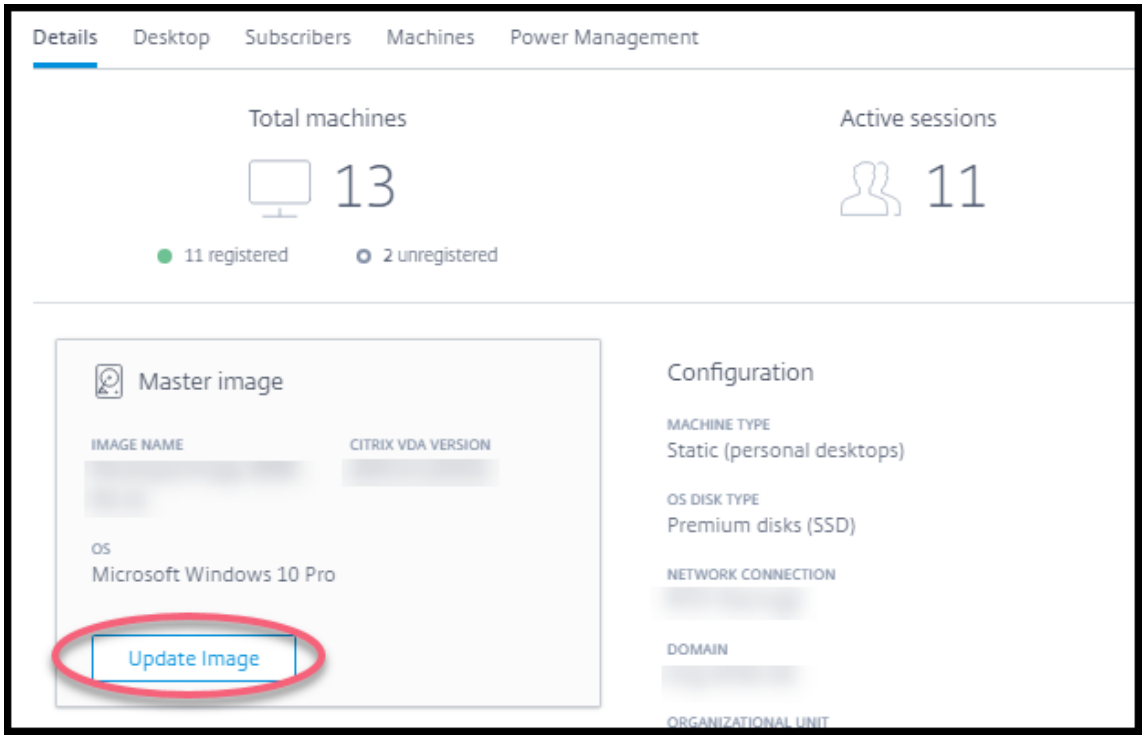
- En el caso de un catálogo aleatorio, todas las máquinas que se encuentran actualmente en el catálogo se actualizan con la imagen más reciente. Si agrega más escritorios a ese catálogo, se basan en la imagen más reciente.
- En el caso de un catálogo estático, las máquinas que se encuentran actualmente 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 **Administrar > Distribución rápida**, haga clic en cualquier parte de la entrada del catálogo.
2. En la ficha **Detalles**, seleccione **Actualizar imagen**.




3. Seleccione una imagen.
4. Para catálogos aleatorios o multisesión: Seleccione un intervalo de cierre de sesión. Una vez que Citrix DaaS finaliza el procesamiento inicial de imágenes, los suscriptores reciben una advertencia para guardar su trabajo y cerrar 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. Seleccione **Actualizar imagen**.

### Eliminar una imagen de Distribución rápida

1. En **Administrar > Distribución rápida**, expanda **Imágenes maestras** a la derecha.
2. Seleccione la imagen que quiere eliminar.
3. Seleccione **Eliminar imagen** en la parte inferior de la tarjeta. Confirme la eliminación.

### Instalar un VDA de Windows en una imagen

Siga el procedimiento que se indica a continuación al preparar una imagen de Windows que piense importar a Citrix DaaS.

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 bien, use un explorador web para ir a la página de descargas de Citrix DaaS.

   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 mediante MCS y, a continuación, seleccione **Siguiente**.
5. En la página **Componentes principales**, seleccione **Siguiente**.
6. En la página **Delivery Controller**, seleccione **Dejar que Machine Creation Services lo haga automáticamente** y, a continuación, seleccione **Siguiente**. Confirme la selección, si se le indica.
7. Deje la configuración predeterminada en las páginas **Componentes adicionales**, **Funciones** y **Firewall**, a menos que Citrix le indique lo contrario. Seleccione **Siguiente** en cada página.
8. En la página **Resumen**, seleccione **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 conectar, seleccione **Siguiente**.
10. Seleccione **Finish**. 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.

## Conexiones de red en Distribución rápida

May 17, 2024

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

## Introducción

En este artículo, se proporcionan detalles sobre cómo crear conexiones de red a los recursos corporativos cuando se utiliza una suscripción de Azure administrado por Citrix.

Al utilizar su propia suscripción de Azure administrado por el cliente, no es necesario crear una conexión de red.

Al crear un catálogo de Distribución rápida, indica si los usuarios acceden a ubicaciones y recursos de su red corporativa local desde sus escritorios y aplicaciones Citrix y cómo acceden. Al utilizar una conexión, debe crear la conexión antes de crear el catálogo.

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

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

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

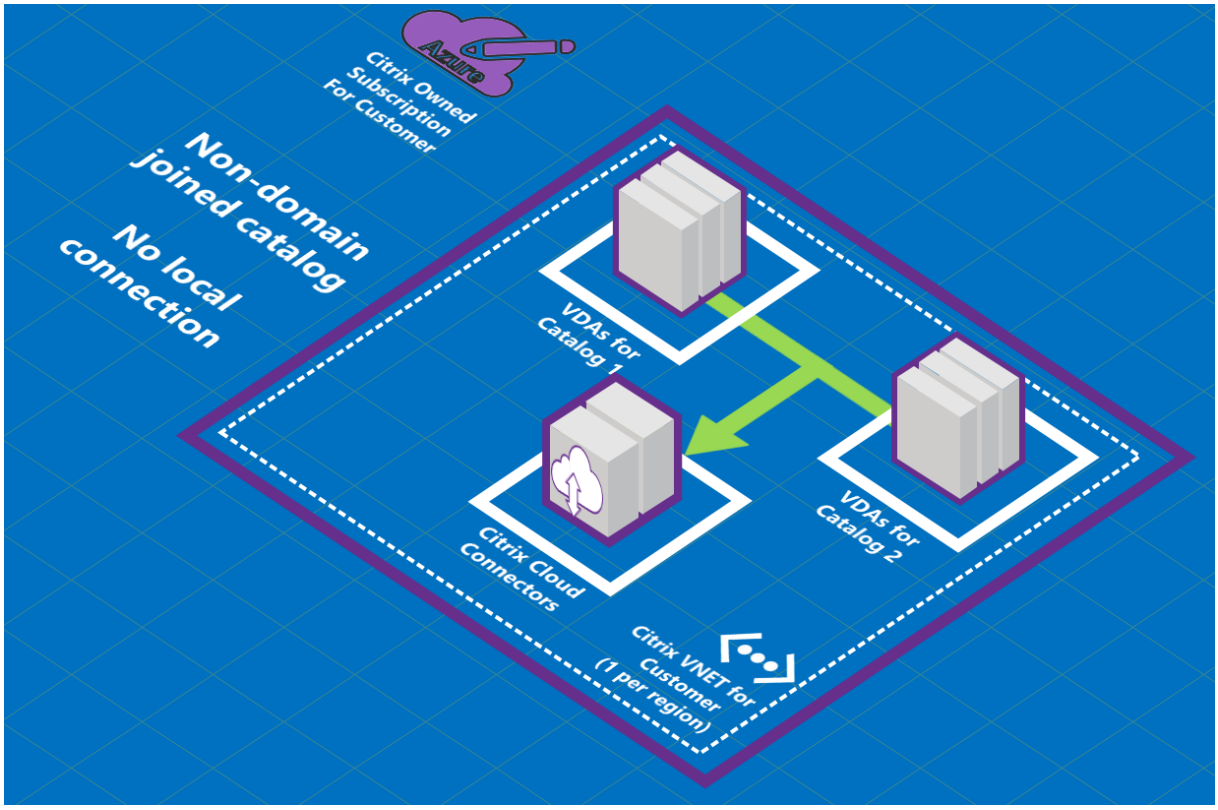
## Requisitos para todas las conexiones de red

- Al crear una conexión, debe tener entradas de servidor DNS válidas.
- Al utilizar DNS seguro o un proveedor de DNS tercero, debe agregar el intervalo de direcciones asignado para uso por parte de Citrix DaaS (antes llamado Citrix Virtual Apps and Desktops Service) a las direcciones IP del proveedor de DNS de 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.

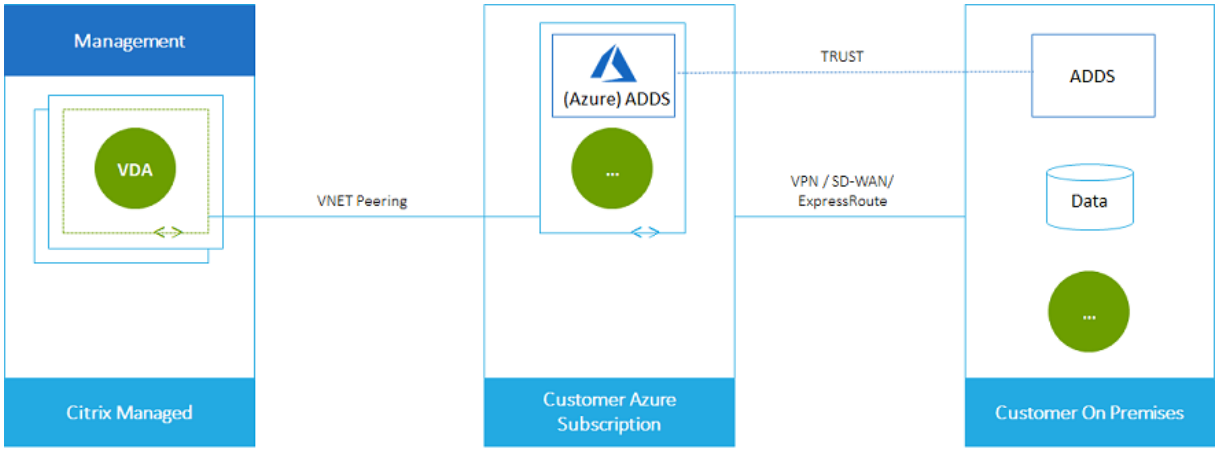
 




### Acerca de las conexiones de emparejamiento de redes virtuales de Azure

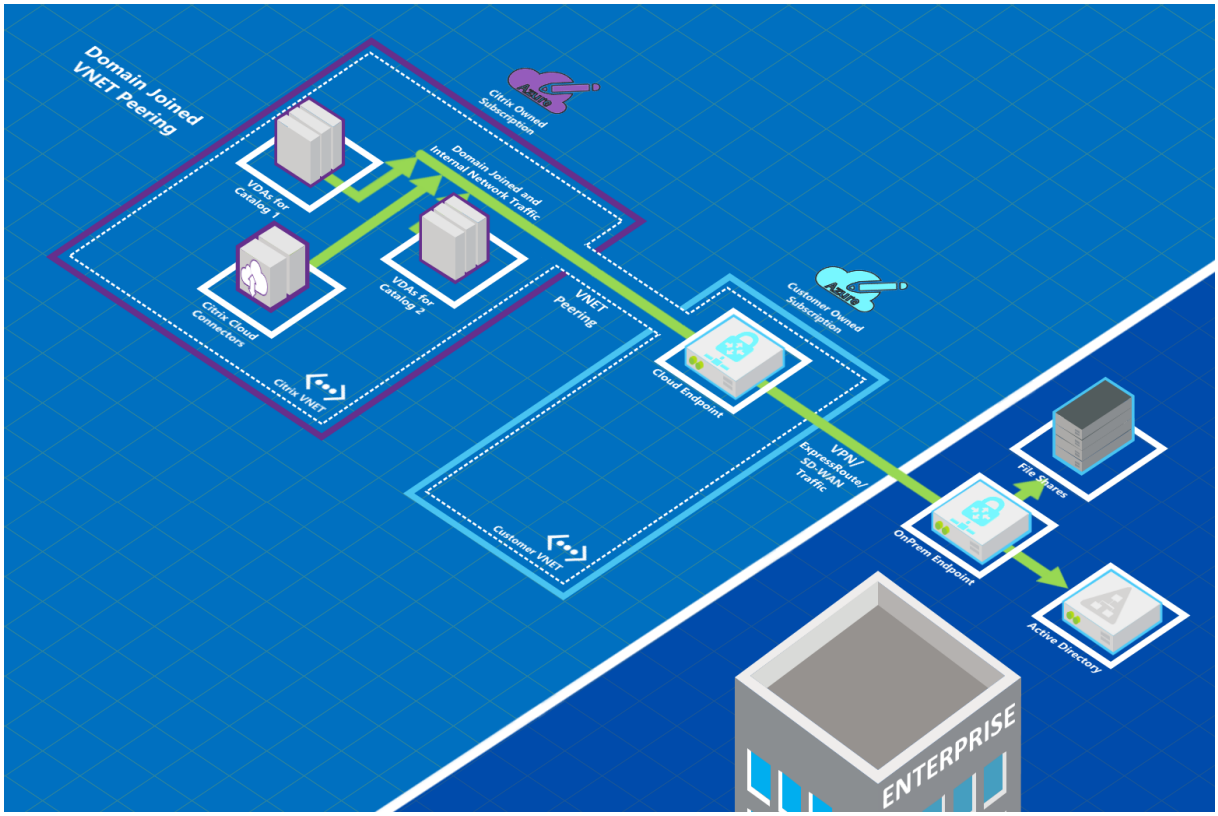
El emparejamiento de redes virtuales conecta sin problemas dos redes virtuales de Azure (VNet): la suya y la red virtual de Citrix DaaS. El emparejamiento también permite a los usuarios acceder a archivos y otros elementos de las redes locales.

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 (como servidores de archivos) uniéndose al dominio local cuando usted crea 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 el emparejamiento de redes virtuales de Azure antes de utilizarlo en este servicio.
> - 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 utilizar rutas personalizadas si hay redes a las que se prevé que accedan los recursos de Citrix DaaS, pero que no están conectadas directamente a través del emparejamiento de redes virtuales. 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 o un dispositivo de red, como Citrix SD-WAN, en su entorno de Citrix DaaS.
- Al agregar rutas personalizadas, debe actualizar las tablas de rutas de su empresa con la información de la red virtual de destino de Citrix DaaS para garantizar la conectividad de extremo a extremo.
- Las rutas personalizadas se muestran en Citrix DaaS 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 emparejamiento de redes virtuales de Azure o a las existentes en su entorno de Citrix DaaS. Cuando esté listo para utilizar rutas personalizadas con el emparejamiento de redes virtuales, consulte las siguientes secciones de este artículo:

- Para las rutas personalizadas con nuevos emparejamientos de redes virtuales de Azure: Crear una conexión de emparejamiento de redes virtuales de Azure
- Para rutas personalizadas con emparejamientos de redes virtuales de Azure existentes: Administrar rutas personalizadas para conexiones de emparejamiento de redes virtuales de Azure existentes

#### Requisitos y preparación del emparejamiento de redes virtuales de Azure

- Credenciales para el propietario de una suscripción de Azure. Debe ser una cuenta de Azure Active Directory. Este servicio no admite otros tipos de cuentas, como live.com o cuentas externas de Azure AD (en otro arrendatario).
- 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 características 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 for 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 intervalo de direcciones IP asignado a las máquinas virtuales de la red virtual interconectada de Citrix DaaS.

  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 red virtual de Azure tiene un espacio de direcciones 10.0.0.0 /16, cree la conexión de emparejamiento de redes virtuales en Citrix DaaS como algo de tipo 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.

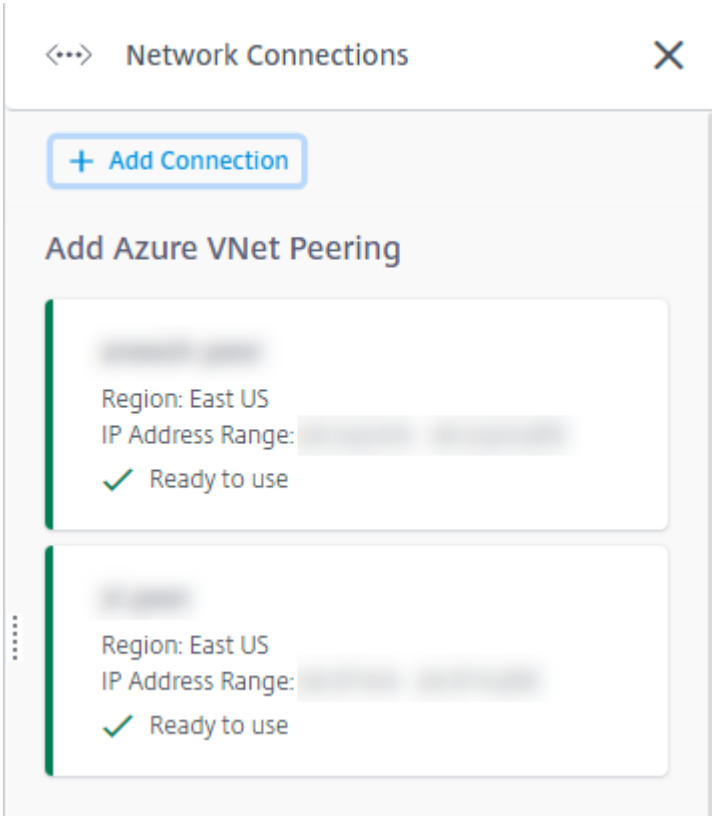
Para obtener más información sobre el emparejamiento de redes virtuales, consulte los siguientes artículos de Microsoft.

- Emparejamiento de redes virtuales
- ¿Qué es VPN Gateway?
- Crear una conexión de sitio a sitio en el portal de Azure
- Preguntas frecuentes sobre VPN Gateway (buscar "superposición")

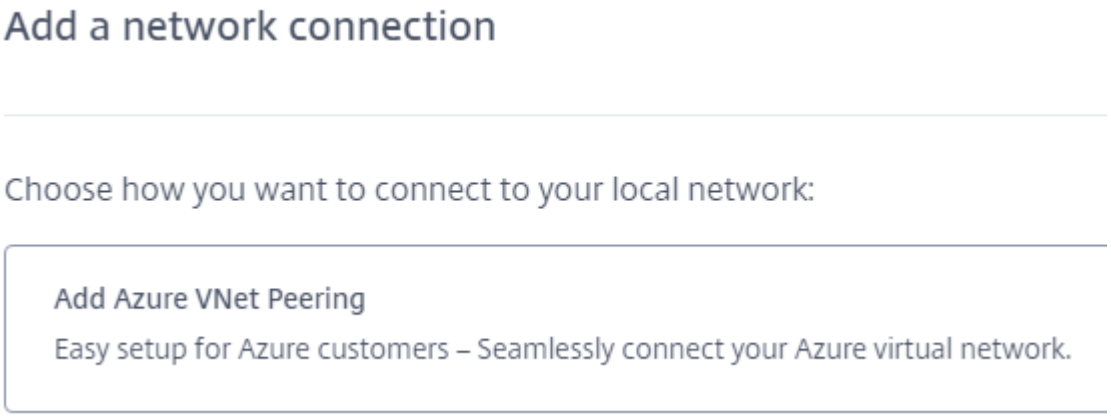
#### Crear una conexión de emparejamiento de redes virtuales de Azure

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha. Si ya ha configurado conexiones, aparecerán en la lista.

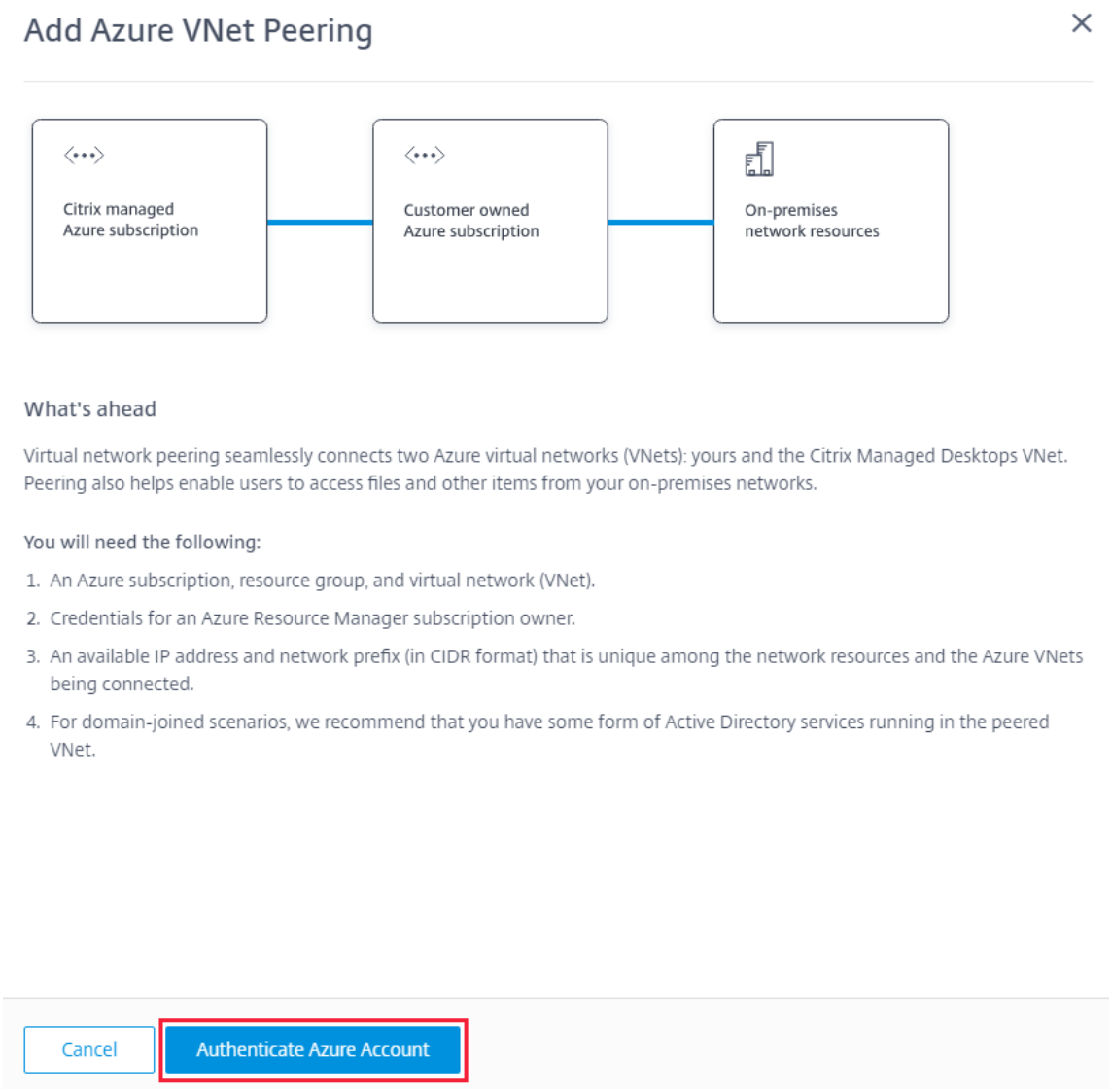



2. Seleccione **Agregar conexión**.
3. Haga clic en cualquier parte del cuadro **Agregar emparejamiento de redes virtuales de Azure**.



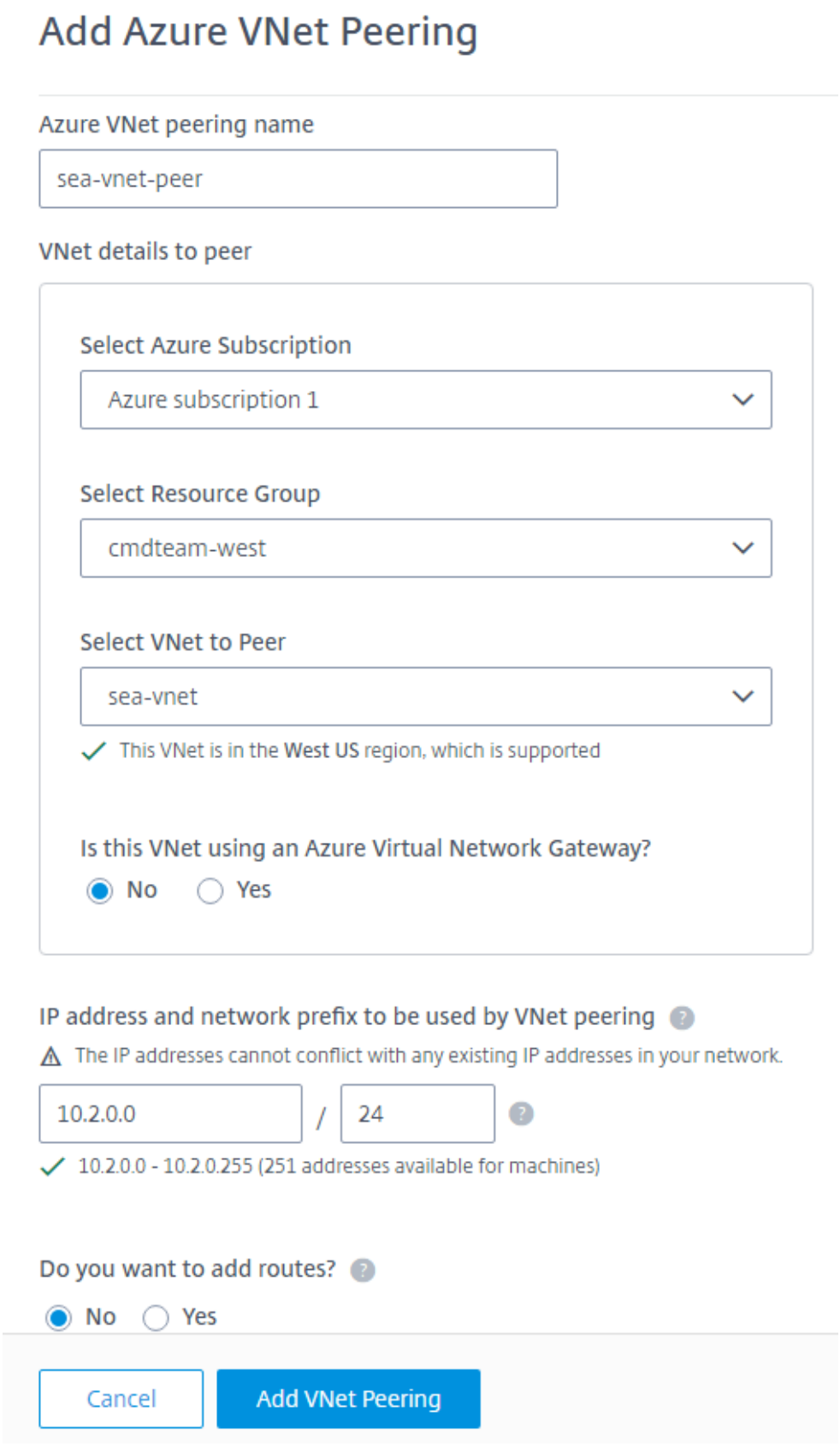

4. Seleccione **Autenticar cuenta de Azure**.




5. Citrix DaaS le dirige automáticamente a la página de inicio de sesión de Azure para que autentique 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 ha respondido **Sí** en el paso anterior (la red virtual 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 la inhabilita más adelante, deberá 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 de direcciones IP no se superponga a ninguna dirección que utilice en redes de Azure y locales.

    - Por ejemplo, si la red virtual de Azure tiene un espacio de direcciones 10.0.0.0 /16, cree la conexión de emparejamiento de redes virtuales en Citrix DaaS como algo de tipo 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 considera un intervalo de direcciones superpuesto.

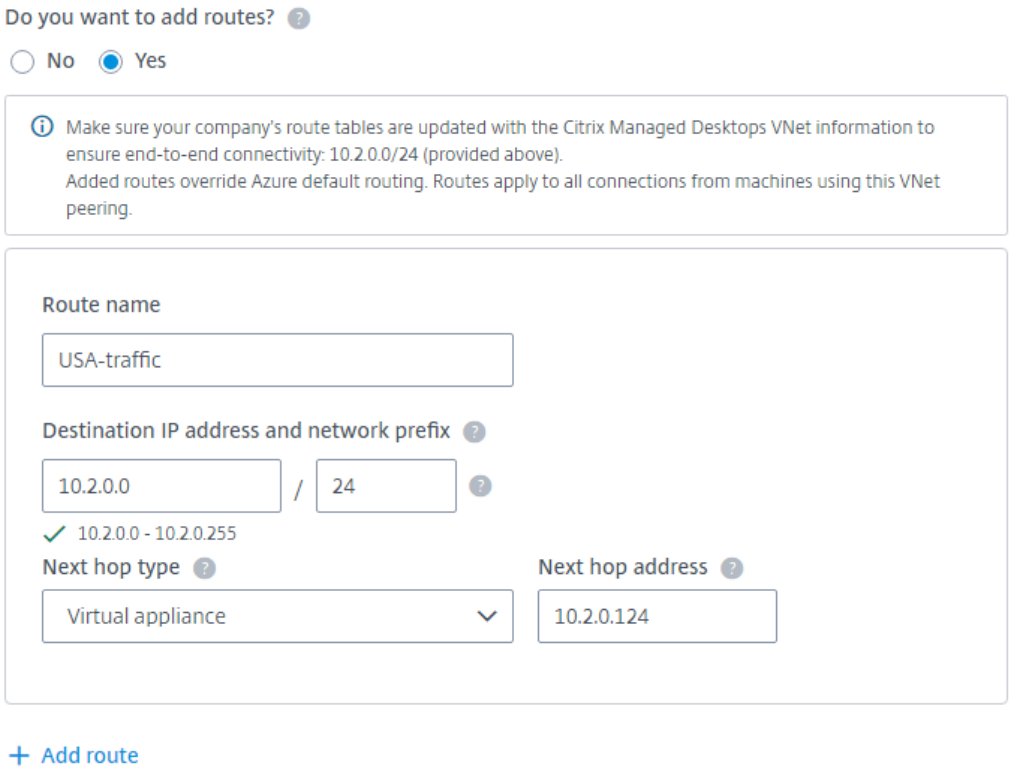
    Si las direcciones se superponen, es posible que la conexión de emparejamiento de redes virtuales no se cree correctamente. Tampoco funcionará correctamente para las tareas de administración del sitio.
11. Indique si desea agregar rutas personalizadas a la conexión de emparejamiento de redes virtuales. 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 redireccione el tráfico. Si selecciona **Dispositivo virtual**, introduzca la dirección IP interna del dispositivo.




Para obtener más información sobre los tipos de próximo salto, consulte la sección Rutas personalizadas del artículo de Microsoft *Enrutamiento del tráfico de redes virtuales*.

d) Para crear otra ruta personalizada para la conexión, seleccione **Agregar ruta**.

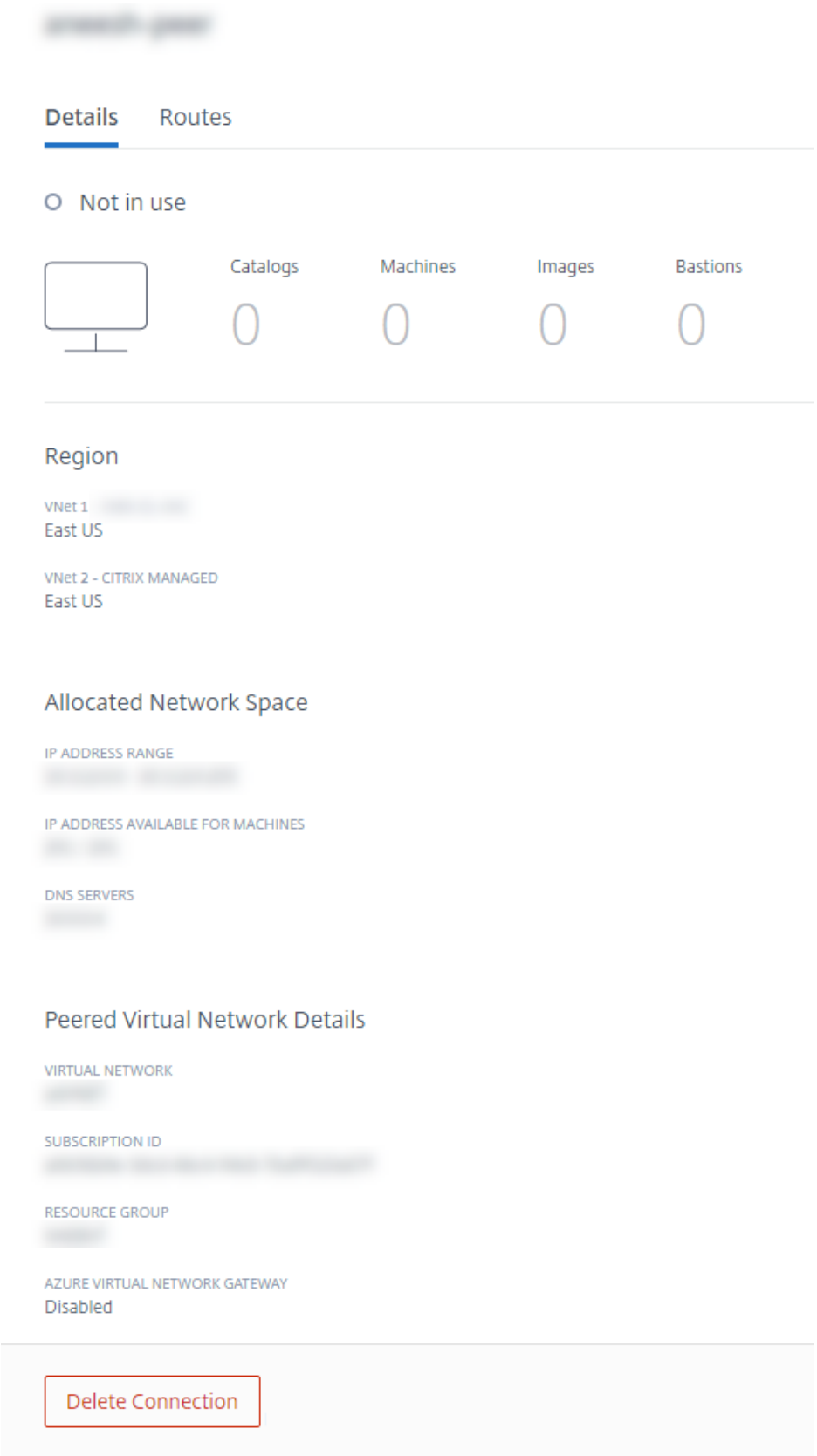
12. Seleccione **Agregar emparejamiento de redes virtuales**.

Una vez creada la conexión, aparece en **Conexiones de red > Pares de redes virtuales de Azure**, a la derecha del panel **Administrar > Distribución rápida**. 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 **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión de emparejamiento de redes virtuales de Azure que desea 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 emparejamiento de redes virtuales de Azure 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.

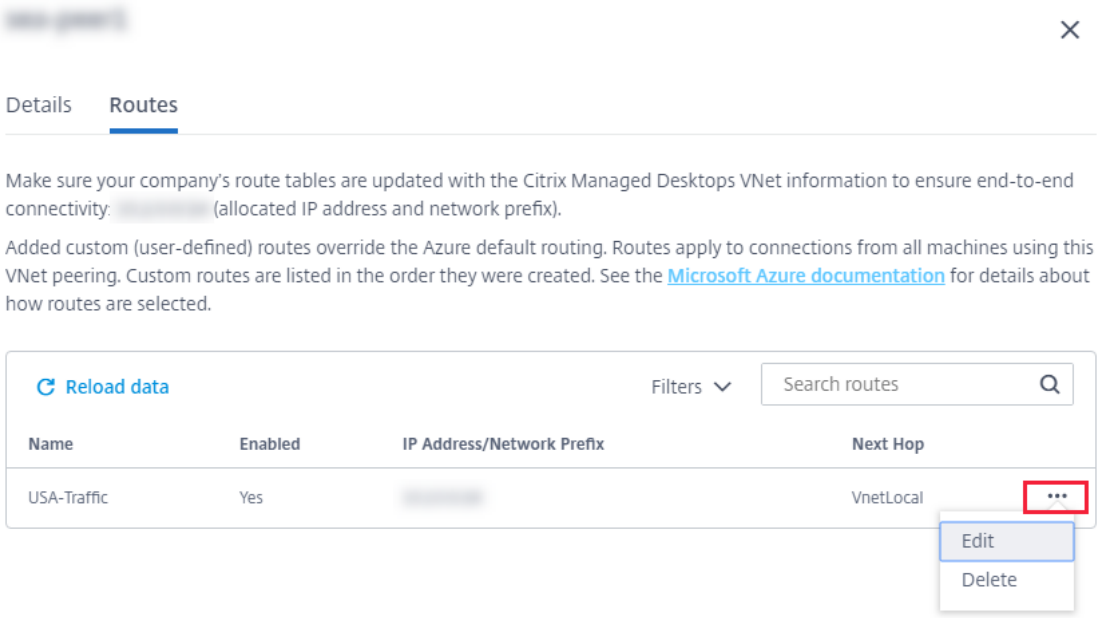
Para agregar una ruta personalizada:

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiere eliminar.
3. En los detalles de la conexión, seleccione **Rutas** y, a continuación, **Agregar ruta**.
4. 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.
5. Indique si quiere habilitar la ruta personalizada. De forma predeterminada, la ruta personalizada está habilitada.
6. Seleccione **Agregar ruta**.

Para modificar o inhabilitar una ruta personalizada:

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiere eliminar.
3. En los detalles de la conexión, seleccione **Rutas** y, a continuación, busque la ruta personalizada que quiere administrar.
4. En el menú de puntos suspensivos, seleccione **Modificar**.




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

Para eliminar una ruta personalizada:

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiere eliminar.
3. En los detalles de la conexión, seleccione **Rutas** y, a continuación, busque la ruta personalizada que quiere administrar.
4. En el menú de puntos suspensivos, seleccione **Eliminar**.
5. Seleccione **El hecho de eliminar rutas puede interrumpir sesiones activas** para aceptar el impacto que puede tener eliminar la ruta personalizada.
6. Seleccione **Eliminar ruta**.

### Eliminar una conexión de emparejamiento de redes virtuales de Azure

Antes de poder eliminar una conexión de emparejamiento de redes virtuales de Azure, quite los catálogos asociados a ella. Consulte Eliminar un catálogo.

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione la conexión que quiere eliminar.
3. En los detalles de la conexión, seleccione **Eliminar conexión**.

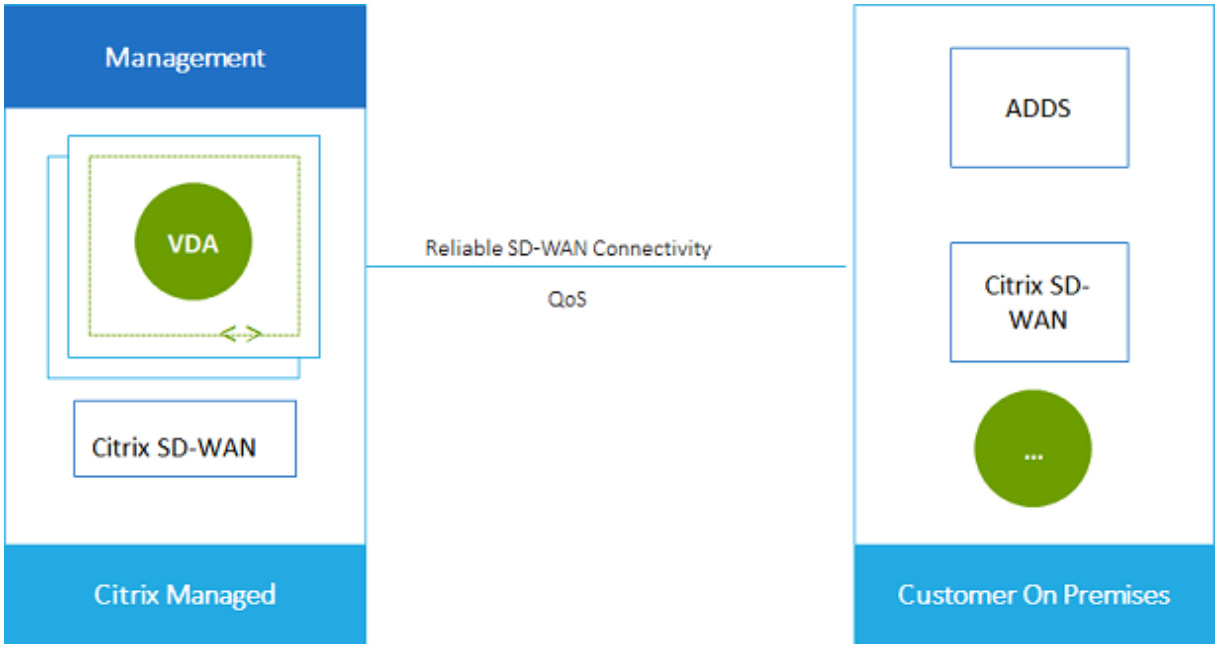
 

### Acerca de las conexiones SD-WAN

Citrix SD-WAN optimiza todas las conexiones de red que necesita Citrix DaaS. En colaboración con las tecnologías HDX, Citrix SD-WAN proporciona calidad de servicio y fiabilidad de conexión para el tráfico de Citrix DaaS fuera de banda e ICA. 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 de vídeos del lado del cliente desde 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.




### Preparación y requisitos de las conexiones SD-WAN

- Si no se cumplen los siguientes requisitos, la opción de conexión de red SD-WAN no estará disponible.

  - Derechos de uso del servicio Citrix Cloud: Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service) 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 la red virtual: Proporcione un espacio de direcciones CIDR disponible (dirección IP y prefijo de red) que sea exclusivo entre los recursos de red que se están conectando. Este es el intervalo de direcciones IP asignado a las máquinas virtuales de la red virtual de Citrix DaaS.

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

  - Por ejemplo, si la red tiene un espacio de direcciones 10.0.0.0 /16, cree la conexión en Citrix DaaS como algo de tipo 192.168.0.0 /24.
  - En este ejemplo, crear una conexión 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 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) 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 información detallada acerca de la configuración de SD-WAN, consulte Configuración de SD-WAN para la integración de Citrix DaaS.

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione **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 haya terminado de leer, seleccione **Iniciar la 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. Para obtener información sobre cómo evitar conflictos, consulte Preparación y requisitos de las conexiones SD-WAN.

6. Cuando haya terminado, seleccione **Crear sucursal**.
7. En la página siguiente se resume lo que debe buscar en el panel de mandos **Administrar > Distribución rápida** . Cuando haya terminado de leer, seleccione **Entendido**.
8. En **Administrar > Distribución rápida**, la nueva entrada SD-WAN en **Conexiones de red** muestra el progreso del proceso de configuración. Cuando la entrada se vuelva de color naranja con el mensaje `Awaiting activation by SD-WAN administrator`, notifique al administrador de SD-WAN Orchestrator.
9. Para obtener información sobre las tareas de administrador de SD-WAN Orchestrator, consulte la documentación del producto SD-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 `You can create catalogs using this connection`.

#### Ver detalles de conexión SD-WAN

1. En **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione **SD-WAN** si no es la única opción.
3. Seleccione la conexión que quiera 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 **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
2. Seleccione SD-WAN si no es la única opción.
3. Seleccione la conexión que quiere eliminar para expandir sus detalles.
4. En la ficha **Detalles**, seleccione **Eliminar conexión**.
5. Confirme la eliminación.

## Usuarios y autenticación en Distribución rápida

May 17, 2024

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

### Métodos de autenticación de usuarios

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

Distribución rápida 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:

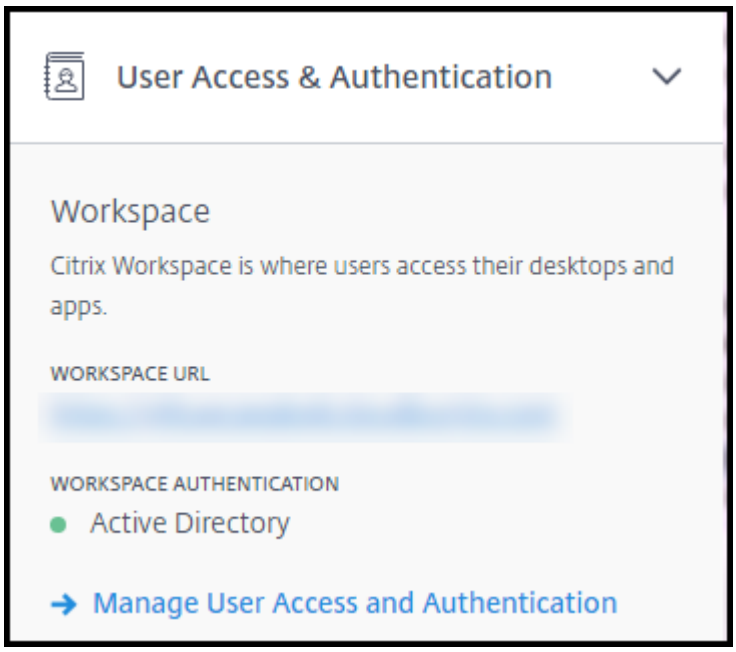
- Conéctese al método de autenticación de usuarios que quiera utilizar. (En Citrix Cloud, se "conecta"o "desconecta"de un método de autenticación.)
- En Citrix Cloud, configure la autenticación de Workspace para utilizar el método conectado.

> **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 configura automáticamente para utilizar Azure AD administrado para Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service). 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.

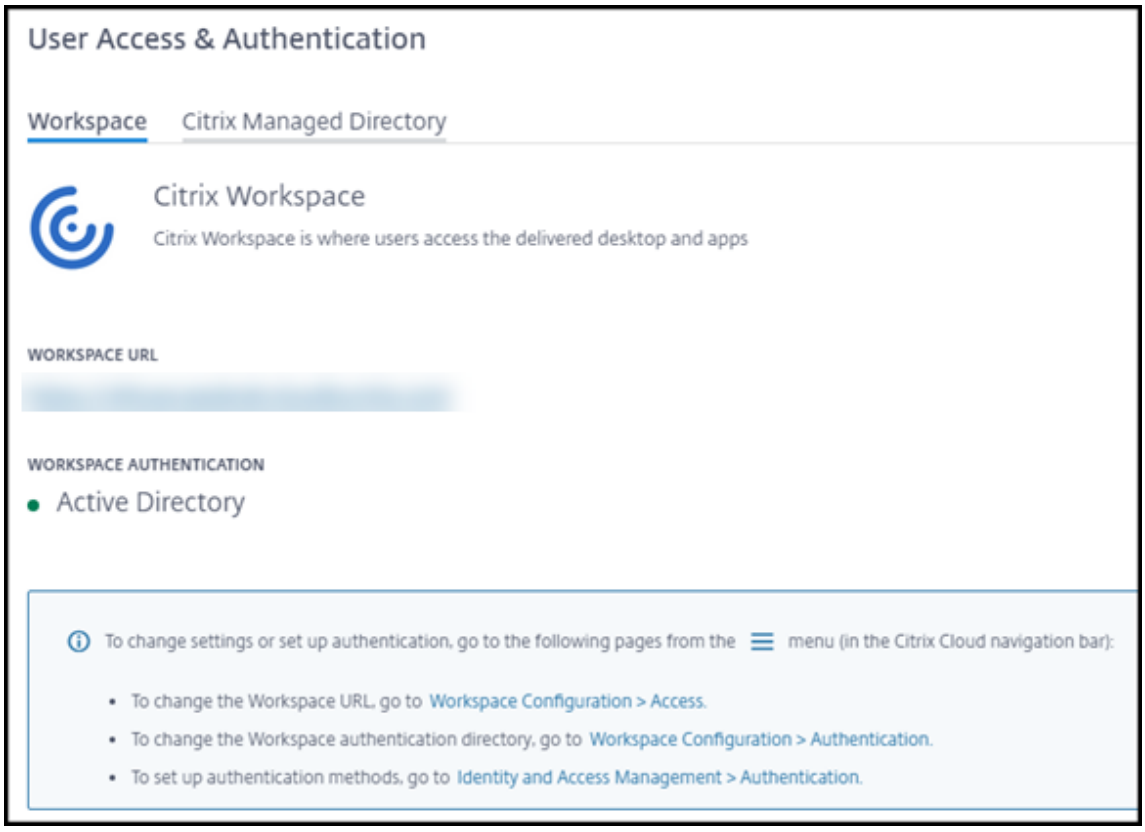
Para cambiar el método de autenticación:

1. En **Administrar > Distribución rápida**, seleccione **Acceso y autenticación de usuario** a la derecha.




2. Seleccione **Administrar el acceso y la autenticación de los 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.

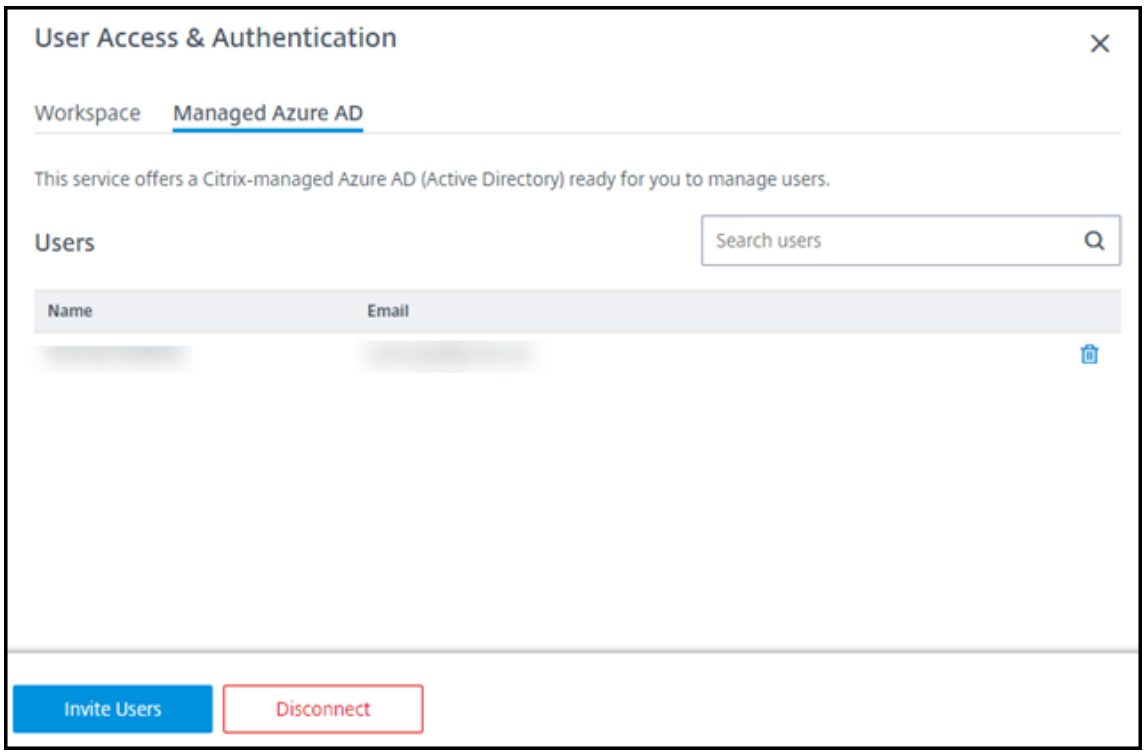
Debe proporcionar el nombre y las direcciones de correo electrónico de sus usuarios. A continuación, Citrix envía una invitación por correo electrónico a cada uno de ellos. El correo electrónico indica a los usuarios que seleccionen un enlace que los une Azure AD administrado por Citrix.

- 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.

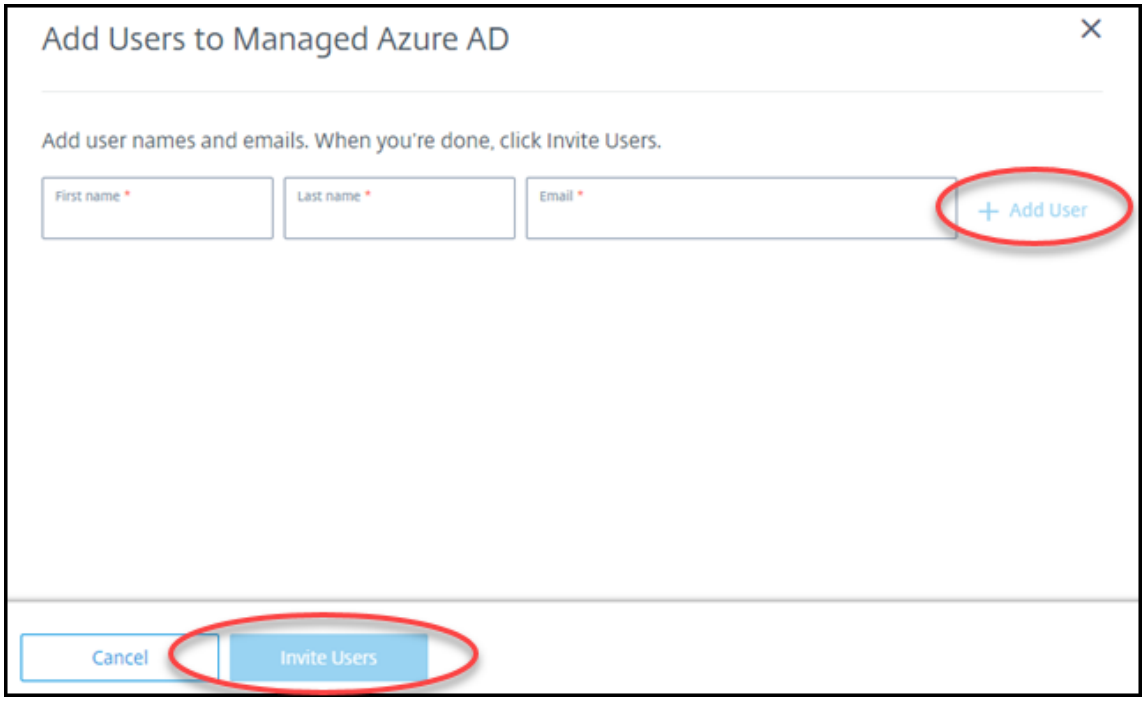
Para agregar e invitar usuarios a Azure AD administrado:

1. En **Administrar > Distribución rápida**, expanda **Acceso y autenticación de usuario** a la derecha. Seleccione **Administrar el acceso y la autenticación de los usuarios**.
2. Seleccione la ficha **Azure AD administrado**.
3. Seleccione **Invitar a usuarios**.




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




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

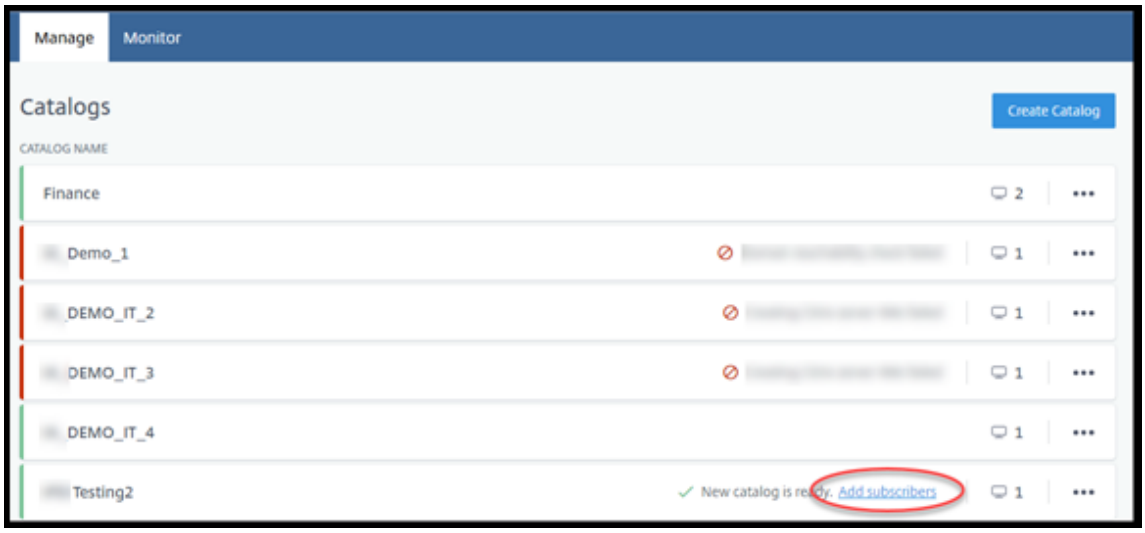
Para eliminar un usuario de Azure AD administrado, seleccione el icono de papelera situado junto al nombre del usuario que quiere eliminar del directorio. Confirme la eliminación.

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.

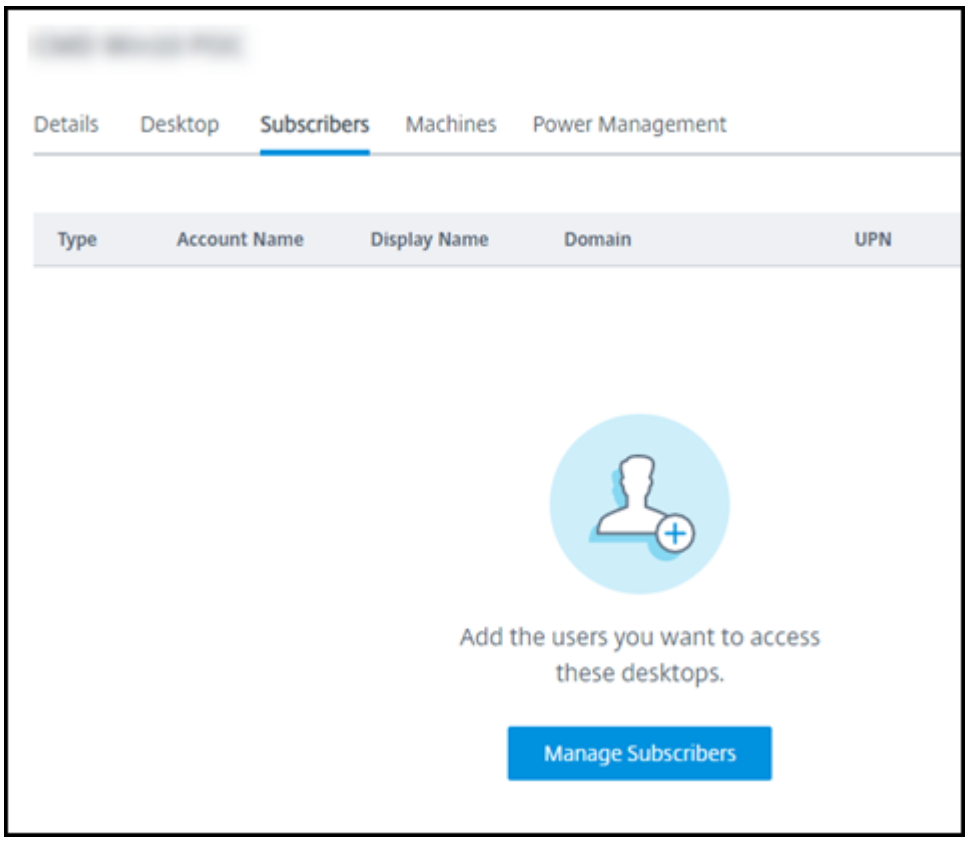
1. En **Administrar > Distribución rápida**, si no ha agregado ningún usuario a un catálogo, seleccione **Agregar suscriptores**.



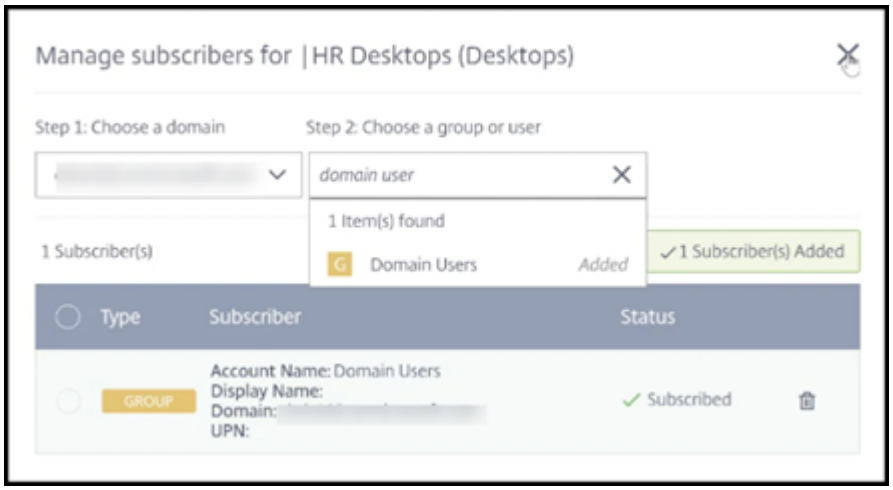

   Para agregar usuarios a un catálogo que ya tiene usuarios, haga clic en cualquier parte de la entrada del catálogo.

2. En la ficha **Suscriptores**, seleccione **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, seleccione la **X** en la esquina superior derecha.

Para quitar usuarios de un catálogo, siga los pasos 1 y 2. En el paso 3, seleccione el icono de papelera situado 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 los usuarios.

### Más información

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

## Acceso con Remote PC en Distribución rápida

August 28, 2023

### Introducción

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.

En este artículo se describe cómo crear una implementación de acceso con Remote PC mediante la interfaz de Distribución rápida. Para crear una implementación de acceso con Remote PC a través de la interfaz de Configuración completa, consulte Acceso con Remote PC.

#### 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 a Citrix DaaS.
    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. En **Administrar > Distribución rápida**:
    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 de acceso con Remote PC con Citrix Virtual Apps and Desktops, la funcionalidad Wake-on-LAN no está disponible en Citrix DaaS.

### 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.
- 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.
- Establezca la opción **Apagar** en la **acción al presionar el botón de encendido**.
- 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, al reacoplarlo, el VDA no pasa a usar la conexión por cable a menos que desconecte el adaptador inalámbrico. Algunos dispositivos ofrecen una funcionalidad integrada para desconectar el adaptador inalámbrico al establecerse una conexión por cable. 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 completamente 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 Workspace

- 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` impide la instalación de componentes adicionales. La opción `/includeadditional` especifica exactamente qué componentes adicionales quiere 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**.
3. Si aún no ha creado ningún catálogo, haga clic en **Empiece aquí** en la página de **bienvenida**.
4. Seleccione **Administrar > Distribución rápida**.
5. Seleccione **Crear catálogo**.
6. En la ficha **Acceso con Remote PC**, seleccione un método para asignar usuarios a máquinas.
7. Introduzca un nombre para el catálogo y seleccione la ubicación de recursos que ha creado.
8. Agregue máquinas.
9. Haga clic en **Crear catálogo**.
10. En la página **Se está creando su catálogo de acceso con Remote PC**, haga clic en **Listo**.
11. Aparecerá una entrada del nuevo catálogo en el panel de mandos **Administrar > Distribución rápida**.

    Una vez creado correctamente el catálogo, haga clic en uno de los enlaces a 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 > Distribución rápida** (haga clic en cualquier parte de

la entrada del catálogo).

- 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.

## Supervisar en Distribución rápida

May 13, 2022

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

Para acceder al panel de mandos **Supervisar**:

1. Inicie sesión en Citrix Cloud si aún no lo ha hecho. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
2. En el panel **Administrar > Distribución rápida**, seleccione 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 puede adaptar el periodo de tiempo: el último día, semana, mes o tres meses.

  Los recuentos de la parte superior de la pantalla indican el número total de máquinas, además del número de máquinas encendidas y apagadas. Pase el puntero sobre un valor para mostrar cuántos son de sesión única y cuántos 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 contiene información sobre los inicios de máquinas durante el último mes, seleccione **Actividad de inicios**. Un mensaje indica que la solicitud se está procesando. El informe se descarga automáticamente en la ubicación de descarga predeterminada de la máquina 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.

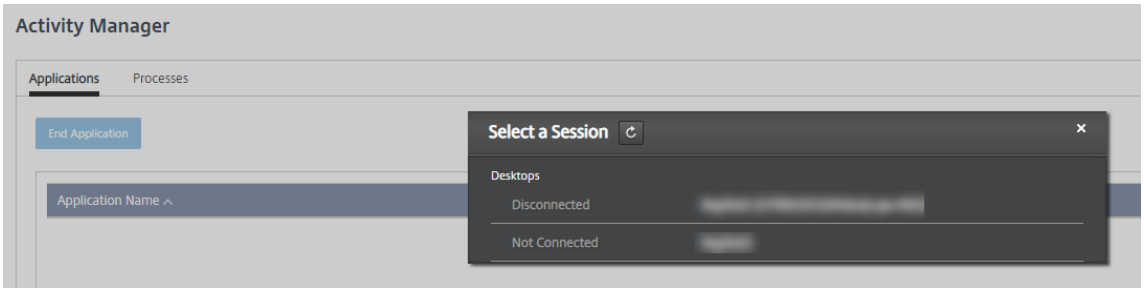
 

- Puede guardar los filtros que cree para reutilizarlos.

### Controlar las aplicaciones de un usuario

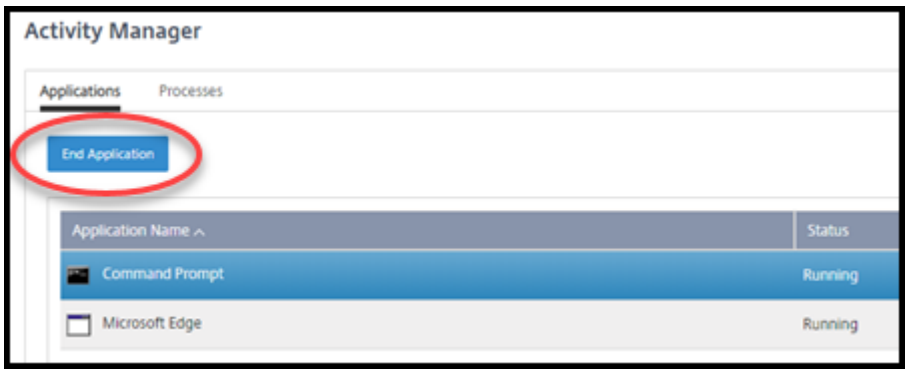
Puede mostrar y administrar las aplicaciones y procesos de un usuario que tenga una sesión en ejecución o un escritorio asignado.

1. En el panel **Supervisar** de Citrix DaaS, seleccione **Buscar** e introduzca el nombre del usuario (o los caracteres iniciales del nombre de usuario), el equipo o el dispositivo de punto final. En los resultados de búsqueda, seleccione el elemento que está buscando. (Para contraer el cuadro de búsqueda sin buscar, seleccione **Buscar** de nuevo).
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, seleccione la fila de la aplicación correspondiente y, a continuación, **Finalizar aplicación**.




4. Para finalizar un proceso, en la ficha **Procesos** del Administrador de actividades, seleccione la fila del proceso correspondiente y, a continuación, **Finalizar proceso**.
5. Para mostrar los detalles de la sesión, seleccione **Detalles** en la parte superior derecha. Para volver a la pantalla de aplicaciones y procesos, seleccione Administrador de actividades en la parte superior derecha.
6. Para controlar la sesión, seleccione **Control de sesión > Cerrar sesión** o **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 verificar esa conexión, compruebe el nombre de la 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.

El remedo solo se admite para los usuarios de máquinas unidas a un dominio. Para remedar una máquina que no esté unida a un dominio, deberá configurar una máquina de 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. En **Administrar > Distribución rápida > Supervisar**, vaya a la vista **Detalles del usuario**.
2. Seleccione la sesión del usuario y, a continuación, **Remedar** en la vista **Administrador de actividades** o el panel **Detalles de la sesión**.

### Remedar agentes Linux VDA

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

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 seleccione **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 seleccione **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.

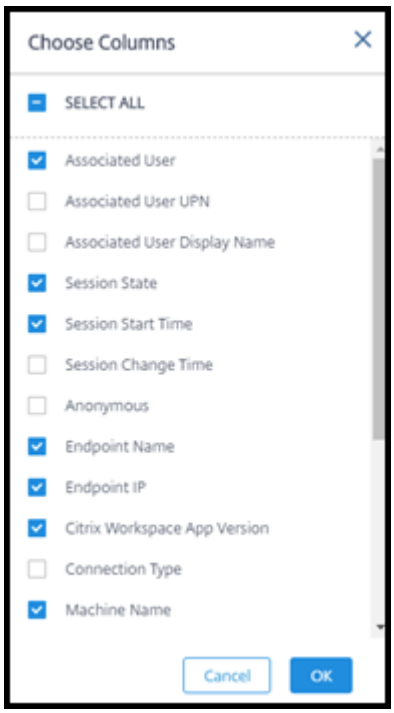
Además de ver las sesiones, puede desconectar una o más sesiones o cerrar las sesiones de los usuarios.

1. En **Administrar > Distribución rápida > Supervisar**, seleccione **Filtros**.


2. Seleccione la vista **Sesiones**.


3. Para adaptar la pantalla, seleccione **Elegir columnas** y, a continuación, las casillas de verificación de los elementos que quiere que aparezcan. Cuando haya terminado, seleccione **Aceptar**. La pantalla de sesiones se actualiza automáticamente.




4. Marque 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 información de una sesión, seleccione **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 de la máquina local.

### Máquinas de supervisión y control de la energía

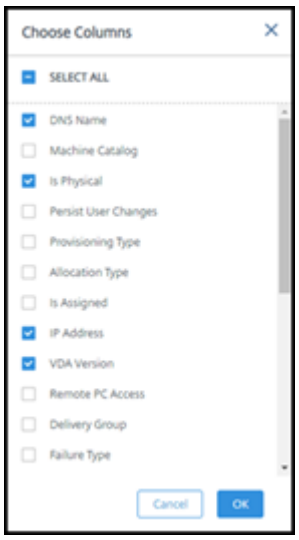
Las pantallas de la máquina se actualizan cada minuto.

1. En **Administrar > Distribución rápida > Supervisar**, seleccione **Filtros**.
2. Seleccione la vista **Máquinas**.

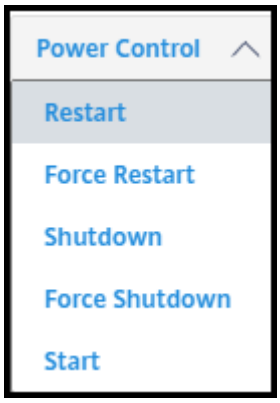
 


De forma predeterminada, la pantalla muestra las máquinas con SO de sesión única. Alternativamente, puede mostrar las máquinas multisesión.

3. Para adaptar la pantalla, seleccione **Elegir columnas** y, a continuación, las casillas de verificación de los elementos que quiere que aparezcan. Cuando haya terminado, seleccione **Aceptar**. La pantalla de las máquinas se actualiza automáticamente.




4. Para controlar la energía de las máquinas o ponerlas o sacarlas del modo de mantenimiento, marque la casilla de verificación situada a la izquierda de cada máquina que quiere controlar.
5. Para controlar la energía de las máquinas seleccionadas, seleccione **Control de energía** y seleccione una acción.




6. Para poner las máquinas seleccionadas en el modo de mantenimiento, o para sacarlas de este,

seleccione **Modo de mantenimiento > ACTIVADO** o **Modo de mantenimiento > DESACTIVADO**, respectivamente.

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 información de sesión, seleccione **Exportar** en la pantalla de máquinas. Un mensaje indica que la solicitud se está procesando. El informe se descarga automáticamente en la ubicación de descarga predeterminada de la máquina 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

## Solucionar problemas en Distribución rápida

April 14, 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. Por lo general, Citrix instala y actualiza los Cloud Connectors.

Opcionalmente, puede iniciar varias acciones de Cloud Connector y ubicación de recursos. Consulte:

- Acciones de ubicaciones de recursos
- Parámetros de ubicación de recursos al crear un catálogo

Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service) cuenta con herramientas de solución de problemas y compatibilidad que pueden ayudar a resolver problemas de configuración y comunicación con las máquinas que entregan los escritorios y las 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. En **Administrar > Distribución rápida**, expanda **Asistencia y Solución de problemas técnicos** 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. En **Administrar > Distribución rápida**, expanda **Asistencia y Solución de problemas técnicos** 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.

## Referencia de Distribución rápida

September 16, 2022

### Fichas de Catálogo en el panel Distribución rápida

En el panel **Administrar > Distribución rápida** de Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service), 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 máquina también están disponibles en la ficha **Supervisar** del panel Distribución rápida. 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 es aplicable a todas las implementaciones que contienen máquinas unidas a dominios. Puede ignorar esta sección si utiliza únicamente máquinas que no están unidas a un dominio.

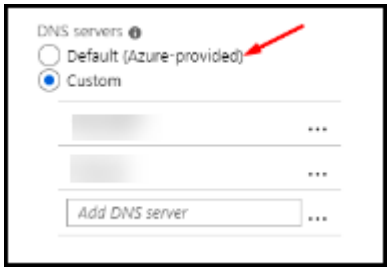
1. Antes de crear un catálogo unido a un dominio (o una conexión, si utiliza una suscripción a Azure administrado por Citrix), compruebe si tiene entradas de servidor DNS que puedan resolver nombres de dominio públicos y privados.

   Cuando Citrix DaaS 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. Este servicio no se puede utilizar con la configuración **Predeterminado (proporcionado 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 quiere utilizar con este servicio pueden 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 cambiarlas en este servicio.
- Cuando utiliza una suscripción a Azure administrado por Citrix, este servicio no sincroniza los cambios de dirección DNS realizados en Azure. Sin embargo, puede cambiar los parámetros de DNS para la conexión en este servicio.

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 este servicio

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 quitar una dirección de servidor DNS al crear una conexión, seleccione **Modificar servidores DNS** en la página **Agregar** *tipo de conexión*. O bien, si un mensaje indica que no se ha encontrado ninguna dirección de servidor DNS, seleccione **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 **Administrar > Distribución rápida**, expanda **Conexiones de red** a la derecha.
   b) Seleccione la conexión que quiere modificar.
   c) Seleccione **Modificar servidores DNS**.

3. Agregue, cambie o quite direcciones.

   a) Para agregar una dirección, seleccione **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 quitar una dirección, seleccione el icono de papelera situado junto a la entrada de dirección. No se pueden quitar todas las direcciones del servidor DNS. La conexión debe tener al menos una.

4. Cuando haya terminado, seleccione **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. Con el comando **Ejecutar**, inicie `gpedit.msc` para abrir el Editor de directivas de grupo.
4. En `User Configuration Citrix Policies > Unfiltered`, seleccione **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 desee 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.

Consulte los artículos de Referencia para configuraciones de directivas para obtener información sobre lo que está disponible. Todas las funciones de directivas están disponibles en la interfaz Configuración completa de Citrix DaaS.

### 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 Acceso con Remote PC, el usuario crea la ubicación de recursos y los Cloud Connectors.

En esta sección se describen las acciones disponibles después de crear una ubicación de recursos.

1. En **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha.
2. Seleccione 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. Este recuento no incluye las máquinas utilizadas con otros fines, como imágenes, Cloud Connectors o servidores de licencias de 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. Seleccione **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 haya terminado, seleccione **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, seleccione **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. Cuando haya terminado, seleccione **Guardar**.

#### Cambio de nombre

Introduzca el nuevo nombre de la ubicación de recursos. Seleccione **Save**.

#### 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 Citrix DaaS 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 de Citrix DaaS 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 **Administrar > Distribución rápida**, seleccione la tarjeta **General**. El valor **Consumo** indica cuánto consumo se ha utilizado en el mes natural en curso. Este valor incluye compromisos mensuales y por plazos.

Al seleccionar **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 sobre el uso, consulte Supervisar el uso activo y de licencias.

Opcionalmente, puede solicitar que las notificaciones aparezcan en el panel **Administrar > Distribución rápida** cuando el uso del consumo (compromiso mensual, por plazos o ambos) alcance un nivel específico. De forma predeterminada, las notificaciones están inhabilitadas.

1. En la ficha **Notificaciones**, seleccione **Modificar las preferencias de las 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. Seleccione **Save**.

Para inhabilitar las notificaciones, haga clic en el control deslizante para que la marca de verificación deje de aparecer y, a continuación, seleccione **Guardar**.

### Supervisar el uso de licencias de Citrix

Para ver la información sobre uso de licencias de Citrix, siga las instrucciones que se indican en Supervisar el uso activo y de licencias. 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 Configuración completa o Distribución rápida).
>
> Asegúrese de que tiene configurados los límites máximos de sesión para todos los catálogos antes de continuar.
>
> - En Distribución rápida, esa configuración se encuentra en la ficha **Detalles** de cada catálogo.
> - En Configuración completa, consulte Equilibrar la carga de las máquinas.

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 de Citrix DaaS.

- **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 calcula y, a continuación, asigna un índice de carga a 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 **Administrar > Distribución rápida**, expanda **General** a la derecha.
2. En **Parámetros globales**, seleccione **Ver todo**.
3. En la página **Parámetros globales**, en **Equilibrio de carga de catálogos multisesión**, elija el método de equilibrio de carga.
4. Seleccione **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. En **Administrar > Distribución rápida**, inicie el proceso de creación de catálogos proporcionando la información necesaria y, a continuación, seleccione **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 el panel **Administrar > Distribución rápida**, expanda **Suscripciones a la nube** a la derecha. 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 se encuentran 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. En **Administrar > Distribución rápida**, 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, abra un tíquet. Para ello, siga las instrucciones que se indican en Cómo obtener ayuda y asistencia técnica.

## Crear grupos de entrega

June 12, 2024

### Introducción

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. El grupo de entrega también puede especificar los usuarios que pueden usar esas máquinas y las aplicaciones y escritorios disponibles para esos usuarios.

Crear un grupo de entrega es el siguiente paso de la configuración de la implementación después de crear un catálogo de máquinas. Posteriormente, puede cambiar los parámetros iniciales del primer grupo de entrega y crear otros. Sin embargo, existen funciones y configuraciones que se pueden definir solo cuando se modifica un grupo de entrega, no cuando se crea.

Antes de crear un grupo de entrega:

- Consulte esta sección para obtener más información acerca de las decisiones que deberá tomar y la información que deberá facilitar.
- Compruebe que ha creado una conexión con el hipervisor, servicio de nube u otro recurso que aloja las máquinas.
- Compruebe que ha creado un catálogo de máquinas que contenga máquinas virtuales o físicas.

Para iniciar el asistente de creación de grupos de entrega:

1. Inicie sesión en Citrix Cloud. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**.
2. Seleccione **Administrar**.
3. Si este es el primer grupo de entrega que se ha creado, la consola le guiará a la selección correcta (por ejemplo, "Configure grupos de entrega para mostrarlos como servicios"). El asistente de creación de grupos de entrega se abre y le guiará por el proceso.
4. Si ya creó un grupo de entrega y quiere crear otro, siga estos pasos:

a) En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
b) Para organizar grupos de entrega mediante carpetas, cree carpetas en la carpeta **Delivery Groups** predeterminada. Para obtener más información, consulte Crear una carpeta de grupos.
c) Seleccione la carpeta en la que quiere crear el grupo y, a continuación, haga clic en **Crear grupo de entrega**. Se abre el asistente de creación de grupos.

El asistente le guiará a través de las páginas que se describen en las secciones siguientes. Es posible que las páginas del asistente varíen según las opciones que escoja.

### Paso 1. Máquinas

Seleccione un catálogo de máquinas y especifique la cantidad de máquinas que quiere usar de ese catálogo.

Información útil:

- Al menos una máquina debe permanecer sin uso en el catálogo de máquinas seleccionado.
- Se puede especificar un mismo catálogo en más de un grupo de entrega. Sin embargo, una máquina se puede utilizar en un solo grupo de entrega.
- Un grupo de entrega puede utilizar máquinas de más de un catálogo. Sin embargo, esos catálogos deben contener los mismos tipos de máquinas (SO multisesión, SO de sesión única o acceso con Remote PC). En otras palabras, no se pueden mezclar tipos de máquinas en un grupo de entrega. Del mismo modo, si la implementación contiene catálogos de máquinas Windows y Linux, un grupo de entrega puede contener máquinas de un tipo de sistema operativo, pero no ambos.
- Un grupo de entrega de MCS solo puede agregar un catálogo de tipo MCS.
- Citrix recomienda instalar o actualizar todos los VDA a la versión más reciente y, a continuación, **cambiar el nivel funcional** de los catálogos de máquinas y los grupos de entrega a medida que sea necesario. Al crear un grupo de entrega, si selecciona máquinas que tienen instaladas versiones diferentes de VDA, el grupo de entrega será compatible con la versión más antigua de VDA. Por ejemplo, si una de las máquinas que seleccione tiene instalada la versión 7.1 de VDA mientras que las demás máquinas tienen la versión más actual, todas las máquinas del grupo solo podrán usar las funciones que se admitían en la versión 7.1 de VDA. Eso significa que algunas funciones que requieran de versiones posteriores de VDA podrían no estar disponibles en ese grupo de entrega.
- Se realizan estas comprobaciones de compatibilidad:
  - MinimumFunctionalLevel debe ser compatible

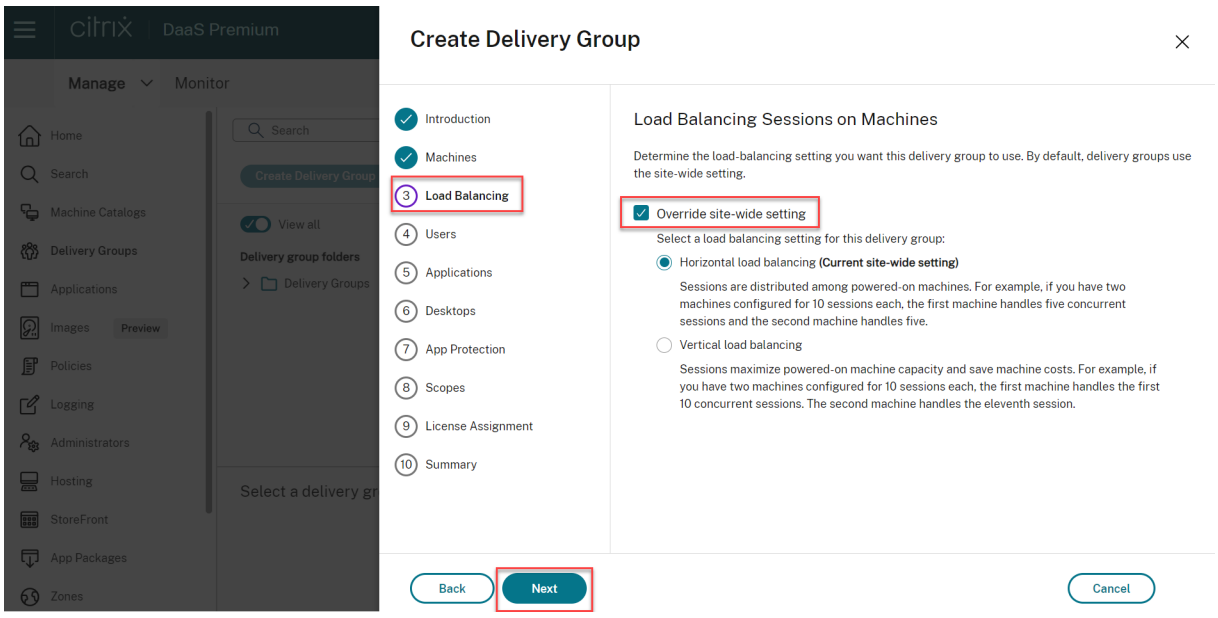
 

- SessionSupport debe ser compatible
- AllocationType debe ser compatible con SingleSession
- ProvisioningType debe ser compatible
- PersistChanges debe ser compatible con MCS y Citrix Provisioning
- El catálogo RemotePC solo es compatible con el catálogo RemotePC
- Comprobación relacionada con AppDisk

### Paso 2. Equilibrio de carga (Technical Preview)

Para configurar los parámetros de equilibrio de carga al crear un grupo de entrega:

1. Inicie sesión en DaaS Premium.
2. En el panel de navegación de la izquierda, haga clic en **Grupos de entrega**.
3. En la página **Grupos de entrega**, haga clic en **Crear grupo de entrega**.
4. En el asistente de **Crear grupo de entrega**, haga clic en **Siguiente**. Se abre el asistente de **Máquina**.
5. En el asistente de **Máquinas**, seleccione un catálogo de máquinas y haga clic en **Siguiente**. Se abre el asistente de **Equilibrio de carga**.
6. En el asistente de **Equilibrio de carga**, seleccione la casilla de verificación **Supeditar la configuración al nivel del sitio**.
7. Seleccione la opción **Equilibrio de carga horizontal** o **Equilibrio de carga vertical** según sea necesario y haga clic en **Siguiente**.

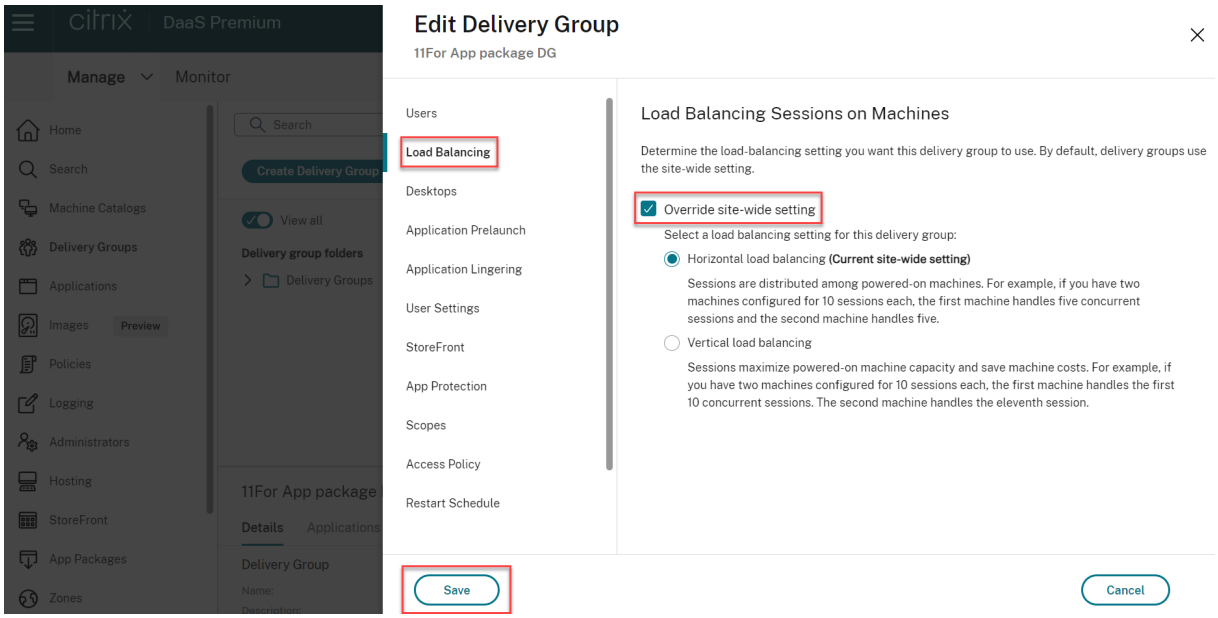



Para configurar los parámetros de equilibrio de carga al modificar un grupo de entrega existente:

1. Inicie sesión en DaaS Premium.

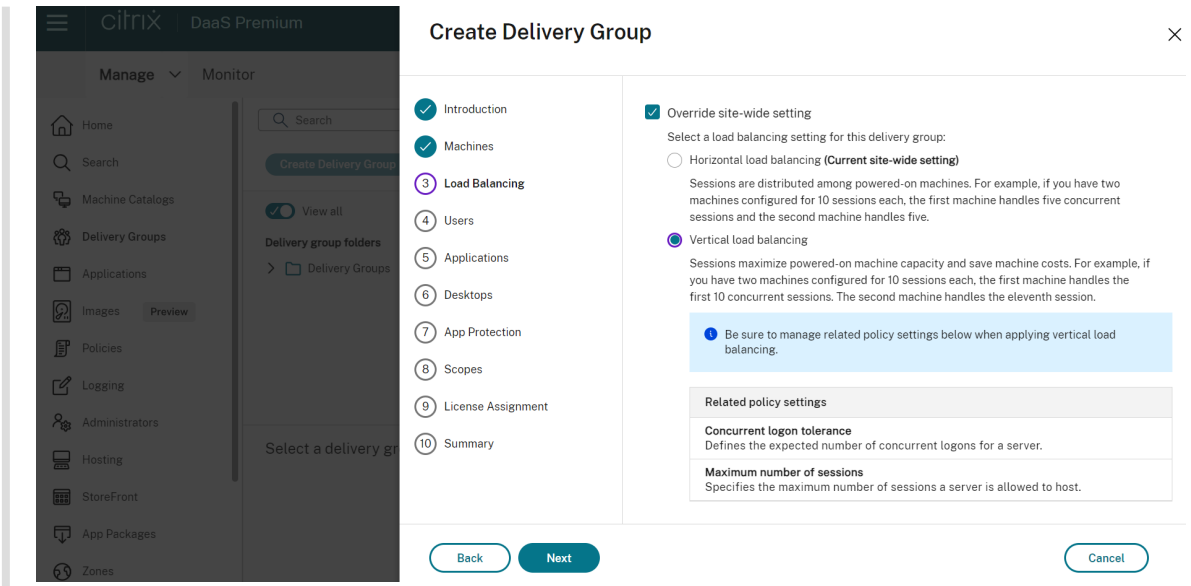
 

2. En el panel de navegación de la izquierda, haga clic en **Grupos de entrega**.
3. Seleccione un **grupo de entrega** de la lista y haga clic en **Modificar**. Se abre el asistente de **Modificar grupo de entrega**.
4. En la página **Modificar grupo de entrega**, haga clic en **Equilibrio de carga**.
5. Selecciona la casilla **Supeditar la configuración al nivel del sitio**.
6. Seleccione la opción **Equilibrio de carga horizontal** o **Equilibrio de carga vertical** según sea necesario y haga clic en **Guardar**.




> **Nota:**
>
> Cuando se aplique el parámetro Equilibrio de carga vertical, asegúrese de que las directivas **Tolerancia de inicios de sesión simultáneos** y **Número máximo de sesiones** estén configuradas correctamente.




Para obtener más información sobre el equilibrio de carga a nivel de sitio y de grupo de entrega, consulte Equilibrar la carga de las máquinas.

### Paso 3. Tipo de entrega

Esta página solo aparece si ha seleccionado un catálogo que contiene máquinas estáticas (asignadas) con SO de sesión única. Elija **Aplicaciones** o **Escritorios**. No se puede habilitar ambas opciones.

Si ha seleccionado máquinas de un catálogo de máquinas aleatorias (agrupadas) de SO de sesión única o SO multisesión, se entiende que el tipo de entrega serán aplicaciones y escritorios. Puede entregar aplicaciones, escritorios, o ambos.

### Paso 4. AppDisks

Puede ignorar esta página. Seleccione **Siguiente.**

### Paso 5. Usuarios

Especifique los usuarios y los grupos de usuarios que pueden utilizar las aplicaciones y los escritorios del grupo de entrega.

#### Dónde se especifican las listas de usuarios

Las listas de usuarios se especifican al crear o modificar lo siguiente:

- Una lista de acceso de usuarios a una implementación, que no se configura desde esta consola. La regla predeterminada de la directiva que rige los derechos a las aplicaciones incluye a todos los usuarios. Consulte los cmdlets `BrokerAppEntitlementPolicyRule` del SDK de PowerShell para obtener más información.
- Grupos de entrega.
- Aplicaciones.

> **Nota:**
>
> Al especificar una lista de usuarios, puede seleccionar cuentas de usuario de cualquiera de estos proveedores de identidades a los que está conectada su cuenta de Citrix Cloud: Active Directory, Azure Active Directory (Microsoft Entra ID) u Okta.

La lista de usuarios que pueden acceder a una aplicación se forma al cruzar las listas de usuarios indicadas arriba.

#### Usuarios autenticados y no autenticados

Hay dos tipos de usuarios: los autenticados y los no autenticados (también llamados anónimos). Puede configurar uno o ambos tipos en un grupo de entrega.

- **Autenticado:** Para acceder a aplicaciones y escritorios, los usuarios y miembros del grupo cuyo nombre especifique deben introducir credenciales (como la tarjeta inteligente o el nombre de usuario y contraseña) en StoreFront o la aplicación Citrix Workspace. Para grupos de entrega que contengan máquinas de SO de sesión única, puede importar más tarde los datos de usuario (una lista de usuarios), al modificar el grupo de entrega.
- **No autenticado (anónimo):** Para grupos de entrega que contienen máquinas de SO multisesión, puede permitir a los usuarios acceder a sus aplicaciones y escritorios sin presentar credenciales a StoreFront o la aplicación Citrix Workspace. Por ejemplo: en máquinas quiosco, es posible que la aplicación requiera credenciales, mientras que el portal de acceso o las herramientas de Citrix no las requieran. Se crea un grupo de usuarios anónimos al instalar el primer Delivery Controller.

  Para conceder acceso a usuarios no autenticados, cada máquina del grupo de entrega debe tener instalado un VDA con SO multisesión. Cuando los usuarios no autenticados están habilitados, se debe disponer de un almacén de StoreFront no autenticado.

  Las cuentas de usuarios no autenticados se crean a demanda cuando se inicia una sesión. El nombre que reciben es AnonXYZ, donde XYZ es un valor único de tres dígitos.

  Las sesiones de usuarios no autenticados tienen un valor predeterminado de tiempo de inactividad de 10 minutos, y se cierran automáticamente cuando el cliente se desconecta. No se

admiten funciones como la reconexión, la itinerancia entre clientes y el control del espacio de trabajo.

En la siguiente tabla, se describen las opciones de la página **Usuarios**:

| Habilitar acceso para | ¿Agregar o asignar usuarios y grupos de usuarios? | ¿Marcar la casilla "Dar acceso a usuarios no autenticados"? |
|---|---|---|
| Solo usuarios autenticados | Sí | No |
| Solo usuarios no autenticados | No | Sí |
| Usuarios autenticados y no autenticados | Sí | Sí |

#### Restringir el acceso de usuarios o grupos

También puede restringir el uso de un grupo de entrega al agregar usuarios o grupos de usuarios a la **lista de permitidos**. Solo los usuarios de la **lista de permitidos** pueden acceder a las aplicaciones y escritorios del grupo de entrega. Igualmente, para agregar usuarios y grupos de usuarios a una lista de bloqueados, haga clic en **Agregar lista de bloqueados**, lo que impide que los usuarios usen las aplicaciones y los escritorios del grupo de entrega seleccionado. Una lista de bloqueados solo tiene sentido cuando se usa para bloquear a usuarios de la lista de permitidos.

### Paso 6. Aplicaciones

Información útil:

- Puede agregar aplicaciones empaquetadas a los grupos de entrega *estáticos de sesión única* y a los de *acceso con Remote PC*. Los paquetes que contienen esas aplicaciones se montan automáticamente cada vez que los usuarios inician sesión en sus escritorios o equipos remotos.
- De forma predeterminada, las nuevas aplicaciones que agregue se colocan en una carpeta denominada Aplicaciones. Puede especificar otra carpeta. Para obtener información detallada, consulte el artículo Aplicaciones.
- Puede cambiar las propiedades de una aplicación cuando la agregue a un grupo de entrega o más tarde. Para obtener información detallada, consulte el artículo Aplicaciones.
- Si intenta agregar una aplicación y ya existe una con el mismo nombre en la carpeta, se le pedirá cambiar el nombre de la aplicación que está agregando. Si rechaza la solicitud, la aplicación se agregará con un sufijo que hará su nombre único en la carpeta de aplicaciones.
- Al agregar una aplicación a más de un grupo de entrega, puede producirse un problema de visibilidad si no tiene permiso para ver la aplicación en todos esos grupos de entrega. En tales

casos, consulte a un administrador con más permisos o amplíe el ámbito para incluir todos los grupos de entrega a los que se haya agregado la aplicación.
- Si publica dos aplicaciones con el mismo nombre para los mismos usuarios, cambie la propiedad Nombre de la aplicación (para el usuario). De lo contrario, los usuarios ven nombres duplicados en la aplicación Citrix Workspace.

Seleccione el menú **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina creada a partir de la imagen en el catálogo de máquinas seleccionado. Al seleccionar este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, seleccione **Aceptar**.
- **Manualmente:** Se trata de las aplicaciones que se encuentran en la implementación o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Una vez introducida esta información, seleccione **Aceptar**.
- **Existentes:** Se trata de aplicaciones agregadas anteriormente a la implementación, existentes posiblemente en otro grupo de entrega. Al seleccionar este origen, se abre una nueva página con una lista de las aplicaciones detectadas; seleccione las que quiera agregar y, a continuación, seleccione **Aceptar**.
- **Paquetes de aplicaciones:** aplicaciones en paquetes de aplicaciones en formato App-V, MSIX, de conexión de aplicaciones MSIX o FlexApp. Al seleccionar este origen, se abre la página **Agregar aplicaciones desde paquetes**. Seleccione un origen del paquete de aplicaciones, en la pantalla resultante seleccione las aplicaciones que quiere agregar y después seleccione **Aceptar**

  > **Nota:**
  >
  > Para publicar aplicaciones en formato MSIX o de conexión de aplicaciones MSIX, el nivel funcional del grupo de entrega debe ser 2106 o posterior. Para las aplicaciones FlexApp, el nivel funcional debe ser 2206 o posterior. Cuando no se cumple un requisito de nivel funcional, las opciones correspondientes de la lista desplegable **Origen del paquete de aplicaciones** se muestran atenuadas.

- **Grupo de aplicaciones:** grupos de aplicaciones que existen en la implementación.

Si una aplicación o su origen no están disponibles o no son válidos, no serán visibles o no se podrán seleccionar. Por ejemplo, el origen **Existentes** no está disponible si no hay aplicaciones que se hayan agregado a la implementación. O bien, una aplicación podría no ser compatible con el tipo de sesiones admitidas en las máquinas del catálogo seleccionado.

### Paso 7. App Protection

La siguiente información complementa el artículo App Protection de la documentación de Citrix Virtual Apps and Desktops. Para utilizar App Protection en una implementación de Citrix DaaS, siga las instrucciones generales de ese artículo y tenga en cuenta los detalles siguientes.

- Debe tener una suscripción válida a Citrix Cloud y derechos de uso válidos con relación a la función de App Protection. Para adquirir la función de App Protection, puede ponerse en contacto con su representante de ventas de Citrix.
- App Protection requiere confianza en XML. Para habilitar la confianza en XML, vaya a **Parámetros > Habilitar confianza en XML**.
- En cuanto a la protección contra la captura de pantalla:
  - En Windows y macOS, solo la ventana del contenido protegido está en blanco. App Protection está activa cuando una ventana protegida no está minimizada.
  - En Linux, toda la captura aparece vacía. App Protection está activa tanto si una ventana protegida está minimizada como si no.

### Paso 8. Escritorios (o reglas de asignación de escritorios)

El título de esta página depende del catálogo de máquinas que haya elegido anteriormente en el asistente:

- Si eligió un catálogo que contiene máquinas agrupadas, esta página se llamará **Escritorios**.
- Si eligió un catálogo que contiene máquinas asignadas y especificó "Escritorios"en la página **Tipo de entrega**, esta página se llamará **Reglas de asignación de escritorio**.
- Si eligió un catálogo que contiene máquinas asignadas y especificó "Aplicaciones"en la página **Tipo de entrega**, esta página se llamará **Aplicaciones**.

Seleccione **Add**. En el cuadro de diálogo:

- En los campos **Nombre simplificado** y **Descripción**, escriba la información que se verá en la aplicación Citrix Workspace.
- Para agregar una restricción por etiquetas a un escritorio, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú.
- Con los botones de opción, puede hacer lo siguiente:
  - **Permitir usar un escritorio a todos los usuarios con acceso a este grupo de entrega.** Todos los usuarios del grupo de entrega pueden iniciar escritorios (para grupos con máquinas agrupadas) o se les puede asignar una máquina cuando inicien escritorios (para grupos con máquinas asignadas).

  - Para **restringir el uso de escritorios**, agregue usuarios y grupos de usuarios a la **lista de permitidos**. Solo los usuarios de la **lista de permitidos** pueden acceder a escritorios. Igualmente, para agregar usuarios y grupos de usuarios a una lista de bloqueados, haga clic en **Agregar lista de bloqueados**, lo que impide que los usuarios usen los escritorios del grupo de entrega seleccionado. Una lista de bloqueados solo tiene sentido cuando se usa para bloquear a usuarios de la lista de permitidos.

- Si el grupo contiene máquinas asignadas, especifique la cantidad máxima de escritorios por usuario. Este debe ser un valor de uno o más.
- Habilite o inhabilite el escritorio (para máquinas agrupadas) o la regla de asignación de escritorios (para máquinas asignadas). Al inhabilitar un escritorio, se detiene la entrega del escritorio. Al inhabilitar una regla de asignación de escritorios, se detiene la asignación automática de escritorios a los usuarios.
- Cuando haya finalizado con el cuadro de diálogo, seleccione **Aceptar**.

### Paso 9. Asignación de licencias

Determine qué licencia quiere que utilice el grupo de entrega. De forma predeterminada, el grupo de entrega usa la licencia del sitio. Para obtener más información, consulte Licencias de varios tipos.

### Paso 10: Configuración de la caché de host local

Este parámetro solo está visible para los grupos de entrega que contienen máquinas agrupadas de sesión única con administración de energía.

De forma predeterminada, esas máquinas no están disponibles en el modo de caché de host local (LHC) debido a los riesgos de exposición de los datos. Para cambiar el comportamiento predeterminado y hacer que estén disponibles para las conexiones de nuevos usuarios en el modo LHC, seleccione **Mantener los recursos disponibles**.

Como alternativa, puede cambiar el comportamiento predeterminado mediante comandos de PowerShell. Para obtener más información, consulte Compatibilidad con aplicaciones y escritorios.

> **Importante:**
>
> Habilitar el acceso a máquinas agrupadas de sesión única con administración de energía puede provocar que los datos y los cambios de las sesiones de usuario anteriores estén presentes en las sesiones posteriores.

### Paso 11. Resumen

Escriba un nombre para el grupo de entrega. También puede indicar una descripción (si quiere), que aparece en la aplicación Workspace y en la interfaz de administración de Configuración completa.

Revise la información de resumen y, a continuación, seleccione **Finalizar**. Si no ha seleccionado ninguna aplicación ni ha especificado escritorios a entregar, se le preguntará si quiere continuar.

### Más información

- Administrar grupos de entrega
- Aplicaciones

## Administrar grupos de entrega

June 12, 2024

### Introducción

Este artículo describe los procedimientos para la administración de los grupos de entrega desde la consola de administración. Además de cambiar los parámetros especificados en el momento de crear el grupo, puede configurar otros parámetros que no estaban disponibles al crear el grupo de entrega.

Los procedimientos se organizan por categorías: general, usuarios, máquinas y sesiones. Algunas tareas abarcan más de una categoría. Por ejemplo, "Impedir que los usuarios se conecten a una máquina"se describe en la categoría de máquinas, pero también afecta a los usuarios. Por lo tanto, si no puede encontrar una tarea en una categoría, compruebe otra categoría relacionada.

Hay otros artículos que también contienen información relacionada:

- Aplicaciones contiene información sobre cómo administrar aplicaciones en los grupos de entrega.
- La administración de grupos de entrega requiere permisos correspondientes al rol integrado de Administrador de grupos de entrega. Para obtener más información, consulte Administración delegada.

## General

- Ver detalles del grupo
- Cambiar el método de entrega
- Cambiar direcciones de StoreFront
- Cambiar el nivel funcional
- Administrar grupos de entrega de acceso con Remote PC
- Cambiar la licencia de un grupo de entrega
- Organizar grupos de entrega mediante carpetas
- Administrar App Protection

### Ver detalles del grupo

1. Use la función de búsqueda para localizar un grupo de entrega específico. Para obtener instrucciones, consulte Buscar instancias.
2. En los resultados de la búsqueda, seleccione un grupo según sea necesario.
3. Consulte la siguiente tabla para ver las descripciones de las columnas del grupo.
4. Haga clic en una ficha del panel de detalles inferior para obtener más información sobre este grupo.

| Columna | Descripción |
|---|---|
| Grupo de entrega | El nombre del grupo y el tipo de sesión. Los tipos de sesión incluyen sistemas operativos de sesión única y sistemas operativos multisesión. |
| Entregando | El tipo de recursos que entrega este grupo. Los valores posibles incluyen Aplicaciones, Escritorios y Aplicaciones y escritorios. Aparece "Asignación de máquina estática"si el grupo de entrega está formado por máquinas dedicadas. |
| Sesión en uso | La cantidad de máquinas que están configuradas y la cantidad de máquinas que están en estado desconectado. |
| Recuento asignado | La cantidad de máquinas del catálogo asignadas a un grupo de entrega. |
| Carpeta | La ubicación del grupo en el árbol de **grupos de entrega**. Muestra el nombre de la carpeta en la que se encuentra el grupo (incluida la barra invertida al final) o − si el grupo está en el nivel raíz. |

### Cambiar el tipo de entrega de un grupo de entrega

El tipo de entrega indica lo que puede entregar el grupo: aplicaciones, escritorios o ambos.

Antes de cambiar un tipo **aplicaciones** al tipo **Escritorios**, elimine todas las aplicaciones del grupo.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Tipo de entrega**, seleccione el tipo de entrega que quiere.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

### Cambiar direcciones de StoreFront

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **StoreFront**, indique si especificará una dirección de servidor de StoreFront más adelante (**Manualmente**) o seleccione **Agregar** para especificar los servidores de StoreFront que quiere utilizar (**Automáticamente**).
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

También puede seleccionar **StoreFront** en el panel de la izquierda de la consola para especificar las direcciones del servidor de StoreFront.

### Cambiar el nivel funcional

Cambie el nivel funcional del grupo de entrega después de actualizar la versión de los VDA de sus máquinas y los catálogos de máquinas que contienen las máquinas utilizadas en el grupo de entrega.

Antes de comenzar:

- Si utiliza Citrix Provisioning (antes Provisioning Services), debe actualizar la versión de VDA en la consola de Citrix Provisioning.
- Inicie las máquinas que contienen el VDA actualizado para que puedan registrarse en Citrix DaaS. Este proceso indica a la consola los elementos del grupo de entrega que deben cambiarse.
- Si debe seguir mediante versiones anteriores de VDA, es posible que las funciones más recientes del producto no estén disponibles. Para obtener más información, consulte la documentación de la actualización de versiones.

Para cambiar el nivel funcional de un grupo de entrega:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Cambiar nivel funcional** en la barra de acciones. La acción **Cambiar el nivel funcional** solo aparece si se detectan los VDA actualizados.

La pantalla le indica qué máquinas, si las hay, no se pueden cambiar al nivel funcional y por qué. A continuación, puede cancelar la acción del cambio, resolver los problemas de la máquina y realizar el cambio de nuevo.

Una vez finalizado el cambio, puede revertir las máquinas a sus estados anteriores. Seleccione el grupo de entrega y, a continuación, seleccione **Deshacer cambio de nivel funcional** en la barra de acciones.

#### Administrar grupos de entrega de acceso con Remote PC

Si una máquina del catálogo de acceso con Remote PC no está asignada a ningún usuario, se asigna temporalmente una máquina a un grupo de entrega asociado a ese catálogo de máquinas. Esta asignación temporal permite que la máquina se asigne más tarde a un usuario.

La asociación de grupo de entrega a catálogo de máquinas tiene un valor prioritario. La prioridad determina a qué grupo de entrega se asigna la máquina cuando esta se registra en el sistema o cuando un usuario necesita que se le asigne una máquina: cuanto menor sea el valor, mayor será la prioridad. Si un catálogo de máquinas de acceso con Remote PC tiene varias asignaciones de grupos de entrega, el software selecciona la de mayor prioridad. Use el SDK de PowerShell para configurar este valor de prioridad.

Nada más crearse, los catálogos de máquinas de acceso con Remote PC se asocian a un grupo de entrega. Esta asociación significa que las cuentas de máquina o unidades organizativas que se agreguen al catálogo de máquinas más adelante se pueden agregar al grupo de entrega. Esta asociación se puede activar o desactivar.

Para agregar o quitar una asociación de catálogo de máquinas de acceso con Remote PC a un grupo de entrega:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de acceso con Remote PC.
3. En la sección **Detalles**, seleccione la ficha **Catálogos de máquinas** y, a continuación, seleccione un catálogo de acceso con Remote PC.
4. Para agregar o restaurar una asociación, seleccione **Agregar escritorios**. Para quitar una asociación, seleccione **Quitar asociación**.

### Cambiar la licencia de un grupo de entrega

Para cambiar los derechos de licencia de un grupo de entrega, siga estos pasos:

1. Seleccione **Grupos de entrega** en el panel de navegación.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de acciones.
3. En la página **Asignación de licencias**, seleccione la licencia que quiere que utilice el grupo.
4. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta. También puede hacer clic en **Guardar** para aplicar los cambios y cerrar la ventana.

Para obtener más información sobre los derechos de nivel de grupo de entrega, consulte Licencias de varios tipos.

### Organizar grupos de entrega mediante carpetas

Puede crear carpetas para organizar grupos de entrega y simplificar el acceso a estos.

**Roles obligatorios** De forma predeterminada, debe tener uno de estos roles integrado para crear y administrar carpetas de grupos de entrega: administrador de la nube, administrador total o administrador de grupos de entrega. Si es necesario, puede personalizar roles para crear y administrar carpetas de grupos de entrega. Para obtener más información, consulte Permisos requeridos.

**Crear una carpeta de grupos de entrega** Antes de empezar, planifique cómo organizar los grupos de entrega. Se deben tener en cuenta las siguientes cuestiones:

- Puede anidar carpetas en hasta cinco niveles (excluyendo la carpeta raíz predeterminada).
- Una carpeta puede contener grupos de entrega y subcarpetas.
- Todos los nodos de **Configuración completa** (como los nodos **Catálogos de máquinas**, **Aplicaciones** y **Grupos de entrega**) comparten un árbol de carpetas en el back-end. Para evitar conflictos de nombres con otros nodos al cambiar el nombre de las carpetas o moverlas, le recomendamos que asigne nombres diferentes a las carpetas de primer nivel de los distintos nodos.

Para crear una carpeta de grupos de entrega, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione **Crear carpeta** en la barra de **acciones**.
3. Introduzca un nombre para la nueva carpeta y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Si crea una carpeta en una ubicación no deseada, puede arrastrarla a la ubicación correcta.

#### Mover un grupo de entrega

Puede mover un grupo de entrega de una carpeta a otra. Estos son los pasos detallados:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Puede ver grupos por carpeta. También puede activar **Ver todo** por encima de la jerarquía de carpetas para ver todos los grupos a la vez.
3. Haga clic con el botón secundario en un grupo y, a continuación, seleccione **Mover grupos de entrega**.
4. Seleccione la carpeta a la que quiere mover el grupo y, a continuación, haga clic en **Listo**.

> **Sugerencia:**
>
> Puede arrastrar un grupo a una carpeta.

#### Administrar carpetas de grupos de entrega

Puede eliminar, cambiar el nombre y mover las carpetas de grupos de entrega.

Tenga en cuenta que solo puede eliminar una carpeta si ni sus subcarpetas contienen grupos de entrega.

Para administrar una carpeta, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. En la jerarquía de carpetas, seleccione una carpeta y, a continuación, seleccione una acción en la barra de **acciones**:
   - Para cambiar el nombre de la carpeta, seleccione **Cambiar nombre de carpeta**.
   - Para eliminar la carpeta, seleccione **Eliminar carpeta**.
   - Para mover la carpeta, seleccione **Mover carpeta**.
3. Siga las instrucciones que aparecen en pantalla para completar los pasos restantes.

**Permisos requeridos** En esta tabla, se enumeran los permisos necesarios para realizar acciones en carpetas de grupos de entrega.

| Acción | Permisos requeridos |
|---|---|
| Crear carpetas de grupos de entrega | Crear carpeta de grupos de entrega |
| Eliminar carpetas de grupos de entrega | Quitar carpeta de grupos de entrega |
| Mover carpetas de grupos de entrega | Mover carpeta de grupos de entrega |
| Cambiar el nombre de carpetas de grupos de entrega | Modificar carpeta de grupos de entrega |
| Mover grupos de entrega a carpetas | Modificar carpeta de grupos de entrega y modificar propiedades de grupo de entrega |

#### Administrar App Protection

La siguiente información complementa el artículo App Protection de la documentación de Citrix Virtual Apps and Desktops. Para utilizar App Protection en una implementación de Citrix DaaS, siga las instrucciones generales de ese artículo y tenga en cuenta los detalles siguientes.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página de **App Protection**, puede activar la función de **protección contra el registro de tecleo** y **contra las capturas de pantalla**.

- Debe tener una suscripción válida a Citrix Cloud y derechos de uso válidos con relación a la función de App Protection. Para adquirir la función de App Protection, puede ponerse en contacto con su representante de ventas de Citrix.
- App Protection requiere confianza en XML. Para habilitar la confianza en XML, vaya a **Parámetros > Habilitar confianza en XML**.
- En cuanto a la protección contra la captura de pantalla:
  - En Windows y macOS, solo la ventana del contenido protegido está en blanco. App Protection está activa cuando una ventana protegida no está minimizada.
  - En Linux, toda la captura aparece vacía. App Protection está activa tanto si una ventana protegida está minimizada como si no.

### Usuarios

> **Nota:**
>
> Se ha eliminado la opción **Dejar a Citrix Cloud la administración de usuarios**. Para administrar las asignaciones de usuarios para los grupos de entrega existentes configurado como **Dejar a Citrix Cloud la administración de usuarios**, tiene dos opciones: Biblioteca de Citrix Cloud o Configuración completa. Para obtener más información sobre el enfoque de Configuración completa, consulte Administrar las asignaciones de usuarios para los grupos de entrega administrados por la biblioteca de Citrix Cloud.

En este tema se tratan las siguientes secciones:

- Cambiar los parámetros del usuario
- Agregar o quitar usuarios
- Administrar las asignaciones de usuarios para los grupos de entrega administrados por la biblioteca de Citrix Cloud

### Cambiar los parámetros de usuario en un grupo de entrega

El nombre de esta página puede aparecer como **Parámetros de usuario** o **Parámetros básicos**.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Parámetros de usuario**, puede cambiar los parámetros de la tabla siguiente.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

| Parámetro | Descripción |
|---|---|
| Descripción | El texto que utiliza Citrix Workspace (o StoreFront) y que verán los usuarios. |
| Habilitar grupo de entrega | Indica si el grupo de entrega está habilitado o no. |
| Zona horaria | La zona horaria en la que deben residir las máquinas de este grupo de entrega. La opción muestra las zonas horarias admitidas por el sitio. **Nota:** Al cambiar la zona horaria de un grupo de entrega, es posible que se reinicien las máquinas de ese grupo de entrega. Para evitarlo, asegúrese de cambiar los parámetros de la zona horaria fuera del horario de producción. |

| Parámetro | Descripción |
| --- | --- |
| Habilitar Secure ICA | Oculta todas las comunicaciones que tienen lugar desde y hacia las máquinas del grupo de entrega mediante SecureICA, que cifra el protocolo ICA. El nivel predeterminado es 128 bits. Este nivel se puede cambiar mediante el SDK. Citrix recomienda el uso de más métodos de cifrado como el cifrado TLS cuando se trabaje en redes públicas. Asimismo, SecureICA no comprueba la integridad de los datos. |
| Máximo de escritorios por usuario | Cuántos escritorios puede tener un usuario. |

### Agregar o quitar usuarios de un grupo de entrega

Para obtener más información acerca de los usuarios, consulte Usuarios.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en la barra de acciones.
3. En la página **Usuarios**:
   - Para agregar usuarios, haga clic en **Agregar** y especifique los usuarios que quiere agregar.
   - Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, seleccione **Quitar**.
   - Marque o desmarque la casilla para permitir el acceso a usuarios no autenticados.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

**Administrar asignaciones de usuarios** Para administrar asignaciones de usuarios:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega**.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Asignación de máquinas**, agregue o quite usuarios. Para agregar usuarios, vaya hasta ellos o introduzca una lista de nombres de usuario separados por puntos y comas.

Al introducir los nombres de usuario, tenga en cuenta lo siguiente:

- Si los usuarios están en Active Directory, introduzca los nombres directamente. Si no es así, introduzca los nombres en este formato: `<identity provider>:<user name>`. Ejemplo: `AzureAD:username`.

#### Administrar las asignaciones de usuarios para los grupos de entrega administrados por la biblioteca de Citrix Cloud

Para administrar las asignaciones de usuarios para los grupos de entrega administrados por la biblioteca de Citrix Cloud, use Biblioteca de Citrix Cloud o Configuración completa.

Para realizar esta tarea con la Configuración completa, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega administrado por Citrix Cloud y, a continuación, seleccione **Modificar** en la barra de acciones.
3. Para restringir el uso de un escritorio a ciertos usuarios, siga estos pasos:

    a) En la página **Escritorios** o **Reglas de asignación de escritorio**, seleccione el escritorio y haga clic en **Modificar**. Aparecerá la página **Modificar escritorio** con la opción **Restringir el uso del escritorio** seleccionada.
    b) Haga clic en **Agregar**, seleccione uno o más usuarios según sea necesario y, a continuación, haga clic en **Listo**.
    c) Haga clic en **Aceptar**.

4. Para restringir el uso de las aplicaciones de este grupo a determinados usuarios, haga clic en **Regla de asignación de aplicaciones** en el panel de la izquierda y siga el procedimiento descrito en el paso 3 para agregar usuarios.

### Máquinas

- Cambio de asignaciones de máquinas a usuarios
- Habilitar la caché de host local para los VDA agrupados de sesión única
- Actualización de una máquina
- Agregar, modificar o eliminar una restricción por etiquetas para un escritorio
- Quitar una máquina
- Restringir el acceso a los recursos
- Impedir que los usuarios se conecten a una máquina (modo de mantenimiento)
- Apagado y reiniciado de las máquinas
- Crear y administrar programaciones de reinicios para las máquinas
- Administrar la carga de las máquinas

- Administrar Autoscale

Además de las funciones descritas en este artículo, consulte Autoscale para obtener información sobre máquinas que administran de manera proactiva la energía.

### Cambiar asignaciones de máquinas a usuarios en un grupo de entrega

Puede cambiar las asignaciones de las máquinas de SO de sesión única aprovisionadas con MCS. No puede cambiar las asignaciones para máquinas de SO multisesión o máquinas aprovisionadas con Citrix Provisioning.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Asignación de máquinas**, especifique los nuevos usuarios.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

### Habilitar la caché de host local para los VDA agrupados de sesión única

De forma predeterminada, las máquinas agrupadas de sesión única con administración de energía no están disponibles en el modo de caché de host local. Puede anular el comportamiento predeterminado por grupo de entrega. Estos son los pasos detallados:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.

   En la lista de grupos, los grupos que contienen máquinas agrupadas de sesión única aprovisionadas por MCS o Citrix Provisioning muestran un icono de advertencia.

2. Seleccione el grupo que quiera y después seleccione **Modificar** en la barra de acciones.
3. En la página **Caché del host local**, seleccione **Mantener los recursos disponibles**.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

Como alternativa, puede anular el comportamiento predeterminado mediante comandos de PowerShell. Para obtener más información, consulte Compatibilidad con aplicaciones y escritorios.

> **Importante:**
>
> Habilitar el acceso a máquinas agrupadas de sesión única con administración de energía puede

> provocar que los datos y los cambios de las sesiones de usuario anteriores estén presentes en las sesiones posteriores.

#### Actualizar una máquina en un grupo de entrega

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Seleccione una máquina y, a continuación, seleccione **Actualizar máquinas** en la barra de acciones.

Para elegir otra imagen, seleccione **Imagen** y, a continuación, seleccione una instantánea.

Para aplicar cambios y notificar a los usuarios de la máquina, seleccione **Notificación de implantación para usuarios finales**. A continuación, especifique:

- El momento de la actualización de la imagen: ahora o en el próximo reinicio
- La hora de la distribución de reinicios (el tiempo total para comenzar a actualizar todas las máquinas del grupo)
- Si se notifica a los usuarios del reinicio
- El mensaje que los usuarios recibirán

#### Agregar, modificar o eliminar una restricción por etiquetas para un escritorio

Agregar, modificar o eliminar restricciones por etiqueta puede tener efectos no esperados en los escritorios que se tengan en cuenta para el inicio. Consulte las precauciones y los aspectos a tener en cuenta en Etiquetas.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Escritorios**, seleccione el escritorio y seleccione **Modificar**.
4. Para agregar una restricción por etiquetas, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta.
5. Para cambiar o eliminar una restricción por etiquetas, ya sea:
   - Seleccione otra etiqueta.
   - Puede eliminar la restricción por etiquetas al desmarcar la casilla **Restringir inicios a máquinas con esta etiqueta**.
6. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta. También puede seleccionar **Aceptar** para aplicar los cambios y cerrar la ventana.

### Quitar una máquina de un grupo de entrega

Al quitar una máquina, se elimina de un grupo de entrega. No se eliminará del catálogo de máquinas que el grupo de entrega utiliza. Por lo tanto, esa máquina está disponible para la asignación a otro grupo de entrega.

Las máquinas deben estar apagadas antes de poder eliminarlas. Para impedir temporalmente que los usuarios se conecten a una máquina mientras se procede a quitarla, ponga la maquina en modo de mantenimiento antes de apagarla.

Las máquinas pueden contener datos personales, así que actúe con precaución a la hora de asignar una máquina a otro usuario. Considere restablecer la imagen inicial de la máquina.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Compruebe que la máquina esté apagada.
4. Seleccione la máquina y, a continuación, seleccione **Quitar del grupo de entrega** en la barra de acciones.

También puede quitar una máquina de un grupo de entrega a través de la conexión que usa la máquina.

### Restringir el acceso a los recursos de un grupo de entrega

Todos los cambios que realice para restringir el acceso a los recursos de un grupo de entrega anulan los parámetros anteriores, independientemente del método que utilice. Puede hacer lo siguiente:

- **Restringir el acceso de los administradores mediante los ámbitos de administración delegada:** Puede crear y asignar un ámbito que permita el acceso de los administradores a todas las aplicaciones, y otro ámbito que conceda acceso solamente a determinadas aplicaciones. Para obtener más información, consulte Administración delegada.
- **Restringir el acceso de los usuarios a través de expresiones de directiva de Smart Access:** Puede configurar reglas de directiva de acceso para controlar el acceso de los usuarios a un grupo de entrega específico. Por ejemplo:
  - Restringir el acceso a un subconjunto de usuarios y especificar los dispositivos de usuario permitidos.
  - Restringir el acceso a los usuarios conectados a través de Workspace (en lugar de StoreFront).
  - Restringir el acceso a los usuarios conectados a través de una URL específica de Workspace.

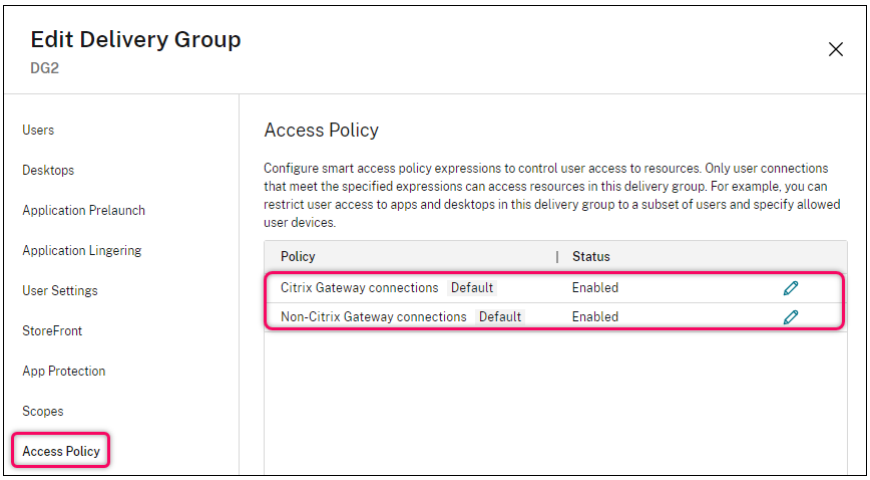
 

En esta sección se explica cómo restringir el acceso de los usuarios a los grupos de entrega mediante reglas de directiva de acceso:

- Acerca de las reglas de directiva de acceso
- Agregar reglas de directiva de acceso
- Administrar reglas de directiva de acceso mediante la Configuración completa
- Agregar y ajustar reglas de directiva con PowerShell

**Acerca de las reglas de directiva de acceso** Puede configurar varias reglas de directiva de acceso para un grupo de entrega. Las aplicaciones y los escritorios de un grupo de entrega aparecen en StoreFront o Workspace de un usuario cuando la conexión del usuario coincide con cualquier regla de directiva de acceso que haya definido para el grupo de entrega, independientemente del orden.

Cada regla se puede habilitar o inhabilitar de forma individual. Una regla inhabilitada se ignora cuando se evalúa la directiva de acceso.




En Configuración completa, la lista Directiva de acceso incluye las siguientes reglas de directiva de SmartAccess predeterminadas. Puede agregar más si es necesario.

- **Conexiones de Citrix Gateway.** Esta directiva solo permite que las conexiones de usuario realizadas a través de Citrix Gateway accedan a los recursos del grupo de entrega. Las conexiones de usuario realizadas a través de Workspace cuando las funciones Postura del dispositivo o Ubicación de red están habilitadas también se consideran conexiones a través de Citrix Gateway.
- **Conexiones que no son de Citrix Gateway.** Esta directiva solo permite que las conexiones de usuario no realizadas a través de Citrix Gateway accedan a los recursos del grupo de entrega.

> **Nota:**
>
> - Para evitar que las reglas predeterminadas anulen una recién configurada, debe inhabilitar las reglas predeterminadas o ajustarlas para excluir los filtros usados en la nueva directiva.
> - Las directivas predeterminadas no se pueden eliminar, pero se pueden inhabilitar. Para

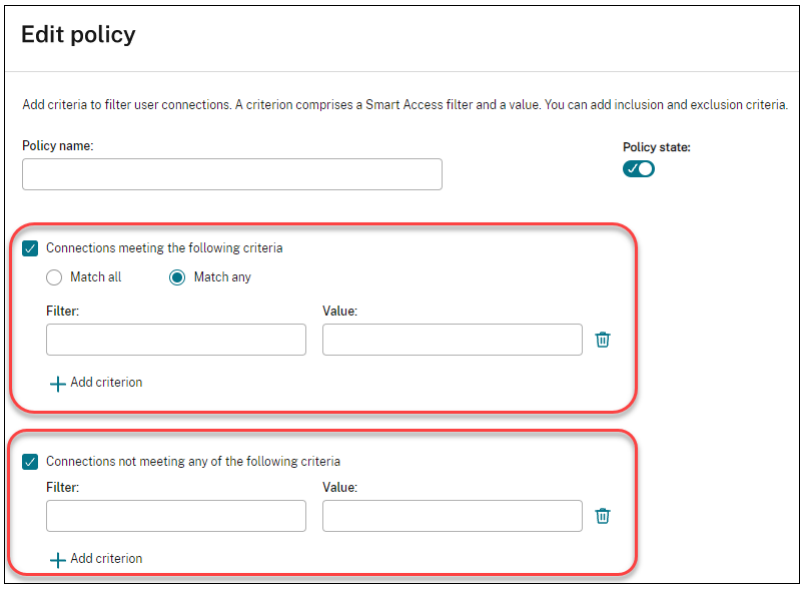
 

> inhabilitar una directiva, haga clic en el icono **Modificar** y, a continuación, cambie el **estado de la directiva** a **Inhabilitada**.
> - La lista de directivas también muestra las reglas agregadas mediante los comandos de PowerShell. Esas directivas se pueden eliminar, pero no se pueden modificar en Configuración completa.

**Agregar reglas de directiva de acceso mediante la Configuración completa** Una regla de directiva de acceso comprende un conjunto de filtros. Para obtener más información sobre los filtros, consulte este artículo. Al agregar una regla de directiva de acceso, agrega varios filtros de condición a la regla según sea necesario.

Para agregar una directiva para un grupo de entrega mediante la Configuración completa, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, haga clic en **Modificar** en la barra de acciones.
3. En la página **Directiva de acceso**, haga clic en **Agregar**. Aparecerá la página **Agregar directiva**.




4. En el campo **Nombre de la directiva**, escriba un nombre descriptivo para la directiva. El nombre debe ser único en la implementación.
5. Para definir los criterios para las conexiones de usuario permitidas, siga estos pasos:
   a) Seleccione **Conexiones que cumplen estos criterios**.
   b) Haga clic en **Agregar criterio**.

c) En el campo **Filtro**, escriba el nombre del filtro que quiere usar. En el campo **Valor**, escriba el valor deseado para el filtro. Por ejemplo, para permitir que solo los usuarios conectados a través de Workspace (en lugar de StoreFront) accedan a los recursos de este grupo de entrega, introduzca `Citrix-Via-Workspace` para **Filtro** y `True` para **Valor**.

d) Para agregar otros criterios, repita los pasos b-c.

e) Seleccione la relación entre los criterios:

- **Hacer coincidir cualquiera**. Permite acceder solo cuando la conexión de usuario entrante cumple con alguno de los criterios de filtro configurados.
- **Hacer coincidir todo**. Permite acceder solo cuando la conexión de usuario entrante cumple con todos los criterios de filtro configurados.

6. Para definir los criterios para las conexiones de usuario prohibidas, siga estos pasos:

a) Seleccione **Conexiones que no cumplen ninguno de estos criterios**.

b) Haga clic en **Agregar criterio**.

c) En el campo **Filtro**, escriba el nombre del filtro que quiere usar. En el campo **Valor**, escriba el valor deseado para el filtro. Por ejemplo, para prohibir que los usuarios conectados a través de la URL `example.cloud.com` de Workspace accedan a los recursos de este grupo de entrega. introduzca `Citrix.Workspace.UsingDomain` para **Filtro** y `example.cloud.com` para **Valor**.

d) Para agregar otros criterios, repita los pasos b-c.

> **Nota:**
>
> Las conexiones de usuario que cumplan cualquiera de los criterios configurados no podrán acceder a los recursos de este grupo de entrega.

7. Haga clic en **Listo**.

   La nueva directiva aparece en la lista de directivas.

8. Revise y ajuste las reglas de directiva predeterminadas para evitar superposiciones involuntarias con las conexiones cubiertas por esta nueva directiva. Para ajustar las directivas existentes, utilice los siguientes métodos:

- Inhabilite las reglas de directiva predeterminadas.
- Configure las reglas de directiva predeterminadas para excluir los filtros de SmartAccess que agregó a los criterios de inclusión de la nueva directiva. Para obtener más información, consulte Administrar reglas de directiva mediante la Configuración completa y Agregar y administrar reglas de directiva de acceso mediante PowerShell.

> **Importante:**
>
> Como se explica en Acerca de las reglas de directiva de acceso, cuando la conexión de un usuario coincide con una o más reglas de directiva de un grupo de entrega, el usuario obtiene acceso a sus recursos. Por lo tanto, después de crear una regla, debe revisar y ajustar cuidadosamente las reglas existentes para evitar cualquier superposición involuntaria con las conexiones cubiertas por la nueva regla.

**Administrar reglas de directiva de acceso mediante la Configuración completa** Puede usar los criterios de inclusión y exclusión para ajustar las directivas predeterminadas. Por ejemplo, para restringir el acceso a un subconjunto de esas conexiones, siga estos pasos:

1. Modifique una directiva predeterminada.
2. Seleccione **Conexiones que cumplen uno de estos criterios**.
3. Agregue, modifique o quite las expresiones de directiva de SmartAccess para los supuestos de acceso de usuario permitidos.

Para obtener más información, consulte la documentación de Citrix Gateway.

**Agregar y administrar reglas de directiva de acceso mediante PowerShell** Puede usar los siguientes cmdlets de PowerShell para agregar y administrar reglas de directiva de acceso para los grupos de entrega:

- New-BrokerAccessPolicyRule
- Get-BrokerAccessPolicyRule
- Set-BrokerAccessPolicyRule
- Rename-BrokerAccessPolicyRule
- Remove-BrokerAccessPolicyRule

Para obtener más información, consulte los artículos correspondientes en la documentación para desarrolladores de Citrix.

### Impedir que los usuarios se conecten a una máquina (modo de mantenimiento) en un grupo de entrega

Cuando tenga que detener temporalmente las conexiones nuevas a las máquinas, puede activar el modo de mantenimiento para una o todas las máquinas de un grupo de entrega. Puede hacerlo antes de aplicar revisiones o mediante herramientas de administración.

- Cuando una máquina con SO multisesión está en modo de mantenimiento, los usuarios pueden conectarse a las sesiones existentes, pero no pueden iniciar sesiones nuevas.

- Cuando una máquina con SO de sesión única (o un PC de acceso con Remote PC) está en modo de mantenimiento, los usuarios no pueden conectarse o volver a conectarse. Las conexiones actuales permanecen conectadas hasta que se desconectan o cierran sesión.

Para activar o desactivar el modo de mantenimiento:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo.
3. Para activar el modo de mantenimiento en todas las máquinas de un grupo de entrega, seleccione **Activar modo de mantenimiento** en la barra de acciones.

   Para activar el modo de mantenimiento en una máquina, seleccione **Ver máquinas** en la barra de acciones. Seleccione una máquina y, a continuación, seleccione **Activar modo de mantenimiento** en la barra de acciones.
4. Para desactivar el modo de mantenimiento en una o todas las máquinas de un grupo de entrega, siga las instrucciones anteriores, pero seleccione **Desactivar modo de mantenimiento** en la barra de acciones.

La configuración de la Conexión a Escritorio remoto (RDC) de Windows también afecta a si una máquina con SO multisesión está en modo de mantenimiento o no. El modo de mantenimiento se activa en cualquiera de las siguientes circunstancias:

- El modo de mantenimiento está activado, tal y como se ha descrito anteriormente.
- Cuando la conexión a Escritorio remoto se establece en **No permitir las conexiones a este equipo**.
- Cuando la conexión a Escritorio remoto no se establece en **No permitir las conexiones a este equipo** y el parámetro "Modo de inicio de sesión de usuario en la Configuración de host remoto" es **Permitir reconexiones, pero impedir nuevos inicios de sesión** o **Permitir reconexiones, pero impedir nuevos inicios de sesión hasta que el servidor se reinicie**.

También puede activar o desactivar el modo de mantenimiento de:

- Una conexión, que afecta a las máquinas que usan esa conexión.
- Un catálogo de máquinas, que afecta a las máquinas en ese catálogo.

#### Apagar y reiniciar máquinas en un grupo de entrega

No se admite este procedimiento en las máquinas de acceso con Remote PC.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.

2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Seleccione la máquina y, a continuación, seleccione una de estas acciones de la barra de acciones:

   > **Nota:**
   >
   > - Estas acciones se aplican únicamente a las máquinas con administración de energía.
   > - Es posible que algunas opciones no estén disponibles según el estado de la máquina.

   - **Forzar apagado:** Apaga la máquina y actualiza la lista de máquinas.
   - **Reiniciar:** Solicita al sistema operativo que se apague y que, a continuación, vuelva a iniciar la máquina. Si el sistema operativo no puede hacerlo, esta permanece en su estado actual.
   - **Forzar reinicio:** Obliga al sistema operativo a apagarse y, a continuación, reinicia la máquina.
   - **Suspender:** Pausa la máquina sin apagarla y actualiza la lista de máquinas.
   - **Apagar:** Solicita al sistema operativo de la máquina que se apague.

Para acciones no forzosas, si la máquina no se apaga en un plazo de 10 minutos, se le obliga a apagarse. Si Windows intenta instalar actualizaciones durante el apagado, existe el riesgo de que la máquina se apague antes de que se completen las actualizaciones.

#### Crear y administrar programaciones de reinicios para las máquinas de un grupo de entrega

> **Nota:**
>
> - Cuando se aplica una programación de reinicios a un grupo de entrega con Autoscale habilitado, sus máquinas simplemente se apagan para que Autoscale las encienda.
> - Cuando se aplican programaciones de reinicios a máquinas aleatorias de sesión única, esas máquinas se apagan en lugar de reiniciarse para ahorrar costes. Le recomendamos que utilice Autoscale para encender las máquinas.
> - Al cambiar la zona horaria de un grupo de entrega, es posible que se reinicien las máquinas de ese grupo de entrega. Para evitarlo, asegúrese de cambiar los parámetros de la zona horaria fuera del horario de producción.

Una programación de reinicios especifica cuándo se reinician periódicamente las máquinas de un grupo de entrega. Puede crear una o varias programaciones para un grupo de entrega. Una programación puede afectar a:

- Todas las máquinas del grupo.
- Una o varias máquinas (pero no todas) del grupo. Las máquinas se identifican mediante una etiqueta que se les aplica. Esta operación se denomina restricción por etiquetas, porque la etiqueta restringe una acción solo a los elementos (en este caso, máquinas) que tienen la etiqueta.

Por ejemplo: Supongamos que todas las máquinas se encuentran en un solo grupo de entrega. Quiere reiniciar todas las máquinas al menos una vez por semana, salvo las máquinas que utiliza el departamento de contabilidad, que deben reiniciarse todos los días. Para ello, configure una programación para todas las máquinas y otra para las máquinas del departamento de contabilidad.

Una programación incluye el día y la hora en que comienza el reinicio, así como la duración de este. La duración es "iniciar todas las máquinas afectadas al mismo tiempo"o el tiempo que normalmente tarda en reiniciar todas las máquinas afectadas.

Puede activar o desactivar una programación. Inhabilitar una programación puede ser útil durante la realización de pruebas, durante intervalos especiales o cuando se preparan programaciones antes de necesitarlas.

No puede usar programaciones para el encendido o el apagado automáticos desde la consola de administración; solo para reiniciar.

**Superposición de programaciones** Es posible que las programaciones se solapen. En el ejemplo anterior, ambas programaciones afectan a las máquinas utilizadas por el equipo de contabilidad. Esas máquinas podrían reiniciarse dos veces el domingo. Ahora bien, la programación está diseñada para evitar tener que reiniciar la misma máquina con más frecuencia de la necesaria, pero eso no puede garantizarse.

- Si las programaciones se solapan en la hora de inicio y la duración, es más probable que las máquinas se reinicien una sola vez.
- Por tanto, cuanto más difieran las programaciones en la hora de inicio y la duración, más probable será que haya varios reinicios.
- La cantidad de máquinas que se vean afectadas por los reinicios programados también puede influir en las posibilidades de superposición. En el ejemplo, la programación semanal que afecta a todas las máquinas podría iniciar los reinicios más rápidamente que el reinicio diario programado para las máquinas de contabilidad (según la duración configurada para cada reinicio).

Para obtener información exhaustiva sobre las programaciones de reinicios, consulte Datos internos de programación de reinicios.

#### Ver programaciones de reinicios

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. Seleccione la página **Programación de reinicios**.

La página **Programación de reinicios** contiene la siguiente información para cada programación configurada:

- Nombre de la programación.
- Restricción por etiquetas utilizada, si la hay.
- La frecuencia con se producen los reinicios de las máquinas.
- Si los usuarios de la máquina reciben una notificación.
- Si la programación está habilitada. Inhabilitar una programación puede ser útil durante la realización de pruebas, durante intervalos especiales o cuando se preparan programaciones antes de necesitarlas.

**Agregar (aplicar) etiquetas** Si configura una programación de reinicios que usa una restricción por etiquetas, compruebe que esa etiqueta se ha agregado (aplicado) a las máquinas a las que esa programación debería afectar. En el ejemplo anterior, cada una de las máquinas utilizadas por el equipo de contabilidad tiene una etiqueta aplicada. Para obtener más información, consulte Etiquetas.

Aunque puede aplicar más de una etiqueta a una máquina, solo se puede especificar una etiqueta en una programación de reinicios.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione el grupo de entrega que contiene las máquinas a las que afectará la programación.
3. Seleccione **Ver máquinas** y, a continuación, seleccione las máquinas a las que agregará la etiqueta.
4. Seleccione **Administrar etiquetas** en la barra de acciones.
5. Si la etiqueta ya existe, marque la casilla situada junto al nombre de la etiqueta. Si la etiqueta no existe, seleccione **Crear** y especifique el nombre de la etiqueta. Una vez creada, marque la casilla situada junto al nombre de la etiqueta recién creada.
6. Seleccione **Guardar** en el cuadro de diálogo **Administrar etiquetas**.

#### Crear una programación de reinicios

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Programación de reinicios**, seleccione **Agregar**.
4. En la página **Agregar programación de reinicios**:
    - Para habilitar la programación, seleccione **Sí**. Para inhabilitar la programación, seleccione **No**.

- Escriba un nombre y una descripción para la programación.
- En **Restringir a la etiqueta**, aplique una restricción de etiqueta.
- En **Incluir máquinas en modo de mantenimiento**, elija si quiere incluir en esta programación las máquinas que estén en modo de mantenimiento. Para usar PowerShell en su lugar, consulte Reinicios programados para máquinas en modo de mantenimiento.
- En **Frecuencia de reinicio**, seleccione la frecuencia con que se produce el reinicio: diariamente, semanalmente, mensualmente o una única vez. Si selecciona **Semanalmente** o **Mensualmente**, puede especificar uno o varios días específicos.
- Para **Se repite cada**, especifique la frecuencia con la que quiere que se realice la programación.
- Para **Fecha de inicio**, especifique una fecha de inicio para la primera instancia de la programación.
- En **Empezar el reinicio a**, especifique, en el formato de 24 horas, la hora del día en que comenzará el reinicio.
- En **Duración del reinicio**:
  - Si no quiere utilizar el reinicio natural, seleccione **Reiniciar todas las máquinas a la vez** o **Reiniciar todas las máquinas en un plazo determinado**.
  - Si quiere utilizar el reinicio natural, seleccione **Reiniciar todas las máquinas después de la purga de sesiones**.

    Al poner en marcha un programa de reinicio que esté configurado para usar el reinicio natural:

    * Todas las máquinas inactivas pertenecientes al grupo de entrega se reinician inmediatamente
    * Las máquinas pertenecientes al grupo de entrega con una o más sesiones activas se reiniciarán cuando se cierren todas las sesiones.

    > **Nota:**
    >
    > Puede usar esta opción para máquinas con administración de energía y también para máquinas sin administración de energía.

- En **Enviar notificación a los usuarios**, elija si mostrar un mensaje de notificación en las máquinas correspondientes antes de empezar un reinicio. De forma predeterminada, no aparece ningún mensaje.
- Si elige mostrar un mensaje 15 minutos antes de empezar el reinicio, puede decidir (en **Frecuencia de notificaciones**) si repetir el mensaje cada cinco minutos después del primer mensaje. De forma predeterminada, el mensaje no se repite.

- Escriba el título y el texto de la notificación. No hay texto predeterminado.

  Si quiere que el mensaje incluya una cuenta atrás para reiniciarse, incluya la variable **%m%**. A menos que haya optado por reiniciar todas las máquinas a la vez, el mensaje de notificación aparece en cada máquina en el momento correspondiente antes de que empiece el reinicio.

5. Haga clic en **Listo** para aplicar los cambios y cerrar la ventana **Agregar programación de reinicios**.
6. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta **Modificar grupo de entrega**. También puede hacer clic en **Guardar** para aplicar los cambios y cerrar la ventana.

**Ejecutar inmediatamente una programación de reinicios** Una programación de reinicios especifica el momento en que las máquinas de un grupo de entrega se reinician de manera regular. También puede ejecutar una programación de reinicios inmediatamente para reiniciar las máquinas de esa programación.

Para ejecutar una programación de reinicios inmediatamente, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione el grupo de entrega aplicable y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Programación de reinicios**, seleccione una programación que quiera ejecutar y, a continuación, seleccione **Ejecutar programación**.

> **Nota:**
>
> - No puede ejecutar una programación inmediatamente si está configurada con el parámetro **Reiniciar todas las máquinas después de la purga de sesiones**.
> - Puede usar **Ejecutar programación** solo en una programación cada vez.
> - Después de modificar una programación, **Ejecutar programación** deja de estar disponible. Seleccione **Aplicar** para que esté disponible.

**Modificar, quitar, habilitar o inhabilitar una programación de reinicios**

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Programación de reinicios**, marque la casilla de una programación.

- Para modificar una programación, seleccione **Modificar**. Actualice los parámetros de la programación siguiendo las instrucciones indicadas en Crear una programación de reinicios.
- Para habilitar o inhabilitar una programación, seleccione **Modificar**. Marque o desmarque la casilla **Habilitar programación de reinicios**.
- Para quitar una programación, seleccione **Quitar**. Confirme la eliminación. La eliminación de una programación no afecta a las etiquetas aplicadas a las máquinas afectadas.

**Reinicios programados que se retrasan por una interrupción de la base de datos**

> **Nota:**
>
> Esta función solo está disponible en PowerShell.

Si se produce una interrupción de la base de datos del sitio antes de que comience un reinicio programado para las máquinas (VDA) de un grupo de entrega, los reinicios comienzan cuando finaliza la interrupción. Esta acción puede provocar resultados imprevistos.

Por ejemplo, supongamos que ha programado reinicios de un grupo de entrega para que se produzcan durante las horas que no son de producción (a partir de las 3:00). Se produce una interrupción de la base de datos del sitio una hora antes de que comience el reinicio programado (2:00). La interrupción dura 6 horas (hasta las 8:00). La programación de reinicios comienza cuando se restaura la conexión entre el Delivery Controller y la base de datos del sitio. Ahora el VDA se reinicia cinco horas después de su programación original. Esta acción podría provocar que los VDA se reinicien durante las horas de producción.

Para evitar esta situación, puede usar el parámetro `MaxOvertimeStartMins` para los cmdlets `New-BrokerRebootScheduleV2` y `Set-BrokerRebootScheduleV2`. El valor especifica el máximo de minutos transcurridos a partir de la hora de inicio programada a la que puede comenzar una programación de reinicios.

- Si la conexión a la base de datos se restaura antes de que haya transcurrido ese tiempo (hora programada +`MaxOvertimeStartMins`), los VDA se reinician.
- Si la conexión a la base de datos no se restaura antes de que haya transcurrido ese tiempo, los VDA no se reinician.
- Si este parámetro se omite o su valor es cero, la programación de reinicios comienza cuando se restablece la conexión a la base de datos, independientemente de la duración de la interrupción.

Para obtener más información, consulte la ayuda de los cmdlets. Esta función solo está disponible en PowerShell.

**Reinicios programados para máquinas en modo de mantenimiento** Para indicar si una programación de reinicio afecta a las máquinas que están en modo de mantenimiento, utilice la opción `IgnoreMaintenanceMode` con los cmdlets `BrokerRebootScheduleV2`.

Por ejemplo, el cmdlet siguiente crea una programación que reinicia tanto las máquinas que están en el modo de mantenimiento como las que no.

```
New-BrokerRebootSchedulev2 rebootSchedule1 -DesktopGroupName <myDesktopGroup
> -IgnoreMaintenanceMode $true
```

El cmdlet siguiente modifica programaciones de reinicio existentes.

```
Set-BrokerRebootSchedulev2 rebootSchedule1 -IgnoreMaintenanceMode
$true
```

Para obtener más información, consulte la ayuda de los cmdlets.

#### Administrar la carga de las máquinas de un grupo de entrega

Solo puede administrar la carga de las máquinas con sistema operativo multisesión.

La administración de carga mide la carga del servidor y determina el servidor que quiere seleccionar en el entorno actual. Esta selección se basa en:

- **Estado del modo de mantenimiento del servidor:** Una máquina de SO multisesión se tiene en cuenta para el equilibrio de carga solo cuando el modo de mantenimiento está desactivado.
- **Índice de carga de servidor**: Este índice determina con qué probabilidad recibirá conexiones un servidor que entrega máquinas de SO multisesión. El índice es una combinación de patrones de carga: la cantidad de sesiones y la configuración de las mediciones de rendimiento (como la CPU, el disco y el uso de memoria). Los patrones de carga se especifican en las configuraciones de la directiva Administración de carga.

  Un índice de carga del servidor de 10000 indica que la carga del servidor es total. Si no hay otros servidores disponibles, es posible que los usuarios reciban un mensaje en el que se les notifica que el escritorio o la aplicación no están disponibles cuando intentan iniciar sesión.

  Puede supervisar el índice de carga en el SDK, en Director (Supervisar) y en la búsqueda de la interfaz de administración de Configuración completa.

  En las pantallas de la consola, para mostrar la columna **Índice de carga del servidor** (que está oculta de forma predeterminada), seleccione una máquina, haga clic con el botón secundario en el encabezado de una columna y, a continuación, elija **Seleccionar columna**. En la categoría **Máquina**, seleccione **Índice de carga**.

  En el SDK, use el cmdlet `Get-BrokerMachine`. Para obtener más información, consulte CTX202150.

- **Parámetro de directiva Tolerancia de inicios de sesión simultáneos**: La cantidad máxima de solicitudes simultáneas para iniciar sesión en el servidor. (esta opción es equivalente a la regulación de carga en las versiones 6.x de XenApp).

  Cuando todos los servidores superan o se encuentran en el límite definido por el parámetro Tolerancia de inicios de sesión simultáneos, la siguiente solicitud de inicio de sesión se asigna al servidor que tenga el menor número de inicios de sesión pendientes. Si hay más de un servidor que cumple esos criterios, se selecciona el servidor que presenta el menor índice de carga.

#### Administrar Autoscale

De forma predeterminada, Autoscale está inhabilitado para los grupos de entrega. Para administrar Autoscale en un grupo de entrega (si corresponde), siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Administrar Autoscale** en la barra de acciones. Aparecerá la ventana **Administrar Autoscale**.
3. Configure los parámetros según sea necesario. Para obtener información sobre parámetros de Autoscale, consulte Autoscale.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y para dejar la ventana abierta. También puede seleccionar **Guardar** para aplicar los cambios y cerrar la ventana.

### Sesiones

- Cerrar o desconectar una sesión, o enviar un mensaje a los usuarios
- Configurar el preinicio y la persistencia de sesiones
- Configurar la itinerancia de sesiones
- Reconexión de sesiones de control al desconectarse de la máquina en modo de mantenimiento

#### Cerrar una sesión, desconectarla o enviar un mensaje a los usuarios de un grupo de entrega

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
3. Para cerrar la sesión de un usuario, seleccione la sesión o el escritorio y, a continuación, seleccione **Cerrar sesión** en la barra de acciones. La sesión se cierra y la máquina queda disponible para otros usuarios, a menos que esté asignada a un usuario concreto.

4. Para desconectar una sesión, seleccione la sesión o el escritorio y, a continuación, seleccione **Desconectar** en la barra de acciones. Las aplicaciones siguen ejecutándose y la máquina permanece asignada a ese usuario. El usuario puede volver a conectarse a la misma máquina.
5. Para enviar un mensaje a los usuarios, seleccione la sesión, la máquina o el usuario y, a continuación, seleccione **Enviar mensaje** en la barra de acciones. Escriba el mensaje.

#### Configurar el preinicio de sesiones y la persistencia de sesiones en un grupo de entrega

Estas funciones solo se admiten en máquinas con sistema operativo multisesión.

Las funciones de preinicio de sesiones y persistencia de sesiones ayudan a los usuarios especificados a acceder rápidamente a las aplicaciones al:

- Iniciar sesiones antes de que se soliciten (preinicio de sesiones)
- Mantener las sesiones de aplicación activas después de que un usuario haya cerrado todas las aplicaciones (persistencia de sesiones)

De forma predeterminada, no se usa el preinicio de sesiones ni la persistencia de sesiones. Una sesión comienza cuando el usuario abre una aplicación y permanece activa hasta que la última aplicación abierta en la sesión se cierra.

Consideraciones:

- El grupo de entrega debe admitir aplicaciones, y las máquinas deben tener activo un VDA para SO multisesión, al menos con la versión 7.6.
- Estas funciones se admiten solamente cuando se usa la aplicación Citrix Workspace para Windows, y también necesitan una configuración adicional de la aplicación Citrix Workspace. Para obtener instrucciones, busque preinicio de sesiones en la documentación de producto correspondiente a la versión de la aplicación Citrix Workspace para Windows de que dispone.
- No se admite la aplicación Citrix Workspace para HTML5.
- La función de preinicio de sesiones no funcionará si la máquina de un usuario se pone en los modos suspensión o hibernación (independientemente de la configuración de esa función). Los usuarios pueden bloquear sus máquinas/sesiones. Sin embargo, si un usuario cierra la sesión de la aplicación Citrix Workspace, esa sesión finaliza y la función de preinicio deja de aplicarse.
- Cuando se usa el preinicio de sesiones, las máquinas de clientes físicos no pueden usar las funciones de suspensión o hibernación. Los usuarios de máquinas cliente pueden bloquear sus sesiones, pero no deben cerrarlas.
- Las sesiones preiniciadas y las persistentes utilizan una licencia simultánea, pero solo cuando están conectadas. Si utiliza una licencia de usuario por dispositivo, la licencia dura 90 días. De manera predeterminada y si no se están utilizando, las sesiones preiniciadas y las persistentes se desconectan pasados 15 minutos. Este valor se puede configurar en PowerShell (con el cmdlet `New`/`Set-BrokerSessionPreLaunch`).

- Una planificación y una supervisión minuciosas de los patrones de actividad de los usuarios son esenciales para adaptar estas funciones y que se complementen entre sí. Una configuración óptima equilibra las ventajas de una disponibilidad más rápida de aplicaciones para los usuarios, por un lado, y el coste del mantenimiento de licencias en uso y recursos asignados, por el otro.
- También puede configurar el preinicio de sesiones para un momento programado del día en la aplicación Citrix Workspace.

**Cuánto tiempo permanecen activas las sesiones preiniciadas y las persistentes** Existen varios métodos para especificar cuánto tiempo se mantiene activa una sesión si el usuario no inicia ninguna aplicación: un tiempo de espera configurado y varios umbrales de carga del servidor. Puede configurarlos todos. El primer evento que tenga lugar pondrá fin a la sesión no utilizada.

- **Tiempo de espera:** El tiempo de espera configurado especifica la cantidad de minutos, horas o días que una sesión preiniciada o persistente permanece activa. Si configura un tiempo de espera demasiado corto, las sesiones preiniciadas terminarán antes de que el usuario se pueda beneficiar de un acceso más rápido a las aplicaciones. Si configura un tiempo de espera demasiado largo, es posible que se denieguen las conexiones entrantes del usuario porque el servidor no tiene recursos suficientes.

  Puede habilitar este tiempo de espera solamente desde el SDK (cmdlet `New`/`Set-BrokerSessionPreLaunch`), no desde la consola de administración. Si inhabilita el tiempo de espera, este no aparece en la pantalla de la consola de ese grupo de entrega ni en las páginas de **Modificar grupo de entrega**.

- **Umbrales:** Finalizar de forma automática sesiones preiniciadas y sesiones persistentes en función de la carga del servidor garantiza que las sesiones permanezcan abiertas el mayor tiempo posible, siempre que el servidor tenga recursos disponibles. Las sesiones preiniciadas y persistentes que no se utilicen no provocan conexiones denegadas porque ambas finalizan de forma automática cuando los recursos sean necesarios para sesiones de usuario nuevas.

  Puede configurar dos umbrales: el porcentaje medio de carga para todos los servidores del grupo de entrega y el porcentaje máximo de carga para un servidor único del grupo de entrega. Cuando se supera un umbral, se finalizan aquellas sesiones que hayan tenido el estado de preinicio o persistente durante más tiempo. Las sesiones se finalizan una a una con intervalos de minutos entre cada cierre hasta que la carga se halle por debajo del umbral. Mientras el umbral permanezca rebasado, no se iniciará ninguna sesión de preinicio.

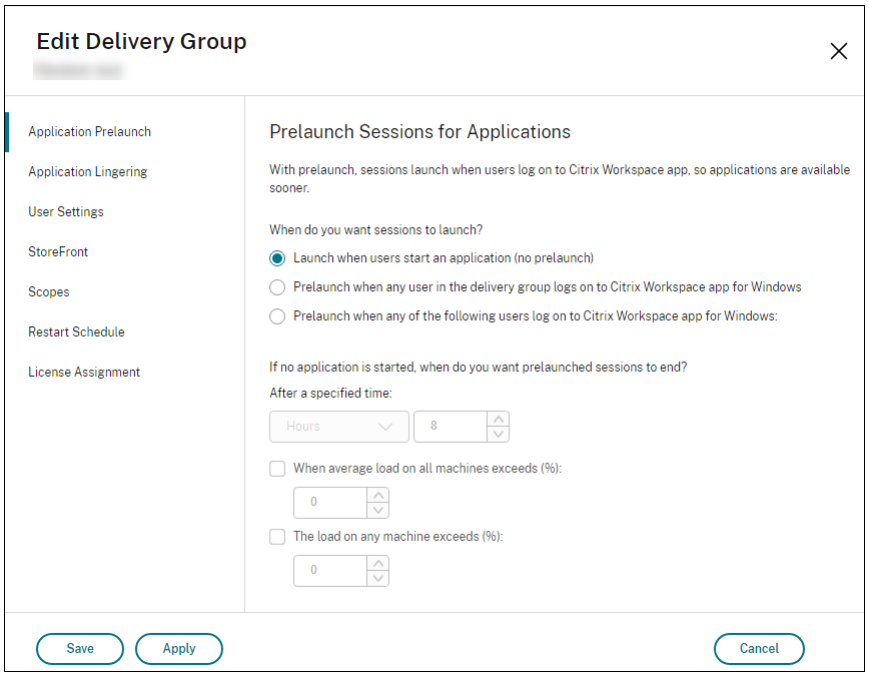
Los servidores con VDA que no se hayan registrado con el Controller y los servidores en el modo de mantenimiento se consideran servidores con carga completa. Una interrupción no planificada tendrá como consecuencia la finalización automática de sesiones de preinicio y sesiones persistentes para liberar capacidad.

**Para habilitar la función de preinicio de sesiones**

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Preinicio de aplicaciones**, habilite el preinicio de sesiones. Para ello, elija cuándo deben iniciarse estas:

    - Cuando un usuario inicia una aplicación. Esta es la opción predeterminada. El preinicio de sesiones está inhabilitado.
    - Cuando un usuario del grupo de entrega inicia sesión en la aplicación Citrix Workspace para Windows.
    - Cuando alguien de una lista de usuarios y grupos de usuarios inicia sesión en la aplicación Citrix Workspace para Windows. Si elige esta opción, compruebe que ha especificado también los usuarios o los grupos de usuarios.




4. Una sesión preiniciada se reemplaza por una sesión habitual cuando el usuario inicia una aplicación. Si el usuario no inicia una aplicación (es decir, la sesión preiniciada no se llega a utilizar), la siguiente configuración afecta a la cantidad de tiempo que esta sesión permanece activa.

    - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo (de 1-99 días, de 1-2376 horas, o de 1-142 560 minutos).
    - Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado (entre el 1 y el 99%).

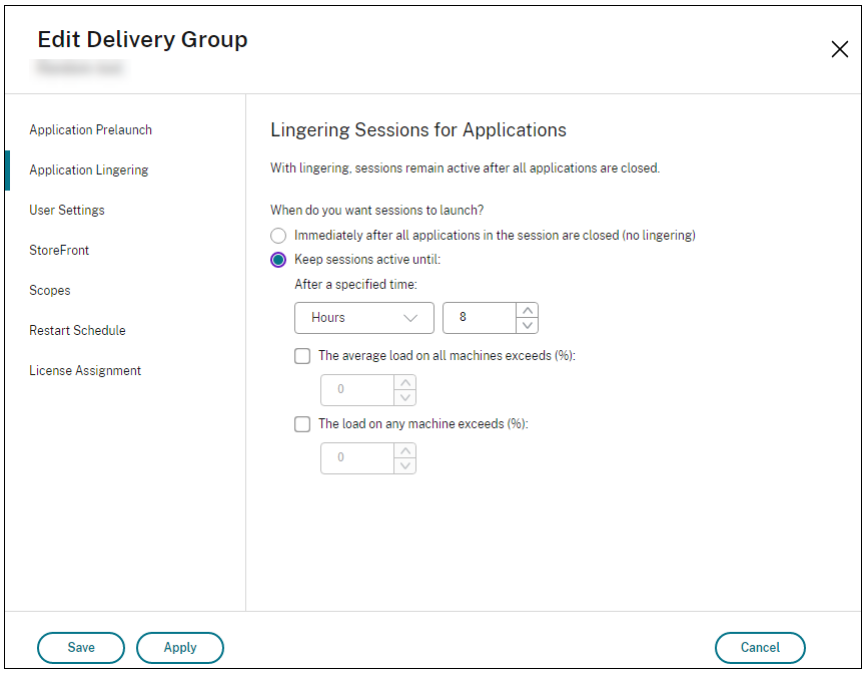
 

- Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado (entre el 1 y el 99%).

En resumen, una sesión preiniciada permanece activa hasta que se da uno de los siguientes eventos: un usuario inicia una aplicación, se agota el tiempo especificado, o se supera un umbral de carga especificado.

**Para habilitar la persistencia de sesiones**

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo y, a continuación, seleccione **Modificar** en la barra de acciones.
3. En la página **Persistencia de aplicaciones**, habilite la persistencia de sesiones seleccionando la opción **Mantener las sesiones activas hasta**.




4. Algunos parámetros influyen en la cantidad de tiempo que las sesiones persistentes pueden permanecer activas si el usuario no inicia otra aplicación.

   - Cuando se agota un intervalo de tiempo especificado. Puede cambiar el intervalo de tiempo: de 1-99 días, de 1-2376 horas, o de 1-142 560 minutos.
   - Cuando el promedio de carga de todas las máquinas del grupo de entrega supera un porcentaje especificado: entre el 1 y el 99%.
   - Cuando la carga de una máquina del grupo de entrega supera un porcentaje especificado: entre el 1 y el 99%.

En resumen, una sesión persistente permanece activa hasta que se da uno de los siguientes eventos: un usuario inicia una aplicación, se agota el tiempo especificado, o se supera un umbral de carga especificado.

### Configurar la itinerancia de sesiones

De forma predeterminada, la itinerancia de sesiones está habilitada para grupos de entrega. Las sesiones se mueven con el usuario entre los diferentes dispositivos cliente. Cuando el usuario inicia una sesión y, más tarde, cambia de dispositivo, se utiliza la misma sesión y las aplicaciones están disponibles simultáneamente en ambos dispositivos. Puede ver las aplicaciones en varios dispositivos. Las aplicaciones se mueven, independientemente del dispositivo o de si las sesiones actuales existen. A menudo, las impresoras y otros recursos asignados a la aplicación también se mueven. También puede usar PowerShell. Para obtener más información, consulte Itinerancia de sesiones.

**Configurar la itinerancia de sesiones para aplicaciones** Para configurar la itinerancia de sesiones para aplicaciones, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en la barra de acciones.
3. En la página **Usuarios**, marque la casilla **Las sesiones se mueven con los usuarios mientras se mueven entre dispositivos** para habilitar la itinerancia de sesiones.
    - Al habilitarse, cuando el usuario inicia una sesión de aplicación y, más tarde, cambia de dispositivo, se usa la misma sesión, y esta están disponible en ambos dispositivos. Al inhabilitarse, la sesión ya no se mueve entre dispositivos.
4. Seleccione **Aceptar** para aplicar los cambios y cerrar la ventana.

**Configurar la itinerancia de sesiones para escritorios** Para configurar la itinerancia de sesiones para un escritorio, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo de entrega y, a continuación, seleccione **Modificar grupo de entrega** en la barra de acciones.
3. En la página **Escritorios**, seleccione el escritorio y seleccione **Modificar**.
4. Marque la casilla **Itinerancia de sesiones** para habilitar la itinerancia de sesiones.

- Al habilitarse, si el usuario inicia un escritorio y, más tarde, cambia de dispositivo, se usa la misma sesión, y las aplicaciones están disponible en ambos dispositivos. Al inhabilitarse, la sesión ya no se mueve entre dispositivos.

5. Seleccione **Aceptar** para aplicar los cambios y cerrar la ventana.

#### Reconexión de sesiones de control al desconectarse de la máquina en modo de mantenimiento

> **Nota:**
>
> Esta función solo está disponible en PowerShell.

Puede controlar si las sesiones que están desconectadas en máquinas en modo de mantenimiento pueden volver a conectarse a máquinas del grupo de entrega.

Antes de finales de mayo de 2021, no se permitía la reconexión de sesiones de escritorio agrupadas de sesión única que se habían desconectado de las máquinas en modo de mantenimiento. Ahora, puede configurar un grupo de entrega para permitir o prohibir las reconexiones (independientemente del tipo de sesión) después de la desconexión de una máquina en modo de mantenimiento.

Al crear o modificar un grupo de entrega (`New-BrokerDesktopGroup`, `Set-BrokerDesktopGroup`), utilice el parámetro `-AllowReconnectInMaintenanceMode <boolean>` para permitir o prohibir las reconexiones de máquinas desconectadas de una máquina en modo de mantenimiento.

- Al establecerse en true, las sesiones pueden volver a conectarse a las máquinas del grupo.
- Al establecerse en false, las sesiones no pueden volver a conectarse a las máquinas del grupo.

Valores predeterminados:

- Sesión única: Inhabilitada
- Multisesión: Habilitada

### Aplicaciones

Vea las aplicaciones de un grupo de entrega y agregue más si fuera necesario.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione un grupo. Si este grupo contiene aplicaciones, la opción **Ver aplicaciones** se muestra en la barra de acciones.
3. Seleccione **Ver aplicaciones**. Se le dirigirá al nodo **Aplicaciones**, donde se muestran todas las aplicaciones disponibles en este grupo.
4. Para agregar más aplicaciones a este grupo, vaya al nodo **Grupos de entrega**, seleccione el grupo y seleccione **Agregar aplicaciones** en la barra de acciones.

### Solucionar problemas técnicos

- Los VDA no registrados en un Delivery Controller no se tienen en cuenta cuando se inicien sesiones con intermediario. Esto provoca una infrautilización de los recursos disponibles. Existen diversos motivos por los que un VDA puede no registrarse, y un administrador puede solucionar muchos de ellos. Para solucionar problemas, los detalles proporcionan información en el asistente para la creación de catálogos y después de agregar el catálogo a un grupo de entrega.

  Tras crear un grupo de entrega, el recuadro Detalles de dicho grupo indica la cantidad de máquinas que se supone están registradas, pero no lo están. Por ejemplo, una o varias máquinas que están activadas y no están en modo de mantenimiento, pero no están actualmente registradas en el Controller. Al ver una máquina que "no está registrada, pero debería estarlo", consulte la ficha **Solución de problemas** del panel de detalles para buscar las posibles causas y las acciones correctivas recomendadas.

  Para ver los mensajes sobre el nivel funcional, consulte Niveles funcionales y versiones de VDA.

  Para obtener información sobre la solución de problemas de registro de VDA, consulte CTX136668.

- En la pantalla de un grupo de entrega, la **versión instalada de VDA** del recuadro Detalles puede ser diferente de la versión real instalada en las máquinas. La pantalla Programas y funciones de la máquina Windows muestra la versión real del VDA.
- Para máquinas que presentan un **Estado de energía desconocido**, consulte CTX131267 para obtener instrucciones.

## Crear grupos de aplicaciones

June 12, 2024

### Introducción

Los grupos de aplicaciones permiten administrar colecciones de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega. Los grupos de aplicaciones son opcionales. Ofrecen una alternativa a agregar las mismas aplicaciones a varios grupos de entrega. Los grupos de entrega se pueden asociar a varios grupos de aplicaciones, y un grupo de aplicaciones puede estar asociado a varios grupos de entrega.

El uso de grupos de aplicaciones puede proporcionar ventajas para la administración de aplicaciones y para el control de los recursos frente a la opción de grupos de entrega:

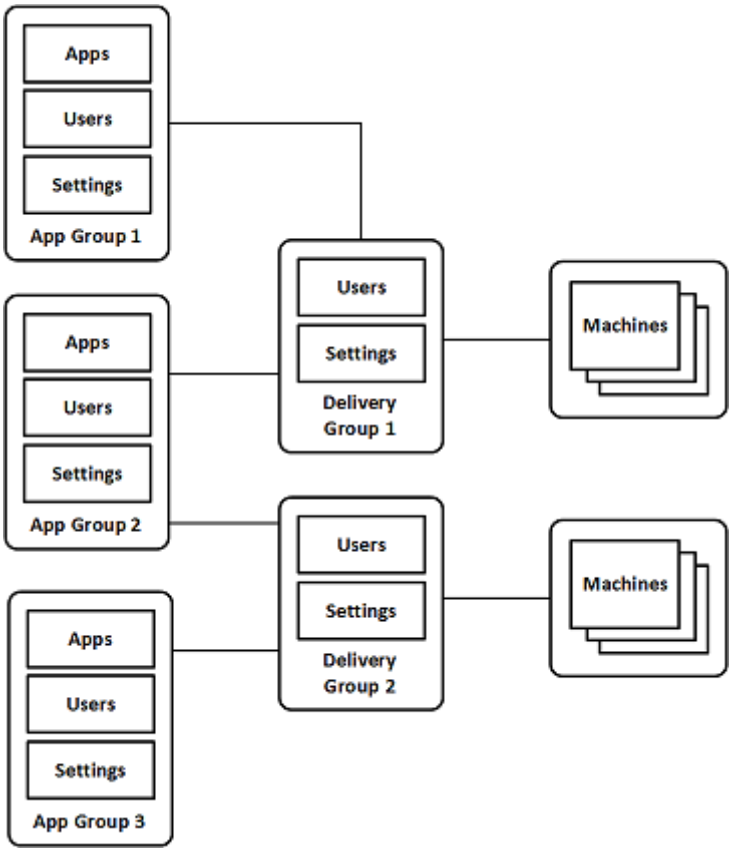
- La agrupación lógica de las aplicaciones y sus parámetros permite administrar esas aplicaciones como una sola unidad. Por ejemplo, no tiene que agregar (publicar) la misma aplicación en grupos de entrega individuales de uno en uno.
- Compartir sesiones entre grupos de aplicaciones puede reducir el consumo de los recursos. En otros casos, la inhabilitación del uso compartido de sesiones entre grupos de aplicaciones puede ser beneficiosa.
- Puede usar la función de restricción por etiquetas para publicar aplicaciones desde un grupo de aplicaciones, con lo que solo se tiene en cuenta un subconjunto de las máquinas que contienen los grupos de entrega seleccionados. Con una restricción por etiquetas, puede usar las máquinas existentes para más de una tarea de publicación, con lo que se ahorran los costes asociados a la implementación y la administración de máquinas adicionales. La restricción por etiquetas puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Usar un grupo de aplicaciones o escritorios con una restricción por etiquetas puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

## Ejemplos de configuración

### Ejemplo 1

El gráfico siguiente muestra una implementación que incluye grupos de aplicaciones:




En esta configuración, las aplicaciones se agregan a los grupos de aplicaciones no a los grupos de entrega. Los grupos de entrega especifican qué máquinas se utilizarán. (Aunque no se muestra, las máquinas se encuentran en catálogos de máquinas.)

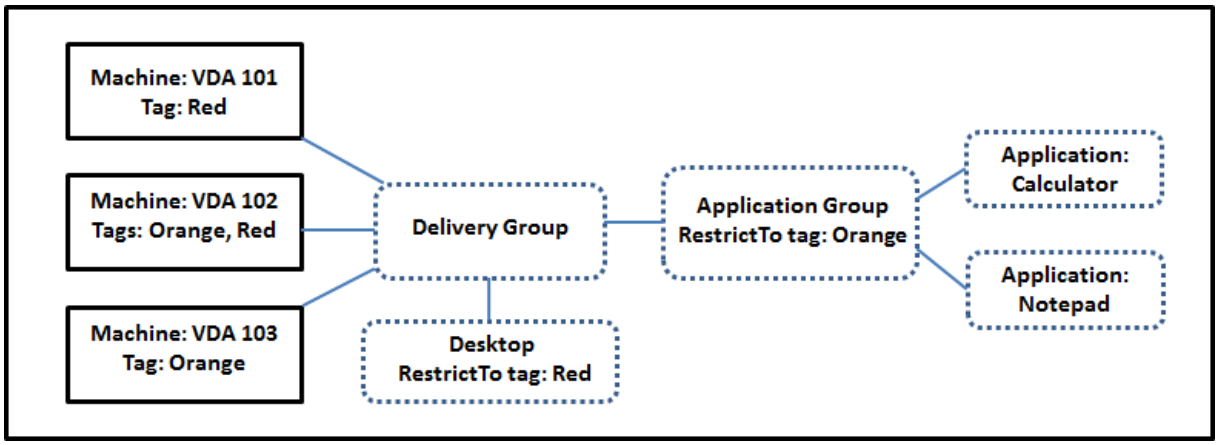
El grupo de aplicaciones 1 está asociado al grupo de entrega 1. A las aplicaciones del grupo de aplicaciones 1 tienen acceso los usuarios especificados en el grupo de aplicaciones 1, siempre y cuando también estén en la lista de usuarios del grupo de entrega 1. Esto es conforme a la recomendación de que la lista de usuarios de un grupo de aplicaciones debe ser un subconjunto (una restricción) de la lista de usuarios del grupo de entrega asociado. Los parámetros del grupo de aplicaciones 1 (tales como el uso compartido de sesiones entre grupos de aplicaciones y los grupos de entrega asociados) se aplican a las aplicaciones y los usuarios de ese grupo. Los parámetros del grupo de entrega 1 (tales como la función para usuarios anónimos) se aplican a los usuarios de los grupos de aplicaciones 1 y 2, porque esos grupos de aplicaciones se han asociado a ese grupo de entrega.

El grupo de aplicaciones 2 está asociado a dos grupos de entrega: 1 y 2. Se puede asignar una prioridad a cada uno de esos grupos de entrega en el grupo de aplicaciones 2, para indicar el orden en que se comprobarán los grupos de entrega cuando se inicie una aplicación. A las aplicaciones del grupo de aplicaciones 2 tienen acceso los usuarios especificados en el grupo de aplicaciones 2, siempre y cuando también estén en la lista de usuarios de los grupos de entrega 1 y 2.

**Ejemplo 2**

En esta sencilla distribución, se usan restricciones por etiqueta para limitar las máquinas que se tendrán en cuenta para ciertos inicios de aplicaciones y escritorios. El sitio tiene un grupo de entrega compartido, un escritorio publicado, y un grupo de aplicaciones configurado con dos aplicaciones.




Se han agregado etiquetas a cada una de las tres máquinas (VDA 101, 102 y 103).

El grupo de aplicaciones se creó con la restricción por etiquetas "Naranja", por lo que cada una de sus aplicaciones (Calculadora y Bloc de notas) solo se pueden iniciar en las máquinas de ese grupo de entrega que tengan la etiqueta "Naranja": VDA 102 y 103.

Para ver instrucciones y ejemplos más detallados sobre cómo usar las restricciones de etiqueta en los grupos de aplicaciones (y escritorios), consulte Etiquetas.

## Información orientativa y consideraciones

Citrix recomienda agregar aplicaciones a grupos de aplicaciones o grupos de entrega, pero no a ambos. De lo contrario, la complejidad de tener las aplicaciones asignadas a dos tipos de grupos puede complicar la administración de estas.

De forma predeterminada, hay un grupo de aplicaciones habilitado. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte Administrar grupos de aplicaciones.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones. Consulte Compartir sesiones entre grupos de aplicaciones.

Citrix recomienda actualizar la versión de los grupos de entrega a la actual. Eso requiere:

1. Actualizar la versión de los VDA de las máquinas utilizadas en el grupo de entrega.
2. Cambiar a un nivel funcional superior para los catálogos de máquinas que contienen esas máquinas

3. Cambiar a un nivel funcional superior para el grupo de entrega.

Para obtener más información, consulte Administrar grupos de entrega.

Para utilizar grupos de aplicaciones, los componentes principales deben tener la versión 7.9 como mínimo.

La creación de grupos de aplicaciones requiere el permiso de administración delegada correspondiente al rol integrado de Administrador de grupos de entrega. Para obtener información detallada, consulte Administración delegada.

Este artículo se refiere a la "asociación"de una aplicación con varios grupos de aplicaciones para diferenciarla de la acción de agregar una nueva instancia de esa aplicación desde algún origen disponible. Del mismo modo, los grupos de entrega se asocian a grupos de aplicaciones (y viceversa), en lugar de ser agregados como componentes unos de otros.

## Compartir sesiones con grupos de aplicaciones

Cuando se habilita la capacidad de compartir sesiones de aplicación, todas las aplicaciones se inician en la misma sesión de aplicación. Lo que reduce los costes asociados al inicio de aplicaciones adicionales y permite las funciones de aplicación que hacen uso del Portapapeles, como las operaciones de copiar y pegar contenido. Sin embargo, podría interesarle desactivar el uso compartido de sesiones en algunas situaciones.

Cuando se usan grupos de aplicaciones, se puede configurar el uso compartido de las sesiones de aplicación de las siguientes tres maneras (que amplían el comportamiento estándar del uso compartido de sesiones que solo está disponible cuando se usan grupos de entrega):

- Uso compartido de sesiones habilitado entre grupos de aplicaciones.
- Uso compartido de sesiones habilitado solamente entre las aplicaciones de un mismo grupo de aplicaciones.
- Uso compartido de sesiones inhabilitado.

### Compartir sesiones entre grupos de aplicaciones

Puede permitir que las sesiones de aplicaciones se compartan entre los grupos de aplicaciones, o bien, puede inhabilitarlo para limitar la capacidad de compartir sesiones solo a las aplicaciones que se encuentren en el mismo grupo de aplicaciones.

- **Este es un ejemplo de cuándo puede ser útil habilitar el uso compartido de sesiones entre los grupos de aplicaciones:**

  El grupo de aplicaciones 1 contiene aplicaciones de Microsoft Office como Word y Excel. El grupo de aplicaciones 2 contiene otras aplicaciones (como el Bloc de notas y la Calculadora), y ambos

grupos de aplicaciones están conectados al mismo grupo de entrega. Un usuario que tiene acceso a ambos grupos de aplicaciones inicia una sesión de aplicación mediante Word y, a continuación, el Bloc de notas. Si la sesión existente del usuario que ejecuta Word es adecuada para ejecutar el Bloc de notas, el Bloc de notas se iniciará dentro de la sesión existente. En cambio, si el Bloc de notas no se puede ejecutar en la sesión existente (por ejemplo, si la restricción por etiquetas excluye la máquina donde se ejecuta la sesión), se crea una nueva sesión en otra máquina, en lugar de compartir sesiones.

- **Este es un ejemplo de cuándo puede ser útil inhabilitar el uso compartido de sesiones entre los grupos de aplicaciones:**

  Tiene un conjunto de aplicaciones que no pueden interactuar correctamente con otras aplicaciones instaladas en las mismas máquinas: por ejemplo, dos versiones diferentes de una misma suite de software o dos versiones diferentes del mismo explorador web. Usted prefiere no permitir que un usuario inicie ambas versiones en una misma sesión.

  Puede crear un grupo de aplicaciones para cada versión de la suite de software y agregar las aplicaciones para cada versión de la suite al grupo de aplicaciones correspondiente. Si el uso compartido de sesiones entre los grupos se inhabilita para cada uno de esos grupos de aplicaciones, un usuario especificado en esos grupos puede ejecutar las aplicaciones de la misma versión en la misma sesión, y puede ejecutar otras aplicaciones al mismo tiempo, pero no en la misma sesión. Si el usuario inicia una de las aplicaciones de diferente versión (que se encuentra en un grupo de aplicaciones distinto) o inicia cualquier aplicación que no está contenida en un grupo de aplicaciones, esa aplicación se inicia en una nueva sesión.

Compartir sesiones entre los grupos de aplicaciones no es una función de seguridad de un espacio aislado. No es totalmente segura y no puede impedir que los usuarios inicien aplicaciones en sus sesiones por otros medios (por ejemplo, a través del Explorador de Windows).

Si una máquina alcanza su capacidad máxima, no se inician nuevas sesiones en ella. Las nuevas aplicaciones se inician en las sesiones existentes en la máquina compartiendo sesiones si fuera necesario (siempre que eso concuerde con las restricciones respecto a compartir sesiones que se describen aquí).

Solo se pueden ofrecer las sesiones preiniciadas a los grupos de aplicaciones que tienen permitido compartir sesiones (las sesiones que usan la función Persistencia de sesiones están disponibles a todos los grupos de aplicaciones). Esas funciones deben habilitarse y configurarse en cada uno de los grupos de entrega asociados al grupo de aplicaciones. No puede configurarlas en los grupos de aplicaciones.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte Administrar grupos de aplicaciones.

#### Inhabilitar el uso compartido de sesiones en un grupo de aplicaciones

Puede impedir que las aplicaciones que se encuentran en el mismo grupo compartan sesiones.

- **Este es un ejemplo de cuándo puede ser útil impedir que se compartan sesiones entre los grupos de aplicaciones:**

  Si quiere que los usuarios accedan a varias sesiones simultáneas de pantalla completa de una aplicación en varios monitores.

  Cree un grupo de aplicaciones y agréguele las aplicaciones. Si las aplicaciones de ese grupo no pueden compartir sesiones, cuando un usuario especificado en el grupo inicia una aplicación y después otra, las aplicaciones se inician en sesiones distintas y el usuario puede mover cada una a un monitor aparte.

De forma predeterminada, se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Después de crear un grupo de aplicaciones, puede modificar el grupo para cambiar este parámetro. Consulte Administrar grupos de aplicaciones.

### Crear un grupo de aplicaciones

Use el proceso de creación de un grupo de aplicaciones para crear categorías de aplicaciones en la aplicación Citrix Workspace. Las categorías de aplicaciones permiten administrar colecciones de aplicaciones en Citrix Workspace.

Para crear un grupo de aplicaciones:

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Para organizar grupos de aplicaciones mediante carpetas, cree carpetas en la carpeta raíz **Application Groups**.
3. Seleccione la carpeta en la que quiere crear el grupo y, a continuación, haga clic en **Crear grupo de entrega**. El asistente de creación de grupos se inicia con una página de **introducción**. Puede quitar la página para futuras versiones de este asistente.
4. Siga las instrucciones del asistente para configurar los parámetros en las páginas que se describen a continuación. Cuando haya terminado con cada página, seleccione **Siguiente** hasta llegar a la página **Resumen**.

#### Paso 1. Grupos de entrega

La página **Grupos de entrega** muestra todos los grupos de entrega, con la cantidad de máquinas que contiene cada grupo.

- La lista **Grupos de entrega compatibles** contiene los grupos de entrega que puede seleccionar. Los grupos de entrega compatibles contienen máquinas con SO de servidor o de escritorio aleatorias (no asignadas de manera permanente o estática).
- La lista **Grupos de entrega incompatibles** contiene grupos de entrega que no puede seleccionar. Cada entrada explica por qué no es compatible, como, por ejemplo, porque contienen máquinas asignadas estáticas.

Un grupo de aplicaciones se puede asociar a grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También puede seleccionar grupos de entrega que contengan máquinas compartidas que solo entregan escritorios, siempre que se cumplan las dos condiciones siguientes:

- El grupo de entrega contiene máquinas compartidas y se creó con una versión de XenDesktop anterior a 7.9.
- Usted tiene el permiso Modificar grupo de entrega.

El tipo de grupo de entrega se convierte automáticamente a "escritorios y aplicaciones"cuando se confirma el asistente Crear grupo de aplicaciones.

Aunque puede crear un grupo de aplicaciones que no tenga grupos de entrega asociados (por ejemplo, para organizar aplicaciones o para servir de almacenamiento para las aplicaciones que no se están utilizando en ese momento), el grupo de aplicaciones no se puede usar para entregar aplicaciones hasta que se especifica al menos un grupo de entrega. Además, no se pueden agregar aplicaciones al grupo de aplicaciones desde la opción de origen **Desde el menú Inicio** si no hay grupos de entrega especificados.

Los grupos de entrega que seleccione especifican las máquinas que se usarán para entregar aplicaciones. Marque las casillas que aparecen junto a los grupos de entrega que quiere asociar al grupo de aplicaciones.

Para agregar una restricción por etiquetas, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú desplegable.

#### Paso 2. Usuarios

Especifique quién puede usar las aplicaciones del grupo de aplicaciones. Puede permitir todos los usuarios y los grupos de usuarios de los grupos de entrega seleccionados en la página anterior, o puede seleccionar un grupo específico de usuarios y grupos de usuarios de los grupos de entrega. Si restringe el uso a unos cuantos usuarios especificados, solo los usuarios especificados en el grupo de entrega y el grupo de aplicaciones pueden acceder a las aplicaciones de este grupo de aplicaciones. Básicamente, la lista de usuarios del grupo de aplicaciones proporciona un filtro en las listas de usuarios de los grupos de entrega.

El uso de las aplicaciones por parte de usuarios no autenticados solo puede habilitarse o inhabilitarse en los grupos de entrega, no en los grupos de aplicaciones.

Para obtener información sobre dónde se especifican las listas de usuarios en una implementación, consulte Dónde se especifican las listas de usuarios.

#### Paso 3. Aplicaciones

Información útil:

- De forma predeterminada, las nuevas aplicaciones que agregue se colocan en una carpeta denominada **Aplicaciones**. Puede especificar otra carpeta. Si intenta agregar una aplicación y ya existe una con el mismo nombre en la carpeta, se le pedirá cambiar el nombre de la aplicación que está agregando. Si acepta el nombre único sugerido, la aplicación se agrega con ese nombre. De lo contrario, cambie el nombre antes de agregarla. Para obtener más información, consulte Administrar carpetas de aplicaciones.
- Puede cambiar las propiedades de una aplicación (parámetros) al agregarla, o más tarde. Consulte Cambiar las propiedades de la aplicación. Si publica dos aplicaciones con el mismo nombre para los mismos usuarios, cambie la propiedad **Nombre de la aplicación (para el usuario)** en la interfaz de administración de Configuración completa. De lo contrario, los usuarios verán nombres duplicados en la aplicación Citrix Workspace.
- Al agregar una aplicación a más de un grupo de entrega, puede haber un problema de visibilidad si no dispone de permisos suficientes para ver la aplicación en todos esos grupos de entrega. En tales casos, consulte a un administrador con más permisos o amplíe su ámbito para incluir todos los grupos a los que se haya agregado la aplicación.

Seleccione la lista desplegable **Agregar** para ver los orígenes de aplicación.

- **Desde el menú Inicio:** Se trata de las aplicaciones que se detectan en una máquina de los grupos de entrega seleccionados. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, seleccione **Aceptar**.

  Este origen no se puede seleccionar si seleccionó una de estas opciones:

  - Grupos de aplicaciones que no tienen grupos de entrega asociados.
  - Grupos de aplicaciones con grupos de entrega asociados que no contienen máquinas.
  - Un grupo de entrega que no contiene máquinas.

- **Manualmente:** Se trata de las aplicaciones que se encuentran en el sitio o en la red. Cuando se selecciona este origen, se abre una nueva página donde se escribe la ruta al archivo ejecutable, al directorio de trabajo, los argumentos de línea de comandos opcionales y los nombres simplificados para administradores y usuarios. Una vez introducida esta información, seleccione **Aceptar**.

- **Existentes**: Se trata de aplicaciones agregadas anteriormente al sitio. Cuando se selecciona este origen, se abre una nueva página con una lista de aplicaciones detectadas. Marque las casillas de verificación de las aplicaciones que quiere agregar y, a continuación, seleccione **Aceptar**. Este origen no se puede seleccionar si el sitio no contiene ninguna aplicación.
- **Paquetes de aplicaciones:** aplicaciones en paquetes de aplicaciones en formato App-V, MSIX, de conexión de aplicaciones MSIX o FlexApp. Al seleccionar este origen, se abre la página **Agregar aplicaciones desde paquetes**. Seleccione un origen del paquete de aplicaciones, en la pantalla resultante seleccione las aplicaciones que quiere agregar y después seleccione **Aceptar**

  > **Nota:**
  >
  > Para publicar aplicaciones en formato MSIX o de conexión de aplicaciones MSIX, el nivel funcional del grupo de entrega debe ser 2106 o posterior. Para las aplicaciones FlexApp, el nivel funcional debe ser 2206 o posterior. Cuando no se cumple un requisito de nivel funcional, las opciones correspondientes de la lista desplegable **Origen del paquete de aplicaciones** se muestran atenuadas.
  >
  > **Nota:**
  >
  > En VDA 2003 y versiones posteriores no se admite la publicación de paquetes de App-V desde direcciones URL HTTP. No puede seleccionar esas aplicaciones de la lista.

Como se ha indicado, algunas de las entradas de la lista desplegable **Agregar** no se pueden seleccionar si no existe ningún origen válido de ese tipo. Los orígenes que son incompatibles no aparecen (por ejemplo, no se pueden agregar grupos de aplicaciones a grupos de aplicaciones, por lo que ese origen no aparece en la lista cuando se crea un grupo de aplicaciones).

#### Paso 4. Ámbitos

Esta página aparecerá solo si se ha creado antes un ámbito personalizado. De forma predeterminada, está seleccionado el ámbito **Todo**. Para obtener más información, consulte Administración delegada.

#### Paso 5. Resumen

Escriba un nombre para el grupo de aplicaciones. También puede especificar una descripción (optativa).

Revise la información de resumen y, a continuación, seleccione **Finalizar**.

# Administrar grupos de aplicaciones

January 26, 2023

## Introducción

En este artículo, se describe cómo administrar grupos de aplicaciones después de crearlos.

Consulte Aplicaciones para obtener información sobre cómo administrar aplicaciones en los grupos de entrega o los grupos de aplicaciones, incluido cómo:

- Agregar o quitar aplicaciones en un grupo de aplicaciones.
- Cambiar asociaciones de grupos de aplicaciones.

La administración de grupos de aplicaciones requiere los permisos de administración delegada correspondientes al rol integrado de Administrador de grupos de entrega. Para obtener más información, consulte Administración delegada.

## Habilitar o inhabilitar un grupo de aplicaciones

Cuando se habilita un grupo de aplicaciones, este grupo puede distribuir las aplicaciones que se hayan agregado a él. Cuando se inhabilita un grupo de aplicaciones, se inhabilitan las aplicaciones incluidas en él. Sin embargo, si esas aplicaciones también están asociadas a otros grupos de aplicaciones que sí están habilitados, esas aplicaciones pueden seguir siendo entregadas desde esos otros grupos. Del mismo modo, si las aplicaciones se agregaron explícitamente a grupos de entrega asociados al grupo de aplicaciones (además de agregarlas al grupo de aplicaciones), cuando se inhabilita el grupo de aplicaciones esto no afecta a esas aplicaciones agregadas a esos grupos de entrega.

Un grupo de aplicaciones está habilitado cuando se crea. No puede cambiar esto cuando crea el grupo.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar grupo de aplicaciones**.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

### Habilitar o inhabilitar el uso compartido de sesiones de aplicación entre grupos de aplicaciones

Se pueden compartir sesiones entre grupos de aplicaciones cuando se crea un grupo de aplicaciones. No puede cambiar esto cuando crea el grupo. Para obtener más información, consulte Compartir sesiones con grupos de aplicaciones.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. En la página **Parámetros**, marque o desmarque la casilla **Habilitar uso compartido de sesiones de aplicaciones entre grupos de aplicaciones**.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

### Inhabilitar el uso compartido de sesiones de aplicación en un grupo de aplicaciones

De forma predeterminada, se pueden compartir sesiones de aplicaciones en el mismo grupo de aplicaciones cuando se crea un grupo de aplicaciones. Aunque inhabilite la posibilidad de compartir sesiones de aplicaciones entre grupos de aplicaciones, se podrán compartir sesiones entre aplicaciones del mismo grupo.

Puede usar el SDK de PowerShell para configurar grupos de aplicaciones con el uso compartido de sesiones inhabilitado entre las aplicaciones que contienen. En algunas circunstancias, esto puede ser conveniente. Por ejemplo, si quiere que los usuarios inicien aplicaciones no integradas en ventanas de aplicación de pantalla completa en monitores diferentes.

Cuando se inhabilita el uso compartido de sesiones dentro de un grupo de aplicaciones, cada aplicación de ese grupo se inicia en una nueva sesión de aplicación. Si está disponible una sesión desconectada adecuada (que ejecuta la misma aplicación), se vuelve a conectar a esa sesión. Por ejemplo, si se inicia el Bloc de notas y hay una sesión desconectada que ejecuta el Bloc de notas, se reconecta a esa sesión en lugar de crear una nueva. Si están disponibles varias sesiones desconectadas adecuadas, se elige una de ellas para reconectarse de forma aleatoria pero determinante. En otras palabras, si se vuelve a dar la situación en las mismas circunstancias, se selecciona la misma sesión, pero la elección no es necesariamente predecible en otras circunstancias

Puede usar el SDK de PowerShell para inhabilitar el uso compartido de sesiones de aplicación para todas las aplicaciones de un grupo existente, o bien, para crear un grupo de aplicaciones con el uso compartido de sesiones inhabilitado.

#### Ejemplos de cmdlets de PowerShell

Para inhabilitar el uso compartido de sesiones, use los cmdlets de Broker PowerShell New-BrokerApplicationGroup o Set-BrokerApplicationGroup con el parámetro SessionSharingEnabled establecido en False y el parámetro SingleAppPerSession establecido en True.

- Por ejemplo, para crear un grupo de aplicaciones con el uso compartido de sesiones de aplicación inhabilitado para todas las aplicaciones del grupo:

  ```
  New-BrokerApplicationGroup AppGr1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

- Por ejemplo, para inhabilitar el uso compartido de sesiones de aplicación entre todas las aplicaciones de un grupo de aplicaciones existente:

  ```
  Set-BrokerApplicationGroup AppGR1 -SessionSharingEnabled $False -SingleAppPerSession $True
  ```

#### Consideraciones

- Para habilitar la propiedad `SingleAppPerSession`, debe establecer la propiedad `SessionSharingEnabled` en False. No se deben habilitar las dos propiedades al mismo tiempo. El parámetro `SessionSharingEnabled` hace referencia a compartir sesiones entre grupos de aplicaciones.
- Compartir sesiones solo funciona para aplicaciones que están asociadas a grupos de aplicaciones, pero no están asociadas a grupos de entrega. Todas las aplicaciones que están asociadas directamente a un grupo de entrega comparten sesiones de forma predeterminada.
- Si una aplicación se asigna a varios grupos de aplicaciones, compruebe que los grupos no tienen parámetros en conflicto. Por ejemplo, un grupo tiene la opción establecida en True, mientras que el otro en False, lo que resulta en un comportamiento inesperado.

### Cambiar el nombre de un grupo de aplicaciones

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Cambiar nombre del grupo de aplicaciones** en la barra de acciones.
3. Especifique el nuevo nombre único y, a continuación, seleccione **Aceptar**.

### Agregar, quitar o cambiar la prioridad de las asociaciones de grupos de entrega con un grupo de aplicaciones

Un grupo de aplicaciones se puede asociar a grupos de entrega que contengan máquinas compartidas (no privadas) que puedan entregar aplicaciones.

También puede seleccionar grupos de entrega que contengan máquinas compartidas que solo entregan escritorios, siempre que se cumplan las dos condiciones siguientes:

- El grupo de entrega contiene máquinas compartidas y se creó con una versión anterior a 7.9.
- Usted tiene el permiso Modificar grupo de entrega.

El tipo de grupo de entrega se convierte automáticamente a "escritorios y aplicaciones"cuando se confirma el cuadro de diálogo **Modificar grupo de aplicaciones**.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. Seleccione la página **Grupos de entrega**.
4. Para agregar grupos de entrega, seleccione **Agregar**. Marque las casillas de los grupos de entrega disponibles (los grupos de entrega incompatibles no se pueden seleccionar). Una vez seleccionados, seleccione **Aceptar**.
5. Para eliminar grupos de entrega, marque las casillas de los grupos que quiere eliminar y luego seleccione **Eliminar**. Confirme la eliminación cuando se le solicite.
6. Para cambiar la prioridad de un grupo de entrega, marque la casilla de ese grupo y, a continuación, seleccione **Modificar prioridad**. Especifique una prioridad (0 = máxima prioridad) y, a continuación, seleccione **Aceptar**.
7. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

### Agregar, modificar o quitar una restricción por etiquetas en un grupo de aplicaciones

Agregar, modificar o quitar restricciones por etiqueta puede tener efectos no esperados en las máquinas que se tengan en cuenta para iniciar las aplicaciones. Consulte las precauciones y los aspectos a tener en cuenta en Etiquetas.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. Seleccione la página **Grupos de entrega**.

4. Para agregar una restricción por etiquetas, elija **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú.
5. Para cambiar o quitar una restricción por etiquetas, seleccione otra etiqueta del menú o quite la restricción por etiquetas por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.
6. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

### Agregar o quitar usuarios de un grupo de aplicaciones

Para obtener más información acerca de los usuarios, consulte Crear grupos de aplicaciones.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. Seleccione la página **Usuarios**. Indique si quiere permitir que todos los usuarios de los grupos de entrega asociados usen las aplicaciones del grupo de aplicaciones, o si solo quiere que la usen grupos y usuarios específicos. Para agregar usuarios, haga clic en **Agregar** y especifique los usuarios que quiere agregar. Para quitar usuarios, seleccione uno o varios usuarios y, a continuación, seleccione **Quitar**.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

### Agregar, cambiar o quitar un icono de aplicación en un grupo de aplicaciones

Lleve a cabo los siguientes pasos para agregar, cambiar o quitar un icono de aplicación.

1. En el panel de navegación, seleccione **Aplicaciones**.
2. En la ficha **Todas las aplicaciones**, seleccione una aplicación y, a continuación, seleccione **Propiedades**.

   Para realizar cambios al nivel del grupo de aplicaciones, vaya a la ficha **Grupos de aplicaciones**, seleccione una aplicación de un grupo y, a continuación, seleccione **Propiedades**.
3. Seleccione la página **Entrega** y, a continuación, seleccione **Cambiar**. Aparecerá la ventana **Seleccionar icono**.
4. En la ventana **Seleccionar icono**, realice una de las siguientes acciones:

   - Para agregar un icono, seleccione **Agregar** y, a continuación, vaya al icono.
   - Para quitar un icono, selecciónelo y, a continuación, seleccione **Quitar**.

- Para cambiar un icono, seleccione el icono de la aplicación.

> **Importante:**
>
> - No se pueden agregar iconos cuyo tamaño sea superior a 200 KB.
> - Solo se pueden agregar archivos .icon.
> - No se pueden quitar iconos integrados.
> - No se puede quitar el icono de una aplicación que está en uso.

5. Seleccione **Aceptar** para aplicar los cambios y cerrar la ventana.

### Cambiar ámbitos en un grupo de aplicaciones

Puede cambiar un ámbito solo si usted lo ha creado (no puede modificar el ámbito Todo). Para obtener más información, consulte Administración delegada.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones en el panel central y, a continuación, seleccione **Modificar grupo de aplicaciones** en la barra de acciones.
3. Seleccione la página **Ámbitos**. Marque o deje sin marcar la casilla de verificación situada junto a los ámbitos que desea cambiar.
4. Seleccione **Aplicar** para aplicar los cambios que haya hecho y deje la ventana abierta, o bien seleccione **Aceptar** para aplicar los cambios y cierre la ventana.

### Eliminar un grupo de aplicaciones

La aplicación debe estar asociada a, al menos, un grupo de entrega o un grupo de aplicaciones. Si eliminar un grupo de aplicaciones provocará que una o varias aplicaciones dejen de pertenecer a un grupo, se le advierte que, al eliminar el grupo, también se eliminarán esas aplicaciones. Entonces, puede confirmar o cancelar la eliminación.

Eliminar una aplicación aquí no la elimina de su lugar de origen. Sin embargo, si quiere que la aplicación vuelva a estar disponible, tendrá que volver a agregarla.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda y, a continuación, seleccione la ficha **Grupos de aplicaciones**.
2. Seleccione un grupo de aplicaciones y, a continuación, seleccione **Eliminar grupo** en la barra de acciones.
3. Confirme la eliminación cuando se le solicite.

## Organizar grupos de aplicaciones mediante carpetas

Puede crear carpetas para organizar grupos de aplicaciones y acceder a ellos fácilmente.

### Roles obligatorios

De forma predeterminada, debe tener uno de estos roles integrados para crear y administrar carpetas para grupos de aplicaciones:

- Administrador de Cloud
- Administrador total
- Administrador de grupos de aplicaciones

Puede delegar acciones de administración a otros usuarios mediante la creación de roles personalizados. En esta tabla se enumeran los permisos necesarios para cada acción.

| Acción | Permisos requeridos |
|---|---|
| Crear carpetas de grupos de aplicaciones | Crear carpeta de grupo de aplicaciones |
| Eliminar carpetas de grupos de aplicaciones | Quitar carpeta de grupo de aplicaciones |
| Mover carpetas de grupos de aplicaciones | Mover carpeta de grupo de aplicaciones |
| Cambiar el nombre de carpetas de grupos de aplicaciones | Modificar carpeta de grupo de aplicaciones |
| Mover grupos de aplicaciones a carpetas | Modificar carpeta de grupo de aplicaciones, Modificar propiedades del grupo de aplicaciones |

Para obtener más información, consulte Crear y gestionar roles.

### Crear y administrar carpetas

Puede utilizar la barra Acciones o el menú contextual para crear y administrar carpetas de grupos de aplicaciones. Además, puede arrastrar un grupo de aplicaciones o una carpeta a la ubicación que quiera en el árbol de carpetas.

Información útil:

- Puede anidar carpetas en hasta cinco niveles (excluyendo la carpeta raíz predeterminada).
- Una carpeta puede contener grupos de aplicaciones y subcarpetas. Solo puede eliminar una carpeta si ni dicha carpeta ni sus subcarpetas contienen grupos de aplicaciones.

- Todos los recursos de Configuración completa (como catálogos de máquinas, grupos de entrega, aplicaciones y grupos de aplicaciones) comparten un árbol de carpetas en el back-end. Para evitar conflictos de nombres con otras carpetas de recursos al cambiar el nombre de las carpetas o al moverlas, le recomendamos que asigne nombres diferentes a las carpetas de primer nivel de los distintos árboles de carpetas.

## Acceso con Remote PC

August 28, 2023

> **Nota:**
>
> En este artículo, se describe cómo configurar Acceso con Remote PC mediante la interfaz Configuración completa. Si utiliza la interfaz de Distribución rápida, siga las instrucciones que se indican en Acceso con Remote PC en Distribución rápida.

Acceso con Remote PC es una funcionalidad de Citrix Virtual Apps and Desktops, gracias a la cual las organizaciones pueden hacer que sus empleados accedan fácilmente a los recursos corporativos de forma remota y segura. La plataforma Citrix hace posible este acceso seguro al proporcionar a los usuarios acceso a sus PC físicos de oficina. Si los usuarios pueden acceder a sus PC de oficina, pueden acceder a todas las aplicaciones, datos y recursos que necesitan para hacer su trabajo. Acceso con Remote PC elimina la necesidad de introducir y proporcionar otras herramientas para adaptarse al teletrabajo. Por ejemplo: aplicaciones o escritorios virtuales y su infraestructura asociada.

Acceso con Remote PC utiliza los mismos componentes de Citrix Virtual Apps and Desktops que facilitan aplicaciones y escritorios virtuales. Como resultado, los requisitos y el proceso de implementación y configuración de Acceso con Remote PC son los mismos que los necesarios para implementar Citrix Virtual Apps and Desktops para la entrega de recursos virtuales. Esta uniformidad ofrece una experiencia de administración homogénea y unificada. Los usuarios disfrutan de la mejor experiencia posible al utilizar Citrix HDX para la entrega de sesiones de PC de oficina.

La función consta de un catálogo de máquinas de tipo **Acceso con Remote PC** que proporciona la siguiente funcionalidad:

- Posibilidad de agregar máquinas especificando unidades organizativas. Esta capacidad facilita la agregación de PC en bloque.
- Posibilidad de agregar máquinas en bloque a partir de archivos CSV. Esta capacidad facilita la operación de agregar PC en bloque cuando se dan restricciones de estructura de unidad organizativa.
- Asignación automática de usuarios basada en el usuario que inicia sesión en el PC de oficina con Windows. La funcionalidad es compatible con asignaciones de un solo usuario y de múltiples

usuarios. De forma predeterminada, Citrix DaaS asigna automáticamente varios usuarios a la siguiente máquina sin asignar. Para restringir la asignación automática a un solo usuario, vaya a **Configuración completa > Parámetros** y desactive el parámetro **Habilitar la asignación automática de varios usuarios para el acceso con Remote PC** .

Citrix Virtual Apps and Desktops puede acomodar otros casos de uso de PC físicos si se utilizan otros tipos de catálogos de máquinas. Entre los casos de uso, se incluyen:

- PC Linux físicos
- PC físicos agrupados (es decir, asignados aleatoriamente, no dedicados)

> **Notas:**
>
> Para obtener información detallada sobre las versiones de sistema operativo compatibles, consulte los requisitos del sistema para VDA de SO de sesión única y Linux VDA.
>
> Para implementaciones locales, el acceso con Remote PC solo es válido para licencias de Citrix DaaS Advanced o Premium. Las sesiones consumen licencias del mismo modo que otras sesiones de Citrix Virtual Desktops. Para Citrix Cloud, el acceso con Remote PC es válido para Citrix DaaS y Workspace Premium Plus.

## Consideraciones

Aunque todos los requisitos técnicos y consideraciones aplicables a Citrix Virtual Apps and Desktops y Citrix DaaS en general también son aplicables a acceso con Remote PC, algunos pueden ser más relevantes o específicos para el caso de uso de PC físico.

> **Importante:**
>
> Los sistemas físicos Windows 11 (y algunos que ejecutan Windows 10) incluyen funciones de seguridad basadas en virtualización que hacen que el software VDA los detecte incorrectamente como máquinas virtuales. Para mitigar este problema, tiene las siguientes opciones:
>
> - Utilice la opción “/physicalmachine”junto con la opción “/remotepc”como parte de la instalación mediante línea de comandos del VDA
> - Agregue este valor del Registro después de instalar el VDA si no se utilizó la opción antes mencionada
>   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`
>
>   - Nombre: ForceEnableRemotePC
>   - Tipo: DWORD
>   - Datos: 1

### Consideraciones sobre la implementación

Mientras planifica la implementación de Acceso con Remote PC, debe adoptar algunas decisiones generales.

- Puede agregar Acceso con Remote PC a una implementación existente de Citrix Virtual Apps and Desktops y Citrix DaaS. Antes de elegir esta opción, considere lo siguiente:
  - ¿Tienen los Delivery Controllers o Cloud Connectors actuales el tamaño adecuado para acomodar la carga adicional asociada a los VDA de acceso con Remote PC?
  - ¿Tienen las bases de datos locales del sitio y los servidores de bases de datos el tamaño adecuado para acomodar la carga adicional asociada a los VDA de acceso con Remote PC?
  - ¿Superarán los VDA existentes y los nuevos VDA de acceso con Remote PC el número máximo de VDA admitidos por sitio?
- Deberá implementar el VDA en los PC de oficina mediante un proceso automatizado. A continuación, se indican dos opciones disponibles:
  - Herramientas de distribución electrónica de software (ESD) como SCCM: Instalar agentes VDA mediante SCCM.
  - Scripts de implementación: Instalar agentes VDA mediante scripts.
- Consulte las consideraciones de seguridad sobre el acceso con Remote PC.

### Consideraciones acerca del catálogo de máquinas

El tipo de catálogo de máquinas requerido depende del caso de uso:

- Catálogo de máquinas de acceso con Remote PC
  - Equipos dedicados con Windows/Linux
  - Equipos multiusuario Windows/Linux dedicados Este caso de uso es aplicable a los equipos de oficina físicos a los que diferentes usuarios pueden acceder de forma remota en distintos turnos.
  - Equipos Windows/Linux agrupados. Este caso de uso es aplicable a los PC físicos a los que pueden acceder varios usuarios aleatorios, como los laboratorios informáticos.

Una vez que haya identificado el tipo de catálogo de máquinas, tenga en cuenta lo siguiente:

- Una máquina solo se puede asignar a un catálogo de máquinas a la vez.
- Para facilitar la administración delegada, considere la posibilidad de crear catálogos de máquinas basados en la ubicación geográfica, el departamento o cualquier otra agrupación que facilite la delegación de la administración de cada catálogo a los administradores correspondientes.

- Al elegir las unidades organizativas en las que residen las cuentas de máquina, seleccione unidades organizativas de nivel inferior para lograr una mayor granularidad. Si no se requiere una granularidad tan estricta, puede elegir unidades organizativas de nivel superior. Por ejemplo: en el caso de bancos, funcionarios o cajeros, seleccione **cajeros**. De lo contrario, puede seleccionar **funcionarios** o **bancos**, en función de los requisitos.
- Mover o eliminar unidades organizativas después de que se hayan asignado a un catálogo de máquinas de acceso con Remote PC afecta a las asociaciones de VDA y genera problemas con futuras asignaciones. Por lo tanto, asegúrese de planificar convenientemente, de manera que la actualización de asignaciones de unidades organizativas para catálogos de máquinas se tenga en cuenta en el plan de cambios de Active Directory.
- Puede optar por utilizar unidades organizativas para agregar máquinas en bloque al catálogo de máquinas. En algunos casos, eso no es fácil debido a restricciones en la estructura de las unidades organizativas. En su lugar, puede agregar máquinas en bloque mediante archivos CSV. Esta función ofrece más flexibilidad para agregar máquinas en bloque. Puede agregar máquinas solamente (para utilizarlas con asignaciones automáticas de usuarios) o agregar máquinas junto con asignaciones de usuarios.
- Wake on LAN integrada solo está disponible con el catálogo de máquinas de tipo **acceso con Remote PC**.

### Consideraciones acerca de Linux VDA

Estas consideraciones son específicas de Linux VDA:

- Está disponible la opción de ocultación del monitor físico para los VDA de acceso con Remote PC, pero no para todas las distribuciones Linux. Para las distribuciones de Linux no compatibles, utilice Linux VDA en máquinas físicas solo en modo que no sea 3D. De lo contrario, debido a las limitaciones del controlador de NVIDIA, la pantalla local del PC no se puede oscurecer completamente y muestra las actividades de la sesión cuando el modo HDX 3D está habilitado. Mostrar esta pantalla representa un riesgo para la seguridad.
- Con máquinas Linux físicas, se recomienda el uso de catálogos de máquinas de tipo SO de sesión única.

### Requisitos técnicos y consideraciones

En esta sección, se incluyen los requisitos técnicos y consideraciones para PC físicos.

- Las siguientes opciones no se admiten:
  - Los conmutadores KVM u otros componentes que pueden desconectar una sesión.

  - Los equipos híbridos, incluidos los equipos portátiles y de sobremesa todo en uno y con NVIDIA Optimus.
  - Máquinas de arranque dual.

- Conecte el teclado y el mouse directamente al PC. La conexión al monitor u otros componentes que se pueden apagar o desconectar puede hacer que estos periféricos no estén disponibles. Si tiene que conectar los dispositivos de entrada a componentes como monitores, no apague esos componentes.
- Los PC deben unirse a un dominio de Active Directory Domain Services.
- La funcionalidad Arranque seguro solo es compatible con Windows 10.
- El PC debe tener una conexión de red activa. Se recomienda una conexión por cable para una mayor fiabilidad y ancho de banda.
- Si utiliza Wi-Fi, haga lo siguiente:

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

- Puede utilizar el acceso con Remote PC en equipos portátiles. Asegúrese de que el portátil esté conectado a una fuente de alimentación, en lugar de funcionar con batería. Configure las opciones de energía del portátil de manera que coincidan con las de un PC de escritorio. Por ejemplo:

  1. Inhabilite la función de hibernación.
  2. Inhabilite la función de suspensión.
  3. Establezca la opción **No hacer nada** en la acción de cierre de tapa.
  4. Establezca la opción **Apagar** en la acción al presionar el botón de encendido.
  5. Inhabilite las funciones de ahorro de energía de las tarjetas de vídeo y de las tarjetas de interfaz de red.

- Acceso con Remote PC es compatible con dispositivos Surface Pro con Windows 10. Siga las mismas pautas para los portátiles mencionados anteriormente.
- Si utiliza una base de acoplamiento, puede desacoplar y reacoplar portátiles. Al desacoplar un portátil, el VDA vuelve a registrarse con los Delivery Controllers o los Cloud Connectors a través de Wi-Fi. Sin embargo, al reacoplarlo, el VDA no pasa a usar la conexión por cable a menos que desconecte el adaptador inalámbrico. Algunos dispositivos ofrecen una funcionalidad integrada para desconectar el adaptador inalámbrico al establecerse una conexión por cable.

Los demás dispositivos requieren soluciones personalizadas o utilidades de terceros para desconectar el adaptador inalámbrico. Consulte las consideraciones mencionadas anteriormente acerca de las redes Wi-Fi.

Para habilitar el acoplamiento y el desacoplamiento de dispositivos de acceso con Remote PC, haga lo siguiente:

1. En el menú **Inicio**, seleccione **Configuración > Sistema > Inicio/apagado y suspensión** y establezca **Suspender** en **Nunca**.
2. En **Administrador de dispositivos > Adaptadores de red > Adaptador Ethernet**, vaya a **Administración de energía** y desmarque la opción **Permitir que el equipo apague este dispositivo para ahorrar energía**. Asegúrese de que la opción **Permitir que este dispositivo reactive el equipo** está marcada.

- Varios usuarios con acceso al mismo PC de oficina ven el mismo icono de Citrix Workspace. Cuando un usuario inicia sesión en Citrix Workspace, ese recurso aparece como no disponible si otro usuario ya lo está utilizando.
- Instale la aplicación Citrix Workspace en cada dispositivo cliente (por ejemplo, un equipo casero) que acceda al PC de la oficina.

### Secuencia de configuración

Esta sección contiene una descripción general de cómo configurar el acceso con Remote PC cuando se utiliza el catálogo de máquinas de tipo **Acceso con Remote PC**. Para obtener información sobre cómo crear otros tipos de catálogos de máquinas, consulte Crear catálogos de máquinas.

1. Solo para un sitio local: Para utilizar la función Wake on LAN integrada, configure los requisitos previos descritos en Wake on LAN.
2. Si se creó un nuevo sitio de Citrix Virtual Apps and Desktops para el acceso con Remote PC:

   a) Seleccione el tipo de sitio del **acceso con Remote PC**.
   b) En la página **Administración de energía**, habilite o inhabilite la administración de energía del catálogo de máquinas predeterminado de acceso con Remote PC. Puede cambiar esta configuración más adelante modificando las propiedades del catálogo de máquinas. Para obtener más información sobre la configuración de Wake on LAN, consulte Wake on LAN.
   c) Complete la información en las páginas **Usuarios** y **Cuentas de máquina**.

   Al completar estos pasos, se crea un catálogo de máquinas llamado **Máquinas de acceso con Remote PC** y un grupo de entrega llamado **Escritorios de acceso con Remote PC**.
3. Si se agrega a un sitio existente de Citrix Virtual Apps and Desktops:

a) Cree un catálogo de máquinas de tipo **Acceso con Remote PC** (página Sistema operativo del asistente). Para obtener información detallada sobre cómo crear un catálogo de máquinas, consulte Crear catálogos de máquinas. Asegúrese de asignar la unidad organizativa correcta para que los equipos de destino estén disponibles para uso con acceso con Remote PC.

b) Cree un grupo de entrega para proporcionar a los usuarios acceso a los equipos del catálogo de máquinas. Para obtener información detallada sobre cómo crear un grupo de entrega, consulte Crear grupos de entrega. Asegúrese de asignar el grupo de entrega a un grupo de Active Directory que contenga los usuarios que requieren acceso a sus equipos.

4. Implemente el VDA en los PC de oficina.

   - Se recomienda utilizar el instalador de componentes principales para instalar VDA de SO de sesión única (`VDAWorkstationCoreSetup.exe`).
   - También puede utilizar el instalador completo de VDA de SO de sesión única (`VDAWorkstationSetup.exe`) con la opción `/remotepc /physicalmachine`, que ofrece el mismo resultado que usar el instalador básico de VDA.
   - Considere la posibilidad de habilitar la Asistencia remota de Windows para que los equipos del servicio de asistencia puedan proporcionar asistencia remota a través de Citrix Director. Para ello, utilice la opción `/enable_remote_assistance`. Para obtener más información, consulte Instalación desde la línea de comandos.
   - Para poder ver la información sobre la duración del inicio de sesión en Director, debe utilizar el instalador completo de VDA de SO de sesión única e incluir el componente **Citrix User Profile Management WMI Plugin**. Para incluir este componente, utilice la opción `/includeadditional`. Para obtener más información, consulte Instalación desde la línea de comandos.
   - Para obtener información sobre cómo implementar el VDA con SCCM, consulte Instalar agentes VDA mediante SCCM.
   - Para obtener información sobre cómo implementar el VDA con scripts de implementación, consulte Instalar agentes VDA mediante scripts.

   Después de completar correctamente los pasos 2 a 4, los usuarios se asignan automáticamente a sus propias máquinas cuando inician sesión localmente en los PC.

5. Indique a los usuarios que descarguen e instalen la aplicación Citrix Workspace en cada dispositivo cliente que utilicen para acceder al equipo de oficina de forma remota. La aplicación Citrix Workspace está disponible en la página de descargas de Citrix o en los almacenes de aplicaciones para los dispositivos móviles compatibles.

### Funciones administradas a través del Registro

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

#### Modo de suspensión (versión mínima 7.16)

Para permitir que un equipo de acceso con Remote PC entre en el modo de suspensión, agregue este parámetro al Registro en el VDA y reinicie la máquina. Después del reinicio, se respetan los parámetros de ahorro de energía del sistema operativo. La máquina entra en el modo de suspensión pasado el tiempo preconfigurado en el temporizador de inactividad. Después de que la máquina despierte, vuelve a registrarse en el Delivery Controller.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nombre: DisableRemotePCSleepPreventer
- Tipo: DWORD
- Datos: 1

#### Administrar sesiones

De forma predeterminada, la sesión de un usuario remoto se desconecta automáticamente cuando un usuario local inicia una sesión en esa máquina (presionando CTRL + ALT + SUPR). Para evitar esta acción automática, agregue la siguiente entrada de Registro en el PC de la oficina y, a continuación, reinícielo.

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nombre: SasNotification
- Tipo: DWORD
- Datos: 1

De forma predeterminada, el usuario remoto tiene preferencia sobre el usuario local cuando el mensaje de conexión no se reconoce dentro del plazo de tiempo de espera. Para configurar el comportamiento, utilice este parámetro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC`

- Nombre: RpcaMode
- Tipo: DWORD

- Datos:
  - 1: El usuario remoto siempre tiene preferencia si no responde a los mensajes de la interfaz de usuario en el tiempo de espera especificado. Este comportamiento es el predeterminado si este parámetro no está configurado.
  - 2: El usuario local tiene preferencia.

De forma predeterminada, el tiempo de espera para aplicar el modo de acceso con Remote PC es de 30 segundos. Puede configurar este tiempo de espera, pero no lo establezca en menos de 30 segundos. Para configurar el tiempo de espera, utilice este parámetro de Registro:

`HKLM\SOFTWARE\Citrix\PortICA\RemotePC`

- Nombre: RpcaTimeout
- Tipo: DWORD
- Datos: número de segundos de tiempo de espera en valores decimales

Cuando el usuario local quiera forzar el acceso a la consola, puede presionar Ctrl + Alt + Supr dos veces en 10 segundos para obtener el control local sobre una sesión remota y forzar la desconexión.

Después de cambiar el Registro y reiniciar la máquina, si un usuario local presiona Ctrl + Alt + Supr para iniciar sesión en ese PC mientras está siendo utilizado por un usuario remoto, el usuario remoto recibe un mensaje. En el mensaje, se le pregunta si quiere permitir o denegar la conexión del usuario local. Si permite la conexión, la sesión del usuario remoto se desconecta.

### Wake on LAN

La función de acceso con Remote PC admite Wake on LAN, el cual ofrece a los usuarios la capacidad de encender equipos físicos de forma remota. Esta función permite a los usuarios mantener apagados sus equipos de oficina cuando no estén en uso, lo que reduce los costes de energía. También permite el acceso remoto cuando una máquina se ha apagado inadvertidamente.

Con la función Wake on LAN, los Magic Packets se envían directamente desde el VDA a la subred en la que reside el equipo cuando se lo indica el Delivery Controller. Esto permite que la función no requiera dependencias de componentes de infraestructura adicionales ni soluciones de terceros para la entrega de Magic Packets.

La función Wake on LAN difiere de la función Wake on LAN que se basa en una versión de SCCM antigua. La función Wake on LAN integrada en SCCM es una alternativa a Wake on LAN para el acceso con Remote PC que solo está disponible con instancias de Citrix Virtual Apps and Desktops locales. Para obtener información sobre Wake on LAN basada en SCCM, consulte Función Wake on LAN integrada en SCCM.

### Requisitos del sistema

A continuación, se indican los requisitos del sistema para usar la función Wake on LAN:

- Plano de control:
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2009 o una versión posterior
- PC físicos:
  - Versión 2009 de VDA o una posterior
  - Windows 10 o Windows 11. Para obtener información detallada sobre la compatibilidad, consulte los requisitos del sistema de VDA.
  - Wake on LAN habilitado en BIOS/UEFI
  - Wake on LAN habilitado en las propiedades del adaptador de red dentro de la configuración de Windows

### Configurar Wake on LAN

Para configurar Wake on LAN, puede utilizar la interfaz de administración de Configuración completa o PowerShell.

**Configurar Wake on LAN en la interfaz de Configuración completa** Para crear la conexión Wake on LAN:

1. Vaya al nodo **Alojamiento** de la izquierda.
2. Seleccione **Agregar conexión y recursos**.
3. En la página **Conexión** del asistente, proporcione la información siguiente:
   a) Tipo de conexión: Wake on LAN para Remote PC
   b) Nombre de la zona: Seleccione la zona en la que reside el catálogo de acceso con Remote PC
   c) Nombre de la conexión: Escriba el nombre de la conexión Wake on LAN.
4. Finalice los pasos restantes del asistente Agregar conexión y recursos.

Para agregar la conexión Wake on LAN a un catálogo de máquinas de acceso con Remote PC:

1. Si va a crear un nuevo catálogo de máquinas de acceso con Remote PC, puede agregar la conexión mediante la lista desplegable de la página **Tipo de máquina** del asistente Configuración de catálogo de máquinas.
2. Si quiere agregar la conexión Wake on LAN a un catálogo de máquinas existente:

a) Vaya al nodo **Catálogos de máquinas** de la izquierda.
b) Seleccione el catálogo de máquinas de acceso con Remote PC apropiado.
c) Haga clic con el botón secundario en el catálogo de máquinas o seleccione el menú **Más** arriba.
d) Seleccione **Modificar catálogo de máquinas**.
e) En la página **Administración de energía**, seleccione **Sí**.
f) Seleccione la conexión adecuada en la lista desplegable.
g) Seleccione **Guardar**.

> **Nota:**
>
> En este momento, la configuración de Wake on LAN a través de la interfaz de configuración completa solo está disponible con Citrix DaaS.

**Configurar Wake on LAN a través de PowerShell** Para configurar Wake on LAN a través de PowerShell:

1. Cree el catálogo de máquinas de acceso con Remote PC si aún no tiene uno.
2. Cree la conexión de host Wake on LAN si aún no tiene una.
3. Obtenga el identificador único de la conexión de host Wake on LAN.
4. Asocie la conexión de host Wake on LAN a un catálogo de máquinas.

Para crear la conexión de host Wake on LAN:

```
# Load Citrix SnapIns
Add-PSSnapIn -Name "\*citrix\*"

# Provide the name of the Wake on LAN host connection
[string]$connectionName = "Remote PC Access Wake on LAN"

# Create the hypervisor connection
$hypHc = New-Item -Path xdhyp:\Connections `
                -Name $connectionName `
                -HypervisorAddress "N/A" `
                -UserName "woluser" `
                -Password "wolpwd" `
                -ConnectionType Custom `
                -PluginId VdaWOLMachineManagerFactory `
                -CustomProperties "<CustomProperties></CustomProperties
                   >" `
                -Persist

$bhc = New-BrokerHypervisorConnection -HypHypervisorConnectionUid
   $hypHc.HypervisorConnectionUid

# Wait for the connection to be ready before trying to use it
while (-not $bhc.IsReady)
{
```

```
23
24      Start-Sleep -s 5
25      $bhc = Get-BrokerHypervisorConnection -HypHypervisorConnectionUid
            $hypHc.HypervisorConnectionUid
26   }
27
28  <!--NeedCopy-->
```

Cuando la conexión de host esté lista, ejecute los siguientes comandos para obtener el identificador único de la conexión de host:

```
1  $bhc = Get-BrokerHypervisorConnection -Name "<WoL Connection Name>"
2  $hypUid = $bhc.Uid
3  <!--NeedCopy-->
```

Después de obtener el identificador único de la conexión, ejecute los siguientes comandos para asociar la conexión al catálogo de máquinas de acceso con Remote PC:

```
1  Get-BrokerCatalog -Name "<Catalog Name>" | Set-BrokerCatalog -
       RemotePCHypervisorConnectionUid $hypUid
2  <!--NeedCopy-->
```

#### Consideraciones sobre el diseño

Cuando planee usar Wake on LAN con acceso con Remote PC, tenga en cuenta lo siguiente:

- Varios catálogos de máquinas pueden utilizar la misma conexión de host Wake on LAN.
- Para que un equipo reactive otro equipo, ambos deben estar en la misma subred y utilizar la misma conexión de host Wake on LAN. No importa si los equipos están en los mismos catálogos de máquinas o en catálogos diferentes.
- Las conexiones de host se asignan a zonas específicas. Si la implementación contiene más de una zona, debe disponer de una conexión de host Wake on LAN en cada zona. Lo mismo es aplicable a los catálogos de máquinas.
- Los Magic Packets se transmiten mediante la dirección de difusión global 255.255.255.255. Asegúrese de que la dirección no esté bloqueada.
- Debe haber al menos un equipo encendido en la subred por cada conexión Wake on LAN para poder activar máquinas en esa subred.

#### Consideraciones operativas

A continuación, se incluyen consideraciones para uso de la función Wake on LAN:

- El VDA debe registrarse al menos una vez antes de que el PC pueda activarse mediante la función Wake on LAN integrada.

- Wake on LAN solo se puede utilizar para activar PC. No admite otras acciones de energía, como reinicio o apagado.
- Los Magic Packets se envían de una de dos maneras:
  1. Cuando un usuario intenta iniciar una sesión en su PC y el VDA no está registrado
  2. Cuando un administrador envía manualmente un comando de encendido desde la interfaz de Configuración completa o PowerShell
- Como el Delivery Controller no conoce el estado de energía de un equipo, la interfaz de Configuración completa muestra **No compatible** en el estado de energía. El Delivery Controller utiliza el estado del registro del VDA para determinar si un equipo está encendido o apagado.

## Solucionar problemas

### La puesta en blanco del monitor no funciona

Si el monitor local del PC con Windows no se pone en blanco mientras hay una sesión HDX activa (el monitor local muestra lo que está sucediendo en la sesión) es probable que se deba a problemas con el controlador del proveedor de la GPU. Para resolver el problema, asigne a Citrix Indirect Display Driver (IDD) una prioridad mayor que al controlador del proveedor de la tarjeta gráfica estableciendo el siguiente valor del Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Graphics\AdapterMerits`

- Nombre: CitrixIDD
- Tipo: DWORD
- Datos: 3

Para obtener más información acerca de las prioridades del adaptador de pantalla y la creación de monitores, consulte el artículo CTX237608 de Knowledge Center.

### La sesión se desconecta cuando se selecciona Ctrl+Alt+Supr en la máquina que tiene habilitada la notificación de administración de sesiones

La notificación de administración de sesiones, controlada por el valor de Registro **SasNotification**, solo funciona cuando el modo acceso con Remote PC está habilitado en el VDA. Si el PC físico tiene habilitado el rol Hyper-V o alguna otra función de seguridad basada en la virtualización, el PC informa como una máquina virtual. Si el VDA detecta que se está ejecutando en una máquina virtual, inhabilita automáticamente el modo acceso con Remote PC. Para habilitar el modo acceso con Remote PC, agregue el siguiente valor de Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nombre: ForceEnableRemotePC
- Tipo: DWORD
- Datos: 1

Reinicie el PC para que la configuración surta efecto.

#### Información de diagnóstico

El diagnóstico sobre el acceso con Remote PC se escribe en el registro de eventos de aplicación que ofrece Windows. Los mensajes informativos no tienen limitaciones. Los mensajes de error se limitan mediante el descarte de mensajes duplicados.

- 3300 (informativo): Máquina agregada al catálogo
- 3301 (informativo): Máquina agregada al grupo de entrega
- 3302 (informativo): Máquina asignada al usuario
- 3303 (error): Excepción

#### Administración de energía

Cuando se habilita la administración de energía para el acceso con Remote PC, es posible que las difusiones dirigidas a subredes no puedan iniciar las máquinas que se encuentran en una subred diferente a la del Controller. Si necesita la administración de energía en las subredes que utilicen difusiones dirigidas a subredes y la tecnología AMT no está disponible, pruebe el método de unidifusión o de proxy de reactivación. Compruebe que estos parámetros están habilitados en las propiedades avanzadas de la administración de energía de la conexión.

#### La sesión remota activa graba la entrada de la pantalla táctil local

Cuando el VDA habilita el modo acceso con Remote PC, la máquina ignora la entrada de la pantalla táctil local durante una sesión activa. Si el PC físico tiene habilitado el rol Hyper-V o alguna otra función de seguridad basada en la virtualización, el PC informa como una máquina virtual. Si el VDA detecta que se está ejecutando en una máquina virtual, inhabilita automáticamente el modo acceso con Remote PC. Para habilitar el modo acceso con Remote PC, agregue el siguiente parámetro de Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PortICA`

- Nombre: ForceEnableRemotePC
- Tipo: DWORD
- Datos: 1

Reinicie el PC para que la configuración surta efecto.

### Más recursos

A continuación, se muestran otros recursos para acceso con Remote PC:

- Guía de diseño de soluciones: Remote PC Access Design Decisions.
- Ejemplos de arquitecturas de acceso con Remote PC: Reference Architecture for Citrix Remote PC Access Solution.

## Eliminar componentes

August 28, 2023

Para quitar los componentes que haya instalado (como agentes VDA), Citrix recomienda usar la función de Windows para quitar o cambiar programas. También puede quitar componentes desde la línea de comandos o con un script.

Cuando se quitan componentes, no se eliminan sus requisitos previos ni se cambian los parámetros del firewall.

Al quitar un VDA, la máquina se reinicia automáticamente después de la eliminación de forma predeterminada.

### Eliminar componentes con la función de Windows para quitar o cambiar programas

Con la función de Windows para quitar o cambiar programas:

- Para quitar un VDA, seleccione **Citrix Virtual Delivery Agent** <*versión*>, haga clic con el botón secundario y seleccione **Desinstalar**. Se inicia el instalador y puede seleccionar los componentes que quiere quitar.
- Para quitar Universal Print Server, seleccione **Citrix Universal Print Server** y, a continuación, haga clic con el botón secundario y seleccione **Desinstalar**.

### Eliminar un VDA mediante la línea de comandos

Ejecute el comando que se utilizó para instalar el VDA: `VDAServerSetup.exe`, `VDAWorkstationSetup.exe` o `VDAWorkstationCoreSetup.exe`. Consulte Instalar mediante línea de comandos para ver descripciones completas de sintaxis.

- Para quitar solo el VDA o solo la aplicación Citrix Workspace, use las opciones `/remove` y `/components`.

- Para quitar el VDA y la aplicación Citrix Workspace, use la opción `/removeall`.

Por ejemplo, el siguiente comando elimina el VDA y la aplicación Citrix Workspace de una máquina con SO multisesión.

```
VDAServerSetup.exe /removeall
```

Por ejemplo, el siguiente comando elimina el VDA, pero no la aplicación Citrix Workspace para Windows (si está instalada), de una máquina con SO de sesión única.

```
VDAWorkstationSetup.exe /remove /components vda
```

También puede quitar un VDA mediante un script suministrado por Citrix. Consulte Eliminar agentes VDA mediante el script.

## Capa de personalización de usuarios

February 12, 2024

La función de capa de personalización de usuarios de Citrix Virtual Apps and Desktops amplía las prestaciones de los catálogos de máquinas no persistentes para conservar en todas las sesiones los datos de los usuarios y las aplicaciones instaladas localmente. Con la tecnología subyacente de Citrix App Layering, la capa de personalización de usuarios funciona con Citrix Provisioning y Machine Creation Services (MCS) en catálogos de máquinas no persistentes.

Los componentes de la capa de personalización de usuarios se instalan con Virtual Delivery Agent dentro de la imagen maestra. Un archivo VHD almacena localmente las aplicaciones instaladas por el usuario. El VHD montado en la imagen hace las veces de disco duro virtual del usuario.

> **Importante:**
>
> Puede implementar capas de personalización de usuarios en Citrix Virtual Apps and Desktops o capas de usuarios de App Layering habilitadas en una plantilla de imagen, pero no puede hacer las dos cosas. No instale la función de capa de personalización de usuarios en una capa de App Layering.

Esta función reemplaza los discos Personal vDisks (PvD), al tiempo que proporciona a los usuarios una experiencia persistente para los espacios de trabajo en un entorno de escritorios agrupados y no persistentes.

Para implementar la función de capa de personalización de usuarios, instálela y configúrela con los pasos detallados en el artículo. Hasta entonces, la función no estará disponible.

## Compatibilidad con aplicaciones

Aparte de las excepciones siguientes, todas las aplicaciones que un usuario instala localmente en el escritorio se admiten en la capa de personalización de usuarios.

### Excepciones

Las siguientes aplicaciones son la excepción, y no se admiten en la capa de personalización de usuarios:

- Aplicaciones de empresa, como MS Office y Visual Studio.
- Aplicaciones que modifican el hardware o la pila de red. Ejemplo: un cliente VPN.
- Aplicaciones que tienen controladores de nivel de arranque. Ejemplo: un antivirus.
- Aplicaciones con controladores que utilizan el almacén de controladores. Ejemplo: un controlador de impresora.

  > **Nota:**
  >
  > Puede hacer que las impresoras estén disponibles mediante Objetos de directiva de grupo (GPO) de Windows.

*No* permita que los usuarios instalen localmente aplicaciones no admitidas. En su lugar, instale estas aplicaciones directamente en la imagen maestra.

### Aplicaciones que requieren una cuenta de administrador o usuario local

Cuando un usuario instala una aplicación localmente, la aplicación pasa a su capa de usuarios. Si el usuario agrega o modifica a un usuario o grupo locales, los cambios no se conservan más allá de la sesión.

> **Importante:**
>
> Agregue cualquier usuario o grupo local requerido en la imagen maestra.

## Requisitos

La funcionalidad de capa de personalización de usuarios requiere los siguientes componentes:

- Citrix Virtual Apps and Desktops 7 1909 o una versión posterior
- Virtual Delivery Agent (VDA), versión 1912 o una posterior
- Citrix Provisioning, versión 1909 o una posterior

- Recurso compartido de archivos (SMB) de Windows o Azure Files con autenticación de AD local habilitada

Puede implementar la función Capa de personalización de usuarios en las siguientes versiones de Windows cuando el sistema operativo se implementa como SO de sesión única. La compatibilidad está limitada a un solo usuario en una sola sesión.

- Windows 11 Enterprise x64
- Windows 10 Enterprise x64, versión 1607 o una posterior
- Windows 10 multisesión (compatible con Azure Files)
- Windows Server 2016 (compatible con Azure Files)
- Windows Server 2019 (compatible con Azure Files)

Para Citrix Virtual Apps and Desktops 7, se admite Azure Files con capas de personalización de usuarios en Windows Server 2019, Windows Server 2016v y el cliente Windows 10.

> **Nota:**
>
> Si utiliza un SO de servidor, solo se admite la VDI de servidor. Para obtener información detallada sobre las implementaciones, consulte el artículo VDI de servidor.
>
> La capa de personalización de usuarios admite solo un usuario a la vez por máquina y, a continuación, la máquina tiene que reiniciar para restablecer los discos. No se puede utilizar la capa de personalización de usuario con sistemas operativos de servidor multisesión: esa capa solo se puede utilizar con sistemas de servidor de sesión única. La capa de personalización de usuario solo funciona con escritorios no persistentes.

Desinstale la función de capa de personalización de usuario, si está instalada. Reinicie la imagen maestra antes de instalar la versión más reciente.

### Configurar el recurso compartido de archivos

La función de capa de personalización de usuarios requiere almacenamiento de Windows Server Message Block (SMB). Para crear un recurso compartido de archivos de Windows, siga los pasos habituales para el sistema operativo Windows en el que se encuentra.

Para obtener más información sobre el uso de Azure Files con catálogos basados en Azure, consulte Configurar el almacenamiento de Azure Files para capas de personalización de usuarios.

### Recomendaciones

Siga las recomendaciones que se indican en esta sección para implementar correctamente la capa de personalización de usuarios.

#### Microsoft System Center Configuration Manager (SCCM)

Si utiliza SCCM con la funcionalidad de capa de personalización de usuarios, siga las instrucciones de Microsoft para preparar la imagen en un entorno VDI. Consulte este artículo de Microsoft TechNet para obtener más información.

#### Tamaño de capa de usuarios

Una capa de usuarios es un disco aprovisionado ligero que se expande a medida que se utiliza espacio en el disco. El tamaño predeterminado de la capa de usuarios es de 10 GB, el mínimo que recomendamos.

> **Nota:**
>
> Durante la instalación, si el valor se establece en cero (0), el tamaño predeterminado de la capa de usuarios se establece en 10 GB.

Si quiere cambiar el tamaño de la capa de usuarios, puede introducir un valor diferente para la directiva **Tamaño de capa de usuarios** de Studio. Consulte el **Paso 5: Crear directivas personalizadas de grupo de entrega**, en **Opcional: haga clic en Seleccionar junto a Tamaño de capa de usuarios en GB.**

#### Herramientas para invalidar el tamaño de capa de usuarios (opcional)

Puede pasar por alto el tamaño de capa de usuarios definiendo, con una herramienta de Windows, una cuota para el recurso compartido de archivos en la capa de usuarios.

Utilice una de las siguientes herramientas de configuración de cuotas de Microsoft para establecer una cuota fija en el directorio de capa de usuarios denominado **Usuarios**:

- Administrador de recursos del servidor de archivos (FSRM)
- Administrador de cuotas

> **Nota:**
>
> Aumentar la cuota afecta a las nuevas capas de usuarios y expande las existentes. Disminuir la cuota solo afecta a las nuevas capas de usuarios. Las capas de usuarios existentes nunca disminuyen de tamaño.

### Implementar una capa de personalización de usuarios

Al implementar la función de personalización de usuarios, defina las directivas en Studio. A continuación, asigne las directivas al grupo de entrega vinculado al catálogo de máquinas, donde se implementa la función.

Si deja la imagen maestra sin configuración de capa de personalización de usuarios, los servicios permanecen inactivos y no interfieren con las actividades de creación.

Si establece las directivas en la imagen maestra, los servicios intentarán ejecutar y montar una capa de usuarios en la imagen maestra. La imagen maestra mostraría comportamientos inesperados e inestabilidad.

Para implementar la funcionalidad "capa de personalización de usuarios", siga estos pasos, por orden:

- Paso 1: Verifique la disponibilidad de un entorno Citrix Virtual Apps and Desktops.
- Paso 2: Prepare la imagen maestra.
- Paso 3: Cree un catálogo de máquinas.
- Paso 4: Cree un grupo de entrega.
- Paso 5: Cree directivas personalizadas de grupo de entrega.

> **Nota:**
>
> Iniciar sesión por primera vez después de actualizar la versión de Windows 10 en la imagen tarda más de lo habitual. La capa del usuario debe actualizarse para la nueva versión de Windows 10, lo que prolonga el inicio de sesión.

#### Paso 1: Verifique la disponibilidad de un entorno Citrix Virtual Apps and Desktops

Asegúrese de que su entorno Citrix Virtual Apps and Desktops esté disponible para su uso con esta nueva función. Para obtener información detallada sobre la configuración, consulte Instalar y configurar Citrix Virtual Apps and Desktops.

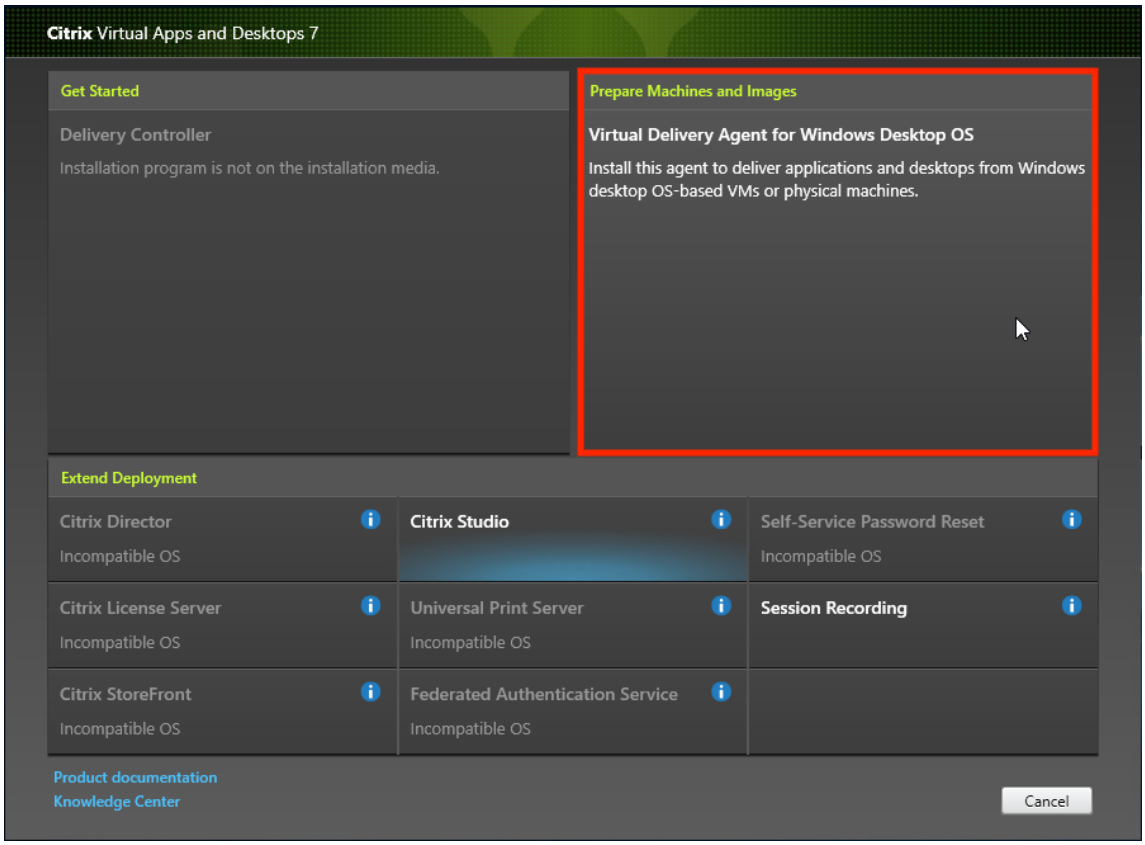
#### Paso 2: Prepare la imagen maestra

Para preparar la imagen maestra:

1. Localice la imagen maestra. Instale las aplicaciones de empresa de su organización y todas las demás aplicaciones que los usuarios puedan encontrar útiles.
2. Si va a implementar VDI de servidor, siga los pasos descritos en el artículo VDI de servidor. Debe incluir el componente opcional, la **Capa de personalización de usuarios**. Para obtener información detallada, consulte Opciones de línea de comandos para instalar un VDA.
3. Si utiliza Windows 10, instale Virtual Delivery Agent (VDA) 1912 o una versión posterior. Si ya hay instalada una versión anterior del VDA, desinstale antes la versión anterior. Al instalar la nueva versión, seleccione e instale el componente opcional, la **Capa de personalización de usuarios de Citrix**, de la siguiente manera:

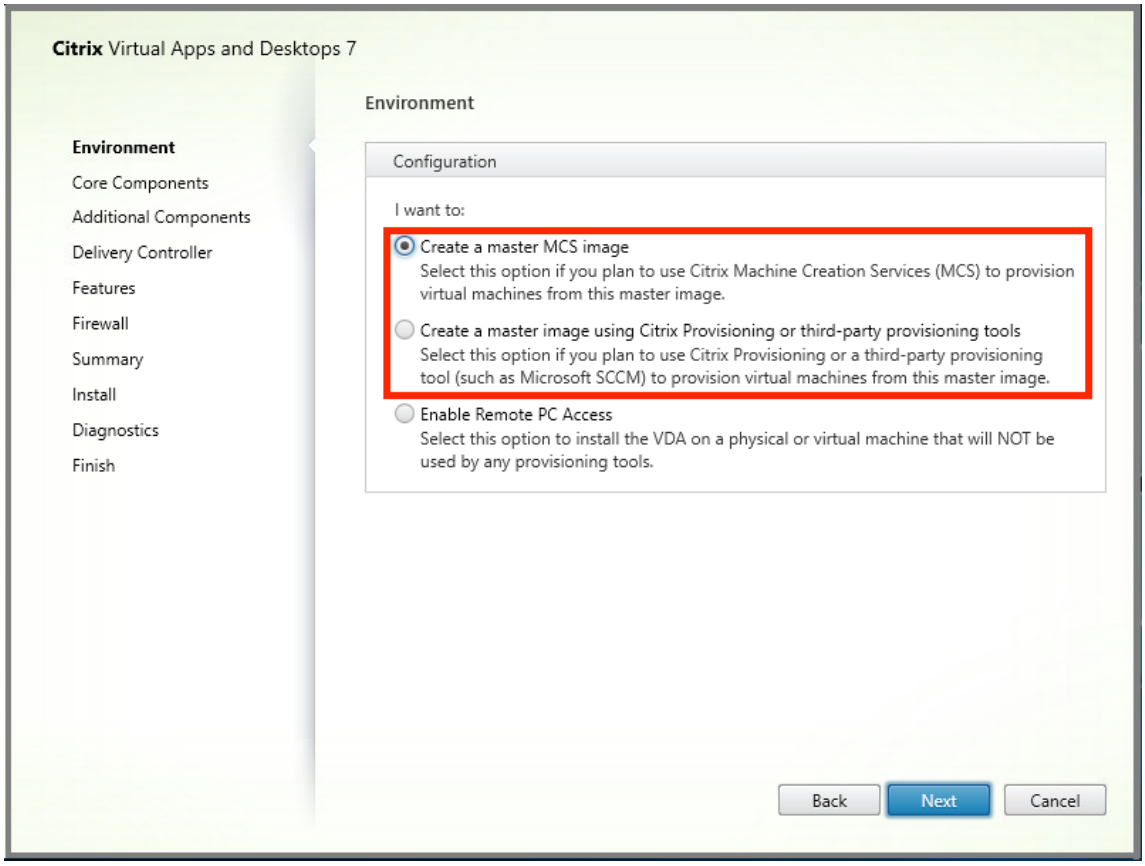
 

a) Haga clic en el icono **Virtual Delivery Agent para SO de escritorio Windows**:




a) **Entorno:** Seleccione **Crear una imagen maestra de MCS** o **Crear una imagen maestra mediante Citrix Provisioning o herramientas de aprovisionamiento de terceros**.

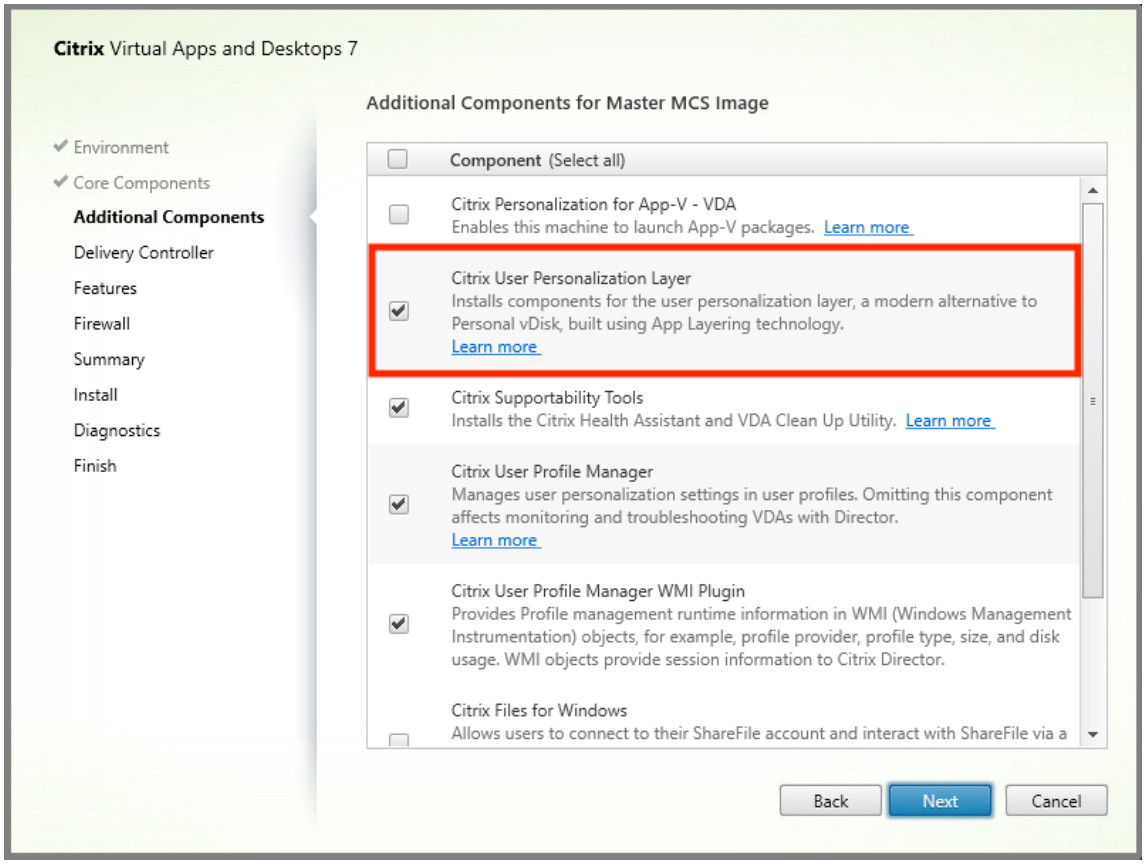
 




a) **Componentes principales:** Haga clic en **Siguiente**.

b) **Componentes adicionales:** Marque **Capa de personalización de usuarios de Citrix**.




a) Haga clic en las pantallas de instalación restantes, configure el VDA según sea necesario y haga clic en **Instalar**. La imagen se reinicia una o más veces durante la instalación.

4. Deje las **actualizaciones de Windows** inhabilitadas. El instalador de la capa de personalización de usuarios inhabilitará las actualizaciones de Windows en la imagen. Deje las actualizaciones inhabilitadas.

La imagen estará lista para que la cargue en Studio.

> **Nota:**
>
> Si simplemente quiere actualizar la versión de la capa de personalización de usuarios (UPL), puede hacerlo con una versión más reciente de UPL y el paquete independiente. No necesita actualizar la versión del VDA.

#### Paso 3: Cree un catálogo de máquinas

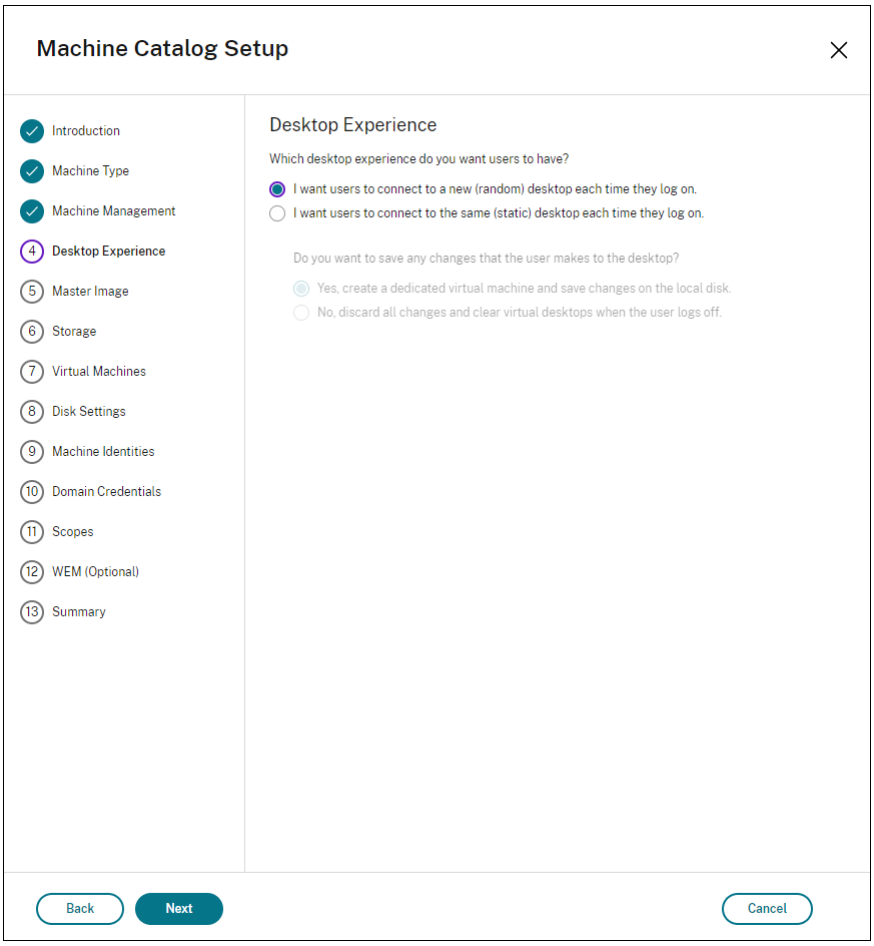
En Studio, siga los pasos para crear un catálogo de máquinas. Utilice las siguientes opciones durante la creación del catálogo:

1. Seleccione **Sistema operativo** y establezca el valor en **SO de sesión única**.

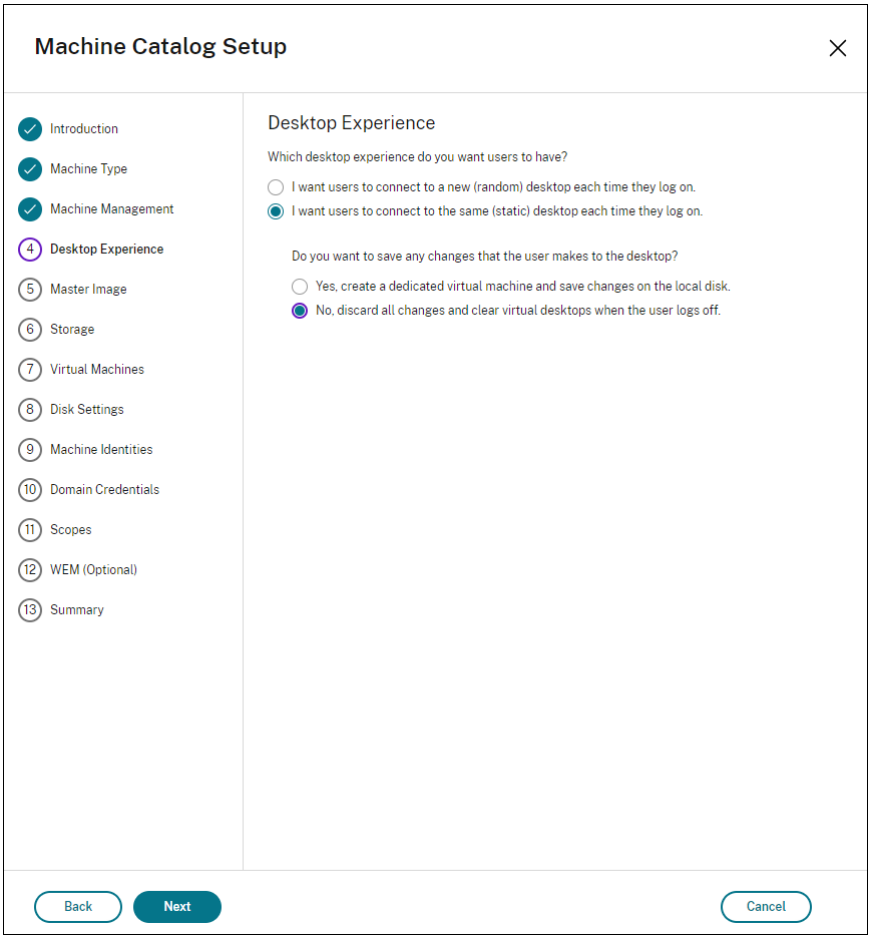
2. Seleccione **Administración de máquinas** y establezca el valor en **Máquinas con administración de energía**. (por ejemplo, máquinas virtuales o PC blade).
3. Seleccione **Experiencia de escritorio** y establezca el tipo de catálogo en **agrupadas aleatorias** o **agrupadas estáticas**, como se muestra en los ejemplos siguientes:

   - **Agrupadas aleatorias:**




   - **Agrupadas estáticas:** Si selecciona agrupadas estáticas, configure los escritorios para descartar todos los cambios y borrar los escritorios virtuales cuando el usuario cierre la sesión, como se muestra en la siguiente captura de pantalla:




> **Nota:**
>
> La capa de personalización de usuarios no admite catálogos de máquinas agrupadas estáticas configuradas para uso con Citrix Personal vDisk o asignadas como máquinas virtuales dedicadas.

4. Si utiliza MCS, seleccione **Imagen** y la instantánea de la imagen creada en la sección anterior.
5. Configure las propiedades de catálogo restantes según sea necesario para su entorno.

### Paso 4: Cree un grupo de entrega

Cree y configure un **grupo de entrega**, incluidas las máquinas del catálogo de máquinas que ha creado. Para obtener más información, consulte Crear grupos de entrega.

### Paso 5: Cree directivas personalizadas de grupo de entrega

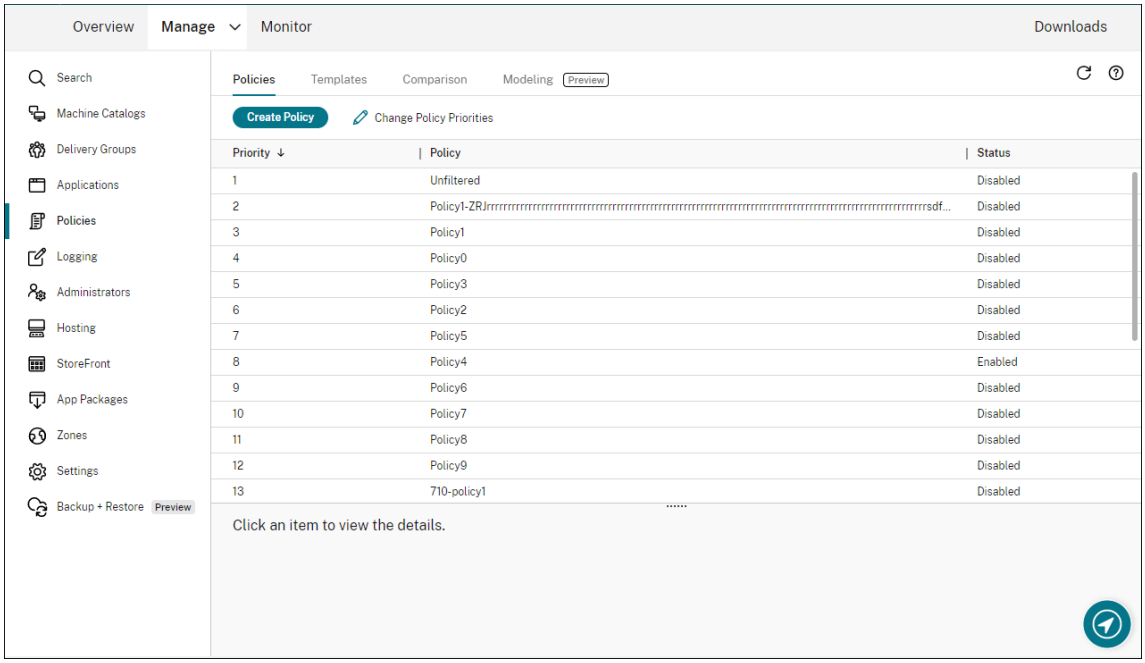
Para habilitar el montaje de capas de usuarios dentro de Virtual Delivery Agents, utilice los parámetros de configuración para especificar:

- En qué lugar de la red se accede a las capas de usuarios.
- Hasta qué tamaño puede permitir que los discos de capa de usuarios crezcan.

Para definir los parámetros como directivas de Citrix personalizadas en Web Studio y asignarlos al grupo de entrega.

1. Inicie sesión en Web Studio y seleccione **Directivas** en el panel de la izquierda:




2. Seleccione **Crear directiva** en la barra de acciones. Aparecerá la ventana Crear directiva.
3. Escriba "capa de usuarios"en el campo de búsqueda. En la lista de directivas disponibles, aparecen las tres directivas siguientes:

   - Exclusiones de capas de usuarios
   - Ruta del repositorio de capas de usuarios
   - Tamaño de capa de usuarios en GB

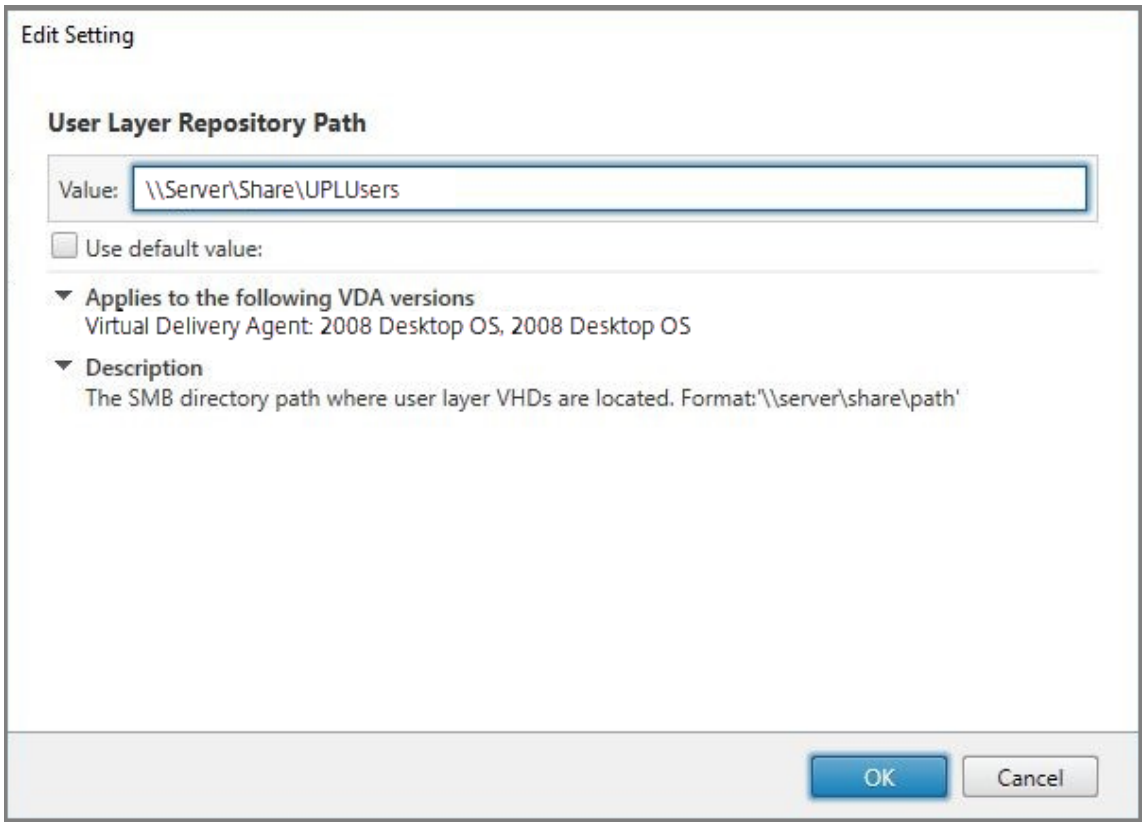
   > **Nota:**
   >
   > Aumentar el tamaño afecta a las nuevas capas de usuarios y expande las existentes. Disminuir el tamaño solo afecta a las nuevas capas de usuarios. Las capas de usuarios existentes nunca disminuyen de tamaño.

4. Marque la casilla situada junto a **Ruta del repositorio de capas de usuarios** y haga clic en **Modificar**. Se muestra la ventana Modificar configuración.
5. Introduzca una ruta en el campo **Valor** y haga clic en **Guardar**:

   - **Formato de ruta:** `\\server-name-or-address\share-name\folder`

- **Ejemplo de ruta:** `\\Server\Share\UPLUsers`
- **Ejemplo de ruta resultante:** Para un usuario llamado **Alex** en **CoolCompanyDomain**, la ruta sería: `\\Server\Share\UPLUsers\Users\CoolCompanyDomain_Alex\A_OK`

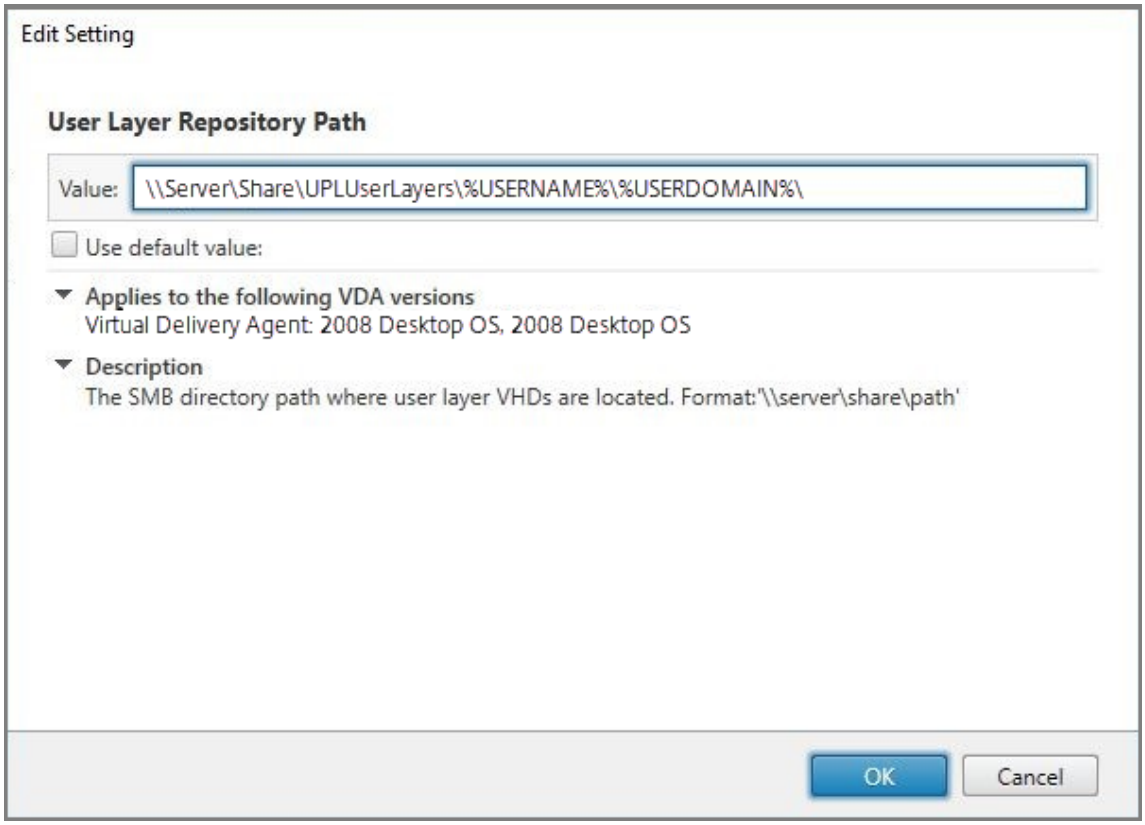



Puede personalizar la ruta mediante las variables %USERNAME% y %USERDOMAIN%, las variables de entorno de la máquina y los atributos de Active Directory (AD). Cuando se expanden, estas variables dan como resultado rutas explícitas.

Ejemplo de variables de entorno:

- **Formato de ruta:** `\\Server-name-or-address\share-name\folder-with-environment-variables`
- **Ejemplo de ruta:** `\\Server\Share\UPLUserLayers\\%USERNAME%\\%USERDOMAIN%`
- **Ejemplo de ruta resultante:** Para un usuario llamado **Alex** en **CoolCompanyDomain**, la ruta sería: `\\Server\Share\UPLUserLayers\Alex\CoolCompanyDomain\A_OK`

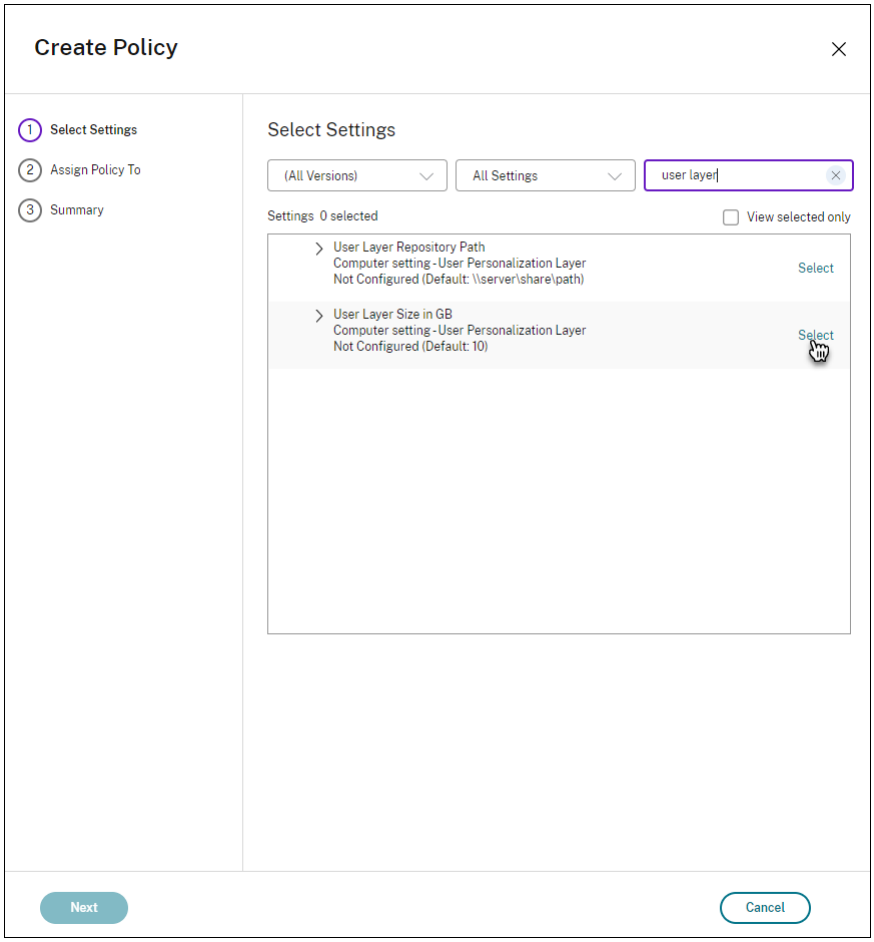



Ejemplo de atributos de AD personalizados:

- Formato de ruta: `\\Server-name-or-address\share-name\AD-attribute`
- Ejemplo de ruta: `\\Server\share\\#sAMAccountName#`
- Ejemplo de rutas resultantes: `\\Server\share\JohnSmith` (si #sAMAccountName# se resuelve en JohnSmith para el usuario actual)

6. Opcional: Marque la casilla situada junto a **Tamaño de las capas de usuarios en GB** y haga clic en **Modificar**:

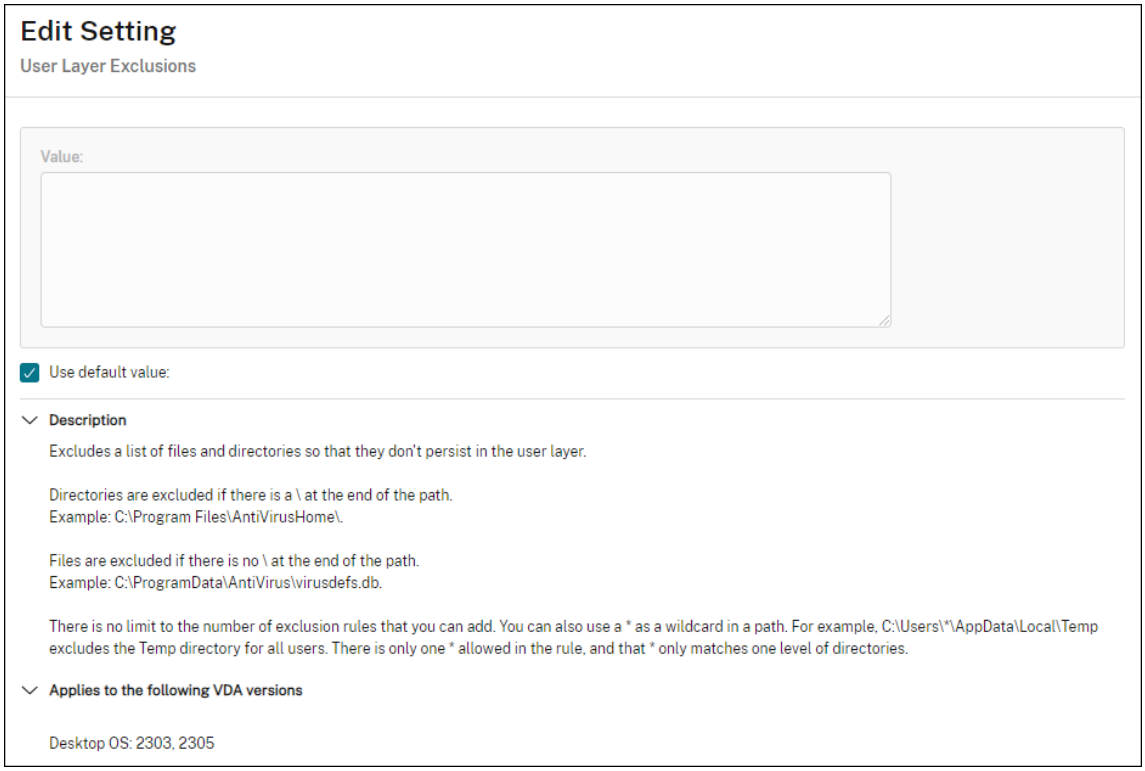
 




Aparecerá la ventana Modificar parámetros.

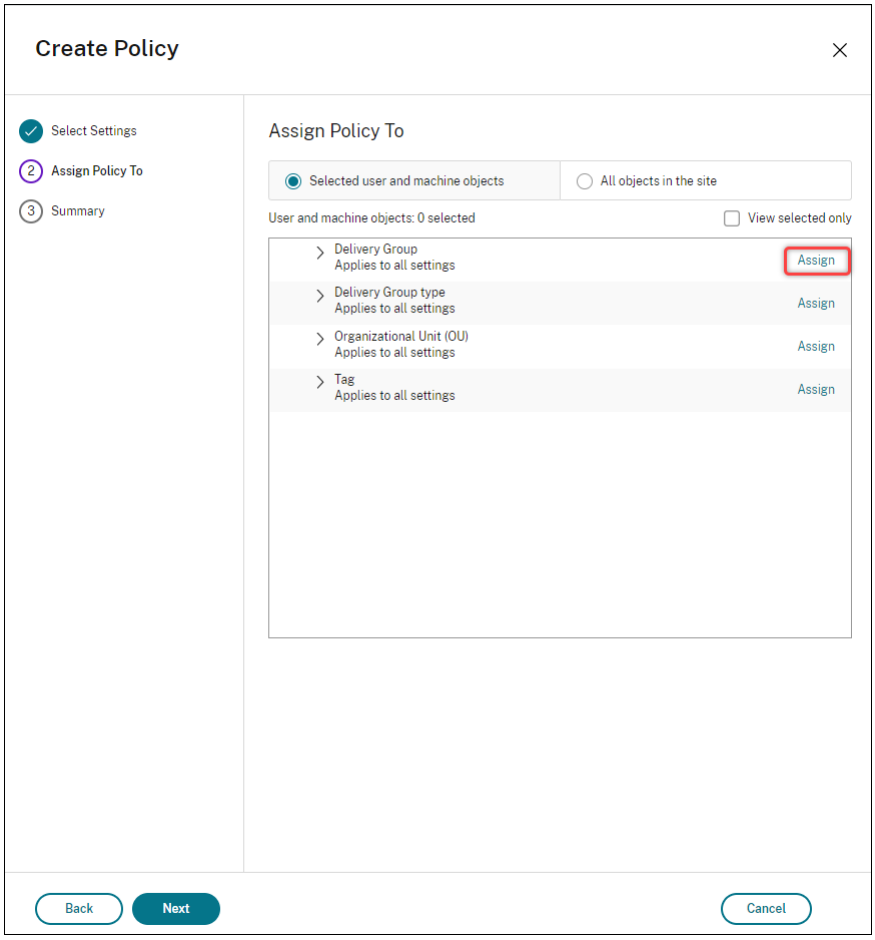
7. Opcional: Cambie el valor predeterminado de **10 GB** al tamaño máximo que puede tener cada capa de usuario. Haga clic en **Guardar**.
8. Opcional: Marque la casilla situada junto a **Exclusiones de capas de usuarios** y haga clic en **Modificar**.

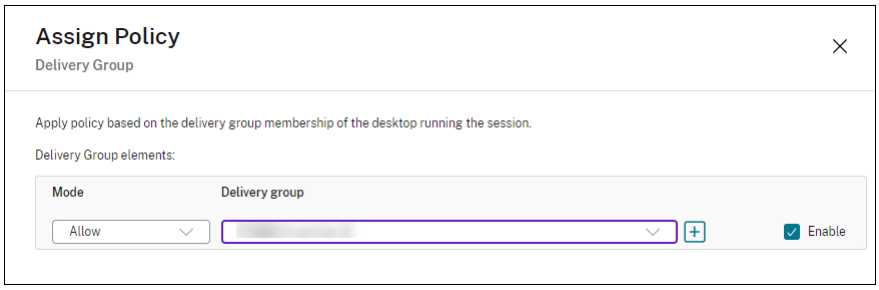



9. Opcional: Especifique los archivos y carpetas que quiera excluir y, a continuación, haga clic en **Guardar**. Para obtener más información, consulte la documentación de Citrix App Layering.
10. Haga clic en **Siguiente** para configurar usuarios y máquinas a los que quiera asignar. Haga clic en el enlace **Asignar grupo de entrega** resaltado en esta imagen:

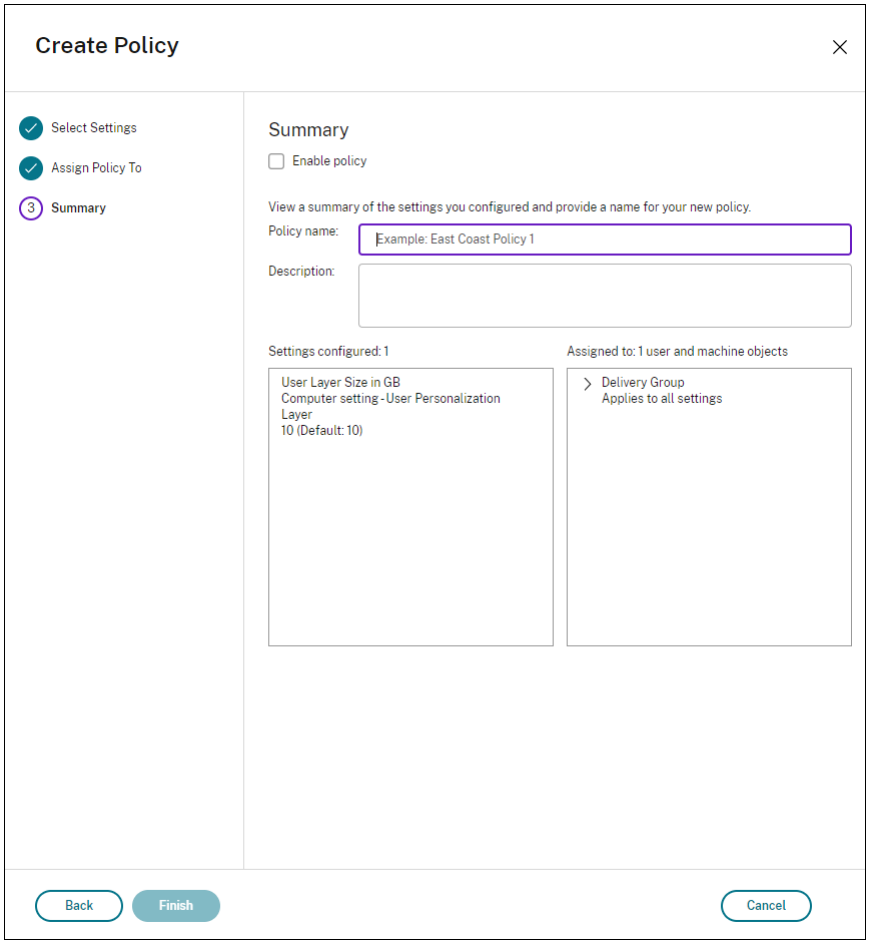



11. En el menú **Grupo de entrega**, seleccione el grupo de entrega creado en la sección anterior. Haga clic en **Aceptar**.




12. Introduzca un nombre para la directiva. Marque la casilla para habilitar la directiva y haga clic en **Finalizar**.




### Configurar los parámetros de seguridad en la carpeta de la capa de usuarios

Como administrador de dominios, puede especificar más de una ubicación de almacenamiento para las capas de usuarios. Cree una subcarpeta `\Users` para cada ubicación de almacenamiento (incluida la ubicación predeterminada). Proteja cada ubicación mediante la siguiente configuración.

| Nombre del parámetro | Valor | Aplicar a |
|---|---|---|
| Propietario creador | Modificar | Subcarpetas y archivos únicamente |
| Derechos de propietario | Modificar | Subcarpetas y archivos únicamente |
| Usuarios o grupo | Crear carpeta/anexar datos; Atravesar carpeta/ejecutar archivo; Mostrar lista de carpetas/leer datos; Leer atributos | Solo carpeta seleccionada |

| Nombre del parámetro | Valor | Aplicar a |
|---|---|---|
| Sistema | Control total | Carpeta, subcarpetas y archivos seleccionados |
| Administradores de dominio y grupo de administradores seleccionado | Control total | Carpeta, subcarpetas y archivos seleccionados |

### Mensajes de capa de usuarios

Cuando un usuario no puede acceder a su capa de usuarios, recibe uno de los siguientes mensajes de notificación.

- **Capa de usuarios que se está utilizando**

  ```
  We were unable to attach your user layer because it is in use.
  Any changes you make to application settings or data will not be
  saved. Be sure to save any work to a shared network location.<!--
  NeedCopy-->
  ```

- **Capa de usuarios no disponible**

  ```
  We were unable to attach your user layer. Any changes you make to
   application settings or data will not be saved. Be sure to save
  any work to a shared network location.<!--NeedCopy-->
  ```

- **El sistema no se restablece después de que el usuario haya cerrado la sesión**

  ```
  This system was not shut down properly. Please log off immediately
   and contact your system administrator.<!--NeedCopy-->
  ```

### Archivos de registro para solución de problemas

El archivo de registro, ulayersvc.log, contiene la salida del software de capa de personalización de usuarios donde se registran los cambios.

```
1 C:\ProgramData\Unidesk\Logs\ulayersvc.log
2 <!--NeedCopy-->
```

### Limitaciones

Tenga en cuenta las siguientes limitaciones al instalar y usar la funcionalidad de capa de personalización de usuarios.

- *No* intente implementar el software de la capa de personalización del usuario en una capa dentro de App Layering. Implemente capas de personalización de usuarios en Citrix Virtual Apps and Desktops o habilite capas de usuarios en una plantilla de imagen de App Layering, pero no realice ambos procesos. Cualquiera de los dos produce las capas de usuarios que necesita.
- *No* configure la funcionalidad de capa de personalización de usuarios con catálogos de máquinas persistentes.
- *No* utilice hosts de sesión.
- *No* actualice el catálogo de máquinas con una imagen que ejecute una nueva instalación del sistema operativo (incluso la misma versión de Windows 10). La práctica recomendada es aplicar las actualizaciones al sistema operativo dentro de la misma imagen maestra utilizada al crear el catálogo de máquinas.
- *No* utilice controladores de tiempo de arranque, ni ninguna otra personalización de primera fase de arranque.
- *No* migre datos de PvD a la función de la capa de personalización de usuarios.
- *No* migre capas de usuarios existentes del producto App Layering completo a la función de la capa de personalización de usuarios.
- *No* cambie la ruta SMB de capa de usuarios para acceder a las capas de usuarios creadas con una imagen maestra de un sistema operativo diferente.
- Cuando un usuario cierra la sesión y vuelve a iniciarla, la nueva sesión se ejecuta en otra máquina del grupo. En un entorno VDI, Microsoft Software Center muestra una aplicación como **Instalada** en la primera máquina, pero la muestra como **No disponible** en la segunda máquina.

  Para averiguar el verdadero estado de la aplicación, indique al usuario que seleccione la aplicación en el Centro de software y haga clic en **Instalar**. A continuación, SCCM actualiza el estado al valor verdadero.
- Centro de software en ocasiones se detiene inmediatamente después de iniciarse en un VDA que tiene habilitada la funcionalidad de capa de personalización de usuarios. Para evitar este problema, siga las recomendaciones de Microsoft para Implementación de SCCM en un entorno VDI de XenDesktop. Además, asegúrese de que el servicio `ccmexec` se está ejecutando antes de iniciar el Centro de software.
- En Directivas de grupo (configuraciones de equipo), los parámetros de capa de usuarios anulan los parámetros aplicables a la imagen maestra. Por consiguiente, los cambios que realice en Configuración del equipo mediante un objeto de directiva de grupo no siempre están presentes para el usuario en el inicio de sesión siguiente.

  Para evitar este problema, cree un script de inicio de sesión de usuario que emita el comando:

```
gpupdate /force
```

Por ejemplo: un cliente definió el siguiente comando para que se ejecute en cada inicio de sesión de usuario:

```
gpudate /Target:Computer /force
```

Para obtener los mejores resultados, aplique los cambios a Configuración del equipo directamente en la capa de usuarios, después de que el usuario haya iniciado sesión.

- Una cuenta de usuario de dominio no debe ser el último usuario que haya iniciado sesión en una imagen maestra. De lo contrario, las máquinas aprovisionadas desde esa imagen tendrán problemas.
- Los certificados personalizados no persisten cuando la capa UPL está habilitada en un entorno de Azure AD puro por un problema subyacente en Windows que se ejecuta en Azure. Si Microsoft corrige este problema en una mejora futura, actualizaremos este artículo.

## Actualizar la versión de los VDA

May 17, 2024

### Introducción

Citrix mantiene todos los componentes de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) que haya en la implementación, excepto los agentes VDA.

Antes de comenzar la actualización de versión de un VDA:

- Lea todo este artículo para saber a qué atenerse.
- Revise la directiva de vida útil de Citrix DaaS.

Para actualizar un VDA, descargue el instalador correspondiente y ejecútelo en la máquina o en la imagen. Puede usar la interfaz gráfica o de línea de comandos del instalador. Para obtener instrucciones, consulte:

- Instaladores de VDA
- Instalar los VDA mediante la interfaz gráfica
- Instalar los VDA mediante la línea de comandos

Si en su momento instaló el VDA mediante `VDAWorkstationCoreSetup.exe`:

- Conservará esa configuración si actualiza el VDA a la versión más reciente del mismo instalador.

- Si ejecuta `VDAWorkstationSetup.exe` en esa máquina, puede habilitar las funciones que no se admitían en `VDAWorkstationCoreSetup.exe`. Algunas de esas funciones podrían estar habilitadas de forma predeterminada en el `VDAWorkstationSetup.exe` instalador. También puede instalar la aplicación Citrix Workspace.

> **Nota:**
>
> Se produce un reinicio al actualizar un VDA a la versión 7.17 o una versión posterior compatible. Este reinicio no se puede evitar. La actualización se reanuda automáticamente después del reinicio (a menos que especifique `/noresume` en la línea de comandos).

Después de actualizar los VDA, actualice las imágenes y los catálogos que utilicen ese VDA.

### Actualizar la versión de los VDA mediante la interfaz de Configuración completa

> **Importante:**
>
> - Como práctica recomendada, se aconseja probar minuciosamente las actualizaciones de VDA antes de pasar a un entorno de producción.
> - Puede cambiar entre VDA CR (Current Release) y VDA LTSR (Long Term Service Release) siempre que cambie de una versión anterior a una versión posterior. No puede cambiar de una versión posterior a una anterior porque se considera una reversión. Por ejemplo, no puede cambiar de la versión 2212 CR a 2203 LTSR (cualquier CU), pero puede actualizar la versión 2112 CR a 2203 LTSR (cualquier CU).
> - No se admiten las actualizaciones a demanda (como revisiones hotfix y parches entre versiones principales).
> - VDA CVAD 2402 está disponible a través del servicio de actualización de versiones de VDA.

Con la interfaz de Configuración completa, puede actualizar la versión de los VDA por catálogo o por máquina. Puede actualizarlos inmediatamente o en un momento programado.

Para obtener más información sobre el servicio de actualización de versiones de VDA, consulte Resumen técnico: Servicio de actualización de Citrix VDA. Allí encontrará una descripción general del servicio, información detallada sobre cómo funciona y otros recursos útiles.

#### Requisitos previos

- Plano de control: Citrix DaaS
- Tipo de VDA: VDA para SO de sesión única o multisesión. Actualmente, solo se admiten VDA Windows.
- Versión de VDA: 2109 o una versión posterior, o bien 2203 LTSR o una versión posterior

> **Nota:**
>
> Se recomienda utilizar la versión CR o LTSR CU más reciente de VDA.

- Tipo de aprovisionamiento: Máquinas persistentes (como máquinas aprovisionadas por MCS, máquinas de acceso con Remote PC o Citrix HDX Plus para Windows 365). Consulte Tipos de máquinas admitidas.
- Los VDA deben tener el agente de actualización de versiones de VDA instalado y el servicio debe estar ejecutándose.
- Tiene permisos para actualizar la versión de los VDA.
- La actualización del VDA se configura con la opción CR o LTSR adecuada en Configuración completa.
- Los VDA no están en uso. (Los usuarios deben cerrar sesión en ellos).

  > **Nota:**
  >
  > La actualización se omite en los VDA que estén en uso o desconectados. Recomendamos programar una franja horaria de actualización y solicitar a los usuarios que cierren sesión en los VDA.

- Los VDA no están en modo de mantenimiento. (Un administrador puede poner un VDA en modo de mantenimiento. También se puede poner automáticamente en modo de mantenimiento si ha superado el número máximo de intentos de registro permitidos).
- Se han agregado las URL relevantes a la lista de permitidos si se ha implementado el filtrado de URL. Consulte Requisito de actualización de versiones de VDA.
- Los VDA deben pertenecer a un grupo de entrega y estar registrados en DaaS.
- El nivel funcional se establece correctamente para que la función de actualización del VDA esté disponible para uso. Consulte Niveles funcionales y versiones de VDA.
- El VDA de destino admite el sistema operativo del VDA actual.

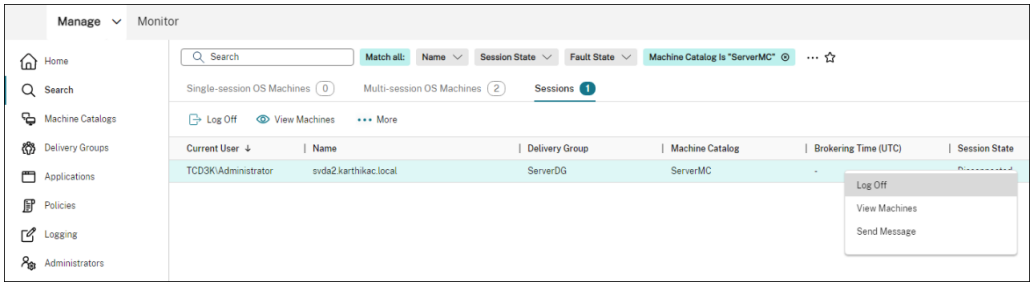
#### Problemas conocidos

**Problema 1: No se pudo actualizar la versión de los VDA de LTSR a las versiones LTSR Cumulative Update (CU)** El proceso de actualización de los VDA LTSR a las versiones LTSR CU (actualización acumulativa) puede fallar. Si bien el proceso parece completarse correctamente en la Configuración completa, la versión instalada del VDA no cambia y el estado revierte al de **Actualización disponible** al cabo de uno o dos minutos. El problema se produce con los VDA que tienen instalada la versión 7.35.0.7 o anterior del agente de actualización de versiones de VDA.

Para solucionar este problema, inicie sesión en el VDA y actualice el agente de actualización de versiones de VDA a la versión 7.37.0.7 o posterior (mediante la versión 2303 o posterior del instalador de VDA). A partir de la versión 7.37.0.7, el agente de actualización de versiones de VDA admite la actualización automática para que los agentes de versiones anteriores que se ejecutan en los VDA puedan actualizarse automáticamente a la versión más reciente. Con esta función de actualización automática, el servicio de actualización de VDA comprueba la versión del VDA notificada por el agente y, a continuación, programa las actualizaciones en el plazo de una hora para actualizar automáticamente el agente a la versión más reciente. Con esta función de actualización automática de versión, se reduce el esfuerzo de mantenimiento.

Para que la versión del agente del VDA se actualice automáticamente, cierre las sesiones, de manera que el servicio de actualización de VDA pueda iniciar las actualizaciones automáticas. Puede cerrar las sesiones en Configuración completa.




Si la versión del agente no se actualiza automáticamente, inicie sesión en el VDA y actualice la versión del agente manualmente de la siguiente manera:

1. Ejecute el siguiente cmdlet para mostrar el agente de actualización de versiones de VDA en Panel de control > Desinstalar o cambiar un programa.

```
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ).GetValue('SystemComponent')
(Get-ChildItem  -Path 'HKLM:\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Uninstall' | ? {
  $_.GetValue('DisplayName') -eq 'Citrix VDA Upgrade Agent Service
      - x64'  }
 ) | Set-ItemProperty -Name SystemComponent -Value 0
<!--NeedCopy-->
```

2. Instale el agente de actualización de versiones de VDA más reciente. Para realizar una instalación silenciosa, utilice el siguiente cmdlet:

   - `msiexec /i CitrixUpgradeAgent_x64.msi /q`

Puede identificar la versión del agente de actualización de versiones de VDA mediante el cmdlet o un script. Consulte Solucionar problemas.

**Problema 2: Proxy no compatible** Actualmente, el agente de actualización de versiones de VDA no admite configuraciones de proxy. Esta limitación puede provocar problemas de conectividad cuando el agente intenta establecer conexiones a través de un servidor proxy.

Puede aplicar una solución temporal para resolver el problema. Siga los pasos que aparecen a continuación:

1. Busque el archivo de configuración del agente de actualización de versiones de VDA en: `C:\Program Files\Citrix\CitrixUpgradeAgent\Citrix.UpdateServices.UpdateAgent.exe.config`.
2. Abra el archivo de configuración con un editor de texto.
3. Agregue estas líneas al final del archivo y sustituya `ProxyServerName` por el nombre real del servidor proxy:

```
<system.net>
  <defaultProxy enabled="true" useDefaultCredentials="true">
    <proxy proxyaddress="http://PROXYSERVER:PORT" usesystemdefault
       ="false" />
  </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

4. Reinicie Citrix VDA Upgrade Agent Service para aplicar la configuración actualizada.

### Flujo de trabajo general de las tareas

El flujo de trabajo general para actualizar la versión de los VDA mediante la interfaz de Configuración completa es el siguiente:

1. Habilite la actualización de versión de VDA para un catálogo.
   - Puede habilitarla al crear un catálogo.
   - Puede habilitarla al modificar un catálogo.
2. Actualice la versión de los VDA por catálogo o por máquina. Para obtener más información, consulte Configurar la actualización automática de versiones de los VDA.

> **Nota:**
>
> Al programar la actualización de versiones de VDA para un catálogo, tenga en cuenta que se incluirán todas las máquinas del catálogo en el ámbito de la actualización. Por lo tanto, se recomienda hacer una copia de seguridad de esas máquinas antes de iniciar la actualización.

### Solucionar problemas técnicos

Si hay errores en la actualización de versiones, puede utilizar estos registros para solucionar los problemas por su cuenta o proporcionarlos al servicio de asistencia técnica de Citrix cuando se ponga en contacto con ellos para obtener ayuda.

- Registros de instalación para la instalación inicial del VDA en `%temp%/Citrix/XenDesktop Installer`
- Registros de actualización en `C:\Windows\Temp\Citrix\XenDesktop Installer`

Para comprobar las versiones del agente de actualización de versiones de VDA, utilice el siguiente cmdlet: `Get-VusComponentVersion -ComponentType VUS`. Muestra todos los VDA y sus versiones del agente de actualización de versiones de VDA.

Para obtener los nombres de VDA, utilice el siguiente cmdlet: `Get-BrokerMachine -UUID "<version number>"`, donde <`version number`> corresponde a la versión del agente de actualización de versiones de VDA que se obtiene del cmdlet `Get-VusComponentVersion`.

Para comprobar las versiones del agente de actualización de versiones de VDA a nivel de catálogo, puede utilizar el siguiente script:

> **Nota:**
>
> El script sirve de ejemplo y es posible que necesite adaptarlo a su entorno específico. Se recomienda probar exhaustivamente el script antes de usarlo en un entorno de producción.

```
Param(
    [Parameter (Mandatory=$true)]
    [string] $CatalogName
)

try
{

    $Uuids = Get-BrokerMachine -CatalogName $CatalogName | Select-
       Object -Property UUID

    if($Uuids -eq $null)
    {

        throw "Cannot find CatalogName "+$CatalogName
     }

    Write-Output("Catalog Name passed is "+$CatalogName)

   foreach($Uuid in $Uuids)
    {

```

```
22          $compVersion = Get-VusComponentVersion -MachineId $machine.UUID
                -ComponentType VUS
23          $Machine = Get-BrokerMachine -UUID $compVersion.MachineId
24          Write-Output("MachineName: "+$Machine.MachineName+", Machine
               UUID:"+$machine.MachineId+", VUA Version:"+$compVersion.
               Version)
25       }
26
27    }
28
29  catch
30  {
31
32      Write-Output("Exception Occured")
33      Write-Host $_
34    }
35
36  <!--NeedCopy-->
```

**Registros relacionados con el agente de actualización de versiones de VDA** También puede recopilar registros relacionados con el agente de actualización de versiones de VDA. Los registros que puede recopilar incluyen:

- **Rastreos de Citrix Diagnostic Facility (CDF)**
- **Registros de eventos de Windows**. Información escrita en el registro de eventos de Windows. Consulte los registros en **Visor de eventos > Registros de aplicaciones y servicios > Citrix VDA Upgrade Agent Service**.

Si es necesario, puede modificar el archivo de configuración del agente de actualización de versiones de VDA para que los registros se escriban continuamente en un archivo. Para habilitar la captura de registros en un archivo, siga estos pasos:

1. Vaya a la carpeta `C:\Program Files\Citrix\CitrixUpgradeAgent`.
2. Abra el archivo `Citrix.UpdateServices.UpdateAgent.exe.config`.
3. Cambie el valor de `LogToFile` a `1`.
4. Reinicie Citrix VDA Upgrade Agent Service. Esto crea un archivo de registros en `C:\ProgramData\Citrix\Update Services\Logs`.

> **Nota:**
>
> - Al habilitar la captura de registros en un archivo, se escriben registros de forma continua, lo que puede consumir espacio de almacenamiento. Recuerde inhabilitar la captura de registros una vez que se haya resuelto el problema. Para inhabilitar la captura de registros, primero defina `LogToFile` en `0` y, a continuación, reinicie Citrix VDA Upgrade Agent Ser-

> vice.
> - Al definir `LogToFile=1`, los registros solo se escriben en el archivo. No aparecerán en los rastros de CDF.

**Solucionar errores de descarga en la actualización de versiones de VDA** Siga los pasos que se indican a continuación para solucionar problemas y errores de descarga relacionados con la función de actualización de versiones de VDA:

1. Asegúrese de que se hayan agregado las URL relevantes a la lista de permitidos si se ha implementado el filtrado de URL. Consulte Requisito de actualización de versiones de VDA.
2. Tras agregar las URL necesarias a la lista de permitidos, pruebe a reprogramar la actualización de versiones de VDA.

Puede habilitar el rastreo de CDF o configurar `LogToFile` en 1 con el objetivo de capturar registros detallados para su análisis. Si el problema del error de descarga persiste, compruebe los errores. Si ve el mensaje de error "Error en la descarga: Esta lista de control de acceso no está en formato canónico y, por lo tanto, no se puede modificar", significa que los permisos de la carpeta `C:/ProgramData/Citrix/UpgradeServices/Downloads/VDA` son incorrectos. Para solucionar el problema, realice una de estas acciones:

- **Opción 1**: Restablezca las listas de control de acceso (ACL) de la carpeta mediante este comando (el comando restablece las ACL con las ACL heredadas predeterminadas para todos los archivos coincidentes).

  ```
  - icacls.exe "C:\ProgramData\Citrix\UpgradeServices\Downloads\
    VDA"/reset /T /C /L /Q
  ```

- **Opción 2**: Elimine la carpeta del VDA en Descargas y, a continuación, programe la actualización de versión del VDA.

**Solucionar errores de validación en la actualización de versiones de VDA** Siga los pasos que se indican a continuación para solucionar problemas y errores de descarga relacionados con la función de actualización de versiones de VDA:

1. Asegúrese de agregar las URL pertinentes a la lista de permitidos si existe el filtrado de URL, especialmente las URL de la lista de revocación de certificados (CRL) o del protocolo de estado de certificados en línea (OCSP) necesarias para comprobar la revocación. Consulte Requisito de actualización de versiones de VDA.
2. Tras agregar las URL necesarias a la lista de permitidos, pruebe a reprogramar la actualización de versiones de VDA.

Sugerimos habilitar el rastreo de CDF o configurar `LogToFile` en 1 con el objetivo de capturar registros detallados para su análisis. Los registros pueden incluir estos errores:

- RevocationStatusUnknown
- La función de revocación no pudo comprobar el estado de revocación del certificado.
- La función de revocación no pudo comprobar la revocación porque el servidor de revocación estaba desconectado.

El agente de actualización de versiones de VDA recurre a las llamadas del sistema de Windows para validar certificados y comprobar revocaciones. Los errores anteriores indican que el agente no puede establecer una conexión con las URL de CRL u OCSP.

Tenga en cuenta que el agente de actualización de versiones de VDA no admite actualmente parámetros de proxy. Las llamadas de CRL y OCSP salientes realizadas por CryptoAPI no conocen las configuraciones de proxy, lo que puede provocar errores.

Si su entorno tiene un proxy, puede configurar el proxy del sistema en el VDA para facilitar las llamadas de CRL salientes. Siga los pasos que se indican a continuación para configurar el proxy del sistema:

```
netsh winhttp import proxy source=ie

Or

netsh winhttp set proxy proxy-server=http://Proxy_Server:Port
<!--NeedCopy-->
```

### Actualizar la versión de los VDA mediante PowerShell

Puede configurar la actualización de versiones de VDA mediante el SDK de PowerShell remoto. Para obtener más información sobre el SDK de PowerShell remoto, consulte el SDK de PowerShell remoto de Citrix DaaS.

Estos son los cmdlets de PowerShell:

- **Get-VusCatalog**

  Use este cmdlet para obtener detalles de los catálogos, como `Name`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR), `Upgrade scheduled` y `StateId` (estado de `Upgrade scheduled`).

- **Get-VusMachine**

  Use este cmdlet para obtener detalles de las máquinas, como `MachineName`, `Uid`, `Uuid`, `UpgradeState` (`Available`, `UpToDate`, `Scheduled`, `Unknown`), `UpgradeType` (CR/LTSR) y `StateId` (estado de `Upgrade scheduled`).

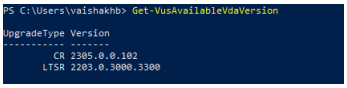
 

- **Get-VusComponentVersion**

  Use este cmdlet para comprobar si los VDA han notificado las versiones de los componentes. Use `MachineId` para filtrar los VDA. `MachineId` es el UUID de `Get-BrokerMachine`.

- **Get-VusAvailableVdaVersion**

  Use este cmdlet para comprobar la versión más reciente de CR/LTSR publicada a través del servicio de actualización de versiones de VDA.




- **Set-VusCatalogUpgradeType**

  Use este cmdlet para establecer el tipo de actualización de versión de un catálogo en CR o LTSR. El tipo de actualización solo se puede configurar al nivel de catálogo de máquinas.

- **New-VusMachineUpgrade**

  Use este cmdlet para configurar la actualización de versiones de los VDA al nivel de máquina.

- **New-VusCatalogSchedule**

  Use este cmdlet para programar la actualización de versiones al nivel de catálogo de máquinas.

#### Ejemplos de cmdlets al nivel de máquina

- Defina el tipo de actualización.

  Ejemplo:

  ```
  - Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType
    LTSR
  ```

- Use `Get-VusMachine` para comprobar el `UpgradeState` de las máquinas de un catálogo.

  Ejemplo:

  ```
  -Get-VusMachine -CatalogName test-catalog
  ```

```
PS C:\Users> Get-VusMachine -CatalogName test-catalog


CatalogName       : test-catalog
DNSName           : test-machine-1
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-1
MachineUid        : 35
MachineUuid       : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :

CatalogName       : test-catalog
DNSName           : test-machine-2
DurationInHours   :
LastStateChange   :
MachineName       : test-machine-2
MachineUid        : 36
MachineUuid       : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType  : MCS
ScheduledTime     :
SessionSupport    : SingleSession
StateId           :
StatusMessage     :
UpgradeState      : UpgradeAvailable
UpgradeType       : LTSR
UpgradeVersion    :
```

Si ve que `UpgradeState` es `Unknown`, una posible razón es que el agente de actualización de versiones de Citrix VDA instalado en el VDA no ha notificado la versión al servicio de actualización de versiones del VDA. Puede usar el cmdlet `Get-VusComponentVersion` para comprobar si el VDA ha notificado las versiones de los componentes.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Si no se muestran resultados, compruebe lo siguiente:

- El VDA forma parte de un catálogo y un grupo de entrega.
- El agente de actualización de versiones del VDA está instalado en el VDA y en ejecución. Si es necesario, intente reiniciar el agente.

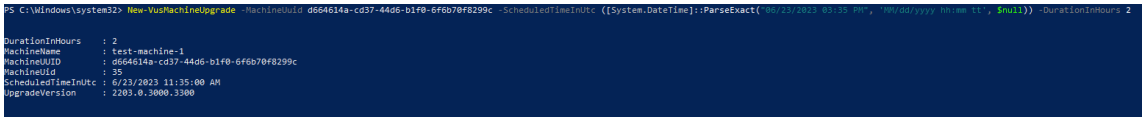
**Nota**: Si siguen sin obtener resultados, recopile el rastreo de Citrix Diagnostic Facility mientras reinicia el agente de actualización de versiones del VDA y soluciona los problemas que pueda haber.

- Programe actualizaciones de versión de VDA. Antes de empezar, tenga en cuenta lo siguiente:
  - `DurationInHours`: Le permite especificar la duración en horas del proceso de actualización. Los VDA pasarán al modo de mantenimiento. Se descargará el instalador de VDA y se actualizará la versión. Proporcione una mayor duración si hay muchos VDA que actualizar.
  - `UpgradeNow`: Utilice esta opción para programar una actualización de forma inmediata o para configurar `ScheduledTimeInUtc`.
  - `ScheduledTimeInUtc`: Le permite programar una actualización para una fecha y hora específicas.

  Ejemplo:

  - `New-VusMachineUpgrade -MachineUuid d664614a-cd37-44d6-b1f0-6f6b70f8299c -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 03:35 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 2`

  Puede usar `MachineUuid`, `MachineUid` y `MachineName` para programar la actualización de versiones de VDA.




- Compruebe el estado de la actualización.

  Ejemplo:

  - `Get-VusMachine -MachineName test-machine-1`

```
PS C:\Windows\system32> Get-VusMachine -MachineName test-machine-1


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 2
LastStateChange  : 6/23/2023 11:47:35 AM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 11:35:00 AM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

```
PS C:\Users\vaishakhb> Get-VusMachine -MachineName test-machine-1

CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

**Ejemplos de cmdlets al nivel de catálogo**

- Defina el tipo de actualización al nivel de catálogo de máquinas.

  Ejemplo:
  - `Set-VusCatalogUpgradeType -CatalogName test-catalog -UpgradeType LTSR`

- Use `Get-VusCatalog` para comprobar el `UpgradeState` de las máquinas de un catálogo:

  Ejemplo:
  - `Get-VusCatalog -Name test-catalog`

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog

CancelledUpgrades           :
DurationInHours             :
FailedUpgrades              :
InProgressUpgrades          :
LastStateChangeInUtc        :
MaxConcurrentUpgrades       :
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          :
SecurityCheckFailedUpgrades :
SessionSupport              : SingleSession
StateId                     :
SuccessfulUpgrades          :
TotalMachines               :
Uid                         : 30
UpgradeState                : UpgradeAvailable
UpgradeType                 : LTSR
UpgradeVersion              :
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

Si ve que `UpgradeState` es `Unknown`, una posible razón es que el agente de actualización de versiones de Citrix VDA instalado en el VDA no ha notificado la versión al servicio de actualización de versiones del VDA. Puede usar el cmdlet `Get-VusComponentVersion` para comprobar si el VDA ha notificado las versiones de los componentes.

- `Get-VusComponentVersion -MachineId ""`

```
PS C:\Users> Get-VusComponentVersion -MachineId  d664614a-cd37-44d6-b1f0-6f6b70f8299c

      ComponentType MachineId                            Uid                                  Version
      ------------- ---------                            ---                                  -------
                VDA d664614a-cd37-44d6-b1f0-6f6b70f8299c 7505fa4c-1811-ee11-907e-0022484becbd 2203.0.0.33220
                VUS d664614a-cd37-44d6-b1f0-6f6b70f8299c 7705fa4c-1811-ee11-907e-0022484becbd 7.37.0.7
                Mps d664614a-cd37-44d6-b1f0-6f6b70f8299c 7805fa4c-1811-ee11-907e-0022484becbd 7.33.0.26
SupportabilityTools d664614a-cd37-44d6-b1f0-6f6b70f8299c 7a05fa4c-1811-ee11-907e-0022484becbd 1.5.0.17
                Upm d664614a-cd37-44d6-b1f0-6f6b70f8299c 7c05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
       UpmVdaPlugin d664614a-cd37-44d6-b1f0-6f6b70f8299c 7d05fa4c-1811-ee11-907e-0022484becbd 22.3.0.7
```

Si no se muestran resultados, compruebe lo siguiente:

  - El VDA forma parte de un catálogo y un grupo de entrega.
  - El agente de actualización de versiones del VDA está instalado en el VDA y en ejecución. Si es necesario, intente reiniciar el agente.

**Nota**: Si siguen sin obtener resultados, recopile el rastreo de Citrix Diagnostic Facility mientras reinicia el agente de actualización de versiones del VDA y soluciona los problemas que pueda haber.

- Programe actualizaciones de versión de VDA. Antes de empezar, tenga en cuenta lo siguiente:

  - `DurationInHours`: Le permite especificar la duración en horas del proceso de actualización. Los VDA del catálogo pasarán al modo de mantenimiento. Se descargará el instalador de VDA y se actualizará la versión en cada VDA. Proporcione una mayor duración si el catálogo contiene muchos VDA.
  - `UpgradeNow`: Utilice esta opción para programar una actualización de forma inmediata o para configurar `ScheduledTimeInUtc`.
  - `ScheduledTimeInUtc`: Le permite programar una actualización para una fecha y hora específicas.

  Ejemplo:

  - `New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null))-DurationInHours 4`

  Puede usar `CatalogName`, `Uid` y `Uuid` para programar la actualización de versión.

```
PS C:\Windows\system32> New-VusCatalogSchedule -CatalogName test-catalog -ScheduledTimeInUtc ([System.DateTime]::ParseExact("06/23/2023 04:00 PM", 'MM/dd/yyyy hh:mm tt', $null)) -DurationInHours 4

CatalogName          : test-catalog
CatalogUUID          : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
CatalogUid           : 30
DurationInHours      : 4
LastStateChangeInUtc : 6/23/2023 12:08:14 PM
ScheduledTimeInUtc   : 6/23/2023 12:00:00 PM
State                : UpgradeScheduled
UpgradeVersion       : 2203.0.3000.3300
```

- Compruebe el estado de la actualización. Use los cmdlets `Get-VusCatalog` o `Get-VusMachine` para comprobar periódicamente el estado de actualización de los VDA. Use `MachineUuid`, `MachineUid` y `MachineName` para filtrar los VDA.

  Ejemplo:
  - `Get-VusCatalog -Name test-catalog`

```
PS C:\Windows\system32> Get-VusCatalog -Name test-catalog


CancelledUpgrades           : 0
DurationInHours             : 4
FailedUpgrades              : 0
InProgressUpgrades          : 0
LastStateChangeInUtc        : 6/23/2023 12:08:43 PM
MaxConcurrentUpgrades       : 100
Name                        : test-catalog
ProvisioningType            : MCS
ScheduledTimeInUtc          : 6/23/2023 12:00:00 PM
SecurityCheckFailedUpgrades : 0
SessionSupport              : SingleSession
StateId                     : UpgradeInProgress
SuccessfulUpgrades          : 0
TotalMachines               : 2
Uid                         : 30
UpgradeState                : UpgradeScheduled
UpgradeType                 : LTSR
UpgradeVersion              : 2203.0.3000.3300
Uuid                        : 3ad4253c-3dfa-4982-8e6e-7686bf904da1
```

  Use `Get-VusMachine` para ver el estado de actualización de los VDA de cada máquina de un catálogo.

```
PS C:\Users\vaishakhb> Get-VusMachine -CatalogName test-catalog


CatalogName      : test-catalog
DNSName          : test-machine-1
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:18:21 PM
MachineName      : test-machine-1
MachineUid       : 35
MachineUuid      : d664614a-cd37-44d6-b1f0-6f6b70f8299c
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeSuccess
StatusMessage    : Upgrade completed successfully or is already up to date
UpgradeState     : UpToDate
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300

CatalogName      : test-catalog
DNSName          : test-machine-2
DurationInHours  : 4
LastStateChange  : 6/23/2023 12:17:33 PM
MachineName      : test-machine-2
MachineUid       : 36
MachineUuid      : cfa55303-6000-4973-bee8-e38c9916719e
ProvisioningType : MCS
ScheduledTime    : 6/23/2023 12:00:00 PM
SessionSupport   : SingleSession
StateId          : UpgradeInProgress
StatusMessage    :
UpgradeState     : UpgradeScheduled
UpgradeType      : LTSR
UpgradeVersion   : 2203.0.3000.3300
```

### Si el VDA tiene un disco Personal vDisk instalado

Si el componente Personal vDisk (PvD) se ha instalado alguna vez en un VDA, dicho VDA no se puede actualizar a la versión 1912 LTSR ni a ninguna posterior hasta que se quite ese componente.

Este paso debe seguirse aunque nunca haya usado PvD. Así es como el componente PvD podría haberse instalado en versiones anteriores:

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

#### Qué se debe hacer

Si el instalador de VDA no detecta el componente PvD en el VDA instalado actualmente, la actualización de la versión continúa como de costumbre.

Si el instalador detecta el componente PvD en el VDA instalado actualmente:

- **Interfaz gráfica:** La actualización de la versión queda en pausa. Un mensaje le pregunta si quiere que el componente no admitido se quite automáticamente. Si hace clic en **Aceptar**, el componente se quita automáticamente y la actualización continúa.
- **Interfaz de línea de comandos:** El comando falla si el instalador detecta el componente PvD. Para evitar errores de comando, incluya la siguiente opción en el comando: `/remove_pvd_ack`.

Si quiere continuar mediante PvD en sus máquinas con Windows 10 (1607 y versiones anteriores, sin actualizaciones), VDA 7.15 LTSR es la última versión compatible. Tenga en cuenta que el programa ampliado para XenApp y XenDesktop 7.15 LTSR no se aplica a los VDA que se utilizan con Citrix DaaS. Para obtener más información, consulte el documento Extended Support Customer Guide en Citrix Support Knowledge Center.

### Sistemas operativos anteriores

En el artículo Requisitos del sistema se enumeran los sistemas operativos Windows compatibles con los VDA de la versión actual.

- Para los VDA LTSR, consulte el artículo de requisitos del sistema de su versión LTSR.
- Para los VDA de Linux, consulte la documentación de Linux Virtual Delivery Agent.

Para las máquinas con sistemas operativos Windows donde ya no se pueden instalar los VDA más recientes, dispone de varias opciones.

Para entornos que no son WVD:

- Restablezca la imagen de la máquina a una versión Windows compatible y, a continuación, instale el nuevo VDA.
- Si restablecer la imagen de la máquina no es una opción, pero quiere actualizar el sistema operativo, desinstale el agente VDA antes de actualizar el sistema operativo. De lo contrario, el VDA entrará en un estado no admitido. Después de actualizar la versión del sistema operativo, instale el nuevo VDA.
- Si la máquina tiene instalada la versión LTSR 7.15 e intenta instalar una versión más reciente, aparecerá un mensaje que le informará de que usa la versión compatible más reciente.
- Si la máquina tiene instalada una versión anterior a LTSR 7.15, aparecerá un mensaje que le guiará a CTX139030 para obtener más información. Puede descargar los VDA 7.15 LTSR desde el sitio web de Citrix.

# Migrar la configuración a Citrix Cloud

March 30, 2024

## Por qué utilizar la Configuración automatizada

Los administradores de TI encargados de entornos grandes o complejos suelen ver que las migraciones son un proceso tedioso. Con frecuencia terminan programando sus propias herramientas para llevar a cabo esta tarea correctamente, ya que suele ser específica para sus casos de uso.

Citrix quiere ayudar a facilitar este proceso mediante la automatización del proceso de migración mediante la herramienta Configuración automatizada. Los administradores pueden probar fácilmente las configuraciones actuales en Citrix Cloud y aprovechar las ventajas que ofrece Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) mientras mantienen *intactos* sus entornos actuales. Tampoco afecta al usuario final, ya que la Configuración automatizada funciona perfectamente en segundo plano. Estas ventajas incluyen la reducción de la sobrecarga administrativa cuando Citrix administra parte del plano de control y del back-end, y las actualizaciones automáticas y personalizables de componentes de Citrix Cloud, entre otras.

Citrix utiliza la configuración estándar del sector como código para proporcionar un mecanismo que ayude a automatizar los procesos de migración. La Configuración automatizada detecta y exporta uno o varios sitios locales como un conjunto de archivos de configuración. La configuración de estos archivos se puede importar a Citrix DaaS.

La Configuración automatizada también permite a los administradores fusionar varios sitios locales en un único sitio, al tiempo que evita la colisión de nombres. Los administradores pueden controlar si la configuración local o de la nube controla los recursos.

La Configuración automatizada no es solo una herramienta de migración única, sino que también puede automatizar su configuración diaria en Citrix Cloud. Mover la configuración de Citrix DaaS puede tener muchos beneficios:

- Sincronización de su sitio desde la prueba o etapa a la producción
- Copia de seguridad y restauración de la configuración
- Límites de recursos alcanzados
- Migrar de una región a otra

Este vídeo de *2 minutos* ofrece un recorrido rápido por la Configuración automatizada.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Para obtener información adicional sobre la Configuración automatizada, consulte Proof of Concept: Automated Configuration Tool en Tech Zone.

Para obtener información más detallada sobre cómo mover la implementación y preparar la configuración local para la migración, consulte Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud en Tech Zone.

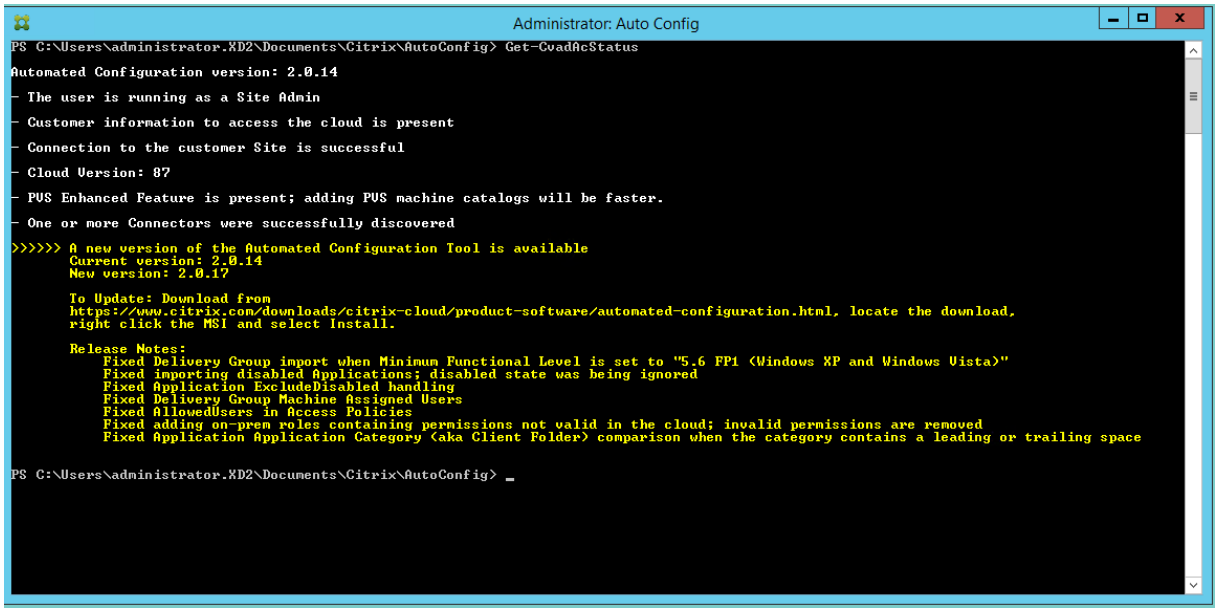
### Descargar la Configuración automatizada

Descargue e instale la herramienta de Configuración automatizada desde Descargas de Citrix.

> **Importante:**
>
> Para evitar errores de funcionalidad, utilice siempre la versión más reciente disponible de la Configuración automatizada.

### Actualizar la versión de la Configuración automatizada

Al ejecutar cmdlets que acceden a la nube en la Configuración automatizada, la herramienta le avisa cuando hay una versión más reciente disponible para su descarga.




Siga estos pasos para asegurarse de que dispone de la versión más reciente:

1. Haga doble clic en el icono de **configuración automática**. Aparece una ventana de PowerShell.
2. Ejecute el siguiente comando para comprobar el número de versión.

   ```
   Get-CvadAcStatus
   ```

3. Compare la versión de la herramienta con la que aparece en la alerta o en Descargas de Citrix. La versión más reciente de la herramienta se encuentra allí.

4. Descargue e instale la versión más reciente de la herramienta. *No* necesita desinstalar la versión anterior para actualizar la versión de la Configuración automatizada.

> **Nota:**
>
> La alerta aparece cada vez que ejecuta un cmdlet que accede a la nube. Para obtener más información sobre cmdlets, consulte Cmdlets de la herramienta de Configuración automatizada.

### Limitaciones conocidas

- Hay aspectos especiales que considerar para los catálogos de máquinas aprovisionados a través de Machine Creation Services. Para obtener más información sobre MCS, consulte Descripción de la migración de catálogos aprovisionados de Machine Creation Services.

### Objetos admitidos para la migración

La Configuración automatizada permite mover la configuración de estos componentes:

- Etiquetas
- Administrador delegado
  - Ámbitos
  - Roles
- Conexiones de host
  - Un único grupo de recursos
  - Ámbitos de administración
- Catálogos de máquinas
  - Ámbitos de administración
  - Máquinas
  - Acceso con Remote PC, físicas, agrupadas, aprovisionadas, MCS, asignadas
- Almacenes de StoreFront
- Grupos de entrega
  - Directiva de acceso
  - Asociación de ámbitos de administración
  - Directiva de acceso a aplicaciones
  - Directiva de asignaciones
  - Directiva de derechos o de escritorio
  - Programaciones de energía

  - Persistencia de sesiones
  - Preinicio de sesiones
  - Programaciones de reinicio
  - Etiquetas
- Grupos de aplicaciones
  - Asociación de ámbitos de administración
  - Grupos de entrega
  - Usuarios y grupos
- Aplicaciones
  - Carpetas de aplicaciones
  - Iconos
  - Aplicaciones
  - Asociaciones de tipos de archivo configuradas por un intermediario
  - Etiquetas
- Directivas de grupo
- Preferencias de zona de usuario

### Orden de migración de componentes

Los componentes y sus dependencias aparecen aquí. Las dependencias de un componente deben estar en su lugar para poder importarlo o fusionarlo. Si falta una dependencia, puede provocar un error en el comando de importación o fusión. La sección **Fixups** del archivo de registro muestra las dependencias que faltan si falla una importación o fusión.

1. Etiquetas
   - Sin dependencias previas
2. Administrador delegado
   - Sin dependencias previas
3. Conexiones de host
   - Información de seguridad en CvadAcSecurity.yml
4. Catálogos de máquinas
   - Máquinas presentes en Active Directory
   - Conexiones de host
   - Etiquetas

5. Almacenes de StoreFront
6. Grupos de entrega
    - Máquinas presentes en Active Directory
    - Usuarios presentes en Active Directory
    - Catálogos de máquinas
    - Etiquetas
7. Grupos de aplicaciones
    - Grupos de entrega
    - Etiquetas
8. Aplicaciones
    - Grupos de entrega
    - Grupos de aplicaciones
    - Etiquetas
9. Directivas de grupo
    - Grupos de entrega
    - Etiquetas
10. Preferencias de zona de usuario

## Requisitos previos comunes

A continuación, se indican algunos requisitos previos comunes necesarios para que la Configuración automatizada funcione correctamente. Estos requisitos previos se utilizan tanto en las migraciones de configuraciones locales a la nube como de la nube a la nube.

### Generar el ID del cliente, el ID de la máquina cliente y la clave secreta

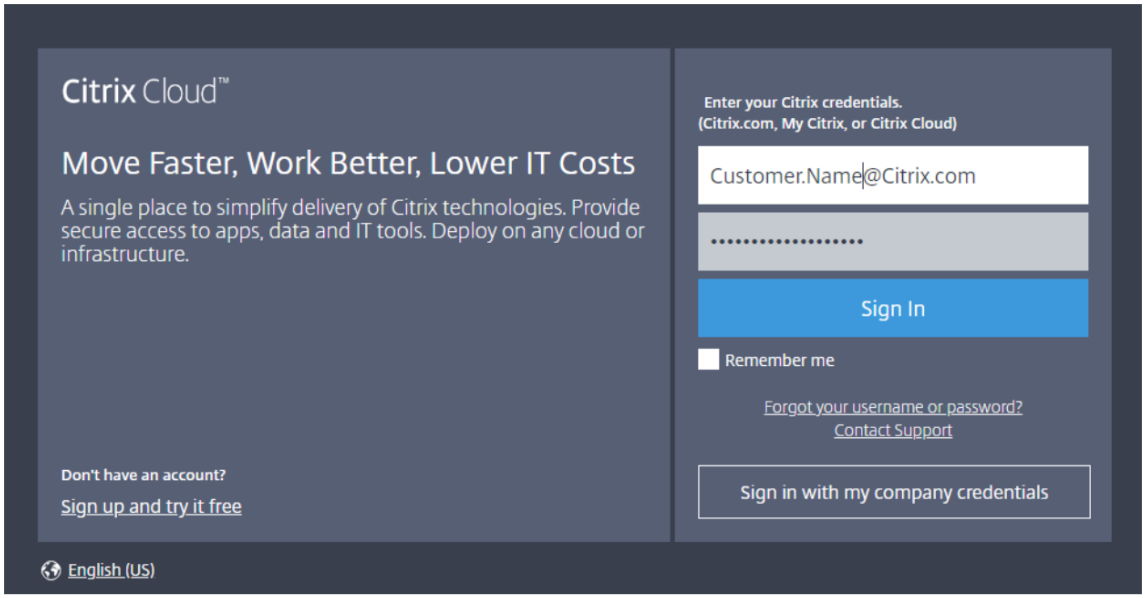
Antes de comenzar la migración con la Configuración automatizada, necesita su ID de cliente de Citrix Cloud y debe crear un ID de cliente y una clave secreta para importar la configuración a Citrix Cloud. Todos los cmdlets que acceden a la nube requieren estos valores.

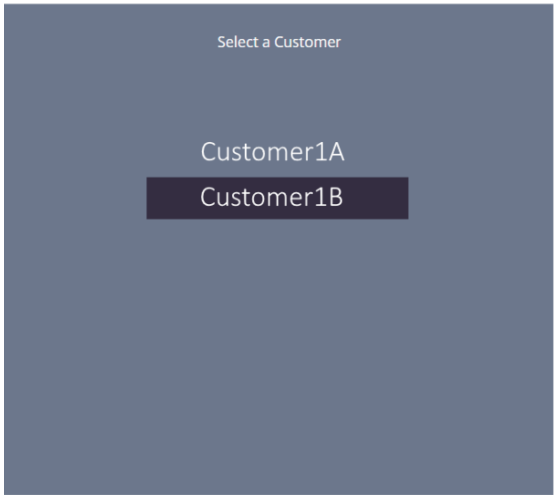
Estos pasos le permiten obtener el ID del cliente y crear el ID de la máquina cliente y la clave secreta.

Para obtener el **ID de cliente**:

1. Inicie sesión en su cuenta de Citrix Cloud y seleccione el cliente.

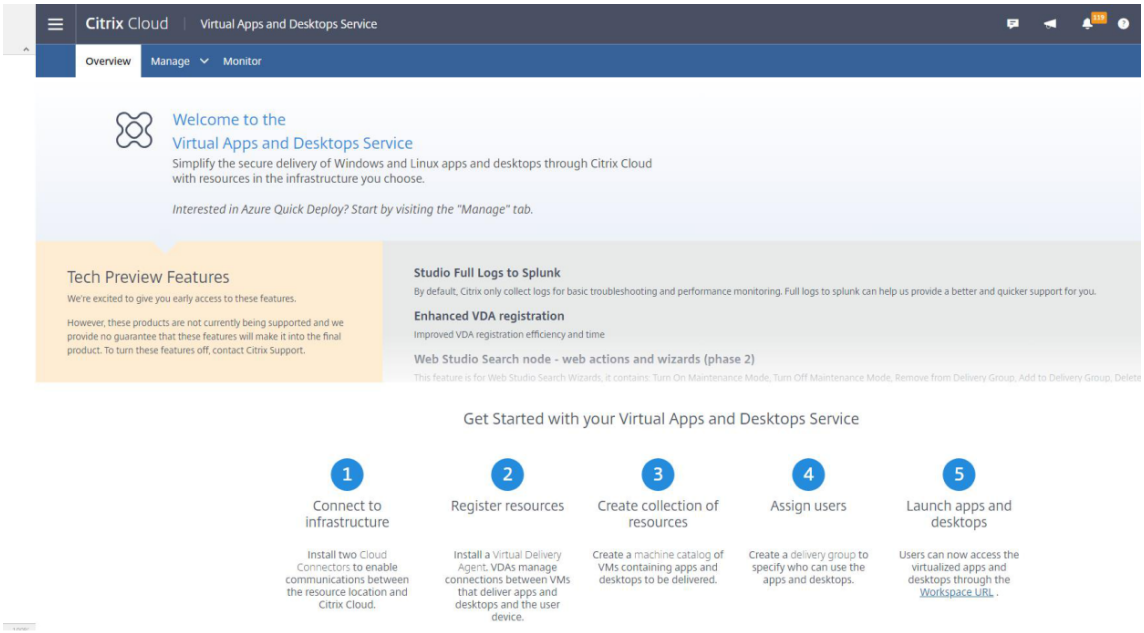
 

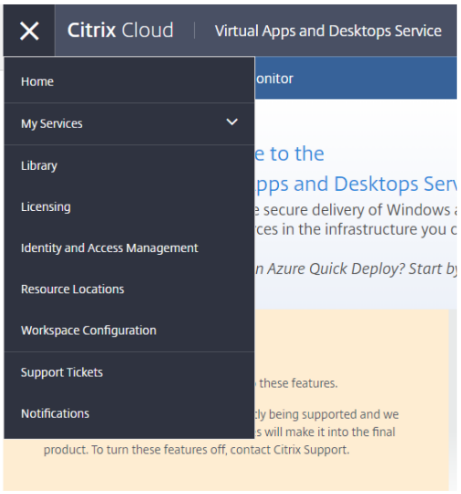


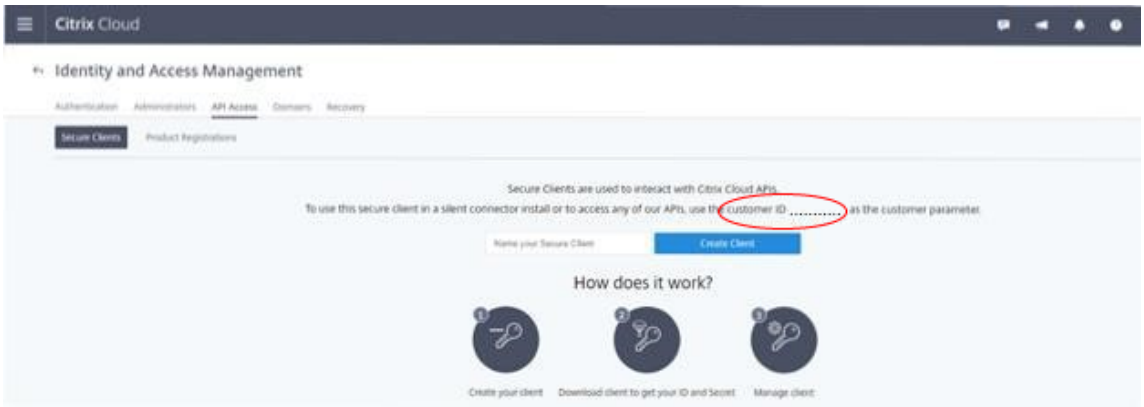

2. Haga clic en el menú de tres líneas y, a continuación, seleccione **Administración de acceso e identidad** en el menú desplegable.



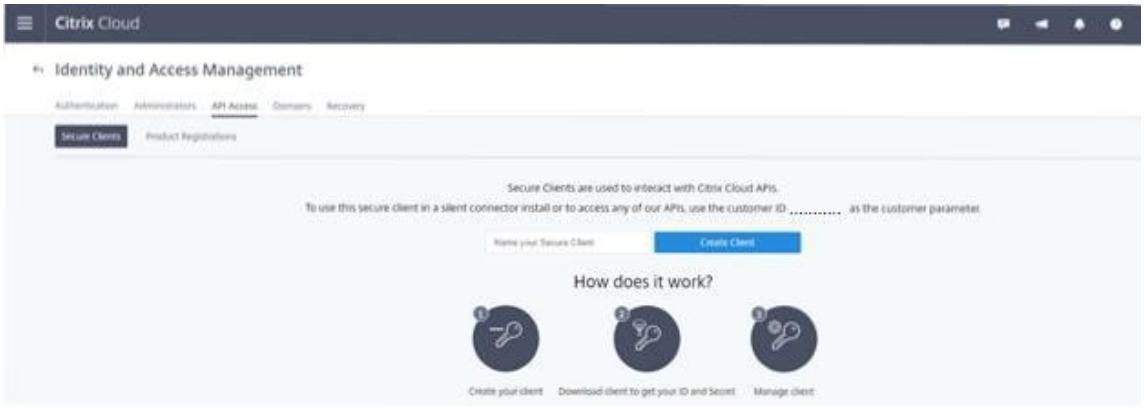

3. El **ID de cliente** se encuentra en la página **Administración de acceso e identidad**.



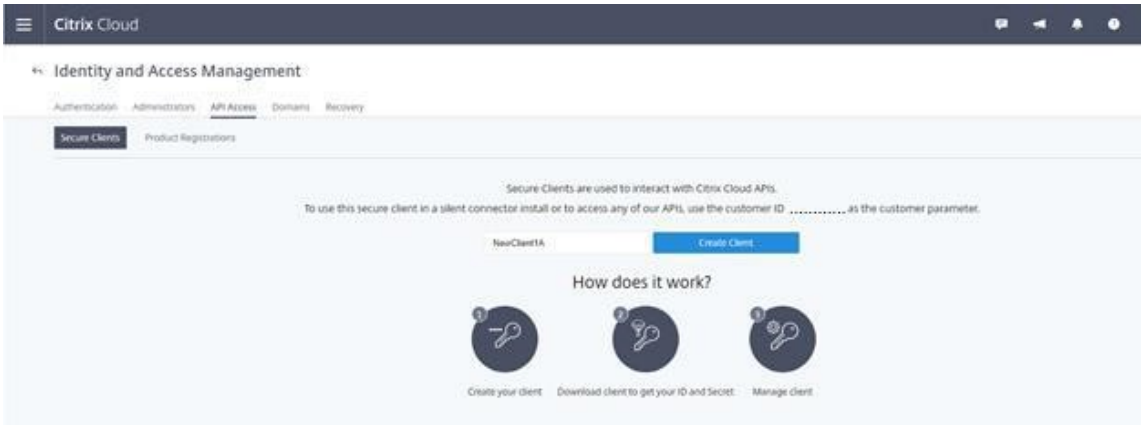

 

Para obtener el **ID de la máquina cliente** y la **clave secreta**:

1. En la página **Administración de acceso e identidad**, haga clic en la ficha **Acceso a API**.

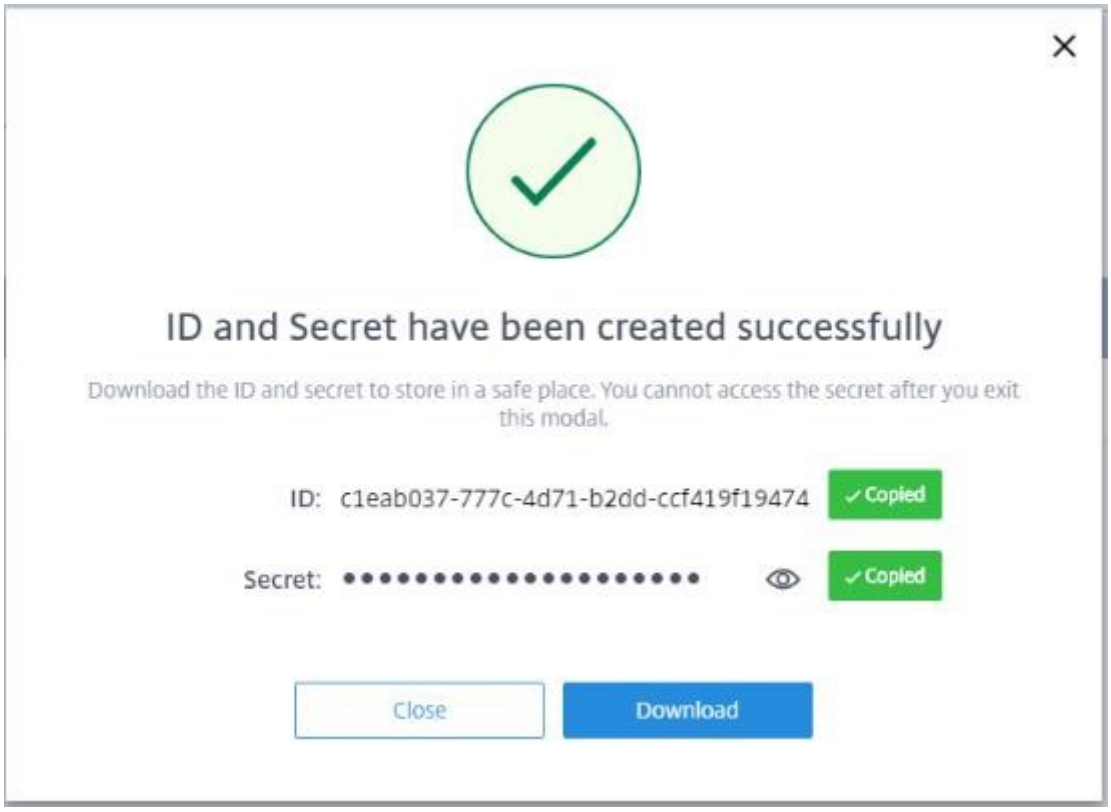



2. Escriba un nombre en el cuadro. Este nombre se utiliza para diferenciar múltiples ID de máquinas cliente y claves secretas. Haga clic en **Crear cliente** para crear el ID de la máquina cliente y la clave secreta.

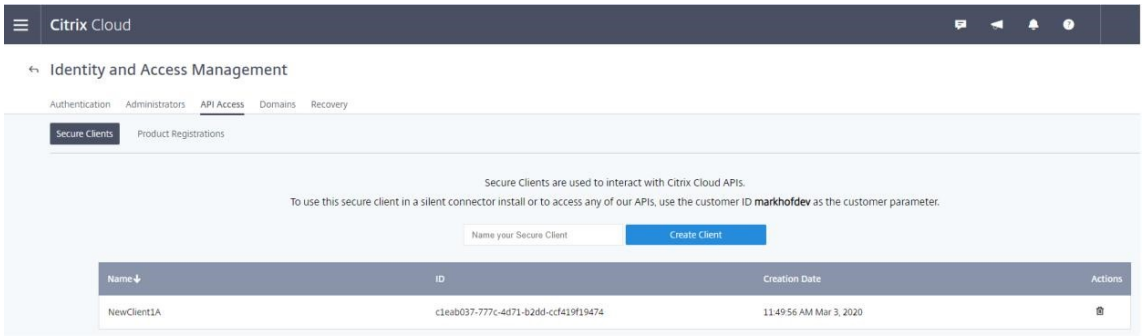



3. El siguiente cuadro de diálogo aparece después de crear correctamente el ID de la máquina cliente y la clave secreta. Asegúrese de copiar los dos valores en una ubicación segura y descargue el archivo CSV que contiene esta información. El archivo CSV se puede utilizar para crear el archivo CustomerInfo.yml.




4. El ID de la máquina cliente y la clave secreta se crean correctamente.




Coloque estos valores en una ubicación segura y compártalos solamente con miembros de confianza de la empresa que necesiten acceder a la herramienta o a las API de REST de la nube. El ID de la máquina cliente y la clave secreta no caducan. Si corren peligro, elimínelos inmediatamente con el icono de **papelera** y cree otros.

> **Nota:**
>
> No se puede obtener una clave secreta si se pierde o se olvida; debe crearse otro ID de máquina cliente y otra clave secreta.

### Rellenar el archivo de información del cliente

El uso del archivo CustomerInfo.yml elimina la necesidad de proporcionar parámetros de información del cliente al ejecutarse cada cmdlet. Cualquier información del cliente se puede reemplazar mediante parámetros de cmdlet.

Cree el archivo CustomerInfo.yml mediante el cmdlet `New-CvadAcCustomerInfoFile`.

> **Importante:**
>
> No modifique manualmente el archivo CustomerInfo.yml. Si lo hace, se pueden producir errores de formato involuntarios.

`New-CvadAcCustomerInfoFile` tiene estos parámetros obligatorios.

- CustomerId: ID del cliente.
- ClientId: ID de la máquina cliente creado en Citrix Cloud.
- Secret: Secreto del cliente creado en Citrix Cloud.

```
New-CvadAcCustomerInfoFile -CustomerId markhof123 -ClientId 6813EEA6
-46CC-4F8A-BC71-539F2DAC5984 -Secret TwBLaaaaaaaaaaaaaaaaw==
```

También puede crear CustomerInfo.yml mediante el parámetro `SecurityCsvFileSpec` que apunta al archivo security.csv descargado. También debe especificar el campo CustomerId.

```
New-CvadAcCustomerInfoFile -SecurityCsvFileSpec C:\Users\my_user_name
\downloads/security.csv -CustomerId markhof123
```

Actualice el archivo CustomerInfo.yml mediante el cmdlet `Set-CvadAcCustomerInfoFile`. Este cmdlet solo cambia el ID de la máquina cliente.

```
Set-CvadAcCustomerInfoFile -ClientId C80487EE-7113-49F8-85DD-2CFE30CC398E
```

A continuación, se muestra un archivo CustomerInfo.yml de ejemplo.

```
# Created/Updated on 2020/01/29 16:46:47
CustomerId: 'markhof123'
ClientId: '6713FEA6-46CC-4F8A-BC71-539F2DDK5384'
Secret: 'TwBLaaabbbaaaaaaaaaaw=='
Environment: Production
AltRootUrl: ''
StopOnError: False
AlternateFolder: ''
Locale: 'en-us'
Editor: 'C:\Program Files\Notepad++\notepad++.exe'
Confirm: True
DisplayLog: True
```

### Rellenar el archivo de asignación de zonas

Una zona local equivale a la ubicación de recursos en la nube. A diferencia de otros componentes del sitio, no puede importar automáticamente la zona local en la nube. En su lugar, debe asignarse manualmente mediante el archivo ZoneMapping.yml. Pueden producirse errores de importación si el nombre de zona no está asociado a un nombre de ubicación de recursos existente.

Para los sitios locales que tienen una sola zona y los sitios en la nube que tienen una sola ubicación de recursos, la herramienta de Configuración automatizada establece la asociación correcta, lo que elimina la necesidad de administrar manualmente el archivo ZoneMapping.yml.

Para los sitios locales que tienen varias zonas o los sitios en la nube que tienen varias ubicaciones de recursos, el archivo ZoneMapping.yml debe actualizarse manualmente a fin de reflejar la asignación correcta de zonas locales a ubicaciones de recursos en la nube. Esto debe hacerse antes de intentar cualquier operación de importación a la nube.

El archivo ZoneMapping.yml se encuentra en *%HOMEPATH%\Documentos\Citrix\AutoConfig*. El contenido del archivo YML es un diccionario con el nombre de la zona como la clave y el nombre de la ubicación de recursos como el valor.

Por ejemplo, un sitio local de Citrix Virtual Apps and Desktops con una zona principal denominada "Zone-1"y una zona secundaria denominada "Zone-2"se migra a una implementación en la nube de Citrix DaaS con dos ubicaciones de recursos recién creadas denominadas "Cloud-RL-1"y "Cloud-RL-2" . En este caso, ZoneMapping.yml se configuraría de la siguiente manera:

```
1               Zone-1: Cloud-RL-1
2
3               Zone-2: Cloud-RL-2
```

> **Nota:**
>
> Debe haber un espacio entre los dos puntos y el nombre de la ubicación de recursos. Si se utilizan espacios en el nombre de la zona o de la ubicación de recursos, escriba el nombre entre comillas.

### Conexiones de host

Las conexiones de host y sus hipervisores asociados se pueden exportar e importar mediante la Configuración automatizada.

Agregar un hipervisor a una conexión de host requiere información de seguridad específica del tipo de hipervisor. Esta información no se puede exportar desde el sitio local por motivos de seguridad. Debe proporcionar la información manualmente para que la Configuración automatizada pueda importar correctamente las conexiones de host y los hipervisores al sitio en la nube.

El proceso de exportación crea el archivo CvadAcSecurity.yml en *%HOMEPATH%\Documentos\Citrix\AutoConfig* y contiene marcadores de posición para cada elemento de seguridad que necesita el tipo de hiper-

visor específico. Debe actualizar el archivo CvadAcSecurity.yml antes de realizar la importación en el sitio de la nube. Las actualizaciones de administrador se conservan en varias exportaciones con nuevos marcadores de posición de seguridad agregados según sea necesario. Los elementos de seguridad nunca se eliminan. Para obtener más información, consulte Manually update the CvadAcSecurity.yml file.

```
            HostConn1:
            ConnectionType: XenServer
            UserName: root
            PasswordKey: rootPassword
            HostCon2:
            ConnectionType: AWS
            ApiKey: 78AB6083-EF60-4D26-B2L5-BZ35X00DA5CH
            SecretKey: TwBLaaaaaaaaaaaaaaaaw==
            Region: East
```

**Información de seguridad por hipervisor** A continuación, se muestra la información de seguridad necesaria para cada tipo de hipervisor.

- XenServer, Hyper-V, VMware
  - Nombre de usuario
  - Contraseña de texto no cifrado
- Microsoft Azure
  - ID de suscripción
  - ID de aplicación
  - Secreto de la aplicación
- Amazon Web Services
  - ID de cuenta de servicio
  - Secreto de la aplicación
  - Region

**Consideraciones especiales sobre seguridad** Toda la información de seguridad se introduce como texto no cifrado. Si no se recomienda texto sin cifrar, se pueden crear manualmente las conexiones de host y los hipervisores asociados mediante la interfaz de **Administrar > Configuración completa**. Las conexiones de host y los nombres de hipervisor deben coincidir exactamente con sus homólogos locales para que los catálogos de máquinas que utilizan las conexiones de host puedan importarse correctamente.

### Activar sitios

El Delivery Controller tanto en sitios locales como en la nube controla recursos como la intermediación con escritorios y aplicaciones y el reinicio de máquinas. Los problemas se producen cuando un conjunto común de recursos está controlado por dos o más sitios. Una situación así puede ocurrir al migrar de un sitio local a un sitio en la nube. Tanto los Delivery Controllers locales como los de la nube pueden administrar el mismo conjunto de recursos. Esta administración dual puede hacer que los recursos no estén disponibles y que no se puedan administrar, y puede ser difícil de diagnosticar.

La activación del sitio le permite controlar dónde se controla el sitio activo.

La activación del sitio se gestiona mediante el modo de mantenimiento del grupo de entrega. Los grupos de entrega se colocan en modo de mantenimiento cuando el sitio está inactivo. Para los sitios que están activos, se quita el modo de mantenimiento de los grupos de entrega.

La activación del sitio no afecta ni administra el registro de VDA ni los catálogos de máquinas.

- `Set-CvadAcSiteActiveStateCloud`
- `Set-CvadAcSiteActiveStateOnPrem`

Todos los cmdlets admiten el filtrado `ExcludeByName` y `IncludeByName`. Este parámetro permite seleccionar los grupos de entrega a los que se puede cambiar el modo de mantenimiento. Los grupos de entrega se pueden cambiar de forma selectiva según sea necesario.

#### Importar y transferir el control a la nube

A continuación, se ofrece una descripción de alto nivel sobre cómo importar y transferir el control desde el sitio local al sitio en la nube.

1. Exporte el sitio local a la nube. Asegúrese de que el parámetro `–SiteActive` no está presente en ninguno de los cmdlets de importación. El sitio local está activo y el sitio en la nube está inactivo. De forma predeterminada, los grupos de entrega de sitios en la nube se encuentran en modo de mantenimiento.
2. Verifique el contenido y la configuración de la nube.
3. Durante las horas de descanso, establezca el sitio local en inactivo. El parámetro `–SiteActive` no debe estar presente. Todos los grupos de entrega de sitios locales se encuentran en modo de mantenimiento.
    - `Set-CvadAcSiteActiveStateOnPrem`
4. Establezca el sitio en la nube como activo. El parámetro `–SiteActive` debe estar presente. No hay grupos de entrega del sitio en la nube en modo de mantenimiento.
    - `Set-CvadAcSiteActiveStateCloud –SiteActive`

5. Compruebe que el sitio en la nube esté activo y que el sitio local esté inactivo.

#### Transferir el control de nuevo al sitio local

Para transferir el control del sitio en la nube al sitio local:

1. Durante las horas de descanso, establezca el sitio en la nube como inactivo. Todos los grupos de entrega del sitio en la nube están en modo de mantenimiento.
   - `Set-CvadAcSiteActiveStateCloud`
2. Establezca el sitio local como activo. No hay grupos de entrega del sitio local en modo de mantenimiento.
   - `Set-CvadAcSiteActiveStateOnPrem -SiteActive`

#### Información adicional sobre la activación de sitios

- Si no hay máquinas con administración de energía ni programaciones de reinicio (lo que normalmente significa que tampoco hay conexiones de host), todos los grupos de entrega en la nube se pueden importar como activos. Agregue `-SiteActive` a `Merge-CvadAcToSite`/`Import-CvadAcToSite` o ejecute `Set-CvadAcSiteActiveStateCloud -SiteActive` tras la importación.
- Si se trata de máquinas con administración de energía o hay programaciones de reinicio, se utiliza un proceso diferente. Por ejemplo, al cambiar de local a la nube en este caso, establezca el sitio local en inactivo mediante `Set-CvadAcSiteActiveStateOnPrem`. A continuación, configure el sitio en la nube como activo mediante `Set-CvadAcSiteActiveStateCloud -SiteActive`.
- Los cmdlets `Set-CvadAcSiteActiveStateCloud` y `Set-CvadAcSiteActiveStateOnPrem` también sirven para invertir el proceso. Por ejemplo, ejecute `Set-CvadAcSiteActiveStateCloud` sin el parámetro `-SiteActive` y, a continuación, ejecute `Set-CvadAcSiteActiveStateOnPrem` con el parámetro `-SiteActive`.

### Descripción de la migración de catálogos aprovisionados de Machine Creation Services

> **Nota:**
>
> Esta función solo está disponible a partir de la versión 3.0. Para comprobar la versión, use `Get-CvadAcStatus` en la Configuración automatizada.

Los catálogos de Machine Creation Services (MCS) crean dos tipos diferentes de catálogos:

- Cuando se pierden o se revierten cambios realizados en una máquina (normalmente con SO de servidor, donde se publican las aplicaciones), se trata de un caso de uso de VDI agrupados o multisesión.
- Cuando se conservan cambios realizados en una máquina durante el reinicio (normalmente con SO cliente con un usuario dedicado), se trata de un caso de uso de VDI estáticos.

El tipo de catálogo se puede confirmar en el nodo de catálogo de Citrix Studio y en el valor "Datos del usuario:"del catálogo.

> **Nota:**
>
> No se puede realizar una copia de seguridad de MCS desde la nube mediante la Configuración automatizada.

#### Catálogos multisesión o de VDI agrupados

Los catálogos con "Datos del usuario: Descartar"son catálogos de VDI agrupados y solo pueden migrar la imagen principal y la configuración. Las máquinas virtuales de estos catálogos no se migran. Esto se debe a que el sitio desde el que realiza la importación mantiene el ciclo de vida de la máquina virtual, lo que significa que, cada vez que se encienden las máquinas, es posible que su estado cambie. Esto impide la importación, ya que los datos de importación de las máquinas virtuales se desincronizan rápidamente.

Al migrar estos catálogos con la herramienta, esta crea metadatos del catálogo e inicia la creación de la imagen principal, pero no se importa ninguna máquina.

Dado que este proceso puede tardar algún tiempo en crearse en función del tamaño de la imagen principal, el comando de importación de la herramienta solo inicia la creación de catálogos de MCS y no espera a que finalice. Una vez finalizada la importación, supervise el progreso de la creación de catálogos mediante la interfaz de administración de Configuración completa en la implementación en la nube.

Una vez creada la imagen principal, puede aprovisionar máquinas. Es necesario tener en cuenta aspectos sobre la capacidad, ya que se consumiría capacidad del uso local.

Todos los demás objetos (grupos de entrega, aplicaciones, directivas…) que utilizan ese catálogo se pueden importar y no tienen que esperar a que se cree la imagen principal. Cuando el catálogo haya terminado de crearse, las máquinas se pueden agregar al catálogo importado y, a continuación, los usuarios pueden iniciar sus recursos.

> **Nota:**
>
> Utilice los mismos comandos disponibles en la herramienta para migrar catálogos y todos los demás objetos.

### Catálogos de VDI estáticos

> **Nota:**
>
> Dado que esta operación importa detalles de bajo nivel que se almacenan en la base de datos, este proceso debe ejecutarse desde una máquina con acceso a la base de datos.

Los catálogos de VDI estáticos migran la imagen principal, las configuraciones y todas las máquinas virtuales. A diferencia del caso de uso de VDI agrupados, no es necesario crear imágenes.

Los VDA deben apuntar al conector para que se registren en la nube.

Consulte la sección Activar sitios para activar el sitio de la nube, de modo que la nube controle la programación de reinicios, la administración de energía y otros elementos.

Una vez completada la migración, si quiere eliminar este catálogo de su sitio local, debe abandonar cuenta la VM y la cuenta de AD. De lo contrario, se eliminan, y el sitio en la nube quedaría apuntando a la máquina virtual eliminada.

## Actualizar las etiquetas MCS para detectar recursos huérfanos después de la migración

Después de migrar la configuración de un sitio de local a la nube o de la nube a otro sitio en la nube, debe actualizar las etiquetas de identificación del sitio de MCS en el caso de máquinas virtuales persistentes para que los recursos huérfanos se puedan detectar correctamente. Para hacer esto, use el comando de PowerShell `Set-ProvResourceTags`. Actualmente, esta función se aplica a Azure.

Estos son los pasos detallados:

1. Actualice las etiquetas de identificación del sitio MCS desde el nuevo sitio de Citrix mediante el comando de PowerShell `Set-ProvResourceTags`. Por ejemplo:

   ```
   1 Set-ProvResourceTags -ProvisioningSchemeUid xxxxx  [-VMName <
       String>] [-VMBatchSize XX] [-ResourceType XX]
   2 <!--NeedCopy-->
   ```

   O bien:

   ```
   1 Set-ProvResourceTags -ProvisioningSchemeName xxxxx  [-VMName <
       String>] [-VMBatchSize XX] [-ResourceType XX]
   2 <!--NeedCopy-->
   ```

Los detalles de los parámetros son los siguientes:

- `ProvisioningSchemeUid` o `ProvisioningSchemeName` es un parámetro obligatorio.
- `VMName` es un parámetro opcional. Si no se especifica ningún `VMName`, se actualizan las etiquetas de todas las máquinas virtuales de este catálogo de máquinas.

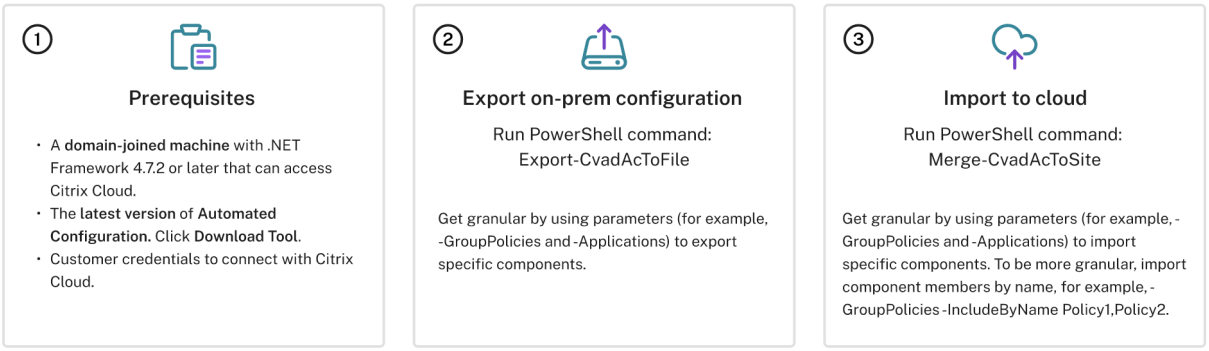
- `VMBatchSize` es un parámetro opcional para dividir todas las máquinas virtuales en lotes. Si no se especifica ningún `VMBatchSize`, se aplica el valor predeterminado (10). El rango es de 1 a 60.
- `ResourceType` puede ser uno de los siguientes:
  - `MachineCatalog`: Para actualizar las etiquetas de los recursos del catálogo de máquinas.
  - `VirtualMachine`: Para actualizar las etiquetas de los recursos relacionados con las máquinas virtuales.
  - `All`: (ResourceType predeterminado): para actualizar las etiquetas del catálogo de máquinas y de los recursos relacionados con las máquinas virtuales.

## Migrar configuraciones locales a la nube

May 17, 2024

La Configuración automatizada le permite automatizar el traslado de la configuración local a un sitio en la nube.

Esta imagen es una vista general de lo que puede hacer la Configuración automatizada para migrar su configuración a la nube.




### Requisitos previos para migrar una configuración

Para *exportar* su configuración desde Citrix Virtual Apps and Desktops, necesita:

- Versión Current Release de Citrix Virtual Apps and Desktops y su predecesora inmediata, o bien todas las versiones LTSR de Citrix Virtual Apps and Desktops y XenApp y XenDesktop
- Una máquina unida a un dominio con .NET Framework 4.7.2 o una versión posterior y el SDK de Citrix PowerShell. Se instala automáticamente en el Delivery Controller (para ejecutarse en

una máquina que no sea el Delivery Controller local, Citrix Studio debe estar instalado, ya que Studio instala los complementos correctos de PowerShell; el instalador de Studio se encuentra en los medios de instalación de Citrix Virtual Apps and Desktops).

Para *importar* su configuración en Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service), necesita:

- Una máquina con acceso a Citrix Cloud. No tiene por qué ser un Delivery Controller ni una máquina unida a un dominio.
- Citrix DaaS aprovisionado.
- Una ubicación de recursos activa con Connector instalado y unido al mismo dominio que la instalación local.
- La conectividad con los sitios que acceden a Citrix Cloud debe estar permitida y disponible. Para obtener más información, consulte Requisitos del sistema y de conectividad.

> **Nota:**
>
> La Configuración automatizada no se puede instalar en un sistema de Cloud Connector.

### Exportar la configuración local de Citrix Virtual Apps and Desktops

> **Importante:**
>
> - Debe tener su archivo CustomerInfo.yml con el ID del cliente, el ID de la máquina cliente y la información de la clave secreta. Para obtener más información sobre cómo obtener el ID del cliente, el ID de la máquina cliente y la clave secreta, consulte Generar el ID del cliente, el ID de la máquina cliente y la clave secreta. Para obtener información sobre cómo agregar esta información al archivo CustomerInfo.yml, consulte Rellenar el archivo de información del cliente.
> - El archivo ZoneMapping.yml debe incluir información que asigne la zona local a ubicaciones de recursos en la nube. Para obtener más información sobre cómo asignar las zonas, consulte Rellenar el archivo de asignación de zonas.
> - Si tiene conexiones de host, debe introducir la información correspondiente en el archivo CvadAcSecurity.yml.

1. Instalar la Configuración automatizada.
2. Haga doble clic en el icono de **configuración automática**. Aparece una ventana de PowerShell.
3. Ejecute el siguiente comando para exportar todos los componentes. La exportación de la configuración local *no* la modifica en modo alguno.

   ```
   Export-CvadAcToFile
   ```

Después de ejecutar un cmdlet por primera vez, se crea una carpeta de exportación con los registros y archivos de configuración YML. La carpeta se encuentra en *%HOMEPATH%\Documentos\Citrix\AutoConfig*. Con cada exportación sucesiva, se crea una subcarpeta. La carpeta principal *%HOMEPATH%\Documentos\Citrix\Aut* contiene siempre los archivos exportados de la exportación más reciente.

> **Nota:**
>
> Si la Configuración automatizada no está instalada en el Delivery Controller, ejecute `import -module Citrix.AutoConfig.Commands` antes de usar la herramienta a través de PowerShell. Este paso no es necesario si abre la Configuración automatizada mediante el icono de **configuración automática**.

Si ve algún error o excepción, consulte la sección **Fixups** del archivo de registros.

## Importación de la configuración en Citrix DaaS

> **Importante:**
>
> - Debe tener su archivo CustomerInfo.yml con el ID del cliente, el ID de la máquina cliente y la información de la clave secreta. Para obtener más información sobre cómo obtener el ID del cliente, el ID de la máquina cliente y la clave secreta, consulte Generar el ID del cliente, el ID de la máquina cliente y la clave secreta. Para obtener información sobre cómo agregar esta información al archivo CustomerInfo.yml, consulte Rellenar el archivo de información del cliente.
> - El archivo ZoneMapping.yml debe incluir información que asigne la zona local a ubicaciones de recursos en la nube. Para obtener más información sobre cómo asignar las zonas, consulte Rellenar el archivo de asignación de zonas.
> - Si tiene conexiones de host, debe introducir la información correspondiente en el archivo CvadAcSecurity.yml.
> - Al migrar una implementación local a la nube, asegúrese de que los objetos de directiva de grupo (GPO) de dominio y de unidades organizativas (OU) que contienen los parámetros de Citrix se migren a la nube. Citrix Web Studio no admite GPMC y, por lo tanto, los GPO de dominio y OU no son visibles en Web Studio. El motor de directivas de Citrix aplica los GPO de dominio y OU en los VDA y los usuarios que se encuentran en los dominios y las OU. Tras iniciar sesión en un VDA, un usuario puede ver que las directivas de los GPO de dominio y OU se aplican a su sesión. Sin embargo, los administradores no pueden ver estas directivas y parámetros, lo que puede generar confusión.

### Ejecutar una importación

1. Haga doble clic en el icono de **configuración automática**. Aparece una ventana de PowerShell.

2. Ejecute el siguiente comando para importar todos los componentes.

   ```
   Merge-CvadAcToSite
   ```

Verifique el estado esperado y compárelo con el nuevo estado actual. Diversas opciones de importación controlan si los resultados de la importación son idénticos o un subconjunto del sitio local.

Después de ejecutar el cmdlet, se crea una carpeta de exportación con los registros y archivos de configuración YML. La carpeta se encuentra en *%HOMEPATH%\Documentos\Citrix\AutoConfig*.

Si ve algún error o excepción, consulte la sección **Fixups** del archivo de registros.

> **Nota:**
>
> Si la Configuración automatizada no está instalada en el Delivery Controller, ejecute `import -module Citrix.AutoConfig.Commands` antes de usar la herramienta a través de PowerShell. Este paso no es necesario si abre la Configuración automatizada mediante el icono de **configuración automática**.

Para revertir a la configuración original de Citrix DaaS, consulte Copia de seguridad de la configuración de Citrix DaaS.

### Operación de importación en detalle

El proceso de importación está diseñado para realizar actualizaciones con precisión, realizar únicamente las actualizaciones necesarias y comprobar que todas las actualizaciones se han realizado correctamente. A continuación, se muestran los pasos seguidos en todas las operaciones de importación.

1. Lea el archivo YML exportado (estado esperado).
2. Lea la nube (estado actual).
3. Realice una copia de seguridad del estado de la nube previo a la importación en archivos YML (la copia de seguridad se puede restaurar si es necesario).
4. Evalúe las diferencias entre el estado esperado y el actual. Esto determina qué actualizaciones realizar.
5. Realice las actualizaciones.
6. Vuelva a leer la nube (nuevo estado actual).
7. Realice una copia de seguridad del estado de la nube posterior a la importación en archivos YML (la copia de seguridad se puede restaurar si es necesario).
8. Compare el nuevo estado actual con el estado esperado.
9. Informe de los resultados de la comparación.

### Migración granular

> **Importante:**
>
> Para obtener más información sobre el orden de la migración de los componentes, consulte Orden de la migración de los componentes.

Puede migrar componentes de forma selectiva únicamente o incluso solo nombres de componentes.

- Los parámetros de componentes admitidos incluyen `MachineCatalogs`, `Tags` y más.
- Los parámetros de nombre de componente admitidos incluyen los parámetros `IncludeByName` y `ExcludeByName`, entre otros.

Para obtener más información sobre los parámetros y cómo utilizarlos, consulte Parámetros de la migración granular.

### Activar sitios

La activación del sitio le permite controlar qué sitio está activo y controla sus recursos. Para obtener más información, consulte Activar sitios.

## Fusionar varios sitios en uno

March 30, 2024

La compatibilidad con varios sitios para la Configuración automatizada proporciona un método para fusionar varios sitios locales en un único sitio en la nube.

La compatibilidad con varios sitios agrega prefijos y sufijos únicos a los nombres de los componentes por sitio local, lo que garantiza la exclusividad de los nombres al fusionar varios sitios locales en un solo sitio en la nube.

Se pueden asignar prefijos y sufijos para cada uno de estos componentes por sitio local.

- `AdminScope`
- `AdminRole`
- `ApplicationAdmin`
- `ApplicationFolder`
- `ApplicationGroup`
- `ApplicationUser`
- `DeliveryGroup`

- GroupPolicy
- HostConnection
- MachineCatalog
- StoreFront
- Tag

Las carpetas de aplicaciones admiten prefijos, sufijos y cambio de raíz. El cambio de raíz agrega una carpeta de nivel superior adicional a la estructura de carpetas de una aplicación.

### Reglas de prefijos y sufijos

1. Los prefijos y sufijos no pueden contener ninguno de los siguientes caracteres especiales: `\ , / ; : # . * ? = < > | ( )"' { } [ ]`
2. Los prefijos y sufijos pueden contener espacios al final, pero no al principio.
3. Los prefijos y sufijos deben estar entre comillas dobles para contener espacios al final.
4. Los prefijos y sufijos se aplican en el momento de importar, fusionar y agregar. Los archivos YML de origen nunca se modifican.
5. El proceso de asignación de prefijos y sufijos agrega automáticamente estos a los nombres de los componentes dependientes cuando procede. Por ejemplo, si los nombres del catálogo de máquinas tienen el prefijo "East", los grupos de entrega que hacen referencia a ellos también tienen el prefijo "East".
6. Si un nombre de componente ya empieza por el prefijo o sufijo, no se agregará ningún prefijo o sufijo. Los nombres de componentes no pueden contener prefijos o sufijos dobles idénticos.
7. Los prefijos y sufijos se pueden usar individualmente o en combinación.
8. El uso de un prefijo o un sufijo en un componente es opcional.

> **Nota:**
>
> La interfaz de Configuración completa muestra los componentes en orden alfabético.

#### Agrupar por sitio

Utilice prefijos para agrupar visualmente componentes de un mismo sitio. Cada sitio se enumera en su propio grupo, con prefijo alfabético que controla el orden de los diferentes grupos del sitio.

#### Agrupar por nombre

Utilice sufijos para agrupar visualmente componentes con nombres similares de diferentes sitios. Los componentes con nombres similares de diferentes sitios se alternan visualmente.

#### Archivo SitePrefixes.yml

El prefijado de sitios comienza con el archivo SiteMerging.yml que contiene el prefijo del sitio y la asignación de sufijos para uno o varios sitios locales. Puede administrar el archivo SiteMerging.yml manualmente o con los cmdlets disponibles que se indican en la sección Cmdlets sobre la fusión de varios sitios locales.

#### Exportación, importación, fusión e incorporación

La fusión no puede comenzar hasta que haya exportado un sitio local. Para exportar un sitio local, consulte Migrar configuraciones locales a la nube.

#### Carpeta de destino de exportación central

Los métodos descritos en esta sección emplazan las exportaciones de varios sitios en una ubicación central de recursos compartidos. El archivo SiteMerging.yml, el archivo CustomerInfo.yml y todos los archivos de exportación residen en esa ubicación de recursos compartidos, lo que le permite realizar la importación desde una ubicación independiente de los sitios locales.

Las operaciones de acceso a la nube nunca hacen referencia a los sitios locales o a Active Directory, lo que le permite efectuar las operaciones de acceso a la nube desde cualquier lugar.

### Recursos compartidos directos

Las operaciones de exportación, importación, fusión y nuevo/adición proporcionan un parámetro para usar como origen o destino una carpeta distinta de la predeterminada *%HOMEPATH%\Documentos\Citrix\Auto*
En los siguientes ejemplos, se utiliza un recurso compartido central ubicado en `\\share.central.net`, al que el administrador tiene acceso tras proporcionar las credenciales necesarias.

Para destinar la exportación a una carpeta específica del sitio, utilice el parámetro `–TargetFolder`:

Desde el DDC East:

```
mkdir \\share.central.net\AutoConfig\SiteEast
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteEast
```

Desde el DDC West:

```
mkdir \\share.central.net\AutoConfig\SiteWest
```

```
Export-CvadAcToFile –TargetFolder \\share.central.net\AutoConfig\
SiteWest
```

Una vez completadas las exportaciones, cree los archivos CustomerInfo.yml y SiteMerging.yml y colóquelos en `\\share.central.net\AutoConfig`.

> **Nota:**
>
> No utilice el parámetro `SiteRootFolder` al crear el archivo SitePrefixes.yml cuando utilice este método de referencia para recursos compartidos directos.

Para importar, fusionar o agregar desde el recurso compartido directo, debe decidir desde qué máquina quiere efectuar la operación de acceso a la nube. Entre las opciones se incluyen:

- Uno de los DDC locales donde la herramienta ya está instalada.
- La máquina que aloja el recurso compartido.
- Una máquina diferente.

La Configuración automatizada debe estar instalada en la máquina con la que se accede a la nube. No se utilizan instancias de SDK de PowerShell, DDC ni Active Directory locales, por lo que los requisitos de ejecución para acceso a la nube son más simples que los requisitos de exportación.

Para fusionar el DDC East con la nube:

```
Merge-CvadAcToSite –SiteName East –SourceFolder \\share.central.
net\AutoConfig\SiteEast -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

Para fusionar el DDC West con la nube:

```
Merge-CvadAcToSite –SiteName West –SourceFolder \\share.central.
net\AutoConfig\SiteWest -CustomerInfoFileSpec \\share.central.net\
AutoConfig\CustomerInfo.yml
```

A continuación se muestra un archivo SitePrefixes.yml de muestra utilizado en el ejemplo anterior.

```
    East:
      SiteRootFolder: "" # Important: leave this empty
      AdminScopePrefix: "East_"
      AdminRolePrefix: "East_"
      ApplicationAdminPrefix: "East_"
      ApplicationFolderPrefix: "" # Note that a new parent root folder
          is used instead
      ApplicationFolderRoot: "East"
      ApplicationGroupPrefix: "East_"
      ApplicationUserPrefix: "East_"
      DeliveryGroupPrefix: "East_"
      GroupPolicyPrefix: "East_"
      HostConnectionPrefix: "East_"
      MachineCatalogPrefix: "East_"
```

```
      StoreFrontPrefix: "East_"
      TagPrefix: "East_"
      AdminScopeSuffix: "_east"
      AdminRoleSuffix: "_east"
      ApplicationAdminSuffix: "_east"
      ApplicationFolderSuffix: "_east"
      ApplicationGroupSuffix: "_east"
      ApplicationUserSuffix: "_east"
      DeliveryGroupSuffix: "_east"
      GroupPolicySuffix: "_east"
      HostConnectionSuffix: "_east"
      MachineCatalogSuffix: "_east"
      StoreFrontSuffix: "_east"
      TagSuffix: "_east"
    West:
      SiteRootFolder: "" # Important: leave this empty
      AdminScopePrefix: "Western "
      AdminRolePrefix: "Western "
      ApplicationAdminPrefix: "Western "
      ApplicationFolderPrefix: "" # Note that a new parent root folder
          is used instead
      ApplicationFolderRoot: "Western"
      ApplicationGroupPrefix: "Western "
      ApplicationUserPrefix: "Western "
      DeliveryGroupPrefix: "Western "
      GroupPolicyPrefix: "Western "
      HostConnectionPrefix: "Western "
      MachineCatalogPrefix: "Western "
      StoreFrontPrefix: "Western "
      TagPrefix: "Western "
      AdminScopeSuffix: ""
      AdminRoleSuffix: ""
      ApplicationAdminSuffix: ""
      ApplicationFolderSuffix: ""
      ApplicationGroupSuffix: ""
      ApplicationUserSuffix: ""
      DeliveryGroupSuffix: ""
      GroupPolicySuffix: ""
      HostConnectionSuffix: ""
      MachineCatalogSuffix: ""
      StoreFrontSuffix: ""
      TagSuffix: ""
```

### Referencia de recurso compartido con SiteMerging.yml

Este método utiliza el miembro `SiteRootFolder` del conjunto de prefijos del sitio. Aunque más involucrado que el método de recurso compartido directo, este método reduce las probabilidades de apuntar a una carpeta incorrecta al exportar, importar, fusionar o agregar.

En primer lugar, establezca `SiteRootFolder` para cada sitio en el archivo SiteMerging.yml. Debe hacer esto en la ubicación compartida.

```
New-CvadAcSiteMergingInfo –SiteName East –SiteRootFolder \\share.
central.net\AutoConfig\SiteEast -SitePrefixesFolder \\share.central.
net\AutoConfig

New-CvadAcSiteMergingInfo –SiteName West –SiteRootFolder SiteWest -
SitePrefixesFolder \\share.central.net\AutoConfig
```

En este ejemplo, "East"es una especificación de carpeta completa y "West"es una especificación de carpeta relativa.

Para dirigir la exportación a una carpeta específica del sitio mediante el archivo SiteMerging.yml:

Desde el DDC East:

```
mkdir \\share.central.net\AutoConfig\SiteEast

Export-CvadAcToFile -SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Desde el DDC West:

```
mkdir \\share.central.net\AutoConfig\SiteWest

Export-CvadAcToFile -SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

El cmdlet de exportación utiliza la ubicación de la carpeta CustomerInfo.yml para localizar el archivo SiteMerging.yml. En el caso de "East", `SiteRootFolder` es una referencia completa. Se usa tal cual. En el caso de West, `SiteRootFolder` no es una referencia completa. Se combina con la ubicación de la carpeta CustomerInfo.yml para obtener una ubicación de carpeta completa para "West".

Para fusionar el DDC East con la nube:

```
Merge-CvadAcToSite –SiteName East -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

Para fusionar el DDC West con la nube:

```
Merge-CvadAcToSite –SiteName West -CustomerInfoFileSpec \\share.
central.net\AutoConfig\CustomerInfo.yml
```

A continuación se muestra un archivo SitePrefixes.yml de muestra utilizado en el ejemplo anterior.

```
1       East:
2       SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteEast"
3       AdminScopePrefix: "East_"
4       AdminRolePrefix: "East_"
5       ApplicationAdminPrefix: "East_"
6       ApplicationFolderPrefix: "" # Note that a new parent root folder
           is used instead
7       ApplicationFolderRoot: "East"
8       ApplicationGroupPrefix: "East_"
```

```
      ApplicationUserPrefix: "East_"
      DeliveryGroupPrefix: "East_"
      GroupPolicyPrefix: "East_"
      HostConnectionPrefix: "East_"
      MachineCatalogPrefix: "East_"
      StoreFrontPrefix: "East_"
      TagPrefix: "East_"
      AdminScopeSuffix: "_east"
      AdminRoleSuffix: "_east"
      ApplicationAdminSuffix: "_east"
      ApplicationFolderSuffix: "_east"
      ApplicationGroupSuffix: "_east"
      ApplicationUserSuffix: "_east"
      DeliveryGroupSuffix: "_east"
      GroupPolicySuffix: "_east"
      HostConnectionSuffix: "_east"
      MachineCatalogSuffix: "_east"
      StoreFrontSuffix: "_east"
      TagSuffix: "_east"
    West:
      SiteRootFolder: "\\\\share.central.net\\AutoConfig\\SiteWest"
      AdminScopePrefix: "Western "
      AdminRolePrefix: "Western "
      ApplicationAdminPrefix: "Western "
      ApplicationFolderPrefix: "" # Note that a new parent root folder
          is used instead
      ApplicationFolderRoot: "Western"
      ApplicationGroupPrefix: "Western "
      ApplicationUserPrefix: "Western "
      DeliveryGroupPrefix: "Western "
      GroupPolicyPrefix: "Western "
      HostConnectionPrefix: "Western "
      MachineCatalogPrefix: "Western "
      StoreFrontPrefix: "Western "
      TagPrefix: "Western "
      AdminScopeSuffix: ""
      AdminRoleSuffix: ""
      ApplicationAdminSuffix: ""
      ApplicationFolderSuffix: ""
      ApplicationGroupSuffix: ""
      ApplicationUserSuffix: ""
      DeliveryGroupSuffix: ""
      GroupPolicySuffix: ""
      HostConnectionSuffix: ""
      MachineCatalogSuffix: ""
      StoreFrontSuffix: ""
      TagSuffix: ""
```

Si no se utiliza un método de recurso compartido central y la importación, fusión o adición se realiza desde los DDC individuales, cree y replique el archivo SiteMerging.yml en cada DDC que se migre a la nube. La ubicación predeterminada es *%HOMEPATH%\Documentos\Citrix\AutoConfig*. Debe especificar el parámetro `–SiteName` para seleccionar los prefijos de sitio correctos.

### Fusionar los sitios

Citrix recomienda realizar las operaciones en la nube por pasos y hacer una revisión completa de cada resultado antes de pasar a la siguiente operación en la nube. Por ejemplo, si se fusionan tres sitios en un único sitio en la nube:

1. Para fusionar el sitio inicial en la nube, use el valor `SiteName` apropiado.
2. Revise los resultados en la interfaz de administración de Configuración completa.
3. Si los resultados no son correctos, determine el problema y su causa, corríjalo y vuelva a ejecutar la fusión. Si es necesario, quite los componentes de la nube y comience desde cero; para ello, use `Remove-CvadAcFromSite` para el componente y los miembros seleccionados. Si los resultados son correctos, continúe.
4. Si la fusión inicial es correcta, fusiones el segundo sitio con el sitio único en la nube.
5. Repita los pasos 2 y 3.
6. Si la segunda fusión es correcta, fusione el tercer sitio con el sitio único en la nube.
7. Repita los pasos 2 y 3.
8. Revise los recursos desde la perspectiva del usuario y compruebe que la vista se encuentra en el estado deseado.

#### Quitar un componente con el prefijo del sitio

Para quitar de forma selectiva componentes de un solo sitio, use el prefijo en el parámetro `–IncludeByName` del cmdlet `Remove-CvadAcFromSite`. En el ejemplo siguiente, los grupos de entrega de DDC West no son correctos. Para quitar los grupos de entrega solo del sitio West:

```
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
```

Para quitar todos los componentes de West, ejecute los siguientes cmdlets en orden.

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “Western *”
Remove-CvadAcFromSite –Applications –IncludeByName “Western *”
Remove-CvadAcFromSite – ApplicationGroups –IncludeByName “Western *”
Remove-CvadAcFromSite –DeliveryGroups –IncludeByName “Western *”
Remove-CvadAcFromSite –MachineCatalogs –IncludeByName “Western *”
Remove-CvadAcFromSite –HostConnections –IncludeByName “Western *”
Remove-CvadAcFromSite –Tags –IncludeByName “Western *”
```

Para quitar directivas de grupo de los componentes de East, utilice el sufijo:

```
Remove-CvadAcFromSite –GroupPolicies –IncludeByName “*_east”
```

# Migrar de la nube a la nube

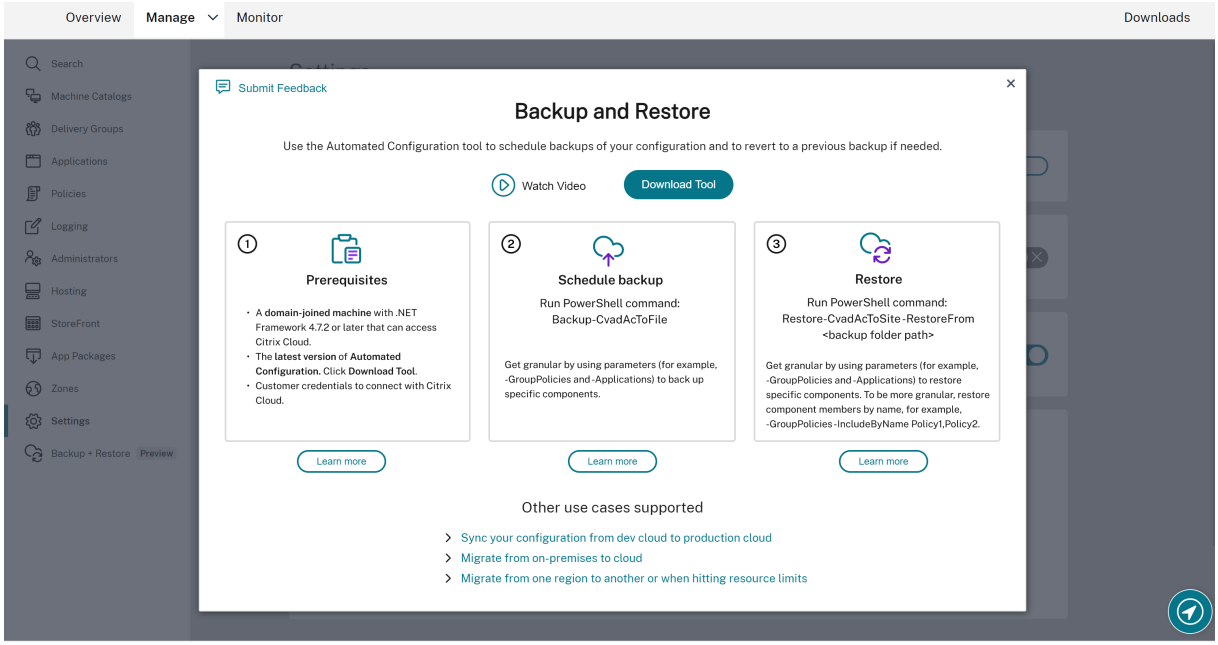
April 18, 2024

La Configuración automatizada le permite automatizar el traslado de su configuración de la nube a otro sitio en la nube o le permite restaurar su propio sitio en la nube.

El uso de la Configuración automatizada puede resolver muchos casos de uso:

- Sincronización de su sitio desde la prueba o etapa a la producción
- Copia de seguridad y restauración de la configuración
- Límites de recursos alcanzados
- Migrar de una región a otra

En Configuración completa, en Citrix Cloud, consulte el nodo Copia de seguridad y restauración para obtener información sobre la Configuración automatizada y cómo se puede utilizar para migrar su configuración de nube a nube.




## Requisitos previos para migrar una configuración

Para realizar copias de seguridad y restaurar la configuración, necesita:

- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) aprovisionado.
- Un ubicación de recursos activa con Connector instalado.
- La conectividad con los sitios que acceden a Citrix Cloud debe estar permitida y disponible. Para obtener más información, consulte Requisitos del sistema y de conectividad.

> **Nota:**
>
> No se puede realizar una copia de seguridad de MCS desde la nube mediante la Configuración automatizada.

### Copia de seguridad de la configuración de Citrix DaaS

> **Importante:**
>
> - Debe tener su archivo CustomerInfo.yml con el ID del cliente, el ID de la máquina cliente y la información de la clave secreta. Para obtener más información sobre cómo obtener el ID del cliente, el ID de la máquina cliente y la clave secreta, consulte Generar el ID del cliente, el ID de la máquina cliente y la clave secreta. Para obtener información sobre cómo agregar esta información al archivo CustomerInfo.yml, consulte Rellenar el archivo de información del cliente.
> - Al ejecutar los comandos de copia de seguridad, CustomerInfo.yml debe contener los detalles del cliente del sitio de origen desde el que está realizando la copia de seguridad.
> - Al ejecutar los comandos de restauración, CustomerInfo.yml debe contener los detalles del cliente del sitio de destino en el que va a restaurar las configuraciones.
> - El archivo ZoneMapping.yml debe incluir información que asigne sus ubicaciones de recursos en la nube. Para obtener más información sobre cómo asignar las zonas, consulte Rellenar el archivo de asignación de zonas.
> - Si tiene conexiones de host, debe introducir la información correspondiente en el archivo CvadAcSecurity.yml.

1. Instalar la Configuración automatizada.

   > **Nota:**
   >
   > Para la migración de nube a nube, la Configuración automatizada se puede instalar en una máquina que tenga acceso a Internet y a la que el administrador tenga acceso directo.

2. Haga doble clic en el icono de **configuración automática**. Aparece una ventana de PowerShell.
3. Ejecute el siguiente comando para realizar una copia de seguridad.

   ```
   Backup-CvadAcToFile
   ```

Después de ejecutar un cmdlet por primera vez, se crea una carpeta de exportación con los registros y archivos de configuración YML. La carpeta se encuentra en *%HOMEPATH%\Documentos\Citrix\AutoConfig*.

Si ve algún error o excepción, consulte la sección **Fixups** del archivo de registros.

### Restauración de la configuración en Citrix DaaS

1. Haga doble clic en el icono de **configuración automática**. Aparece una ventana de PowerShell.
2. Ejecute el siguiente comando para realizar una restauración.

   ```
   Restore-CvadAcToSite -RestoreFolder <folder path of the backup files>
   ```

Verifique el estado esperado y compárelo con el nuevo estado actual.

Después de ejecutar el cmdlet, se crea una carpeta de exportación con los registros y archivos de configuración YML. La carpeta se encuentra en *%HOMEPATH%\Documentos\Citrix\AutoConfig*.

Si ve algún error o excepción, consulte la sección **Fixups** del archivo de registros.

El proceso de copia de seguridad y restauración le protege de cambios o daños no intencionados en la configuración del sitio en la nube. Mientras que la Configuración automatizada realiza copias de seguridad cada vez que se realiza un cambio, esta copia de seguridad refleja el estado de la configuración del sitio en la nube antes de los cambios. Para protegerse, debe realizar periódicamente una copia de seguridad de la configuración del sitio en la nube y guardarla en un lugar seguro. Si se produce un cambio no deseado o daños, la copia de seguridad se puede utilizar para corregirlos en un nivel de configuración del sitio completo o granular.

### Migración granular

> **Importante:**
>
> Para obtener más información sobre el orden de la migración de los componentes, consulte Orden de la migración de los componentes.

#### Restauración de componentes enteros

La restauración de un componente implica la selección de uno o más parámetros de componente.

Para restaurar todos los componentes del grupo de entrega y el catálogos de máquinas, siga este ejemplo:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

#### Restauración de miembros de componentes

La restauración de uno o más miembros de componentes se realiza mediante la función `IncludeByName`. El cmdlet `Restore` se invoca con el parámetro `RestoreFolder` junto con el componente único seleccionado y la lista de inclusión.

Para restaurar dos directivas de grupo a partir de una copia de seguridad, siga este ejemplo:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
-GroupPolicies -IncludeByName Policy1,Policy2
-DeliveryGroups -MachineCatalogs
```

#### Restaurar toda la configuración del sitio en la nube

Restaurar la configuración completa del sitio en la nube significa seleccionar todos los componentes para restaurar.

Para restaurar toda la configuración del sitio en la nube, siga este ejemplo:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

### Activar sitios

La activación del sitio le permite controlar qué sitio está activo y controla sus recursos. Para obtener más información, consulte Activar sitios.

## Cmdlets de la herramienta de Configuración automatizada

March 30, 2024

En esta página se enumeran todos los cmdlets y parámetros que ofrece la herramienta.

Todos los cmdlets toman parámetros que tienen uno de estos tipos.

- Cadena
- Lista de cadenas
- Booleano: `$true` o `$false`
- SwitchParameter: La presencia del parámetro significa `$true`; la ausencia del parámetro significa `$false`

> **Nota:**
>
> SwitchParameter es el método preferido para las selecciones de true o false, pero los booleanos se siguen utilizando en la herramienta por problemas antiguos.

Esta tabla es un resumen de todos los cmdlets. Consulte cada sección para averiguar qué parámetros admite cada cmdlet.

| Categoría | Cmdlet | Descripción |
| --- | --- | --- |
| Migración de configuraciones locales a la nube | `Export-CvadAcToFile` | Exporta archivos locales a archivos YAML.<br>`Import-CvadAcToSite`<br>`Merge-CvadAcToSite`<br>`New-CvadAcToSite`<br>`Sync-CvadAcToSite`<br>*Migración granular*: Para los componentes, utilice los parámetros con los comandos anteriores. Ejemplos: `MachineCatalogs`, `Tags` Para los nombres de componentes, utilice los parámetros con los comandos anteriores. Ejemplos: `IncludeByName`, `ExcludeByName` |
| Cmdlets de nube a nube | `Backup-CvadAcToFile` | Realiza una copia de seguridad de toda la configuración de su sitio de la nube.<br>`Restore-CvadAcToSite`<br>`Remove-CvadAcFromSite` |

| Categoría | Cmdlet | Descripción |
| --- | --- | --- |
| | | *Migración granular*: Para los componentes, utilice los parámetros con los comandos anteriores. Ejemplos: `MachineCatalogs`, `Tags` Para los nombres de componentes, utilice los parámetros con los comandos anteriores. Ejemplos: `IncludeByName`, `ExcludeByName` |
| Otros cmdlets básicos | `Compare-CvadAcToSite` | Compara los archivos YML locales con la configuración de la nube. |
| Cmdlets relacionados con requisitos previos | `New-CvadAcCustomerInfoFile` | Cree un archivo de información del cliente. |
| | `Set-CvadAcCustomerInfoFile` | |
| Asistencia y solución de problemas con cmdlets | `New-CvadAcZipInfoForSupport` | Comprime todos los archivos de registro e YML en un único archivo ZIP para enviarlos a Citrix para asistencia técnica. |
| | `Get-CvadAcStatus` | |
| | `Test-CvadAcConnectionWithSite` | |
| | `Find-CvadAcConnector` | |
| | `Get-CvadAcCustomerSites` | |
| | `New-CvadAcTemplateToFile` | |
| | `Show-CvadAcDocument` | |
| | `Find-CvadAcInFile` | |

| Categoría | Cmdlet | Descripción |
| --- | --- | --- |
| Cmdlets de activación del sitio | `Set-CvadAcSiteActiveStateOnPrem` | Establece el estado del sitio local en activo o inactivo. |
| | | `Set-CvadAcSiteActiveStateCloud` |
| Cmdlets sobre la fusión de varios sitios locales | `New-CvadAcSiteMergingInfo` | Crea un conjunto de información de prefijos/sufijos para fusión de sitios. |
| | | `Set-CvadAcSiteMergingInfo` |
| | | `Remove-CvadAcSiteMergingInfo` |

Para obtener más información sobre los parámetros y cómo utilizarlos, consulte Parámetros de la migración granular.

## Cmdlets básicos

### Cmdlets de configuraciones locales a la nube

- `Export-CvadAcToFile`: Exporta archivos locales a archivos YAML.

  Exporta la configuración desde su instalación local. Esta es la operación predeterminada de exportación de la Configuración automatizada. No se realizan modificaciones en la configuración del sitio local. Los archivos exportados se colocan en el directorio *%HOMEPATH%\Documents\Citrix\AutoConfig* en una subcarpeta con el nombre exclusivo **Export**. La carpeta *%HOMEPATH%\Documentos\Citrix\AutoConfig* siempre contiene la configuración del sitio local exportada más reciente.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
| --- | --- | --- | --- |
| Migración por componentes | Consulte Migración por componentes | | SwitchParameters |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto | | Lista de cadenas |
| `TargetFolder` | Especifica la carpeta de destino de la exportación. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `AdminAddress` | Especifica la dirección IP o DNS del Delivery Controller cuando la exportación no se ejecuta en el Delivery Controller. | | Cadena |
| `CheckUserAndMachines` | Comprueba si los usuarios y las máquinas están presentes en Active Directory. Los usuarios y las máquinas que no están en Active Directory pueden dar lugar a errores de importación. | | `$true` o `$false` |
| `ZipResults` | Comprime las copias de seguridad de los archivos YAML en un único archivo ZIP. El archivo se encuentra en la misma carpeta que las copias de seguridad de los archivos YAML y tiene el mismo nombre que la carpeta. | | SwitchParameter |

Devuelve:

- Consulte Valores devueltos de cmdlet

Existen tres formas de importar datos a la nube. La ejecución de cmdlets específicos puede dar lugar a una de las tres combinaciones de acciones del sitio de la nube:

- Add, Update y Delete
- Add y Update solamente
- Add solamente

| Cmdlet | Add | Actualización | Eliminar |
|---|---|---|---|
| Import | X | X | X |
| Merge | X | X | |
| New | X | | |

- `Import-CvadAcToSite`: Importa archivos YAML a la nube. Permite operaciones de creación, actualización y eliminación.

  Importa todos los archivos locales en la nube. Este comando garantiza que el estado final de la nube sea idéntico al estado local. Esta opción elimina los cambios que existan en la nube. Los archivos de configuración de sitios importados proceden de *%HOMEPATH%\Documents\Citrix\AutoConfig*. *Úsela con cuidado.*

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes. | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto. | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube. | | SwitchParameters |
| `SourceFolder` | Identifica una carpeta raíz alternativa para *%HOMEPATH%\Documentos\Citrix\AutoConfig*. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `Merge` | Cuando se establece en `$true`, solo agrega componentes al sitio de la nube. Los componentes no se quitan. Establézcalo en `$false` para quitar componentes. | | `$true` o `$false` |
| `AddOnly` | Cuando se establece en `$true`, solo agrega componentes nuevos y no actualiza ni elimina componentes existentes. Establézcalo en `$false` para permitir actualizaciones y eliminaciones. `Merge` se ignora cuando este parámetro tiene el valor `$true`. | | `$true` o `$false` |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `MergePolicies` | Fusiona parámetros de directivas y filtros. La fusión se produce solamente cuando una directiva que se está importando ya existe en el DDC de la nube. El resultado de la fusión de directivas es que las directivas de DDC de la nube contienen los parámetros y los filtros que ya tenía, así como los parámetros y filtros nuevos que se importen. Tenga en cuenta que, cuando se producen colisiones entre parámetros y filtros, los valores importados son prioritarios. | | SwitchParameter |
| `OnErrorAction` | Consulte Parámetro OnErrorAction. | | Cadena |

Devuelve:

- Consulte Valores devueltos de cmdlet

- `Merge-CvadAcToSite`: Importa archivos YAML a la nube. Permite operaciones de creación y actualización.

  Fusiona los archivos locales en la nube, pero *no* elimina ningún componente de la nube ni del sitio local. Esto preserva los cambios ya realizados en la nube. Si existe un componente en Citrix Cloud con el mismo nombre, este comando puede modificarlo. Esta es la operación predeterminada de importación de la Configuración automatizada. Los archivos de configuración de sitios combinados proceden de *%HOMEPATH%\Documents\Citrix\AutoConfig*.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes. | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto. | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube. | | SwitchParameters |
| `SourceFolder` | Identifica una carpeta raíz alternativa para *%HOMEPATH%\Documentos\Citrix\AutoConfig*. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `Merge` | Cuando se establece en `$true`, solo agrega componentes al sitio de la nube. Los componentes no se quitan. Establézcalo en `$false` para quitar componentes. | | `$true` o `$false` |
| `AddOnly` | Cuando se establece en `$true`, solo agrega componentes nuevos y no actualiza ni elimina componentes existentes. Establézcalo en `$false` para permitir actualizaciones y eliminaciones. `Merge` se ignora cuando este parámetro tiene el valor `$true`. | | `$true` o `$false` |
| `MergePolicies` | Fusiona parámetros de directivas y filtros. La fusión se produce solamente cuando una directiva que se está importando ya existe en el DDC de la nube. El resultado de la fusión de directivas es que las directivas de DDC de la nube contienen los parámetros y los filtros que ya tenía, así como los parámetros y filtros nuevos que se importen. Tenga en cuenta que, cuando se producen colisiones entre parámetros y filtros, los valores importados son prioritarios. | | SwitchParameter |
| `OnErrorAction` | Consulte Parámetro OnErrorAction. | | Cadena |

Devuelve:

- Consulte Valores devueltos de cmdlet

- `New-CvadAcToSite`: Importa archivos YAML a la nube. Permite operaciones de creación y actualización.

  Importa la configuración de un sitio local en la nube, pero solo agrega nuevos componentes. Los componentes existentes del sitio en la nube no se actualizan ni se eliminan. Utilice este comando si los componentes existentes del sitio en la nube deben permanecer sin cambios.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes. | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto. | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube. | | SwitchParameters |
| `SourceFolder` | Identifica una carpeta raíz alternativa para *%HOMEPATH%\Documentos\Citrix\AutoConfig*. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `OnErrorAction` | Consulte Parámetro OnErrorAction. | | Cadena |

Devuelve:

- Consulte Valores devueltos de cmdlet

- `Sync-CvadAcToSite`: Exporta e importa archivos en un solo paso.

  Sync realiza tanto una exportación como una importación en un solo paso. Utilice el parámetro `SourceTargetFolder` para especificar la carpeta de destino de exportación/importación.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |
| `SourceTargetFolder` | Especifica la carpeta de destino de exportación/importación. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `AdminAddress` | Especifica la dirección IP o el DNS del Delivery Controller cuando la exportación no se ejecuta en el Delivery Controller. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `Merge` | Cuando se establece en `$true`, solo agrega componentes al sitio de la nube. Los componentes no se quitan. Establézcalo en `$false` para quitar componentes. | | `$true` o `$false` |
| `AddOnly` | Cuando se establece en `$true`, solo agrega componentes nuevos y no actualiza ni elimina componentes existentes. Establézcalo en `$false` para permitir actualizaciones y eliminaciones. `Merge` se ignora cuando este parámetro tiene el valor `$true`. | | `$true` o `$false` |
| `MergePolicies` | Fusiona parámetros de directivas y filtros. La fusión se produce solamente cuando una directiva que se está importando ya existe en el DDC de la nube. El resultado de la fusión de directivas es que las directivas de DDC de la nube contienen los parámetros y los filtros que ya tenía, así como los parámetros y filtros nuevos que se importen. Tenga en cuenta que, cuando se producen colisiones entre parámetros y filtros, los valores importados son prioritarios. | | SwitchParameter |

Devuelve:

- Consulte Valores devueltos de cmdlet

**Cmdlets de nube a nube**

- `Backup-CvadAcToFile`: Realiza una copia de seguridad de toda la configuración de su sitio de la nube.

Exporta la configuración de la nube en archivos YML. Esta copia de seguridad se puede utilizar en un proceso de copia de seguridad y restauración para restaurar componentes perdidos.

Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes | | SwitchParameters |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |
| `TargetFolder` | Especifica la carpeta de destino de la exportación. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `ZipResults` | Comprime las copias de seguridad de los archivos YAML en un único archivo ZIP. El archivo se encuentra en la misma carpeta que las copias de seguridad de los archivos YAML y tiene el mismo nombre que la carpeta. | | SwitchParameter |

Devuelve:

- Consulte Valores devueltos de cmdlet

- `Restore-CvadAcToSite`: Restaura copias de seguridad de archivos YAML en el sitio de la nube. Este sitio de la nube puede ser el mismo o uno distinto del sitio de la nube de origen.

  Restaura el sitio en la nube a la configuración anterior. Los archivos importados se obtienen de la carpeta especificada mediante el parámetro `-RestoreFolder`, que identifica la carpeta que contiene los archivos YML que restaurar en el sitio de la nube. Debe ser una especificación de carpeta completa. Este cmdlet se puede utilizar para volver a la configuración anterior o para hacer copias de seguridad y restaurar su sitio en la nube. Este comando puede agregar, eliminar y actualizar su sitio de la nube.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes. | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto. | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube. | | SwitchParameters |
| `RestoreFolder` | Identifica la carpeta que contiene los archivos YML que se va a restaurar en el sitio en la nube. Debe ser una especificación de carpeta completa. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `Merge` | Cuando se establece en `$true`, solo agrega componentes al sitio de la nube. Los componentes no se quitan. Establézcalo en `$false` para quitar componentes. | | `$true` o `$false` |
| `AddOnly` | Cuando se establece en `$true`, solo agrega componentes nuevos y no actualiza ni elimina componentes existentes. Establézcalo en `$false` para permitir actualizaciones y eliminaciones. `Merge` se ignora cuando este parámetro tiene el valor `$true`. | | `$true` o `$false` |
| `MergePolicies` | Fusiona parámetros de directivas y filtros. La fusión se produce solamente cuando una directiva que se está importando ya existe en el DDC de la nube. El resultado de la fusión de directivas es que las directivas de DDC de la nube contienen los parámetros y los filtros que ya tenía, así como los parámetros y filtros nuevos que se importen. Tenga en cuenta que, cuando se producen colisiones entre parámetros y filtros, los valores importados son prioritarios. | | SwitchParameter |
| `OnErrorAction` | Consulte Parámetro OnErrorAction. | | Cadena |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|

Devuelve:

- Consulte Valores devueltos de cmdlet

- `Remove-CvadAcFromSite`: Quita miembros de componentes de la nube.

  Puede restablecer todo el sitio o quitar elementos que haya en un componente (por ejemplo, quitar un catálogo de máquinas de la lista de catálogos). Esto se puede usar cuando se combina con el parámetro `IncludeByName` para quitar miembros específicos.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |

Devuelve:

- Consulte Valores devueltos de cmdlet

**Otros cmdlets básicos**

- `Compare-CvadAcToSite`: Compara los archivos YML locales con la configuración de la nube y produce un informe de los cambios realizados por un cmdlet `Import`, `Merge` o `Restore`.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes. | | SwitchParameters |
| Filtrado por nombres de objeto | Consulte Filtrado por nombres de objeto. | | Lista de cadenas |
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube. | | SwitchParameters |
| `SourceFolder` | Identifica una carpeta raíz alternativa para *%HOMEPATH%\Documentos\Citrix\AutoConfig*. | | Cadena |
| `Locale` | Especifica el idioma del texto en formato legible para las personas que se puede exportar. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true` o `$false` |
| `Merge` | Cuando se establece en `$true`, solo agrega componentes al sitio de la nube. Los componentes no se quitan. Establézcalo en `$false` para quitar componentes. | | `$true` o `$false` |
| `AddOnly` | Cuando se establece en `$true`, solo agrega componentes nuevos y no actualiza ni elimina componentes existentes. Establézcalo en `$false` para permitir actualizaciones y eliminaciones. `Merge` se ignora cuando este parámetro tiene el valor `$true`. | | `$true` o `$false` |
| `OnErrorAction` | Consulte Parámetro OnErrorAction. | | Cadena |

Devuelve:

- Consulte Valores devueltos de cmdlet

## Parámetros de migración granular

### Migración por componentes

Los siguientes componentes se pueden especificar con cmdlets que los admitan. La opción `All` se selecciona automáticamente cuando no se especifica ningún parámetro de componente. Para evitar errores, le recomendamos migrar los componentes en este orden:

- `All`
- `Tags`
- `AdminRoles`
- `AdminScopes`
- `HostConnections`
- `MachineCatalogs`
- `StoreFronts`
- `DeliveryGroups`
- `ApplicationGroups`
- `ApplicationFolders`
- `Applications`
- `GroupPolicies`
- `UserZonePreference`

#### Filtrado por nombres de objeto

**Migración por nombres de componentes** Los parámetros `IncludeByName` y `ExcludeByName` permiten incluir y excluir por nombre miembros de componentes en cmdlets. Solo se puede elegir un componente (por ejemplo, grupos de entrega) en un momento dado en cualquiera de los cmdlets compatibles. Si un miembro de un componente se halla en las dos zonas, la exclusión supedita cualquier otro parámetro, y se crea una entrada en la lista Fixups del registro que identifica el componente y el nombre del miembro excluidos.

`IncludeByName` y `ExcludeByName` toman una lista de nombres de miembros de componentes. Los nombres pueden contener comodines. Se admiten dos tipos de comodines. La lista de nombres de miembros de componentes debe estar entre comillas simples si alguno de esos nombres contiene caracteres especiales.

- * coincide con cualquier cantidad de caracteres
- ? coincide con un solo carácter

`IncludeByName` y `ExcludeByName` también pueden tomar un archivo que contenga una lista de miembros, donde cada miembro puede ser explícito o contener comodines. Cada línea del archivo puede contener un miembro. Los espacios del principio y del final se recortan del nombre del miembro. El nombre del archivo debe ir precedido por el signo @ y estar rodeado por comillas simples (un requisito de PowerShell para que no se reinterprete @). Se pueden enumerar varios archivos, además de mezclarse con nombres de miembros.

Un ejemplo de fusión de todos los grupos de entrega cuyos nombres comiencen por `DgSite1` y contengan `Home2` se escribiría así:

```
Merge-CvadAcToSite –DeliveryGroups –IncludeByName DgSite1*,*Home2*
```

**Por nombre de grupo de entrega** `ByDeliveryGroupName` filtra por el nombre del grupo de entrega para aplicaciones y grupos de aplicaciones. Este parámetro es siempre una lista de inclusión que identifica a los miembros que se incluirán en función de su asociación de grupos de entrega.

`ByDeliveryGroupName` toma una lista de nombres de grupos de entrega. Los nombres pueden contener comodines. Se admiten dos tipos de comodines.

- * coincide con cualquier cantidad de caracteres
- ? coincide con un solo carácter

En el ejemplo siguiente se combinan todas las aplicaciones que hacen referencia a todos los nombres de grupos de entrega que empiezan por `EastDg`.

```
Merge-CvadAcToSite –Applications –ByDeliveryGroupName EastDg*
```

**Excluir inhabilitado** `ExcludeDisabled` filtra de las operaciones de importación todas las aplicaciones y grupos de aplicaciones que están inhabilitados. `ExcludeDisabled` tiene como valor predeterminado **`false`**, lo que significa que se importan todas las aplicaciones y grupos de aplicaciones independientemente de su estado habilitado.

**Por nombre de máquina** `ByMachineName` filtra catálogos de máquinas y grupos de entrega por nombre de máquina. Este parámetro es siempre una lista de inclusión que identifica a los miembros que se incluirán en función de su asociación de nombre de máquina.

`ByMachineName` toma una lista de nombres de máquina donde cualquier nombre puede contener uno o más comodines. Se admiten dos tipos de comodines.

- * coincide con cualquier cantidad de caracteres
- ? coincide con un solo carácter

Si al exportar o importar y utilizar `ByMachineName` y un filtro de nombre de máquina no da como resultado ninguna máquina en el catálogo de máquinas o grupo de entrega, el catálogo de máquinas o grupo de entrega se excluyen de la exportación o importación.

> **Nota:**
>
> Al usar `ByMachineName` en cualquier cmdlet de tipo "importación", `MergeMachines` se establece en `$true`.

**Fusionar máquinas** Cuando `MergeMachines` se establece en `$true`, indica a la operación de importación que agregue máquinas solo al catálogo de máquinas o al grupo de entrega. Las máquinas no se quitan, lo que posibilita las operaciones aditivas incrementales.

El valor predeterminado de `MergeMachines` es "false", lo que significa que las máquinas se quitan si no están presentes en el archivo YML del catálogo de máquinas o el grupo de entrega. Cuando se usa `ByMachineName`, `MergeMachines` se establece en `$true`, pero se puede anular estableciendo `MergeMachines` en "false".

### Cmdlets relacionados con requisitos previos

- `New-CvadAcCustomerInfoFile`: Cree un archivo de información del cliente. De forma predeterminada, el archivo de información del cliente se encuentra en *%HOMEPATH%\Documentos\Citrix\AutoConfig*.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `CustomerId` | ID del cliente. | x | Cadena |
| `ClientId` | ID de la máquina cliente creado en Citrix Cloud. Deben especificarse los campos CustomerId y Secret al utilizar este parámetro. | Con condiciones | Cadena |
| `Secret` | Clave secreta del cliente creada en Citrix Cloud. Deben especificarse los campos CustomerId y ClientId al utilizar este parámetro. | Con condiciones | Cadena |
| `Environment` | Entorno Production, ProductionGov o ProductionJP. | | Enumeración |
| `LogFileName` | Cambie el prefijo del archivo de registros de CitrixLog a otra cosa. | | Cadena |
| `AltRootUrl` | Utilícelo solo si se lo indica Citrix. | | Cadena |
| `StopOnError` | Detiene la operación tras el primer error. | | `$true` o `$false` |
| `TargetFolder` | Utilice la carpeta especificada como carpeta raíz en lugar de *%HOMEPATH%\Documentos\Citrix\AutoConfig*. | | Cadena |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `Locale` | Utilice la configuración regional especificada, en lugar de la configuración regional del sistema en el que se ejecuta la herramienta. | | Cadena |
| `Editor` | Utilice el editor especificado para mostrar el registro al finalizar cada cmdlet. Notepad.exe es el editor predeterminado. Este parámetro debe incluir la especificación de archivo completa para el editor, y el editor debe tomar la especificación del archivo de registro como único parámetro. | | Cadena |
| `SecurityCsvFileSpec` | La especificación de archivo completo que apunta al archivo SecurityClient.csv descargado de la Administración de acceso e identidad de Citrix. Debe especificarse el campo CustomerId al utilizar este parámetro. | | Cadena |

Devuelve:

- Consulte Valores devueltos de cmdlet

- `Set-CvadAcCustomerInfoFile`: Actualice un archivo de información del cliente existente. Solo se cambian los parámetros especificados por el cmdlet. Todos los valores de parámetros sin especificar en el archivo CustomerInfo.yml permanecen igual.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `CustomerId` | ID del cliente. | | Cadena |
| `ClientId` | ID de la máquina cliente creado en Citrix Cloud. | | Cadena |
| `Secret` | Clave secreta del cliente creada en Citrix Cloud. | | Cadena |
| `Environment` | Entorno Production, ProductionGov o ProductionJP. | | Enumeración |
| `LogFileName` | Cambie el prefijo del archivo de registros de CitrixLog a otra cosa. | | Cadena |
| `StopOnError` | Detiene la operación tras el primer error. | | `$true` o `$false` |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `TargetFolder` | Utilice la carpeta especificada como carpeta raíz en lugar de *%HOMEPATH%\Documentos\Citrix\AutoConfig*. | | Cadena |
| `Locale` | Utilice la configuración regional especificada, en lugar de la configuración regional del sistema en el que se ejecuta la herramienta. | | Cadena |
| `Editor` | Utilice el editor especificado para mostrar el registro al finalizar cada cmdlet. Notepad.exe es el editor predeterminado. Este parámetro debe incluir la especificación de archivo completa para el editor, y el editor debe tomar la especificación del archivo de registro como único parámetro. | | Cadena |
| `SecurityCsvFileSpec` | La especificación de archivo completo que apunta al archivo SecurityClient.csv descargado de la Administración de acceso e identidad de Citrix. Debe especificarse el campo CustomerId al utilizar este parámetro. | | Cadena |

Devuelve:

- Consulte Valores devueltos de cmdlet

**Parámetros relacionados con requisitos previos**

Junto con los parámetros de acceso a la nube, estos parámetros se pueden utilizar con cmdlets relacionados con requisitos previos:

- `Environment`: Entorno Production o ProductionGov.
- `LogFileName`: Cambie el prefijo del archivo de registro de CitrixLog a otra cosa.
- `StopOnError`: Detiene la operación tras el primer error.
- `AlternateRootFolder`: Utilice la carpeta especificada como carpeta raíz en lugar de *%HOMEPATH%\Documentos\Citrix\AutoConfig*.
- `Locale`: Utilice la configuración regional especificada, en lugar de la configuración regional del sistema en el que se ejecuta la herramienta.
- `Editor`: Utilice el editor especificado para mostrar el registro al finalizar cada cmdlet. Notepad.exe es el editor predeterminado. Este parámetro debe incluir la especificación de

archivo completa para el editor, y el editor debe tomar la especificación del archivo de registro como único parámetro.

### Asistencia y solución de problemas con cmdlets

- `New-CvadAcZipInfoForSupport`: Comprime todos los archivos de registro e YML en un único archivo ZIP para enviarlos a Citrix para asistencia técnica. La información confidencial del cliente (CustomerInfo.yml y CvadAcSecurity.yml) no se incluye en el archivo ZIP. El archivo Icon.yml también se excluye debido a su tamaño. El archivo zip se coloca en *%HOMEPATH%\Documentos\Citrix\AutoConfig* y se denomina *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, según la fecha y la marca de hora. Este archivo ZIP también puede servir de copia de seguridad.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `TargetFolder` | Especifica una carpeta de destino para crear y guardar el archivo ZIP. | | Cadena |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |

  Devuelve:

  - El archivo ZIP, con su nombre y ubicación, se muestra en el símbolo del sistema.

- `Get-CvadAcStatus`: Se utiliza para probar la conectividad y garantizar que se cumplen todos los requisitos previos. Devuelve información sobre la herramienta, como el número de versión y la conectividad con la nube y el estado del conector.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |
| `SiteId` | Identifica el sitio al que conectarse. | | Cadena |
| `AdminAddress` | Esta es la dirección IP o DNS del Delivery Controller local utilizado para verificar el nivel de acceso de los administradores. Es necesario si la herramienta no se está ejecutando en un Delivery Controller. | | Cadena |

Devuelve:

- Muestra los resultados de cada elemento.

- `Test-CvadAcConnectionWithSite`: Prueba la conexión con el sitio en la nube para comprobar que la conexión de comunicación funciona. Este cmdlet emplea los parámetros de acceso a la nube o el archivo CustomerInfo.yml de información del cliente para especificar la información de conexión del cliente.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |

  Devuelve:

- Los resultados de las pruebas se muestran en la línea de comandos.

- `Find-CvadAcConnector`: Ubica los conectores existentes y determina su estado de ejecución. Este cmdlet utiliza información del archivo CustomerInfo.yml de información del cliente o del parámetro del ID de la máquina cliente para ubicar los conectores del cliente.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `CustomerInfoFileSpec` | La especificación de archivo que apunta a un archivo de información del cliente para supeditar la ubicación y el nombre predeterminados. Este parámetro se ignora cuando se proporciona el parámetro `CustomerId`. | | Cadena |
| `CustomerId` | El ID del cliente. Este parámetro supedita el mismo valor del archivo CustomerInfo.yml. | | Cadena |

  Devuelve:

- Los resultados se muestran en la línea de comandos.

- `Get-CvadAcCustomerSites`: Devuelve la lista de todos los sitios del cliente. Este cmdlet emplea los parámetros de acceso a la nube o el archivo CustomerInfo.yml de información del cliente para especificar la información de conexión del cliente.

Parámetros:

- Consulte Parámetros de acceso a la nube

Devuelve:

- Muestra una lista de identificadores de sitios del cliente encontrados.

- `New-CvadAcTemplateToFile`: Crea un archivo de plantilla para los componentes seleccionados, lo que le permite crear manualmente un archivo de importación.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes | | SwitchParameters |
| `TargetFolder` | Especifica la carpeta de destino de la exportación. | | Cadena |

  Devuelve:

  - Consulte Valores devueltos de cmdlet

- `Show-CvadAcDocument`: Muestra esta documentación en el explorador predeterminado.

  Parámetros:

  - Ninguno.

  Devuelve:

  - Muestra esta página web en el explorador web predeterminado.

- `Find-CvadAcInFile`: En las búsquedas de archivos, busca archivos YAML de componentes en busca de miembros que coincidan con uno o varios nombres que pueden contener caracteres comodín. El resultado es un informe de los miembros encontrados. En las búsquedas de archivos, solo se puede buscar un componente a la vez. En las búsquedas de archivos, se busca en todos los archivos YAML de la carpeta actual y todas sus subcarpetas. Se utiliza `FindSourceFolder` para limitar la cantidad de archivos en los que buscar.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Migración por componentes | Consulte Migración por componentes. Nota: El valor `-All` no es válido. | | SwitchParameters |
| `IncludeByName` | Una lista que especifica los nombres de los grupos de entrega que se incluirán al establecer el estado del sitio como activo. Se admiten los comodines "*"y "?"en los nombres. | | Lista de cadenas |
| `Unique` | Notifica solamente miembros encontrados y únicos. | | SwitchParameter |
| `IncludeYaml` | Incluye el YAML específico del miembro. | | SwitchParameter |
| `FindSourceFolder` | La carpetas en que comienza la búsqueda. | | Cadena |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | SwitchParameter |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |

Devuelve:

- Crea un informe que contiene los miembros encontrados para el componente especificado.

### Cmdlets de activación del sitio

Para obtener más información sobre la activación de sitios y el uso de estos cmdlets, consulte Activar sitios.

- `Set-CvadAcSiteActiveStateOnPrem`: Establece el estado del sitio local en activo o inactivo.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `SiteActive` | Cuando está presente, establece el sitio local en activo y quita el modo de mantenimiento de todos los grupos de entrega. Cuando este parámetro no está presente, se establece el modo de mantenimiento en todos los grupos de entrega. | | SwitchParameter |
| `IncludeByName` | Una lista que especifica los nombres de los grupos de entrega que se incluirán al establecer el estado del sitio como activo. Se admiten los comodines "*"y "?"en los nombres. | | Lista de cadenas |
| `ExcludeByName` | Una lista que especifica los nombres de los grupos de entrega que se excluirán al establecer el estado del sitio como activo. Se admiten los comodines "*"y "?"en los nombres. | | Lista de cadenas |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true or $false` |

Devuelve:

- Consulte Valores devueltos de cmdlet

- `Set-CvadAcSiteActiveStateCloud`: Establece el estado del sitio en la nube en activo o inactivo.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| Parámetros de acceso a la nube | Consulte Parámetros de acceso a la nube | | SwitchParameters |
| `SiteActive` | Cuando está presente, establece el sitio de la nube en activo y quita el modo de mantenimiento de todos los grupos de entrega. Cuando este parámetro no está presente, se establece el modo de mantenimiento en todos los grupos de entrega. | | SwitchParameter |

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `IncludeByName` | Una lista que especifica los nombres de los grupos de entrega que se incluirán al establecer el estado del sitio como activo. Se admiten los comodines "*"y "?"en los nombres. | | Lista de cadenas |
| `ExcludeByName` | Una lista que especifica los nombres de los grupos de entrega que se excluirán al establecer el estado del sitio como activo. Se admiten los comodines "*"y "?"en los nombres. | | Lista de cadenas |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |
| `DisplayLog` | Muestra el archivo de registros al finalizar el cmdlet. Establézcalo en `$false` para suprimir la visualización del registro. | | `$true or $false` |

Devuelve:

- Consulte Valores devueltos de cmdlet

### Cmdlets sobre la fusión de varios sitios locales

Para obtener más información acerca de la combinación de sitios y el uso de estos cmdlets, consulte Fusionar varios sitios en uno.

- `New-CvadAcSiteMergingInfo`: Crea un conjunto de información de prefijos/sufijos para fusión de sitios. No es necesario conocer todos los prefijos o sufijos al principio. Se pueden actualizar con `Set-CvadAcSiteMergingInfo` o modificando manualmente el archivo SiteMerging.yml.
  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `SiteName` | El nombre utilizado para identificar el conjunto de prefijos/sufijos de un sitio específico. Puede coincidir con el nombre del sitio real, pero no es necesario. | x | Cadena |
| Parámetros de fusión de sitios | Consulte Parámetros de fusión de sitios. | | SwitchParameters |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |

Devuelve:

- Ninguno

- `Set-CvadAcSiteMergingInfo`: Actualiza un sitio fusionando el conjunto de información de prefijo/sufijo.

  Parámetros:

| Nombre | Descripción | ¿Obligatorio? | Tipo |
|---|---|---|---|
| `SiteName` | El nombre utilizado para identificar el conjunto de prefijos/sufijos de un sitio específico. Puede coincidir con el nombre del sitio real, pero no es necesario. | x | Cadena |
| Parámetros de fusión de sitios | Consulte Parámetros de fusión de sitios. | | SwitchParameters |
| `Quiet` | Suprime los registros en la consola. | | SwitchParameter |

  Devuelve:

  - Ninguno

- `Remove-CvadAcSiteMergingInfo`: Quita un sitio fusionando el conjunto de información de prefijo/sufijo.

  Parámetros:

  - `SiteName`: Identifica el conjunto de prefijos y sufijos del sitio. Se trata de una cadena y es obligatoria.

  Devuelve:

  - Ninguno

#### Parámetros de fusión de sitios

Estos parámetros se pueden utilizar al ejecutar los cmdlets de fusión de sitios. Todos los parámetros que se indican son cadenas.

- `SiteName`: El nombre utilizado para identificar el conjunto de prefijos/sufijos de un sitio específico. Puede coincidir con el nombre del sitio real, pero no es necesario. SiteName es un parámetro obligatorio.
- `AdminScopedPrefix`: El prefijo que se aplica a los ámbitos de administrador.
- `ApplicationPrefix`: El prefijo que se aplica a las aplicaciones.
- `ApplicationFolderPrefix`: El prefijo que se aplica a las carpetas de aplicaciones; `ApplicationFolderPrefix` puede combinarse con `ApplicationFolderRoot`.
- `ApplicationFolderRoot`: La nueva carpeta raíz de las carpetas de aplicaciones. Crea una jerarquía de carpetas adicional. `ApplicationFolderRoot` puede combinarse con `ApplicationFolderPrefix`.
- `ApplicationGroupPrefix`: El prefijo de los grupos de aplicaciones.
- `ApplicationUserPrefix`: El prefijo que se aplica al nombre de la aplicación que ve el usuario.
- `ApplicationAdminPrefix`: El prefijo que se aplica al nombre de la aplicación que ve el administrador.
- `DeliveryGroupPrefix`: El prefijo que se aplica a los grupos de entrega.
- `GroupPolicyPrefix`: El prefijo que se aplica a los nombres de directivas.
- `HostConnectionPrefix`: El prefijo que se aplica a las conexiones de host.
- `MachineCatalogPrefix`: El prefijo que se aplica a los catálogos de máquinas.
- `StoreFrontPrefix`: El prefijo que se aplica a los nombres de StoreFront.
- `TagPrefix`: El prefijo que se aplica a las etiquetas.
- `AdminScopedSuffix`: El sufijo que se aplica a los ámbitos de administrador.
- `ApplicationSuffix`: El sufijo que se aplica a las aplicaciones.
- `ApplicationFolderSuffix`: El sufijo que se aplica a las carpetas de aplicaciones; `ApplicationFolderSuffix` puede combinarse con `ApplicationFolderRoot`.

- `ApplicationGroupSuffix`: El sufijo de los grupos de aplicaciones.
- `ApplicationUserSuffix`: El sufijo que se aplica al nombre de la aplicación que ve el usuario.
- `ApplicationAdminSuffix`: El sufijo que se aplica al nombre de la aplicación que ve el administrador.
- `DeliveryGroupSuffix`: El sufijo que se aplica a los grupos de entrega.
- `GroupPolicySuffix`: El sufijo que se aplica a los nombres de directivas.
- `HostConnectionSuffix`: El sufijo que se aplica a las conexiones de host.
- `MachineCatalogSuffix`: El sufijo que se aplica a los catálogos de máquinas.
- `StoreFrontSuffix`: El sufijo que se aplica a los nombres de StoreFront.
- `TagSuffix`: El sufijo que se aplica a las etiquetas.
- `SiteRootFolder`: El nombre de carpeta completo que se utilizará para las exportaciones e importaciones; puede ser una carpeta local o un recurso compartido.

## Parámetros genéricos

### Parámetros de acceso a la nube

Todos los cmdlets que acceden a la nube admiten los siguientes parámetros adicionales.

> **Nota:**
>
> CustomerId, ClientId y Secret se pueden colocar en el archivo CustomerInfo.yml o especificarse con el cmdlet mediante los parámetros siguientes. Cuando se especifican en ambos lugares, los parámetros del cmdlet tienen prioridad.

- `CustomerId`: El ID del cliente utilizado en las API de REST. Es necesario para acceder a todas las API de REST. Su ID de cliente se encuentra en Citrix Cloud.
- `ClientId`: El parámetro clientID creado en el sitio web de administración de acceso e identidad de Citrix Cloud. Es necesario para obtener el token de portador requerido para la autenticación de todas las API de REST.
- `Secret`: La clave secreta creada en el sitio web de administración de acceso e identidad de Citrix Cloud. Es necesario para obtener el token de portador requerido para la autenticación de todas las API de REST.
- `CustomerInfoFileSpec`: La especificación de archivo que apunta a un archivo de información del cliente para supeditar la ubicación y el nombre predeterminados.

### Parámetros de los modos de migración

Cmdlets que modifican la configuración del sitio en la nube (`Import`, `Restore`, `Merge`, `New` y `Sync`) admiten los siguientes parámetros adicionales para ofrecer una mayor flexibilidad.

- `CheckMode`: Lleva a cabo la operación de importación pero *no* realiza cambios. Todos los cambios esperados se notifican antes de que se complete la importación. Puede utilizar este comando para probar la importación antes de que esta se produzca.
- `BackupFirst`: Hace una copia de seguridad del contenido de la nube en archivos YML antes modificar la configuración de la nube. Esto está habilitado de forma predeterminada.
- `Confirm`: Si el valor es true, solicita a los usuarios que confirmen si quieren efectuar cambios en la configuración del sitio en la nube. El cmdlet `Remove` muestra un mensaje debido a su naturaleza destructiva. Establézcalo en false si no quiere ningún mensaje, como en la ejecución en scripts automatizados. El valor predeterminado de `Confirm` es true.
- `SecurityFileFolder`: Esta es la carpeta completa que contiene el archivo CustomerInfo.yml, que es posible que apunte a una carpeta local o a una carpeta compartida de red que pueda estar bajo control de autenticación. La herramienta no solicitará credenciales; se debe obtener acceso al recurso controlado antes de ejecutar la herramienta.
- `SiteName`: Especifica el conjunto de prefijos y sufijos de fusión de sitios que va a utilizarse al importar.
- `SiteActive`: Especifica si el sitio importado está activo o inactivo. De forma predeterminada, este parámetro se establece en `$false`, lo que indica que el sitio importado está inactivo.

#### Parámetros de visualización del registro

Los cmdlets `Export`, `Import`, `Sync`, `Restore`, `Backup`, `Compare` y `Remove` muestran el archivo de registros cuando se completa la operación. Para suprimir la visualización, establezca el parámetro `-DisplayLog` en `$false`. Se utiliza Notepad.exe de forma predeterminada para mostrar el archivo de registros. Puede especificar otro editor en el archivo CustomerInfo.yml.

```
Editor: C:\Program Files\Notepad++\notepad++.exe
```

### Valores devueltos de cmdlet

#### ActionResult

Todos los cmdlets devuelven el siguiente valor.

```
1             public class ActionResult
2             {
3
4                 public bool                         Overall_Success;
5                 public Dictionary<string, string>   Individual_Success;
6                 public object                       CustomResult;
7              }
```

`Overall_Success` devuelve un único valor booleano que muestra el estado global del proceso del

cmdlet en todos los componentes seleccionados: “true”significa que el proceso se completó correctamente y “false”significa que no se completó correctamente.

`Individual_Success` devuelve uno o tres valores para cada componente principal. El resultado de un componente puede ser Success (Correcto), Failure (Error) o Skipped (Omitido). Skipped indica que el cmdlet no seleccionó dicho componente para su ejecución.

`CustomResult` es específico de cada cmdlet.

#### CustomResult

`Import`, `Merge`, `Restore`, `Sync`, `Compare`, `Compare File` y `Remove` devuelven la siguiente información de resultados personalizados a una sola instancia de `EvaluationResultData`.

> **Nota:**
>
> Los cmdlets `Export` y `Template` no devuelven un resultado personalizado.

```
1                public class EvaluationResultData
2                {
3
4                    public Dictionary<string, Dictionary<string,
                        ActionResultValues >> EvaluationResults;
5                    public int                  Added;
6                    public int                  Updated;
7                    public int                  Deleted;
8                    public int                  NoChange;
9                    public int                  TotalChanged;
10                   public EvaluationResults     OverallResult;
11                   public string               CloudBackupFolder;
12                   public string               SourceBackupFolder;
13                }
14
15               Where:
16               public enum ActionResultValues
17               {
18
19                   Add,
20                   Update,
21                   Delete,
22                   Identical,
23                   DoNothing
24                }
25
26               public enum EvaluationResults
27               {
28
29                   Success,
30                   Failure,
31                   Skipped
```

```
32                          }
```

`EvaluationResults` muestra una lista con una entrada por componente seleccionado. La clave es el nombre del componente y el valor es una lista de cada miembro del componente y la acción realizada en el miembro correspondiente del componente. Las acciones pueden ser cualquiera de los valores de `ActionResultValues`.

`Added`, `Updated`, `Deleted` y `NoChange` indican la cantidad total de componentes que los miembros agregaron, actualizaron, eliminaron o para los que no se realizó ninguna acción, en ese orden.

`TotalChanged` es la suma de `Added`, `Updated` y `Deleted`.

`OverallResult` es un único valor booleano que indica el resultado del cmdlet. "True"indica que el proceso se completó correctamente en todos los componentes, y "false"indica un error en el procesamiento de uno o más componentes.

`CloudBackupFolder` es la especificación de archivo válido de la copia de seguridad de la configuración del sitio en la nube antes de que el cmdlet lleve a cabo acciones de modificación de la nube.

`SourceBackupFolder` es la especificación de archivo válido de la copia de seguridad del archivo de origen realizada después de que el cmdlet haya finalizado. De forma predeterminada, estos archivos se hallan en *%HOMEPATH%\Documentos\Citrix\AutoConfig*.

### Ayuda de PowerShell

La ayuda de PowerShell está disponible para cada cmdlet. Todos los parámetros se documentan con cada cmdlet, junto con una breve explicación del cmdlet. Para obtener acceso a la ayuda de un cmdlet, escriba `Get-Help` delante del cmdlet.

```
Get-Help Import-CvadAcToSite
```

## Solucionar problemas con Configuración automatizada e información adicional

March 30, 2024

> **Importante:**
>
> Para ver mensajes de error habituales para Configuración automatizada y las soluciones correspondientes, consulte las *preguntas frecuentes sobre la solución de problemas* en el artículo CTX277730 de Knowledge Center.

### Errores de la herramienta de Configuración automatizada

Las operaciones de la herramienta de Configuración automatizada a veces pueden generar errores. Cuando esto ocurre, pueden producirse errores al procesar componentes como catálogos de máquinas, grupos de entrega o directivas de grupo, por ejemplo. El uso de `OnErrorAction` y los parámetros de continuación le permiten detectar errores durante el procesamiento, resolverlos y reanudar el proceso.

El valor predeterminado de `OnErrorAction` es `StopCompEnd`. Cuando se produce un error, la herramienta termina de procesar el componente actual. No se procesan componentes adicionales, y los errores no se transfieren a los componentes dependientes posteriores. Tras resolver los errores, puede ejecutar de nuevo los cmdlets con los parámetros de continuación aplicados que quiera.

#### Parámetro OnErrorAction

Puede definir valores del parámetro `OnErrorAction` en los comandos de la migración para controlar la forma en que la herramienta responde a los errores que encuentra al procesar los componentes.

En esta tabla se muestran los valores de los parámetros y sus descripciones:

| Valor | Descripción |
|---|---|
| `Continue` | Intenta procesar cuantos componentes le sea posible. |
| `Pause` | Se detiene al final del procesamiento y le pregunta si continuar o parar. |
| `StopCompEnd` | Intenta procesar la mayor parte posible del componente. Se detiene cuando el componente ha terminado. (valor predeterminado) |
| `StopImmediately` | El procesamiento se detiene cuando se detecta un error. |

#### Cmdlets de migración

Puede aplicar el parámetro `OnErrorAction` a estos comandos de migración:

- `Compare-CvadAcToSite`
- `Import-CvadAcToSite`
- `Merge-CvadAcToSite`
- `New-CvadAcToSite`

- `Restore-CvadAcToSite`

Ejemplo:`Merge-CvadAcToSite -OnErrorAction StopImmediately`

#### Parámetros de Reanudar

Estos parámetros definen cómo se reanuda la herramienta después de que una operación se ponga en pausa o se detenga debido a un error.

Puede aplicar parámetros de reanudación a cmdlets de migración que incluyan uno de estos valores del parámetro `OnErrorAction`:

- `Pause`
- `StopCompEnd`
- `StopImmediately`

En esta tabla se muestran los valores de los parámetros y sus descripciones:

| Valor | Descripción |
|---|---|
| `-AllRemaining` | Requiere un componente inicial. El procesamiento comienza en el componente inicial y procesa todos los componentes restantes. Se procesan varios componentes. |
| `-Resume` | Usa el componente de `CurrentComponent.txt` como punto de partida. Todo el resto está establecido en true. Se procesan varios componentes. |
| `-Repeat` | Usa el componente de `CurrentComponent.txt` como punto de partida. Todo el resto está establecido en false. Solo se procesa un componente. |

El último componente procesado se almacena en el archivo `CurrentComponent.txt` en la carpeta AutoConfig. No se recomienda modificar este archivo.
Si especifica `-Resume` o `-Repeat` y `CurrentComponent.txt` falta o no es válido, el procesamiento se detiene y se le pide que seleccione un componente.

#### Configurar OnErrorAction en el archivo CustomerInfo.yml

También puede establecer valores de `OnErrorAction` en el archivo `CustomerInfo.yml`. Defina los valores mediante estos cmdlets:

- Para un archivo nuevo: `New-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`
- Para un archivo existente: `Set-CvadAcCustomerInfoFile -OnErrorAction Continue | Pause | StopCompEnd | StopImmediately`

### Registros

La ejecución de cualquier cmdlet da como resultado la creación de un archivo de registros y una entrada en el archivo principal de registros del historial. Todos los archivos de registros de operaciones se colocan en una carpeta de copia de seguridad. Todos los nombres de archivos de registros comienzan por `CitrixLog` y, a continuación, muestran la operación de configuración automática junto con la fecha y la hora de la ejecución de los cmdlets. Los registros no se eliminan automáticamente.

El registro del historial principal se encuentra en `*%HOMEPATH%\Documents\Citrix\AutoConfig*`, en el archivo denominado **History.Log**. Cada ejecución de cmdlets genera una entrada en el registro principal que contiene las ubicaciones de los archivos de registros, la fecha, la operación, el resultado y la copia de seguridad de la ejecución.

También puede usar el cmdlet `New-CvadAcZipInfoForSupport` para recopilar registros y enviarlos a Citrix para obtener asistencia. Este cmdlet comprime todos los archivos de registros y YML en un único archivo ZIP. La información confidencial del cliente (CustomerInfo.yml y CvadAcSecurity.yml) no se incluye en el archivo ZIP. El archivo Icon.yml también se excluye debido a su tamaño. El archivo zip se coloca en *%HOMEPATH%\Documentos\Citrix\AutoConfig* y se denomina *CvadAcSupport_yyyy_mm_dd_hh_mm_ss.zip*, según la fecha y la marca de hora. Este archivo ZIP también puede servir de copia de seguridad.

Cada archivo de registros incluye lo siguiente:

- El nombre de la operación y si el modo de comprobación está habilitado
- La fecha y la hora de inicio y finalización
- Varias entradas para las acciones de cada componente y notificaciones para indicar que el proceso se completó correctamente o no se completó
- Resumen de las acciones realizadas, incluido un recuento de los objetos creados
- Correcciones sugeridas donde corresponda
- Ubicación de la carpeta de copia de seguridad donde corresponda
- Ubicación del registro principal
- Duración

### Archivos de diagnóstico

Los archivos de diagnóstico le ayudan a determinar y resolver problemas. Los archivos siguientes se crean al ejecutar la operación relacionada. Se encuentran en la subcarpeta específica de cada

acción, en *%HOMEPATH%\Documentos\Citrix\AutoConfig*. Incluya estos archivos cuando proporcione información para la asistencia en la resolución de problemas.

#### Exportar

`PoshSdk_yyyy_mm_dd_hh_mm_ss.ps1`

Este archivo cuenta todas las llamadas del SDK de Broker PowerShell realizadas para exportar la configuración del sitio en archivos.

#### Import, Merge, Restore, Sync, Backup, Compare

`Transaction_yyyy_mm_dd_hh_mm_ss.txt`

Este archivo documenta cada llamada de la API de REST y la información relacionada.

`RestApiContent_yyyy_mm_dd_hh_mm_ss.txt`

Este archivo alberga todo el contenido de `Add`, `Update` y `Delete` de la API de REST.

### Problemas resultantes de dependencias

Es posible que las importaciones y las fusiones fallen debido a las dependencias que faltan. Algunos problemas comunes son:

1. Faltan filtros de grupo de entrega en las directivas de grupo. Las causas habituales son grupos de entrega que no se importaron.
2. Las aplicaciones no se pueden importar o fusionar. La causa habitual es que faltan grupos de entrega o grupos de aplicaciones que no se importaron.
3. A los grupos de aplicaciones les falta un parámetro RestrictToTag. Las causas habituales son etiquetas que no se importaron.
4. Las conexiones de host fallan. La causa habitual es falta de información de seguridad en el archivo CvadAcSecurity.yml.
5. Los catálogos de máquinas fallan. La causa habitual son conexiones de host que no se importaron.
6. Faltan máquinas en catálogos de máquinas y grupos de entrega. La causa habitual son máquinas que no se encontraron en Active Directory.
7. Faltan usuarios en los grupos de entrega. La causa habitual son los usuarios que no se encontraron en Active Directory.

## Recomendaciones

- No ejecute más de una instancia de Configuración automatizada a la vez. Ejecutar varias instancias simultáneas produce resultados impredecibles en el sitio de Citrix Cloud. Si eso ocurre, ejecute de nuevo una instancia de Configuración automatizada para llevar el sitio al estado esperado.
- No trabaje ni modifique los datos de la ficha Administrar de Configuración completa mientras Configuración automatizada está activa.
- Verifique siempre visualmente los resultados de las operaciones de fusión, importación y restauración en Configuración completa para asegurarse de que el sitio en la nube cumple con las expectativas.

## Carpetas

### Ubicación raíz predeterminada de la carpeta

Todas las operaciones de la herramienta de Configuración automatizada se llevan a cabo en la carpeta raíz o en subcarpetas dentro de ella. La carpeta raíz se halla en *%HOMEPATH%\Documentos\Citrix\AutoConfig*.

### Exportar

Todos los archivos exportados se colocan en dos carpetas, lo que facilita su uso y proporciona un historial de exportaciones. Las exportaciones siempre se colocan en la carpeta raíz. Las copias se colocan en una subcarpeta denominada **Export** con la fecha y la hora de la exportación.

La carpeta raíz siempre contiene la configuración del sitio local que se ha exportado más recientemente. Cada subcarpeta **Export** contiene la exportación realizada en la fecha y la hora indicadas, que mantiene un historial de exportaciones. Puede utilizar cualquier subcarpeta **Export** para configurar el sitio en la nube. Configuración automatizada no elimina ni modifica subcarpetas de exportación existentes.

### Import/Merge/Sync/Compare

Las operaciones `Import`, `Merge` y `Compare` siempre proceden de archivos ubicados en la carpeta raíz. Cada operación da como resultado la creación de una subcarpeta en la que se copian los archivos de la carpeta raíz, lo que proporciona un historial los archivos de origen que han cambiado en el sitio en la nube.

#### Restore

La operación `Restore` utiliza una subcarpeta existente para configurar el sitio en la nube. La carpeta de origen se especifica en el parámetro `-RestoreFolder` requerido. A diferencia de otros comandos, no se crea ninguna subcarpeta porque la operación `Restore` utiliza una subcarpeta existente. La carpeta de restauración puede ser la carpeta raíz, pero aún debe especificarse en el parámetro `-RestoreFolder`.

### Copias de seguridad

La Configuración automatizada inicializa, actualiza y realiza copias de seguridad de la configuración de un sitio en la nube. Al utilizarse en el tiempo, muchas configuraciones diferentes pueden cambiar en el sitio en la nube. Para facilitar el uso a largo plazo y conservar los cambios del historial, la Configuración automatizada utiliza un esquema de preservación para guardar este historial de cambios y ofrecer un método para restaurar estados anteriores.

Las copias de seguridad de la configuración de los sitios en la nube siempre se llevan a cabo en una subcarpeta denominada **Backup** con los datos y el momento de la copia de seguridad. Configuración automatizada no elimina ni modifica subcarpetas de exportación existentes.

Puede utilizar las copias de seguridad para restaurar componentes específicos o toda la configuración. Para restaurar todos los componentes de los grupos de entrega y los catálogos de máquinas, utilice el cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss -DeliveryGroups -MachineCatalogs
```

> **Nota:**
>
> La información del archivo de la copia de seguridad del cmdlet anterior se basa en sus propias copias de seguridad.

Para restaurar toda la configuración del sitio en la nube, utilice el cmdlet:

```
Restore-CvadAcToSite -RestoreFolder %HOMEPATH%\Documents\Citrix\
AutoConfig/Backup_yyyy_mm_dd_hh_mm_ss
```

> **Nota:**
>
> La información del archivo de la copia de seguridad del cmdlet anterior se basa en sus propias copias de seguridad.

#### Cambiar la carpeta raíz predeterminada

Las operaciones `Export`, `Import`, `Merge`, `Sync` y `Compare` pueden cambiar la carpeta raíz predeterminada mediante el parámetro `–AlternateFolder`. La creación y administración de subcarpetas por operación sigue siendo la misma que la descrita anteriormente.

#### Archivos copiados en subcarpetas

Todos los archivos que tengan una extensión "YML"se copian en subcarpetas de operación, excepto los siguientes:

- CustomerInfo.yml
- ZoneMapping.yml
- CvadAcSecurity.yml

#### Copias de seguridad automatizadas de sitios en la nube a prueba de fallos

Se realiza una copia de seguridad de la configuración del sitio en la nube actual antes de ejecutar operaciones que cambien la configuración. Esto incluye los parámetros `Import`, `Merge`, `Sync` y `Restore`. La copia de seguridad siempre está en una subcarpeta debajo de la subcarpeta operativa.

En el caso de `Restore`, la carpeta de la copia de seguridad es una subcarpeta de la carpeta especificada en el parámetro `-RestoreFolder`.

### Automatización

Para que los cmdlets de la herramienta de Configuración automatizada se puedan ejecutar en scripts de automatización sin intervención del administrador, suprima los mensajes emergentes; los resultados del registro se mostrarán al finalizar el cmdlet. También puede establecer parámetros para hacer lo mismo mediante el archivo CustomerInfo.yml.

Agregue el siguiente parámetro a los cmdlets de modificación de la nube para no ver mensajes emergentes.

```
-Confirm $false
```

Agregue el siguiente parámetro a los cmdlets para no mostrar el registro al finalizar el cmdlet.

```
-DisplayLog $false
```

Agregue el siguiente parámetro a los cmdlets para suprimir el registro en la ventana de comandos de PowerShell.

```
-Quiet
```

Como otro método, los siguientes parámetros se pueden colocar en el archivo CustomerInfo.yml.

```
Confirm: False
```

```
DisplayLog: False
```

### Exportaciones desde equipos que no tengan Delivery Controllers

La herramienta de Configuración automatizada utiliza varios SDK de PowerShell de Citrix para exportar la configuración del sitio local en archivos. Estos SDK se instalan automáticamente en el Delivery Controller, lo que permite que la herramienta se ejecute en el Delivery Controller sin tener que hacer nada más. En máquinas que no tienen Delivery Controllers, es necesario instalar el conjunto de SDK de PowerShell de Citrix que necesita la herramienta. Este conjunto de SDK forma parte de Citrix Studio, y se puede instalar desde los medios de instalación de Citrix Virtual Apps and Desktops.

> **Nota:**
>
> Configuración automatizada no se puede ejecutar en el Cloud Connector.

### Pasar al plano de control de Citrix Cloud Government y Citrix Cloud Japan

Los entornos del plano de control de Citrix Cloud Government y Citrix Cloud Japan utilizan diferentes puntos de acceso para autenticar y asignar tokens de acceso. Este requisito único se aplica a cualquier herramienta de Configuración automatizada que acceda a la nube. Siga estos pasos para utilizar Configuración automatizada en estos entornos.

1. En la carpeta *%HOMEPATH%\Documents\Citrix\AutoConfig*, modifique CustomerInfo.yml.
2. Agregue una de estas líneas, según el entorno al que quiera conectarse, a CustomerInfo.yml (o cámbiela, si ya está presente).

   ```
   Environment: 'ProductionGov'
   ```

   o bien

   ```
   Environment: 'ProductionJP'
   ```

Ahora la Configuración automatizada se puede utilizar en estos entornos.

### Recopilación de datos de Citrix Cloud

Para obtener información sobre los datos que Citrix Cloud recopila, consulte Gestión de registros y contenido para clientes de Citrix Cloud Services.

### Recursos adicionales

#### Foro de debate

Visite el foro de debate de Citrix Discussions para la Configuración automatizada.

#### Vídeo

Consulte Under the Hood of the Automated Configuration Tool for Citrix Virtual Apps and Desktops en YouTube.

#### Aprendizaje

El centro de aprendizaje de Cloud contiene guías detalladas en vídeo para crear una implementación de servicios, incluidas las tareas descritas en este artículo. Consulte Migrating Citrix Virtual Apps and Desktops to Citrix Cloud Learning Path.

## Migrar cargas de trabajo entre ubicaciones de recursos mediante Image Portability Service

May 17, 2024

Image Portability Service simplifica la administración de imágenes en distintas plataformas. Las API de REST de Citrix Virtual Apps and Desktops sirven para automatizar la administración de recursos en un sitio de Citrix Virtual Apps and Desktops.

El flujo de trabajo de Image Portability comienza cuando usa Citrix Cloud para iniciar la migración de una imagen entre dos ubicaciones de recursos. Tras exportar la imagen, Image Portability Service le ayuda a transferir y preparar la imagen para que se ejecute en el hipervisor o la nube pública de destino. Por último, Citrix Provisioning o Machine Creation Services aprovisionan la imagen en el entorno de destino.

### Componentes

Los componentes de Image Portability Service incluyen:

- Servicios de Citrix Cloud
- Citrix Credential Wallet
- Dispositivo Citrix Connector

- Máquina virtual de Compositing Engine
- Scripts de ejemplo de PowerShell

#### Servicios de Citrix Cloud

La API de Citrix Cloud Services es un servicio de API de REST que interactúa con Image Portability Service. Con el servicio de API de REST, puede crear y supervisar trabajos de Image Portability. Por ejemplo, puede hacer una llamada a la API para iniciar un trabajo de Image Portability, como exportar un disco, y luego realizar llamadas para obtener el estado del trabajo.

#### Citrix Credential Wallet

El servicio Citrix Credential Wallet administra de forma segura las credenciales del sistema, lo que permite que Image Portability Service interactúe con sus activos. Por ejemplo, al exportar un disco de vSphere a un recurso compartido de SMB, Image Portability Service requiere credenciales para abrir una conexión con el recurso compartido de SMB para escribir en el disco. Si las credenciales se almacenan en Credential Wallet, Image Portability Service puede recuperar y usar esas credenciales.

Este servicio le ofrece la posibilidad de administrar completamente sus credenciales. La API de Cloud Services sirve de punto de acceso, lo que le permite crear, actualizar y eliminar credenciales.

#### Compositing Engine

Compositing Engine es el caballo de tiro de Image Portability Service. Compositing Engine (CE) es una virtual única que se crea al comienzo de un trabajo de exportación o preparación de Image Portability. Estas máquinas virtuales se crean en el mismo entorno en el que tiene lugar el trabajo. Por ejemplo, al exportar un disco desde vSphere, CE se crea en el servidor vSphere. Del mismo modo, cuando se ejecuta un trabajo de preparación en Azure, AWS o Google Cloud, CE se crea en Azure, AWS o Google Cloud, respectivamente. CE monta el disco en sí mismo y, a continuación, hace las manipulaciones necesarias. Al finalizar el trabajo de preparación o exportación, se eliminan la máquina virtual de CE y todos sus componentes.

#### Connector Appliance

El Connector Appliance, que ejecuta software de proveedor para administrar los recursos de IPS, se ejecuta en su entorno (tanto local como en la suscripción de Azure, AWS o Google Cloud) y actúa como controlador para trabajos individuales. Así, recibe instrucciones de trabajo del servicio en la nube y crea y administra las máquinas virtuales de Compositing Engine. La máquina virtual del Connector Appliance actúa como un punto de comunicación único y seguro entre los servicios en la nube y sus

entornos. Implemente uno o más Connector Appliances en cada una de sus ubicaciones de recursos (locales, Azure, AWS o Google Cloud). Se implementa un Connector Appliance en cada ubicación de recursos por motivos de seguridad. Al ubicar conjuntamente el Connector Appliance y Compositing Engine, mejora en gran medida la estrategia de seguridad de la implementación, ya que todos los componentes y las comunicaciones se mantienen dentro de su ubicación de recursos.

#### Módulos de PowerShell

Proporcionamos una colección de módulos de PowerShell para su uso en scripts como punto de partida para que desarrolle su propia automatización personalizada. Los módulos suministrados se admiten tal cual, pero puede modificarlos si es necesario para su implementación.

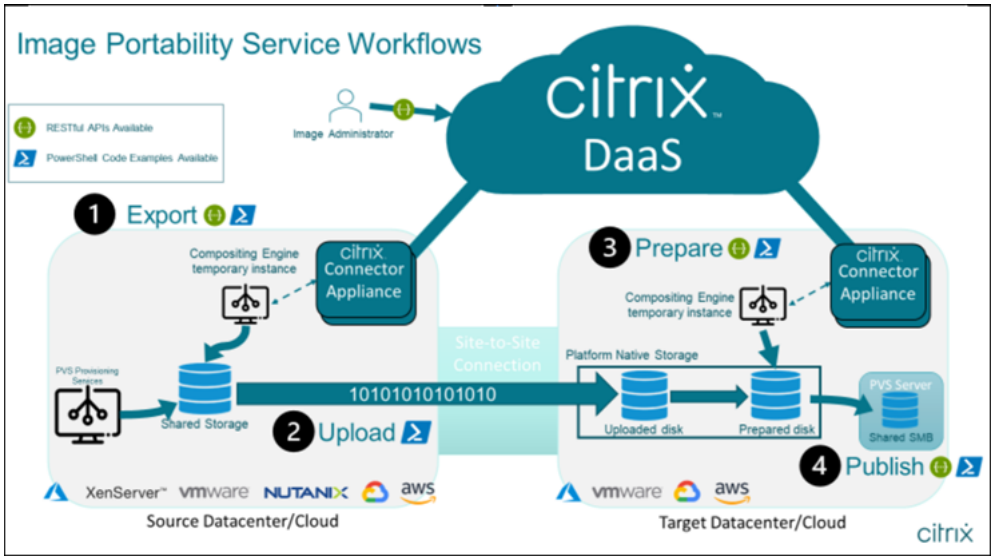
La automatización de PowerShell utiliza los parámetros de configuración suministrados para crear una llamada REST al servicio de API de Citrix Cloud con el fin de iniciar el trabajo y, a continuación, proporcionarle actualizaciones periódicas a medida que este avanza.

Si prefiere desarrollar su propia solución de automatización, puede realizar llamadas al servicio en la nube directamente mediante su lenguaje de programación preferido. Consulte el portal de API para obtener información detallada sobre la configuración y el uso de los dispositivos de punto final de REST y los módulos de PowerShell de Image Portability Service.

### Flujos de trabajo

Image Portability Service utiliza un flujo de trabajo de varias fases para preparar una imagen de catálogo maestra a partir de una ubicación de recursos local para su suscripción a la nube pública. El servicio exporta la imagen desde la plataforma de hipervisor local y usted la carga en su suscripción en la nube pública (nuestra utilidad de carga de PowerShell proporcionada puede ayudar a automatizar esta tarea). A continuación, Image Portability prepara la imagen para hacerla compatible con su plataforma de nube pública. Por último, la imagen se publica y está lista para implementarse como un nuevo catálogo de máquinas dentro de su ubicación de recursos en la nube.




Estos flujos de trabajo de alto nivel se basan en la configuración de aprovisionamiento de origen y destino de la imagen (Machine Creation o Citrix Provisioning). El flujo de trabajo elegido determina qué pasos de la tarea de Image Portability son necesarios.

Consulte la siguiente tabla para comprender qué tareas se requieren para cada uno de los flujos de trabajo de IPS admitidos.

| Flujo de trabajo (de origen a destino) | Exportar | Cargar | Preparar | Publicar |
|---|---|---|---|---|
| MCS a MCS | S | S | S | N |
| PVS a MCS* | N | S | S | N |
| PVS a PVS | N/D | S | S | S |
| MCS a PVS | S | S | S | S |

*Se supone que tiene la imagen original como un disco virtual de Citrix Provisioning y no necesita exportarla directamente desde el hipervisor de la plataforma de origen.

## Requisitos

Para empezar a trabajar con Image Portability, debe cumplir con los siguientes requisitos.

### Una imagen del catálogo de máquinas de Citrix

IPS requiere el uso de imágenes que tengan una de las siguientes configuraciones probadas:

- Windows Server 2016, 2019 y 2022H2
- Windows 10 u 11
- Aprovisionamiento mediante Machine Creation Services o Citrix Provisioning
- Agente Citrix Virtual Delivery Agent:
  - Las dos actualizaciones acumulativas más recientes para 1912 y 2203 LTSR
  - Las dos versiones actuales más recientes
- Servicios de escritorio remoto habilitados para el acceso a la consola en Azure

Image Portability Service admite los siguientes hipervisores y plataformas en la nube:

**Plataformas de origen:**

- VMware vSphere 7.0 y 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (solo Prism Element)
- Microsoft Azure
- Google Cloud Platform

**Plataformas de destino:**

- VMware vSphere 8.0
- XenServer 8/Citrix Hypervisor 8.2
- Nutanix AHV (solo Prism Element)
- Microsoft Azure
- AWS
- Google Cloud Platform

#### Un dispositivo Citrix Connector

Necesita un dispositivo Citrix Connector instalado y configurado en cada ubicación de recursos donde tenga pensado usar Image Portability. Por ejemplo, si usa portabilidad de imágenes para mover una imagen de vSphere a Azure, AWS y Google Cloud, necesita al menos cuatro dispositivos Citrix Connector:

Consulte Implementar Connector Appliances para obtener instrucciones detalladas.

#### Un recurso compartido de archivos de SMB (Windows)

Necesita un **recurso compartido de archivos SMB** de Windows para almacenar los resultados de los trabajos de exportación. La máquina virtual de Compositing Engine debe poder acceder al recurso compartido, que se creará en la ubicación de recursos en la que utilice Image Portability Service. Asegúrese de que el espacio libre disponible en el recurso compartido es al menos el doble del tamaño configurado del sistema de archivos de la imagen.

#### Una máquina para ejecutar scripts de PowerShell

Compruebe que la máquina donde se ejecutan los scripts de PowerShell tiene lo siguiente:

- PowerShell versión 5.1.
- Una conexión de red rápida al recurso compartido de archivos de SMB. Puede ser la misma máquina que aloja el recurso compartido de archivos.
- Una conexión de red rápida a las plataformas de nube pública en las que tiene pensado usar la funcionalidad Image Portability. Por ejemplo, Azure, AWS o Google Cloud.

  Consulte la sección Preparar una máquina para PowerShell para obtener más información sobre cómo descargar y configurar los módulos de Image Portability desde la Galería de PowerShell.

#### Su ID de cliente de Citrix Cloud

Asegúrese de tener una suscripción válida a Citrix DaaS.

Para continuar, necesita acceso a Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Si no tiene acceso, póngase en contacto con su representante de Citrix.

Consulte la documentación de API Getting Started para obtener instrucciones sobre cómo crear y configurar un cliente de API para uso con portabilidad de imágenes.

#### Configuración y permisos requeridos de Azure

Para que Image Portability Service realice acciones en su recurso de Azure, debe otorgar permisos para ciertas capacidades de Azure a la entidad de servicio de Azure que utiliza Image Portability Service. Para obtener una lista detallada, consulte Permisos requeridos de Microsoft Azure.

Puede asignar el rol **Colaborador** a la entidad de servicio del recurso asociado. Si no, para asignar los permisos mínimos requeridos, puede crear roles personalizados con los permisos necesarios y asignarlos a la entidad principal del servicio limitada los recursos adecuados.

Consulte la documentación de Azure sobre cómo configurar los roles de seguridad para la entidad de servicio de Azure y cómo crear roles personalizados.

#### Configuración y permisos requeridos de Google Cloud

Para que Image Portability Service realice acciones en su proyecto de Google Cloud, debe otorgar permisos para ciertas capacidades a la entidad de servicio de Google Cloud que utiliza Image Portability Service.

Para obtener una lista detallada, consulte Permisos requeridos de Google Cloud.

Puede asignar estos permisos mediante los siguientes roles:

- Editor de compilaciones en la nube
- Administrador de procesos
- Administrador de almacenamiento
- Usuario de cuenta de servicio

Para obtener más información sobre cómo configurar los permisos de las cuentas de servicio, consulte la documentación de Google Cloud.

#### Amazon Web Services requiere permisos y configuración

Para realizar flujos de trabajo de Image Portability Service con una cuenta de Amazon Web Services (AWS), la identidad de Administración de acceso e identidad (IAM) correspondiente debe tener los permisos correctos.

Para obtener la lista detallada, consulte Permisos necesarios de AWS.

### Configurar Image Portability Service

Para configurar Image Portability Service, debe hacer lo siguiente:

- Implementar Connector Appliances
- Preparar una máquina para PowerShell
- Agregar credenciales a Credential Wallet

#### Implementar Connector Appliances

Image Portability Service requiere dispositivos Citrix Connector para crear trabajos. Los Connector Appliances ayudan a proteger las interacciones con sus entornos locales y de nube pública. Los Connector Appliances se comunican de nuevo con Image Portability Service para informar sobre el estado del trabajo y el estado general del servicio.

Para implementar y configurar Connector Appliances en su entorno, siga los pasos que se indican en Connector Appliance para Cloud Services.

Tenga en cuenta la configuración de hardware y el acceso al puerto de red requeridos para el dispositivo cuando planifique la implementación.

Al implementar y registrar el dispositivo, los componentes necesarios para habilitar Image Portability se instalan automáticamente.

### Preparar una máquina para PowerShell

Para ayudarle a ponerse en marcha con Image Portability, hemos creado módulos de PowerShell que puede personalizar y usar con el servicio.

En las siguientes secciones, se describe cómo preparar una máquina para ejecutar los scripts de PowerShell. Estos scripts son solo algunos ejemplos. Modifíquelos para que se adapten a sus necesidades.

> **Nota:**
>
> Después de la instalación inicial, use **Update-Module** para actualizar el módulo de PowerShell.

**Requisitos de PowerShell** Para usar los scripts de PowerShell, necesita lo siguiente:

- Una máquina Windows para ejecutar los scripts de PowerShell que procesan los trabajos de portabilidad de imágenes. La máquina:
  - Cuenta con la versión más reciente de PowerShell.
  - Tiene una conexión de red de 10 Gbs o más al recurso compartido de archivos SMB local y una conexión rápida a la nube pública (por ejemplo, Azure, AWS o Google Cloud).
  - Puede ser la misma máquina que aloja el recurso compartido de archivos.
  - Es una máquina que ejecuta Windows 10, Windows Server 2019 o Windows Server 2022, con los últimos parches de Microsoft.
  - Se puede conectar a la Galería de Microsoft PowerShell para descargar las bibliotecas de PowerShell necesarias.

Según la versión de Windows, es posible que deba inhabilitar la compatibilidad con TLS 1.0/1.1. Para obtener más información, consulte la documentación sobre compatibilidad con TLS de la Galería de Microsoft PowerShell.

De forma predeterminada, PowerShell no se autentica automáticamente a través de un servidor proxy. Asegúrese de haber configurado la sesión de PowerShell para que use su servidor proxy, según las prácticas recomendadas de Microsoft y de su proveedor de proxy.

Si observa errores al ejecutar los scripts de PowerShell relacionados con una versión antigua o ausente de PowerShellGet, deberá instalar la versión más reciente de la siguiente manera:

```
Install-Module -Name PowerShellGet -Force -Scope CurrentUser -
    AllowClobber
<!--NeedCopy-->
```

**Instalar bibliotecas y módulos** Image Portability Service utiliza bibliotecas de la Galería de Microsoft PowerShell para procesar las operaciones de portabilidad.

> **Importante:**
>
> Después de la instalación inicial, use **Update-Module** para instalar nuevas versiones.

1. Ejecute el siguiente comando de PowerShell para descargar los módulos más recientes:

   ```
   Install-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
       Uploader" -Scope CurrentUser
   <!--NeedCopy-->
   ```

   - Para cambiar la variable de entorno PATH:

     Pulse **Y** e **Intro** para aceptar.

   - Para instalar el proveedor de NuGet:

     Pulse **Y** e **Intro** para aceptar.

   - Si se informa sobre un repositorio que no es de confianza:

     Pulse **A** (Sí a Todo) e **Intro** para continuar.

2. Ejecute el siguiente comando para confirmar que se descargaron todos los módulos necesarios:

   ```
   Get-InstalledModule -Name Citrix.*
   <!--NeedCopy-->
   ```

   Este comando devuelve un resultado similar al siguiente:

| Nombre | Repositorio | Descripción |
|---|---|---|
| Citrix.Image.Uploader | PSGallery | Comandos para cargar un VHD(x) en una cuenta de almacenamiento de Azure, AWS o GCP y obtener información sobre un VHD(x) |

| Nombre | Repositorio | Descripción |
| --- | --- | --- |
| Citrix.Workloads.Portability | PSGallery | Cmdlet independiente para el trabajo de imagen de Citrix Image Portability Service |

**Actualizar los módulos a la última versión** Ejecute el siguiente comando para actualizar el script a la última versión.

```
Update-Module -Name "Citrix.Workloads.Portability","Citrix.Image.
    Uploader" -Force
<!--NeedCopy-->
```

**Instalar el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops** Image Portability Service requiere el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops para crear y administrar trabajos de portabilidad en Citrix Cloud.

Descargue e instale el SDK de PowerShell remoto en su máquina.

**Instalar componentes de terceros específicos de la plataforma** El módulo PowerShell de Image Portability Service no instala dependencias de terceros. Por lo tanto, puede limitar la instalación solo a las plataformas a las que se dirige. Si utiliza una de las siguientes plataformas, siga las instrucciones correspondientes para la instalación de las dependencias de la plataforma:

**VMware** Si va a crear trabajos de Image Portability que se comuniquen con su entorno de VMware, ejecute el siguiente comando para instalar los módulos de PowerShell necesarios para VMware.

```
Install-Module -Name VMWare.PowerCLI -Scope CurrentUser -AllowClobber -
    Force -SkipPublisherCheck
<!--NeedCopy-->
```

**Amazon Web Services** Si piensa crear trabajos de portabilidad de imágenes en AWS, descargue e instale la interfaz de línea de comandos de AWS y, a continuación, ejecute estos comandos para instalar los módulos de PowerShell para AWS necesarios:

```
Install-Module -Name AWS.Tools.Installer
Install-AWSToolsModule AWS.Tools.EC2,AWS.Tools.S3
<!--NeedCopy-->
```

**Azure** Si va a crear trabajos de Image Portability en Azure, descargue e instale las utilidades de línea de comandos de Azure y, a continuación, ejecute estos comandos para instalar los módulos de PowerShell necesarios para Azure:

```
Install-Module -Name Az.Accounts -Scope CurrentUser -AllowClobber -
    Force
Install-Module -Name Az.Compute -Scope CurrentUser -AllowClobber -Force
<!--NeedCopy-->
```

**Google Cloud** Si va a crear trabajos de Image Portability en Google Cloud, descargue e instale el SDK de Google Cloud en su máquina.

**Desinstalar scripts y módulos** Ejecute los siguientes comandos para desinstalar los módulos que utiliza el software Image Portability.

> **Nota:**
>
> Los scripts y componentes de terceros no se eliminan automáticamente al desinstalar módulos IPS.

Para desinstalar módulos:

```
Get-InstalledModule -Name "Citrix.Workloads.Portability","Citrix.Images
    .Uploader" | Uninstall-Module
<!--NeedCopy-->
```

### Agregar credenciales a Credential Wallet

Para casos de automatización de extremo a extremo, puede configurar Image Portability Service de manera que se autentique de forma no interactiva con los recursos locales, de su nube pública y de Citrix Cloud. Además, Image Portability Service utiliza credenciales almacenadas en Citrix Credential Wallet cada vez que nuestras API se autentican directamente con sus recursos locales y en la nube pública. Establecer credenciales como se describe en esta sección es un paso obligatorio para ejecutar trabajos de exportación, preparación y publicación.

Al ejecutar trabajos, Image Portability Service requiere acceso a recursos que usted puede controlar. Por ejemplo, para que Image Portability Service exporte un disco desde un servidor de vSphere a un recurso compartido de SMB, el servicio necesita acceso de inicio de sesión a ambos sistemas. Para proteger esta información de cuenta, Image Portability Service utiliza el servicio Citrix Credential Wallet. Este servicio almacena sus credenciales en Wallet con un nombre definido por el usuario. Cuando quiera ejecutar un trabajo, proporcione el nombre de la credencial que se va a usar. Además, estas credenciales se pueden actualizar o eliminar de la cartera en cualquier momento.

A menudo, se almacenan credenciales para estas plataformas:

- Microsoft Azure
- AWS
- Google Cloud
- Recurso compartido de SMB
- VMware vSphere
- Nutanix AHV
- XenServer

Para administrar credenciales, consulte la sección Administración de credenciales y API de Image Portability Service del Portal de API para desarrolladores.

## Usar Image Portability Service

La preparación de imágenes en las ubicaciones de recursos locales en su suscripción a la nube pública requiere crear los trabajos de Image Portability en Citrix Cloud. Puede crear un trabajo para realizar llamadas de API directas al servicio dentro de su script o programa o con los módulos de PowerShell de ejemplo que hemos desarrollado para automatizar las llamadas de API. Consulte el Portal de API para desarrolladores de Image Portability Service para obtener información sobre el uso de API de REST y módulos de PowerShell para crear trabajos de IPS.

### Publicar catálogos de máquinas con Citrix Provisioning

Image Portability Service (IPS) se usa con Machine Creation Services (MCS) en Azure, AWS, Google Cloud, Nutanix, vSphere y XenServer, o con Citrix Provisioning (PVS) en Azure, Google Cloud, vSphere y XenServer. Puede combinar las soluciones de PowerShell y REST que se describen en esta guía con las herramientas de su plataforma, las API de su plataforma o los SDK de Citrix DaaS para crear un flujo de trabajo integral y automatizado para crear un catálogo de máquinas basado en la imagen preparada. Según la plataforma de la nube que elija, es posible que se requieran pasos intermedios entre la finalización de un trabajo de preparación de IPS y la creación de un catálogo o una tarea para un destino de PVS.

**AWS** Los trabajos de preparación de IPS en AWS producen un volumen. Machine Creation Services requiere una imagen de máquina de Amazon (AMI) durante la creación del catálogo. Para generar una AMI a partir de la imagen migrada, primero debe crear una instantánea de imagen a partir del volumen resultante y, a continuación, crear una AMI basada en esa instantánea. Esto se puede hacer con la interfaz de línea de comandos (CLI) de AWS:

```
1 > aws ec2 create-snapshot --volume-id <VolumeId>
2 > aws ec2 register-image --name <AmiName> --architecture 'x86_64' --
      root-device-name '/dev/sda1 --boot-mode uefi --ena-support --
```

```
    virtualization-type 'hvm' --block-device-mappings 'DeviceName=/dev/
    sda1,Ebs={
 SnapshotId=<SnapshotID> }
 '
<!--NeedCopy-->
```

<VolumeId> es el resultado del trabajo de preparación de IPS. La AMI resultante se puede utilizar como imagen maestra de MCS.

En el módulo Citrix.Workloads.Portability se proporciona un script de ejemplo de PowerShell para automatizar esta parte del flujo de trabajo como un script denominado `New-IpsAwsImage.ps1` .

**Azure** En Azure, IPS produce discos administrados que se pueden utilizar directamente como imágenes maestras de MCS. Para asignar la imagen resultante a los destinos de PVS, IPS proporciona una operación "publish"para copiar el disco administrado en un archivo VHD(x) de su almacén de PVS.

**Google Cloud** Los trabajos de preparación de IPS en Google Cloud producen un disco. MCS requiere una plantilla de instancias de Google Cloud. El proceso para crear una plantilla de instancias de MCS a partir de un disco se describe en detalle en Preparar la instancia de una VM maestra y un disco persistente.

Para los destinos de PVS en Google Cloud, IPS proporciona una operación "publish"para copiar el disco en un archivo VHD(x) de su almacén de PVS.

#### Automatizar la configuración de VDA

Al preparar una imagen administrada por Citrix originada localmente, puede reconfigurar el VDA dentro de la imagen para que admita el entorno de destino para el que se prepara la imagen. Image Portability Service puede aplicar cambios de configuración de VDA sobre la marcha durante la fase de preparación del flujo de trabajo. Los siguientes parámetros de configuración definen el funcionamiento del VDA en la imagen migrada: **InstallMisa**, **XdReconfigure** e **InstallMcsio**. Consulte los ejemplos de PowerShell de Image Portability Service para definir estos parámetros al crear trabajos de IPS.

#### Configuraciones

- Si se configura **InstallMisa** en **`true`**, Image Portability Service puede instalar cualquier componente del VDA que falte y que sea necesario para aprovisionar la imagen mediante MCS.
- Si se configura **InstallMisa** en **`true`** o **InstallMcsio** en **`true`** también es necesario configurar **CloudProvisioningType** en `Mcs`.

- Establezca **InstallPvs** en la versión del servidor PVS en la que se está implementando la imagen. Al establecer **InstallPvs**, Image Portability Service (IPS) instala automáticamente la versión especificada del software del dispositivo de destino PVS en la imagen durante los trabajos de preparación. IPS admite las dos compilaciones más recientes (versión base o actualizaciones acumulativas) para las dos últimas versiones Long Term Service Releases (LTSR) y Current Release (CR).

Tanto para **InstallMisa** como para **InstallMcsio**, tenga en cuenta lo siguiente:

- Estas funciones solo se admiten en las versiones LTSR y CR recientes del VDA.
- Si los componentes necesarios ya están presentes para el VDA instalado, no tienen lugar cambios, incluso si los parámetros están configurados.
- Para las versiones compatibles del VDA, Image Portability instala la versión adecuada de los componentes requeridos, incluso si los componentes necesarios del VDA no están presentes.
- Para las versiones no compatibles del VDA, se produce un error en la reconfiguración y se registra un mensaje si los componentes necesarios del VDA no están presentes. El trabajo de preparación se completa incluso si la reconfiguración del VDA no lo hace.

**XdReconfigure** requiere uno de los valores siguientes: `controllers` o `site_guid`. A continuación, se muestran ejemplos de parámetros de configuración que utilizan cada valor:

Uso de **controllers**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'controllers'
        ParameterValue = 'comma-separated-list-of-your-cloud-connectors
           -fqdns'
     }

)
<!--NeedCopy-->
```

donde **ParameterValue** es la lista de FQDN de los nuevos DDC a los que quiere apuntar con el VDA. Se pueden especificar varios DDC en formato separado por comas.

Uso de **site_guid**:

```
XdReconfigure = @(
    [pscustomobject]@{

        ParameterName = 'site_guid'
        ParameterValue = 'active-directory-site-guid'
     }

)
<!--NeedCopy-->
```

**XdReconfigure** también acepta valores admitidos al ejecutar el instalador de línea de comandos del VDA con el modificador de instalación **/reconfigure**, por ejemplo, **XenDesktopVdaSetup.exe /reconfigure**. Algunos ejemplos de estos valores incluyen **wem_agent_port**, **wem_cached_data_sync_port**, **wem_cloud_connectors** o **wem_server**. Para obtener una lista completa de las opciones de línea de comandos de reconfiguración de VDA, consulte la documentación sobre VDA de Citrix DaaS.

Configure **InstallMcsio** en `true` para instalar automáticamente MCSIO en la imagen. Para inhabilitar la instalación automática de MCSIO en la imagen, configure **InstallMcsio** en `false`.

> **Nota:**
>
> Puede utilizar `-DryRun` mientras ejecuta los comandos para validar la configuración y los parámetros de red del Connector Appliance.

## Referencia

En esta sección, se detalla la información de referencia técnica, en función de sus necesidades.

### Permisos requeridos por Image Portability Service

En esta sección se detallan los permisos requeridos por Image Portability Services en cada una de las plataformas locales y en la nube compatibles.

**Permisos necesarios para Connector Appliance** Connector Appliance necesita acceso a estas URL para preparar las imágenes en Image Portability Service:

```
api-ap-s.cloud.com
api-eu.cloud.com
api-us.cloud.com
credentialwallet.citrixworkspaceapi.net
graph.microsoft.com
login.microsoftonline.com
management.azure.com
*.blob.storage.azure.net
<!--NeedCopy-->
```

**Permisos requeridos para VMware vCenter** Los siguientes permisos de vCenter son necesarios para ejecutar el trabajo de disco de exportación de IPS en un entorno de VMware. Estos permisos se encuentran en **Roles**, en la sección sobre **control de acceso** del panel de administración de vCenter.

```
-  Cryptographic operations
    -  Direct Access

```

```
- Datastore
    - Allocate space
    - Browse datastore
    - Low level file operations
    - Remove file

- Folder
    - Create folder
    - Delete folder

- Network
    - Assign network

- Resource
    - Assign virtual machine to resource pool

- Virtual machine
    - Change Configuration
        - Add existing disk
        - Add new disk
        - Remove disk

    - Edit Inventory
        - Create from existing
        - Create new
        - Remove

    - Interaction
        - Power off
        - Power on
<!--NeedCopy-->
```

**Permisos requeridos para Microsoft Azure** Image Portability requiere que su cuenta de servicio de Azure tenga los siguientes permisos.

Cuando se especifica el grupo de recursos que se usará en el motor de composición (es decir, en la propiedad *resourceGroup* de una solicitud de REST o en el parámetro *-AzureVmResourceGroup* cuando se utilizan los comandos Citrix.Workloads.Portability de PowerShell), se requieren estos permisos en el ámbito del grupo de recursos.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/delete
Microsoft.Network/networkInterfaces/join/action
```

```
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/delete
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourcegroups/read
<!--NeedCopy-->
```

Si no se especifica el grupo de recursos que se usará en el motor de composición, se requieren estos permisos en el ámbito de la suscripción.

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/endGetAccess/action
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/virtualMachines/powerOff/action
Microsoft.Compute/virtualMachines/read
Microsoft.Compute/virtualMachines/write
Microsoft.Network/networkInterfaces/join/action
Microsoft.Network/networkInterfaces/read
Microsoft.Network/networkInterfaces/write
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/networkSecurityGroups/read
Microsoft.Network/networkSecurityGroups/write
Microsoft.Resources/deployments/operationStatuses/read
Microsoft.Resources/deployments/read
Microsoft.Resources/deployments/write
Microsoft.Resources/subscriptions/resourceGroups/delete
Microsoft.Resources/subscriptions/resourceGroups/write
Microsoft.Authorization/roleAssignments/read
Microsoft.Authorization/roleDefinitions/read
<!--NeedCopy-->
```

Se requieren estos permisos en el ámbito del grupo de recursos de destino especificado (es decir, el grupo de recursos especificado en la propiedad *targetDiskResourceGroupName* de una solicitud de REST o en el parámetro *-TargetResourceGroup* cuando se utiliza PowerShell).

```
Microsoft.Compute/disks/beginGetAccess/action
Microsoft.Compute/disks/delete
Microsoft.Compute/disks/read
Microsoft.Compute/disks/write
Microsoft.Compute/snapshots/delete
Microsoft.Compute/snapshots/read
Microsoft.Compute/snapshots/write
<!--NeedCopy-->
```

Se requieren estos permisos en el ámbito del grupo de recursos de la red virtual especificado (es decir, el grupo de recursos especificado en la propiedad *virtualNetworkResourceGroupName* de una so-

licitud de REST o en el parámetro *-AzureVirtualNetworkResourceGroupName* cuando se utiliza PowerShell).

```
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
<!--NeedCopy-->
```

> **Importante:**
>
> La opción `ceVmSku` de los trabajos "prepare"y "prepareAndPublish"controla el tipo de máquina virtual de Azure para la que es adecuado el disco administrado resultante. Debe seleccionar una ceVmSku con la misma familia y la misma versión que las máquinas virtuales que pretende aprovisionar a partir de la imagen de salida. El valor predeterminado de `Standard_D2S_v3` es adecuado para ejecutarse en todas las máquinas de la familia v3 D. No se admite la especificación de SKU de máquinas que no incluyan un disco temporal.

**Permisos requeridos para Google Cloud** Image Portability requiere que su cuenta de servicio de Google Cloud tenga los siguientes permisos:

```
cloudbuild.builds.create
cloudbuild.builds.get
cloudbuild.builds.list
compute.disks.create
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setLabels
compute.disks.use
compute.globalOperations.get
compute.images.create
compute.images.delete
compute.images.get
compute.images.list
compute.images.setLabels
compute.images.useReadOnly
compute.instances.create
compute.instances.delete
compute.instances.get
compute.instances.setLabels
compute.instances.setMetadata
compute.instances.setServiceAccount
compute.instances.setTags
compute.instances.stop
compute.instances.updateDisplayDevice
compute.networks.get
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zones.list
iam.serviceAccounts.actAs
```

```
iam.serviceAccounts.get
iam.serviceAccounts.list
resourcemanager.projects.get
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
<!--NeedCopy-->
```

**Permisos requeridos por AWS** La portabilidad de imágenes requiere adjuntar un documento de directiva JSON con esta configuración para el usuario de Administración de acceso e identidad (IAM):

```
{

    "Version": "2012-10-17",
    "Statement": [
        {

            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot",
                "ec2:CreateTags",
                "ec2:CreateImage",
                "ec2:DeleteSnapshot",
                "ec2:DeleteVolume",
                "ec2:DeregisterImage",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:RebootInstances",
                "ec2:RegisterImage",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
            ],
            "Effect": "Allow",
            "Resource": "*"
         }

    ]
 }

<!--NeedCopy-->
```

> **Nota:**
>
> Es posible que quiera reducir aún más el ámbito del recurso, según sus necesidades.

**Permisos necesarios para Nutanix AHV** Image Portability requiere que sea administrador de clústeres en su configuración de Nutanix AHV.

**Permisos requeridos de XenServer** Image Portability requiere que tenga como mínimo el rol de "administrador de VM"para el grupo en el que se encuentra el host de XenServer.

**Redes** Image Portability Service (IPS) crea una máquina virtual de trabajo denominada motor de composición (CE) para realizar operaciones de imagen. Todos los Connector Appliances de la ubicación de recursos asociada deben poder comunicarse a través de HTTPS con el CE.
El Connector Appliance (CA) inicia todas las comunicaciones entre el CA y el CE, con la única excepción en el caso de vSphere, en el que existe una comunicación HTTPS bidireccional entre el CE y el CA.

En entornos de nube (Azure, AWS, Google Cloud), el CE se crea con una dirección IP privada. Por lo tanto, el CE debe estar en la misma red virtual que el CA o en una red virtual a la que el CA pueda acceder.

Además, para los trabajos que implican archivos en un recurso compartido de SMB (por ejemplo, trabajos de exportación), el CE debe estar en una red con conectividad al recurso compartido de SMB.

Consulte la documentación de la API de Image Portability Service para obtener detalles sobre cómo especificar la red que se utilizará para el CE en cada plataforma compatible.

Para los trabajos "prepare", el sistema operativo que aparece en la imagen arranca (en el CE) para realizar tareas de especialización y otras tareas. Si la imagen contiene agentes de administración o seguridad que se comunican por teléfono con un servidor de control, estos procesos pueden interferir con el proceso de preparación.

Si se especifica la opción "unjoin"del dominio, la conectividad de red puede afectar a los resultados. Si la máquina virtual del motor de composición puede contactar con el controlador de dominio de Active Directory a través de la red, "unjoin"quita la cuenta de equipo del dominio. Esto interrumpe la pertenencia al dominio de la máquina virtual de origen de la que se extrajo la imagen.

Por lo tanto, se recomienda aislar la red proporcionada para la operación de otros recursos de la red. Esto se puede hacer mediante el aislamiento de subredes o con reglas de firewall. Para obtener información más detallada, consulte Aislamiento de red.

En algunos entornos de hipervisor locales, el hipervisor puede configurarse con un certificado de servidor TLS, que no es de confianza para el conjunto de entidades de certificación raíz del CA o no coincide con el nombre de host del servidor. Para estos casos, **IPS proporciona propiedades de solicitud de**

**trabajo** que sirven para solucionar el problema. Para obtener información más detallada, consulte Certificados TLS.

**Proxies de red** Si el tráfico de red entre el CA e Internet atraviesa un proxy que realiza introspección TLS, podría ser necesario agregar la entidad de certificación raíz del proxy (es decir, el certificado que el proxy usa para firmar los certificados TLS que genera) al conjunto de entidades de certificación raíz del CA. Para obtener más información, consulte Registrar el Connector Appliance en Citrix Cloud.

#### Aislamiento de red

- Azure

  En Azure, el CE se crea de forma predeterminada con un grupo de seguridad de red (NSG) conectado a su NIC si la entidad principal de servicio de Azure usada en la operación tiene los permisos de Azure necesarios [1].

  - Microsoft.Network/networkSecurityGroups/join/action
  - Microsoft.Network/networkSecurityGroups/read
  - Microsoft.Network/networkSecurityGroups/write

    En otro caso, los siguientes permisos en el ámbito de la suscripción si no se usa ningún grupo de recursos explícito:

    * Microsoft.Network/networkSecurityGroups/delete
    * Microsoft.Network/networkSecurityGroups/join/action
    * Microsoft.Network/networkSecurityGroups/read
    * Microsoft.Network/networkSecurityGroups/write

  Este NSG está configurado para bloquear todo el tráfico de entrada/salida del CE, excepto:

  - SMB (puerto 445) saliente
  - HTTPS (puerto 443) entrante
  - el que se requiere para los servicios internos de Azure

  El uso del NSG se puede forzar estableciendo la propiedad *networkIsolation* de la solicitud de trabajo en *true*. En este caso, el trabajo falla si la entidad principal de servicio usada en la operación no tiene los permisos necesarios. El uso del NSG se puede inhabilitar estableciendo la propiedad *networkIsolation* en *false*.

- AWS

En AWS, para lograr el aislamiento de red del CE, puede crear uno o varios grupos de seguridad de red que bloqueen todo el tráfico no deseado y, a continuación, en la solicitud de trabajo, asignar los

grupos de seguridad a la instancia de CE mediante el parámetro de solicitud *securityGroupIds*, que toma como valor una lista de identificadores de grupos de seguridad.

- Google Cloud

En Google Cloud, para lograr el aislamiento de red del CE, puede crear reglas de firewall que bloqueen todo el tráfico no deseado y, a continuación, aplicarlas al CE mediante etiquetas de red. IPS crea el CE con la etiqueta de red *compositing-engine* y puede asignarle otras etiquetas de red mediante el parámetro de solicitud de trabajo *networkTags*, que toma una lista de etiquetas como valor.

**Certificados TLS** Si el certificado del servidor del hipervisor está firmado por una entidad en la que el CA no confía, se pueden seguir dos enfoques alternativos para resolver el problema.

1. Especificar en la solicitud de trabajo un certificado de entidad de certificación raíz adicional para usarlo en la verificación del certificado. Este certificado debe ser la entidad de certificación raíz usada para firmar el certificado del servidor del hipervisor.
2. Especificar en la solicitud de trabajo la huella digital SHA-1 del certificado del servidor del hipervisor. En este caso, la validación del certificado se realiza verificando que la huella digital SHA-1 del certificado devuelto por el hipervisor coincide con la proporcionada en la solicitud de trabajo. Es posible que este método no funcione si hay un proxy de interceptación de TLS entre el CE y el hipervisor.

Los parámetros de las solicitud de trabajo para lo anterior, que se indican respectivamente a continuación para cada plataforma, son:

- vSphere
    1. vCenterSslCaCertificate
    2. vCenterSslFingerprint
- Nutanix
    1. prismSslCaCertificate
    2. prismSslFingerprint
- XenServer
    1. xenSslCaCertificate
    2. xenSslFingerprint

Consulte la documentación de la API de Image Portability Service para obtener información más detallada.

Los errores de validación de certificados también pueden producirse cuando no coinciden el nombre de host del servidor del hipervisor y el nombre de host del certificado. En este caso, la coincidencia

del nombre de host se puede inhabilitar configurando el siguiente parámetro en *true* en la solicitud de trabajo:

- vSphere
  - vCenterSslNoCheckHostname
- Nutanix
  - prismSslNoCheckHostname
- XenServer
  - xenSslNoCheckHostname

### Documentación relacionada

- Documentación de la API de Image Portability Service
- Connector Appliance para Cloud Services
- Documentación de Google Cloud
- Cuentas de servicio de Google Cloud
- Registro y autenticación de aplicaciones de Microsoft Azure

1. If se utiliza un grupo de recursos explícito para la operación y después los siguientes permisos en el ámbito del grupo de recursos: 

## Imprimir

April 14, 2022

La administración de impresoras en el entorno es un proceso compuesto por varias fases:

1. Familiarización con los conceptos de impresión, en el caso de que no se haya hecho ya.
2. Planificación de la arquitectura de impresión. Esto incluye analizar las necesidades del negocio, la infraestructura existente de impresión, la interacción entre usuarios y aplicaciones con la impresión hoy día y el modelo de administración de impresión que mejor se ajusta al entorno.
3. Configuración del entorno de impresión al seleccionar un método de aprovisionamiento de impresoras y, a continuación, crear directivas para implementar el diseño de impresión. Actualización de directivas cuando se agreguen empleados o servidores nuevos.
4. Prueba de una instalación de configuración piloto de impresión antes de implementarla a los usuarios.

5. Mantenimiento del entorno de impresión Citrix mediante la administración de controladores de impresora y la optimización del rendimiento de impresión.
6. Solución de los problemas que puedan surgir.

Para obtener información completa sobre la impresión en un entorno de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), puede empezar con Imprimir. Desde ese artículo, puede ir a:

- Ejemplos de configuración de la impresión
- Prácticas recomendadas
- Directivas y preferencias de impresión
- Aprovisionar impresoras
- Mantener el entorno de impresión

### Instalar Universal Print Server en los servidores de impresión

1. Cada servidor de impresión debe tener instalado Microsoft Virtual C++ Runtime 2017, de 32 bits y 64 bits.
2. Vaya a la página de descarga de Citrix Universal Print Server y haga clic en **Download File**.
3. Ejecute alguno de los siguientes comandos en cada servidor de impresión:
    - Para un sistema operativo de 32 bits: **UpsServer_x86.msi**.
    - Para un sistema operativo de 64 bits: **UpsServer_x64.msi**.

Después de instalar Universal Print Server, configúrelo siguiendo las instrucciones de Aprovisionar impresoras.

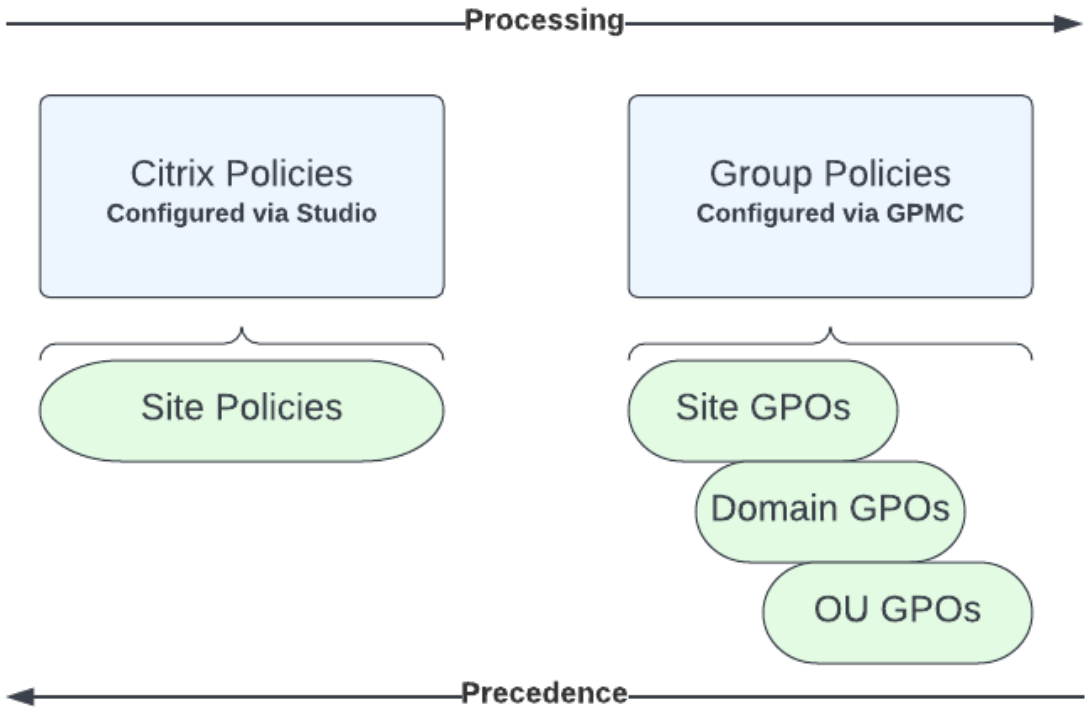
## Directivas

April 12, 2023

Las directivas son un conjunto de configuraciones que definen la forma en que se administran las sesiones, el ancho de banda y la seguridad para un grupo de usuarios, dispositivos o tipos de conexión.

Puede aplicar configuraciones de directiva a VDA o a los usuarios. Puede modificar las configuraciones en Web Studio o en los objetos de directiva de grupo (GPO) de Active Directory. Puede especificar filtros (asignaciones de objetos) para las . Si no asigna específicamente directivas a filtros, la configuración se aplica a todas las sesiones de usuario.




Puede aplicar las directivas en diferentes niveles de la red. Las configuraciones de directiva colocadas en el nivel de objeto de directiva de grupo (GPO) de unidad organizativa (OU) tienen precedencia en la red. Las directivas en el nivel de grupo GPO del dominio anulan las directivas de GPO del sitio. Las directivas en el nivel de GPO del sitio, a su vez, anulan las directivas en conflicto que haya en los niveles de directivas locales de Citrix y de Microsoft.

Todas las directivas locales de Citrix se crean y administran desde la consola de Citrix Studio y se almacenan en la base de datos de configuración del sitio. Las directivas de grupo se crean y administran mediante la consola Microsoft Management Console (GPMC) y se almacenan en Active Directory. Las Directivas locales de Microsoft se crean en el sistema operativo y se guardan en el Registro de Windows.

Web Studio usa un asistente de Modelado para ayudar a los administradores a comparar los parámetros de configuración incluidos en las plantillas y las directivas, de modo que puedan eliminar parámetros redundantes o conflictivos.

Las configuraciones se fusionan según su condición y prioridad. Una configuración inhabilitada anula una configuración habilitada de menor prioridad. Las configuraciones de directiva sin definir se omiten y no supeditan las configuraciones de menor rango.

Las directivas de Web Studio también pueden tener conflictos con directivas de grupo en Active Directory, lo que podría invalidarlas mutuamente, dependiendo de la situación.

Todas las directivas se procesan en el orden siguiente:

1. Desde la aplicación Citrix Workspace, el usuario final inicia sesión en un VDA con las credenciales de dominio.
2. Las directivas de Citrix se procesan para el usuario final y para el VDA.
3. Las directivas se aplican en el siguiente orden:
    a) Directivas locales
    b) Directivas de sitio
    c) Directivas de dominio
    d) Directivas de unidad organizativa

> **Nota:**
>
> - Es posible que no todas las directivas estén presentes en los cuatro niveles. Para la mayoría de los clientes, solo se utilizan las directivas del sitio. Las directivas locales requieren que el usuario inicie sesión en el VDA para modificarlas. Por lo tanto, estas directivas casi nunca se utilizan.
> - No se admite la combinación de directivas de Windows y Citrix en el mismo objeto de directiva de grupo.

Para obtener información detallada sobre las directivas de Citrix, consulte lo siguiente:

- Trabajar con directivas
- Plantillas de directiva
- Crear directivas
- Priorizar, modelar, comparar y solucionar problemas de directivas
- Configuraciones predeterminadas de directivas
- Referencia para configuraciones de directivas

  > **Nota:**
  >
  > Las referencias a la configuración de directivas de Citrix DaaS son las mismas que las de Citrix Virtual Apps and Desktops. Por lo tanto, también puede consultar la sección Referencia de configuración de directiva de la documentación de Citrix Virtual Apps and Desktops para Citrix DaaS.

## Trabajar con directivas

May 23, 2023

Configure directivas de Citrix para controlar el acceso de los usuarios y los entornos de sesión. Las directivas de Citrix son el método más eficaz para controlar los parámetros de conexión, seguridad y ancho de banda. Puede crear directivas para grupos de usuarios, dispositivos o tipos de conexión específicos. Cada directiva puede contener varias configuraciones.

### Herramientas para trabajar con las directivas de Citrix

- Studio –Las directivas que se crean con Studio se almacenan en la base de datos del sitio y las actualizaciones se envían al VDA en cualquiera de las siguientes situaciones:
  - Cuando ese VDA se registra en el Controller
  - Cuando un usuario inicia una sesión
- Consola de administración de directivas de grupo: Si su entorno de red utiliza Active Directory y usted tiene permisos para administrar las directivas de grupo, puede usar la Consola de administración de directivas de grupo (GPMC) para crear y modificar directivas para su sitio. En la consola, puede configurar los objetos de directiva de grupo (GPO) con los parámetros y los filtros que quiera. Estas directivas tendrán prioridad sobre las directivas configuradas en Studio. Para obtener más información, consulte CTX238166.

### Procesamiento de directivas y precedencia

Las configuraciones de directiva de grupo se procesan en el orden siguiente:

1. Objeto de directiva de grupo (GPO) del sitio Citrix DaaS (almacenado en la base de datos del sitio)
2. GPO de dominio
3. Unidades organizativas

Sin embargo, si se aplican diferentes configuraciones a la misma directiva en dos GPO, la configuración de la directiva procesada en último lugar sobrescribe la procesada anteriormente. Esto significa que las configuraciones de directiva toman precedencia en el orden siguiente:

1. Unidades organizativas
2. GPO de dominio
3. Objeto de directiva de grupo (GPO) del sitio Citrix DaaS (almacenado en la base de datos del sitio)

Cuando se utilizan varias directivas, puede priorizar las que contienen configuraciones conflictivas. Para obtener más información, consulte Priorizar, modelar, comparar y solucionar problemas de directivas.

### Flujo de trabajo para las directivas de Citrix

El proceso para la configuración de directivas es el siguiente:

1. Cree la directiva.
2. Configure los parámetros de la configuración de directiva.
3. Asigne la directiva a los objetos de usuario y máquina.
4. Dé una prioridad a la directiva.
5. Compruebe que la directiva funciona ejecutando el asistente de Modelado de Directivas de grupo de Citrix.

   > **Nota:**
   >
   > Para abrir el asistente de modelado de Directivas de grupo Citrix, vaya a la ficha **Directivas > Modelado** y, a continuación, haga clic en **Iniciar Asistente de modelado** en el panel **Acciones**. La ficha **Modelado** no está disponible en las instancias de Web Studio alojadas en Citrix Cloud a petición del cliente.

### Explorar las directivas y las configuraciones de Citrix

Las configuraciones de directiva se ordenan en categorías según la funcionalidad o la característica a la que afectan. Por ejemplo, la sección Profile Management incluye las configuraciones de directiva de Profile Management.

- Las configuraciones de equipo (configuraciones de directiva que se aplican a las máquinas) definen el comportamiento de los escritorios virtuales y se aplican cuando se inicia un escritorio virtual. Estas configuraciones se aplican incluso cuando no hay sesiones de usuario activas en el escritorio virtual.
- Las configuraciones de usuario definen la experiencia del usuario. Las configuraciones de usuario se aplican cuando un usuario se conecta o se vuelve a conectar

Para acceder a las directivas, sus configuraciones y plantillas, seleccione **Directivas** en el panel de navegación de Web Studio.

- La ficha **Directivas** muestra todas las directivas. Al seleccionar una directiva, las fichas en la parte inferior muestran lo siguiente:
  - Resumen: Muestra el nombre, prioridad, estado habilitado/inhabilitado y descripción
  - Parámetros: Muestra todos los parámetros configurados
  - Asignado a: Muestra el grupo de entrega. Puede modificar o eliminar las configuraciones asignadas. Aplicar directiva según el grupo de entrega al que pertenezca al escritorio que ejecuta la sesión. Para obtener más información, consulte Creación de directivas.

- La ficha **Plantillas** enumera las plantillas suministradas por Citrix y las plantillas que usted haya creado. Al seleccionar una plantilla, las fichas de la parte inferior muestran lo siguiente:
  - Descripción (por qué le podría interesar utilizar la plantilla)
  - Parámetros (lista de parámetros configurados). Para obtener más información, consulte Plantillas de directiva.
  - La ficha **Comparación** permite comparar las configuraciones de una directiva o de una plantilla con las de otras directivas o plantillas. Por ejemplo, puede que quiera verificar los valores de configuración para asegurar que se cumplen las directrices recomendadas. Para obtener más información, consulte Priorizar, modelar, comparar y solucionar problemas de directivas.
  - En la ficha **Modelado**, puede simular escenarios de conexión con directivas de Citrix. Para obtener más información, consulte Priorizar, modelar, comparar y solucionar problemas de directivas.

  Para buscar una configuración dentro de una directiva o una plantilla:

  1. Seleccione la directiva o la plantilla.
  2. Seleccione la ficha **Modificar directiva** o **Modificar plantilla**.
  3. En la página **Seleccionar configuraciones**, comience a escribir el nombre de la configuración.

  Puede refinar la búsqueda si selecciona:

  - Una categoría (por ejemplo, Ancho de banda)
  - La casilla de verificación **Ver solo seleccionadas**
  - Para buscar solo las configuraciones que se han agregado a la directiva seleccionada.

- Para buscar una configuración dentro de una directiva:

  1. Seleccione la directiva.
  2. Seleccione la ficha **Configuraciones** y comience a escribir el nombre de la configuración.

Una vez creada, una directiva es independiente de la plantilla utilizada. Puede usar el campo **Descripción** de una nueva directiva para realizar un rastreo de la plantilla de origen utilizada.

## Plantillas de directiva

November 17, 2022

Las plantillas son un punto de partida para la creación de directivas a partir de opciones iniciales predefinidas. Las plantillas integradas de Citrix, optimizadas para condiciones de red o entornos específicos, se pueden utilizar como:

- Un borrador para crear unas directivas y plantillas propias que se compartirán entre diferentes sitios.
- Una referencia para una comparación más fácil de los resultados entre las implementaciones, ya que puede citar los resultados; por ejemplo, "[…] cuando se usa la plantilla X o Y de Citrix […]".
- Método para comunicar directivas a Citrix Support o a terceros de confianza. Puede hacerlo importando o exportando plantillas.

### Plantillas integradas de Citrix

Están disponibles las siguientes plantillas de directiva:

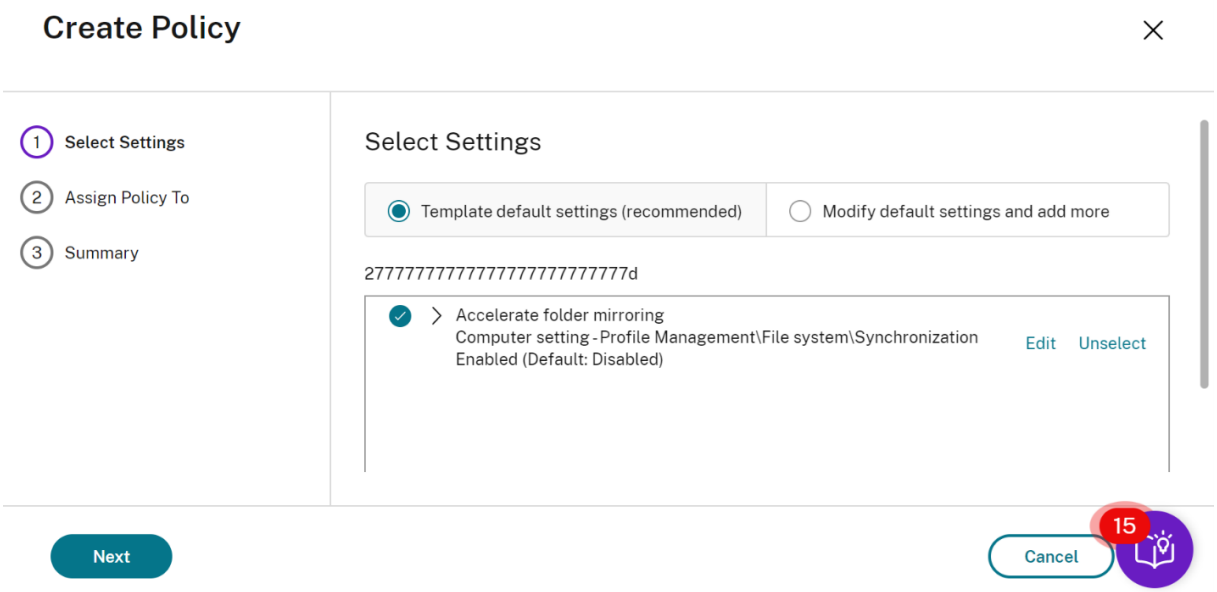
- **Experiencia de usuario de muy alta definición**. Con esta plantilla, se aplica la configuración predeterminada que optimiza la experiencia de usuario. Use esta plantilla en situaciones donde se procesan varias directivas por orden de prioridad.
- **Alta escalabilidad de servidores**. Aplique esta plantilla para ahorrar recursos de servidor. Esta plantilla equilibra la experiencia del usuario y la capacidad de escalabilidad del servidor. Ofrece una buena experiencia de usuario al mismo tiempo que aumenta la cantidad de usuarios que se pueden alojar en un solo servidor. Esta plantilla no usa ningún códec de vídeo para la compresión de gráficos e impide la generación multimedia de contenido en el lado del servidor.
- **Alta escalabilidad de servidores - SO antiguos**. Esta plantilla de alta escalabilidad de servidores se aplica solo a los agentes VDA con Windows Server 2008 R2 o Windows 7 y versiones anteriores. Esta plantilla se basa en el modo de gráficos antiguo, que es más eficaz para esos sistemas operativos.
- **Optimizado para NetScaler SD-WAN.** Aplique esta plantilla para optimizar la entrega de Citrix Virtual Desktops a los usuarios que trabajan en sucursales con NetScaler SD-WAN implementado. (NetScaler SD-WAN es el nuevo nombre de CloudBridge.)
- **Optimizado para WAN**. Esta plantilla está destinada a los empleados de las sucursales que utilizan una WAN compartida o a las ubicaciones remotas con conexiones de poco ancho de banda. Los trabajadores acceden a las aplicaciones con interfaces gráficas de usuario sencillas y poco contenido multimedia. Esta plantilla intercambia la experiencia de reproducción de vídeos y parte de la escalabilidad de los servidores por una eficiencia optimizada del ancho de banda.
- **Optimizado para WAN - SO antiguos**. Esta plantilla de se aplica solo a los agentes VDA con Windows Server 2008 R2 o Windows 7 y versiones anteriores. Esta plantilla se basa en el modo de gráficos antiguo, que es más eficaz para esos sistemas operativos.
- **Seguridad y control**. Use esta plantilla en entornos con poca tolerancia a fallos para minimizar las funciones habilitadas de forma predeterminada en Citrix DaaS. Esta plantilla incluye configuraciones que inhabilitan el acceso a lo siguiente:

- Impresión
- Portapapeles
- Dispositivos periféricos
- Asignación de unidades
- Redirección de puertos
- Aceleración de Flash en dispositivos de usuario

Aplicar esta plantilla puede usar más ancho de banda y reducir la densidad de usuarios por servidor.

Aunque se recomienda usar las plantillas integradas de Citrix con la configuración predeterminada, hay opciones que no tienen ningún valor concreto recomendado. Por ejemplo, el **límite de ancho de banda global de la sesión**, incluido en las plantillas de optimización de redes WAN. En este caso, en la plantilla se ofrece la opción de configuración para que el administrador entienda que esta opción se puede aplicar.




Tenga en cuenta que trabaja con una implementación (administración de directivas y agentes VDA) anterior a XenApp y XenDesktop 7.6 FP3. Además, requiere alta escalabilidad de servidores y plantillas optimizadas para WAN. En este caso, utilice las versiones de estas plantillas del sistema operativo antiguo cuando proceda.

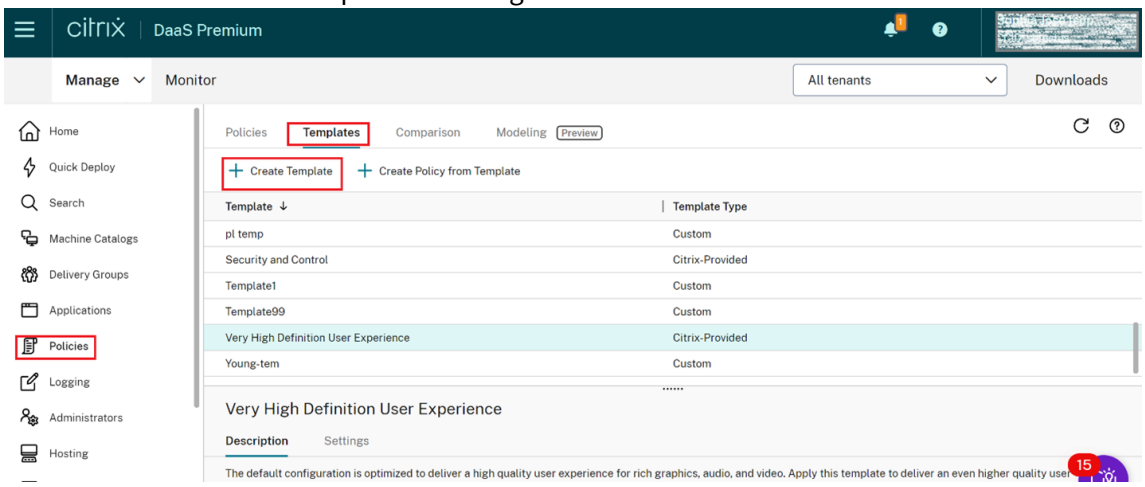
> **Nota:**
>
> Citrix crea y actualiza las plantillas integradas. No se puede modificar ni eliminar estas plantillas.

### Crear y administrar plantillas con Web Studio

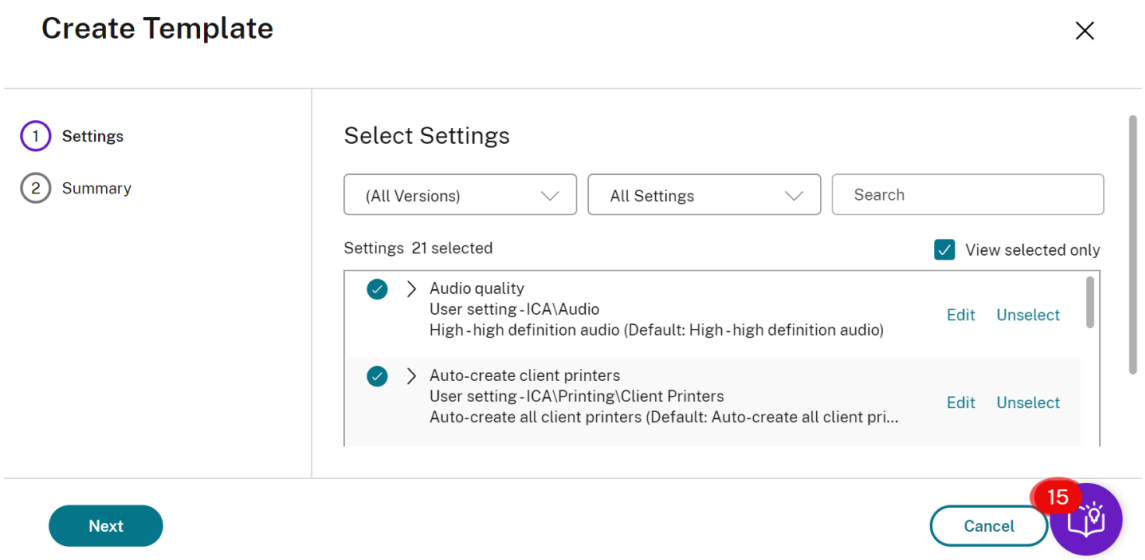
Para crear una plantilla basada, a su vez, en una plantilla:

1. Seleccione **Directivas** en el panel de navegación de Web Studio.




2. Haga clic en la ficha **Plantillas** y seleccione la plantilla a partir de la cual crea otra.
3. Seleccione la ficha **Crear plantilla**. Aparecerá la pantalla **Seleccionar configuraciones**.

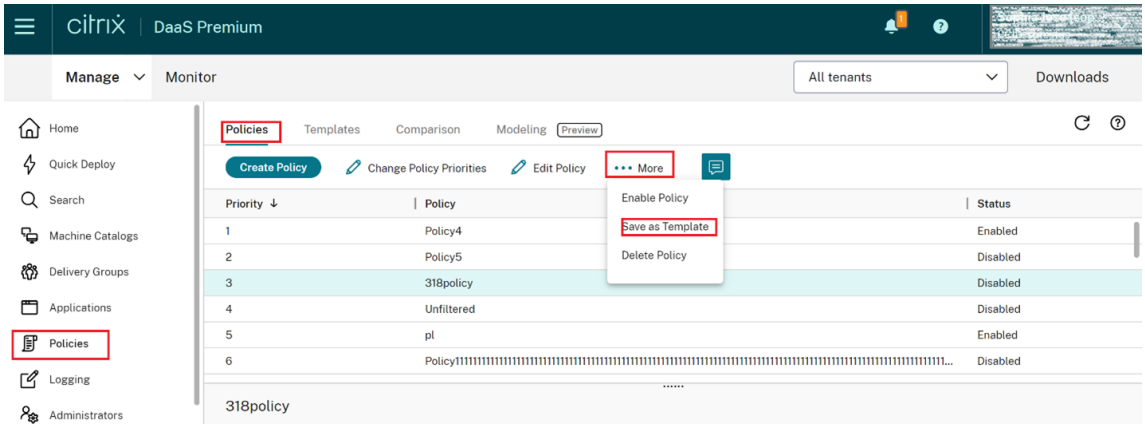



4. Seleccione y configure las configuraciones de directiva que desea incluir en la plantilla.
5. Haga clic en **Siguiente**. Aparecerá la pantalla **Resumen** .
6. Introduzca un nombre para la plantilla.
7. Haga clic en **Finalizar**. La nueva plantilla aparece en la ficha Plantillas.

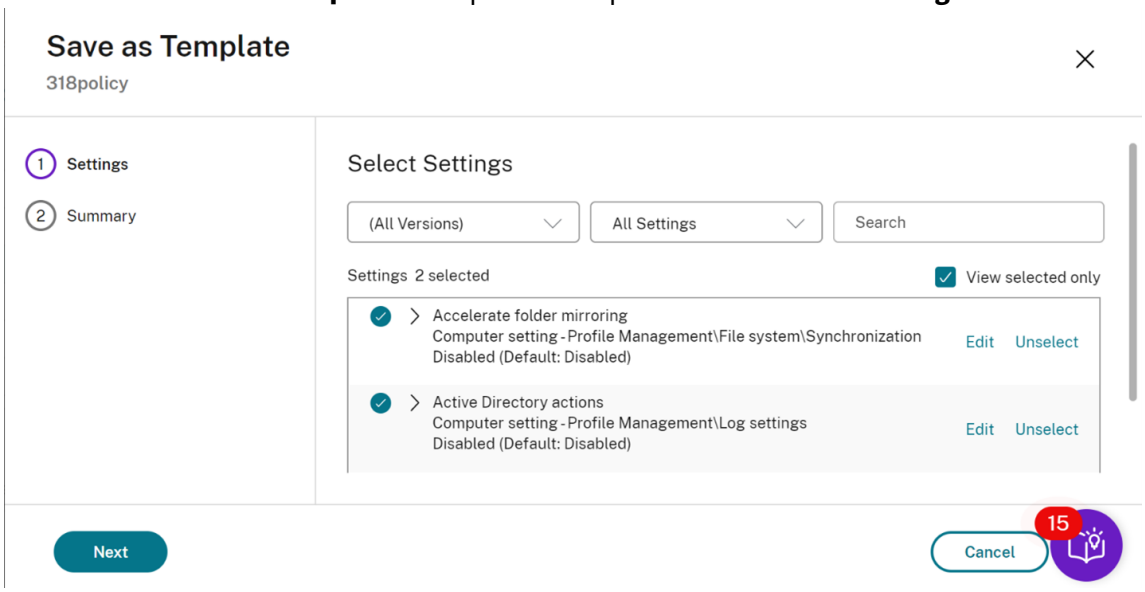
**Para crear una plantilla basada en una directiva**:

1. Seleccione **Directivas** en el panel de navegación de Web Studio.
2. Haga clic en la ficha **Directivas** y seleccione la directiva a partir de la cual crea la plantilla.

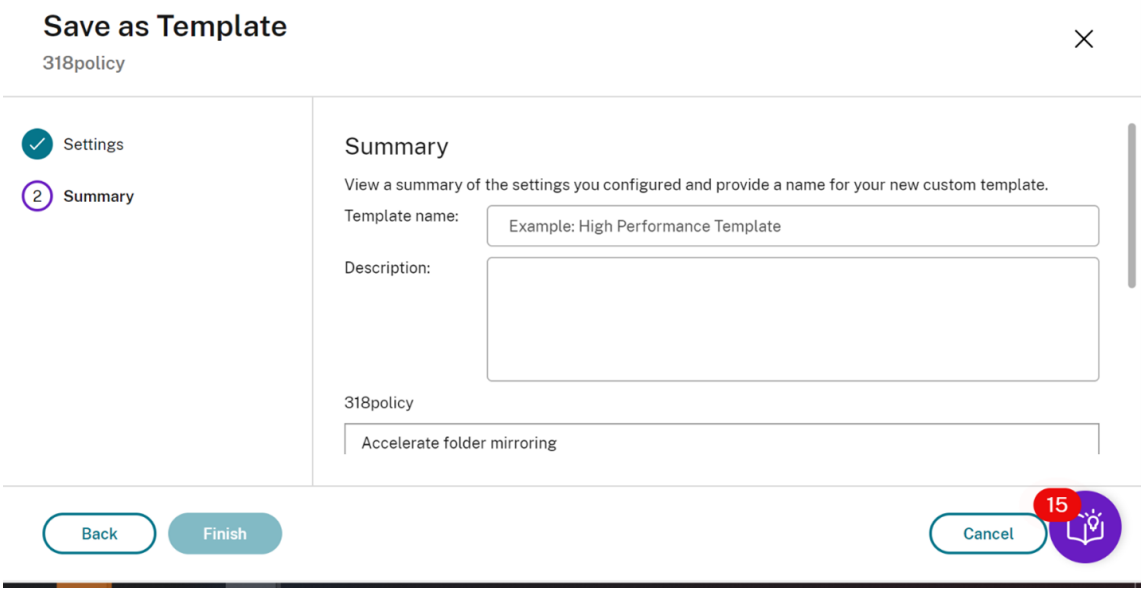



3. Haga clic en la ficha **Más**.
4. Seleccione **Guardar como plantilla**. Aparecerá la pantalla **Seleccionar configuraciones**.




5. Seleccione y defina las configuraciones de directiva que desea incluir en la plantilla.
6. Haga clic en **Siguiente**. Aparecerá la pantalla **Resumen** .




7. Introduzca un nombre y una descripción para la nueva plantilla y haga clic en **Finalizar**.

## Crear directivas

October 30, 2023

Antes de crear una directiva, decida a qué grupo de usuarios o dispositivos puede afectar. Puede crear una directiva según las funciones laborales del usuario, el tipo de conexión, el dispositivo de usuario o la ubicación geográfica.

Si ya creó una directiva aplicable a un grupo, considere la posibilidad de modificar dicha directiva, en lugar de crear otra directiva nueva. Después de modificar la directiva, configure los parámetros correspondientes. Evite la creación de una directiva exclusivamente para habilitar una configuración específica o para excluir la aplicación de la directiva a determinados usuarios.

Al crear una directiva, puede basarla en las configuraciones de una plantilla de directiva y personalizarlas según sea necesario. También puede crearla sin usar una plantilla y agregar las configuraciones que necesite.

En Citrix Studio, las nuevas directivas creadas se establecen como inhabilitadas a menos que se marque explícitamente la casilla **Habilitar directiva**.

Durante la creación de directivas y al configurar los parámetros, el sistema ofrece una opción para ver el tipo de parámetros. Puede ver los siguientes tipos de parámetros:

- Todos los parámetros: Ver todos los parámetros de todas las versiones de VDA
- Solo parámetros actuales: Ver solo los parámetros de las versiones actuales de VDA

- Solo parámetros antiguos: Ver solo los parámetros de las versiones retiradas de VDA

Para ver los parámetros mientras los configura:

1. Inicie sesión en DaaS Premium.
2. En el menú de navegación de la izquierda, haga clic en **Directivas**.
3. En la ficha **Directivas**, haga clic en **Crear directiva**.
4. En la tabla **Seleccionar configuraciones**, haga clic en el menú desplegable situado junto a **Parámetros**.
5. Seleccione una de las siguientes opciones del menú desplegable:
    - Todos los parámetros: Ver todos los parámetros de todas las versiones de VDA
    - Solo parámetros actuales: Ver solo los parámetros de las versiones actuales de VDA
    - Solo parámetros antiguos: Ver solo los parámetros de las versiones retiradas de VDA
6. La tabla Parámetros muestra los parámetros disponibles en función del paso anterior.

## Configuraciones de directivas

Las configuraciones de directiva pueden estar habilitadas, inhabilitadas o sin configurar. De forma predeterminada, las configuraciones de directiva no están definidas; es decir, que no están agregadas a una directiva. La configuración solamente puede aplicarse cuando se agrega a una directiva.

Al configurar los parámetros para crear o modificar una directiva, si todos los grupos de entrega están inhabilitados, el sistema muestra una señal de notificación de advertencia de que **ninguno de los elementos de este filtro está habilitado**. Si hay al menos un grupo de entrega habilitado, el sistema no muestra la señal de advertencia.

Para ver la advertencia al crear una directiva:

1. Inicie sesión en DaaS Premium.
2. En el menú de navegación de la izquierda, haga clic en **Directivas**.
3. En la ficha **Directivas**, haga clic en **Crear directiva**.
4. En la tabla **Seleccionar configuraciones**, seleccione cualquier configuración y haga clic en **Siguiente**.
5. En la tabla **Asignar directiva a**, seleccione un filtro del menú desplegable.
6. Desmarque la casilla **Habilitar** y haga clic en **Guardar**.

> **Nota:**
>
> No todos los filtros permiten desmarcar la casilla **Habilitar**.
> En la tabla **Filtros**, el filtro muestra la advertencia.

Para ver la advertencia al modificar una directiva:

1. Inicie sesión en DaaS Premium.
2. En el menú de navegación de la izquierda, haga clic en **Directivas**.
3. En la ficha **Directivas**, seleccione cualquiera de las directivas de la lista y haga clic en **Modificar directiva**.
4. En la página **Modificar directiva**, haga clic en **Asignar directiva a** en el menú de navegación de la izquierda.
5. En la tabla **Filtro**, seleccione o haga clic en **Modificar** para el filtro requerido:
   - Si un filtro no tiene el botón **Modificar**, seleccione el filtro.
   - Si un filtro tiene el botón de modificación, haga clic en **Modificar**.
6. Desmarque la opción **Habilitar** y haga clic en **Guardar**.

> **Nota:**
>
> No todos los filtros permiten desmarcar la casilla **Habilitar**.
> En la tabla **Filtros**, el filtro muestra la advertencia.

Algunas configuraciones de directiva pueden tener uno de los siguientes estados:

```
1 - Allowed or Prohibited allows or prevents the action controlled by
    the setting. Sometimes users are allowed or prevented from managing
    the setting's action in a session. For example, if the menu
    animation setting is set to Allowed, users can control menu
    animations in their client environment
2 - Enabled or Disabled turns the setting on or off. If you disable a
    setting, it is not enabled in lower-ranked policies.
```

Asimismo, algunas configuraciones controlan la eficacia de otras configuraciones dependientes. Por ejemplo: la configuración Redirección de unidades del cliente controla si los usuarios pueden acceder a las unidades de sus dispositivos. Para permitir que los usuarios accedan a sus unidades de red, es necesario agregar tanto esta configuración como la configuración **Unidades de red del cliente** a la directiva. Si la configuración **Redirección de unidades del cliente** está inhabilitada, los usuarios no pueden acceder a sus unidades de red aunque la configuración **Unidades de red del cliente** esté habilitada.

En general, los cambios de configuraciones de directiva que afectan a máquinas surten efecto cuando se reinicia el escritorio virtual o cuando un usuario inicia una sesión. Los cambios de configuraciones de directiva que afectan a usuarios surten efecto la próxima vez que el usuario inicia una sesión.

Para algunas configuraciones de directiva, puede especificar o seleccionar un valor cuando se las agrega a una directiva. Puede limitar la configuración del parámetro si selecciona Usar el valor predeterminado. Esta selección impide configurar el parámetro y permite usar solo el valor predetermi-

nado al aplicar la directiva. Esta selección es independiente del valor que se haya introducido antes de seleccionar Usar valor predeterminado.

Recomendaciones:

- Asigne las directivas a grupos y no a usuarios individuales. Si asigna directivas a un grupo, las asignaciones se actualizan automáticamente cuando se agregan o se quitan usuarios.
- Inhabilite las directivas que no use. Las directivas sin configuración generan una actividad de procesamiento innecesaria.

### Asignaciones de directiva

Al crear una directiva, se asigna a determinados objetos de usuario y máquina. Esa directiva se aplica a las conexiones según criterios o reglas específicos. Por lo general, es posible agregar tantas asignaciones como se desee a una directiva, según una combinación de criterios. Si no se especifica ninguna asignación, la directiva se aplica a todas las conexiones.

Si no especifica ninguna asignación o especifica asignaciones, pero las inhabilita, la directiva se aplica a **todas** las conexiones.

> **Nota:**
>
> Las asignaciones de directivas también se conocen como filtros de directivas. Para obtener información adicional, consulte los siguientes temas:
>
> - Crear, modificar o eliminar un filtro para una directiva
> - ¿Cómo se aplican los filtros?

En la siguiente tabla se muestran las asignaciones disponibles:

| Nombre de asignación | Aplica una directiva según |
|---|---|
| Control de acceso | Condiciones de control de acceso del cliente. *Tipo de conexión*: Si se debe aplicar la directiva a las conexiones realizadas con o sin NetScaler Gateway. *Nombre de la comunidad de NetScaler Gateway*: Nombre del servidor virtual de NetScaler Gateway. *Condición de acceso*: Nombre de la directiva de análisis o de la directiva de sesión que se va a usar en el dispositivo de punto final. |

| Nombre de asignación | Aplica una directiva según |
|---|---|
| Citrix SD-WAN | Si se inicia una sesión de usuario a través de Citrix SD-WAN. **Nota:** Puede agregar solo una asignación de Citrix SD-WAN a una directiva. |
| Dirección IP del cliente | Dirección IP del dispositivo del usuario, utilizado para conectarse a la sesión. Ejemplos de IPv4: 12.0.0.0, 12.0.0.*, 12.0.0.1-12.0.0.70, 12.0.0.1/24. Ejemplos de IPv6: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54 |
| Nombre del cliente | Nombre del dispositivo de usuario. Coincidencia exacta: ClientABCName. Uso de comodines: Client*Name. |
| Grupo de entrega | Pertenencia a un grupo de entrega. |
| Tipo de grupo de entrega | Tipo de escritorio o aplicación: escritorio privado, escritorio compartido, aplicación privada o aplicación compartida. |
| Unidad organizativa (UO) | Unidad organizativa. |
| Etiqueta | Etiquetas. **Nota:** Aplique esta directiva a todas las máquinas etiquetadas. Las etiquetas de aplicación no están incluidas. |
| Usuario o grupo | Nombre de usuario o grupo. |

Cuando un usuario inicia sesión, se identifican todas las directivas que coinciden con las asignaciones para la conexión. Las directivas se ordenan por prioridad y se comparan varias instancias de cualquier configuración. Cada configuración se aplica según la clasificación de prioridades de la directiva. Toda configuración de directiva que esté inhabilitada prevalece sobre las configuraciones habilitadas de menor prioridad. Las configuraciones de directiva que no están configuradas se ignoran.

> **Importante:**
>
> Si configura las directivas de Active Directory y Citrix mediante la Consola de administración de directivas de grupo, es posible que las asignaciones y las configuraciones no se apliquen de la forma esperada. Para obtener más información, consulte CTX127461.

De forma predeterminada se proporciona una directiva "Sin filtro".

- Si utiliza Web Studio para administrar las directivas de Citrix, las configuraciones que agregue a la directiva sin filtro se aplican a todos los servidores, escritorios y conexiones de un sitio.

- Los sitios y las conexiones deben estar en el ámbito de los objetos de directiva de grupo (GPO) que incluye la directiva. Por ejemplo: la unidad organizativa Ventas incluye un GPO denominado Ventas-EE. UU. que incluye a todos los miembros del equipo de ventas de los Estados Unidos. El GPO Ventas-EE. UU. tiene configurada una directiva sin filtro que incluye varias configuraciones de directiva de usuario. Cuando el jefe de Ventas-EE. UU. inicia sesión en el sitio, la configuración de la directiva sin filtro se aplica automáticamente a la sesión. Esto se debe a que el usuario es miembro del GPO Ventas-EE. UU.

El modo de una asignación determina si la directiva se aplica exclusivamente a las conexiones que coinciden con todos los criterios de la asignación. Si el modo está establecido en Permitir (Allow) (valor predeterminado), la directiva se aplica solamente a las conexiones que coinciden con los criterios de la asignación. Si el modo está establecido en Denegar (Deny), la directiva se aplica si la conexión no coincide con las asignaciones del filtro. Los siguientes ejemplos ilustran cómo los modos de las asignaciones afectan a las directivas de Citrix cuando hay varias asignaciones.

- **Ejemplo: Asignaciones del mismo tipo en modos distintos:** En las directivas con dos asignaciones del mismo tipo, donde una está establecida en Permitir y la otra en Denegar, la asignación establecida en Denegar tiene precedencia, siempre que la conexión satisfaga ambas asignaciones. Por ejemplo:

  La directiva 1 incluye las siguientes asignaciones:

  - La asignación A especifica el grupo Ventas. El modo está establecido en Permitir.
  - La asignación B especifica la cuenta del jefe de ventas. El modo está establecido en Denegar.

  Como el modo de la asignación B es Denegar, no se aplica la directiva cuando el jefe de Ventas inicia sesión en el sitio, aunque este usuario sea miembro del grupo Ventas.

- **Ejemplo: Asignaciones de diferentes tipos con modos iguales:** En las directivas con dos o más asignaciones de diferentes tipos, establecidas en Permitir, la conexión debe satisfacer al menos una asignación de cada tipo para que se aplique la directiva. Por ejemplo:

  La directiva 2 incluye las siguientes asignaciones:

  - La asignación C es una asignación de usuario que especifica el grupo Ventas. El modo está establecido en Permitir.
  - La asignación D es una asignación de dirección IP del cliente que especifica 10.8.169.* (la red de la empresa). El modo está establecido en Permitir.

  Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, se aplica la directiva, ya que la conexión satisface ambas asignaciones.

  La directiva 3 incluye las siguientes asignaciones:

- La asignación E es una asignación de usuario que especifica el grupo Ventas. El modo está establecido en Permitir.
- La asignación F es una asignación de control de acceso que especifica condiciones de conexión de NetScaler Gateway. El modo está establecido en Permitir.

Cuando el jefe de Ventas inicia sesión en el sitio desde la oficina, no se aplica la directiva, ya que la conexión no cumple con los requisitos de la asignación F.

## Conjuntos de directivas (Tech Preview)

May 17, 2024

Los conjuntos de directivas son objetos de Citrix DaaS que acumulan directivas para permitir un acceso simplificado y basado en roles, y una administración sencilla. Puede crear conjuntos de directivas para reflejar las divisiones lógicas de su empresa y su equipo de administradores. Por ejemplo, puede crear un conjunto de directivas para cada región geográfica, unidad de negocio o caso de uso específico. Una vez creados, los ámbitos y los grupos de entrega se asignan a conjuntos de directivas para que solo los administradores autorizados puedan administrar las directivas que se aplican a sus usuarios y máquinas pertinentes.

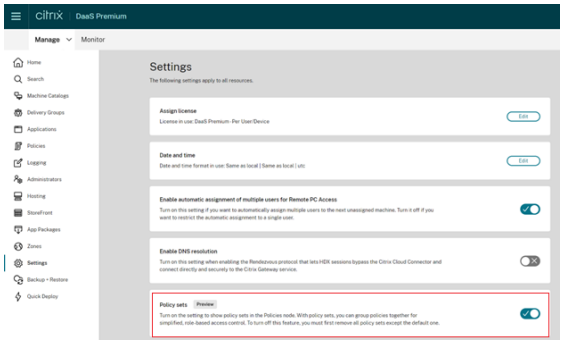
### Ventajas

- Control de acceso por roles para equipos de administradores distribuidos
- Fusiones, adquisiciones y consolidaciones simplificadas
- Dominio de errores limitado
- Función multiarrendataria para directivas

### Habilitar conjuntos de directivas

En la ficha **Administrar** de Citrix DaaS, vaya a **Parámetros** y active el parámetro **Conjuntos de directivas**.




> **Nota:**
>
> Debe habilitar conjuntos de directivas antes de crear un conjunto de directivas.

## Comparación de funciones

| Antes de aplicar conjuntos de directivas | Tras aplicar conjuntos de directivas |
|---|---|
| Las directivas, los parámetros, los filtros y las prioridades de directivas de todo el sitio se configuran en un solo lugar dentro de Citrix Studio. | Las directivas, los parámetros, los filtros y las prioridades de directivas se configuran por separado para cada conjunto de directivas. |
| Si administra una directiva, debe administrar todas las directivas. | Los administradores totales pueden delegar en administradores de nivel inferior la capacidad de administrar un conjunto de directivas determinado de forma individual. |
| Las directivas de entornos grandes y distribuidos se vuelven complejas y difíciles de administrar. | Las directivas de entornos grandes y distribuidos se pueden dividir y administrar fácilmente. |

## ¿Cómo funcionan los conjuntos de directivas?

### Descripción general

- Los conjuntos de directivas se asignan a grupos de entrega
- Los conjuntos de directivas tienen uno o varios ámbitos
- Los grupos de entrega sin ningún conjunto de directivas asignado reciben el conjunto de directivas predeterminado
- Un grupo de entrega solo puede tener asignado un conjunto de directivas
- Varios grupos de entrega pueden usar el mismo conjunto de directivas
- Aunque los conjuntos de directivas se asignen a grupos de entrega, las directivas mantienen sus filtros

Para obtener más información, consulte How do filters get applied. No hay ningún cambio en la forma en la que funcionan las asignaciones de directivas o los filtros de directivas para los conjuntos de directivas. Es decir, funcionan de la misma manera que lo hacen para las directivas individuales.

### Conjunto de directivas predeterminado

- Cuando el parámetro del conjunto de directivas está activado, todas las directivas existentes se agrupan en el conjunto de directivas predeterminado
- Cada grupo de entrega recibe el conjunto de directivas predeterminado, a menos que el equipo de administradores cree un conjunto de directivas y lo asigne a un grupo de entrega.
- Cuando a un grupo de entrega se le asigna un conjunto de directivas diferente, ya no recibirá directivas del conjunto de directivas predeterminado

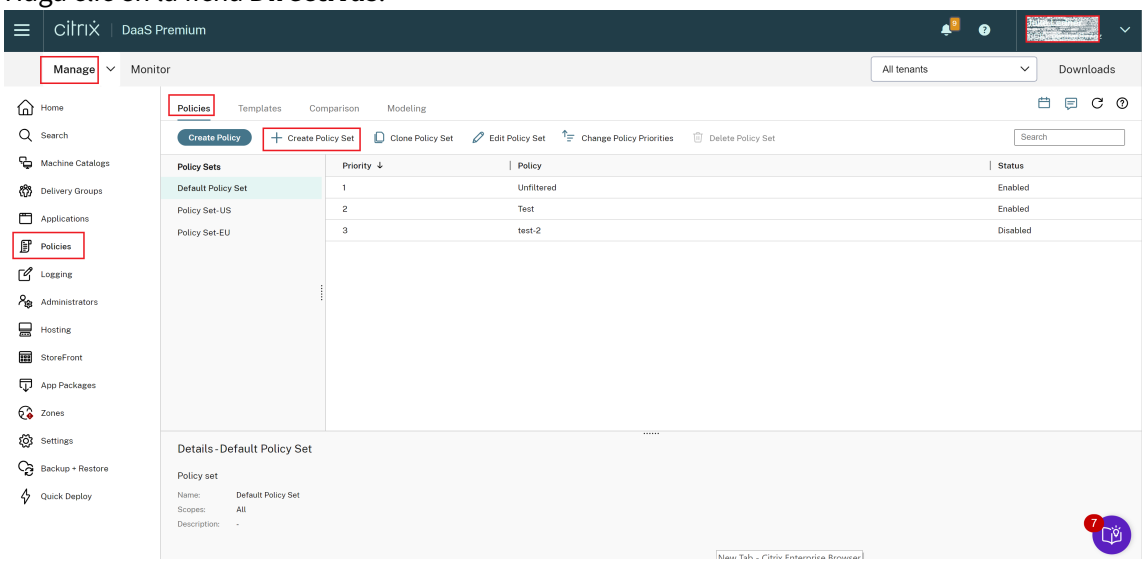
### Creación de conjuntos de directivas

Los conjuntos de directivas se pueden crear de estas dos maneras:

- Crear conjunto de directivas: Esta acción crea un conjunto de directivas vacío
- Clonar conjunto de directivas: Esta acción crea un conjunto de directivas basado en un conjunto de directivas existente

### Crear conjuntos de directivas

1. En la página de configuración de Citrix DaaS, haga clic en la ficha **Administrar**.
2. Haga clic en la ficha **Directivas**.




3. Seleccione **Crear conjunto de directivas**. Aparece la ficha **Introducción**.
4. Haga clic en **Siguiente** o en la ficha **Nombre y descripción**.

5. Introduzca el nombre y la descripción del conjunto de directivas.
6. Haga clic en **Siguiente** o en la ficha **Asignaciones**.
7. Seleccione uno o más grupos de entrega a los que quiera asignar el conjunto de directivas.
8. Haga clic en **Siguiente** o en la ficha **Ámbitos**.
9. Seleccione los ámbitos del conjunto de directivas.
10. Haga clic en **Crear**. El conjunto de directivas se crea con la asignación y el ámbito definidos.

#### Clonar conjuntos de directivas

1. En la página de configuración de Citrix DaaS, haga clic en la ficha **Administrar**.
2. Haga clic en la ficha **Directivas**.
3. Seleccione **Clonar conjunto de directivas**.
4. Modifique el nombre del conjunto de directivas.
5. Modifique o cree asignaciones para el conjunto de directivas y haga clic en **Siguiente**.
6. Seleccione o anule la selección de directivas que quiera incluir en el conjunto de directivas clonado.
7. Modifique el ámbito de la directiva.
8. Haga clic en **Crear**. Se crea el conjunto de directivas.

#### Modificar conjuntos de directivas

1. En la página de configuración de Citrix DaaS, haga clic en la ficha **Administrar**.
2. Haga clic en la ficha **Directivas**.
3. Seleccione **Modificar conjunto de directivas**.
4. Modifique el nombre del conjunto de directivas y haga clic en **Siguiente**.
5. Modifique o cree asignaciones para el conjunto de directivas y haga clic en **Siguiente**.
6. Modifique el ámbito de la directiva.
7. Haga clic en **Crear**.

#### Asignación de conjuntos de directivas

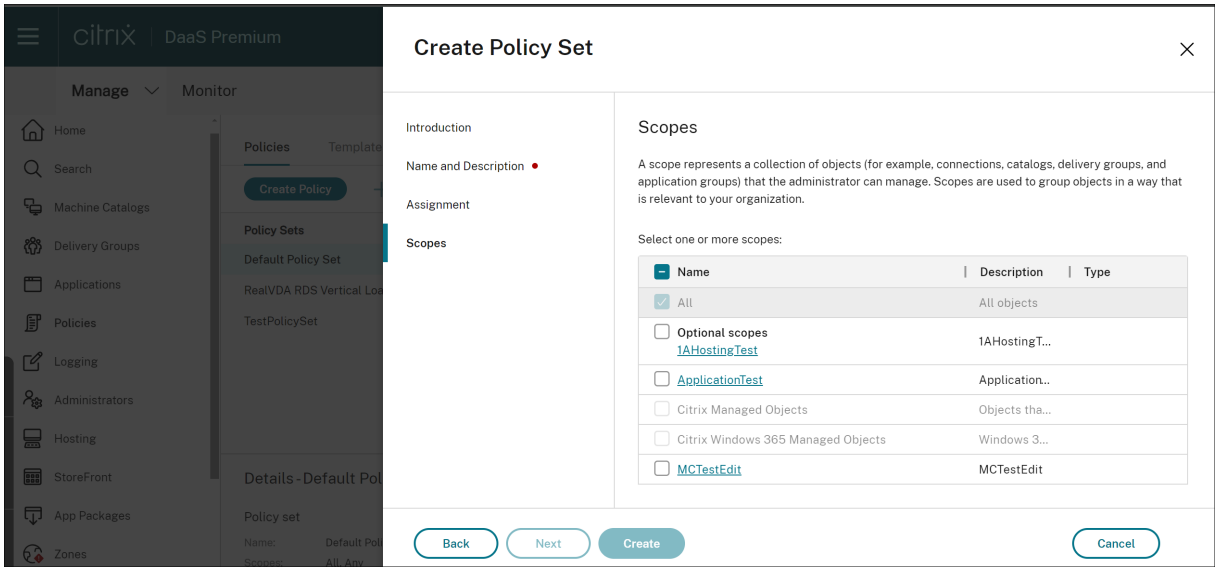
Los conjuntos de directivas se asignan a grupos de entrega. Puede configurar asignaciones cuando se crea o se modifica el conjunto de directivas. También puede configurar asignaciones al crear o modificar grupos de entrega.

#### Ámbitos de conjuntos de directivas

Los administradores pueden definir el ámbito del conjunto de directivas para que solo administradores autorizados puedan verlo o modificarlo. Puede configurar los ámbitos al crear o al modificar el conjunto de directivas.

Con la introducción de los conjuntos de directivas, también puede crear y administrar directivas de Citrix mediante la API. Para obtener más información, consulte How to create a policy set in Citrix DaaS.




## Priorizar, modelar, comparar y solucionar problemas de directivas

June 1, 2023

Puede usar directivas para personalizar su entorno a fin de satisfacer las necesidades de los usuarios en función de lo siguiente:

- Funciones de trabajo
- Ubicaciones geográficas
- Tipos de conexión

Por ejemplo, por motivos de seguridad, puede establecer restricciones en los grupos de usuarios que interactúan regularmente con datos confidenciales.

Además, puede crear una directiva para evitar que los usuarios guarden archivos con información confidencial en sus unidades de cliente locales. Puede crear otra directiva para los usuarios del grupo que necesitan acceder a sus unidades locales. A continuación, puede clasificar las dos directivas para establecer cuál de ellas tiene preferencia. Al usar diversas directivas, debe determinar:

- Cómo priorizar las directivas
- Cómo crear excepciones
- Cómo ver la directiva efectiva cuando las directivas entran en conflicto

### Priorizar directivas

La asignación de prioridades en las directivas le permite definir la prioridad de las directivas cuando contienen configuraciones conflictivas. La identificación de todas las directivas que coinciden con las asignaciones de la conexión tiene lugar cuando un usuario inicia sesión en el sistema. Las directivas identificadas y sus configuraciones asociadas se clasifican por orden de prioridad. Cada configuración se aplica según la clasificación de prioridades de la directiva.

Usted puede asignar la prioridad de las directivas asignándoles diferentes números de prioridad en **Web Studio**. De forma predeterminada, las directivas nuevas tienen la prioridad más baja. Si hay conflictos entre las configuraciones de las directivas, una directiva con una prioridad más alta anula otra que tenga una prioridad más baja. Una directiva con el número de prioridad 1 es la de mayor prioridad. Las configuraciones de directivas se combinan de la siguiente manera:

- Prioridades de las directivas
- Condiciones especificadas en los filtros de las directivas

Para priorizar las directivas, siga estos pasos:

1. Seleccione **Directivas** en el panel de la izquierda.
2. En la ficha **Directivas**, seleccione **Cambiar prioridades de directiva** en la barra de acciones. Aparecerá la página **Cambiar prioridades de directiva**.
3. En la lista de prioridades, haga lo siguiente para cambiar la prioridad de una directiva:
    - Arrastre la directiva a la posición que quiera.
    - Para moverla una posición hacia arriba o hacia abajo, haga clic en el icono de flecha arriba o abajo, respectivamente.
    - Para moverla a la parte superior o inferior de la lista, haga clic en el icono de flecha superior o inferior, respectivamente.
    - Para cambiar el número de prioridad, haga clic en el icono **Modificar**, introduzca un número y, a continuación, haga clic en **Guardar**.
4. Haga clic en **Guardar**.

### Excepciones

Al crear directivas y utilizar filtros para asignarlas a grupos de usuarios, dispositivos de usuario o máquinas, es posible que algunos miembros del grupo necesiten excepciones a algunas configuraciones. Para crear excepciones, debe:

- Crear una directiva exclusiva para los miembros del grupo que necesitan las excepciones y luego dar mayor prioridad a esta directiva que a la directiva de la totalidad del grupo.

- Usar el modo *Denegar* para una asignación agregada a la directiva

Una asignación con el modo *Denegar* aplica una directiva solo a las conexiones que no coinciden con los criterios de asignación. Por ejemplo: una directiva incluye las siguientes asignaciones:

- La *asignación A* es una asignación de dirección IP del cliente que especifica el intervalo `208.77.88.*`. El modo está establecido en *Permitir*.
- La *asignación B* es una asignación de usuario que especifica una cuenta de usuario determinada. El modo está establecido en *Denegar*.

La directiva se aplica a todos los usuarios que inician sesión en el sitio con las direcciones IP incluidas en el intervalo especificado en la *asignación A*. Sin embargo, la directiva no se aplica al usuario que inicia sesión en el sitio con la cuenta de usuario especificada en la *asignación B*.

> **Nota:**
>
> Durante el paso **Asignar directiva**, si desactiva la casilla de verificación para habilitar, la asignación se inhabilita para la directiva. Si la única asignación de la directiva está inhabilitada, es lo mismo que no tener ninguna asignación y, por lo tanto, la directiva se aplica a todos los objetos del sitio.

### Determinar las directivas que se aplican a una conexión

En ocasiones, una conexión no responde según lo previsto debido a que se aplican varias directivas. Si se aplica una directiva de mayor prioridad a una conexión, esta puede anular la configuración definida en la directiva original. Es posible calcular el **Conjunto resultante de directivas** o RSOP (Resultant Set of Policies) y determinar cómo se combinan las configuraciones de directiva finales para una conexión.

El **Conjunto resultante de directivas** se puede calcular de diversas maneras:

- Con el **asistente de modelado de directivas de grupo de Citrix** para simular un caso de conexión y observar la forma en que se aplicarían las directivas de Citrix. Puede especificar condiciones para un escenario de conexión, por ejemplo:
  - Usuarios
  - Valores de prueba de asignación de directivas Citrix
- Use los **Resultados de directivas de grupo** para generar un informe donde se describen las directivas de Citrix vigentes para un usuario o un Virtual Delivery Agent (VDA) específico.

Las configuraciones de directivas del sitio creadas con **Web Studio** no se incluyen en el **Conjunto resultante de directivas** al ejecutar el asistente de **Modelado de directivas de grupo Citrix** desde la Consola de **administración de directivas de grupo**. Para verificar que obtiene el **grupo de directivas resultante**más completo, Citrix recomienda iniciar el asistente de **Modelado de directivas de**

**grupo Citrix** desde **Web Studio**, a menos que cree las directivas mediante solo la **Consola de administración de directivas de grupo**.

### Usar el asistente de modelado de directivas

El modelado de directivas le ayuda a simular directivas habilitadas con filtros a efectos de planificación y prueba. Solo se modelan las directivas habilitadas con filtros. Las directivas inhabilitadas nunca se aplican y las directivas habilitadas sin filtros siempre se aplican.

Siga estos pasos para abrir el asistente de **Modelado de directivas**:

1. En Configuración completa, seleccione **Directivas**.
2. Seleccione la ficha **Modelado**.
3. Seleccione **Modelado de directivas** en la barra de acciones.
4. Lea la página **Introducción** y haga clic en **Siguiente**.
5. Seleccione usuarios o equipos. Puede buscar contenedores o usuarios o equipos específicos. Haga clic en **Siguiente**.
6. Elija una evidencia de filtro. Si lo desea, puede obtener una simulación más detallada introduciendo detalles adicionales, como el **grupo de entrega**, las **etiquetas**, la **dirección IP del cliente**, etc. Haga clic en **Siguiente**.
7. Revise el resumen de opciones elegidas y haga clic en **Ejecutar**.

Al hacer clic en **Ejecutar**, el asistente genera un informe de los resultados del modelado. Mientras consulta este informe, puede hacer lo siguiente:

- Seleccionar si quiere ver **Todas las configuraciones**, la **Configuración de equipo** o los **Parámetros de usuario** en el menú desplegable.
- Usar la barra de búsqueda para buscar configuraciones específicas.
- Hacer clic en una configuración específica para ver sus detalles. Por ejemplo, si no se aplicaron todos los parámetros de usuario a una directiva específica, el panel **Detalles** muestra el motivo por el que no se aplicaron.
- Haga clic en **Exportar** para exportar los resultados del modelado en formato JSON, HTML o ambos.

Tras ejecutar el modelado de directivas, dispondrá de más opciones. Puede hacer lo siguiente:

- **Ver informe de modelado**: Se abre el mismo informe de modelado de arriba para que pueda volver a verlo o exportarlo.
- **Ejecutar de nuevo el modelado de directivas**: Esto le permite volver a ejecutar el modelado de directivas con el mismo conjunto de criterios seleccionado anteriormente y generar nuevos resultados de modelado. Puede resultar útil si algunas directivas han cambiado y quiere ver cómo afectan esos cambios al modelo actual.
- **Eliminar informe de modelado**: Elimina el informe de modelado actual.

### Comparar directivas y plantillas

Puede comparar la configuración de una directiva o plantilla con las de otras directivas o plantillas. Por ejemplo, puede que quiera verificar los valores de configuración para garantizar que se cumplan las directrices recomendadas. También puede comparar las configuraciones de una directiva o plantilla con las configuraciones predeterminadas.

1. Seleccione **Directivas** en el panel de navegación de **Web Studio**.
2. Haga clic en la ficha **Comparación** y, a continuación, haga clic en **Seleccionar**.
3. Seleccione las directivas o plantillas que desea comparar. Para incluir los valores predeterminados en la comparación, marque la casilla **Comparar con la configuración predeterminada**.
4. Al hacer clic en **Comparar**, las configuraciones definidas se mostrarán en columnas.
5. Para ver todas las configuraciones, seleccione **Mostrar todas las configuraciones**. Para volver a la vista predeterminada, seleccione **Mostrar configuraciones en común**.

### Solucionar problemas de directivas

Los usuarios, las direcciones IP y otros objetos asignados pueden tener varias directivas que se aplican de forma simultánea. Este supuesto puede ocasionar conflictos en los que puede que una directiva no se comporte como se espera. Al ejecutar el asistente de **Modelado de directivas de grupo Citrix**, es posible que detecte que no se aplican directivas a las conexiones de usuario. En este caso, los usuarios que se conectan a sus aplicaciones y escritorios en condiciones que coinciden con los criterios de evaluación de la directiva no se ven afectados por ninguna configuración de directiva. Esta situación se produce cuando:

- Ninguna de las directivas tiene asignaciones que coinciden con los criterios de evaluación de la directiva.
- Las directivas que coinciden con la asignación no tienen ninguna configuración definida.
- Las directivas que coinciden con la asignación están inhabilitadas.

Si desea aplicar configuraciones de directiva a las conexiones que cumplen un criterio determinado, asegúrese de lo siguiente:

- Las directivas que desea aplicar a esas conexiones están habilitadas.
- Las directivas que desea aplicar tienen definidas las configuraciones adecuadas.

> **Nota:**
>
> En el segundo salto de los casos de doble salto, tenga en cuenta que un VDA de SO de sesión única se conecta a un VDA de SO multisesión. En este caso, las directivas de Citrix actúan en el VDA de SO de sesión única como si fuera el dispositivo del usuario. Por ejemplo: considere que las directivas están configuradas para guardar en caché las imágenes en el dispositivo del usuario.

> En este ejemplo, las imágenes almacenadas en caché para el segundo salto en un escenario de doble salto se almacenan en caché en la máquina VDA con SO de sesión única.

### Director

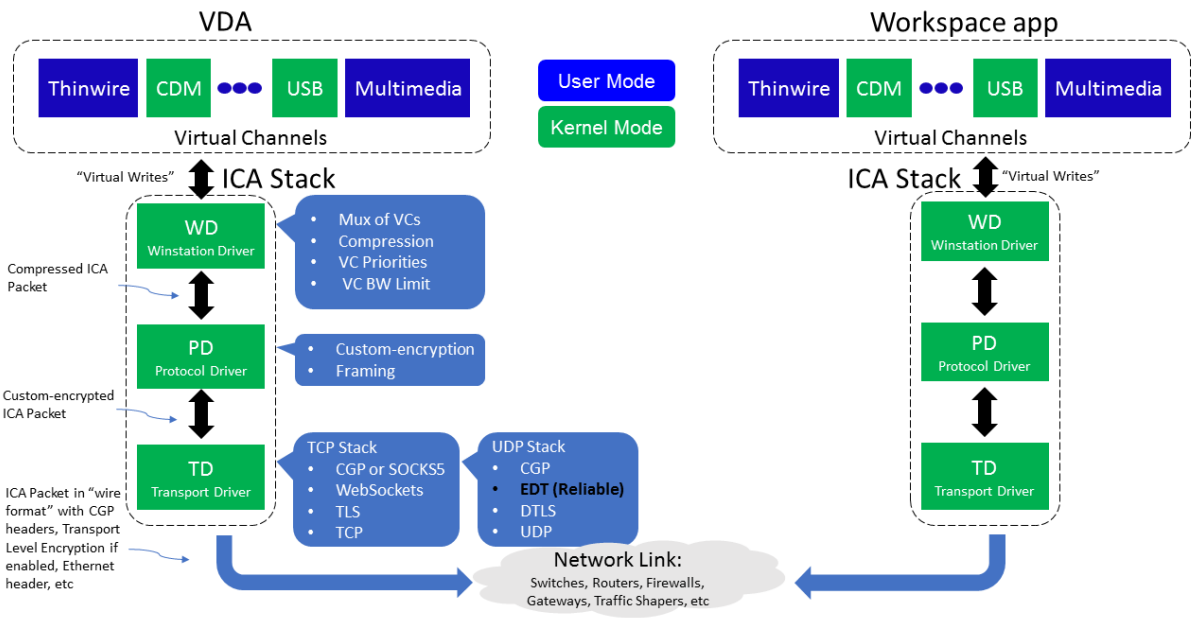
Los usuarios que no son administradores pueden usar Director para ver las directivas que se aplican a una sesión de usuario.

## Descripción general de HDX

April 18, 2024

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

Citrix HDX incluye una amplia gama de tecnologías que ofrecen una experiencia de alta definición a los usuarios de aplicaciones y escritorios centralizados, en cualquier dispositivo y en cualquier red.



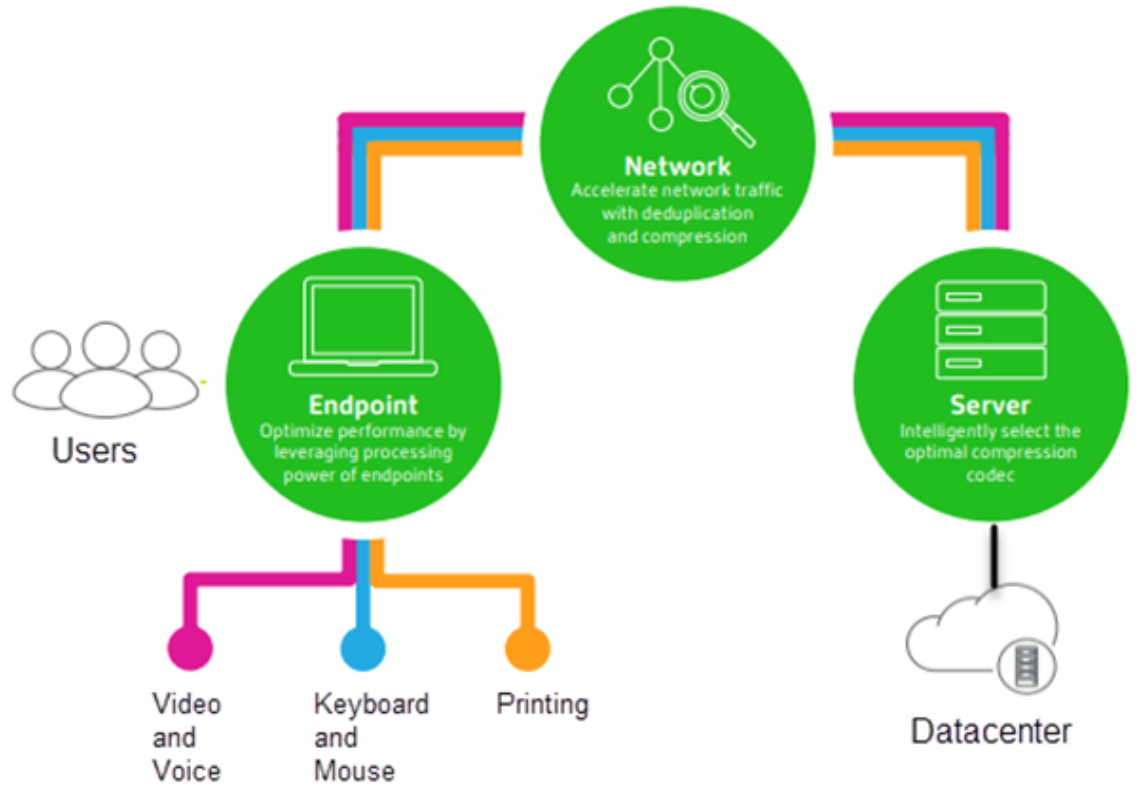

El diseño de HDX responde a tres principios técnicos:

- Redirección inteligente
- Compresión adaptable
- Evitar solapamiento de datos

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

- **Redirección inteligente:** La redirección inteligente examina la actividad de la pantalla, los comandos de la aplicación, el dispositivo de punto final y las capacidades de la red y el servidor para determinar de manera instantánea cómo y dónde generar una actividad de escritorio o aplicación. La representación puede ocurrir en el dispositivo de punto final o en el servidor de alojamiento.
- **Compresión adaptable:** La compresión adaptable permite que se entreguen pantallas con muchos contenidos multimedia en conexiones de red débiles. HDX primero evalúa algunas variables, como el tipo de entrada, el dispositivo y la pantalla (texto, vídeo, voz y multimedia). Elige el códec de compresión óptimo y la mejor proporción de uso de CPU y GPU. A continuación, se adapta de forma inteligente según cada usuario y frecuencia únicos. Esta adaptación inteligente es por usuario o incluso por sesión.




- **Evitar solapamiento de datos:** Al evitar el solapamiento del tráfico de red se reducen los datos agregados enviados entre el cliente y el servidor. Esto se consigue aprovechando los patrones repetidos en los datos a los que se accede de forma común, como gráficos de mapas de bits,

documentos, trabajos de impresión y contenido en streaming. El almacenamiento en caché de estos patrones permite que solo los cambios se transmitan a través de la red, eliminando el tráfico duplicado. HDX también admite la multidifusión de transmisiones multimedia, donde varios suscriptores ven una única transmisión desde la fuente en una ubicación, en lugar de tener que establecer una conexión individual para cada usuario.

Para obtener más información, consulte Potenciar la productividad con un espacio de trabajo de usuario de alta definición.

### En el dispositivo

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

### En la red

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

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

### En el centro de datos

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

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

### HDX Insight

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

mación incluye la latencia de sesión ICA del lado del cliente y del lado del servidor, el uso del ancho de banda por parte de los canales ICA y el valor de tiempo de ida y vuelta de ICA en cada sesión.

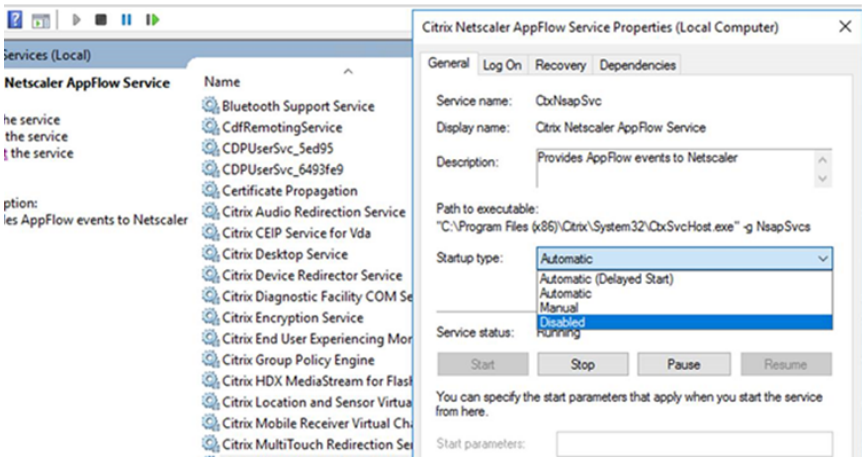
Puede habilitar NetScaler para usar el canal virtual HDX Insight y mover todos los puntos de datos requeridos en un formato sin comprimir. Si inhabilita esta función, el dispositivo NetScaler descifrará y descomprimirá el tráfico ICA que haya en varios canales virtuales. Usar el canal virtual único disminuye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

**Requisitos mínimos:**

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

### Habilitar o inhabilitar el canal virtual HDX Insight

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




### Experimentar con las capacidades HDX en su escritorio virtual

- Para ver cómo la redirección de contenido de exploradores (una de las cuatro tecnologías HDX de redirección multimedia) acelera la entrega de contenido multimedia HTML5 y WebRTC:

1. Descargar la Extensión del explorador Chrome e instalarla en el escritorio virtual.
2. Para ver cómo la redirección de contenido de exploradores acelera la entrega de contenido multimedia a los escritorios virtuales, vea un vídeo en su escritorio desde un sitio web que contenga vídeos HTML5, como YouTube. Los usuarios no saben cuándo se está ejecutando la redirección de contenido de exploradores. Para ver si se está utilizando la redirección de contenido de exploradores, arrastre la ventana del explorador rápidamente. Verá una demora o falta de marco entre la ventana gráfica y la interfaz de usuario. También puede hacer clic con el botón derecho en la página web y buscar **Acerca de la Redirección de explorador HDX** en el menú.

- Para ver cómo HDX entrega sonido de alta definición:

  1. Configure el cliente Citrix con la máxima calidad de audio; consulte la documentación de la aplicación Citrix Workspace para obtener más información.
  2. Reproduzca archivos de música mediante un reproductor de audio digital (como iTunes) en el escritorio.

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

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

Información útil:

- Para obtener información acerca de la asistencia y los requisitos de las funciones HDX, consulte el artículo Requisitos del sistema. A menos que se indique lo contrario, las funciones de HDX están disponibles para máquinas con los sistemas operativos compatibles multisesión Windows y de sesión única Windows, además de los escritorios de acceso con Remote PC.

- Esta sección describe cómo optimizar más la experiencia de usuario, mejorar la escalabilidad de los servidores o reducir los requisitos de ancho de banda. Para obtener más información sobre cómo usar las directivas Citrix y sus configuraciones, consulte la documentación de las directivas Citrix para esta versión.
- Para las instrucciones que impliquen modificar el Registro, tenga cuidado: si se modifica de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

## Fiabilidad de la sesión y reconexión automática de clientes

A la hora de acceder a aplicaciones o escritorios alojados, pueden producirse interrupciones de red. Para una reconexión más fluida, se ofrecen las funcionalidades Fiabilidad de la sesión y Reconexión automática de clientes. En una configuración predeterminada, se empieza con la Fiabilidad de la sesión, seguida de la Reconexión automática de clientes.

**Reconexión automática de clientes:**

La reconexión automática de clientes reinicia el motor del cliente para volver a conectarse a una sesión desconectada. La reconexión automática de clientes cierra (o desconecta) la sesión del usuario después del tiempo especificado en la configuración. Durante la reconexión automática de clientes, el sistema envía la siguiente notificación de interrupción de red al usuario de las aplicaciones y los escritorios:

- **Escritorios**. La ventana de sesión se oscurece y aparece un temporizador de cuenta atrás que muestra el tiempo que falta hasta que se produzcan las reconexiones.
- **Aplicaciones.** La ventana de sesión se cierra y aparece un diálogo con un temporizador de cuenta atrás que muestra el tiempo que falta hasta que se intenten reconexiones.

Durante la reconexión automática de clientes, las sesiones se reinician a condición de una buena conectividad de red. El usuario no puede interactuar con las sesiones mientras la reconexión automática de clientes está en curso.

En la reconexión, las sesiones desconectadas vuelven a conectarse mediante la información guardada de la conexión. El usuario puede interactuar con las aplicaciones y los escritorios de la forma habitual.

Configuración predeterminada de la reconexión automática de clientes:

- Tiempo de espera de la reconexión automática de clientes: 120 segundos
- Reconexión automática de clientes: Habilitada
- Autenticación para la reconexión automática de clientes: Inhabilitada

- Captura de registro de la reconexión automática de clientes: Inhabilitada

Para obtener más información, consulte Configuraciones de directiva de Reconexión automática de clientes.

**Fiabilidad de la sesión:**

La fiabilidad de la sesión vuelve a conectar sesiones ICA sin problemas cuando se producen interrupciones de red. La fiabilidad de la sesión cierra (o desconecta) la sesión de usuario después de que haya trascurrido el tiempo especificado en la opción de configuración. Una vez agotado el tiempo de espera de la fiabilidad de la sesión, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada. Durante la fiabilidad de la sesión, se envían las siguientes notificaciones de interrupción de red al usuario de las aplicaciones y los escritorios:

- **Escritorios**. La ventana de sesión se vuelve transparente y aparece un temporizador de cuenta atrás que muestra el tiempo hasta que se produzcan las reconexiones.
- **Aplicaciones.** La ventana se vuelve transparente y aparecen elementos emergentes que indican una conexión interrumpida en el área de notificaciones.

Mientras la fiabilidad de la sesión está activa, el usuario no puede interactuar con las sesiones ICA. No obstante, las acciones del usuario (como pulsaciones de teclado) se almacenan en búfer durante los segundos inmediatos tras la interrupción de red y se retransmiten una vez que la red está disponible.

En la reconexión, el cliente y el servidor reanudan la actividad desde el mismo punto donde estaban en su intercambio de protocolo. Las ventanas de sesión pierden transparencia y aparecen las notificaciones correspondientes en forma de elementos emergentes en el área de notificaciones para las aplicaciones.

Configuración predeterminada de fiabilidad de la sesión

- Tiempo de espera de fiabilidad de la sesión: 180 segundos
- Nivel de opacidad de la interfaz de usuario durante la reconexión: 80 %
- Conexión de fiabilidad de la sesión: Habilitada
- Número de puerto para fiabilidad de la sesión: 2598

Para obtener más información, consulte Configuraciones de directiva de Fiabilidad de la sesión.

**NetScaler con fiabilidad de la sesión y reconexión automática de clientes:**

La reconexión automática de clientes no funciona si las directivas de Multisecuencia y de Puertos múltiples están habilitadas en el servidor y si se da una de las siguientes condiciones o todas ellas:

- La fiabilidad de la sesión está inhabilitada en NetScaler Gateway.
- Se produce una conmutación por error en el dispositivo NetScaler.
- NetScaler SD-WAN se utiliza con NetScaler Gateway.

### Rendimiento HDX adaptable

El rendimiento HDX adaptable ajusta de manera inteligente el rendimiento máximo de la sesión ICA porque adapta los búferes de salida. Al principio, la cantidad de búferes de salida se establece en un valor alto. Este valor alto permite que los datos se transmitan al cliente de manera más rápida y eficiente, especialmente en redes de latencia alta. Así, se obtiene una mejor interactividad, transferencias de archivos más rápidas, reproducciones de vídeo más fluidas, mayor velocidad de fotogramas y mayor resolución en una experiencia de usuario mejorada.

La interactividad de la sesión se mide constantemente para determinar si algún flujo de datos de la sesión ICA está afectando negativamente a la interactividad. Si eso ocurre, el rendimiento se reduce para disminuir el impacto del flujo de datos de gran tamaño en la sesión y permitir que se recupere la interactividad.

> **Importante:**
>
> El rendimiento HDX adaptable cambia la forma en que se configuran los búferes de salida, porque transfiere este mecanismo del cliente al VDA y no se necesita ninguna configuración manual.

Esta función presenta los siguientes requisitos:

- VDA 1811 o una versión posterior
- Aplicación Workspace para Windows 1811 o una versión posterior

### Mejorar la calidad de imagen enviada a los dispositivos de usuario

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

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

### Mejorar el rendimiento de las conferencias de vídeo

Se han optimizado varias aplicaciones conocidas de conferencias de vídeo para la entrega con Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) a través de la redirección multimedia (consulte, por ejemplo, HDX RealTime Optimization Pack). Para las aplicaciones que no se han optimizado, la compresión de vídeo de cámara web HDX mejora la eficiencia del ancho de banda y la tolerancia a la latencia para las cámaras web durante las sesiones de conferencias de vídeo. Esta compresión de vídeo dirige el tráfico de la cámara web a través de un canal virtual multimedia dedicado. Esta tecnología utiliza menos ancho de banda en comparación con la funcionalidad de redirección USB de HDX Plug-n-Play isócrono, y funciona bien en conexiones WAN.

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

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

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

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

### Prioridades del tráfico de red

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

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

Cada canal virtual se asocia a una prioridad específica y se transporta en la conexión correspondiente. Según el número de puerto TCP usado para la conexión, se pueden definir canales de forma independiente.

Se admiten conexiones de multisecuencia de canales múltiples para los agentes VDA (Virtual Delivery Agent) instalados en máquinas Windows 10 y Windows 8. Póngase en contacto con el administrador de la red para comprobar que los puertos del protocolo CGP definidos en la configuración de Directiva de puertos múltiples están correctamente asignados en los enrutadores de la red.

La función de calidad de servicio (QoS) solo se admite si se configuran múltiples puertos de fiabilidad de sesión o los puertos CGP.

> **Advertencia:**
>
> Use algún tipo de seguridad en el transporte cuando aplique esta función. Citrix recomienda el uso del protocolo de seguridad de Internet (IPsec) o Transport Layer Security (TLS). Las conexiones TLS (Secure Sockets Layer) solo se admiten cuando atraviesan un dispositivo NetScaler Gateway compatible con ICA de multisecuencia. Dentro de una red interna de la empresa, no se admiten las conexiones multisecuencia con TLS.

Para establecer la calidad de servicio en conexiones de multisecuencia, agregue las siguientes configuraciones de directiva Citrix (consulte Configuraciones de directiva de Conexiones de multisecuencia para obtener más información):

- Directiva de puertos múltiples: Esta configuración especifica los puertos para el tráfico ICA en varias conexiones y establece prioridades de red.
  - En la lista de prioridades de puertos CGP predeterminados, seleccione una prioridad. De forma predeterminada, el puerto primario (2598) tiene prioridad Alta.
  - Escriba los puertos CGP adicionales en CGP port1, CGP port2 y CGP port3 según sea necesario, e identifique las prioridades para cada puerto. Cada puerto debe tener una prioridad exclusiva.

  Configure explícitamente los firewalls en los VDA para que permitan el tráfico TCP adicional.
- Configuración de equipo para multisecuencia: Esta configuración está inhabilitada de forma predeterminada. Si usa Citrix NetScaler SD-WAN con la funcionalidad de multisecuencia en el entorno, no es necesario definir esta configuración. Defina esta configuración de directiva cuando esté utilizando enrutadores externos o versiones antiguas de Branch Repeater para conseguir el nivel de Calidad de servicio (QoS) que necesite.
- Configuración de usuario para multisecuencia: Esta configuración está inhabilitada de forma predeterminada.

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

### Mostrar u ocultar la barra de idioma remota

La barra de idioma muestra el idioma de entrada preferido en una sesión de aplicación. Si esta función está habilitada (la configuración predeterminada), puede mostrar u ocultar la barra de idioma en la interfaz de usuario desde **Preferencias avanzadas > Barra de idioma** en la aplicación Citrix Workspace para Windows. Mediante una configuración de Registro en el lado del VDA, puede inhabilitar el control sobre la función de la barra de idioma por parte del cliente. Si esta función está inhabilitada, la configuración de la interfaz de usuario del cliente no surte efecto, y la configuración actual por usuario determina el estado de la barra de idioma. Para obtener más información, consulte Mejorar la experiencia del usuario.

Para inhabilitar el control sobre la función de la barra de idioma por parte del cliente desde el VDA:

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

### Asignar teclado Unicode

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

#### Habilitar o inhabilitar la asignación de distribución de teclado Unicode

De forma predeterminada, la función está inhabilitada en el lado del agente VDA. Para habilitar la función, debe activarla desde el editor del Registro regedit en el VDA. Agregue la siguiente clave del Registro:

KEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nombre: EnableKlMap

Tipo: DWORD

Valor: 1

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

**Habilitar el modo compatible de la asignación de distribución de teclado Unicode**

De forma predeterminada, la asignación de distribución de teclado Unicode vincula automáticamente algunas API de Windows para volver a cargar el nuevo mapa de distribución de teclado Unicode cuando la distribución del teclado se cambia en el servidor. Algunas aplicaciones no se pueden vincular. Para mantener la compatibilidad, puede cambiar la función al modo compatible para admitir esas aplicaciones no vinculadas. Agregue la siguiente clave del Registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/CtxKlMap

Nombre: DisableWindowHook

Tipo: DWORD

Valor: 1

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

## Canales virtuales ICA de Citrix

March 6, 2024

> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada de un Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### ¿Qué son los canales virtuales ICA?

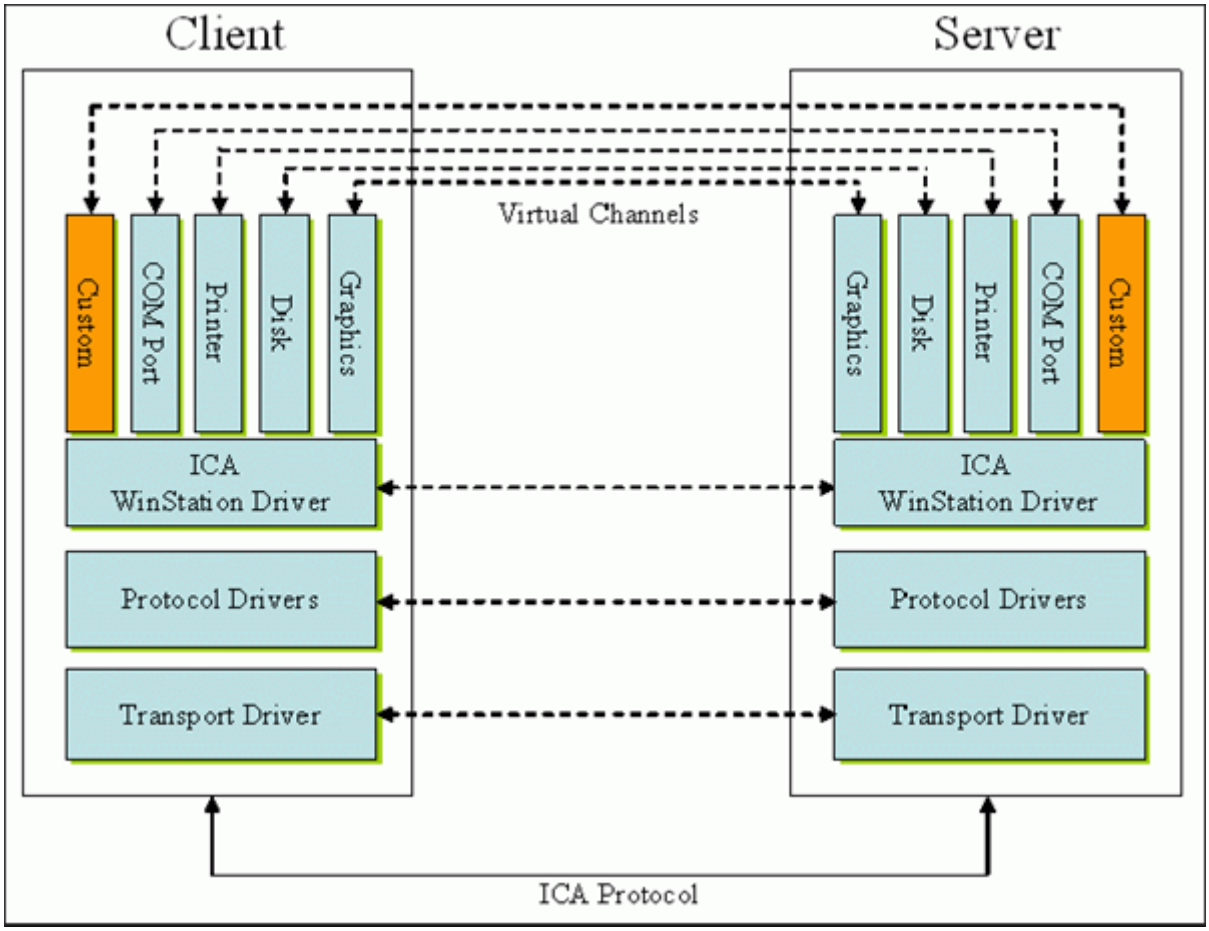
Una gran parte de la funcionalidad y la comunicación entre la aplicación Citrix Workspace y los servidores de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) se produce a través de canales virtuales. Los canales virtuales son una parte necesaria de la experiencia informática remota de los servidores de Citrix DaaS. Los canales virtuales se utilizan en los siguientes aspectos:

- Audio
- Puertos COM
- Discos
- Gráficos
- Puertos LPT

- Impresoras
- Tarjetas inteligentes
- Canales virtuales personalizados de terceros
- Vídeo

A veces se publican nuevos canales virtuales con productos de la aplicación Citrix Workspace y Citrix DaaS para ofrecer más funcionalidades.




Un canal virtual es un controlador virtual del lado del cliente que se comunica con una aplicación del lado del servidor. Citrix DaaS ya contiene varios canales virtuales. Estos están diseñados para que los clientes y los proveedores externos puedan crear sus propios canales virtuales mediante uno de los kits de desarrollo de software (SDK) que se proporcionan.

Los canales virtuales ofrecen una forma segura de realizar varias tareas. Por ejemplo: una aplicación que se ejecuta en un servidor de Citrix Virtual Apps y se comunica con un dispositivo del lado del cliente o una aplicación que se comunica con el entorno del lado del cliente.

En el lado del cliente, los canales virtuales corresponden a los controladores virtuales. Cada controlador virtual ofrece una función específica. Algunos son necesarios para un funcionamiento normal y otros son opcionales. Los controladores virtuales operan al nivel del protocolo de la capa de pre-

sentación. Puede haber varios protocolos activos en un momento dado mediante la multiplexación de canales que proporciona la capa de protocolos de Windows Station (WinStation).

Las siguientes funciones se encuentran en el valor de Registro VirtualDriver de esta ruta de acceso del Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0`

o bien

`HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0` (para 64 bits)

- Thinwire 3.0 (obligatoria)
- ClientDrive
- ClientPrinterQueue
- ClientPrinterPort
- Portapapeles
- ClientComm
- ClientAudio
- LicenseHandler (obligatoria)
- TWI (obligatoria)
- SmartCard
- ICACTL (obligatoria)
- SSPI
- TwainRdr
- UserEXperience
- Vd3d

> **Nota:**
>
> Puede inhabilitar funcionalidades específicas del cliente si quita uno o varios de estos valores de la clave de Registro. Por ejemplo: si quiere quitar el Portapapeles del cliente, quite la palabra **Clipboard**.

Esta lista contiene los archivos de controlador virtual del cliente y sus funciones respectivas. Citrix Virtual Apps y la aplicación Citrix Workspace para Windows los utilizan. Tienen forma de bibliotecas de vínculos dinámicos (modo usuario) y no de controladores de Windows (modo kernel), excepto la función USB genérico tal y como se describe en Canal virtual USB genérico.

- vd3dn.dll: Canal virtual Direct3D utilizado para la redirección de composiciones de escritorio.
- vdcamN.dll: Audio bidireccional.
- vdcdm30n.dll: Asignación de unidades del cliente.

- vdcom30N.dll: Asignación de puertos COM del cliente.
- vdcpm30N.dll: Asignación de impresoras del cliente.
- vdctln.dll: Canal de controles ICA.
- vddvc0n.dll: Canal virtual dinámico.
- vdeuemn.dll: Supervisión de la experiencia de usuario final.
- vdgusbn.dll: Canal virtual USB genérico.
- vdkbhook.dll: Paso de clave transparente.
- vdlfpn.dll: Canal de visualización Framehawk por transporte similar al protocolo UDP.
- vdmmn.dll: Compatibilidad multimedia.
- vdmrvc.dll: Canal virtual de Mobile Receiver.
- vdmtchn.dll: Funcionalidad multitoque.
- vdscardn.dll: Compatibilidad con tarjetas inteligentes.
- vdsens.dll: Canal virtual de sensores.
- vdspl30n.dll: Protocolo UDP del cliente.
- vdsspin.dll: Kerberos.
- vdtuin.dll: Interfaz de usuario transparente.
- vdtw30n.dll: Cliente Thinwire.
- vdtwin.dll: Conexión directa.
- vdtwn.dll: TWAIN.

Algunos canales virtuales se compilan en otros archivos. Por ejemplo: la asignación de Clipboard está disponible en wfica32.exe.

#### Compatibilidad con 64 bits

La aplicación Citrix Workspace para Windows es compatible con 64 bits. Al igual que con la mayoría de los binarios compilados para 32 bits, estos archivos de cliente tienen equivalentes compilados de 64 bits:

- brapi64.dll
- confmgr.dll
- ctxlogging.dll
- ctxmui.dll
- icaconf.exe
- icaconfs.dll
- icafile.dll
- pnipcn64.dll
- pnsson.dll
- ssoncom.exe
- ssonstub.dll

- vdkbhook64.dll

#### Canal virtual USB genérico

La implementación del canal virtual USB genérico utiliza dos controladores en modo kernel junto con el controlador de canal virtual vdgusbn.dll:

- ctxusbm.sys
- ctxusbr.sys

#### Cómo funcionan los canales virtuales ICA

Los canales virtuales se cargan de varias maneras. El Shell (WfShell para el servidor y PicaShell para la estación de trabajo) carga algunos canales virtuales. Algunos canales virtuales se alojan como servicios de Windows.

Módulos de canal virtual cargados por el Shell. Por ejemplo:

- EUEM
- TWAIN
- Portapapeles
- Contenido multimedia
- Uso compartido de sesiones integradas
- Zona horaria

Algunos se cargan en modo kernel. Por ejemplo:

- CtxDvcs.sys: Canal virtual dinámico.
- Icausbb.sys: Redirección de USB genérico.
- Picadm.sys: Asignación de unidades del cliente.
- Picaser.sys: Redirección de puertos COM.
- Picapar.sys: Redirección de puertos LPT.

#### Canal virtual de gráficos en el lado del servidor

A partir de XenApp 7.0 y XenDesktop7.0, `ctxgfx.exe` aloja el canal virtual de gráficos para las sesiones basadas en estaciones de trabajo y servidores Terminal Server. `Ctxgfx` aloja módulos de plataformas específicas que interactúan con el controlador correspondiente (`Icardd.dll` para RDSH, y `vdod.dll` y `vidd.dll` para las estaciones de trabajo).

Para las implementaciones de XenDesktop 3D Pro, se instala un controlador de gráficos OEM para la GPU correspondiente del VDA. `Ctxgfx` carga módulos adaptadores especializados para interactuar con el controlador de gráficos OEM.

**Alojar canales especializados en servicios de Windows**

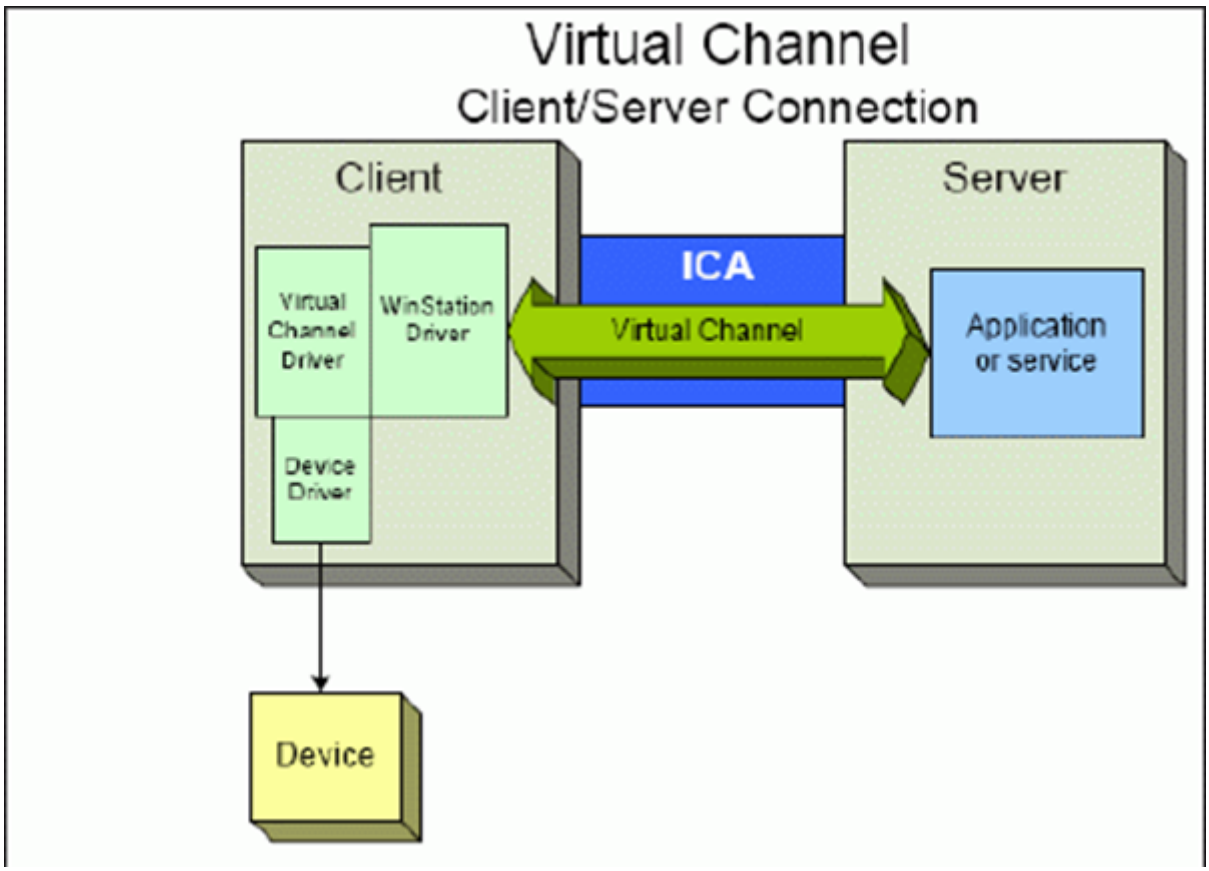
En los servidores de Citrix DaaS, varios canales se alojan como servicios de Windows. Este alojamiento ofrece una semántica del tipo "uno a varios"para múltiples aplicaciones en una sesión y múltiples sesiones en el servidor. He aquí algunos ejemplos de tales servicios:

- Citrix Device Redirector Service
- Citrix Dynamic Virtual Channel Service
- Citrix End User Experience Monitoring Service
- Citrix Location and Sensor Virtual Channel Service
- Citrix MultiTouch Redirection Service
- Citrix Print Manager Service
- Citrix Smartcard Service
- Citrix Audio Redirection Service (solo para Citrix Virtual Desktops)
- Servicio Citrix ICA Status Channel

El canal virtual de audio de Citrix Virtual Apps se aloja mediante el Servicio de Audio de Windows.

En el lado del servidor, todos los canales virtuales del cliente se enrutan a través del controlador de WinStation: Wdica.sys. En el lado del cliente, el controlador de WinStation correspondiente, integrado en wfica32.exe, sondea los canales virtuales del cliente. Esta imagen ilustra la conexión servidor-cliente del canal virtual.




He aquí un resumen con un intercambio de datos cliente-servidor mediante un canal virtual.

1. El cliente se conecta al servidor de Citrix DaaS. El cliente pasa información al servidor sobre los canales virtuales que admite.
2. La aplicación del lado del servidor se inicia, obtiene un identificador para el canal virtual y, de forma opcional, envía consultas para obtener más información sobre el canal.
3. El controlador virtual del cliente y la aplicación del lado del servidor pasan datos mediante estos dos métodos:
    - Si la aplicación del servidor tiene datos para enviar al cliente, los datos se envían al cliente inmediatamente. Cuando el cliente recibe los datos, el controlador de WinStation desmultiplexa los datos del canal virtual de la secuencia ICA e inmediatamente los pasa al controlador virtual del cliente.
    - Si el controlador virtual del cliente tiene datos para enviar al servidor, los datos se envían la próxima vez que el controlador de WinStation lo sondee. Cuando el servidor recibe los datos, se ponen en cola hasta que la aplicación del canal virtual los lea. No hay forma de alertar a la aplicación del canal virtual del servidor de que los datos se han recibido.
4. Cuando se completa la aplicación del canal virtual del servidor, el canal virtual se cierra y se liberan los recursos asignados.

### Crear un canal virtual propio mediante Virtual Channel SDK

La creación de un canal virtual mediante Virtual Channel SDK requiere conocimientos intermedios de programación. Utilice este método para proporcionar una ruta principal de comunicación entre el cliente y el servidor. Por ejemplo: si implementa el uso de un dispositivo en el lado del cliente, como un escáner, que se utilizará con algún proceso de la sesión.

> **Nota:**
>
> - El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual.
> - Debido a la seguridad mejorada para Citrix DaaS, debe especificar qué canales virtuales pueden abrirse en una sesión ICA. Para obtener más información, consulte Configuraciones de la directiva Lista de canales virtuales permitidos.

### Crear un canal virtual propio mediante ICA Client Object SDK

Crear un canal virtual con el objeto de cliente ICA (ICO) es más fácil que usar Virtual Channel SDK. Utilice el ICO mediante la creación de un objeto con nombre asignado en el programa con el método **CreateChannels**.

> **Importante:**
>
> Debido a la seguridad mejorada que llega con la versión 10.00 de Citrix Receiver para Windows y versiones posteriores (y las aplicaciones de Citrix Workspace para Windows), debe dar un paso más al crear un canal virtual ICO.

Para obtener más información, consulte Client Object API Specification Programmer's Guide.

### Funcionalidad de paso de canales virtuales

La mayoría de los canales virtuales que Citrix proporciona funcionan sin modificar cuando se utiliza la aplicación Citrix Workspace para Windows en sesiones ICA (también conocidas como sesiones de paso). Hay ciertos aspectos a tener en cuenta al usar el cliente en saltos adicionales.

Las siguientes funciones operan de la misma manera tanto en saltos simples como en múltiples:

- Asignación de puertos COM del cliente
- Asignación de unidades del cliente
- Asignación de impresoras del cliente
- UDP del cliente
- Supervisión de la experiencia de usuario final

- USB genérico
- Kerberos
- Compatibilidad multimedia
- Compatibilidad con tarjetas inteligentes
- Paso de clave transparente
- TWAIN

Como la naturaleza inherente de la latencia y de factores como la compresión, la descompresión y el renderizado de cada salto, el rendimiento puede verse afectado con cada salto adicional que haga el cliente. Las zonas afectadas son:

- Audio bidireccional
- Transferencias de archivos
- Redirección de USB genérico
- Conexión directa
- Thinwire

> **Importante:**
>
> De forma predeterminada, las unidades del cliente asignadas por una instancia del cliente que se ejecuta en una sesión de paso están restringidas a las unidades del cliente que se conecta.

### Funcionalidad de paso de canales virtuales entre una sesión de Citrix Virtual Desktops y una sesión de Citrix Virtual Apps

La mayoría de los canales virtuales proporcionados por Citrix funcionan sin modificar cuando se utiliza la aplicación Citrix Workspace para Windows en sesiones ICA (también conocidas como sesiones de paso) en un servidor de Citrix Virtual Desktops.

En concreto, en el servidor de Citrix Virtual Desktops, hay un enlace de VDA que ejecuta **picaPassthruHook**. Este enlace hace que el cliente crea que se ejecuta en un servidor CPS y coloca al cliente en su modo tradicional de paso.

Se admiten los siguientes canales virtuales tradicionales y su funcionalidad:

- Cliente
- Asignación de puertos COM del cliente
- Asignación de unidades del cliente
- Asignación de impresoras del cliente
- USB genérico (limitado por rendimiento)
- Compatibilidad multimedia
- Compatibilidad con tarjetas inteligentes
- SSON
- Paso de clave transparente

## Seguridad y canales virtuales ICA

La seguridad es una parte importante de la planificación, el desarrollo y la implementación de canales virtuales. Hay varias referencias a áreas específicas de seguridad en este documento.

## Prácticas recomendadas

Abra los canales virtuales cuando **se conecte** y **se vuelva a conectar**. Cierre los canales virtuales cuando cierre la sesión y **se desconecte**.

Tenga en cuenta las siguientes pautas al crear scripts que utilizan funciones de los canales virtuales.

**Asignar nombres a los canales virtuales:**

Puede crear hasta 32 canales virtuales. 17 de los 32 canales están reservados para fines especiales.

- Los nombres de los canales virtuales no deben tener más de 7 caracteres.
- Los 3 primeros caracteres están reservados para el nombre del proveedor, y los 4 siguientes, para el tipo de canal. Por ejemplo: **CTXAUD** representa el canal virtual de audio de Citrix.

Los canales virtuales tienen un nombre ASCII de 7 caracteres (o menos). En algunas versiones anteriores del protocolo ICA, los canales virtuales estaban numerados. Ahora, los números se asignan de forma dinámica en función del nombre ASCII, lo que facilita la implementación. Los usuarios que estén desarrollando código de un canal virtual para uso interno solo pueden usar nombres de 7 caracteres que coincidan con otros canales virtuales existentes. Utilice solamente números y caracteres ASCII en mayúsculas y minúsculas. Siga la convención de nomenclatura existente al agregar canales virtuales propios. Hay varios canales predefinidos. Los canales predefinidos comienzan con el identificador OEM "CTX"y son de uso exclusivo de Citrix.

**Compatibilidad con doble salto:**

| Canal virtual | ¿Compatible con doble salto? |
|---|---|
| Audio | No |
| Redirección de contenido del explorador web | No |
| CDM | Sí |
| CEIP | No |
| Portapapeles | Sí |
| Continuum (MRVC) | No |
| Control VC | Sí |

| Canal virtual | ¿Compatible con doble salto? |
|---|---|
| Redirección de vídeo HTML5 (v1) | Sí |
| Teclado, puntero | Sí |
| Multitoque | No |
| NSAPVC | No |
| Impresión | Sí |
| SensVC | No |
| Tarjeta inteligente | Sí |
| TWAIN | Sí |
| USB VC | Sí |
| Dispositivos WAYCOM-K2M con USB VC | Sí |
| Compresión de vídeo de cámara web | Sí |
| Redirección de Windows Media | Sí |

### También puede consultar

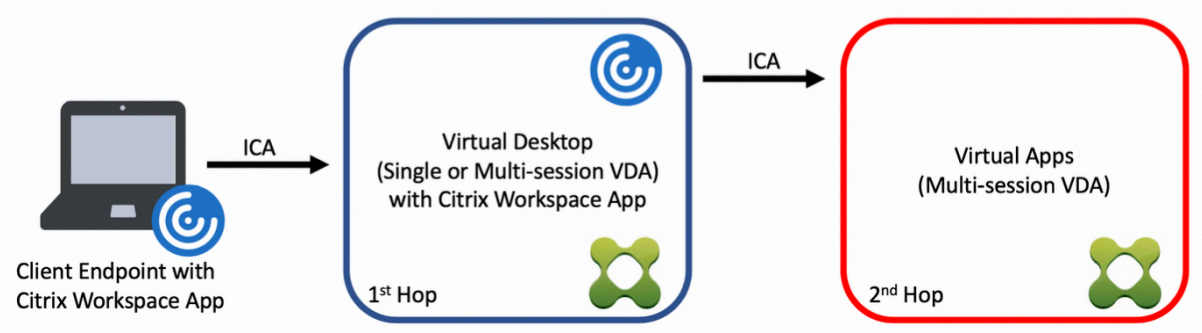
- ICA Virtual Channel SDK
- Citrix Developer Network es el centro de todos los recursos y debates técnicos relacionados con el uso los SDK de Citrix. En esta red, puede encontrar acceso a los SDK, código y scripts de ejemplo, extensiones, plug-ins y documentación de los SDK. También se encuentran los foros de Citrix Developer Network, donde se llevan a cabo debates técnicos sobre cada SDK de Citrix.

## Doble salto en Citrix DaaS

May 17, 2024

En el contexto de una sesión de cliente de Citrix, el término “doble salto”se refiere a una sesión de Citrix Virtual Apps activa dentro de una sesión de Citrix Virtual Desktops. El siguiente diagrama ilustra un doble salto.




En el caso de un salto doble, cuando el usuario se conecta a una sesión de Citrix Virtual Desktops, en un VDA de SO de sesión única (conocido como VDI) o en un VDA de SO multisesión (conocido como escritorio publicado), se considera el primer salto. Una vez que el usuario se haya conectado al escritorio virtual, puede iniciar una sesión de Citrix Virtual Apps. Eso se considera el segundo salto.

Puede utilizar un modelo de implementación de doble salto para disponer de varios casos de uso. Un ejemplo común es el caso en el que diferentes entidades administran los entornos de Citrix Virtual Desktops y Citrix Virtual Apps. Este método también puede ser eficaz para resolver problemas de compatibilidad de aplicaciones.

### Requisitos del sistema

El doble salto está disponible en todas las ediciones de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

El primer salto debe utilizar una versión compatible del VDA de SO de sesión única o multisesión y de la aplicación Citrix Workspace. El segundo salto debe utilizar una versión compatible del VDA de SO multisesión. Consulte la página Tabla de productos para ver las versiones compatibles.

Para obtener un rendimiento y una compatibilidad óptimos, Citrix recomienda utilizar un cliente Citrix de la misma versión o de una más reciente que las versiones de VDA que se utilicen.

En entornos en los que el primer salto implica una solución de escritorios virtuales de terceros (que no sea de Citrix) junto con una sesión de Citrix Virtual Apps, la compatibilidad se limita al entorno de Citrix Virtual Apps. En caso de que surja algún problema relacionado con el escritorio virtual de terceros, como, entre otros, la compatibilidad de la aplicación Citrix Workspace, la redirección de dispositivos de hardware o el rendimiento de la sesión, Citrix puede proporcionar asistencia técnica limitada. Es posible que se necesite Citrix Virtual Desktops en el primer salto como parte de la solución de problemas.

### Aspectos a tener en cuenta en las implementaciones para HDX en doble salto

En general, cada sesión en un doble salto es única, y las funciones cliente-servidor están limitadas a un salto específico. Esta sección incluye áreas que requieren una atención especial por parte de

los administradores de Citrix. Citrix recomienda que los clientes realicen pruebas exhaustivas de las prestaciones de HDX necesarias para garantizar que la experiencia de usuario y el rendimiento sean adecuados para una configuración de entorno determinada.

#### Gráficos

Utilice los parámetros gráficos predeterminados (codificación selectiva) en el primer y el segundo salto. En el caso de HDX 3D Pro, Citrix recomienda encarecidamente que todas las aplicaciones que requieran aceleración gráfica se ejecuten localmente en el primer salto con los recursos de GPU adecuados que haya disponibles para el VDA.

#### Latencia

La latencia de extremo a extremo puede afectar a la experiencia general del usuario. Tenga en cuenta la latencia adicional entre el primer y el segundo salto. Esto es especialmente importante con la redirección de dispositivos de hardware.

#### Contenido multimedia

La representación de contenido de audio y vídeo en el lado del servidor (en sesión) funciona mejor en el primer salto. La reproducción de vídeo en el segundo salto requiere decodificación y recodificación en el primer salto, lo que aumenta el ancho de banda y el consumo de recursos de hardware. El contenido de audio y vídeo debe limitarse al primer salto siempre que sea posible.

#### Redirección de dispositivos USB

HDX incluye modos de redirección genéricos y optimizados para admitir una amplia gama de tipos de dispositivos USB. Preste especial atención al modo que se utilice en cada salto y sírvase de la tabla siguiente como referencia para obtener resultados óptimos. Para obtener más información sobre los modos de redirección genéricos y optimizados, consulte Dispositivos USB genéricos.

| Primer salto (VDI o escritorio publicado) | Segundo salto (Virtual Apps) | Notas sobre la compatibilidad |
|---|---|---|
| Optimizado | Optimizado | Recomendado (según la compatibilidad del dispositivo). Por ejemplo: almacenamiento masivo USB, escáneres TWAIN, cámara web, audio. |

| Primer salto (VDI o escritorio publicado) | Segundo salto (Virtual Apps) | Notas sobre la compatibilidad |
|---|---|---|
| Genérico | Genérico | Para dispositivos donde la opción optimizada no está disponible. |
| Genérico | Optimizado | Aunque técnicamente es posible, se recomienda utilizar el modo optimizado en ambos saltos cuando la compatibilidad del dispositivo lo permita. |
| Optimizado | Genérico | No se admite |

> **Nota:**
>
> Debido a la elevada actividad inherente de los protocolos USB, el rendimiento puede disminuir entre saltos. La funcionalidad y los resultados varían según los requisitos específicos de los dispositivos y las aplicaciones. Las pruebas de validación son muy recomendables en todos los casos de redirección de dispositivos y son especialmente importantes en casos de doble salto.

### Excepciones de compatibilidad

Las sesiones de doble salto admiten la mayoría de las funciones y prestaciones HDX, excepto las siguientes:

- Redirección de contenido de explorador web
- Acceso a aplicaciones locales
- RealTime Optimization Pack para Skype Empresarial
- Optimización para Microsoft Teams

## Conectividad HDX

May 17, 2024

Citrix HDX incluye una amplia gama de tecnologías que ofrecen una experiencia de alta definición a los usuarios de aplicaciones y escritorios centralizados, en cualquier dispositivo y en cualquier red.

El diseño de HDX responde a tres principios técnicos:

- Redirección inteligente
- Compresión adaptable
- Evitar solapamiento de datos

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

En la oferta de HDX, puede conectarse a través de un protocolo de transporte exclusivo y patentado, utilizar el máximo de unidades de transmisión al establecer sesiones y optimizar la conectividad con Citrix SD-WAN.

## Transporte adaptable

May 17, 2024

El transporte adaptable es un mecanismo de Citrix Virtual Apps and Desktops que permite establecer conexiones para las sesiones HDX mediante un protocolo de transporte preferido y, al mismo tiempo, proporciona una alternativa con TCP si la conectividad con el protocolo preferido no está disponible.

Se admiten los siguientes protocolos de transporte:

- Enlightened Data Transport (EDT)
- Protocolo de control de transferencias (TCP)

### Configuración

El transporte adaptable está habilitado de forma predeterminada. Puede configurar el transporte adaptable para que funcione de los siguientes modos:

- **Preferido**: (Predeterminado) El cliente intenta conectarse con el protocolo preferido y recurre a TCP si la conectividad con el protocolo preferido no está disponible.
- **Modo de diagnóstico**: El cliente solo intenta conectarse mediante el protocolo preferido. Se inhabilita la posibilidad de recurrir a TCP.
- **Desactivado**: El cliente solo intenta conectarse mediante TCP.

### Funcionamiento

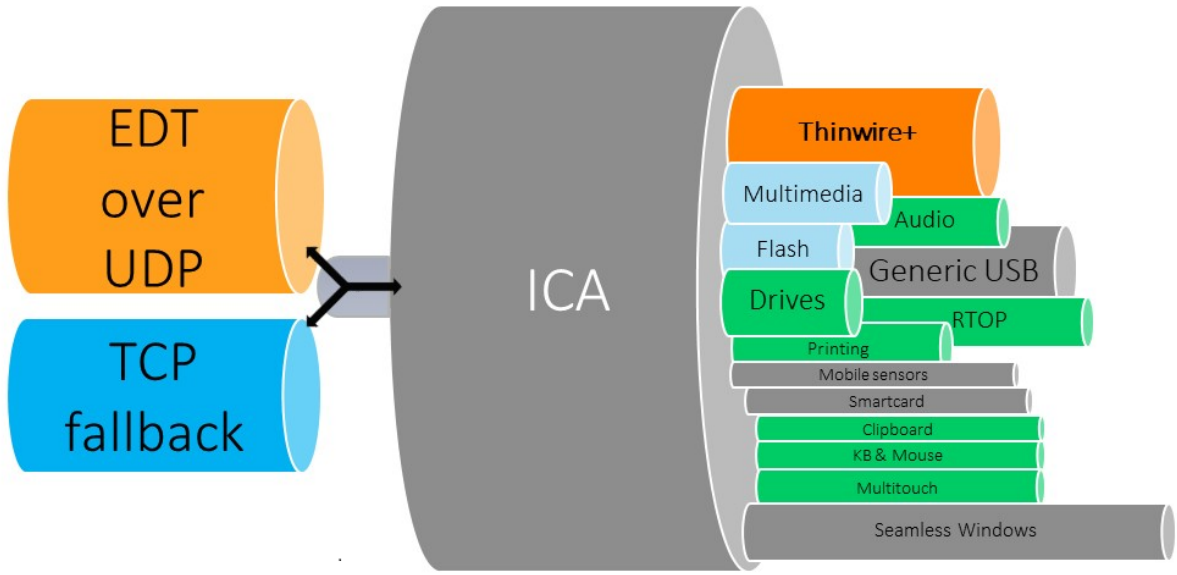
Cuando el **transporte adaptable** está establecido en `Preferred`, el cliente intenta conectarse a la sesión con el protocolo preferido y TCP en paralelo. Esto permite optimizar el tiempo de conexión

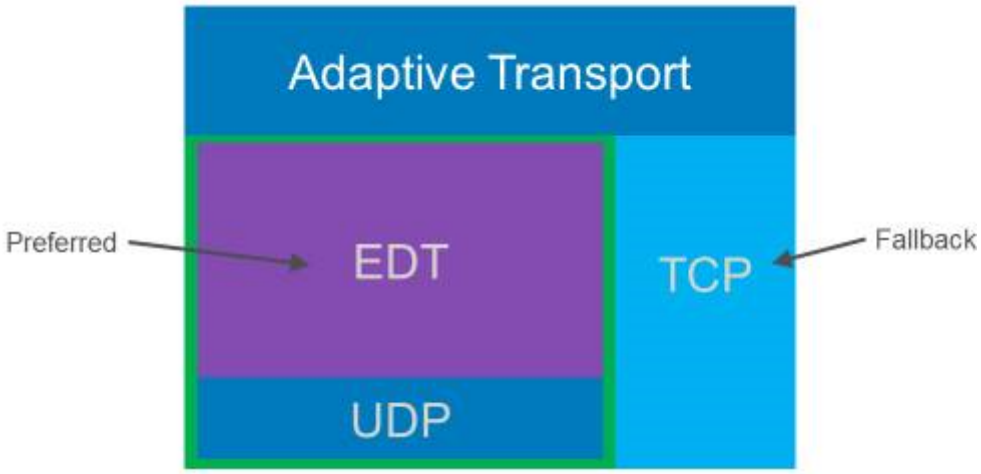
 

si no es posible conectarse con el protocolo preferido y el cliente debe recurrir a TCP. Si la conexión se establece mediante TCP, el cliente intenta conectarse con el protocolo preferido en segundo plano cada cinco minutos.

Cuando el **transporte adaptable** está establecido en `Diagnostic mode`, el cliente se conecta a la sesión solo con el protocolo preferido. Si el cliente no puede establecer una conexión mediante el protocolo preferido, no recurre al uso de TCP y la conexión falla.

Cuando el **transporte adaptable** está establecido en `Off`, el **transporte adaptable** está inhabilitado y el cliente se conecta a la sesión mediante TCP únicamente.




## Requisitos del sistema

A continuación se detallan los requisitos para utilizar el transporte adaptable y EDT:

- Plano de control
  - Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
  - Citrix Virtual Apps and Desktops: Versión compatible actualmente
- Virtual Delivery Agent
  - Windows: Versión compatible actualmente (se recomienda 2402 o posterior)
  - Linux: Versión compatible actualmente (se recomienda 2402 o posterior)
- Aplicación Citrix Workspace
  - Windows: Versión compatible actualmente (se recomienda 2402 o posterior)
  - Linux: Versión compatible actualmente (se recomienda 2402 o posterior)
  - Mac: Versión compatible actualmente (se recomienda 2402 o posterior)
  - iOS: La versión más reciente disponible en el App Store de Apple
  - Android: La versión más reciente disponible en Google Play
- Citrix NetScaler Gateway
  - 14.1.12.30 o posterior (recomendado)
  - 13.1.17.42 o posterior (se recomienda 13.1-52.19 o posterior)

> **Nota:**
>
> Para obtener más información sobre Linux VDA, consulte la documentación de Linux Virtual Delivery Agent.

## Requisitos de la red

Las siguientes secciones contienen los requisitos de red para usar EDT con transporte adaptable:

### Hosts de sesión

Si los hosts de la sesión tienen un firewall como el Firewall de Windows Defender, debe permitir el siguiente tráfico entrante para las conexiones internas.

| Descripción | Origen | Protocolo | Puerto |
|---|---|---|---|
| Conexión interna: Fiabilidad de la sesión habilitada | Cliente | UDP | 2598 |

| Descripción | Origen | Protocolo | Puerto |
|---|---|---|---|
| Conexión interna: Fiabilidad de la sesión inhabilitada | | | 1494 |
| Conexión interna: HDX Direct o VDA SSL | | | 443 |

> **Nota:**
>
> El instalador del VDA agrega las reglas de entrada apropiadas al Firewall de Windows Defender. Si usa un firewall diferente, debe agregar las reglas anteriores.

**Red interna**

La siguiente tabla muestra las reglas de firewall necesarias para usar EDT en la red:

| Descripción | Protocolo | Origen | Destino | Puerto de destino |
|---|---|---|---|---|
| Conexión interna directa: Fiabilidad de la sesión habilitada | UDP | Red del cliente | Red VDA | 2598 |
| Conexión interna directa: Fiabilidad de la sesión inhabilitada | | | | 1494 |
| Conexión interna directa: HDX Direct o VDA SSL | | | | 443 |
| NetScaler Gateway | | SNIP de NetScaler | | 2598 |
| NetScaler Gateway: VDA SSL | | | | 443 |

> **Nota:**
>
> Si usa Citrix Gateway Service, debe habilitar **Rendezvous** para usar EDT como protocolo de trans-

> porte. Consulte la documentación de Rendezvous para conocer los requisitos del sistema y la red.

**Red del cliente**

En la siguiente tabla se describen los requisitos de conectividad de los dispositivos cliente:

| Descripción | Protocolo | Origen | Destino | Puerto de destino |
|---|---|---|---|---|
| Conexión interna: Fiabilidad de la sesión habilitada | UDP | IP de cliente | Red VDA | 2598 |
| Conexión interna: Fiabilidad de la sesión inhabilitada | | | | 1494 |
| Conexión interna: HDX Direct o SSL VDA | | | | 443 |
| Conexión externa: NetScaler Gateway | | | Dirección IP pública de NetScaler Gateway | 443 |
| Conexión externa: Citrix Gateway Service | | | Citrix Gateway Service | 443 |

> **Nota:**
>
> Si usa Citrix Gateway Service, los clientes deben poder acceder a https://*.*.nssvc.net. Si no puede autorizar todos los subdominios con https://*.*.nssvc.net, puede usar https://*.c.nssvc.net y https://*.g.nssvc.net en su lugar. Para obtener más información, consulte el artículo CTX270584 de Knowledge Center.

## Enlightened Data Transport

May 17, 2024

Enlightened Data Transport (EDT) es un protocolo de transporte propiedad de Citrix basado en el protocolo de datagramas de usuario (UDP). Ofrece una experiencia de usuario superior en complicadas conexiones de larga distancia al tiempo que mantiene la escalabilidad de los servidores. EDT mejora el procesamiento de datos de todos los canales virtuales ICA en redes no fiables para ofrecer una experiencia de usuario mejor y más coherente.

Cuando el **transporte adaptable** está habilitado, EDT es el protocolo preferido.

### Qué debe saber

- **Fiabilidad de la sesión** debe estar habilitada para usar **detección de MTU** y EDT con NetScaler Gateway y Citrix Gateway Service.
- La fragmentación de paquetes puede degradar el rendimiento o, en algunos casos, incluso impedir que se abran las sesiones. Para evitar esto, debe ajustar la MTU de EDT a un valor adecuado para sus redes. Puede usar la detección de MTU de EDT o una solución manual que se describe en How to configure MSS when using EDT on networks with non-standard MTU.
- Para obtener más información sobre cómo habilitar el uso de EDT con NetScaler Gateway, consulte Configurar NetScaler Gateway para que sea compatible con Enlightened Data Transport.

### Detección de MTU en EDT

La detección de MTU permite a EDT determinar automáticamente la unidad de transmisión máxima (MTU) al establecer una sesión. Al hacerlo, se evita la fragmentación de paquetes de EDT que podría provocar una degradación del rendimiento o un error al establecer una sesión.

La detección de MTU está habilitada de forma predeterminada. Si necesita inhabilitarla, consulte Funciones HDX administradas a través del registro para obtener más información.

> **Nota:**
>
> - **Fiabilidad de la sesión** debe estar habilitada para que Detección de MTU funcione.
> - La detección MTU con ICA multisecuencia está disponible a partir de la versión 2209 de VDA.

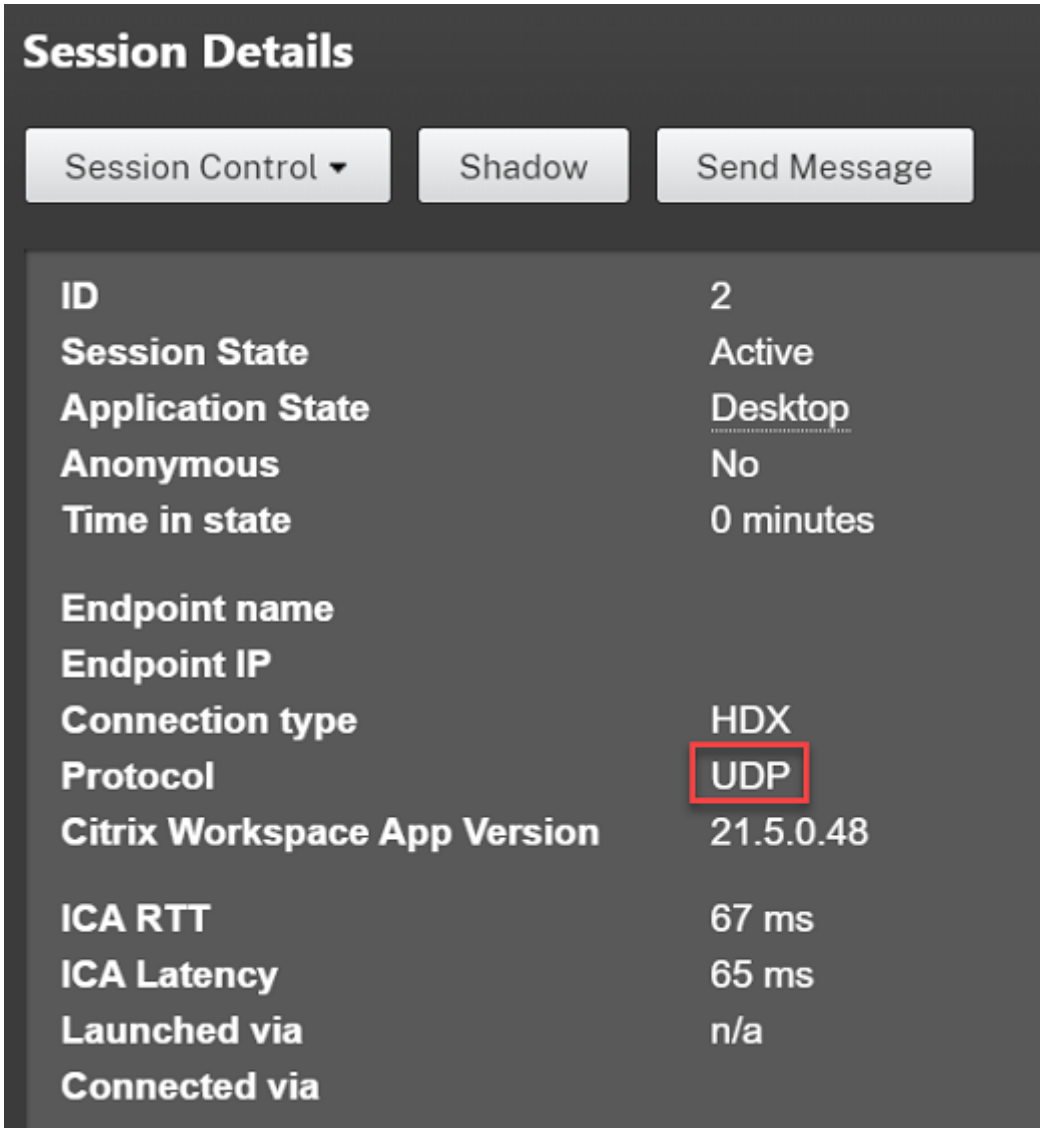
## Solución de problemas

May 17, 2024

Para confirmar que EDT se usa como protocolo de transporte de la sesión, puede utilizar Director o la utilidad de la línea de comandos `CtxSession.exe` en el VDA.

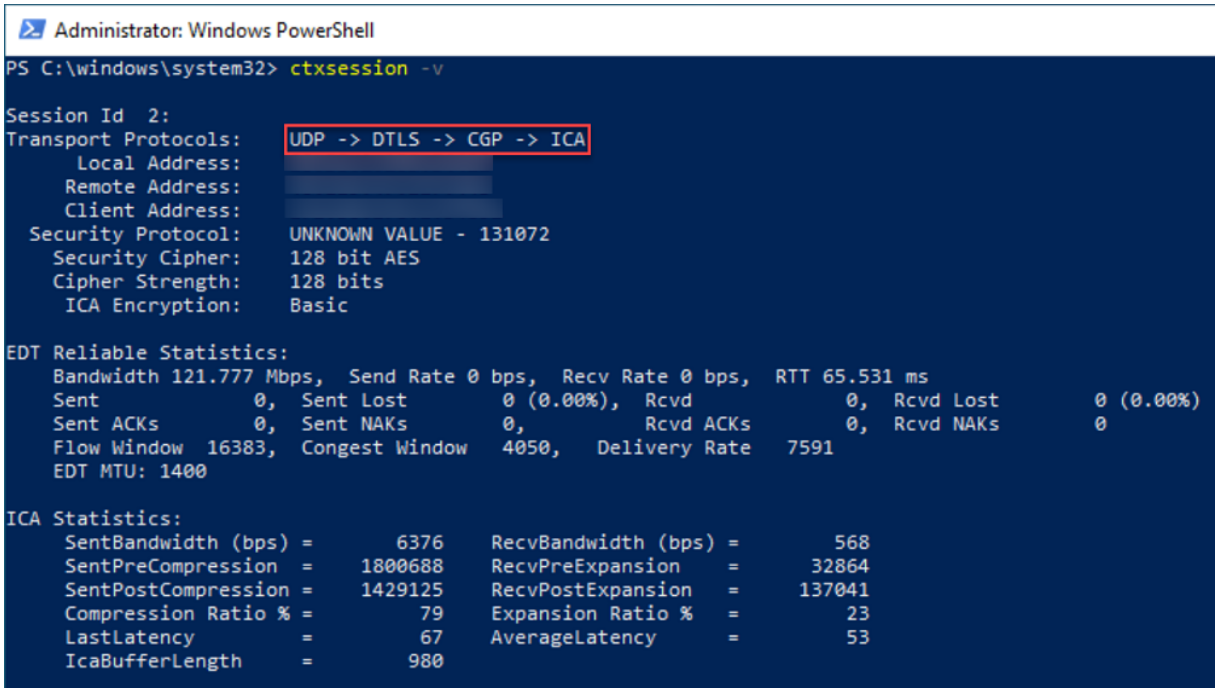
En Director, busque la sesión y seleccione **Detalles**. Si el **Tipo de conexión** es HDX y el **Protocolo** es UDP, EDT se usa como protocolo de transporte de la sesión.




Para usar la utilidad CtxSession.exe, inicie un símbolo del sistema o PowerShell dentro de la sesión y ejecute `ctxsession.exe`. Para ver estadísticas detalladas, ejecute `ctxsession.exe -v`. Si EDT se está usando, el protocolo de transporte muestra uno de estos elementos:

- **UDP > ICA** (fiabilidad de la sesión inhabilitada)
- **UDP > CGP > ICA** (fiabilidad de la sesión habilitada)
- **UDP > DTLS > CGP > ICA** (ICA está cifrada con DTLS de extremo a extremo)




### Cuando las sesiones no se conectan con EDT

Para solucionar problemas relacionados con el **transporte adaptable** y **EDT**, sugerimos lo siguiente:

1. Revise las secciones Requisitos del sistema, Requisitos de red, Problemas conocidos y Qué debe saber.
2. Compruebe si hay directivas de Citrix en Studio o GPO que sobrescriben la configuración de **HDX Adaptive Transport** deseada.
3. Compruebe si hay parámetros en el cliente que sobrescriben la configuración de HDX Adaptive Transport deseada. Puede ser una preferencia de GPO, un parámetro configurado mediante la plantilla administrativa opcional de la aplicación Workspace o una configuración manual del parámetro **HDXoverUDP** del Registro o del archivo de configuración del cliente.
4. En máquinas VDA con multisesión, compruebe que las escuchas UDP estén activas. Abra un símbolo del sistema en la máquina VDA y ejecute `netstat -a -p udp`. Para obtener más información, consulte Cómo confirmar el protocolo HDX Enlightened Data Transport.
5. Compruebe si se han configurado las reglas de firewall adecuadas tanto en los firewalls de la red como en los firewalls activos en las máquinas VDA.
6. Inicie una sesión directa internamente, omita NetScaler Gateway o Citrix Gateway Service y compruebe qué protocolo se usa. Si la sesión usa EDT, el VDA está listo para usar EDT para conexiones externas a través de NetScaler Gateway o Citrix Gateway Service.

7. Si EDT funciona para conexiones internas directas y no para sesiones que pasan por NetScaler Gateway o Citrix Gateway Service:
    - Compruebe que la **fiabilidad de la sesión** esté habilitada.
    - Si usa NetScaler Gateway, asegúrese de que su configuración cumpla con los requisitos descritos en Configurar NetScaler Gateway para que sea compatible con Enlightened Data Transport y HDX Insight.
8. Si usa Citrix Gateway Service, asegúrese de que Rendezvous esté habilitado y funcione.
9. Compruebe si las conexiones de sus usuarios requieren una MTU no estándar. Las conexiones con una MTU efectiva inferior a 1500 bytes provocan la fragmentación de paquetes EDT, lo que a su vez puede afectar al rendimiento o incluso impedir el inicio de sesiones. Este problema es común cuando se usan VPN, algunos puntos de acceso Wi-Fi y redes móviles, como 4G y 5G. Asegúrese de que tiene habilitada la detección de MTU o de que está configurando una MTU personalizada como se describe en How to configure MSS when using EDT on networks with non-standard MTU.

### Problemas conocidos

- Las rutas de red asimétricas pueden provocar que la detección de MTU falle en las conexiones que no pasan por NetScaler Gateway o Citrix Gateway Service. Para solucionar este problema, actualice la versión del VDA a la 2103 o a una posterior. [CVADHELP-16654]
- Al usar NetScaler Gateway, las rutas de red asimétricas pueden provocar un error en la detección de MTU. Esto se debe a un problema en Gateway que provoca que la parte Don't Fragment (DF) del encabezado de los paquetes EDT no se propague. Hay disponible una corrección para este problema, a partir de la versión de firmware 13.1 compilación 17.42. Para obtener información detallada sobre cómo habilitar la corrección, consulte la documentación de NetScaler Gateway. [CGOP-18438]
- La detección de MTU puede fallar para los usuarios que se conectan a través de una red DS-Lite. Algunos módems no respetan la parte DF cuando el procesamiento de paquetes está habilitado, lo que impide que la detección de MTU detecte la fragmentación. En esta situación, estas son las opciones disponibles:
    - Inhabilitar el procesamiento de paquetes en el módem del usuario.
    - Inhabilite la **detección de MTU** y use una MTU fija como se describe en How to configure MSS when using EDT on networks with non-standing MTU.
    - Inhabilitar el **transporte adaptable** para obligar a las sesiones a usar TCP. Si solo se ve afectado un subconjunto de usuarios, considere inhabilitarlo en el lado del cliente para que otros usuarios puedan seguir usando EDT.

# Protocolo Rendezvous

June 19, 2023

Cuando se utiliza Citrix Gateway Service, el protocolo Rendezvous permite que los VDA omitan los Citrix Cloud Connectors para conectarse de forma directa y segura con el plano de control de Citrix Cloud.

Hay dos tipos de tráfico que deben tenerse en cuenta:

1. Tráfico de control para registro de VDA e intermediación de sesiones.
2. Tráfico de sesiones HDX.

Hay dos versiones de Rendezvous disponibles:

- Versión 1 (V1): Admite solo omitir los Citrix Cloud Connectors para el tráfico de sesión HDX.
- Versión 2 (V2): Admite omitir los Citrix Cloud Connectors tanto para el tráfico de control como para el tráfico de sesión HDX.

Para obtener información detallada sobre los requisitos del sistema, las consideraciones y la configuración de cada una de las versiones de Rendezvous, consulte la documentación correspondiente.

Documentación de Rendezvous V1

Documentación de Rendezvous V2

# Rendezvous V1

April 21, 2023

Cuando se utiliza Citrix Gateway Service, el protocolo Rendezvous permite que los VDA omitan los Citrix Cloud Connectors para conectarse de forma directa y segura con el plano de control de Citrix Cloud.

## Requisitos

- Acceda al entorno mediante Citrix Workspace y Citrix Gateway Service.
- Plano de control: Citrix DaaS (Citrix Cloud).
- VDA: Versión 1912 o posterior.
  - La versión 2012 es la mínima requerida para Rendezvous con EDT.

  - La versión 2012 es la mínima requerida para compatibilidad con proxy no transparente (sin compatibilidad con archivos PAC).
  - La versión 2103 es la mínima requerida para la configuración de proxy con un archivo PAC.

- Habilite el protocolo Rendezvous en la directiva de Citrix. Para obtener más información, consulte Configuración de directiva del protocolo Rendezvous.
- Los agentes VDA deben tener acceso a `https://*.nssvc.net`, incluidos todos los subdominios. Si no puede agregar a la lista de permitidos todos los subdominios de esa manera, use `https://*.c.nssvc.net` y `https://*.g.nssvc.net` en su lugar. Para obtener más información, consulte la sección Requisitos de la conectividad a Internet de la documentación de Citrix Cloud (en Citrix DaaS) y el artículo CTX270584 de Knowledge Center.
- Los VDA deben poder conectarse a las direcciones mencionadas anteriormente en TCP 443 y UDP 443 para Rendezvous con TCP y Rendezvous con EDT, respectivamente.
- Los Cloud Connectors deben obtener los FQDN de los VDA al hacer de intermediarios en una sesión. Puede hacer esta tarea de una de estas dos maneras:
  - **Habilitar la resolución de DNS en el sitio.** Vaya a **Configuración completa > Parámetros** y active el parámetro **Habilitar resolución de DNS**. También puede usar el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops y ejecutar el comando `Set-BrokerSite -DnsResolutionEnabled $true`. Para obtener más información sobre el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops, consulte SDK y API.
  - **Zona de búsqueda inversa DNS con registros PTR para los agentes VDA.** Si elige esta opción, se recomienda configurar los VDA para que siempre intenten capturar registros PTR. Para ello, utilice el Editor de directivas de grupo u el objeto de directiva de grupo, vaya a **Configuración del equipo > Plantillas administrativas > Red > Cliente DNS** y establezca la opción de **capturar registros PTR** en **Habilitado y Registrar**. Si el sufijo DNS de la conexión no coincide con el sufijo DNS del dominio, también debe definir la configuración del **sufijo DNS específico de la conexión** para que las máquinas puedan capturar los registros PTR.

> **Nota:**
>
> Si se usa la opción de resolución de DNS, los Cloud Connectors deben poder resolver los nombres de dominio completos (FQDN) de las máquinas VDA. En caso de que los usuarios internos se conecten directamente a las máquinas VDA, los dispositivos cliente también deben poder resolver los FQDN de las máquinas VDA.
>
> Si se utiliza una zona de búsqueda inversa de DNS, los FQDN de los registros PTR deben coincidir con los FQDN de las máquinas VDA. Si el registro PTR contiene un nombre FQDN diferente, se produce un error en la conexión de Rendezvous. Por ejemplo, si el nombre

> de dominio completo (FQDN) de la máquina es `vda01.domain.net`, el registro PTR debe contener `vda01.domain.net`. Un nombre de dominio completo (FQDN) diferente como `vda01.sub.domain.net` no funciona.

## Configuración de proxy

Se pueden establecer conexiones Rendezvous a través de un proxy en el VDA.

### Consideraciones sobre servidores proxy

Tenga en cuenta lo siguiente al usar servidores proxy con Rendezvous:

- Se admiten proxies transparentes, HTTP no transparentes y SOCKS5.
- No se admite el descifrado y la inspección de paquetes. Configure una excepción para que el tráfico ICA entre el VDA y Gateway Service no se intercepte, descifre o inspeccione. De lo contrario, la conexión se interrumpe.
- Los proxies HTTP admiten la autenticación basada en máquina mediante protocolos de autenticación Negotiate y Kerberos o NT LAN Manager (NTLM).

  Cuando se conecta al servidor proxy, el esquema de autenticación Negotiate selecciona automáticamente el protocolo Kerberos. Si Kerberos no es compatible, Negotiate recurre a NTLM para la autenticación.

  > **Nota:**
  >
  > Para utilizar Kerberos, debe crear el nombre principal de servicio (SPN) para el servidor proxy y asociarlo a la cuenta de Active Directory del proxy. El VDA genera el SPN en el formato `HTTP/<proxyURL>` al establecer una sesión, donde la URL del proxy se obtiene de la configuración de directiva de **proxy Rendezvous**. Si no crea un SPN, la autenticación recurre a NTLM. En ambos casos, la identidad de la máquina VDA se utiliza para la autenticación.

- Actualmente, no se admite la autenticación con un proxy SOCKS5. Si utiliza un proxy SOCKS5 , deberá configurar una excepción para que el tráfico destinado a las direcciones de Gateway Service (especificadas en los requisitos) pueda omitir la autenticación.
- Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como el protocolo de transporte para ICA.

### Proxy transparente

Si utiliza un proxy transparente en la red, no se requiere configuración adicional en el VDA.

#### Proxy no transparente

Si utiliza un proxy no transparente en la red, configure el parámetro Configuración del proxy Rendezvous. Cuando la configuración está habilitada, especifique la dirección de proxy HTTP o SOCKS5, o bien introduzca la ruta al archivo PAC para que el VDA sepa qué proxy usar. Por ejemplo:

- Dirección de proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`
- Archivo PAC: `http://<URL or IP>/<path>/<filename>.pac`

Si utiliza el archivo PAC para configurar el proxy, defina el proxy con la sintaxis requerida por el servicio HTTP de Windows: `PROXY [<scheme>=]<URL or IP>:<port>`. Por ejemplo: `PROXY socks5=<URL or IP>:<port>`.

### Comprobación de Rendezvous

Si cumple todos los requisitos, siga estos pasos para comprobar si se utiliza Rendezvous:

1. Inicie PowerShell o un símbolo del sistema dentro de la sesión HDX.
2. Ejecute `ctxsession.exe –v`
3. Los protocolos de transporte en uso indicarán el tipo de conexión:
    - Rendezvous con TCP: **TCP - SSL - CGP - ICA**
    - Rendezvous con EDT: **UDP > DTLS > CGP > ICA**
    - Proxy a través de Cloud Connector: **TCP > CGP > ICA**

### Otras consideraciones

#### Orden de conjuntos de cifrado de Windows

Para un orden personalizado de los conjuntos de cifrado, debe incluir los conjuntos de cifrado compatibles con VDA que haya en la lista siguiente:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Si el orden personalizado de los conjuntos de cifrado no contiene estos conjuntos, falla la conexión de Rendezvous.

**Zscaler Private Access**

Si utiliza Zscaler Private Access (ZPA), se recomienda que configure las opciones de omisión para Gateway Service si quiere evitar una mayor latencia y el impacto que conlleva esta latencia en el rendimiento. Para ello, debe definir segmentos de aplicaciones para las direcciones de Gateway Service (especificadas en los requisitos) y establecerlos de modo que la omisión sea permanente. Si quiere obtener información sobre cómo configurar segmentos de aplicaciones para omisiones de ZPA, consulte la documentación de Zscaler.

## Rendezvous V2

May 17, 2024

Cuando se utiliza Citrix Gateway Service, el protocolo Rendezvous permite que los VDA omitan los Citrix Cloud Connectors para conectarse de forma directa y segura con el plano de control de Citrix Cloud.

Rendezvous V2 es compatible con máquinas unidas a un dominio estándar, máquinas unidas a Azure AD híbrido, máquinas unidas a Azure AD y máquinas no unidas a un dominio.

> **Nota:**
>
> En la actualidad, las implementaciones sin conector solo son posibles con máquinas *unidas a Azure AD* y *no unidas a ningún dominio*. Las máquinas unidas a un dominio de AD estándar y las máquinas unidas a Azure AD híbrido aún requieren Cloud Connectors para el registro de VDA y la intermediación de sesiones. Sin embargo, no hay requisitos de DNS para usar Rendezvous V2.
>
> Los requisitos de Cloud Connector para otras funciones no relacionadas con la comunicación de los VDA, como la conexión al dominio de AD local o el aprovisionamiento de MCS a hipervisores locales, siguen siendo los mismos.

### Requisitos

Los requisitos para usar Rendezvous V2 son:

- Acceso al entorno mediante Citrix Workspace y Citrix Gateway Service
- Plano de control: Citrix DaaS
- Versión 2203 de VDA
- Habilite el protocolo Rendezvous en la directiva de Citrix. Para obtener más información, consulte Configuración de directiva del protocolo Rendezvous.

- Fiabilidad de la sesión debe estar habilitada en los VDA
- Las máquinas VDA deben tener acceso a:
  - `https://*.xendesktop.net` en `TCP 443`. Si no puede permitir todos los subdominios de esa manera, puede usar `https://<customer_ID>.xendesktop.net`, donde <customer_ID> es su ID de cliente de Citrix Cloud, tal y como se muestra en el portal de administradores de Citrix Cloud.
  - `https://*.*.nssvc.net` en `TCP 443` para la conexión de control con Gateway Service.
  - `https://*.*.nssvc.net` en `TCP 443` y `UDP 443` para sesiones HDX a través de TCP y EDT, respectivamente.

> **Nota:**
>
> Si no puede autorizar todos los subdominios con `https://*.*.nssvc.net`, puede usar `https://*.c.nssvc.net` y `https://*.g.nssvc.net` en su lugar. Para obtener más información, consulte el artículo CTX270584 de Knowledge Center.

## Configuración de proxy

El VDA admite la conexión a través de proxy tanto para el tráfico de control como para el tráfico de sesiones HDX cuando se usa Rendezvous. Los requisitos y consideraciones para ambos tipos de tráfico son diferentes, así que revíselos detenidamente.

### Consideraciones sobre el proxy de tráfico

- Solo se admiten proxies HTTP.
- No se admite el descifrado y la inspección de paquetes. Configure una excepción para que el tráfico de control entre el VDA y el plano de control de Citrix Cloud no se intercepte, descifre ni inspeccione. De lo contrario, la conexión falla.
- No se admite la autenticación de proxy.

### Consideraciones sobre el proxy de tráfico HDX

- Se admiten los proxies HTTP y SOCKS5.
- EDT solo se puede usar con proxies SOCKS5.
- De forma predeterminada, el tráfico HDX usa el proxy definido para el tráfico de control. Si debe usar un proxy diferente para el tráfico HDX, ya sea un proxy HTTP diferente o un proxy SOCKS5, use la configuración de directiva Configuración del proxy de Rendezvous.

- No se admite el descifrado y la inspección de paquetes. Configure una excepción para que el tráfico HDX entre el VDA y el plano de control de Citrix Cloud no se intercepte, descifre ni inspeccione. De lo contrario, la conexión falla.
- La autenticación basada en máquina solo se admite con proxies HTTP y si la máquina VDA está unida a un dominio de AD. Puede usar autenticación Negotiate/Kerberos o NTLM.

  > **Nota:**
  >
  > Para utilizar Kerberos, cree el nombre principal de servicio (SPN) para el servidor proxy y asociarlo a la cuenta de Active Directory del proxy. El VDA genera el SPN en el formato `HTTP/<proxyURL>` al establecer una sesión, donde la URL del proxy se obtiene de la configuración de directiva Configuración del proxy de Rendezvous. Si no crea un SPN, la autenticación recurre a NTLM. En ambos casos, la identidad de la máquina VDA se utiliza para la autenticación.

- Actualmente, no se admite la autenticación con un proxy SOCKS5. Si utiliza un proxy SOCKS5, configure una excepción para que el tráfico destinado a las direcciones de Gateway Service (especificadas en los requisitos) pueda omitir la autenticación.
- Solo los proxies SOCKS5 admiten el transporte de datos a través de EDT. Para un proxy HTTP, utilice TCP como el protocolo de transporte para ICA.

#### Proxy transparente

Si utiliza un proxy transparente en la red, no se requiere configuración adicional en el VDA.

#### Proxy no transparente

Si utiliza un proxy no transparente en la red, especifique ese proxy durante la instalación del VDA, de manera que el tráfico de control pueda llegar al plano de control de Citrix Cloud. Revise las consideraciones del proxy de tráfico de control antes de continuar con la instalación y la configuración.

En el asistente de instalación del VDA, seleccione **Configuración del proxy de Rendezvous** en la página **Componentes adicionales**. Esta opción hace que la página **Configuración del proxy de Rendezvous** esté disponible más adelante en el asistente de instalación. Una vez aquí, introduzca la dirección del proxy o la ruta del archivo PAC para que el VDA sepa qué proxy debe usar. Por ejemplo:

- Dirección proxy: `http://<URL or IP>:<port>`
- Archivo PAC: `http://<URL or IP>/<path/<filename>.pac`

Como se indica en las consideraciones sobre el proxy de tráfico HDX, el tráfico HDX utiliza, de forma predeterminada, el proxy definido durante la instalación del VDA. Si debe usar un proxy diferente para

el tráfico HDX, ya sea un proxy HTTP diferente o un proxy SOCKS5, use la configuración de directiva Configuración del proxy de Rendezvous. Cuando la configuración esté habilitada, especifique la dirección de proxy HTTP o SOCKS5. También puede introducir la ruta al archivo PAC para que el VDA sepa qué proxy debe usar. Por ejemplo:

- Dirección de proxy: `http://<URL or IP>:<port>` o `socks5://<URL or IP>:<port>`
- Archivo PAC: `http://<URL or IP>/<path/<filename>.pac`

Si utiliza el archivo PAC para configurar el proxy, defina el proxy con la sintaxis requerida por el servicio HTTP de Windows: `PROXY [<scheme>=]<URL or IP>:<port>`. Por ejemplo, `PROXY socks5=<URL or IP>:<port>`.

### Cómo configurar Rendezvous

A continuación, se muestran los pasos necesarios para configurar Rendezvous en su entorno:

1. Compruebe que se cumplen todos los requisitos.
2. Si debe usar un proxy HTTP no transparente en su entorno, configúrelo durante la instalación del VDA. Consulte la sección sobre configuración de proxy para obtener más información.
3. Reinicie la máquina VDA una vez finalizada la instalación.
4. Cree una directiva de Citrix o modifique una existente:
    - Establezca el parámetro **Protocolo Rendezvous** en **Permitido**.
    - Si debe configurar un proxy HTTP o SOCKS5 para el tráfico HDX, configure el parámetro **Configuración del proxy de Rendezvous**.
    - Asegúrese de que los filtros de directivas de Citrix estén configurados correctamente. La directiva se aplica a las máquinas que necesitan habilitar Rendezvous.
5. Compruebe que la directiva de Citrix tenga la prioridad correcta para que no sobrescriba a otra.

> **Nota:**
>
> Si usa la versión 2308 de VDA o una anterior, se usa V1 de forma predeterminada. Para obtener más información sobre cómo configurar la versión que se va a utilizar, consulte Funciones HDX administradas a través del registro.

#### Comprobación de Rendezvous

Si cumple con todos los requisitos y ha completado la configuración, siga estos pasos para comprobar si se utiliza Rendezvous:

1. En el escritorio virtual, abra un símbolo del sistema o PowerShell.

2. Ejecute `ctxsession.exe -v`.
3. Los protocolos de transporte en uso indican el tipo de conexión:

    - Rendezvous con TCP: TCP - SSL - CGP - ICA
    - Rendezvous con EDT: UDP > DTLS > CGP > ICA
    - No Rendezvous: TCP > CGP > ICA

4. La versión de Rendezvous mostrada indica la versión en uso.

## Otras consideraciones

### Orden de conjuntos de cifrado de Windows

Si el orden de los conjuntos de cifrado se ha modificado en las máquinas VDA, asegúrese de incluir los conjuntos de cifrado compatibles con el VDA:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Si el orden personalizado de los conjuntos de cifrado no contiene estos conjuntos, falla la conexión de Rendezvous.

### Zscaler Private Access

Si utiliza Zscaler Private Access (ZPA), se recomienda que configure las opciones de omisión para Gateway Service si quiere evitar una mayor latencia y el impacto que conlleva esta latencia en el rendimiento. Para ello, debe definir segmentos de aplicaciones para las direcciones de Gateway Service (especificadas en los requisitos) y establecerlos de modo que la omisión sea permanente. Si quiere obtener información sobre cómo configurar segmentos de aplicaciones para omisiones de ZPA, consulte la documentación de Zscaler.

## Problemas conocidos

### El instalador de VDA 2203 no permite introducir una barra diagonal (/) para la dirección de proxy

Como solución temporal, puede configurar el proxy en el Registro después de instalar el VDA:

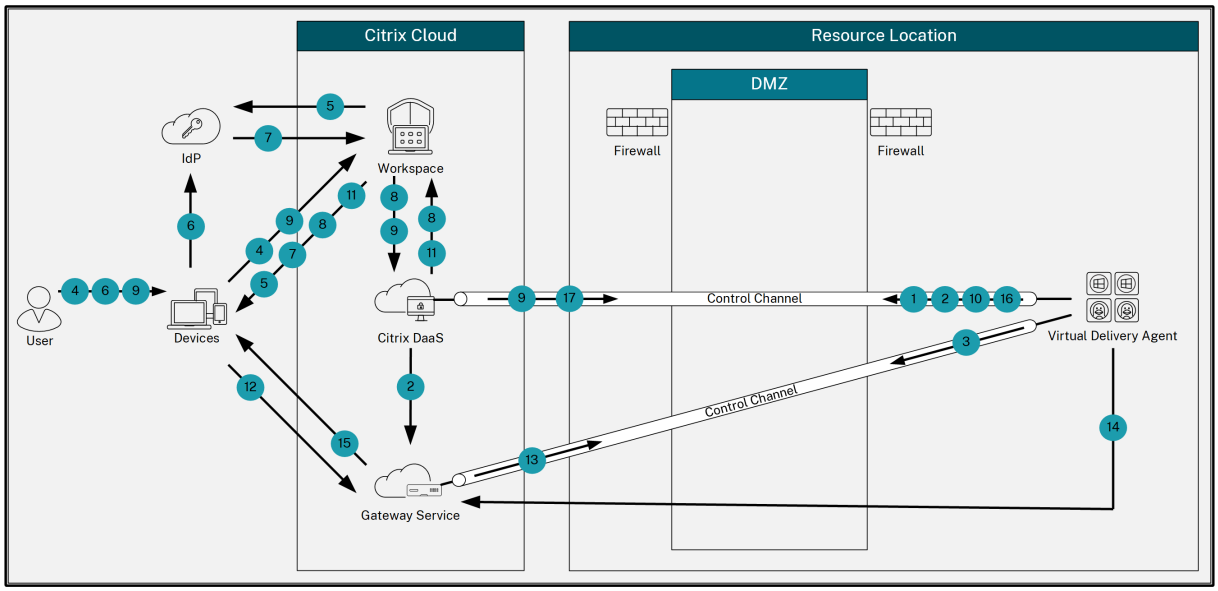
```
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\VirtualDesktopAgent
Value type: String
Value name: ProxySettings
```

```
4               Value data: Proxy address or path to pac file. For example:
5                   Proxy address: http://squidk.test.local:3128
6                   Pac file: http://file.test.com/config/proxy.pac
```

### Flujo de tráfico de Rendezvous

En el siguiente diagrama, se ilustra la secuencia de pasos en el flujo de tráfico de Rendezvous.




1. El VDA establece una conexión de WebSockets con Citrix Cloud y se registra.
2. El VDA se registra en Citrix Gateway Service y obtiene un token dedicado.
3. El VDA establece una conexión de control persistente con Gateway Service.
4. El usuario navega a Citrix Workspace.
5. Workspace evalúa la configuración de la autenticación y redirige a los usuarios al proveedor de identidades (IdP) adecuado para la autenticación.
6. El usuario introduce sus credenciales.
7. Tras validarse correctamente las credenciales de usuario, se redirige a este a Workspace.
8. Workspace hace recuento de los recursos del usuario y los muestra.
9. El usuario selecciona un escritorio o una aplicación de Workspace. Workspace envía la solicitud a Citrix DaaS, que hace de intermediario en la conexión e indica al VDA que se prepare para la sesión.
10. El VDA responde con la funcionalidad Rendezvous y su identidad.
11. Citrix DaaS genera un tíquet de inicio y lo envía al dispositivo del usuario a través de Workspace.
12. El dispositivo de punto final del usuario se conecta a Gateway Service y proporciona el tíquet de inicio para autenticar e identificar el recurso al que conectarse.
13. Gateway Service envía la información de conexión al VDA.
14. El VDA establece una conexión directa para la sesión con Gateway Service.

15. Gateway Service completa la conexión entre el dispositivo de punto final y el VDA.
16. El VDA verifica las licencias de la sesión.
17. Citrix DaaS envía las directivas aplicables al VDA.

## HDX Direct (Technical Preview)

June 13, 2024

Al acceder a los recursos entregados por Citrix, HDX Direct permite que los dispositivos cliente internos y externos establezcan una conexión directa segura con el host de la sesión si es posible la comunicación directa.

> **Importante:**
>
> HDX Direct se encuentra actualmente en versión Technical Preview. Esta función se proporciona sin asistencia y aún no se recomienda su uso en entornos de producción. Para enviar comentarios o notificar problemas, use este formulario.

### Requisitos del sistema

Estos son los requisitos para usar HDX Direct:

- Plano de control
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 o posterior
- Virtual Delivery Agent (VDA)
  - Windows: versión 2402 o posterior
- Aplicación Workspace
  - Windows: versión 2402 o posterior
- Nivel de acceso
  - Citrix Gateway Service y Citrix Workspace
  - Citrix Workspace con NetScaler Gateway
- Otros
  - El transporte adaptable debe estar habilitado para las conexiones directas externas

## Requisitos de la red

Estos son los requisitos de la red para usar HDX Direct.

### Hosts de sesión

Si los hosts de la sesión tienen un firewall como el Firewall de Windows Defender, debe permitir el siguiente tráfico entrante para las conexiones internas.

| Descripción | Origen | Protocolo | Puerto |
|---|---|---|---|
| Conexión interna directa | Cliente | TCP | 443 |
| Conexión interna directa | Cliente | UDP | 443 |

> Nota:
>
> El instalador del VDA agrega las reglas de entrada apropiadas al Firewall de Windows Defender. Si usa un firewall diferente, debe agregar las reglas anteriores.

### Red del cliente

En la tabla siguiente se describe la red de clientes para usuarios internos y externos.

#### Usuarios internos

| Descripción | Protocolo | Origen | Puerto de origen | Destino | Puerto de destino |
|---|---|---|---|---|---|
| Conexión interna directa | TCP | Red del cliente | 1024–65535 | Red VDA | 443 |
| Conexión interna directa | UDP | Red del cliente | 1024–65535 | Red VDA | 443 |

#### Usuarios externos

| Descripción | Protocolo | Origen | Puerto de origen | Destino | Puerto de destino |
|---|---|---|---|---|---|
| STUN (solo usuarios externos) | UDP | Red del cliente | 1024–65535 | Internet (ver nota más abajo) | 3478, 19302 |
| Conexión de usuarios externos | UDP | Red del cliente | 1024–65535 | Dirección IP pública del centro de datos | 1024–65535 |

**Red de centros de datos**

En la siguiente tabla se describe la red del centro de datos para usuarios internos y externos.

**Usuarios internos**

| Descripción | Protocolo | Origen | Puerto de origen | Destino | Puerto de destino |
|---|---|---|---|---|---|
| Conexión interna directa | TCP | Red del cliente | 1024–65535 | Red VDA | 443 |
| Conexión interna directa | UDP | Red del cliente | 1024–65535 | Red VDA | 443 |

**Usuarios externos**

| Descripción | Protocolo | Origen | Puerto de origen | Destino | Puerto de destino |
|---|---|---|---|---|---|
| STUN (solo usuarios externos) | UDP | Red VDA | 1024–65535 | Internet (ver nota más abajo) | 3478, 19302 |
| Conexión de usuarios externos | UDP | DMZ/ Red interna | 1024–65535 | Red VDA | 55000–55250 |

| Descripción | Protocolo | Origen | Puerto de origen | Destino | Puerto de destino |
|---|---|---|---|---|---|
| Conexión de usuarios externos | UDP | Red VDA | 55000–55250 | IP pública del cliente | 1024–65535 |

> **Nota:**
>
> Tanto el VDA como la aplicación Workspace intentan enviar solicitudes STUN a los siguientes servidores en el mismo orden:
>
> - stunserver.stunprotocol.org:3478
> - employees.org:3478
> - stun.l.google.com:19302
>
> Si cambia el intervalo de puertos predeterminado para las conexiones de usuarios externos mediante la configuración de directiva de **intervalo de puertos de HDX Direct**, las reglas de firewall correspondientes deben coincidir con su intervalo de puertos personalizado.

### Configuración

HDX Direct está inhabilitado de forma predeterminada. Puede configurar esta función mediante el parámetro **HDX Direct** de la directiva de Citrix.

- **HDX Direct**: para habilitar o inhabilitar una función.
- **Modo HDX Direct**: determina si **HDX Direct** está disponible solo para clientes internos o para clientes internos y externos.
- **Intervalo de puertos de HDX Direct**: define el intervalo de puertos que usa el VDA para las conexiones desde clientes externos.

### Consideraciones

Estos son los aspectos a tener en cuenta al usar HDX Direct:

- HDX Direct para usuarios externos solo está disponible con EDT (UDP) como protocolo de transporte. Por lo tanto, el **transporte adaptable** debe estar habilitado.
- Si usa **HDX Insight**, tenga en cuenta que el uso de **HDX Direct** impide la recopilación de datos de HDX Insight, ya que la sesión ya no se redirigiría mediante proxy a través de NetScaler Gateway.
- Cuando use máquinas no persistentes para sus Virtual Apps and Desktops, Citrix recomienda habilitar **HDX Direct** en los hosts de sesión en lugar de en la imagen maestra o de plantilla para que cada máquina genere sus propios certificados.

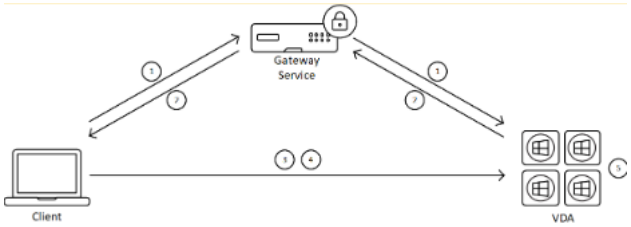
- Actualmente, no es compatible el uso de sus propios certificados con HDX Direct.

## Funcionamiento

HDX Direct permite a los clientes establecer una conexión directa con el host de la sesión cuando hay una comunicación directa disponible. Cuando se realizan conexiones directas mediante HDX Direct, se usan los certificados autofirmados para protegerlas con el cifrado a nivel de red (TLS/DTLS).

### Usuarios internos

El diagrama siguiente muestra el proceso general de conexión de usuarios internos con HDX Direct.



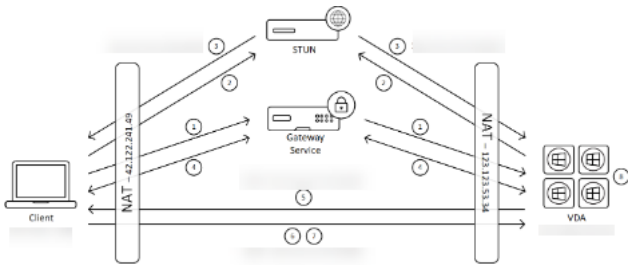

1. El cliente establece una sesión HDX a través del Gateway Service.
2. Una vez realizada la conexión, el VDA envía al cliente el nombre de dominio completo (FQDN) de la máquina VDA, una lista de sus direcciones IP y el certificado de la máquina VDA a través de la conexión HDX.
3. El cliente sondea las direcciones IP para ver si pueden comunicarse directamente con el VDA.
4. Si el cliente puede acceder al VDA directamente con cualquiera de las direcciones IP compartidas, establece una conexión directa con el VDA, protegida con (D)TLS, mediante un certificado que coincide con el intercambiado en el paso (2).
5. Una vez que la conexión directa se haya establecido correctamente, la sesión se transferirá a la nueva conexión, y se cancelará la conexión con Gateway Service.

> **Nota:**
>
> Tras establecer la conexión en el paso 2 anterior, la sesión está activa. Los pasos posteriores no provocan ninguna demora ni interfieren con la capacidad del usuario para usar la aplicación o el escritorio virtuales. Si se produce un error en alguno de los pasos posteriores, se mantiene la conexión a través de Gateway sin interrumpir la sesión del usuario.

### Usuarios externos

El diagrama siguiente muestra el proceso general de conexión de usuarios externos con HDX Direct:




1. El cliente establece una sesión HDX a través del Gateway Service.
2. Tras establecerse la conexión, tanto el cliente como el VDA envían una solicitud STUN para detectar sus puertos y direcciones IP públicas.
3. El servidor STUN responde al cliente y al VDA con sus puertos y direcciones IP públicas correspondientes.
4. A través de la conexión HDX, el cliente y el VDA intercambian sus direcciones IP públicas y sus puertos UDP, y el VDA envía su certificado al cliente.
5. El VDA envía paquetes UDP a la dirección IP pública y al puerto UDP del cliente. El cliente envía paquetes UDP a la dirección IP pública y al puerto UDP del VDA.
6. Al recibir un mensaje del VDA, el cliente responde con una solicitud de conexión segura.
7. Durante el protocolo de enlace (handshake) DTLS, el cliente verifica que el certificado coincide con el certificado intercambiado en el paso (4). Tras la validación, el cliente envía su token de autorización. Ahora se ha establecido una conexión directa segura.
8. Una vez que la conexión directa se haya establecido correctamente, la sesión se transferirá a la nueva conexión, y se cancelará la conexión con Gateway Service.

> **Nota:**
>
> Tras establecer la conexión en el paso 2 anterior, la sesión está activa. Los pasos posteriores no provocan ninguna demora ni interfieren con la capacidad del usuario para usar la aplicación o el escritorio virtuales. Si se produce un error en alguno de los pasos posteriores, se mantiene la conexión a través de Gateway sin interrumpir la sesión del usuario.

## Administración de certificados

### Host de la sesión

Los dos servicios siguientes de la máquina VDA gestionan la creación y la administración de certificados, y ambos están configurados para ejecutarse automáticamente al iniciar la máquina:

- Citrix ClxMtp Service: Responsable de la generación y la rotación de certificados de CA.
- Citrix Certificate Manager Service: Responsable de la generación y la administración del certificado de CA raíz autofirmado y los certificados de la máquina.

Los siguientes pasos describen el proceso de administración de certificados:

1. Los servicios se inician al iniciar la máquina.
2. `Citrix ClxMtp Service` crea claves si aún no se creó ninguna.
3. Citrix Certificate Manager Service comprueba si **HDX Direct** está habilitado. De lo contrario, el servicio se detiene solo.
4. Si **HDX Direct** está habilitado, Citrix Certificate Manager Service comprueba si existe un certificado de CA raíz autofirmado. De lo contrario, se crea un certificado raíz autofirmado.
5. Una vez que haya un certificado de CA raíz disponible, Citrix Certificate Manager Service comprueba si existe un certificado de máquina autofirmado. De lo contrario, el servicio genera claves y crea un certificado mediante el FQDN de la máquina.
6. Si existe un certificado de máquina creado por Citrix Certificate Manager Service, y el nombre del asunto no coincide con el FQDN de la máquina, se genera un certificado nuevo.

> **Nota:**
>
> Citrix Certificate Manager Service genera certificados RSA que emplean claves de 2048 bits.

#### Dispositivo cliente

Para establecer correctamente una conexión segura de **HDX Direct**, el cliente debe confiar en los certificados utilizados para proteger la sesión. Para facilitar esto, el cliente recibe el certificado de CA para la sesión a través del archivo ICA (suministrado por Workspace), por lo que no es necesario distribuir los certificados de CA a los almacenes de certificados de los dispositivos cliente.

## Compatibilidad con NAT

June 12, 2024

Para establecer una conexión directa entre un dispositivo de usuario externo y el host de la sesión, HDX Direct utiliza una técnica conocida como "hole punching"(perforación de agujeros) para NAT transversal y STUN a fin de facilitar el intercambio de la dirección IP pública y las asignaciones de puertos para el dispositivo cliente y el host de la sesión. Es algo parecido a cómo funcionan las soluciones VoIP, comunicaciones unificadas y P2P.

Siempre que los firewalls y otros componentes de red estén configurados para permitir el tráfico UDP para las solicitudes STUN y las sesiones HDX, se prevé que HDX Direct para los usuarios externos funcione. Sin embargo, hay algunos casos en los que los tipos de NAT de las redes de usuario y host de sesión dan lugar a una combinación incompatible, lo que provoca el error de HDX Direct.

### Validaciones

Puede validar el tipo de NAT en el cliente y el host de la sesión mediante la utilidad de cliente STUN de STUNTMAN:

1. Descargue el paquete correspondiente a la plataforma de destino desde stunprotocol.org y extraiga el contenido.
2. Abra un el símbolo del sistema en un terminal y vaya al directorio donde se extrajo el contenido.
3. Ejecute este comando:
   `.\stunclient.exe stunserver.stunprotocol.org --mode behavior`
4. Tome nota del resultado.

Si las pruebas de enlace y comportamiento se realizan correctamente, tanto la **prueba de enlace** como la **prueba de comportamiento** informan de su correcta realización y se especifica un comportamiento de NAT:


Si las pruebas fallan, tanto la **prueba de enlace** como la **prueba de comportamiento** informan de la falla.


Consulte la siguiente tabla para determinar si se prevé que HDX Direct funcione para los usuarios externos conforme a los resultados de las pruebas del cliente y del host de sesión:

| Dispositivo cliente | Host de la sesión | ¿Se prevé que funcione? |
|---|---|---|
| Asignación independiente de los dispositivos de punto final | Asignación independiente de los dispositivos de punto final | Sí |
| Asignación independiente de los dispositivos de punto final | Asignación dependiente de los dispositivos de punto final | Sí |
| Asignación dependiente de los dispositivos de punto final | Asignación independiente de los dispositivos de punto final | Sí |
| Asignación dependiente de los dispositivos de punto final | Asignación dependiente de los dispositivos de punto final | No |
| Asignación dependiente de la dirección y el puerto | Cualquier tipo de NAT | No |

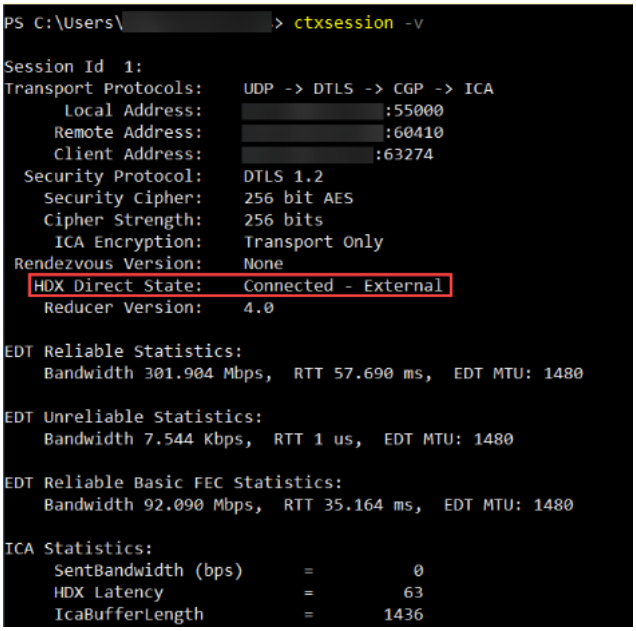
| Dispositivo cliente | Host de la sesión | ¿Se prevé que funcione? |
|---|---|---|
| Cualquier tipo de NAT | Asignación dependiente de la dirección y el puerto | No |
| error | Cualquier tipo de NAT | No |
| Cualquier tipo de NAT | error | No |
| error | error | No |

## Solución de problemas

January 24, 2024

Para confirmar que **HDX Direct** haya establecido correctamente una conexión directa, puede usar la utilidad `CtxSession.exe` en la máquina VDA.

Para usar la utilidad `CtxSession.exe`, inicie un símbolo del sistema o PowerShell dentro de la sesión y ejecute `ctxsession.exe -v`. Si la conexión **HDX Direct** se establece correctamente, el **estado de HDX Direct** es `Connected`.




También puede consultar los registros de eventos del host de la sesión para obtener información sobre si la conexión HDX Direct se estableció correctamente o no. Para obtener más información, consulte la sección **Registros de eventos**.

> Nota:
>
> En función del entorno y la cantidad de direcciones IP disponibles para los hosts de sesión, la conexión HDX Direct puede tardar hasta 5 minutos en establecerse.

### Cuando HDX Direct no puede establecer una conexión directa

Si HDX Direct no puede establecer una conexión directa, revise los pasos siguientes:

1. Asegúrese de que la versión del VDA y la versión de la aplicación Workspace en uso son compatibles con la función según los requisitos del sistema.
2. Confirme que se ha aplicado una directiva al VDA que habilita HDX Direct y que no hay otras directivas con mayor prioridad que inhabilitan la función.
3. Confirme que se ha aplicado una directiva al VDA que establece el modo HDX Direct deseado y que no hay otras directivas con mayor prioridad que sobrescriben la configuración.
4. Asegúrese de que el servicio Citrix ClxMtp se esté ejecutando en el host de la sesión.
5. Asegúrese de que Citrix Certificate Manager Service se esté ejecutando en el host de la sesión. Si no se está ejecutando, pruebe a iniciarlo manualmente. El servicio se detiene automáticamente si HDX Direct está inhabilitado.
6. Compruebe si el host de la sesión tiene su propio certificado de CA raíz autofirmado:
    a) Emitido para: `CA-<hostname>` (por ejemplo, CA-FTLW11-001)
    b) Emitido por: `CA-<hostname>` (por ejemplo, CA-FTLW11-001)
    c) Detalles del emisor: La organización es Citrix Systems, Inc.
7. Compruebe si el host de la sesión tiene su propio certificado de servidor autofirmado:
    a) Emitido para: `<host FQDN>` (por ejemplo, FTLW11-001.ctxlab.net)
    b) Emitido por: `CA-<hostname>` (por ejemplo, CA-FTLW11-001)
    c) Detalles del emisor: La organización es Citrix Systems, Inc.
8. Si faltan los certificados, contacte con la asistencia técnica de Citrix.
9. Si los certificados están presentes:
    a) Detenga Citrix Certificate Manager Service en el host de la sesión.
    b) Elimine tanto el certificado de CA raíz autofirmado como el certificado de servidor autofirmado.
    c) Inicie Citrix Certificate Manager Service en el host de la sesión. El servicio crea nuevos certificados una vez que se inicia.
10. Para usuarios internos:
    a) Asegúrese de que el firewall del host de la sesión no bloquee el tráfico entrante en UDP 443 o TCP 443, para HDX por EDT y HDX por TCP, respectivamente.

b) Asegúrese de que su firewall de red no bloquee el tráfico en UDP 443 y TCP 443 entre la red de sus clientes y la red de los hosts de sesión.

11. Para usuarios externos:

a) Compruebe el tipo de NAT para el cliente y el host de sesión y asegúrese de que se prevé que la combinación funcione. Para obtener más información, consulte la sección Compatibilidad con NAT.
b) Si la prueba de NAT falla en el cliente o en el host de la sesión:
   i. Si hay un firewall ejecutándose en el sistema, asegúrese de que no esté bloqueando el tráfico saliente en UDP 3478.
   ii. Asegúrese de que los firewalls de red no bloqueen el tráfico saliente en UDP 3478.
   iii. Asegúrese de que los firewalls no bloqueen la respuesta del servidor STUN.
c) Asegúrese de que los firewalls de red tengan configuradas las reglas adecuadas para permitir todo el tráfico necesario. Para obtener más información, consulte la sección Requisitos de la red.
d) Si cambia el intervalo de puertos predeterminado mediante la configuración de directiva Intervalo de puertos HDX Direct, asegúrese de que las reglas de firewall estén configuradas para el intervalo de puertos personalizado.

### Registros de eventos

Los siguientes eventos se registran en el registro de eventos de la máquina VDA:

| Registro | ID | Origen | Nivel | Descripción |
|---|---|---|---|---|
| Registros de aplicaciones y servicios > Citrix-HostCore-HDX Direct/Operational | 1 | HDX Direct | Información | Se estableció la conexión HDX Direct para el usuario <username> interno. |
| Registros de aplicaciones y servicios > Citrix-HostCore-HDX Direct/Operational | 2 | HDX Direct | Información | Se estableció la conexión HDX Direct para el usuario <username> externo. |

| Registro | ID | Origen | Nivel | Descripción |
|---|---|---|---|---|
| Registros de aplicaciones y servicios > Citrix-HostCore-HDX Direct/Operational | 3 | HDX Direct | Información | Error en la conexión HDX Direct para el usuario <username>. |

### Problemas conocidos

Es posible que HDX Direct deje de funcionar después de realizar una actualización en contexto de la versión del VDA en una máquina que ya tenga **HDX Direct** habilitado.
Para resolver el problema, siga estos pasos:

1. Detenga Citrix Certificate Manager Service en el host de la sesión.
2. Elimine el certificado de CA raíz autofirmado y el certificado de servidor autofirmado.
3. Abra el registro.
4. Elimine la clave `HKLM\Software\Citrix\HDX-Direct`.
5. Vaya a `HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\icawd`.
6. Establezca el valor de **SSLEnabled** en `0`.
7. Elimine el contenido del valor de **SSLThumbprint**.
8. Inicie **Citrix Certificate Manager Service**.

## Secure HDX (Tech Preview)

June 12, 2024

Secure HDX es una solución de cifrado a nivel de aplicación (ALE) que impide que ningún elemento de la red en la ruta del tráfico pueda inspeccionar el tráfico HDX. Para ello, proporciona un verdadero cifrado de extremo a extremo (E2EE) a nivel de aplicación entre la aplicación Citrix Workspace (cliente) y el VDA (host de sesión) mediante el cifrado AES-256-GCM.

> **Importante:**
>
> Secure HDX se encuentra actualmente en Technical Preview. Esta función se proporciona sin

> asistencia y aún no se recomienda su uso en entornos de producción. Para enviar comentarios o notificar problemas, use este formulario.

### Requisitos del sistema

La siguiente lista describe los requisitos del sistema para usar Secure HDX.

- Plano de control
  - Citrix DaaS
  - Citrix Virtual Apps and Desktops 2402 o posterior
- Virtual Delivery Agent (VDA)
  - Windows: versión 2402 o posterior
- Aplicación Workspace
  - Windows: versión 2402 o posterior
- Nivel de acceso
  - Citrix Workspace
  - Citrix StoreFront 2402 o posterior

### Configuración

Secure HDX está inhabilitado de forma predeterminada. Puede configurar esta función mediante el parámetro Secure HDX de la directiva de Citrix:

**Secure HDX**: define si se debe habilitar la función para todas las sesiones, solo para las conexiones directas, o si se inhabilita.

### Consideraciones

Estas son algunas consideraciones para usar Secure HDX:

- Si un usuario intenta conectarse a un host de sesión con Secure HDX habilitado usando un cliente que no admite esta función, se denegará la conexión.
- Si usa HDX Insight, tenga en cuenta que el uso de Secure HDX impide la recopilación de datos de HDX Insight, ya que NetScaler no puede inspeccionar el tráfico HDX cifrado. Si debe usar HDX Insight, puede configurar Secure HDX para que solo se habilite para conexiones directas.

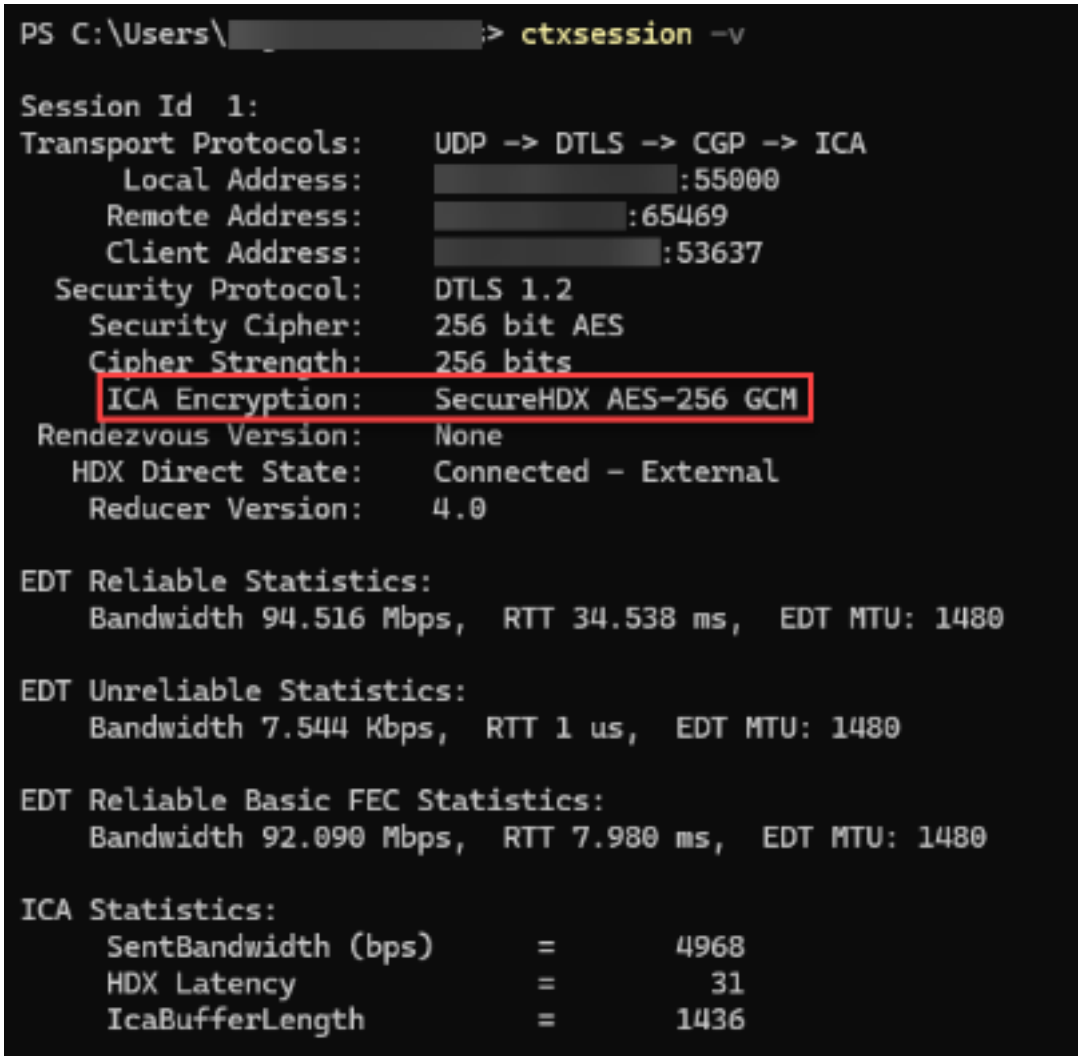
- La continuidad del servicio no es compatible actualmente con Secure HDX. Si tiene habilitada la continuidad del servicio en su entorno de Citrix Cloud, es posible que no pueda conectarse a ningún host de sesión que tenga Secure HDX habilitado si se produce una interrupción del servicio en la nube.
- Si utiliza SmartControl, tenga en cuenta que el uso de Secure HDX impide que funcione SmartControl, ya que el NetScaler no puede inspeccionar el tráfico HDX cifrado. Si debe usar SmartControl, puede configurar Secure HDX para que solo se habilite para conexiones directas.
- No se admite ICA multisecuencia cuando Secure HDX está habilitado.
- Si usa soluciones de terceros que dependen de la inspección del tráfico HDX, dejarán de funcionar si habilita Secure HDX, ya que el tráfico de HDX está cifrado.

### Solución de problemas

Para confirmar que Secure HDX está activo, puede usar la utilidad `ctxsession.exe` en la máquina VDA.

Para usar la utilidad `CtxSession.exe`, abra un símbolo del sistema o PowerShell dentro de la sesión y ejecute `ctxsession.exe -v`. Si Secure HDX está en uso, el cifrado ICA muestra `SecureHDX AES-256 GCM`.




**Cuando Secure HDX no se habilita en la sesión**

- Asegúrese de que la versión del VDA en uso es compatible con la función según los requisitos del sistema.
- Confirme que tiene una directiva aplicada al VDA que habilita Secure HDX y que no hay otras directivas con mayor prioridad para inhabilitar la función.
- Si el dispositivo cliente se conecta a través de NetScaler Gateway o Gateway Service, asegúrese de que Secure HDX no esté configurado como "Solo conexiones directas".
- Si el host de sesión ya estaba en ejecución cuando configuró Secure HDX, reinicie la máquina para asegurarse de que los cambios surtan efecto.

# Lista de canales virtuales permitidos

May 17, 2024

La lista de canales virtuales permitidos es una función que le permite controlar qué canales virtuales que no son de Citrix están permitidos en su entorno. De forma predeterminada, la funcionalidad de lista de canales virtuales permitidos está habilitada. Como resultado, solo se pueden abrir los canales virtuales de Citrix en las sesiones de Citrix Virtual Apps and Desktops. Si hay necesidad de utilizar canales virtuales personalizados, ya sean internos o de un tercero, deben agregarse explícitamente a la lista de permitidos.

## Configuración

La lista de canales virtuales permitidos está habilitada de forma predeterminada. Puede configurar esta función mediante los siguientes parámetros de la directiva de Citrix:

- **Lista de canales virtuales permitidos**: Para habilitar o inhabilitar la función y agregar canales virtuales a la lista.
- **Limitación de los registros de la lista de canales virtuales permitidos**: Establece el período de limitación para el registro de eventos de la lista de canales virtuales permitidos.
- **Registros de la lista de canales virtuales permitidos**: Establece el nivel de registro de la lista de canales virtuales permitidos.

## Agregar canales virtuales a la lista de permitidos

Para agregar un canal virtual a la lista de permitidos, necesita la siguiente información:

1. El nombre del canal virtual tal y como se define en el código, que puede tener hasta 7 caracteres. Por ejemplo, `CTXCVC1`.
2. Las rutas a los procesos que abren el canal virtual en la máquina VDA. Por ejemplo, `C:\Program Files\Application\run.exe`.

Una vez que tenga la información necesaria, deberá agregar el canal virtual a la lista de permitidos mediante la configuración de la directiva Lista de canales virtuales permitidos. Para agregar un canal virtual a la lista, escriba el nombre del canal virtual seguido de una coma y, a continuación, la ruta del proceso que accede al canal virtual. Si hay varios procesos, puede agregarlos separando cada proceso con comas.

#### Para procesos individuales

Con los ejemplos anteriores, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe
```

#### Para varios procesos

Si hay varios procesos, agregue la entrada siguiente a la lista:

```
CTXCVC1,C:\Program Files\Application\run.exe,C:\Program Files\Application
\run2.exe
```

#### Uso de comodines

Se admite el uso de comodines (*). Puede usar caracteres comodín cuando los nombres de los directorios o ejecutables cambian en función de la versión de la aplicación o si el componente de terceros está instalado en los perfiles de los usuarios.

Puede usar caracteres comodín en los siguientes casos:

- Para reemplazar el nombre completo del directorio.
  Por ejemplo: `C:\Program Files\Application\*\run1.exe`
- Para reemplazar parte del nombre del directorio.
  Por ejemplo: `C:\Program Files\Application\v*\run1.exe`
- Para reemplazar el nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\*.exe`
- Para reemplazar parte del nombre del ejecutable.
  Por ejemplo: `C:\Program Files\Application\v1.2\run*.exe`

Se aplican las siguientes restricciones:

- El comodín solo se puede usar para reemplazar un único directorio. Por ejemplo: si el ejecutable se encuentra en `C:\Program Files\Application\v1.2\run1.exe`
  - Permitido: `C:\Program Files\Application\*\run1.exe`
  - No permitido: `C:\Program Files\*\run1.exe`
- Las entradas deben contener la extensión de archivo.
  - Permitido: `C:\Program Files\Application\v1.2\*.exe`
  - No permitido: `C:\Program Files\Application\v1.2\*`
- Todas las rutas deben ser locales.

> **Nota:**
>
> - No se permiten las rutas de red.
> - La compatibilidad con caracteres comodín está disponible a partir de Citrix Virtual Apps and Desktops 2206.
> - La compatibilidad con caracteres comodín está disponible en Citrix Virtual Apps and Desktops 2203 LTSR a partir de la CU2.

#### Uso de variables de entorno del sistema

Puede usar variables de entorno del sistema para simplificar la definición de los procesos de confianza en su lista de permitidos. Puede usar cualquiera de las variables listas para usar, como `%programfiles%`, `%programfiles(x86)%`, `%systemdrive%` y `%systemroot%`.

También puede usar variables de entorno personalizadas siempre que estén definidas a nivel del sistema.

En los siguientes ejemplos se muestran variables de entorno listas para usar:

- `%programfiles%\Application\v1.2\run.exe`
- `%programfiles%\Application\*\run.exe`
- `%programfiles(x86)%\Application\v1.*\run.exe`

En el siguiente ejemplo se muestra una variable de entorno del sistema personalizada:

- Nombre de variable personalizada: `app`
- Valor de variable personalizada: `%programfiles%\Application\`
- Entrada en la lista de permitidos: `CTXCVC1,%app%\run.exe`

> **Nota:**
>
> No se admiten variables de entorno de usuario.
>
> La compatibilidad con variables de entorno está disponible a partir de la versión 2209 de Citrix Virtual Apps and Desktops.

### Obtener nombres y procesos de canales virtuales

La forma más sencilla de obtener el nombre del canal virtual y el proceso que lo abre en la máquina VDA es obtener la información del desarrollador o del proveedor tercero que proporcionó el canal virtual.

También puede obtener esta información aplicando los registros de la funcionalidad y siguiendo estos pasos:

1. Una vez establecidos los componentes del cliente y del servidor del canal virtual personalizado, inicie una aplicación virtual o un escritorio virtual.
2. En el registro de eventos del sistema de la máquina VDA, busque el nombre del canal virtual personalizado y el proceso que lo intentó abrir. Para obtener más información sobre los eventos disponibles, consulte Registros de eventos.
3. Cierre la sesión.
4. Agregue una entrada a la configuración de directiva Lista de canales virtuales permitidos para el canal virtual y el proceso identificados.
5. Reinicie la máquina.
6. Una vez registrado el VDA, ejecute la aplicación virtual o el escritorio virtual para comprobar que los canales virtuales personalizados se abren correctamente.

## Consideraciones sobre canales virtuales Citrix

Todos los canales virtuales Citrix integrados son de confianza y se permite abrirlos sin ninguna configuración adicional. Sin embargo, las dos funcionalidades siguientes requieren entradas explícitas en la lista de permitidos debido a dependencias externas:

- Redirección multimedia
- HDX RealTime Optimization Pack para Skype for Business

### Redirección multimedia

Si usa un reproductor multimedia distinto de Windows Media Player como reproductor multimedia del sistema, debe agregarlo a la lista de permitidos como proceso de confianza. Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: `CTXMM`
- Proceso: Ruta al reproductor multimedia utilizado en la máquina VDA. Por ejemplo, `C:\Program Files (x86)\Windows Media Player\wmplayer.exe`.
- Entrada en la lista de permitidos: `CTXMM,C:\Program Files (x86)\Windows Media Player\wmplayer.exe`

### HDX RealTime Optimization Pack para Skype for Business

Esta información es necesaria para la entrada en la lista de permitidos:

- Nombre del canal virtual: `CTXRMEP`
- Proceso: Ruta al archivo ejecutable de Skype for Business en la máquina VDA, que puede variar según la versión de Skype for Business o si se ha usado una ruta de instalación personalizada.

Por ejemplo, `C:\Program Files\Microsoft Office\root\Office16\lync.exe`.

- Entrada en la lista de permitidos: `CTXRMEP,C:\Program Files\Microsoft Office\root\Office16\lync.exe`

## Solución de problemas

May 17, 2024

Si su canal virtual personalizado no se abre, revise los pasos siguientes:

1. Asegúrese de usar la versión de VDA correcta.
2. Confirme que tiene una directiva aplicada al VDA con el canal virtual personalizado en la lista de canales virtuales permitidos y que no hay otras directivas con mayor prioridad que sobrescriban esta configuración.
3. Compruebe el registro de eventos del VDA y confirme que el nombre del canal virtual notificado coincide con el definido en la lista de permitidos.
    a) Si tiene varios procesos, asegúrese de que estén definidos correctamente como se describe en Agregar canales virtuales a la lista de permitidos.
    b) Si usa caracteres comodín en la ruta de proceso definida, asegúrese de cumplir las directrices sobre uso de comodines.
    c) Si usa variables de entorno en la ruta de proceso definida, asegúrese de cumplir las directrices sobre uso de variables de entorno del sistema.

### Registros de eventos

Los siguientes eventos se registran en el registro de eventos de la máquina VDA.

#### VDA de sesión única

Los siguientes eventos se registran en el registro de eventos de la máquina VDA de sesión única:

| Nombre de registro | ID | Origen | Nivel | Descripción |
|---|---|---|---|---|
| Sistema | 2001 | Picadd | Información | El proceso <processName> ha abierto el canal virtual personalizado <vcName> |
| Sistema | 2002 | Picadd | Advertencia | El proceso <processName> no puede abrir el canal virtual personalizado <vcName> |
| Sistema | 2003 | Picadd | Información | <username> abrió el canal virtual personalizado <vcName> |
| Sistema | 2004 | Picadd | Advertencia | <username> intentó abrir el canal virtual personalizado <vcName> |
| Sistema | 2005 | Picadd | Error | La ruta indicada en la directiva <pathInPolicy> no puede resolverse en la ruta del proceso |
| Sistema | 2007 | Picadd | Información | La ruta del proceso cargado es <processPath> |

| Nombre de registro | ID | Origen | Nivel | Descripción |
|---|---|---|---|---|
| Sistema | 2008 | Picadd | Error | No se encuentra la variable de entorno <varName> en la ruta de la directiva de canal virtual |

**VDA multisesión**

Los siguientes eventos se registran en el registro de eventos de la máquina VDA multisesión:

| Nombre de registro | ID | Origen | Nivel | Descripción |
|---|---|---|---|---|
| Sistema | 13 | Rpm | Información | El proceso <processName> ha abierto el canal virtual personalizado <vcName> |
| Sistema | 14 | Rpm | Advertencia | El proceso <processName> no puede abrir el canal virtual personalizado <vcName> |
| Sistema | 15 | Rpm | Información | <username> abrió el canal virtual personalizado <vcName> |
| Sistema | 16 | Rpm | Advertencia | <username> intentó abrir el canal virtual personalizado <vcName> |

| Nombre de registro | ID | Origen | Nivel | Descripción |
|---|---|---|---|---|
| Sistema | 17 | Rpm | Error | La ruta indicada en la directiva <pathInPolicy> no puede resolverse en la ruta del proceso |
| Sistema | 18 | Rpm | Información | La ruta del proceso cargado es <processPath> |
| Sistema | 19 | Rpm | Error | No se encuentra la variable de entorno <varName> en la ruta de la directiva de canal virtual |

## Canales virtuales de terceros conocidos

May 17, 2024

A continuación se indican soluciones de terceros conocidas que utilizan canales virtuales Citrix. Esta lista no incluye todas las soluciones que usan un canal virtual personalizado Citrix.

- Cerner
- ControlUp
- Cisco WebEx Teams
- Cisco WebEx Meetings Virtual Desktop Software
- deviceTrust
- Epic Warp Drive
- Epic Slingshot
- Imprivata OneSign
- Extensiones de cliente Midmark IQPath
- Extensiones de cliente Nuance PowerMic

- Nuance Dragon Medical Network Edition 360 vSync
- Zoom Meetings para VDI
- Ultima IA-Connect

Para obtener detalles sobre cómo agregar los canales virtuales asociados a la lista de permitidos, consulte a los proveedores de las soluciones. Como alternativa, siga los pasos descritos en la sección Obtener nombres y procesos de canales virtuales.

## Dispositivos

August 28, 2023

HDX proporciona una experiencia de usuario de alta definición en cualquier dispositivo y en cualquier ubicación. Los artículos en la sección Dispositivos describen estos dispositivos:

- Asignación de unidades del cliente
- Dispositivo USB genérico
- Dispositivos móviles y de pantalla táctil
- Dispositivos en serie
- Teclados especiales
- Dispositivos TWAIN
- Cámaras web
- Dispositivos WIA

### Dispositivo USB optimizado y genérico

Un dispositivo USB optimizado es aquel para el cual la aplicación Citrix Workspace ofrece funcionalidades específicas. Por ejemplo: la capacidad de redirigir cámaras web mediante el canal virtual multimedia HDX. Un dispositivo genérico es un dispositivo USB para el que no hay ninguna funcionalidad específica en la aplicación Citrix Workspace.

De forma predeterminada, la redirección de USB genérico no puede redirigir dispositivos USB con funcionalidad optimizada para el canal virtual a menos que se coloquen en el modo Genérico.

En general, se obtiene un mejor rendimiento para dispositivos USB en el modo Optimizado que en el modo Genérico. Sin embargo, hay casos en que un dispositivo USB no tiene funcionalidad completa en el modo Optimizado. Puede que sea necesario cambiar al modo Genérico para obtener acceso completo a sus funciones.

Con dispositivos de almacenamiento masivo USB, puede utilizar la asignación de unidades del cliente, la redirección de USB genérico o ambos, controlados mediante directivas de Citrix. Las principales

diferencias son:

Si la directiva de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se inserta un dispositivo de almacenamiento masivo antes o después de iniciar una sesión, el dispositivo se redirigirá mediante la asignación de unidades del cliente.

Cuando se dan estas condiciones, el dispositivo de almacenamiento masivo se redirige mediante la redirección de USB genérico:

- Tanto la redirección de USB genérico como las directivas de asignación de unidades del cliente están habilitadas.
- Un dispositivo está configurado para la redirección automática.
- Se inserta un dispositivo de almacenamiento masivo antes o después de que se inicie sesión.

Para obtener más información, consulte http://support.citrix.com/article/CTX123015.

| Función | Asignación de unidades del cliente | Redirección de USB genérico |
|---|---|---|
| Habilitada de forma predeterminada | Sí | No |
| Configuración para acceso de solo lectura | Sí | No |
| Acceso a dispositivo cifrado | Sí, si el cifrado se desbloquea antes de acceder al dispositivo en la sesión virtual. | Solo Citrix Virtual Desktops |

## Asignación de unidades del cliente (CDM)

October 30, 2023

La asignación de unidades del cliente hace que las unidades de almacenamiento del dispositivo de punto final del cliente estén disponibles dentro de una sesión de Citrix HDX para permitir la transferencia de archivos y carpetas del cliente al host de la sesión, y viceversa. Esta función está habilitada de forma predeterminada con privilegios de lectura y escritura. Si quiere impedir que los usuarios agreguen o modifiquen archivos y carpetas de los dispositivos de cliente asignados, habilite la configuración de directiva **Acceso de lectura solamente a unidades del cliente**. Al agregar esta configuración a una directiva, compruebe que la configuración **Redirección de unidades del cliente** está establecida en **Permitida** y también se ha agregado a la directiva.

Como medida de seguridad, las unidades de los dispositivos de punto final se asignan sin el permiso de ejecución de forma predeterminada. Para permitir a los usuarios ejecutar ejecutables directamente desde las unidades de cliente asignadas, modifique el valor de Registro **ExecuteFromMappedDrive** en el host de la sesión. Para obtener información, consulte Unidades de cliente asignadas en la sección de **funciones HDX administradas a través del Registro**.

## Requisitos

Estos son los requisitos para usar CDM:

### Plano de control de Citrix

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
- Citrix DaaS

### Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows Server 2016 o una versión posterior
  - Linux: Consulte los requisitos del sistema de Linux VDA
- VDA
  - Windows: Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
  - Linux: Consulte la documentación de Linux VDA

### Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Linux: Consulte los requisitos del sistema de la aplicación Workspace para Linux.

## Directivas relacionadas

Con relación a los parámetros de CDM, consulte la sección Referencia para configuración de directivas.

### Supuestos de doble salto

CDM es compatible con supuestos de doble salto. De forma predeterminada, la unidad del dispositivo de punto final del cliente se asigna a la sesión del segundo salto y las unidades del primer salto no están disponibles. Sin embargo, se puede configurar de manera que las unidades del primer salto se asignen en la sesión del segundo salto, en lugar de las unidades del dispositivo de punto final del cliente.

Para configurar la funcionalidad, modifique este valor de Registro:

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advance
- Nombre del valor: NativeDriveMapping
- Tipo de valor: REG_SZ
- Información del valor:
  - True: Asigna las unidades de la sesión del primer salto en la sesión del segundo salto
  - False: Asigna las unidades del dispositivo de punto final del cliente en la sesión del segundo salto

> **Nota:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

## Dispositivos USB genéricos

April 18, 2024

La tecnología HDX ofrece **optimización** con los dispositivos USB más comunes. Estos dispositivos son:

- Monitores
- Mouse
- Teclados
- Teléfonos VoIP
- Auriculares con micro
- Cámaras web
- Escáneres
- Cámaras

- Impresoras
- Unidades
- Lectores de tarjetas inteligentes
- Tabletas de dibujo
- Paneles táctiles de firma electrónica

La optimización ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión por red WAN. La optimización suele ser la mejor opción, sobre todo en entornos de alta latencia o cuando se requiera confidencialidad.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin optimización o cuando esta no es adecuada. Para obtener más información sobre la redirección de USB genérico, consulte Redirigir USB genérico.

Para obtener más información sobre dispositivos USB y la aplicación Citrix Workspace para Windows, consulte Configurar la redirección de dispositivos USB compuestos y Configurar la compatibilidad con USB.

## Compatibilidad con dispositivos cliente móviles y con pantalla táctil

February 21, 2024

Citrix Virtual Apps and Desktops permite a los usuarios acceder a sus aplicaciones y escritorios publicados desde dispositivos cliente móviles y con pantalla táctil.

### Requisitos

#### Plano de control de Citrix

- Citrix Virtual Apps and Desktops 7.15 o una versión posterior
- Citrix DaaS

#### Host de la sesión

- Sistema operativo
  - Windows 10 1903 o una versión posterior
  - Windows Server 2016 o una versión posterior
- VDA
  - Windows: Versión 7.15 o una posterior

#### Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
- Aplicación Citrix Workspace para Windows, versión 1808 o una posterior

### Modo tableta para dispositivos de pantalla táctil mediante Windows Continuum

Continuum es una función de Windows 10 que se adapta al uso que se le da al dispositivo cliente. Cuando el VDA detecta la presencia de un teclado o mouse en un cliente táctil, hace que el cliente pase al modo de escritorio. Si el teclado o el mouse no están presentes, el VDA coloca al cliente en el modo móvil o tableta. Esta detección se produce al conectarse y al reconectarse sesiones, y también durante las sesiones, cuando el teclado o el mouse se conectan o se desconectan.

Esta función está activada de forma predeterminada. Para inhabilitar esta función, defina la configuración de directiva Cambiar modo tableta (configuración de directiva).

Además de los requisitos para los dispositivos de pantalla táctil mencionados anteriormente, se requieren estos requisitos para Windows Continuum:

#### XenServer

- Citrix Hypervisor 8.2 o una versión posterior
- Ejecute el comando CLI de XenServer para permitir que se pueda cambiar entre el equipo portátil y la tableta:
  **xe vm-param-set uuid=<VM_UUID> platform:acpi_laptop_slate=1**

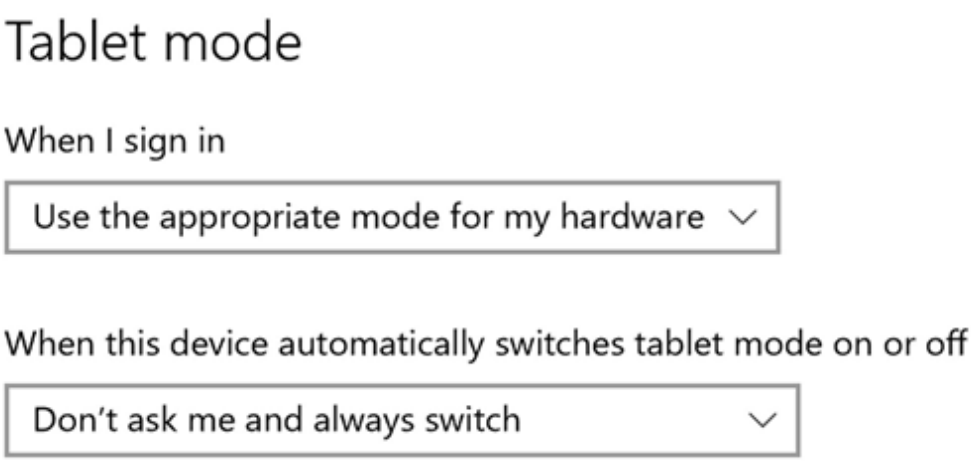
> **Importante:**
>
> Actualizar la imagen base de un catálogo existente de máquinas después de cambiar el parámetro de metadatos no afecta a las máquinas virtuales previamente aprovisionadas. Después de cambiar la imagen base de la VM de XenServer, cree un catálogo, seleccione la imagen base y aprovisione una nueva máquina con Machine Creation Services (MCS).

#### Host de la sesión

- Sistema operativo
  - Windows 10 1903 o una versión posterior
  - Windows 11
- VDA

- Windows: Versión 7.16 o una posterior
- **Debido a las limitaciones actuales en las configuraciones del sistema operativo, los usuarios tendrán que configurar estas opciones en los menús desplegables después de iniciar la primera sesión ICA y reiniciar el VDA:**
  - **Parámetros > Sistema > Modo tableta**
    - Usar el modo adecuado para mi hardware
    - No preguntarme y cambiar siempre




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

- Botones ligeramente más grandes
- La pantalla de inicio y cualquier aplicación que abra se inician en modo de pantalla completa
- La barra de tareas contiene un botón Atrás
- Se han eliminado iconos de la barra de tareas

Puede utilizar el Explorador de archivos.

Windows 10 carga el controlador GPIO en la máquina virtual de destino basándose en esta BIOS actualizada. Se utiliza para alternar entre los modos escritorio y tableta dentro de la máquina virtual.

La aplicación Citrix Workspace para HTML5 no admite las funciones de Windows Continuum.

El **modo escritorio** ofrece la interfaz de usuario tradicional, donde se interactúa de la misma manera que con un PC, un teclado y un mouse.

## Lápices para Microsoft Surface Pro y Surface Book

Se admite la funcionalidad de lápiz estándar en aplicaciones basadas en Windows Ink. Se puede señalar, borrar y presionar con el lápiz, y se admiten las señales de Bluetooth y otras funciones que varían según el firmware del sistema operativo y el modelo del lápiz. Por ejemplo: la presión del lápiz puede ser de 4096 niveles como máximo. Esta función está habilitada de manera predeterminada.

Estos son los requisitos para la funcionalidad del lápiz:

#### Plano de control de Citrix

- Citrix Virtual Apps and Desktops 1903 o una versión posterior
- Citrix DaaS

#### Host de la sesión

- Sistema operativo
  - Windows 10 1809 o una versión posterior
  - Windows Server 2016 o una versión posterior
  - Windows 11
- VDA
  - Windows: Versión 1903 o una posterior

#### Dispositivo cliente

- Sistema operativo
  - Windows 10 1809 o una versión posterior
- Aplicación Citrix Workspace para Windows 1902 (versión mínima)

Para obtener una demostración de Windows Ink y la funcionalidad del lápiz, haga clic en este gráfico:


Para habilitar o inhabilitar esta función, consulte Lápices para Microsoft Surface Pro y Surface Book en la lista de funciones administradas a través del Registro.

### Problemas conocidos

Estos son problemas conocidos relacionados con la compatibilidad con lápices:

- Debido a las limitaciones del sistema operativo de Windows Server 2k22, los usuarios no podrán establecer accesos directos para el lápiz ni realizar ajustes en los parámetros del lápiz o la tinta en el Panel de control cuando se conecten a aplicaciones o escritorios del servidor de 2k22.
- Los accesos directos del lápiz no se aceptan en clientes con Windows 11 y lápiz habilitado debido a las limitaciones del sistema operativo.

## Puertos serie

April 14, 2022

La mayoría de los PC nuevos no tienen puertos serie integrados (COM). Es fácil agregar puertos mediante convertidores USB. Las aplicaciones adecuadas para los puertos serie suelen ser sensores, controladores, lectores antiguos de cheques, paneles táctiles, etc. Algunos dispositivos USB de puerto COM virtual utilizan controladores específicos del fabricante en lugar de los controladores que ofrece Windows (usbser.sys). Estos controladores permiten forzar el puerto COM virtual del dispositivo USB

para que no cambie incluso aunque se conecte a otras ranuras USB. Se puede hacer desde **Administrador de dispositivos > Puertos (COM y LPT) > Propiedades** o desde la aplicación que controla el dispositivo.

La asignación de puertos COM del cliente permite utilizar los dispositivos conectados a los puertos COM del dispositivo de usuario durante las sesiones virtuales. Estas asignaciones se pueden utilizar de la misma forma que cualquier otra asignación de red.

Un controlador del sistema operativo asigna un nombre de enlace simbólico a cada puerto COM, como COM1 y COM2. Las aplicaciones usan ese enlace para acceder al puerto.

> **Importante:**
>
> El hecho de que un dispositivo se pueda conectar al dispositivo de punto final directamente por USB no significa que ese dispositivo se pueda redirigir mediante la redirección de USB genérico. Algunos dispositivos USB funcionan como puertos COM virtuales, a los que las aplicaciones pueden acceder de la misma manera que al puerto serie físico. El sistema operativo puede abstraer puertos COM y tratarlos como archivos compartidos. Dos protocolos frecuentes para COM virtual son: CDC ACM o MCT. Cuando se conecta a través de un puerto RS-485, es posible que las aplicaciones no funcionen en absoluto. Debe obtener un convertidor de RS-485 a RS232 para usar RS-485 como puerto COM.
>
> **Importante:**
>
> Algunas aplicaciones reconocen el dispositivo (por ejemplo, un panel táctil de firmas) correctamente solo si está conectado a COM1 o COM2 en la estación de trabajo del cliente.

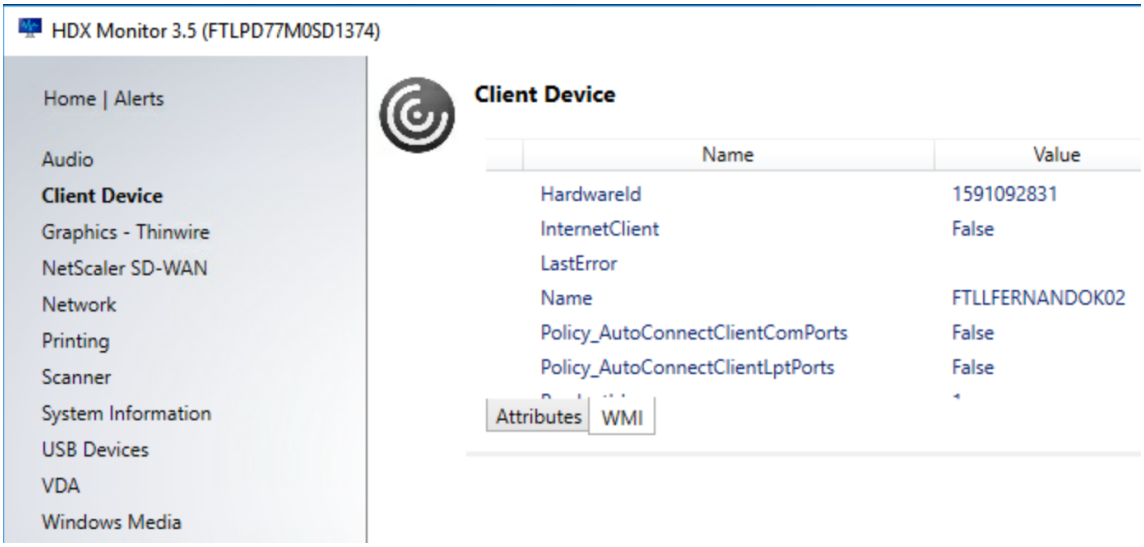
### Asignar un puerto COM de cliente a un puerto COM de servidor

Puede asignar los puertos COM del cliente a una sesión de Citrix de tres maneras:

- Con la administración de directivas de consola. Para obtener más información acerca de las directivas, consulte Configuraciones de directiva de Redirección de puertos.
- El símbolo del sistema del VDA.
- Herramienta de configuración del escritorio remoto (Terminal Services).

1. Habilite las directivas **Redirección de puertos COM del cliente** y **Conectar automáticamente puertos COM del cliente de Studio**. Después de aplicarlas, se ofrece información en HDX Monitor.




2. Si **Conectar automáticamente puertos COM del cliente** no puede asignar el puerto, puede asignarlo manualmente o usar scripts de inicio de sesión. Inicie sesión en el VDA y, en una ventana de símbolo del sistema, escriba:

   NET USE COMX: \\CLIENT\COMZ:

   O bien:

   NET USE COMX: \\CLIENT\CLIENTPORT:COMZ:

   **X** es el número del puerto COM en el VDA (los puertos del 1 al 9 están disponibles para la asignación). **Z** es el número del puerto COM del cliente que quiere asignar.

   Para confirmar que la operación se ha realizado correctamente, escriba **NET USE** en un símbolo del sistema de VDA. Aparecerá la lista de las unidades, puertos LPT y puertos COM asignados.

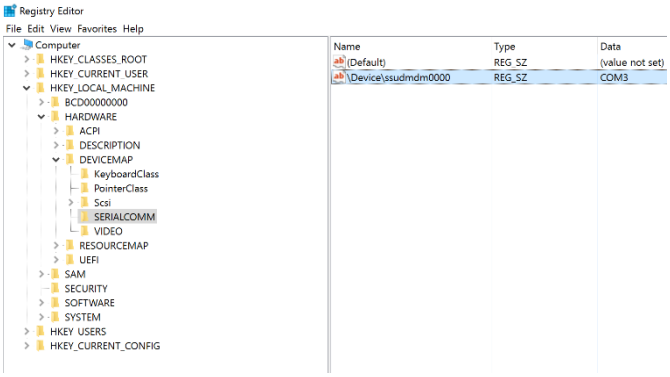

3. Para utilizar este puerto COM en una sesión de aplicación o escritorio virtual, instale la aplicación del dispositivo de usuario y apúntela al nombre del puerto COM asignado. Por ejemplo, si asigna COM1 en el cliente a COM3 en el servidor, instale la aplicación del dispositivo de puerto COM en el VDA y apúntela a COM3 durante la sesión. Utilice este puerto COM asignado del mismo modo que lo haría con un puerto COM del dispositivo del usuario.

> **Importante:**
>
> La asignación de puertos COM no es compatible con TAPI. No puede asignar dispositivos Windows Telephony Application Programming Interface (TAPI) de Windows a los puertos COM del cliente. TAPI define una forma estándar que tienen las aplicaciones para controlar las funciones del teléfono para datos, fax y llamadas de voz. TAPI administra la señalización, incluido el marcado, la respuesta y la finalización de llamadas. Asimismo, gestiona servicios complementarios (como poner en espera, transferir y hacer llamadas de conferencia).

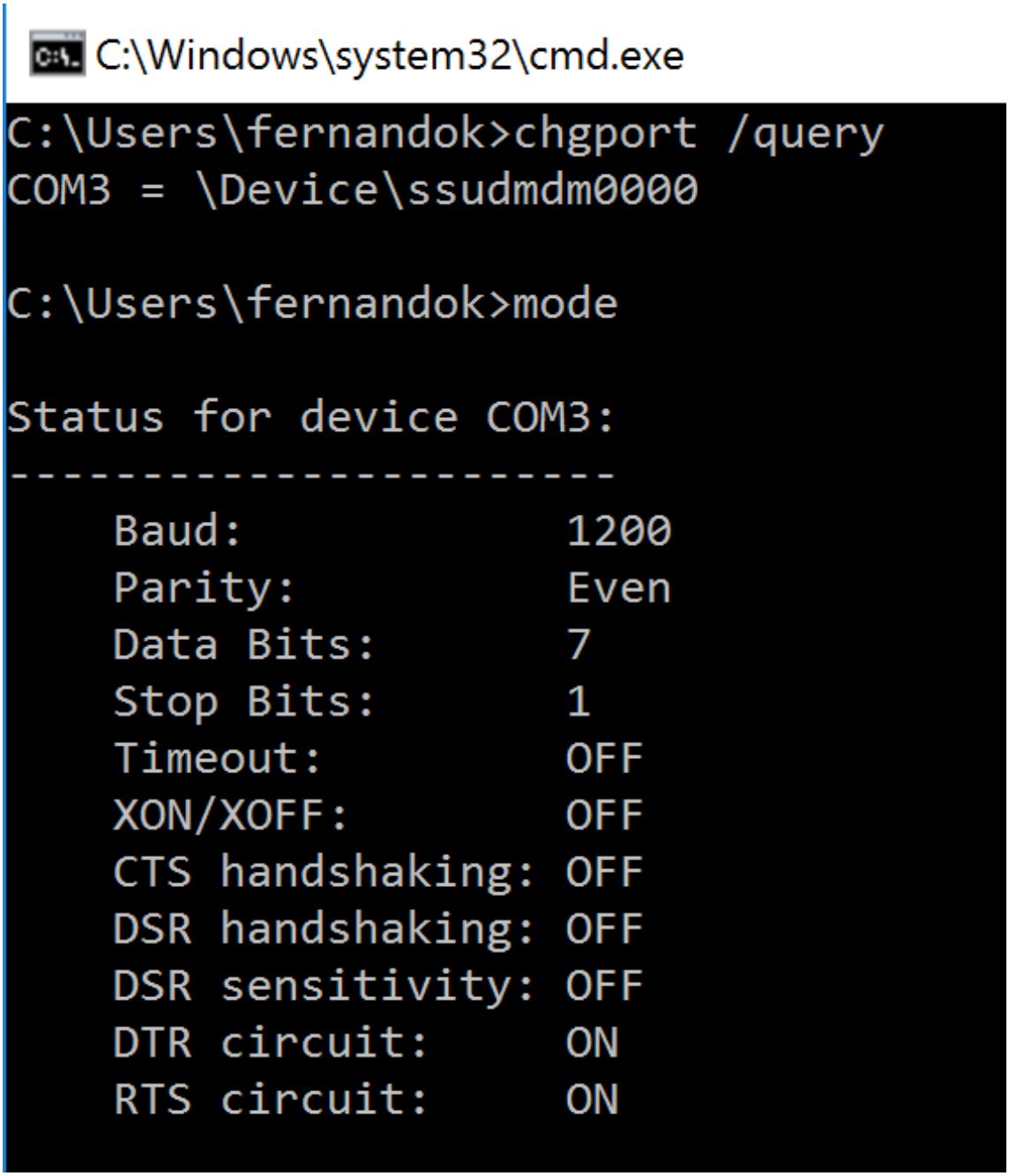
## Solucionar problemas

1. Compruebe que puede acceder al dispositivo directamente desde el dispositivo de punto final, sin pasar por Citrix. Mientras el puerto no se asigne al VDA, no podrá conectarse a una sesión de Citrix. Siga las instrucciones de solución de problemas incluidas con el dispositivo y primero compruebe que funciona localmente.
   Cuando un dispositivo se conecta a un puerto serie COM, se crea una clave de Registro en el subárbol que se muestra aquí:



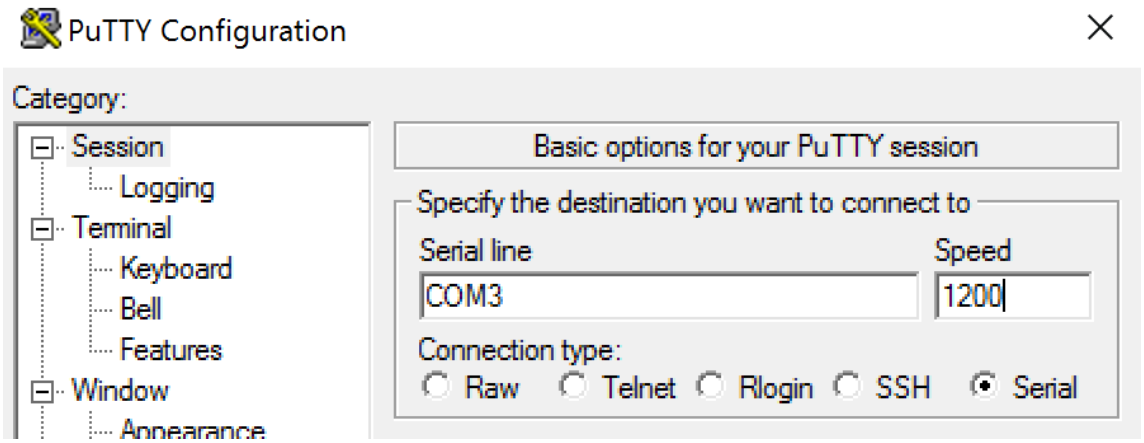

   También puede encontrar esta información desde el símbolo del sistema ejecutando **chgport /query**.




Si no dispone de instrucciones de solución de problemas para el dispositivo, intente solucionar problemas con una sesión PuTTY. Elija **Session** y, en **Serial line**, especifique su puerto COM.




Puede ejecutar **MODE** en una ventana de comando local. El resultado muestra el puerto COM en uso y los bits de parada, los bits de datos, la paridad y los baudios que necesita en su sesión PuTTY. Si se puede establecer la conexión con PuTTY, presione **Entrar** para ver la información que envíe el dispositivo. Los caracteres que escriba pueden repetirse en pantalla, o bien, puede recibir directamente respuesta a ellos. Sin este paso, no puede acceder al dispositivo desde una sesión virtual.

2. Asigne el puerto COM local al VDA (mediante directivas o **NET USE COMX: \\CLIENT\COMZ:**) y repita los mismos procedimientos de PuTTY que en el paso anterior, pero esta vez desde el PuTTY del VDA. Si PuTTY falla con el error **Unable to open connection to COM1. Unable to open serial port**, puede que otro dispositivo esté utilizando COM1.

3. Ejecute **chgport /query**. Si el controlador serie de Windows integrado en el VDA asigna automáticamente \Device\Serial0 a un puerto COM1 del VDA, haga lo siguiente:
   A. Abra CMD en el VDA y escriba **NET USE**.

   B. Elimine cualquier asignación existente (por ejemplo, COM1) en el VDA.

   **NET USE COM1 /DELETE**

   C. Asigne el dispositivo al VDA.

   **NET USE COM1: \\CLIENT\COM3:**

   D. Apunte la aplicación en el VDA a COM3.

   Por último, intente asignar su puerto COM local (por ejemplo, COM3) a otro puerto COM en el VDA (que no sea COM1 si no, por ejemplo, COM3). Compruebe que su aplicación apunta a él:
   **NET USE COM3: \\CLIENT\COM3**

4. Si ahora ve el puerto asignado, PuTTY está funcionando, pero no pasa ningún dato, podría tratarse de una condición de carrera. La aplicación puede conectarse y abrir el puerto antes de que se asigne, con lo que se bloquea su asignación. Pruebe una de las siguientes soluciones:

- Abra una segunda aplicación publicada en el mismo servidor. Espere unos segundos para que se asigne el puerto y abra la aplicación que intenta usar el puerto.
- Habilite las directivas de redirección de puertos COM desde el Editor de directivas de grupo en Active Directory en lugar de la interfaz de Administrar > Configuración completa del servicio. Esas directivas son: **Redirección de puertos COM del cliente** y **Conectar automáticamente puertos COM del cliente**. Las directivas aplicadas de esta manera se pueden procesar antes de las directivas de la consola Administrar, lo que garantiza que el puerto COM se asigne. Las directivas de Citrix se envían al VDA y se almacenan en: `HKLN\SOFTWARE\Policies\Citrix \<user session ID\>`
- Utilice este script de inicio de sesión para el usuario o, en lugar de publicar la aplicación, publique un script .bat que borre primero cualquier asignación en el VDA, vuelva a asignar el puerto COM virtual y luego inicie la aplicación:

```
@echo off
NET USE COM1 /delete
NET USE COM2 /delete
NET USE COM1: \\CLIENT\COM1:
NET USE COM2: \\CLIENT\COM2:
MODE COM1: BAUD=1200 (o el valor que necesite)
MODE COM2: BAUD=9600 PARITY=N Data=8 Stop=1 (o el valor que necesite)
START C:\Archivos de programa\<Ruta a su software>\
```

5. Process Monitor de Sysinternals es la herramienta de último recurso. Cuando ejecute la herramienta en el VDA, busque y filtre objetos como COM3, picaser.sys, CdmRedirector y, sobre todo, \<su_aplicación\>.exe. Los errores aparecen como "Acceso denegado"o similar.

## Teclados especiales

April 18, 2024

### Teclados Bloomberg

> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de

> modificarlo.

Citrix Virtual Apps and Desktops admite el teclado Starboard modelo 4 de Bloomberg (y el modelo anterior 3). Este teclado permite a los clientes del sector financiero utilizar funciones especiales en el teclado para poder acceder a datos del mercado financiero y realizar transacciones rápidamente.

Este teclado es compatible con los cuadros de conmutadores KVM y puede funcionar en dos modos:

- PC (un cable USB sin KVM)
- Modo KVM (dos cables USB con uno enrutado a través de KVM)

> **Importante:**
>
> Se recomienda usar el teclado Bloomberg con una sola sesión. Es decir, no se recomienda utilizar este teclado con varias sesiones simultáneas (de un cliente a varias sesiones).

El teclado Bloomberg 4 es un dispositivo USB compuesto que consta de cuatro dispositivos USB en una carcasa física:

- Teclado.
- Lector de huellas dactilares.
- Dispositivo de audio con teclas para aumentar y disminuir el volumen o silenciar el altavoz y el micrófono. Este dispositivo incluye altavoz, micrófono y conector integrado para el micrófono y los auriculares.
- Concentrador USB para conectar todos estos dispositivos al sistema.

**Requisitos:**

- La sesión a la que se conecta la aplicación Citrix Workspace para Windows debe admitir dispositivos USB.
- La aplicación Citrix Workspace 1808 para Windows o Citrix Receiver para Windows 4.8, como mínimo, para admitir los modelos 3 y 4 del teclado Bloomberg.
- Aplicación Citrix Workspace 1808 para Windows o Citrix Receiver para Windows 4.12, como mínimo, para usar el modo KVM (dos cables USB con uno enrutado a través de KVM) para el modelo 4.

Para obtener información sobre cómo configurar los teclados Bloomberg en la aplicación Citrix Workspace para Windows, consulte Configurar teclados Bloomberg.

Para habilitar la compatibilidad con teclados Bloomberg, consulte Teclado Bloomberg en la lista de funciones administradas a través del Registro.

**Comprobar que está disponible:**

Para determinar si el teclado Bloomberg está habilitado en la aplicación Citrix Workspace, compruebe si Desktop Viewer informa correctamente de los dispositivos del teclado Bloomberg.

En el escritorio:

Abra Desktop Viewer. Si el teclado Bloomberg está habilitado, Desktop Viewer muestra tres dispositivos debajo del icono USB:

- Escáner de huellas dactilares de Bloomberg
- Funciones del teclado de Bloomberg
- Bloomberg LP Keyboard 2013

Solo aplicación integrada:

Abra el menú **Central de conexiones** desde el icono del área de notificaciones de la aplicación Citrix Workspace. Si el teclado Bloomberg está habilitado, los tres dispositivos aparecen en el menú **Dispositivos**.

La marca de verificación situada junto a cada uno de estos dispositivos indica que están conectados remotamente a la sesión.

## Dispositivos TWAIN

April 14, 2022

### Requisitos

- El escáner debe ser compatible con TWAIN.
- Instale los controladores TWAIN en el dispositivo local. No son necesarios en el servidor.
- Conecte el escáner localmente (por ejemplo, por USB).
- Compruebe que el escáner esté utilizando el controlador TWAIN local, no el servicio Adquisición de imágenes de Windows.
- Compruebe que no se aplica ninguna directiva (por ejemplo, que limite el ancho de banda en la sesión ICA) a la cuenta de usuario que se utiliza para la prueba. Por ejemplo, la directiva Límite de ancho de banda de redirección de dispositivos USB del cliente.

Para obtener información acerca de las configuraciones de directiva, consulte Configuraciones de directiva de Dispositivos TWAIN.

## Cámaras web

August 16, 2022

### Streaming por cámara web de alta definición

Las aplicaciones de videoconferencia que se ejecutan en la sesión virtual pueden utilizar cámaras web. La aplicación presente en el servidor selecciona el formato de cámara web y la resolución en función de los tipos de formato compatibles. Cuando se inicia una sesión, el cliente envía la información de la cámara web al servidor. Puede elegir una cámara web en la aplicación de videoconferencia. Si la cámara web y la aplicación admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Admitimos resoluciones de cámara web hasta 1920 x 1080.

Esta función requiere Citrix Receiver para Windows, versión mínima 4.10. Para obtener una lista de las plataformas de aplicaciones Citrix Workspace que admiten la redirección de la cámara web HDX, consulte la tabla de funciones de la aplicación Citrix Workspace.

Para obtener más información sobre el streaming de cámaras web de alta definición, consulte HDX y los requisitos de las conferencias de vídeo para la compresión de vídeo de cámaras web.

Puede usar una clave del Registro para inhabilitar y habilitar la función y, a continuación, configurar una resolución específica. Para obtener más información, consulte Streaming por cámara web de alta definición y Resolución de cámara web de alta definición en la lista de funciones administradas a través del Registro.

## Dispositivos WIA

April 14, 2022

### Requisitos

- El escáner debe ser compatible con WIA.
- Instale los controladores WIA en el dispositivo local. No son necesarios en el servidor.
- Conecte el escáner localmente (por ejemplo, por USB).
- Compruebe que el escáner esté utilizando el servicio Adquisición de imágenes de Windows, no el controlador TWAIN local.
- Compruebe que no se aplica ninguna directiva (por ejemplo, que limite el ancho de banda en la sesión ICA) a la cuenta de usuario que se utiliza para la prueba. Por ejemplo, la directiva Límite de ancho de banda de redirección de dispositivos USB del cliente.

#### Lista de aplicaciones permitidas de Adquisición de imágenes de Windows

Una lista de permitidos le permite controlar qué aplicaciones del VDA pueden acceder a la redirección del escáner de Adquisición de imágenes de Windows (WIA). El Editor del Registro utiliza la informa-

ción de configuración de la lista de permitidos en cada VDA que contiene Adquisición de imágenes de Windows. De forma predeterminada, ninguna aplicación tiene acceso a Adquisición de imágenes de Windows.

Para ajustar Adquisición de imágenes de Windows para las aplicaciones del VDA, consulte la configuración de Lista de aplicaciones permitidas de Adquisición de imágenes de Windows en la lista de funciones administradas a través del Registro.

Para obtener información acerca de las configuraciones de directiva, consulte Configuraciones de directiva de dispositivos WIA.

## Gráficos

April 14, 2022

Citrix HDX Graphics contiene un conjunto amplio de tecnologías de codificación y aceleración de gráficos que optimiza la entrega de aplicaciones con gráficos sofisticados desde Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Estas tecnologías ofrecen la misma experiencia que con un escritorio físico cuando se trabaja de forma remota en aplicaciones virtuales de uso intensivo de gráficos.

Puede usar el software o el hardware para la generación de gráficos. La generación por software requiere una biblioteca de terceros que se denomina "rasterizador de software". Por ejemplo, Windows incluye el rasterizador WARP para gráficos DirectX. En ocasiones, puede interesarle usar un elemento de representación alternativa por software. La representación por hardware (aceleración de hardware) requiere un procesador de gráficos (GPU).

Citrix HDX Graphics ofrece una configuración de cifrado predeterminado que está optimizada para los casos de uso más comunes. Con las directivas Citrix, los administradores de TI también pueden configurar varios parámetros relacionados con gráficos para cumplir los diferentes requisitos y ofrecer la experiencia de usuario pertinente.

### Thinwire

Thinwire es la tecnología predeterminada de Citrix para pantallas remotas que se utiliza en Citrix DaaS.

Las tecnologías de pantallas remotas permiten que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí. Los gráficos se generan como resultado de una entrada de usuario (por ejemplo, pulsaciones de teclado o acciones del mouse).

### HDX 3D Pro

Las capacidades HDX 3D Pro de Citrix DaaS permiten entregar escritorios y aplicaciones que rinden más gracias a una unidad de procesamiento de gráficos (GPU) para la aceleración de hardware. Estas aplicaciones incluyen gráficos 3D profesionales basados en OpenGL y DirectX. El VDA estándar solo admite la aceleración GPU de DirectX.

### Aceleración de GPU para SO Windows de sesión única

Cuando utiliza HDX 3D Pro, puede entregar aplicaciones de uso intensivo de gráficos como parte de escritorios o aplicaciones que se alojan en máquinas con SO de sesión única. HDX 3D Pro admite equipos host físicos (incluido el escritorio, blade y estaciones de trabajo en rack), así como GPU PassThrough y tecnologías de virtualización de GPU que ofrecen los hipervisores de XenServer, vSphere y Hyper-V (solo PassThrough).

Mediante GPU PassThrough, puede crear máquinas virtuales con acceso exclusivo a hardware de procesamiento de gráficos dedicado. Es posible instalar varias GPU en el hipervisor y asignar, una a una, diversas VM a cada GPU.

Con la virtualización de GPU, varias máquinas virtuales pueden acceder directamente a la capacidad de procesamiento de gráficos de una única GPU física.

### Aceleración de GPU para SO Windows multisesión

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones de sistema operativo multisesión Windows se representen en la unidad de procesamiento de gráficos (GPU) del servidor. Al trasladar la representación de los gráficos de OpenGL, DirectX, Direct3D y Windows Presentation Foundation (WPF) a la GPU del servidor, la CPU del servidor no se ve ralentizada. Además, el servidor es capaz de procesar más gráficos, dado que la carga de trabajo se divide entre la CPU y la GPU.

### Framehawk

> **Importante:**
>
> A partir de Citrix Virtual Apps and Desktops 7 1903, Framehawk ya no se admite. En su lugar, utilice Thinwire con el transporte adaptable habilitado.

Framehawk es una tecnología de pantallas remotas para usuarios móviles con conexiones inalámbricas de banda ancha (redes de telefonía móvil Wi-Fi, 4G o LTE). Framehawk resuelve obstáculos como interferencias espectrales y propagaciones multirruta para ofrecer una experiencia de usuario fluida e interactiva a los usuarios de aplicaciones y escritorios virtuales.

### Marca de agua de sesión basada en texto

Las marcas de agua de la sesión basadas en texto ayudan a disuadir del robo de datos y rastrear los datos robados. Esta información rastreable aparece en el escritorio de la sesión como un elemento de disuasión para quienes usan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto. La marca de agua se puede mostrar en la pantalla de

toda la sesión sin cambiar el contenido del documento original. Las marcas de agua de la sesión basadas en texto requieren que se admita el VDA.

### Información relacionada

- HDX 3D Pro
- Aceleración de GPU para SO Windows de sesión única
- Aceleración de GPU para SO Windows multisesión
- Thinwire
- Marca de agua de sesión basada en texto

## HDX 3D Pro

January 24, 2024

Las capacidades HDX 3D Pro de Citrix Virtual Apps and Desktops permiten entregar escritorios y aplicaciones que rinden más gracias a una unidad de procesamiento de gráficos (GPU) para la aceleración de hardware. Estas aplicaciones incluyen gráficos 3D profesionales basados en OpenGL y DirectX. El VDA estándar solo admite la aceleración GPU de DirectX.

Para conocer las configuraciones de la directiva de HDX 3D Pro, consulte Optimizar para cargas de trabajo de gráficos 3D,

Todas las aplicaciones Citrix Workspace compatibles se pueden usar con gráficos 3D. Para obtener el mejor rendimiento con cargas de trabajo complejas de 3D, monitores de alta resolución, configuraciones de varios monitores y aplicaciones con alta velocidad de fotogramas, se recomienda usar las versiones más recientes de la aplicación Citrix Workspace para Windows y la aplicación Citrix Workspace para Linux. Para obtener más información sobre las versiones compatibles de la aplicación Citrix Workspace, consulte Lifecycle Milestones for Citrix Workspace app.

Los ejemplos de aplicaciones profesionales de 3D incluyen:

- Aplicaciones de ingeniería, fabricación y diseño asistidos por computadora (CAE/CAM/CAD)
- Software de sistema de información geográfica (GIS)
- Sistema de archivado y transmisión de imágenes (PACS) para la imagen médica
- Aplicaciones con las versiones más recientes de OpenGL, DirectX, NVIDIA CUDA y OpenCL y WebGL
- Aplicaciones no gráficas que consumen muchos recursos informáticos y que usan GPU CUDA (Compute Unified Device Architecture), la arquitectura de cálculo paralelo de NVIDIA, para el procesamiento paralelo

HDX 3D Pro ofrece la mejor experiencia de usuario en cualquier ancho de banda:

- En conexiones de red de área extensa (WAN). Entrega una experiencia de usuario interactiva en conexiones WAN con anchos de banda bajos, incluso hasta 1,5 Mbps.
- En conexiones de red de área local (LAN). Entrega una experiencia de usuario equivalente a la de un escritorio local en las conexiones LAN.

  Puede reemplazar estaciones de trabajo complejas y costosas por dispositivos de usuario más simples, al mover el procesamiento de gráficos al centro de datos para una administración centralizada.

HDX 3D Pro ofrece la aceleración de GPU para las máquinas con sistema operativo de sesión única de Windows o multisesión de Windows. Para obtener más información, consulte Aceleración de GPU para sistemas operativos de sesión única Windows y Aceleración de GPU para sistemas operativos multisesión Windows.

HDX 3D Pro es compatible con máquinas sin sistema operativo, además de las tecnologías de virtualización de GPU y GPU PassThrough que ofrecen los siguientes hipervisores:

- XenServer
  - GPU PassThrough con NVIDIA GRID, AMD e Intel GVT-d
  - Virtualización de GPU con NVIDIA GRID, AMD e Intel GVT-g
  - Consulte la compatibilidad de hardware en la Lista de compatibilidad de hardware de Hypervisor.

La herramienta HDX Monitor permite validar la operación y la configuración de las tecnologías de visualización HDX, así como diagnosticar y solucionar problemas relacionados con HDX. Para descargar la herramienta y obtener más información acerca de ella, consulte https://taas.citrix.com/hdx/download/.

## Aceleración de GPU para SO Windows multisesión

January 24, 2024

HDX 3D Pro permite que las aplicaciones con muchos gráficos que se ejecutan en sesiones con SO Windows multisesión se representen en la unidad de procesamiento de gráficos (GPU) del servidor. Al trasladar la representación de los gráficos de OpenGL, DirectX, Direct3D y Windows Presentation Foundation (WPF) a la unidad de procesamiento de gráficos (GPU) del servidor, la CPU del servidor no se ralentiza. Además, el servidor es capaz de procesar más gráficos, dado que la carga de trabajo se divide entre la CPU y la GPU.

Como Windows Server es un sistema operativo multiusuario, varios usuarios pueden compartir una GPU a la que se accede mediante Citrix Virtual Apps sin necesidad de virtualización de GPU (vGPU).

Para las instrucciones que impliquen modificar el Registro, tenga cuidado: si se modifica de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### Compartir GPU

El uso compartido de GPU permite la generación por hardware de GPU de aplicaciones OpenGL y DirectX en las sesiones de escritorio remoto. Tiene las siguientes características:

- Se puede usar en máquinas físicas o virtuales para aumentar el rendimiento y la escalabilidad de las aplicaciones.
- Permite que varias sesiones simultáneas compartan los recursos de la GPU (la mayoría de los usuarios no necesitan el rendimiento de generación de gráficos que da una GPU dedicada).
- No necesita ninguna configuración especial.

Se puede asignar una GPU a la máquina virtual Windows Server en modo de PassThrough completo o GPU virtual (vGPU) siguiendo los requisitos del proveedor de GPU e hipervisor. También se admiten implementaciones bare metal en máquinas físicas con Windows Server.

El uso compartido de GPU no depende de ninguna tarjeta gráfica específica.

- Para máquinas virtuales, seleccione una tarjeta gráfica compatible con el hipervisor en uso. Para obtener una lista de compatibilidad de hardware de XenServer, consulte Lista de compatibilidad de hardware de Hypervisor.
- Cuando se ejecuta directamente sobre el hardware (“bare metal”) se recomienda contar con un único adaptador de pantalla habilitado por el sistema operativo. Si hay varias GPU instaladas en el hardware, inhabilite todas menos una mediante Device Manager.

La escalabilidad mediante el uso compartido de GPU depende de varios factores:

- Las aplicaciones que se ejecuten
- La cantidad de memoria RAM de vídeo que consuman
- La capacidad de procesamiento de la tarjeta gráfica

Algunas aplicaciones administran la falta de memoria RAM de vídeo mejor que otras. Si el hardware se sobrecarga, esto puede provocar inestabilidad o incluso el bloqueo del controlador de la tarjeta gráfica. Limite el número de usuarios simultáneos para evitar esos problemas.

Para confirmar que está teniendo lugar la aceleración por GPU, use una herramienta de terceros, como GPU-Z. GPU-Z está disponible en http://www.techpowerup.com/gpuz/.

- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA y los procesadores gráficos de Intel Iris Pro. Una configuración de directiva (habilitada de forma predeterminada) controla esta funcionalidad y permite el uso de codificación por hardware para la codificación H.264 (si está disponible). Si no está disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software. Para obtener más información, consulte Configuraciones de directiva de gráficos.

### Presentación de DirectX, Direct3D y WPF

La presentación de DirectX, Direct3D y WPF solo está disponible en servidores con una GPU que admita una interfaz de control de presentación (DDI), versión 9ex, 10 u 11.

- En Windows Server 2008 R2, DirectX y Direct3D no requieren ninguna configuración especial para usar una única GPU.
- En Windows Server 2012 y versiones posteriores, las sesiones de Servicios de Escritorio remoto (RDS) en el servidor host de sesión de Escritorio remoto usan el Controlador de representación básica de Microsoft como el adaptador predeterminado. Para usar la GPU en sesiones de RDS en Windows Server 2012 y versiones posteriores, habilite la configuración **Usar el adaptador de gráficos de hardware predeterminado para todas las sesiones de Servicios de Escritorio remoto** en la directiva de grupo **Directiva de equipo local** > **Configuración del equipo** > **Plantillas administrativas** > **Componentes de Windows** > **Servicios de Escritorio remoto** > **Host de sesión de Escritorio remoto** > **Entorno de sesión remota**.
- Para habilitar las aplicaciones WPF para que representen gráficos mediante la GPU del servidor, cree los parámetros en el Registro de Windows del servidor que ejecuta sesiones de SO multisesión Windows. Para obtener información sobre el parámetro de Registro, consulte Representación de Windows Presentation Foundation (WPF) en la lista de funciones administradas a través del Registro.

### Aceleración de GPU para aplicaciones OpenCL o CUDA

La aceleración de GPU para aplicaciones OpenCL y CUDA que se ejecutan en una sesión de usuario está inhabilitada de forma predeterminada.

Para usar las funcionalidades POC de aceleración de CUDA, habilite los parámetros de Registro. Para obtener información, consulte Aceleración de GPU para aplicaciones OpenCL o CUDA en la lista de funciones administradas a través del Registro.

# Aceleración de GPU para SO Windows de sesión única

January 24, 2024

Con HDX 3D Pro, puede entregar aplicaciones de uso intensivo de gráficos como parte de escritorios o aplicaciones que se alojan en máquinas con SO de sesión única. HDX 3D Pro admite equipos host físicos (incluido el escritorio, blade y estaciones de trabajo en rack), así como GPU PassThrough y tecnologías de virtualización de GPU que ofrecen los hipervisores de XenServer, vSphere, Nutanix y Hyper-V (solo PassThrough).

HDX 3D Pro ofrece las siguientes funciones:

- Compresión intensa y adaptable por H.264 o H.265 para un rendimiento WAN e inalámbrico óptimos. HDX 3D Pro utiliza la compresión H.264 de pantalla completa basada en CPU como técnica de compresión predeterminada para la codificación. La codificación por hardware con H.264 se puede usar con tarjetas de NVIDIA, Intel y AMD que admiten NVENC. La codificación por hardware con H.265 se puede usar con tarjetas de NVIDIA que admiten NVENC.
- La opción de compresión sin pérdida para casos de uso especiales. HDX 3D Pro también ofrece un códec sin pérdida basado en CPU para admitir las aplicaciones que necesitan gráficos de calidad perfecta, como, por ejemplo, la creación de imágenes para uso en medicina. La compresión sin pérdida solo se recomienda para casos de uso especializados, ya que consume más recursos de red y de procesamiento.

  Cuando se utiliza la compresión sin pérdida:

  - El indicador de compresión sin pérdida es un icono del área de notificaciones que avisa al usuario cuando la pantalla muestra fotogramas con o sin pérdida. Este icono ayuda cuando la configuración de directiva **Calidad visual** está definida como **Gradual sin pérdida**. El indicador sin pérdida se vuelve verde cuando los fotogramas se envían sin pérdida.
  - La opción para cambiar la calidad sin pérdida permite que el usuario cambie al modo Siempre sin pérdida, en cualquier momento, dentro de la sesión. Para seleccionar o anular la selección de la **compresión sin pérdida en cualquier momento de la sesión**, haga clic con el botón secundario en el icono y haga clic en **Cambiar a Píxel perfecto** o use el atajo ALT+MAYÚS+1.

    Para la compresión sin pérdida: HDX 3D Pro utiliza el códec de compresión sin pérdida, independientemente del códec seleccionado a través de la directiva.

    Para la compresión con pérdida: HDX 3D Pro utiliza el códec original, o el predeterminado o el seleccionado a través de la directiva.

Los parámetros de la opción Cambiar calidad sin pérdida no se conservan para las sesiones subsiguientes. Para usar un códec de compresión sin pérdida en cada conexión, seleccione **Siempre sin pérdida** en la configuración de directiva **Calidad visual**.

- Puede reemplazar el acceso directo predeterminado, ALT + MAYÚS + 1, para seleccionar o anular la selección de la compresión sin pérdida en sesión. Configure un nuevo parámetro del Registro en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Nombre: HKEY_LOCAL_MACHINE_HotKey, Tipo: String
  - El formato para configurar una combinación de acceso directo es: C=0 | 1, A=0 | 1, S=0 | 1, W=0 | 1, K=val. Las claves deben estar separadas por comas (,). El orden de las claves no importa.
  - A, C, S, W y K son teclas que equivalen a las teclas siguientes: C a Control, A a ALT, S a MAYÚS, W a Windows y K a una clave válida. Los valores permitidos para K van de 0 a 9 y de "a"a "z", y son cualquier código de tecla virtual.
  - Por ejemplo:
    - Para F10, defina K = 0x79.
    - Para Ctrl + F10, defina C = 1, K = 0x79.
    - Para Alt + A, defina A = 1, K = a; o bien A = 1, K = A; o bien, K = A, A = 1.
    - Para Ctrl + Alt + 5, defina C = 1, A = 1, K = 5; o bien, A = 1, K = 5, C = 1.
    - Para Ctrl + Mayús + F5, defina A = 1, S = 1, K = 0x74.

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

- Funcionalidad para varios monitores de alta resolución. Para máquinas con SO de sesión única, HDX 3D Pro es compatible con dispositivos de usuario de hasta cuatro monitores. Los usuarios pueden organizar sus monitores con la configuración que deseen y pueden mezclar monitores con resoluciones y orientaciones diferentes. La cantidad de monitores se ve limitada solamente por la capacidad de la GPU del equipo host, el dispositivo de usuario y el ancho de banda disponible. HDX 3D Pro admite todas las resoluciones de monitor. Solo la capacidad de la GPU en el equipo host limita el uso de ciertas resoluciones.
- Resolución dinámica. Puede cambiar el tamaño de la ventana de la aplicación o del escritorio virtual a cualquier resolución. **Nota**: El único método admitido para cambiar la resolución es cambiar el tamaño de la ventana de la sesión de VDA. No se admite el cambio de resolución desde dentro de la sesión de VDA (mediante el **Panel de control > Apariencia** y **Personalización > Pantalla > Resolución de pantalla**).

- Compatibilidad con la arquitectura de GPU virtual de NVIDIA. HDX 3D Pro es compatible con tarjetas de GPU virtual de NVIDIA. Para obtener información, consulte Tecnología de GPU virtual de NVIDIA para PassThrough y uso compartido de GPU. La GPU virtual de NVIDIA permite que múltiples máquinas virtuales tengan acceso directo y simultáneo a una única GPU física, mediante los mismos controladores de gráficos de NVIDIA que se implementan en sistemas operativos no virtualizados.
- Compatibilidad con VMware vSphere y VMware ESX mediante vDGA. Puede utilizar HDX 3D Pro con vDGA para cargas de trabajo RDS y VDI.
- Compatibilidad con VMware vSphere/ESX mediante GPU virtual de NVIDIA y MxGPU de AMD.
- Compatibilidad con Microsoft Hyper-V mediante la asignación de dispositivos diferenciados de Windows Server 2016.
- Compatibilidad con gráficos para centros de datos con la familia de procesadores Intel Xeon E3. HDX 3D Pro admite varios monitores (hasta 3), poner en blanco la consola, una resolución personalizada y una alta velocidad de fotogramas con la familia compatible de procesadores Intel. Para obtener más información, consulte http://www.citrix.com/intel y http://www.intel.com/content/www/us/en/servers/data-center-graphics.html.
- Compatibilidad con RapidFire de AMD en las tarjetas de servidor FirePro de serie S de AMD. HDX 3D Pro admite varios monitores (6 como máximo), consola vacía, resolución personalizada y alta velocidad de fotogramas. Nota: La compatibilidad de HDX 3D Pro con MxGPU de AMD (virtualización de GPU) solo es posible con GPU virtuales de VMware vSphere. XenServer y Hyper-V son compatibles con GPU PassThrough. Para obtener más información, consulte AMD Virtualization Solution.
- Acceso a un codificador de vídeo de alto rendimiento para las GPU de NVIDIA, las de AMD y los procesadores gráficos de Intel Iris Pro. Una configuración de directiva (habilitada de forma predeterminada) controla esta función. Dicha función permite usar la codificación por hardware para la codificación H.264 (si está disponible). Si no está disponible, el VDA recurre a la codificación basada en CPU con el códec de vídeo del software. Para obtener más información, consulte Configuraciones de directiva de gráficos.

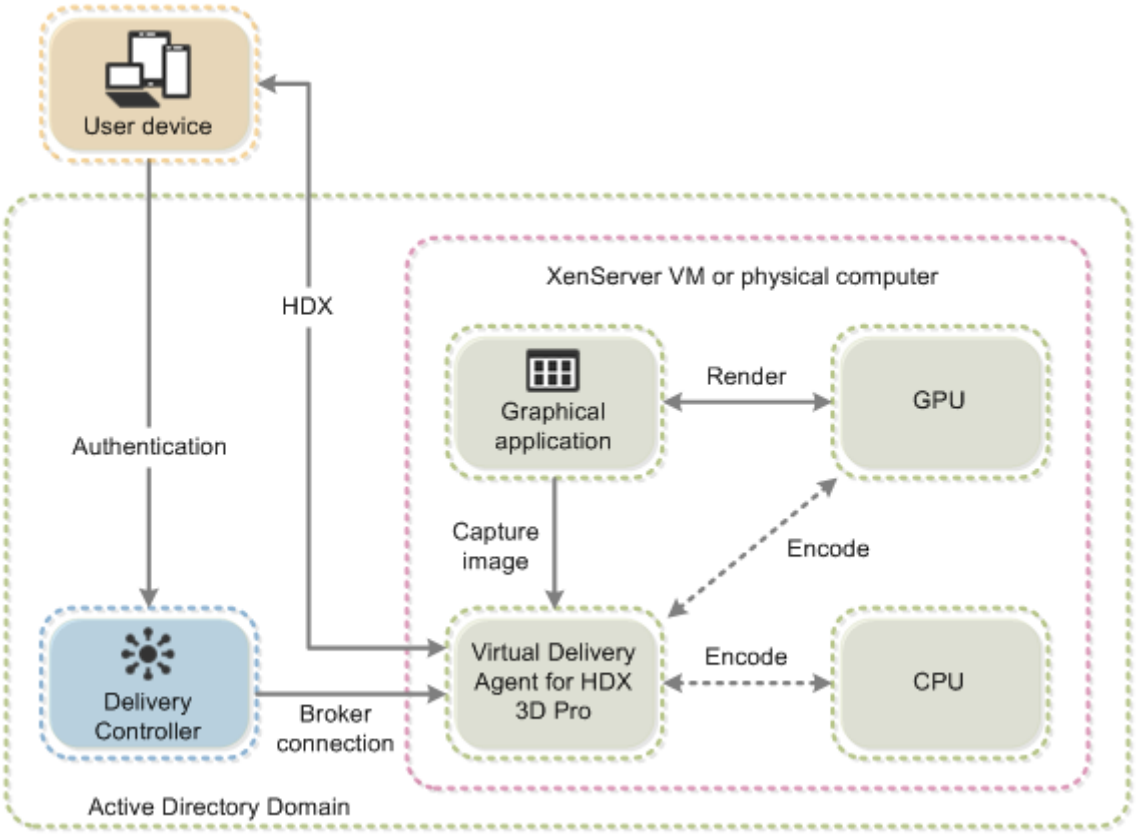
Como se muestra en la siguiente imagen:

- Cuando un usuario inicia sesión en la aplicación Citrix Workspace y accede a la aplicación o escritorio virtual, el Controller autentica al usuario. A continuación, el Controller se pone en contacto con el VDA para HDX 3D Pro con el objetivo de establecer una conexión con el equipo que aloja la aplicación gráfica.

El VDA para HDX 3D Pro utiliza el hardware adecuado en el host para comprimir las vistas del escritorio completo o solamente de la aplicación gráfica.

- Las vistas de escritorio o aplicación y las interacciones del usuario con ellas se transmiten entre el equipo host y el dispositivo del usuario. Esta transmisión se realiza a través de una conexión HDX directa entre la aplicación Citrix Workspace y el VDA para HDX 3D Pro.




## Optimizar la experiencia del usuario de HDX 3D Pro

Para utilizar HDX 3D Pro con varios monitores, asegúrese de que el equipo host está configurado para, al menos, el número de monitores conectados a los dispositivos de usuario. Los monitores conectados al equipo host pueden ser físicos o virtuales.

No conecte un monitor (ya sea físico o virtual) a un equipo host mientras un usuario está conectado a la aplicación o escritorio virtual que proporciona la aplicación gráfica. Si lo hace, puede causar inestabilidad durante la sesión de un usuario.

Indique a los usuarios que no se admiten cambios en la resolución del escritorio (por ellos o una aplicación) mientras haya sesiones de aplicaciones gráficas en curso. Después de cerrar la sesión de la aplicación, el usuario puede cambiar la resolución de la ventana de Desktop Viewer en la aplicación Citrix Workspace: Preferencias de Desktop Viewer.

Cuando varios usuarios comparten una conexión con ancho de banda limitado (como los usuarios en una sucursal), se recomienda utilizar la configuración de directiva **Límite de ancho de banda**

**global de la sesión** para limitar el ancho de banda disponible para cada usuario. Usar este parámetro garantiza que el ancho de banda disponible no fluctúe demasiado a medida que los usuarios inician y cierran sesiones. Como HDX 3D Pro se ajusta automáticamente para usar todo el ancho de banda disponible, las grandes variaciones en el ancho de banda disponible durante el transcurso de las sesiones de usuario pueden afectar negativamente al rendimiento.

Por ejemplo: si 20 usuarios comparten una conexión de 60 Mbps, el ancho de banda disponible para cada usuario puede variar entre 3 y 60 Mbps, según la cantidad de usuarios simultáneos. Para optimizar la experiencia de usuario en este caso, determine el ancho de banda requerido por usuario en los períodos de mayor uso y limite los usuarios a esta cantidad siempre.

Para los usuarios de punteros 3D, se recomienda aumentar la prioridad del canal virtual Redirección de USB genérico a 0. Para obtener información sobre cómo cambiar la prioridad del canal virtual, consulte el artículo CTX128190 de Knowledge Center.

## Thinwire

May 23, 2023

### Introducción

Thinwire, una parte de la tecnología de Citrix HDX, es la tecnología predeterminada de Citrix para pantallas remotas que se utiliza en Citrix Virtual Apps and Desktops.

Las tecnologías de pantallas remotas permiten que los gráficos generados en una máquina se transmitan (normalmente a través de una red) a otra máquina para que se vean desde allí.

Una buena solución de pantallas remotas ofrece una experiencia de usuario altamente interactiva que sea similar a la de un equipo local. Thinwire lo consigue porque utiliza un abanico de técnicas complejas y eficientes para la compresión y el análisis de imágenes. Thinwire maximiza la escalabilidad de los servidores y consume menos ancho de banda que otras tecnologías de pantallas remotas.

Gracias a este equilibrio, Thinwire cubre la mayoría de los casos de uso generales que pueda haber en una empresa, y se usa como la tecnología predeterminada para pantallas remotas en Citrix Virtual Apps and Desktops.

### HDX 3D Pro

En su configuración predeterminada, Thinwire puede entregar gráficos 3D o de interacción elevada y emplear una unidad de procesamiento de gráficos (GPU), si está presente. Sin embargo, se recomienda habilitar el modo HDX 3D Pro mediante las directivas **Optimizar para cargas de trabajo**

**de gráficos 3D** o **Calidad visual > Gradual sin pérdida** para casos en los que las GPU están presentes. Estas directivas configuran Thinwire para que utilice un códec de vídeo (H.264 o H.265) que codifica toda la pantalla mediante la aceleración de hardware si hay una GPU presente. Esto ofrece una experiencia más fluida para gráficos 3D profesionales. Para obtener más información, consulte H.264 gradual sin pérdida, HDX 3D Pro y Aceleración de GPU para SO Windows de sesión única.

### Requisitos

Thinwire está optimizado para sistemas operativos modernos, como Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows 10. Para Windows Server 2008 R2, se recomienda el modo de gráficos antiguo. Utilice las plantillas de directivas Citrix integradas, las plantillas "Alta escalabilidad de servidores para sistemas operativos antiguos"y "Optimización de redes WAN para sistemas operativos antiguos"para entregar las combinaciones de configuraciones de directiva que Citrix recomienda para estos casos de uso.

> **Nota:**
>
> No se admite el modo de gráficos antiguo en esta versión. Este modo se incluye para la compatibilidad con versiones anteriores cuando se usa XenApp 7.15 LTSR y XenDesktop 7.15 LTSR, así como las versiones anteriores de VDA.

- La configuración de directiva que controla el comportamiento de Thinwire, **Usar códec de vídeo para compresión**, está disponible en las versiones de VDA de Citrix Virtual Apps and Desktops 7 1808 y versiones posteriores, así como XenApp y XenDesktop 7.6 FP3 y versiones posteriores. La opción **Usar códec de vídeo si se prefiere** es la configuración predeterminada en las versiones de VDA de Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores, así como XenApp y XenDesktop 7.9 o versiones posteriores.
- Todas las aplicaciones Citrix Workspace admiten Thinwire. Sin embargo, es posible que algunas aplicaciones Citrix Workspace admitan funciones de Thinwire que otras no admiten (por ejemplo, gráficos de 8 o 16 bits para reducir el uso del ancho de banda). La aplicación Citrix Workspace negocia automáticamente si admitir o no esas funciones.
- Thinwire emplea más recursos de servidor (CPU, memoria) cuando hay varios monitores y una alta resolución de pantalla. Es posible ajustar la cantidad de recursos que utiliza Thinwire. Sin embargo, puede que eso provoque un aumento del uso de ancho de banda.
- En situaciones de bajo ancho de banda o latencia elevada, tenga en cuenta la posibilidad de habilitar los gráficos de 8 o 16 bits para mejorar la interactividad. Es posible que la calidad visual se vea afectada, especialmente a una profundidad de color de 8 bits.

### Métodos de codificación

Thinwire puede operar en dos modos de codificación diferentes en función de las prestaciones de las directivas y del cliente:

- Thinwire a pantalla completa con H.264 o H.265
- Thinwire con H.264 o H.265 selectivo

En la comunicación remota GDI antigua, se utilizaba el controlador remoto de XPDM, no un codificador Thinwire de mapa de bits.

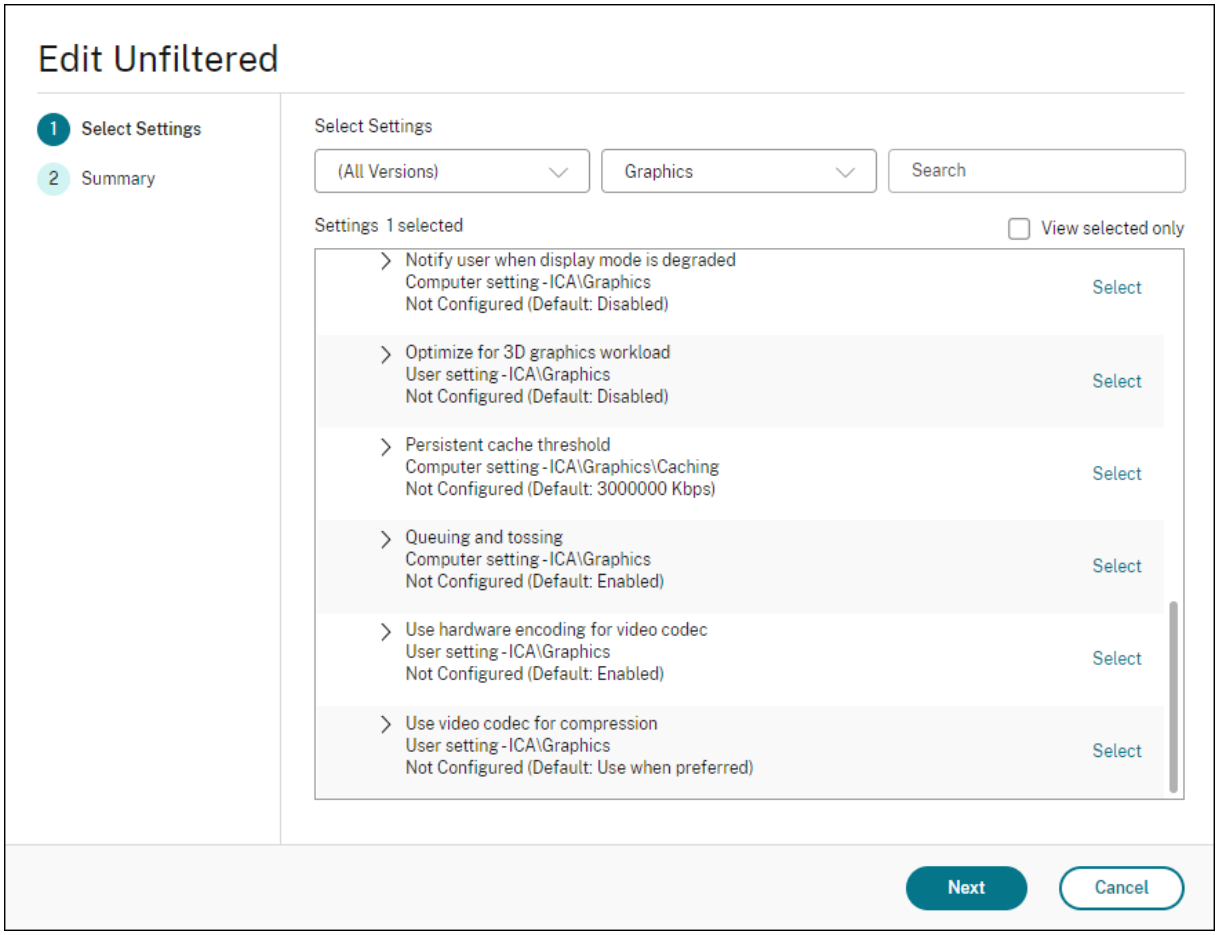
### Configuración

Thinwire es la tecnología predeterminada de pantallas remotas.

La siguiente configuración de directiva de Gráficos establece las opciones predeterminadas y ofrece alternativas a diferentes casos de uso:

- Usar códec de vídeo para compresión
  - **Usar códec de vídeo si se prefiere**. Esta es la opción predeterminada. No se requiere ninguna configuración adicional. Si mantiene esta configuración como predeterminada, Thinwire se seleccionará para todas las conexiones de Citrix, y se optimizará para la escalabilidad, el ancho de banda y una calidad de imagen superior para cargas de trabajo típicas de escritorio. Esto equivale funcionalmente a la opción **Para áreas en cambio constante**.
- Las demás opciones de esta configuración de directiva siguen utilizando Thinwire combinado con otras tecnologías para diferentes casos de uso. Por ejemplo:
  - **Para áreas en cambio constante**. En Thinwire, la tecnología de pantalla adaptable identifica las imágenes en movimiento (vídeo, 3D en movimiento) y usa H.264 o H.265 solo en aquella parte de la pantalla donde se mueva la imagen.
  - **Para la pantalla entera**. Entrega Thinwire con H.264 o H.265 en pantalla completa para mejorar la experiencia del usuario y optimizar el ancho de banda cuando haya un uso intensivo de gráficos 3D. En el caso de H.264 4:2:0 (la directiva **Compresión sin pérdida visual** está inhabilitada), la imagen final no es perfecta (sin pérdida), y es posible que no sea adecuada para ciertas situaciones. En tales casos, considere la posibilidad de usar, en su lugar, H.264 gradual sin pérdida.




Hay otras configuraciones de directiva, incluidas las siguientes configuraciones de directiva de Presentación visual, que se pueden emplear para optimizar el rendimiento de la tecnología de pantallas remotas: Thinwire admite todas.

- Profundidad de color preferida para gráficos simples
- Velocidad de fotogramas de destino
- Calidad visual

Para conocer las combinaciones de configuraciones de directiva que Citrix recomienda para diferentes casos de uso en empresas, use las plantillas de directivas de Citrix integradas. Las plantillas **Alta escalabilidad de servidores** y **Experiencia de usuario de muy alta definición** usan Thinwire con las mejores combinaciones de configuraciones de directiva para las prioridades de la empresa y las expectativas de los usuarios.

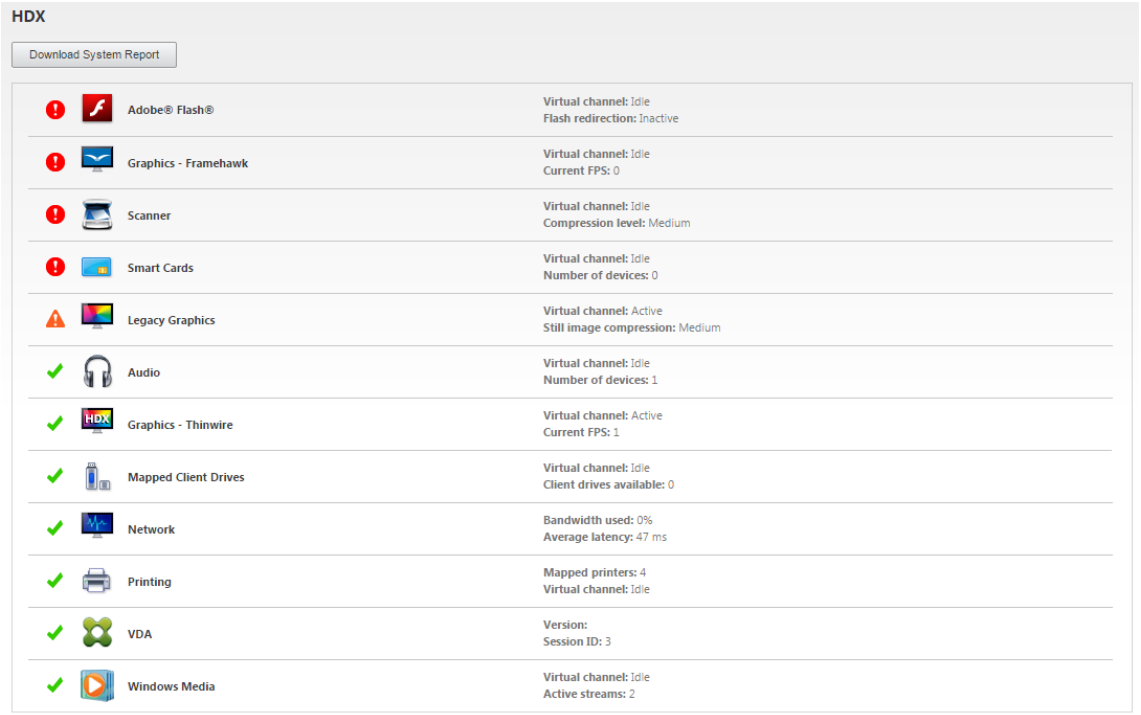
### Supervisar Thinwire

Puede supervisar el uso y el rendimiento de Thinwire desde Citrix Director. La vista de detalles del canal virtual HDX ofrece información útil para la supervisión y la solución de problemas relacionados

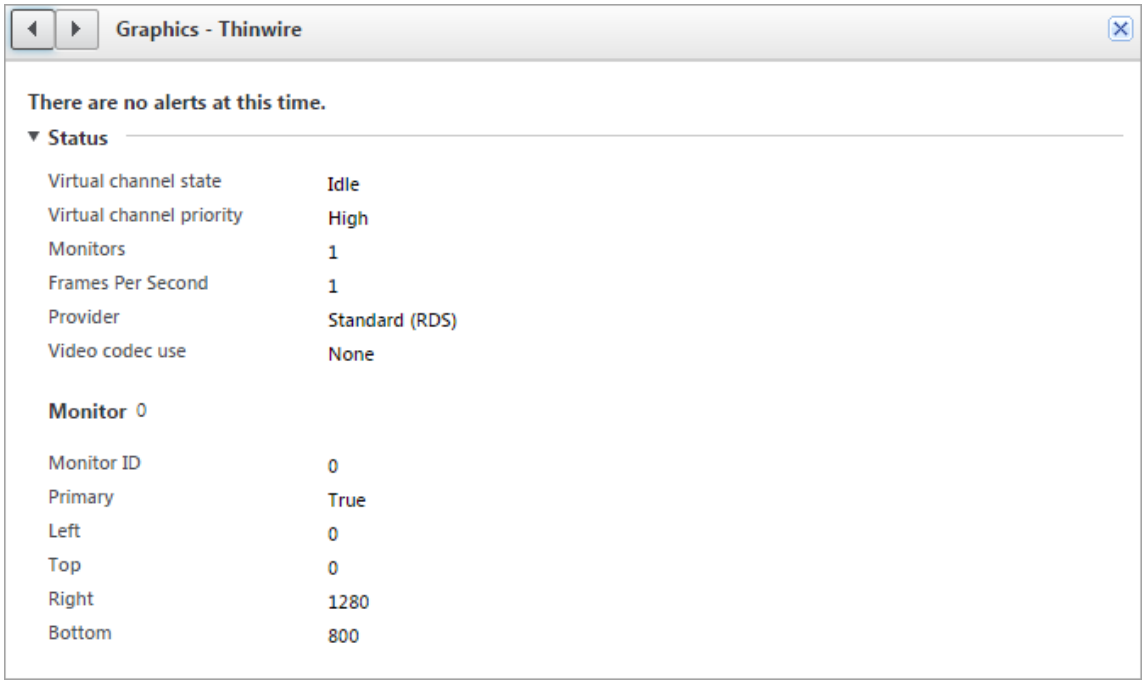
con Thinwire en cualquier sesión. Para ver las métricas relacionadas con Thinwire:

1. En Director, busque un usuario, una máquina o un dispositivo de punto final, abra una sesión activa y haga clic en **Detalles**. Si no, puede seleccionar **Filtros > Sesiones > Todas las sesiones**, abrir una sesión activa y hacer clic en **Detalles**.
2. Desplácese hacia abajo hasta el panel **HDX**.




3. Seleccione **Gráficos: Thinwire**.




## Códec de compresión sin pérdida (MDRLE)

En una sesión de escritorio estándar, la mayoría de las imágenes son gráficos simples o regiones de texto. Thinwire determina dónde se encuentran estas áreas y las selecciona para la codificación sin pérdida mediante el códec 2DRLE. En el lado del cliente de la aplicación Citrix Workspace, esos elementos se decodifican mediante el decodificador 2DRLE del lado de la aplicación Citrix Workspace para mostrarlos en la sesión.

En XenApp y XenDesktop 7.17, agregamos un códec MDRLE, con una razón de compresión más alta y menor consumo de ancho de banda que el códec 2DRLE en sesiones de escritorio estándar. Este nuevo códec no afecta a la escalabilidad de los servidores.

Por lo general, un menor consumo de ancho de banda implica una interactividad de sesión mejorada (especialmente en enlaces compartidos o restringidos) y costes reducidos. Por ejemplo: el consumo de ancho de banda previsto cuando se utiliza el códec MDRLE es, aproximadamente, entre un 10 y un 15 % más pequeño que con XenApp y XenDesktop 7.15 LTSR para cargas de trabajo estándar de Office.

No se requiere ninguna configuración para el códec MDRLE. Si la aplicación Citrix Workspace admite la decodificación MDRLE, el VDA utiliza su propia codificación de MDRLE y la decodificación MDRLE de la aplicación Citrix Workspace. En cambio, si la aplicación Citrix Workspace no admite la decodificación MDRLE, el VDA recurre automáticamente a la codificación 2DRLE.

**Requisitos de MDRLE:**

- Agentes VDA de Citrix Virtual Apps and Desktops 7 1808 (versión mínima)

- Agentes VDA de XenApp y XenDesktop 7.17 (versión mínima)
- Aplicación Citrix Workspace para Windows 1808 (versión mínima)
- Citrix Receiver para Windows 4.11 (versión mínima)

## Modo progresivo

Citrix Virtual Apps and Desktops 1808 presentó el modo progresivo y lo habilitó de forma predeterminada. En condiciones de red restringida (valor predeterminado: ancho de banda < 2 Mbps o latencia > 200 ms), Thinwire aumentó la compresión de texto e imágenes estáticas para mejorar la interactividad durante la actividad en pantalla. Cuando se detiene la actividad en pantalla, el texto y las imágenes altamente comprimidos se vuelven más nítidos de forma progresiva y aleatoria por bloques. Esta compresión y esta mayor nitidez mejoran la interactividad general, reducen la eficiencia de la caché y aumentan el uso del ancho de banda.

A partir de Citrix Virtual Apps and Desktops 1906, el modo progresivo está inhabilitado de forma predeterminada. Ahora empleamos otra estrategia. La calidad de las imágenes estáticas se basa ahora en las condiciones de la red y se halla entre un valor mínimo y un valor máximo predefinidos para cada parámetro de la **calidad visual**. Como no existe ningún paso explícito para aumentar la nitidez, Thinwire optimiza la entrega de imágenes y mantiene la eficiencia de la caché, al tiempo que ofrece casi todos los beneficios del modo progresivo.

### Cambiar el comportamiento del modo progresivo

Puede cambiar el estado del modo progresivo con la clave de Registro. Para obtener información, consulte Modo progresivo en la lista de funciones administradas a través del Registro.

## H.264 gradual sin pérdida

**Gradual sin pérdida** es una configuración especial de Thinwire que optimiza la entrega de gráficos en pos de la interactividad y la calidad final de las imágenes. Para habilitar esta configuración, establezca la directiva **Calidad visual** en **Gradual sin pérdida**.

La opción Gradual sin pérdida comprime la pantalla mediante H.264 (o H.265) durante la actividad en pantalla y la vuelve totalmente nítida (sin pérdida) al cesar la actividad. La calidad de las imágenes de H.264 (o H.265) se adapta a los recursos disponibles para mantener la mejor velocidad de fotogramas posible. El aumento de nitidez se hace gradualmente y da una respuesta inmediata si el usuario inicia la actividad en pantalla poco después de iniciar dicho aumento. Por ejemplo: al seleccionar un modelo y girarlo.

La opción **Gradual sin pérdida** de H.264 ofrece todas las ventajas de H.264 o H.265 en pantalla completa, incluida la aceleración de hardware, pero con el beneficio adicional de una pantalla final y sin

pérdida garantizada. Esto es fundamental para cargas de trabajo de tipo 3D que requieren una imagen final totalmente nítida. Por ejemplo: al manipular imágenes médicas. Además, la opción **Gradual sin pérdida** de H.264 emplea menos recursos que H.264 en pantalla completa 4:4:4. Como resultado, la opción **Gradual sin pérdida** generalmente proporciona una velocidad de fotogramas mayor que H.264 en Compresión sin pérdida visual 4:4:4.

> **Nota:**
>
> Además de la directiva **Calidad visual**, establezca la directiva **Uso de códec de vídeo** en **Usar si se prefiere** (opción predeterminada) o **Para áreas en cambio constante**. Para volver a la opción que no es gradual sin pérdida de H.264, establezca la directiva **Uso de códec de vídeo** en **No usar códec de vídeo**. El resultado es la codificación de las imágenes en movimiento con JPEG en lugar de H.264 (o H.265).

## Marca de agua de sesión basada en texto

March 30, 2022

Las marcas de agua de la sesión basadas en texto ayudan a disuadir del robo de datos y rastrear los datos robados. Esta información rastreable aparece en el escritorio de la sesión como un elemento de disuasión para quienes usan fotografías y capturas de pantalla para robar datos. Puede especificar una marca de agua que sea una capa de texto y aparezca en toda la pantalla de la sesión, sin cambiar por ello el contenido del documento original. Las marcas de agua de la sesión basadas en texto requieren que se admita el VDA.

> **Importante:**
>
> La marca de agua de la sesión basada de texto no es una función de seguridad. Esta solución no impide por completo el robo de datos, pero ofrece cierto nivel de disuasión frente al robo de datos y rastreabilidad de los datos robados. Aunque no garantizamos una rastreabilidad completa de la información cuando se utiliza esta función, recomendamos combinar esta función con otras soluciones de seguridad, según corresponda.

La marca de agua de la sesión es texto y se aplica a la sesión que se entrega al usuario. La marca de agua de la sesión contiene información para rastrear datos robados. La información más importante es la identidad del usuario que inició la sesión en la que se realizó la captura de la pantalla. Para rastrear la filtración de datos de manera más efectiva, incluya otra información (como la hora de conexión y la dirección del protocolo de Internet del servidor o del cliente).

Para ajustar la experiencia del usuario, use las configuraciones de directiva de Marca de agua para definir la ubicación y la apariencia de la marca de agua en la pantalla.

**Requisitos:**

Agentes Virtual Delivery Agent:

SO multisesión 7.17
SO de sesión única 7.17

**Limitaciones:**

- No se admiten las marcas de agua en las sesiones donde se utiliza el acceso a aplicaciones locales, la redirección de Windows Media, MediaStream, la redirección de contenido del explorador web y la redirección de vídeo HTML5. Por tanto, para usar la marca de agua de la sesión, estas funciones deben estar inhabilitadas.
- No se admite la marca de agua de la sesión, y esta no aparece si la sesión se ejecuta en modos de aceleración de hardware en pantalla completa (codificación H.264 o H.265 en pantalla completa).
- Si configura estas directivas HDX, la configuración de la marca de agua no tendrá efecto y no se mostrará ninguna marca de agua en la pantalla de la sesión.

**Usar codificación por hardware para códec de vídeo** en **Habilitado**
**Usar códec de vídeo para compresión** en **Para la pantalla entera**

- Si configura estas directivas HDX, el comportamiento será desconocido y es posible que la marca de agua no aparezca.

  **Usar codificación por hardware para códec de vídeo** en **Habilitado**
  **Usar códec de vídeo para compresión** en **Usar códec de vídeo si se prefiere**

  Para asegurarse de que la marca de agua aparezca, establezca **Usar codificación por hardware para códec de vídeo** en **Inhabilitado** o establezca **Usar códec de vídeo para compresión** en **Para áreas en cambio constante** o **No usar códec de vídeo**.
- La marca de agua de las sesiones solo es compatible con el modo de gráficos Thinwire.
- Si usa la Grabación de sesiones, la sesión grabada no incluirá la marca de agua.
- Si usa la Asistencia remota de Windows, la marca de agua no aparece.
- Si un usuario presiona la tecla **Imprimir pantalla**, la pantalla capturada en el lado del VDA no incluirá las marcas de agua. Le recomendamos que tome las medidas oportunas para evitar que se copie la imagen capturada.

## Contenido multimedia

April 1, 2022

El conjunto de tecnologías HDX admite la entrega de aplicaciones multimedia a través de dos enfoques complementarios:

- Entrega de contenido multimedia generado en el servidor
- Redirección de contenido multimedia generado en el cliente

Esta estrategia le garantiza la entrega de una gama completa de formatos multimedia con una excelente experiencia del usuario, al mismo tiempo que maximiza la escalabilidad de los servidores para reducir el coste por usuario.

Con la entrega de contenido multimedia generado en el servidor, la aplicación decodifica y genera el contenido de audio y vídeo en el servidor de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Una vez recibido, el contenido se comprime y se entrega por protocolo ICA a la aplicación Citrix Workspace presente en el dispositivo del usuario. Este método proporciona la máxima compatibilidad con aplicaciones y formatos de medios distintos. Puesto que el procesamiento de vídeo consume muchos recursos de procesamiento, la entrega multimedia generada en el servidor aprovecha considerablemente la aceleración integrada de hardware. Por ejemplo, la aceleración de vídeo DirectX (DXVA) reduce la carga en la CPU porque realiza la decodificación H.264 en otro hardware aparte. Las tecnologías Intel Quick Sync, AMD RapidFire y NVIDIA NVENC proporcionan la codificación H.264 acelerada por hardware.

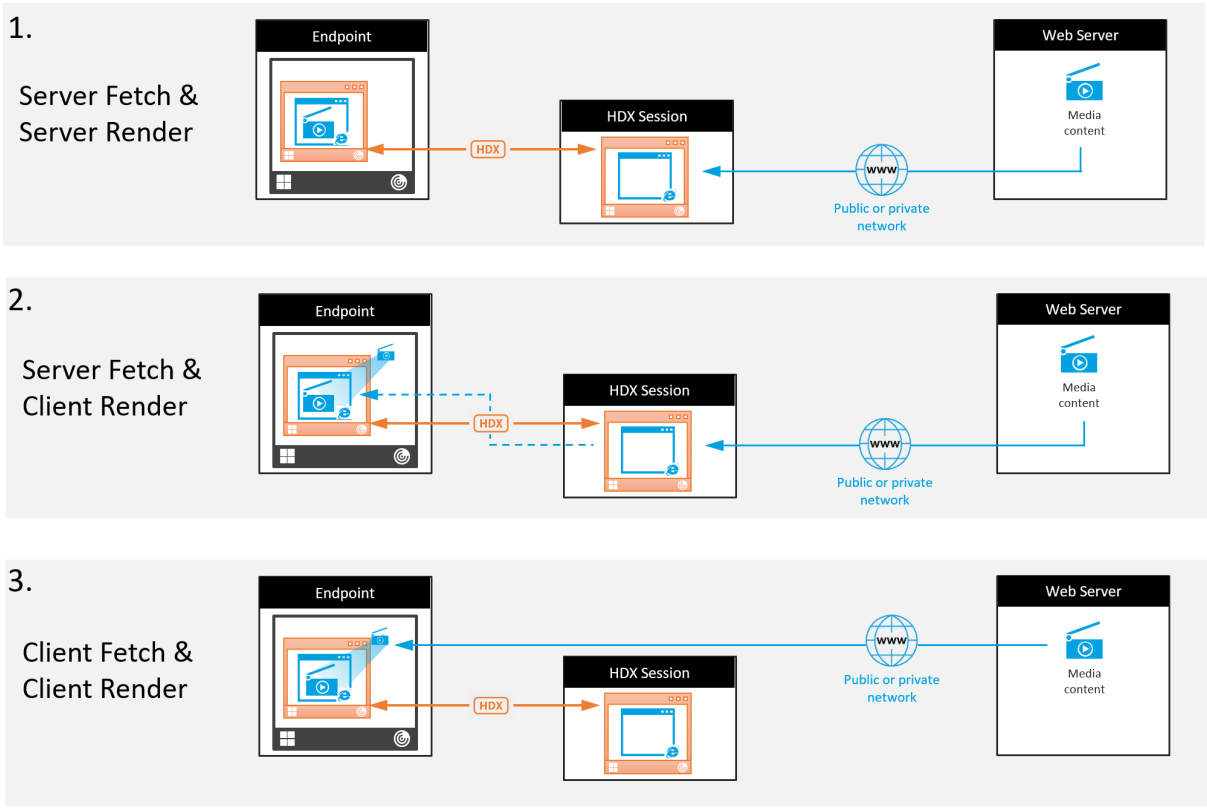
Puesto que la mayoría de los servidores no ofrecen ninguna aceleración de hardware para la compresión de vídeo, la escalabilidad de servidor se ve afectada negativamente si todo el procesamiento de vídeo se realiza en el servidor de la CPU. Para mantener una alta escalabilidad de servidor, redirija muchos formatos multimedia al dispositivo del usuario para su generación local.

- La redirección de Windows Media reduce la carga del servidor cuando se trata de una amplia variedad de formatos de medios normalmente asociados al Reproductor de Windows Media.
- El vídeo HTML5 se ha vuelto popular, y Citrix presentó una tecnología de redirección para este tipo de contenido. Recomendamos el redireccionamiento de contenido de explorador para sitios web que utilizan HTML5, HLS, DASH o WebRTC.
- Puede aplicar tecnologías generales de redirección del host al cliente y el acceso a aplicaciones locales para el contenido multimedia.

Si combina estas dos tecnologías pero no configura la redirección, HDX genera el contenido en el servidor.
En cambio, si configura la redirección, HDX utiliza la opción "obtener en el servidor y generar en el cliente"u "obtener en el cliente y generar en el cliente". Si se producen fallos cuando utiliza estos métodos, HDX recurre a la generación en el servidor cuando sea necesario y se rige por la directiva de prevención de reserva.

### Casos de ejemplo




**Caso 1. (Obtener en servidor y generar en servidor):**

1. El servidor obtiene el archivo multimedia desde su origen, lo decodifica y, a continuación, presenta su contenido a un dispositivo de sonido o un dispositivo de pantalla.
2. El servidor extrae la imagen o el sonido presentados del dispositivo de pantalla o del dispositivo de sonido respectivamente.
3. El servidor puede comprimirlo y, a continuación, lo transmite al cliente.

Este enfoque implica un alto consumo de CPU, de alto ancho de banda (si la imagen o el sonido extraídos no se comprimen eficazmente), y tiene una escalabilidad de servidor baja.

Thinwire y los canales virtuales de sonido se ocupan de este enfoque. La ventaja de este enfoque es que reduce los requisitos de hardware y software para los clientes. Con este enfoque, la decodificación ocurre en el servidor y funciona para una mayor variedad de dispositivos y formatos.

**Caso 2. (Obtener en servidor y generar en cliente):**

Este enfoque necesita poder interceptar el contenido multimedia antes de que se decodifique y se presente al dispositivo de sonido o de pantalla. El contenido de audio o vídeo comprimidos se envía al cliente, donde se decodifica y se presenta localmente. La ventaja de este enfoque es que se transmite a los dispositivos cliente, con lo que se ahorran ciclos de CPU en el servidor.

Sin embargo, conlleva algunos requisitos de hardware y software adicionales para el cliente. El cliente debe poder decodificar todos los formatos que pueda recibir.

**Caso 3. (Obtener en cliente y generar en cliente):**

Este enfoque se basa en la capacidad de interceptar la URL del contenido multimedia antes de que se obtenga desde el origen. La dirección URL se envía al cliente, donde el contenido multimedia se obtiene, se decodifica y se presenta localmente. Este enfoque es conceptualmente simple. Su ventaja es que ahorra ancho de banda y ciclos de CPU en el servidor, porque el servidor solo envía comandos de control. No obstante, el contenido multimedia no siempre está disponible para los clientes.

**Entorno y plataforma:**

Los sistemas operativos de sesión única (Windows, Mac OS X y Linux) ofrecen entornos multimedia que permiten un desarrollo más rápido de aplicaciones multimedia. En esta tabla se muestran algunos de los entornos multimedia más comunes. En cada entorno se divide el procesamiento multimedia en varias etapas y se usa una arquitectura adaptada.

| Framework | Platform |
|---|---|
| DirectShow | Windows (98 y versiones posteriores) |
| Media Foundation | Windows (Vista y versiones posteriores) |
| Gstreamer | Linux |
| QuickTime | Mac OS X |

## Funcionalidad de doble salto con tecnologías de redirección multimedia

| | | |
|---|---|---|
| | Redirección de sonido | No |
| | Redirección de contenido de explorador web | No |
| | Redirección de cámara web HDX | Sí |
| | Redirección de vídeo HTML5 | Sí |
| | Redirección de Windows Media | Sí |

# Funciones de audio

September 26, 2022

Puede configurar y agregar las siguientes configuraciones de directiva de Citrix a una directiva que optimice las funciones de audio de HDX. Para obtener información acerca del uso, las relaciones y las dependencias con otras configuraciones de directiva, consulte Configuraciones de directiva de audio, Configuraciones de directiva de ancho de banda y Configuraciones de directiva de conexiones de multisecuencia.

> **Importante:**
>
> Recomendamos entregar el audio mediante el protocolo de datagramas de usuario (UDP) en lugar de TCP. Solo Virtual Delivery Agent (VDA) de Windows admite audio por UDP.
>
> El cifrado de audio por UDP mediante DTLS solo está disponible entre Citrix Gateway y la aplicación Citrix Workspace. Por lo tanto, a veces puede ser preferible utilizar el transporte TCP. TCP admite el cifrado TLS de punto a punto desde el VDA a la aplicación Citrix Workspace.

## Calidad de audio

En general, un audio de mayor calidad consume más ancho de banda y utiliza más recursos de CPU del servidor, al enviar más datos de audio a los dispositivos de los usuarios. La compresión de audio permite llegar a un equilibrio entre calidad de audio y rendimiento general de la sesión; use las configuraciones de directiva de Citrix para configurar los niveles de compresión que se deben aplicar a los archivos de audio.

De forma predeterminada, la configuración de **la directiva Calidad de audio** está establecida en "Alta: audio de alta definición"cuando se utiliza el transporte TCP. En cambio, la directiva "Calidad de audio" se establece en "Medio: optimizado para voz"cuando se utiliza el transporte UDP (opción recomendada). El parámetro **Alta: audio de alta definición** ofrece audio estéreo de alta fidelidad, pero consume más ancho de banda que los demás parámetros de calidad. No use este nivel de calidad de audio para aplicaciones de videochat o chat de voz no optimizadas (por ejemplo, programas de softphone). Puede provocar unos niveles de latencia en la ruta de audio que no son adecuados para las comunicaciones en tiempo real. Se recomienda la configuración de directiva "Medio: optimizado para voz"para audio en tiempo real, independientemente del protocolo de transporte seleccionado.

Cuando el ancho de banda es limitado (conexiones por satélite o acceso telefónico), reducir la calidad del audio a **Baja** consume el menor ancho de banda posible. En este caso, deberá crear directivas distintas para los usuarios en las conexiones de poco ancho de banda para que los usuarios que disponen de conexiones con buen ancho de banda no se vean afectados negativamente.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de audio. Recuerde que debe habilitar "Parámetros de audio del cliente"en el dispositivo del usuario.

Directrices sobre ancho de banda para la reproducción y grabación de audio:

- Alta calidad (valor predeterminado)
  - Velocidad de bits: ~ 100 kbps (mín. 75, máx. 175 kbps) para reproducción / ~ 70 kbps para captura de micrófono
  - Número de canales: 2 (estéreo) para reproducción, 1 (mono) para captura de micrófono
  - Frecuencia: 44100 Hz.
  - Profundidad de bits: 16 bits
- Calidad media (recomendada para VoIP)
  - Velocidad de bits: ~ 16 kbps (mín. 20, máx. 40 kbps) para reproducción, ~ 16 kbps para captura de micrófono
  - Número de canales: 1 (Mono) para reproducción y captura
  - Frecuencia: 16000 Hz (banda ancha)
  - Profundidad de bits: 16 bits
- Calidad baja
  - Velocidad de bits: ~ 11 kbps (mín. 10, máx. 25 kbps) para reproducción, ~ 11 kbps para captura de micrófono
  - Número de canales: 1 (Mono) para reproducción y captura
  - Frecuencia: 8000 Hz (banda estrecha)
  - Profundidad de bits: 16 bits

### Redirección de audio del cliente

Para permitir que los usuarios reciban audio desde una aplicación en un servidor mediante los altavoces u otros dispositivos de audio en sus dispositivos de usuario, deje la configuración **Redirección de audio del cliente** en **Permitida**. Esta es la opción predeterminada.

La asignación de audio del cliente genera una carga adicional para los servidores y para la red. Cuando la Redirección de audio del cliente está Prohibida, toda la función de audio de HDX queda inhabilitada.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de audio. Recuerde que debe habilitar "Parámetros de audio del cliente"en el dispositivo del usuario.

### Redirección de micrófonos del cliente

Para permitir que los usuarios graben audio por medio de dispositivos de entrada (por ejemplo, micrófonos) en sus dispositivos, deje el parámetro **Redirección de micrófonos del cliente** en su opción predeterminada (Permitida).

Por motivos de seguridad, se alerta a los usuarios si un servidor en el que no confía el dispositivo de usuario intenta acceder a su micrófono. El usuario puede elegir entre aceptar o rechazar dicho acceso, antes de usar el micrófono. Los usuarios pueden inhabilitar esta alerta en la aplicación Citrix Workspace.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de audio. Recuerde que debe habilitar "Parámetros de audio del cliente"en el dispositivo del usuario.

### Audio Plug and Play

La configuración de directiva Audio Plug and Play controla si se permite o se impide el uso de varios dispositivos de audio para grabar y reproducir audio. Esta configuración está **habilitada** de forma predeterminada. Audio Plug N Play permite reconocer los dispositivos de audio. Los dispositivos se reconocen aunque no estén conectados hasta después de que se haya iniciado la sesión de usuario.

Esta configuración solo se aplica a máquinas de SO multisesión Windows.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de audio.

### Límite de ancho de banda de redirección de audio y Porcentaje límite de ancho de banda de redirección de audio

La configuración de directiva Límite de ancho de banda de redirección de audio especifica el ancho de banda máximo (en kilobits por segundo) que se puede usar para la reproducción y grabación de audio en una sesión.

La configuración Porcentaje límite de ancho de banda de redirección de audio especifica el ancho de banda máximo que se puede usar para la redirección de audio, expresado como un porcentaje del ancho de banda total disponible.

De manera predeterminada, el valor para ambos es cero (no hay máximo). Si se han configurado ambos parámetros, se usará aquél que ofrezca la menor limitación de ancho de banda.

Para obtener más información acerca de la configuración, consulte Configuraciones de directiva de ancho de banda. Recuerde que debe habilitar "Parámetros de audio del cliente"en el dispositivo del usuario.

### Transporte de audio en tiempo real por UDP e Intervalo de puertos UDP de audio

De manera predeterminada, la opción "Transporte de audio en tiempo real por UDP"está "Permitida" (si se selecciona en el momento de la instalación). Esa opción abre un puerto UDP en el servidor para las conexiones que usan el transporte de audio en tiempo real por UDP. En caso de una congestión de red o pérdida de paquetes, se recomienda configurar UDP/RTP para el audio para garantizar la mejor experiencia de usuario Para cualquier audio en tiempo real típico de aplicaciones softphone, se prefiere el audio UDP antes que EDT. UDP permite la pérdida de paquetes sin retransmisión, con lo que no se agrega latencia en las conexiones con pérdidas grandes de paquetes.

> **Importante:**
>
> Cuando Citrix Gateway no está en la ruta, los datos de audio transmitidos por UDP no se cifran. Si Citrix Gateway está configurado para acceder a los recursos de Citrix Virtual Apps and Desktops, el tráfico de audio entre el dispositivo de punto final y Citrix Gateway se protege mediante el protocolo DTLS.

El "Intervalo de puertos UDP de audio"especifica el intervalo de números de puerto que Windows VDA utiliza para intercambiar datos de paquetes de audio con el dispositivo de usuario.

De manera predeterminada, el intervalo es de 16500 a 16509.

Para obtener más información sobre el Transporte de audio en tiempo real por UDP, consulte Configuraciones de directiva de audio. Para obtener más información sobre el Intervalo de puertos UDP de audio, consulte Configuraciones de directiva de conexiones de multisecuencia. Recuerde que debe habilitar "Parámetros de audio del cliente"en el dispositivo del usuario.

El audio por UDP requiere el Windows VDA. Para obtener información sobre las directivas compatibles en Linux VDA, consulte Lista de directivas disponibles.

### Configuraciones de directiva de audio para los dispositivos de usuario

1. Cargue las plantillas de directiva de grupo siguiendo las instrucciones de Configurar la plantilla administrativa de objeto de directiva de grupo.
2. En el Editor de directivas de grupo, expanda **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
3. En **Configuración del audio del cliente**, seleccione **No configurada**, **Habilitada** o **Inhabilitada**.
    - **No configurada**. De forma predeterminada, la redirección de audio está habilitada con alta calidad de audio, o con los parámetros de audio personalizados configurados previamente.
    - **Habilitada**. Habilita la redirección de audio mediante las opciones seleccionadas.

- **Inhabilitado**. Inhabilita la redirección de audio.

4. Si ha seleccionado **Habilitada**, elija una calidad de audio. Para el audio UDP, use solo la calidad de audio **media** (la predeterminada).
5. Para el audio UDP solamente, seleccione **Enable Real-Time Transport** y configure el intervalo de puertos de entrada que se abrirán en el Firewall de Windows local.
6. Para utilizar el audio UDP con Citrix Gateway, seleccione **Permitir transporte en tiempo real a través de NetScaler Gateway**. Configure Citrix Gateway con DTLS. Para obtener más información, consulte este artículo.

Como administrador, si no tiene control sobre los dispositivos de punto final para hacer estos cambios, use los atributos del archivo default.ica de StoreFront para habilitar el audio UDP. Por ejemplo, en el caso de dispositivos que son propiedad de los usuarios (Bring Your Own Device) o equipos domésticos.

1. En la máquina de StoreFront, abra C:\inetpub\wwwroot\Citrix\<nombre del almacén>\App_Data\default.ica con un editor de texto como el Bloc de notas.
2. Cree estas entradas en la sección [Aplicación].

   ; Este texto permite el transporte en tiempo real

   EnableRtpAudio=true

   ; Este texto permite el transporte en tiempo real a través de la puerta de enlace

   EnableUDPThroughGateway=true

   ; Este texto establece la calidad del audio en Media

   AudioBandwidthLimit=1

   ; Intervalo de puertos UDP

   RtpAudioLowestPort=16500

   RtpAudioHighestPort=16509

Si el audio UDP se habilita mediante la edición de default.ica, el audio UDP estará habilitado para todos los usuarios que utilicen ese almacén.

### Evitar eco durante conferencias multimedia

Los usuarios de conferencias de audio o de vídeo pueden escuchar un eco. El eco normalmente ocurre cuando los altavoces están muy cerca del micrófono. En estos casos, se recomiendan auriculares para conferencias con audio y vídeo.

HDX ofrece una opción de eliminación de ecos (habilitada de forma predeterminada), que permite minimizarlos. La eficacia de la eliminación del eco depende de la distancia entre los altavoces y el micrófono. Los dispositivos no deben estar demasiado cerca ni demasiado lejos el uno del otro.

La eliminación de eco se puede inhabilitar mediante un parámetro de Registro. Para obtener información, consulte Evitar eco durante conferencias multimedia en la lista de funciones administradas a través del Registro.

### Softphone

Una aplicación softphone es un software que actúa como una interfaz de teléfono. Se utiliza un software softphone para realizar llamadas por Internet desde un equipo o una tableta, por ejemplo. Con softphone, puede marcar números de teléfono y llevar a cabo otras funciones relacionadas con el teléfono a través de una pantalla.

Citrix Virtual Apps and Desktops admiten varias alternativas para la entrega de aplicaciones softphone.

- **Modo de control**. La aplicación softphone alojada controla un teléfono físico configurado. En este modo, no hay tráfico de audio que pase por el servidor de Citrix Virtual Apps and Desktops.
- **Optimización de HDX RealTime para softphone (recomendado)**. El motor de medios se ejecuta en el dispositivo de usuario, y el tráfico VoIP (Voice over Internet Protocol) pasa de un homónimo a otro. Para ver ejemplos, consulte:
  - Optimización de HDX para Microsoft Teams
  - HDX RealTime Optimization Pack, que optimiza la entrega de Skype Empresarial de Microsoft
  - Cisco Jabber Softphone para VDI (anteriormente conocido como VXME)
  - Reuniones de Cisco Webex para VDI
  - Avaya VDI Equinox (antes conocido como VDI Communicator)
  - Plugin Zoom para entornos VDI
  - Genesys PureEngage Cloud
  - Dispositivo de dictado Nuance PowerMic para Dragon
- **Acceso a aplicaciones locales**. Una función de Citrix Virtual Apps and Desktops y Citrix DaaS (antes, Citrix Virtual Apps and Desktops service) que permite que una aplicación softphone se ejecute localmente en el dispositivo Windows del usuario, al mismo tiempo que aparece perfectamente integrada en el escritorio virtual o publicado. Con esta función, toda la carga del procesamiento de audio pasa al dispositivo del usuario. Para obtener más información, consulte Acceso a aplicaciones locales y redirección de URL.
- **Funcionalidad genérica de HDX RealTime para softphone.** VoIP por ICA.

***Funcionalidad genérica para softphone***

La funcionalidad genérica para softphone permite alojar un softphone no modificado en el centro de datos de XenApp o XenDesktop. El tráfico de audio se dirige mediante el protocolo ICA de Citrix (preferentemente por UDP/RTP) al dispositivo de usuario que ejecuta la aplicación Citrix Workspace.

La funcionalidad genérica para softphone es una función de HDX RealTime. Este enfoque a la entrega de softphone es especialmente útil para:

- La solución optimizada para entregar el softphone no está disponible y el usuario no está en un dispositivo Windows donde se pueda utilizar el Acceso a aplicaciones locales.
- El motor de medios necesario para la entrega optimizada del softphone no se ha instalado en el dispositivo de usuario o no está disponible para la versión de sistema operativo que ejecuta el dispositivo del usuario. En este caso, HDX RealTime genérico ofrece una buena solución a la que recurrir.

Existen dos aspectos a tener en cuenta en la entrega de softphone con Citrix Virtual Apps and Desktops:

- ¿Cómo se entrega la aplicación softphone al escritorio virtual o publicado?
- ¿Cómo se entrega el audio desde y hacia los auriculares, el micrófono y el altavoz o el set USB para teléfonos del usuario?

Citrix Virtual Apps and Desktops contiene numerosas tecnologías para ofrecer la entrega genérica de softphone:

- Códec optimizado para voz si quiere codificar rápidamente audio en tiempo real y quiere un uso eficiente del ancho de banda.
- Pila de audio para latencia baja.
- Búfer de vibración en el servidor para suavizar el audio cuando fluctúa la latencia de red.
- Etiquetado de paquetes (DSCP y WMM) para la calidad de servicio.
  - Etiquetado de DSCP para paquetes RTP (Layer 3)
  - Etiquetado de WMM para Wi-Fi

Las versiones de la aplicación Citrix Workspace para Mac, Windows, Linux y Chrome también admiten VoIP. La aplicación Citrix Workspace para Windows ofrece estas funciones:

- Búfer de vibración en el cliente: Suaviza el audio incluso cuando fluctúa la latencia de red.
- Eliminación de eco: Permite mayor variación en la distancia entre el micrófono y los altavoces para usuarios que no disponen de auriculares con micrófono.
- Audio Plug and Play: Los dispositivos de audio no necesitan estar conectados antes de iniciar una sesión. Se pueden conectar en cualquier momento.
- Redirección de dispositivos de audio: Los usuarios pueden dirigir tonos a los altavoces, mientras que la voz va a sus auriculares.
- ICA de multisecuencia: Permite la redirección flexible basada en la calidad de servicio (QoS) a través de la red.

- ICA admite cuatro flujos TCP y dos UDP. Uno de los flujos UDP admite el audio en tiempo real por RTP.

Para ver un resumen de las funciones de la aplicación Citrix Workspace, consulte la Tabla de funciones de Citrix Receiver.

***Recomendaciones de configuración del sistema***

*Hardware y software del cliente*:
Para una calidad óptima del sonido, le recomendamos la versión más reciente de la aplicación Citrix Workspace y unos auriculares de buena calidad con eliminación de eco acústico (AEC). Las versiones de la aplicación Citrix Workspace para Windows, Linux y Mac admiten VoIP. Además, Dell Wyse ofrece compatibilidad con VoIP en ThinOS (WTOS).

*Consideraciones sobre CPU*:
Supervise el consumo de CPU en el VDA para determinar si es necesario asignar dos CPU virtuales a cada máquina virtual. La transmisión de voz y vídeo en tiempo real consumen muchos recursos. Configurar dos CPU virtuales reduce la latencia generada por cambiar de subprocesos. Por lo tanto, se recomienda configurar dos unidades CPU virtuales en un entorno de VDI de Citrix Virtual Desktops.

Tener dos CPU virtuales no significa necesariamente doblar la cantidad de unidades CPU físicas, porque las CPU físicas existentes pueden compartirse entre varias sesiones.

Citrix Gateway Protocol (CGP), que se utiliza para la función de fiabilidad de la sesión, también aumenta el consumo de CPU. Puede inhabilitar esta función para reducir el consumo de CPU en el VDA cuando se trate de conexiones de red de alta calidad. Ninguno de los pasos anteriores es necesario en un servidor potente.

*Audio UDP*:
El audio por UDP ofrece una tolerancia excelente frente a la congestión de red y a la pérdida de datos. Se recomienda UDP en lugar de TCP cuando esté disponible.

*Configuración de LAN o WAN*:
Configurar correctamente la red es fundamental para una buena calidad de audio en tiempo real. Por lo general, debe configurar LAN virtuales (vLAN) porque demasiados paquetes de difusión pueden provocar vibración. Los dispositivos habilitados con IPv6 pueden generar una gran cantidad de paquetes de difusión. Si no se necesita compatibilidad con IPv6, puede inhabilitar IPv6 en esos dispositivos. Configure esta funcionalidad para admitir la calidad de servicio.

*Parámetros para usar conexiones WAN*:
Puede usar el chat de voz a través de conexiones LAN y WAN. En una conexión WAN, la calidad del audio depende de la latencia, la pérdida de paquetes y la vibración existentes en la conexión. Si entrega aplicaciones softphone a los usuarios por una conexión WAN, se recomienda usar NetScaler SD-WAN entre el centro de datos y la oficina remota. Así, se mantiene una alta calidad de servicio (QoS). NetScaler SD-WAN admite ICA de multisecuencia, incluido UDP. Además, en caso de un único flujo

TCP, puede establecer prioridades distintas para los diferentes canales virtuales ICA para garantizar que los datos de audio en tiempo real de alta prioridad se traten de manera preferente.

Use Director o HDX Monitor para validar la configuración de HDX.

*Conexiones de usuarios remotos*:
Citrix Gateway admite DTLS para entregar el tráfico UDP/RTP de forma nativa (sin encapsulación en TCP).
Abra los firewalls en los dos sentidos para el tráfico UDP en el puerto 443.

*Selección de códecs y consumo de ancho de banda*:
Entre el dispositivo de usuario y el VDA del centro de datos, se recomienda usar el parámetro de códec **optimizado para voz**, también conocido como calidad de audio media. Entre la plataforma VDA y la PBX de IP, el softphone utiliza el códec configurado o negociado. Por ejemplo:

- G711 ofrece una calidad de voz muy buena, pero presenta un requisito de ancho de banda de 80 a 100 kilobits por segundo y por llamada (según la sobrecarga de Network Layer2).
- G729 ofrece una buena calidad de voz y presenta un requisito de ancho de banda de 30 a 40 kilobits por segundo y por llamada (según la sobrecarga de Network Layer2).

#### *Entregar aplicaciones softphone al escritorio virtual*

Existen dos métodos para entregar una aplicación softphone al escritorio virtual XenDesktop:

- La aplicación puede instalarse en la imagen del escritorio virtual.
- La aplicación puede distribuirse por streaming al escritorio virtual mediante Microsoft App-V. Este enfoque ofrece ventajas de capacidad de administración, porque la imagen del escritorio virtual se mantiene limpia. Después de distribuirse por streaming al escritorio virtual, la aplicación se ejecuta en ese entorno como si se hubiera instalado de la forma habitual. No todas las aplicaciones son compatibles con App-V.

#### *Entregar audio desde y hacia el dispositivo de usuario*

HDX RealTime genérico admite dos métodos para entregar audio desde y hacia el dispositivo de usuario:

- **Citrix Audio Virtual Channel**. Por lo general, se recomienda Citrix Audio Virtual Channel porque se ha diseñado específicamente para el transporte de audio.
- **Redirección de USB genérico**. Admite dispositivos de audio que tienen botones y/o pantalla o es un dispositivo de interfaz humana (HID) si el dispositivo del usuario se encuentra en una LAN (o una conexión de este tipo) al servidor de Citrix Virtual Apps and Desktops.

#### *Citrix Audio Virtual Channel*

Citrix Audio Virtual Channel (CTXCAM) bidireccional permite la entrega de audio de forma eficiente en la red. HDX RealTime genérico toma el audio desde los auriculares o el micrófono del usuario y

lo comprime. Luego, lo envía por ICA a la aplicación softphone presente en el escritorio virtual. Del mismo modo, el audio resultante de la aplicación softphone se comprime y se envía en la dirección opuesta, hacia los auriculares o los altavoces del usuario. Esta compresión no depende de la compresión utilizada por el sistema softphone en sí (por ejemplo, G.729 o G.711). Se lleva a cabo mediante el códec optimizado para voz (calidad media). Sus funciones son ideales para VoIP. Presenta un tiempo muy pequeño de codificación y consume aproximadamente solo 56 Kilobits por segundo del ancho de banda de red (28 Kbps en cada dirección) en las horas punta. Este códec debe seleccionarse explícitamente en la consola Administrar del servicio porque no es el códec predeterminado de sonido. La opción predeterminada es el códec de audio HD (calidad alta). Ese códec es ideal para melodías en estéreo de alta fidelidad, pero es más lento para codificar en comparación con el códec optimizado para voz.

***Redirección de USB genérico***

La tecnología de redirección de USB genérico de Citrix (canal virtual CTXGUSB) ofrece un medio genérico para comunicar dispositivos USB remotos, incluidos los dispositivos compuestos (audio más HID) y los dispositivos USB isócronos. Este enfoque está limitado a los usuarios conectados por LAN. Ya que el protocolo USB tiende a ser sensible a la latencia de red y requiere un ancho de banda considerable. La redirección de USB isócrono funciona bien cuando se usan determinadas aplicaciones softphone. Esta redirección ofrece una calidad de voz excelente y una latencia baja. Sin embargo, se prefiere Citrix Audio Virtual Channel porque está optimizado para el tráfico de audio. La excepción principal es cuando se usa un dispositivo de audio con botones. Por ejemplo, un teléfono USB conectado al dispositivo de usuario que está conectado a su vez a la central de datos por LAN. En este caso, la redirección de USB genérico admite botones en el teléfono o en los auriculares, utilizados para controlar las funciones por el envío de señales a la aplicación softphone. Este no es un problema con los botones que funcionan de forma local en el dispositivo.

### Limitación

Después de instalar un dispositivo de audio en el cliente, habilitar la redirección de audio e iniciar una sesión RDS, es posible que los archivos de audio no se reproduzcan. Como solución alternativa, agregue la clave al Registro en la máquina RDS y reiníciela. Para obtener información, consulte Limitación de audio en la lista de funciones administradas a través del Registro.

## Redirección de contenido de explorador web

June 24, 2022

Redirigir el contenido del explorador web impide que las páginas web incluidas en la lista de permitidos se generen en el lado del agente VDA. Esta función utiliza la aplicación Citrix Workspace para

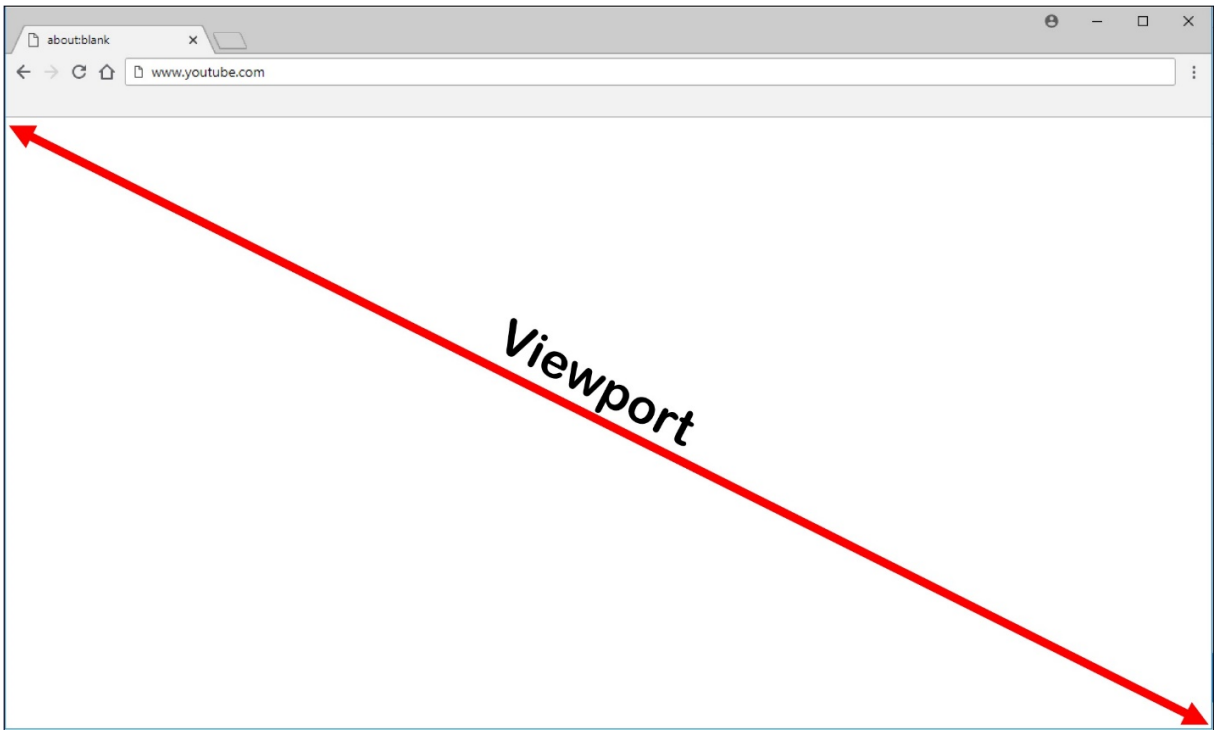
 

crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

> **Nota:**
>
> Puede especificar que las páginas web se redirijan al lado del VDA (no al lado del cliente) mediante una lista de bloqueados.

Este motor web de distribución superpuesta se ejecuta en el dispositivo de punto final, en lugar de ejecutarse en el VDA, y utiliza la CPU, la GPU, la memoria RAM y la red del dispositivo de punto final.

Solo se redirige la ventanilla del explorador web. La ventanilla es el área rectangular del explorador web donde aparece el contenido. La ventanilla no incluye elementos como la barra de direcciones, la barra de favoritos ni la barra de estado. Esos elementos están en la interfaz de usuario, que todavía se ejecutan en el explorador en el VDA.




1. Configure una directiva de la interfaz de Administrar > Configuración completa que especifique la lista de control de acceso que contenga las URL para la redirección desde las listas de URL permitidas o bloqueadas. Para que el explorador web presente en el VDA detecte que la URL a la que se dirige el usuario está incluida en la lista de permitidos o en la lista de bloqueados la extensión del explorador web busca la URL en esas listas. La extensión del explorador web (BHO) para Internet Explorer 11 está incluida en los medios de instalación y se instala automáticamente. Para Chrome, la extensión del explorador está disponible en Chrome Web Store y puede implementarla mediante las directivas de grupo y los archivos ADMX. Las extensiones de

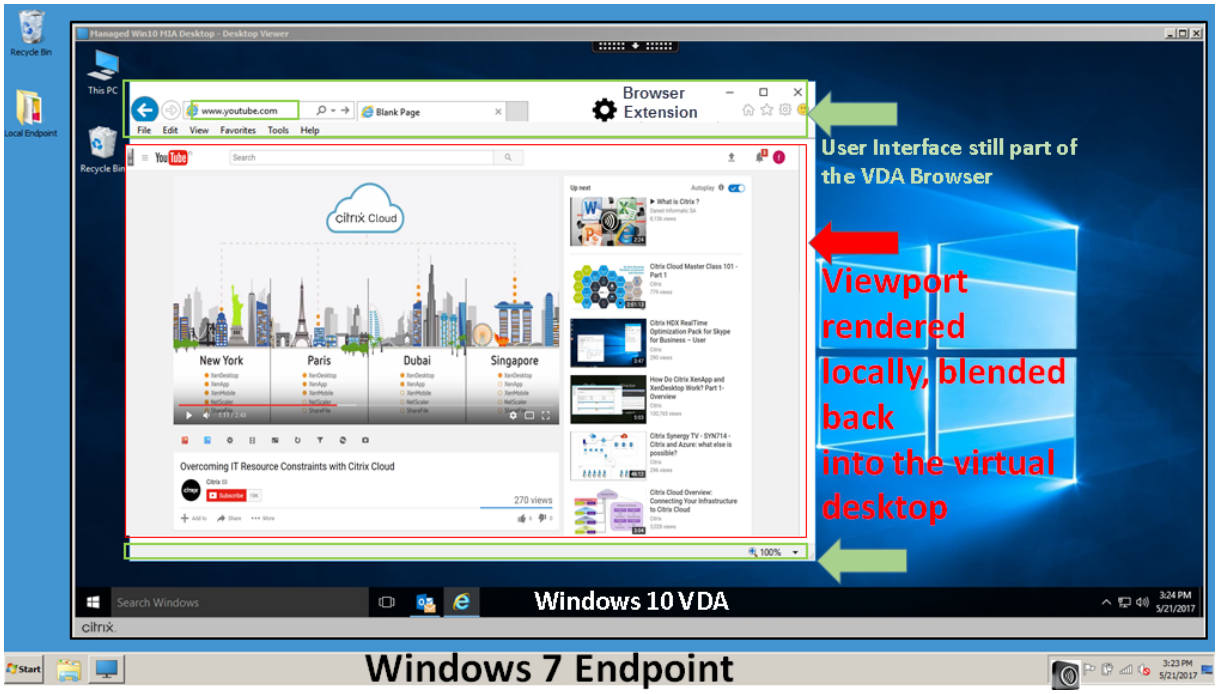
Chrome se instalan basándose en el usuario. No es necesario actualizar una imagen maestra para agregar o eliminar una extensión.

2. Si se encuentra una coincidencia en la lista de permitidos (por ejemplo, `https://www.mycompany.com/`) y no hay ninguna coincidencia en la lista de bloqueados (por ejemplo, `https://www.mycompany.com/engineering`), un canal virtual (CTXCSB) indica a la aplicación Citrix Workspace que se necesita una redirección y transmite la URL. La aplicación Citrix Workspace crea una instancia de motor de generación local y muestra el sitio web.
3. La aplicación Citrix Workspace introduce el sitio web en el área de contenido del explorador web que tenga el escritorio virtual.

El color del logotipo especifica el estado de la extensión de Chrome. Es uno de estos tres colores:

- Verde: Activo y conectado.
- Gris: No activo/inactivo en la ficha actual.
- Rojo: No funciona.

Puede depurar el registro mediante **Opciones**, en el menú de extensiones.




La aplicación Citrix Workspace obtiene el contenido de estas maneras:

- **Obtención en el servidor y generación en el servidor:** No hay redirección porque el sitio no consta en la lista de permitidos o la redirección ha fallado. Se recurre a la generación de la página web en el VDA y se usa Thinwire para generar remotamente los gráficos. Se usan directivas para controlar el comportamiento cuando se recurre al mecanismo alternativo. Alto consumo de CPU, memoria RAM y ancho de banda en el VDA.

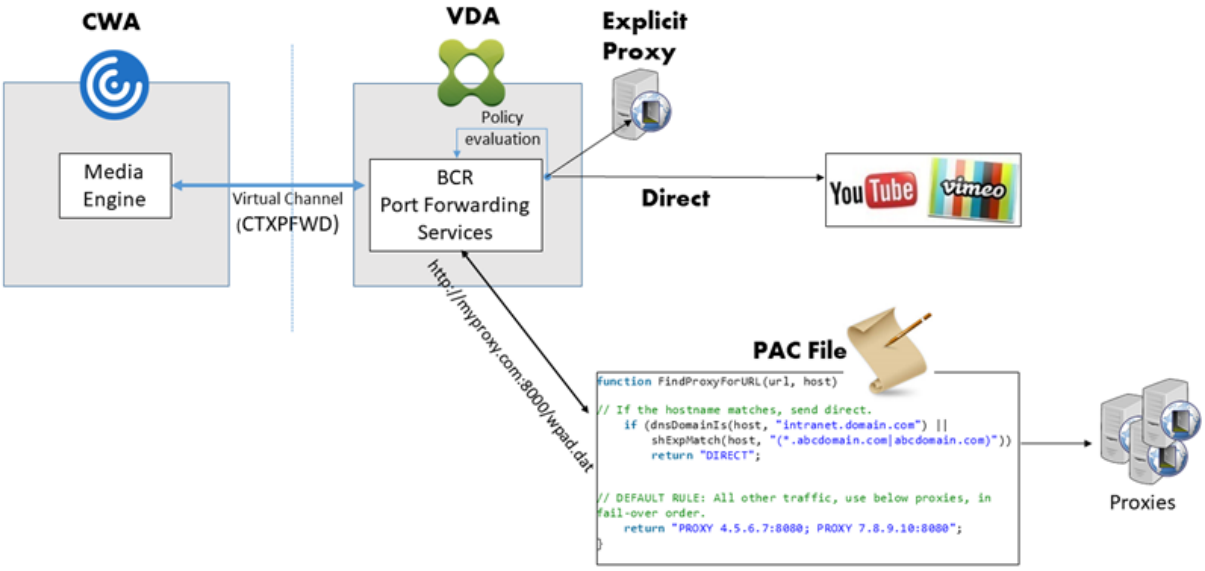
 

- **Obtención en el servidor y generación en el cliente:** La aplicación Citrix Workspace se comunica con el servidor web y obtiene el contenido desde este a través del VDA mediante un canal virtual (CTXPFWD). Esta opción es útil cuando el cliente no tiene acceso a Internet (por ejemplo, clientes ligeros). Bajo consumo de CPU y RAM en el VDA, pero se consume ancho de banda para el canal virtual ICA.

  Hay tres modos de funcionamiento para este caso. El término proxy hace referencia a un dispositivo proxy al que accede el VDA para obtener acceso a Internet.

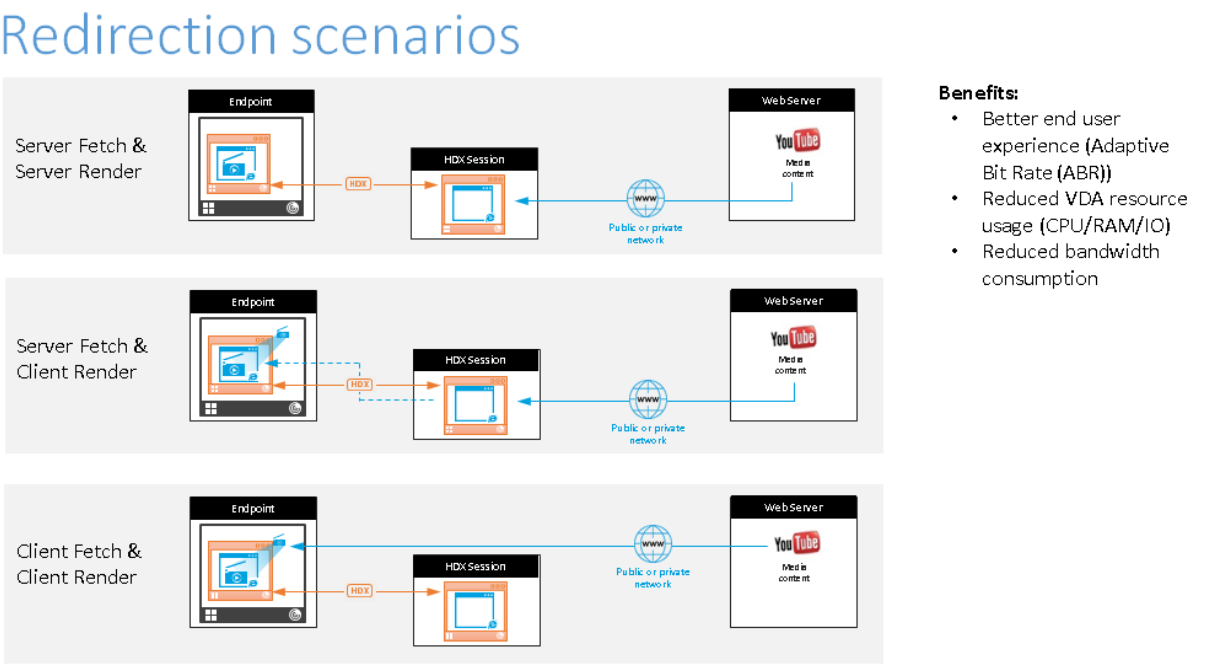
  Qué opción de directiva elegir:

  - Proxy explícito: Si tiene un solo proxy explícito en su centro de datos.
  - Directo o transparente: Si no tiene proxies o si utiliza proxies transparentes.
  - Archivos PAC: Si confía en archivos PAC, los exploradores del VDA pueden elegir automáticamente el servidor proxy apropiado para obtener la URL especificada.




- **Obtención en el cliente y generación en el cliente:** Como la aplicación Citrix Workspace se comunica directamente con el servidor web, requiere acceso a Internet. En este caso, no se consume la red, la CPU ni la memoria RAM del sitio de XenApp y XenDesktop.




**Mecanismo alternativo:**

La redirección de cliente puede fallar a veces. Por ejemplo, si la máquina cliente no tiene acceso directo a Internet, el VDA puede recibir una respuesta de error. En tales casos, el explorador presente en el VDA puede volver a cargar la página web y generarla en el servidor.

Puede impedir la generación de elementos de vídeo en el lado del servidor mediante la directiva existente **Prevención de reserva de Windows Media**. Establezca esta directiva en **Reproducir todo el contenido solo en el cliente** o **Reproducir solo el contenido accesible por el cliente en el cliente**. Estas configuraciones bloquean la reproducción de elementos de vídeo en el servidor si hay fallos en la redirección de cliente. Esta directiva tiene efecto solo cuando la redirección de contenido del explorador web está habilitada y la directiva **Lista de control de acceso** contiene la URL alternativa. La dirección URL no puede estar en la directiva de lista de bloqueados.

**Requisitos del sistema:**

Dispositivos de punto final de Windows:

- Windows 10 u 11
- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores

> **Nota:**
>
> La redirección de contenido del explorador solo se admite en la versión Current Release de la aplicación Citrix Workspace para Windows, pero no en las versiones LTSR de la aplicación Citrix Workspace, 1912 y 2203.1.

Dispositivos de punto final de Linux:

- Aplicación Citrix Workspace 1808 para Linux o versiones posteriores
- Citrix Receiver para Linux 13.9 o versiones posteriores
- Los terminales de clientes ligeros deben incluir WebKitGTK+

Citrix Virtual Apps and Desktops 7 1808; XenApp y XenDesktop 7.15 CU5, 7.18, 7.17, 7.16:

- Sistema operativo del VDA: Windows 10 (versión mínima 1607), Windows Server 2012 R2, Windows Server 2016
- Explorador en el VDA:
  - Google Chrome v66 o versiones posteriores (Chrome requiere la aplicación Citrix Workspace 1809 para Windows en el dispositivo de punto final del usuario, Citrix Virtual Apps and Desktops 7 1808 VDA y la extensión de redirección de contenido de explorador)
  - Internet Explorer 11 con estas opciones configuradas:
    * Desmarque **Modo protegido mejorado** en: **Opciones de Internet** > **Avanzado > Seguridad**.
    * Marque **Habilitar extensiones de explorador de terceros** en: **Opciones de Internet > Avanzado > Exploración**

## Solución de problemas

Para obtener información sobre la solución de problemas, consulte el artículo de Knowledge Center https://support.citrix.com/article/CTX230052

## Extensión de Chrome de redirección de contenido de explorador web

Para usar la redirección de contenido de explorador con Chrome, agregue la extensión de redirección de contenido de explorador desde Chrome Web Store. Haga clic en **Agregar a Chrome** en el entorno de Citrix Virtual Apps and Desktops.

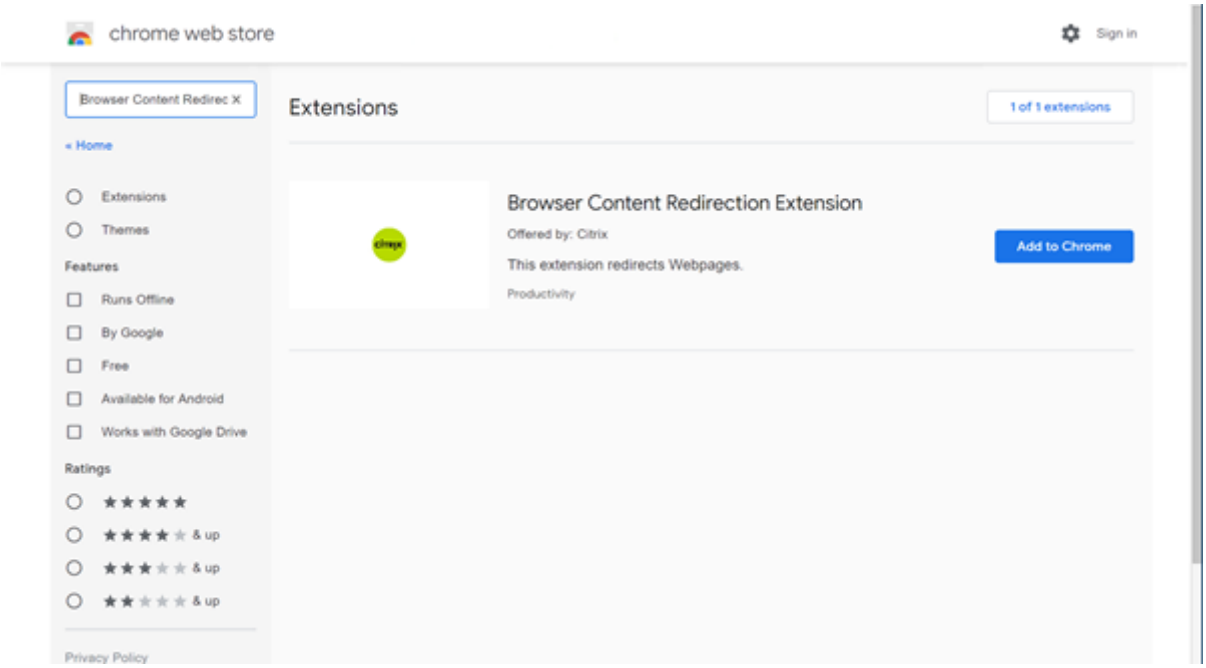
La extensión **no** se requiere en la máquina cliente del usuario, solo en el VDA.

### Requisitos del sistema

- Chrome v66 o versiones posteriores
- Extensión de redirección de contenido de explorador web
- Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores
- Aplicación Citrix Workspace para Windows 1809 o versiones posteriores

> **Nota:**
>
> La redirección de contenido del explorador solo se admite en la versión Current Release de la aplicación Citrix Workspace para Windows, pero no en las versiones LTSR de la aplicación Citrix Workspace, 1912 y 2203.1.

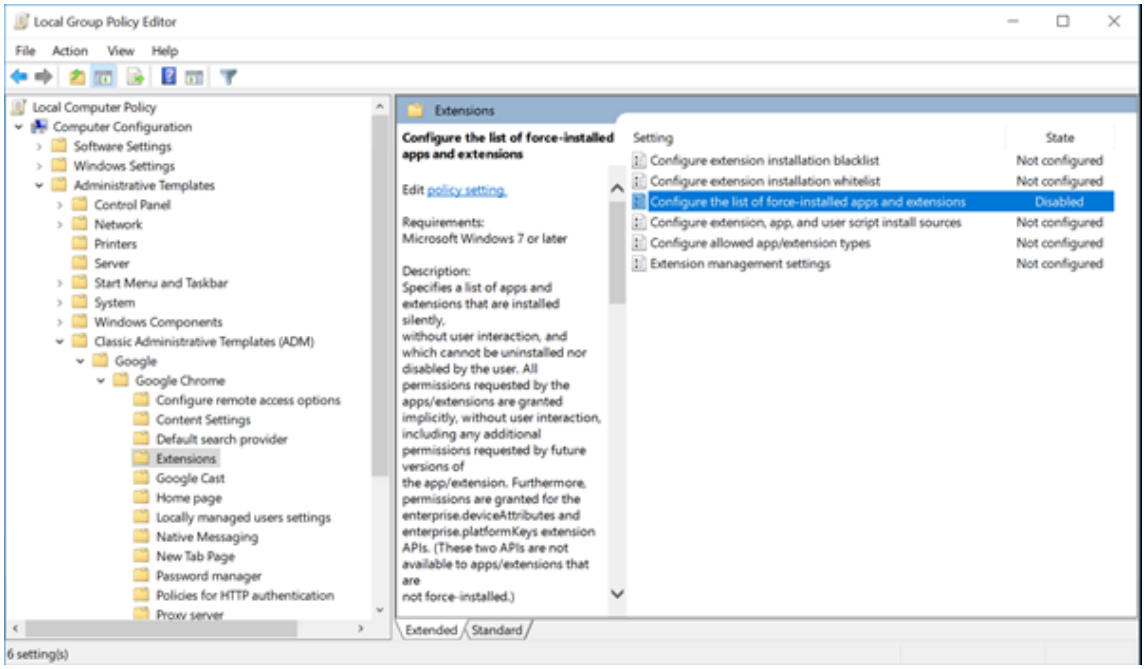



Este método funciona para usuarios individuales. Para implementar la extensión a un gran grupo de usuarios en su organización, implemente la extensión mediante la directiva de grupo.

**Implementar la extensión mediante la directiva de grupo**

1. Importe los archivos ADMX de Google Chrome a su entorno. Para obtener información sobre cómo descargar plantillas de directivas, e instalar y configurar las plantillas en su editor de directivas de grupo, consulte Definir políticas del explorador Chrome en equipos gestionados.
2. Abra su Consola de administración de directivas de grupo y vaya a **Configuración de usuario\Plantillas administrativas\Plantillas administrativas clásicas (ADM)\Google\Google Chrome\Extensiones**. Habilite el parámetro **Configurar la lista de aplicaciones y extensiones con instalación forzada**.

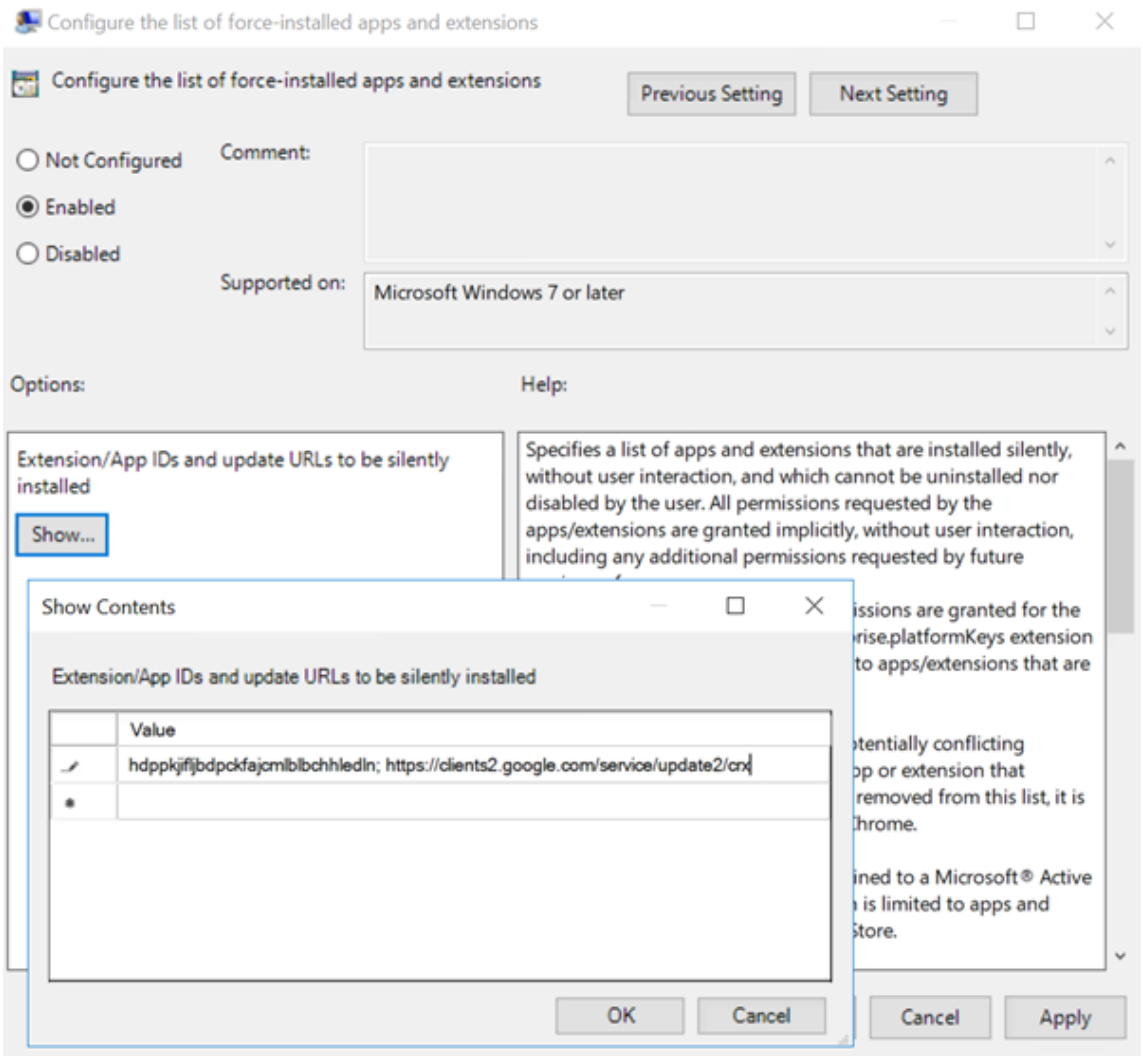
 




3. Haga clic en **Mostrar** y escriba la siguiente cadena, que corresponde a la ID de extensión. Actualice la URL de la extensión de redirección de contenido de explorador web.

   ```
   hdppkjifljbdpckfajcmlblbchhledln; https://clients2.google.com/service/update2/crx
   ```




4. Aplique el parámetro y después de actualizar **gpupdate**, el usuario recibe automáticamente la extensión. Si inicia el explorador Chrome en la sesión del usuario, la extensión ya está aplicada y no pueden quitarla.

   Todas las actualizaciones de la extensión se instalan automáticamente en las máquinas de los usuarios a través de la URL de actualización que especificó en la configuración.

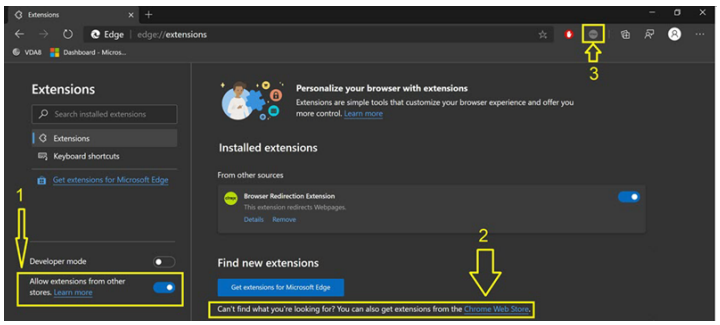
   Si el parámetro **Configurar la lista de aplicaciones y extensiones con instalación forzada** se establece en **Inhabilitado**, la extensión se elimina automáticamente de Chrome para todos los usuarios.

### Extensión de Edge Chromium de redirección de contenido de explorador web

Para instalar la extensión de redirección de contenido de explorador web en Edge, compruebe que tiene instalada la versión **83.0.478.37** o una posterior del explorador Edge.

1. Haga clic en la opción **Extensiones** del menú y active **Permitir extensiones de otras tiendas**.
2. Haga clic en el enlace **Chrome Web Store** y la extensión aparecerá en la barra de la parte superior derecha.
   Para obtener más información sobre las extensiones de Microsoft Edge, consulte Extensions.




## PPP y redirección de contenido del explorador

Cuando se utiliza la redirección de contenido del explorador con los PPP (escalado) establecidos por encima del 100% en el equipo del usuario, la pantalla de contenido del explorador redirigido se muestra incorrectamente. Para evitar este problema, no establezca los PPP cuando utilice la redirección de contenido del explorador. Otra forma de evitar el problema es inhabilitar la aceleración de la GPU en la redirección del contenido del explorador para Chrome. Para ello, cree la clave de Registro en la máquina del usuario. Para obtener información, consulte PPP y redirección de contenido del explorador en la lista de funciones administradas a través del Registro.

## Encabezado de solicitud user-agent

El encabezado user-agent ayuda a identificar las solicitudes HTTP enviadas desde la redirección de contenido del explorador web. Este parámetro puede ser útil al configurar reglas de proxy y firewall. Por ejemplo, si el servidor bloquea las solicitudes enviadas desde la redirección de contenido del explorador web, puede crear una regla que contenga el encabezado user-agent para omitir ciertos requisitos.

Solo los dispositivos con Windows admiten el encabezado de solicitud user-agent.

De forma predeterminada, la cadena del encabezado de solicitud user-agent está inhabilitada. Para habilitar el encabezado user-agent para el contenido generado en el cliente, utilice el Editor del Registro. Para obtener información, consulte Encabezado de solicitud user-agent en la lista de funciones administradas a través del Registro.

# Conferencias de vídeo de HDX y compresión de vídeo para cámaras web de HDX

April 14, 2022

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

Las aplicaciones que se ejecutan en la sesión virtual pueden utilizar cámaras web. Para ello, se debe definir la compresión de vídeo de cámaras web de HDX o la redirección de USB genérico Plug-n-Play de HDX. Para cambiar de modo, vaya a la **aplicación Citrix Workspace > Preferencias > Dispositivos**. Citrix recomienda que siempre use la compresión de vídeo de cámaras web de HDX si es posible. La redirección de USB genérico de HDX solo se recomienda cuando hay problemas de compatibilidad de las aplicaciones con compresión de vídeo de HDX o cuando se requieren funcionalidades nativas avanzadas de la cámara web. Para obtener un mejor rendimiento, Citrix recomienda que Virtual Delivery Agent tenga al menos dos CPU virtuales.

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

## Compresión de vídeo de cámaras web de HDX

La compresión de vídeo de cámaras web de HDX también se llama modo de cámara web **optimizado**. Este tipo de compresión de vídeo por cámara web envía el vídeo en H.264 directamente a la aplicación de videoconferencias de la sesión virtual. Para optimizar los recursos de los VDA, la compresión de cámaras web de HDX no codifica, transcodifica ni decodifica el vídeo de las cámaras web. Esta función está habilitada de manera predeterminada.

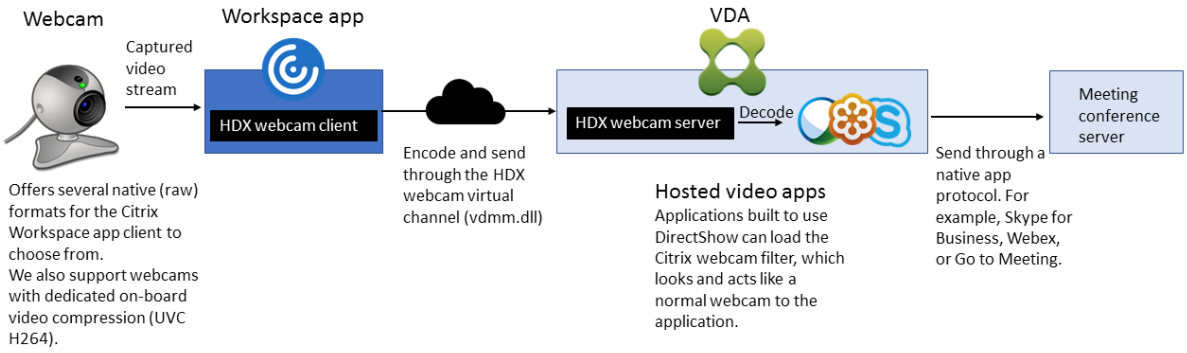
Para inhabilitar el streaming directo de vídeo del servidor a la aplicación de videoconferencias, establezca la clave de Registro en 0 en el VDA. Para obtener información, consulte Compresión de vídeo de cámara web en la lista de funciones administradas a través del Registro.

Si inhabilita la funcionalidad predeterminada para los recursos de streaming de vídeo, la compresión de vídeo de cámaras web de HDX utiliza la tecnología marco multimedia que forma parte del sistema

operativo cliente para interceptar vídeo de dispositivos de captura, transcodificarlo y comprimirlo. Los fabricantes de los dispositivos de captura suministran controladores que complementan la arquitectura de streaming del kernel del sistema operativo.

El cliente gestiona la comunicación con la cámara web. El cliente envía el vídeo solo al servidor que puede mostrarlo correctamente. El servidor no trata directamente con la cámara web, pero su integración le ofrece la misma experiencia en el escritorio que un tratamiento directo. La aplicación Workspace comprime el vídeo para ahorrar ancho de banda y proporcionar una mejor capacidad de recuperación en conexiones WAN.




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

- Conferencia multimedia
- Redirección de Windows Media

Si una cámara web es compatible con la codificación por hardware, la compresión de vídeo de HDX utiliza la codificación por hardware de manera predeterminada. La codificación por hardware puede consumir más ancho de banda que la codificación por software. Para forzar la compresión de software, modifique la clave de Registro en el cliente. Para obtener información, consulte Compresión de software de cámara web en la lista de funciones administradas a través del Registro.

#### Requisitos para la compresión de vídeo de cámaras web de HDX

La compresión de vídeo de cámaras web de HDX admite las siguientes versiones de la aplicación Citrix Workspace:

| Platform | Procesador |
| --- | --- |
| Aplicación Citrix Workspace para Windows | La aplicación Citrix Workspace para Windows admite la compresión de vídeo de cámara web para aplicaciones de 32 y 64 bits en XenApp y XenDesktop 7.17 y versiones posteriores. En versiones anteriores, la aplicación Citrix Workspace para Windows solo es compatible con aplicaciones de 32 bits. |
| Aplicación Citrix Workspace para Mac | La aplicación Citrix Workspace para Mac 2006 o versiones posteriores admite la compresión de vídeo de cámara web para aplicaciones de 64 bits en XenApp y XenDesktop 7.17 y versiones posteriores. En versiones anteriores, la aplicación Citrix Workspace para Mac solo es compatible con aplicaciones de 32 bits. |
| Aplicación Citrix Workspace para Linux | La aplicación Citrix Workspace para Linux solo admite aplicaciones de 32 bits en el escritorio virtual. |
| Aplicación Citrix Workspace para Chrome | Debido a que algunos dispositivos Chromebook ARM no son compatibles con la codificación H.264, solo las aplicaciones de 32 bits pueden utilizar la compresión de vídeo de cámaras web de HDX optimizada. |

Las aplicaciones de vídeo basadas en Media Foundation admiten la compresión de vídeo de cámaras web de HDX en Windows 8.x o posterior, Windows Server 2012 R2 y versiones posteriores. Para obtener más información, consulte el artículo CTX132764 de Knowledge Center.

Otros requisitos del dispositivo de usuario:

- Hardware adecuado para reproducir sonido.
- Cámara web compatible con DirectShow (use la configuración predeterminada de la cámara web). Las cámaras web que pueden codificar por hardware reducen el uso de la CPU en el lado del cliente.
- Para la compresión de vídeo de cámaras web de HDX, instale los controladores de cámara web en el cliente, obtenidos del fabricante de la cámara, si es posible. No es necesario instalar los controladores del dispositivo en el servidor.

Las distintas cámaras web ofrecen diferentes velocidades de fotogramas y tienen diferentes niveles de brillo y contraste. Ajustar el contraste de la cámara web puede reducir considerablemente el tráfico

ascendente. Citrix utiliza las siguientes cámaras web para la validación inicial de funciones:

- Modelos de Microsoft LifeCam VX (2000, 3000, 5000, 7000)
- Creative Live! Cam Optia Pro
- Logitech QuickCam Messenger
- Logitech C600, C920
- HP Deluxe Webcam

Para ajustar la velocidad de fotogramas de vídeo preferida, modifique la clave de Registro en el cliente: Para obtener información, consulte Velocidad de fotogramas en compresión de vídeo por cámara web en la lista de funciones administradas a través del Registro.

### Streaming por cámara web de alta definición

La aplicación de videoconferencias presente en el servidor selecciona el formato de cámara web y la resolución en función de los tipos de formato compatibles. Cuando se inicia una sesión, el cliente envía la información de la cámara web al servidor. Usted elige la cámara web desde la aplicación. Si la cámara web y la aplicación de videoconferencias admiten la generación de alta definición, la aplicación usa la resolución de alta definición. Admitimos resoluciones de cámara web hasta 1920 x 1080.

Esta función requiere la aplicación Citrix Workspace para Windows (versión mínima 1808) o Citrix Receiver para Windows (versión mínima 4.10).

Puede usar una clave de Registro para inhabilitar y habilitar la función. Para obtener más información, consulte Streaming por cámara web de alta definición en la lista de funciones administradas a través del Registro.

Si hay algún error en la negociación del tipo de medio, HDX vuelve a la resolución CIF predeterminada de 352x288. Puede usar claves de Registro en el cliente para configurar la resolución predeterminada. Compruebe que la cámara admite la resolución especificada. Para obtener más información, consulte Resolución de cámara web de alta definición en la lista de funciones administradas a través del Registro.

La compresión de vídeo de cámaras web de HDX utiliza considerablemente menos ancho de banda en comparación con la redirección de USB genérico Plug-n-Play y funciona bien en conexiones WAN. Para ajustar el ancho de banda, establezca la clave de Registro en el cliente. Para obtener más información, consulte Ancho de banda de cámara web de alta definición en la lista de funciones administradas a través del Registro.

Introduzca un valor en bits por segundo. Si no especifica el ancho de banda, las aplicaciones de videoconferencias utilizan 350 000 bps de forma predeterminada.

### Redirección de USB genérico Plug-n-Play de HDX

La redirección de USB genérico Plug-n-Play de HDX (isócrona) también se denomina modo de cámara web **genérico**. La ventaja de la redirección de USB genérico Plug-n-Play de HDX es que no es necesario instalar controladores en el cliente ligero o el dispositivo de punto final. La pila USB está virtualizada, de modo que todo lo que conecte al cliente local se envía a la máquina virtual remota. El escritorio remoto actúa como si lo hubiera conectado al entorno nativo. El escritorio Windows se ocupa de toda la interacción con el hardware, y se ejecuta siguiendo la lógica Plug-n-Play para buscar los controladores correctos. La mayoría de las cámaras web funcionan si los controladores existen en el servidor y pueden funcionar sobre ICA. El modo genérico de cámara web consume mucho más ancho de banda (muchos megabits por segundo) porque se envían vídeos sin comprimir con el protocolo USB a través de la red.

## Redirección multimedia HTML5

June 12, 2024

La redirección multimedia HTML5 amplía las funciones de redirección multimedia de HDX MediaStream para incluir audio y vídeo de HTML5. Debido al aumento de la distribución en línea de contenido multimedia, sobre todo para dispositivos móviles, la industria de exploración ha desarrollado métodos más eficientes para presentar audio y vídeo.

Flash ha sido el estándar, pero requiere un complemento, no funciona en todos los dispositivos y resulta en un mayor uso de batería en los dispositivos móviles. Empresas como YouTube o Netflix, y versiones más recientes de los exploradores de Mozilla, Google y Microsoft están migrando a HTML5, con lo que HTML5 se convierte en el nuevo estándar.

El contenido multimedia basado en HTML5 presenta muchas ventajas frente los plug-ins propietario, incluidos:

- Estándares independientes de empresas (W3C)
- Flujo de trabajo simplificado para la administración de los derechos digitales (DRM)
- Mejor rendimiento sin los problemas de seguridad que implican los complementos

### Descargas progresivas HTTP

La descarga progresiva HTTP es un método de semidistribución por streaming basado en HTTP que admite HTML5. En una descarga progresiva, el explorador web reproduce un solo archivo (codificado con una sola calidad) mientras ese archivo se descarga desde un servidor web HTTP. El vídeo se al-

macena en el disco tal cual se recibe, y se reproduce desde ese disco. Si vuelve a reproducir el vídeo, el explorador web puede cargar el vídeo desde la memoria caché.

Para ver un ejemplo de descarga progresiva, consulte la página para pruebas de redirección de vídeo HTML5. Utilice las herramientas de desarrollo que facilita su explorador web para inspeccionar los elementos de vídeo en la página web y buscar los orígenes (un formato de contenedor mp4) en la etiqueta de vídeos HTML5:

### Comparación entre HTML5 y Flash

| Función | HTML5 | Flash |
|---|---|---|
| Requiere un reproductor propietario | No | Sí |
| Se ejecuta en dispositivos móviles | Sí | Algunos |
| Velocidad de ejecución en distintas plataformas | Alto | Lento |
| Compatible con iOS | Sí | No |
| Consumo de recursos | Menos | Más |
| Carga más rápida | Sí | No |

### Requisitos

Solo se admite la redirección para las descargas progresivas en formato mp4. No se admiten tecnologías de streaming WebM y Adaptive bitrate, como DASH/HLS.

Se admite lo siguiente, y se utilizan directivas para controlarlo. Para obtener más información, consulte Configuraciones de directiva Multimedia.

- Generación en el lado del servidor
- Obtención en servidor, generación en cliente
- Obtención y generación en el lado del cliente

Versiones mínimas de la aplicación Citrix Workspace y Citrix Receiver:

- Aplicación Citrix Workspace para Windows 1808
- Citrix Receiver para Windows 4.5
- Aplicación Citrix Workspace 1808 para Linux
- Citrix Receiver para Linux 13.5

| Versión mínima del explorador web en el VDA | SO Windows versión/compilación/SP |
|---|---|
| Internet Explorer 11.0 | Windows 10 x86 (1607 RS1) y x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Firefox 47 Debe agregar manualmente los certificados al almacén de certificados de Firefox o configurar Firefox para buscar certificados provenientes de un almacén de certificados de confianza de Windows. Para obtener más información, consulte https://wiki.mozilla.org/CA:AddRootToFirefox | Windows 10 x86 (1607 RS1) y x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |
| Chrome 51 | Windows 10 x86 (1607 RS1) y x64 (1607 RS1); Windows Server 2016 RTM 14393 (1607); Windows Server 2012 R2 |

### Componentes de la solución de redirección de vídeo HTML5

- **HdxVideo.js:** Enlace de JavaScript que intercepta los comandos vídeo en el sitio web. HdxVideo.js se comunica con WebSocketService mediante Secure WebSockets (SSL/TLS).
- **Certificados SSL de WebSocket**
  - Para la CA (raíz): **Citrix XenApp/XenDesktop HDX In-Product CA** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX In-Product CA)
    Ubicación: Certificados (Equipo local) > Entidades de certificación raíz de confianza > Certificados.
  - Para la entidad final (hoja): **Citrix XenApp/XenDesktop HDX Service** (C = US; S = Florida; L = Fort Lauderdale; O = Citrix Systems, Inc.; OU = XenApp/XenDesktop Engineering; CN = Citrix XenApp/XenDesktop HDX Service)
    Ubicación: Certificados (Equipo local) > Personal > Certificados.
- **WebSocketService.exe:** Se ejecuta en el sistema local y realiza la terminación SSL y la asignación de sesiones de usuario. TLS Secure WebSocket escucha en 127.0.0.1 en el puerto 9001.
- **WebSocketAgent.exe:** Se ejecuta en la sesión del usuario y genera el vídeo según las instrucciones de los comandos de WebSocketService.

### Cómo habilito la redirección de vídeo HTML5

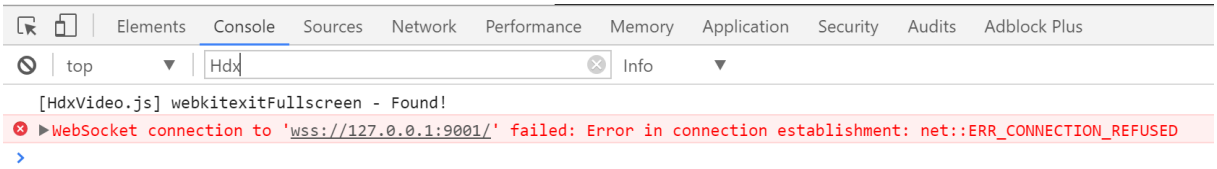
En esta versión, esta funcionalidad está disponible solo para las páginas web controladas. Requiere que se agregue HdxVideo.js de JavaScript (incluido en los medios de instalación de Citrix Virtual Apps and Desktops) a las páginas web donde está disponible el contenido multimedia HTML5. Por ejemplo: vídeos en un sitio de formación interna.

Los sitios como youtube.com, que están basados en tecnologías de velocidad de bits adaptable, como HTTP Live Streaming (HLS) y Dynamic Adaptive Streaming over HTTP (DASH), no se admiten.

Para obtener más información, consulte *Configuraciones de directiva Multimedia*.

### Sugerencias para solucionar problemas

Pueden producirse errores cuando la página web intenta ejecutar HdxVideo.js. Si JavaScript no se puede cargar, se produce un error en el mecanismo de redirección de HTML5. Debe comprobar que no hay errores relacionados con HdxVideo.js. Para ello, examine la consola en las ventanas de herramientas de desarrolladores del explorador web. Por ejemplo:




## Optimización para Microsoft Teams

June 12, 2024

> **Nota:**
>
> El nuevo Microsoft Teams 2.1 ya está disponible de forma generalizada para VDA. Esta versión de Microsoft Teams es compatible con la Optimización para Microsoft Teams de Citrix mediante WebRTC (VDI 1.0).
>
> Si está usando Citrix Virtual Apps and Desktops 2402, no es necesario configurar manualmente la entrada `msedgewebview2.exe` del Registro, ya que aparece en la lista blanca de forma predeterminada.
>
> Las aplicaciones publicadas ahora son compatibles con el nuevo Microsoft Teams.
>
> Si utiliza Citrix Virtual Apps and Desktops 2311 o una versión anterior, se requiere un nuevo parámetro de configuración del Registro en el VDA para permitir que las nuevas instancias de

> Microsoft Teams accedan al canal virtual de Citrix. Para habilitar la optimización para Microsoft Teams 2.1, configure la siguiente clave de Registro en el VDA:
>
> **Ubicación**: `HKLM\SOFTWARE\WOW6432Node\Citrix\WebSocketService`
>
> **Clave** (REG_Multi_SZ): `ProcessWhitelist`
>
> **Valor**: `msedgewebview2.exe`
>
> Para obtener más información, consulte la documentación de Microsoft.

Citrix ofrece la optimización para Microsoft Teams de escritorio mediante Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace. De forma predeterminada, agrupamos todos los componentes necesarios en la aplicación Citrix Workspace y en Virtual Delivery Agent (VDA).

Nuestra optimización para Microsoft Teams incluye una API y servicios de HDX del lado de VDA para interactuar con la aplicación alojada Teams y recibir comandos. Estos componentes abren un canal virtual de control (CTXMTOP) en el motor de medios de la aplicación Citrix Workspace. El dispositivo de punto final descodifica y proporciona el contenido multimedia de manera local, y devuelve la ventana de la aplicación Citrix Workspace a la aplicación Microsoft Teams alojada.

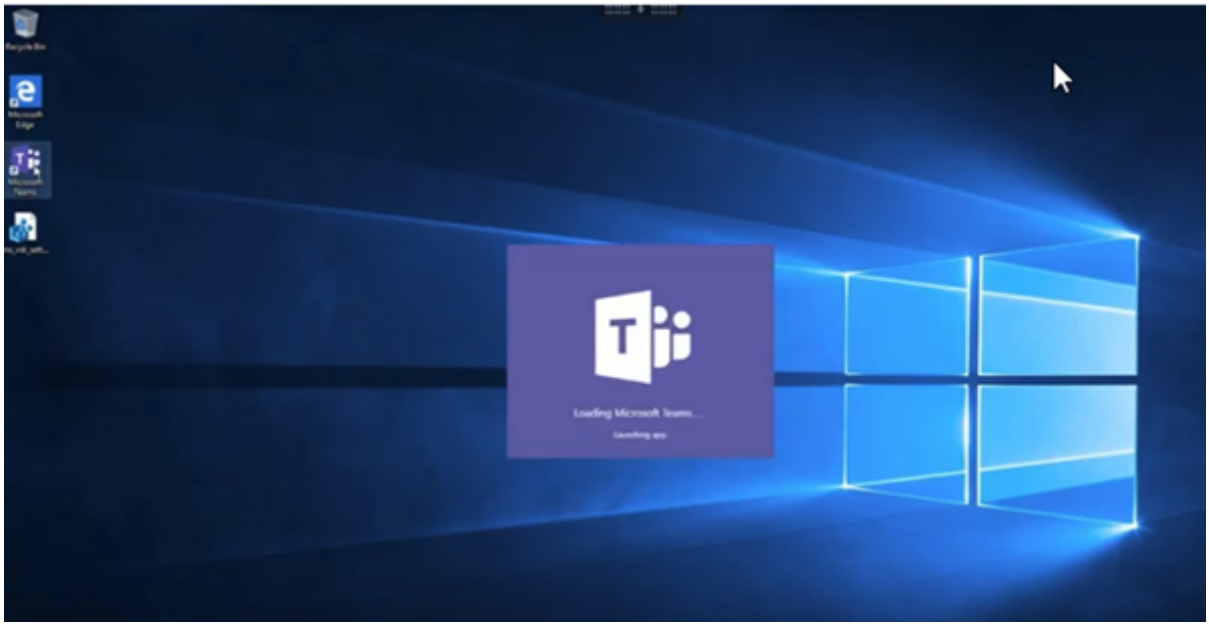
La autenticación y la señalización se producen de forma nativa en la aplicación alojada de Microsoft Teams, al igual que los demás servicios de Microsoft Teams (por ejemplo, el chat o la colaboración). La redirección de audio/vídeo no les afecta.

`CTXMTOP` es un canal virtual de comando y control. Esto significa que los medios no se intercambian entre la aplicación Citrix Workspace y el VDA.

Solo la obtención del cliente/generación del cliente está disponible.

Este vídeo de demostración le da una idea de cómo funciona Microsoft Teams en un entorno virtual Citrix.



### Instalación de Microsoft Teams

Citrix y Microsoft recomiendan la última versión disponible de Microsoft Teams y mantenerla actualizada.
No se admiten las versiones de la aplicación de escritorio de Microsoft Teams con fechas de publicación que son más de 90 días anteriores a la fecha de publicación de la versión actual.
Las versiones no compatibles de la aplicación de escritorio de Microsoft Teams muestran una página de bloqueo a los usuarios y solicitan actualizar la aplicación.

Para obtener información sobre las últimas versiones disponibles, consulte Update history for Teams App (Desktop and Mac).

Le recomendamos que siga las directrices de instalación para toda la máquina de Microsoft Teams. Además, no utilice el instalador EXE que instala Microsoft Teams en `AppData`. En su lugar, instálelo en `C:\Program Files (x86)\Microsoft\Teams` con el indicador `ALLUSER=1` desde la línea de comandos.

```
msiexec /i <path_to_msi> /l*v <install_logfile_name> ALLUSER=1
ALLUSERS=1
```

En este ejemplo también se usa el parámetro `ALLUSERS=1`. Al establecer este parámetro, el instalador de Microsoft Teams a nivel de equipo aparece en **Programas y funciones**, en el **Panel de control**. También en **Aplicaciones y funciones**, en Configuración de Windows, para todos los usuarios del equipo. Todos los usuarios pueden desinstalar Microsoft Teams si tienen credenciales de administrador.

Es importante entender la diferencia entre `ALLUSERS=1` y `ALLUSER=1`. Puede utilizar el parámetro

ALLUSERS=1 en entornos VDI y no VDI. Utilice el parámetro ALLUSER=1 solo en entornos VDI para especificar una instalación por máquina.

En el modo ALLUSER=1, la aplicación Microsoft Teams no se actualiza automáticamente cuando hay una nueva versión. Recomendamos este modo para entornos no persistentes, como aplicaciones o escritorios compartidos alojados fuera de catálogos aleatorios/agrupados de Windows Server o Windows 10. Para obtener más información, consulte Instalar Microsoft Teams mediante MSI (sección Instalación de VDI).

Supongamos que tiene entornos VDI persistentes dedicados en Windows 10. Quiere que la aplicación Microsoft Teams se actualice automáticamente y prefiere que Microsoft Teams se instale por usuario en Appdata/Local. En este caso, utilice el instalador .exe o el MSI sin ALLUSER=1.

> **Nota:**
>
> Recomendamos instalar el VDA antes de instalar Microsoft Teams en la imagen dorada. Este orden de instalación es necesario para que el indicador ALLUSER=1 surta efecto. Si la máquina virtual tenía Microsoft Teams instalado antes de instalar el VDA, desinstale Microsoft Teams y vuelva a instalarlo.

### Para el acceso con Remote PC

Se recomienda instalar la versión 1.4.00.22472 de Microsoft Teams o una posterior después de instalar el VDA. De lo contrario, deberá cerrar sesión e iniciar sesión de nuevo para que Microsoft Teams detecte el VDA según lo previsto. A partir de la versión 1.4.00.22472, se incluye lógica aumentada ejecutada en el inicio de Microsoft Teams y en el inicio de sesión para la detección de VDA. En estas versiones también se incluye la identificación del tipo de sesión activa (HDX, RDP o conectada localmente a la máquina cliente). Si se conectó localmente, es posible que las versiones anteriores de Microsoft Teams no detecten ni inhabiliten determinadas funciones o elementos de la interfaz de usuario. Por ejemplo, salas para sesión de subgrupo, ventanas emergentes para reuniones y chats o reacciones en las reuniones.

> **Importante:**
>
> Al pasar de una sesión local a una sesión HDX y si Microsoft Teams se mantiene abierto y ejecutándose en segundo plano, debe salir y volver a iniciar Microsoft Teams para optimizar la sesión con HDX correctamente.
> Por el contrario, si utiliza Microsoft Teams de forma remota a través de una sesión HDX optimizada, desconecte la sesión HDX y vuelva a conectarse a la misma sesión de Windows localmente en el dispositivo. Cuando trabaje desde la oficina, deberá volver a iniciar Microsoft Teams para que pueda detectar correctamente el estado de Remote PC (HDX o local). Esto se debe a que Microsoft Teams solo puede evaluar el modo VDI en el momento de iniciarse la aplicación, y no mientras ya se está ejecutando en segundo plano. Sin un reinicio, es posible que Microsoft

> Teams no cargue funciones como ventanas emergentes, grupos de trabajo o reacciones en las reuniones.

### Para App Layering

Si utiliza Citrix App Layering para administrar instalaciones de VDA y Microsoft Teams en diferentes capas, deberá crear una nueva clave de Registro en los VDA con Windows antes de instalar Microsoft Teams con el indicador `ALLUSER=1` desde la línea de comandos. Para obtener más información, consulte la sección *Optimización para Microsoft Teams con Citrix App Layering* en Multimedia.

### Recomendaciones para Profile Management

Se recomienda utilizar el instalador a nivel de equipo para entornos Windows Server y VDI agrupados de Windows 10.

Cuando el indicador **ALLUSER =1** se transfiere al MSI desde la línea de comandos (instalador a nivel de equipo), la aplicación Microsoft Teams se instala en `C:\Program Files (x86)` (unos 300 MB). La aplicación utiliza `AppData\Local\Microsoft\TeamsMeetingAddin` para los registros y `AppData\Roaming\Microsoft\Teams` (~600–700 MB) para configuraciones específicas de usuario, almacenamiento en caché de elementos de la interfaz de usuario, etc.

> **Importante:**
>
> Si no transfiere el indicador **ALLUSER=1**, el MSI coloca el instalador Teams.exe y `setup.json` en `C:\Program Files (x86)\Teams Installer`. Se agrega una clave del Registro (TeamsMachineInstaller) en: `HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run`
>
> Un inicio de sesión de usuario posterior desencadena la instalación final en **AppData** en su lugar.

#### Instalador a nivel de equipo

A continuación, se muestra un ejemplo de carpetas, accesos directos de escritorio y registros creados al instalar el instalador a nivel de equipo de Microsoft Teams en una máquina virtual Windows Server 2016 de 64 bits:

*Carpeta:*

- `C:\Program Files (x86)\Microsoft\Teams`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

*Acceso directo de escritorio:*

`C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe`

*Registro:*

- HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Nombre: Teams
- Tipo: REG_SZ
- Valor: C:\Program Files (x86)\Microsoft\Teams\current\Teams.exe

> **Nota:**
>
> La ubicación del Registro varía según los sistemas operativos subyacentes y la cantidad de bits.

#### Recomendaciones

- Recomendamos inhabilitar el inicio automático eliminando las claves de Registro de Microsoft Teams. Al hacerlo, se evita que muchos inicios de sesión que ocurren al mismo tiempo (por ejemplo, al comenzar la jornada laboral) saturen la CPU de la máquina virtual.
- Si el escritorio virtual no tiene una GPU/vGPU, se recomienda **Inhabilitar la aceleración de hardware de GPU** en la **Configuración** de Microsoft Teams para mejorar el rendimiento. Este parámetro (`"disableGpu":true`) se almacena en %Appdata%\Microsoft\Teams, en desktop-config.json. Puede utilizar un script de inicio de sesión para modificar ese archivo y establecer el valor en **true**.
- Si utiliza Citrix Workspace Environment Management (WEM), habilite la **protección contra picos de CPU** para administrar el consumo de procesador para Microsoft Teams.

#### Instalador por usuario

Cuando se utiliza el instalador .exe, el proceso de instalación es diferente. Todos los archivos se colocan en AppData.

*Carpeta:*

- C:\Users\<username>\AppData\Local\Microsoft\Teams
- C:\Users\<username>\AppData\Local\Microsoft\TeamsPresenceAddin
- C:\Users\<username>\AppData\Local\Microsoft\TeamsMeetingAddin
- C:\Users\<username>\AppData\Local\SquirrelTemp
- C:\Users\<username>\AppData\Roaming\Microsoft\Teams

*Acceso directo de escritorio:*

```
C:\Users\<username>\AppData\Local\Microsoft\Teams\Update.exe --
processStart "Teams.exe"
```

*Registro:*

```
HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

#### Prácticas recomendadas

Las recomendaciones se basan en casos de uso.
El uso de Microsoft Teams con una configuración no persistente requiere un administrador de almacenamiento en caché de perfiles para una sincronización eficiente de los datos de runtime de Microsoft Teams. Con un administrador de almacenamiento en caché de perfiles, la información específica del usuario necesaria se almacena en caché durante la sesión de usuario. La información específica del usuario incluye los datos de usuario, el perfil y la configuración. Sincronice los datos de estas dos carpetas:

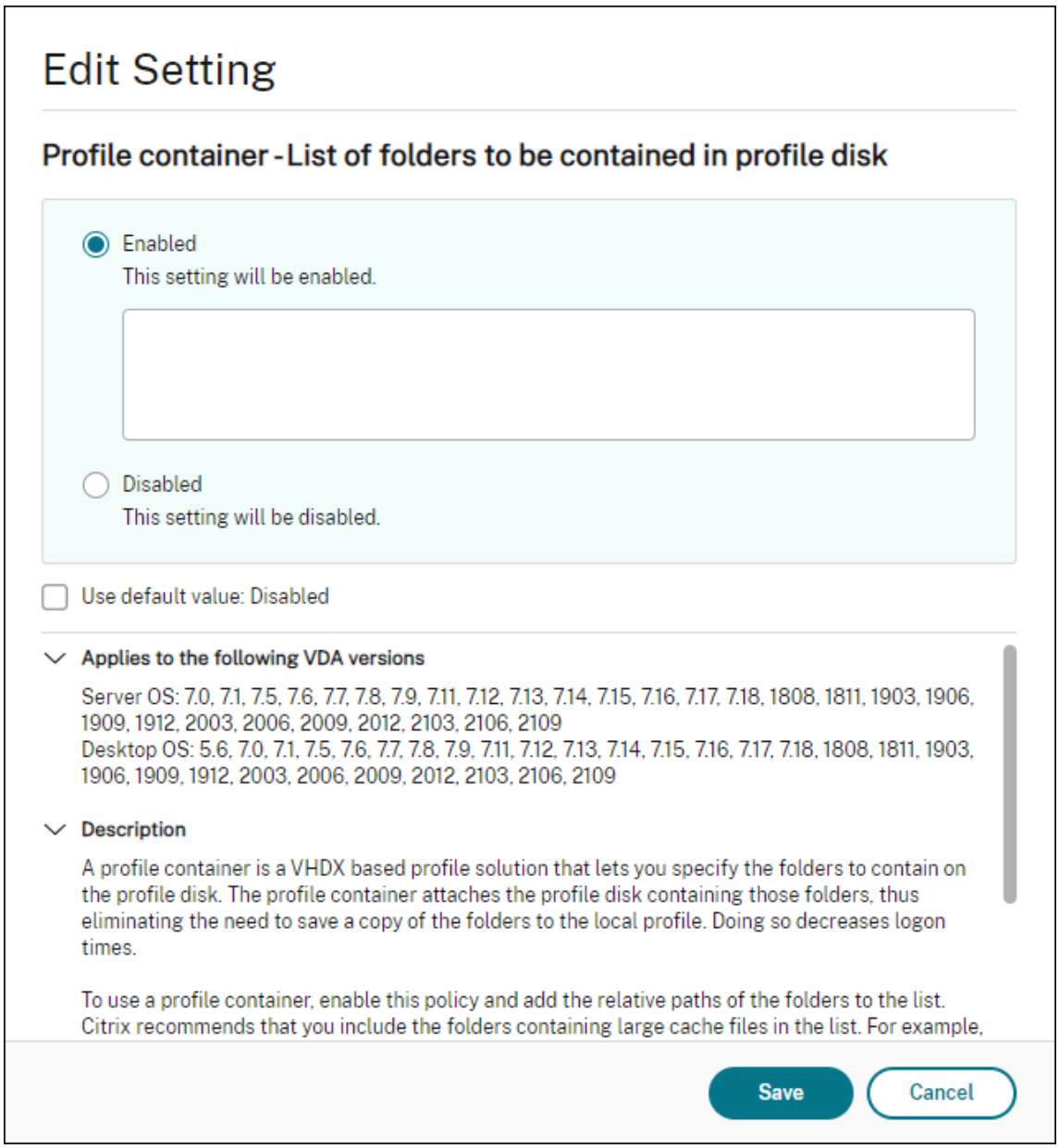
- `C:\Users\<username>\AppData\Local\Microsoft\IdentityCache`
- `C:\Users\<username>\AppData\Roaming\Microsoft\Teams`

**Lista de exclusión de contenido almacenado en caché de Microsoft Teams para una configuración no persistente** Excluya los archivos y directorios de la carpeta de almacenamiento en caché de Microsoft Teams como se describe en la documentación de Microsoft. Esta acción ayuda a reducir el tamaño del almacenamiento en caché del usuario para optimizar aún más la configuración no persistente.

**Caso de uso: Sesión única** En este caso, el usuario final utiliza Microsoft Teams en una ubicación cada vez. No es necesario que ejecuten Microsoft Teams en dos sesiones de Windows al mismo tiempo. En una implementación de escritorio virtual común, cada usuario se asigna a un escritorio y Microsoft Teams se implementa en el escritorio virtual como una aplicación.
Se recomienda habilitar el contenedor de perfiles de Citrix y redirigir los directorios por usuario que se indican en Instalador por usuario al contenedor.

1. Implemente el instalador a nivel de equipo de Microsoft Teams (**ALLUSER=1**) en la imagen maestra.
2. Habilite Citrix Profile Management y configure el almacén de perfiles de usuario con los permisos adecuados.
3. Habilite la siguiente configuración de directiva de Profile Management: **Sistema de archivos > Sincronización > Contenedor de perfiles —Lista de carpetas que se incluirán en el disco de perfiles**.




Enumera todos los directorios por usuario en esta configuración. También puede configurar estas opciones a través del servicio Citrix Workspace Environment Management (WEM).

4. Aplique la configuración al grupo de entrega correspondiente.
5. Inicie sesión para validar la implementación.

## Requisitos del sistema

### Versión mínima recomendada: Delivery Controller (DDC) 1906.2

Si utiliza una versión anterior, consulte Habilitar la optimización de Microsoft Teams:

Sistemas operativos compatibles:

- Windows Server 2022, 2019, 2016, 2012R2 ediciones Standard y Datacenter, y con opción Server Core

**Versión mínima: Virtual Delivery Agent (VDA) 1906.2**

Sistemas operativos compatibles:

- Windows 11.
- Windows 10 de 64 bits, versión 1607 y versiones posteriores. Las aplicaciones alojadas en máquinas virtuales se admiten en la aplicación Citrix Workspace para Windows 2109.1 y versiones posteriores.
- Windows Server 2022, 2019, 2016 y 2012 R2 (ediciones Standard y Datacenter).

Requisitos:

- BCR_x64.msi: El MSI que incluye el código de optimización de Microsoft Teams y se inicia automáticamente desde la GUI. Si utiliza la interfaz de línea de comandos para la instalación de VDA, no la excluya.

**Versión recomendada: La versión Current Release más reciente de la aplicación Citrix Workspace para Windows; versión mínima: aplicación Citrix Workspace 1907 para Windows**

- Windows 11.
- Windows 10 (ediciones de 32 y 64 bits, incluidas las ediciones Embedded; la compatibilidad con Windows 7 dejó de ofrecerse en la versión 2006, y la compatibilidad con Windows 8.1 dejó de ofrecerse en la versión 2204.1).
- Windows 10 IoT Enterprise 2016 LTSB (versión 1607) y 2019 LTSC (versión 1809).
- Arquitecturas de procesador (CPU) compatibles: x86 y x64 (ARM no es compatible)
- Requisito del dispositivo de punto final: CPU dual de aproximadamente 2,2-2,4 GHz que puede admitir una resolución HD de 720p durante una llamada de conferencia en vídeo de punto a punto.
- CPU de núcleo doble o cuádruple con velocidades base más bajas (unos 1,5 GHz) equipadas con Intel Turbo Boost o AMD Turbo Core que pueden aumentar hasta al menos 2,4 GHz.
- Clientes ligeros HP verificados: t630/t640, t730/t740, mt44/mt45.
- Clientes ligeros Dell verificados: 5070/5470 Mobile TC y AIO.
- Clientes ligeros 10ZiG verificados: 4510 y 5810q.
- Para obtener una lista completa de dispositivos de punto final verificados, consulte Clientes ligeros.

- La aplicación Citrix Workspace requiere un mínimo de 600 MB de espacio libre en disco y 1 GB de RAM.
- El requisito mínimo de Microsoft .NET Framework es la versión 4.8. La aplicación Citrix Workspace descarga e instala automáticamente .NET Framework, si no está presente en el sistema.

Los administradores pueden habilitar/inhabilitar Microsoft Teams iniciando en el modo optimizado y cambiando la directiva Optimización de Teams. Los usuarios que inician en modo optimizado en la aplicación Citrix Workspace no pueden inhabilitar Microsoft Teams.

#### Versión mínima: Aplicación Citrix Workspace 2006 para Linux

Software:

- `GStreamer` 1.0 o una versión posterior o Cairo 2
- libc++-9.0 o una versión posterior
- `libgdk` 3.22 o una versión posterior
- OpenSSL 1.1.1d
- Distribución de Linux x64

Hardware:

- Como mínimo, una CPU de doble núcleo de 1,8 GHz que admita una resolución de 720p HD durante llamadas de conferencia en vídeo de punto a punto
- CPU de doble o cuádruple núcleo con una velocidad base de 1,8 GHz y una velocidad Intel Turbo Boost alta de al menos 2,9 GHz

Para obtener una lista completa de dispositivos de punto final verificados, consulte Clientes ligeros.

Para obtener más información, consulte Requisitos previos para instalar la aplicación Citrix Workspace.

Puede inhabilitar la optimización para Microsoft Teams. Para ello, actualice el valor del campo **VDWEBRTC** a Off en el archivo `/opt/Citrix/ICAClient/config/module.ini`. El valor predeterminado es VDWEBRTC = On. Una vez finalizada la actualización, reinicie la sesión. (se requiere permiso en la raíz).

#### Versión mínima: Aplicación Citrix Workspace 2012 para Mac

Sistemas operativos compatibles:

- macOS Catalina (10.15).
- macOS Big Sur 11.0.1 y versiones posteriores.
- macOS Monterrey.

Funciones compatibles:

- Audio
- Vídeo
- Optimización para compartir pantalla (entrante y saliente)

> **Nota:**
>
> La aplicación Citrix Viewer necesita acceder a las preferencias de Seguridad y privacidad de macOS para que el uso compartido de la pantalla funcione. Los usuarios configuran esta preferencia en el **menú Apple > Preferencias del Sistema > Seguridad y privacidad > Ficha Privacidad > Grabación de pantalla** y al seleccionar **Citrix Viewer**.

La optimización para Microsoft Teams funciona de forma predeterminada con la aplicación Citrix Workspace 2012 y versiones posteriores y macOS 10.15.

Si quiere desactivar la optimización de Microsoft Teams, ejecute este comando en el terminal y reinicie la aplicación Citrix Workspace:

```
defaults write com.citrix.receiver.nomas mtopEnabled -bool NO
```

**Versión mínima: La versión más reciente de la aplicación Citrix Workspace para Chrome OS activa en la versión más reciente de Chrome OS**

Hardware:

- Procesadores que funcionan igual o mejor que Intel i3 de cuatro núcleos a 2,4 GHz.

Funciones compatibles:

- Audio
- Vídeo
- Optimización para compartir pantalla (entrante y saliente): Inhabilitada de forma predeterminada. Consulte estos parámetros para obtener instrucciones sobre cómo activarla.

## Escalabilidad de un solo servidor

En esta sección se ofrecen recomendaciones y orientación para estimar cuántos usuarios o máquinas virtuales (VM) puede admitir un único host físico. Esto se conoce comúnmente como "escalabilidad de un solo servidor"(SSS/Single Server Scalability) de Citrix Virtual Apps and Desktops. En el contexto de Citrix Virtual Apps (CVA) o virtualización de sesiones, también se conoce comúnmente como densidad de usuarios. La idea es averiguar cuántos usuarios o máquinas virtuales pueden trabajar en un único componente de hardware que ejecute un hipervisor principal.

> **Nota:**
>
> Esta sección incluye información para estimar la escalabilidad de un solo servidor (SSS). Tenga en cuenta que esta información es general y no necesariamente aplicable a su situación o entorno en particular. La única forma de entender realmente el valor de SSS en Citrix Virtual Apps and Desktops es utilizando una herramienta para pruebas de carga o escalabilidad como Login VSI. Citrix recomienda usar esta información y estas reglas simples únicamente para estimar rápidamente el valor SSS. Sin embargo, Citrix recomienda usar Login VSI o la herramienta de pruebas de carga que elija para validar los resultados, especialmente antes de comprar hardware o tomar cualquier decisión de carácter financiero.

#### Hardware (sistema sometido a prueba)

- Dell PowerEdge R740
- Intel Xeon (Gold) 6126 a 2,60 GHz (máx. Turbo 3,70 GHz), 12 núcleos por socket, socket doble con Hyper-Threading habilitado
- 382 GB de RAM
- Almacenamiento SSD RAID 0 local (11 discos) 6 TB

#### Software

Una sola máquina virtual (40 procesadores lógicos) con Windows 2019 (TSVDA) que ejecute Citrix Virtual Apps and Desktops 2106
VMware ESXi 6.7

#### Terminología

- Carga de trabajo de los trabajadores del conocimiento: Incluye Acrobat Reader, Freemind/Java, visor de fotos, Edge y aplicaciones de MS Office como Excel, Outlook, PowerPoint y Word.
- Base de referencia: Las pruebas de escalabilidad del servidor se ejecutan con la carga de trabajo los trabajadores del conocimiento (sin Microsoft Teams).
- Carga de trabajo de Microsoft Teams: Carga de trabajo típica de trabajador del conocimiento + Microsoft Teams

#### Cómo es la prueba de estrés de Microsoft Teams

- Microsoft Teams se optimiza con HDX. Por lo tanto, todo el procesamiento multimedia se envía al dispositivo de punto final o al cliente y no forma parte de la medición.

- Todos los procesos de Microsoft Teams se detienen o finalizan antes del comienzo de la carga de trabajo.
- Abra Microsoft Teams (arranque en frío).
- Mida el tiempo que tarda Microsoft Teams en cargar y captar el foco de la ventana principal de Microsoft Teams.
- Cambie a la ventana de chat con los atajos de teclado.
- Cambie a la ventana del calendario con los atajos de teclado.
- Envíe el mensaje de chat a un usuario específico con los atajos de teclado.
- Cambie a la ventana de Microsoft Teams con los atajos de teclado.

**Resultados**

- Impacto de escalabilidad del 40 % con la carga de trabajo de Microsoft Teams (81 usuarios), en comparación con la base de referencia (137 usuarios).
- Al aumentar la capacidad del servidor en un ~40 % (en CPU), se restaura el número de usuarios como ocurre con la carga de trabajo de referencia.
- Se requiere un 20 % de memoria adicional con la carga de trabajo de Microsoft Teams, en comparación con la base de referencia.
- Aumento del tamaño de almacenamiento por usuario de 512 a 1024 MB.
- ~50 % de aumento en la escritura de IOPS, ~100 % de aumento en las lecturas de IOPS. Microsoft Teams puede tener un impacto significativo en entornos con un almacenamiento más lento.

## Tabla de funciones y compatibilidad de versiones

| Función | Microsoft Teams (versión mínima) | VDA (versión mínima) | Aplicación Citrix Workspace para Windows CR (versión mínima) | Aplicación Citrix Workspace para Mac (versión mínima) | Aplicación Citrix Workspace para Linux (versión mínima) | Aplicación Citrix Workspace para Chrome OS |
|---|---|---|---|---|---|---|
| Audio/vídeo (P2P y conferencias) | versión actual menos 90 días | 1906 | 1907 | 2009 | 2004 | 2105.5 |

| Función | Microsoft Teams (versión mínima) | VDA (versión mínima) | Aplicación Citrix Workspace para Windows CR (versión mínima) | Aplicación Citrix Workspace para Mac (versión mínima) | Aplicación Citrix Workspace para Linux (versión mínima) | Aplicación Citrix Workspace para Chrome OS |
|---|---|---|---|---|---|---|
| Uso compartido de pantalla | Versión actual menos 90 días | 1906 | 1907 | 2012 | 2006 | 2105.5 |
| i. Borde rojo del indicador de la pantalla | Versión actual menos 90 días | 1906 | 2002 | 2012 | 2006 | No |
| ii. Limitar la captura a Desktop Viewer | Versión actual menos 90 días | 1906 | 2009.5 | 2012 | 2006 | No |
| iii. Varios monitores | Versión actual menos 90 días | 1912 CU6+ | 2106 (1) | 2106 | 2106 | No |
| DTMF | Versión actual menos 90 días | N/D | 2102 | 2101 | 2101 | 2111.1 |
| Compatibilidad con servidores proxy | Versión actual menos 90 días | N/D | 2012 (2) | 2104 (3) | 2101 (3) | 2305 |
| Uso compartido de aplica-ciones | Versión actual menos 90 días | 2109 | 2109.1 | 2203.1 | 2209 | No |

| Función | Microsoft Teams (versión mínima) | VDA (versión mínima) | Aplicación Citrix Workspace para Windows CR (versión mínima) | Aplicación Citrix Workspace para Mac (versión mínima) | Aplicación Citrix Workspace para Linux (versión mínima) | Aplicación Citrix Workspace para Chrome OS |
|---|---|---|---|---|---|---|
| Subtítulos en directo | Versión actual menos 90 días | N/A (4) | 2109.1 | 2109 | 2109 | 2303 |
| e911 dinámico | Versión actual menos 90 días | N/D | 2112.1 | 2112 | 2112 | 2112 |
| Dar control | Versión actual menos 90 días | N/D | 2112.1 | 2203.1 | No | No |
| Solicitar el control | Versión actual menos 90 días | N/D | 2112.1 | 2203.1 | 2203 | 2303 |
| Multiventana | 1.5.00.11865 | 2112, 1912 CU6 (5) | 2112.1 | 2203.1 | 2203 | 2303 |
| Transcripciones de reuniones | Versión actual menos 90 días | 2112.1, 1912 CU6 y versiones posteriores | 2112 | 2203.1 | 2203 | 2303 |
| Desenfoque de fondo | Versión actual menos 90 días | 2112, 1912 CU6 y versiones posteriores | 2207 | 2301 | 2212 | 2303 |

1. El visor del CD en modo de pantalla completa solamente. MAYÚS+F2 no disponible.
2. Negotiate/Kerberos, NTLM, Basic y Digest. Los archivos `Pac` también son compatibles.
3. Anónimos solamente.
4. Si el VDA tiene la versión 2112 o una posterior, los subtítulos en directo solo funcionarán si la versión de la aplicación Citrix Workspace es 2203.1 para Mac y 2203 para Linux o 2112 para Win-

dows. Esto se debe a que los subtítulos en directo se comportan de manera diferente si Microsoft Teams está en modo de interfaz de ventana única o en modo de varias ventanas.

5. El modo multiventana se introdujo en la versión 2112 de VDA, pero se transfirió a la versión 1912 LTSR CU6 de VDA.

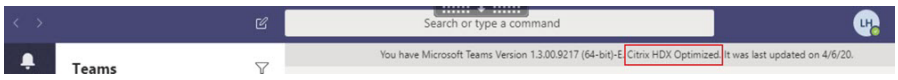
> **Nota:**
>
> Todas las funciones enumeradas en la **Aplicación Citrix Workspace para Windows 1912 CU6 (o una versión posterior)** son válidas para la aplicación Citrix Workspace para Windows 2203.1 LTSR CU1.

### Habilitar la optimización de Microsoft Teams

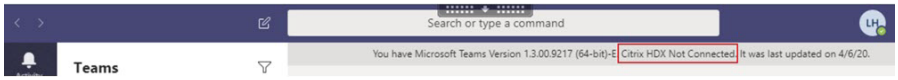
Para habilitar la optimización de Microsoft Teams, utilice la directiva de la consola Administrar descrita en la directiva de redirección de Microsoft Teams. Esta directiva está **activada** de forma predeterminada. Además de habilitar esta directiva, HDX comprueba si la versión de la aplicación Citrix Workspace es, al menos, la mínima requerida. Si se ha habilitado la directiva y se admite la versión de la aplicación Citrix Workspace, **HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\MSTeamsRedirSupp** se establece en **1** automáticamente en el VDA. Microsoft Teams lee la clave para cargar en modo VDI.

> **Nota:**
>
> Si utiliza agentes VDA de la versión 1906.2, o una posterior, con versiones de controladores anteriores (por ejemplo, versión 7.15) que no tienen la directiva disponible en la consola Administrar (Studio), el VDA aún puede optimizarse. La optimización HDX para Microsoft Teams está habilitada de forma predeterminada en el VDA.

Si hace clic en **Acerca de > Versión**, aparecerá la leyenda **Optimizado para Citrix HDX**:

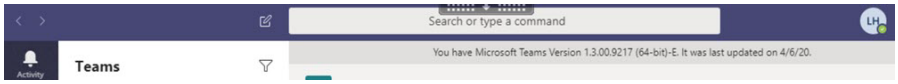



Si se muestra que **Citrix HDX no está conectado**, la API de Citrix se carga en Microsoft Teams. Cargar la API es el primer paso hacia la redirección. Pero hay un error en las partes posteriores de la pila. Es muy probable que el error esté en los servicios de VDA o en la aplicación Citrix Workspace.




Si no aparece ninguna leyenda, Microsoft Teams no pudo cargar la API de Citrix. Salga de Microsoft Teams haciendo clic con el botón secundario en el icono del área de notificaciones y reiniciando. Asegúrese de que la directiva de la consola Administrar no esté establecida en **Prohibido** y de que la versión de la aplicación Citrix Workspace sea compatible.




**Importante: Reconexiones de sesión**

- Es posible que tenga que iniciar Microsoft Teams de nuevo para obtener una sesión optimizada para HDX cuando su conectividad cambia. Por ejemplo, si se traslada de un dispositivo de punto final no compatible (aplicación Workspace para iOS, Android o versiones anteriores de Windows/Linux/Mac) a uno compatible (aplicación Workspace para Windows/Linux/Mac/Chrome OS/HTML5) o viceversa.
- También es necesario reiniciar Microsoft Teams si ha instalado la aplicación con el instalador EXE de Microsoft Teams en el VDA. Se recomienda el instalador EXE para implementaciones de VDI persistentes. En estos casos, Microsoft Teams puede actualizarse automáticamente mientras la sesión HDX está en estado desconectado. Por lo tanto, los usuarios que se reconectan a una sesión HDX descubren que Microsoft Teams no se ejecuta de forma optimizada.
- Al pasar de una sesión local a una sesión HDX, debe iniciar Microsoft Teams de nuevo para optimizar la sesión con HDX. Esta acción es necesaria en caso de acceso con Remote PC.

## Requisitos de la red

Microsoft Teams se basa en servidores Media Processor (procesador de multimedia) en Microsoft 365 para las reuniones o llamadas con múltiples participantes. Además, Microsoft Teams se basa en Transport Relay (traspaso de transporte) de Microsoft 365 para estos casos:

- Dos pares en una llamada punto a punto sin conectividad directa
- Un participante no tiene conectividad directa con el procesador de multimedia.

Así, el estado de la red entre el par y la nube de Microsoft 365 determina el rendimiento de la llamada. Para obtener pautas detalladas sobre la planificación de redes, consulte Principios de conectividad de red de Microsoft 365.

Se recomienda analizar el entorno para identificar los riesgos y los requisitos que puedan influir en la implementación general de voz y vídeo en la nube.
Utilice la Herramienta de evaluación de la red de Skype for Business para comprobar si la red está lista para Microsoft Teams. Para obtener información sobre asistencia, consulte Asistencia.

### Resumen de las recomendaciones de red clave para el tráfico con protocolo de transporte en tiempo real (RTP)

- Conéctese a la red de Microsoft 365 de la forma más directa posible desde la sucursal.
- Planifique y proporcione suficiente ancho de banda en la sucursal.

- Compruebe la conectividad y la calidad de la red en cada sucursal.
- Si debe usar una de estas opciones en la sucursal, asegúrese de que el tráfico RTP/UDP (gestionado por HdxRtcEngine.exe en la aplicación Citrix Workspace) no se vea obstaculizado.
  - Omitir servidores proxy
  - Interceptación SSL de red
  - Dispositivos de inspección profunda de paquetes (PPP)
  - Bifurcaciones VPN (utilice túnel dividido si es posible)

> **Importante: Configuración de túneles divididos de VPN**
>
> El tráfico de HdxRtcEngine.exe debe desviarse del túnel VPN y debe poder usar la conexión a Internet local del usuario para conectarse directamente al servicio. El modo varía según el producto de la VPN y la plataforma de la máquina que se usen, pero la mayoría de las soluciones de VPN permitirán una configuración simple de la directiva para aplicar esta lógica. Para obtener más información sobre las instrucciones de túneles divididos específicas de cada plataforma VPN, consulte este artículo de Microsoft.

El motor multimedia WebRTC en la aplicación Workspace (HdxRtcEngine.exe) utiliza el protocolo de transporte seguro en tiempo real (SRTP) para secuencias multimedia que se descargan en el cliente. SRTP proporciona confidencialidad y autenticación a RTP. Para esta funcionalidad, se utilizan claves simétricas (negociadas con DTLS) para cifrar el contenido multimedia y los mensajes de control mediante cifrado AES.

Para lograr una experiencia de usuario positiva, se recomiendan las siguientes métricas:

| Métrica | Del dispositivo de punto final a Microsoft 365 |
|---|---|
| Latencia (ida) | < 50 ms |
| Latencia (RTT) | < 100 ms |
| Pérdida de paquetes | < 1% durante cada intervalo de 15 segundos |
| Fluctuación entre la llegada de paquetes | < 30 ms durante cada intervalo de 15 segundos |

Para obtener más información, consulte Preparación de la red de la organización para Microsoft Teams.

En cuanto a los requisitos de ancho de banda, la optimización para Microsoft Teams puede utilizar una amplia variedad de códecs para audio (OPUS/G.722/PCM G711) y vídeo (H264).

Los pares negocian estos códecs durante el proceso de establecimiento de llamadas mediante la oferta/respuesta de Session Description Protocol (SDP).
Las recomendaciones mínimas de Citrix por usuario son:

| Tipo | Ancho de banda | Códec |
|---|---|---|
| Audio (en cada sentido) | ~ 90 Kbps | G.722 |
| Audio (en cada sentido) | ~ 60 Kbps | Opus* |
| Vídeo (en cada sentido) | ~ 700 Kbps | H264 360p @ 30 fps 16:9 |
| Pantalla compartida | ~ 300 Kbps | H.264 1080p @ 15 fps |

Opus y H264 son los códecs preferidos para llamadas de conferencias y entre dos usuarios.

> **Importante:**
>
> En cuanto concierne al rendimiento, el uso de CPU es más elevado en la codificación que en la descodificación en la máquina cliente. Puede integrar como parte del código la resolución máxima de codificación en la aplicación Citrix Workspace para Linux y Windows. Consulte Estimador de rendimiento del codificador y Optimización para Microsoft Teams.

### Servidores proxy

Según la ubicación del proxy, tenga en cuenta lo siguiente:

- Configuración del proxy en el VDA:

  Si configura un servidor proxy explícito en el VDA y redirige las conexiones al host local a través de un proxy, la redirección falla. Para configurar el proxy correctamente, debe seleccionar la configuración **Omitir servidor proxy para las direcciones locales** en **Opciones de Internet > Conexiones > Configuración de LAN > Servidores proxy** y omitir `127.0.0.1:9002`.

  Si utiliza un archivo PAC, el script de configuración del proxy de VDA del archivo PAC debe devolver **DIRECT** para `wss://127.0.0.1:9002`. Si no, la optimización falla. Para asegurarse de que el script devuelva **DIRECT**, utilice `shExpMatch(url, "wss://127.0.0.1:9002/*")`.

- Configuración del proxy en la aplicación Citrix Workspace:

  Si la sucursal está configurada para acceder a Internet a través de un proxy, estas versiones admiten servidores proxy:

  - Aplicación Citrix Workspace para Windows versión 2012 (Negotiate/Kerberos, NTLM, Basic y Digest. Los archivos Pac también son compatibles)
  - Aplicación Citrix Workspace para Windows versión 1912 CU5 (Negotiate/Kerberos, NTLM, Basic y Digest. Los archivos Pac también son compatibles)
  - Aplicación Citrix Workspace para Linux versión 2101 (autenticación anónima)

- Aplicación Citrix Workspace para Mac versión 2104 (autenticación anónima)

Los dispositivos cliente con versiones anteriores de la aplicación Citrix Workspace no pueden leer configuraciones de proxy. Estos dispositivos envían tráfico directamente a los servidores TURN de Microsoft 365.

> **Importante:**
>
> - Compruebe que el dispositivo cliente se puede conectar al servidor DNS para procesar resoluciones DNS. Un dispositivo cliente debe poder resolver estos FQDN del servidor de retransmisión de Microsoft Teams:
>
>   - `worldaz.relay.teams.microsoft.com`
>   - `inaz.relay.teams.microsoft.com`
>   - `uaeaz.relay.teams.microsoft.com`
>   - `euaz.relay.teams.microsoft.com`
>   - `usaz.relay.teams.microsoft.com`
>   - `turn.dod.teams.microsoft.us`
>   - `turn.gov.teams.microsoft.us`
>
> Si las solicitudes de DNS no se realizan correctamente, fallan las llamadas P2P con usuarios externos y el establecimiento de archivos multimedia en llamadas de conferencias.
>
> - La ubicación del servidor de conferencias se selecciona en función de la ubicación del escritorio virtual del primer participante (y no del cliente).

### Establecimiento de llamadas y rutas de flujo de medios

Cuando sea posible, el motor de medios HDX WebRTC de la aplicación Citrix Workspace (HdxRtcEngine.exe) intenta establecer una conexión SRTP (protocolo de transporte seguro en tiempo real) de red directa mediante el protocolo de datagramas de usuario (UDP) en una llamada de un par homologo a otro. Si los puertos UDP altos están bloqueados, el motor de medios recurre a TCP 443 con TLS.

El motor de contenido multimedia HDX admite ICE, el protocolo STUN (Session Traversal Utilities for NAT) y el protocolo TURN (Traversal Using Relays around NAT) para la detección de candidatos y el establecimiento de conexiones. Esta compatibilidad significa que el dispositivo de punto final debe ser capaz de procesar resoluciones DNS.

Supongamos que no hay una ruta directa entre los dos pares o entre un par y un servidor de conferencias y se une a una llamada o reunión de varios participantes. HdxRtcEngine.exe utiliza un servidor de traspaso de transporte de Microsoft Teams en Microsoft 365 para llegar al otro par o al procesador multimedia, donde se alojan las reuniones. La máquina cliente debe tener acceso a tres intervalos de

direcciones IP de subred de Microsoft 365 y a cuatro puertos UDP (o a TCP 443 con TLS como alternativa si UDP está bloqueado). Para obtener más información, consulte el diagrama de arquitectura en Configuración de llamadas y Direcciones URL e intervalos de direcciones IP de ID 11 para Office 365.

| ID | Categoría | Direcciones | Puertos de destino |
|---|---|---|---|
| 11 | Precisa optimización | 13.107.64.0/18, 52.112.0.0/14, 52.120.0.0/14 | **UDP:** 3478, 3479, 3480, 3481, **TCP:** 443 (reserva) |

Estos intervalos incluyen tanto servidores de traspaso de transporte como procesadores de multimedia, con un front-end de Azure Load Balancer.
Los servidores de traspaso de transporte de Microsoft Teams proporcionan funcionalidad para los protocolos STUN y TURN, pero no son dispositivos de punto final ICE. Además, los servidores de traspaso de transporte de Microsoft Teams no finalizan el contenido multimedia, TLS ni hacen ninguna transcodificación. Pueden puentear TCP (si HdxRtcEngine.exe utiliza TCP) a UDP cuando reenvían tráfico a otros pares o procesadores de multimedia.

El motor de medios WebRTC de la aplicación Workspace conecta con el servidor de traspaso de transporte de Microsoft Teams más cercano en la nube de Microsoft 365. El motor de medios utiliza la técnica IP Anycast y los puertos UDP 3478 a 3481 (puertos UDP diferentes por carga de trabajo, aunque puede haber multiplexación) o el puerto TCP 443 con TLS de reserva. La calidad de la llamada depende del protocolo de red subyacente. Debido a que siempre se recomienda UDP antes que TCP, se recomienda diseñar las redes para dar cabida al tráfico UDP en la sucursal.

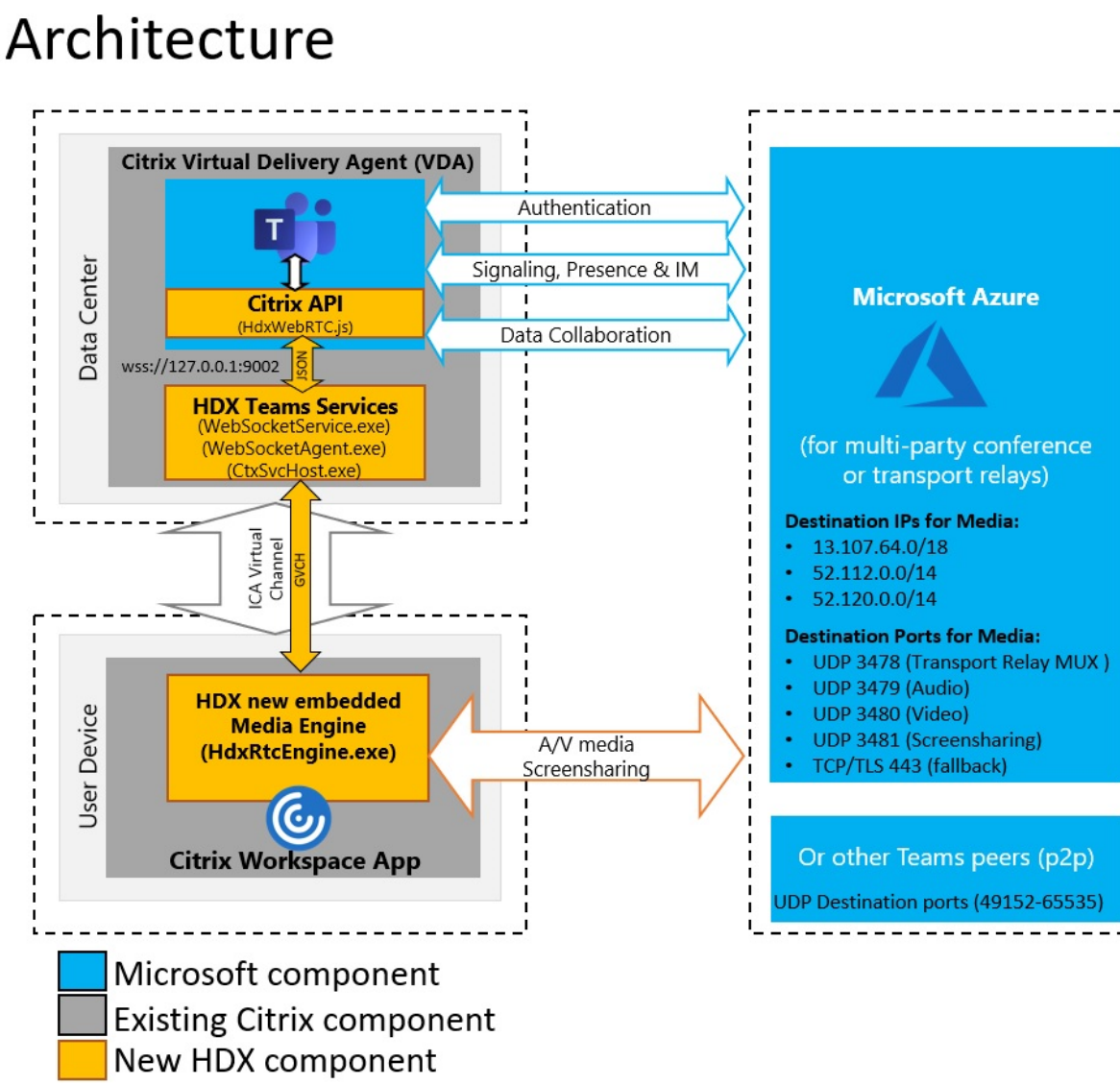
Si Microsoft Teams se carga en modo optimizado y HdxRtcEngine.exe se está ejecutando en el terminal, los errores de ICE pueden provocar un error de configuración de llamada o transmisión de audio/vídeo en una sola dirección. Cuando no se pueda completar una llamada o las secuencias multimedia no sean dúplex completo, compruebe primero la **traza Wireshark** en el dispositivo de punto final. Para obtener más información sobre el proceso de recopilación de candidatos de ICE, consulte "Recopilar registros"en la sección Asistencia.

> **Nota:**
>
> Si los dispositivos de punto final no tienen acceso a Internet, es posible que los usuarios aún puedan realizar una llamada de un par homólogo a otro si están en la misma red de área local (LAN). Las reuniones no funcionan. En este caso, hay un tiempo de espera de 30 segundos antes de que comience la configuración de la llamada.

### Configuración de llamadas

Utilice este diagrama de arquitectura como referencia visual para la secuencia del flujo de llamadas. Los pasos correspondientes se indican en el diagrama.




### Arquitectura

1. Inicie Microsoft Teams.
2. Microsoft Teams se autentica en O365. Las directivas de arrendatario se envían al cliente de Microsoft Teams, y la información pertinente del canal de señalización y del protocolo TURN se transmite a la aplicación.
3. Microsoft Teams detecta que se ejecuta en un VDA y realiza llamadas API a la API de JavaScript de Citrix.

4. JavaScript de Citrix en Microsoft Teams abre una conexión WebSocket segura con WebSocketService.exe en el VDA, que genera WebSocketAgent.exe dentro de la sesión de usuario.
5. WebSocketAgent.exe crea una instancia de un canal virtual genérico mediante una llamada al servicio de redirección de Microsoft Teams para Citrix HDX (CtxSvcHost.exe).
6. El archivo wfica32.exe (motor de HDX) de la aplicación Citrix Workspace genera un nuevo proceso denominado HdxRtcEngine.exe, que es el nuevo motor de WebRTC utilizado para la optimización de Microsoft Teams.
7. El motor de medios de Citrix y Teams.exe tienen una ruta bidireccional de canales virtuales y pueden comenzar a procesar solicitudes multimedia.

   ——Llamadas de usuario——

8. El **interlocutor A** hace clic en el botón de **llamada**. Teams.exe se comunica con los servicios de Microsoft Teams de Microsoft 365 y establece una ruta de señalización de extremo a extremo con el **interlocutor B**. Microsoft Teams solicita a HdxRtcEngine una serie de parámetros de llamada admitidos (códecs, resoluciones, etc., lo que se conoce como una oferta de protocolo de descripción de sesiones o SDP). A continuación, estos parámetros de llamada se retransmiten mediante la ruta de señalización a los servicios de Microsoft Teams en Microsoft 365 y, desde allí, al otro interlocutor.
9. La oferta/respuesta SDP (negociación de paso único) tiene lugar a través del canal de señalización, y las comprobaciones de conectividad de ICE (recorrido de NAT y firewalls mediante solicitudes de enlace STUN) se completan. A continuación, el contenido multimedia con Secure Real-Time Transport Protocol (SRTP) circula directamente entre HdxRtcEngine y el otro interlocutor (o servidores de conferencia de Microsoft 365 si se trata de una reunión).

### Sistema telefónico de Microsoft

Sistema telefónico es la tecnología de Microsoft que posibilita el control de llamadas y las funciones de central de conmutación (PBX) en la nube de Microsoft 365 con Microsoft Teams. La optimización para Microsoft Teams es compatible con el sistema telefónico mediante planes de llamada de Microsoft 365 o enrutamiento directo. Con Enrutamiento directo, puede conectar su propio controlador de borde de sesión (SBC) compatible directamente al sistema telefónico de Microsoft sin necesidad de software local adicional.
Se admiten colas de llamadas, transferencia, reenvío, retención, silenciamiento y reanudación de una llamada.

#### DTMF

Las siguientes versiones de la aplicación Citrix Workspace (y posteriores) son compatibles con la funcionalidad multifrecuencia de doble tono (DTMF):

- Versión 2102 de la aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace 1912 LTSR CU5 para Windows (solo SO con Windows 10)
- Versión 2101 de la aplicación Citrix Workspace para Linux
- Versión 2101 de la aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para Chrome OS versión 2111.1

#### Compatibilidad con e911 dinámico

A partir de la versión 2112, la aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, le permite:

- Configurar y redirigir llamadas de emergencia.
- Notificar al personal de seguridad.

La notificación se proporciona en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams que se ejecuta en el VDA.

La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. La optimización de Microsoft Teams con HDX es conforme a la ley de Ray Baum cuando se utiliza con las siguientes versiones de la aplicación Citrix Workspace:

- Aplicación Citrix Workspace para Windows 2112.1 y versiones posteriores
- Aplicación Citrix Workspace para Linux 2112 y versiones posteriores
- Aplicación Citrix Workspace para Mac 2112 y versiones posteriores
- Aplicación Citrix Workspace para Chrome OS 2112 y versiones posteriores

Para habilitar las llamadas de emergencia dinámicas, el administrador debe usar Centro de administración de Microsoft Teams y configurar lo siguiente para crear un mapa de ubicación de emergencia o de red:

- Parámetros de red
- Servicio de información de ubicación (LIS)

Para obtener más información sobre las llamadas de emergencia dinámicas, consulte la documentación de Microsoft.

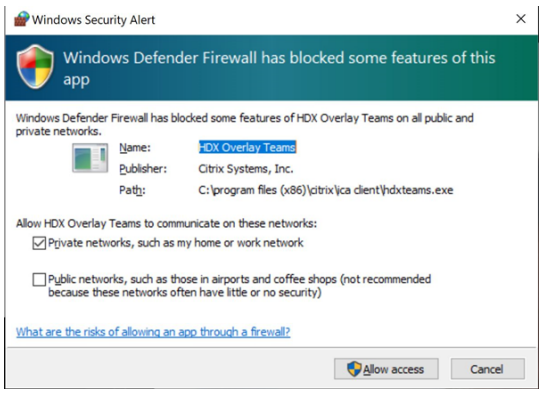
 

La información de ubicación transmitible que la aplicación Citrix Workspace transmite a Microsoft Teams es:

- ID de chasis o ID de puerto mediante el protocolo de detección de la capa de enlace (LLDP) para conexiones Ethernet/Switch. Ethernet/Switch (LLDP) se admite en:
  - Versiones 8.1 y 10 de Windows
  - macOS, que requiere software de habilitación de LLDP. Para descargar el software de habilitación de LLDP, vaya a `www.microsoft.com` y busque el software de habilitación de LLDP.
  - Linux, que requiere que la biblioteca LLDP se incluya en la distribución del sistema operativo (SO) del cliente ligero.
- BSSID de WLAN y {IPv4-IPv6; subred; dirección MAC} del dispositivo de punto final en el que está instalada la aplicación Citrix Workspace.
  - Las ubicaciones basadas en subredes y Wi-Fi son compatibles con la aplicación Workspace para Windows, Linux y Mac.
- Latitud y longitud, si se concede el permiso de usuario en el nivel de SO donde está instalada la aplicación Citrix Workspace.
  - Compatible con todas las plataformas de la aplicación Workspace. Sin embargo, para Citrix Workspace para Linux, debe incluir la biblioteca `libgps` en la distribución del sistema operativo del cliente ligero (sudo apt-get install libgps23 gpsd lldpd).

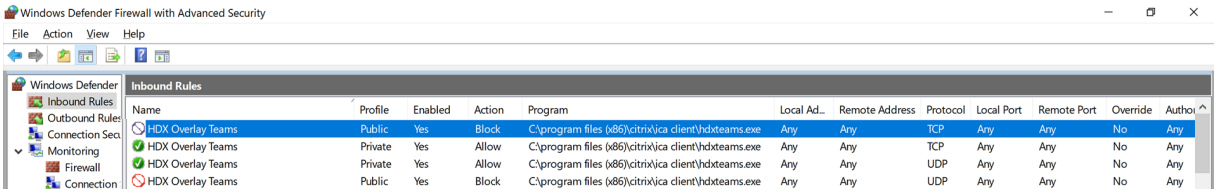
### Consideraciones sobre el firewall

Cuando los usuarios inician una llamada optimizada mediante el cliente de Microsoft Teams por primera vez, es posible que aparezca una advertencia relacionada con la configuración del **firewall de Windows** . En la advertencia, se pide a los usuarios que permitan la comunicación para HdxTeams.exe o HdxRtcEngine.exe (HDX Overlay Microsoft Teams).



Las cuatro entradas siguientes se agregan en **Reglas de entrada**, en la consola **Firewall de Windows Defender > Seguridad avanzada**. Puede aplicar reglas más restrictivas si quiere.

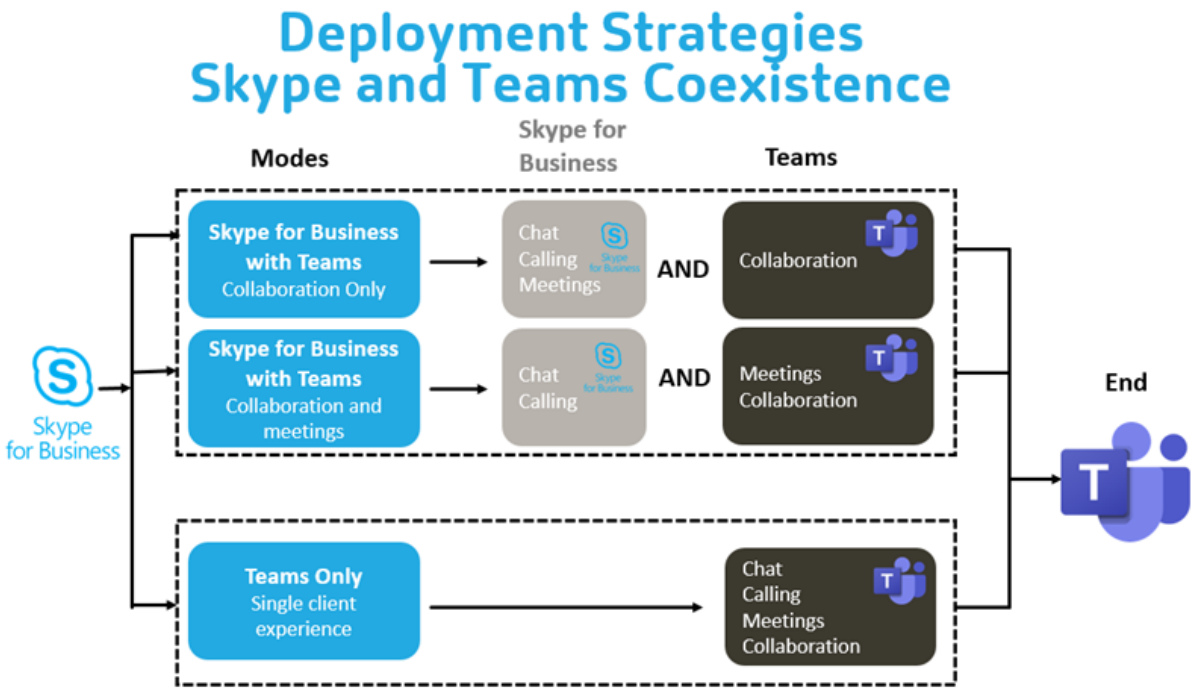



## Coexistencia de Microsoft Teams y Skype for Business

Puede implementar Microsoft Teams y Skype for Business en paralelo, como dos soluciones independientes con prestaciones superpuestas.
Para obtener más información, consulte Coexistencia e interoperabilidad de Microsoft Teams y Skype for Business.

Citrix RealTime Optimization Pack y Optimización de HDX para motores multimedia de Microsoft Teams respetan la configuración establecida en su entorno. Los ejemplos incluyen modos de isla y Skype for Business con la colaboración de Microsoft Teams. Asimismo, Skype for Business con las reuniones y la colaboración de Microsoft Teams.

El acceso periférico solo se puede conceder a una sola aplicación a la vez. Por ejemplo, el acceso a la cámara web de parte de RealTime Media Engine durante una llamada bloquea el dispositivo de imágenes durante dicha llamada. Cuando el dispositivo se libera, está disponible para Microsoft Teams.



### Citrix SD-WAN: conectividad de red optimizada para Microsoft Teams

Para lograr una calidad de audio y vídeo óptima, se requiere una conexión de red a la nube de Microsoft 365 que tenga baja latencia, baja vibración y baja pérdida de paquetes. El uso de una red de retorno (backhaul) para canalizar el tráfico RTP de audio y vídeo de Microsoft Teams desde los usuarios de la aplicación Citrix Workspace que se encuentran en sucursales a un centro de datos antes de dirigirlo a Internet puede agregar una latencia excesiva. También podría provocar congestión en los vínculos WAN. Citrix SD-WAN optimiza la conectividad para Microsoft Teams en base a los principios de conectividad de red de Microsoft 365. Citrix SD-WAN utiliza la dirección IP y el servicio web de Microsoft 365 basados en REST de Microsoft y DNS próximo. Este uso sirve para identificar, clasificar y dirigir el tráfico de Microsoft Teams.

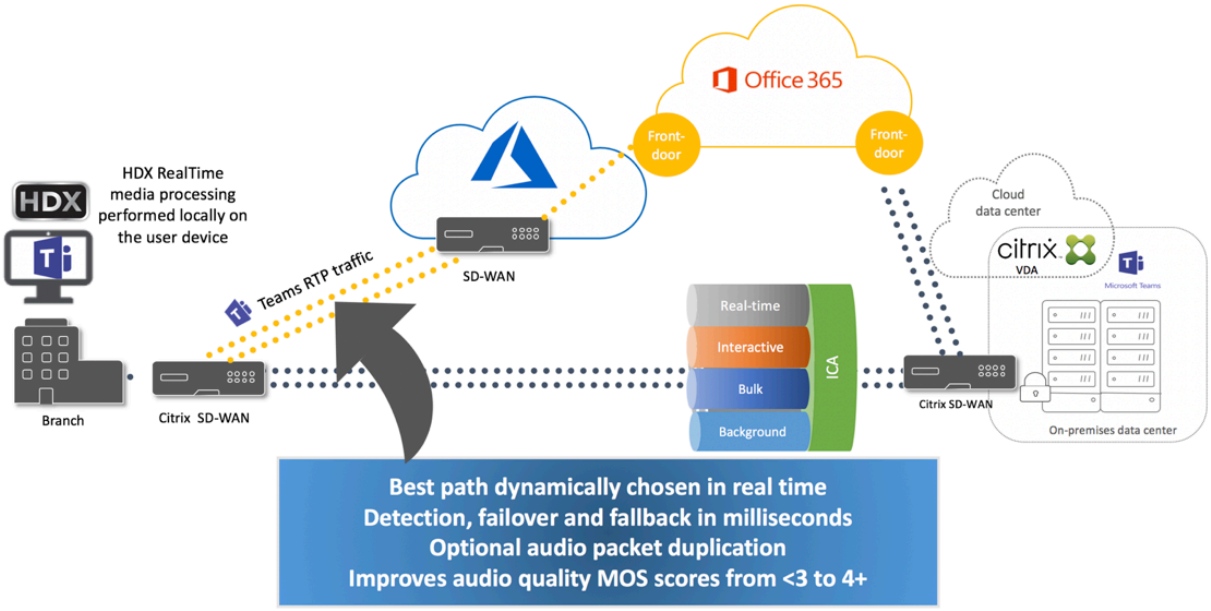
Las conexiones de banda ancha empresarial de Internet en muchas áreas sufren pérdida intermitente de paquetes, períodos de vibración excesiva e interrupciones.

Citrix SD-WAN ofrece dos soluciones para preservar la calidad de audio y vídeo de Microsoft Teams cuando la red tiene un estado variable o degradado.

- Si utiliza Microsoft Azure, un dispositivo virtual Citrix SD-WAN (VPX) implementado en la red virtual de Azure ofrece optimizaciones de conectividad avanzadas. Estas optimizaciones incluyen conmutación por error de enlaces y duplicación de paquetes de audio.
- Los clientes de Citrix SD-WAN pueden conectarse a Microsoft 365 a través de Citrix Cloud Direct Service. Este servicio garantiza una entrega fiable y segura de todo el tráfico de Internet.

Si la calidad de la conexión a Internet de la sucursal no es un problema, puede ser suficiente para minimizar la latencia. Dirija el tráfico de Microsoft Teams directamente desde el dispositivo de sucursal Citrix SD-WAN a la puerta de entrada de Microsoft 365 más cercana para minimizar la latencia. Para obtener más información, consulte Optimización de Citrix SD-WAN Office 365.




### Reuniones y chat en modo multiventana

En Windows, puede utilizar varias ventanas de reuniones o chat para Microsoft Teams. Para obtener más información sobre la función emergente, consulte Microsoft Teams Pop-Out Windows for Chats and Meetings en el sitio de Microsoft 365.

> **Nota:**
>
> Esta función está disponible en la aplicación Citrix Workspace para Windows 2112.1, Mac 2203, Linux 2203 y ChromeOS 2303. Requiere un VDA 2112 o una versión posterior, y se transfirió a 1912 CU6 LTSR y versiones posteriores, y a VDA 2112.

### Desenfoque y efectos de fondo

La aplicación Citrix Workspace para Windows, Mac, Linux y ChromeOS/HTML5 admite efectos y desenfoque de fondo en la optimización de Microsoft Teams con HDX.

Puede difuminar o reemplazar el fondo por una imagen predeterminada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). Puede utilizar esta función con llamadas de conferencia o P2P.

> **Nota:**
>
> Esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en

> modo multiventana.

Los controles de la interfaz de usuario de Microsoft Teams para desenfoque y efectos de fondo requieren las siguientes versiones mínimas:

- Aplicación Citrix Workspace para Windows 2207
- Aplicación Citrix Workspace para Mac 2301
- Aplicación Citrix Workspace para Linux 2212
- Aplicación Citrix Workspace para ChromeOS 2303

**Limitaciones:**

- El cliente debe estar conectado a Internet mientras se reemplaza la imagen de fondo por una imagen predeterminada de Microsoft Teams.
- La interfaz de usuario de Microsoft Teams no admite el reemplazo de imágenes de fondo definidas por el administrador y el usuario. Las imágenes de fondo personalizadas se pueden configurar mediante los parámetros de configuración del cliente, si la imagen también está almacenada en el cliente.

#### Establecimiento de una imagen de fondo personalizada

Las siguientes claves de Registro solo son necesarias si no tiene previsto utilizar la interfaz de usuario de Microsoft Teams para controlar la función o si un administrador quiere anular el funcionamiento predeterminado. Por ejemplo: inhabilitar el desenfoque de fondo porque el dispositivo de punto final no es lo suficientemente potente.

**En Windows** Para establecer una imagen de fondo personalizada, los administradores o los usuarios finales deben configurar la siguiente clave del Registro en el cliente o el dispositivo de punto final:

Ubicación: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- Nombre: VideoBackgroundEffect
- Tipo: DWORD
- Valor: 0 (inhabilitado), 1 (habilitado), 2 (reemplazo de imagen de fondo)

Al establecer el valor en 1, se desenfoca el fondo. Este valor lo puede establecer el usuario final o el administrador.

Si se establece el valor en 2, también debe estar presente la clave **VideoBackgroundImage**. Este valor solo puede establecerlo el administrador. Esta clave solo es necesaria si quiere reemplazar la imagen de fondo, no desenfocarla:

- Nombre: VideoBackgroundImage

- Tipo: REG_SZ
- Valor: nombre_de_imagen.jpeg

La imagen de fondo del vídeo debe estar presente en el directorio `C:\Program Files (x86)\Citrix\ICA Client`.

Esta configuración del Registro también sirve para habilitar el desenfoque de fondo o el reemplazo de imágenes en la aplicación Citrix Workspace 2206 sin el selector de interfaz de usuario de Microsoft Teams. En otras palabras, si su entorno o VDA no admiten el modo multiventana, puede usar la solución alternativa (claves del Registro en HKCU) con la aplicación Citrix Workspace 2206 o posterior para lograr un resultado parecido, aunque el usuario no podrá controlar la funcionalidad en medio de la sesión HDX o la llamada de Microsoft Teams.

Los cambios en las claves del Registro solo surten efecto cuando se conecta la sesión HDX.

**En Mac** Ubicación de la imagen descargada por el usuario: */Usuarios/nombre_de_usuario/Descargas/cualquier_i*

Ejecute los siguientes comandos para establecer la imagen personalizada como imagen predeterminada:

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundEffect -int 2
```

```
defaults write com.citrix.HdxRtcEngine VideoBackgroundImage -string "
/Users/username/Downloads/any_image.png"
```

**En Linux** Ubicación de la imagen descargada por el usuario: */home/nombre_de_usuario/Downloads/cualquier_ir*

Cree el archivo */var/.config/citrix/hdx_rtc_engine/config.json* y agregue estas claves de configuración en formato JSON. Por ejemplo,

```
1  {
2
3
4  "VideoBackgroundEffect":2,
5
6  "VideoBackgroundImage":"/home/username/Downloads/any_image.jpg"
7
8   }
9
10 <!--NeedCopy-->
```

**En HTML5** Para HTML5, solo se admite el desenfoque de fondo. No se admite el reemplazo de imágenes personalizadas.

Para desenfocar el fondo, haga lo siguiente:

1. Vaya al archivo **configuration.js** que se encuentra en la carpeta **HTML5Client**.

2. Agregue el atributo **backgroundEffects** y establezca el atributo en **true**. Por ejemplo,

```
'features' : {

    'msTeamsOptimization' :
    {

        'backgroundEffects' : true
     }

 }

<!--NeedCopy-->
```

3. Guarde los cambios.

#### Consideraciones sobre el consumo de CPU

Si bien la funcionalidad de desenfoque es frugal en cuanto respecta a la CPU, puede esperar un aumento del consumo. Por ejemplo: en un cliente ligero con un chip Intel® Pentium® Silver de 4 núcleos y 1,5 GHz con TurboBoost de hasta 2,8 GHz, el desenfoque del fondo agrega aproximadamente un 2% al uso de CPU. El uso medio de CPU es inferior al 20%.

### Vista de galería y participantes activos en Microsoft Teams

Microsoft Teams permite los modos **Gallery**, **Large Gallery** y **Together**.

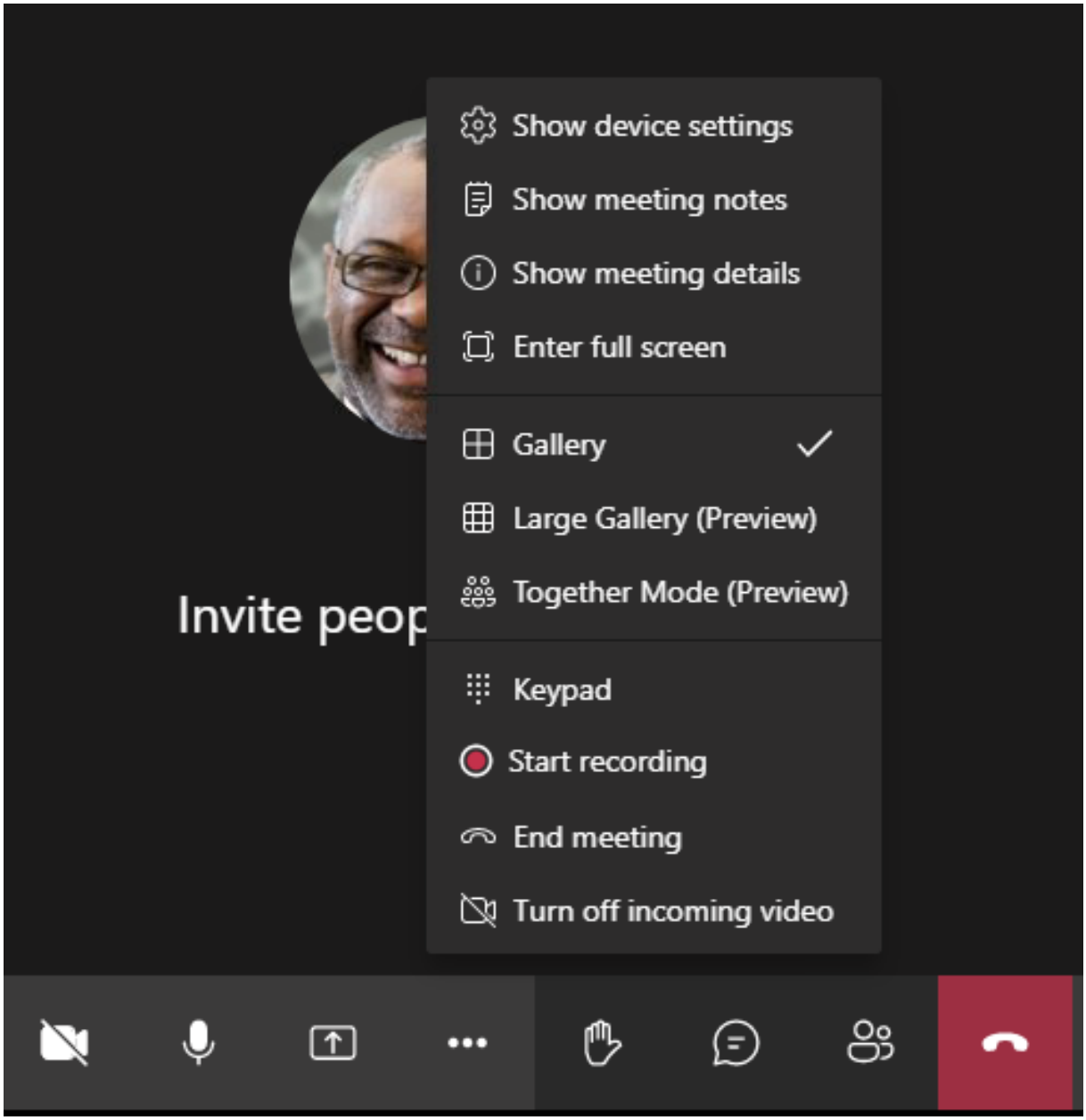
Microsoft Teams muestra una cuadrícula 2x2 con secuencias de vídeo de cuatro participantes (denominada **Gallery**). En este caso, Microsoft Teams envía cuatro secuencias de vídeo al dispositivo cliente para su decodificación. Cuando hay más de cuatro participantes que comparten vídeo, solo aparecen los últimos cuatro participantes más activos en la pantalla.

Microsoft Teams también ofrece la vista Large Gallery con una cuadrícula de hasta 7x7. Como resultado, el servidor de conferencias de Microsoft Teams compone un único feed de vídeo y lo envía al dispositivo cliente para su descodificación, lo que reduce el consumo de CPU. Es posible que este único feed de tipo tabla también incluya el vídeo de autoprevisualización del usuario.

Por último, Microsoft Teams permite el **modo Together**, que forma parte de la nueva experiencia de las reuniones. Con la tecnología de segmentación de IA para colocar digitalmente a los participantes en un fondo compartido, Microsoft Teams coloca a todos los participantes en el mismo auditorio.

El usuario puede controlar estos modos durante una llamada de conferencia con seleccionar los modos **Gallery**, **Large Gallery** o **Together** en el menú de puntos suspensivos.




Compatibilidad con restricciones de relación de aspecto de vídeo (CWA para Windows 2102, CWA para Linux 2106, CWA para MAC 2106 y versiones posteriores):

- La opción **Fit to frame** está disponible en la vista Gallery/Large Gallery. Esta opción recorta el tamaño del vídeo para ajustarlo a la subventana. **Fill to frame**, por otro lado, muestra barras negras (buzón) en los laterales del vídeo para que no haya recortes.

En esta tabla se ofrece una comparación de los diseños Gallery y Large Gallery:

| | Vista Gallery 2x2 (predeterminada) | Vista Large Gallery |
|---|---|---|
| Diseño / Cuadrícula | Muestra una cuadrícula 2x2 con secuencias de vídeo de cuatro participantes. Solo los cuatro últimos participantes más activos aparecen en la pantalla, y los demás participantes no aparecen en la cuadrícula. | Muestra una cuadrícula de 7x7 con transmisiones de vídeo de 49 participantes. |
| Técnica de mezcla | Un enrutador multimedia reenvía transmisiones individuales de cada participante a cada usuario. | Un servidor central de conferencias mezcla y transcodifica todo el audio o vídeo para crear un diseño compuesto personalizado para cada participante. Esta acción agrega alguna latencia adicional. |
| Participante activo | El nuevo participante activo sustituye al participante menos activo de la cuadrícula. | Muestra todos los participantes independientemente de si están activos o inactivos. |
| Codificación en el dispositivo de punto final | Es posible que se codifiquen al menos una secuencia de vídeo en el dispositivo de punto final si la transmisión simultánea está habilitada. Para obtener más información sobre la compatibilidad con la transmisión simultánea, consulte Transmisión simultánea. | Es posible que se codifiquen al menos una secuencia de vídeo en el dispositivo de punto final si la transmisión simultánea está habilitada. Para obtener más información sobre la compatibilidad con la transmisión simultánea, consulte Transmisión simultánea. |
| Descodificación en el dispositivo de punto final | Cada participante recibe hasta cuatro transmisiones multimedia individuales. Esto aumenta el consumo de CPU en el dispositivo de punto final por parte de HdxRtcEngine.exe (para la descodificación/generación). | Cada participante recibe una única transmisión de audio y vídeo. Esta configuración reduce el consumo de CPU en el dispositivo de punto final. |

| | Vista Gallery 2x2 (predeterminada) | Vista Large Gallery |
|---|---|---|
| Resolución máxima | 720p. Cuando cuatro participantes comparten vídeo, la resolución máxima es de 360p por fuente de vídeo. Si menos de cuatro participantes comparten vídeo, entonces es posible que la resolución por fuente de vídeo sea más alta. | 720p para el diseño compuesto o la mezcla. No hay necesidad de una transmisión de vídeo de alta calidad para cada participante en un diseño compuesto. Debido a esta condición, cada usuario remitente reduce la resolución o la velocidad de bits de carga. |
| Problema de "usuarios lentos" | El usuario remitente modifica la calidad de cada modalidad (audio/vídeo/pantalla compartida) a la calidad común más baja de las redes de los participantes. Esta transmisión multimedia se reenvía a todos los demás participantes. Como resultado, un participante con una red en mal estado afecta a la calidad de todos los demás participantes de la llamada. | Menos susceptible al caso de calidad común más baja de las redes. El servidor de conferencias ofrece diferentes calidades en función de las condiciones de red de cada participante. |
| Vista previa propia | Aparece usted en una miniatura pequeña en directo. | Aparece usted en una miniatura y se mezcla con el resto de las fuentes de vídeo. Como resultado, es posible que usted se incluya en el diseño principal de los vídeos con una ligera demora adicional. |

### Uso compartido de la pantalla en Microsoft Teams

Microsoft Teams utiliza el uso compartido de la pantalla basado en vídeo (VBSS), que codifica el escritorio que se comparte con códecs de vídeo, como H264, y crea un flujo de alta definición. Con la optimización HDX, la pantalla compartida entrante se trata como una transmisión de vídeo.

A partir de la aplicación Citrix Workspace 2109 o versiones posteriores para Windows, Linux o Mac y la aplicación Citrix Workspace 2303 para ChromeOS, los usuarios pueden compartir sus pantallas y

cámaras de vídeo simultáneamente.

Con versiones anteriores, si está en medio de una videollamada y el otro participante comienza a compartir el escritorio, la fuente de vídeo de la cámara original se pone en pausa. En su lugar, se muestra la fuente de vídeo de la pantalla compartida. A continuación, el participante debe reanudar manualmente el uso compartido de la cámara.

> **Nota para PowerPoint Live**
>
> Esta limitación no existe si comparte contenido de PowerPoint Live. En ese caso, otros compañeros pueden ver su cámara web y el contenido, además de desplazarse hacia adelante y hacia atrás para revisar otras diapositivas. En este caso, las diapositivas se generan en el VDA. Para acceder a una presentación con diapositivas de PowerPoint Live, haga clic en el botón "Share tray" y seleccione una de las diapositivas sugeridas de PowerPoint, o haga clic en "Browse"y busque un archivo de PowerPoint en su equipo o en OneDrive.

El uso compartido saliente de la pantalla también se optimiza y se descarga en la aplicación Citrix Workspace. En este caso, el motor de medios captura y transmite solo la ventana de Citrix Desktop Viewer (CDViewer.exe), con un borde rojo a su alrededor. Las aplicaciones locales que se superponen con Desktop Viewer no se capturan.

> **Nota**
>
> Establezca permisos específicos en la aplicación Citrix Workspace para Mac para habilitar el uso compartido de la pantalla. Para obtener más información, consulte Requisitos del sistema.

#### Varios monitores

Si Desktop Viewer (CDViewer.exe) está en modo de pantalla completa y se extiende por configuraciones de varios monitores, la aplicación Citrix Workspace 2106 o versiones posteriores (Windows/Linux/Mac) permite al selector de pantalla seleccionar el monitor que compartir.

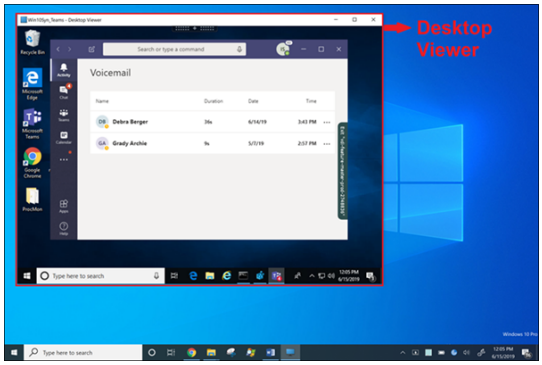
**Limitación conocida:**

- Si Desktop Viewer está inhabilitado o si se está utilizando Desktop Lock, la selección de varios monitores no está disponible en el selector de pantallas de Microsoft Teams. Es posible que Desktop Viewer se inhabilite al modificar la plantilla de archivo `.ICA` o `StoreFront web.config`. La tecla de acceso rápido MAYÚS+F2 no es compatible con el uso compartido de la pantalla en varios monitores.
- En las versiones de la aplicación Workspace anteriores a 2106, solo se comparte el monitor principal. Arrastre la aplicación del escritorio virtual al monitor principal para que el otro participante de la llamada la pueda ver.
- Es posible que el uso compartido de la pantalla para varios monitores no funcione si configura la aplicación Citrix Workspace con la función de diseño de monitores virtuales (partición lógica

de un único monitor físico). En este caso, todos los monitores virtuales se comparten en una imagen compuesta.

- Las versiones anteriores de la aplicación Citrix Workspace para Windows (de 1907 a 2008) también comparten una aplicación local que se ejecuta en la máquina cliente. Este uso compartido solo es posible si la aplicación local se superpone a Desktop Viewer. Este comportamiento se eliminó a partir de las versiones 2009.6 y 1912 CU5.
- Al compartir la pantalla, si pasa del modo de ventana a la pantalla completa, se detiene el uso compartido de la pantalla. Debe dejar de compartir la pantalla y compartirla de nuevo para que funcione.




**Uso compartido de la pantalla desde una aplicación integrada:**

Si publica Microsoft Teams como aplicación independiente integrada, el uso compartido de la pantalla captura el escritorio local del dispositivo de punto final físico. Se requiere la versión 1909 de la aplicación Citrix Workspace para Windows como mínimo.

### Uso compartido de aplicaciones

A partir de la aplicación Citrix Workspace para Windows 2112.1 y el VDA 2112, Microsoft Teams admite el uso compartido de aplicaciones.

A partir de la aplicación Citrix Workspace para Windows 2109, para Mac 2203, para Linux 2209 y para VDA 2109, Microsoft Teams admite el uso compartido de la pantalla de aplicaciones específicas que se ejecutan en la sesión virtual. Para compartir una aplicación específica:

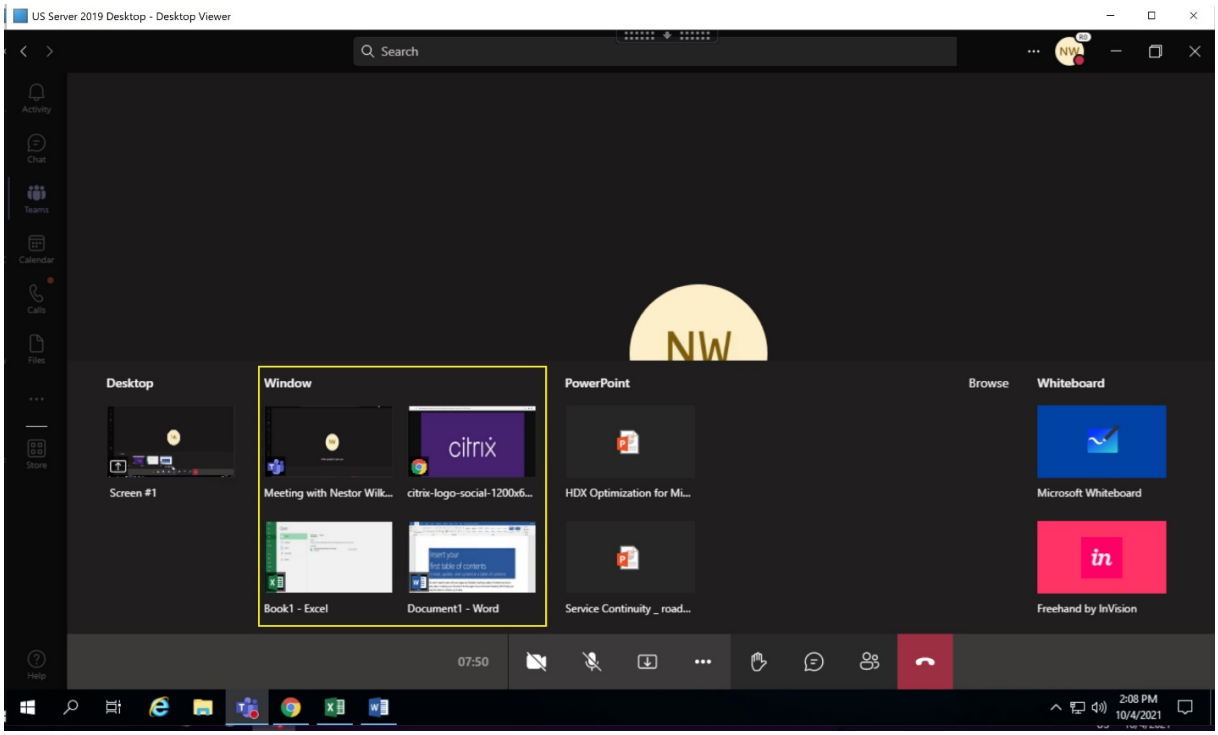
1. Vaya a la aplicación Microsoft Teams de su sesión remota.
2. Haga clic en **Compartir contenido** en la interfaz de usuario de Microsoft Teams.
3. Seleccione una aplicación para compartirla en la reunión. Aparecerá un borde rojo alrededor de la aplicación seleccionada y los interlocutores de la llamada podrán ver la aplicación compartida.

Para compartir una aplicación diferente, haga clic en **Compartir contenido** de nuevo y seleccione otra aplicación.

Si quiere inhabilitar el uso compartido de aplicaciones, cree esta clave del Registro en el VDA en `HKLM\SOFTWARE\Citrix\Graphics`:
Nombre: `UseWsProvider`
Tipo: `DWORD`
Valor: 0

> **Nota:**
>
> - Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.
> - Si minimiza una aplicación, Microsoft Teams muestra la última imagen de la aplicación compartida. Puede maximizar la ventana para reanudar el uso compartido de la pantalla.
> - La pantalla compartida depende de la captura de la ventana en el lado del VDA. A continuación, el contenido se transmite a velocidad máxima a la aplicación Citrix Workspace. La velocidad máxima es de 30 fotogramas por segundo. La aplicación Citrix Workspace reenvía el contenido a los homólogos o al servidor de conferencias.




**Limitaciones conocidas en el uso compartido de la pantalla de una aplicación específica:**

- El puntero del mouse no se muestra al compartir la pantalla de una aplicación.
- Si minimiza una aplicación al compartirla, solo aparece el icono de la aplicación en el selector de pantallas. La miniatura de la aplicación no se previsualiza en el selector de pantallas. No se puede compartir el contenido y el borde rojo no aparece hasta que se maximiza la aplicación.
- Acceso a aplicaciones locales (LAA) muestra una lista de aplicaciones que se pueden compartir

con aplicaciones de escritorio en las instancias de Microsoft Teams optimizadas del VDA. Sin embargo, al seleccionar la aplicación de la lista, es posible que el resultado no sea el previsto.

**Compatibilidad con App Protection**
El uso compartido de la pantalla de una aplicación específica es compatible con la función de App Protection de Microsoft Teams optimizado para HDX. Puede compartir la pantalla de una aplicación específica si ha iniciado la aplicación o el escritorio desde un grupo de entrega que tiene habilitada App Protection.

Al hacer clic en **Compartir contenido** en la interfaz de usuario de Microsoft Teams, el selector de pantallas quita la opción **Escritorio**. Solo se puede seleccionar la opción **Ventana** para compartir cualquier aplicación abierta.

> **Nota:**
>
> Cuando se inician aplicaciones o escritorios desde un grupo de entrega con App Protection habilitada, no se puede ver el vídeo entrante ni compartir la pantalla.

**Dar y solicitar el control en Microsoft Teams** Esta función se admite en las siguientes versiones de la aplicación Citrix Workspace (no depende de la versión del VDA ni del sistema operativo, sesión única o multisesión):

- Aplicación Citrix Workspace para Windows 2112.1 y versiones posteriores
- Aplicación Citrix Workspace para Mac 2203.1 y versiones posteriores
- Aplicación Citrix Workspace para Linux 2203 y versiones posteriores
- Aplicación Citrix Workspace para ChromeOS 2303 y versiones posteriores

Durante una llamada de Microsoft Teams, puede solicitar el control cuando un participante comparte la pantalla. Una vez que tiene el control, puede hacer selecciones, modificaciones u otras actividades con el teclado y el mouse en la pantalla compartida.

Para tomar el control cuando se comparte una pantalla, haga clic en el botón **Solicitar control** de la interfaz de usuario de Microsoft Teams. El participante de la reunión que comparte la pantalla puede aceptar o rechazar su solicitud.

Mientras tenga el control, puede realizar selecciones, modificaciones y otras acciones en la pantalla compartida. Para estas acciones, puede usar el teclado y el mouse. Cuando haya terminado, haga clic en **Solicitar el control**.

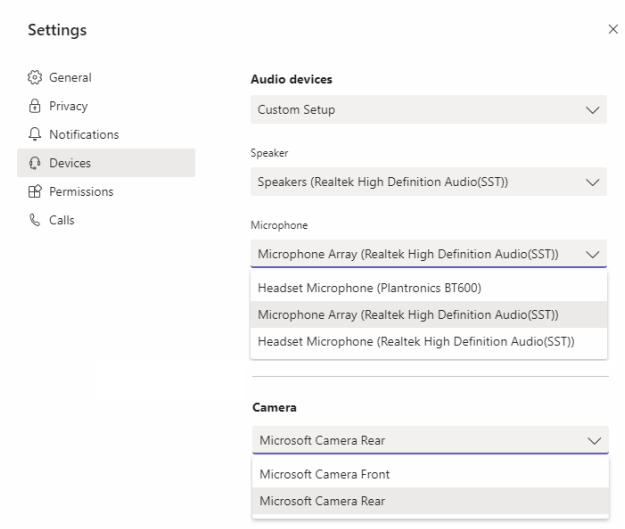
> **Limitaciones:**
>
> - La entrega y solicitud de control no están disponibles si el usuario comparte una sola aplicación (también conocido como uso compartido de aplicaciones). Se debe compartir todo el escritorio o monitor.

> - La función para anclar la barra de control en una ubicación específica no está disponible.

### Periféricos en Microsoft Teams

Cuando la optimización para Microsoft Teams está activa, la aplicación Citrix Workspace accede a los periféricos (auriculares, micrófonos, cámaras, altavoces…). A continuación, los periféricos se indican correctamente en la IU de Microsoft Teams (**Configuración > Dispositivos**).




Microsoft Teams no accede directamente a los dispositivos. En su lugar, recurre al motor de medios WebRTC de la aplicación Workspace para adquirir, capturar y procesar los objetos multimedia. Microsoft Teams indica los dispositivos que debe seleccionar el usuario.

Los periféricos que se insertan mientras Microsoft Teams está activo no están seleccionados de forma predeterminada. Tiene que seleccionar manualmente los periféricos en la pantalla **Configuración > Dispositivos** de la interfaz de usuario de Microsoft Teams. Una vez seleccionado un periférico, Microsoft Teams almacena en caché la información correspondiente. Como resultado, los periféricos se seleccionan automáticamente cuando se vuelve a conectar a una sesión desde el mismo dispositivo de punto final.

**Recomendaciones:**

- Auriculares con micrófono certificados por Microsoft Teams con eliminación de eco integrada. En configuraciones con varios periféricos, donde el micrófono y los altavoces se encuentran en dispositivos separados, puede producirse eco. Por ejemplo, una cámara web con un micrófono incorporado y un monitor con altavoces. Cuando utilice altavoces externos, colóquelos lo más lejos posible del micrófono. Además, colóquelos lejos de cualquier superficie que pueda refractar el sonido hacia el micrófono.
- Cámaras certificadas por Microsoft Teams, aunque los periféricos certificados por Skype Empresarial son compatibles con Microsoft Teams.

- El motor de medios de la aplicación Citrix Workspace no puede aprovechar la descarga de CPU con cámaras web que emplean codificación H.264 integrada UVC 1.1 y 1.5.

> **Nota:**
>
> La aplicación Workspace 2009.6 para Windows ahora puede adquirir periféricos con formatos de audio de 24 bits o con frecuencias superiores a 96 kHz.
>
> HdxTeams.exe (en la aplicación Citrix Workspace para Windows 2009 o versiones anteriores) solo admite estos formatos específicos de dispositivo de audio (canales, profundidad de bits y tasa de muestreo):
>
> - Dispositivos de reproducción: Hasta 2 canales, 16 bits, frecuencias de hasta 96 000 Hz
> - Dispositivos de grabación: Hasta 4 canales, 16 bits, frecuencias de hasta 96 000 Hz
>
> Aunque un solo altavoz o micrófono no tenga la configuración prevista, la enumeración de dispositivos en Microsoft Teams falla y aparece **Ninguno** en **Configuración > Dispositivos**.
>
> **Webrpc**: Sus registros en **HdxTeams.exe** muestran este tipo de información:
>
> ```
> Mar 27 20:58:22.885 webrtcapi.WebRTCEngine Info: init. initializing
> ...
> Mar 27 20:58:23.190 webrtcapi.WebRTCEngine Error: init. couldn't
> create audio module!
> ```
>
> Como solución temporal, inhabilite el dispositivo en cuestión o:
>
> 1. Abra el **Panel de control Audio** (mmsys.cpl).
> 2. Seleccione el dispositivo de reproducción o grabación.
> 3. Vaya a **Propiedades > Avanzadas** y cambie la configuración a un modo compatible.

#### Modo de reserva

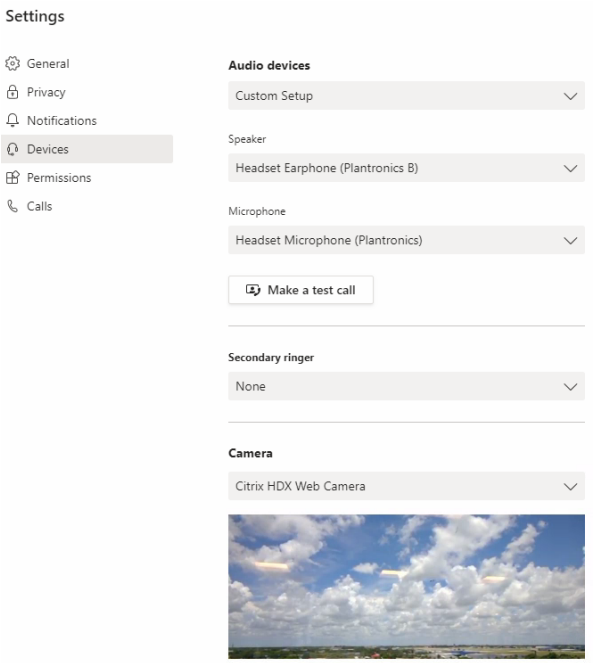
Si Microsoft Teams no se carga en el modo VDI optimizado (“Citrix HDX no está conectado”en Teams/Acerca de/Versión), el VDA recurre a tecnologías HDX heredadas. Las tecnologías HDX heredadas pueden ser la redirección de cámara web y la redirección de audio y micrófono del cliente. Si está utilizando un SO de plataforma o versión de la aplicación Workspace que no admite la optimización de Microsoft Teams, no se aplicarán las claves de registro de reserva.
En el modo de reserva, los periféricos se asignan al VDA. Los periféricos aparecen en la aplicación Microsoft Teams como si estuvieran conectados localmente al escritorio virtual.

Ahora puede controlar granularmente el mecanismo de reserva estableciendo las claves de Registro en el VDA. Para obtener información, consulte Modo de reserva de Microsoft Teams en la lista de funciones administradas a través del Registro.

Esta función requiere Microsoft Teams 1.3.0.13565 o una versión posterior.

Para determinar si está en el modo optimizado o no en la ficha **Configuración > Dispositivos** de la aplicación Microsoft Teams, la diferencia más significativa es el nombre de la cámara. Si Microsoft Teams se carga en modo no optimizado, se inician las tecnologías HDX antiguas. El nombre de la cámara web tiene el sufijo **Citrix HDX**, como se muestra en el gráfico siguiente. Es posible que los nombres de los altavoces y del micrófono sean ligeramente distintos (o estar truncados) si se comparan con sus nombres en el modo optimizado.




Cuando se utilizan tecnologías HDX heredadas, Microsoft Teams no descarga el procesamiento de audio, vídeo y uso compartido de la pantalla al motor multimedia WebRTC de la aplicación Citrix Workspace del dispositivo de punto final. En su lugar, las tecnologías HDX emplean la generación de contenido del lado del servidor. Espere un alto consumo de CPU en el VDA cuando active vídeo. Es posible que el rendimiento del audio en tiempo real no sea óptimo.

## Limitaciones conocidas

### Limitaciones de Citrix

Limitaciones en la aplicación Citrix Workspace:

- Botones HID: Respuesta y finalización de llamada no disponibles. Compatible con subir y bajar el volumen.
- Los parámetros de calidad de servicio que ofrece el Centro de administración de Microsoft Teams no se aplican a los usuarios de VDI.

- La función complementaria de App Protection para la aplicación Citrix Workspace evita el uso compartido de la pantalla saliente y bloquea el uso compartido de la pantalla y el vídeo entrantes.
- Los usuarios no pueden hacer capturas de pantalla del contenido de Microsoft Teams con una herramienta de recorte en el VDA. Sin embargo, si la herramienta de recorte se utiliza en el lado del cliente, se puede capturar el contenido.

Limitación en el VDA:

- Al configurar el parámetro PPP elevado de la aplicación Citrix Workspace en **Sí**, la ventana de vídeo redirigido aparece fuera de lugar. Esta limitación se produce cuando el factor de escalado de PPP del monitor está configurado en un valor superior al 100%.

Limitaciones en la aplicación Citrix Workspace y el VDA:

- Solo se puede controlar el volumen de una llamada optimizada desde la barra de volumen presente en la máquina cliente, no en el VDA.

#### Transmisión simultánea

La función de transmisión simultánea está habilitada para llamadas de videoconferencias en Microsoft Teams optimizado tanto en Windows como en Mac. Para Linux, consulte con el proveedor de su cliente ligero.
Con la transmisión simultánea, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran al adaptarse a la resolución adecuada para ofrecer la mejor experiencia en llamadas a todos los usuarios.

Con esta experiencia mejorada, es posible que cada usuario cuente con varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p…) en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red y más. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

> **Nota:**
>
> Esta función está disponible solamente después de la implantación de una actualización de Microsoft Teams. Para obtener información sobre el valor de ETA, vaya a https://www.microsoft.com/ y busque la hoja de ruta de Microsoft 365. Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

#### Limitaciones de Microsoft

- No se ofrece la vista de galería 3x3. Dependencia de Microsoft Teams: Póngase en contacto con Microsoft para saber cuándo esperar una cuadrícula 3x3.
- La interoperabilidad con Skype for Business se limita a llamadas de audio, sin modalidad de vídeo.
- La resolución máxima de transmisión de vídeo entrante y saliente es 720p. Dependencia de Microsoft Teams: Póngase en contacto con Microsoft para saber cuándo esperar el modo 1080p.
- No se admite el tono de espera de las llamadas RTC.
- No se admite la omisión de medios para enrutamiento directo.
- Los roles de productor y presentador para difusión y eventos en directo no están disponibles. El rol de asistente está disponible, pero no está optimizado (renderizado en el VDA).
- No está disponible la función de zoom en Microsoft Teams.
- No se admiten el enrutamiento basado en ubicación ni la omisión de medios.
- No se permite la combinación de llamadas (la opción no se muestra en la interfaz de usuario).

#### Limitaciones de Citrix y Microsoft

- Al hacer uso compartido de pantalla, la opción de **Incluir audio del sistema** no está disponible.
- La transmisión simultánea no es compatible con ChromeOS.

### Próximo fin de vida (EOL) de la función de ventana única en Microsoft Teams

El 31 de enero de 2024, Microsoft retirará la compatibilidad de Microsoft Teams con la interfaz de usuario de ventana única cuando se utilice la optimización de Microsoft Teams en entornos de imagen de disco virtual (VDI) y solo admitirá la experiencia multiventana. Microsoft notificó esta retirada el 8 de septiembre de 2023 en el Centro de administración de M365s (ID de publicación: MC674419).
Los detalles sobre la función de multiventana se encuentran en el artículo New Meeting and Calling Experience in Microsoft Teams de Tech Community.

Para seguir usando Microsoft Teams en modo optimizado para compartir pantallas y vídeo, debe actualizar su VDA y la aplicación Citrix Workspace a las versiones compatibles. Si no actualiza su infraestructura y dispositivos de punto final para que admitan el modo multiventana, solo podrá establecer llamadas de audio. No podrá usar la funcionalidad optimizada de vídeo y pantalla compartida.

En la siguiente tabla se muestran las versiones mínima, LTSR y recomendada de VDA y la aplicación Citrix Workspace necesarias para seguir usando las llamadas optimizadas en Microsoft Teams con Citrix VDI:

| Componente | Versión mínima | Versión LTSR compatible | Versión recomendada |
|---|---|---|---|
| Microsoft Teams | 1.5.00.11865 | No aplicable | Más reciente |
| VDA | 1912 CU6 LTSR, 2203 LTSR, 2112 CR | 1912 CU7+, 2203 CU2+ | 2308 CR+ |
| Aplicación Citrix Workspace para Windows | 2205 CR | 2203 CU2+ | 2309 CR+ |
| Aplicación Citrix Workspace para Mac | 2209 CR | No aplicable | 2308 CR+ |
| Aplicación Citrix Workspace para Linux | 2209 CR | No aplicable | 2308 CR+ |
| Aplicación Citrix Workspace para ChromeOS o HTML5 | 2303 CR | No aplicable | 2309 CR+ |

### Anuncio de obsolescencia del formato SDP (Plan B) en WebRTC

Citrix tiene previsto retirar la compatibilidad con el formato SDP (Plan B) en WebRTC en versiones futuras. Para poder hacer uso de las funcionalidades optimizadas de Microsoft Teams, deberá usar Unified Plan en WebRTC.

#### Productos afectados

En una de las versiones futuras de la aplicación Citrix Workspace, no se admitirán las llamadas entre dispositivos de punto final con la próxima versión de la aplicación Citrix Workspace y dispositivos de punto final con la aplicación Citrix Workspace 2108 o versiones anteriores. Esta incompatibilidad en las llamadas incluye a los clientes de la aplicación Citrix Workspace (CWA) 1912 LTSR. Los siguientes clientes de CWA se ven afectados:

- Aplicación Citrix Workspace para Windows
- Aplicación Citrix Workspace para Linux
- Aplicación Citrix Workspace para Mac
- Aplicación Citrix Workspace para Chrome

#### Reemplazo para el Plan B

Si utiliza una versión de la aplicación Citrix Workspace anterior a 2109, debe actualizar a una versión compatible (preferiblemente, la última versión Current Release). De lo contrario, no se conectarán las llamadas con una versión futura o dispositivos de punto final más recientes. Es posible que las llamadas entre versiones futuras y sus socios de comunicación federados tampoco se completen si el socio federado no ha actualizado su versión de Citrix Workspace.

La versión 2108 de la aplicación Citrix Workspace dejó recibir asistencia en marzo de 2023 y debe actualizarse a una versión más reciente. Para obtener más información sobre la compatibilidad de versiones de la aplicación Citrix Workspace, consulte la aplicación Workspace.

Para obtener más información sobre la retirada del Plan B, consulte la documentación de WebRTC.

### Información adicional

- Supervisión, solución de problemas y asistencia para Microsoft Teams
- Implementar la aplicación de escritorio de Microsoft Teams en la VM
- Instalar Microsoft Teams mediante MSI (sección Instalación de VDI)
- Clientes ligeros
- Herramienta de evaluación de la red de Skype for Business
- Coexistencia e interoperabilidad de Microsoft Teams y Skype for Business

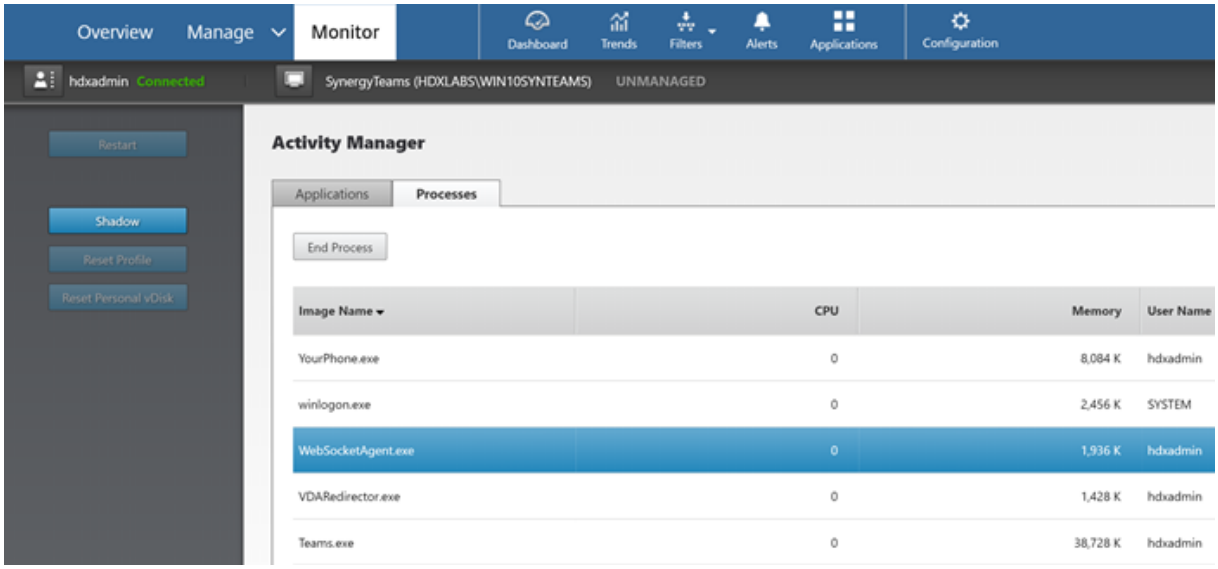
## Supervisión, solución de problemas y asistencia para Microsoft Teams

April 18, 2024

### Supervisar Teams

En esta sección, se ofrecen líneas generales para supervisar la optimización de Microsoft Teams con HDX.
Si está ejecutando en modo optimizado y `HdxRtcEngine.exe` se está ejecutando en la máquina cliente, un proceso en el VDA llamado `WebSocketAgent.exe` se ejecuta en la sesión. Utilice **Administrador de actividades** en Director para ver la aplicación.




Con la versión mínima de VDA 1912, puede supervisar las llamadas activas de Teams a través de Citrix HDX Monitor (versión mínima 3.11). La imagen ISO del producto Citrix Virtual Apps and Desktops contiene la último versión de `hdxmonitor.msi` en la carpeta `layout\image-full\Support\HDX Monitor`.

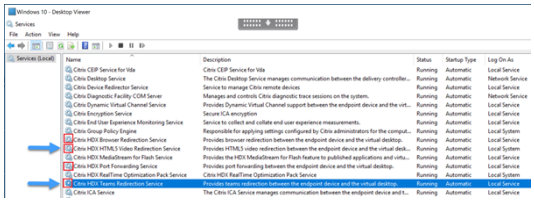
Para obtener más información, consulte *Supervisión* en el artículo CTX253754 de Knowledge Center.

## Solucionar problemas técnicos

En esta sección se proporcionan sugerencias para solucionar problemas que pueden surgir al usar la optimización para Microsoft Teams. Para obtener más información, consulte CTX253754.

### En el Virtual Delivery Agent

Hay cuatro servicios instalados por BCR_x64.msi. Solo dos son responsables de la redirección de Microsoft Teams en el VDA.



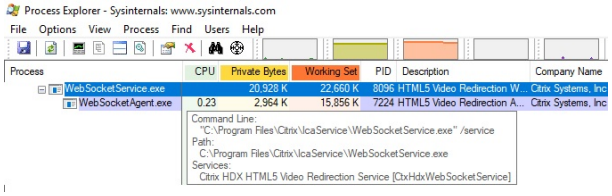
- **Citrix HDX Teams Redirection Service** establece el canal virtual utilizado en Microsoft Teams. El servicio se basa en CtxSvcHost.exe.
- **Citrix HDX HTML5 Video Redirection Service** se ejecuta como WebSocketService.exe y escucha el puerto TCP 127.0.0.1:9002. WebSocketService.exe realiza dos funciones principales:

i. La **finalización de TLS para WebSockets seguros** recibe una conexión WebSocket segura desde vdiCitrixPeerConnection.js, que es un componente de la aplicación Microsoft Teams. Puede hacer un seguimiento de esto con Process Monitor. Para obtener más información sobre los certificados, consulte la sección "TLS, la redirección de vídeo HTML5 y la redirección de contenido del explorador web"en Comunicación entre Controller y VDA.

Algunos antivirus y software de seguridad de escritorio interfieren con el correcto funcionamiento de `WebSocketService.exe` y sus certificados. Aunque es posible que el servicio de Redirección de vídeo HTML5 de Citrix HDX se esté ejecutando en la consola de `services.msc`, el socket TCP de localhost `127.0.0.1:9002` nunca está en modo de escucha como se ve en netstat. Intentar reiniciar el servicio hace que se bloquee ("Deteniendo…"). Asegúrese de que aplica las exclusiones adecuadas para el proceso `WebSocketService.exe`.

ii. **Asignación de sesiones de usuario.** Cuando se inicia la aplicación Microsoft Teams, WebSocketService.exe inicia el proceso WebSocketAgent.exe en la sesión del usuario en el VDA. WebSocketService.exe se ejecuta en la sesión 0 como una cuenta LocalSystem.




Puede utilizar **netstat** para comprobar si el servicio WebSocketService.exe se encuentra en un estado de escucha activa en el VDA.

Ejecute `netstat -anob -p tcp` desde una ventana elevada de símbolo del sistema:

```
 TCP    127.0.0.1:9001         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
 TCP    127.0.0.1:9002         0.0.0.0:0              LISTENING       11740
[WebSocketService.exe]
```

En una conexión correcta, el estado cambia a ESTABLECIDO:

```
 TCP    127.0.0.1:9002         127.0.0.1:58069        ESTABLISHED     8096
[WebSocketService.exe]
 TCP    127.0.0.1:58069        127.0.0.1:9002         ESTABLISHED     748
[Teams.exe]
```

> **Importante:**
>
> WebSocketService.exe escucha dos sockets TCP: 127.0.0.1:9001 y 127.0.0.1:9002. El puerto 9001 se utiliza para la redirección de contenido del explorador y la redirección de vídeo HTML5. El

> puerto 9002 se utiliza para la redirección de Microsoft Teams. No debe tener ninguna configuración de proxy en el sistema operativo Windows del VDA que pueda impedir una comunicación directa entre Teams.exe y WebSocketService.exe. A veces, al configurar un proxy explícito en Internet Explorer 11 (**Opciones de Internet > Conexiones > Configuración de LAN > Servidor proxy**), es posible que las conexiones circulen por un servidor proxy asignado. Compruebe que la opción **Omitir servidor proxy para las direcciones locales** esté activada cuando utilice una configuración de proxy manual y explícita.

**Ubicaciones y descripciones de servicios**

| Servicio | Ruta al archivo ejecutable en el SO de servidor Windows | Iniciar sesión como | Descripción |
|---|---|---|---|
| Servicio de redirección de vídeo para Citrix HTML5 | "C:\Archivos de programa (x86)\Citrix\System32\WebSocketService.exe" /service | Cuenta del sistema local | Proporciona varios servicios HDX Multimedia con el marco inicial necesario para realizar la redirección multimedia entre el escritorio virtual y el dispositivo de punto final. |
| Servicio de redirección de explorador para Citrix HDX | "C:\Archivos de programa (x86)\Citrix\System32\CtxSvcHost.exe" -g BrowserRedirSvcs | Esta cuenta (servicio local) | Permite redirigir el contenido del explorador entre el dispositivo de punto final y el escritorio virtual. |
| Servicio de reenvío de puertos para Citrix | "C:\Archivos de programa (x86)\Citrix\System32\CtxSvcHost.exe" -g PortFwdSvcs | Esta cuenta (servicio local) | Permite reenviar puertos entre el dispositivo de punto final y el escritorio virtual para la redirección de contenido del explorador web. |

| Servicio | Ruta al archivo ejecutable en el SO de servidor Windows | Iniciar sesión como | Descripción |
|---|---|---|---|
| Servicio de redirección de Teams para Citrix HDX | "C:\Archivos de programa (x86)\Citrix\System32\CtxSvcHost.exe" -g TeamsSvcs | Cuenta del sistema local | Permite redirigir Microsoft Teams entre el dispositivo de punto final y el escritorio virtual. |

**Aplicación Citrix Workspace**

En el dispositivo de punto final del usuario, la aplicación Citrix Workspace para Windows crea una instancia de un nuevo servicio denominado HdxTeams.exe. Lo hace cuando Microsoft Teams se inicia en el VDA y el usuario intenta llamar o acceder a los periféricos en la vista previa automática. Si no ve este servicio, compruebe lo siguiente:

1. Debe haber instalado como mínimo la versión 1905 de la aplicación Workspace para Windows. ¿Ve HdxTeams.exe y los binarios de webrpc.dll en la ruta de instalación de la aplicación Workspace?
2. Si validó el paso 1, haga lo siguiente para comprobar si se va a iniciar HdxTeams.exe.
    a) Salga de Microsoft Teams en el VDA.
    b) Inicie services.msc en el VDA.
    c) Detenga Citrix HDX Teams Redirection Service.
    d) Desconecte la sesión ICA.
    e) Conecte la sesión ICA.
    f) Inicie Citrix HDX Teams Redirection Service.
    g) Reinicie Citrix HDX HTML5 Video Redirection Service.
    h) Inicie Microsoft Teams en el VDA.
3. Si aún no ve que HdxTeams.exe se inicia en el dispositivo de punto final del cliente, haga lo siguiente:
    a) Reinicie el VDA.
    b) Reinicie el dispositivo de punto final del cliente.

## Asistencia

Citrix y Microsoft ofrecen soporte conjunto a la entrega de Microsoft Teams desde Citrix Virtual Apps and Desktops mediante la optimización para Microsoft Teams. Este soporte conjunto es el resultado

de una estrecha colaboración entre ambas empresas. Si tiene contratos de soporte válidos y sufre problemas con esta solución, abra un tíquet de asistencia con el proveedor cuyo código sospeche que está causando el problema. Es decir, Microsoft si se trata de Teams o Citrix si se trata de los componentes de optimización.

Citrix o Microsoft reciben el tíquet, evalúan el problema y lo escalan según corresponda. No es necesario que se ponga en contacto con el equipo de asistencia de cada empresa.

Cuando tenga un problema, le recomendamos que haga clic en **Ayuda > Informar de un problema** en la interfaz de usuario de Teams. Los registros del lado del VDA se comparten automáticamente entre Citrix y Microsoft para resolver los problemas técnicos con mayor rapidez.

### Recopilar registros

Los registros del motor de medios HDX se pueden encontrar en la máquina del usuario (no en el VDA). Si ocurre algún problema, adjunte los registros al caso de asistencia técnica.

**Registros de Windows:**

Los registros de Windows se encuentran en %TEMP%, dentro de la carpeta **HDXTeams** (AppData/Local/Temp/HDXTeams o AppData/Local/Temp/HdxRtcEngine). Busque un archivo TXT llamado webrpc_día_mes_hora_año.txt. Si utiliza versiones más recientes de la aplicación Citrix Workspace, por ejemplo, la aplicación Citrix Workspace 2009.5 o una versión posterior, guarde los registros en AppData\Local\Temp\HdxRtcEngine.

Cada sesión crea una carpeta independiente para los registros.

**Registros de Mac:**

1. Registro VDWEBRTC: Registra la ejecución del canal virtual.

   Ubicación /Users/<User Name>/Library/Logs/Citrix Workspace/CitrixViewer_<Y_M_D_H_M_S>.txt

2. Registro HdxRtcEngine: Registra la ejecución de los procesos en HdxRtcEngine.

   Ubicación: $TMPDIR/hdxrtcengine/<W_M_D_H_M_S_Y>/hdxrtcengine.log

   El registro HdxRtcEngine está habilitado de forma predeterminada.

3. Registros de WebRPC: Son los registros más importantes que registran la ejecución del empaquetado de la biblioteca WebRTC.

   Ubicación: /Users/<USERNAME>/Library/Logs/HdxRtcEngine/<W_M_D_H_M_S_Y>/webrpc.log

**Registros de Linux:**

Puede localizar los registros de Linux en las carpetas /tmp/webrpc/<current date>/ and /tmp/hdxrtcengine/<current date>/.
Registro de WebRTC: /tmp/webrpc/<current date>/webrtc.log
Registro del kernel: /var/log/syslog

**Registros ICE/STUN/TURN/:**

Al establecer una llamada, se requieren estas cuatro fases ICE:

- Recopilación de candidatos
- Intercambio de candidatos
- Comprobaciones de conectividad (solicitudes de enlace STUN)
- Promoción de candidatos

En los registros de HdxRtcEngine.exe, las siguientes entradas son las entradas pertinentes del establecimiento interactivo de conectividad (ICE). Estas entradas deben estar allí para que una configuración de llamada se realice correctamente. Consulte el siguiente fragmento de muestra para la fase de recopilación:

```
1  RPCStubs Info: -> device id = \?\display#int3470#4&1835d135&0&uid13424
       #{
2   65e8773d-8f56-11d0-a3b9-00a0c9223196 }
3   {
4   bf89b5a5-61f7-4127-a279-e187013d7caf }
5    label = Microsoft Camera Front groupId =
6
7  webrtcapi.RTCPeerConnection Info: createOffer. audio = 1 video = 1
8  webrtcapi.RTCPeerConnection Info: setLocalDescription.
9  >>> begin:sdp
10 [...]
11
12 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
       HaveLocalOffer
13
14 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
       Gathering
15
16 [...]
17 >>> begin:sdp
18 candidate:840548147 1 udp 2122194687 10.108.124.215 56927 typ host
       generation 0 ufrag oVk6 network-id 1
19 <<< end:sdp
20 [...]
21 >>> begin:sdp
22 candidate:1938109490 1 udp 24911871 52.114.xxx.xxx 52786 typ relay
       raddr 73.205.xxx.x rport 25651 generation 0 ufrag dDML network-id 1
       network-cost 10
23 <<< end:sdp
24 [...]
25 >>> begin:sdp
```

```
26 candidate:4271145120 1 udp 1685987071 66.xxx.xxx.xxx 55839 typ srflx
      raddr 10.108.124.215 rport 55839 generation 0 ufrag uAVH network-id
      1
27 <<< end:sdp
28 [...]
29
30 webrtcapi.RTCPeerConnection Info: OnIceGatheringChange. state =
      Complete webrtcapi.RTCPeerConnection Info: setRemoteDescription.
31 >>> begin:sdp
32 [...]
33
34 webrtcapi.RTCPeerConnection Info: OnSignalingChange. signaling state =
      HaveRemotelOffer
35
36 <!--NeedCopy-->
```

Si hay varios candidatos de ICE, el orden de preferencia es el siguiente:

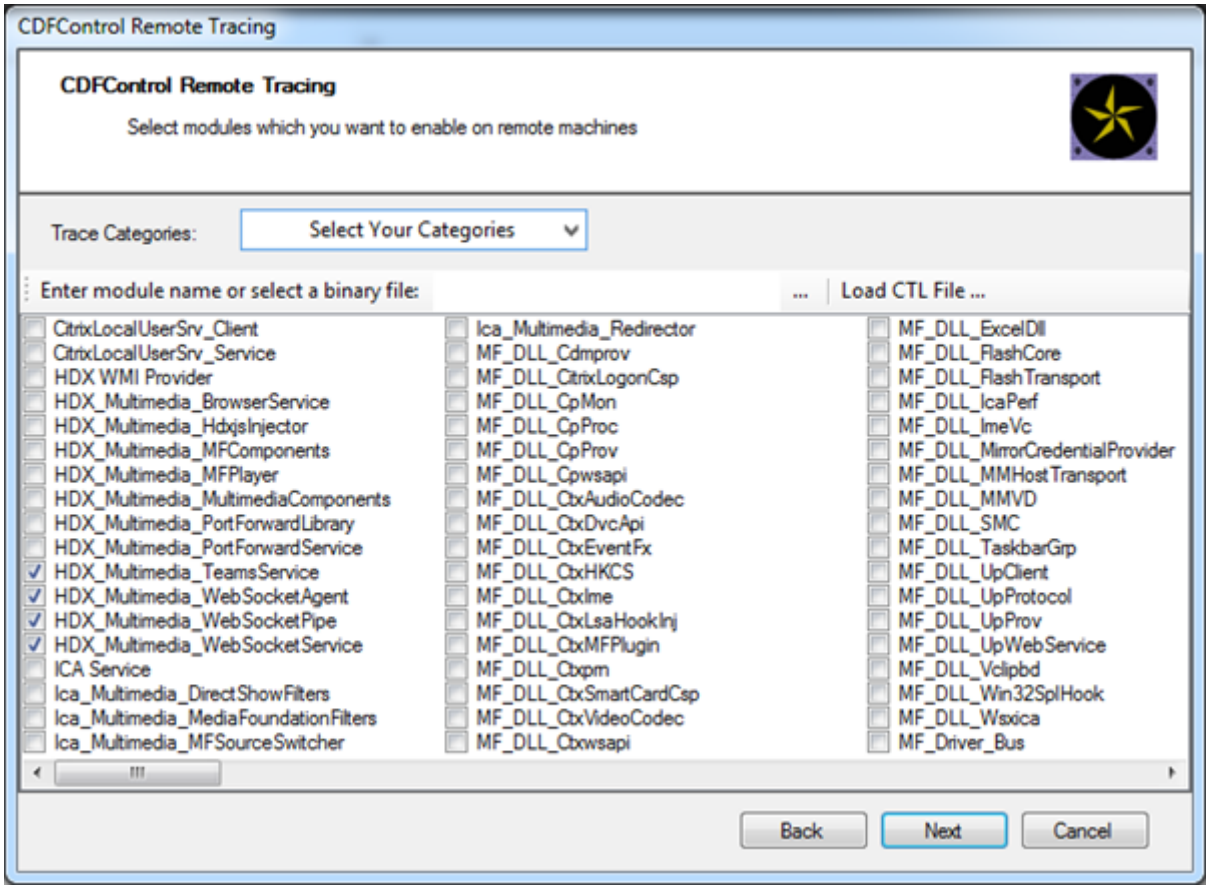
1. host
2. par reflexivo
3. servidor reflexivo
4. traspaso de transporte

Si encuentra un problema y puede reproducirlo, le recomendamos que haga clic en**Ayuda > Informar de un problema** en Teams. Citrix y Microsoft comparten los registros para resolver los problemas técnicos si abre un caso con Microsoft.
La captura de rastros CDF antes de ponerse en contacto con Citrix Support también puede resultar beneficiosa. Para obtener más información, consulte el artículo CDFcontrol de Knowledge Center.

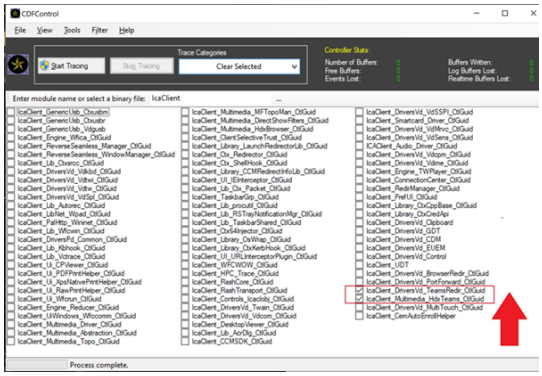
Para obtener recomendaciones para recopilar trazas CDF, consulte el artículo Recommendations for Collecting the CDF Traces de Knowledge Center.

**Rastros CDF del lado de VDA. Habilite los siguientes proveedores de rastros CDF:**




**Rastros CDF del lado de la aplicación Workspace. Habilite los siguientes proveedores de rastros CDF:**



- IcaClient_DriversVd_TeamsRedir (opcional)
- IcaClient_Multimedia_HdxTeams (requiere la aplicación Citrix Workspace 2012 o una versión posterior)

# Redirección de Windows Media

March 30, 2022

La Redirección de Windows Media controla y optimiza el modo en que los servidores entregan a los usuarios sonido y vídeo por streaming. Al reproducir los archivos en tiempo de ejecución multimedia en el dispositivo del usuario y no en el servidor, la Redirección de Windows Media reduce los requisitos de ancho de banda para reproducir archivos multimedia. La Redirección de Windows Media mejora el rendimiento del Reproductor de Windows Media y de los reproductores compatibles que se ejecutan en escritorios virtuales Windows.

Si no se cumplen los requisitos de Windows Media para la obtención de contenido en el cliente, la entrega de contenido multimedia pasa automáticamente a utilizar la obtención en el servidor. Este método es transparente para los usuarios. Puede usar Citrix Scout para rastrear el método utilizado con Citrix Diagnosis Facility (CDF) desde HostMMTransport.dll. Para obtener más información, consulte Citrix Scout.

La Redirección de Windows Media intercepta los procesos multimedia del servidor host, captura los datos multimedia en el formato nativo comprimido y redirige el contenido al dispositivo cliente. A continuación, el dispositivo cliente vuelve a crear los procesos multimedia para descomprimir y generar los datos multimedia recibidos de parte del servidor host. La Redirección de Windows Media funciona bien en dispositivos cliente que ejecutan un sistema operativo Windows. Esos dispositivos disponen del marco multimedia necesario para reconstruir los procesos multimedia que existen en el servidor host. Los clientes Linux usan marcos multimedia similares de código abierto para reconstruir los procesos multimedia.

La configuración **Redirección de Windows Media** controla esta función y está establecida en **Permitida** de forma predeterminada. Por lo general, esta configuración aumenta la calidad de sonido y vídeo que se generan desde el servidor a un nivel comparable al del sonido y el vídeo reproducidos localmente en un dispositivo cliente. En casos contados, la reproducción multimedia con la Redirección de Windows Media resulta ser peor que cuando se genera mediante la compresión básica de ICA y el sonido normal. Para inhabilitar esta función, agregue la configuración **Redirección de Windows Media** a una directiva y establezca su valor en **Prohibida**.

Para obtener más información sobre las configuraciones de directiva, consulte Configuraciones de directiva de Multimedia.

**Limitación:**

Cuando usa Windows Media Player con Remote Audio & Video Extensions (RAVE) habilitado dentro de una sesión, puede aparecer una pantalla en negro. Esta pantalla en negro puede aparecer si hace clic con el botón secundario en el vídeo y selecciona **Reproducción en curso siempre visible**.

# Redirección de contenido general

April 14, 2022

La redirección de contenido permite controlar si los usuarios acceden a la información desde aplicaciones publicadas en servidores o desde aplicaciones que se ejecutan localmente en dispositivos de usuario.

### Redirección de carpetas del cliente

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host.

- Cuando se habilita solo la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention).
- Cuando se habilita la redirección de carpetas del cliente en el servidor y, a continuación, el usuario lo configura en el dispositivo de escritorio Windows, solo se redirige la parte del volumen local que especifique el usuario.

### Redirección del host al cliente

La redirección del host al cliente resulta útil para casos concretos y poco frecuentes. En la mayoría de los casos, existen formas mejores de redirigir el contenido. Solo admitimos este tipo de redirección en los VDA con SO multisesión, y no en los VDA con SO de sesión única.

### Acceso a aplicaciones locales y redirección de URL

El acceso a aplicaciones locales integra sin problemas las aplicaciones de Windows instaladas localmente en un entorno de escritorio alojado. Lo hace sin cambiar de un equipo a otro.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin optimización o cuando esta no es adecuada.

# Redirección de carpetas del cliente

March 30, 2022

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Si se habilita solamente la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention). Cuando se habilita la redirección de carpetas del cliente

en el servidor y, a continuación, el usuario lo configura en el dispositivo de usuario, solo se redirige la parte del volumen local que especifique el usuario.

Solo las carpetas especificadas por el usuario aparecen como enlaces UNC dentro de las sesiones. Es decir, en lugar del sistema de archivos completo en el dispositivo del usuario. Si se inhabilitan los enlaces UNC mediante el Registro, las carpetas del cliente aparecen como unidades asignadas dentro de la sesión.

La redirección de carpetas del cliente solo se admite en máquinas con SO de sesión única Windows.

La redirección de carpetas del cliente para una unidad USB externa no se guarda al desconectar y volver a conectar el dispositivo.

Habilite la redirección de carpetas del cliente en el servidor. Luego, en el dispositivo cliente, especifique qué carpetas redirigir. La aplicación que se utiliza para especificar las opciones de carpeta del cliente está incluida en la aplicación Citrix Workspace proporcionada con esta versión.

**Requisitos:**

Para servidores:

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

Para clientes:

- Windows 10, ediciones de 32 y 64 bits (versión mínima: 1607)
- Windows 8.1, ediciones de 32 y 64 bits (y Embedded)
- Windows 7, ediciones de 32 y 64 bits (incluida la Embedded Edition)

Para habilitar la redirección de carpetas del cliente en el servidor, consulte Redirección de carpetas del cliente en la lista de funciones administradas a través del Registro.

En el dispositivo de usuario, especifique qué carpetas quiere redirigir:

1. Compruebe que está instalada la versión más reciente de la aplicación Citrix Workspace.
2. En el directorio de instalación de la aplicación Citrix Workspace, inicie CtxCFRUI.exe.
3. Seleccione el botón de opción **Personalizada** y agregue, modifique o quite carpetas.
4. Desconecte y vuelva a conectar sus sesiones para que la configuración tenga efecto.

## Configuración de redirección de contenido bidireccional

February 12, 2024

La redirección bidireccional de contenido permite redirigir las URL de un cliente a un servidor o de un servidor a un cliente, según las configuraciones. Esta configuración de directiva reemplaza las tres configuraciones siguientes, que se han retirado:

- Permitir redirección bidireccional de contenido
- Direcciones URL permitidas para redirigir al VDA
- Direcciones URL permitidas para redirigir al cliente

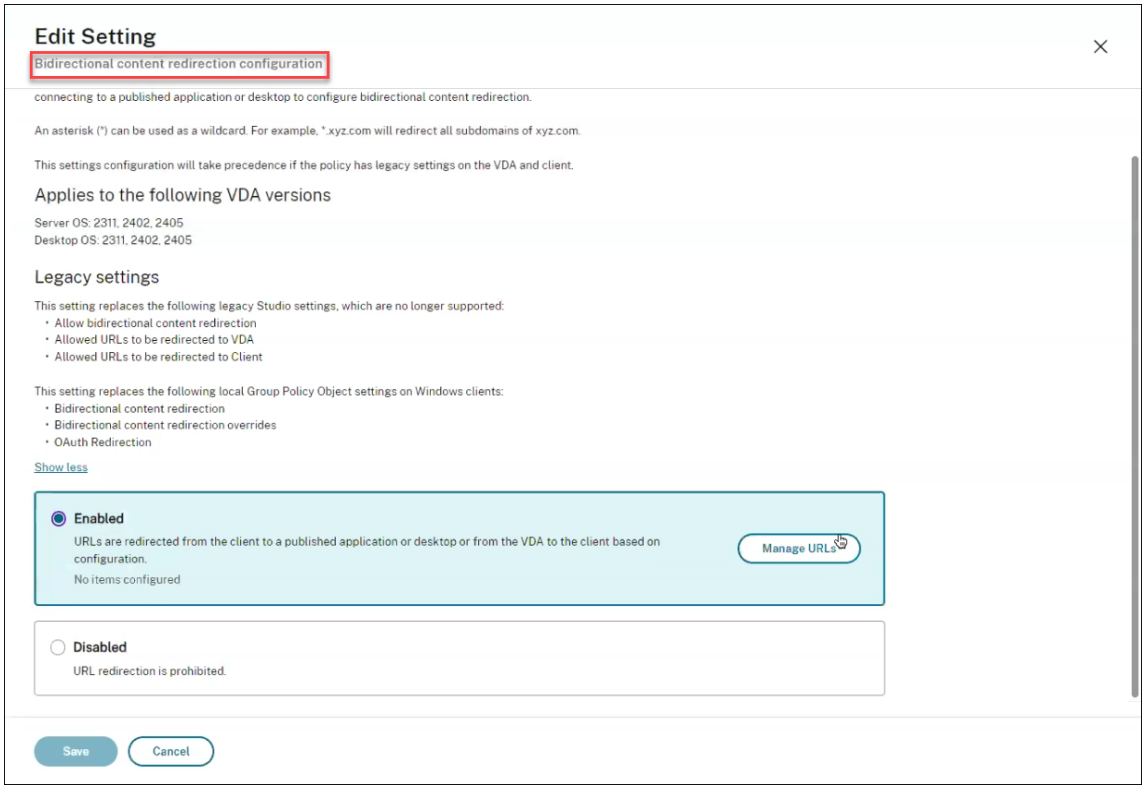
También reemplaza las tres configuraciones de GPO locales siguientes en los clientes de Windows:

- Redirección bidireccional de contenido
- Anulaciones de redirección bidireccional de contenido
- Redirección de OAuth

Si este parámetro está configurado, prevalece sobre la configuración anterior en Studio y en el cliente. Para configurar la directiva de Redirección bidireccional de contenido, haga lo siguiente:

1. En la página de configuración de Citrix DaaS, haga clic en la ficha **Administrar**.
2. Haga clic en la ficha **Directivas**.
3. Haga clic en **Crear directiva**. Se abrirá la hoja **Crear directiva**.
4. Busque `Bidirectional content redirection configuration` en el campo **Buscar**, seleccione la casilla de verificación y haga clic en **Modificar**.
5. En la hoja **Modificar configuración**, configure esta directiva como **Habilitada** y haga clic en **Administrar URL**.




6. En la hoja **Administrar URL**, especifique lo siguiente para la **redirección de VDA a cliente**:

   - **URL** (obligatorio): Agregue la URL que debe redirigirse desde el VDA para que se abra en el cliente. Para la redirección de OAuth, defina el esquema y el patrón de autenticación en el cliente para redirigir la sesión de nuevo al host.
   - **Patrón** (opcional): Expresión regular de URL que, cuando se redirige al cliente mediante la redirección de URL de VDA a cliente, se rastrea como si se hubiera iniciado un flujo de autenticación de OAuth y, cuando el flujo finaliza (lo detecta el esquema resultante o el patrón de URL de redirección que se abre), la URL resultante se redirige de nuevo al VDA host que inició ese flujo.
   - **Esquema** (opcional): Si se especifica un esquema, se espera que la URL de finalización tenga el formato: `scheme://<something>`. Si no se especifica un esquema (está vacío), el patrón de URL original resultante se extrae del patrón a través de un grupo de captura de expresiones regulares (debe especificarse en el patrón) y la URL original se reescribe para usar una URL de redirección de `citrix-oauth-redir://`. Cuando se completa el flujo, la URL de redirección original se redirige de nuevo al host (VDA). En este caso, cualquier servidor de autorización de OAuth debe configurarse para permitir a `citrix-oauth-redir://byIndex/1 (2, 3, ... N)`redireccionar URL.

   > **Nota:**
   >
   > Aunque tanto **Patrón** como **Esquema** son opcionales, si se especifica **Patrón**, también

> debe especificarse **Esquema**.

7. En la hoja **Administrar URL**, especifique lo siguiente para la **redirección del cliente al VDA**:
   - **Tipo**: Elija **Escritorio** o **Aplicación**.
   - **Nombre**: Proporcione un nombre para el tipo.
   - **URL**: Proporcione la URL que quiere redirigir al origen. Puede agregar varias URL y eliminar las que no sean necesarias
8. Haga clic en **Guardar**. La hoja **Modificar configuración** muestra la cantidad de elementos configurados.
9. Haga clic en **Guardar**. La hoja **Crear directiva** muestra el **Valor actual** configurado. Haga clic en **Siguiente**.
10. En el paso **Asignar directiva a**, haga clic en **Siguiente**.
11. En el paso **Resumen**, seleccione la casilla **Habilitar directiva** y escriba un nombre en el campo **Nombre de la directiva**.
12. Haga clic en **Finalizar**. La nueva directiva aparece en la lista.
13. Seleccione la nueva directiva creada para revisar los parámetros configurados.

Para las configuraciones antiguas, consulte Redirección del host al cliente y Redirección bidireccional de contenido.

## Redirección del host al cliente

February 12, 2024

> **Nota:**
>
> En este artículo se describen las configuraciones antiguas de redirección del host al cliente. Para ver las configuraciones más recientes, consulte Configuración de redirección de contenido bidireccional. Las nuevas configuraciones de directiva tendrán prioridad sobre las antiguas. Citrix recomienda usar solo las nuevas configuraciones de directiva y eliminar las antiguas para evitar comportamientos imprevistos.

La redirección del host al cliente permite que las URL, incrustadas como enlaces en las aplicaciones que se ejecutan en una sesión de Citrix, se abran mediante la aplicación correspondiente en el dispositivo de punto final del usuario. Algunos casos de uso comunes para la redirección del host al cliente incluyen:

- Redirección de sitios web en los casos en que el servidor Citrix no tiene acceso a Internet o de red al origen.
- Por motivos de seguridad, rendimiento, compatibilidad o escalabilidad, no se quiere redireccionar los sitios web cuando se ejecuta un explorador web en la sesión de Citrix.
- Redirección de tipos de URL específicos en los casos en que las aplicaciones requeridas para abrir la URL no están instaladas en el servidor Citrix.

La redirección del host al cliente no está pensada para URL a las que accede en una página web o se introducen en la barra de direcciones del explorador web que se ejecuta en la sesión de Citrix. Para obtener información sobre la redirección de URL en exploradores web, consulte Redirección bidireccional de URL o Redirección de contenido del explorador web.

### Requisitos del sistema

- VDA de SO multisesión
- Clientes compatibles:
  - Aplicación Citrix Workspace para Windows
  - Aplicación Citrix Workspace para Mac
  - Aplicación Citrix Workspace para Linux
  - Aplicación Citrix Workspace para HTML5
  - Aplicación Citrix Workspace para Chrome

El dispositivo cliente debe tener instalada y configurada una aplicación para gestionar la redirección de los tipos de URL.

### Configuración

Utilice la directiva de Citrix Redirección del host al cliente para habilitar esta funcionalidad. La **redirección del host al cliente** está inhabilitada de forma predeterminada. Después de habilitar la directiva de redirección del host al cliente, la aplicación Citrix Launcher se registra en el servidor Windows para asegurarse de que puede interceptar URL y enviarlas al dispositivo cliente.

A continuación, deberá configurar la directiva de grupo de Windows para utilizar Citrix Launcher como aplicación predeterminada para los tipos de URL requeridos. En el VDA de servidor Citrix, cree el archivo ServerFTAdefaultPolicy.xml e inserte el siguiente código XML.

```
<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="
    ServerFTA" />
```

```
6
7  <Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName=
       "ServerFTA" />
8
9  </DefaultAssociations>
10 <!--NeedCopy-->
```

En la Consola de administración de directivas de grupo, vaya a **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Explorador de archivos > Definir un archivo de configuración de asociaciones predeterminadas** y guarde el archivo ServerFTAdefaultPolicy.xml.

> **Nota:**
>
> Si un servidor Citrix no tiene la configuración de directiva de grupo, Windows pide a los usuarios que seleccionen una aplicación para abrir las URL.

De forma predeterminada, se admite la redirección de los siguientes tipos de URL:

- HTTP
- HTTPS
- RTSP
- RTSPU
- PNM
- MMS

Para incluir otros tipos de URL estándar o personalizados en la lista para redirección, cree una nueva línea de **identificador de asociación** en el archivo ServerFTAdefaultPolicy.xml al que se hace referencia anteriormente. Por ejemplo:

```
<Association Identifier="ftp"ProgId="ServerFTAHTML"ApplicationName="
ServerFTA"/>
```

```
<Association Identifier="mailto"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype1"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

```
<Association Identifier="customtype2"ProgId="ServerFTAHTML"ApplicationName
="ServerFTA"/>
```

La adición de tipos de URL a la lista también requiere la configuración del cliente. Cree la siguiente clave y valores del Registro en el cliente Windows.

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

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

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Citrix\ICA Client\SFTA
- Nombre del valor: ExtraURLProtocols
- Tipo de valor: REG_SZ
- Información del valor: Especifique los tipos de URL requeridos separados por punto y coma. Incluya todo antes de la sección de autoridad de la URL. Por ejemplo: `ftp://;mailto:;customtype1://;custometype2://`

Puede agregar tipos de URL solo para clientes Windows. Los clientes que faltan en la configuración del registro anterior rechazan el redireccionamiento de vuelta a la sesión de Citrix. El cliente debe tener instalada y configurada una aplicación para gestionar los tipos de URL especificados.

Para quitar tipos de URL de la lista de redirección predeterminada, cree la siguiente clave de Registro y valores en el VDA del servidor.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nombre del valor: DisableServerFTA
- Tipo de valor: DWORD
- Información del valor: 1
- Nombre del valor: NoRedirectClasses
- Tipo de valor: REG_MULTI_SZ
- Información del valor: Especifique cualquier combinación de los valores: `http`, `https`, `rtsp`, `rtspu`, `pnm` o `mms`. Si especifica varios valores, debe ser en líneas independientes. Por ejemplo:

```
http
https
rtsp
```

Para habilitar la redirección del host al cliente para un conjunto específico de sitios web, cree una clave de Registro y valores en el VDA de servidor.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\SFTA
- Nombre del valor: ValidSites
- Tipo de valor: REG_MULTI_SZ
- Información del valor: Especifique una combinación de nombres de dominio completo (FQDN). Si especifica varios nombres de dominio completos, debe ser en líneas independientes. Incluya solo el nombre de dominio completo, sin protocolos (`http://` o `https://`). Un nombre de

dominio completo puede incluir un asterisco (*) como carácter comodín solo a la izquierda. Ese comodín coincide con un único nivel de dominio, lo que es coherente con las reglas de RFC 6125. Por ejemplo:

`www.exmaple.com`

`*.example.com`

> **Nota:**
>
> No se puede utilizar la clave **ValidSites** en combinación con las claves **DisableServerFTA** y **NoRedirectClasses** .

### Configuración predeterminada del explorador del VDA del servidor

Al habilitar la redirección del host al cliente, tal como se hace referencia en esta sección, sustituye cualquier configuración predeterminada anterior del explorador en el VDA del servidor. Si no se redirige una URL web, Citrix Launcher transmite la URL al explorador configurado en la clave de Registro `command_backup`. La clave apunta a Internet Explorer de forma predeterminada, pero puede modificarla para incluir la ruta de acceso a otro explorador. Para obtener más información, consulte Configuración predeterminada del explorador del VDA del servidor en la lista de funciones administradas a través del Registro.

## Redirección bidireccional de contenido

April 18, 2024

> **Nota:**
>
> En este artículo se describen las configuraciones antiguas de la redirección bidireccional de contenido. Para ver las configuraciones de directiva más recientes, consulte Configuración de redirección de contenido bidireccional. Las nuevas configuraciones de directiva tendrán prioridad sobre las antiguas. Citrix recomienda usar solo las nuevas configuraciones de directiva y eliminar las antiguas para evitar comportamientos imprevistos.

La redirección bidireccional de contenido permite que las URL HTTP o HTTPS de los exploradores web, o integradas en aplicaciones, se reenvíen entre la sesión de Citrix VDA y el dispositivo de punto final del cliente en ambas direcciones. Una dirección URL introducida en un explorador que se ejecuta en la sesión de Citrix se puede abrir con el explorador predeterminado del cliente. A la inversa, una URL introducida en un explorador que se ejecuta en el cliente se puede abrir en una sesión de Citrix, ya sea con una aplicación o un escritorio publicados. Algunos casos de uso comunes para la redirección bidireccional de contenido incluyen:

- Redirección de URL web en los casos en que el explorador de inicio no tiene acceso de red al origen.
- Redirección de URL web por motivos de compatibilidad y seguridad del explorador.
- La redirección de URL web incrustadas en aplicaciones cuando se ejecuta un explorador web en la sesión de Citrix o no se quiere el cliente.

### Requisitos del sistema

- VDA para SO de sesión única o multisesión
- Aplicación Citrix Workspace para Windows

Exploradores web:

- Google Chrome con extensión de redireccionamiento de explorador Citrix (disponible en Google Chrome Web Store)
- Microsoft Edge (Chromium) con extensión de redireccionamiento de explorador Citrix (disponible en Google Chrome Web Store)

### Configuración

La redirección bidireccional de contenido debe habilitarse mediante la directiva de Citrix tanto en el VDA como en el cliente para que funcione. La redirección bidireccional de contenido está inhabilitada de forma predeterminada.

Para la configuración del VDA, consulte Redirección bidireccional de contenido en Configuración de directiva de ICA.

Para la configuración del cliente, consulte Redirección bidireccional de contenido en la documentación de la aplicación Citrix Workspace para Windows.

Las extensiones del explorador deben registrarse con los comandos que se muestran. Ejecute los comandos según sea necesario en el VDA y en el cliente en función del explorador en uso.

Para registrar las extensiones del explorador en el VDA, abra un símbolo del sistema. A continuación, ejecute `%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe` con la opción de explorador requerida, como se indica en los siguientes ejemplos:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regIE
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regChrome
```

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regEdge
```

Para registrar la extensión en todos los exploradores disponibles, ejecute:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /regall
```

Para cancelar el registro de una extensión de explorador, use la opción `/unreg<browser>`, como en el ejemplo mostrado:

```
%ProgramFiles(x86)%\Citrix\HDX\bin\vdaredirector.exe /unregIE
```

Para registrar las extensiones de explorador en el cliente, abra un símbolo del sistema y ejecute `%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe` con las mismas opciones que en los ejemplos mostrados.

> **Nota:**
>
> El comando "register"hace que los exploradores Chrome y Edge soliciten a los usuarios que habiliten la extensión de redirección de explorador web Citrix durante el primer inicio. La extensión de explorador también se puede instalar manualmente desde Google Chrome Web Store.

### Redirección con comodines de Citrix VDA al cliente

La redirección bidireccional de contenido admite el uso de comodines al definir las URL que se van a redirigir. Para configurar la redirección bidireccional de contenido, consulte las instrucciones de configuración.

En Citrix Studio, defina la URL comodín en **Direcciones URL permitidas para redirigir al cliente**. El asterisco (*) es el carácter comodín.

> **NOTA:**
>
> - No defina las **Direcciones URL permitidas para redirigir al VDA** en la directiva del cliente. Asegúrese de que los sitios establezcan las **Direcciones URL permitidas para redirigir al VDA** para evitar bucles de redirección infinitos.
> - No se admiten los dominios de nivel superior. Por ejemplo: `https://www.citrix.*` o `http://www.citrix.co*` no se redirigen.

### Redirección de protocolos personalizados del VDA al cliente

La redirección bidireccional de contenido admite la redirección de protocolos personalizados desde el VDA de Citrix al cliente. Se admiten protocolos distintos de HTTP o HTTPS. Para configurar la redirección bidireccional de contenido, consulte las instrucciones de configuración.

En Citrix Studio, defina el protocolo personalizado en **Direcciones URL permitidas para redirigir al cliente**.

> **NOTA:**
>
> - El cliente debe tener una aplicación registrada para gestionar el protocolo. De lo contrario, la URL redirige al cliente y no se inicia.

> - Las URL de protocolo personalizado que introduce o inicia en los exploradores Chrome y Edge no son compatibles ni se redirigen.
> - No se admiten los siguientes protocolos: `rtsp://, rtspu://, pnm://, mms://`.

### Otras consideraciones

- Los requisitos y configuraciones de explorador solo se aplican al explorador que inicia la redirección. El explorador de destino, en el que se abre la URL una vez que ha tenido lugar la redirección, no se tiene en cuenta. Al redirigir las URL desde el VDA a un cliente, solo se requiere una configuración de explorador compatible en el VDA. A la inversa, al redirigir las URL desde el cliente a un VDA, solo se requiere una configuración de explorador compatible en el cliente. Las URL redirigidas se transfieren al explorador predeterminado configurado en la máquina de destino, ya sea el cliente o el VDA, según la dirección. NO es necesario usar el mismo tipo de explorador en el VDA y en el cliente.
- Compruebe que las reglas de redirección no resultan en un bucle. Por ejemplo: si se establece una directiva de VDA para redirigir `https://www.citrix.com` y la directiva de cliente está establecida para redirigir esa misma URL, se produce un bucle infinito.
- Solo se admiten las URL con protocolo HTTP/HTTPS. No se admiten acortadores de URL.
- La redirección de cliente a VDA requiere que el cliente Windows se instale con derechos de administrador.
- Si el explorador de destino ya está abierto, la URL redirigida se abre en una nueva ficha. De lo contrario, la URL se abre en una nueva ventana de explorador.
- La redirección bidireccional de contenido no funciona cuando el acceso a aplicaciones locales (LAA) está habilitado.

## Acceso a aplicaciones locales y redirección de URL

June 15, 2022

### Introducción

La función Acceso a aplicaciones locales integra perfectamente las aplicaciones Windows instaladas localmente en un entorno de escritorio alojado sin cambiar de un escritorio a otro. Con la función Acceso a aplicaciones locales, puede:

- Acceder a las aplicaciones instaladas localmente en un equipo portátil, un PC u otro dispositivo físico, directamente desde el escritorio virtual.

- Proporcionar una solución flexible para la entrega de aplicaciones. Si los usuarios disponen de aplicaciones locales que no se pueden virtualizar o que el departamento de TI no mantiene, dichas aplicaciones se comportan como si estuvieran instaladas en un escritorio virtual.
- Eliminar la latencia de doble salto que se produce cuando las aplicaciones no están alojadas en el escritorio virtual. Para ello, ponga un acceso directo a la aplicación publicada en el dispositivo Windows del usuario.
- Usar aplicaciones como:
  - Videoconferencia; por ejemplo, GoToMeeting.
  - Aplicaciones nicho o especializadas que aún no están virtualizadas.
  - Aplicaciones y periféricos que de otro modo transferirían grandes cantidades de datos desde un dispositivo de usuario a un servidor y de vuelta al dispositivo del usuario. Por ejemplo, grabadoras de DVD y sintonizadores de TV.

En Citrix Virtual Apps and Desktops, las sesiones de escritorio alojado usan la redirección de URL para iniciar aplicaciones de acceso local. La función Redirección de URL permite que la aplicación esté disponible en más de una URL. Inicia un explorador local (basado en la lista de URL bloqueadas de su explorador) tras seleccionar enlaces insertados en un explorador en una sesión de escritorio. Si va a una URL que no está en la lista de URL bloqueadas, esa URL se vuelve a abrir en la sesión de escritorio.

La función Redirección de URL solo funciona en sesiones de escritorio, no las sesiones de aplicación. La única función de redirección que puede usar para sesiones de aplicación es la redirección de contenido de host a cliente, que es un tipo de redirección FTA (asociación de tipos de archivo) para servidor. Esta FTA redirige ciertos protocolos al cliente, como HTTP, HTTPS, RTSP o MMS. Por ejemplo, si abre enlaces insertados solo con HTTP, estos se abren directamente con la aplicación cliente. No se admiten ni la lista de URL permitidas ni la de URL bloqueadas.

Cuando el acceso a aplicaciones locales está habilitado, las direcciones URL que se muestran a los usuarios como enlaces desde aplicaciones ejecutadas localmente, desde aplicaciones alojadas por el usuario o como accesos directos en el escritorio se redirigen de una de las siguientes maneras:

- Desde el equipo del usuario al escritorio alojado
- Desde el servidor de Citrix Virtual Apps and Desktops al equipo del usuario
- Generadas en el entorno donde se abren (no redirigidas)

Para especificar la ruta de redirección de contenido desde sitios web específicos, configure la lista de URL permitidas y la lista de URL bloqueadas en el Virtual Delivery Agent. Estas listas contienen claves de Registro de cadena múltiple que especifican la configuración de la directiva Redirección de URL. Para obtener más información, consulte las configuraciones de directiva de Acceso a aplicaciones locales.

Las direcciones URL pueden generarse en el VDA, con las siguientes excepciones:

- Configuración regional y geográfica. Los sitios web que requieren configuración regional, como msn.com o news.google.com (abre la página de un país concreto, basada en la ubicación geográfica). Por ejemplo: si el VDA se aprovisionó desde un centro de datos en el Reino Unido y el cliente se conecta desde la India, el usuario espera ver in.msn.com. Sin embargo, el usuario ve uk.msn.com.
- Contenido multimedia. Los sitios web con contenido multimedia que, cuando se generan en el dispositivo cliente, ofrecen una experiencia nativa a los usuarios finales y ahorran ancho de banda incluso en redes de latencia alta. Esta función redirige sitios con otros tipos de contenido multimedia, como Silverlight. Este proceso se realiza en un entorno seguro. Es decir, las direcciones URL que el administrador haya aprobado se ejecutan en el cliente, mientras que el resto de las direcciones URL se redirigen al VDA.

Además de la redirección de URL, también puede utilizar la redirección de asociación de tipos de archivo (FTA). FTA inicia aplicaciones locales cuando se encuentra un archivo en la sesión. Si se inicia la aplicación local, esta debe tener acceso al archivo para abrirlo. Por lo tanto, solo puede abrir archivos que residen en recursos compartidos de red o en las unidades del cliente (mediante la asignación de unidades del cliente) con aplicaciones locales. Por ejemplo, cuando se abre un archivo PDF, si un lector de PDF es una aplicación local, el archivo se abre con ese lector de PDF. Debido a que la aplicación local puede acceder al archivo directamente, este no se transfiere por la red a través de ICA para abrirse.

### Requisitos, consideraciones y limitaciones

Acceso a aplicaciones locales recibe soporte en los sistemas operativos válidos para los VDA de SO multisesión Windows y los VDA de SO de sesión única Windows. Acceso a aplicaciones locales requiere la aplicación Citrix Workspace para Windows 4.1 (versión mínima). Se admiten los siguientes exploradores web:

- Edge, la versión más reciente
- Firefox, la versión más reciente y la versión de asistencia extendida
- Chrome, la versión más reciente

Tenga en cuenta las siguientes consideraciones y limitaciones al usar las funciones Acceso a aplicaciones locales y Redirección de URL.

- La función Acceso a aplicaciones locales está diseñada para escritorios virtuales en pantalla completa expandida a todos los monitores:
  - Si la función Acceso a aplicaciones locales se usa con un escritorio virtual que se ejecuta en modo de ventana o no se expande por todos los monitores, la experiencia de usuario puede ser confusa.

  - Varios monitores: Si uno de ellos está maximizado, se convierte en el escritorio predeterminado de todas las aplicaciones que se inician en esa sesión. Este comportamiento predeterminado se da aunque las aplicaciones posteriores se iniciaran habitualmente en otro monitor.
  - Esta función admite un solo VDA. No hay integración con varios VDA simultáneos.

- Algunas aplicaciones pueden funcionar de manera inesperada, afectando a los usuarios:
  - Las letras de unidad pueden resultar confusas; por ejemplo, C: local, en lugar de C: del escritorio virtual.
  - Las impresoras disponibles en el escritorio virtual no están disponibles para las aplicaciones locales.
  - Las aplicaciones que requieren permisos elevados no se pueden iniciar como aplicaciones alojadas en el cliente.
  - No hay tratamiento especial para aplicaciones de una sola instancia (como el Reproductor de Windows Media).
  - Las aplicaciones locales aparecen con el tema de Windows de la máquina local.
  - No se admiten las aplicaciones de pantalla completa. Estas aplicaciones pueden ser aquellas que se abren en el modo de pantalla completa, como las presentaciones con diapositivas de PowerPoint o los visores de fotos que ocupan todo el escritorio.
  - La función Acceso a aplicaciones locales copia al VDA las propiedades de la aplicación local (como los accesos directos en el escritorio del cliente y el menú Inicio). No obstante, no copia otras propiedades, como las teclas de acceso directo y los atributos de solo lectura.
  - Las aplicaciones que personalizan cómo se trata el orden de las ventanas superpuestas pueden mostrar resultados impredecibles. Por ejemplo, es posible que algunas ventanas estén ocultas.
  - No se admiten los accesos directos, incluidos los de Mi PC, Papelera de reciclaje, Panel de control, Unidad de red y carpetas.
  - Los siguientes archivos y tipos de archivo no se admiten: tipos de archivo personalizados, archivos que no están asociados a ningún programa, archivos ZIP y archivos ocultos.
  - La agrupación de la barra de tareas no recibe soporte en caso de aplicaciones alojadas en el cliente o aplicaciones del VDA que combinan 32 bits y 64 bits. Es decir, la agrupación de aplicaciones locales de 32 bits con aplicaciones de VDA de 64 bits.
  - Las aplicaciones no se pueden iniciar con COM. Por ejemplo: si hace clic en un documento de Office incrustado desde una aplicación de Office, el inicio del proceso no se puede detectar y falla la integración de la aplicación local.

- Los escenarios de doble salto, en los que un usuario inicia un escritorio virtual desde otra sesión de escritorio virtual, no se admiten.
- La función Redirección de URL solo admite direcciones URL explícitas (es decir, aquellas que aparecen en la barra de direcciones del explorador o las que se encuentran navegando dentro

del explorador, según el explorador que se esté utilizando).
- Redirección de URL solo funciona con sesiones de escritorio, no con sesiones de aplicación.
- La carpeta de escritorio local en una sesión de VDA no permite que los usuarios creen archivos.
- Varias instancias de una aplicación que se ejecuta localmente se comportan de acuerdo con la configuración de barras de tareas establecida para el escritorio virtual. Sin embargo, los accesos directos de aplicaciones ejecutadas localmente no se agrupan con las instancias en ejecución de esas aplicaciones. Tampoco se agrupan con instancias en ejecución de aplicaciones alojadas ni con los accesos directos anclados a aplicaciones alojadas. Los usuarios solo pueden cerrar las ventanas de las aplicaciones que se ejecutan localmente desde la barra de tareas. Si bien los usuarios pueden anclar las ventanas de las aplicaciones locales a la barra de tareas del escritorio y al menú Inicio, es posible que las aplicaciones no se inicien de forma consistente cuando se usen estos accesos directos.
- Si **habilita** la configuración de directiva **Permitir acceso a aplicaciones locales**, no se admite la redirección de contenido del explorador web.

### Interacción con Windows

La interacción de la función Acceso a aplicaciones locales con Windows incluye los siguientes comportamientos.

- Comportamiento de los accesos directos en Windows 8 y Windows Server 2012
  - Las aplicaciones de la Tienda Windows instaladas en el cliente no se indican en la lista de accesos directos de la función Acceso a aplicaciones locales.
  - Los archivos de imagen y vídeo se abren de forma predeterminada con las aplicaciones de la Tienda Windows. Sin embargo, la función Acceso a aplicaciones locales enumera las aplicaciones de la Tienda Windows y abre los accesos directos con aplicaciones de escritorio.
- Programas locales
  - Para Windows 7, la carpeta está disponible en el menú Inicio.
  - Para Windows 8, Programas locales solo está disponible si el usuario selecciona **Todas las aplicaciones** como una categoría desde la pantalla de Inicio. No se muestran todas las subcarpetas en Programas locales.
- Funciones de elementos gráficos de Windows 8 para aplicaciones
  - Las aplicaciones de escritorio están limitadas al área del escritorio y las cubren la pantalla Inicio y las aplicaciones de estilo de Windows 8.
  - Las aplicaciones de acceso local no se comportan como aplicaciones de escritorio cuando se tienen varios monitores. En el modo de varios monitores, la pantalla de Inicio y el escritorio se muestran en monitores diferentes.

- Windows 8 y redirección de URL de acceso a aplicaciones locales
  - Como el Internet Explorer de Windows 8 no tiene complementos habilitados, use el Internet Explorer de escritorio para habilitar la redirección de URL.
  - En Windows Server 2012, Internet Explorer inhabilita los complementos de forma predeterminada. Para implementar la redirección de URL, inhabilite la configuración mejorada de Internet Explorer. A continuación, restablezca las opciones de Internet Explorer y reinicie el programa para asegurarse de que los complementos están habilitados para los usuarios estándar.

## Configurar el acceso a aplicaciones locales y la redirección de URL

Para usar las funciones Acceso a aplicaciones locales y Redirección de URL con la aplicación Citrix Workspace:

- Instale la aplicación Citrix Workspace en la máquina cliente local. Puede habilitar ambas funciones durante la instalación de la aplicación Citrix Workspace, o bien, puede habilitar la plantilla de Acceso a aplicaciones locales mediante el Editor de directivas de grupo.
- Establezca la configuración de directiva **Permitir acceso a aplicaciones locales** como **Habilitada**. También puede configurar la lista de URL permitidas y la lista de URL bloqueadas para la redirección de URL. Para obtener más información, consulte Configuraciones de directiva de Acceso a aplicaciones locales.

### Habilitar el acceso a aplicaciones locales y la redirección de URL

Para habilitar el acceso a aplicaciones locales para todas las aplicaciones locales, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Directivas** en el panel de la izquierda.
2. Seleccione **Crear directiva** en la barra de acciones.
3. En la ventana Crear directiva, escriba "Permitir acceso a aplicaciones locales"en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**.
4. En la ventana Modificar parámetros, seleccione **Permitido**. De forma predeterminada, la directiva **Permitir acceso a aplicaciones locales** está prohibida. Con esta configuración habilitada, el VDA permite que el cliente decida si se habilitan los accesos directos de acceso a aplicaciones locales y aplicaciones publicadas por el administrador de cara a la sesión (si esta configuración está prohibida, no funcionan en el VDA ni los accesos directos de Acceso a aplicaciones locales ni las aplicaciones publicadas). Esta configuración de directiva se aplica a toda la máquina y a la directiva Redirección de URL.
5. En la ventana Crear directiva, escriba "Lista de redirección de URL permitidas"en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**. La lista de permitidos para la redirección

de URL especifica las URL que se pueden abrir en el explorador predeterminado de la sesión remota.

6. En la ventana Modificar configuración, haga clic en **Agregar** para agregar las URL y, a continuación, haga clic en **Aceptar**.
7. En la ventana Crear directiva, escriba "Lista de redirección de URL bloqueadas"en el cuadro de búsqueda y, a continuación, haga clic en **Seleccionar**. La lista de bloqueados de redirección de URL especifica las URL que se redirigen al explorador predeterminado que se ejecuta en el dispositivo de punto final.
8. En la ventana Modificar configuración, haga clic en **Agregar** para agregar las URL y, a continuación, haga clic en **Aceptar**.
9. En la página Parámetros, haga clic en **Siguiente**.
10. En la página Usuarios y máquinas, asigne la directiva a los grupos de entrega correspondientes y, a continuación, haga clic en **Siguiente**.
11. En la página Resumen, revise los parámetros y, a continuación, haga clic en **Finalizar**.

Para habilitar la redirección de URL en todas las aplicaciones locales durante la instalación de la aplicación Citrix Workspace, siga estos pasos:

1. Habilite y la redirección de URL durante la instalación de la aplicación Citrix Workspace para todos los usuarios de una máquina. Al hacerlo, también se registran los complementos del explorador necesarios para la redirección de URL.
2. En el símbolo del sistema, ejecute el comando apropiado para instalar la aplicación Citrix Workspace con una de las opciones siguientes:

    - Para CitrixReceiver.exe, utilice `/ALLOW_CLIENTHOSTEDAPPSURL=1`.
    - Para CitrixReceiverWeb.exe, utilice `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

#### Habilitar la plantilla de acceso a aplicaciones locales mediante el Editor de directivas de grupo

> **Nota:**
>
> - Antes de habilitar la plantilla de acceso a aplicaciones locales mediante el Editor de directivas de grupo, agregue los archivos de plantilla `receiver.admx/adml` al GPO local. Para obtener más información, consulte Introducción y busque *plantilla administrativa de objetos de directiva de grupo*.
> - Los archivos de plantilla de la aplicación Citrix Workspace para Windows están disponibles en el GPO local, en la carpeta **Plantillas administrativas > Componentes de Citrix > Citrix Workspace** solamente al agregar `CitrixBase.admx/CitrixBse.adml` a la carpeta %systemroot%\policyDefinitions.

Para habilitar la plantilla de acceso a aplicaciones locales mediante el Editor de directivas de grupo, siga estos pasos:

1. Ejecute **gpedit.msc**.
2. Vaya a **Configuración del equipo > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
3. Haga clic en **Configuración del acceso a aplicaciones locales**.
4. Seleccione **Habilitada** y, a continuación, seleccione **Permitir redirección de URL**. Para la redirección de URL, registre los complementos del explorador web desde la línea de comandos, como se describe en la sección *Registro de complementos del explorador web* que aparece más abajo en este artículo.

#### Proporcionar acceso solo a las aplicaciones publicadas

Puede proporcionar acceso a las aplicaciones publicadas mediante el Editor del Registro o el SDK de PowerShell.

Para el Editor del Registro, consulte Acceso a aplicaciones locales para aplicaciones publicadas en la lista de funciones administradas a través del Registro.

Para usar el SDK de PowerShell.

1. Abra PowerShell en la máquina donde se ejecuta el Delivery Controller.
2. Escriba el siguiente comando: `set-configsitemetadata -name "studio_clientHostedApps"-value "true"`.

Para tener acceso a **Agregar aplicación de acceso local** en una implementación de Citrix DaaS, use el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops. Para obtener más información, consulte SDK de PowerShell remoto de Citrix Virtual Apps and Desktops.

1. Descargue el instalador:

   https://download.apps.cloud.com/CitrixPoshSdk.exe

2. Ejecute estos comandos:

   a) `asnp citrix.*`
   b) `Get-XdAuthentication`

3. Escriba el siguiente comando: `set-configsitemetadata -name “studio_clientHostedAppsI” -value “true”`.

Después de completar los pasos correspondientes anteriores, siga estos pasos para continuar.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda.
2. En el panel central superior, haga clic con el botón secundario en el área vacía y seleccione **Agregar aplicación de acceso local** en el menú. También puede hacer clic en **Agregar aplicación**

**de acceso local** en el panel Acciones. Para mostrar la opción Agregar aplicación de acceso local en el panel Acciones, haga clic en **Actualizar**.

3. Publique aplicaciones de acceso local.

    - El asistente de acceso a aplicaciones locales se inicia con una página introductoria, la cual se puede eliminar de futuros inicios de este asistente.
    - El asistente le guiará a través de las páginas Grupos, Ubicación, Identificación, Entrega y Resumen que se describen a continuación. Cuando haya terminado con cada página, haga clic en **Siguiente** para ir a la página Resumen.
    - En la página Grupos, seleccione uno o varios grupos de entrega donde se agregarán las nuevas aplicaciones y, a continuación, haga clic en **Siguiente**.
    - En la página Ubicación, escriba toda la ruta ejecutable de la aplicación que hay en la máquina local del usuario y, también, la ruta a la carpeta donde se encuentra la aplicación. Citrix recomienda utilizar la ruta con variables de entorno del sistema; por ejemplo, %ProgramFiles(x86)%\Internet Explorer\iexplore.exe.
    - En la página Identificación, acepte los valores predeterminados o escriba la información que quiera y, a continuación, haga clic en **Siguiente**.
    - En la página Entrega, configure cómo se entregará esta aplicación a los usuarios y, a continuación, haga clic en **Siguiente**. Puede especificar el icono de la aplicación seleccionada. También puede indicar si el acceso directo a la aplicación local en el escritorio virtual estará visible en el menú Inicio, en el escritorio o en ambos.
    - En la página Resumen, revise los parámetros y, a continuación, haga clic en **Finalizar** para salir del asistente de acceso a aplicaciones locales.

#### Registrar complementos del explorador web

> **Nota:**
>
> Los complementos del explorador web necesarios para la redirección de URL se registran automáticamente al instalar la aplicación Citrix Workspace desde la línea de comandos con la opción `/ALLOW_CLIENTHOSTEDAPPSURL=1`.

Puede usar los siguientes comandos para registrar y cancelar el registro de uno o todos los complementos:

- Para registrar complementos en un dispositivo cliente: *<carpeta de instalación del cliente>*\redirector.exe /reg*<explorador>*
- Para cancelar el registro de complementos en un dispositivo cliente: *<carpeta de instalación del cliente>*\redirector.exe /unreg*<explorador>*

- Para registrar complementos en un VDA: <*carpeta de instalación del VDA*>\VDARedirector.exe /reg<*explorador*>
- Para cancelar el registro de complementos en un VDA: <*carpeta de instalación del VDA*>\VDARedirector.exe /unreg<*explorador*>

Donde <*explorador*> es Internet Explorer, Firefox, Chrome o Todo.

Por ejemplo, el siguiente comando registra complementos de Internet Explorer en un dispositivo que ejecuta la aplicación Citrix Workspace.

C:\Archivos de programa\Citrix\ICA Client\redirector.exe/regIE

El siguiente comando registra todos los complementos en un VDA para sistemas operativos multisesión Windows.

C:\Archivos de programa (x86)\Citrix\HDX\bin\VDARedirector.exe /regAll

#### Interceptación de URL entre exploradores web

- De manera predeterminada, Internet Explorer redirige la dirección URL que se haya introducido. Si la URL no está en la lista de bloqueados, pero el explorador o el sitio web la redirigen a otra URL, la URL final no se redirige. No se redirige incluso aunque esté en la lista de bloqueados.

Para que la redirección de URL funcione correctamente, habilite el complemento cuando lo solicite el explorador web. Si se inhabilitan los complementos que usan las opciones de Internet o los que pide el sistema, la redirección de URL no funciona correctamente.

- Los complementos de Firefox siempre redirigen las direcciones URL.

Cuando se instala un complemento, Firefox pide confirmación para permitir o impedir la instalación del complemento en una página de nueva pestaña. Permita el complemento para poder usar esta función.

- El complemento de Chrome siempre redirige la URL final de navegación y no las direcciones URL introducidas.

Las extensiones han sido instaladas externamente. Al inhabilitar la extensión, la función Redirección de URL no funciona en Chrome. Si se necesita la redirección de URL en modo de incógnito, permita que la extensión se ejecute en ese modo en la Configuración del explorador.

#### Configurar el comportamiento de la aplicación local al cerrar sesión y al desconectar

> **Nota:**
>
> Si no sigue estos pasos para configurar los parámetros, de forma predeterminada las aplica-

> ciones locales siguen ejecutándose cuando un usuario cierra la sesión o se desconecta del escritorio virtual. Tras la reconexión, las aplicaciones locales vuelven a integrarse si están disponibles en el escritorio virtual.

Para configurar el comportamiento de la aplicación local al cerrar sesión y al desconectar, consulte Comportamiento de la aplicación local al cerrar sesión y al desconectar en la lista de funciones administradas a través del Registro.

## Consideraciones sobre unidades del cliente y redirección de USB genérico

April 18, 2024

La tecnología HDX ofrece **optimización** con los dispositivos USB más comunes. La optimización ofrece una experiencia de usuario mejorada, con mejor rendimiento y eficiencia del ancho de banda en una conexión por red WAN. La optimización suele ser la mejor opción, sobre todo en entornos de alta latencia o cuando se requiera confidencialidad.

La tecnología HDX ofrece la **redirección de USB genérico** para dispositivos específicos sin optimización o cuando esta no es adecuada; por ejemplo:

- El dispositivo USB tiene otras funciones avanzadas que no forman parte de la optimización, como mouse o cámaras web con botones adicionales.
- Los usuarios necesitan funciones que no forman parte de la optimización.
- Los dispositivos USB es un dispositivo especializado, como un equipo de pruebas o mediciones, o bien un automatismo industrial.
- Una aplicación requiere acceso directo al dispositivo como dispositivo USB.
- El dispositivo USB solo tiene disponible un controlador Windows. Por ejemplo, un lector de tarjetas inteligentes puede no tener disponible un controlador para la aplicación Citrix Workspace para Android.
- La versión de la aplicación Citrix Workspace no ofrece ninguna optimización para este tipo de dispositivo USB.

Con la redirección de USB genérico:

- Los usuarios no necesitan instalar controladores de dispositivos en el dispositivo de usuario.
- Los controladores de cliente de USB se instalan en la máquina del VDA.

> **Importante:**
>
> - La redirección de USB genérico puede utilizarse junto con la optimización. Si habilita la

redirección USB genérica, configure las directivas de dispositivos USB de Citrix tanto para la redirección USB genérica como para la funcionalidad optimizada.
- La configuración de directiva en Reglas de optimización de dispositivos USB del cliente de Citrix es una configuración específica para la redirección de USB genérico, para un determinado de dispositivo USB. No se aplica a la optimización que se describe aquí.
- Al hacer de intermediario de una sesión mediante el software de Citrix con una máquina virtual de Azure, Citrix proporciona el máximo soporte para la redirección USB a la máquina virtual de Azure. Ofrecemos soporte para la solución de problemas del software de Citrix, pero no para la máquina virtual de Azure subyacente.
- Los dispositivos CD/DVD con capacidad de grabación de discos se pueden redirigir, pero no se pueden utilizar las capacidades de grabación de estos dispositivos. Esto se debe a los límites de búfer de una sesión.

### Consideraciones de rendimiento para dispositivos USB

Con la redirección de USB genérico, para algunos tipos de dispositivos USB, la latencia de red y el ancho de banda pueden afectar a la experiencia de usuario y al funcionamiento del dispositivo USB. Por ejemplo: es posible que los dispositivos que tengan en cuenta el tiempo no funcionen correctamente en conexiones con enlaces de alta latencia y poco ancho de banda. En su lugar, se usa la optimización, si es posible.

Algunos dispositivos USB requieren mucho ancho de banda para poderse usar, por ejemplo, un mouse 3D (se usa con aplicaciones 3D que también suelen requerir una gran cantidad de ancho de banda). Si no se puede aumentar el ancho de banda, es posible que pueda mitigar el problema ajustando el uso del ancho de banda de otros componentes mediante las configuraciones de directiva de ancho de banda. Para obtener más información, consulte Configuraciones de directiva de Ancho de banda para la redirección de dispositivos USB del cliente y Configuraciones de directiva de Conexiones de multisecuencia.

### Consideraciones de seguridad para dispositivos USB

Algunos dispositivos USB implican el uso de información confidencial por naturaleza; por ejemplo, los lectores de tarjetas inteligentes, los lectores de huellas digitales y los paneles táctiles de firma electrónica. Otros dispositivos USB, como los dispositivos de almacenamiento USB, se pueden usar para la transmisión de datos confidenciales.

Los dispositivos USB se utilizan con frecuencia para distribuir software malicioso (malware). Configurar la aplicación Citrix Workspace y Citrix Virtual Apps and Desktops puede reducir (pero no eliminar) el riesgo proveniente de esos dispositivos USB. Esta situación se aplica cuando se utiliza la optimización o la redirección de USB genérico.

> **Importante:**
>
> En caso de dispositivos y datos confidenciales, proteja siempre la conexión HDX mediante TLS o IPsec.
>
> Habilite solo los dispositivos USB que necesite. Configure la redirección de USB genérico y la optimización para ello.
>
> Proporcione instrucciones a los usuarios para el uso seguro de dispositivos USB:
>
> - Usar solo dispositivos USB que se hayan obtenido de una fuente fiable.
> - No dejar los dispositivos USB desatendidos en entornos abiertos (por ejemplo, una unidad flash en un cibercafé).
> - Explique los riesgos de usar un dispositivo USB en más de un equipo.

### Compatibilidad con la redirección de USB genérico

La redirección de USB genérico se admite en dispositivos USB 2.0 y versiones anteriores. También se admite la redirección de USB genérico en dispositivos USB 3.0 conectados a puertos USB 2.0 o USB 3.0. En cambio, la redirección de USB genérico no admite las funciones de USB introducidas en USB 3.0 tales como la velocidad extra.

Estas aplicaciones Citrix Workspace admiten la redirección de USB genérico:

- Aplicación Citrix Workspace para Windows; consulte Configurar la entrega de aplicaciones
- Aplicación Citrix Workspace para Mac; consulte Aplicación Citrix Workspace para Mac.
- Aplicación Citrix Workspace para Linux; consulte Optimizar
- Aplicación Citrix Workspace para Chrome OS; consulte Aplicación Citrix Workspace para Chrome

Para ver las versiones de la aplicación Citrix Workspace, consulte Tabla de funciones de la aplicación Citrix Workspace.

Si usa versiones anteriores de la aplicación Citrix Workspace, consulte la documentación de la aplicación Citrix Workspace para ver si se admite la redirección de USB genérico. Consulte la documentación de la aplicación Citrix Workspace para ver las limitaciones de los tipos de dispositivos USB que se admiten.

La redirección de USB genérico se admite en sesiones de escritorio a partir de la versión 7.6 del VDA para SO de sesión única hasta la versión actual.

La redirección de USB genérico se admite en sesiones de escritorio a partir de la versión 7.6 del VDA para SO multisesión hasta la versión actual con las siguientes restricciones:

- El VDA debe estar ejecutándose en Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 o Windows Server 2022.

- Los controladores del dispositivo USB deben ser compatibles con el host de sesión de Escritorio remoto (RDSH) para el SO del VDA (Windows 2012 R2), incluida la virtualización al completo.

A continuación, se ofrecen algunos tipos de dispositivos USB que no se admiten para la redirección de USB genérico porque no sería útil redirigirlos:

- Módems USB.
- Adaptadores de red USB.
- Concentradores USB. Los dispositivos USB conectados a los concentradores USB se administran de forma individual.
- Puertos USB COM virtuales. Use la redirección de puertos COM en lugar de la redirección de USB genérico.

Para obtener información acerca de los dispositivos USB que se han probado con la redirección de USB genérico, consulte Citrix Ready Marketplace. Algunos dispositivos USB no funcionan correctamente con la redirección de USB genérico.

### Configurar la redirección de USB genérico

Puede decidir los tipos de dispositivos USB que usarán la redirección de USB genérico y configurar cada uno por separado.

- En el VDA, mediante configuraciones de directivas de Citrix. Para obtener más información, consulte Redirección de dispositivos del cliente y dispositivos del usuario y Configuraciones de directiva de Dispositivos USB en la Referencia para configuraciones de directivas.
- En la aplicación Citrix Workspace, mediante los mecanismos que dependen de la aplicación Citrix Workspace. Por ejemplo: una plantilla administrativa controla los parámetros de Registro que configuran la aplicación Citrix Workspace para Windows. De manera predeterminada, se permite la redirección USB para ciertas clases de dispositivos USB, y se rechaza para otras. Para obtener más información, consulte Configurar en la documentación de la aplicación Citrix Workspace para Windows.

Esta configuración independiente tiene la ventaja de ofrecer flexibilidad. Por ejemplo:

- Si dos departamentos o empresas diferentes se encargan de la aplicación Citrix Workspace y del VDA, pueden aplicar medidas de control por separado. Esta configuración se aplica cuando un usuario, ubicado en una empresa, acceda a una aplicación ubicada en otra empresa.
- Las configuraciones de directivas de Citrix sirven para controlar si se permiten dispositivos USB a ciertos usuarios o solo a aquellos usuarios que se conecten por medio de una red de área local (en lugar de hacerlo con Citrix Gateway).

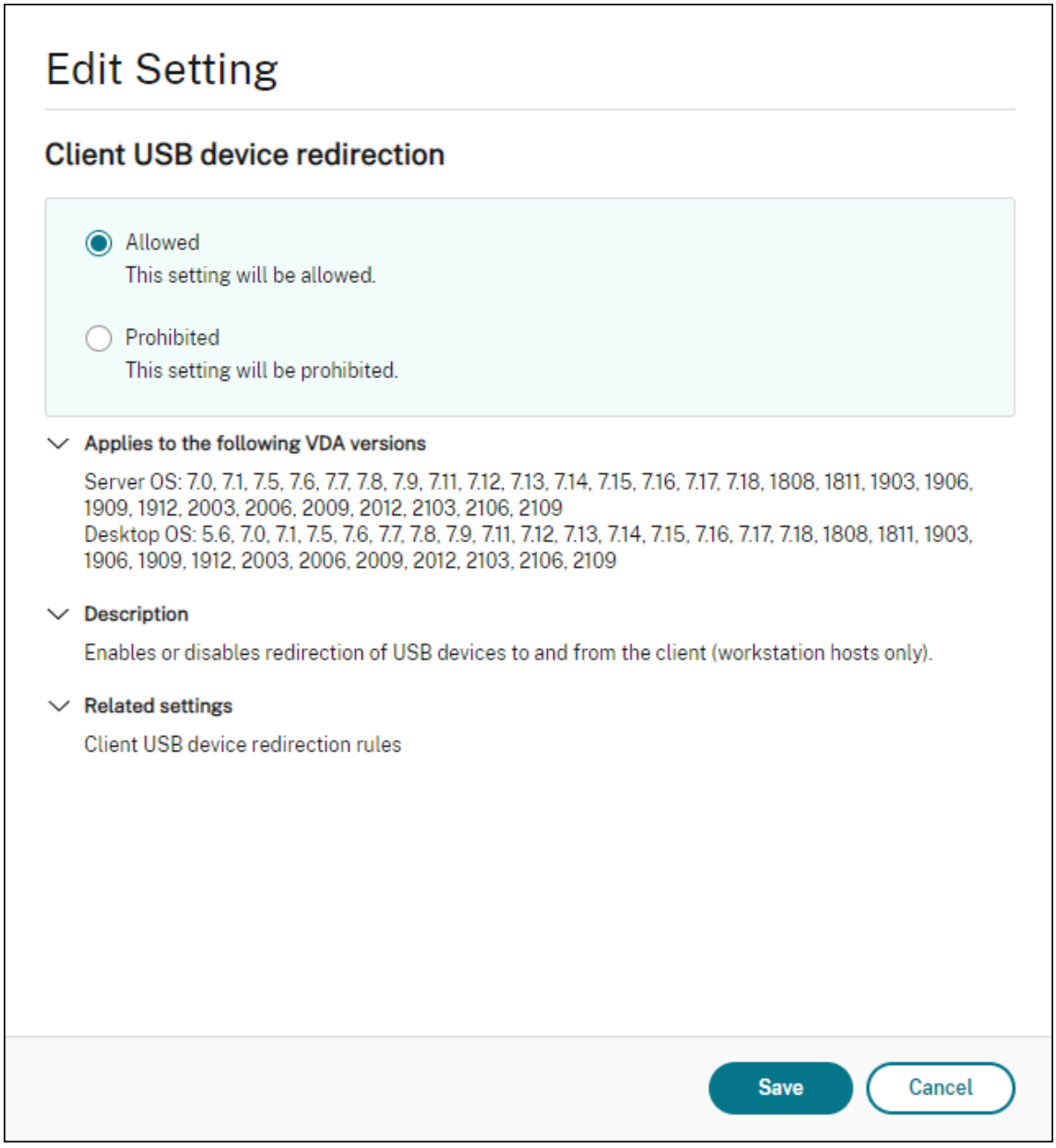
 

### Habilitar la redirección de USB genérico

Para habilitar la redirección de USB genérico y no requerir una redirección manual por parte del usuario, defina las configuraciones de directivas Citrix y las preferencias de conexión de la aplicación Citrix Workspace.

En configuraciones de directiva de Citrix:

1. Agregue Redirección de dispositivos USB del cliente a una directiva y establezca su valor en **Permitida**.



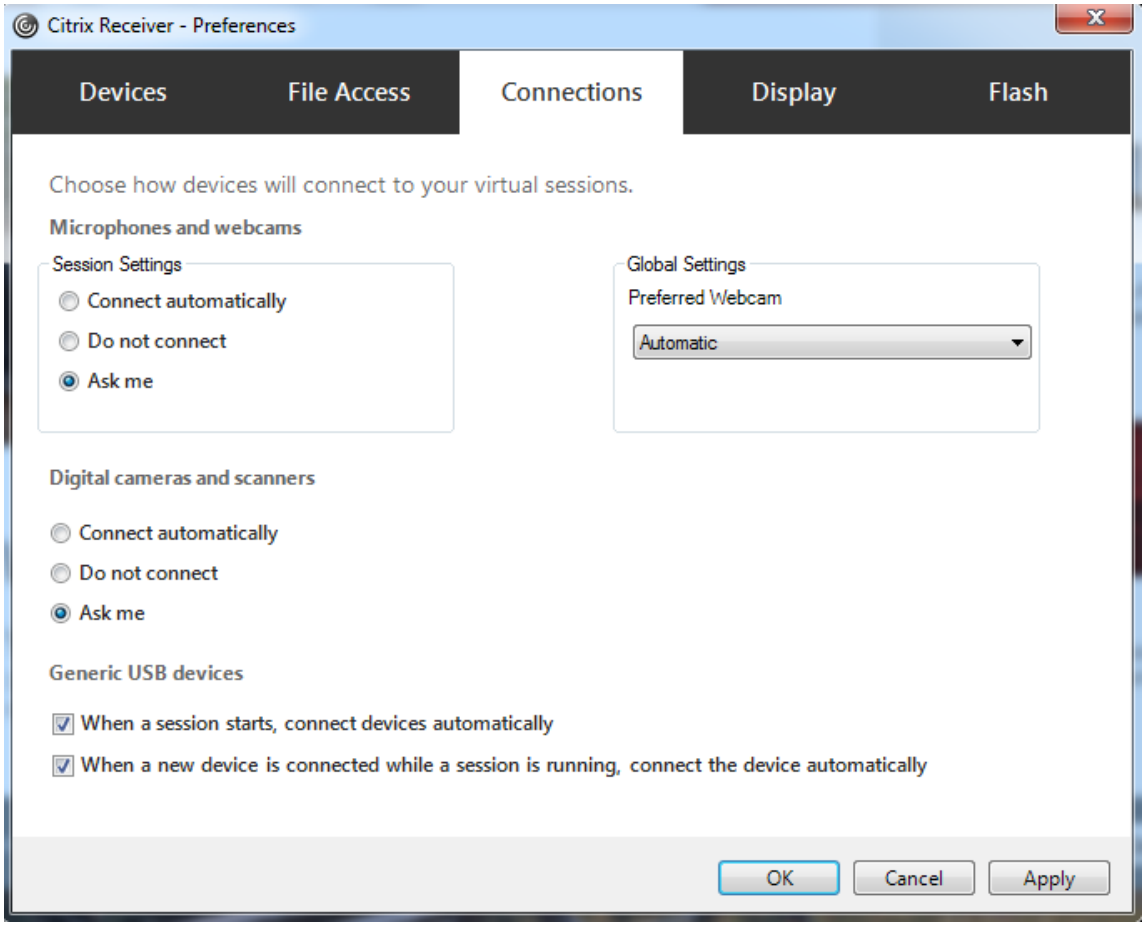

2. (Optativo.) Para actualizar la lista de dispositivos USB disponibles para la redirección, agregue la configuración Reglas de redirección de dispositivos USB del cliente a una directiva y especifique

las reglas de la directiva USB.

En la aplicación Citrix Workspace:

3. Especifique que los dispositivos se conecten automáticamente, sin redirección manual. Puede hacerlo mediante una plantilla administrativa, o bien en la aplicación Citrix Workspace para Windows > Preferencias > Conexiones.




Si especificó reglas de directiva USB para el VDA en el paso anterior, especifique las mismas reglas de directiva para la aplicación Citrix Workspace.

Para los clientes ligeros, consulte al fabricante para obtener detalles sobre la compatibilidad con USB y cualquier configuración requerida.

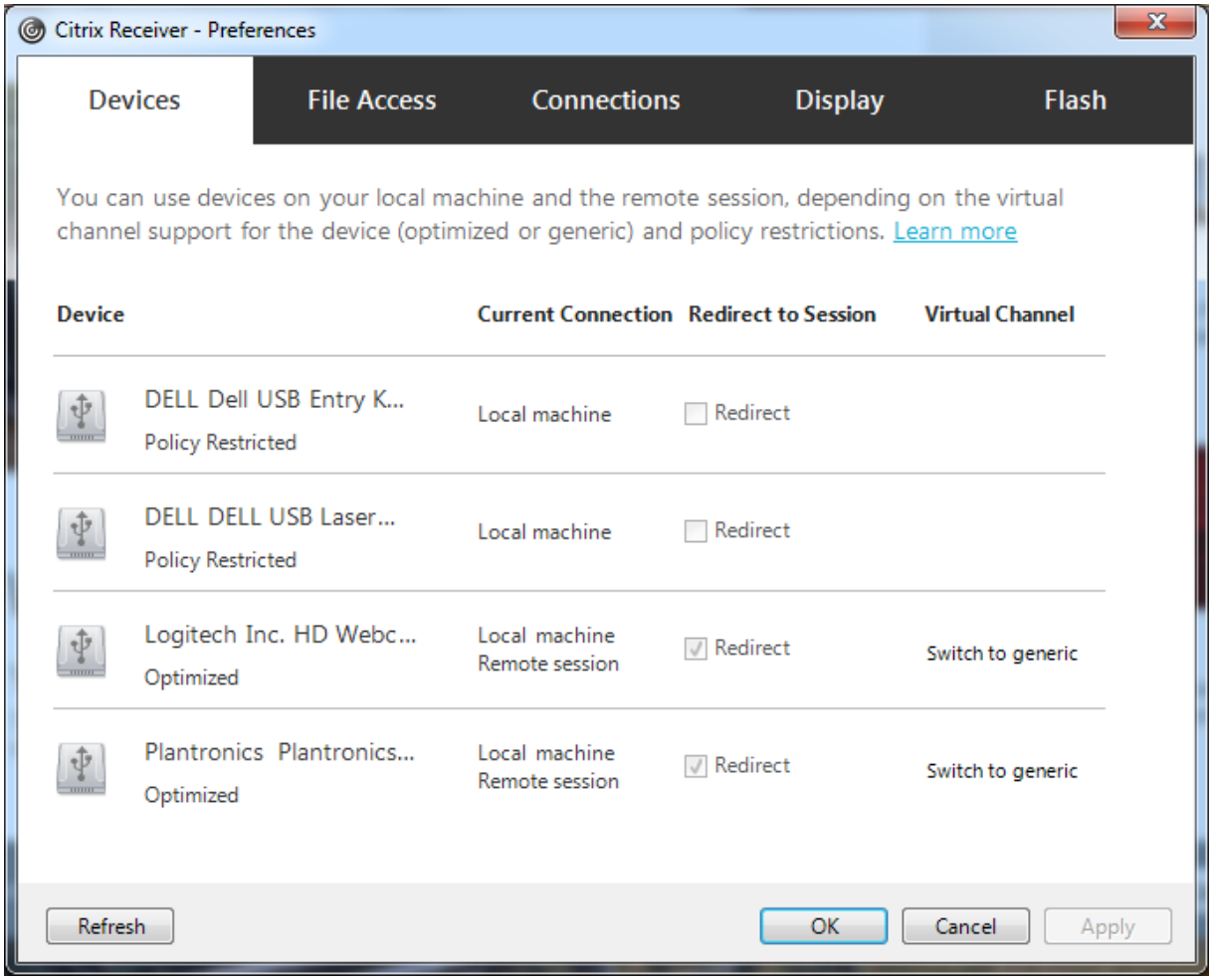
## Configurar los tipos de dispositivos USB disponibles para la redirección de USB genérico

Los dispositivos USB se redirigen automáticamente cuando la compatibilidad con USB está habilitada y la configuración de las preferencias de usuario para USB está definida para conectar automáticamente los dispositivos USB. Los dispositivos USB también se redirigen automáticamente cuando la

barra de conexión no está presente.

Los usuarios pueden redirigir explícitamente dispositivos que no se redirigen automáticamente. Para ello, deberán seleccionarlos en la lista de dispositivos USB. Para obtener más información, consulte el artículo Mostrar los dispositivos en Desktop Viewer en la ayuda de la aplicación Citrix Workspace para Windows.




Para usar la redirección de USB genérico en lugar de la optimización, puede:

- En la aplicación Citrix Workspace, seleccione manualmente el dispositivo USB con que se va a usar la redirección de USB genérico, elija **Cambiar a genérico** en la ficha "Dispositivos"del cuadro de diálogo "Preferencias".
- Seleccione automáticamente el dispositivo USB con que se va a usar la redirección de USB genérico. Para ello, configure la redirección automática para el tipo de dispositivo USB (por ejemplo, AutoRedirectStorage=1) y establezca las preferencias de usuario para USB en la conexión automática de los dispositivos USB. Para obtener más información, consulte Configure automatic redirection of USB devices.

> **Nota:**
>
> Configure la redirección de USB genérico para cámara web solo si esta no resulta compatible con la redirección multimedia HDX.

Para evitar que los dispositivos USB se redirijan o se enumeren, puede especificar reglas de dispositivo para la aplicación Citrix Workspace y el VDA.

Para la redirección de USB genérico, debe conocer al menos la clase y la subclase del dispositivo USB. No todos los dispositivos USB utilizan una clase y una subclase obvias. Por ejemplo:

- Las llaves de memoria o datos utilizan la clase de dispositivo del mouse.
- Los lectores de tarjeta inteligente pueden usar la clase de dispositivo HID o la que defina el proveedor.

Para un control más preciso, necesitará saber el ID de proveedor, el ID de producto y el ID de versión. Puede obtener esa información del proveedor del dispositivo.

> **Importante:**
>
> Los dispositivos USB dañinos pueden presentar funciones de dispositivo USB que no coincidan con el uso previsto para ellos. Las reglas de dispositivos no se han diseñado para evitar este comportamiento.

Puede definir qué dispositivos USB están disponibles para la redirección de USB genérico especificando reglas de redirección de dispositivos USB tanto para el VDA como para la aplicación Citrix Workspace. De esta manera, se anularán las reglas predeterminadas de la directiva USB.

Para el VDA:

- Modifique las reglas de invalidación del administrador para las máquinas con sistema operativo multisesión mediante las reglas de directiva de grupo. La Consola de administración de directivas de grupo se incluye en los medios de instalación:
  - Para x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement_x64.msi
  - Para x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement_x86.msi

En la aplicación Citrix Workspace para Windows:

- Modifique el Registro en el dispositivo del usuario. En los medios de instalación, se incluye una plantilla administrativa (archivo ADM) que permite cambiar el dispositivo cliente mediante la Directiva de grupo de Active Directory:
  dvd root \os\lang\Support\Configuration\icaclient_usb.adm.

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

Las reglas predeterminadas del producto se almacenan en HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRu
No modifique las reglas predeterminadas del producto. En su lugar, úselas como una guía para la creación de reglas de suplantación del administrador, según se explica a continuación en este artículo. Las suplantaciones del objeto de directiva de grupo (GPO) se evalúan antes que las reglas predeterminadas del producto.

Las reglas de suplantación del administrador se almacenan en HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericU
Las reglas de directivas de GPO toman el formato **{Allow:||Deny:}** seguidas de un conjunto de expresiones *etiqueta=valor* separadas por un espacio en blanco.

Se admiten las siguientes etiquetas:

| Etiqueta | Descripción |
|---|---|
| VID | Identificador del proveedor tomado del descriptor del dispositivo |
| PID | Identificador del producto tomado del descriptor del dispositivo |
| REL | Identificador de la versión tomado del descriptor del dispositivo |
| Class | Clase tomada del descriptor del dispositivo o de un descriptor de interfaz; consulte el sitio web de USB http://www.usb.org/ para ver los códigos de clase USB disponibles. |
| SubClass | Subclase, tomada del descriptor del dispositivo o de un descriptor de la interfaz |
| Prot | Protocolo tomado del descriptor del dispositivo o de un descriptor de la interfaz |

Al crear reglas de directivas, tenga en cuenta lo siguiente:

- Las reglas no distinguen entre mayúsculas y minúsculas.
- Las reglas pueden tener un comentario optativo al final que se introduce #. No es obligatorio utilizar un delimitador y el comentario se ignora para la comparación.

- Se ignoran las líneas en blanco y las que son exclusivamente de comentario.
- El espacio en blanco se usa como separador pero no puede aparecer en el medio de un número o de un identificador. Por ejemplo: Deny: Class = 08 SubClass=05 es una regla válida, pero Deny: Class=0 Sub Class=05 no lo es.
- Las etiquetas deben utilizar el operador de coincidencia =. Por ejemplo: VID=1230.
- Cada regla debe comenzar en una línea nueva o formar parte de una lista de reglas, separadas por punto y coma.

> **Nota:**
>
> Si utiliza el archivo de plantilla ADM, debe crear reglas en una única línea, como una lista separada por punto y coma.

Ejemplos:

- Este ejemplo muestra una regla de directiva de USB definida por un administrador para identificadores de producto y proveedor:

```
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse
 Deny: VID=046D # Deny all Logitech products
```

- Este ejemplo muestra una regla de directiva de USB definida por un administrador para una clase, una subclase y un protocolo definidos:

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
Allow: Class=EF SubClass=01 # Allow Sync devices Allow: Class=EF
# Allow all USB-Miscellaneous devices
```

### Usar y quitar dispositivos USB

Los usuarios pueden conectar un dispositivo USB antes o después de iniciar una sesión virtual.

Cuando se usa la aplicación Citrix Workspace para Windows, ocurre lo siguiente:

- Los dispositivos que se conectan después haber iniciado la sesión aparecen inmediatamente en el menú USB de Desktop Viewer.
- Si un dispositivo USB no se redirige correctamente, puede intentar resolver el problema esperando para conectar el dispositivo hasta después de que la sesión virtual se haya iniciado.
- Para evitar la pérdida de datos, use el icono de "Extracción segura"de Windows antes de quitar el dispositivo USB.

### Controles de seguridad para dispositivos de almacenamiento USB

Se ofrece optimización para dispositivos de almacenamiento USB Esta funcionalidad forma parte de la asignación de unidades del cliente que ofrecen Citrix Virtual Apps and Desktops. En el momento en

que los usuarios inician sesión, las unidades del dispositivo del usuario se asignan automáticamente a las letras de las unidades del escritorio virtual. Las unidades se muestran como carpetas compartidas que tienen letras de unidades asignadas. Para configurar la asignación de unidades del cliente, use la configuración **Unidades extraíbles del cliente.** Esta configuración se encuentra en la sección Configuraciones de directiva de Redirección de archivos en la configuración de la directiva ICA.

Con dispositivos de almacenamiento USB, puede utilizar la asignación de unidades del cliente, la redirección de USB genérico o ambas. Contrólelas mediante directivas de Citrix. Las principales diferencias son:

| Función | Asignación de unidades del cliente | Redirección de USB genérico |
|---|---|---|
| Habilitada de forma predeterminada | Sí | No |
| Configuración para acceso de solo lectura | Sí | No |
| Acceso a dispositivo cifrado | Sí, si el cifrado se desbloquea antes de acceder al dispositivo | Sí |
| Dispositivos BitLocker To Go | No | No |
| Dispositivo que eliminar con seguridad durante una sesión | No | Sí, si se siguen las recomendaciones del sistema operativo para quitar con seguridad el dispositivo |

Si la directiva de redirección de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se inserta un dispositivo de almacenamiento masivo antes o después de iniciar una sesión, el dispositivo se redirige mediante la asignación de unidades del cliente. Cuando la directiva de redirección de USB genérico y la directiva de asignación de unidades del cliente están ambas habilitadas y se configura un dispositivo para la redirección automática, y se introduce un dispositivo de almacenamiento masivo antes o después de iniciar una sesión, el dispositivo se redirige mediante la redirección de USB genérico. Para obtener más información, consulte el artículo CTX123015 de Knowledge Center.

> **Nota:**
>
> Se admite la redirección USB en conexiones de poco ancho de banda: por ejemplo, conexiones de 50 kbps. Sin embargo, no se admite copiar archivos de gran tamaño.

# Administración

April 14, 2022

Para administrar implementaciones de Citrix Virtual Apps and Desktops Service, Citrix instala y mantiene los componentes principales y las funciones en Citrix Cloud.

Usted se encarga de las máquinas (VDA) ubicadas en las ubicaciones de recursos que entregan aplicaciones y escritorios. También administra las conexiones a esas ubicaciones de recursos, además de las aplicaciones, los escritorios y los usuarios.

- **Autoscale:** Solución robusta y de alto rendimiento para administrar de forma proactiva la energía de sus máquinas.
- **Aplicaciones:** Las aplicaciones se administran en los grupos de entrega.
- **IP virtual y bucle invertido virtual:** La función de dirección IP virtual de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. Con la función de bucle invertido virtual de Citrix, puede configurar aplicaciones que dependen de la comunicación con el host local (127.0.0.1 de forma predeterminada) para utilizar una dirección de bucle invertido virtual exclusiva en el intervalo de host local (127.*).
- **Registro de VDA:** Para que un VDA pueda facilitar la entrega de aplicaciones y escritorios, debe registrarse en un Cloud Connector (establecer comunicación con él). Puede especificar direcciones de Cloud Connector mediante varios métodos que se describen en este artículo. A medida que agrega los Cloud Connectors, los agentes VDA deben tener información actualizada.
- **Sesiones:** Mantener la actividad de las sesiones es fundamental para ofrecer la mejor experiencia de usuario. Existen varias funciones que pueden optimizar la fiabilidad de sesiones, reducir los problemas, el tiempo de inactividad y la pérdida de la productividad.
- **Usar la búsqueda:** Si quiere ver información acerca de las máquinas, las sesiones, los catálogos de máquinas, las aplicaciones o los grupos de entrega en la interfaz de administración Configuración completa, utilice la función de búsqueda flexible.
- **Compatibilidad con IPv4 o IPv6:** Citrix Virtual Apps and Desktops admiten IPv4 puro, IPv6 puro, así como implementaciones de doble pila que usan redes IPv4 e IPv6 superpuestas. En este artículo, se describen y se muestran estas implementaciones. También se describen las configuraciones de directivas Citrix que determinan el uso de IPv4 o IPv6.
- **Profile Management:** Se puede instalar Citrix Profile Management al instalar un VDA. Si usa esta solución de perfiles de usuario, consulte la documentación correspondiente.
- **Citrix Insight Services (CIS):** Es una plataforma de Citrix para instrumentación, telemetría y generación de información empresarial. Los análisis y los diagnósticos se recopilan cuando instala un VDA.

- **Caché de host local:** La función Caché de host local (LHC) permite que las operaciones de intermediación de las conexiones continúen cuando un Cloud Connector de una ubicación de recursos no pueda comunicarse con Citrix Cloud. También se proporcionan consideraciones relativas a la escala, el tamaño y otros aspectos de la configuración.
- **Administración delegada:** Con la administración delegada, puede configurar los permisos de acceso que todos sus administradores necesitarán en función del rol que desempeñan en la organización.
- **Registro de configuración:** Registro de configuración hace seguimiento de los cambios de configuración y las actividades administrativas
- **Registros de eventos:** Los servicios dentro de Citrix Virtual Apps and Desktops registran los eventos que ocurren. Los registros de eventos se pueden usar para supervisar y solucionar problemas de las operaciones.
- **Licencias:** Desde la consola de Citrix Cloud, puede ver la información de uso de licencias de Citrix para este servicio.
- **Equilibrar la carga de las máquinas:** Permite controlar cómo equilibrar la carga de las máquinas.

## Acceso adaptable

June 24, 2022

En un mundo tan dinámico como el de hoy, la seguridad de las aplicaciones es vital para cualquier empresa. Tomar decisiones de seguridad contextuales y habilitar el acceso a las aplicaciones reduce los riesgos asociados y, al mismo tiempo, permite el acceso a los usuarios.

La función de acceso adaptable ofrece un enfoque integral al acceso de confianza cero que ofrece un acceso seguro a las aplicaciones. El acceso adaptable permite a los administradores proporcionar un acceso a nivel granular a las aplicaciones a las que los usuarios pueden acceder en función del contexto. El término "contexto"se refiere a:

- Usuarios y grupos (usuarios y grupos de usuarios)
- Dispositivos (dispositivos de escritorio o móviles)
- Ubicación (ubicación geográfica o ubicación de red)
- Posición del dispositivo (comprobación de la posición del dispositivo)
- Riesgo (puntuación de riesgo del usuario)

## Device Posture

February 21, 2024

Citrix Device Posture Service es una solución basada en la nube que ayuda a los administradores a aplicar ciertos requisitos que los dispositivos finales deben cumplir para acceder a recursos de Citrix DaaS (Citrix Virtual Apps and
Desktops) o Citrix Secure Private Access (aplicaciones SaaS y web o aplicaciones TCP y UDP). Establecer confianza de los dispositivos mediante la comprobación de la posición del dispositivo es fundamental para implementar un acceso basado en la confianza cero. Device Posture Service aplica principios de confianza cero en la red al comprobar el cumplimiento de los dispositivos finales (dispositivos administrados/BYOD y posición de seguridad) antes de permitir que un usuario final inicie sesión.

Para obtener más información, consulte Device Posture.

## Servicio de autenticación adaptable

March 30, 2024

Los clientes de Citrix Cloud pueden usar Citrix Workspace para proporcionar autenticación adaptable a Citrix DaaS. La autenticación adaptable es un servicio de Citrix Cloud que permite la autenticación avanzada para clientes y usuarios que inician sesión en Citrix Workspace. El servicio de autenticación adaptable es un ADC administrado por Citrix y alojado en Citrix Cloud que proporciona todas las prestaciones de autenticación avanzada, como estas:

- Autenticación de varios factores con diferentes métodos de autenticación, como AD, RADIUS, certificado y varios IDP de terceros mediante SAML 2.0, OAuth, OIDC o Google Captcha.
- Verificar la identidad de los usuarios y los niveles de autorización en función de factores como la ubicación, el estado del dispositivo y el grupo de usuarios.
- Permitir el acceso contextual o inteligente a DaaS (recursos virtualizados) y la autenticación de contraseña segura o SPA (recursos no virtualizados, como aplicaciones web y SaaS).
- Personalización de la página de inicio de sesión

Para obtener detalles completos sobre la autenticación adaptable, consulte Servicio de autenticación adaptable.

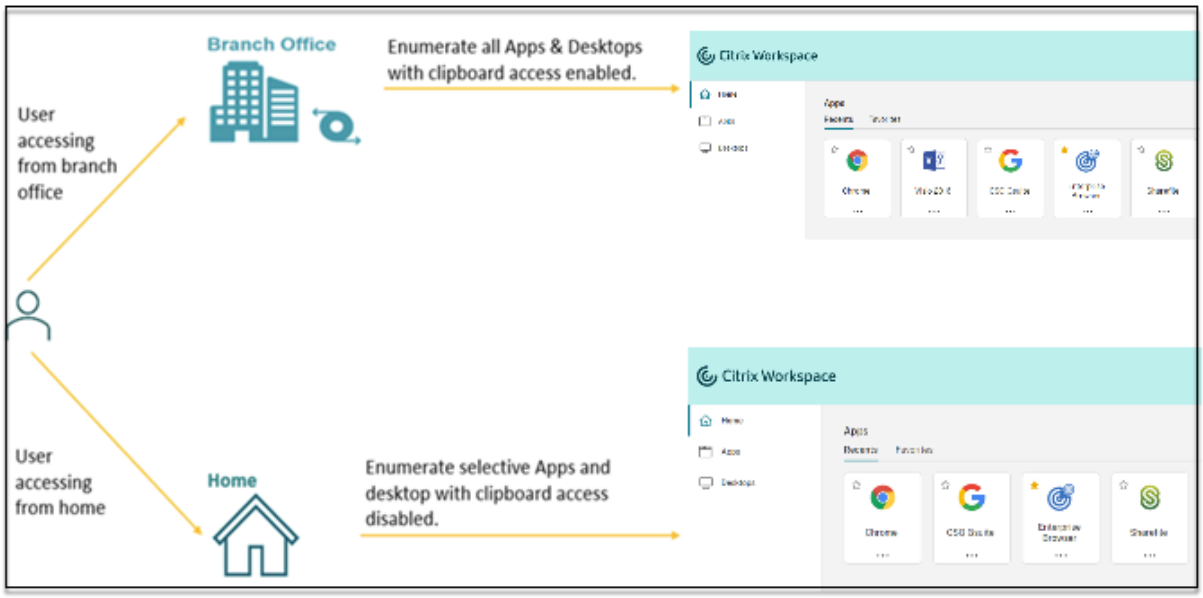
 

# Acceso adaptable en función de la ubicación de red del usuario

June 12, 2024

La función de acceso adaptable de Citrix Workspace usa una infraestructura de directivas avanzada para habilitar el acceso a Citrix DaaS en función de la ubicación de red del usuario. La ubicación se define mediante el rango de direcciones IP o las direcciones de subred.

Los administradores pueden definir directivas para enumerar, o no, aplicaciones y escritorios virtuales en función de la ubicación de red del usuario. También pueden controlar las acciones de usuario al habilitar o inhabilitar el acceso al portapapeles, las impresoras, la asignación de unidades del cliente, etc., en función de la ubicación de red del usuario. Por ejemplo, los administradores pueden configurar directivas para que los usuarios que accedan a los recursos desde casa tengan acceso limitado a aplicaciones y los usuarios que accedan a los recursos desde las sucursales tengan acceso total.




Un administrador puede implementar estas directivas para acceder a las aplicaciones:

- Enumerar algunas aplicaciones de carácter confidencial solo desde la ubicación corporativa o desde sus sucursales.
- No enumerar las aplicaciones de carácter confidencial si los empleados acceden al espacio de trabajo desde una red externa.
- Inhabilitar el acceso a las impresoras desde las sucursales.
- Inhabilitar el acceso al portapapeles y a las impresoras cuando los usuarios están fuera de la red corporativa.

### Derechos de uso

La función Acceso adaptable está disponible para los clientes con cualquiera de estas licencias.

- DaaS Premium / Premium Plus
- Secure Private Access Advanced

### Requisitos previos

- Asegúrese de que la función **Acceso adaptable** esté habilitada (**Citrix Workspace > Acceso > Acceso adaptable**). Para obtener detalles, consulte Habilitar la función Acceso adaptable.

  Al habilitar el acceso adaptable, las directivas de acceso de DaaS se actualizan para utilizar la opción **Conexiones a través de Citrix Gateway**.

  > **Nota:**
  >
  > NetScaler Gateway es necesario para agregar etiquetas de Smart Access en las directivas de acceso de DaaS. Sin embargo, dado que DaaS consume etiquetas de los servicios de Device Posture, Acceso adaptable y Autenticación adaptable, no es necesario tener un dispositivo NetScaler Gateway configurado en su entorno.

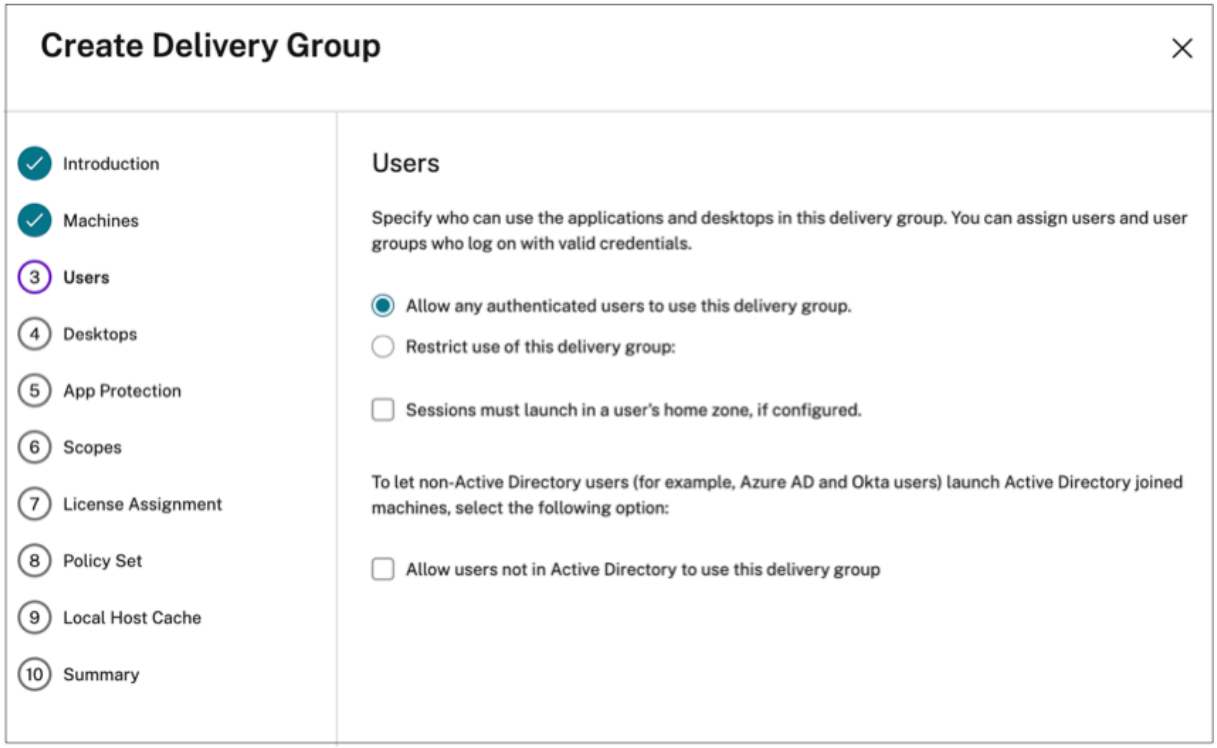
- Comprensión de las etiquetas de ubicación. Para obtener más información, consulte Etiquetas de ubicación de red.

### Puntos que tener en cuenta

Estos puntos solo son aplicables si quiere restringir la enumeración de aplicaciones en función de la ubicación. Si piensa utilizar el acceso adaptable para restringir controles de usuario, como inhabilitar el acceso al portapapeles, la redirección de impresoras o la asignación de unidades del cliente, en función de la ubicación de red, puede ignorar estas directrices.

- Si piensa enumerar de forma selectiva Citrix DaaS en función de la ubicación de la red, la administración de usuarios para esos grupos de entrega debe realizarse mediante directivas de Citrix Studio, en lugar de hacerlo con espacios de trabajo. Al crear un grupo de entrega, en **Configuración de usuarios**, elija **Restringir el uso de este grupo de entrega a los usuarios siguientes** o **Permitir que cualquier usuario no autenticado use este grupo de entrega**. Esto le permite configurar el acceso adaptable en la ficha **Directiva de acceso** de **Grupo de entrega**.



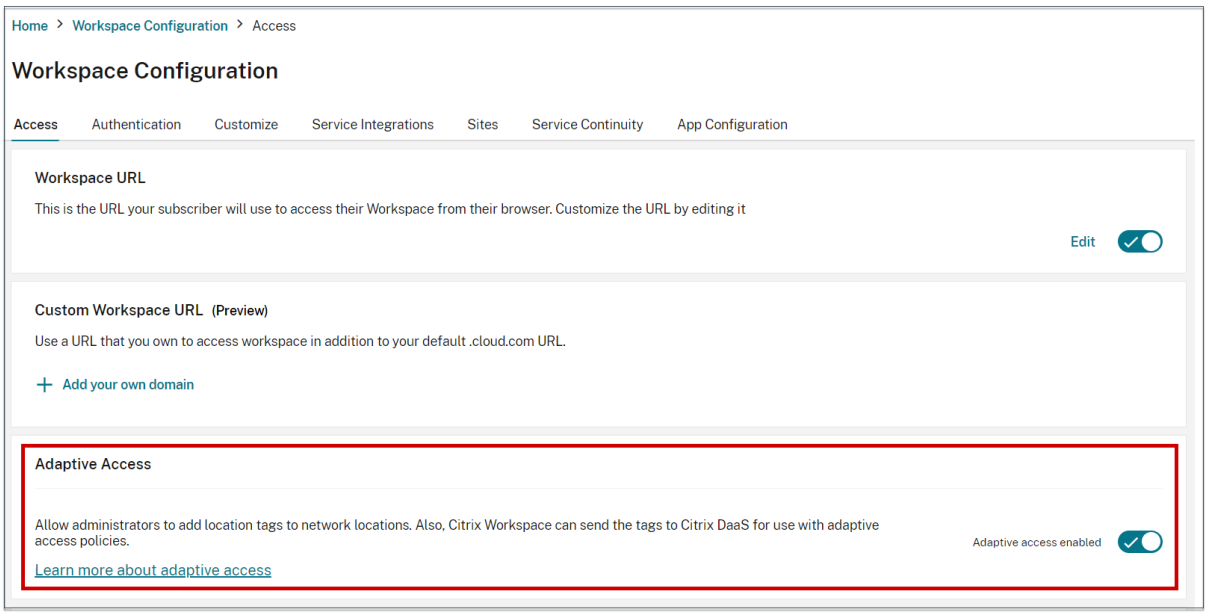

- Cambia a la conexión directa de carga de trabajo cuando se habilita el acceso adaptable.
  - El campo **Etiquetas de ubicación** se puede ver en **Citrix Cloud > Ubicaciones de red > Agregar una ubicación de red > Etiquetas de ubicación**.
  - Las directivas de conexión directa de carga de trabajo existentes funcionan según lo previsto.
  - Se deben crear otras directivas en el servicio de ubicaciones de red (sin definir etiquetas) y también en el grupo de entrega. Además, el tipo de conectividad de red debe ser **interno**.
  - En el caso de nuevas directivas de conexión directa de carga de trabajo con etiquetas, las etiquetas deben definirse en el servicio de ubicaciones de red y, también, deben definirse las mismas etiquetas en el grupo de entrega o en la directiva de acceso de DaaS Studio. Además, el tipo de conectividad de red debe ser **interno**. Las etiquetas de ubicación no son relevantes para la conexión directa de carga de trabajo.
- A continuación, se recomienda probar la implementación de Citrix DaaS.
  - Identifique un grupo de entrega de prueba o cree un grupo de entrega para implementar esta funcionalidad.
  - Cree o identifique una directiva que pueda utilizarse con un grupo de entrega de prueba.

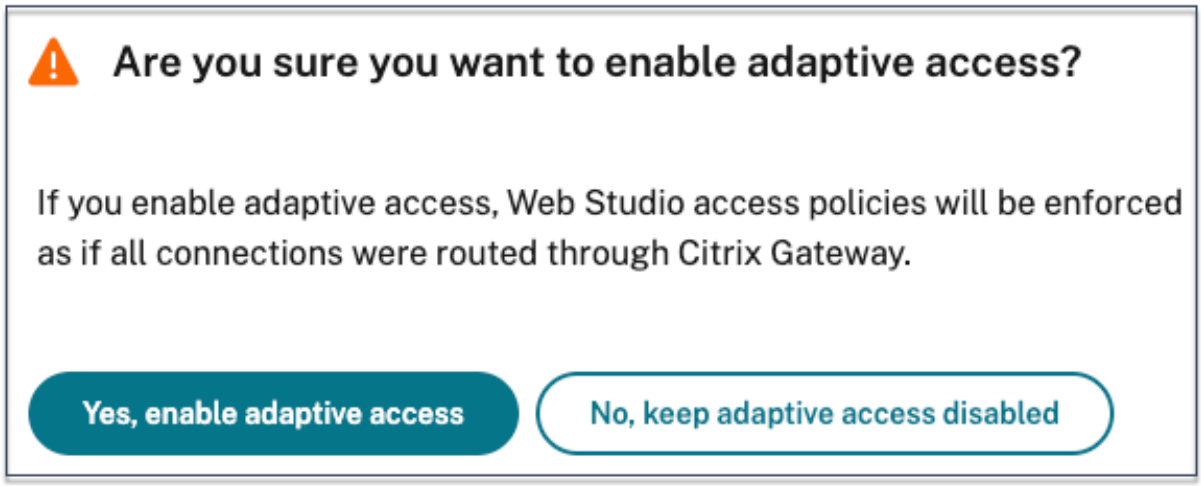
### Habilitar la función Acceso adaptable

1. Inicie sesión en Citrix Cloud.

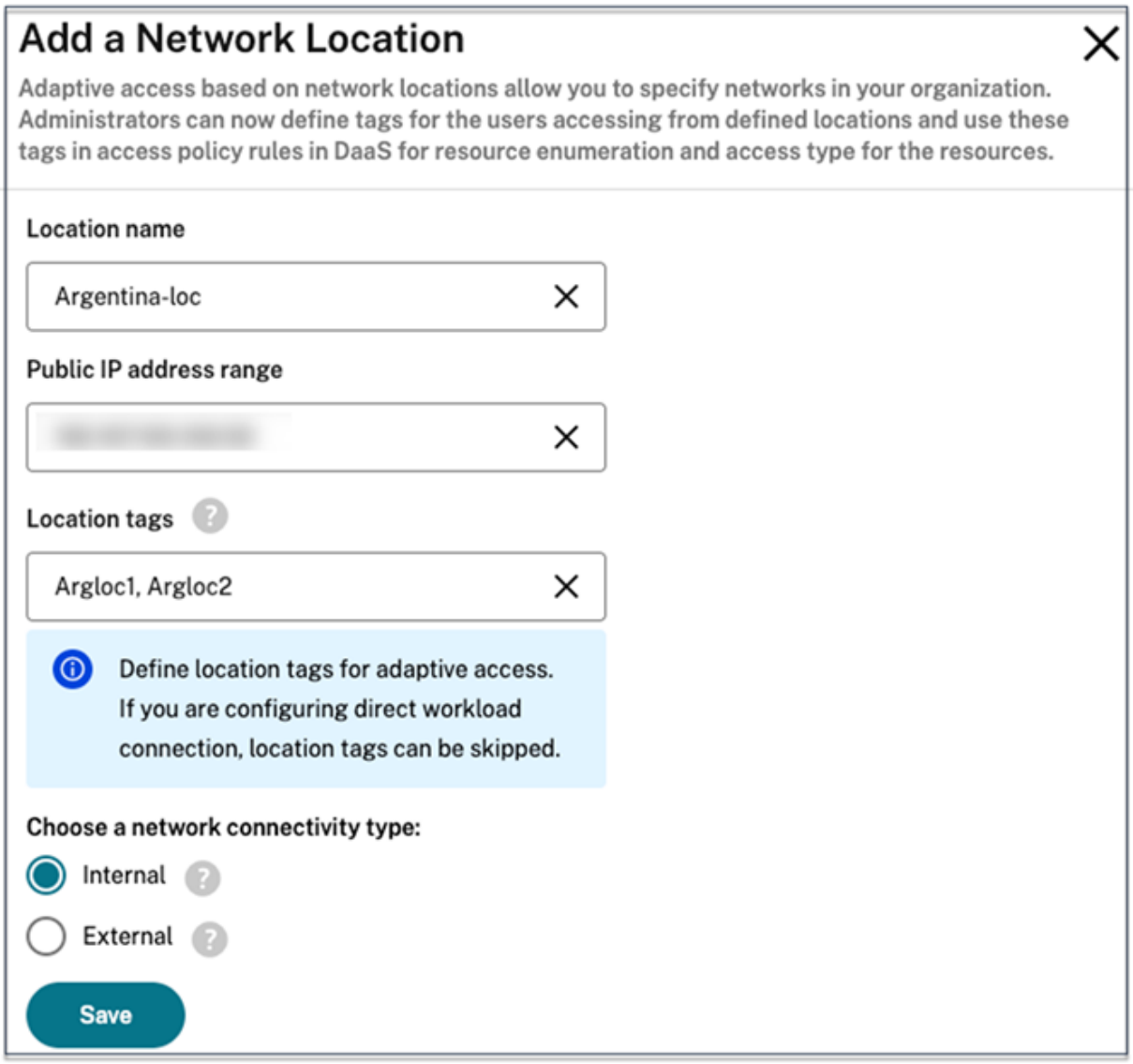
2. Seleccione **Configuración de Workspace** en el menú desplegable.
3. La opción **Acceso adaptable** está desactivada de forma predeterminada. Active el interruptor **Acceso adaptable**.
4. Haga clic en **Sí, habilitar el acceso adaptable** en el mensaje de confirmación.



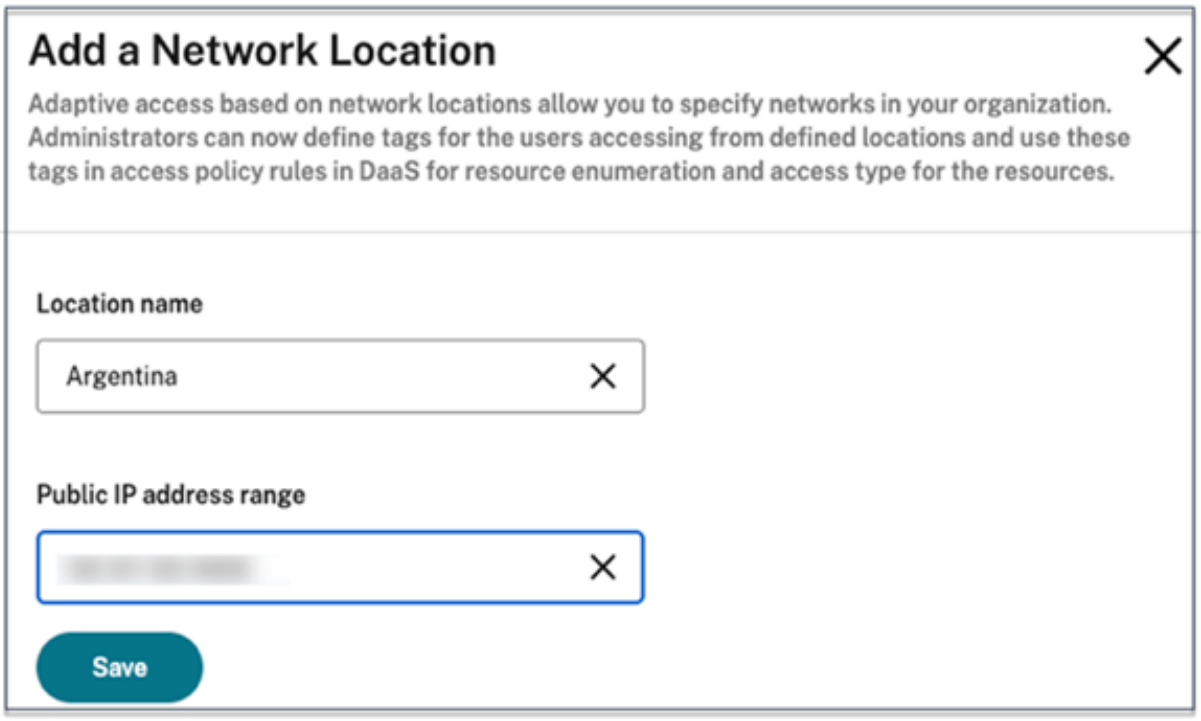

Cuando el acceso adaptable está habilitado, puede definir las etiquetas de ubicación para el acceso adaptable (**Citrix Cloud > Ubicaciones de red > Agregar una ubicación de red > Etiquetas de ubicación**).



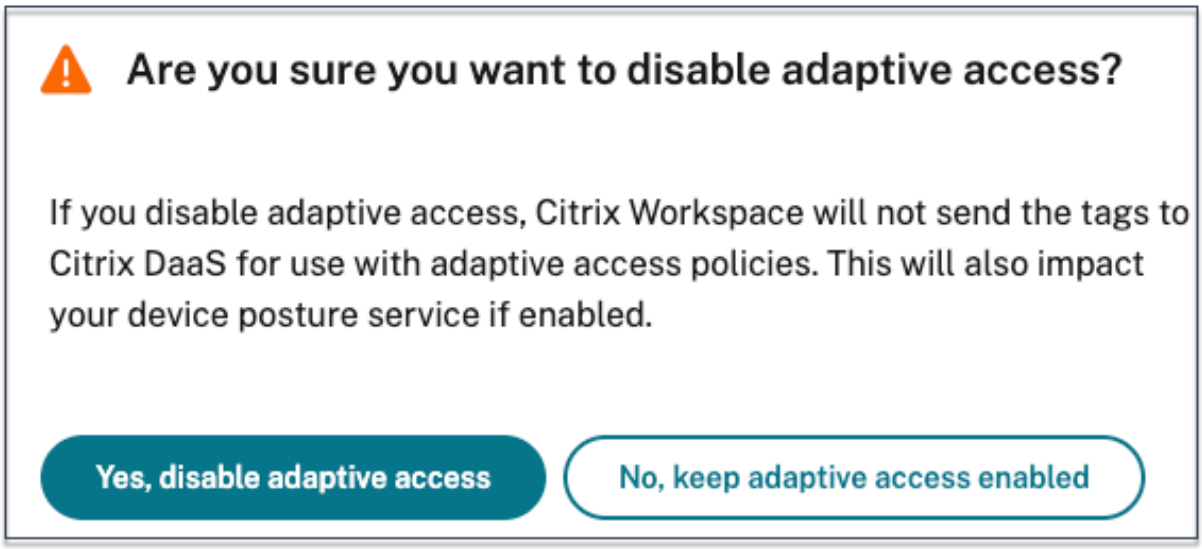

Cuando el acceso adaptable está inhabilitado, no puede agregar una ubicación de red. Las etiquetas de ubicación no son aplicables en este caso.




**Importante:**

Cuando intenta inhabilitar la función Acceso adaptable, aparece este mensaje. Tenga en cuenta que Workspace no envía las etiquetas a DaaS para su acceso adaptable cuando la función está inhabilitada.



## Configurar el acceso adaptable

La configuración del acceso adaptable en función de las ubicaciones de red implica estos pasos de alto nivel.

1. Definir las directivas de ubicación de red
2. Definir las etiquetas en DaaS Studio

Como ejemplos de configuración, se seleccionan dos tipos de usuarios (usuarios de **BranchOffice** y usuarios de **WorkFromHome**) para lograr el siguiente caso de uso.

- Los usuarios de BranchOffice deben poder acceder a las aplicaciones con todos los accesos.
- Los usuarios de WorkFromHome no deben tener acceso al portapapeles.

En este ejemplo de configuración, se utilizan **Home** y **Office** como etiquetas en los ejemplos.

### Configurar directivas de ubicación de red

1. Inicie sesión en Citrix Cloud.
2. Seleccione **Ubicaciones de red** en el menú desplegable.
   Asegúrese de que la opción de acceso adaptable esté habilitada. De lo contrario, se mostrará la interfaz de usuario de la conexión directa de carga de trabajo.
3. Haga clic en **Agregar ubicación de red**.

   - **Nombre de la ubicación:** Introduzca un nombre apropiado para la directiva.

     Ejemplo: BranchOffice o WorkFromHome
   - **Intervalo de direcciones IP públicas:** Defina el intervalo de direcciones IP públicas de la red.

     Ejemplo: 172.9.2.1-172.9.2.30
   - **Etiquetas de ubicación:** Defina etiquetas para su ubicación. Puede ser un nombre que haga referencia a su ubicación. Estas etiquetas sirven para configurar las directivas de acceso adaptable en Citrix Studio. Para obtener detalles, consulte **Definir etiquetas en Citrix Studio**.

     Ejemplo: *BranchOffice* o *WorkFromHome*
   - **Tipo de conectividad:** Defina el tipo de inicio de la aplicación.

   **Interno**: Omite la puerta de enlace para iniciar la aplicación.
   **Externo**: Usa Citrix Gateway Service o la puerta de enlace tradicional para iniciar la aplicación.
4. Haga clic en **Guardar**.

Ahora puede usar estas etiquetas en DaaS Studio para habilitar el acceso adaptable.

> **Nota:**
>
> Al definir las etiquetas de ubicación, asegúrese de introducir únicamente el nombre de etiqueta preferido sin el prefijo "LOCATION_TAG", por ejemplo, "BranchOffice". No obstante, al definir etiquetas en Citrix Studio, debe anteponer "LOCATION_TAG"al nombre de la etiqueta. Por ejemplo, "LOCATION_TAG_BRANCHOFFICE".

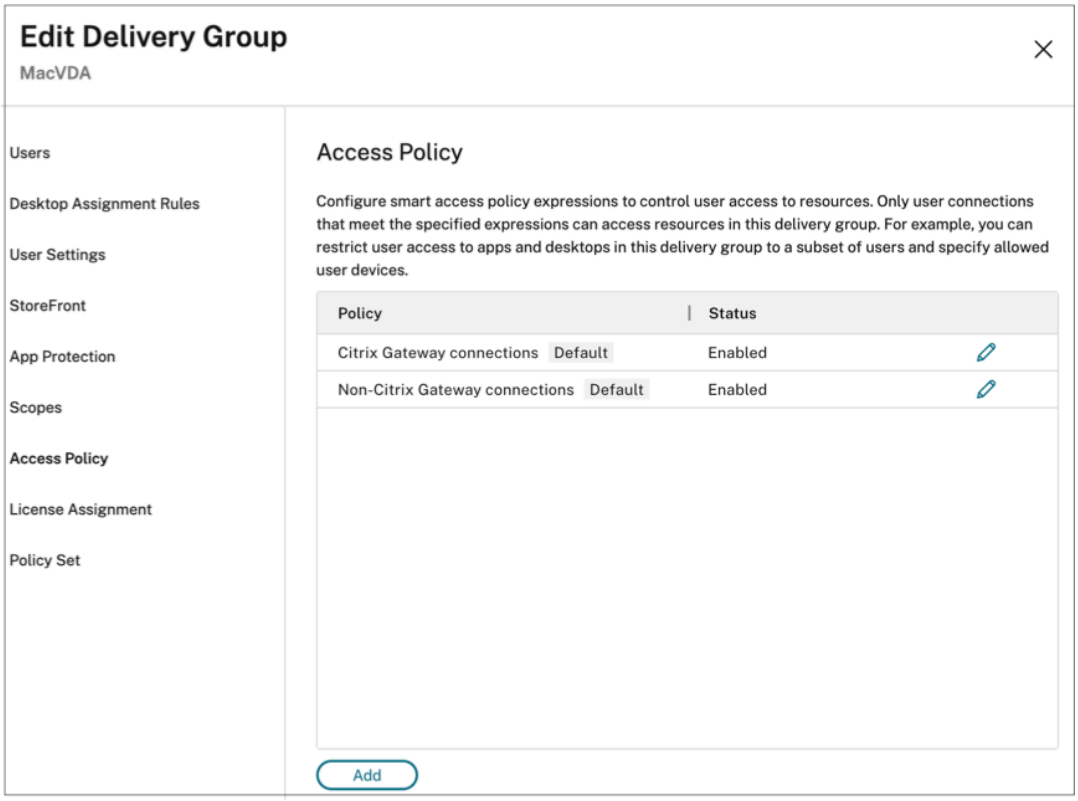
#### Definir etiquetas en Citrix Studio mediante la GUI

En este ejemplo, las etiquetas se definen en los grupos de entrega para restringir la enumeración de aplicaciones para los usuarios. Se crean dos grupos de entrega.

- Grupo de entrega de acceso adaptable: Para los usuarios de la ubicación **BranchOffice**. Estos usuarios deben ver todas las aplicaciones de este grupo de entrega.
- Grupo de entrega en teletrabajo: Para los usuarios de la ubicación **WorkFromHome**. Estos usuarios deben ver las aplicaciones de este grupo de entrega.

1. Inicie sesión en Citrix Cloud.
2. En el mosaico de **Citrix DaaS**, haga clic en **Administrar**.
3. Cree un grupo de entrega. Para obtener información detallada, consulte Crear grupos de entrega.
4. Seleccione el grupo de entrega que ha creado y haga clic en **Modificar grupo de entrega**.
5. Haga clic en **Directiva de acceso**.
6. Para los clientes que usan el acceso adaptable en la plataforma de Citrix Workspace, siga estos pasos para restringir el acceso de un grupo de entrega a las redes internas solamente:
    a) Haga clic con el botón derecho en el grupo de entrega y seleccione **Modificar**.
    b) Seleccione la directiva de acceso en el panel de la izquierda.
    c) Haga clic en el icono de modificación para modificar la directiva de conexiones predeterminada de Citrix Gateway.




d) En la página **Modificar directiva**, seleccione **Conexiones que cumplen estos criterios**, seleccione **Cotejar cualquiera** y, a continuación, agregue los criterios.


Para los usuarios de WorkFromHome, introduzca los siguientes valores en el Delivery Controller correspondiente.

**Comunidad**: Workspace

**Filtro**: LOCATION_TAG_WORKFROMHOME

Para los usuarios de BranchOffice, introduzca los siguientes valores en el Delivery Controller correspondiente.

**Filtro**: Workspace

**Valor**: LOCATION_TAG_BRANCHOFFICE

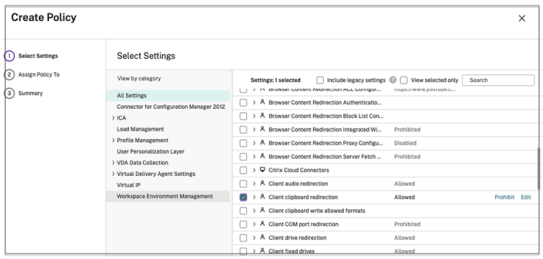
Ahora puede usar estas etiquetas para restringir el acceso a las aplicaciones.

> **Nota:**
>
> Asegúrese de introducir en el campo **Valor** el nombre correcto de la etiqueta de ubicación tal como la definió al crear las directivas de ubicación de red con el prefijo "LOCATION_TAG". Por ejemplo, si ha definido la etiqueta de ubicación como "BranchOffice", debe introducir "LOCATION_TAG_BRANCHOFFICE"en el campo **Valor**. Para obtener más información sobre la configuración de las etiquetas de ubicación, consulte Configurar directivas de ubicación de red.

### Restringir el acceso a las aplicaciones

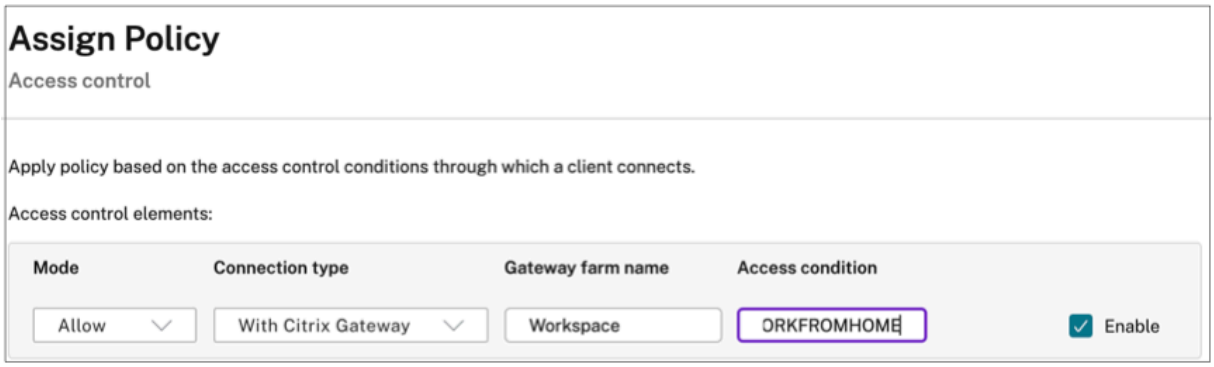
En este ejemplo, la redirección del portapapeles del cliente está inhabilitada para usuarios de la ubicación WorkFromHome.

1. Inicie sesión en Citrix DaaS.
2. Vaya a **Directivas** y haga clic en **Crear directiva**.
3. Seleccione **Redirección del portapapeles del cliente** y, a continuación, haga clic en **Prohibir**.
4. Haga clic en **Siguiente**.




1. En **Asignar directiva a** la página, seleccione **Control de acceso**.
2. Defina estos valores para la directiva:
   - Modo: **Permitir**
   - Tipo de conexión: **Con Citrix Gateway**
   - Nombre de la comunidad de Gateway: **Workspace**
   - Condición de acceso: **LOCATION_TAG_WORKFROMHOME** (todo en mayúsculas)




1. Haga clic en **Siguiente**.
2. Introduzca un nombre para la directiva y agregue una descripción de la directiva.
3. Haga clic en **Finalizar**.

Los usuarios de la ubicación **WorkFromHome** no pueden acceder al portapapeles desde los recursos iniciados.

#### Configurar directivas de grabación de sesiones en función de las etiquetas

La grabación de sesiones permite a las organizaciones registrar la actividad de los usuarios en pantalla en las sesiones virtuales. Puede especificar etiquetas, incluidas las etiquetas de ubicación de red, cuando cree directivas personalizadas de grabación de sesiones, de detección de eventos o de respuesta a eventos. Para ver un ejemplo, consulte Crear una directiva de grabación personalizada.

### Etiquetas de ubicación de red

El servicio de ubicaciones de red proporciona estas etiquetas.

- **Etiquetas predeterminadas:** Estas etiquetas se definen en el servicio de ubicaciones de red. Hay disponibles estas etiquetas predeterminadas.
  - **Location_internal:** Etiqueta que se envía de forma predeterminada cuando el tipo de conectividad de red se establece como **INTERNAL**.
  - **Location_external:** Etiqueta que se envía de forma predeterminada cuando el tipo de conectividad de red se establece como **EXTERNAL**.
  - **Location_undefined:** Etiqueta enviada para una dirección IP que no está definida en la directiva, pero que proviene del servicio de ubicaciones de red. Los inicios para estos usuarios son los mismos que los definidos en el grupo de recursos.
- **Etiquetas personalizadas:** Los administradores pueden definir nombres de etiquetas personalizadas en las directivas. Por ejemplo: office, home, branch

**Ejemplos:**

Etiquetas predeterminadas: LOCATION_INTERNAL, LOCATION_EXTERNAL, LOCATION_UNDEFINED

Etiquetas personalizadas: LOCATION_TAG_OFFICE, LOCATION_TAG_HOME

> **Nota:**
>
> Al definir etiquetas para el servicio de ubicación de red, asegúrese de lo siguiente:
>
> - Las etiquetas predeterminadas siempre comienzan con el prefijo "LOCATION_<tag name>". Por ejemplo, LOCATION_INTERNAL.
> - Las etiquetas personalizadas siempre comienzan con el prefijo "LOCATION_TAG<tag name>". Por ejemplo, LOCATION_TAG_OFFICE.

### Problemas conocidos

Si inhabilita la función de acceso adaptable después de habilitarla y de establecer las reglas (etiquetas y tipo de conectividad), no se quitarán las ubicaciones de la página Ubicaciones de red, aunque las columnas de etiquetas de ubicación y tipo de conectividad estén ocultas. Sin embargo, estas ubicaciones están inhabilitadas en el back-end. Se trata de una cuestión estética.

## Paquetes de aplicaciones

June 12, 2024

Existen varias tecnologías de empaquetado para entregar aplicaciones a los usuarios, incluidos los formatos App-V, MSIX, de conexión de aplicaciones MSIX y FlexApp. En este artículo se explica cómo implementar y entregar estas aplicaciones empaquetadas en el entorno de Citrix DaaS:

- Implementar y entregar aplicaciones de App-V
- Implementar y entregar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX
- Implementar y entregar aplicaciones FlexApp

### Implementar y entregar aplicaciones de App-V

En esta sección se incluye la siguiente información:

- Descripción general. Describe los métodos de administración que Citrix DaaS utiliza para entregar y administrar los paquetes de App-V.
- Procedimientos. Muestra procedimientos para implementar y entregar estos paquetes.

### Información general

En esta sección se describen los métodos de administración que Citrix DaaS utiliza para entregar y administrar los paquetes de App-V. Para obtener más información sobre los componentes y conceptos con los que se interactúa al entregar aplicaciones empaquetadas de App-V, consulte la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-for-windows.

Citrix DaaS entrega y administra paquetes de App-V mediante los siguientes métodos:

- **Administración dual**. Los paquetes de aplicaciones se configuran y se administran en servidores de App-V. Los servidores de Citrix DaaS y App-V trabajan juntos para entregar y administrar paquetes.

  Este método requiere que Citrix DaaS actualice periódicamente la vista de instantáneas del estado del servidor de App-V. Esto provoca una sobrecarga de hardware, infraestructura y administración. Los servidores de Citrix DaaS y App-V deben permanecer sincronizados, especialmente para los permisos de usuario.

  La administración dual funciona mejor en implementaciones en que App-V y Citrix Cloud están estrechamente unidos:

  - **Servidor de administración de App-V**. Publica y administra el ciclo de vida de paquetes de App-V y los archivos de configuración dinámica.
  - **Componente Citrix Personalization** instalado en máquinas VDA. Administre el registro del servidor de publicación de App-V adecuado que se necesite para el inicio de aplicaciones.

  Este método garantiza que, en un momento dado, el servidor de publicación de App-V esté sincronizado para el usuario. El servidor de publicación mantiene otros aspectos del ciclo de vida de los paquetes, como, por ejemplo, la actualización en inicios de sesión y grupos de conexión.

- **Administración única**. Los paquetes de aplicaciones se almacenan en recursos compartidos de red. Citrix DaaS entrega y administra paquetes de forma independiente.

  Este método reduce la sobrecarga porque los servidores de App-V y la infraestructura de bases de datos no son necesarios en la implementación.

  En este método, se almacenan paquetes de App-V en un recurso compartido de red y se cargan sus metadatos desde esa ubicación en Citrix Cloud. A continuación, el componente Citrix Personalization instalado en las máquinas VDA administra y entrega las aplicaciones de la siguiente manera:

  - Procesan los archivos de configuración de implementación y los archivos de configuración de usuario cuando se inicie una aplicación.

- Gestionan todos los aspectos de los ciclos de vida de los paquetes en la máquina host.

Puede usar los dos métodos de administración de forma simultánea. En otras palabras, al agregar aplicaciones a grupos de entrega, esas aplicaciones pueden proceder de paquetes de App-V presentes en servidores de App-V o en recursos compartidos de red.

> **Nota:**
>
> Si utiliza simultáneamente ambos métodos de administración, y el paquete de App-V tiene un archivo de configuración dinámica en ambas ubicaciones, se utiliza el archivo que se encuentra en el servidor de App-V (administración dual).

#### Procedimientos

Para poder entregar aplicaciones de App-V, debe instalar el componente Citrix Personalization en las máquinas VDA. Consulte Instalar el componente Citrix Personalization en máquinas VDA para obtener información detallada.

Para entregar aplicaciones empaquetadas de App-V a sus usuarios, siga estos pasos:

1. Almacenar paquetes de aplicaciones en recursos compartidos de red.
2. Cargar paquetes de aplicaciones en Citrix Cloud.
3. Agregar aplicaciones a grupos de entrega.
4. Para habilitar la entrega automática de paquetes de App-V interdependientes, cree grupos de aislamiento.

Para que Citrix DaaS reconozca y aplique los archivos de configuración dinámica de App-V con el método de administración única, consulte este blog de Citrix.

### Implementar y entregar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX

En esta sección se incluye la siguiente información:

- Descripción general. Describe cómo Citrix DaaS entrega y administra los paquetes en formato MSIX y de conexión de aplicaciones MSIX.
- Procedimientos. Muestra procedimientos para implementar y entregar estos paquetes.

#### Información general

Citrix DaaS entrega las aplicaciones en formato MSIX y de conexión de aplicaciones MSIX a los usuarios a través del componente Citrix Personalization instalado en las máquinas VDA. Este componente gestiona todos los aspectos de los ciclos de vida de los paquetes en la máquina host.

Para obtener más información sobre el formato MSIX y de conexión de aplicaciones MSIX, consulte la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/msix/ y https://docs.microsoft.com/en-us/azure/virtual-desktop/what-is-app-attach, respectivamente.

#### Procedimientos

Para permitir la entrega de paquetes en formato MSIX y de conexión de aplicaciones MSIX debe instalar el componente Citrix Personalization en las máquinas VDA. Consulte Instalar el componente Citrix Personalization en máquinas VDA para obtener información detallada.

Para entregar aplicaciones en formato MSIX y de conexión de aplicaciones MSIX a sus usuarios, siga estos pasos:

1. Almacenar paquetes de aplicaciones en recursos compartidos de red.
2. Cargar paquetes de aplicaciones en Citrix Cloud.
3. Agregar aplicaciones a grupos de entrega.

### Implementar y entregar aplicaciones FlexApp

En esta sección se incluye la siguiente información:

- Descripción general. Describe cómo Citrix DaaS entrega y administra los paquetes FlexApp.
- Procedimientos. Muestra procedimientos para implementar y entregar estos paquetes.

#### Información general

Citrix DaaS entrega aplicaciones FlexApp a los usuarios a través del componente Citrix Personalization y el agente de entrega FlexApp instalado en las máquinas VDA. Estos dos componentes gestionan todos los aspectos de los ciclos de vida de los paquetes en la máquina host.

#### Procedimientos

Para permitir la entrega de aplicaciones FlexApp, debe instalar los siguientes componentes en las máquinas VDA:

- El componente Citrix Personalization en máquinas VDA. Consulte Instalar el componente Citrix Personalization en máquinas VDA para obtener información detallada.
- El agente FlexApp en los VDA. Consulte Instalar el agente FlexApp para obtener más información.

Entregue aplicaciones empaquetadas FlexApp a sus usuarios siguiendo estos pasos:

1. Almacenar paquetes de aplicaciones en recursos compartidos de red.

2. Cargar paquetes de aplicaciones en Citrix Cloud.
3. Agregar aplicaciones a grupos de entrega.

### Instalar el componente Citrix Personalization en máquinas VDA

El componente Citrix Personalization administra el proceso de publicación de paquetes de aplicaciones en formatos App-V, MSIX, de conexión de aplicaciones MSIX y FlexApp. Este componente no se instala de forma predeterminada cuando se instala un VDA. Puede instalar el componente durante o después de la instalación del VDA.

Para instalarlo durante la instalación del VDA, use una de estas opciones:

- En el asistente de instalación, vaya a la página **Componentes adicionales** y, a continuación, marque la casilla **Citrix Personalization para App-V: VDA**.
- En la interfaz de línea de comandos, use la opción **/includeadditional "Citrix Personalization para App-V: VDA"**.

Para instalar el componente después de la instalación del VDA, siga estos pasos:

1. En la máquina VDA, vaya a **Panel de control > Programas > Programas y funciones**, haga clic con el botón secundario en **Citrix Virtual Delivery Agent** y, a continuación, seleccione **Cambiar**.
2. En el asistente que aparece, vaya a la página **Componentes adicionales** y, a continuación, marque la casilla **Citrix Personalization para App-V: VDA**.

> **Nota:**
>
> El cliente de escritorio de Microsoft App-V es el componente que ejecuta aplicaciones virtuales de paquetes App-V en dispositivos de usuario. Windows 10 (1607 o una versión posterior), Windows Server 2016 y Windows Server 2019 ya incluyen este software cliente de App-V. Solo tiene que habilitarlo en máquinas VDA. Para obtener más información, consulte este artículo de la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-enable-the-app-v-desktop-client.

### Almacenar paquetes de aplicaciones en recursos compartidos de red

Después de configurar la infraestructura, genere los paquetes de aplicaciones y guárdelos en una ubicación de red, como un recurso compartido de red UNC o SMB, o en un recurso compartido de archivos de Azure.

Estos son los pasos detallados:

1. Genere paquetes de aplicaciones. Consulte la documentación de Microsoft para obtener más detalles.

2. Almacene paquetes de aplicaciones en una ubicación de red:

    - Para la **administración única de App-V**: Almacene los paquetes y los archivos de configuración dinámica (App-V) correspondientes en un recurso compartido de red UNC o SMB, o en un recurso compartido de archivos de Azure.
    - Para la **administración dual de App-V**: Publique los paquetes en el servidor de administración de App-V desde una ruta UNC. (no se admite la publicación desde direcciones URL de HTTP.)
    - Para el formato **MSIX o de conexión de aplicaciones MSIX**: almacene los paquetes en un recurso compartido de red UNC o SMB o en un recurso compartido de archivos de Azure.
    - Para **FlexApp**: almacene los paquetes en un recurso compartido de red UNC o SMB o en un recurso compartido de archivos de Azure.

3. Asegúrese de que el VDA tenga permiso de lectura en la ruta de almacenamiento de paquetes:

    - Si almacena paquetes en un recurso compartido de red UNC o SMB en su dominio de AD, conceda permiso de lectura a la máquina VDA para leer la ruta de almacenamiento. Para hacerlo, puede conceder el permiso de lectura de la cuenta de AD de la máquina al recurso compartido de forma explícita o incluir la cuenta en un grupo de AD que tenga ese permiso.
    - Si almacena paquetes en un recurso compartido de archivos de Azure, primero conceda permiso de lectura a una cuenta de usuario para leer la ruta de almacenamiento en Azure. A continuación, configure el servicio `ctxAppVService` que se ejecuta en la máquina VDA para que use esa cuenta de usuario para acceder a la ruta de almacenamiento de paquetes. Consulte la siguiente sección para conocer los pasos detallados.

#### Cambiar la cuenta de inicio de sesión del usuario

El VDA llama a `ctxAppVService` para acceder a las rutas de almacenamiento de paquetes. De forma predeterminada, `ctxAppVService` accede a las rutas de almacenamiento de paquetes mediante la **cuenta del sistema local** de la máquina. Este tipo de autenticación de máquina funciona en los dominios de AD. Sin embargo, no funciona en los casos de integración de AD y Azure AD, los cuales requieren autenticación basada en cuentas de usuario.

Si almacena paquetes en un recurso compartido de archivos de Azure, cambie la cuenta de inicio de sesión de `ctxAppVService` a una cuenta de usuario que tenga permiso de lectura en la ruta de almacenamiento de paquetes. Estos son los pasos detallados:

1. Inicie **Servicios**, haga clic con el botón secundario en **ctxAppVService** y seleccione **Propiedades**.

2. En la ficha **Iniciar sesión**, seleccione **Esta cuenta**, introduzca una cuenta de usuario que tenga permiso de lectura para la ruta de almacenamiento de paquetes y, a continuación, introduzca la contraseña del usuario dos veces.
3. Haga clic en **Aceptar**.

## Cargar paquetes de aplicaciones en Citrix Cloud

Después de almacenar los paquetes de aplicaciones en una ubicación de red según sea necesario, cárguelos en Citrix Cloud para su entrega. Utilice uno de estos métodos según sea necesario:

- Carga en bloque
- Cargar uno a uno

### Preparativos

Citrix DaaS usa una máquina VDA para establecer la conexión con la ubicación de red para la detección de paquetes. Por lo tanto, cree un grupo de entrega de antemano y asegúrese de que al menos un VDA del grupo cumpla con estos requisitos:

- Versión de VDA:
  - Para detectar paquetes de App-V: 2203 o versiones posteriores
  - Para detectar paquetes en formato MSIX y de conexión de aplicaciones MSIX: 2209 o posterior
  - Para detectar paquetes FlexApp: 2311 o posterior
- Componente de Citrix Personalization para App-V: Instalado
- Permiso en la ubicación del paquete: Lectura (consulte el paso 2: Almacenar paquetes de aplicaciones en recursos compartidos de red para obtener más información).
- Encendido
- Estado: Registrado

### Roles obligatorios

De forma predeterminada, si tiene rol de administrador de la nube o administrador total, puede cargar paquetes de aplicaciones en Citrix Cloud. También puede crear roles personalizados para realizar las acciones de carga. En esta tabla se indican los permisos que requieren las acciones de paquetes de aplicaciones.

| Acción | Permisos necesarios |
| --- | --- |
| Agregar paquete (cargar uno a uno) | Crear sesiones de detección de aplicaciones |
| Agregar origen (cargar en bloque) | Crear perfiles de detección de aplicaciones |
| Buscar actualizaciones de paquetes | Crear sesiones de detección de aplicaciones |
| Quitar origen | Quitar perfiles de detección de aplicaciones |

#### Cargar paquetes de aplicaciones en bloque

Cargar paquetes a una ubicación de red en Citrix Cloud. Asegúrate de tener estos elementos listos antes de cargarlos:

- Un grupo de entrega que cumpla con los requisitos indicados en Preparación
- La ruta de la ubicación de red

Para cargar paquetes en bloque, sigue estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Paquetes de aplicaciones** en el panel de la izquierda.
2. En la ficha **Orígenes**, haga clic en el botón **Agregar origen**. Aparecerá la página **Agregar origen**.
3. En el campo **Nombre**, introduzca un nombre descriptivo del origen del paquete.
4. En el campo **Grupo de entrega**, haga clic en **Seleccione un grupo de entrega**. A continuación, seleccione un grupo de entrega que cumpla los requisitos establecidos en Preparación y, a continuación, haga clic en **Aceptar**.
5. En el campo **Tipo de ubicación**, seleccione **Servidor de Microsoft App-V** o **Recurso compartido de red** según el lugar en el que almacene los paquetes y, a continuación, complete los parámetros correspondientes:
    - Si selecciona **Servidor de Microsoft App-V**, introduzca esta información:
        - URL del servidor de administración. Ejemplo: `http://appv-server.example.com`
        - Credenciales de inicio de sesión del administrador del servidor de administración.
        - URL y número de puerto del servidor de publicación. Ejemplo: `http://appv-server.example.com:3330`
    - Si seleccionó **Recurso compartido de red**, especifique esta información:
        - Introduzca la ruta UNC del recurso compartido de red. Ejemplo: `\\Package-Server\apps\`

- Seleccione los tipos de paquetes que quiere cargar. Las opciones incluyen los formatos App-V, MSIX, de conexión de aplicaciones MSIX y FlexApp.
- Especifique si quiere buscar paquetes en las subcarpetas.

6. Haga clic en **Agregar origen**.

   La página Agregar origen se cierra y el origen recién agregado aparece en la lista de orígenes. Citrix DaaS carga los paquetes en Citrix Cloud mediante un VDA en el grupo de entrega. Una vez completada la carga, el campo Estado muestra *Importación correcta*. Los paquetes correspondientes aparecen en la ficha **Paquetes**.

   > **Nota:**
   >
   > Para comprobar si hay actualizaciones de paquetes en la ubicación de un origen e importarlas a Citrix Cloud, seleccione la ubicación en la lista de orígenes y haga clic en **Buscar actualizaciones de paquetes**.

#### Cargar paquetes de aplicaciones uno a uno

Cargue un paquete de aplicaciones desde un recurso compartido de red en Citrix Cloud. Antes de cargarlo, asegúrate de tener estos elementos listos:

- Un grupo de entrega que cumpla con los requisitos establecidos en Preparación
- La ruta de la ubicación de red.

Para cargar un paquete en Citrix Cloud, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Paquetes de aplicaciones** en el panel de la izquierda.
2. En la ficha **Paquetes**, haga clic en el botón **Agregar paquete**. Aparecerá la página **Agregar paquete**.
3. En el campo **Grupo de entrega**, haga clic en **Seleccione un grupo de entrega**. A continuación, seleccione un grupo de entrega que cumpla los requisitos establecidos en Preparación y, a continuación, haga clic en **Aceptar**.
4. En el campo **Ruta completa del paquete**, introduzca una ruta según sea necesario:

   - Para cargar varios paquetes a la vez, introduzca sus rutas completas, separadas por punto y coma (`;`). Ejemplo: `\\Package-Server\apps\office365.appv;\\Package-Server\apps\skype.msix;\\Package-Server\apps\slack.vhd`
   - Para cargar todos los paquetes presentes en un recurso compartido de red, introduzca la ruta de almacenamiento. Ejemplo: \servidor-paquetes\aplicaciones\

5. Haga clic en **Agregar paquete**.

   El paquete de aplicaciones aparece en la ficha **Paquetes**.

### Agregar aplicaciones a grupos de entrega

Una vez que se haya cargado por completo un paquete de aplicaciones, agregue sus aplicaciones a uno o más grupos de entrega según sea necesario. Como resultado, los usuarios asociados a esos grupos de entrega pueden acceder a las aplicaciones.

> **Nota:**
>
> - Puede entregar aplicaciones empaquetadas a los VDA de sesión única y a los VDA multisesión a través de grupos de entrega.
> - De forma predeterminada, los usuarios finales tienen acceso a todas las aplicaciones empaquetadas asignadas a los grupos de entrega asociados a sus VDA *de sesión única* (o denominados *de escritorio*). Para limitar la visibilidad de una aplicación empaquetada en los VDA *de escritorio* a usuarios o grupos específicos, vaya al nodo **Aplicaciones**, seleccione la app y después seleccione **Modificar propiedades de aplicación > Limitar visibilidad** para realizar cambios.

Para agregar una o más aplicaciones de un paquete a varios grupos de entrega, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Paquetes de aplicaciones** en el panel de la izquierda.
2. En la ficha **Paquetes**, seleccione el paquete que necesite.
3. En la barra de acciones, haga clic en **Asignar aplicaciones a grupos de entrega**. Aparece la página Asignar aplicaciones a grupos de entrega.
4. Seleccione una o más aplicaciones del paquete en función de sus necesidades y, a continuación, haga clic en **Siguiente**.
5. En la lista de grupos de entrega, seleccione los grupos a los que quiere asignar las aplicaciones y, a continuación, haga clic en **Siguiente**.

   > **Nota:**
   >
   > - Si seleccionó un paquete en formato *MSIX* o de *conexión de aplicaciones* MSIX, solo se mostrarán en la lista los grupos de entrega cuyo nivel funcional sea 2106 o posterior.
   > - Si seleccionó un paquete *FlexApp*, solo se muestran en la lista los grupos de entrega cuyo nivel funcional sea 2206 o posterior.

6. Haga clic en **Finalizar**.

Para agregar aplicaciones de varios paquetes a varios grupos de entrega, siga estos pasos:

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda.
2. En la ficha **Aplicaciones**, seleccione **Agregar aplicaciones**.
3. En la página **Grupos**, seleccione uno o más grupos de entrega según necesite.
4. En la página **Aplicaciones**, seleccione uno o más paquetes de aplicaciones de esta manera:

    a) Haga clic en **Agregar** y después seleccione **Paquetes de aplicaciones**.
    b) Seleccione el tipo de origen del paquete necesario (por ejemplo, administración única de App-V). Se muestran todos los paquetes de este tipo.
    c) Seleccione uno o más paquetes según necesite.
    d) Haga clic en **Aceptar** y **Siguiente**.
    e) Para agregar más aplicaciones de un tipo de paquete diferente, repita los pasos a a d.

5. Haga clic en **Finalizar**.

También puede agregar aplicaciones empaquetadas a un grupo de entrega cuando:

- Se crea un grupo de entrega. Para obtener más información, consulte Crear grupos de entrega.
- Se modifica n grupos de entrega o grupos de aplicaciones existentes. Para obtener más información, consulte Agregar aplicaciones.

## (Opcional) Crear grupos de aislamiento para paquetes de App-V

Puede crear grupos de aislamiento para habilitar la entrega automática de paquetes de App-V interdependientes.

> **Nota:**
>
> Los grupos de aislamiento son compatibles con el método de administración única de App-V. Si usa el método de administración dual de App-V, puede lograr el mismo objetivo mediante la creación de *grupos de conexiones* en la infraestructura de Microsoft App-V. Para obtener más información, consulte este artículo de la documentación de Microsoft: https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-connection-group-file.

### Acerca de los grupos de aislamiento

Un grupo de aislamiento es una colección de paquetes de aplicaciones interdependientes que deben ejecutarse en el mismo espacio aislado de Windows para crear un entorno virtual. Los grupos de aislamiento de App-V de Citrix son similares, pero no idénticos, a los grupos de conexión de App-V. Un grupo de aislamiento incluye dos tipos de paquetes:

- Paquetes de aplicaciones **explícitas**. Aplicaciones con requisitos específicos de licencia. Puede restringir esas aplicaciones a un grupo específico de usuarios al agregarlas a grupos de entrega.
- Paquetes de aplicaciones **automáticas**. Aplicaciones que están siempre disponibles para todos los usuarios, independientemente de si se agregan a grupos de entrega.

Por ejemplo: la aplicación app-a requiere JRE 1.7 para ejecutarse. Puede crear un grupo de aislamiento que contenga app-a (marcada como *Explícita*) y JRE 1.7 (marcada como *Automática*). A continuación, agregue el paquete de App-V de app-a a uno o más grupos de entrega. Cuando un usuario inicie la aplicación A, JRE 1.7 se implementará automáticamente con ella.

Cuando un usuario inicia una aplicación de App-V marcada como *Explícita* en un grupo de aislamiento, Citrix DaaS comprueba los permisos de acceso del usuario a la aplicación en los grupos de entrega. Si el usuario tiene permiso para acceder a la aplicación, todos los paquetes de aplicaciones *automáticas* del mismo grupo de aislamiento estarán disponibles para el usuario.

No es necesario agregar los paquetes *automáticos* a ningún grupo de entrega. Si hay otro paquete de aplicaciones *explícitas* en el grupo de aislamiento, ese paquete estará disponible para el usuario solo si está en el mismo grupo de entrega.

Para obtener más información sobre los grupos de aislamiento, consulte este blog de Citrix.

**Crear un grupo de aislamiento de App-V** Cree un grupo de aislamiento y agréguele paquetes de aplicaciones interdependientes. Estos son los pasos detallados:

1. En la ficha **Grupos de aislamiento**, haga clic en **Agregar grupo de aislamiento**.
2. Introduzca un nombre y una descripción para el grupo de aislamiento. Todos los paquetes de aplicaciones de Citrix Cloud aparecen en la lista **Paquetes disponibles**.
3. En la lista **Paquetes disponibles**, seleccione la aplicación que necesite y, a continuación, haga clic en la flecha de la derecha. Las aplicaciones seleccionadas aparecen en la lista **Paquetes en grupo de aislamiento**.
4. En el campo **Implementación**, seleccione **Explícita** o **Automática** para la aplicación.
5. Repita los pasos 2 y 3 para agregar más paquetes.
6. Para ajustar el orden de los paquetes de la lista, haga clic en la flecha hacia arriba o hacia abajo.
7. Haga clic en **Guardar**.

> **Nota:**
>
> Las configuraciones de grupos de aislamiento resultan en la creación de grupos de conexiones de App-V en el VDA. Los casos de implementación pueden volverse complejos, y el cliente de App-V admite paquetes que solo están en un grupo de conexiones activo a la vez. Le recomendamos no agregar el mismo paquete a dos grupos de aislamiento diferentes que se hayan agregado al mismo grupo de entrega.

# AutoScale

March 6, 2024

Autoscale ofrece una solución robusta y de alto rendimiento para administrar de forma proactiva la energía de sus máquinas. Su objetivo es equilibrar los costes y la experiencia de usuario. Autoscale incorpora la antigua tecnología Smart Scale en la solución de administración de energía de la consola **Administrar**.

Autoscale permite administrar de forma proactiva la energía de todas las máquinas con SO de sesión única y de SO multisesión registradas en un grupo de entrega.

Las funciones de Autoscale incluyen:

- Parámetros basados en la programación y en la carga
- Tiempos de espera de sesión dinámicos
- Autoscale de máquinas etiquetadas (ampliación en la nube)
- Aprovisionamiento dinámico de máquinas
- Notificaciones de cierre de sesión del usuario

## Plataformas compatibles de alojamiento de VDA

Autoscale admite todas las plataformas compatibles con Citrix DaaS. Esto incluye varias plataformas de infraestructura en la nube, como XenServer (antes denominado Citrix Hypervisor), Amazon Web Services, Google Cloud Platform, Microsoft Azure Resource Manager, VMware vSphere y muchas más. Para obtener una lista completa de las plataformas compatibles, consulte los requisitos del sistema para Citrix DaaS.

## Cargas de trabajo admitidas

Autoscale admite grupos de entrega tanto de SO multisesión como de SO de sesión única. Hay tres interfaces de usuario a tener en cuenta:

- Interfaz de usuario de Autoscale para grupos de entrega de SO multisesión (antes denominados grupos de entrega de RDS)
- Interfaz de usuario de Autoscale para grupos de entrega aleatorios (agrupados) de SO de sesión única (antes denominados grupos de entrega de VDI agrupados)
- Interfaz de usuario de Autoscale para grupos de entrega estáticos de SO de sesión única (antes denominados grupos de entrega de VDI estáticos)

Para obtener más información sobre las interfaces de usuario para diferentes grupos de entrega, consulte Interfaces de usuario de Autoscale.

### Ventajas

La función Autoscale ofrece las siguientes ventajas:

- Ofrezca un mecanismo único y coherente para administrar la energía de las máquinas de un grupo de entrega.
- Garantice la disponibilidad y el control de los costes con administración de energía de máquinas por carga o por programación, o una combinación de ambas.
- Para supervisar métricas como el ahorro de costes y la utilización de capacidades, y para habilitar las notificaciones, use Director, disponible en la ficha **Supervisar**.

### Vídeo de 2 minutos

Este vídeo ofrece un recorrido rápido por Autoscale.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

## Introducción a Autoscale

October 30, 2023

Autoscale funciona a nivel de grupos de entrega. Administra de forma proactiva la energía de las máquinas de un grupo de entrega en función de los horarios que usted establezca.

Autoscale se aplica a todos los tipos de grupos de entrega:

- SO estático de sesión única
- SO aleatorio de sesión única
- SO aleatorio multisesión

En este artículo se describen los conceptos básicos relacionados con Autoscale y se proporcionan instrucciones sobre cómo habilitar y configurar Autoscale para un grupo de entrega.

### Conceptos básicos

Antes de empezar, obtenga información sobre estos conceptos básicos en Autoscale:

- Horarios
- Búfer de capacidad
- Índice de carga

#### Horarios

Autoscale enciende y apaga máquinas de un grupo de entrega según el horario que usted establezca.

Los horarios incluyen la cantidad de máquinas activas para cada franja horaria, con las horas punta y las horas de actividad normal definidas.

Los parámetros de los horarios varían según el tipo de grupo de entrega. Para obtener más información, consulte:

- Grupos de entrega de SO multisesión
- Grupos de entrega aleatorios de SO de sesión única
- Grupos de entrega estáticos de SO de sesión única

#### Búfer de capacidad

El búfer de capacidad se utiliza para agregar capacidad de reserva a la demanda actual y, así, tener en cuenta los aumentos de carga dinámica. Existen dos casos a tener en cuenta:

- Para los grupos de entrega de SO multisesión, el búfer de capacidad se define como un porcentaje de la capacidad total del grupo de entrega en términos de índice de carga.
- Para los grupos de entrega de SO de sesión única, el búfer de capacidad se define como un porcentaje del total de máquinas del grupo de entrega.

#### Índice de carga

> **IMPORTANTE:**
>
> El índice de carga se aplica solamente a grupos de entrega multisesión.

La métrica del índice de carga determina la probabilidad de que una máquina reciba solicitudes de inicio de sesión de los usuarios. Se calcula mediante la configuración de directiva de **administración de carga de Citrix** definida para el uso simultáneo de inicios de sesión, sesiones, CPU, discos y memoria.

El índice de carga oscila entre 0 y 10 000. De forma predeterminada, una máquina se considera a carga completa cuando aloja 250 sesiones.

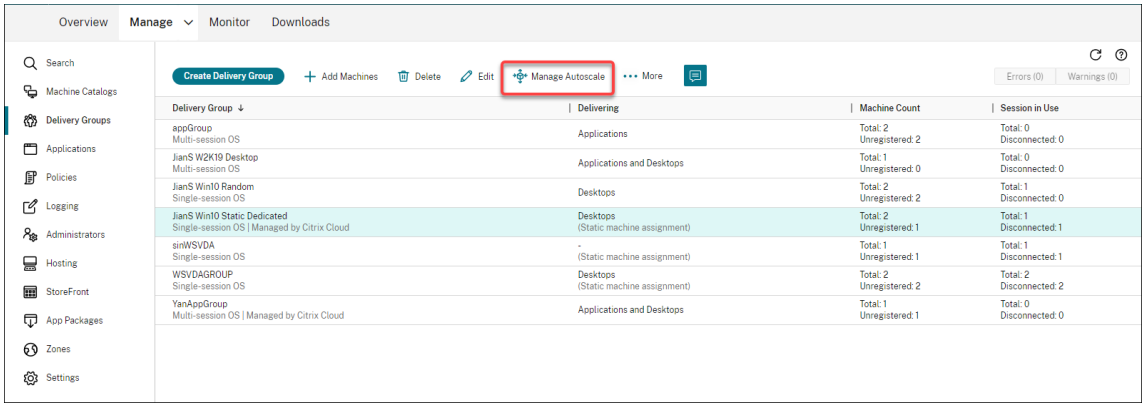
- La cifra “0”indica una máquina descargada. Una máquina con un valor 0 de índice de carga se halla en una carga base.
- La cifra “10 000”indica una máquina completamente cargada que no puede ejecutar más sesiones.

### Habilitar Autoscale para un grupo de entrega

De forma predeterminada, Autoscale está inhabilitado al crear grupos de entrega. Para habilitar y configurar Autoscale para un grupo de entrega mediante la interfaz de Configuración completa, siga estos pasos:

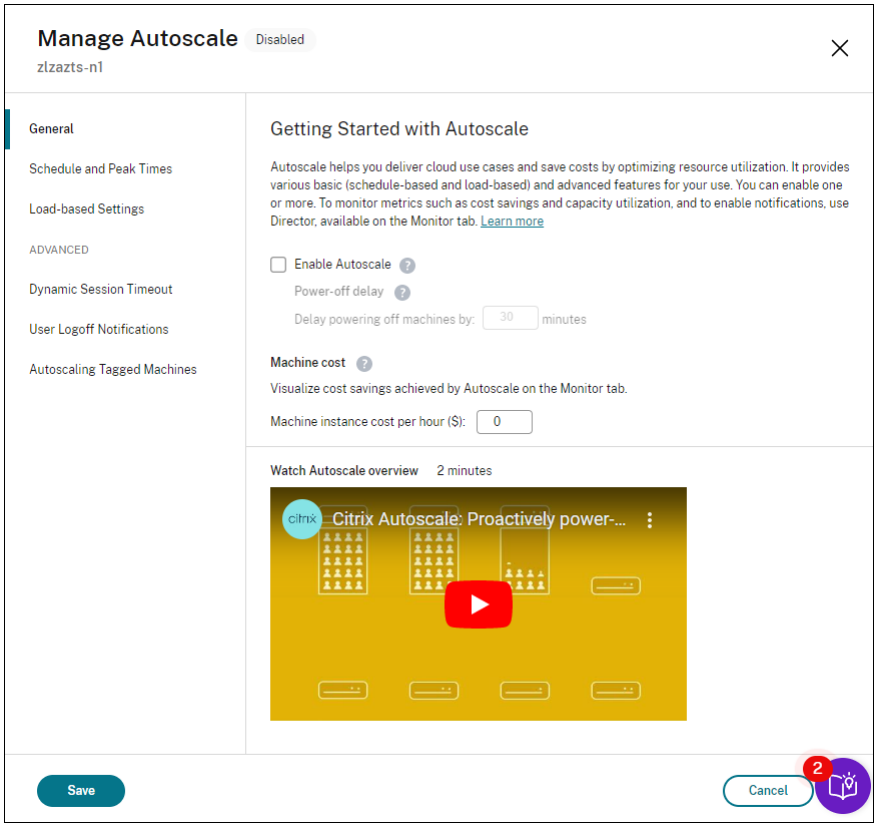
También puede usar comandos de PowerShell para habilitar y configurar Autoscale para un grupo de entrega. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda.
2. Seleccione el grupo de entrega que quiere administrar y, a continuación, haga clic en **Administrar Autoscale**.




3. En la página **Administrar Autoscale**, marque la casilla **Habilitar Autoscale** para activar la función. Después de habilitar Autoscale, se habilitan las opciones de la página.




4. Para cambiar los parámetros predeterminados en función de las necesidades de su organización, complete estos parámetros:

   - Configurar horarios
   - Para apagar máquinas inactivas de manera más eficiente, utilice Tiempos de espera de sesión dinámicos y Notificaciones de cierre de sesión.
   - Para administrar la energía de un subconjunto de máquinas del grupo de entrega, utilice Autoscale de máquinas etiquetadas.

Para inhabilitar Autoscale, desmarque la casilla **Autoscale**. Las opciones de la página quedan atenuadas para indicar que Autoscale no está habilitado en el grupo de entrega seleccionado.

> **Importante:**
>
> - Si inhabilita Autoscale, todas las máquinas administradas por Autoscale permanecen en el estado en que se encuentren al inhabilitarse.
> - Después de inhabilitar Autoscale, las máquinas en estado de purga salen de dicho estado. Para obtener más información sobre el estado de purga, consulte Estado de purga.

Puede aprovisionar máquinas de forma dinámica para el grupo mediante un script de PowerShell. Para obtener más información, consulte Aprovisionamiento dinámico de máquinas.

### Supervisar métricas

Tras habilitar Autoscale para un grupo de entrega, puede supervisar estas métricas de las máquinas administradas por Autoscale desde la ficha **Supervisar**.

- Uso de máquinas
- Ahorro estimado
- Notificaciones de alerta para máquinas y sesiones
- Estado de la máquina
- Tendencias de los patrones de carga

> **Nota:**
>
> Al habilitar inicialmente Autoscale en un grupo de entrega, puede tardar unos instantes en mostrar los datos de supervisión de ese grupo de entrega.
> Los datos de supervisión siguen estando disponibles si Autoscale está habilitado y, a continuación, se inhabilita en el grupo de entrega. Autoscale recopila datos de supervisión en intervalos de 5 minutos.

Para obtener más información sobre las métricas, consulte Supervisar máquinas administradas con Autoscale.

### Información útil

Autoscale funciona a nivel de grupos de entrega. Se configura por grupo de entrega. Administrará la energía solamente de las máquinas que haya en el grupo de entrega seleccionado.

#### Capacidad y registro de máquinas

Autoscale solo incluye máquinas registradas en el sitio al determinar la capacidad. Las máquinas encendidas que no están registradas no pueden aceptar solicitudes de sesión. Como consecuencia, no se incluyen en la capacidad general del grupo de entrega.

#### Escalado en varios catálogos de máquinas

En algunos sitios, es posible que varios catálogos de máquinas estén asociados a un único grupo de entrega. Autoscale enciende de forma aleatoria máquinas de cada catálogo para cumplir con los requisitos de programación o de demanda de sesiones.

Por ejemplo, un grupo de entrega tiene dos catálogos de máquinas: el catálogo A tiene tres máquinas encendidas, y el catálogo B, una. Si Autoscale necesita encender una máquina adicional, es posible que la encienda desde el catálogo A o el catálogo B.

#### Aprovisionamiento de máquinas y demanda de sesiones

El catálogo de máquinas asociado al grupo de entrega debe tener suficientes máquinas para encender y apagar a medida que la demanda aumente o disminuya. Si la demanda de sesiones supera la cantidad total de máquinas registradas en el grupo de entrega, Autoscale garantiza el encendido de todas las máquinas registradas. No obstante, **Autoscale no proporciona máquinas adicionales**.

Para superar este cuello de botella, puede usar un script de PowerShell para crear máquinas y eliminarlas de forma dinámica. Para obtener más información, consulte Aprovisionar máquinas de forma dinámica.

#### Consideraciones sobre el tamaño de las instancias

Puede optimizar los costes si tiene el tamaño adecuado de sus instancias en nubes públicas. Recomendamos aprovisionar instancias más pequeñas siempre que coincidan con los requisitos de capacidad y rendimiento de la carga de trabajo.

Las instancias más pequeñas alojan menos sesiones de usuario que las de mayor tamaño. Por lo tanto, Autoscale pone a las máquinas en estado de purga mucho más rápido porque tarda menos tiempo en cerrar la última sesión de usuario. Como resultado, Autoscale apaga antes las instancias más pequeñas, lo que reduce los costes.

#### Estado de purga

Autoscale intenta reducir la cantidad de máquinas encendidas en el grupo de entrega para equipararla al búfer de capacidad y al tamaño del grupo configurados.

Para lograr este objetivo, Autoscale pone en "estado de purga"las máquinas sobrantes con la menor cantidad de sesiones y las apaga cuando se cierran todas las sesiones. Este comportamiento se da cuando la demanda de sesiones disminuye y la programación requiere menos máquinas de las que están encendidas.

Autoscale pone el exceso de máquinas en "estado de purga"una por una.

- Si dos o más máquinas tienen la misma cantidad de sesiones activas, Autoscale purga la máquina que se ha encendido durante un tiempo equivalente a la demora de apagado especificada.

Al hacerlo, se evita poner máquinas encendidas recientemente en estado de purga porque es más probable que esas máquinas tengan menos sesiones.

- Si se han encendido dos o más máquinas durante un tiempo equivalente a la demora de apagado especificada, Autoscale purga esas máquinas una por una al azar.

Las máquinas en estado de purga ya no alojan nuevos inicios de sesión y esperan a que se cierren las sesiones existentes. Una máquina se convierte en candidata para apagarse únicamente cuando todas las sesiones se cierran. Sin embargo, si no hay máquinas disponibles inmediatamente para iniciar sesión, Autoscale prefiere dirigir los inicios de sesión a una máquina en estado de purga en vez de tener que encender una máquina.

Una máquina sale del estado de purga cuando se cumple una de las siguientes condiciones:

- La máquina se apaga.
- Autoscale se inhabilita para el grupo de entrega al que pertenece la máquina.
- Autoscale utiliza la máquina para cumplir con los requisitos de demanda de carga o programación. Este caso se produce cuando la programación (escalado por programación) o la demanda actual (escalado por carga) requiere más máquinas de la cantidad de máquinas que están actualmente encendidas.

> **Importante:**
>
> Si no hay máquinas disponibles inmediatamente para iniciar sesión, Autoscale prefiere dirigir inicios de sesión a una máquina en estado de purga en vez de tener que encender una máquina. Una máquina en estado de purga que aloja un inicio de sesión permanece en estado de purga.

Para averiguar qué máquinas están en estado de purga, utilice el comando de PowerShell `Get-BrokerMachine`. Por ejemplo: `Get-BrokerMachine -DrainingUntilShutdown $true`. Como alternativa, puede utilizar la consola Administrar. Consulte, Mostrar máquinas en estado de purga.

#### Mostrar máquinas en estado de purga

> **Nota:**
>
> Esta función solo se aplica a máquinas multisesión.

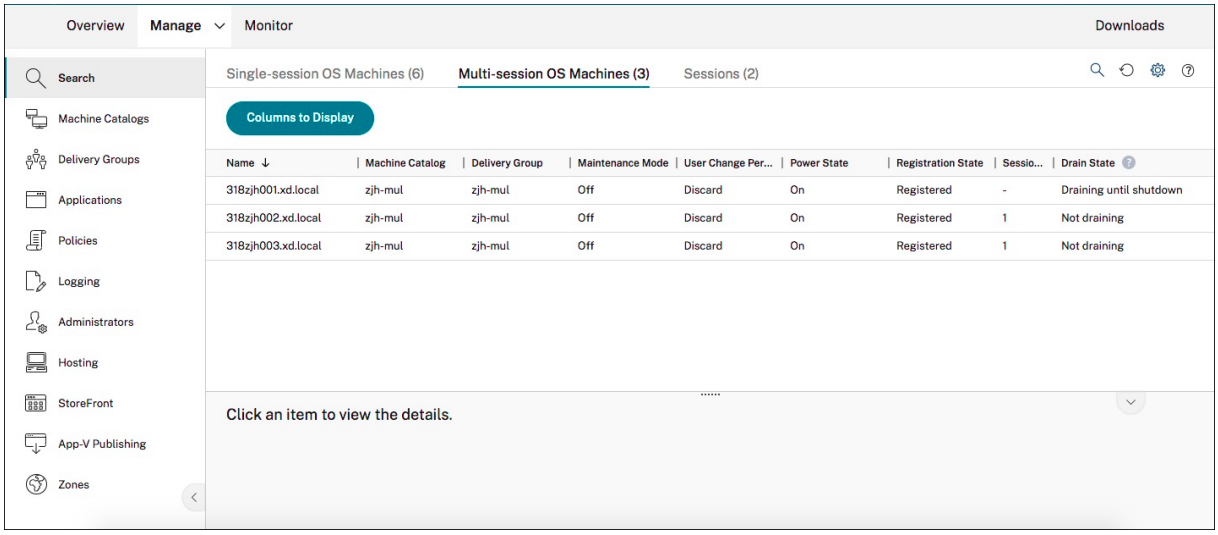
En **Administrar > Configuración completa**, puede mostrar máquinas que están en estado de purga, lo que le permite saber qué máquinas están a punto de apagarse. Siga estos pasos:

1. Vaya al nodo **Buscar** y, a continuación, haga clic en **Columnas que mostrar**.
2. En la ventana **Columnas que mostrar**, marque la casilla situada junto a **Estado de la purga**.
3. Haga clic en **Guardar** para salir de la ventana **Columnas que mostrar**.

La columna **Estado de la purga** puede mostrar esta información:

- **Purga hasta el apagado.** Aparece cuando las máquinas se hallan en estado de purga hasta que se apagan.
- **Sin purga.** Aparece cuando las máquinas aún no se hallan en estado de purga.




### Más información

Para obtener más información sobre Autoscale, consulte Citrix Autoscale en Tech Zone.

## Parámetros basados en la programación y en la carga

October 30, 2023

### Cómo administra Autoscale la energía de las máquinas

Autoscale enciende y apaga las máquinas en función de la programación seleccionada. Autoscale permite establecer varias programaciones que incluyen días específicos de la semana y ajustar la cantidad de máquinas disponibles durante esos días. Si espera que un conjunto de usuarios consuma los recursos de las máquinas a una hora específica en días específicos, Autoscale ayuda a proporcionar una experiencia optimizada. Tenga en cuenta que esas máquinas se encenderán durante la programación, independientemente de si hay sesiones activas en ellas.

> **Nota:**
>
> Autoscale admite cualquier máquina con administración de energía.

La programación se basa en la **zona horaria** del grupo de entrega. Para cambiar la zona horaria, puede cambiar la configuración del usuario en un grupo de entrega. Para obtener más información, consulte Administración de grupos de entrega.

Autoscale tiene dos horarios: *días laborables* (de lunes a viernes) y *fin de semana* (sábado y domingo). De forma predeterminada, la programación de **días laborables** mantiene una máquina encendida entre las 7:00 y las 18:30 durante las horas punta y ninguna durante las horas normales. El búfer de capacidad predeterminado se establece en 10% durante las horas punta y las horas normales De forma predeterminada, la programación de **fin de semana** no mantiene ninguna máquina encendida.

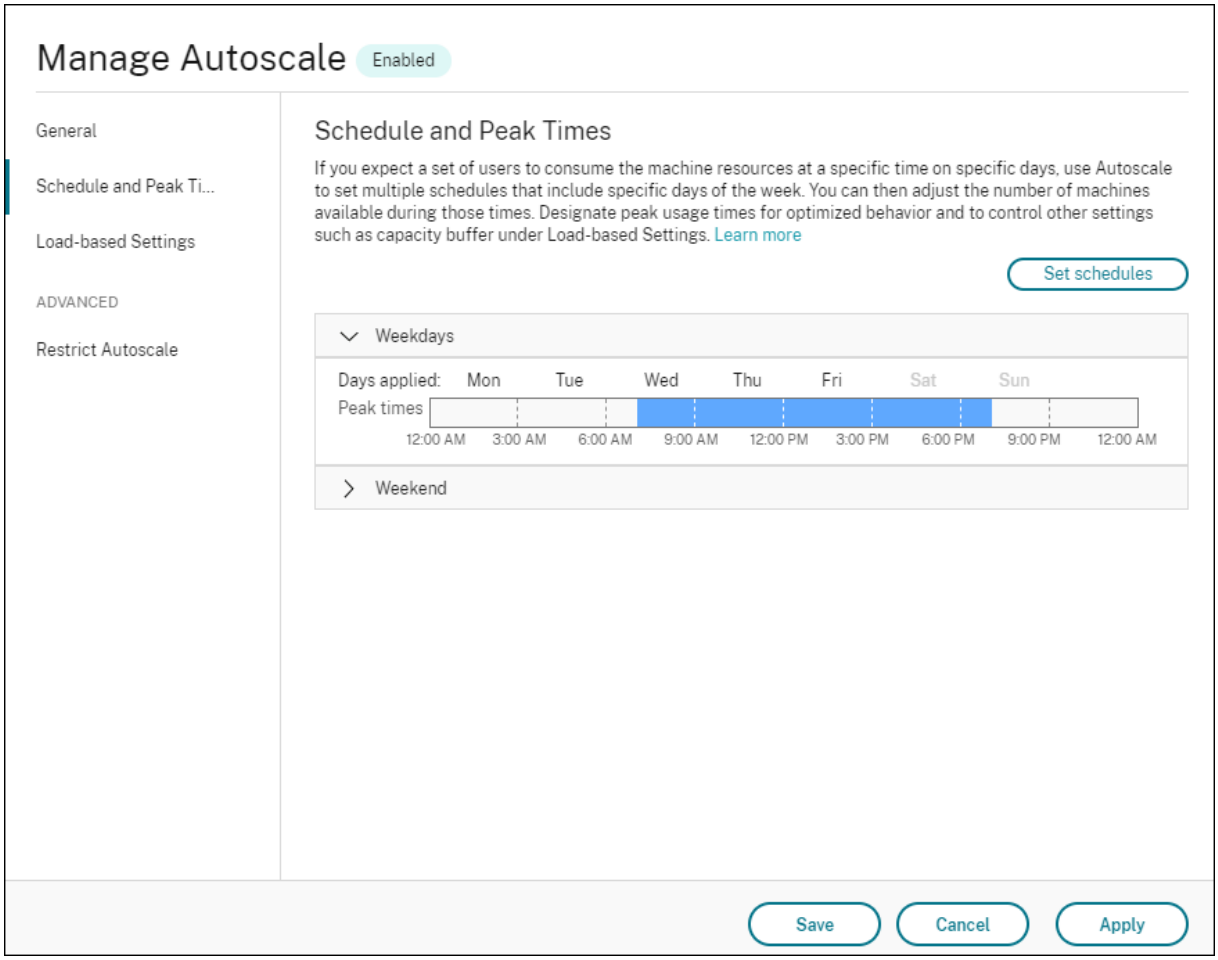
> **Nota:**
>
> Autoscale trata solamente aquellas máquinas que estén registradas en el sitio como parte de la capacidad disponible en los cálculos que realiza. "Registrado"significa que la máquina puede utilizarse o que ya se está utilizando. Esto asegura que solamente las máquinas que pueden aceptar sesiones de usuario se incluyan en la capacidad del grupo de entrega.

### Interfaces de usuario

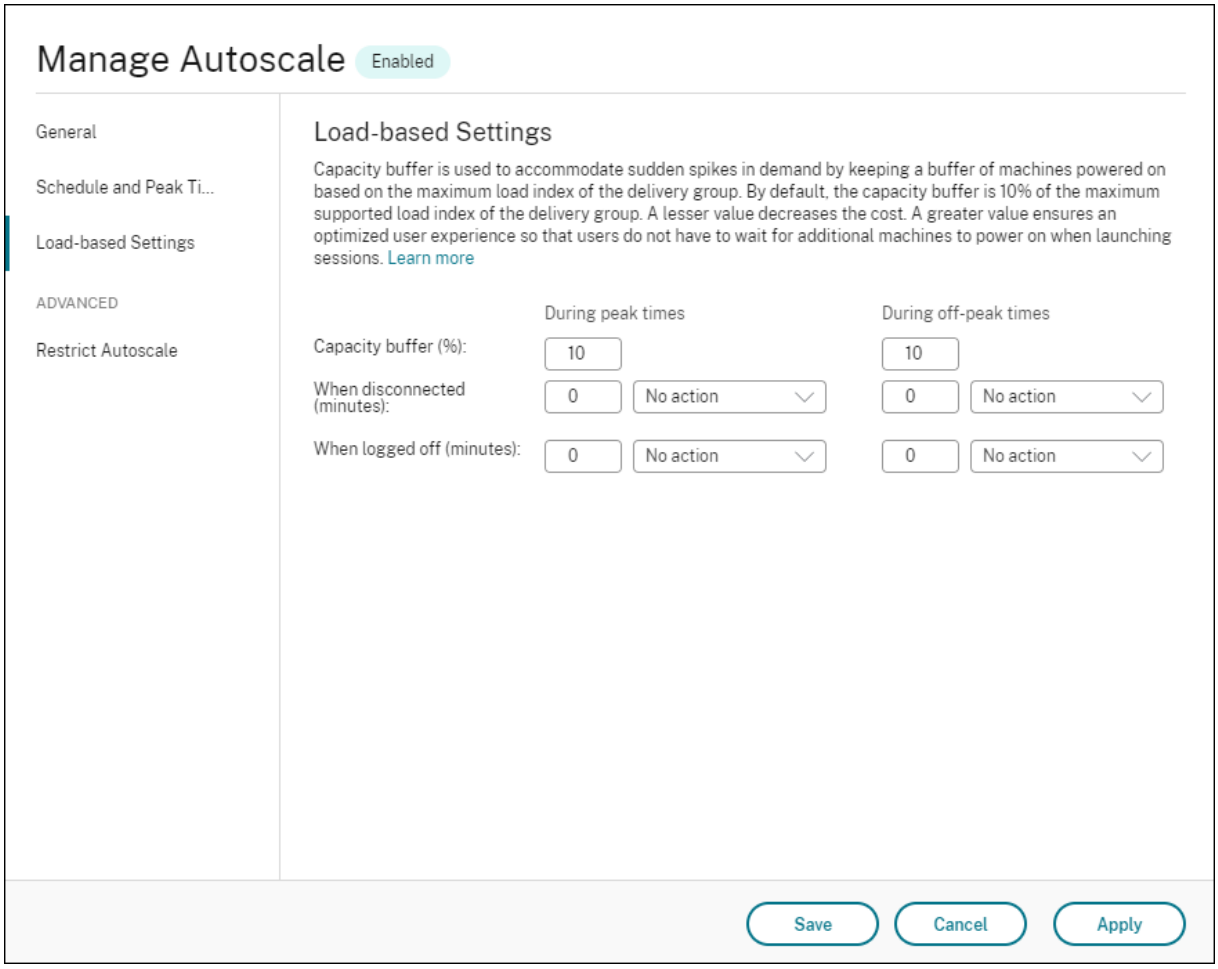
Hay tres tipos de interfaces de usuario a tener en cuenta.

Interfaz de usuario para *grupos de entrega estáticos de SO de sesión única*:

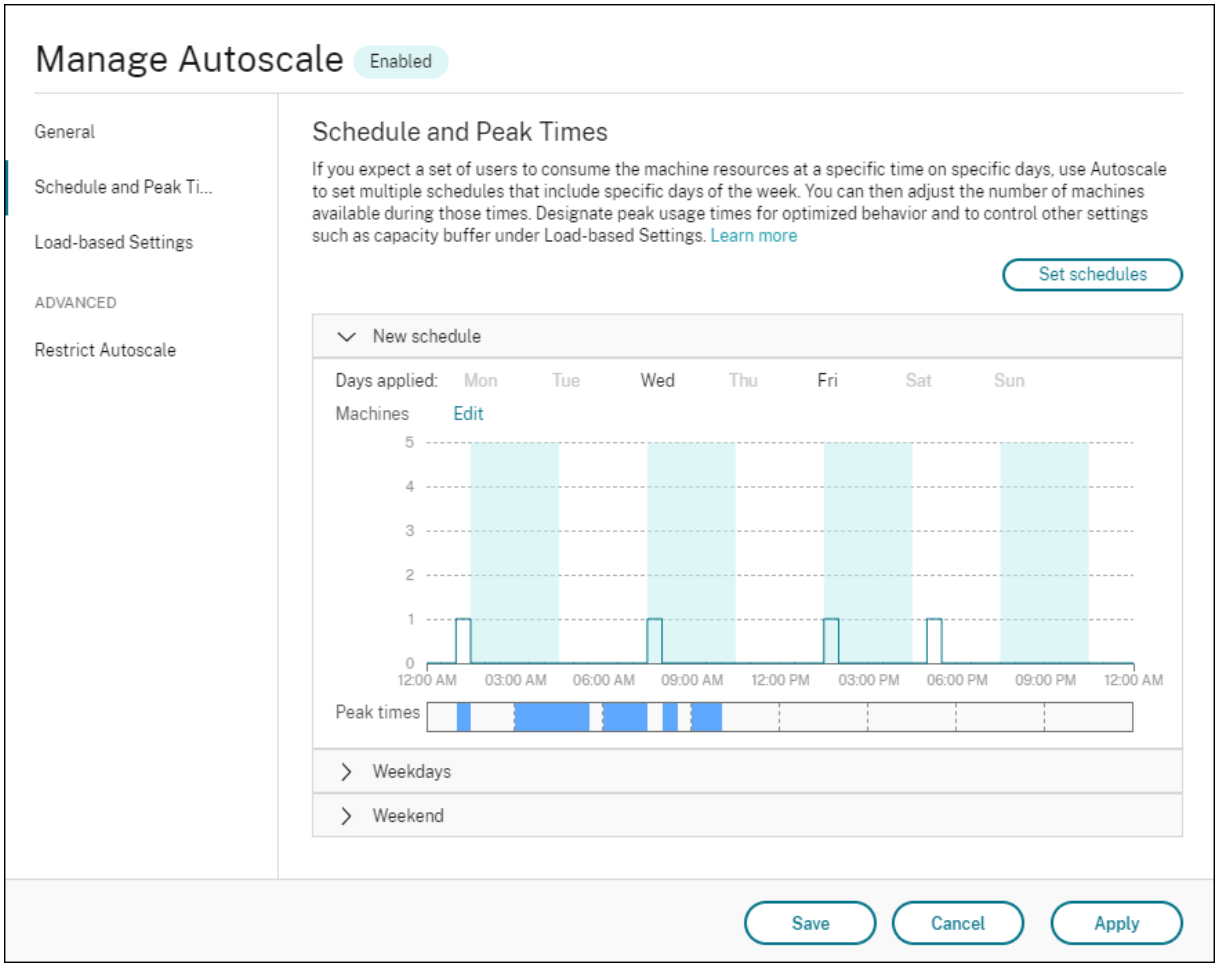


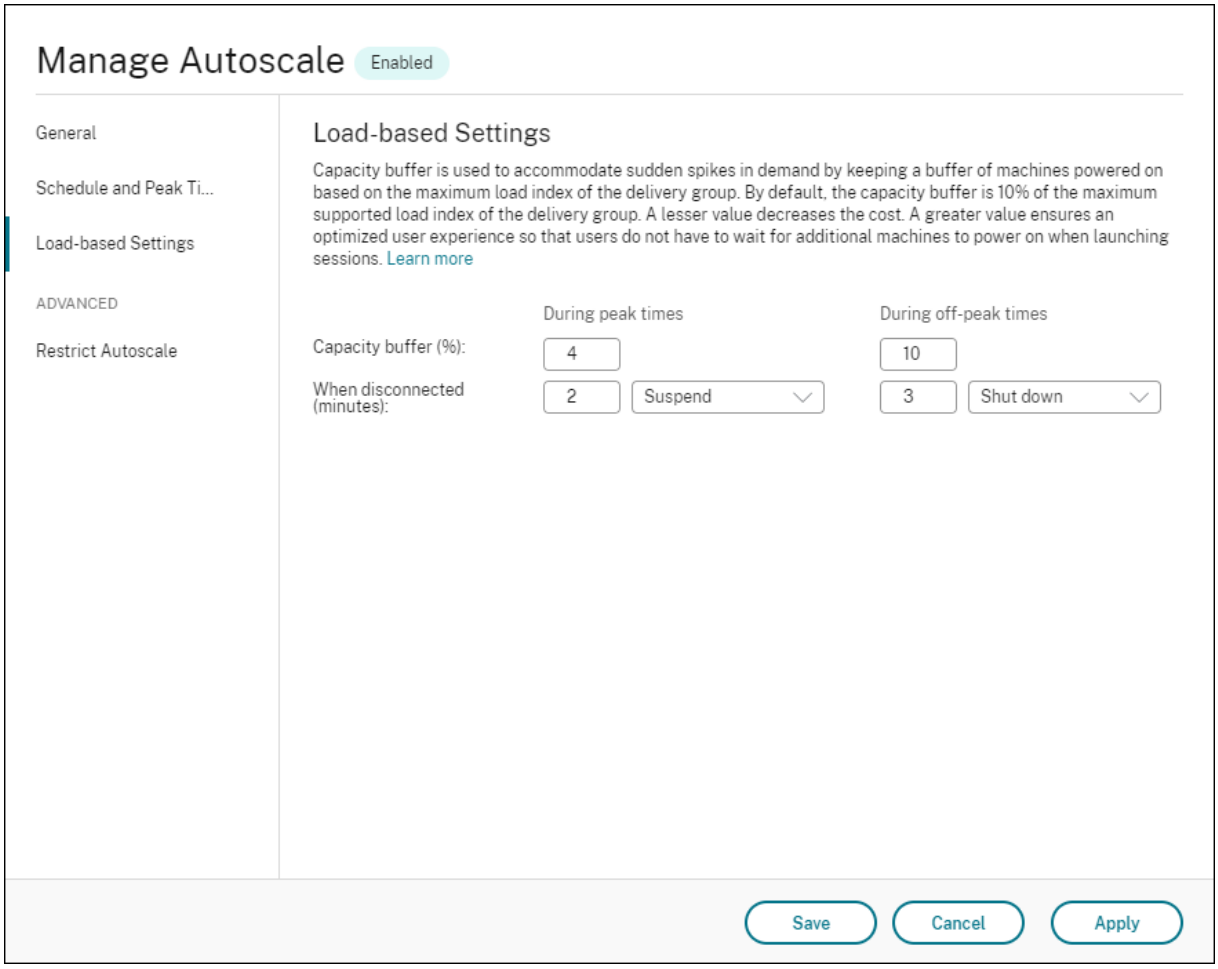



Interfaz de usuario de Autoscale para *grupos de entrega aleatorios de SO de sesión única*:

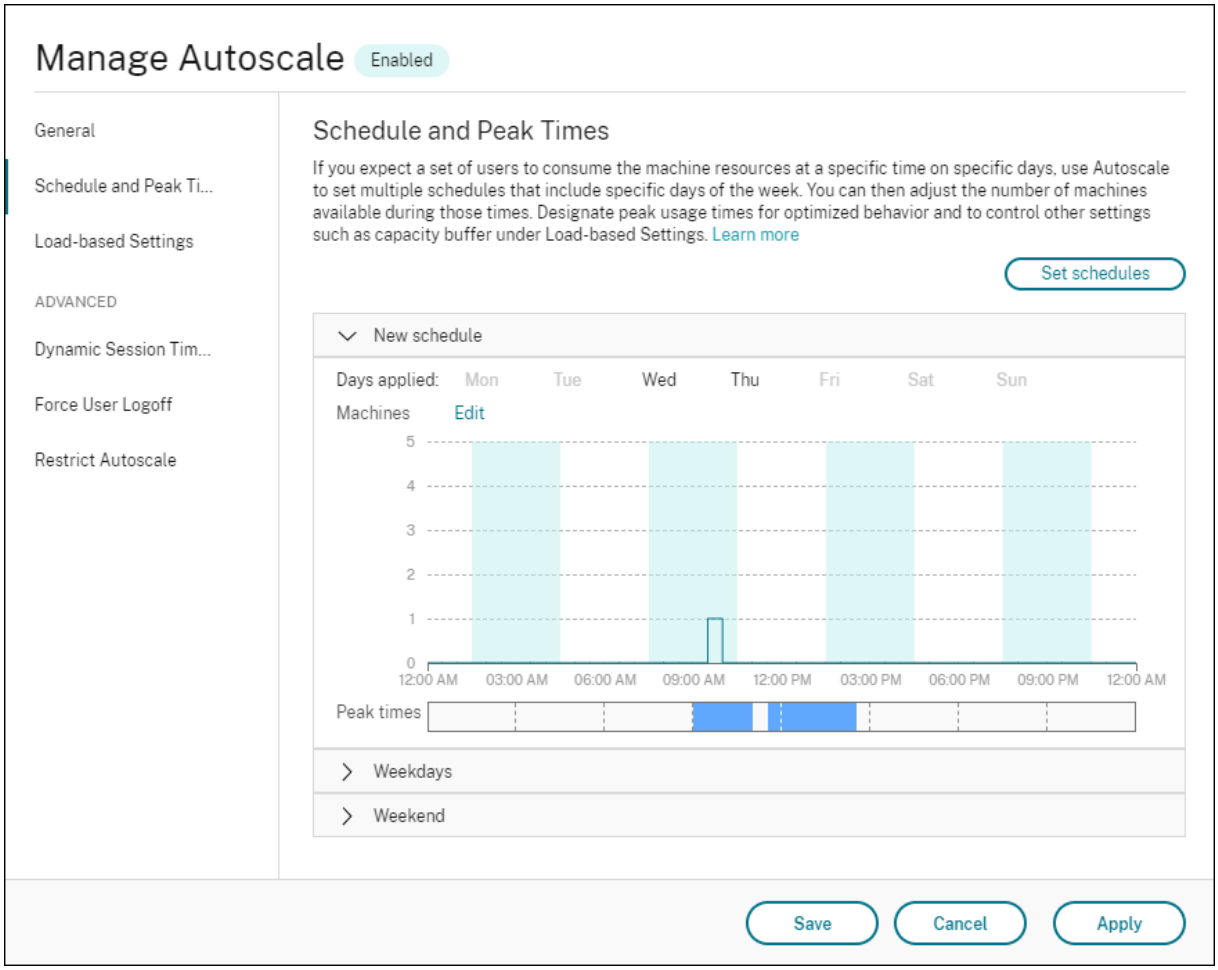


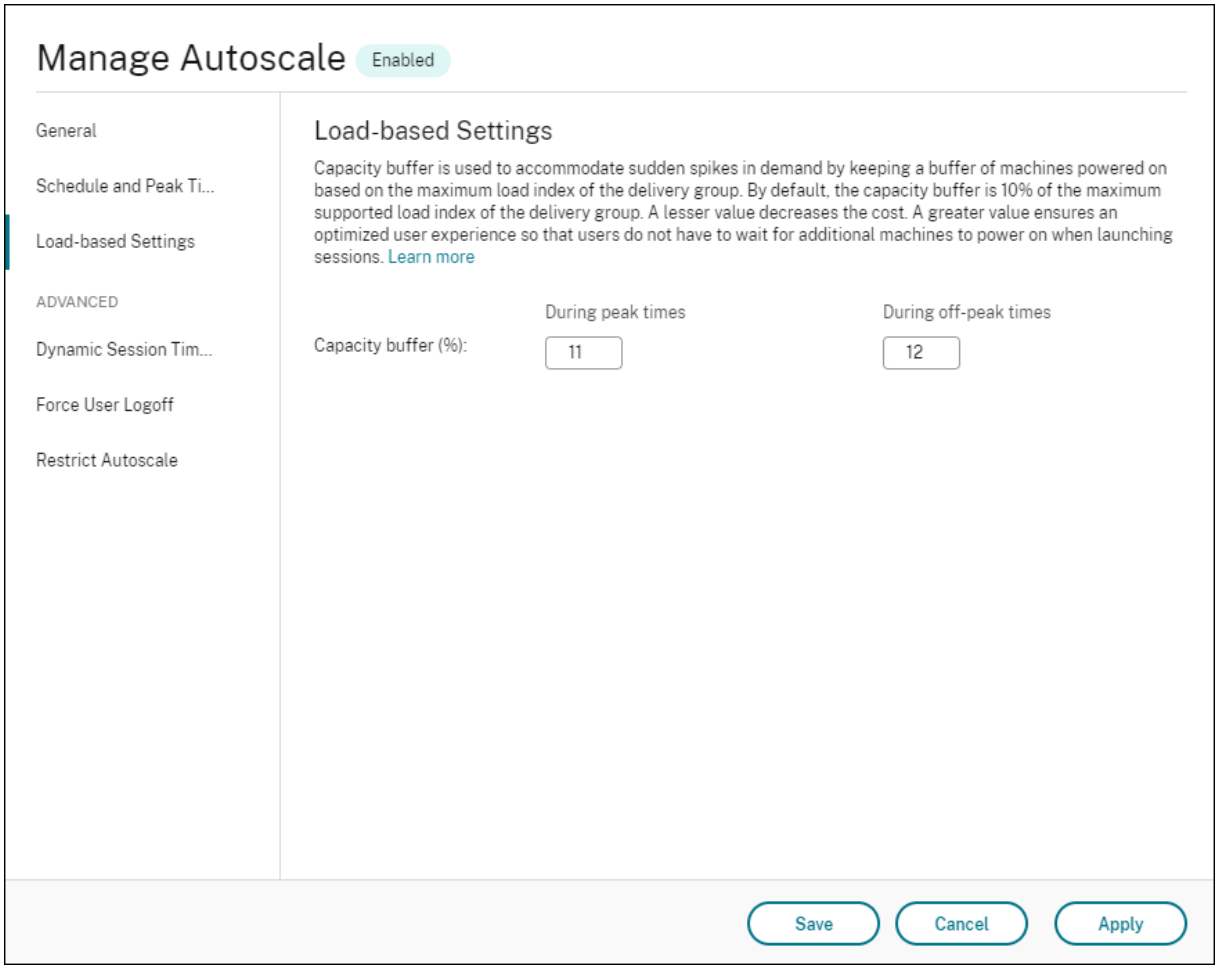



Interfaz de usuario de Autoscale para *grupos de entrega de SO multisesión*:






### Configuración basada en la programación

**Programación de Autoscale**. Permite agregar, modificar, seleccionar y eliminar programaciones.

**Días aplicados**. Resalta los días aplicados a la programación seleccionada. Los días restantes quedan atenuados.

**Modificar**. Permite asignar las máquinas en cada hora o cada media hora. Puede asignar las máquinas por cantidad y por porcentaje.

> **Nota:**
>
> - Esta opción solo está disponible en las interfaces de usuario de Autoscale para grupos de entrega aleatorios de SO multisesión y SO de sesión única.
> - El histograma situado junto a **Modificar** muestra la cantidad o el porcentaje de máquinas activas en diferentes intervalos de tiempo.
> - Puede **asignar máquinas** en cada intervalo de tiempo a través de la opción **Modificar** situada encima de **Horas punta**. Según la opción que haya seleccionado en el menú de la ven-

tana **Máquinas para iniciar**, puede asignar las máquinas por cantidad o por porcentaje.
- Para los grupos de entrega de SO multisesión, puede establecer por separado la cantidad mínima de máquinas activas en incrementos granulares de 30 minutos durante cada día. Para los grupos de entrega aleatorios de SO de sesión única, puede establecer por separado la cantidad mínima de máquinas activas en incrementos granulares de 60 minutos durante cada día.

Para definir sus propias programaciones, siga estos pasos:

1. En la página **Programación y horas punta** de la ventana **Administrar Autoscale**, haga clic en **Establecer programaciones**.
2. En la ventana **Modificar programaciones de Autoscale**, seleccione los días que quiere aplicar a cada programación. También puede suprimir programaciones cuando corresponda.
3. Haga clic en **Listo** para guardar las programaciones y volver a la página **Programación y horas punta**.
4. Seleccione la programación correspondiente y configúrela según sea necesario.
5. Haga clic en **Aplicar** para salir de la ventana **Administrar Autoscale** o configurar los parámetros en otras páginas.

**Importante:**

- Autoscale no permite que el mismo día coincida en diferentes programaciones. Por ejemplo, si selecciona Lunes en la programación2 después de seleccionar Lunes en la programación1, el lunes se borra automáticamente en la programación1.
- El nombre de las programaciones no distingue entre mayúsculas y minúsculas.
- El nombre de las programaciones no debe estar vacío ni contener solamente espacios.
- Autoscale permite espacios vacíos entre caracteres.
- Los nombres de las programaciones no deben contener estos caracteres: \ / ; : # . * ? = < > | [ ] ( ) { } ‘“‘
- Autoscale no admite nombres duplicados para las programaciones. Introduzca un nombre distinto para cada programa.
- Autoscale no admite programaciones vacías. Esto significa que las programaciones sin días seleccionados no se guardan.

**Nota:**

Los días incluidos en la programación seleccionada quedan resaltados, mientras que los no incluidos aparecen atenuados.

### Configuración basada en la carga

**Horas punta**. Permite definir las horas punta de los días aplicados en la programación seleccionada. Para ello, haga clic con el botón secundario en el gráfico de barras horizontales. Tras definir las horas punta, las horas restantes y sin definir son, de manera predeterminada, horas normales. **De forma predeterminada**, el intervalo horario de 7:00 a 19:00 se define como horas punta en los días incluidos en la programación seleccionada.

> **Importante:**
>
> - Para los grupos de entrega de SO multisesión, el gráfico de barras de las horas punta se utiliza para el búfer de capacidad.
> - Para los grupos de entrega de SO de sesión única, el gráfico de barras de las horas punta se utiliza para el búfer de capacidad y controla las acciones que se desencadenarán después de una desconexión o un cierre de sesión.
> - Se pueden definir las horas punta que tendrán los días incluidos en una programación con una precisión de 30 minutos tanto para los grupos de entrega de SO multisesión como para los de SO de sesión única. También puede usar el comando New-BrokerPowerTimeScheme PowerShell. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.

**Búfer de capacidad**. Le permite mantener un búfer de máquinas encendidas. Un valor menor disminuye el coste. Un valor mayor garantiza una experiencia de usuario optimizada para que, al iniciar sesiones, los usuarios no tengan que esperar a que se enciendan máquinas adicionales. De forma predeterminada, el búfer de capacidad es del 10% para las horas punta y las horas normales. Si establece el búfer de capacidad en 0 (cero), es posible que los usuarios tengan que esperar a que se enciendan máquinas adicionales al iniciar las sesiones. Autoscale permite determinar el búfer de capacidad por separado para las horas punta y las horas normales.

### Otros parámetros

> **Sugerencia:**
>
> - Puede configurar las opciones diversas mediante el SDK de Broker PowerShell. Para obtener más información, consulte Comandos del SDK de Broker PowerShell.
> - Para entender los comandos del SDK asociados a la configuración de cuando se desconecta y cuando se cierra la sesión, consulte https://citrix.github.io/delivery-controller-sdk/Broker/about_Broker_PowerManagement/#power-policy.

**Cuando está desconectado**. Le permite especificar el tiempo que una máquina desconectada y bloqueada permanece encendida después de la desconexión de una sesión antes de que la máquina se suspenda o se apague. Si se especifica un valor de tiempo, la máquina se suspende o se apaga cuando

haya transcurrido el tiempo de desconexión especificado según la acción que haya configurado. De forma predeterminada, no se asigna ninguna acción a las máquinas desconectadas. Puede definir acciones por separado para las horas punta y las horas normales. Para ello, haga clic en la flecha hacia abajo y, a continuación, seleccione una de las siguientes opciones en el menú:

- **Ninguna acción**. Si se selecciona, la máquina, después de que la sesión se haya desconectado, permanece encendida. Autoscale no interviene.
- **Suspender**. Si se selecciona, Autoscale pausa la máquina sin apagarla una vez transcurrido el tiempo de desconexión especificado. La siguiente opción está disponible después de seleccionar **Suspender**.
  - **Al no reconectarse en (minutos)**. Las máquinas suspendidas permanecen disponibles para los usuarios desconectados cuando se vuelven a conectar, pero no están disponibles para nuevos usuarios. Para que las máquinas estén disponibles de nuevo para manejar todas las cargas de trabajo, apáguelas. Especifique el tiempo de espera, en minutos, tras el cual Autoscale las apaga.
- **Apagar**. Si se selecciona, Autoscale apaga la máquina una vez transcurrido el tiempo de desconexión especificado.

> **Nota:**
>
> Esta opción solo está disponible en las interfaces de usuario de Autoscale para grupos de entrega aleatorios y estáticos de SO de sesión única.

**Al cerrar la sesión**. Permite especificar el tiempo que una máquina permanece encendida después de cerrar sesión antes de que la máquina se suspenda o se apague. Si se especifica un valor de tiempo, la máquina se suspende o se apaga cuando haya transcurrido el tiempo de cierre de sesión especificado según las acciones que haya configurado. De forma predeterminada, no se asigna ninguna acción a las máquinas cuya sesión se haya cerrado. Puede definir acciones por separado para las horas punta y las horas normales. Para ello, haga clic en la flecha hacia abajo y, a continuación, seleccione una de las siguientes opciones en el menú:

- **Ninguna acción**. Si se selecciona, la máquina, después de que la sesión se haya cerrado, permanece encendida. Autoscale no interviene.
- **Suspender**. Si se selecciona, Autoscale pausa la máquina sin apagarla una vez transcurrido el tiempo de cierre de sesión especificado.
- **Apagar**. Si se selecciona, Autoscale apaga la máquina una vez transcurrido el tiempo de cierre de sesión especificado.

> **Nota:**
>
> Esta opción solo está disponible en las interfaces de usuario de Autoscale para grupos de entrega

> estáticos de SO de sesión única.

**Administrar la energía de máquinas con SO de sesión única que pasan a otro período de tiempo con sesiones desconectadas**

> **Importante:**
>
> - Esta mejora solo se aplica a máquinas con SO de sesión única y sesiones desconectadas. No se aplica a máquinas con SO de sesión única y sesiones cerradas.
> - Para que esta mejora surta efecto, debe habilitar Autoscale para el grupo de entrega correspondiente. De lo contrario, las acciones de directiva de energía para desconexiones no se activan al cambiar de período.

En versiones anteriores, las máquinas con SO de sesión única que pasaban a un período de tiempo en el que se requería una acción (acción de desconexión=”**Suspender**”o “**Apagar**”) permanecían encendidas. Este caso se producía si la máquina se desconectaba durante un período de tiempo (horas punta u horas normales) donde no se requería ninguna acción (acción de desconexión=”**Nada**”).

A partir de esta versión, Autoscale suspende o apaga las máquinas cuando transcurre el tiempo de desconexión especificado, en función de la acción de desconexión configurada para el período de tiempo de destino.

Por ejemplo, configure estas directivas de energía para un grupo de entrega de SO de sesión única:

- Establezca `PeakDisconnectAction` en “Nada”
- Establezca `OffPeakDisconnectAction` en “Apagar”
- Establezca “OffPeakDisconnectTimeout”en “10”

> **Nota:**
>
> Para obtener más información sobre la directiva de energía para las acciones de desconexión, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/about_Broker_PowerManagement/#power-policy y https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

En versiones anteriores, una máquina con SO de sesión única y una sesión desconectada durante horas punta permanecía encendida cuando pasaba del período de horas punta al de horas normales. A partir de esta versión, las acciones de directiva `OffPeakDisconnectAction` y `OffPeakDisconnectTimeout` se aplican a la máquina con SO de sesión única al cambiar de período. Como resultado, la máquina se apaga 10 minutos después de pasar a las horas normales.

En caso de que quiera volver al comportamiento anterior (es decir, no realizar ninguna acción en máquinas que pasen de horas punta a horas normales o de horas normales a horas punta con sesiones desconectadas), dispone de varias opciones:

- Establezca el valor del Registro "LegacyPeakTransitionDisconnectedBehaviour"en 1 (true; habilita el comportamiento anterior). De forma predeterminada, el valor es 0 (false; desencadena acciones de directiva de energía para desconexiones al cambiar de período).
  - Ruta: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer
  - Nombre: LegacyPeakTransitionDisconnectedBehaviour
  - Tipo: REG_DWORD
  - Datos: 0x00000001 (1)
- Configure el parámetro mediante el comando `Set-BrokerServiceConfigurationData` de PowerShell. Por ejemplo:
  - `PS C:\> Set-BrokerServiceConfigurationData HostingManagement.LegacyPeakTransitionDisconnectedBehaviour -SettingValue $true`

Las máquinas deben cumplir los siguientes criterios antes de que se puedan aplicar acciones de directiva de energía al cambiar de período:

- Tiene una sesión desconectada.
- No tiene acciones de energía pendientes.
- Pertenece a un grupo de entrega de SO de sesión única que pasa a otro período de tiempo.
- Tiene una sesión que se desconecta durante un período de tiempo determinado (horas pico u horas normales) y pasa a un período en el que se asigna una acción de energía.

### Cómo funciona el búfer de capacidad

El búfer de capacidad se utiliza para agregar capacidad de reserva a la demanda actual y, así, tener en cuenta los aumentos de carga dinámica. Existen dos casos a tener en cuenta:

- Para los grupos de entrega de SO multisesión, el búfer de capacidad se define como un porcentaje de la capacidad total del grupo de entrega en términos de índice de carga. Para obtener más información acerca del índice de carga, consulte Índice de carga.
- Para los grupos de entrega de SO de sesión única, el búfer de capacidad se define como un porcentaje de la capacidad total del grupo de entrega en términos de cantidad de máquinas.

> **Nota:**
>
> En situaciones en las que se restringe Autoscale a las máquinas etiquetadas, el búfer de capacidad se define como un porcentaje de la capacidad total de las máquinas etiquetadas del grupo de entrega en términos de índice de carga.

Autoscale le permite establecer el búfer de capacidad por separado para las horas punta y las horas normales. Un valor menor en el campo de búfer de capacidad disminuye el coste porque Autoscale utiliza energía de una capacidad de reserva menor. Un valor mayor garantiza una experiencia de usuario

optimizada para que los usuarios no tengan que esperar a que se enciendan máquinas adicionales al iniciar sesiones. De forma predeterminada, el búfer de capacidad es del 10%.

> **Importante:**
>
> El búfer de capacidad provoca que las máquinas se enciendan cuando la capacidad total de reserva cae por debajo de un "X"por ciento de la capacidad total del grupo de entrega. Esto reserva el porcentaje requerido de la capacidad de reserva.

## Grupos de entrega de SO multisesión

### ¿Cuándo se encienden las máquinas?

> **Importante:**
>
> Si se selecciona una programación, Autoscale enciende todas las máquinas configuradas para encenderse en la programación. Autoscale mantiene encendida esta cantidad especificada de máquinas durante la programación, independientemente de la carga.

Cuando la cantidad de máquinas encendidas en el grupo de entrega ya no satisface la demanda deseada para respetar la capacidad del búfer en términos de índice de carga, Autoscale enciende máquinas adicionales. Por ejemplo, un grupo de entrega tiene 20 máquinas, y 3 están programadas para encenderse como parte del escalado programado con un búfer de capacidad del 20 %. Al final, 4 máquinas se encenderán cuando no haya carga. Esto se debe a que se necesita un índice de carga de 4 x 10 k como búfer; por lo tanto, al menos 4 máquinas deben encenderse. Es posible que esto se produzca durante horas punta, un aumento de la carga en las máquinas, el inicio de nuevas sesiones y al agregar nuevas máquinas al grupo de entrega. Tenga en cuenta que Autoscale solo enciende las máquinas que cumplen los siguientes criterios:

- Las máquinas no se hallan en modo de mantenimiento.
- El hipervisor en el que se ejecutan las máquinas no está en modo de mantenimiento.
- Las máquinas están actualmente apagadas.
- Las máquinas no tienen ninguna acción de energía pendiente.

### ¿Cuándo se apagan las máquinas?

> **Importante:**
>
> - Si se selecciona una programación, Autoscale apaga las máquinas en función de la programación.
> - Autoscale no apaga las máquinas configuradas en la programación para encenderse du-

> rante la programación.

Cuando hay más máquinas de las suficientes para admitir la cantidad deseada de máquinas encendidas (búfer incluido) en el grupo de entrega, Autoscale apaga las máquinas adicionales. Es posible que esto se produzca durante horas de actividad normal, una disminución de la carga en las máquinas, el cierre de sesiones y al quitar máquinas del grupo de entrega. Autoscale apaga solamente las máquinas que cumplen los siguientes criterios:

- Las máquinas y el hipervisor en el que estas se ejecutan no están en modo de mantenimiento.
- Las máquinas están actualmente encendidas.
- Las máquinas están registradas como disponibles o a la espera de registrarse después de la puesta en marcha.
- Las máquinas no tienen sesiones activas.
- Las máquinas no tienen ninguna acción de energía pendiente.
- Las máquinas satisfacen la demora de apagado especificada. Esto significa que las máquinas se encendieron durante al menos "X"minutos, donde "X"es la demora de apagado especificada para el grupo de entrega.

#### Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del grupo de entrega**. El grupo de entrega al que quiere aplicar Autoscale para administrar la energía contiene 10 máquinas (de M1 a M10).
- **Configuración de Autoscale**
  - El búfer de capacidad es del 10%.
  - No se incluye ninguna máquina en la programación seleccionada.

El escenario se desarrolla de la siguiente manera:

1. Ningún usuario inicia sesión.
2. Las sesiones de usuario aumentan.
3. Se inician más sesiones de usuario.
4. La carga por sesión de usuario disminuye por la finalización de sesiones.
5. La carga de sesiones de usuario disminuye aún más hasta que la carga de sesiones se controla solamente mediante recursos locales.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Sin carga de usuarios (estado inicial)
  - Se enciende una máquina (por ejemplo, M1). La máquina se enciende debido al búfer de capacidad configurado. En este caso, 10 (cantidad de máquinas) x 10 000 (índice de carga) x 10% (búfer de capacidad configurado) equivale a 10 000. Por lo tanto, se enciende una máquina.
  - El valor del índice de carga de la máquina encendida (M1) se halla en una carga base (el índice de carga es igual a 0).
- El primer usuario inicia sesión
  - La sesión se dirige para alojarse en la máquina M1.
  - El índice de carga de la máquina encendida M1 aumenta y la máquina M1 deja de estar en una carga base.
  - Autoscale comienza a encender una máquina adicional (M2) para satisfacer la demanda debido al búfer de capacidad configurado.
  - El valor del índice de carga de la máquina M2 se halla en una carga base.
- Los usuarios aumentan la carga
  - Se equilibra la carga de las sesiones entre las máquinas M1 y M2. Como resultado, aumenta el índice de carga de las máquinas encendidas (M1 y M2).
  - La capacidad total de reserva sigue estando por encima de 10 000 en términos de índice de carga.
  - El valor del índice de carga de la máquina M2 deja de estar en una carga base.
- Se inician más sesiones de usuario
  - Se equilibra la carga de las sesiones entre las máquinas (M1 y M2). Como resultado, aumenta todavía más el índice de carga de las máquinas encendidas (M1 y M2).
  - Cuando la capacidad total de reserva cae por debajo de 10 000 en términos de índice de carga, Autoscale comienza a encender una máquina adicional (M3) para satisfacer la demanda debido al búfer de capacidad configurado.
  - El valor del índice de carga de la máquina M3 se halla en una carga base.
- Se inician todavía más sesiones de usuario
  - Se equilibra la carga de las sesiones entre las máquinas (M1 y M3). Como resultado, aumenta el índice de carga de las máquinas encendidas (M1 y M3).
  - La capacidad total de reserva está por encima de 10 000 en términos de índice de carga.
  - El valor del índice de carga de la máquina M3 deja de estar en una carga base.
- La carga de las sesiones de usuario disminuye debido a la finalización de sesiones

  - Después de que los usuarios hayan cerrado sus sesiones o tras agotarse el tiempo de espera de las sesiones inactivas, la capacidad liberada de las máquinas M1 a M3 se reutiliza para alojar sesiones iniciadas por otros usuarios.
  - Cuando la capacidad total de reserva está por encima de 10 000 en términos de índice de carga, Autoscale pone una de las máquinas (por ejemplo, M3) en estado de purga. Como resultado, las sesiones iniciadas por otros usuarios ya no se dirigen a esa máquina, a no ser que ocurran nuevos cambios. Por ejemplo, la carga del usuario final aumenta de nuevo u otras máquinas tienen menor carga.

- La carga de las sesiones de usuario continúa disminuyendo
  - Una vez finalizadas todas las sesiones de la máquina M3 y transcurrida la demora de apagado especificada, Autoscale apaga la máquina M3.
  - Una vez que más usuarios hayan finalizado sus sesiones, la capacidad liberada en máquinas encendidas (M1 y M2) se reutiliza para alojar sesiones iniciadas por otros usuarios.
  - Cuando la capacidad total de reserva está por encima de 10 000 en términos de índice de carga, Autoscale pone una de las máquinas (por ejemplo, M2) en estado de purga. Como resultado, las sesiones iniciadas por otros usuarios ya no se dirigen a esa máquina.
- La carga de las sesiones de usuario continúa disminuyendo hasta que no queden sesiones
  - Una vez finalizadas todas las sesiones de la máquina M2 y transcurrida la demora de apagado especificada, Autoscale apaga la máquina M2.
  - El valor del índice de carga de la máquina encendida (M1) se halla en una carga base. Autoscale no pone la máquina M1 en estado de purga debido al búfer de capacidad configurado.

> **Nota:**
>
> Para los grupos de entrega de SO multisesión, todos los cambios en el escritorio se pierden cuando los usuarios cierran la sesión. Sin embargo, si se configuran, los parámetros específicos del usuario se mueven junto con el perfil de usuario.

### Grupos de entrega aleatorios de SO de sesión única

El búfer de capacidad se utiliza para adaptarse a picos repentinos de demanda y, al mismo tiempo, mantener un búfer de máquinas encendidas en función de la cantidad total de máquinas del grupo de entrega. De forma predeterminada, el búfer de capacidad es el 10 % de la cantidad total de máquinas del grupo de entrega.

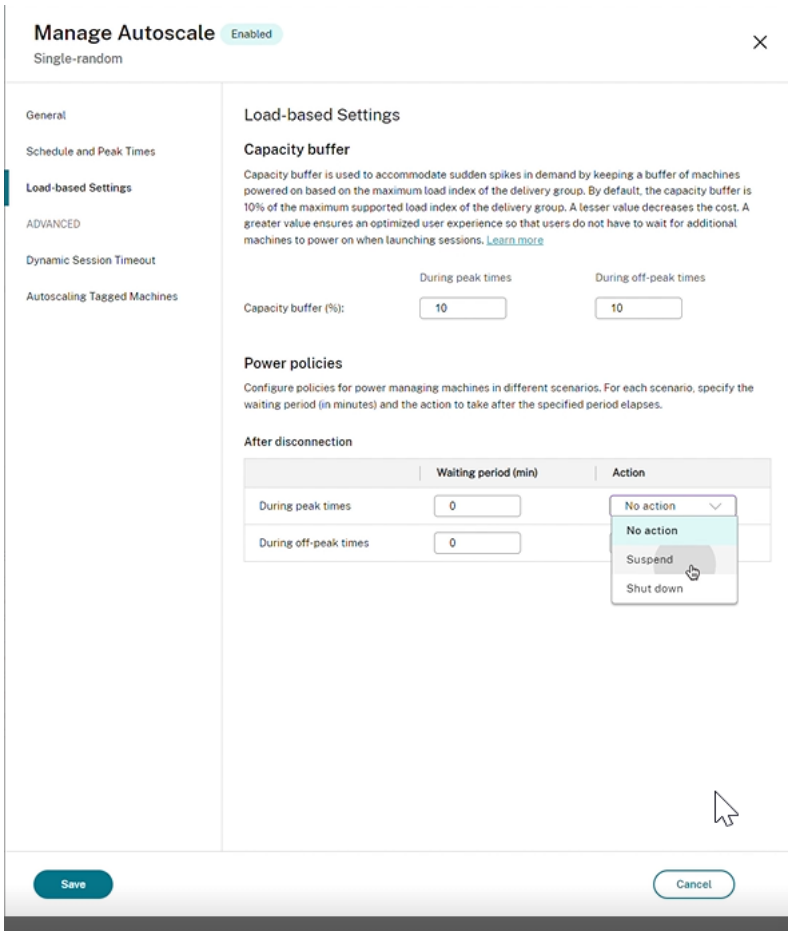
Si la cantidad de máquinas (búfer de capacidad incluido) supera la cantidad total de máquinas encendidas en un momento dado, se encienden máquinas adicionales para satisfacer la demanda. Si

la cantidad de máquinas (búfer de capacidad incluido) es inferior a la cantidad total de máquinas encendidas en un momento dado, las máquinas sobrantes se apagarán o se suspenderán, según las acciones que usted haya configurado.

**Directivas de energía**

Configure directivas para administrar la energía de las máquinas en diferentes supuestos. Para cada supuesto, puede especificar el tiempo de espera (en minutos) y la acción prevista una vez finalizado el tiempo especificado. Las directivas de energía se aplican a los grupos de entrega aleatorios de SO de sesión única y a los grupos de entrega estáticos de SO de sesión única.



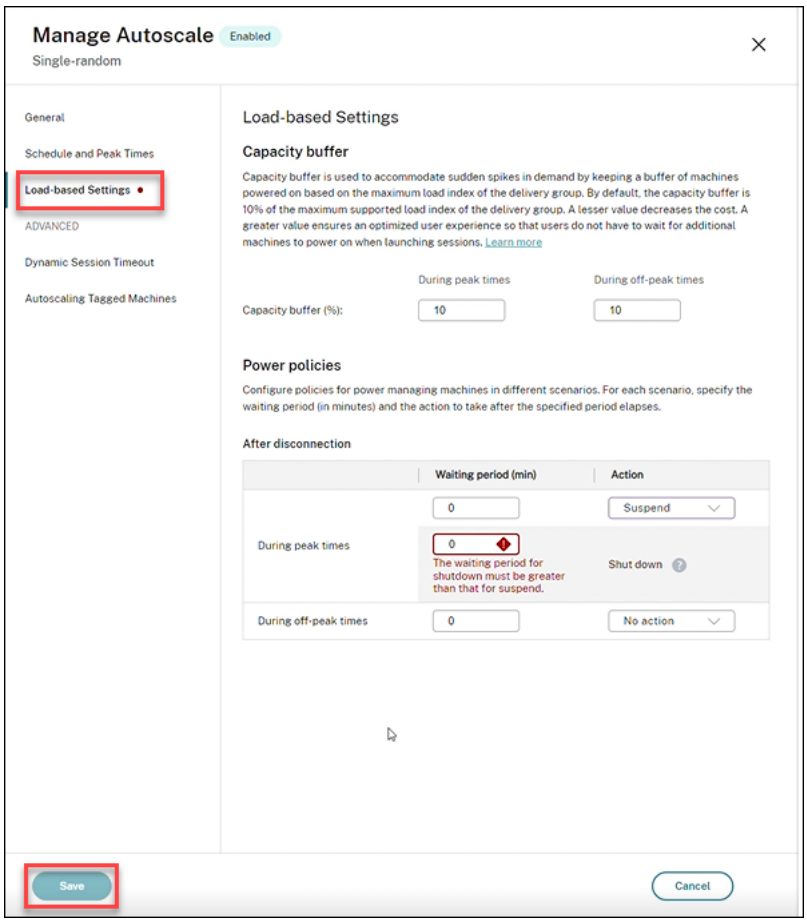

Tras la desconexión, se pueden aplicar los siguientes parámetros tanto en las horas punta como fuera de ellas:

- Puede establecer el tiempo de espera en minutos y acciones como no realizar ninguna acción, suspender o cerrar desde el menú desplegable.
- Si selecciona la acción suspender, configure un tiempo de espera adicional para apagar la máquina.

**Nota:**

- Durante las horas punta y fuera de ellas, el tiempo de espera para la acción de apagado debe ser mayor que el tiempo de espera para suspensión.
- Las máquinas suspendidas solo son accesibles para los usuarios desconectados cuando se vuelven a conectar. Para que las máquinas suspendidas estén disponibles para nuevos usuarios, apáguelas.
- Si los parámetros de tiempo se configuran incorrectamente para los campos de suspensión y apagado, la opción **Guardar** está desactivada y aparece también un punto rojo junto a los elementos de navegación que indica los errores de configuración.




Por ejemplo

- Si establece el tiempo de espera en 12 minutos y elige que la primera acción sea no realizar ninguna acción, una vez transcurridos 12 minutos, la máquina seguirá encendida.
- Si establece el tiempo de espera en 15 minutos y elige que la primera acción sea suspender y el segundo tiempo de espera sea de 20 minutos, una vez transcurridos los 15 minutos, la máquina se suspenderá. Una vez transcurrido el segundo tiempo de espera, la máquina se apagará.

- Si establece el tiempo de espera en 18 minutos y elige que la primera acción sea apagar, transcurridos 18 minutos, la máquina se apagará.

#### Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del grupo de entrega**. El grupo de entrega al que quiere aplicar Autoscale para administrar la energía contiene 10 máquinas (de M1 a M10).
- **Configuración de Autoscale**
  - El búfer de capacidad es del 10%.
  - No se incluye ninguna máquina en la programación seleccionada.

El escenario se desarrolla de la siguiente manera:

1. Ningún usuario inicia sesión.
2. Las sesiones de usuario aumentan.
3. Se inician más sesiones de usuario.
4. La carga por sesión de usuario disminuye por la finalización de sesiones.
5. La carga de sesiones de usuario disminuye aún más hasta que la carga de sesiones se controla solamente mediante recursos locales.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Sin carga de usuarios (estado inicial)
  - Se enciende una máquina (M1). La máquina se enciende debido al búfer de capacidad configurado. En este caso, 10 (cantidad de máquinas) x 10% (búfer de capacidad configurado) es igual a 1. Por lo tanto, se enciende una máquina.
- Un primer usuario inicia sesión
  - La primera vez que un usuario inicia sesión para utilizar un escritorio, se le asigna un escritorio de un grupo de escritorios alojado en máquinas encendidas. En este caso, al usuario se le asigna un escritorio de la máquina M1.
  - Autoscale comienza a encender una máquina adicional (M2) para satisfacer la demanda debido al búfer de capacidad configurado.
- Un segundo usuario inicia sesión
  - Al usuario se le asigna un escritorio de la máquina M2.

  - Autoscale comienza a encender una máquina adicional (M3) para satisfacer la demanda debido al búfer de capacidad configurado.

- Un tercer usuario inicia sesión
  - Al usuario se le asigna un escritorio de la máquina M3.
  - Autoscale comienza a encender una máquina adicional (M4) para satisfacer la demanda debido al búfer de capacidad configurado.
- Un usuario cierra la sesión
  - Después de que un usuario haya cerrado la sesión o se haya agotado el tiempo de espera del escritorio del usuario, la capacidad liberada (por ejemplo, M3) queda disponible como búfer. Como resultado, Autoscale comienza a apagar la máquina M4 porque el búfer de capacidad está configurado al 10%.
- Más usuarios cierran la sesión hasta que no quedan usuarios
  - Después de que más usuarios hayan cerrado la sesión, Autoscale apaga las máquinas (por ejemplo, M2 o M3).
  - Aunque no queden usuarios, Autoscale no apaga la máquina restante (por ejemplo, M1) porque esa máquina queda reservada como capacidad de reserva.

> **Nota:**
>
> Para los grupos de entrega aleatorios de SO de sesión única, todos los cambios en el escritorio se pierden cuando los usuarios cierran la sesión. Sin embargo, si se configuran, los parámetros específicos del usuario se mueven junto con el perfil de usuario.

### Grupos de entrega estáticos de SO de sesión única

El búfer de capacidad se utiliza para adaptarse a picos repentinos de demanda y, al mismo tiempo, mantener un búfer de máquinas encendidas sin asignar en función de la cantidad total de máquinas sin asignar del grupo de entrega. De forma predeterminada, el búfer de capacidad es el 10 % de la cantidad total de máquinas sin asignar del grupo de entrega.

> **Importante:**
>
> Una vez asignadas todas las máquinas del grupo de entrega, el búfer de capacidad no desempeña ningún papel en el encendido ni en el apagado de las máquinas.

Si la cantidad de máquinas (búfer de capacidad incluido) supera la cantidad total de máquinas encendidas en un momento dado, se encienden máquinas adicionales sin asignar para satisfacer la demanda. Si la cantidad de máquinas (búfer de capacidad incluido) es inferior a la cantidad total de

máquinas encendidas en un momento dado, el exceso de máquinas se apagarán o se suspenderán, según las acciones que usted haya configurado.

Para grupos de entrega estáticos de SO de sesión única, Autoscale:

- Enciende las máquinas asignadas durante las horas punta y las apaga durante las horas de actividad normal solo cuando la propiedad `AutomaticPowerOnForAssigned` del grupo de entrega de SO de sesión única aplicable está establecida en true.
- Enciende automáticamente una máquina durante las horas punta si está apagada, y la propiedad `AutomaticPowerOnForAssignedDuringPeak` del grupo de entrega al que pertenece está establecida en true.

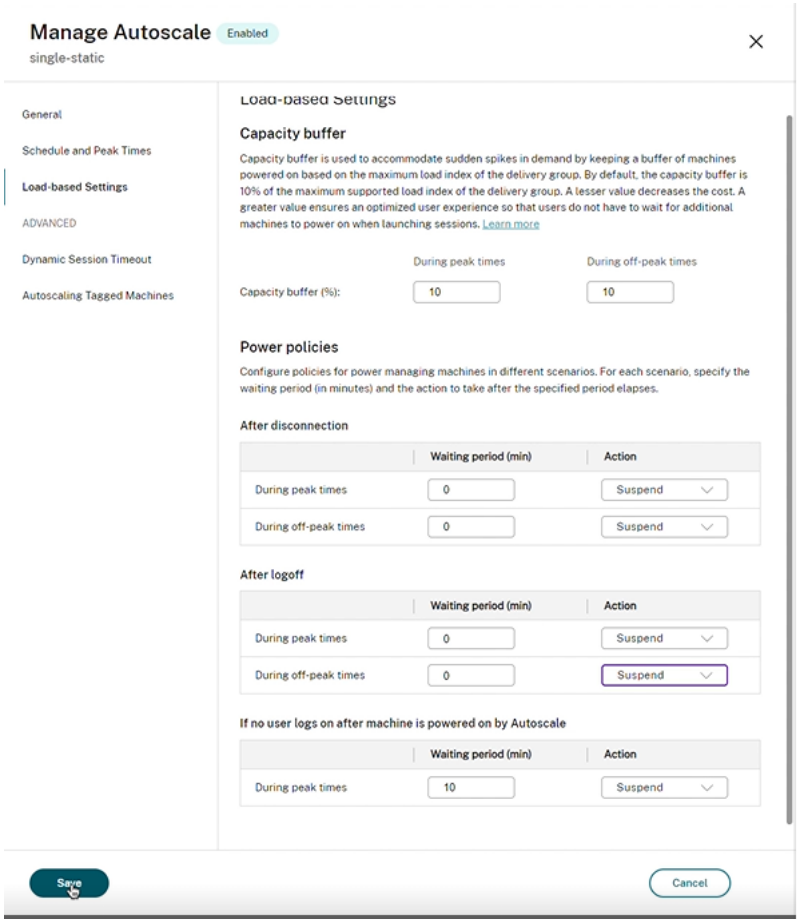
Para entender cómo funciona el búfer de capacidad con las máquinas asignadas, tenga en cuenta lo siguiente:

- El búfer de capacidad solo funciona cuando el grupo de entrega tiene una o más máquinas sin asignar.
- Si el grupo de entrega no tiene máquinas sin asignar (todas las máquinas del grupo de entrega están asignadas), el búfer de capacidad no desempeña ningún papel en el encendido o apagado de las máquinas.
- La propiedad `AutomaticPowerOnForAssignedDuringPeak` determina si las máquinas asignadas se encienden durante las horas punta. Si se establece en true, Autoscale mantiene las máquinas encendidas durante las horas punta. Autoscale también las encenderá, incluso si están apagadas.

#### Directivas de energía

Configure directivas para administrar la energía de las máquinas en diferentes supuestos. Para cada supuesto, puede especificar el tiempo de espera (en minutos) y la acción prevista una vez finalizado el tiempo especificado. Las directivas de energía se aplican a los grupos de entrega aleatorios de SO de sesión única y a los grupos de entrega estáticos de SO de sesión única.




Para **Tras la desconexión** y **Tras el cierre de sesión**, se aplican los siguientes parámetros tanto en las horas punta como fuera de ellas:
Puede establecer el tiempo de espera en minutos y acciones como no realizar ninguna acción, suspender o cerrar desde el menú desplegable.

**Si ningún usuario inicia sesión después de encenderse la máquina con Autoscale**, los siguientes parámetros solo se aplican durante las horas punta:
Puede establecer el tiempo de espera en minutos y acciones como no realizar ninguna acción, suspender o apagar desde el menú desplegable durante las horas punta.

### Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del grupo de entrega**. El grupo de entrega al que quiere aplicar Autoscale para administrar la energía contiene 10 máquinas (de M1 a M10).
- **Configuración de Autoscale**
  - Las máquinas que van de la M1 a la M3 se asignan, y las máquinas que van de la M4 a la M10, no.

  - El búfer de capacidad se establece en 10% para las horas punta y las horas normales.
  - Según la programación seleccionada, Autoscale administra la energía de las máquinas entre las 9:00 y las 18:00.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

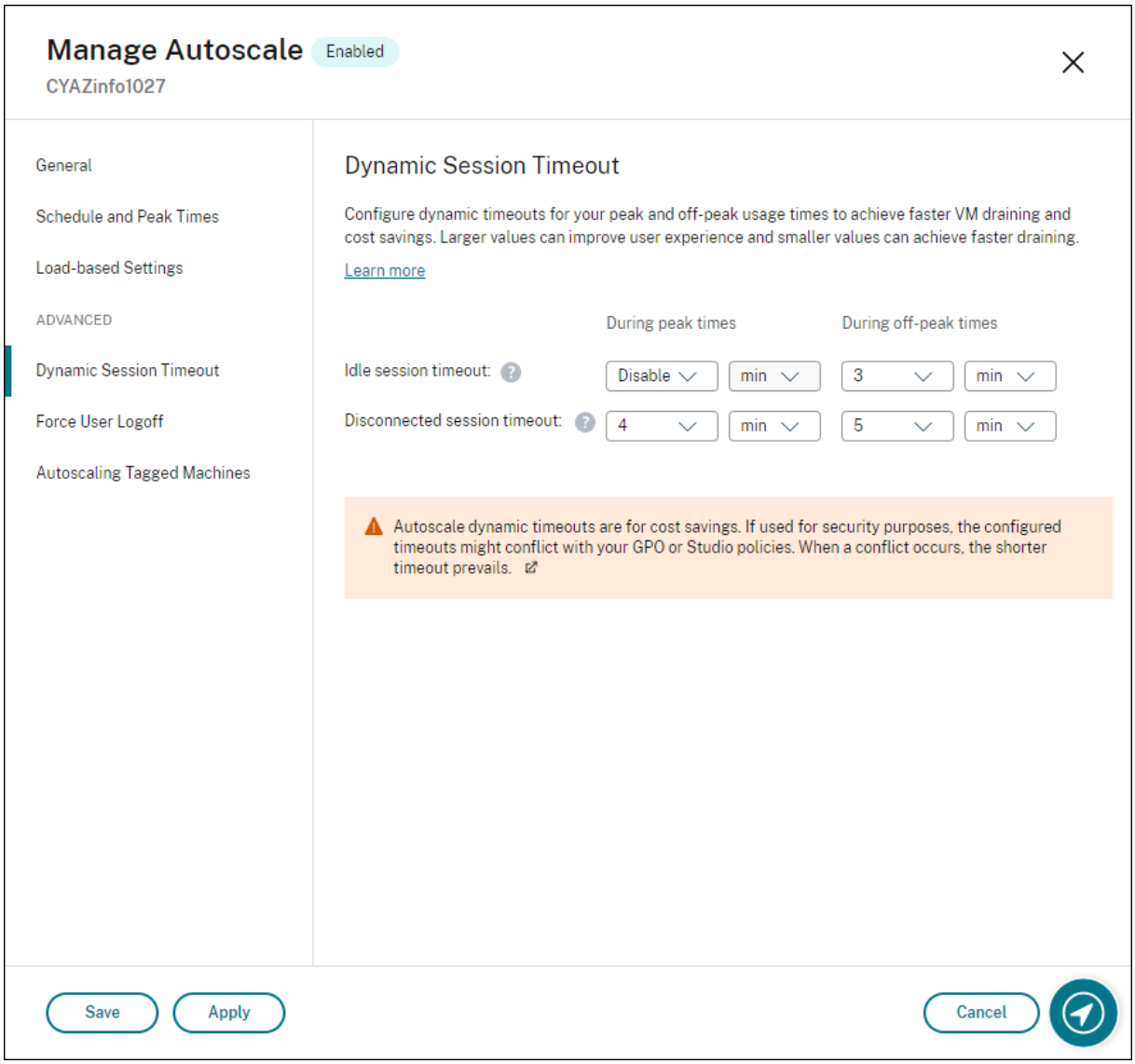
- Inicio de la programación: 9:00
  - Autoscale enciende las máquinas que van de la M1 a la M3.
  - Autoscale enciende una máquina adicional (por ejemplo, M4) debido al búfer de capacidad configurado. La máquina M4 no está asignada.
- Un primer usuario inicia sesión
  - La primera vez que un usuario inicia sesión para utilizar un escritorio, se le asigna un escritorio de un grupo de escritorios alojado en máquinas encendidas sin asignar. En este caso, al usuario se le asigna un escritorio de la máquina M4. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez.
  - Autoscale comienza a encender una máquina adicional (por ejemplo, M5) para satisfacer la demanda debido al búfer de capacidad configurado.
- Un segundo usuario inicia sesión
  - Al usuario se le asigna un escritorio de las máquinas encendidas sin asignar. En este caso, al usuario se le asigna un escritorio de la máquina M5. Las siguientes conexiones del usuario se establecen con el mismo escritorio que se asignó la primera vez.
  - Autoscale comienza a encender una máquina adicional (por ejemplo, M6) para satisfacer la demanda debido al búfer de capacidad configurado.
- Los usuarios cierran la sesión
  - A medida que los usuarios cierran la sesión de sus máquinas de escritorio o transcurren los tiempos de espera de estas, Autoscale mantiene encendidas de la máquina M1 a la M5 entre las 9:00 y las 18:00. La próxima vez que esos usuarios inician sesión, se conectan al mismo escritorio que se asignó la primera vez.
  - La máquina sin asignar M6 está esperando para publicar un escritorio para un usuario entrante y sin asignar.
- Fin de la programación: 18:00
  - A las 18:00, Autoscale apaga de la máquina M1 a la M5.
  - Autoscale mantiene encendida la máquina M6 sin asignar debido al búfer de capacidad configurado. Esa máquina está esperando para publicar un escritorio para un usuario entrante y sin asignar.
  - En el grupo de entrega, las máquinas que van de la M6 a la M10 son máquinas sin asignar.

# Tiempos de espera de sesión dinámicos

June 19, 2023

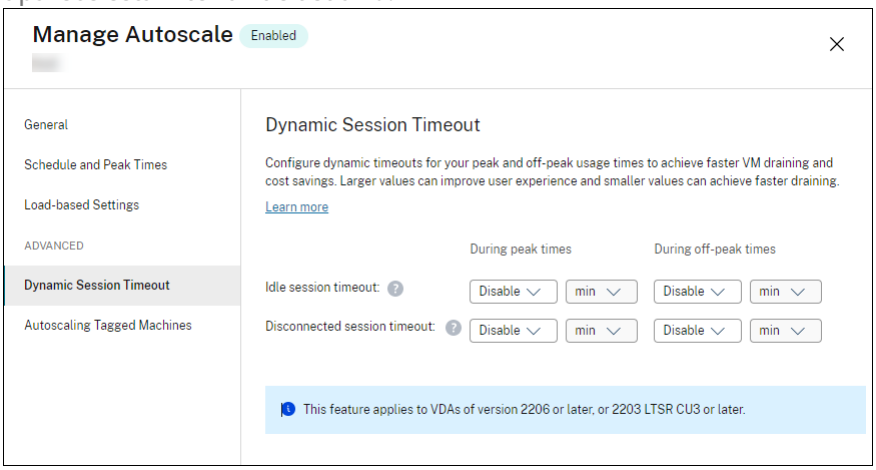
Esta función le permite configurar los tiempos de espera de sesión por desconexión y por inactividad para los tiempos de uso de horas punta y horas normales con el fin de lograr una purga más rápida de las máquinas y ahorrar costes. Esta función se aplica a máquinas con SO de sesión única y multi-sesión. Un VDA registra tiempos de inactividad de las sesiones que han estado inactivas durante más de 10 minutos, por lo que los tiempos de espera dinámicos de las sesiones no podrán desconectar las sesiones inactivas durante esos 10 minutos de inactividad. Un valor menor elimina las sesiones persistentes antes, lo que reduce los costes.



**Nota:**

- Esta función siempre está disponible para grupos de entrega con SO multisesión.
- Para los grupos de entrega con SO de sesión única, esta función se aplica a los VDA con la versión 2206 CR o una posterior, o con la 2203 LTSR CU3 o una posterior. Asegúrese de que dichos VDA se hayan registrado en Citrix Cloud al menos una vez. Cuando no está disponible, aparece esta interfaz de usuario:




- Los tiempos de espera dinámicos de Autoscale son para ahorrar costes. Si se utilizan por motivos de seguridad, es posible que los tiempos de espera configurados entren en conflicto con sus directivas de GPO o de la consola Administrar. Cuando se produce un conflicto, prevalece el menor tiempo de espera.

**Tiempo de espera de sesión por inactividad**. Habilita o inhabilita un temporizador que especifica cuánto tiempo se mantiene una conexión de usuario ininterrumpida si no hay ninguna acción por parte del usuario. Cuando se agota el tiempo de este temporizador, la sesión pasa al estado desconectado y se aplica el **Tiempo de espera de sesión por desconexión**. Si el **Tiempo de espera de sesión por desconexión** está inhabilitado, la sesión no se cierra.

**Importante:**

- Si especifica un valor inferior o igual a 10 minutos (600 segundos), Autoscale desconecta las sesiones correspondientes después de que hayan estado inactivas durante 10 minutos. Esto se debe a que Autoscale se basa en los tiempos de inactividad de las sesiones que registran los VDA. Los VDA registran tiempos de inactividad solo para las sesiones que hayan estado inactivas durante más de 10 minutos.
- Una sesión inactiva seguirá pasando al estado desconectado si el usuario interactúa con ella dentro de los 5 últimos minutos de alcanzar el tiempo de espera de la sesión inactiva.

**Tiempo de espera de sesión por desconexión**. Habilita o inhabilita un temporizador para determinar cuánto tiempo permanece desconectado un escritorio antes de que se cierre la sesión. Si se habilita, la sesión desconectada se cierra cuando se agota el tiempo del temporizador.

# Autoscale de máquinas etiquetadas (ampliación en la nube)

March 2, 2023

> **Nota:**
>
> Esta función se denominaba anteriormente Restringir Autoscale.

## Introducción

Autoscale proporciona la flexibilidad necesaria para administrar la energía solo en un subconjunto de máquinas de un grupo de entrega. Para hacer esto, aplique una etiqueta a una o varias máquinas y, a continuación, configure Autoscale para que administre solo las máquinas etiquetadas.

Esta función puede ser útil en casos de uso de "cloud bursting"(ampliación en la nube), en los que quiera utilizar los recursos locales (o instancias reservadas de nube pública) para gestionar las cargas de trabajo antes de usar los basados en la nube para hacer frente a la demanda adicional (es decir, cargas de trabajo en ráfagas). Para que las máquinas locales (o las instancias reservadas) se encarguen de las cargas de trabajo primero, debe usar la restricción por etiquetas junto con la preferencia de zonas.

La restricción por etiquetas especifica qué máquinas se administrarán con Autoscale. La preferencia de zona especifica qué máquinas de la zona preferida gestionarán las solicitudes de inicio del usuario. Para obtener más información, consulte Etiquetas y Preferencias de zona.

Para administrar con Autoscale determinadas máquinas etiquetadas, puede usar la consola Administrar o PowerShell.

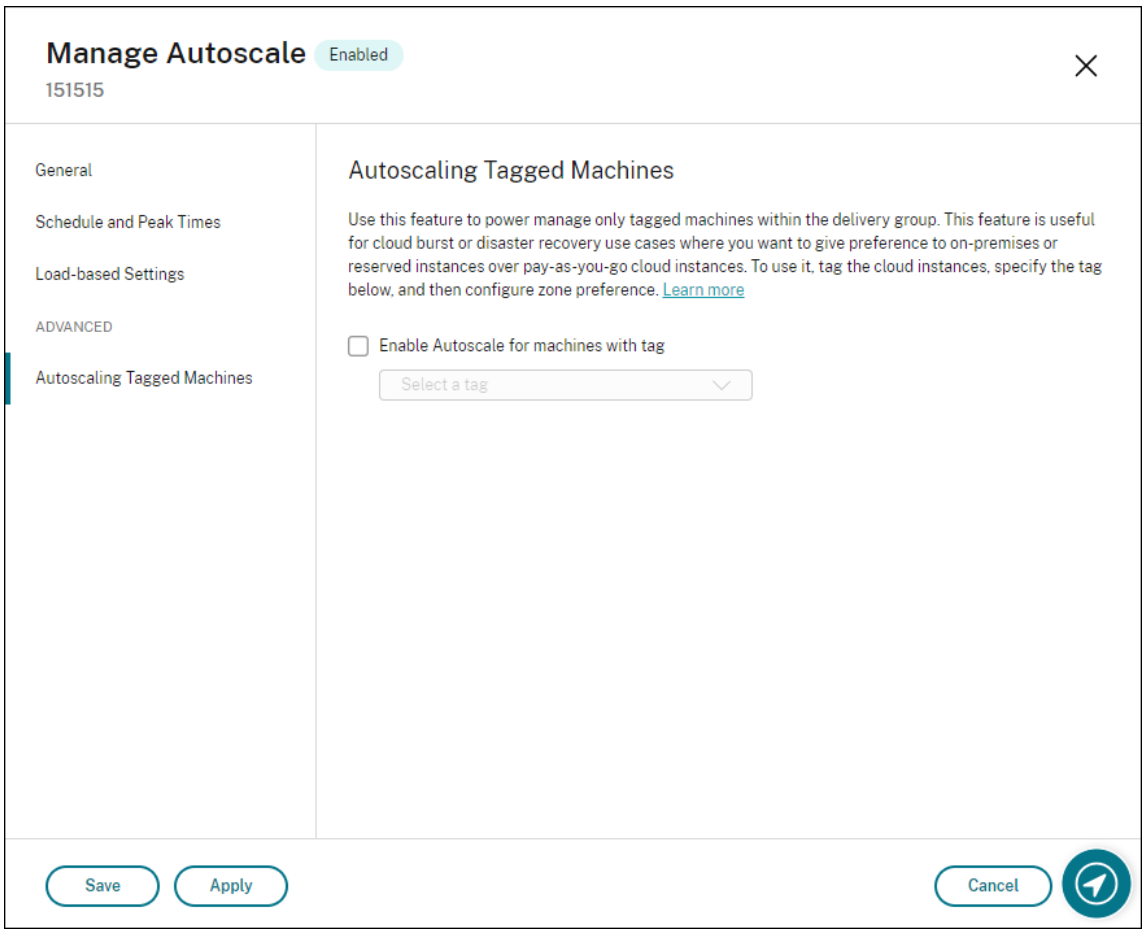
## Usar la consola Administrar para administrar con Autoscale determinadas máquinas etiquetadas

Para administrar con Autoscale ciertas máquinas etiquetadas, complete los siguientes pasos:

1. Cree una etiqueta y aplíquela a las máquinas correspondientes del grupo de entrega. Para obtener más información, consulte Administrar etiquetas y restricciones por etiqueta.
2. Seleccione el grupo de entrega y, a continuación, abra el asistente **Administrar Autoscale**.
3. En la página **Autoscale de máquinas etiquetadas**, seleccione **Habilitar Autoscale para máquinas con etiquetas**, seleccione una etiqueta de la lista y, a continuación, haga clic en **Aplica** para guardar los cambios.

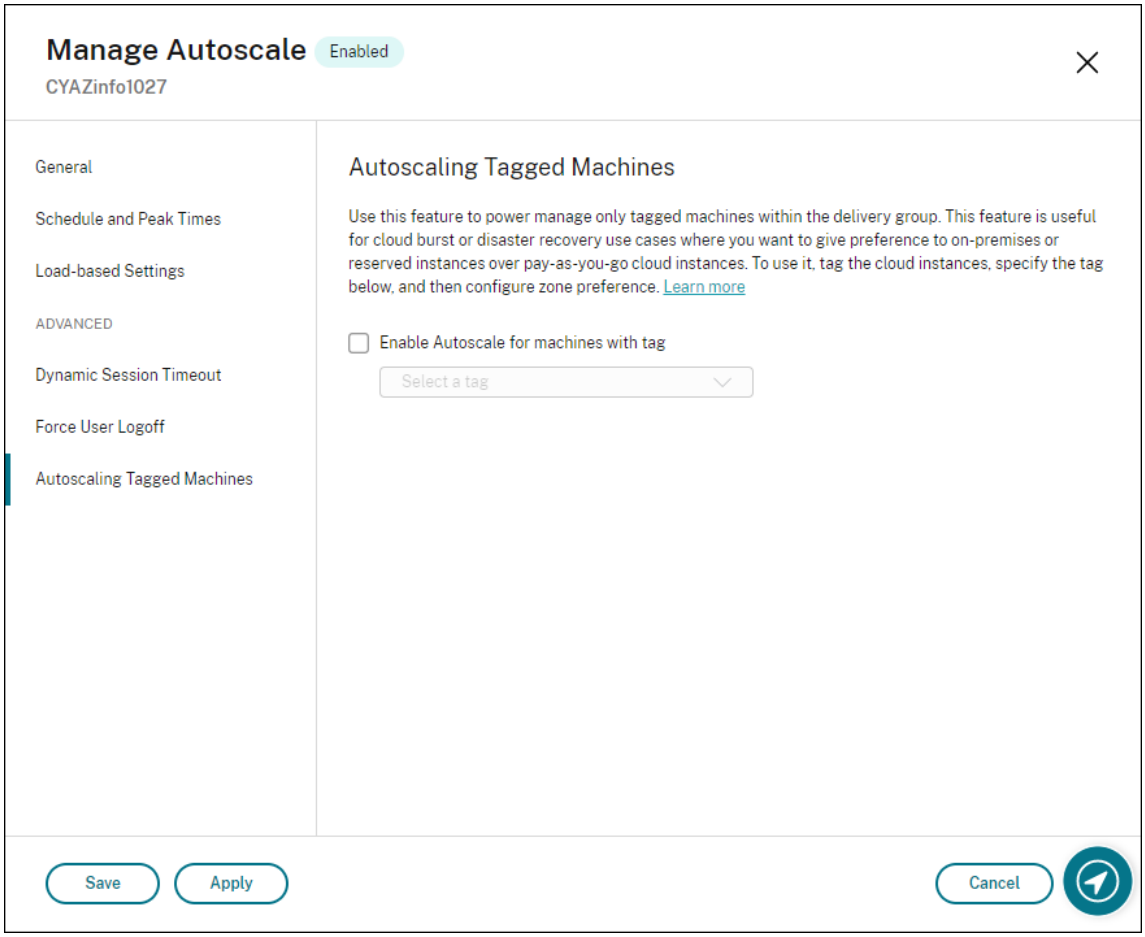
   Interfaz de usuario para grupos de entrega *estáticos* y *aleatorios* de SO de sesión única:




Interfaz de usuario para *grupos de entrega de SO multisesión*:




> **Advertencia:**
>
> - Es posible que, al usar Autoscale en máquinas con una etiqueta específica, el histograma se actualice automáticamente para reflejar la cantidad de máquinas para la etiqueta. En la página **Programación y horas punta**, puede asignar máquinas manualmente en cada intervalo de tiempo si fuera necesario.
> - No puede eliminar una etiqueta que se esté utilizando en máquinas. Para eliminarla, primero debe eliminar la restricción de las etiquetas en cuestión.

Después de aplicar la restricción por etiquetas, es posible que quiera quitarla del grupo de entrega más tarde. Para eso, vaya a la página **Administrar Autoscale > Autoscale de máquinas etiquetadas** y desactive **Habilitar Autoscale para máquinas con etiquetas**.

> **Advertencia:**
>
> - Si quita la etiqueta de las máquinas correspondientes sin desmarcar **Habilitar Autoscale para máquinas con etiquetas**, es posible que reciba una advertencia al abrir el asistente **Administrar Autoscale**. Al quitar la etiqueta de las máquinas, es posible que no queden

> máquinas por administrar para Autoscale porque la etiqueta especificada en Autoscale no es válida. Para resolver esto, vaya a la página **Autoscale de máquinas etiquetadas**, quite la etiqueta no válida y, a continuación, haga clic en **Aplicar** para guardar los cambios.

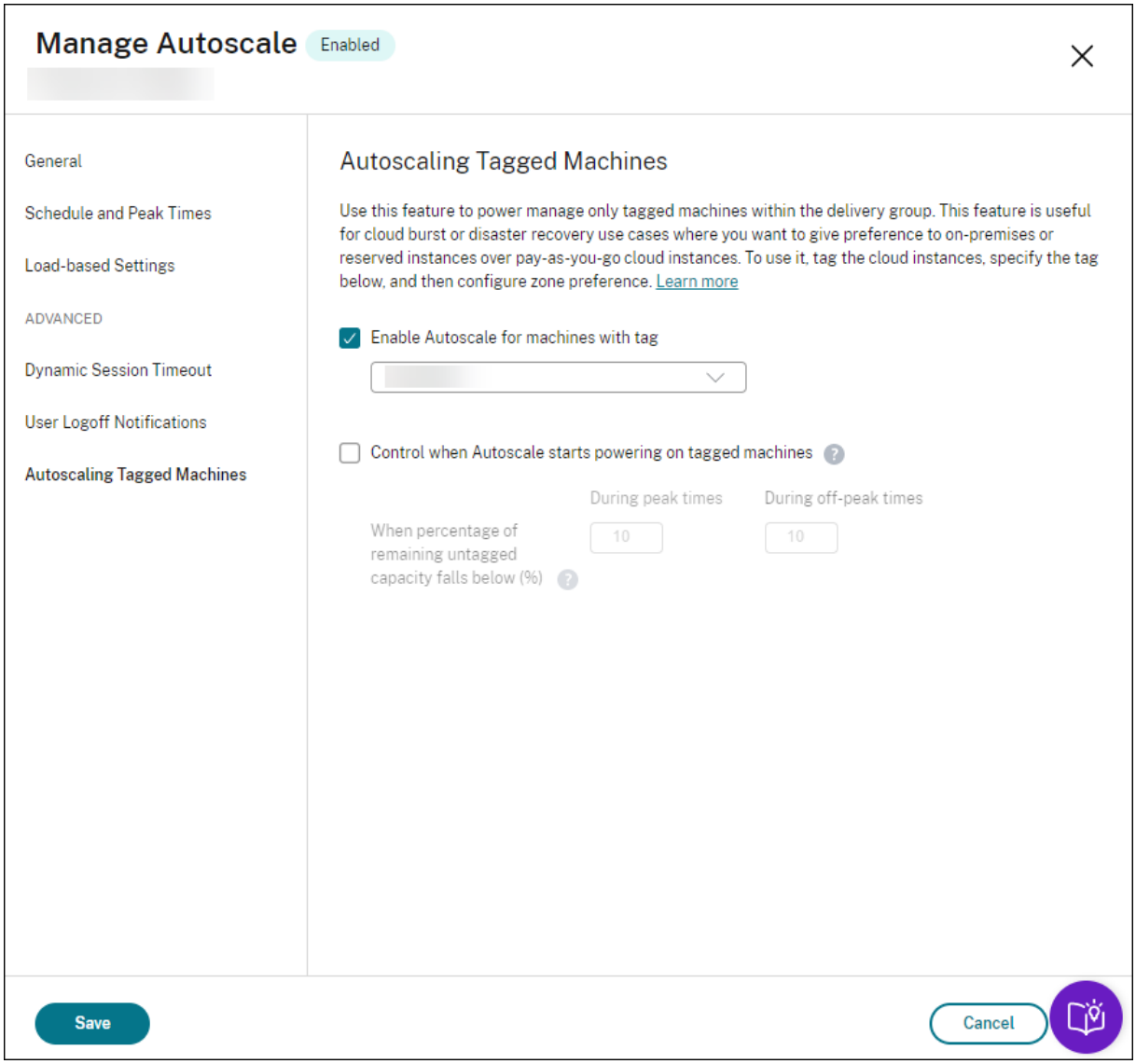
#### Controlar cuándo Autoscale enciende los recursos

También puede controlar cuándo Autoscale comienza a encender máquinas etiquetadas en función del uso de máquinas sin etiquetar. De esta forma, puede optimizar aún más el consumo de sus cargas de trabajo de nube pública o etiquetadas.

Para eso, complete los pasos siguientes:

1. En la página **Autoscale de máquinas etiquetadas**, seleccione **Controle cuándo Autoscale comienza a encender máquinas etiquetadas**.
2. Introduzca la cantidad porcentual de uso de máquinas sin etiquetar que desea alcanzar tanto para las horas punta como para las horas no punta y, a continuación, haga clic en **Aplicar**. Valores admitidos: 0—100.




**Sugerencia:**

El porcentaje controla el momento en que AutoScale comienza a encender las máquinas etiquetadas. Cuando el porcentaje cae por debajo del umbral (el valor predeterminado es 10%), AutoScale comienza a encender las máquinas etiquetadas. Cuando el porcentaje supera el umbral, AutoScale pasa al modo de apagado. Al introducir el porcentaje, considere dos situaciones:

- Para grupos de entrega con SO de sesión única: El valor se define como un porcentaje de la cantidad total de máquinas sin etiquetar en estado inactivo. Ejemplo: Tiene 10 máquinas con sistema operativo de sesión única sin etiquetar. Cuando solo queda una sin sesión, AutoScale comienza a encender una máquina etiquetada.
- Para grupos de entrega con SO multisesión: El valor se define como un porcentaje de la capacidad total (en términos de índice de carga) de las máquinas sin etiquetar disponibles.

> Ejemplo: Tiene 10 máquinas con sistema operativo multisesión sin etiquetar. Cuando están cargadas al 90%, AutoScale comienza a encender una máquina etiquetada.

### Usar PowerShell para administrar con Autoscale determinadas máquinas etiquetadas

Para usar el SDK de PowerShell directamente, siga estos pasos:

1. **Cree una etiqueta.** Utilice el comando New-Brokertag de PowerShell para crear una etiqueta.
   - Por ejemplo: `$managed = New-BrokerTag Managed`. En este caso, la etiqueta se denomina "Managed". Para obtener más información acerca del comando New-Brokertag de PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/New-BrokerTag/.
2. **Aplique la etiqueta a máquinas**. Utilice el comando Get-Brokermachine de PowerShell para aplicar la etiqueta a las máquinas de un catálogo en las que quiere que Autoscale administre la energía.
   - Por ejemplo: `Get-BrokerMachine -CatalogName "cloud" | Add-BrokerTag $managed.Name`. En este caso, el catálogo se denomina "cloud".
   - Para obtener más información acerca del comando Get-Brokermachine de PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerMachine/.

   > **Nota:**
   >
   > Puede agregar nuevas máquinas al catálogo después de aplicar la etiqueta. La etiqueta *NO* se aplica automáticamente a esas nuevas máquinas.

3. **Agregue máquinas etiquetadas al grupo de entrega en el que quiere que Autoscale administre la energía.** Utilice el comando Get-BrokerDesktopGroup de PowerShell para agregar una restricción por etiqueta al grupo de entrega que contiene las máquinas (es decir, "restringir el inicio a las máquinas con la etiqueta X").
   - Por ejemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscaleTagUid $managed.Uid`. En este caso, el UID del grupo de entrega es 1.
   - Para obtener más información acerca del comando Get-BrokerDesktopGroup de PowerShell, consulte https://developer-docs.citrix.com/projects/delivery-controller-sdk/en/latest/Broker/Get-BrokerDesktopGroup/.

Después de aplicar la restricción por etiquetas, es posible que quiera quitarla del grupo de entrega más tarde. Para eso, utilice el comando Get-BrokerDesktopGroup de PowerShell.

Ejemplo: `Get-BrokerDesktopGroup -Uid 1 | Set-BrokerDesktopGroup -RestrictAutoscal $null`. En este caso, el UID del grupo de entrega es 1.

> **Nota:**
>
> Las máquinas sin etiquetar se reinician automáticamente después de que los usuarios las apaguen. Este sistema garantiza que estén disponibles para gestionar las cargas de trabajo antes. Esto se puede habilitar o inhabilitar por grupo de escritorios a través de la propiedad `AutomaticRestartForUntaggedMachines` de `Set-BrokerDesktopGroup`. Para obtener más información, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

### Caso de ejemplo

Supongamos que tiene ante usted este caso:

- **Configuración del catálogo de máquinas**. Hay dos catálogos de máquinas (C1 y C2).
  - El catálogo C1 contiene 5 máquinas (M1 a M5) que son locales en implementaciones locales.
  - El catálogo C2 contiene 5 máquinas (M6 a M10) que son remotas en implementaciones en la nube.
- **Restricción por etiquetas**. Se crea una etiqueta denominada "Cloud", la cual se aplica a las máquinas M6 a M10 del catálogo C2.
- **Configuración de zonas**. Se crean dos zonas (Z1 y Z2).
  - La zona Z1 que contiene el catálogo C1 corresponde a las implementaciones locales.
  - La zona Z2 que contiene el catálogo C2 corresponde a las implementaciones en la nube.
- **Configuración del grupo de entrega**
  - El grupo de entrega contiene 10 máquinas (de M1 a M10), 5 máquinas del catálogo C1 (de M1 a M5) y 5 del catálogo C2 (de M6 a M10).
  - Las máquinas M1 a M5 se encienden manualmente y permanecen encendidas durante toda la programación.
- **Configuración de Autoscale**
  - El búfer de capacidad es del 10%.
  - AutoScale administra solo la energía de las máquinas que tienen la etiqueta "Cloud". En este caso, Autoscale administra la energía de las máquinas M6 a M10 en la nube.

- **Configuración de escritorios o aplicaciones publicados**. Las preferencias de zona se configuran para los escritorios publicados (por ejemplo), donde hay preferencia de la Zona Z1 sobre la Zona Z2 para las solicitudes de inicio del usuario.
  - La zona Z1 se configura como la zona preferida (zona particular) para los escritorios publicados.

El escenario se desarrolla de la siguiente manera:

1. Ningún usuario inicia sesión.
2. Las sesiones de usuario aumentan.
3. Las sesiones de usuario aumentan hasta que se consumen todas las máquinas locales disponibles.
4. Se inician más sesiones de usuario.
5. Las sesiones de usuario disminuyen por la finalización de sesiones.
6. Las sesiones de usuario disminuyen aún más hasta que la carga de sesiones se controla solamente mediante máquinas locales.

Consulte lo que hay a continuación para obtener información detallada sobre cómo funciona Autoscale en este escenario.

- Sin carga de usuarios (estado inicial)
  - Todas las máquinas locales, M1 a M5, están encendidas.
  - Una máquina en la nube (por ejemplo, M6) está encendida. La máquina se enciende debido al búfer de capacidad configurado. En este caso, 10 (cantidad de máquinas) x 10 000 (índice de carga) x 10% (búfer de capacidad configurado) equivale a 10 000. Por lo tanto, se enciende una máquina.
  - El valor del índice de carga de las máquinas encendidas (M1 a M6) se halla en una carga base (el índice de carga es igual a 0).
- Los usuarios inician sesión
  - Las sesiones se dirigen para alojamiento en las máquinas M1 a M5, según la preferencia de zona configurada y existe un equilibrio de carga entre estas máquinas locales.
  - El valor del índice de carga de las máquinas encendidas (M1 a M5) aumenta.
  - El valor del índice de carga de la máquina encendida (M6) se halla en una carga base.
- Los usuarios aumentan la carga y se consumen todos los recursos locales
  - Las sesiones se dirigen para alojamiento en las máquinas M1 a M5, según la preferencia de zona configurada y existe un equilibrio de carga entre estas máquinas locales.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina encendida (M6) permanece en una carga base.

- Un usuario más inicia sesión
  - La sesión desborda la preferencia de zona y se dirige para alojamiento en la máquina M6 en la nube.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina encendida (M6) aumenta y deja de estar en una carga base. Cuando la capacidad total de reserva cae por debajo de 10 000 en términos de índice de carga, Autoscale comienza a encender una máquina adicional (M7) para satisfacer la demanda debido al búfer de capacidad configurado. La máquina M7 podría tardar un tiempo en encenderse. Por tanto, podría haber una demora hasta que la máquina M7 esté lista.
- Más usuarios inician sesión
  - Las sesiones se dirigen para alojamiento en la máquina M6.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina M6 encendida sigue aumentando, pero la capacidad total de reserva está por encima de 10 000 en términos del índice de carga.
  - El valor del índice de carga de la máquina encendida (M7) permanece en una carga base.
- Aún más usuarios inician sesión
  - Una vez que la máquina M7 está lista, las sesiones se dirigen para alojamiento en las máquinas M6 y M7 y la carga se equilibra entre estas máquinas.
  - El índice de carga de todas las máquinas encendidas (M1 a M5) ha alcanzado el valor 10 000.
  - El valor del índice de carga de la máquina M7 deja de estar en una carga base.
  - El valor del índice de carga de las máquinas encendidas (M6 y M7) aumenta.
  - La capacidad total de reserva sigue estando por encima de 10 000 en términos de índice de carga.
- La carga de las sesiones de usuario disminuye debido a la finalización de sesiones
  - Después de que los usuarios hayan cerrado sus sesiones o tras agotarse el tiempo de espera de las sesiones inactivas, la capacidad liberada de las máquinas M1 a M7 se reutiliza para alojar sesiones iniciadas por otros usuarios.
  - Cuando la capacidad total de reserva está por encima de 10 000 en términos de índice de carga, Autoscale pone una de las máquinas (M6 a M7) en estado de purga. Como resultado, las sesiones iniciadas por otros usuarios ya no se dirigen a esa máquina (por ejemplo, M7), a menos que se produzcan nuevos cambios; por ejemplo, la carga del usuario final aumenta de nuevo o las demás máquinas en la nube se cargan menos.

- La carga de la sesión de usuario disminuye aún más hasta que ya no se necesitan uno o más máquinas en la nube
  - Una vez finalizadas todas las sesiones de la máquina M7 y transcurrida la demora de apagado especificada, Autoscale apaga la máquina M7.
  - El valor del índice de carga de todas las máquinas encendidas (M1 a M5) podría caer a un nivel inferior a 10 000.
  - El valor del índice de carga de la máquina encendida (M6) aumenta.
- Las sesiones de usuario disminuyen, hasta un nivel en que no se necesitan máquinas en la nube.
  - Aunque no hay sesiones de usuario en la máquina M6, Autoscale no la apaga, porque esa máquina queda reservada como capacidad de reserva.
  - Autoscale mantiene encendida la máquina M6 en la nube, debido al búfer de capacidad configurado. Esa máquina está esperando para publicar un escritorio para un usuario entrante.
  - Las sesiones no se dirigen para alojarse en la máquina M6 siempre que las máquinas locales tengan capacidad disponible.

## Aprovisionar máquinas de forma dinámica

November 21, 2022

Autoscale ofrece la posibilidad de crear máquinas y eliminarlas dinámicamente. Puede hacer uso de esta función a través de un script de PowerShell. El script le ayuda a aumentar o reducir dinámicamente la cantidad de máquinas del grupo de entrega en función de las condiciones de carga actuales.

El script ofrece las siguientes ventajas (y más):

- **Reducción de los costes de almacenamiento**. A diferencia de Autoscale, que ayuda a reducir los costes informáticos, el script proporciona una solución más rentable para aprovisionar máquinas.
- **Gestión eficaz de los cambios de carga**. El script le ayuda a gestionar los cambios de carga con el aumento o la reducción automática de la cantidad de máquinas en función de la carga actual del grupo de entrega.

### Descargar el script

El script de PowerShell está disponible en https://github.com/citrix/Powershell-Scripts/tree/master/XAXD/AutoscaleMcs.

### Cómo funciona el script

> **Importante:**
>
> - No se puede especificar un catálogo de máquinas perteneciente a más de un grupo de entrega que se vaya a administrar a través del script. Es decir, que, si varios grupos de entrega comparten un mismo catálogo de máquinas, el script no funciona con ninguno de esos grupos de entrega.
> - No puede ejecutar simultáneamente el script para el mismo grupo de entrega desde varias ubicaciones.

El script funciona a nivel de grupos de entrega. Mide la carga (en términos de índice de carga) y, a continuación, determina si se deben crear o eliminar máquinas.

Las máquinas creadas a través de este script se etiquetan de forma individual (por medio del parámetro `ScriptTag`), de manera que puedan identificarse más tarde. La creación o eliminación de máquinas se basa en:

- **Porcentaje máximo de carga de un grupo de entrega**. Especifica el nivel máximo a partir del cual se crearán máquinas, de manera que Autoscale gestione las cargas adicionales. Cuando se supera este umbral, se crean máquinas en lotes a fin de garantizar que la carga actual disminuya hasta o por debajo del umbral.
- **Porcentaje mínimo de carga de un grupo de entrega**. Especifica el nivel mínimo a partir del cual se eliminarán las máquinas creadas mediante este script que no tengan sesiones activas. Cuando se supera este umbral, se eliminan las máquinas creadas a través de este script que no tienen sesiones activas.

Este script se diseñó para supervisar todo un grupo de entrega y para crear o eliminar máquinas cuando se cumpla el criterio desencadenador. Se ejecuta proceso por proceso. Esto significa que debe ejecutar el script de forma periódica para que pueda funcionar según lo previsto. Le recomendamos que ejecute el script a intervalos mínimos de cinco minutos. Al hacerlo, mejora la capacidad de respuesta general.

El script se basa en los siguientes parámetros para funcionar:

| Parámetro | Tipo | Valor predeterminado | Descripción |
| --- | --- | --- | --- |
| DeliveryGroupName | Cadena | X | Nombre del grupo de entrega que se va a supervisar para determinar la carga actual. Puede proporcionar una lista de nombres separados por punto y coma. Por ejemplo: `Invoke-AutoscaleMachineCreation.ps1 -DeliveryGroupName 'dg1;dg2;dg3' -XdProfileName profile`. |
| XdProfileName | Cadena | X | Nombre del perfil que se va a utilizar para autenticación en servidores remotos. Para obtener información detallada sobre la autenticación en servidores remotos mediante este parámetro, consulte API de autenticación. |
| HighWatermark | Número entero | 80 | Carga porcentual máxima (en términos de índice de carga) a partir de la cual se crearán máquinas para que Autoscale gestione las cargas adicionales. |

| Parámetro | Tipo | Valor predeterminado | Descripción |
|---|---|---|---|
| LowWatermark | Número entero | 15 | Porcentaje mínimo de carga (en términos de índice de carga) a partir del cual se eliminarán las máquinas creadas mediante este script que no tengan sesiones activas. |
| MachineCatalogName | Cadena | X | Nombre del catálogo de máquinas donde se van a crear las máquinas. |
| MaximumCreatedMachines | Número entero | -1 | Cantidad máxima de máquinas que se pueden crear en un grupo de entrega especificado. Si el valor es igual o menor que 0, el script no procesa este parámetro. |
| ScriptTag | Cadena | AutoscaledScripted | Etiqueta que se aplica a las máquinas creadas a través del script. |
| EventLogSource | Cadena | X | Nombre de origen que aparece en Visor de eventos de Windows. |

> **Nota:**
>
> Una "X"indica que no se ha especificado ningún valor predeterminado para ese parámetro.

De forma predeterminada, el script requiere todos los parámetros (excepto `ScriptTag`) la primera vez que se ejecuta. En instancias posteriores, solo se requieren los parámetros `DeliveryGroupName` y `XdProfileName`. Opcionalmente, puede optar por actualizar las cargas porcentuales mínima y máxima.

La primera vez que ejecute el script, deberá especificar un solo grupo de entrega. Por ejemplo, el script *no* funcionará si utiliza el siguiente comando de PowerShell para especificar dos grupos de entrega la primera vez que lo ejecute:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

En su lugar, especifique primero un solo grupo de entrega (en este ejemplo, dg1) con el siguiente comando:

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1'-XdProfileName profile -LowWatermark 20 -HighWatermark 70 -MachineCatalogName 'cat1'\`

A continuación, utilice el siguiente comando para ejecutar el script para el segundo grupo de entrega (en este ejemplo, dg2):

- `Invoke-AutoscaleMachineCreations.ps1 -DeliveryGroupName 'dg1;dg2' -XdProfileName profile`

### Requisitos previos

Para ejecutar el script, asegúrese de que se cumplen estos requisitos previos:

- La máquina reside en el mismo dominio que las máquinas que se van a crear.
- SDK de PowerShell remoto está instalado en esa máquina. Para obtener más información sobre el SDK de PowerShell remoto, consulte SDK y API.
- Otros requisitos previos:
  - Un grupo de entrega que supervisar
  - Un catálogo de máquinas creado con Machine Creation Services (MCS) que tenga un esquema de aprovisionamiento asociado (plantilla)
  - Un grupo de identidades asociado al esquema de aprovisionamiento
  - Un origen de registro de eventos que se creará para que el script pueda escribir información en Registro de eventos de Windows
  - Un cliente seguro que le permite autenticarse en servidores remotos

### Permisos, recomendaciones y avisos

Cuando ejecute el script, tenga en cuenta lo siguiente:

- Para autenticarse en servidores remotos mediante el parámetro `XdProfileName`, deberá definir un perfil de autenticación con un cliente seguro de acceso a API, creado en la consola de Citrix Cloud. Para obtener información detallada, consulte API de autenticación.
- Debe tener permisos para crear y eliminar cuentas de máquina en Active Directory.
- Se recomienda automatizar el script de PowerShell con Programador de tareas de Windows. Para obtener información detallada, consulte Crear una tarea automatizada con Programador de tareas de Windows.
- Si quiere que el script escriba información (por ejemplo, errores y acciones) en Registro de eventos de Windows, debe especificar primero un nombre de origen mediante el cmdlet `New-EventLog`. Por ejemplo: `New-EventLog -LogName Application –Source <sourceName>`. A continuación, podrá ver los eventos en el panel **Aplicación** del Visor de eventos de Windows.
- Si se produjeron errores durante la ejecución del script, ejecute el script manualmente y, a continuación, solucione los problemas haciendo las comprobaciones necesarias.

### API de autenticación

Antes de ejecutar el script, debe definir un perfil de autenticación mediante un cliente seguro de acceso a API. Deberá crear un cliente seguro mediante la misma cuenta en la que se ejecutará el script.

El cliente seguro debe tener los siguientes permisos:

- Crear y eliminar máquinas con MCS.
- Modificar catálogos de máquinas (para agregar y quitar máquinas).
- Modificar grupos de entrega (para agregar y quitar máquinas).

Cuando cree un cliente seguro, asegúrese de que su cuenta tiene los permisos anteriores, ya que el cliente seguro heredará automáticamente los permisos de su cuenta actual.

Para crear un cliente seguro, siga estos pasos:

1. Inicie sesión en la consola de Citrix Cloud y abra **Administración de acceso e identidad > Acceso a API**.
2. Escriba el nombre del cliente seguro y, a continuación, haga clic en **Crear cliente**.

Para autenticarse en servidores remotos, use el comando `Set-XDCredentials` de PowerShell. Por ejemplo:

- `Set-XDCredentials -APIKey <key_id> -CustomerId <customer_id> -SecretKey <secret_key> -StoreAs <name specified by the XdProfileName parameter>`

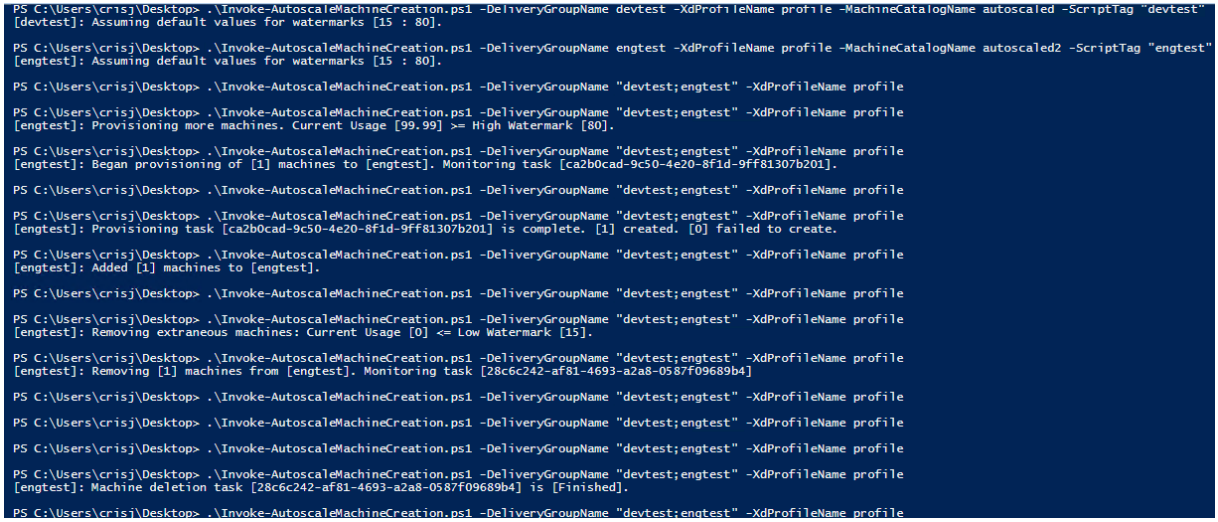
 

### Crear una tarea automatizada con Programador de tareas de Windows

Puede automatizar el script de PowerShell con Programador de tareas de Windows. Al hacerlo, el script se ejecuta automáticamente a determinados intervalos o cuando se cumplen ciertas condiciones. Para ejecutar este script con Programador de tareas de Windows, seleccione **No iniciar una instancia nueva** en la ficha **Crear tarea > Configuración**. Al hacerlo, se impide que Programador de tareas de Windows ejecute una nueva instancia del script si este ya se está ejecutando.

### Ejemplo de ejecución del script

Vea a continuación un ejemplo de ejecución del script. Tenga en cuenta que el archivo del script se invoca varias veces. En este ejemplo, para simular la carga, se inicia y se termina una sesión.




### Lista de comprobación para solución de problemas con el script

El script escribe información (por ejemplo, errores y acciones) en Registro de eventos de Windows. Esta información le ayuda a solucionar problemas que se producen durante la ejecución del script. La siguiente lista de comprobación para solución de problemas puede ser útil:

- Error al comunicar con servidores remotos. Acciones posibles:
  - Compruebe la conexión con el servidor.
  - Compruebe que la clave API que utiliza es válida.
- Error al crear máquinas. Acciones posibles:
  - Compruebe que la cuenta de usuario que ejecuta el script tiene permisos suficientes para crear cuentas de usuario en el dominio.

  - Compruebe que el usuario que creó la clave de API tiene permisos suficientes para aprovisionar máquinas mediante MCS.
  - Verifique la validez del catálogo de máquinas (es decir, su imagen aún existe y está en buen estado).

- Error al agregar máquinas a un catálogo de máquinas o a un grupo de entrega. Acción posible:
  - Compruebe que el usuario que creó la clave de API tiene permisos suficientes para agregar máquinas a catálogos de máquinas y grupos de entrega, y también para quitar máquinas de catálogos de máquinas y grupos de entrega.

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

June 1, 2023

> **Importante:**
>
> Esta funcionalidad solo está disponible en la interfaz de usuario de Autoscale para grupos de entrega multisesión basados en aplicaciones.

Para ahorrar más costes, Autoscale le permite forzar la cierre de sesión de las sesiones persistentes. Para ello, le permite enviar una notificación personalizada a los usuarios y especificar un período de gracia tras el cual se fuerza el cierre de sesión de las sesiones. Esto se hace solo para máquinas en el estado de purga y no para todas las máquinas encendidas. Para evitar la posible pérdida de datos causada por el cierre de sesión forzado, puede configurar esta función para que solo envíe recordatorios de cierre de sesión sin forzar el cierre de sesión del usuario.

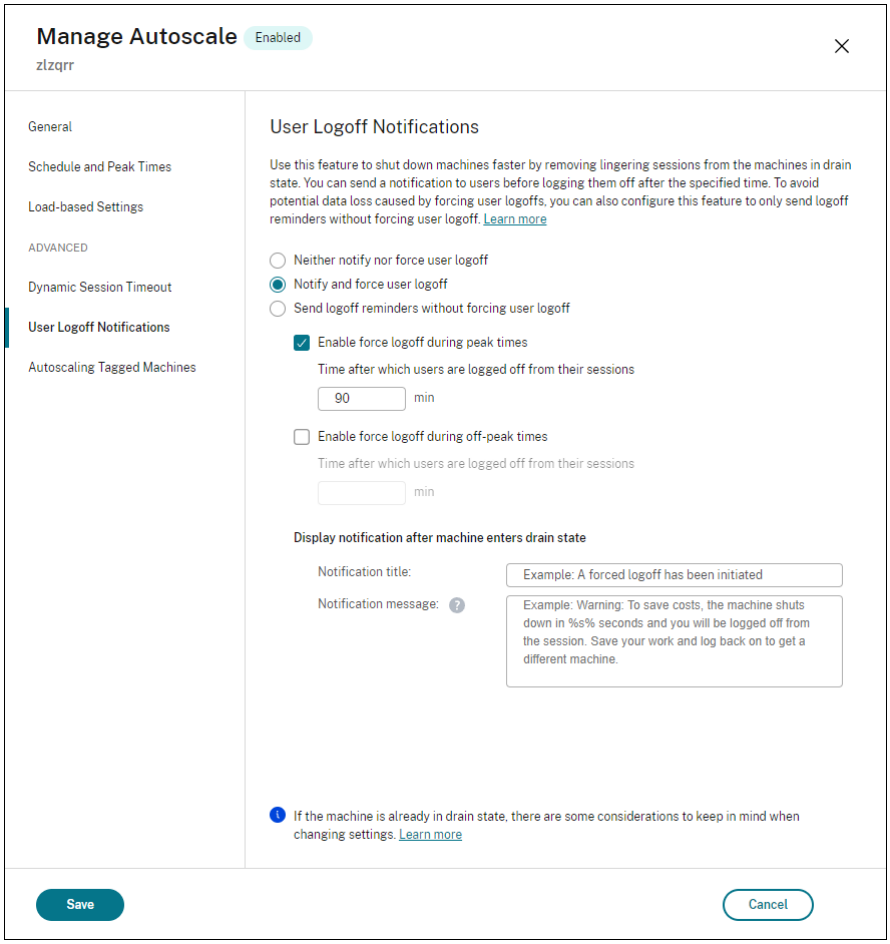
Dispone de estas opciones:

- **Notificar y forzar al usuario a cerrar la sesión**
- **Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión**
- **No notificar ni forzar el cierre de sesión del usuario**

### Notificar y forzar al usuario a cerrar la sesión

Si se selecciona, Autoscale cierra la sesión de los usuarios después de las horas especificadas a continuación.




**Habilitar cierre de sesión forzado durante horas punta**. Si se selecciona, Autoscale cerrará la sesión de esos usuarios durante las horas punta cuando transcurra el tiempo indicado.

**Habilitar cierre de sesión forzado durante horas normales**. Si se selecciona, Autoscale cerrará la sesión de esos usuarios durante las horas de baja actividad cuando transcurra el tiempo indicado.

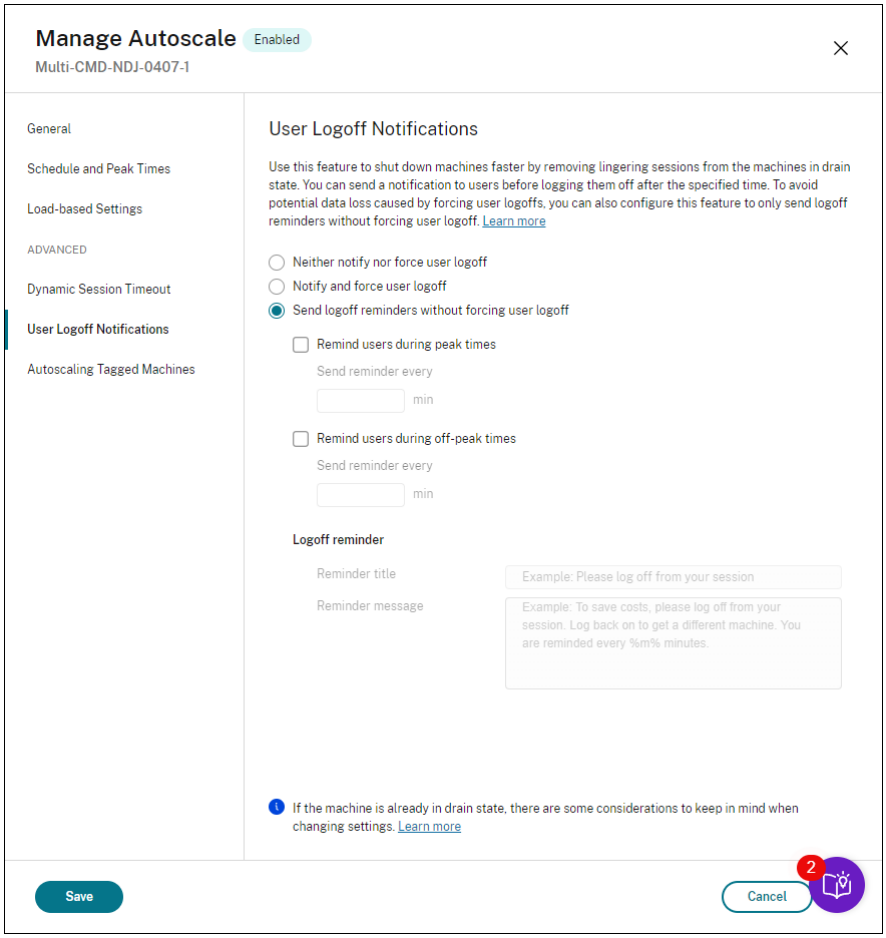
**Mostrar una notificación cuando la máquina entra en estado de purga**. Le permite enviar notificaciones a los usuarios después de que su máquina haya entrado en estado de purga.

- **Título de la notificación**. Permite especificar un título de la notificación que se enviará a los usuarios. Ejemplo:`A forced logoff has been initiated`.
- **Mensaje de notificación**. Permite especificar el contenido de la notificación que se enviará a los usuarios. Puede utilizar %s% o %m% como variables para indicar la hora especificada en el mensaje. Para expresar el tiempo en segundos, utilice %s%. Para expresar el tiempo en minutos, utilice %m%. Ejemplo: `Warning: To save costs, the machine shuts down in %s% seconds and you will be logged off from the session. Save your work and log back on to get a different machine`.

### Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión

Si se selecciona, los usuarios recibirán un recordatorio para cerrar la sesión de sus máquinas después de que estas hayan entrado en estado de purga. Este recordatorio se puede configurar para que se envíe en el intervalo especificado a continuación.




**Enviar un recordatorio a los usuarios durante las horas punta**. Si se selecciona, los usuarios reciben un recordatorio para que cierren sus sesiones durante las horas punta cada X minutos (X indica el tiempo especificado).

**Enviar un recordatorio a los usuarios durante las horas normales**. Si se selecciona, los usuarios reciben un recordatorio para que cierren sus sesiones durante las horas de menor actividad cada X minutos (X indica el tiempo especificado).

**Recordatorio de cierre de sesión**. Le permite configurar el recordatorio que se envía a los usuarios después de que su máquina haya entrado en estado de purga.

- **Título del recordatorio**. Le permite especificar un título para que el recordatorio se envíe a los usuarios. Ejemplo: `Please log off from your session`.
- **Mensaje del recordatorio**. Le permite especificar un mensaje que se enviará a los usuarios.

Ejemplo: `Please log off from your session and log back on to save costs`.

### No notificar ni forzar el cierre de sesión del usuario

Si se selecciona, Autoscale no obliga a los usuarios a cerrar sesión en las máquinas en estado de purga ni notifica a los usuarios para que cambien manualmente a otra máquina.

### Consideraciones

Si la máquina ya se halla en estado de purga, tenga en cuenta lo siguiente al cambiar parámetros:

- Si cambia el parámetro de **Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión** a **Notificar y forzar al usuario a cerrar sesión**, el nuevo parámetro se aplica de inmediato.
- Si cambia el parámetro de **Notificar y forzar al usuario a cerrar sesión** a **Enviar recordatorios de cierre de sesión sin forzar al usuario a cerrar sesión**, el nuevo parámetro no se aplicará hasta la próxima vez que la máquina entre en estado de purga. Se sigue forzando al usuario a cerrar la sesión.

## Analizar la eficacia de los parámetros de Autoscale

February 21, 2024

Para usar esta función, active la opción **Datos detallados de Autoscale** en **DaaS > Inicio > Funciones de Tech Preview**. **Datos detallados de Autoscale** puede tardar unos 15 minutos en aparecer después de habilitarlo.

Puede analizar la eficacia de los parámetros de Autoscale en función del uso de las máquinas durante la semana anterior. A través del análisis, puede obtener información sobre la eficacia de los parámetros de Autoscale:

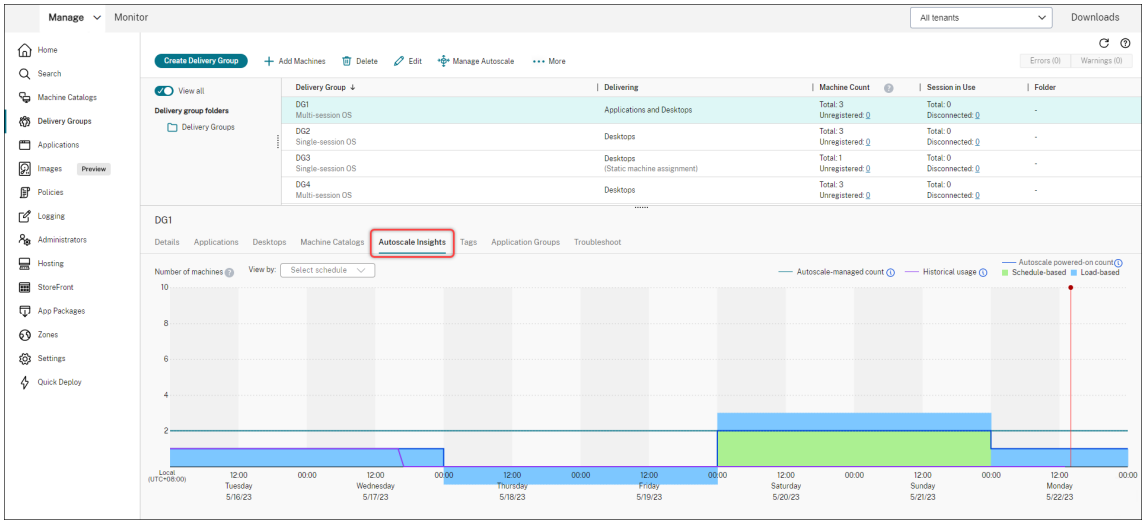
- Identifique despilfarros por exceso de aprovisionamiento.
- Determine si la experiencia del usuario se ve afectada negativamente debido a un aprovisionamiento insuficiente.
- Asegúrese de que la capacidad aprovisionada esté correctamente alineada con el uso de las máquinas.

Para lograr este objetivo, siga estos pasos:

1. Seleccione un grupo de entrega habilitado para Autoscale.
2. En el panel inferior, haga clic en la ficha **Datos detallados de Autoscale**.

   Aparece este gráfico, que muestra la comparación entre los datos de uso de las máquinas de la semana anterior y la cantidad de máquinas que se encenderán según los parámetros de Autoscale.




* La línea vertical roja identifica la hora actual.

Esta tabla proporciona descripciones de las métricas que se muestran en este gráfico.

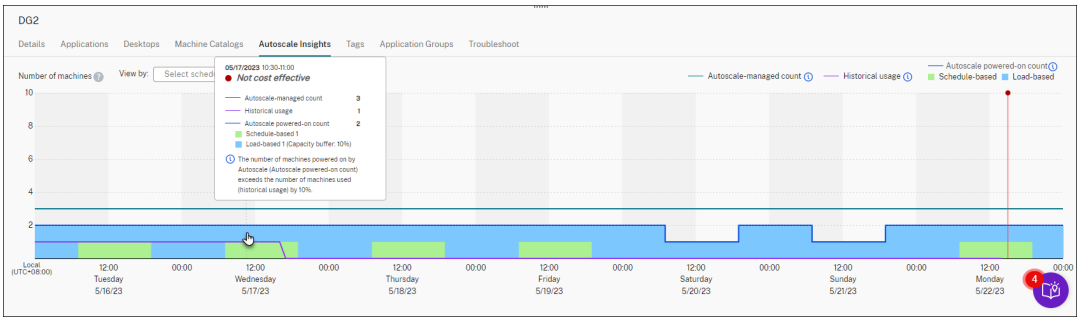
| Métrica | Descripción |
|---|---|
| Recuento administrado por Autoscale | Cantidad total de máquinas administradas por Autoscale. Recuento administrado por Autoscale = Cantidad total de máquinas del grupo de entrega —Cantidad de máquinas en modo de mantenimiento —Cantidad de máquinas no etiquetadas para Autoscale (si la función Autoscale con etiqueta está habilitada). |
| Recuento de encendidas por Autoscale | Cantidad total de máquinas encendidas por Autoscale. Recuento de encendidas por Autoscale = Recuento de máquinas basadas en programación + Recuento de máquinas basadas en carga. |
| Uso histórico | Cantidad de máquinas entregadas a los usuarios. |

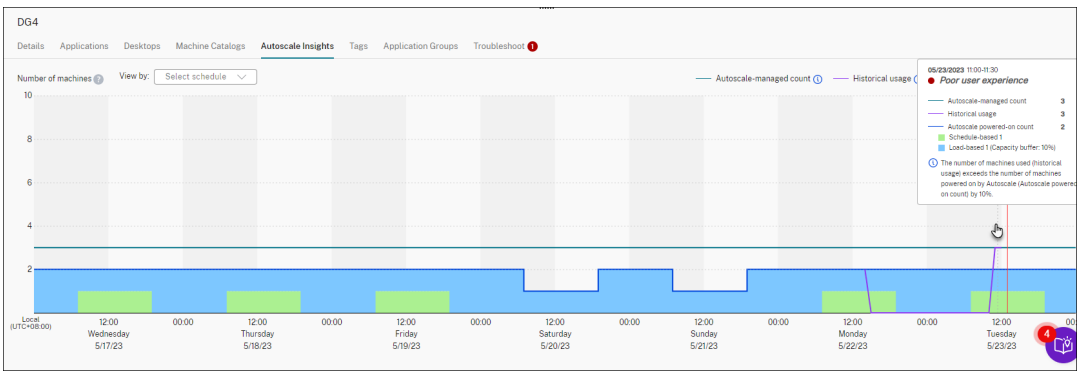
| Métrica | Descripción |
| --- | --- |
| Basado en programación | Cantidad de máquinas que se encienden en función de los parámetros basados en programación de Autoscale ( **Nota:** Los parámetros basados en programación no se aplica a grupos de entrega del tipo SO de sesión única estático). |
| Basado en carga | Cantidad de máquinas que se encienden en función de los parámetros de Autoscale basados en carga. |

3. Para comprobar la eficacia de los parámetros de Autoscale en un intervalo de tiempo específico, coloque el mouse sobre ese intervalo del gráfico. Aparecerá un cuadro de información que muestra los resultados de la comparación y los recuentos detallados de las máquinas:

   - **No es rentable**. El uso histórico es inferior al 90% de los parámetros de Autoscale (recuento de máquinas encendidas de Autoscale). Como resultado, es posible que se desperdicie capacidad.

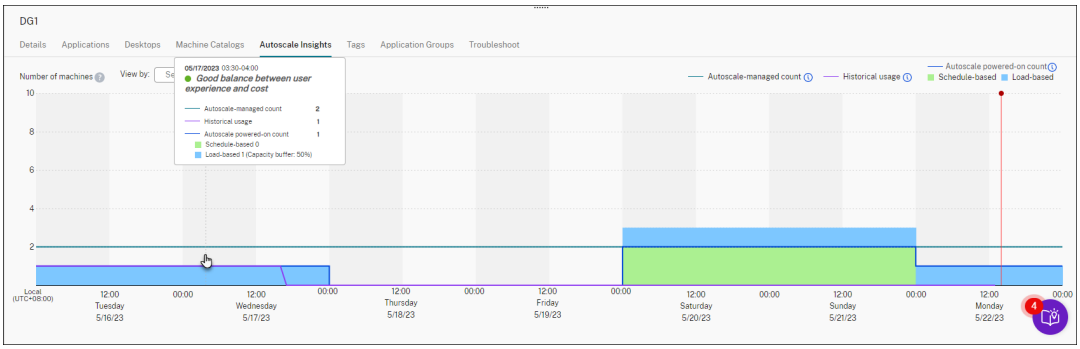



   - **Mala experiencia de usuario**. El uso histórico representa más del 110% de los parámetros de Autoscale (recuento de máquinas encendidas de Autoscale). Como resultado, es posible que los usuarios esperen más a que las máquinas se enciendan.

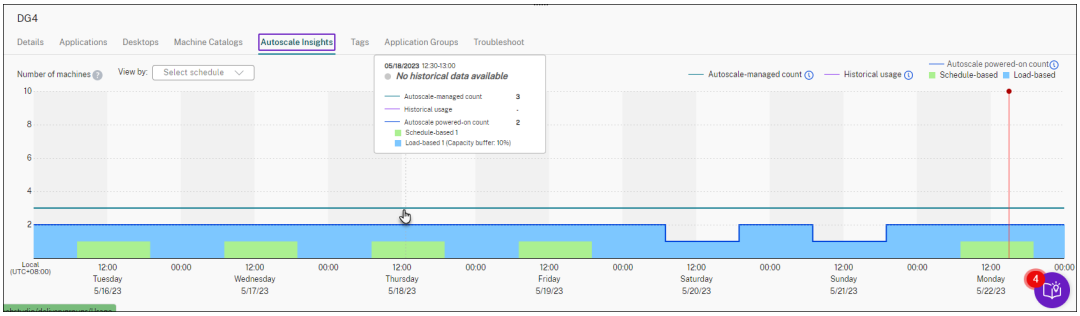


- **Buen equilibrio entre la experiencia de usuario y el coste**. La diferencia entre el uso histórico y los parámetros de Autoscale (recuento de máquinas encendidas de Autoscale) es inferior al 10%. Los parámetros de Autoscale están alineados con el uso histórico.




- **No hay datos históricos disponibles**. No hay datos históricos disponibles. Las posibles causas incluyen que Autoscale se habilitó para el grupo de entrega hace menos de una semana.




4. Para resaltar un intervalo de fechas en función de una programación de Autoscale, seleccione la programación en el campo **Ver por**.
5. Según su análisis, ajuste los parámetros de Autoscale. Para obtener más información, consulte Parámetros basados en la programación y en la carga.

## Comandos del SDK de Broker PowerShell

November 17, 2023

Puede configurar Autoscale para grupos de entrega mediante el SDK de Broker PowerShell. Para configurar Autoscale con comandos de PowerShell, debe utilizar la versión 7.21.0.12 del SDK de PowerShell remoto o una posterior. Para obtener más información sobre el SDK de PowerShell remoto, consulte SDK y API.

### Set-BrokerDesktopGroup

Inhabilita o habilita un grupo BrokerDesktopGroup o altera su configuración. Para obtener más información sobre este cmdlet, consulte https://citrix.github.io/delivery-controller-sdk/Broker/Set-BrokerDesktopGroup/.

#### Ejemplos

Consulte los ejemplos siguientes para obtener información detallada sobre cómo utilizar los cmdlets de PowerShell.

Habilitar Autoscale

- Supongamos que quiere habilitar Autoscale para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-AutoscalingEnabled $true
  ```

Configurar el búfer de capacidad por separado para las horas punta y las horas normales

- Supongamos que quiere establecer el búfer de capacidad en un 20 % para las horas punta y un 10 % para las horas de actividad normal en el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakBufferSizePercent 20 -OffPeakBufferSizePercent 10
  ```

Configurar el parámetro del **tiempo de espera cuando se desconecta**

- Supongamos que quiere establecer el valor del **tiempo de espera cuando se desconecta** en 60 minutos para las horas punta y 30 minutos para las horas de actividad normal para un grupo de entrega llamado "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

  ```
  PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakDisconnectTimeout 60 -OffPeakDisconnectTimeout 30
  ```

Configurar el parámetro del **tiempo de espera cuando se cierra la sesión**

- Supongamos que quiere establecer el valor del **tiempo de espera cuando se cierra la sesión** en 60 minutos para las horas punta y 30 minutos para las horas de actividad normal para un grupo de entrega llamado "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PeakLogOffTimeout
  60 -OffPeakLogOffTimeout 30
```

Configurar el parámetro de **demora de apagado**

- Supongamos que quiere establecer la demora de apagado en 15 minutos para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-PowerOffDelay 15
```

Configurar un período de tiempo durante el cual la demora del apagado no se produzca

- Supongamos que quiere que la demora del apagado no se produzca hasta que hayan transcurrido 30 minutos para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

```
- C:\PS> Set-BrokerDesktopGroup "MyDesktop"-SettlementPeriodBeforeAutoSh
  30.
```

Configurar el parámetro del **coste de instancia de máquina**

- Supongamos que quiere establecer el coste de instancia de máquina por hora en 0,2 USD para el grupo de entrega "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

```
- PS C:\> Set-BrokerDesktopGroup "MyDesktop"-MachineCost 0.2
```

### New-BrokerPowerTimeScheme

Crea un esquema BrokerPowerTimeScheme para un grupo de entrega. Para obtener más información, consulte https://citrix.github.io/delivery-controller-sdk/Broker/New-BrokerPowerTimeScheme/.

#### Ejemplo

Supongamos que quiere crear un esquema de tiempo de energía para un grupo de entrega cuyo valor UID es 3. El nuevo esquema cubre el fin de semana, el lunes y el martes. La franja horaria de 8:00 a 18:30 se define como horas punta en los días incluidos en el esquema. Para las horas punta, el tamaño del grupo (la cantidad de máquinas que se mantienen encendidas) es 20. Para las horas normales, es 5. Puede utilizar el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

```
• PS C:\> $ps48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ 5 } else
  { 20 } } )
```

- `PS C:\> $pt48=(0..47 | %{ if ($_ -lt 16 -or $_ -gt 37){ $false } else { $true } } )`
- `PS C:\> New-BrokerPowerTimeScheme -Name 'First Half Week'-DaysOfWeek Weekend,Monday,Tuesday -DesktopGroupUid 3 -PeakHalfHours $pt48 -PoolSize $ps48`

### Parámetros para los tiempos de espera dinámicos de las sesiones

Estos cmdlets del SDK de Broker PowerShell se han ampliado para permitir tiempos de espera de sesión dinámicos gracias a varios parámetros nuevos:

- Get-BrokerDesktopGroup
- New-BrokerDesktopGroup
- Set-BrokerDesktopGroup

Estos parámetros incluyen:

- **DisconnectPeakIdleSessionAfterSeconds**: Representa el tiempo en segundos tras el cual se desconecta una sesión inactiva durante las horas punta. Esta propiedad tiene un valor predeterminado de 0, que indica la inhabilitación de su comportamiento asociado durante las horas punta. Un valor superior a 0 habilita su comportamiento para el grupo de entrega solamente durante las horas punta.
- **DisconnectOffPeakIdleSessionAfterSeconds**: Representa el tiempo en segundos tras el cual se desconecta una sesión inactiva durante las horas de actividad normal. El valor predeterminado de esta propiedad es 0, lo que indica la inhabilitación de su comportamiento asociado durante las horas de actividad normal. Un valor superior a 0 habilita su comportamiento asociado para el grupo de entrega solamente durante las horas de actividad normal.
- **LogoffPeakDisconnectedSessionAfterSeconds**: Representa el tiempo en segundos tras el cual finaliza una sesión desconectada durante las horas punta. El valor predeterminado de esta propiedad es 0, lo que indica la inhabilitación de su comportamiento asociado durante las horas punta. Un valor superior a 0 habilita su comportamiento asociado para el grupo de entrega solamente durante las horas punta.
- **LogoffOffPeakDisconnectedSessionAfterSeconds**: Representa el tiempo en segundos tras el cual finaliza una sesión desconectada durante las horas de actividad normal. El valor predeterminado de esta propiedad es 0, lo que indica la inhabilitación de su comportamiento asociado durante las horas de actividad normal. Un valor superior a 0 habilita su comportamiento asociado para el grupo de entrega solamente durante las horas de actividad normal.

**Ejemplo**

Supongamos que quiere establecer el tiempo de espera de sesión inactiva en 3600 segundos durante las horas punta de un grupo de entrega cuyo nombre es "MyDesktop". Utilice el comando `Set-BrokerDesktopGroup` de PowerShell. Por ejemplo:

- `C:\PS> Set-BrokerDesktopGroup "MyDesktop"-DisconnectOffPeakIdleSessionAfte 3600`

Al hacerlo, se desconectan las sesiones que hayan estado inactivas durante más de 1 hora en horas normales para el grupo de escritorios denominado "MyDesktop".

## Comprobación de estado de Cloud

December 9, 2022

> **Nota:**
>
> Comprobación de estado de Cloud está integrado en Citrix DaaS. La integración está disponible en forma de acción Realizar comprobación de estado en la interfaz de administración de Configuración completa. Para obtener más información, consulte Solucionar problemas de registro de VDA e inicio de sesión.

Comprobación de estado de Cloud le permite hacer comprobaciones en las que se evalúa el estado y la disponibilidad del sitio y sus componentes. Puede hacer comprobaciones de estado de agentes VDA, servidores StoreFront y Profile Management. Las comprobaciones de estado de los VDA identifican posibles causas de problemas comunes con el registro y el inicio de sesión de los VDA.

Si hay problemas durante las comprobaciones, Comprobación de estado de Cloud proporciona un informe detallado y medidas para solucionar los problemas. Cada vez que Comprobación de estado de Cloud se inicia, comprueba la última versión de los scripts en la red de entrega de contenido (CDN) y descarga automáticamente los scripts si no existen en la máquina local. Comprobación de estado de Cloud elige siempre la última versión local de los scripts para ejecutar las comprobaciones de estado.

> **Nota:**
>
> Comprobación de estado de Cloud no se actualiza cada vez que se ejecuta.

En un entorno de Citrix Cloud, ejecute Comprobación de estado de Cloud desde una máquina unida a un dominio para hacer las comprobaciones en uno o varios VDA o servidores StoreFront.

> **Nota:**
>
> Comprobación de estado de Cloud no se puede instalar ni ejecutar en Cloud Connector.

El registro de la aplicación Comprobación de estado de Cloud se almacena en `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`. Puede utilizar este archivo para solucionar problemas.

Aquí dispone de una introducción a la Comprobación de estado de Cloud.


Aquí puede ver cuándo usar la Comprobación de estado de Cloud.

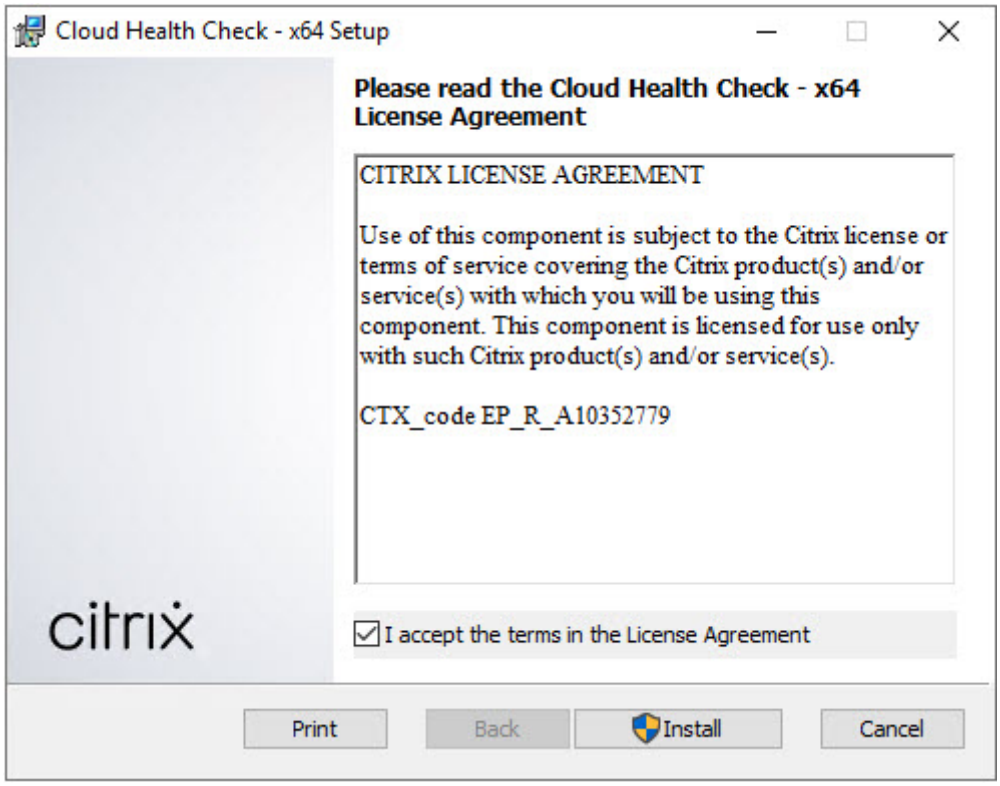
## Instalación

Para preparar su entorno para la instalación de Comprobación de estado de Cloud, debe tener una máquina Windows unida a un dominio.

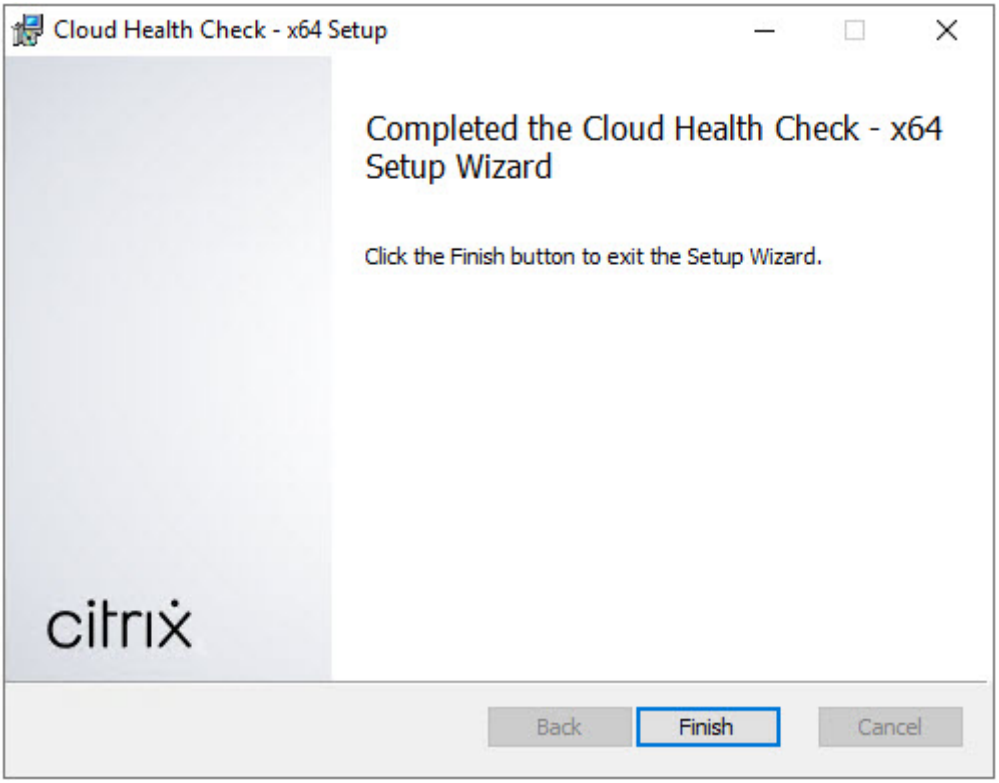
> **Nota:**
>
> Comprobación de estado de Cloud no se puede instalar ni ejecutar en Cloud Connector.

1. En la máquina unida a un dominio, descargue el instalador de Cloud Health Check.
2. Haga doble clic en el archivo CloudHealthCheckInstaller_x64.msi.
3. Haga clic en la casilla para aceptar las condiciones.
4. Haga clic en Instalar.




5. Una vez completada la instalación, haga clic en **Finalizar**.



### Permisos y requisitos

Permisos:

- Para realizar comprobaciones de estado:
  - Debe ser miembro del grupo de usuarios del dominio.
  - Debe ser administrador total o tener un rol personalizado con permisos de solo lectura y de **ejecución de pruebas de entorno** para el sitio.
  - Establezca la directiva de ejecución de scripts en, al menos, `RemoteSigned` para permitir que se ejecuten los scripts. Por ejemplo: `Set-ExecutionPolicy RemoteSigned`. **Nota:** Otros permisos de ejecución de scripts también pueden funcionar.
- Use la opción **Ejecutar como administrador** al iniciar Comprobación de estado de Cloud.

Para cada máquina VDA o StoreFront en la que ejecute comprobaciones de estado:

- El sistema operativo debe ser de 64 bits.
- Comprobación de estado de Cloud debe poder comunicarse con la máquina.
- La posibilidad de compartir archivos e impresoras debe estar activada.
- PSRemoting y WinRM deben estar habilitados. La máquina también debe ejecutar PowerShell 3.0 o posterior.
- El acceso a Windows Management Infrastructure (WMI) debe estar habilitado en la máquina.

### Acerca de las comprobaciones de estado

Los datos de las comprobaciones de estado se almacenan en carpetas dentro de `C:\ProgramData\Citrix\TelemetryService\`.

#### Comprobaciones de estado en el VDA

Para el registro en el VDA, Comprobación de estado de Cloud comprueba lo siguiente:

- Instalación del software en el VDA
- Pertenencia al dominio de máquinas en el VDA
- Disponibilidad del puerto de comunicación en el VDA
- Estado del servicio en el VDA
- Configuración del firewall de Windows
- Comunicación con el Controller
- Sincronización de tiempo con el Controller
- Estado de registro de VDA

Para inicio de sesiones en VDA, Comprobación de estado de Cloud comprueba lo siguiente:

- Disponibilidad del puerto de comunicación en el inicio de sesión
- Estado de los servicios en el inicio de sesión
- Configuración del firewall de Windows en el inicio de sesión
- Licencias de acceso de cliente a Servicios de Escritorio remoto en VDA
- Ruta de inicio de aplicaciones en VDA
- Parámetros de Registro para el inicio de sesiones
- Estado del controlador de inyección universal de Citrix (CTXUVI)

Para Profile Management en VDA, Comprobación de estado de Cloud comprueba lo siguiente:

- Detección de hipervisor
- Detección de aprovisionamiento
- Citrix Virtual Apps and Desktops
- Configuración de disco Personal vDisk
- Almacén de usuarios
- Detección de estado de Profile Management Service
- Prueba de enlazado de Winlogon.exe

Para ejecutar comprobaciones en Profile Management, debe instalar y habilitar Profile Management en el VDA. Para obtener más información sobre las comprobaciones de configuración de Profile Management, consulte el artículo CTX132805 de Knowledge Center

#### Comprobaciones de estado de StoreFront

Las comprobaciones de StoreFront verifican si:

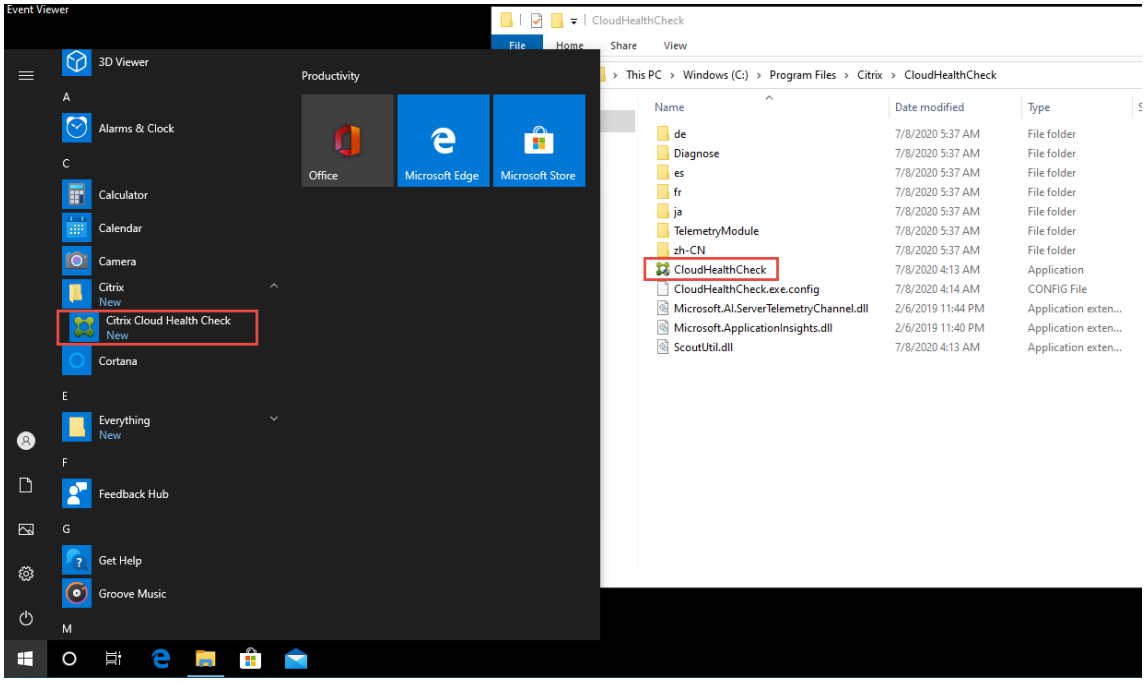
- Citrix Default Domain Service no está activo
- Citrix Credential Wallet Service no está activo
- La conexión desde el servidor de StoreFront a Active Directory es a través del puerto 88
- La conexión desde el servidor de StoreFront a Active Directory es a través del puerto 389
- La conexión desde el servidor de StoreFront a Active Directory es a través del puerto 464
- La URL base tiene un nombre FQDN válido
- La dirección IP correcta de la URL base se puede obtener
- El grupo de aplicaciones de IIS utiliza .NET 4.0
- El certificado está enlazado al puerto SSL para la URL del host
- La cadena de certificados está completa
- Los certificados han caducado
- Un certificado caduca en un plazo de 30 días

### Ejecución de Comprobación de estado de Cloud

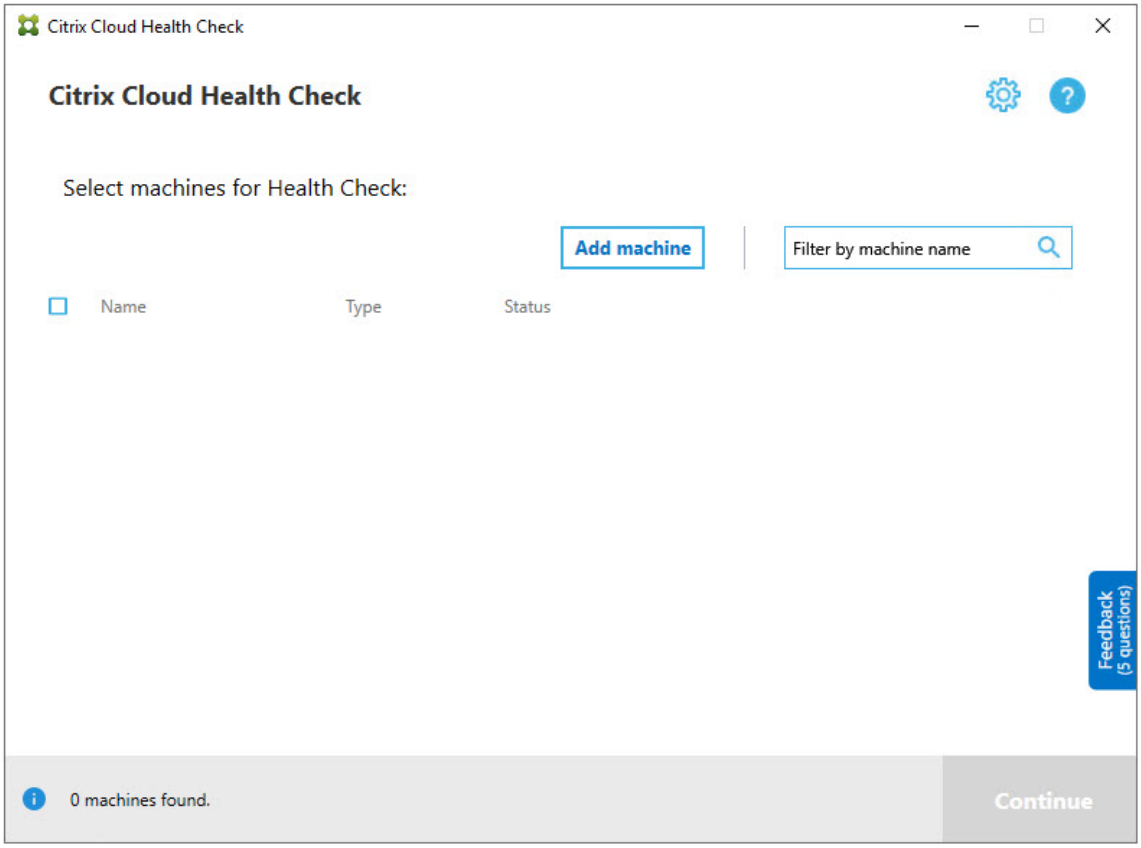
Para ejecutar Comprobación de estado de Citrix Cloud:

1. Seleccione **Citrix > Comprobación de estado de Citrix Cloud** en el menú Inicio de la máquina o ejecute `CloudHealthCheck.exe` en `C:\Program Files\Citrix\CloudHealthCheck`.



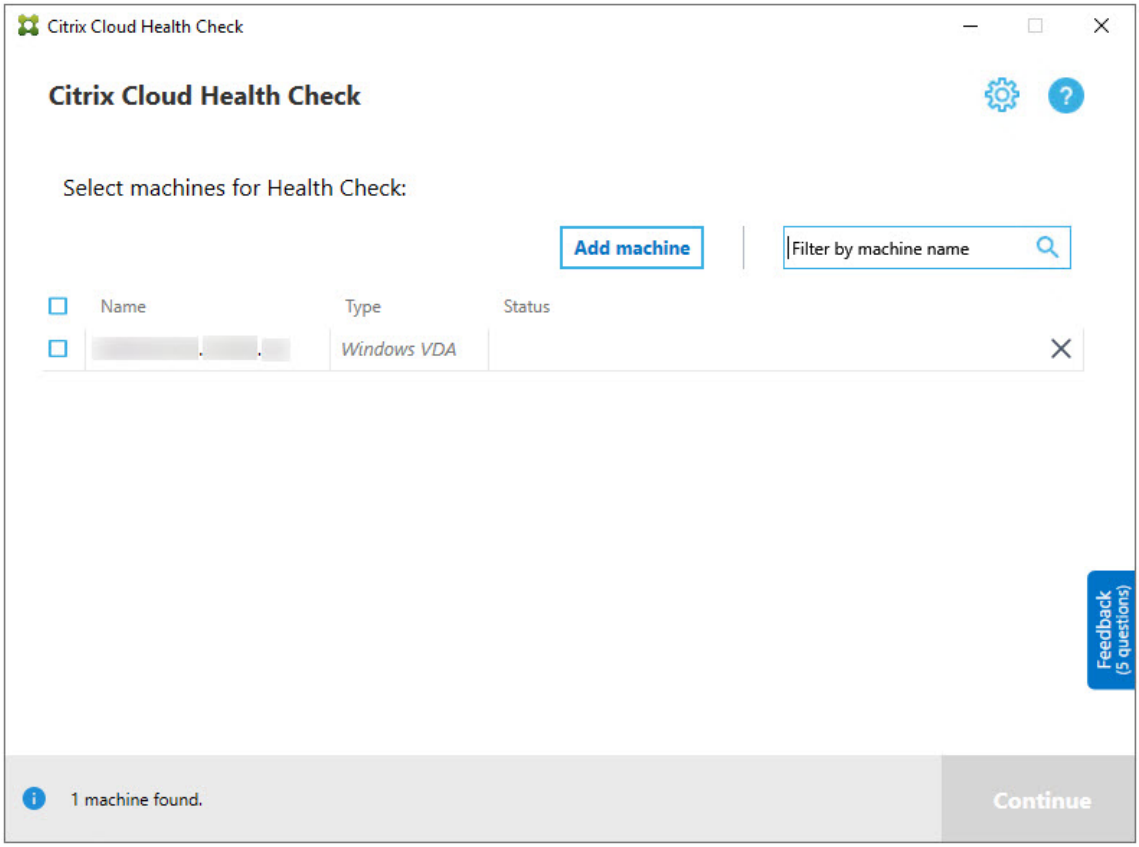

2. En la pantalla principal de Comprobación de estado de Cloud, haga clic en **Agregar máquina**.




3. Introduzca el nombre FQDN de la máquina que quiera agregar. **Nota:** Aunque introducir un alias DNS en lugar de un nombre FQDN pueda parecer válido, es posible que las comprobaciones de estado fallen.
4. Haga clic en **Continue**.
5. Repita los pasos para agregar otras máquinas si fuera necesario.




6. Para quitar una máquina agregada manualmente, haga clic en la **X** situada en el extremo derecho de la fila y confirme la eliminación. Repita los pasos para eliminar otras máquinas que se hayan agregado manualmente.

Comprobación de estado de Cloud recuerda las máquinas agregadas manualmente hasta que las quita. Al cerrar y volver a abrir Comprobación de estado de Cloud, las máquinas agregadas manualmente siguen figurando en la parte superior de la lista.

### Importar máquinas VDA

Puede importar máquinas VDA en la implementación al realizar comprobaciones de estado.

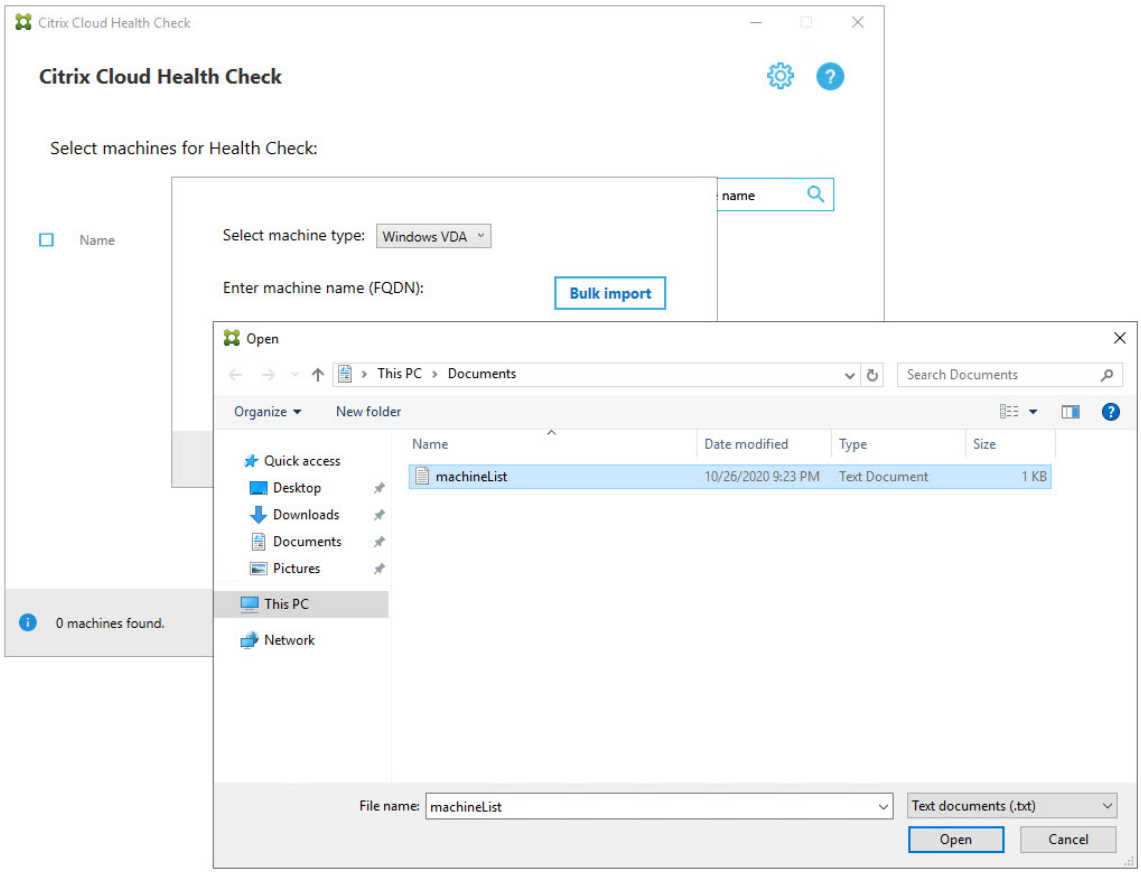
1. En Connector, genere el archivo de lista de máquinas con el siguiente comando de PowerShell. En Connector, debe introducir credenciales de Citrix y seleccionar al cliente en el cuadro de diálogo emergente.

```
Get-BrokerMachine| foreach { $_.DnsName } | out-file C:\machineList.
txt
```

1. Copie el archivo machineList.txt en la máquina unida al dominio donde quiere ejecutar Comprobación de estado de Cloud.

2. En la página Comprobación de estado de Cloud, haga clic en **Agregar máquina**.
3. Seleccione el tipo de máquina Windows VDA.
4. Haga clic en **Importar máquinas VDA**.
5. Seleccione el archivo machineList.txt.
6. Haga clic en **Abrir**.




Las máquinas VDA importadas se enumeran en la página Comprobación de estado de Cloud.

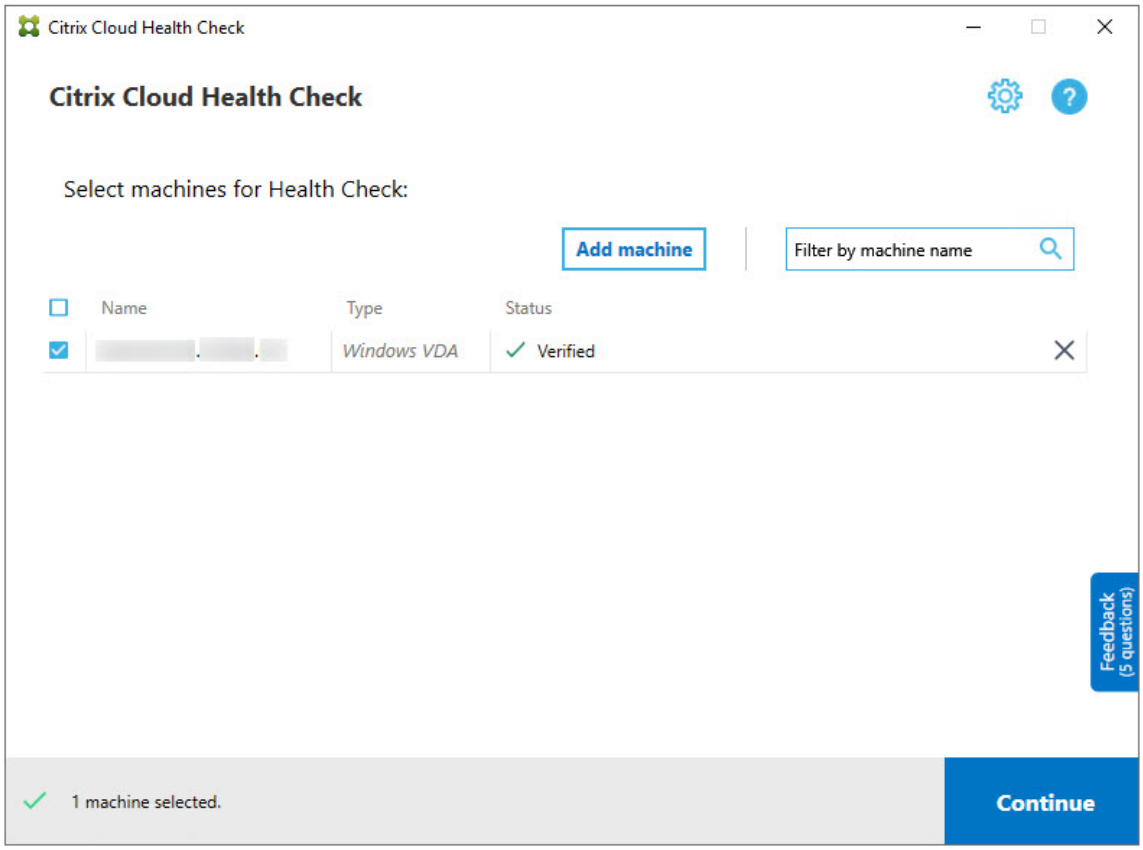
7. Marque la casilla de verificación situada junto a cada máquina en la que quiera realizar comprobaciones de estado.

   Comprobación de estado de Cloud inicia automáticamente pruebas en cada máquina seleccionada para comprobar que cumple los criterios que figuran en las pruebas de verificación. Si se produce un error en la verificación, aparece un mensaje en la columna **Estado** y la casilla de verificación correspondiente a la máquina se desmarca. A continuación, puede:

   - Resolver el problema y, a continuación, volver a marcar la casilla de verificación de la máquina. Esto provoca un reintento de las pruebas de verificación.
   - Omitir esa máquina (dejando la casilla de verificación desmarcada). Las comprobaciones de estado no se ejecutan para esa máquina.

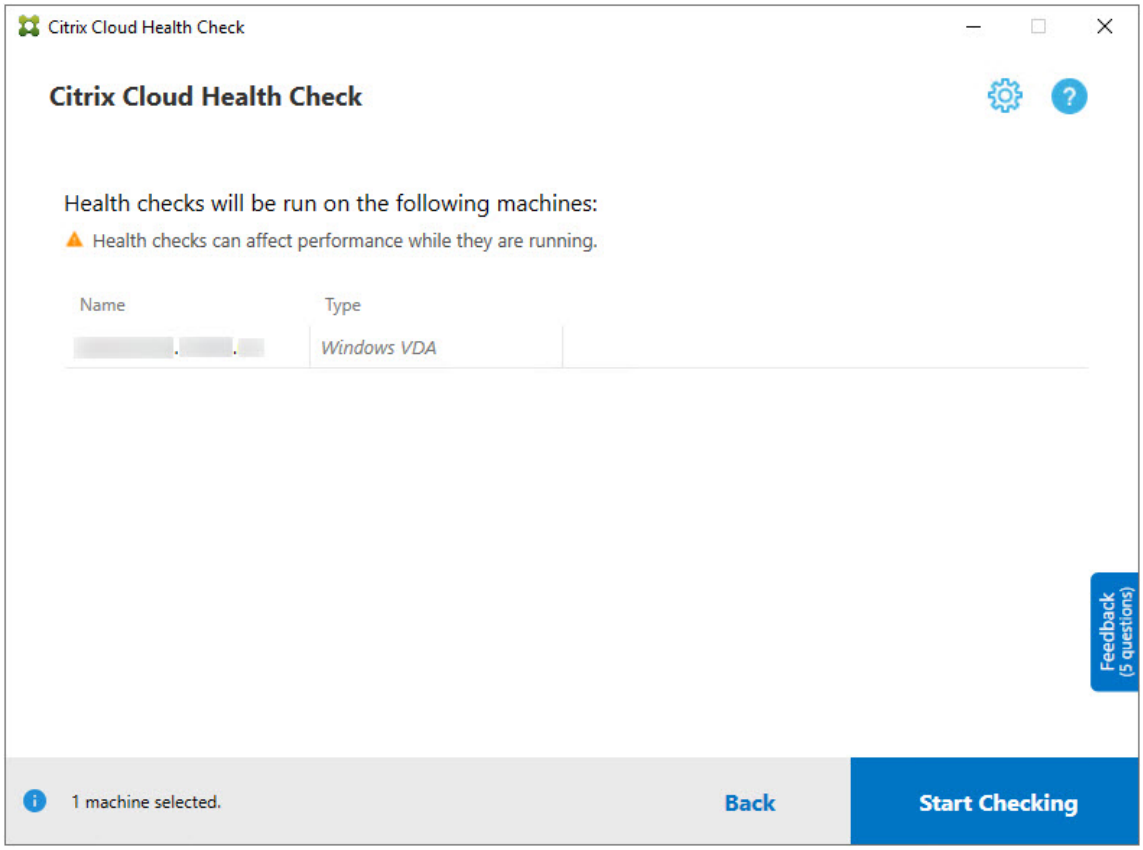
 

8. Cuando finalicen las pruebas de verificación, haga clic en **Continuar**.




9. Realice las comprobaciones de estado en las máquinas seleccionadas. En el resumen, se ofrece una lista de las máquinas en que se realizan las pruebas (las máquinas seleccionadas que han superado las pruebas de verificación).
10. Haga clic en **Iniciar la comprobación**.

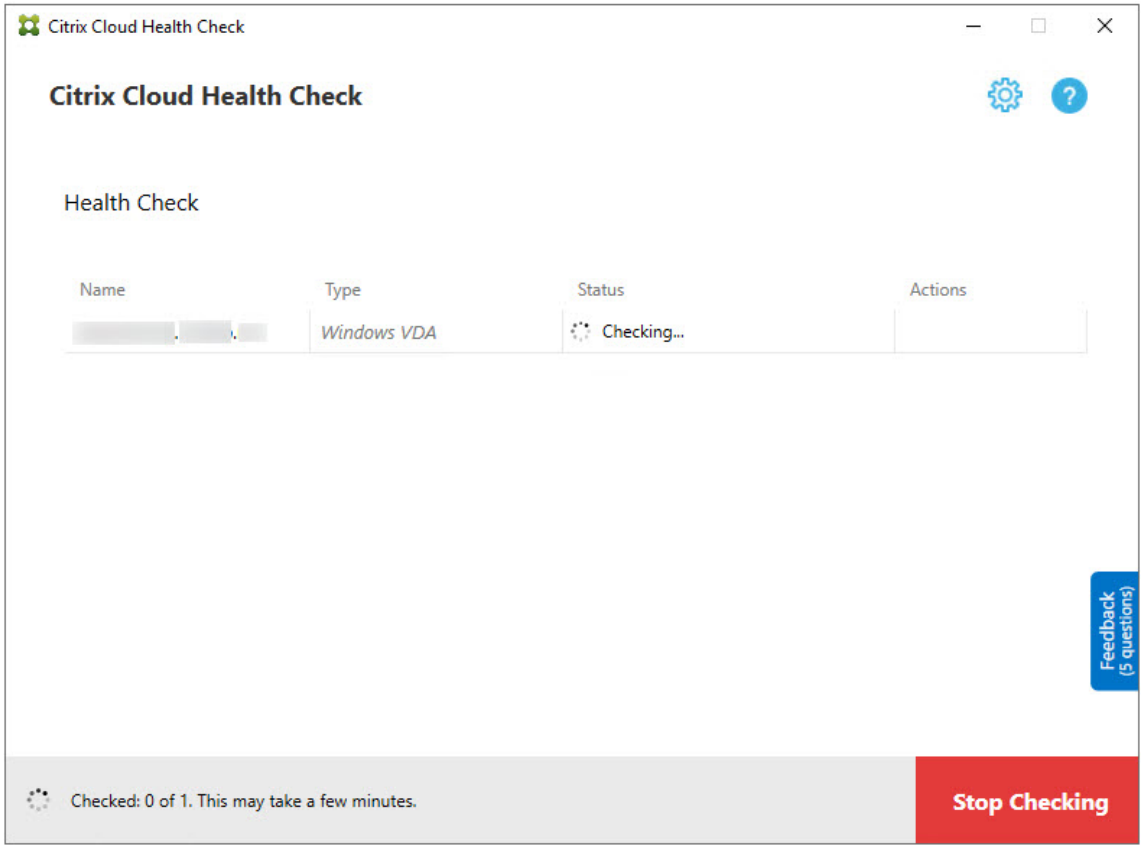
 




Durante y después de la comprobación, la columna **Estado** indica el estado de comprobación actual de una máquina.

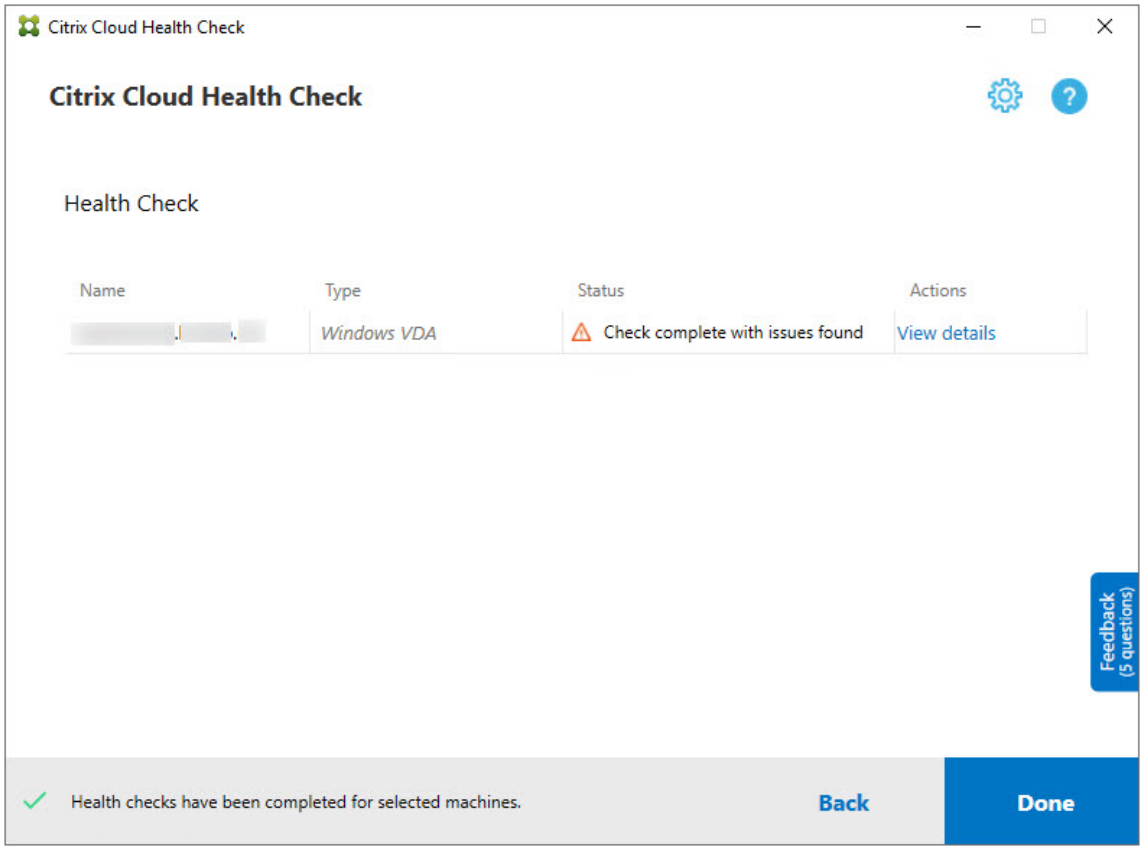
11. Para detener todas las comprobaciones en curso, haga clic en **Detener comprobación** en la esquina inferior derecha de la página No puede cancelar la comprobación de estado de una sola máquina; solamente puede hacerlo para todas las máquinas seleccionadas.

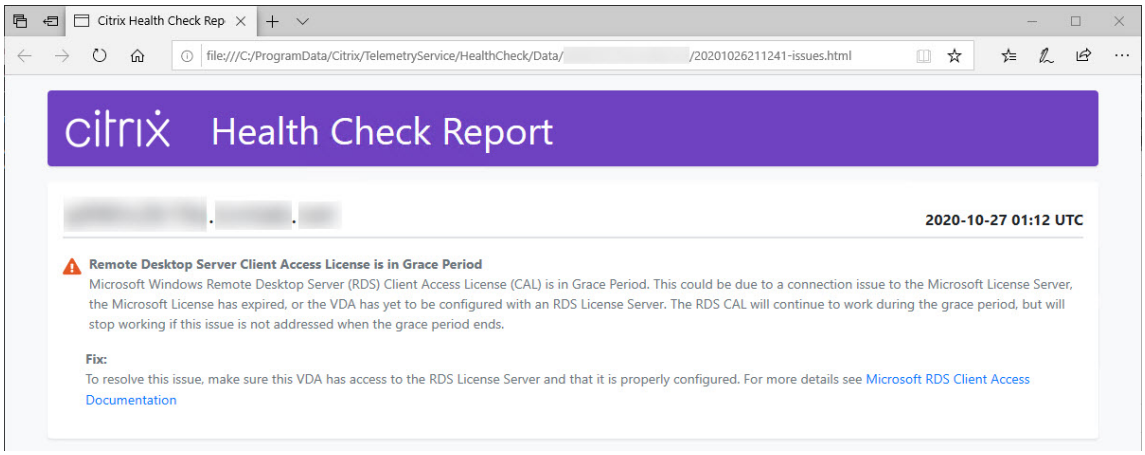



12. Cuando se completa la comprobación de todas las máquinas seleccionadas, el botón **Detener comprobación** de la esquina inferior derecha cambia a **Listo**.

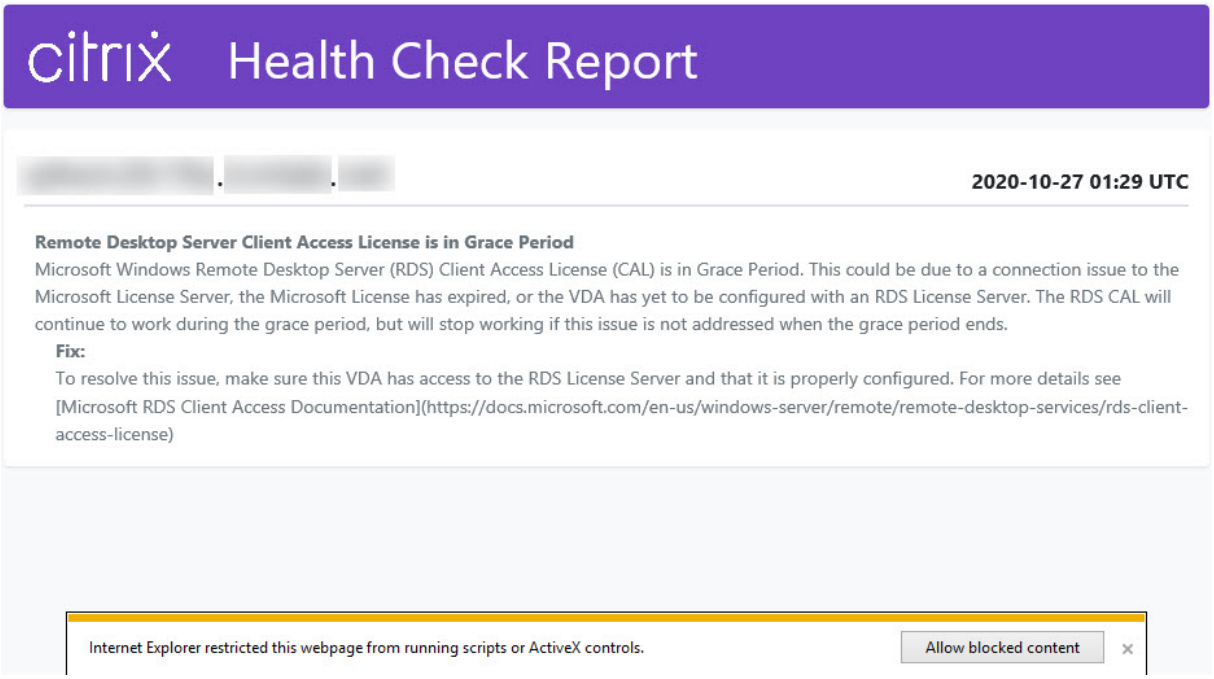



- Si se produce un error en una comprobación, haga clic en **Reintentar** en la columna **Acción**.
- Si se completa una comprobación sin que se haya encontrado ningún problema, la columna **Acción** estará vacía.
- Si una comprobación encuentra problemas, haga clic en **Ver detalles** para consultar los resultados.




Si utiliza Internet Explorer para ver el informe, debe hacer clic en **Permitir contenido bloqueado** para mostrar el hipervínculo.




Si una vez finalizada la comprobación para todas las máquinas seleccionadas se hace clic en **Atrás**, se pierden los resultados de la comprobación.

Cuando finalicen las comprobaciones, haga clic en **Listo** para volver a la pantalla principal de Comprobación de estado de Cloud.

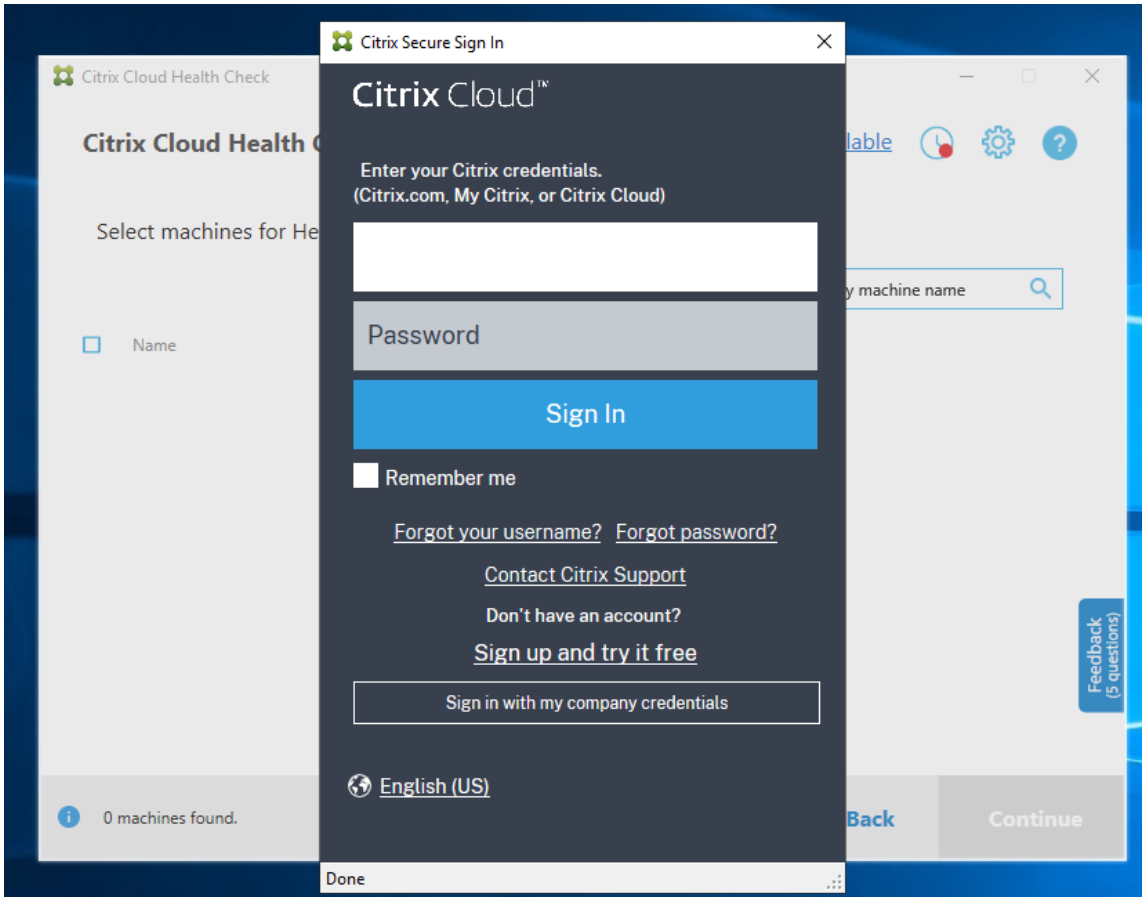
### Obtener máquinas VDA

Comprobación de estado de Cloud puede detectar y obtener automáticamente los VDA de las implementaciones de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service).

Para obtener los agentes VDA:

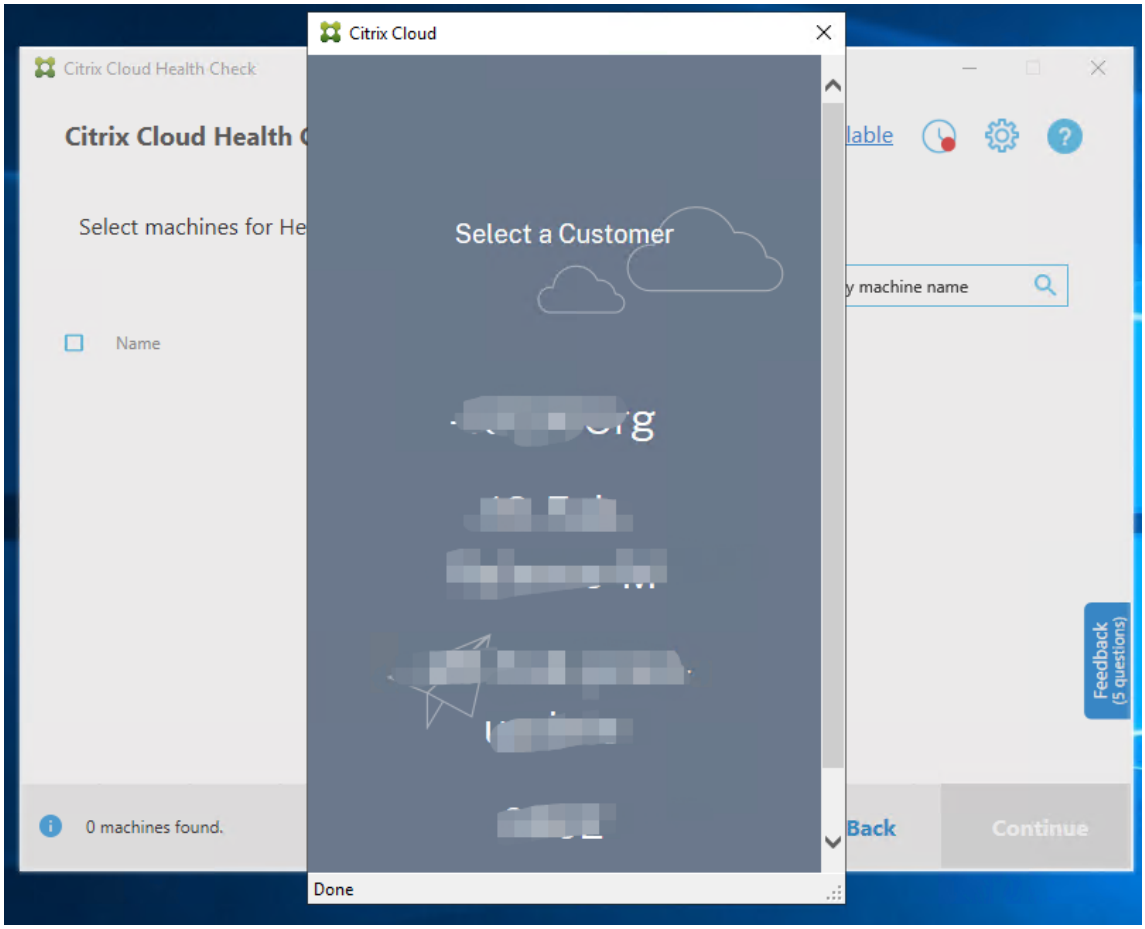
1. Prepare una nueva máquina que esté unida al mismo bosque de dominios en el que se ejecuta Comprobación de estado de Cloud.
2. Abra Comprobación de estado de Cloud y haga clic en **Buscar máquina** para iniciar sesión en Citrix Cloud.



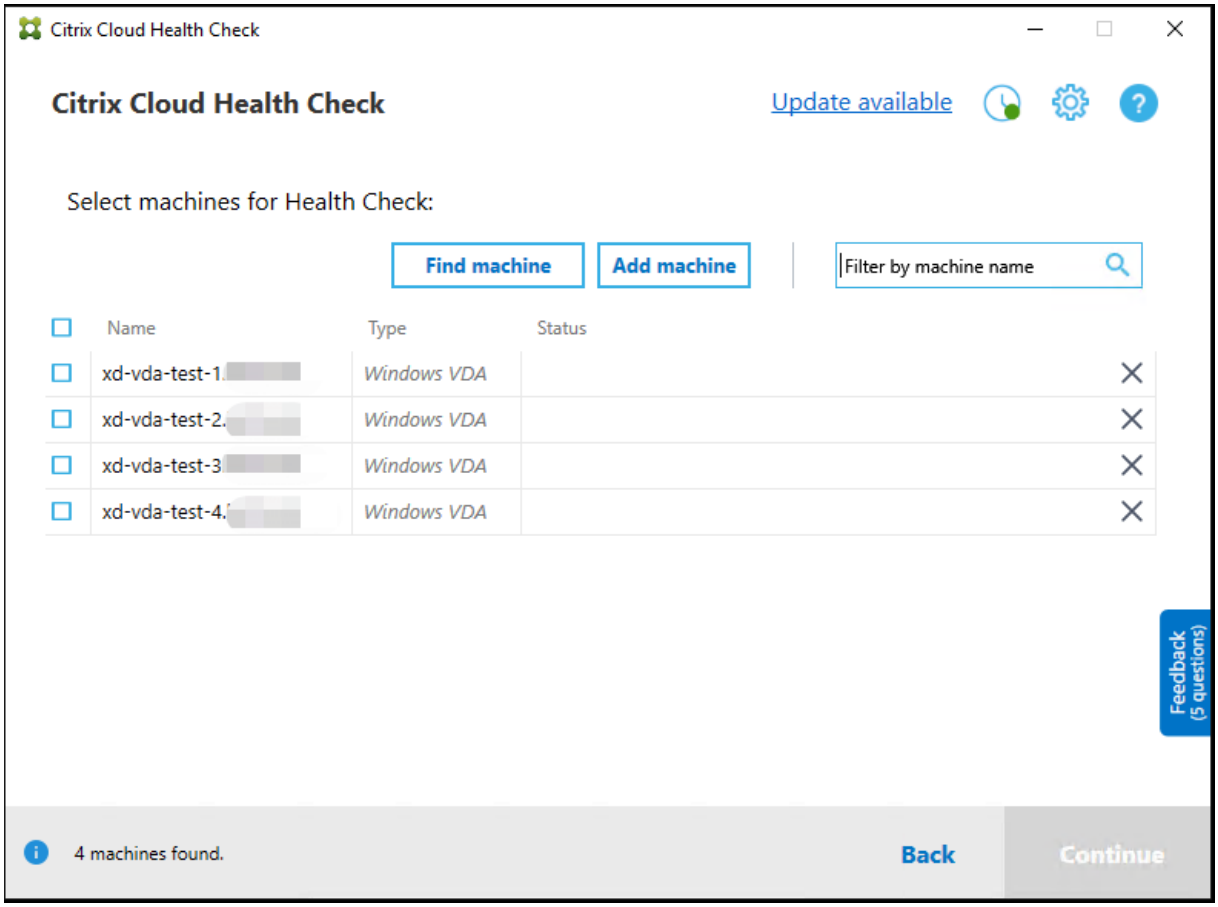

3. Seleccione el cliente con el sitio en la nube que desea obtener.




La lista de VDA aparece en Comprobación de estado de Cloud. La lista también se guarda en un archivo local ubicado en `\ProgramData\Citrix\TelemetryService\ChcDiscovery\ChcDiscoveredMachineList.json`.

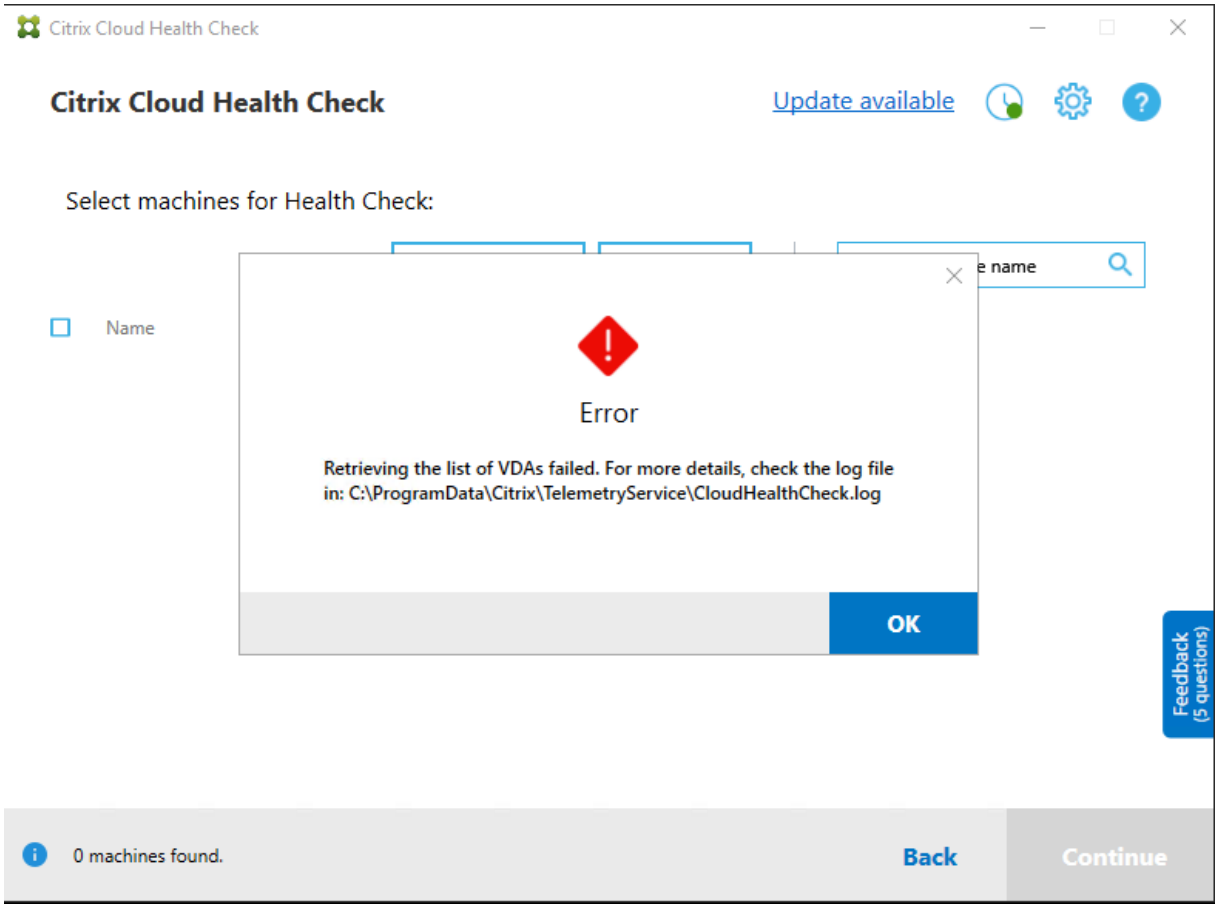
 




La lista de sus máquinas carga la caché local al abrir de nuevo Comprobación de estado de Cloud. Si ha hecho alguna actualización en la implementación, debe hacer clic en **Buscar máquina** para actualizar la lista de máquinas.

> **Nota:**
>
> - Comprobación de estado de Cloud solo encuentra máquinas del mismo bosque de dominios en el que se ejecuta.
> - Las sesiones de Citrix Cloud caducan en una hora. Después de una hora, debe hacer clic en **Buscar máquina** de nuevo para obtener la lista de VDA más reciente.
> - Aparecerá un mensaje de error si la obtención de la lista de VDA falla. Puede consultar los detalles en `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.




### Resultados de la comprobación de estado

Las comprobaciones de estado con las que se generan informes contienen los siguientes elementos:

- Hora y fecha en que se generó el informe de resultados
- Nombre de dominio completo de las máquinas que se verificaron
- Condiciones comprobadas en las máquinas de destino

### Ejecución de Comprobación de estado de Cloud en la línea de comandos

Se puede ejecutar Comprobación de estado de Cloud en la línea de comandos para ayudar a los clientes a realizar comprobaciones de estado. Para usar Comprobación de estado de Cloud en la línea de comandos, debe ser administrador de la máquina en la que se está ejecutando.

> **Nota:**
>
> Cuando se utiliza Comprobación de estado de Cloud en la línea de comandos, solo se puede com-

> probar una máquina cada vez. Solo se puede ejecutar una instancia de `CloudHealthCheck.exe` al mismo tiempo en la máquina de destino. Si quiere comprobar varios equipos, deben comprobarse uno por uno, mediante el empaquetado de cmdlets en un bucle en scripts de cmdlet/PowerShell. También se debe cerrar cualquier instancia abierta de interfaz de usuario de Comprobación de estado de Cloud.

#### Cmdlets

Los cmdlets de línea de comandos admitidos son:

- `MachineFQDN`: Este cmdlet es **obligatorio**. Este es el nombre de dominio completo de la máquina de destino.
- `MachineType`: Este cmdlet es opcional. El valor del cmdlet puede ser el VDA de Windows (valor predeterminado) o StoreFront.
- `ReportName`: Este cmdlet es opcional. El valor del cmdlet debe ser un nombre de archivo válido en Windows. El valor predeterminado de `HealthCheckReport`.
- `SkipAdminCheck`: Este cmdlet es opcional. Se puede agregar para omitir las comprobaciones que requieren permisos de administrador.
- `UpdateScripts`: Este cmdlet es opcional. Se puede agregar para actualizar los scripts de comprobación del servidor CDN.
- `DisableCeip` - Este cmdlet es opcional si CEIP está habilitado en la interfaz de usuario; agréguelo para inhabilitar CEIP.
- `Help` - Muestra información de ayuda sobre los parámetros.

Ejemplos:

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -ReportName checkreport
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -SkipAdminCheck
```

```
HealthCheckCLI.exe -MachineFQDN machine.domain.local -UpdateScripts
```

```
HealthCheckCLI.exe -MachineFQDN machine1.domain.local,machine2.domain.local,machine3.domain.local
```

```
HealthCheckCLI.exe -Help
```

> **Nota:**
>
> Los nombres de parámetros no distinguen entre mayúsculas y minúsculas.

De forma predeterminada, la salida de la consola no aparece en la ventana de la consola de línea de comandos. Puede mostrar manualmente el resultado al agregar `|more` al cmdlet.

Ejemplo:`HealthCheckCLI.exe -MachineFQDN machine.domain.local|more`

La línea de comandos predeterminada necesita permisos de administrador para ejecutarse. Agregue el parámetro `-SkipAdminCheck` para omitir la necesidad de utilizar permisos de administrador.

### Códigos de salida

Los códigos de salida explican el resultado de las comprobaciones de Comprobación de estado de Cloud dentro de la línea de comandos. Para obtener el código de salida, debe agregar `start /wait` antes del cmdlet.

Ejemplo:`start /wait HealthCheckCLI.exe -MachineFQDN machine.domain.local`

Los códigos de salida son:

- 0: Normal, comprobación completada y correcta.
- 1: Error, comprobación completada con problemas.
- 2: Error, comprobación no completada con errores.

También puede usar el cmdlet `echo %errorlevel%` para obtener el código de salida del último comando ejecutado.

### Informes

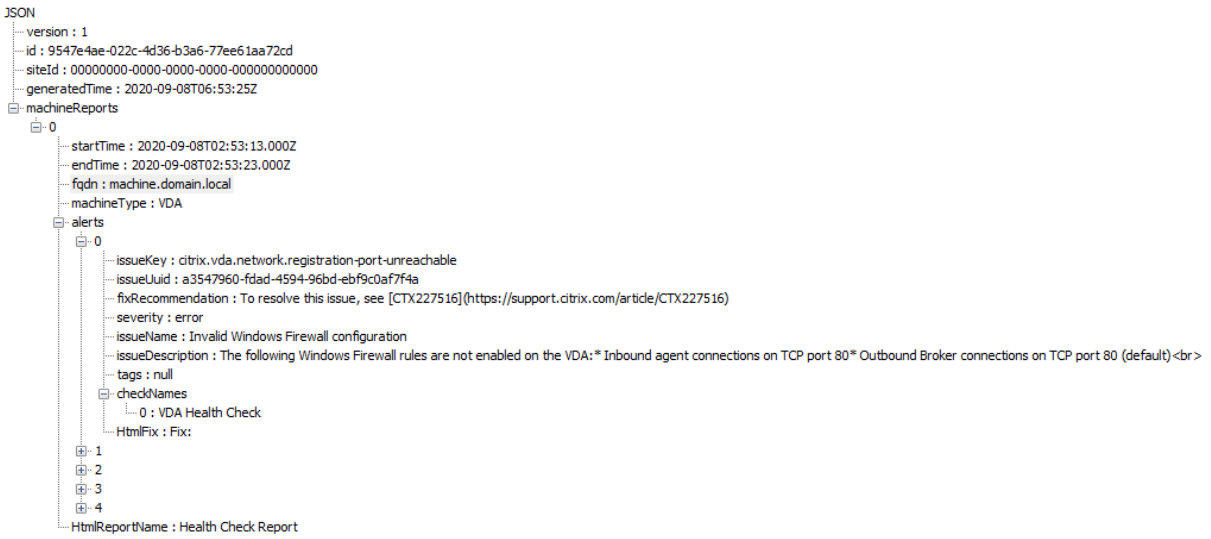
Comprobación de estado de Cloud crea carpetas con el nombre de la máquina en `HealthCheckDataFolder` para la máquina de destino. Se crea un archivo HTML y un archivo JSON en la máquina en la que está instalado Comprobación de estado de Cloud. Los informes de comprobación de estado se encuentran en `HealthCheckDataFolder`, en `%ProgramData%\Citrix\TelemetryService\HealthCheck\Data`.

Los informes solo se crean cuando existen problemas en la máquina de destino.

> **Nota:**
>
> Los archivos de informe se sobrescriben si el nombre de informe especificado existe.

Las alertas y la información básica se almacenan en el informe .json.



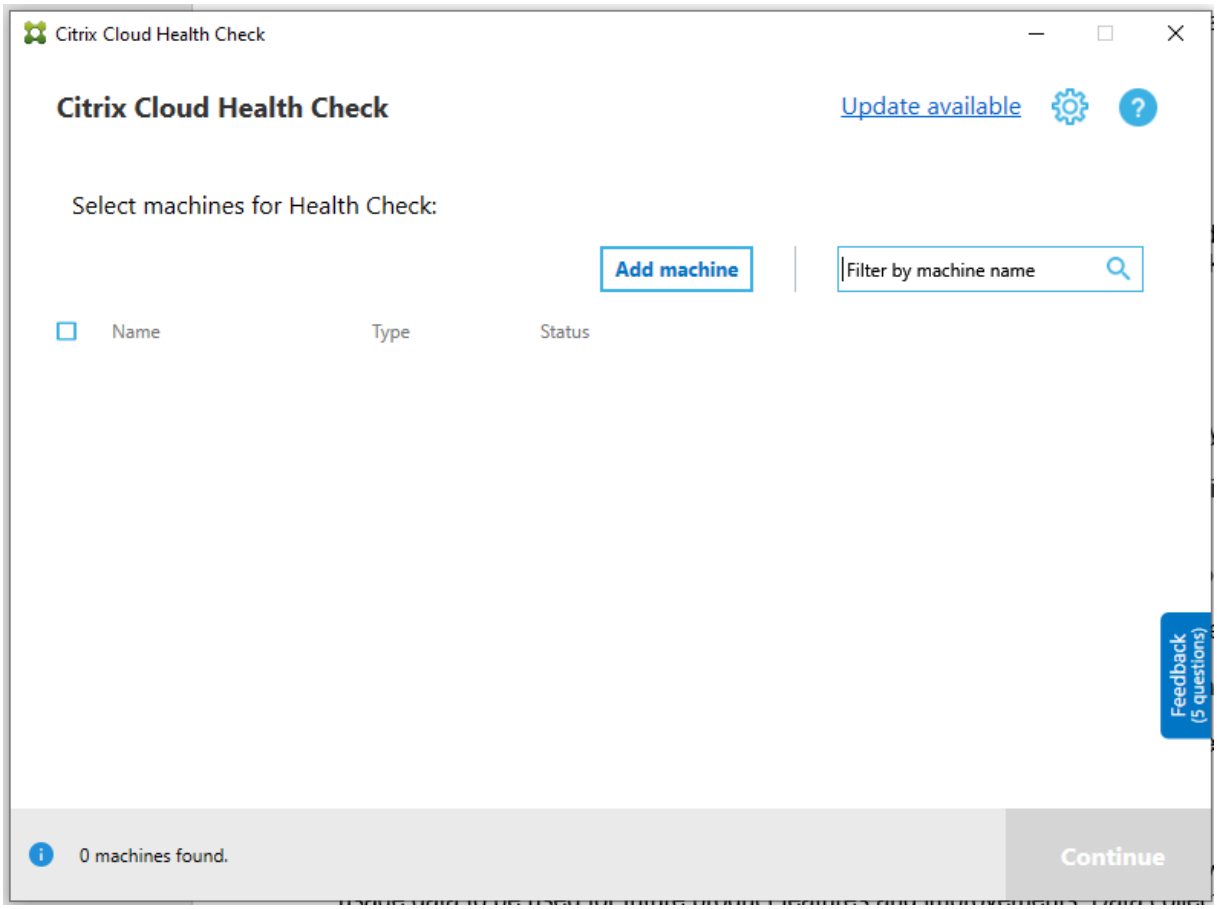

Los códigos de informe son:

- **issueKey**: Una descripción del problema en texto sin formato.
- **issueUuid**: Una cadena de identificación única para el problema.
- **fixRecommendation**: La corrección recomendada para el problema.
- **severity**: Indica si el problema debe corregirse. Un error puede indicar que el componente (VDA o StoreFront) funcionó mal y una advertencia indica que el componente puede funcionar pero podría tener algunos problemas potenciales.
- **issueName**: El título del problema.
- **issueDescription**: Una descripción detallada del problema.

### Actualizar Comprobación de estado de Cloud

Si hay disponible una nueva versión de Comprobación de estado de Cloud, aparece un enlace de actualización disponible en la parte superior derecha de la ventana de Comprobación de estado de Cloud. Haga clic en el enlace para ir a las descargas de Citrix y obtener la nueva versión.



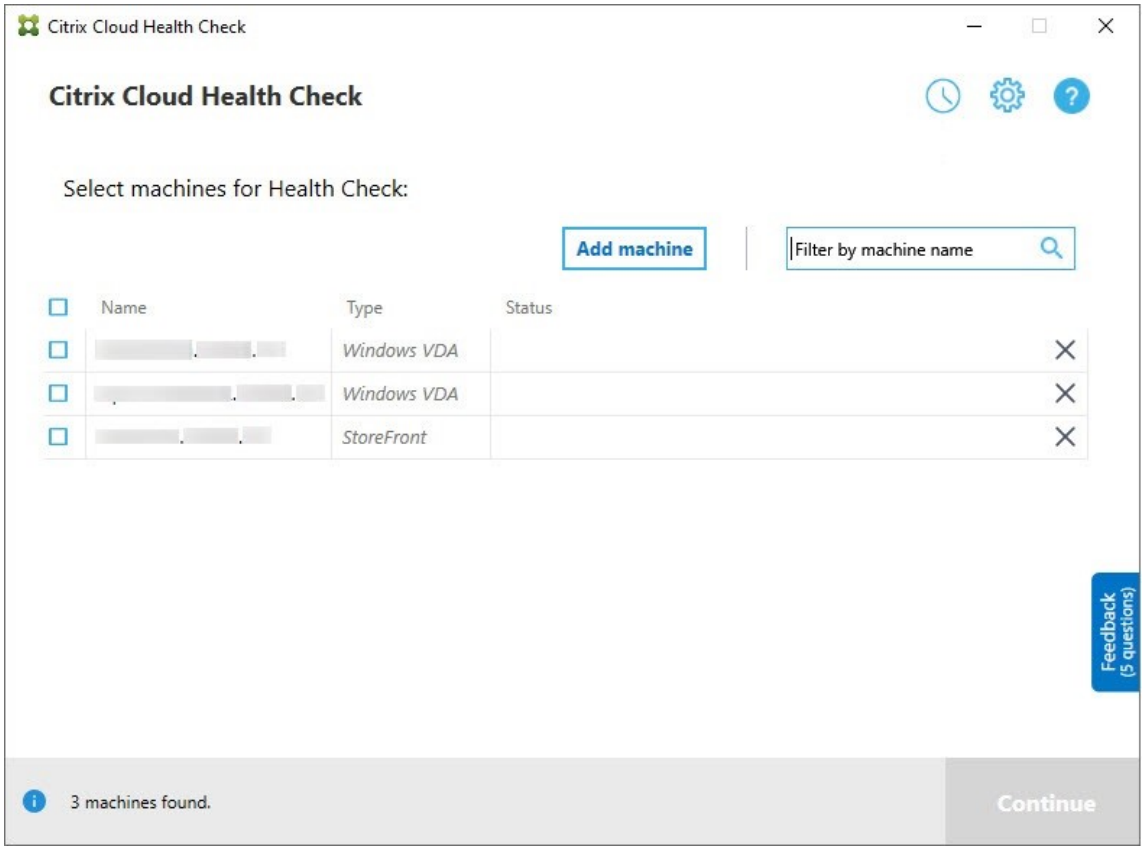

## Programador de Comprobación de estado de Cloud

Utilice el programador de Comprobación de estado de Cloud para realizar comprobaciones de estado periódicas.

### Configurar la programación

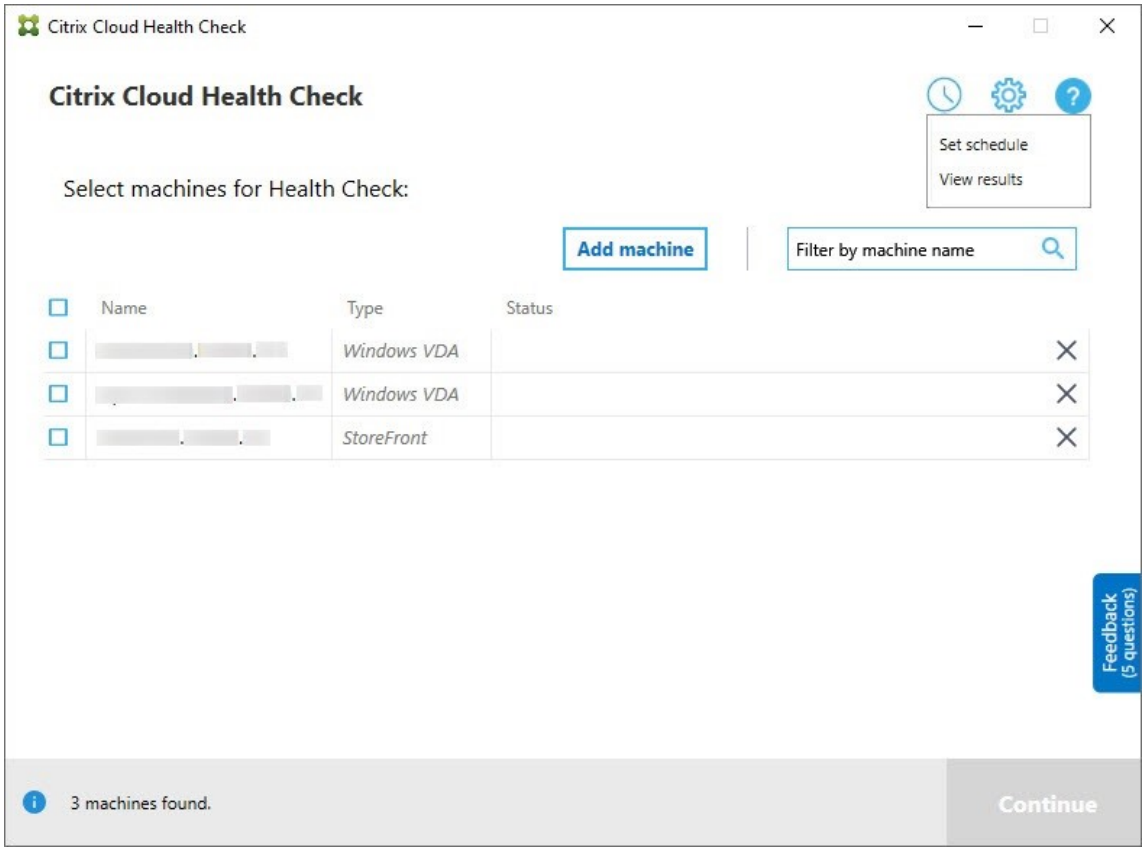
1. Haga clic en **Agregar máquina** en la ventana principal de Comprobación de estado de Cloud para máquinas equipos en las que quiere ejecutar comprobaciones periódicas.




2. Haga clic en el icono del reloj y, a continuación, en **Establecer programación**.




3. Seleccione una hora para la programación y, a continuación, haga clic en **Siguiente**. La tarea se puede establecer para que se repita activando la casilla de verificación **Repita la tarea cada**.
4. Seleccione esta opción para generar resultados en el registro de eventos de Windows. La tarea se puede configurar para escribir los resultados en el registro de eventos de Windows.
5. Seleccione activar un script personalizado de PowerShell una vez finalizada la comprobación programada y, a continuación, haga clic en **Siguiente**.

    - Haga clic en **Modificar** para modificar el contenido del script en Windows PowerShell ISE si es necesario.
    - Haga clic en **Locate** para abrir la ubicación del archivo y utilizar un editor diferente para abrir el archivo y modificar el script.
    - Haga clic en **Restablecer** para restablecer el script a su configuración original.

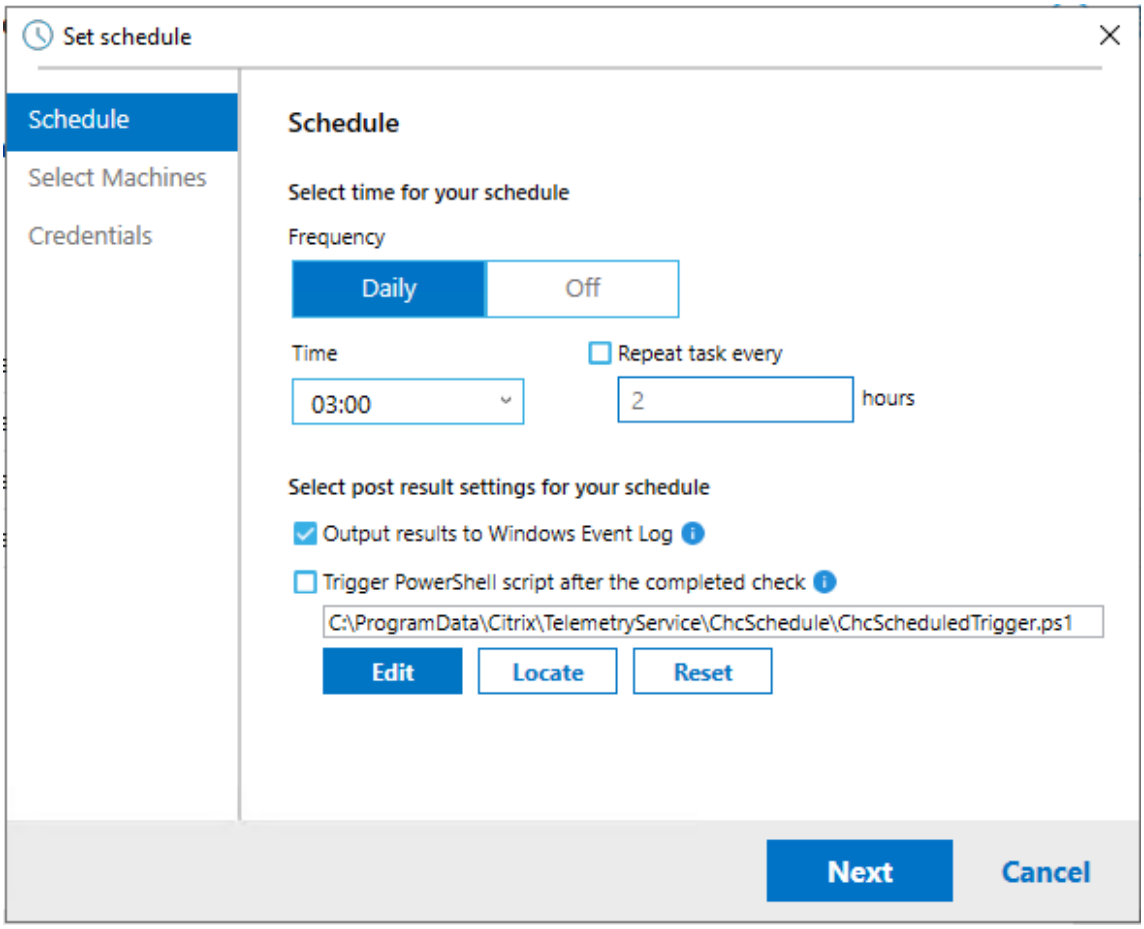
    > **Nota:**
    >
    > – No se puede cambiar el nombre y la ruta de acceso del script.
    > – Puede implementar acciones personalizadas con el script ChcScheduledTrigger.ps1, como enviar un correo electrónico una vez que esté listo el informe de comprobación programada. Agregue el código siguiente al final del script.

> Personalice el código para agregar las cuentas de correo electrónico y la dirección del servidor SMTP correspondientes. Se enviará una notificación por correo electrónico mediante las credenciales de la cuenta que ejecuta la tarea programada.

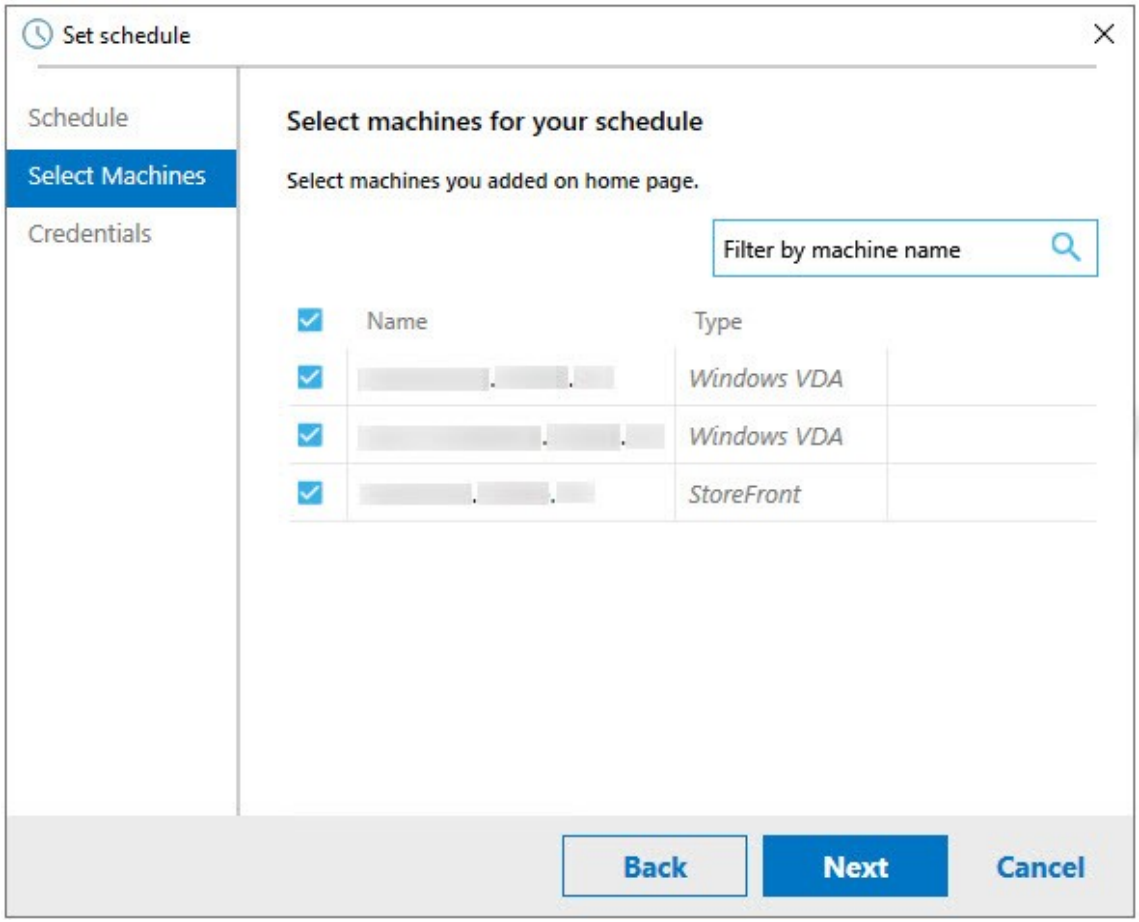
```
#Sending email example code:
$body = "CreatedTime: $($report.CreatedTime)"
$body = $body + "`nStatusCode: $($report.StatusCode)"
$body = $body + "`nMachineCount: $($report.MachineReports.Count)"
$from = "mock_email_accout"
$to = "mock_email_accout"
$smtpServer = "mock_smtp_server"

Send-MailMessage -Subject "Citrix Cloud Health Check Scheduler
    Report" -Body $body -From $from -To $to -SmtpServer $smtpServer
<!--NeedCopy-->
```



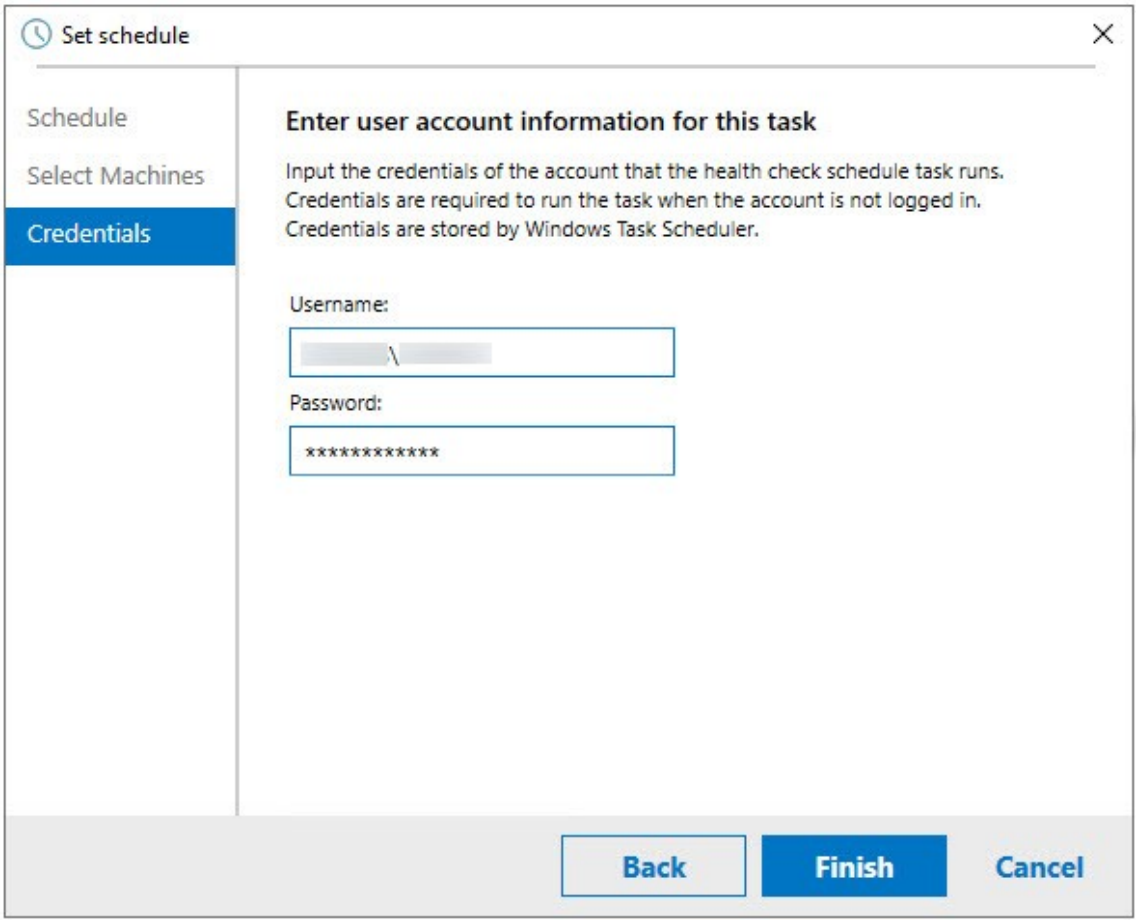

6. Seleccione las máquinas para la programación y haga clic en **Siguiente**.

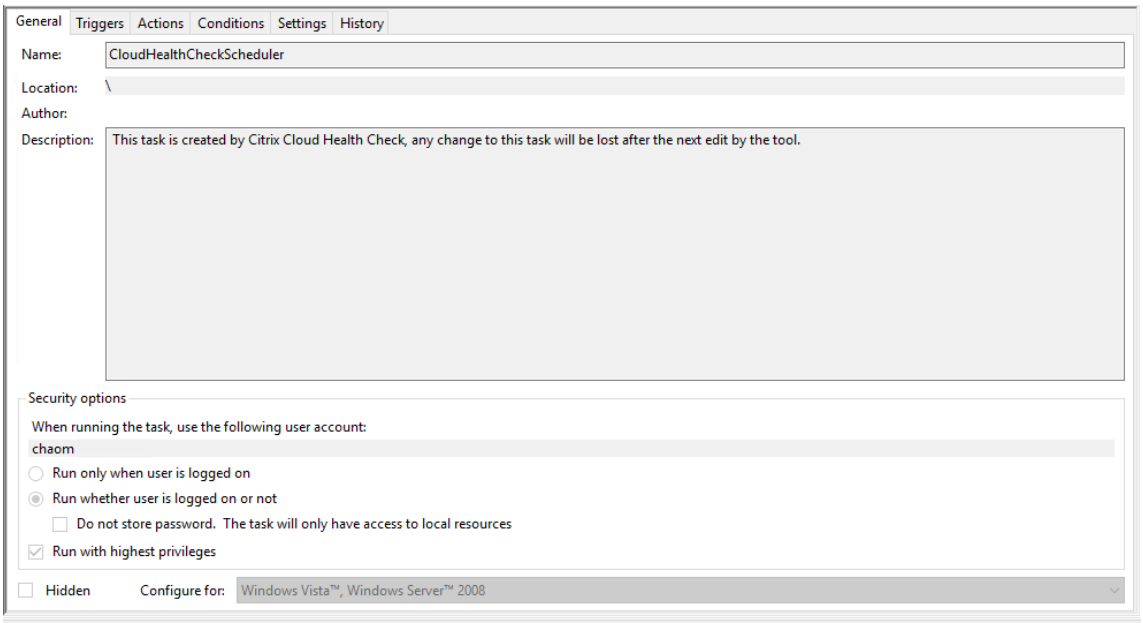



7. Introduzca las credenciales de la cuenta en la que se ejecuta la tarea y, a continuación, haga clic en **Finalizar**.



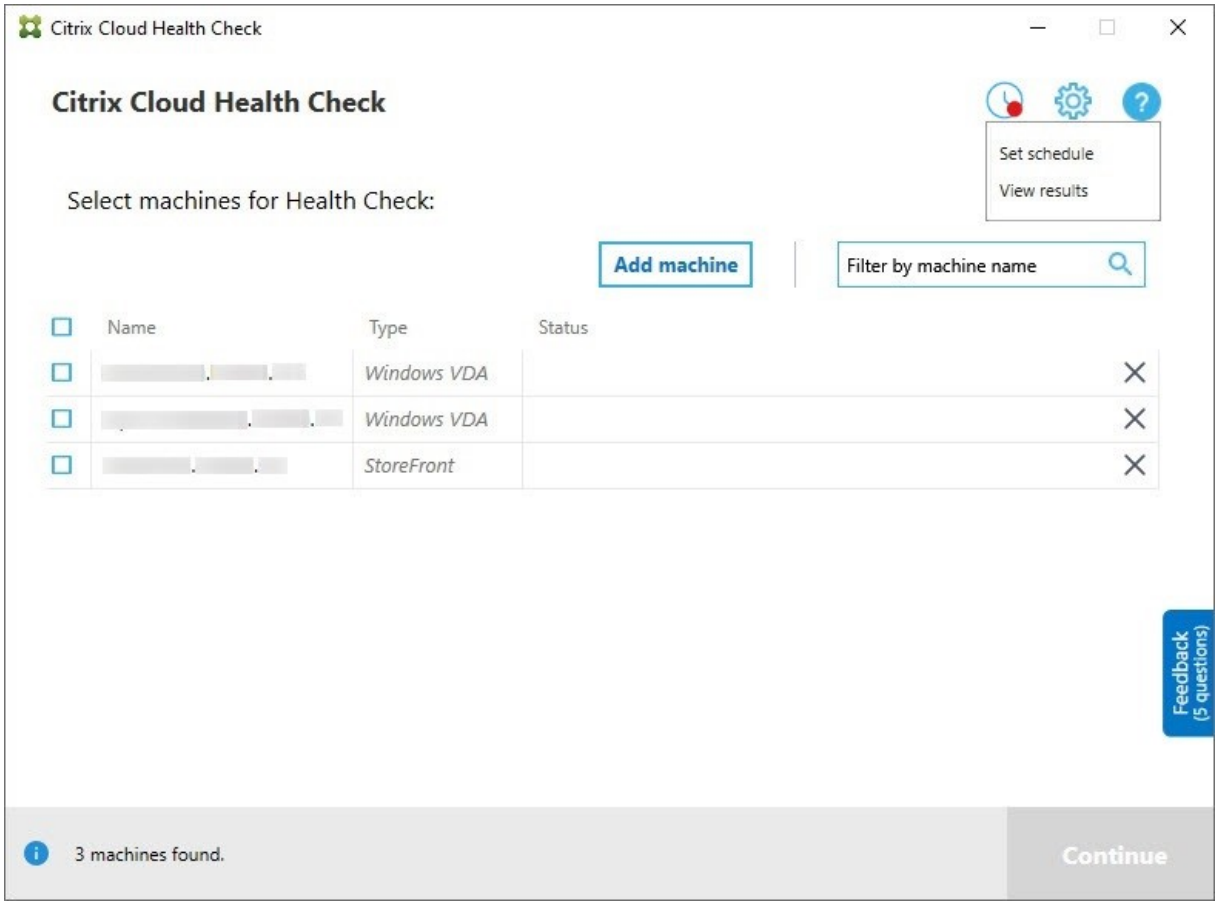

8. Se creará una tarea del programador de Comprobación de estado de Cloud en el Programador de tareas de Windows.



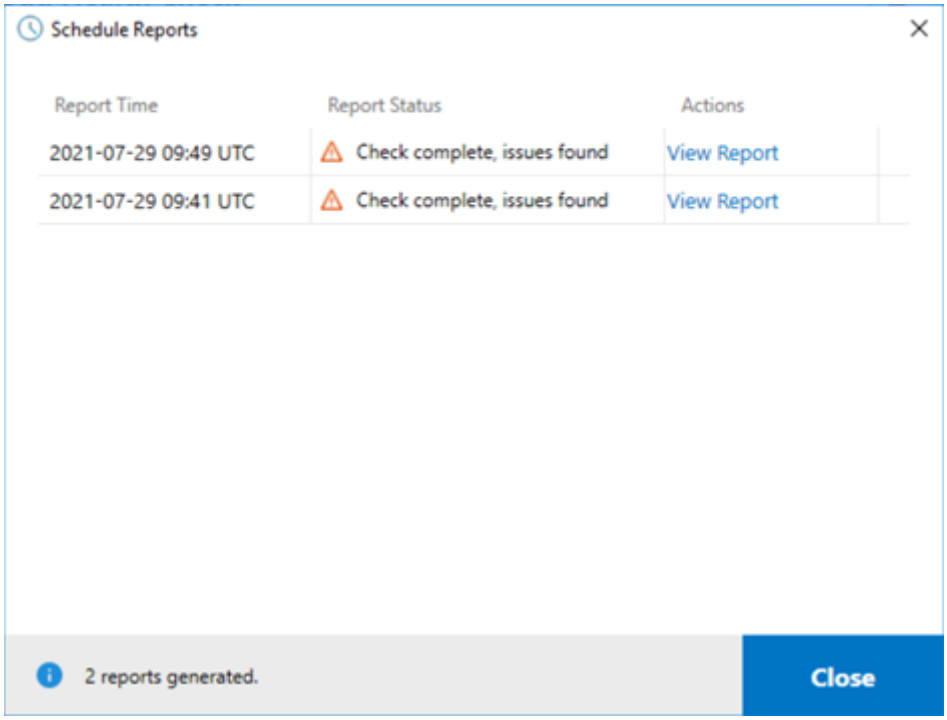
**Ver resultados de programación**

El icono del reloj con un punto rojo indica que se detectaron problemas en la última comprobación. Para ver los resultados, haga clic en el icono de reloj y, a continuación, haga clic en **Ver resultados**.

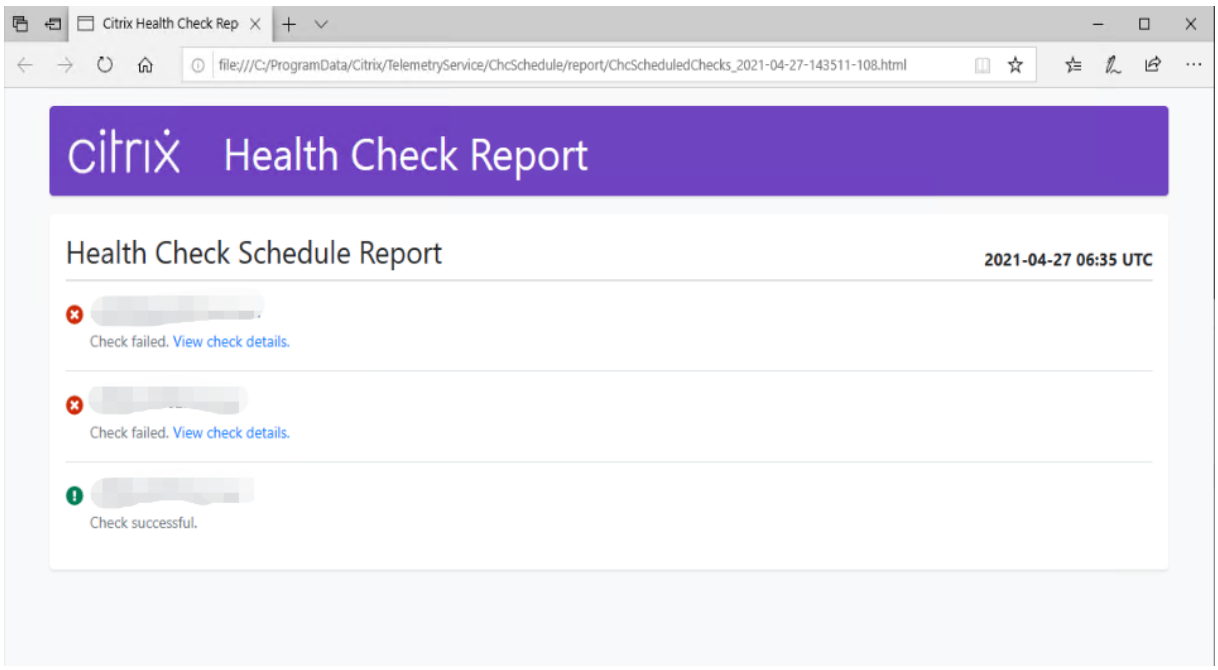



La página Informes de programaciones muestra los resultados de todas las tareas de verificación de estado programadas. Haga clic en **Ver informe** para comprobar el informe de cada programación.

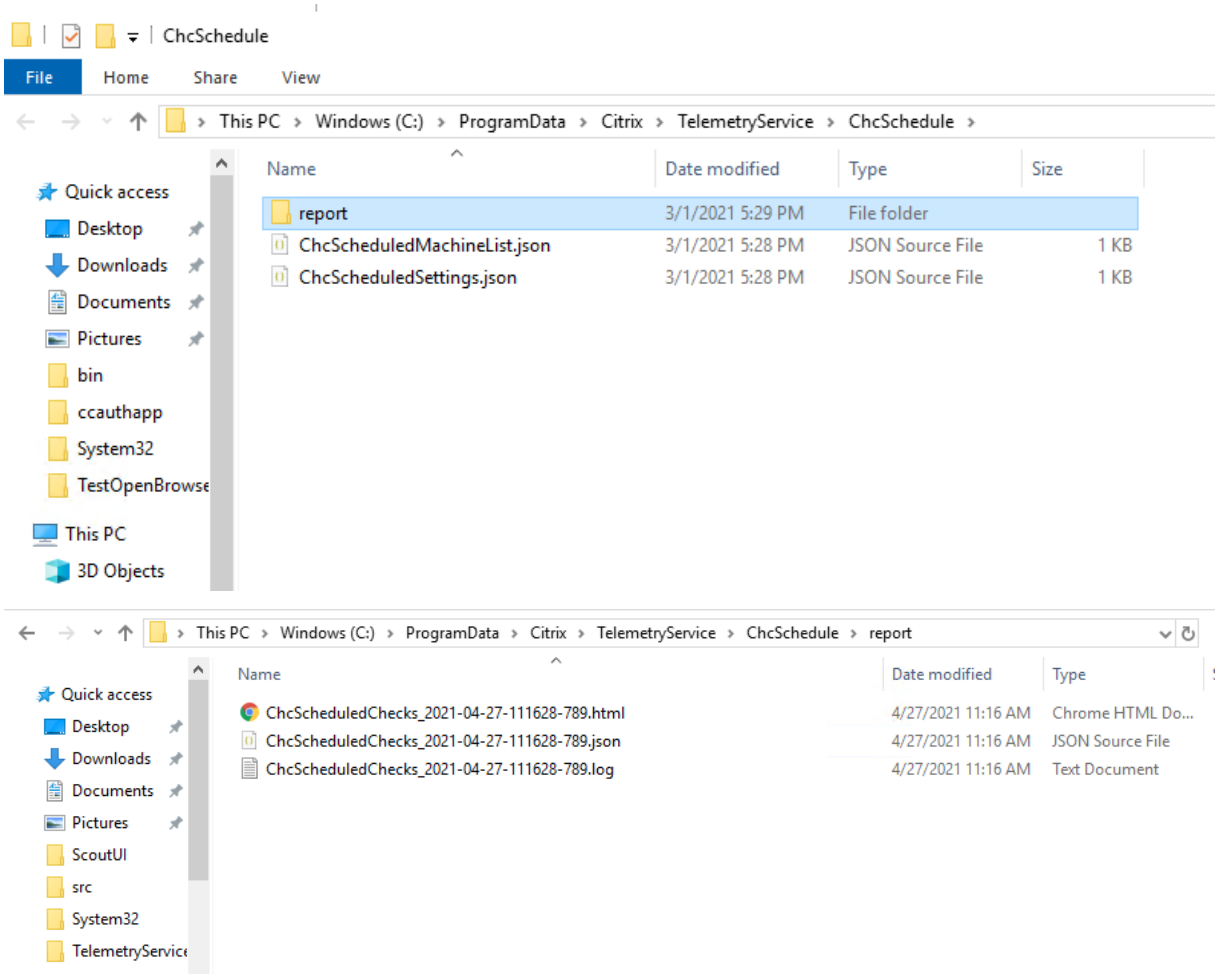



El informe HTML enumera el informe general de cada programación. A continuación, se muestra un ejemplo del informe:

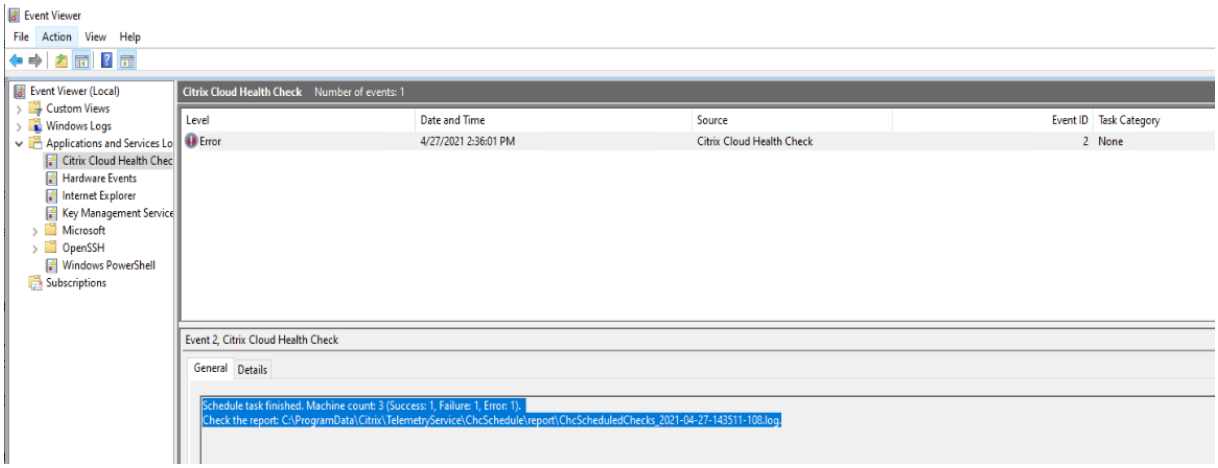



Todos los resultados de la comprobación de estado se almacenan en una carpeta llamada ChcSchedule. Comprobación de estado de Cloud crea tres archivos durante cada comprobación. Se conservan hasta 500 registros por iteración.



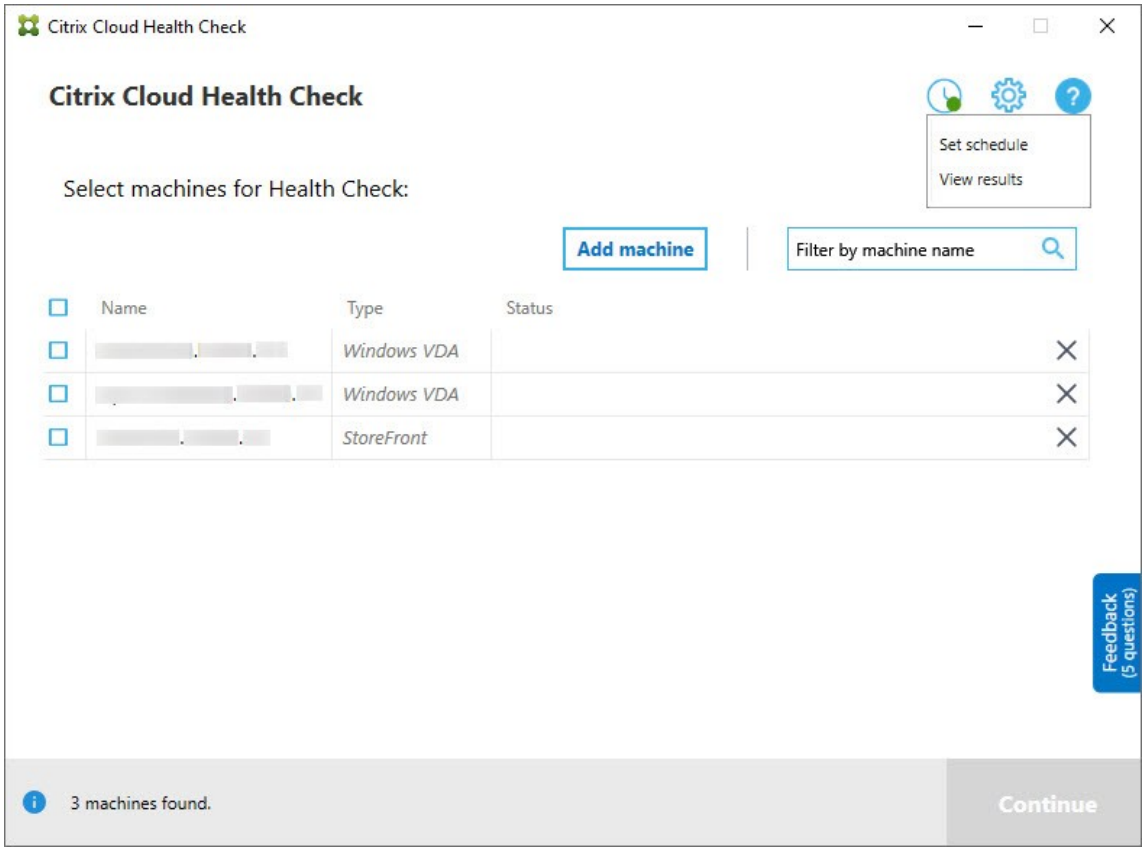

Si la casilla de verificación **Enviar resultados al registro de eventos de Windows** está activada, el resultado de la comprobación se envía al también registro de eventos de Windows.



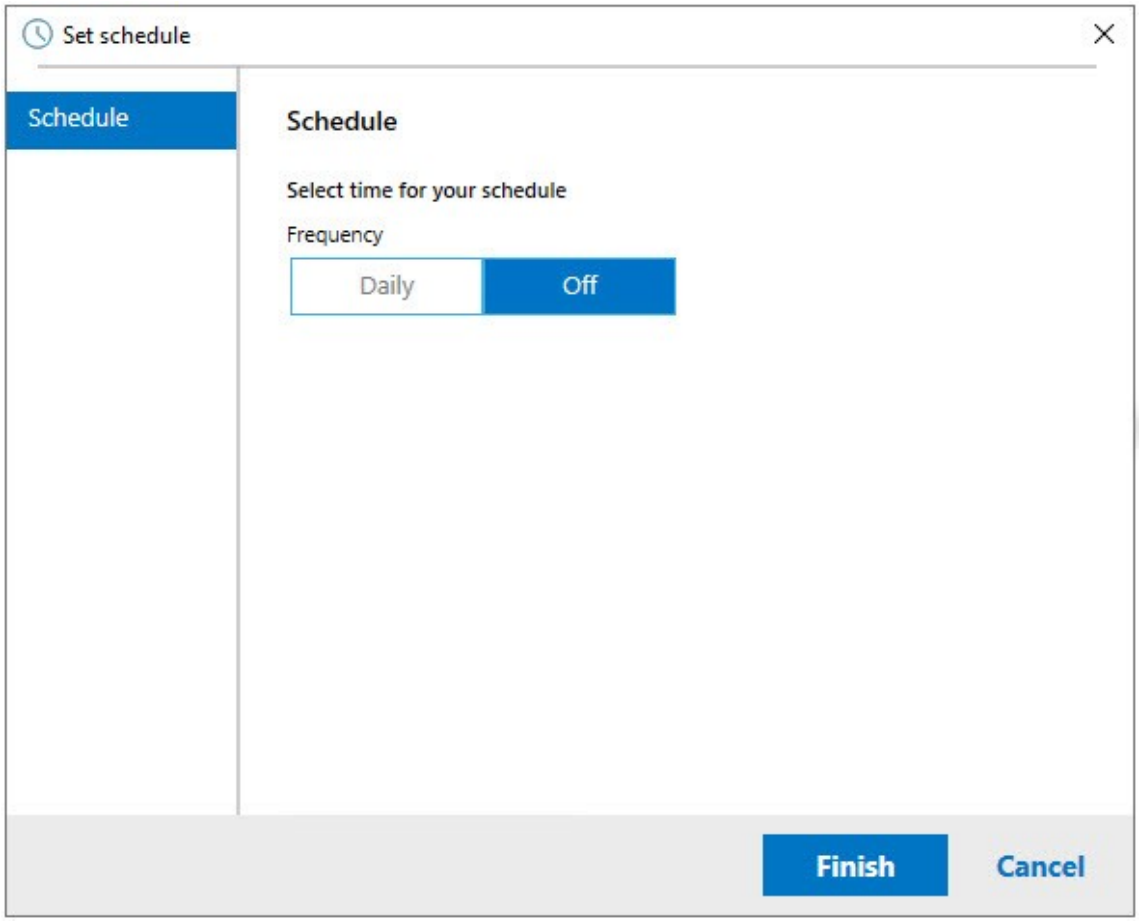
### Inhabilitar programaciones

1. Haga clic en el icono del reloj y, a continuación, en **Establecer programación**.




2. **Desactive** la opción y, a continuación, en **Finalizar** para inhabilitar el programador.




**Más información**

- Primero debe agregar o importar agentes VDA a Comprobación de estado de Cloud. Para obtener más información, consulte Importar máquinas VDA.
- El programador de Comprobación de estado de Cloud solo puede programar una tarea simultáneamente en un equipo unido a un dominio. Si establece la programación varias veces, solo tendrá efecto la última.

## Pruebas de verificación

Antes del inicio de una comprobación de estado, se ejecutan automáticamente pruebas de verificación en cada máquina seleccionada. Estas pruebas tienen por finalidad comprobar que se cumplen los requisitos para la comprobación de estado. Si la prueba de una máquina falla, Comprobación de estado de Cloud muestra un mensaje en el que sugiere acciones correctivas.

- **Comprobación de estado de Cloud no puede acceder a esta máquina**: Compruebe que:
  - La máquina está encendida.

  - La conexión de red funciona correctamente (es posible que esto implique verificar que el firewall está configurado correctamente).
  - Se pueden compartir archivos e impresoras. Consulte la documentación de Microsoft para obtener instrucciones.

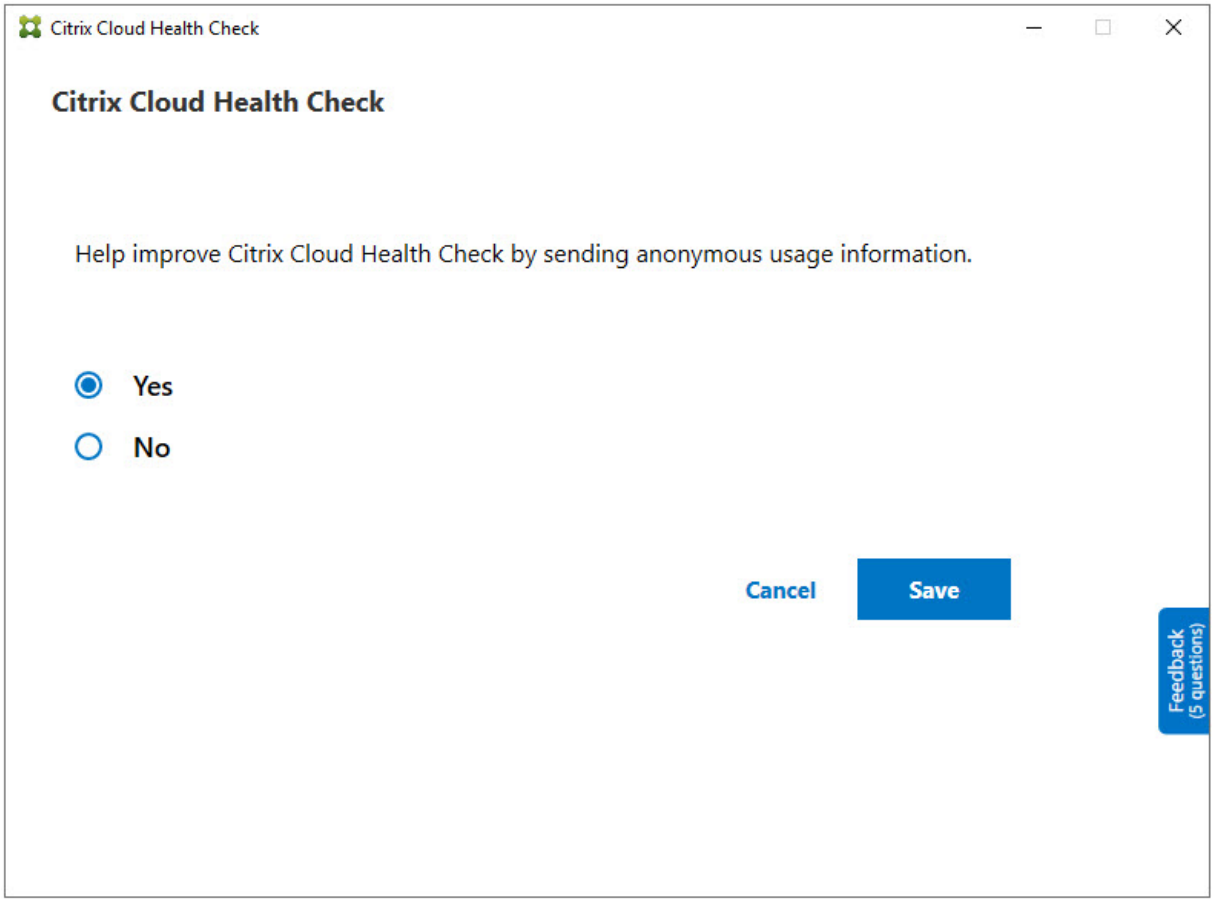
- **Habilitar PSRemoting y WinRM**: Puede habilitar la comunicación remota de PowerShell y WinRM ejecutando PowerShell como administrador y, a continuación, ejecutando el cmdlet Enable-PSRemoting. Para obtener más información, consulte la Ayuda de Microsoft para el cmdlet.
- **Comprobación de estado de Cloud requiere PowerShell 3.0 o posterior**: Instale PowerShell 3.0 o una versión posterior en la máquina y, a continuación, habilite la comunicación remota de PowerShell.
- **WMI no se está ejecutando en la máquina**: Compruebe que el acceso del Instrumental de administración de Windows (WMI) está habilitado.
- **Conexiones de WMI bloqueadas**: Habilite WMI en el servicio Firewall de Windows.

### Recopilación de datos de uso

Al utilizar Comprobación de estado de Cloud, Citrix emplea Google Analytics para recopilar datos de uso anónimos que se usarán para futuras funciones y mejoras del producto. La recopilación de datos se habilita de forma predeterminada.

Para cambiar la recopilación y carga de datos de uso, haga clic en el icono con forma de engranaje **Parámetros** en la interfaz de usuario de Comprobación de estado de Cloud. A continuación, puede elegir si enviar la información. Para ello, seleccione **Sí** o **No** y, a continuación, haga clic en **Guardar**.




## Corrección automática

La corrección automática permite que Comprobación de estado de Cloud detecte y corrija automáticamente ciertos problemas cambiando la configuración o reiniciando los servicios.

La corrección automática comprueba los siguientes elementos de registro de VDA, con las correcciones recomendadas:

- Pertenencia al dominio de máquinas en el VDA
  - Corrección: Probar el canal de seguridad de la conexión con un modelo de "reparación" para corregir
- Estado de los servicios en el VDA
  - Corrección: Reiniciar el servicio BrokerAgent
- Comunicación con el Controller
  - Corrección: Reiniciar el servicio BrokerAgent
- Sincronización de tiempo con el Controller

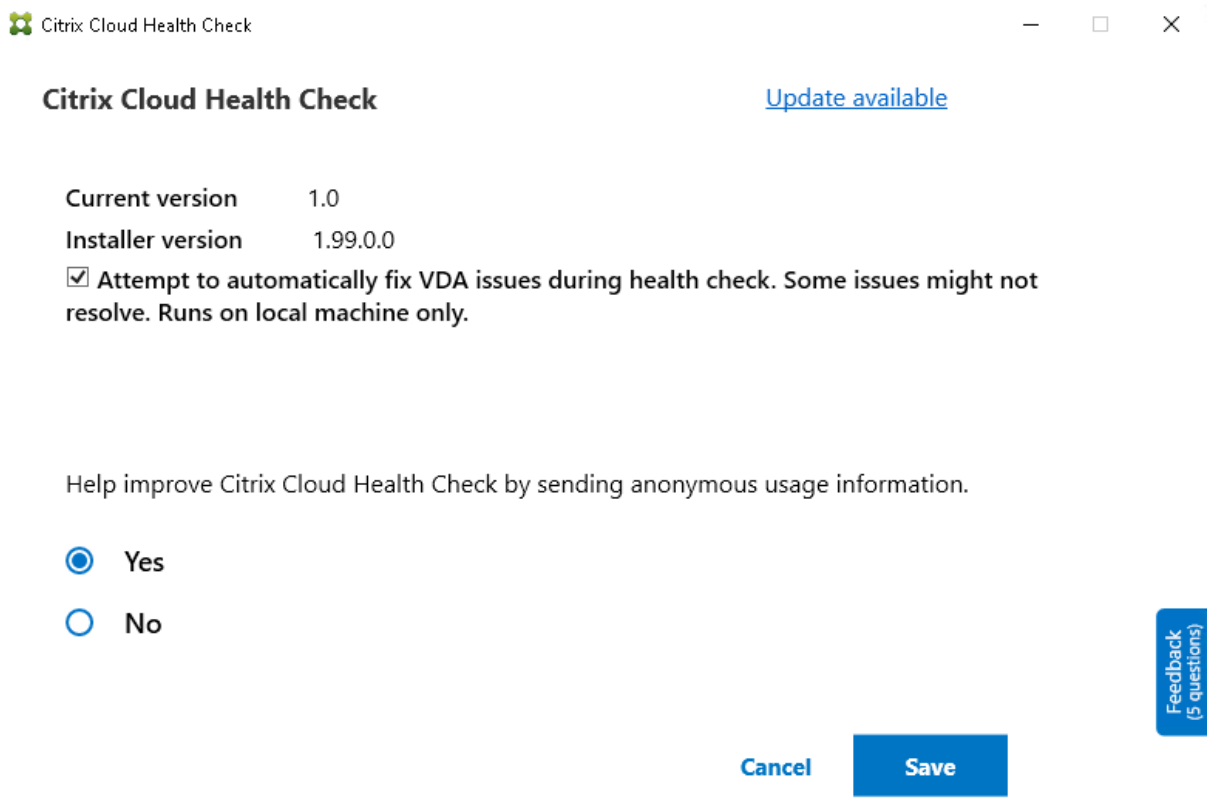
 

  - Corrección: Ejecutar el comando W32TM

Para los inicios de sesión, la corrección automática comprueba el siguiente elemento, con la corrección recomendada:

- Estado del servicio en el inicio de sesión
  - Corrección: Reiniciar el servicio BrokerAgent

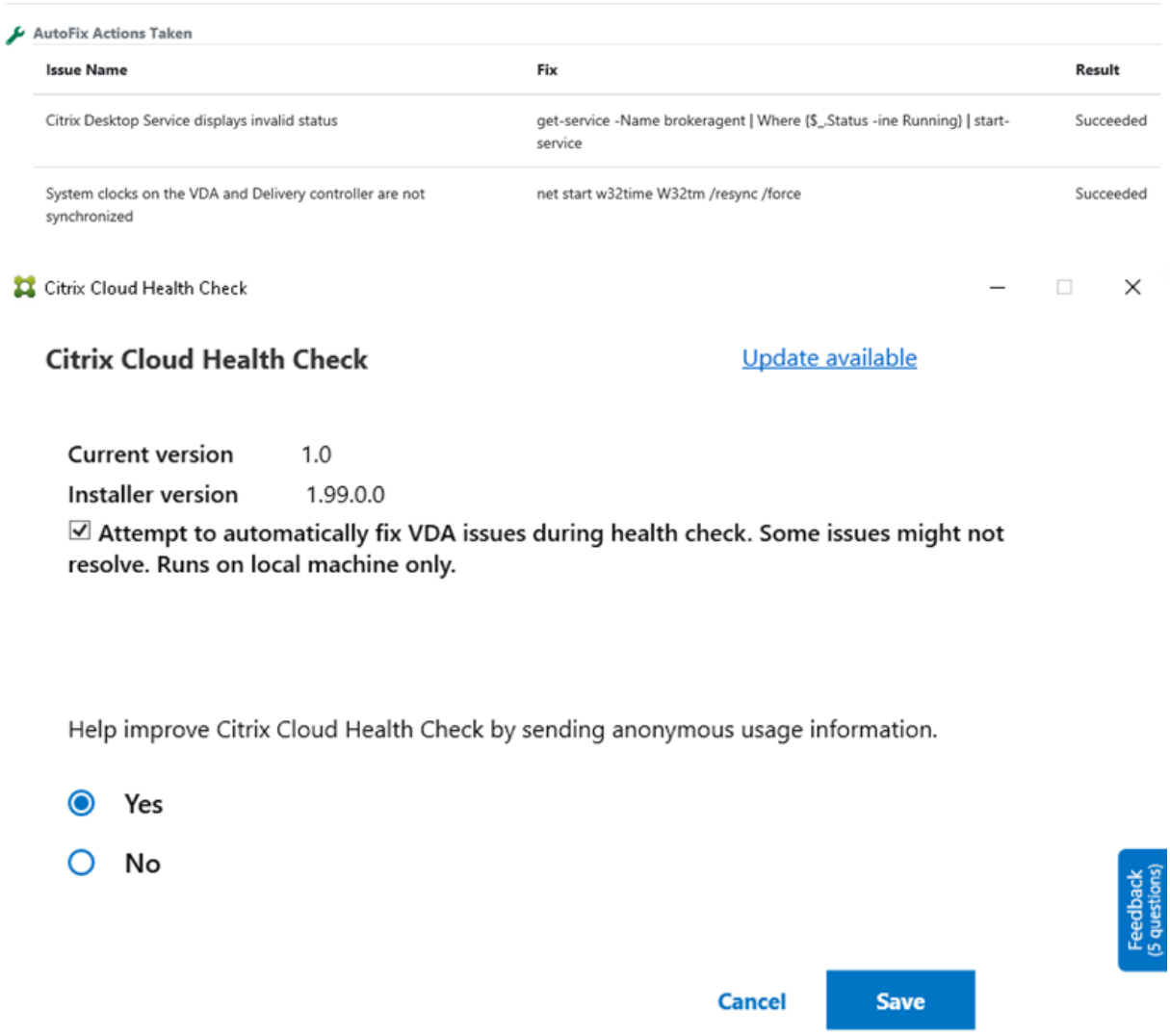
Esta función está habilitada de manera predeterminada. Para inhabilitarla, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la ventana principal de Comprobación de estado de Cloud y, a continuación, desactive **Intenta solucionar problemas de VDA automáticamente durante la comprobación de estado**.




**Informe de resultados**

Después de ejecutar la corrección automática, hay una sección en el informe de resultados de la comprobación que muestra todos los detalles:




## Solución de problemas

Cuando Comprobación de estado de Cloud no se ejecute o se produzca alguna excepción, compruebe el registro de Comprobación de estado de Cloud en `C:\ProgramData\Citrix\TelemetryService\CloudHealthCheck.log`.

El registro de Comprobación de estado de Cloud para cada máquina de destino está en `C:\ProgramData\Citrix\TelemetryService\HealthCheck\Data\$TargetMachineFQDN\log.txt`.

Para habilitar el registro de depuración:

Modifique `C:\Program Files\Citrix\CloudHealthCheck\CloudHealthCheck.exe.config`, actualice `<add name="TraceLevelSwitch"value="3"/>` to `<add name="`

`TraceLevelSwitch"value="4"/>`, guarde el archivo y vuelva a abrir Comprobación de estado de Cloud.

### Comentarios

Para dejar comentarios sobre Comprobación de estado de Cloud, rellene la encuesta de Citrix.

## Registro de configuraciones

May 17, 2024

> **Nota:**
>
> Los registros de configuración aparecen solo en inglés, independientemente del idioma que seleccione para su cuenta de Citrix Cloud. Las fechas y horas asociadas a esos registros están en formato MM/DD/AA, expresadas en tiempo universal coordinado (UTC).

La función Registros de configuración captura las actividades administrativas y los cambios de configuración realizados en la implementación de Citrix Virtual Apps and Desktops y Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service), y los vuelca en una base de datos de registros en Citrix Cloud. Puede usar el contenido registrado para:

- Diagnosticar y solucionar problemas tras haberse realizado cambios de configuración. El registro proporciona un rastro de los pasos seguidos.
- Ayudar en la administración de cambios y en el seguimiento de las configuraciones.
- Realizar informes sobre las actividades administrativas.

En esta instancia de Citrix DaaS, el registro de configuración siempre está habilitado. No se puede inhabilitar.

Desde la interfaz de administración de Configuración completa, puede ver el contenido de los registros de configuración, filtrado por intervalos de fechas o por búsquedas de texto completo. También puede generar un informe CSV mediante PowerShell. Desde esta consola, no se puede modificar ni eliminar el contenido del registro. Puede usar el SDK de PowerShell remoto para programar la eliminación periódica de datos del registro.

### Actualización de la retención de registros de configuración de DaaS

Para mantener el rendimiento de los arrendatarios de DaaS, a partir del 9 de septiembre de 2024, la retención de los registros de configuración se establecerá en 180 días.

Los registros que tengan más de 180 días a partir del 9 de septiembre de 2024, se eliminarán. A medida que aumentamos nuestros límites de DaaS para un único arrendatario de DaaS, esta implementación garantiza el mejor rendimiento y resiliencia para nuestros clientes.

Como práctica recomendada, aconsejamos a los clientes que cuenten con un mecanismo de exportación trimestral. Esto se puede hacer mediante PowerShell; consulte Generar informes. También recomendamos a los clientes programar la eliminación periódica de datos; consulte Programar la eliminación periódica de datos.

Permisos requeridos (consulte Administración delegada):

- Los administradores totales en Citrix Cloud, los administradores de Cloud de Citrix DaaS, así como los administradores de solo lectura pueden ver los registros de configuración en la consola **Administrar**.
- Los administradores totales y los administradores de Cloud también pueden descargar un informe CSV de la actividad de inicios de sesión mediante PowerShell.

### Qué se registra

Las siguientes operaciones se registran:

- Cambios de configuración y actividades administrativas iniciados desde las fichas **Administrar** y **Supervisar**
- Scripts de PowerShell
- Solicitudes de API de REST

> **Nota:**
>
> No se pueden ver las entradas de registro para las operaciones internas de la plataforma Citrix Cloud, como la configuración o la administración de la base de datos.

Los ejemplos de cambios de configuración registrados incluyen trabajar con (crear, modificar, eliminar y asignar):

- Catálogos de máquinas
- Grupos de entrega (incluido cambiar la configuración de la administración de energía)
- Roles y ámbitos de administrador
- Recursos y conexiones de host
- Directivas de Citrix disponibles desde la consola **Administrar**

Algunos ejemplos de actividades de tipo administrativo que se registran:

- Administrar energía de una máquina virtual o un escritorio de usuario
- Administrar o supervisar funciones enviando un mensaje a un usuario

Las siguientes operaciones no se registran. (Muchas de ellas no están disponibles para los administradores de clientes.)

- Operaciones automáticas, como el encendido de máquinas virtuales mediante la administración de agrupaciones.
- Acciones de directivas, implementadas mediante la Consola de administración de directivas de grupo (GPMC). Puede utilizar herramientas de Microsoft para ver los registros de estas acciones.
- Los cambios realizados a través del Registro u otros orígenes distintos de la interfaz de administración de Configuración completa, Supervisar o PowerShell.

### Ver contenido de los registros de configuración

Para ver el contenido de los registros de configuración, siga estos pasos:

1. Inicie sesión en Citrix Cloud. Seleccione **Mis servicios > DaaS** en el menú superior de la izquierda.
2. En **Administrar > Configuración completa**, seleccione **Registros > Eventos** en el panel de la izquierda.

De forma predeterminada, la pantalla en el panel central muestra el contenido de las entradas de los registros por orden cronológico (primero las entradas más recientes), separadas por su fecha. Puede hacer lo siguiente:

- Ordenar los elementos en pantalla por el encabezado de la columna.
- Filtrar los elementos en pantalla mediante un intervalo de un día o un periodo de tiempo personalizado, o bien introduciendo texto en el cuadro Buscar. Para volver a la versión estándar después de utilizar la búsqueda, borre el texto del cuadro Buscar.
- Elija qué columnas aparecerán en la pantalla. Para ello, seleccione el icono **Columnas que mostrar** en la esquina superior derecha de la tabla. Por ejemplo, para ver la dirección IP que usa el administrador para acceder a DaaS, haga clic en el icono y agregue la columna **IP de cliente**.

Características que se muestran:

- Las operaciones de alto nivel creadas durante la administración y la supervisión se indican en el panel central superior. Una operación de alto nivel tiene como resultado la llamada a uno o varios servicios y SDK de PowerShell, que son operaciones de bajo nivel. Cuando se selecciona una operación de alto nivel en el panel central superior, el panel inferior muestra las operaciones de bajo nivel.
- Si se crea una operación de bajo nivel en PowerShell sin especificar su correspondiente operación de alto nivel, la función de registros de configuración crea una operación de alto nivel suplente.

- Si la operación falla antes de completarse, la operación de registro puede no completarse en la base de datos. Por ejemplo, puede que una entrada inicial no tenga una entrada final. En estos casos, el registro indica que hay información que falta. Cuando se muestran registros correspondientes a intervalos de tiempo, los registros incompletos se muestran si los datos cumplen los requisitos. Por ejemplo, si se solicitan los registros de los últimos cinco días y hay un registro con una hora de inicio dentro de esos cinco días, pero no tiene hora de fin, se incluirá de todos modos.
- Recuerde: No se pueden ver las entradas de registro para las operaciones internas de la plataforma Citrix Cloud, como la configuración o la administración de la base de datos.

### Ver tareas relacionadas con las operaciones del catálogo de máquinas

Para ver las tareas relacionadas con las operaciones del catálogo de máquinas, vaya a **Administrar > Configuración completa > Registros > Tareas**. La ficha **Tareas** muestra solo las tareas relacionadas con catálogos creados a través de Machine Creation Services (MCS) o Provisioning Services (PVS). Específicamente, aparecen las tareas asociadas a las siguientes operaciones del catálogo de máquinas:

- Crear catálogos
- Clonar catálogos
- Agregar máquinas
- Quitar máquinas
- Actualizar un catálogo (actualización de imágenes o máquinas)
- Revertir actualizaciones de máquinas

> **Sugerencia:**
>
> La ficha **Tareas** muestra solo las tareas relacionadas con los cambios en el esquema de aprovisionamiento (creación o modificación de un esquema de aprovisionamiento).

Una tarea puede estar en el siguiente estado:

- Completado
- No iniciado
- En ejecución
- Cancelado
- Error
- Desconocido

Para cancelar una tarea en ejecución, selecciónela y, a continuación, haga clic en **Cancelar**. La cancelación tarda algún tiempo en completarse.

Algunos ejemplos de tareas registradas incluyen:

- Actualización de imagen completada para un determinado catálogo
- Error al actualizar la imagen de un catálogo determinado
- Actualización de imagen cancelada para un determinado catálogo
- Aprovisionamiento de máquinas virtuales en un catálogo determinado
- Eliminación de máquinas virtuales de un catálogo determinado
- Creación de un catálogo determinado

De forma predeterminada, la pantalla en el panel central muestra las tareas registradas por orden cronológico (primero las entradas más recientes), separadas por fecha. Puede ordenar los elementos en pantalla por el encabezado de la columna. Para borrar las tareas completadas, haga clic en **Borrar tareas completadas** en la ficha **Tareas**. Para elegir qué columnas se mostrarán en la pantalla, seleccione el icono **Columnas que mostrar** en la esquina superior derecha de la tabla.

### Ver registros de API

Para ver los registros de la API de REST, vaya a **Administrar > Configuración completa > Registros > API**. La ficha **API** muestra las solicitudes de API de REST realizadas durante un período de tiempo determinado.

Tenga en cuenta las siguientes consideraciones:

- Los registros de API de REST se borran después de cerrar sesión en la consola. (También se borran si actualiza la ventana del explorador web).
- Para las operaciones de la consola que resulten en llamadas de API, se mostrarán sus solicitudes de API correspondientes en la ficha **API**.
- La pantalla muestra las solicitudes de API por orden cronológico (primero las entradas más recientes), separadas por fecha. La cantidad máxima de solicitudes de API en pantalla es 1000.

### Ver los registros de PowerShell

Para ver los comandos de PowerShell correspondientes a acciones de interfaz de usuario que ha realizado durante el día, vaya a la ficha **Administrar > Configuración completa > Registros > PowerShell**.

### Asociar metadatos a registros de configuración

Puede adjuntar metadatos a los registros de configuración asociando un par `name-value` llamado `MetadataMap` a los registros de registro.

> **Nota:**
>
> - Solo puede adjuntar metadatos a objetos de operaciones de alto nivel.
> - Los metadatos se asocian a los registros existentes en el momento de la ejecución.

#### Establecer los metadatos

Ejecute el comando `Set-LogHighLevelOperationMetadata` de PowerShell para asociar un registro a `MetadataMap`.
`Set-LogHighLevelOperationMetadata` toma los siguientes parámetros:

- **Id**: ID de la operación de alto nivel.
- **InputObject**: Las operaciones de alto nivel a las que se agregan los metadatos. Esta es una alternativa al parámetro `Id`, en el que se pasa un objeto de operación de alto nivel o una lista de objetos al comando de PowerShell.
- **Name**: Nombre de la propiedad de los metadatos por agregar. La propiedad debe ser única para la operación de alto nivel especificada. La propiedad no puede contener ninguno de los siguientes caracteres:
  `()\/;:#.*?=<>|[]"'`
- **Value**: Valor de la propiedad.
- **Mapa**: Diccionario de pares (nombre, valor) para las propiedades. Esta es una alternativa a configurar los metadatos mediante los parámetros `-Name` y `-Value`.

Por ejemplo, para adjuntar los metadatos a todos los registros de registro de alto nivel con el ID 40, ejecute el siguiente comando de PowerShell:

```
Get-LogHighLevelOperation – Id 40 | Set-LogHighLevelOperationMetadata
 -Name A -Value B
```

Para adjuntar los metadatos al registro de alto nivel con el usuario `abc@example.com`, ejecute el siguiente comando de PowerShell:

```
Get-LogHighLevelOperation – User `abc@example.com` | Set-LogHighLevelOperation
 -Name C -Value D
```

#### Obtención con los metadatos

Ejecute los siguientes comandos de PowerShell para usar los metadatos asociados para obtener los registros:

- Búsqueda por clave y valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:Value"
  ```

- Búsqueda por valor y cualquier clave:

  ```
  Get-LogHighLevelOperation -Metadata "*:Value"
  ```

- Búsqueda por clave y cualquier valor:

  ```
  Get-LogHighLevelOperation -Metadata "Key:*"
  ```

#### Quitar los metadatos

Ejecute el comando `Remove-LogHighLevelOperationMetadata` de PowerShell para quitar los metadatos asociados.
`Remove-LogHighLevelOperationMetadata` toma los siguientes parámetros:

- **Id**: ID de la operación de alto nivel.
- **InputObject**: Las operaciones de alto nivel a las que se agregan los metadatos. Esta es una alternativa al parámetro `Id`‘, en el que se pasa un objeto de operación de alto nivel o una lista de objetos al comando de PowerShell.
- **Name**: Nombre de la propiedad de los metadatos por quitar. Establézcalo en $null para quitar todos los metadatos del objeto especificado.
- **Mapa**: Diccionario de pares (nombre, valor) para las propiedades. Puede ser una tabla hash (creada con @{“nombre1”= “val1”; “nombre2”= “val2”}) o un diccionario de cadenas (creado con el nuevo objeto “System.Collections.Generic.Dictionary[Cadena, Cadena]”). Se quitan las propiedades cuyos nombres coinciden con las claves del mapa.

### Generar informes

Para generar un informe CSV o HTML que contenga los datos de los registros de configuración, use los cmdlets de PowerShell para ConfigLogging Service en el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops. Para obtener más detalles, consulte:

- `Export-LogReportCsv`
- `Export-LogReportHtml`

### Programar la eliminación periódica de datos

Use el SDK de PowerShell remoto para especificar cuánto tiempo se conservan los datos en la base de datos de registros de configuración (esta función no está disponible en la consola de administración de Configuración completa). En Citrix DaaS, debe tener acceso total.

En el cmdlet `Set-LogSite`, el parámetro `-LoggingDBPurgeDurationDays` especifica cuántos días se conservan los datos de la base de datos de registros de configuración antes de eliminarlos automáticamente.

- De forma predeterminada, el valor de este parámetro es 0. El valor cero significa que los datos de la base de datos de registros de configuración nunca se eliminan automáticamente.
- Cuando se establece un valor distinto de cero, la base de datos se comprueba una vez cada 120 minutos. Se eliminan los datos anteriores al período de retención.

Utilice `Get-LogSite` para ver el valor actual del parámetro.

### Diferencias de Citrix Virtual Apps and Desktops local

Si conoce la función de registros de configuración en el producto local de Citrix Virtual Apps and Desktops, la versión de Citrix Cloud presenta varias diferencias. En Citrix Cloud:

- La función de registros de configuración siempre está habilitada. No se puede inhabilitar. El registro obligatorio no está disponible.
- No se puede cambiar la ubicación de la base de datos de registros de configuración, ya que esa base de datos se administra en la plataforma de Citrix Cloud.
- En Registros de configuración no se incluyen operaciones ni actividades que se realizan dentro de la plataforma Citrix Cloud.
- PowerShell es la única opción para crear un informe en formato CSV o HTML de las operaciones registradas. En el producto local, se pueden generar informes desde Citrix Studio o PowerShell.
- No se puede eliminar el contenido de los registros de configuración.

## Administración delegada

March 30, 2024

### Información general

Con la administración delegada de Citrix Cloud, puede configurar los permisos de acceso que todos sus administradores necesitarán en función del rol que desempeñan en la organización.

De forma predeterminada, los administradores tienen acceso total. Con lo que se permite el acceso a todas las funciones de administración y gestión de clientes que haya disponibles en Citrix Cloud, además de todos los servicios suscritos. Para adaptar el acceso de un administrador:

- Configure un acceso personalizado a los permisos de administración generales de un administrador en Citrix Cloud.

- Configure un acceso personalizado a los servicios suscritos. En Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service), puede configurar un acceso personalizado cuando invite a un nuevo administrador. Puede cambiar más tarde el acceso de un administrador.

Para obtener información sobre cómo ver la lista de administradores y definir los permisos de acceso, consulte Administrar el acceso de administrador a Citrix Cloud.

En este artículo se describe cómo configurar el acceso personalizado en Citrix DaaS.

## Administradores, roles y ámbitos

En la administración delegada se utilizan tres conceptos para el acceso personalizado: los administradores, los roles y los ámbitos.

- **Administradores:** Un administrador representa a una persona identificada por su inicio de sesión en Citrix Cloud, que generalmente es una dirección de correo electrónico. Cada administrador está asociado a uno o varios pares de rol y ámbito.
- **Roles:** Un rol representa una función de trabajo a la que se han asociado permisos. Estos permisos autorizan ciertas tareas que son exclusivas de Citrix DaaS. Por ejemplo, el rol de administrador de grupos de entrega tiene permiso para crear un grupo de entrega o eliminar un escritorio que hubiera en un grupo de entrega, además de otros permisos asociados. Un administrador puede tener varios roles. Un administrador puede ser un administrador de grupo de entrega y un administrador de catálogo de máquinas.

  Citrix DaaS ofrece varios roles de acceso integrados y personalizados. No puede cambiar los permisos en esos roles integrados, ni tampoco eliminar esos roles.

  Se pueden crear roles de acceso personalizados para satisfacer las exigencias de la empresa y delegar permisos con mayor flexibilidad. Utilice los roles personalizados para asignar permisos a la granularidad de una acción o tarea. Solo puede eliminar un rol personalizado si no está asignado a un administrador.

  En cambio, sí puede cambiar los roles que tiene un administrador.

  Un rol siempre está emparejado con un ámbito.
- **Ámbitos:** Un ámbito representa una colección de objetos. Los ámbitos se utilizan para agrupar objetos de una manera que sea relevante para la organización. Los objetos pueden estar en más de un ámbito.

  Hay un ámbito integrado: "Todo", que contiene todos los objetos. A los administradores de Citrix Cloud y asistencia técnica siempre se les empareja con el ámbito Todo. Ese ámbito no se puede cambiar para esos administradores.

Cuando invita (agrega) un administrador a este servicio, un rol siempre se empareja con un ámbito (de forma predeterminada, el ámbito Todo).

Puede crear y eliminar ámbitos en la interfaz **Administrar > Configuración completa**. En cambio, los pares de rol y ámbito se asignan desde la consola de Citrix Cloud.

El ámbito no se muestra a los administradores de acceso total. Por definición, esos administradores pueden acceder a todos los objetos de Citrix Cloud y servicios suscritos que gestione el cliente.

### Roles y ámbitos integrados

Citrix DaaS dispone de los siguientes roles integrados.

- **Administrador de Cloud:** Puede realizar todas las tareas que se pueden iniciar desde Citrix DaaS.

  Puede ver las fichas **Administrar** y **Supervisar** en la consola. Este rol siempre se combina con el ámbito Todo. El ámbito no se puede cambiar.

  No se deje engañar por el nombre de este rol. Un administrador de Cloud con acceso personalizado no puede realizar tareas a nivel de Citrix Cloud (las tareas de Citrix Cloud requieren acceso total).

- **Administrador de solo lectura:** Puede ver todos los objetos en los ámbitos especificados, así como información global, pero no puede modificar nada. Por ejemplo, un administrador de solo lectura con ámbito "Londres"puede ver todos los objetos globales y todos los objetos del ámbito Londres (por ejemplo, grupos de entrega de Londres). No obstante, ese administrador no puede ver los objetos del ámbito de Nueva York (a menos que los ámbitos de Londres y Nueva York se superpongan).

  Puede ver las fichas **Administrar** y **Supervisar** en la consola.

- **Administrador de asistencia técnica:** Puede ver los grupos de entrega, y administrar las sesiones y las máquinas asociadas a dichos grupos. Puede ver el catálogo de máquinas y la información de host de los grupos de entrega que están bajo supervisión. También puede realizar tareas de administración de sesiones y de administración de energía en las máquinas de esos grupos de entrega.

  Puede ver la ficha **Supervisar** en la consola. No se puede ver la ficha **Administrar**. Este rol siempre se combina con el ámbito Todo. El ámbito no se puede cambiar.

- **Administrador de catálogo de máquinas:** Puede crear y administrar catálogos de máquinas, así como aprovisionar máquinas en ellos. Asimismo, este rol puede administrar las imágenes base e instalar software, pero no puede asignar las aplicaciones ni los escritorios a los usuarios.

Puede ver las fichas **Supervisar** y **Administrar** en la consola. No puede ver la ficha **Supervisar**. El ámbito se puede cambiar.

- **Administrador de grupo de entrega:** Puede entregar aplicaciones, escritorios y máquinas. También puede administrar las sesiones asociadas. Puede administrar las configuraciones de aplicaciones y escritorios, tales como las configuraciones de directivas y de administración de energía.

  Puede ver las fichas **Supervisar** y **Administrar** en la consola. El ámbito se puede cambiar.

  > **Nota:**
  >
  > Para cambiar el nombre simplificado de un escritorio como administrador de un grupo de entrega, necesita el permiso **Realizar actualización de la máquina**. Este permiso es necesario porque cambiar el nombre simplificado implica actualizar las propiedades de la máquina.

- **Administrador de host:** Puede administrar las conexiones de host y los parámetros de recursos que estas tengan asociados. No puede entregar máquinas, aplicaciones ni escritorios a los usuarios.

  Puede ver la ficha **Administrar** en la consola. No puede ver la ficha **Supervisar**. El ámbito se puede cambiar.

- **Administrador de sesiones:** Puede ver los grupos de entrega que se están supervisando y administrar sus sesiones y máquinas asociadas.

  Puede ver la ficha **Supervisar** en la consola. No se puede ver la ficha **Administrar**. El ámbito no se puede cambiar.

- **Administrador total:** Pueden realizar todas las tareas y operaciones. Un administrador total siempre se combina con **Todos los ámbitos**.

  Puede ver las fichas **Administrar** y **Supervisar** en la consola. Este rol siempre se combina con **Todos los ámbitos**. El ámbito no se puede cambiar.

- **Administrador total de supervisión:** Tiene acceso completo a todas las vistas y comandos de la ficha **Supervisar**.

  Puede ver la ficha **Supervisar** en la consola. No se puede ver la ficha **Administrar**. El ámbito no se puede cambiar.

- **Administrador de Probe Agent:** Tiene acceso a las API de Probe Agent.

  Puede ver las fichas **Supervisar** y **Administrar** en la consola. Tiene acceso de solo lectura a la página **Aplicaciones**, pero no puede acceder a ninguna otra vista.

En la siguiente tabla se ofrece un resumen de las fichas de consola que verá cada rol de acceso personalizado en Citrix DaaS, y se indica si el rol se puede usar con ámbitos personalizados.

| Rol de administrador de acceso personalizado | ¿Puede ver la ficha **Administrar** en la consola? | ¿Puede ver la ficha **Supervisar** en la consola? | ¿Se puede usar el rol con ámbitos personalizados? |
|---|---|---|---|
| Administrador de Cloud | Sí | Sí | No |
| Administrador de solo lectura | Sí | Sí | Sí |
| Administrador de asistencia técnica | No | Sí | No |
| Administrador de catálogos de máquinas | Sí | Sí | Sí |
| Administrador de grupos de entrega | Sí | Sí | Sí |
| Administrador de host | Sí | No | Sí |
| Administrador de sesiones | No | Sí | No |
| Administrador total | Sí | Sí | No |
| Administrador total de supervisión | No | Sí | No |
| Administrador de Probe Agent | Sí | Sí | No |

> **Nota:**
>
> Los roles de administrador con acceso personalizado (excepto Administrador de Cloud y Administrador de asistencia técnica) no están disponibles para Citrix Virtual Apps and Desktops Standard para Azure, Virtual Apps Essentials y Virtual Desktops Essentials.

Para ver los permisos asociados a un rol:

1. Inicie sesión en Citrix Cloud. Seleccione **Mis servicios > DaaS** en el menú superior de la izquierda.
2. En **Administrar > Configuración completa**, seleccione **Administradores** en el panel de la izquierda.
3. Seleccione la ficha **Roles**.
4. Seleccione un rol en el panel central superior. En la ficha **Definición de rol** situada en el panel inferior se muestra una lista de las categorías y los permisos existentes. Seleccione una categoría para ver los permisos específicos. En la ficha **Administradores** se ofrece una lista de los administradores a los que se les ha asignado el rol seleccionado.

Problema conocido: una entrada de administrador total no muestra el conjunto correcto de permisos de un administrador con acceso total a Citrix DaaS.

### Cuántos administradores se necesitan

Por lo general, la cantidad de administradores y la granularidad de sus permisos dependen del tamaño y la complejidad de la implementación.

- En implementaciones pequeñas o de prueba de concepto, un administrador o un número reducido de ellos puede hacer cualquier cosa. No hay delegación de acceso personalizada. En este caso, todos los administradores tienen acceso total, que siempre tiene el ámbito Todo.
- Las implementaciones grandes con más máquinas, aplicaciones y escritorios implican mayor delegación. Varios administradores pueden tener responsabilidades funcionales más específicas (roles). Por ejemplo, dos tienen acceso total y los demás son administradores de asistencia técnica. Asimismo, un administrador puede gestionar solamente grupos determinados de objetos (ámbitos), como los catálogos de máquinas en un departamento concreto. En este caso, cree ámbitos y administradores con los ámbitos y los roles de acceso personalizado que sean adecuados.

### Resumen de la gestión de administradores

En la configuración de administradores para Citrix DaaS se sigue esta secuencia de tareas:

1. Si quiere que el administrador tenga un rol distinto de un administrador total (que cubre todos los servicios suscritos en Citrix Cloud) o un rol integrado, cree un rol personalizado.
2. Si quiere que el administrador tenga un ámbito que no sea Todo (siempre que se permita otro ámbito para el rol en cuestión y aún no se haya creado), cree ámbitos.
3. En Citrix Cloud, invite a un administrador. Si quiere que el nuevo administrador tenga algo que no sea el acceso total predeterminado, especifique un par personalizado de rol y ámbito.

Más adelante, si quiere cambiar el acceso de un administrador (roles y ámbito), consulte Configurar acceso personalizado.

### Agregar un administrador

Para agregar (invitar) administradores, siga las instrucciones de Agregar administradores a una cuenta de Citrix Cloud. Un subconjunto de esa información se repite aquí.

> **Importante:**
>
> No confunda los conceptos "personalizado"y "acceso personalizado".
>
> - Al crear administradores y asignar roles para Citrix DaaS en la consola de Citrix Cloud, el término "acceso personalizado"incluye tanto los roles integrados como cualquier otro rol personalizado que se haya creado en la interfaz de **Administrar > Configuración completa** del servicio.
> - En la interfaz **Administrar > Configuración completa** del servicio, "personalizado"simplemente diferencia ese rol de un rol integrado.

El flujo de trabajo general para agregar administradores es el siguiente:

1. Inicie sesión en Citrix Cloud y, a continuación, seleccione **Administración de acceso e identidad** en el menú superior de la izquierda.
2. En la página **Administración de acceso e identidad**, seleccione **Administradores**. La ficha **Administradores** enumera todos los administradores actuales de la cuenta.
3. En la ficha **Administradores**, seleccione el tipo de identidad, introduzca la dirección de correo electrónico del administrador y, a continuación, haga clic en **Invitar**.

- Seleccione **Acceso completo** si desea que el administrador tenga pleno acceso. De esa manera, el administrador puede acceder a todas las funciones de administrador de clientes en Citrix Cloud y en todos los servicios suscritos.
- Seleccione **Acceso personalizado** si quiere que el administrador tenga acceso limitado. A continuación, puede seleccionar un par de rol de acceso y ámbito personalizado. De ese modo, el administrador tendrá los permisos previstos al iniciar sesión en Citrix Cloud.

1. Haga clic en **Enviar invitación**. Citrix Cloud envía una invitación a la dirección de correo electrónico y agrega al administrador a la lista una vez que este completa la incorporación.

Al recibir el mensaje de correo electrónico, el administrador tiene que hacer clic en el enlace **Iniciar sesión** para aceptar la invitación.

Para obtener más información sobre cómo agregar administradores, consulte Administrar administradores de Citrix Cloud.

También puede ir a **Administrar > Configuración completa > Administradores > Administradores** y hacer clic en **Agregar administrador**. Pasará directamente a **Administración de acceso e identidad > Administradores**, que se abre en una nueva ficha de explorador. Cuando haya terminado de agregar administradores, cierre la ficha y vuelva a la consola para continuar con las demás tareas de configuración.

### Crear y gestionar roles

Cuando los administradores crean o modifican un rol, solo pueden habilitar los permisos que ellos mismos tienen. Este control impide que los administradores creen un rol con más permisos de los que tienen actualmente y luego se lo asignen a sí mismos (o modifiquen un rol que ya tienen asignado).

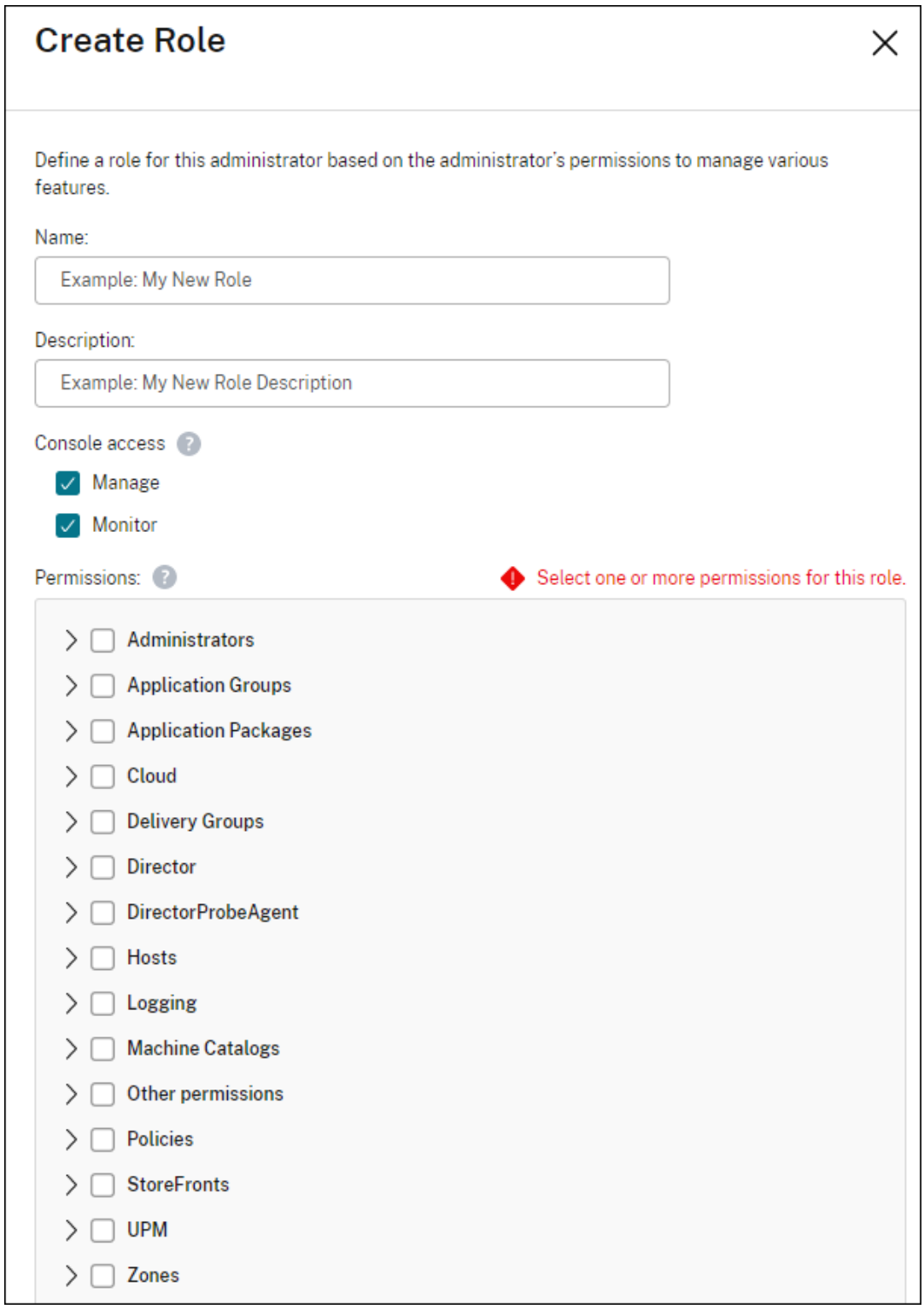
Los nombres de los roles pueden contener un máximo de 64 caracteres Unicode. Los nombres no pueden contener los siguientes caracteres: \ (barra diagonal inversa), / (barra diagonal), ; (punto y coma), : (dos puntos), # (almohadilla) , (coma), * (asterisco), ? (signo de interrogación), = (signo igual), <> (flecha izquierda o derecha), | (barra vertical), [ ] (corchete izquierdo o derecho), () (paréntesis de la izquierda o derecho), “(comillas dobles) ni ‘(apóstrofe).

Las descripciones de los roles pueden contener un máximo de 256 caracteres Unicode.

1. Inicie sesión en Citrix Cloud si aún no lo ha hecho. Seleccione **Mis servicios > DaaS** en el menú superior de la izquierda.
2. En **Administrar > Configuración completa**, seleccione **Administradores** en el panel de la izquierda.
3. Seleccione la ficha **Roles**.
4. Siga las instrucciones correspondientes a la tarea que quiere completar:

    - **Ver información detallada de un rol:** selecciónelo en el panel central. La parte inferior del panel central muestra los tipos de objeto y los permisos asociados al rol. Seleccione la ficha **Administradores** en el panel inferior para ver una lista de los administradores que actualmente tienen ese rol.
    - **Crear un rol personalizado:** Seleccione **Crear rol** en la barra de acciones. Configure los parámetros de la siguiente manera:
        - Escriba un nombre y una descripción.
        - Configure el acceso a la consola. Determine qué consolas son visibles para los administradores. Puede continuar sin seleccionar ninguna consola. En tal caso, los administradores con el rol no pueden acceder a **Administrar** y **Supervisar**, pero pueden ver, administrar o acceder a objetos a través de los SDK y las API.
        - Seleccione los tipos de objeto y los permisos pertinentes. Para conceder permiso de acceso total a un tipo de objeto, seleccione su casilla de verificación correspondiente. Para conceder permisos a nivel detallado, expanda el tipo de objeto y, a continuación, seleccione **Solo lectura** u objetos individuales en **Administrar** dentro del tipo.




- **Copiar un rol:** selecciónelo en el panel central y, a continuación, seleccione **Copiar rol** en la barra de acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario. Cuando haya terminado, seleccione **Guardar**.

- **Modificar un rol personalizado:** selecciónelo en el panel central y, a continuación, seleccione **Modificar rol** en la barra de acciones. Cambie el nombre, la descripción, los tipos de objeto y los permisos, según sea necesario. Los roles integrados no se pueden modificar. Cuando haya terminado, seleccione **Guardar**.
- **Eliminar un rol personalizado:** selecciónelo en el panel central y, a continuación, seleccione **Eliminar rol** en la barra de acciones. Cuando se le solicite, confirme la eliminación. Los roles integrados no pueden eliminarse. No se puede eliminar un rol personalizado si está asignado a un administrador.

### Crear y gestionar ámbitos

De forma predeterminada, todos los roles tienen el ámbito Todo para sus objetos relevantes. Por ejemplo, un administrador de grupos de entrega puede administrar todos los grupos de entrega. Para algunos roles de administrador, puede crear un ámbito que permita a ese rol de administrador acceder a un subconjunto de los objetos relevantes. Por ejemplo, puede que le interese conceder a un administrador de catálogos de máquinas acceso únicamente a los catálogos que contienen un determinado tipo de máquinas, en lugar de a todos los catálogos.

- Los administradores de acceso total o los administradores de Cloud de acceso personalizado pueden crear ámbitos para los roles Administrador de solo lectura, Administrador de catálogo de máquinas, Administrador de grupo de entrega y Administrador de host.
- Los ámbitos no se pueden crear para los administradores de acceso total, ni se pueden crear para los administradores de Cloud o los administradores de asistencia técnica. Esos administradores siempre tienen el ámbito Todo.

Reglas para crear y gestionar ámbitos:

- Los nombres de los ámbitos pueden contener un máximo de 64 caracteres Unicode. Los nombres no pueden contener estos caracteres: \ (barra diagonal inversa), / (barra diagonal), ; (punto y coma), : (dos puntos), # (almohadilla) , (coma), * (asterisco), ? (signo de interrogación), = (signo igual), <> (flecha izquierda o derecha), | (barra vertical), [ ] (corchete izquierdo o derecho), () (paréntesis de la izquierda o derecho), “(comillas dobles) ni ‘(apóstrofe).
- Las descripciones de los ámbitos pueden contener un máximo de 256 caracteres Unicode.
- Al copiar o modificar un ámbito, tenga en cuenta que eliminar objetos del ámbito puede tener como consecuencia que un administrador no pueda acceder a ellos. Si el ámbito modificado está emparejado con uno o varios roles, compruebe que los cambios que haga en el ámbito no hagan que la pareja de rol y ámbito quede inutilizable.

Para crear y administrar ámbitos:

1. Inicie sesión en Citrix Cloud. Seleccione **Mis servicios > DaaS** en el menú superior de la izquierda.

2. En **Administrar > Configuración completa**, seleccione **Administradores** en el panel de la izquierda.
3. Seleccione la ficha **Ámbitos**.
4. Siga las instrucciones correspondientes a la tarea que quiere completar:

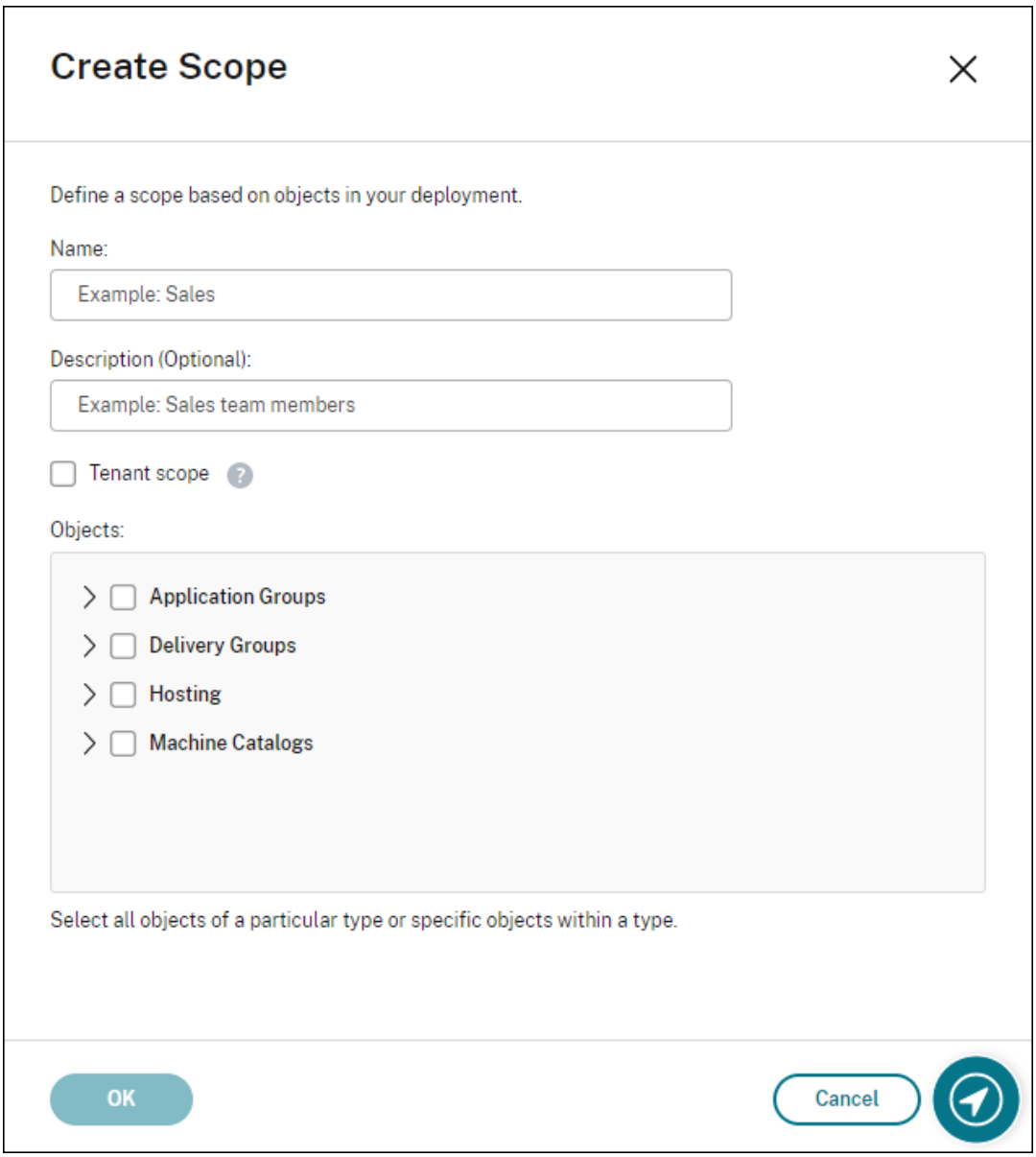
    - **Ver información detallada de un ámbito:** Seleccione el ámbito. La parte inferior del panel muestra los objetos y los administradores que tienen ese ámbito.
    - **Crear un ámbito:** Haga clic en **Crear ámbito** en la barra de acciones. Escriba un nombre y una descripción. Los objetos se enumeran por tipo, como grupo de entrega y catálogo de máquinas.
        - Para incluir todos los objetos de un tipo concreto (por ejemplo, todos los grupos de entrega), marque la casilla correspondiente al tipo de objeto.
        - Para incluir objetos concretos que haya dentro de un tipo de objeto, expanda el tipo y, a continuación, marque las casillas de los objetos (por ejemplo, grupos de entrega concretos).

            > **Nota:**
            >
            > Los grupos de aplicaciones, los grupos de entrega o los catálogos de máquinas se muestran en estructuras de carpetas que se ajustan a su administración en DaaS. Puede seleccionar una carpeta para seleccionar todos sus objetos o expandir una carpeta para seleccionar objetos específicos.

        - Para crear un cliente arrendatario, seleccione la casilla de verificación **Ámbito del arrendatario**. Si se selecciona, el nombre que introdujo para el ámbito es el nombre del arrendatario. Para obtener más información sobre el ámbito del arrendatario, consulte Administración de arrendatarios.

    Cuando haya terminado, seleccione **Aceptar**.




- **Copiar un ámbito:** Selecciónelo en el panel central y, a continuación, seleccione **Copiar ámbito** en la barra de acciones. Cambie el nombre o la descripción. Cambie los objetos y los tipos de objeto, según sea necesario. Cuando haya terminado, seleccione **Guardar**.
- **Modificar un ámbito:** Selecciónelo en el panel central y, a continuación, seleccione **Modificar ámbito** en la barra de acciones. Cambie el nombre, la descripción, los tipos de objeto y los objetos, según sea necesario. Cuando haya terminado, seleccione **Guardar**.
- **Eliminar un ámbito:** Selecciónelo en el panel central y, a continuación, seleccione **Eliminar ámbito** en la barra de acciones. Cuando se le solicite, confirme la eliminación.

  No se puede eliminar un ámbito si está asignado a un rol. Si lo intenta, aparecerá un mensaje de error para indicarle que no tiene permiso para hacerlo. De hecho, el error

se produce porque el par de rol y ámbito que utiliza este ámbito está asignado a un administrador. En primer lugar, elimine la asignación del par de rol y ámbito en todos los administradores que la utilicen. A continuación, elimine el ámbito en la consola **Administrar**.

Después de crear un ámbito, dicho ámbito aparece en la lista **Acceso personalizado** en la consola de Citrix Cloud. A continuación, puede seleccionarlo al asignar un rol a un administrador.

Por ejemplo, supongamos que crea un ámbito llamado CAD y selecciona los catálogos que contienen las máquinas indicadas para las aplicaciones CAD. Cuando regrese a la consola de Citrix Cloud y seleccione **Modificar ámbitos** con relación a un rol, la lista de ámbitos disponibles mostrará el ámbito de CAD que creó anteriormente.

El administrador de Cloud y el administrador de asistencia técnica siempre tienen el ámbito Todo, por lo que el ámbito CAD no se aplica a ellos.

#### Administración de arrendatarios

Con la interfaz de administración de Configuración completa, puede crear arrendatarios que se excluyan mutuamente en una sola instancia de Citrix DaaS. Para ello, cree ámbitos de arrendatario en **Administradores > Ámbitos** y asocie objetos de configuración, como catálogos de máquinas y grupos de entrega, a esos arrendatarios. Como resultado, los administradores con acceso a un arrendatario solo pueden administrar objetos que estén asociados al arrendatario.

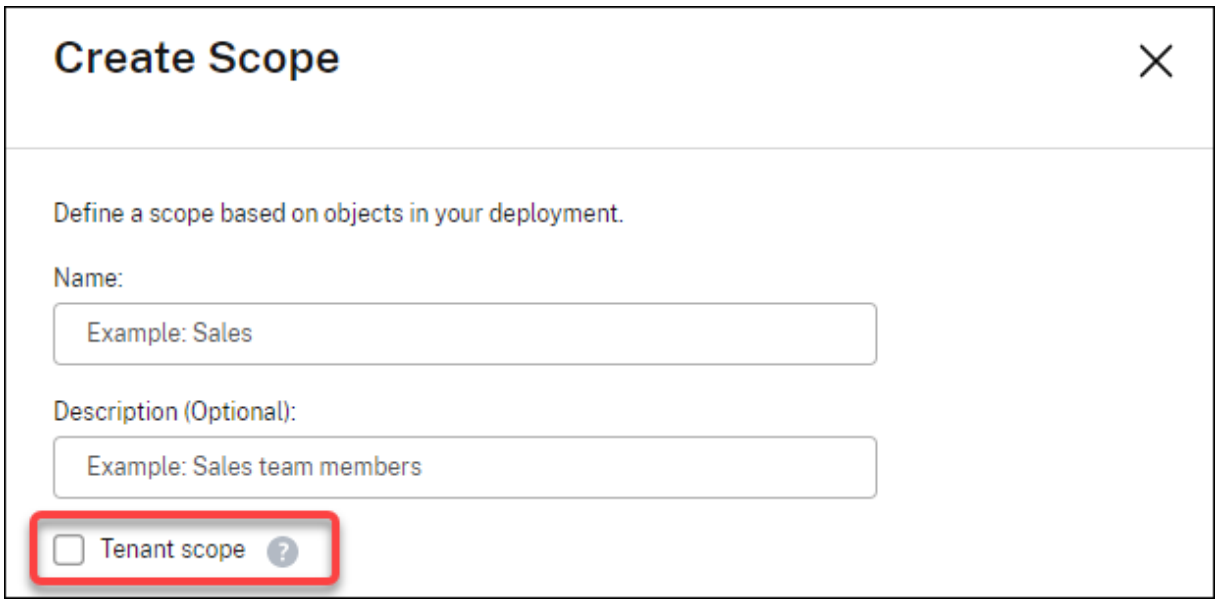
Esta función es útil, por ejemplo, si su organización:

- Tiene diferentes silos empresariales (divisiones independientes o equipos de administración de TI separados)
- O tiene varios sitios locales y quiere mantener la misma configuración en una sola instancia de Citrix DaaS

La interfaz le permite filtrar clientes arrendatarios por nombre. De forma predeterminada, la interfaz muestra información sobre todos los clientes arrendatarios. Para mostrar información sobre un arrendatario específico, selecciónelo en la lista de la esquina superior derecha.

**Crear un cliente arrendatario** Para crear un cliente arrendatario, seleccione **Ámbito del arrendatario** al crear un ámbito. Al seleccionar la opción, crea un tipo de ámbito único que se aplica a los objetos en casos en los que comparte una instancia de Citrix DaaS entre diferentes unidades de negocio, cada una de las cuales es independiente de las demás. Después de crear un ámbito de arrendatario, no puede cambiar el tipo de ámbito.




La ficha **Ámbitos** muestra todos los elementos del ámbito. La única diferencia entre los ámbitos normales y los ámbitos de arrendatario se encuentra en la columna **Tipo**. Un campo de columna en blanco indica un ámbito normal. Puede hacer clic en la columna **Tipo** para ordenar los elementos del ámbito si es necesario.

Para ver los recursos (objetos) asociados a un ámbito, seleccione **Administradores** en el panel de la izquierda. En la ficha **Ámbitos**, seleccione el ámbito y, a continuación, seleccione **Modificar ámbito** en la barra de acciones.

> **Sugerencia:**
>
> La propiedad de arrendatario se asigna a nivel de ámbito. Los catálogos de máquinas, los grupos de entrega, las aplicaciones y las conexiones heredan la propiedad de arrendatario del ámbito aplicable.

Al usar un ámbito de arrendatario, tenga en cuenta las siguientes consideraciones:

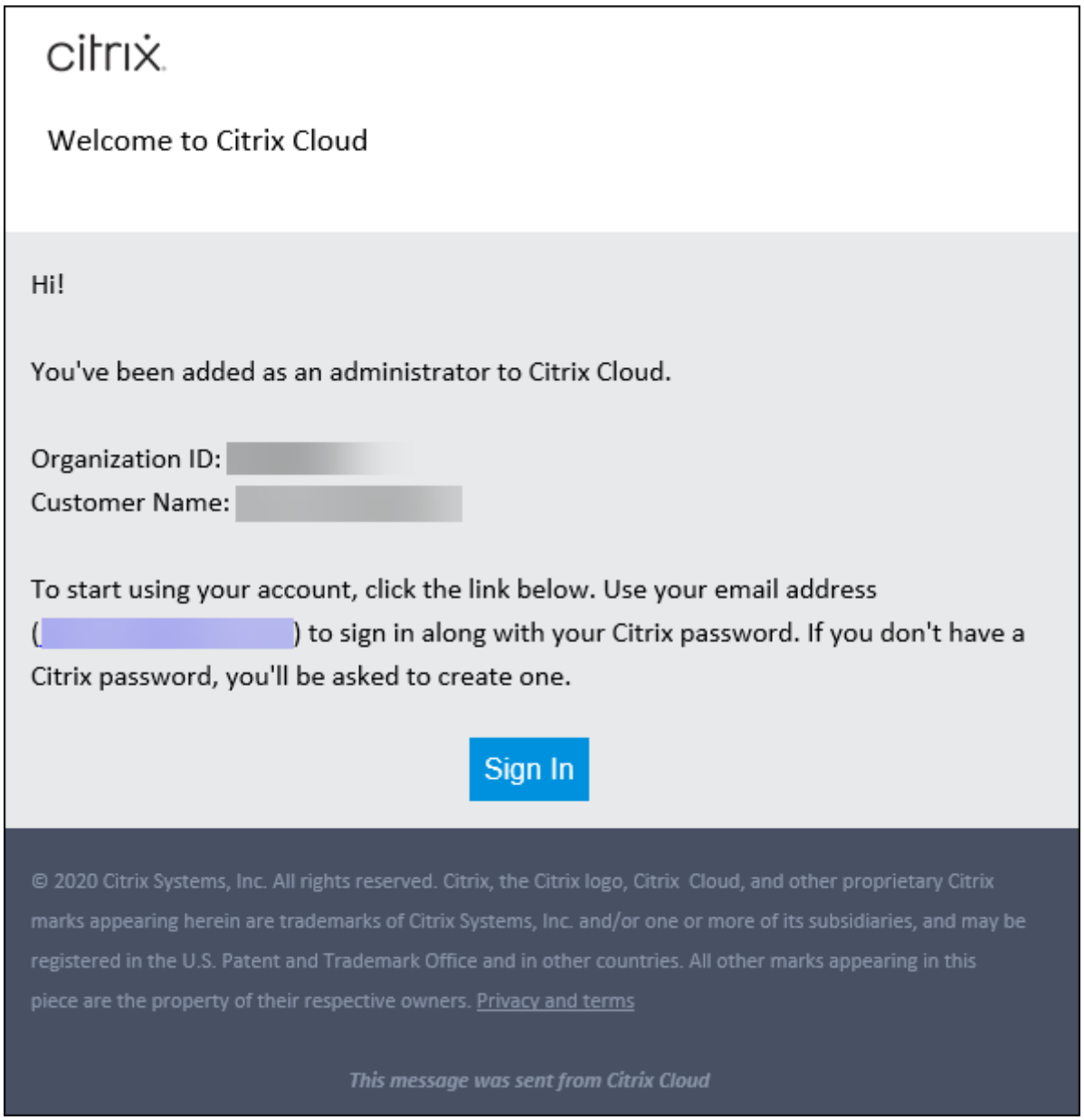
- La propiedad de arrendatario se asigna en el siguiente orden: **Alojamiento > Catálogos de máquinas > Grupos de entrega > Aplicaciones**. Los objetos de nivel inferior dependen de objetos de nivel superior para heredar de ellos la propiedad de arrendatario. Por ejemplo, al seleccionar un grupo de entrega, debe seleccionar el alojamiento y el catálogo de máquinas asociados. De lo contrario, el grupo de entrega no puede heredar la propiedad de arrendatario.
- Después de crear un ámbito de arrendatario, puede modificar los objetos para modificar las asignaciones de arrendatario. Cuando se modifica una asignación de arrendatario, sigue sujeta a la restricción de que debe asignarse a los mismos arrendatarios o a un subconjunto de estos. Sin embargo, los objetos de nivel inferior no se vuelven a evaluar cuando cambian las asignaciones de arrendatario. Asegúrese de que los objetos estén restringidos correctamente cuando cambie las asignaciones de arrendatario. Por ejemplo, si hay un catálogo de máquinas

disponible para TenantA y TenantB, puede crear un grupo de entrega para TenantA y otro para TenantB. (TenantA y TenantB están asociados a ese catálogo de máquinas). A continuación, puede cambiar el catálogo de máquinas para que se asocie solo a TenantA. Como resultado, el grupo de entrega asociado a TenantB deja de ser válido.

**Configurar acceso personalizado para administradores** Después de crear los ámbitos de arrendatario, configure el acceso personalizado para los administradores respectivos. Para obtener más información, consulte Configurar acceso personalizado para un administrador. Citrix Cloud envía una invitación a los administradores de clientes especificados y los agrega a la lista. Al recibir el mensaje de correo electrónico, deben hacer clic **Iniciar sesión** para aceptar la invitación. Una vez que inician sesión en la interfaz de administración de **Configuración completa**, pueden ver los recursos que contienen los pares de roles y ámbitos asignados.




Los administradores con acceso a un arrendatario solo pueden administrar objetos (por ejemplo, un catálogo de máquinas o grupo de entrega) asociados al arrendatario.

### Configurar acceso personalizado para un administrador

Esta función le permite definir los permisos de acceso de los administradores existentes o los administradores que invite para que puedan desempeñar sus roles en la organización.

Los cambios realizados en los permisos de acceso tardan 5 minutos en surtir efecto. Al cerrar la sesión de la interfaz de administración de Configuración completa y volver a iniciar sesión, los cambios surten efecto inmediatamente. En casos en los que los administradores siguen utilizando la interfaz

de administración después de que los cambios surtan efecto sin volver a conectarse a ella, aparece una advertencia cuando intentan acceder a elementos para los que ya no tienen permisos.

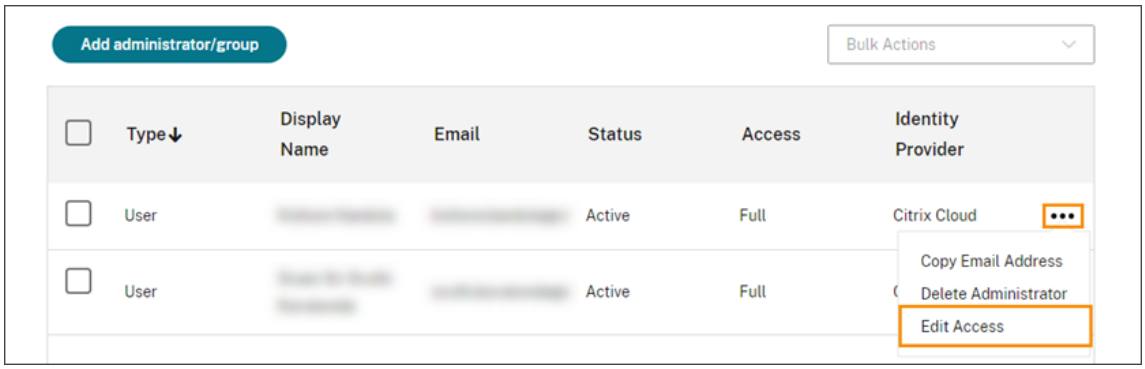
De forma predeterminada, cuando invita a los administradores, estos tienen acceso total. El acceso total permite al administrador gestionar todos los servicios suscritos y todas las operaciones de Citrix Cloud (como invitar a otros administradores). Una implementación de Citrix Cloud necesita al menos un administrador con acceso total.

También puede conceder acceso personalizado al invitar a un administrador. El acceso personalizado permite al administrador gestionar únicamente los servicios y las operaciones que especifique.

Al crear un rol o ámbito en Citrix DaaS, este aparece en la lista de acceso personalizado y se puede seleccionar. Al seleccionar un rol para un administrador, puede modificar los ámbitos según sea necesario para reflejar el rol del administrador en su organización.

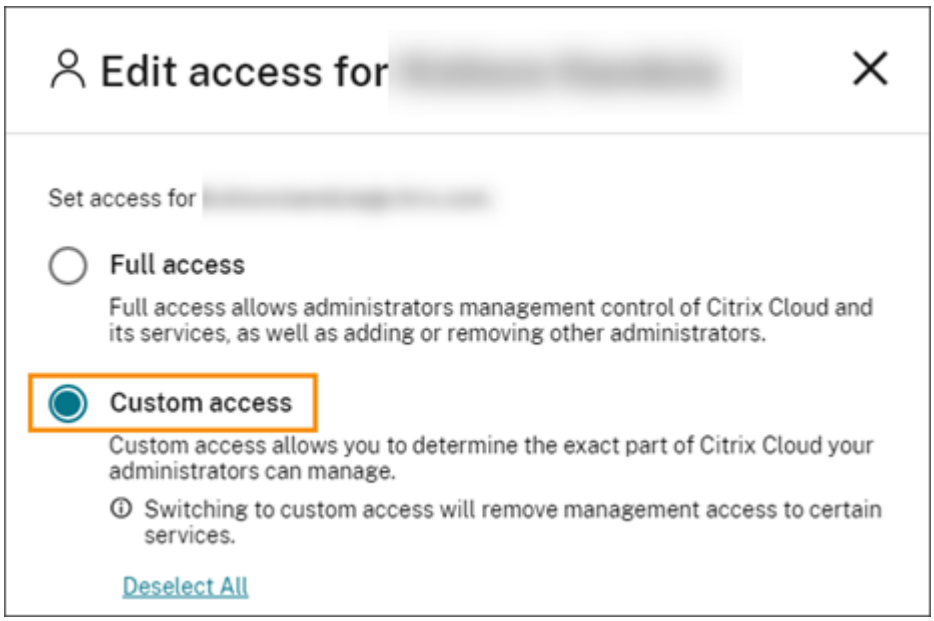
Para configurar el acceso personalizado para un administrador:

1. Inicie sesión en Citrix Cloud. Seleccione **Administración de acceso e identidad** > **Administradores** en el menú superior izquierdo.
2. Busque al administrador que quiere gestionar, seleccione el menú de tres puntos y seleccione **Modificar acceso**.



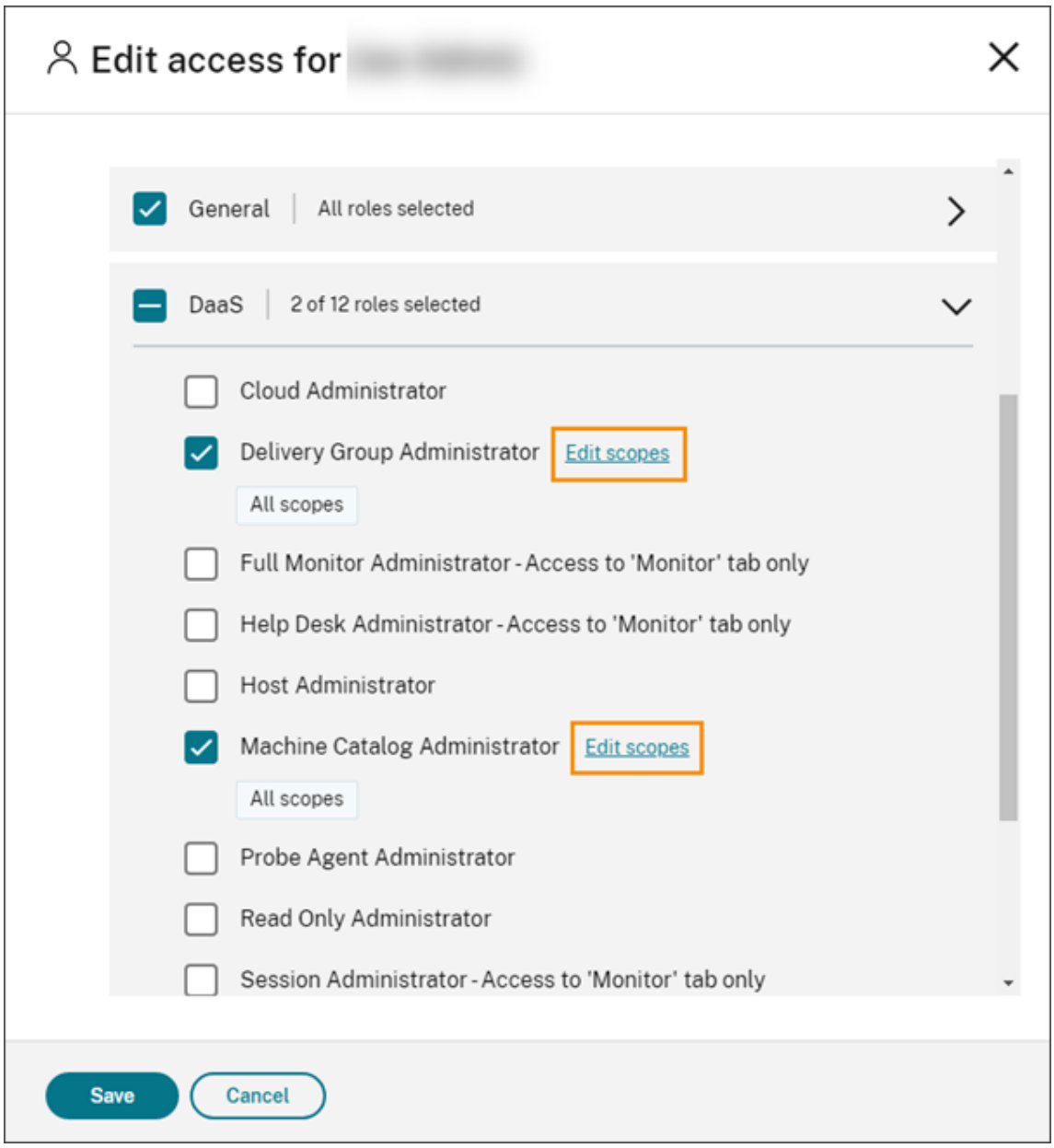

3. Seleccione **Acceso personalizado**.




4. En **DaaS**, seleccione o desactive las casillas situadas junto a uno o varios roles. Para modificar los ámbitos asociados a un rol asignado, seleccione **Modificar ámbitos**.

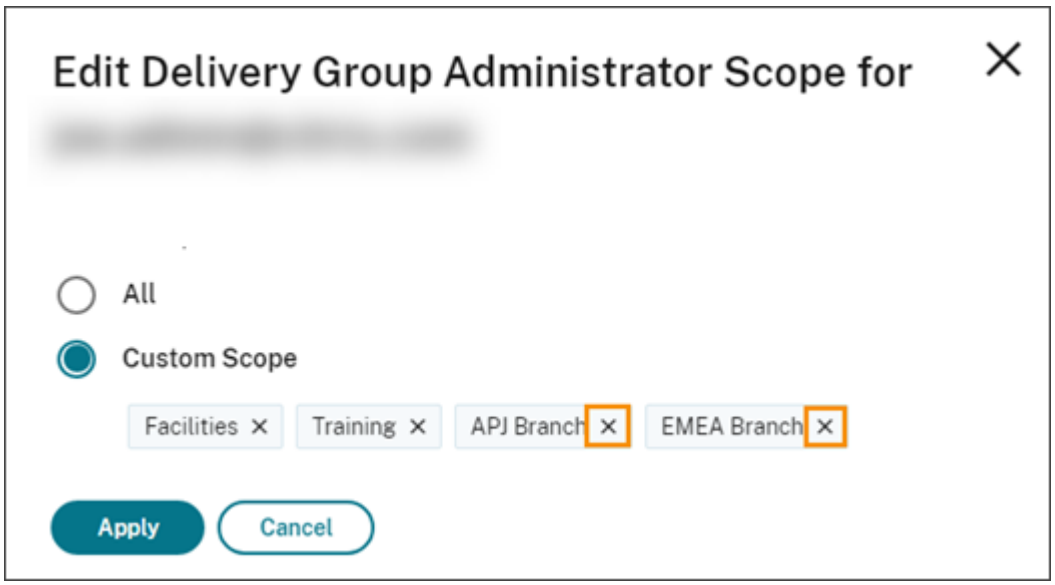
 



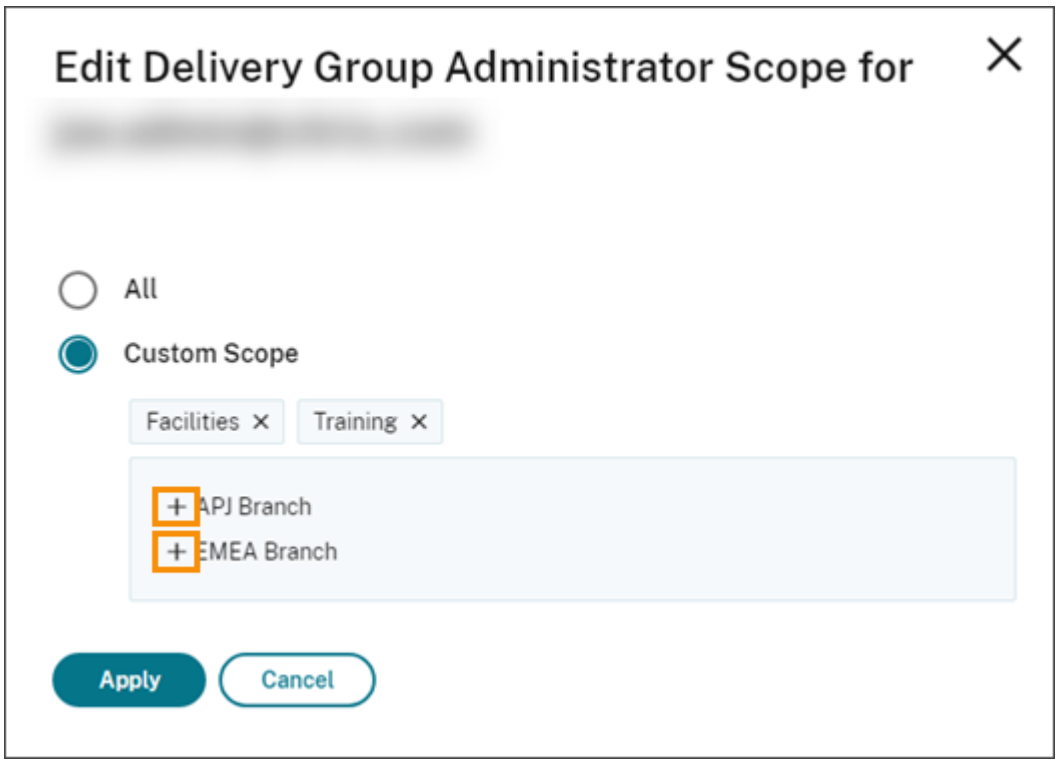

De forma predeterminada, cada rol seleccionado tiene todos los ámbitos seleccionados, como indica la etiqueta **Todos los ámbitos**.

5. Para especificar los ámbitos de un rol seleccionado, seleccione **Ámbito personalizado** y, a continuación, agregue o elimine los ámbitos correspondientes. De forma predeterminada, todos los ámbitos personalizados se agregan a un rol. Para eliminar un ámbito, haga clic en el icono X del ámbito.




Los ámbitos que se han eliminado y que están disponibles para agregarse al rol aparecen en una lista debajo de los ámbitos que ya se han agregado. Para agregar un ámbito al rol, seleccione el icono con el signo más del ámbito.




6. Cuando haya terminado de seleccionar los ámbitos, seleccione **Aplicar**.
7. Seleccione **Guardar** para guardar los roles seleccionados para el administrador.

### Diferencias de Citrix Virtual Apps and Desktops local

Si conoce la administración delegada en la versión local del producto Citrix Virtual Apps and Desktops, la versión de Citrix DaaS presenta varias diferencias.

En Citrix Cloud:

- Se identifica a los administradores por su inicio de sesión en Citrix Cloud, en lugar de su cuenta de Active Directory. Puede crear pares de rol y ámbito para personas de Active Directory, pero no para grupos.
- Los administradores se crean, configuran y eliminan en la consola de Citrix Cloud, en lugar de Citrix DaaS.
- Los pares de rol y ámbito se asignan a los administradores en la consola de Citrix Cloud, en lugar de Citrix DaaS.
- Los informes no están disponibles. Puede ver la información de administrador, rol y ámbito en la interfaz **Administrar > Configuración completa** del servicio.
- El administrador de Cloud con acceso personalizado es similar a un administrador total en la versión local. Ambos tienen permisos totales de administración y supervisión para la versión de Citrix Virtual Apps and Desktops que se está utilizando.

  Sin embargo, en Citrix DaaS, no hay ningún rol de administrador total con nombre. No equipare el "Acceso completo"en Citrix Cloud con el "Administrador total"en Citrix Virtual Apps and Desktops local. El acceso completo en Citrix Cloud abarca los dominios a nivel de plataforma, la biblioteca, las notificaciones y las ubicaciones de recursos, además de todos los servicios suscritos.

### Diferencias con versiones anteriores de Citrix DaaS

Antes de la publicación de la funcionalidad expandida de acceso personalizado (septiembre de 2018), había dos roles de administrador de acceso personalizado: administrador total y administrador de asistencia técnica. Cuando la implementación tiene habilitada la administración delegada (que es una configuración de la plataforma), esos roles se asignan automáticamente.

- Un administrador que estaba configurado con un acceso personalizado **Virtual Apps and Desktops (o XenApp and XenDesktop) Service: Administrador total** ahora tiene un acceso personalizado **Administrador de Cloud**.
- Un administrador que estaba configurado con un acceso personalizado **Virtual Apps and Desktops (o XenApp and XenDesktop) Service: Administrador de asistencia técnica** ahora tiene un acceso personalizado **Administrador de asistencia técnica**.

### Más información

Consulte Administración delegada y supervisión para obtener información acerca de los administradores, los roles y los ámbitos utilizados en la consola **Supervisar** del servicio.

## Página de inicio de la interfaz de Configuración completa

October 30, 2023

Proporciona una descripción general de la implementación y las cargas de trabajo de Citrix DaaS, junto con información que le ayuda a sacar el máximo rendimiento de su suscripción. La página consta de estas partes:

- Descripción general del servicio
- Alertas de estado del servicio
- Recomendaciones
- Novedades
- Funciones en Tech Preview
- Introducción

Para acceder a la página de inicio, siga estos pasos:

1. Inicie sesión en Citrix Cloud.
2. En el mosaico de **DaaS**, haga clic en **Administrar**.
3. Seleccione **Administrar > Configuración completa**. Aparecerá la página de inicio.

### Descripción general del servicio

Proporciona una descripción general de la implementación y las cargas de trabajo de Citrix DaaS:

- **Recursos**. Muestra la cantidad de recursos implementados y sus recuentos por categoría.

| Recurso | Para ver los recuentos por categoría |
| --- | --- |
| Máquinas | Haga clic en **Máquinas**, seleccione un estado y, a continuación, coloque el mouse sobre el gráfico de anillo para obtener información detallada. Opciones disponibles: **Estado de disponibilidad** (Disponible, En uso, Apagado o No disponible), **Estado de registro** (Registrado o No registrado) y **Estado de mantenimiento** (En mantenimiento o No en mantenimiento). Al ver los recuentos de máquinas por estado de disponibilidad, puede hacer clic en un estado para ver los detalles de la máquina correspondiente. |
| Aplicaciones | Haga clic en **Aplicaciones** y coloque el mouse sobre el gráfico de anillo para obtener información detallada. |
| Grupos de entrega | Haga clic en **Grupos de entrega** y coloque el mouse sobre el gráfico de anillo para obtener información detallada. |
| Catálogos de máquinas | Haga clic en **Catálogos de máquinas** y coloque el mouse sobre el gráfico de anillo para obtener información detallada. |

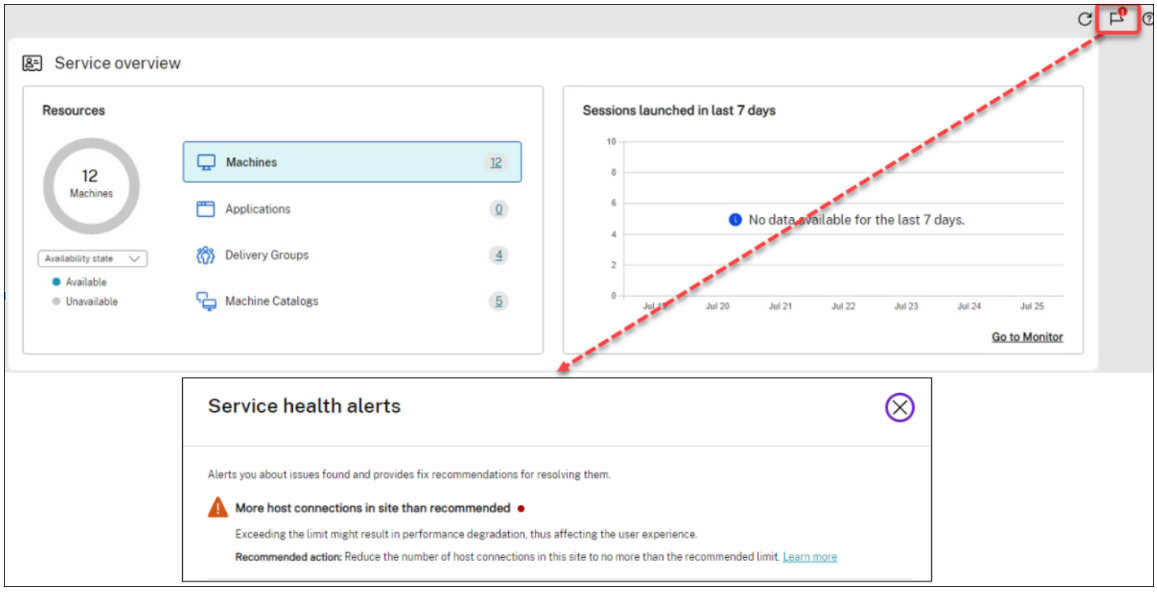
- **Sesiones iniciadas en los últimos 7 días**. Muestra la cantidad de sesiones de escritorio y aplicación iniciadas cada día durante los últimos 7 días. Para obtener un desglose de los detalles, haga clic en **Ir a Supervisar**.

### Alertas de estado del servicio

Le avisa sobre los problemas encontrados y ofrece recomendaciones para resolverlos. Las alertas aparecen con símbolos de advertencia y error.

> **Nota:**
>
> Los diagnósticos se actualizan cada hora.
>
> Ejemplo de alerta:




## Recomendaciones

Se recomiendan funciones disponibles con la suscripción, como Workspace Environment Management y Autoscale. Puede interactuar con nosotros, indicar si le gusta o no una recomendación y dejar sus comentarios.

> **Nota:**
>
> Si no le gusta una recomendación, esta desaparece. Si no le gusta ninguna recomendación o el widget de recomendaciones, el widget desaparecerá.

## Novedades

Muestra una lista selecta de las funciones más recientes de Citrix DaaS que son más valiosas para su empresa. El uso de esas funciones le ayuda a aprovechar al máximo su suscripción. Para obtener una lista completa de las nuevas funciones, consulte Novedades.

## Funciones en Tech Preview

Muestra las funciones que se hallan en Tech Preview. Como administrador de Citrix Cloud con acceso total, puede activar o desactivar las funciones de vista previa sin ponerse en contacto con Citrix. Los cambios tardan hasta 15 minutos en surtir efecto.

Se recomienda utilizar las funciones de previsualización en entornos que no son de producción. El servicio de asistencia técnica de Citrix no atiende a los problemas detectados con las funciones en Tech Preview.

## Introducción

Muestra los pasos que le guían en la configuración inicial de aplicaciones y escritorios.

Los pasos de configuración son los siguientes:

1. Crear ubicaciones de recursos

   Las ubicaciones de recursos se refieren a ubicaciones que contienen aplicaciones y escritorios que quiere entregar a los usuarios. Este paso le permite agregar sus ubicaciones de recursos a DaaS e instalar Cloud Connectors en ellas. Los Cloud Connectors actúan como canales que autentican y cifran todas las comunicaciones entre Citrix Cloud y sus recursos.

2. Crear una conexión de host

   Los hosts son hipervisores o servicios de la nube que se utilizan en las ubicaciones de recursos. Este paso le permite especificar la información que utiliza DaaS para comunicarse con las máquinas virtuales de un host. La información detallada incluye la ubicación del recurso, el tipo de host, las credenciales de acceso, el método de almacenamiento que se va a usar y las redes que pueden usar las máquinas virtuales del host.

3. Preparar una imagen maestra

   Una imagen maestra incluye el sistema operativo, todas las aplicaciones necesarias y el Virtual Delivery Agent (VDA). Los VDA establecen y mantienen conexiones entre las VM y los dispositivos de los usuarios.

4. Crear un catálogo de máquinas

   Un catálogo de máquinas es un conjunto de máquinas virtuales idénticas de SO de sesión única o multisesión que se asignan a los usuarios. Este paso le permite crear un catálogo de máquinas al especificar la tecnología de aprovisionamiento, la imagen maestra y el tamaño de las máquinas virtuales.

5. Asignar usuarios

   Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. Este paso le permite crear grupos de entrega para especificar qué equipos, departamentos o tipos de usuarios pueden usar ciertas máquinas.

6. Configurar Workspace

   Comparta con sus usuarios la URL del espacio de trabajo desde **Configuración de Workspace > Acceso**.

# Licencias

September 16, 2022

En este artículo se tratan las tareas y los recursos de licencias de Microsoft y de licencias de Citrix.

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

Esta información se aplica cuando se entregan 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 2019. Normalmente, esto requiere una licencia de acceso de cliente de Servicios de Escritorio remoto (CAL de RDS). El VDA debe poder comunicarse con un servidor de licencias RDS para solicitar licencias CAL de RDS.

Instale y active el servidor de licencias. Para obtener más información, consulte el documento Activate the Remote Desktop Services License Server de Microsoft. Para entornos de prueba de concepto, puede utilizar el período de gracia que ofrece Microsoft.

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

Para configurar el servidor de licencias RDS mediante configuraciones de directivas de grupo de Microsoft:

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 Model 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 de licencias de Citrix

Para obtener información sobre el uso de licencias de Citrix, consulte:

- Supervisar el uso activo y de licencias en los servicios de la nube
- Supervisar el uso activo y de licencias de Citrix DaaS

## Licencias de varios tipos

August 15, 2023

Las licencias de varios tipos admiten el uso de diferentes derechos de licencia en una misma implementación de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). Este artículo le afecta si tiene más de un derecho de licencia de Citrix. Un derecho de Citrix es una combinación de lo siguiente:

- Producto, que en el contexto actual de DaaS siempre es Citrix DaaS
- Edición de servicio (por ejemplo: Advanced, Advanced Plus, Premium o Premium Plus)
- Modelo de licencia (por ejemplo: usuario/dispositivo o simultánea)

### Reglas para la combinación de derechos

Las reglas para combinar las ediciones de servicio son las siguientes:

- Solo se permite combinar DaaS Advanced y Advanced Plus
- Solo se permite combinar DaaS Premium y Premium Plus
- DaaS Standard no se puede combinar con ninguna otra edición

Puede combinar los modelos de licencias al seguir las reglas de edición de servicio anteriores.

### Derechos al nivel del sitio y del grupo de entrega

Puede configurar y utilizar los derechos de licencia en estos dos niveles:

- Sitio (su implementación del producto Citrix DaaS)
- Grupo de entrega

Si aún no ha configurado los derechos de nivel de sitio o de grupo de entrega, tenga en cuenta el siguiente comportamiento predeterminado:

- Si tiene más de un derecho, se selecciona el más adecuado de los derechos disponibles para todo el sitio, siempre que se haya solicitado al mismo tiempo. De lo contrario, el primero que aparezca se convierte en el predeterminado para todo el sitio a menos que se cambie explícitamente más adelante.
- Se utiliza el derecho del sitio a menos que se configure un derecho de grupo de entrega.

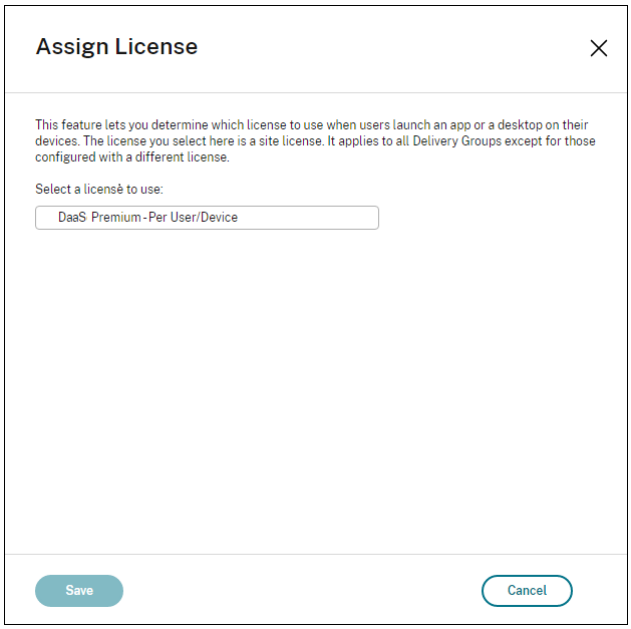
 

> **Nota:**
>
> La configuración de derechos para un sitio o grupo de entrega afecta a la forma de contabilizar el consumo de licencias en las pantallas de uso de licencias de Citrix Cloud.

### Ver y actualizar los derechos de nivel de sitio

Para especificar qué derechos de licencia usar en todo el sitio, vaya a **Configuración completa > Parámetros > Asignar licencia** y haga clic en **Modificar**. Aparecerá la hoja **Asignar licencia**. Para obtener información sobre cómo acceder a la página de **Configuración completa**, consulte la documentación de Citrix DaaS.

En la hoja **Asignar licencia**, seleccione una licencia que quiera que utilice el sitio. La licencia seleccionada se aplica a todos los grupos de entrega del sitio, excepto a los configurados con una licencia diferente.




Las licencias que puede seleccionar son las siguientes:

- Citrix DaaS Premium: Por usuario/dispositivo
- Citrix DaaS Premium: Simultáneas
- Citrix DaaS Premium para Google Cloud: Por usuario/dispositivo
- Citrix DaaS Premium para Google Cloud: Simultánea
- Citrix DaaS Advanced: Por usuario/dispositivo
- Citrix DaaS Advanced: Simultáneas
- Citrix DaaS Advanced Plus: Por usuario/dispositivo
- Citrix DaaS Advanced Plus: Simultáneas
- Citrix DaaS Standard para Azure: Por usuario/dispositivo

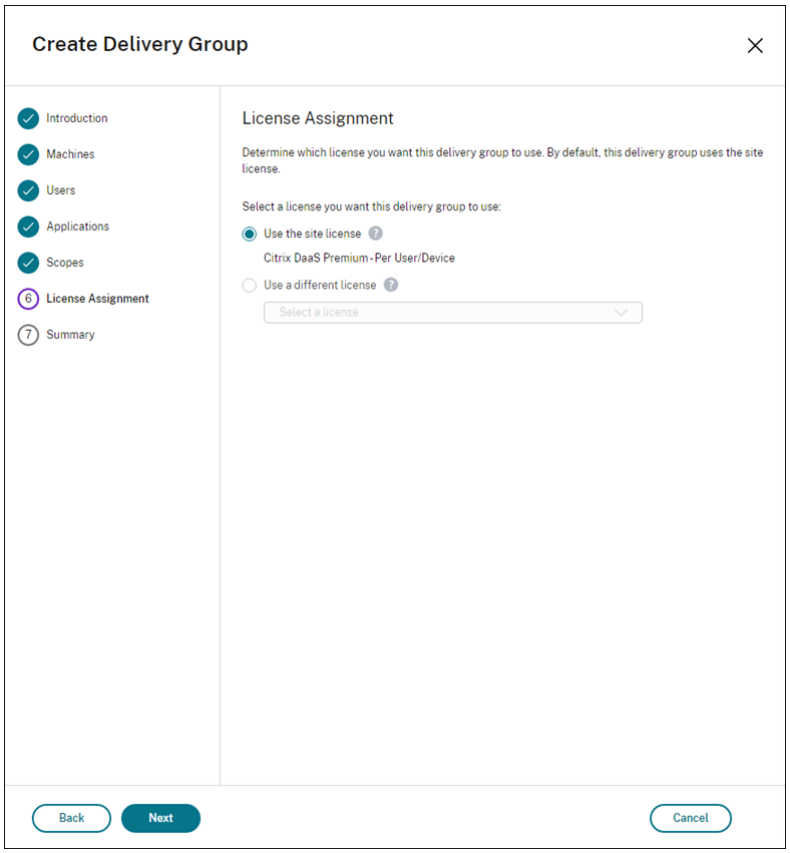
 

- Citrix DaaS Standard para Azure: Simultáneas
- Citrix DaaS Standard para Google Cloud: Por usuario/dispositivo
- Estándar Citrix DaaS para Google Cloud: Simultánea

Si tiene una licencia caducada, contacte con su representante de ventas de Citrix para renovarla o comprar nuevas licencias.

### Ver y actualizar un derecho de nivel de grupo de entrega

Puede especificar qué licencia quiere que utilice un grupo de entrega al crearlo o modificarlo. En la página **Asignación de licencias**, seleccione una opción.




Opciones:

- **Usar la licencia de sitio**. Una licencia de sitio se aplica a todos los grupos de entrega, excepto a los configurados con una licencia diferente. La licencia que aparece en esta opción es la licencia del sitio en uso. Para configurar la licencia del sitio, vaya a **Administrar > Configuración completa**, seleccione el nodo **Parámetros** y, a continuación, modifique **Asignar licencia**.
- **Usar otro tipo de licencia**. Esta opción le permite configurar este grupo de entrega para que use una licencia diferente de la del sitio. Recuerde que los derechos de licencia son una combinación de código de producto, edición y modelo de licencia. El grupo de entrega debe utilizar

la misma edición de licencia (Standard, Premium o Advanced) que el sitio. Si se configura, el grupo de entrega solo consume la licencia seleccionada. Aunque la licencia seleccionada se consuma por completo o se vuelva no válida, el grupo de entrega no recurre a la licencia del sitio.

De forma predeterminada, el grupo de entrega usa la licencia del sitio.

Cuando una licencia de grupo de entrega caduque y ya no sea válida, use una licencia diferente.

> **Nota:**
>
> Si más adelante configura un grupo de entrega para que use una licencia diferente, es posible que los usuarios conectados que consumen la licencia actual pierdan temporalmente el acceso a sus escritorios y aplicaciones.

### Un ejemplo de combinación de derechos

Por ejemplo, el cliente A adquirió inicialmente la edición Advanced y luego adquirió la edición Advanced Plus. En este caso, el cliente A todavía tiene una licencia para todo el sitio únicamente de la edición Advanced. Citrix no modifica el parámetro establecido inicialmente al nivel del sitio por el cliente A. Es responsabilidad del cliente A modificar la edición de la licencia a Advanced Plus al nivel del sitio.

Del mismo modo, el cliente A también puede actualizar la edición de la licencia a Advanced Plus en el grupo de entrega. Si este parámetro no está configurado, el grupo de entrega hereda la edición de la licencia establecida al nivel del sitio.

El administrador del cliente A puede actualizar la edición de la licencia de estas maneras:

- Actualizar la edición de licencia a nivel de sitio: Vaya a **Administrar > Configuración completa**, seleccione el nodo **parámetros** y, a continuación, modifique **Asignar licencia**.
- Actualizar la edición de licencia a nivel de grupo de entrega: Vaya a **Administrar > Configuración completa** y seleccione el nodo **Grupos de entrega**. Modifique el grupo de entrega de destino para realizar cambios.

#### Actualizar el grupo de entrega mediante el comando de PowerShell

El comando de PowerShell para actualizar el grupo de entrega es el siguiente:

```
1 Set-BrokerDesktopGroup -Name <DGName> -ProductCode <Name of the product
      code> -LicenseModel <The type of license model>
2 <!--NeedCopy-->
```

Actualice el comando anterior en función de sus datos.

Por ejemplo, observe lo siguiente:

- `Set-BrokerDesktopGroup -Name DG1 -ProductCode VADS -LicenseModel CONCURRENT`
- `Set-BrokerDesktopGroup -Name DG1 -ProductCode $null -LicenseModel $null` (establezca la configuración al nivel del grupo de entrega para que esté al nivel del sitio)
- `Set-BrokerSite -CloudSiteLicense VADS:ADVANCED:USERDEVICE`

Tenga en cuenta que el modelo de licencia y el código de producto no están configurados al nivel del grupo de entrega. En este caso, se utilizan estas dos propiedades establecidas al nivel del sitio para el grupo de entrega.

Para obtener más información sobre el SDK de PowerShell remoto de Citrix DaaS, consulte la documentación de API y SDK.

### Más información

- Licencias
- Crear grupos de entrega
- Administrar grupos de entrega

## Equilibrar la carga de las máquinas

December 5, 2023

> **Nota:**
>
> Esta función se aplica a todos los catálogos, ya sean de SO de sesión única o de SO multisesión. El equilibrio de carga vertical solo se aplica a las máquinas con SO multisesión.

El equilibrio de carga se puede configurar a nivel de sitio y de grupo de entrega. Tiene dos opciones: vertical y horizontal. El equilibrio de carga horizontal está habilitado de forma predeterminada.

### Parámetros de equilibrio de carga a nivel de sitio

- **Equilibrio de carga vertical**. Asigna la carga entrante a la máquina más cargada que aún no haya alcanzado la carga máxima. De esta forma, se saturan las máquinas existentes antes de pasar a otras máquinas. Cuando los usuarios se desconectan de las máquinas existentes, se libera capacidad en esas máquinas. A continuación, las cargas entrantes se asignan a esas máquinas. El equilibrio de carga vertical degrada la experiencia del usuario, pero reduce los costes (las sesiones maximizan la capacidad de las máquinas encendidas).

Ejemplo: Tiene dos máquinas configuradas para 10 sesiones cada una. La primera máquina gestiona las 10 primeras sesiones simultáneas. La segunda máquina gestiona la undécima sesión.

> **Sugerencia:**
>
> Para especificar la cantidad máxima de sesiones que puede alojar una máquina, utilice la configuración de directiva Número máximo de sesiones.

También puede utilizar PowerShell para habilitar o inhabilitar el equilibrio de carga vertical en todo el sitio. Utilice el parámetro `UseVerticalScalingForRdsLaunches` del cmdlet `Set-BrokerSite`. Use `Get-BrokerSite` para mostrar el valor del parámetro `UseVerticalScalingForRdsLaunches`. Para obtener más información, consulte la ayuda del cmdlet.

- **Equilibrio de carga horizontal**. Asigna una sesión de usuario entrante a la máquina encendida con menos carga que esté disponible. El equilibrio de carga horizontal mejora la experiencia de usuario, pero aumenta los costes (porque se mantienen encendidas más máquinas). El equilibrio de carga horizontal está habilitado de forma predeterminada.

  Ejemplo: Tiene dos máquinas configuradas para 10 sesiones cada una. La primera máquina gestiona cinco sesiones simultáneas. La segunda máquina también gestiona cinco.

Para configurar esta función, desde **Administrar > Configuración completa**, seleccione **Parámetros** en el panel de la izquierda. Seleccione una opción en **Equilibrar la carga de catálogos multisesión**.

### Parámetros de equilibrio de carga a nivel de grupo de entrega

Configurar el equilibrio de carga a nivel de grupo de entrega le permite anular los parámetros de equilibrio de carga heredados del nivel de sitio. Puede lograr la máxima utilización de cada máquina si selecciona el equilibrio de carga vertical en el nivel de grupo de entrega. Esto ayudará a reducir los costes en nubes públicas. Esta configuración se puede realizar durante la creación de un nuevo grupo de entrega o durante la modificación de un grupo de entrega existente.

**Equilibrio de carga horizontal**. Las sesiones se distribuyen entre las máquinas encendidas. Por ejemplo, si tiene dos máquinas configuradas para 10 sesiones cada una, la primera máquina gestiona cinco sesiones simultáneas y la segunda también gestiona cinco.

**Equilibrio de carga vertical**. Las sesiones maximizan la capacidad de las máquinas encendidas y ahorran costes de máquina. Por ejemplo, si tiene dos máquinas configuradas para 10 sesiones cada una, la primera máquina gestionará las 10 primeras sesiones simultáneas. La segunda máquina gestiona la undécima sesión.

# Caché de host local

June 12, 2024

> **Sugerencia:**
>
> En **Configuración completa > Inicio**, la función de alertas de estado del servicio le proporciona alertas proactivas para garantizar que la caché de host local y las zonas estén configuradas correctamente. Por lo tanto, cuando se produce una interrupción, la caché de host local funciona y sus usuarios no se ven afectados. Las alertas se presentan en dos niveles: Las alertas a nivel de todo el sitio que se muestran en la página de inicio (icono de bandera) y las alertas relacionadas con zonas que se muestran en la ficha Solucionar problemas de cada zona. Para obtener más información, consulte Zonas.

Caché de host local (LHC, Local Host Cache) permite que la intermediación de las conexiones en una implementación de Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service) continúe cuando un Cloud Connector no se pueda comunicar con Citrix Cloud. La Caché de host local se activa después de que la conexión de red se haya perdido durante 60 segundos.

Con la Caché de host local, los usuarios que estén conectados cuando se produce una interrupción pueden seguir trabajando sin interrupciones. En las conexiones nuevas y las reconexiones se dan demoras mínimas de conexión.

> **Importante:**
>
> Si usa una implementación local de StoreFront, debe agregar a StoreFront todos los Cloud Connectors que tengan (o puedan tener) VDA registrados en ellos como Delivery Controllers. Un Cloud Connector que no se agrega a StoreFront no puede pasar al modo de interrupción del servicio, lo que podría provocar errores en el inicio del usuario.
>
> Para implementaciones sin StoreFront local, utilice la función de continuidad del servicio de la plataforma Citrix Workspace para que los usuarios puedan conectarse a los recursos durante las interrupciones de servicio. Para obtener más información, consulte Continuidad del servicio.

## Contenido de datos

La Caché de host local incluye la siguiente información, que es un subconjunto de la información contenida en la base de datos principal:

- Identidades de los usuarios y los grupos que tienen derechos asignados a recursos publicados en el sitio.
- Identidades de los usuarios que actualmente usan, o que han utilizado recientemente, recursos publicados en el sitio.

- Identidades de las máquinas VDA (incluidas las máquinas de acceso con Remote PC) configuradas en el sitio.
- Identidades (nombres y direcciones IP) de las máquinas cliente de la aplicación Citrix Workspace que se utilizan activamente para conectarse a los recursos publicados.

También contiene información para las conexiones actualmente activas que se establecieron mientras la base de datos principal no estaba disponible:

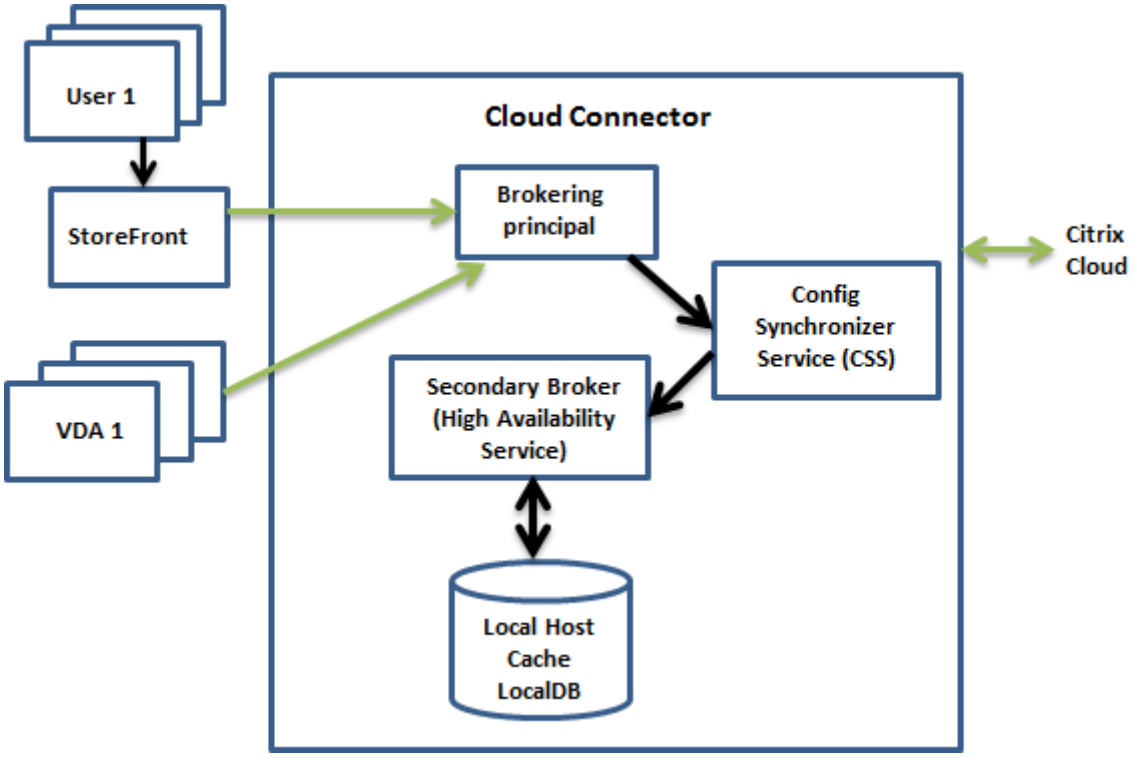
- Resultados de todos los análisis de máquinas de punto final del cliente realizados por la aplicación Citrix Workspace.
- Identidades de las máquinas de la infraestructura (tales como Citrix Gateway y servidores de StoreFront) que intervienen en las operaciones del sitio.
- Fechas, horas y tipos de actividades recientes de los usuarios.

## Funcionamiento

Consulte cómo interactúa la Caché de host local con Citrix Cloud.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

### Durante el funcionamiento normal



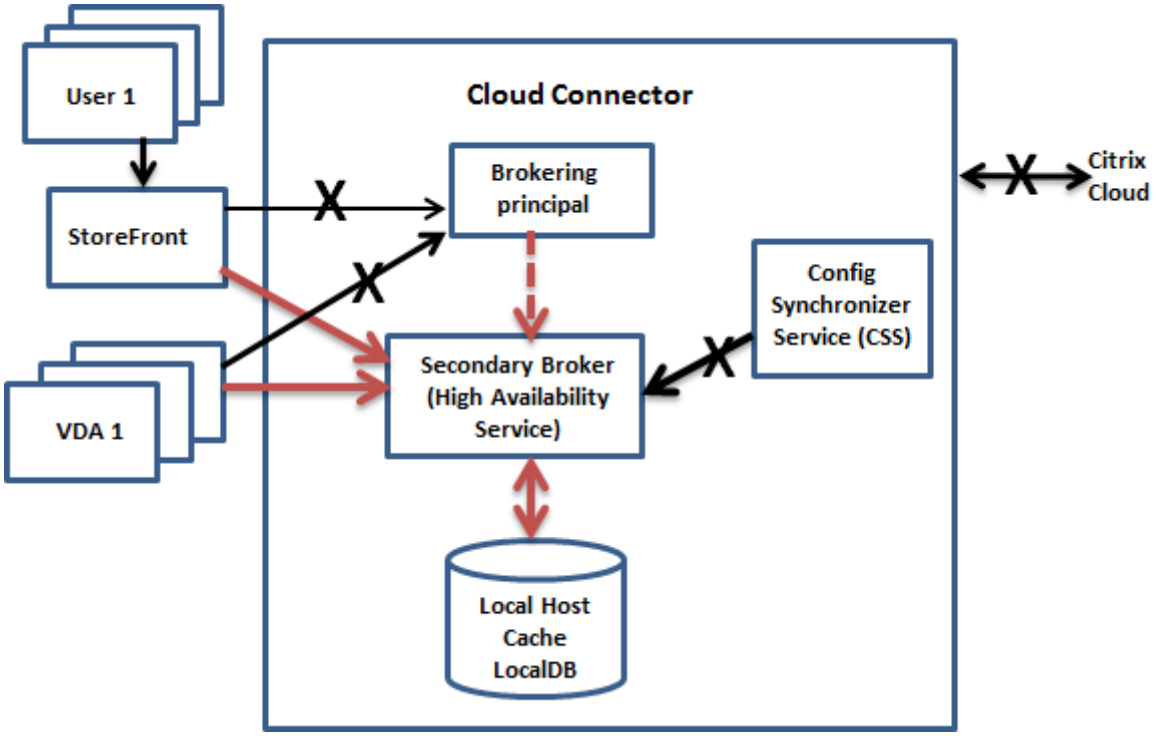
- El broker principal (conocido también como Citrix Remote Broker Provider Service) en un Cloud Connector acepta las solicitudes de conexión provenientes de StoreFront, y se comunica con Citrix Cloud para conectar usuarios a los agentes VDA que están registrados en el Cloud Connector.
- El servicio Citrix Config Synchronizer Service (CSS) se comunica con el broker de Citrix Cloud aproximadamente cada 5 minutos para comprobar si se han hecho cambios de configuración. Esos cambios pueden haberse iniciado por la acción de un administrador (si modifica una propiedad del grupo de entrega, por ejemplo) o por acciones del sistema (como las asignaciones de máquinas).
- Si se ha producido un cambio de configuración desde la comprobación anterior, CSS sincroniza la información (la copia) a un broker secundario presente en el Cloud Connector. (El broker secundario también se conoce como servicio de alta disponibilidad o broker de alta disponibilidad, como se muestra en la imagen anterior.)

  Se copian todos los datos de la configuración, no solo los elementos que han cambiado desde la comprobación anterior. El servicio CSS importa los datos de configuración en una base de datos LocalDB de Microsoft SQL Server Express ubicada en el Cloud Connector. Esta base de datos se conoce como la base de datos de la Caché de host local. El servicio CSS comprueba que la información de la base de datos de la Caché de host local coincida con la información presente en la base de datos del sitio en Citrix Cloud. La base de datos de la Caché de host local se crea con cada sincronización.

  Microsoft SQL Server Express LocalDB (que la base de datos de la Caché de host local utiliza) se instala automáticamente al instalar un Cloud Connector. La base de datos de la Caché de host local no se puede compartir entre los Cloud Connectors. No es necesario realizar una copia de seguridad de la base de datos de la Caché de host local. Se vuelve a crear cada vez que se detecta un cambio de configuración.
- Si no se han producido cambios desde la última comprobación, no se copian los datos de configuración.

**Durante una interrupción del servicio**




Al principio de una interrupción del servicio:

- El broker secundario comienza a escuchar y a procesar las solicitudes de conexión.
- Cuando empieza la interrupción, el broker secundario no dispone de datos actuales de registro de agentes VDA, pero, en cuanto un VDA se comunica con él, comienza un proceso de registro. Durante este proceso, el broker secundario también obtiene información de sesión actualizada acerca de ese VDA.
- Mientras el broker secundario gestiona las conexiones, el broker principal sigue supervisando la conexión a Citrix Cloud. Cuando se restaura la conexión, el broker principal indica al secundario que deje de escuchar para obtener la información de conexión. A continuación, el broker principal reanuda la intermediación. La próxima vez que el VDA se comunica con el broker principal, comienza un proceso de registro. El broker secundario elimina los registros de VDA restantes desde la interrupción anterior. El servicio CSS reanuda la sincronización de información cuando detecta que se han producido cambios de configuración en Citrix Cloud.

En el caso improbable de que se inicie una interrupción durante una sincronización, la importación de ese momento se descarta y se utiliza la última configuración conocida.

El registro de eventos indica cuándo tienen lugar las sincronizaciones y las interrupciones.

No hay límites de tiempo impuestos para el funcionamiento en modo de interrupción.

También puede desencadenar intencionadamente una interrupción. Consulte Forzar una interrupción para obtener más información sobre cómo y por qué hacerlo.

#### Ubicaciones de recursos con varios Cloud Connectors

Entre otras de sus tareas, CSS proporciona constantemente al broker secundario información sobre todos los Cloud Connectors de la ubicación de recursos. Con esta información, cada broker secundario sabe cuáles son todos los demás brokers secundarios que se ejecutan en otros Cloud Connectors de la ubicación de recursos.

Los brokers secundarios se comunican entre sí por un canal independiente. Estos brokers utilizan una lista alfabética de nombres de dominio completo (FQDN) de las máquinas que están ejecutando para determinar (elegir) qué broker secundario intermediará las operaciones de la zona si se produce una interrupción. Durante la interrupción, todos los VDA vuelven a registrarse en el broker secundario que se haya elegido. Los brokers secundarios de la zona que no hayan sido elegidos rechazan las solicitudes entrantes de conexión y de registro que les envíen los agentes VDA.

> **Importante:**
>
> Los conectores de una ubicación de recursos deben poder comunicarse entre sí en `http://<FQDN_OF_PEER_CONNECTOR>:80/Citrix/CdsController/ISecondaryBrokerElection`. Si los conectores no pueden comunicarse en esta dirección, es posible que se elijan varios agentes y que se produzcan errores de inicio intermitentes durante un evento de caché de host local.

Si un broker secundario elegido falla durante una interrupción del servicio, se elegirá otro broker secundario para que le releve, y los VDA se registrarán en el broker secundario que acaba de elegirse.

Durante una interrupción, si se reinicia un Cloud Connector:

- Si ese Cloud Connector no es el broker elegido, el reinicio no tiene repercusión.
- Si ese Cloud Connector sí es el broker elegido, se elegirá otro Cloud Connector y los VDA deberán registrarse en él. Después de que el Cloud Connector reiniciado se encienda, se hace cargo automáticamente de la intermediación, por lo que los VDA deben volver a registrarse. En este caso, el rendimiento puede verse afectado durante los registros.

El registro de eventos proporciona información sobre las opciones elegidas.

### Lo que no está disponible durante una interrupción y otras diferencias

No hay límites de tiempo impuestos para el funcionamiento en modo de interrupción. Sin embargo, si la interrupción se debe a la pérdida de la conectividad de Citrix Cloud con su ubicación de recursos, se recomienda restaurar la conectividad de la ubicación de recursos lo más rápido posible.

Durante una interrupción:

- Durante un evento de caché de host local, es posible que no se pueda acceder temporalmente a la interfaz de Configuración completa. Si se puede acceder a la interfaz de Configuración completa, los VDA de las ubicaciones de recursos que funcionan en modo de alta disponibilidad aparecen como no registrados en la interfaz de Configuración completa. Se puede acceder a estos VDA a través de la caché de host local.
- Tiene acceso limitado al SDK de PowerShell remoto.
  - Primero debe:
    * Agregar una clave del Registro `EnableCssTestMode` con un valor de 1: `New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name EnableCssTestMode -PropertyType DWORD -Value 1`
    * Establecer la autenticación del SDK en `OnPrem` para que el proxy del SDK no intente redirigir las llamadas de cmdlet: `$XDSDKAuth="OnPrem"`
    * Utilizar el puerto 89: `Get-BrokerMachine -AdminAddress localhost:89 | Select MachineName, ContollerDNSName, DesktopGroupName, RegistrationState`
  - Después de ejecutar esos comandos, puede acceder a:
    * Todos los cmdlets `Get-Broker*`.
- Los datos de supervisión no se envían a Citrix Cloud durante una interrupción. Por lo tanto, las funciones de **Supervisar** no mostrarán actividad durante una interrupción del servicio.
- Host Service no puede proporcionar credenciales de hipervisor. Todas las máquinas están en el estado de energía desconocido (unknown) y no se pueden emitir operaciones de administración de energía. No obstante, las máquinas virtuales del host que estén encendidas se pueden utilizar para las solicitudes de conexión.
- Una máquina asignada solo se puede usar si la asignación se dio durante el funcionamiento normal. No se pueden realizar asignaciones nuevas durante una interrupción del servicio.
- No se puede configurar ni inscribir automáticamente las máquinas de acceso con Remote PC. En cambio, las máquinas que se inscribieron y configuraron durante el funcionamiento normal se pueden usar.
- Si los recursos están en zonas diferentes, es posible que los usuarios de aplicaciones y escritorios alojados en servidores superen la cantidad de sesiones indicadas en el límite configurado de sesiones.
- Cada zona actúa de forma independiente durante un evento de caché de host local. Durante una interrupción del servicio, no se admiten inicios entre zonas (desde un broker de una zona en un VDA de otra zona). Use la función de comprobación de estado avanzada de StoreFront para dirigir las solicitudes de inicio a la zona adecuada durante un evento de caché de host local.

- Si se produce una interrupción de la base de datos del sitio antes de que comience un reinicio programado para los agentes VDA de un grupo de entrega, los reinicios comienzan cuando finaliza la interrupción del servicio. Esto puede provocar resultados imprevistos. Para obtener más información, consulte Reinicios programados que se retrasan por una interrupción de la base de datos.
- La preferencia de zonas no puede configurarse. Si se configura, no se tienen en cuenta las preferencias para el inicio de sesión.
- Las restricciones por etiquetas en las que se utilizan etiquetas para designar ubicaciones de recursos no se admiten para el inicio de sesiones. Cuando se configuran tales restricciones por etiquetas y la opción de comprobación avanzada de estado de un almacén de StoreFront está habilitada, es posible que las sesiones no consigan iniciarse de forma intermitente.

## Requisito de StoreFront

Si usa una implementación local de StoreFront, debe agregar a StoreFront todos los Cloud Connectors que tengan (o puedan tener) VDA registrados en ellos como Delivery Controllers. Un Cloud Connector que no se agrega a StoreFront no puede pasar al modo de interrupción del servicio, lo que podría provocar errores en el inicio del usuario.

### Disponibilidad de recursos

Puede garantizar la disponibilidad de recursos (aplicaciones y escritorios) durante una interrupción de servicio de dos maneras:

- Publique los recursos en todas las ubicaciones de recursos de la implementación.
- Si utiliza StoreFront 1912 CU4 o una versión posterior, publique los recursos en al menos una ubicación de recursos y active la comprobación avanzada de estado en todos los servidores StoreFront. En las versiones anteriores a StoreFront 2308, la comprobación avanzada de estado está desactivada de forma predeterminada y debe habilitarla un administrador. Para la versión 2308 y posteriores de StoreFront, esta función está habilitada de forma predeterminada. Para obtener más información e instrucciones sobre cómo activar la comprobación avanzada de estado, consulte comprobación avanzada de estado.

## Compatibilidad con aplicaciones y escritorios

LHC admite los siguientes tipos de VDA y modelos de entrega:

| Tipo de VDA | Modelo de entrega | Disponibilidad de los VDA durante los eventos LHC |
|---|---|---|
| SO multisesión | Aplicaciones y escritorios | Siempre disponible. |
| Sistema operativo de sesión única estático (asignado) | Escritorios | Siempre disponible. |
| Sistema operativo de sesión única con administración de energía aleatorio (agrupado) | Escritorios | No está disponible de forma predeterminada. De forma predeterminada, fallarán todos los intentos de iniciar sesión en los VDA con administración de |

> **Nota:**
>
> Permitir el acceso a los VDA de escritorio con administración de energía en grupos de entrega agrupados no afecta al funcionamiento de la propiedad `ShutdownDesktopsAfterUse` configurada durante las operaciones normales. Cuando se habilita el acceso a estos escritorios en el modo LHC, los VDA no se reinician automáticamente una vez finalizado el evento de LHC. Los VDA de escritorio con administración de energía de los grupos de entrega agrupados pueden retener los datos de las sesiones anteriores hasta que se reinicie el VDA. El reinicio del VDA puede producirse cuando un usuario cierra sesión en el VDA durante operaciones ajenas al LHC o cuando los administradores reinician el VDA.

**Importante:** Habilitar el acceso a máquinas agrupadas de sesión única con administración de energía puede provocar que los datos y los cambios de las sesiones de usuario anteriores estén presentes en las sesiones posteriores.

### Habilite el LHC para los VDA agrupados de SO de sesión única con administración de energía mediante la Configuración completa

Con la Configuración completa, puede hacer que esas máquinas estén disponibles para nuevas conexiones durante los eventos de LHC para los grupos de entrega que seleccione:

- Para habilitar esta función durante la creación de grupos de entrega, consulte Crear grupos de entrega.
- Para habilitar esta función para un grupo de entrega existente, consulte Administrar grupos de entrega

> **Nota:**
>
> Este parámetro solo está disponible en Configuración completa para los grupos de entrega de escritorios agrupados que entregan VDA con administración de energía.

### Habilitar LHC para los VDA agrupados de SO de sesión única con administración de energía mediante PowerShell

Para habilitar LHC para los VDA en un grupo de entrega específico, siga estos pasos:

1. Ejecute este comando para habilitar esta función para todo el sitio:

   ```
   Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
   ```

2. Ejecute este comando con un nombre del grupo de entrega especificado para habilitar LHC para ese grupo de entrega:

   ```
   Set-BrokerDesktopGroup -Name "name"-ReuseMachinesWithoutShutdownInOutage
    $true
   ```

Para cambiar la disponibilidad de LHC predeterminada para los grupos de entrega agrupados recién creados con agentes VDA con administración de energía, ejecute el siguiente comando:

```
Set-BrokerSite -DefaultReuseMachinesWithoutShutdownInOutage $true
```

### Verificar que la Caché de host local está funcionando

Consulte cómo verificar que la Caché de host local está configurada correctamente.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Para verificar que la Caché de host local está configurada y funciona correctamente:

- Si usa StoreFront, compruebe que la implementación local de StoreFront apunte a todos los Cloud Connectors de esa ubicación de recursos.
- Compruebe que las importaciones de sincronización se completan correctamente. Verifique los registros de eventos.
- Compruebe que la base de datos de la Caché de host local se haya creado en cada Cloud Connector. Eso confirma que el servicio de alta disponibilidad High Availability Service puede tomar el control, si fuera necesario.
  - En el servidor de Cloud Connector, vaya a `c:\Windows\ServiceProfiles\NetworkService`.
  - Compruebe que se hayan creado `HaDatabaseName.mdf` y `HaDatabaseName_log.ldf`.
- Fuerce una interrupción en todos los Cloud Connectors de la ubicación de recursos. Una vez que haya verificado que la Caché de host local funciona, recuerde volver a colocar todos los Cloud Connectors de nuevo en el modo normal. Esto puede tardar aproximadamente 15 minutos.

### Registros de eventos

Los registros de eventos indican cuándo tienen lugar las sincronizaciones y las interrupciones. En los registros del visor de eventos, el modo de interrupción se conoce como *modo de alta disponibilidad (HA)*.

**Config Synchronizer Service (Servicio de sincronización de configuraciones)**

Durante las operaciones normales, pueden producirse los siguientes eventos cuando el servicio CSS importa los datos de configuración en la base de datos de la Caché de host local a través del broker correspondiente.

- 503: Citrix Config Sync Service recibió una configuración actualizada. Este evento ocurre cada vez que se recibe una configuración actualizada de Citrix Cloud. Indica el inicio del proceso de sincronización.
- 504: Citrix Config Sync Service importó una configuración actualizada. La importación de la configuración se completó correctamente.
- 505: Falló una importación de Citrix Config Sync Service. La importación de la configuración no se completó correctamente. Si hay una configuración previa disponible, se utiliza si ocurre una interrupción. Sin embargo, estará desactualizada frente a la configuración actual. Si no hay ninguna configuración previa disponible, el servicio no puede participar en la intermediación de sesiones durante una interrupción. En este caso, consulte la sección Solucionar problemas y póngase en contacto con la asistencia de Citrix.
- 507: Citrix Config Sync Service abandonó una importación porque el sistema está en modo de interrupción del servicio y el broker de la Caché de host local se está utilizando para la intermediación. El servicio recibió una nueva configuración, pero la importación fue abandonada debido a una interrupción. Este es el comportamiento esperado.
- 510: No se recibieron datos de configuración del servicio de configuración procedentes del servicio de configuración principal.
- 517: Hubo un problema de comunicación con el broker principal.
- 518: Se ha abortado el script de Config Sync porque el Broker secundario (High Availability Service) no se está ejecutando.

**High Availability Service (Servicio de alta disponibilidad)**

Este servicio también se conoce como broker de la Caché de host local.

- 3502: Se ha producido una interrupción y el broker de la Caché de host local está llevando a cabo operaciones de intermediación.
- 3503: Se ha resuelto una interrupción y se ha reanudado el funcionamiento normal.
- 3504: Indica el broker de la Caché de host local elegido, además de otros brokers de caché de host local que hayan participado en la elección.
- 3507: Proporciona una actualización de estado de la memoria caché de host local cada 2 minutos, lo que indica que el modo de caché de host local está activo en el intermediario elegido. Contiene un resumen de la interrupción del servicio, que incluye la duración de la interrupción, el registro de VDA e información de la sesión.

- 3508: Anuncia que la memoria caché de host local ya no está activa en el intermediario elegido y que se han restablecido las operaciones normales. Contiene un resumen de la interrupción del servicio, que incluye la duración de la interrupción, la cantidad de máquinas que se registraron durante el evento de caché de host local y la cantidad de inicios correctos durante dicho evento.
- 3509: Notifica que la memoria caché de host local está activa en los intermediarios no elegidos. Contiene una duración de interrupción del servicio cada 2 minutos e indica el intermediario elegido.
- 3510: Anuncia que la memoria caché de host local ya no está activa en los intermediarios no elegidos. Contiene la duración de la interrupción del servicio e indica el intermediario elegido.

#### Proveedor de broker remoto

Este servicio actúa como un proxy entre Citrix Cloud y sus VDA y Cloud Connectors.

- 3001: Comprueba si los Cloud Connectors deben entrar en el modo de alta disponibilidad. Este evento se produce después de una única comprobación fallida del estado del Cloud Connector. Si se produce otro error en una comprobación de estado transcurridos 60 segundos, el Cloud Connector pasa al modo de alta disponibilidad.
- 3002: Notifica que el Cloud Connector no puede entrar en el modo de alta disponibilidad. El motivo por el que no se entra en el modo de alta disponibilidad se incluye en la información del evento.
- 3003: Notifica que el Cloud Connector está pasando por varios estados del modo de alta disponibilidad. Este diagrama describe los estados para entrar y salir del modo de alta disponibilidad. El evento proporciona detalles sobre:
  - El estado desde el que se está realizando la transición del Cloud Connector.
  - El estado al que está cambiando el Cloud Connector.
  - La duración del estado anterior.

> **Nota:**
>
> Puede que vea con frecuencia eventos 3001 en sus Cloud Connectors. Estos eventos pueden deberse a problemas en la red y no son motivo de preocupación.

### Forzar una interrupción del servicio

Puede que quiera forzar deliberadamente una interrupción.

- Si la red tiene altibajos repetidos. Forzar una interrupción hasta que se resuelvan los problemas de red impide una transición continua entre los modos normal y de interrupción (con las avalanchas de registros de VDA que ello conlleva).

- Para probar un plan de recuperación ante desastres.
- Para comprobar que la Caché de host local funciona correctamente.

Aunque los Cloud Connectors se puedan actualizar durante una interrupción forzada del servicio, puede haber problemas imprevistos. Se recomienda establecer una programación para las actualizaciones de Cloud Connector que eviten forzar intervalos en modo de interrupción del servicio.

Para forzar una interrupción, modifique el Registro de cada servidor de Cloud Connector. En `HKLM\Software\Citrix\DesktopServer\LHC`, cree y establezca `OutageModeForced` como `REG_DWORD` con el valor `1`. Este parámetro indica al broker de la Caché de host local que se coloque en el modo de interrupción, independientemente del estado de la conexión a Citrix Cloud. Establecer este valor en `0` saca al broker de la Caché de host local del modo de interrupción del servicio.

Para comprobar los eventos, supervise el archivo de registros `Current_HighAvailabilityService` que hay en `C:\ProgramData\Citrix\workspaceCloud\Logs\Plugins\HighAvailabilityServ` .

### Solucionar problemas técnicos

Existen varias herramientas de solución de problemas disponibles cuando falla una importación de sincronización a la base de datos de la Caché de host local y se publica un evento 505.

**Rastreo CDF**: Contiene opciones para los módulos ConfigSyncServer y BrokerLHC. Esas opciones, junto con otros módulos de broker, pueden identificar el problema.

**Informe**: Si falla una importación de sincronización, puede generar un informe. Este informe se detiene en el objeto que causa el error. Esta funcionalidad de informe afecta a la velocidad de sincronización, por lo que Citrix recomienda inhabilitarla cuando no se use.

Para habilitar y generar un informe de seguimiento de CSS, escriba el siguiente comando:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -PropertyType DWORD -Value 1
```

El informe HTML se publica en: `C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\CitrixBrokerConfigSyncReport.html`.

Una vez generado el informe, introduzca el siguiente comando para inhabilitar la funcionalidad de informes:

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
EnableCssTraceMode -Value 0
```

### Comandos de PowerShell para la memoria caché de host local

Puede administrar la caché de host local en sus Cloud Connectors mediante comandos de PowerShell.

El módulo PowerShell se encuentra en la siguiente ubicación de los Cloud Connectors:

```
C:\Program Files\Citrix\Broker\Service\ControlScripts
```

> **Importante:**
>
> Ejecute este módulo solo en los Cloud Connectors.

**Importar módulo de PowerShell** Para importar el módulo, ejecute lo siguiente en su Cloud Connector:

```
cd C:\Program Files\Citrix\Broker\Service\ControlScripts Import-Module .\HighAvailabilityServiceControl.psm1
```

**Comandos de PowerShell para administrar la LHC** Los siguientes cmdlets le ayudan a activar y administrar el modo LHC en los Cloud Connectors.

| Cmdlets | Función |
|---|---|
| `Enable-LhcForcedOutageMode` | Ponga al intermediario en modo LHC. Los archivos de bases de datos de caché de host local debe haberlos creado correctamente ConfigSync Service para que `Enable-LhcForcedOutageMode` funcione correctamente. Este cmdlet solo fuerza a la LHC del Cloud Connector en que se ejecutó. Para que la LHC se active, este cmdlet debe ejecutarse en todos los Cloud Connectors de la ubicación de recursos. |
| `Disable-LhcForcedOutageMode` | Saque al intermediario del modo LHC. Este cmdlet solo inhabilita el modo LHC en el Cloud Connector en el que se ejecutó. `Disable-LhcForcedOutageMode` debe ejecutarse en todos los Cloud Connectors de la ubicación de recursos. |

| Cmdlets | Función |
| --- | --- |
| `Set-LhcConfigSyncIntervalOverride` | Establece el intervalo en que Citrix Config Synchronizer Service (CSS) comprueba cambios de configuración en el sitio de Citrix DaaS. El intervalo de tiempo puede oscilar entre 60 segundos (un minuto) y 3600 segundos (una hora). Este parámetro solo se aplica al Cloud Connector en el que se ejecutó. Para mantener la coherencia en todos los Cloud Connectors, considere la posibilidad de ejecutar este cmdlet en cada Cloud Connector. Por ejemplo: `Set-LhcConfigSyncIntervalOverride -Seconds 1200` |
| `Clear-LhcConfigSyncIntervalOverride` | Establece el intervalo en que Citrix Config Synchronizer Service (CSS) comprueba cambios de configuración en el sitio de Citrix DaaS en función del valor predeterminado de 300 segundos (cinco minutos). Este parámetro solo se aplica al Cloud Connector en el que se ejecutó. Para mantener la coherencia en todos los Cloud Connectors, considere la posibilidad de ejecutar este cmdlet en cada Cloud Connector. |
| `Enable-LhcHighAvailabilitySDK` | Habilita el acceso a todos los cmdlets `Get-Broker*` del Cloud Connector en que se ejecutó. |
| `Disable-LhcHighAvailabilitySDK` | Inhabilita el acceso a los comandos de Broker PowerShell en el Cloud Connector en que se ejecutó. |

**Nota:**

- Use el puerto 89 cuando ejecute los cmdlets `Get-Broker*` en el Cloud Connector. Por ejemplo:

  ```
  - Get-BrokerMachine -AdminAddress localhost:89
  ```

- Cuando no está en modo LHC, el broker de la LHC del Cloud Connector solo contiene información de configuración.
- Durante el modo LHC, el broker de la LHC del Cloud Connector elegido contiene la siguiente información:

- Estados de los recursos
- Detalles de la sesión
- Registros de VDA
- Información de configuración

### Más información

Consulte Consideraciones sobre la escala y el tamaño de la Caché de host local para obtener información sobre:

- Metodologías de pruebas y resultados
- Consideraciones sobre tamaño de RAM
- Consideraciones sobre la configuración de sockets y núcleo de CPU
- Consideraciones sobre almacenamiento

## Supervisar y administrar máquinas y sesiones con Buscar

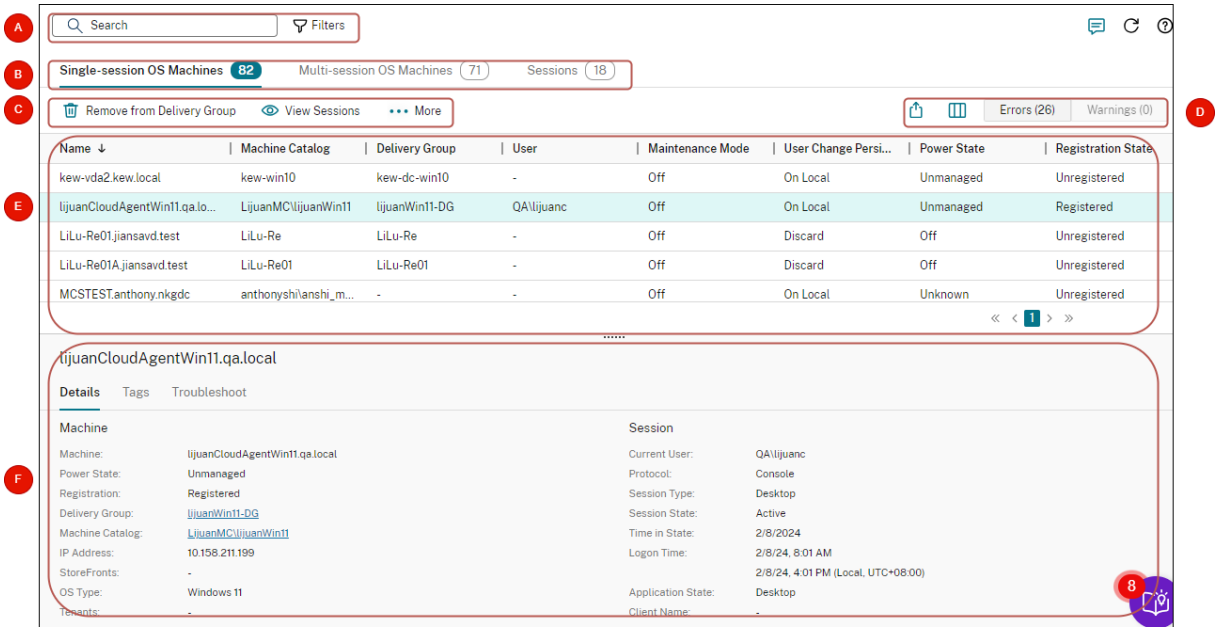
June 12, 2024

En este artículo se explica cómo supervisar y administrar las máquinas y las sesiones mediante el nodo **Configuración completa > Buscar**.

### Más información sobre el nodo

El nodo **Buscar** proporciona un lugar centralizado para supervisar y administrar las máquinas y las sesiones de usuario.




| Leyenda | Área | Descripción |
|---|---|---|
| A | Barra de búsqueda | Proporciona una búsqueda rápida y una búsqueda basada en filtros que permiten definir criterios de búsqueda complejos. Para obtener más información, consulte Búsqueda de instancias. |
| B | Fichas de tipos | Muestra fichas para enumerar las máquinas por tipo o todas las sesiones. Los recuentos de instancias aparecen en los nombres de las fichas. |
| C | Acciones en el nivel de instancia | Muestra las acciones que puede realizar en las *instancias seleccionadas* (máquinas o sesiones). Para obtener más información, consulte Acciones de máquina y Acciones de sesión. |
| D | Acciones en el nivel de lista | Muestra las acciones que puede realizar en la *lista*actual<br>-Icono **Exportar**: Exporta la lista de instancias que se muestra en la vista principal a un archivo CSV.<br>-Icono **Columna que mostrar**: Personaliza la vista principal de la lista.<br>-Etiqueta **Errores**: Habilite esta |

| Leyenda | Área | Descripción |
| --- | --- | --- |
| E | Vista principal | Muestra las instancias y sus propiedades. Puede personalizar la vista principal seleccionando el icono **Columna que mostrar**. Para obtener más información sobre las columnas disponibles, consulte Columnas de máquina y Columnas de sesión. |
| F | Recuadro Detalles | Muestra los siguientes detalles<br>Detalles de la instancia seleccionada (máquina o sesión)<br>Etiquetas aplicadas a la máquina seleccionada<br>Detalles de los errores o advertencias de la máquina seleccionada, incluidos los problemas, las posibles causas y las soluciones sugeridas |

## Búsqueda de instancias

Use la función de búsqueda para localizar máquinas y sesiones específicas.

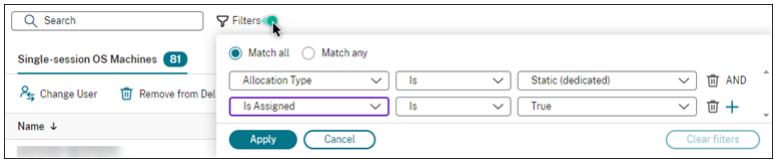
- Búsqueda mediante filtros
- Guardar el conjunto de filtros actual para una búsqueda rápida
- Anclar un campo de filtro en la barra de búsqueda
- Buscar usando el cuadro de búsqueda rápida
- Sugerencias para mejorar las búsquedas

### Búsqueda mediante filtros

Por ejemplo, para localizar todas las máquinas con sistema operativo de sesión única que son *estáticas* y están *asignadas a usuarios*, siga estos pasos:

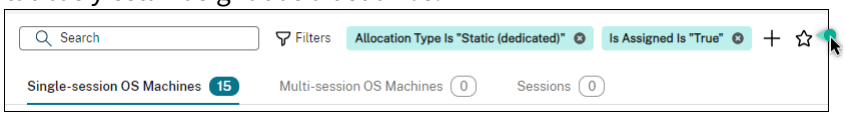
1. En la ficha **Máquinas con SO de sesión única**, haga clic en el icono **Filtros**. Aparecerá el panel Filtros.
2. Agregue los criterios de filtro necesarios.




3. Seleccione **Hacer coincidir todo** (operador AND) si quiere que la búsqueda devuelva resultados que coincidan con todos los criterios del filtro. Seleccione **Hacer coincidir cualquiera** (operador OR) si quiere que la búsqueda devuelva resultados que coincidan con cualquiera de los criterios del filtro.
4. Haga clic en **Aplicar**.

   La lista filtrada muestra todas las máquinas con sistema operativo de sesión única que son estáticas y están asignadas a usuarios.

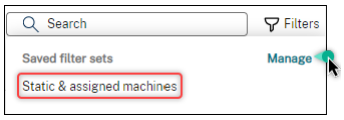



### Guardar el conjunto de filtros actual para una búsqueda rápida

Por ejemplo, para guardar el conjunto de filtros para localizar las máquinas con sistema operativo de sesión única que son estáticas y están asignadas a usuarios para su uso futuro, siga estos pasos:

1. Tras realizar una búsqueda basada en filtros, haga clic en el icono de **estrella** de la barra de búsqueda, como se muestra en la figura anterior.
2. En la página que aparece, introduzca un nombre para este conjunto de filtros (por ejemplo, *Máquinas estáticas y asignadas*).
3. Haga clic en **Guardar**.

   El conjunto de filtros guardado aparece en la lista del historial de búsqueda al hacer clic en el cuadro de búsqueda.




> **Nota:**
>
> Los conjuntos de filtros se guardan por cuenta de usuario. Para administrar los conjuntos de filtros guardados, seleccione **Administrar**.

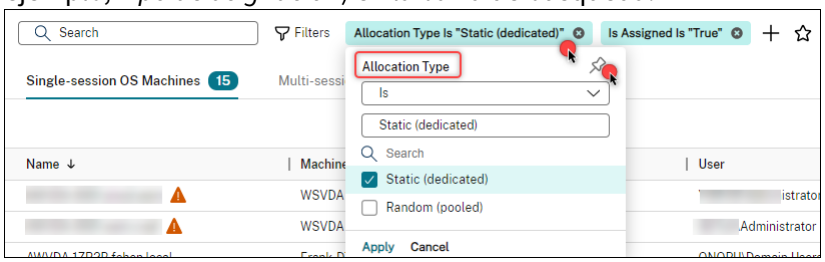
### Anclar un campo de filtro en la barra de búsqueda

Para facilitar el acceso, puede anclar *campos* de filtro de uso frecuente en la barra de búsqueda. Por ejemplo, después de realizar una búsqueda basada en filtros, puede que quiera anclar **Tipo de asi-**

**gnación** en la barra de búsqueda. Siga estos pasos:

1. Haga clic en el *parámetro del filtro* en la barra de búsqueda.
2. En el panel que aparece, haz clic en el icono de **chincheta** para anclar el campo de filtro (en este ejemplo, *Tipo de asignación*) en la barra de búsqueda.




### Buscar usando el cuadro de búsqueda rápida

El cuadro de búsqueda rápida proporciona una forma cómoda de buscar instancias en función de las propiedades relacionadas con el nombre o los conjuntos de filtros guardados. Estos son los pasos detallados:

1. Haga clic en el cuadro de búsqueda. Las búsquedas recientes y los conjuntos de filtros guardados aparecen en la lista desplegable. Puede hacer clic en una búsqueda anterior o en un conjunto de filtros para realizar una búsqueda rápida.
2. Para iniciar una nueva búsqueda, introduzca un nombre completo o parcial de una de las siguientes opciones:
   - Nombre de máquina o nombre DNS
   - Nombre de catálogo de máquinas
   - Nombre de grupo de entrega
   - Nombre de usuario de la sesión
   - Nombre del cliente de la sesión
   - Nombre descriptivo de la máquina virtual que aloja la sesión, tal como lo usa su hipervisor
   - Nombre del servidor de alojamiento

### Sugerencias para mejorar las búsquedas

Tenga en cuenta estos consejos al utilizar la función Buscar:

- En el nodo **Buscar**, seleccione cualquier columna para ordenar los elementos.
- Para mostrar más características que se deben incluir en la pantalla donde puede buscar y ordenar, seleccione **Columnas que mostrar** o haga clic en una columna y seleccione **Columnas que mostrar**. En la ventana **Columnas que mostrar**, marque la casilla de verificación situada junto a los elementos que quiere mostrar y seleccione **Guardar** para salir.

> **Nota:**
>
> Las columnas que degradan el rendimiento se marcan con la etiqueta **Degrada el rendimiento**.

- Para buscar un dispositivo de usuario conectado a una máquina, use **Cliente (IP)** y **Es** y escriba la dirección IP del dispositivo.
- Para buscar sesiones activas, use **Estado de la sesión**, **Es** y **Conectado**.
- Para mostrar todas las máquinas de un grupo de entrega, seleccione **Grupos de entrega** en el panel de la izquierda. Seleccione el grupo y, a continuación, seleccione **Ver máquinas** en la barra de acciones o en el menú contextual.

Tenga en cuenta las siguientes consideraciones al realizar operaciones de ordenación:

- Siempre que el número de elementos no supere los 5000, puede hacer clic en cualquier columna para ordenar los artículos que contiene. Cuando el número supera los 5000, solo se puede ordenar por nombre o por usuario actual (según la ficha en la que se encuentre). Para habilitar la ordenación, utilice filtros para reducir el número de artículos a 5000 o menos.
- Cuando el número de elementos es superior a 500 pero no superior a 5000:
  - Almacenamos en caché todos los datos localmente para mejorar el rendimiento de ordenación. En las fichas **Máquinas con SO de sesión única** y **Máquinas con SO multisesión**, almacenamos los datos en caché la primera vez que se hace clic en una columna (cualquier columna, excepto la columna **Nombre**) para ordenarlos. En la ficha **Sesiones**, almacenamos en caché los datos la primera vez que se hace clic en una columna (cualquier columna, excepto la columna **Usuario actual** ) para ordenarlos. Por ese motivo, la ordenación tarda más en completarse. Para lograr una mayor rapidez, ordene por nombre o usuario actual, o utilice filtros para reducir el número de elementos.
  - El siguiente mensaje bajo la tabla indica que los datos están almacenados en caché: Última actualización: <`the time when you refreshed the table`>. En ese caso, las operaciones de ordenación se basan en elementos que se han cargado anteriormente. Es posible que esos elementos no estén actualizados. Para actualizarlos, haga clic en el icono de actualización.

### Personalizar columnas que mostrar

Cree una vista principal personalizada para mostrar las propiedades y los estados cruciales para sus operaciones diarias. Estos son los pasos detallados:

1. En el nodo **Buscar**, seleccione la ficha **Máquinas con SO multisesión**, **Máquinas con SO de sesión única** o **Sesiones**, según sea necesario.

2. Haga clic en el icono **Columnas que mostrar** de la barra de acciones y seleccione las columnas.

   Para obtener más información sobre las columnas disponibles y sus descripciones, consulte Columnas de máquina y Columnas de sesión.

Al elegir columnas, podrá ver columnas marcadas con la etiqueta **Degrada el rendimiento**. Es posible que, al seleccionar esas columnas, se degrade el rendimiento de la consola. Tenga en cuenta estas consideraciones:

- Una vez completada la personalización, la tabla se actualiza para mostrar las columnas seleccionadas. Es posible que su presencia cause demoras al actualizar la tabla.
- Tras actualizar el explorador o cerrar sesión en la consola y, a continuación, iniciar sesión, aparece un mensaje en el que se pregunta si se deben conservar esas columnas. Si decide conservarlas, no podrá actualizar la tabla más de una vez por minuto para que la consola funcione de forma óptima. Para actualizaciones más frecuentes, elimine cualquier columna que degrade el rendimiento.

## Administrar máquinas y sesiones

Use las acciones del nodo Buscar para solucionar problemas de máquinas y sesiones o para procesar solicitudes de los usuarios.

### Información útil

Puede administrar las máquinas en diferentes niveles:

- En el nivel de máquina individual. Use el nodo **Buscar** para localizar las máquinas de destino y realizar acciones.
- En el nivel de catálogo de máquinas, como cambiar las imágenes maestras de un catálogo, eliminar máquinas de un catálogo y agregar máquinas a un catálogo. Para obtener más información, consulte Administrar catálogos de máquinas.
- En el nivel de grupo de entrega, como activar o desactivar el modo de mantenimiento para las máquinas de un grupo. Para obtener más información, consulte Administrar grupos de entrega.

Además del nivel de sesión individual, también puede administrar las sesiones a nivel de grupo de entrega, por ejemplo, configurar el preinicio y la duración de la sesión para un grupo de entrega. Para obtener más información, consulte Administrar de grupos de entrega.

### Realizar acciones en máquinas o sesiones

Para administrar máquinas o sesiones en el nivel de instancia individual, siga estos pasos:

1. En el nodo **Buscar**, seleccione la ficha **Máquinas con SO multisesión**, **Máquinas con SO de sesión única** o **Sesiones**.
2. Seleccione una o más instancias según sea necesario.
3. En la barra de acciones o en el menú del botón secundario, seleccione una acción en función de los problemas que encuentre con esas instancias o solicitudes de usuario.

   Para obtener más información sobre las acciones disponibles y sus descripciones, consulte Acciones de máquina y Acciones de sesión.

> **Nota:**
>
> Si selecciona dos o más instancias, solo estarán disponibles las acciones aplicables a todas ellas.

### Exportar datos de máquinas o sesiones a archivos CSV

Puede exportar la lista de instancias (máquinas o sesiones) que se muestra en una ficha (hasta 30 000 elementos) a un archivo CSV. Estos son los pasos detallados:

1. En el nodo **Buscar**, seleccione la ficha **Máquinas con SO multisesión**, **Máquinas con SO de sesión única** o **Sesiones**, según sea necesario.
2. Para ello, haga clic en el icono **Exportar** de la esquina superior derecha.
3. En el cuadro de diálogo que aparece, haga clic en **Continuar**.

   Es posible que la exportación tarde varios minutos en completarse. Puede encontrar el archivo en la carpeta de descargas predeterminada de su explorador.

> **Nota:**
>
> En las fichas del nodo **Buscar**, no puede realizar otra exportación mientras haya una exportación en curso.

## Acciones y columnas de máquina

June 12, 2024

En este artículo se enumeran las acciones y las columnas de máquina con descripciones para referencia.

### Acciones

Consulte las acciones que puede realizar en las máquinas y sus descripciones.

| Acción | Descripción | Aplicable a |
|---|---|---|
| Realizar comprobación de estado | Disponible solamente para VDA con Windows registrados, con la versión 2019 o una posterior. Realice una comprobación del estado de una máquina. Para obtener más información sobre el contenido de las comprobaciones, consulte Acerca de las comprobaciones de estado. | Sesión única y multisesión |
| Quitar del grupo de entrega | Quite una máquina de un grupo de entrega. | Sesión única y multisesión |
| Agregar a grupo de entrega | Agregue una máquina a un grupo de entrega. | Sesión única y multisesión |
| Ver sesiones | Consulte las sesiones que se están ejecutando en una máquina | Sesión única y multisesión |
| Administrar etiquetas | Agregue y administre las etiquetas de una máquina. Para obtener más información sobre los casos de uso típicos de las etiquetas, consulte Etiquetas. | Sesión única y multisesión |
| Activar modo de mantenimiento | Puede poner una máquina en modo de mantenimiento antes de aplicar parches o para solucionar problemas. | Sesión única y multisesión |

| Acción | Descripción | Aplicable a |
| --- | --- | --- |
| | Este modo impide que se establezcan nuevas conexiones con esa máquina. Los usuarios pueden conectarse a las sesiones existentes de esa máquina, pero no pueden iniciar nuevas sesiones en la misma. | |
| Desactivar modo de mantenimiento | Desactive el modo de mantenimiento de una máquina. | Sesión única y multisesión |
| Actualizar versión de VDA | Actualice la versión del agente VDA de una máquina. | Máquinas con sistema operativo de sesión única o multisesión que cumplen ciertos requisitos: Más información. |
| Cerrar sesión | Fuerce el cierre de sesión de una máquina | Sesión única y multisesión |
| Eliminar | Elimine una máquina virtual de un catálogo de máquinas mientras la deja intacta en el hipervisor o el servicio de nube. | Sesión única y multisesión |
| Cambiar usuario | Asigne una máquina a un usuario específico. | Máquinas *estáticas* de sesión única. |
| Iniciar | Inicie una máquina. | Sesión única y multisesión |
| Apagar | Apague una máquina. | Sesión única y multisesión |
| Reiniciar | Reinicie una máquina | Sesión única y multisesión |
| Suspender | Ponga una máquina en estado de hibernación o suspensión. Cuando suspende una máquina, DaaS almacena el contenido en memoria de esa máquina en un archivo y, a continuación, la apaga. | Máquinas con SO de sesión única |

| Acción | Descripción | Aplicable a |
| --- | --- | --- |
| Reanudar | Reanude una máquina suspendida. Cuando reanuda una máquina suspendida, DaaS la inicia y la restaura al estado anterior. | Máquinas con SO de sesión única |
| Forzar reinicio | Fuerce el reinicio de una máquina. | Máquinas con SO de sesión única |
| Forzar apagado | Fuerce el apagado de una máquina. | Máquinas con SO de sesión única |

## Columnas

Vea todas las columnas de una máquina y sus descripciones por tipo:

- Máquina
- Detalles de la máquina
- Aplicaciones
- Alojamiento
- Conexión
- Registro
- Detalles de la sesión
- Sesión

### Máquina

Columnas de la categoría **Máquina**.

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Nombre | El nombre de host DNS de la máquina. | Sesión única y multisesión |
| Catálogo de máquinas | El nombre del catálogo al que pertenece la máquina. | Sesión única y multisesión |
| Grupo de entrega | El nombre del grupo de entrega al que pertenece la máquina. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Nombre simplificado de usuario | Los nombres completos de los usuarios asociados a la máquina (normalmente con el formato `Firstname Lastname`). Los usuarios asociados son los usuarios actuales de las máquinas compartidas y los usuarios asignados de las máquinas dedicadas. | Sesión única y multisesión |
| Usuario | Los nombres de usuario de los usuarios asociados a la máquina (con el formato "dominio\ usuario"). Los usuarios asociados son los usuarios actuales de las máquinas compartidas y los usuarios asignados de las máquinas dedicadas. | Sesión única y multisesión |
| Nombre principal del usuario | Los nombres principales de usuario de los usuarios asociados a la máquina (con el formato "usuario @dominio"). Los usuarios asociados son los usuarios actuales de las máquinas compartidas y los usuarios asignados de las máquinas dedicadas. | Sesión única y multisesión |
| Nombre simplificado de escritorio | El nombre publicado de la máquina usada originalmente para iniciar la sesión. Es el nombre que aparece en la aplicación Citrix Workspace o StoreFront. | Solo sesión única |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| | **Nota:** Para cambiar la pantalla de un escritorio, necesita el permiso **Realizar actualización de máquina**, ya que el cambio del nombre de la pantalla implica actualizar la propiedad de la máquina. | |
| Condiciones de escritorio | La lista de condiciones particulares de escritorio para la máquina. Valores posibles: Desconocido, CPU, ICALatency y UPMLogonTime. | Sesión única y multisesión |
| Tipo de asignación | El tipo de asignación de la máquina: **Permanente**, cuando se asigna a un usuario de forma permanente. **Aleatoria**, cuando se asigna de forma aleatoria. | Sesión única y multisesión |
| Modo de mantenimiento | Indica si la máquina está en modo de mantenimiento. | Sesión única y multisesión |
| Parámetro de conexión de Windows | Modo de inicio de sesión notificado por Windows. Valores posibles: LogonEnabled, Draining, DrainingUntilRestart y LogonDisabled. | Solo multisesión |
| Está asignado | Indica si un escritorio dedicado se ha asignado a un usuario o a un cliente (nombre/dirección). Los usuarios se pueden asignar de forma explícita o mediante la asignación en el primer uso de la máquina. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Es físico | Indica si la máquina es física o no. `True` indica que la máquina es física, lo que significa que DaaS no administra la energía. `False` indica lo contrario. | Sesión única y multisesión |
| Tipo de aprovisionamiento | Cómo se aprovisionó la máquina. Valores posibles<br>Manual: No se aprovisiona mediante PVS o MCS.<br>PVS: Se aprovisiona mediante PVS (máquinas físicas, blade y virtuales)<br>MCS: Se aprovisiona mediante MCS (solo máquinas virtuales) | Sesión única y multisesión |
| Reinicio programado | El estado de cualquier operación de reinicio programada para la máquina. Valores posibles<br>Ninguno: No hay ningún reinicio programado.<br>Pendiente: En espera de reiniciarse, pero disponible para nuevas sesiones. Sin embargo, aún se permiten reconexiones a las conexiones existentes.<br>En curso: Actualmente en proceso de reinicio programado.<br>Natural: Reinicio natural en curso. La máquina está a la espera de reiniciarse. | Sesión única y multisesión |
| Zona | El nombre de la zona en la que se encuentra la máquina. | Sesión única y multisesión |
| Estado | El estado general del escritorio asociado a la máquina, derivado de diversos estados específicos, como el estado de la sesión, el estado del registro y el estado de energía.<br>Posibles estados: Desactivado, Sin registrar, Disponible, Desconectado, En uso y En preparación. | Sesión única y multisesión |
| Etiquetas | La lista de etiquetas asociadas a la máquina. | Sesión única y multisesión |
| Actualización de versión de VDA | El estado de la máquina para las acciones de actualización de las versiones de los paquetes del agente VDA. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| | Valores posibles: MissingUpgradeType, UpgradeScheduled, UpgradeAvailable, UpToDate y Desconocido. | |
| Con capacidad de suspensión | Indica si la máquina admite acciones de alimentación (Suspender y Reanudar). | Sesión única y multisesión |
| Índice de carga | El índice de carga actual. Para obtener más información, consulte Más información. | Solo multisesión |
| Estado de purga | Indica si la máquina se está purgando y se apagará cuando terminen todas las sesiones en la máquina. True solo aparece en máquinas multisesión con administración de energía.<br>**Nota:** La máquina no se apaga si está en modo de mantenimiento. Se apaga solo cuando no está en el modo de mantenimiento. | Solo multisesión |

**Detalles de la máquina**

Columnas de la categoría **Detalles de la máquina**.

| **Columna** | **Descripción** | **Aplicable a** |
| --- | --- | --- |
| Versión del agente | La versión del Citrix Virtual Delivery Agent (VDA) instalada en la máquina. | Sesión única y multisesión |
| Dirección IP | La dirección IP de la máquina. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Está asignado | Indica si un escritorio dedicado se ha asignado a un usuario o a un cliente (nombre/dirección). Los usuarios se pueden asignar de forma explícita o mediante la asignación en el primer uso de la máquina. | Sesión única y multisesión |
| Tipo de SO | El sistema operativo que se ejecuta en la máquina. | Solo sesión única |

**Aplicaciones**

Columnas de la categoría **Aplicaciones**.

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Aplicación en uso | La lista de aplicaciones en uso en la máquina (se muestran como nombres de explorador). | Sesión única y multisesión |
| Aplicaciones publicadas | La lista de aplicaciones publicadas por la máquina (se muestran como nombres de explorador). | Sesión única y multisesión |

**Conexiones**

Columnas de la categoría **Conexiones**.

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Cliente (IP) | La dirección IP del cliente conectado a la máquina. | Solo sesión única |
| Cliente | El nombre de host del cliente conectado a la máquina. | Solo sesión única |
| Versión del plug-in | La versión de la aplicación Citrix Workspace en el cliente conectado. | Solo sesión única |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Conectado | El nombre de host de la conexión entrante, normalmente una puerta de enlace, un enrutador o un cliente. | Solo sesión única |
| Conectado (IP) | La dirección IP de la conexión entrante, normalmente una puerta de enlace, un enrutador o un cliente. | Solo sesión única |
| Tipo de conexión | El protocolo usado para la sesión. Valores posibles: HDX, RDP y Consola. Nota: El campo se deja en blanco para las sesiones de consola en los VDA de XenDesktop 5. | Solo sesión única |
| Última conexión (UTC) | La hora del último intento de conexión detectado que falló o tuvo éxito. | Sesión única y multisesión |
| Usuario de la última conexión | El nombre SAM (con el formato "DOMINIO\usuario") del usuario que intentó conectarse a la máquina por última vez. Si el nombre SAM no está disponible, se usa el SID. | Sesión única y multisesión |
| Secure ICA activo | Indica si SecureICA está activo en la sesión actual. Siempre es nulo para máquinas multisesión. | Sesión única y multisesión |

**Alojamiento**

Columnas de la categoría **Alojamiento**.

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| VM | El nombre descriptivo de una máquina alojada que ejecuta la sesión, tal como lo usa su hipervisor. No tiene por qué coincidir necesariamente con el nombre DNS o AD de la máquina. | Sesión única y multisesión |
| Nombre del servidor de alojamiento | El nombre DNS del hipervisor que está alojando la máquina si está administrada. | Sesión única y multisesión |
| Conexión | El nombre de la conexión de host asignada a la máquina que aloja la sesión. | Sesión única y multisesión |
| Actualización pendiente | Indica si la imagen de máquina virtual de una máquina hospedada no está actualizada y se actualizará con una nueva imagen en el próximo reinicio de la máquina. | Sesión única y multisesión |
| Persistencia de cambios de usuario | Indica cómo se gestionan los cambios de usuario y si estos cambios son persistentes<br>Local: Persistentes. Los cambios de usuario se guardan localmente.<br>Descartar: No persistentes. Los cambios de usuario se descartan. | Sesión única y multisesión |
| Acción de energía pendiente | Indica si hay alguna acción de energía pendiente para la máquina. | Sesión única y multisesión |
| Estado de energía | El estado de energía de la máquina. Valores posibles: No administrado, Desconocido, No disponible, Desactivado, Activado, Suspendido, Iniciándose, Apagándose, Suspendiéndose y Reanudándose. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Se apagará después de usarse | Solo se aplica a máquinas de sesión única con administración de energía. Indica si la máquina está contaminada y se apagará cuando finalicen todas las sesiones.<br>**Nota:** La máquina no se apagará si está en modo de mantenimiento. Se apagará solo después de salir del modo de mantenimiento. | Solo sesión única |

**Registro**

Columnas de la categoría **Registro** .

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Último fallo de registro | El motivo de la última cancelación del registro de la máquina con el broker. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| | Los valores posibles son: AgentShutdown, AgentSuspended, AgentRequested, IncompatibleVersion, AgentAddressResolutionFailed, AgentNotContactable, AgentWrongActiveDirectoryOU, EmptyRegistrationRequest, MissingRegistrationCapabilities, MissingAgentVersion, InconsistentRegistrationCapabilities, NotLicensedForFeature, UnsupportedCredentialSecurityVersion, InvalidRegistrationRequest, SingleMultiSessionMismatch, FunctionalLevelTooLowForCatalog, FunctionalLevelTooLowForDesktopGroup, PowerOff, DesktopRestart, DesktopRemoved, AgentRejectedSettingsUpdate, SendSettingsFailure, SessionAuditFailure, SessionPrepareFailure, ContactLost, SettingsCreationFailure, UnknownError y BrokerRegistrationLimitReached. | |
| Hora de último fallo de registro (UTC) | La hora de la última cancelación del registro de la máquina. | Sesión única y multisesión |

| Columna | Descripción | Aplicable a |
| --- | --- | --- |
| Estado de registro | El estado de registro de la máquina. Valores posibles: Sin registrar, Inicializando, Registrado y Error del agente. | Sesión única y multisesión |
| Estado de fallo | El estado resumido de cualquier estado de fallo actual de la máquina. Valores posibles Ninguno: Sin fallos. La máquina está en buen estado. No se inició: Falló la última operación de encendido de la máquina. Atascado en arranque: La máquina no se pudo iniciar después de encenderse. Sin registrar. La máquina no se ha registrado en el período previsto o se ha rechazado su registro. Capacidad máxima. La máquina informa que está a su máxima capacidad. | Sesión única y multisesión |

**Detalles de la sesión**

Columnas de la categoría **Detalles de la sesión**.

| **Columna** | **Descripción** | **Aplicable a** |
| --- | --- | --- |
| Iniciado | El nombre de host del servidor de StoreFront usado para iniciar la sesión de intermediación con broker actual. Siempre es nulo para máquinas multisesión. | Sesión única y multisesión |
| Iniciado (IP) | La dirección IP del servidor de StoreFront usada para iniciar la sesión de intermediación con broker actual. Siempre es nulo para máquinas multisesión. | Sesión única y multisesión |
| Hora de cambio de sesión (UTC) | La hora del último cambio de estado de la sesión actual. | Solo sesión única |
| Filtros SmartAccess | Etiquetas Smart Access para la sesión actual. Siempre es nulo para máquinas multisesión. | Sesión única y multisesión |

### Sesión

Columnas de la categoría **Sesión**.

| Columna | Descripción | Aplicable a |
|---|---|---|
| Estado de la sesión | El estado de la sesión actual. Valores posibles: Otro, Preparando sesión, Conectado, Activo, Desconectado, Reconectando, Sesión sin broker y Desconocido. | Solo sesión única |
| Usuario actual | El nombre del usuario de la sesión actual (con el formato "DOMINIO\usuario"). | Solo sesión única |
| Inicio (UTC) | Hora de inicio de la sesión actual. | Solo sesión única |
| Recuento de sesiones | El número de sesiones en la máquina. | Solo multisesión |

## Acciones y columnas de sesión

June 12, 2024

En este artículo se enumeran las acciones y las columnas de máquina con descripciones para referencia.

### Acciones

Vea las acciones que puede realizar en las sesiones y sus descripciones.

| Acción | Descripción | Se aplica a sesiones de |
|---|---|---|
| Cerrar sesión | Cierra la sesión de un usuario. | Máquinas con SO de sesión única o máquinas con SO multisesión. |

| Acción | Descripción | Se aplica a sesiones de |
|---|---|---|
| Enviar mensaje | Envía un mensaje al usuario de una sesión. | Máquinas con SO de sesión única o máquinas con SO multisesión. |
| Ver máquinas | Muestra la máquina host de una sesión. | Máquinas con SO de sesión única o máquinas con SO multisesión. |
| Desconectar | Desconecta una sesión. Si una sesión se desconecta, la sesión permanece activa y sus aplicaciones siguen ejecutándose, pero el dispositivo de usuario ya no se comunica con DaaS. | Máquinas con SO de sesión única o máquinas con SO multisesión. |
| Apagar máquina | Apaga la máquina asociada a una sesión. | Máquinas con SO de sesión única |
| Reiniciar máquina | Reinicia la máquina asociada a una sesión. | Máquinas con SO de sesión única |

### Columnas

Consulte las columnas de la sesión y sus descripciones.

| Columna | Descripción |
|---|---|
| Usuario actual | El nombre del usuario; el nombre principal de usuario (UPN) del usuario. |
| Nombre | El nombre de host DNS de la máquina que aloja la sesión. |
| Grupo de entrega | El nombre del grupo de entrega que contiene la máquina que aloja la sesión. |
| Catálogo de máquinas | El nombre del catálogo de máquinas que contiene la máquina que aloja la sesión. |
| Versión del agente | La versión del Citrix Virtual Delivery Agent (VDA) instalada en la máquina que aloja la sesión. |
| Aplicación en uso | La lista de aplicaciones en uso en la sesión, identificadas por sus nombres administrativos. |

| Columna | Descripción |
| --- | --- |
| Con broker autónomo | Si se trata de una sesión HDX establecida mediante una conexión directa sin intermediación con broker. |
| Hora de broker (UTC) | La hora en la que se intermedió la sesión. |
| Nombre de usuario de broker | El nombre del usuario broker. |
| Cliente (IP) | La dirección IP del cliente conectado a la sesión. |
| Cliente | El nombre de host del cliente conectado a la sesión. |
| Versión del plug-in | La versión de la aplicación Citrix Workspace que se ejecuta en el cliente conectado a la sesión. |
| Conectado | El nombre de host de las conexiones entrantes, normalmente una puerta de enlace, un enrutador o un cliente. |
| Conectado (IP) | La dirección IP de la conexión entrante, normalmente una puerta de enlace, un enrutador o un cliente. |
| Tipo de asignación | Si la sesión es compartida o dedicada. |
| Oculto | Si la sesión está oculta para el usuario y no se va a volver a conectar a ella. |
| VM | El nombre descriptivo de la máquina virtual que aloja la sesión, tal como lo usa su hipervisor. No tiene por qué coincidir necesariamente con el nombre DNS o AD de la máquina. |
| Nombre del servidor de alojamiento | El nombre DNS del hipervisor que aloja la máquina en la que se ejecuta la sesión. |
| Conexión | El nombre de la conexión de host asignada a la máquina que aloja la sesión. |
| Actualización pendiente | Si la imagen de máquina virtual de una máquina hospedada no está actualizada y se actualizará con una nueva imagen en el próximo reinicio de la máquina. |
| Modo de mantenimiento | Si la máquina que aloja la sesión está en modo de mantenimiento. |
| Dirección IP | La dirección IP de la máquina que aloja la sesión. |

| Columna | Descripción |
| --- | --- |
| Es físico | Si la máquina que aloja la sesión es física o no. `True` indica que la máquina es física, lo que significa que DaaS no administra la energía. `False` indica lo contrario. |
| Iniciado | El nombre de host del servidor de StoreFront usado para iniciar la sesión. Está en blanco si la sesión se inició a través de Workspace. |
| Iniciado (IP) | La dirección IP del servidor de StoreFront usado para iniciar la sesión. Está en blanco si la sesión se inició a través de Workspace. |
| Tipo de SO | La cadena de identificación del sistema operativo que aloja la sesión. |
| Persistencia de cambios de usuario | Indica cómo se gestionan los cambios de usuario y si estos cambios son persistentes<br>Local: Persistentes. Los cambios de usuario se guardan localmente.<br>Descartar: No persistentes. Los cambios de usuario se descartan. |
| Tipo de conexión | El protocolo usado para la sesión, como HDX, RDP o Consola. **Nota:** El campo está en blanco para las sesiones de consola en los VDA de XenDesktop 5. |
| Tipo de aprovisionamiento | Cómo se aprovisionó la máquina que aloja la sesión<br>Manual: No se aprovisiona mediante PVS o MCS.<br>PVS: Se aprovisiona con PVS (máquinas físicas, blade y virtuales).<br>MCS: Se aprovisiona con MCS (solo máquinas virtuales). |
| Secure ICA activo | Si SecureICA está activo en la sesión. |
| Estado de la sesión | El estado de la sesión. Valores posibles: Conectado, Activo o Desconectado. Puede haber otros estados para las sesiones en máquinas con niveles funcionales anteriores a L7, como Preparando sesión, Reconectando, Sesión sin broker, Otro y Desconocido. |
| Hora de cambio de sesión | La hora del último cambio de estado de la sesión. |
| Estado de la aplicación | El estado de las aplicaciones de la sesión. Valores posibles: Preinicio de sesión, Preiniciada, Activa, Escritorio, Persistente y NoApps. |

| Columna | Descripción |
| --- | --- |
| Respaldo para la sesión | Si la máquina que aloja la sesión admite sesiones únicas o multisesión. |
| Zona | Nombre de la zona en la que se encuentra la máquina que aloja la sesión. |
| Filtros SmartAccess | Etiquetas Smart Access para la sesión. |
| Inicio (UTC) | Cuándo se inició la sesión. |
| Estado | El estado resumido de la máquina. Valores posibles: Sin registrar, Desconectada o En uso. |
| Tiempo en este estado (UTC) | Cuánto tiempo ha estado la sesión en su estado actual. |
| Delivery Controller | El nombre de host DNS del controlador en el que está registrada la máquina que aloja la sesión. |
| Nombre simplificado de usuario | El nombre completo del usuario. |
| Nombre simplificado de escritorio | El nombre publicado de la máquina usada originalmente para iniciar la sesión. Es el nombre que aparece en la aplicación Citrix Workspace o StoreFront. En el caso de las sesiones de aplicación, es el nombre de la primera aplicación que se inició en la sesión, incluso si esa aplicación ha finalizado. El nombre se mantiene sin cambios aunque el recurso cambie de nombre o se elimine más adelante. |

## Administrar las claves de seguridad

April 12, 2023

> **Nota:**
>
> - Debe utilizar esta función en combinación con StoreFront 1912 LTSR CU2 o una versión posterior.
> - La función Secure XML se admite solo en Citrix ADC y Citrix Gateway 12.1 y versiones posteriores.

Esta función permite especificar que solo las máquinas StoreFront y Citrix Gateway aprobadas se co-

muniquen con los Delivery Controllers de Citrix. Después de habilitar esta función, se bloquearán todas las solicitudes que no contengan la clave. Utilice esta función para agregar una capa adicional de seguridad y protegerse contra ataques que se originen en la red interna.

He aquí un flujo de trabajo general para utilizar esta función:

1. Muestre la configuración de clave de seguridad en la interfaz de Configuración completa. (Utilice el SDK de PowerShell remoto)
2. Configure los parámetros para su implementación. (Use la interfaz de Configuración completa o el SDK de PowerShell remoto).
3. Configure los parámetros en StoreFront (utilice PowerShell.)
4. Configure los parámetros en Citrix ADC.

### Mostrar la configuración de clave de seguridad en la interfaz de Configuración completa

De forma predeterminada, la configuración de las claves de seguridad está oculta en la interfaz de Configuración completa. Para mostrarlas en esa interfaz, utilice el SDK de PowerShell remoto. Para obtener más información sobre el SDK de PowerShell remoto, consulte SDK y API.

Estos son los pasos detallados:

1. Ejecute el SDK de PowerShell remoto.
2. En una ventana de comandos, ejecute los siguientes comandos:
   - `Add-PSSnapIn Citrix*`. Este comando agrega los complementos de Citrix.
   - `Set-ConfigSiteMetadata -Name "Citrix_DesktopStudio_SecurityKeyManageme "-Value "True"`

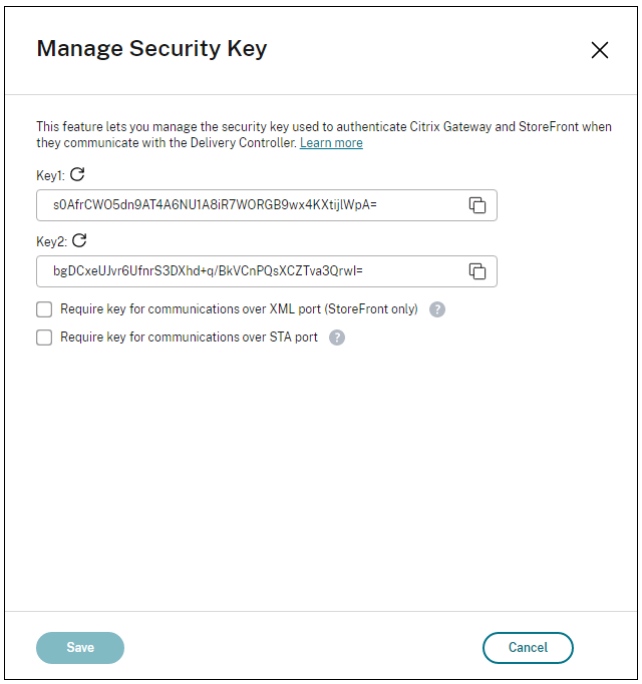
### Configurar los parámetros para su implementación

Puede configurar los parámetros de su implementación a través de Configuración completa o PowerShell.

#### Usar la interfaz de Configuración completa

Una vez habilitada la función, vaya a **Configuración completa > Parámetros > Administrar clave de seguridad** y haga clic en **Modificar**. Aparecerá la hoja **Administrar clave de seguridad**. Haga clic en **Guardar** para aplicar los cambios y cerrar la hoja.




> **Importante:**
>
> - Hay dos claves disponibles para uso. Puede utilizar la misma clave o claves diferentes para las comunicaciones a través de los puertos XML y STA. Le recomendamos usar solo una tecla a la vez. La clave no utilizada solo se utiliza para la rotación de claves.
> - No haga clic en el icono de actualización para actualizar la clave que ya está en uso. Si lo hace, se producirá una interrupción del servicio.

Haga clic en el icono de actualización para generar nuevas claves.

**Requerir clave para las comunicaciones a través del puerto XML (solo para StoreFront)**. Si se selecciona, se necesita una clave para autenticar las comunicaciones a través del puerto XML. StoreFront se comunica con Citrix Cloud a través de este puerto. Para obtener información acerca de cómo cambiar el puerto XML, consulte el artículo CTX127945 de Knowledge Center.

**Requerir clave para las comunicaciones a través del puerto STA**. Si se selecciona, se necesita una clave para autenticar las comunicaciones a través del puerto STA. Citrix Gateway y StoreFront se comunican con Citrix Cloud a través de este puerto. Para obtener información sobre cómo cambiar el puerto STA, consulte el artículo CTX101988 de Knowledge Center.

Después de aplicar los cambios, haga clic en **Cerrar** para salir de la hoja **Administrar clave de seguridad**.

#### Usar el SDK de PowerShell remoto

A continuación, se indican los pasos de PowerShell equivalentes a las operaciones realizadas en la interfaz de Configuración completa.

1. Ejecute el SDK de PowerShell remoto.
2. En una ventana de comandos, ejecute el siguiente comando:
   - `Add-PSSnapIn Citrix*`
3. Ejecute los siguientes comandos para generar una clave y configurar Key1:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey1 <the key you generated>`
4. Ejecute los siguientes comandos para generar una clave y configurar Key2:
   - `New-BrokerXmlServiceKey`
   - `Set-BrokerSite -XmlServiceKey2 <the key you generated>`
5. Ejecute uno o estos dos comandos para habilitar el uso de una clave en la autenticación de comunicaciones:
   - Para autenticar las comunicaciones a través del puerto XML:
     - `Set-BrokerSite -RequireXmlServiceKeyForNFuse $true`
   - Para autenticar las comunicaciones a través del puerto STA:
     - `Set-BrokerSite -RequireXmlServiceKeyForSta $true`

Consulte la ayuda de los comandos de PowerShell para ver instrucciones y sintaxis.

### Configurar los parámetros en StoreFront

Tras completar los parámetros de su implementación, debe configurar los parámetros relevantes en StoreFront mediante PowerShell.

En el servidor de StoreFront, ejecute estos comandos de PowerShell:

- Para configurar la clave para las comunicaciones a través del puerto XML, utilice los comandos `Get-STFStoreServie` y `Set-STFStoreService`. Por ejemplo:
  - `PS C:\> Set-STFStoreFarm $farm -Farmtype XenDesktop -Port 80 -TransportType HTTP -Servers <domain name1, domain name2> -XMLValidationEnabled $true -XMLValidationSecret <the key you generated in Studio>`

- Para configurar la clave para las comunicaciones a través del puerto STA, utilice el comando `New-STFSecureTicketAuthority`. Por ejemplo:

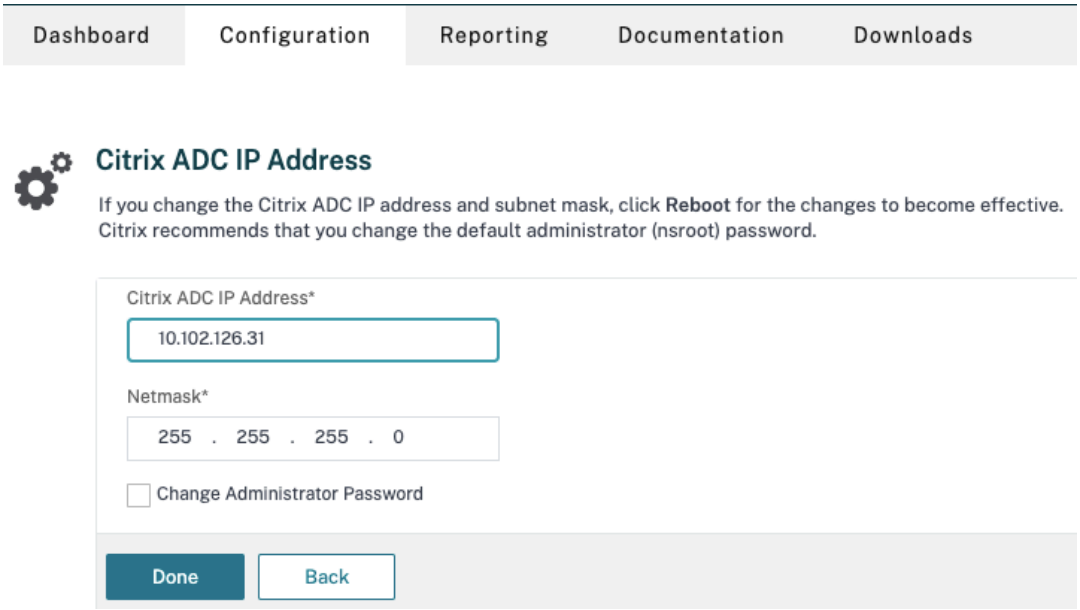
  ```
  PS C:\> $sta = New-STFSecureTicketAuthority –StaUrl <STA URL > -StaValidationEnabled $true -StavalidationSecret <the key you generated in Studio>
  ```

Consulte la ayuda de los comandos de PowerShell para ver instrucciones y sintaxis.

### Configurar los parámetros en Citrix ADC

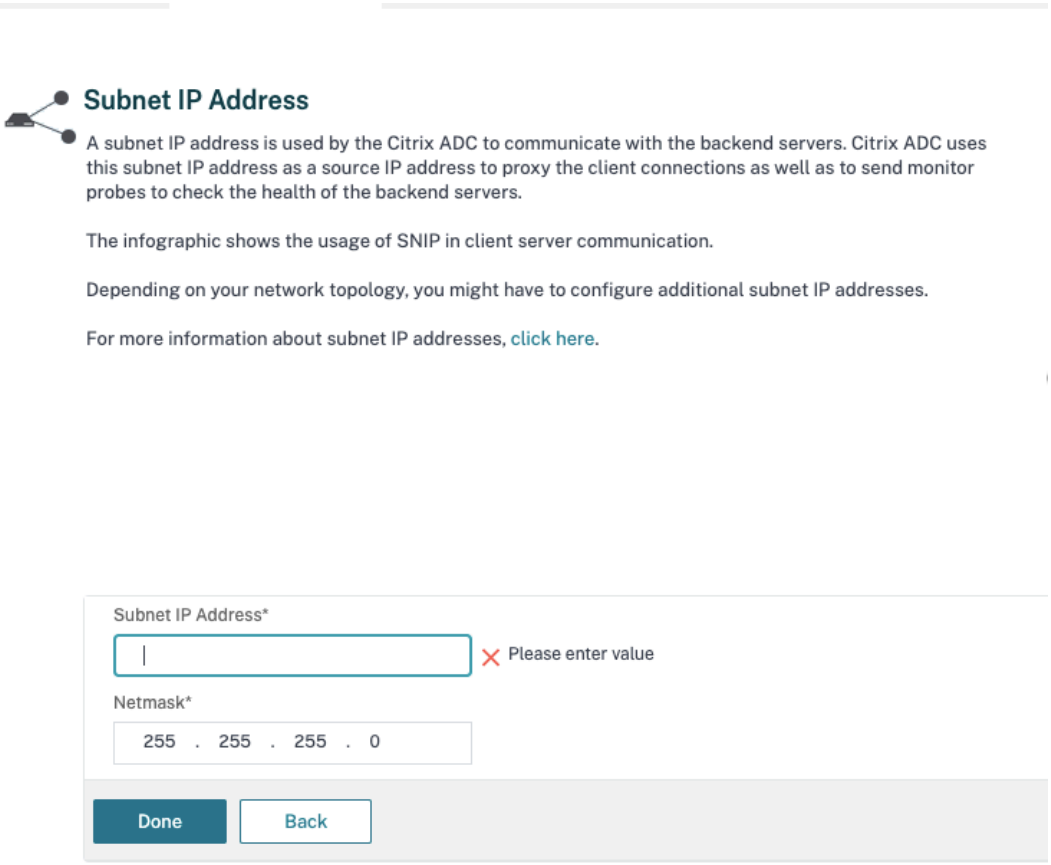
> **Nota:**
>
> No es necesario configurar esta función en Citrix ADC, a no ser que utilice Citrix ADC como puerta de enlace. Si utiliza Citrix ADC, siga los pasos que se indican a continuación.

1. Asegúrese de que ya está implementada la siguiente configuración de requisitos previos:
   - Se configuran las siguientes direcciones IP relacionadas con Citrix ADC.
     - Dirección IP de administración (NSIP) de Citrix ADC para acceder a la consola de Citrix ADC. Para obtener más información, consulte Configurar la dirección IP de NetScaler.



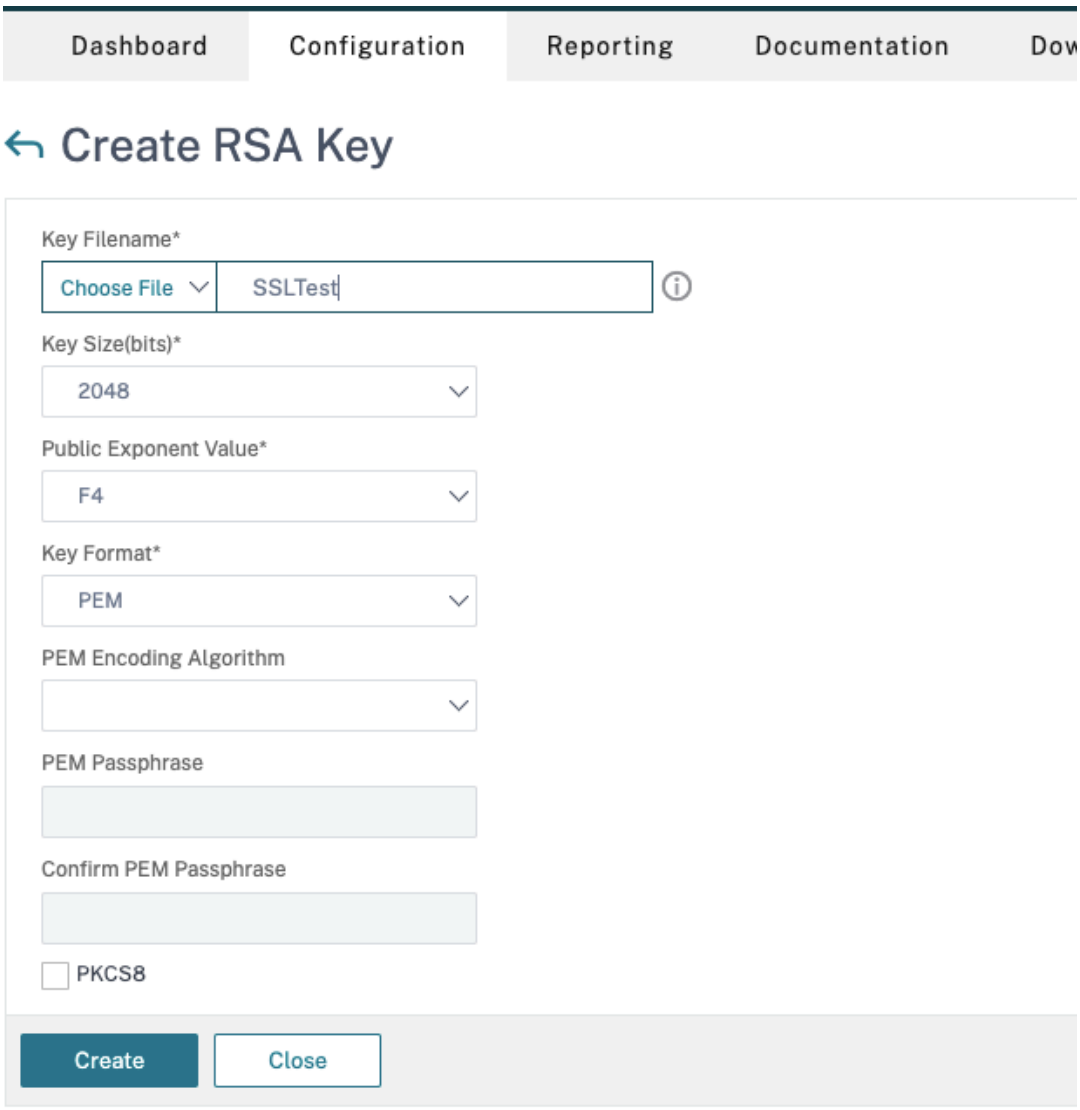

     - Dirección IP de subred (SNIP) para permitir la comunicación entre el dispositivo Citrix ADC y los servidores back-end. Para obtener más información, consulte Configurar direcciones IP de subred.
     - Dirección IP virtual de Citrix Gateway y dirección IP virtual del equilibrador de carga para iniciar sesión en el dispositivo ADC para el lanzamiento de sesiones. Para obtener más información, consulte Crear un servidor virtual.



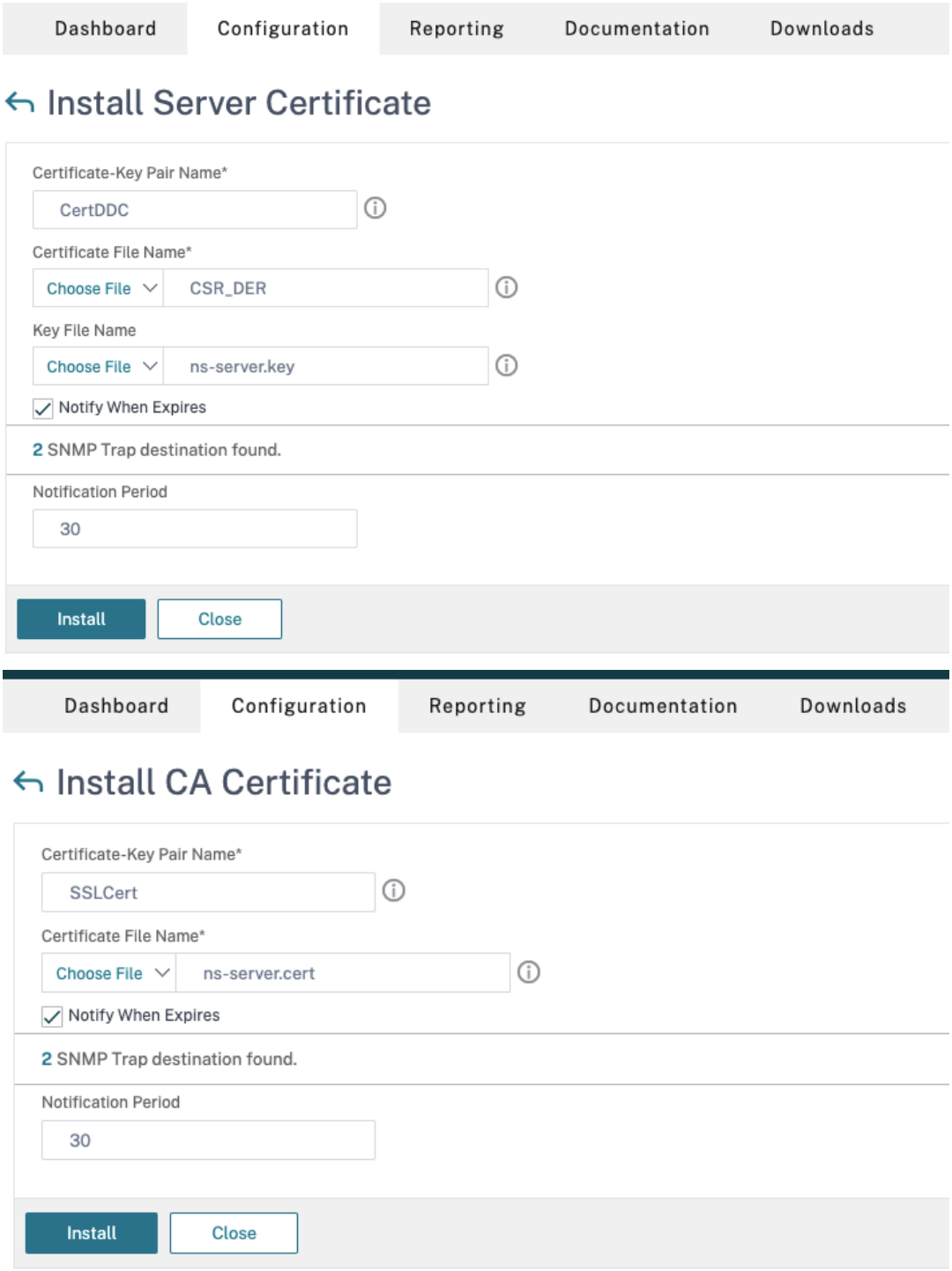

- Los modos y las funciones requeridos en el dispositivo Citrix ADC están habilitados.
  - Para habilitar los modos, en la GUI de Citrix ADC vaya a **System > Settings > Configure Mode**.
  - Para habilitar las funciones, en la GUI de Citrix ADC vaya a **System > Settings > Configure Basic Features**.
- Se han completado las configuraciones relacionadas con los certificados.
  - Se crea la solicitud de firma de certificado (CSR). Para obtener más información, consulte Crear un certificado.



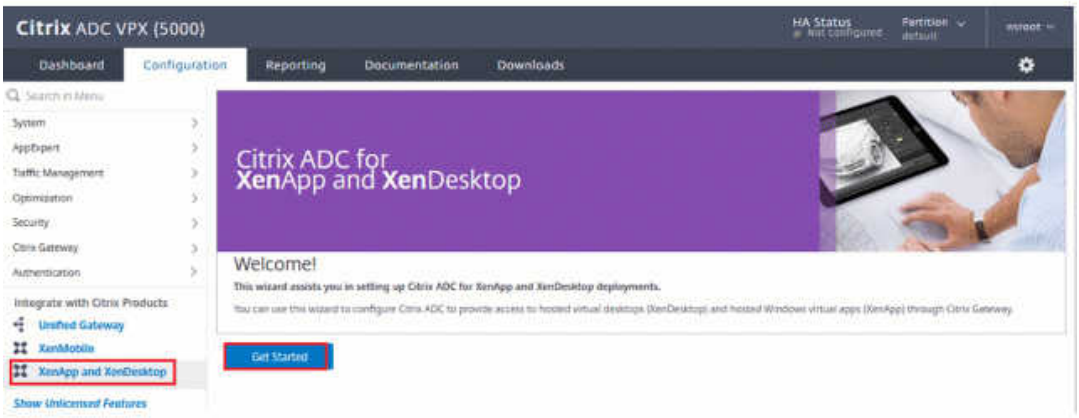

- Los certificados de CA y del servidor y los certificados raíz están instalados. Para obtener más información, consulte Instalación, enlace y actualizaciones.



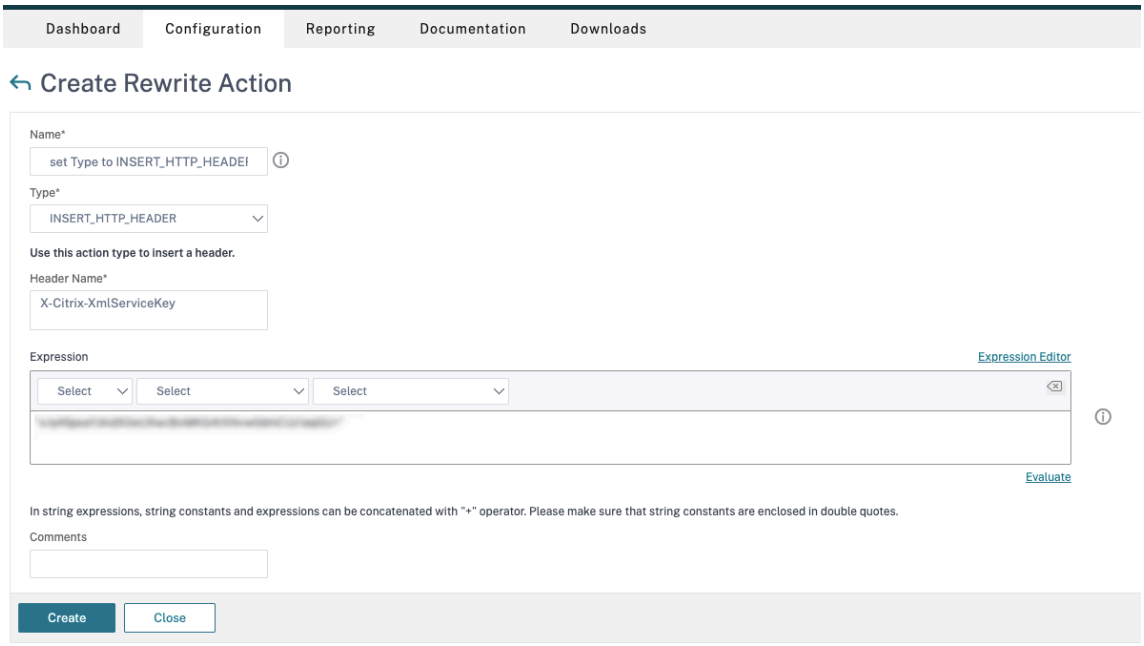

- Se ha creado un Citrix Gateway para Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service). Pruebe la conectividad. Para ello, haga clic en el botón **Test STA Connectivity** para confirmar que los servidores virtuales están conectados. Para obtener más información, consulte Configurar Citrix ADC para Citrix Virtual Apps and Desktops.



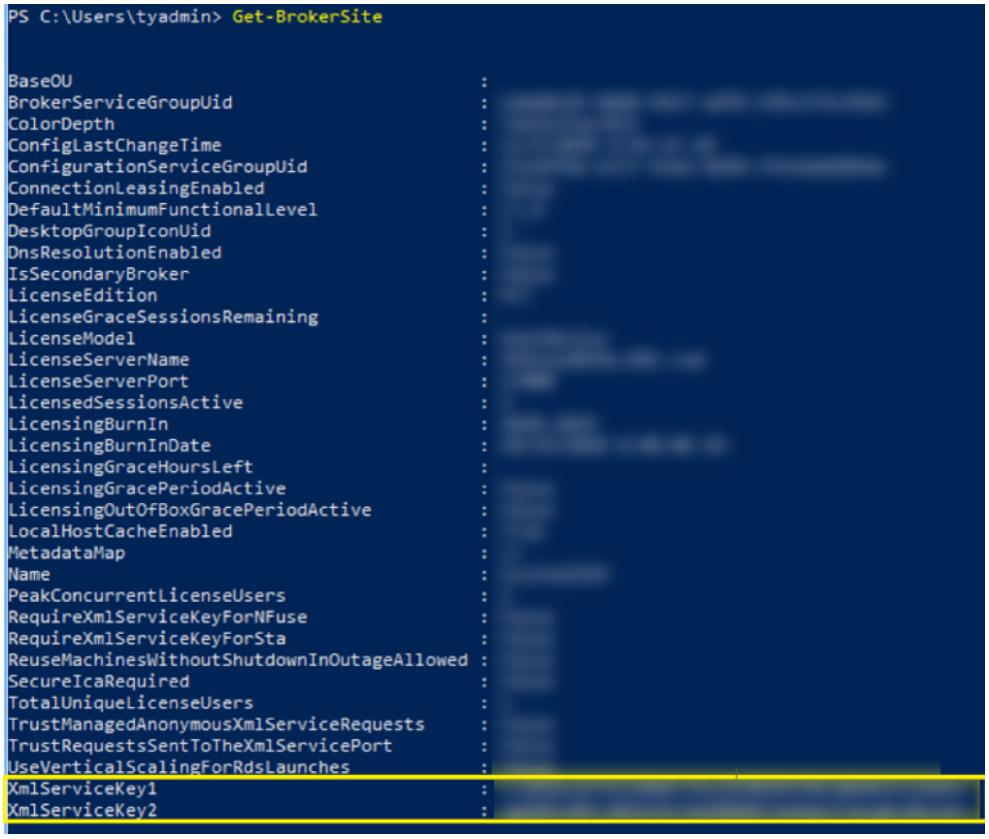

2. Agregue una acción de reescritura. Para obtener más información, consulte Configurar una acción de reescritura.

   a) Vaya a **AppExpert > Rewrite > Actions**.
   b) Haga clic en **Add** para agregar una nueva acción. Puede asignar a la acción el nombre "set Type to INSERT_HTTP_HEADER".




   a) En **Type**, seleccione **INSERT_HTTP_HEADER**.
   b) En **Header Name**, escriba X-Citrix-XmlServiceKey.
   c) En **Expression**, agregue <`XmlServiceKey1 value`> con las comillas. Puede copiar el valor XmlServiceKey1 desde la configuración de Desktop Delivery Controller.

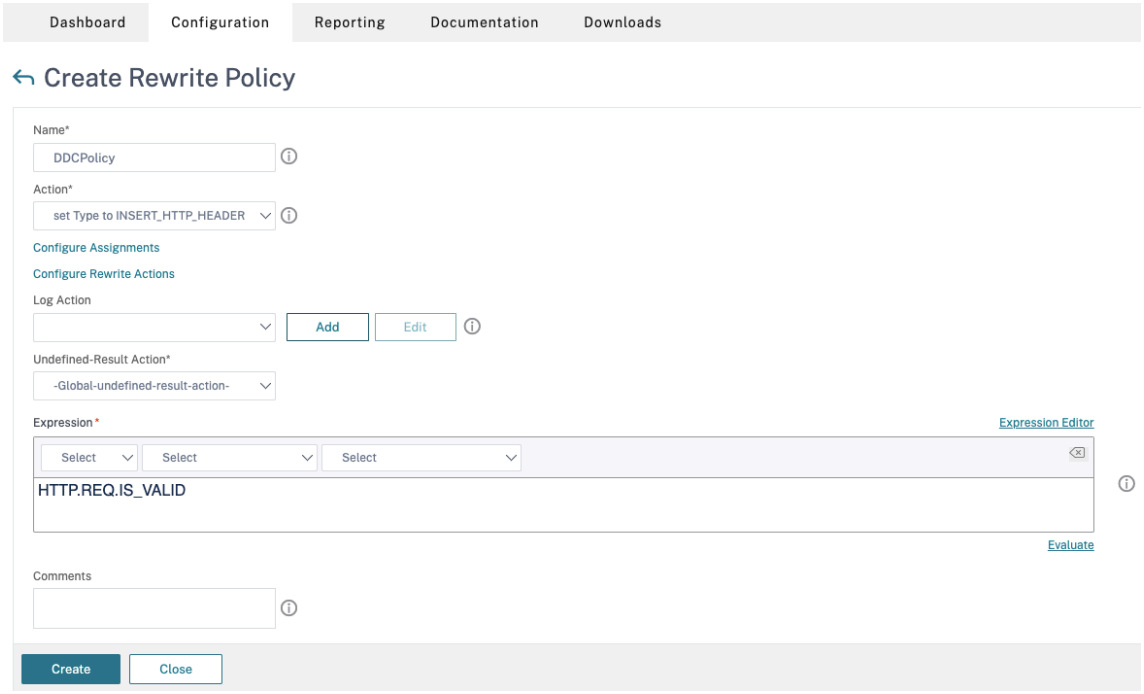



3. Agregue una directiva de reescritura. Para obtener más información, consulte Configurar una directiva de reescritura.

   a) Vaya a **AppExpert > Rewrite > Policies**.

   b) Haga clic en **Add** para agregar una nueva directiva.




a) En **Action**, seleccione la acción creada en el paso anterior.
b) En **Expression**, agregue HTTP.REQ.IS_VALID.
c) Haga clic en **Aceptar**.

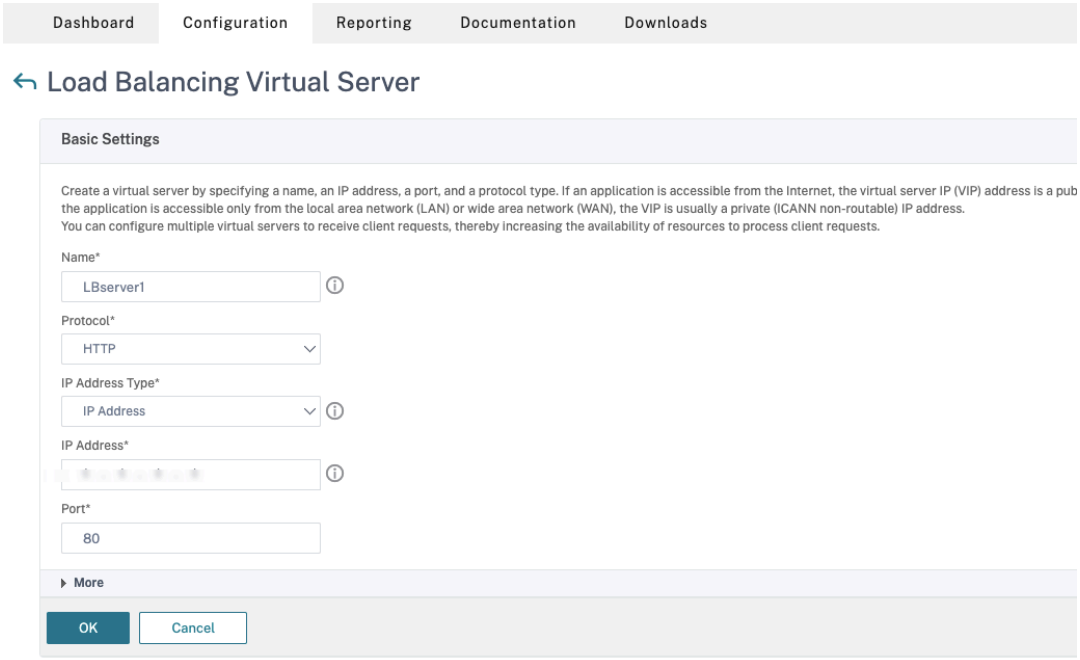
4. Configure el equilibrio de carga. Debe configurar un servidor virtual de equilibrio de carga por cada servidor STA. En caso contrario, no se iniciarán las sesiones.

   Para obtener más información, consulte Configurar el equilibrio de carga básico.

   a) Cree un servidor virtual de equilibrio de carga.

      - Vaya a **Traffic Management -> Load Balancing -> Virtual Servers**.
      - En la página **Virtual Servers**, haga clic en **Add**.

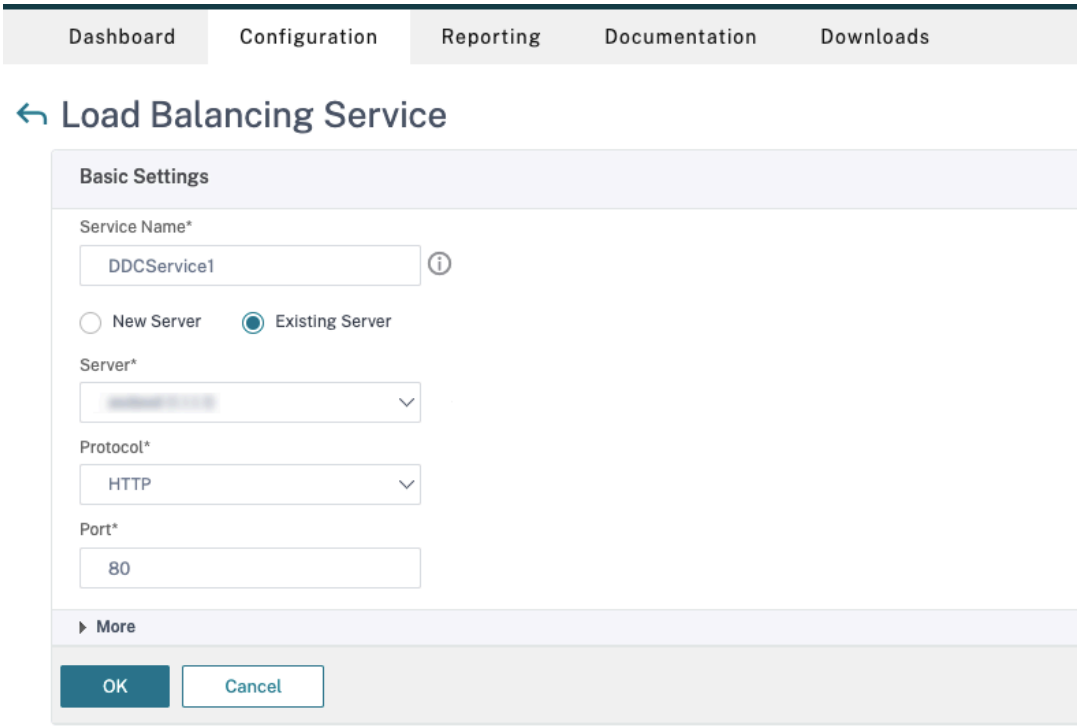
 




- En **Protocol**, seleccione **HTTP**.
- Agregue la dirección IP virtual de equilibrio de carga y, en **Port**, seleccione **80**.
- Haga clic en **Aceptar**.

b) Cree un servicio de equilibrio de carga.

- Vaya a **Traffic Management > Load Balancing > Services**.

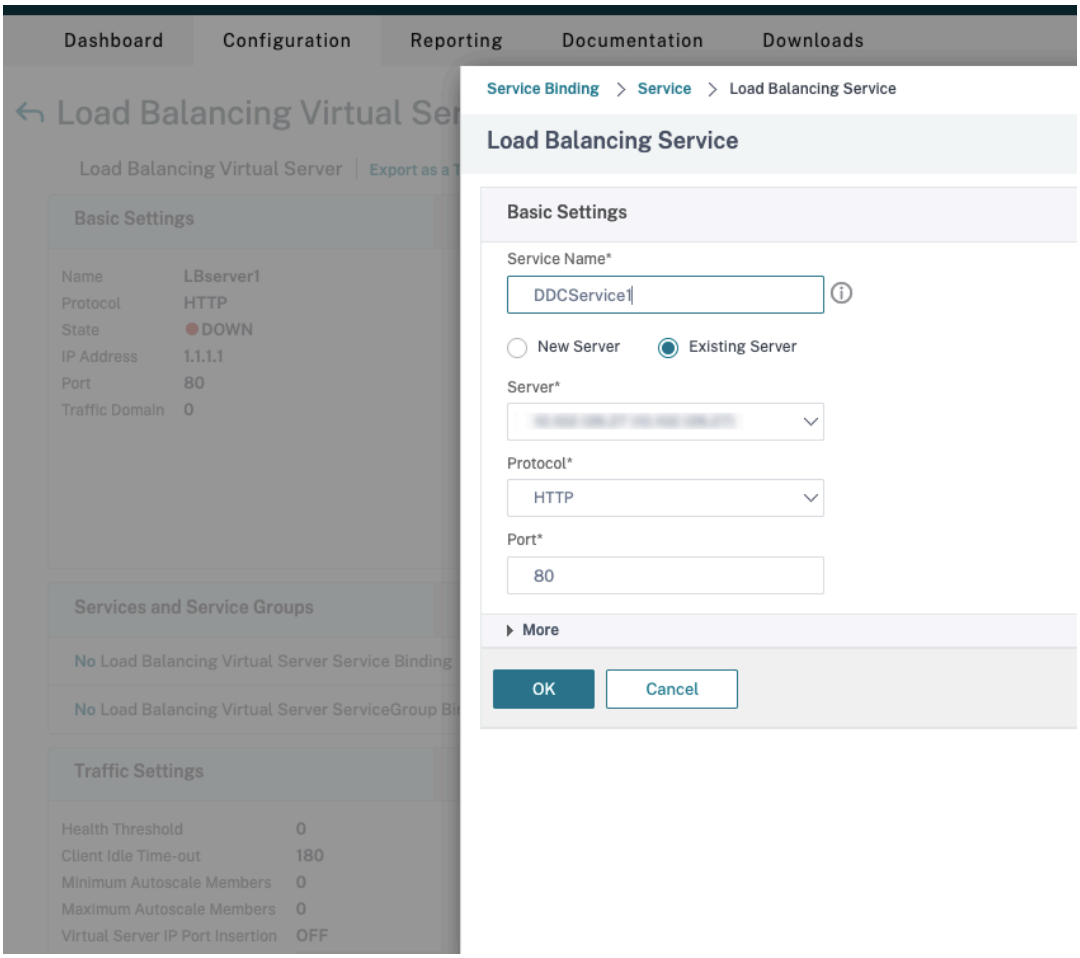


- En **Existing Server**, seleccione el servidor virtual creado en el paso anterior.
- En **Protocol**, seleccione **HTTP** y, en **Port**, seleccione **80**.
- Haga clic en **OK** y, a continuación, en **Done**.

c) Enlace el servicio al servidor virtual.

- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Services and Service Groups**, haga clic en **No Load Balancing Virtual Server Service Binding**.

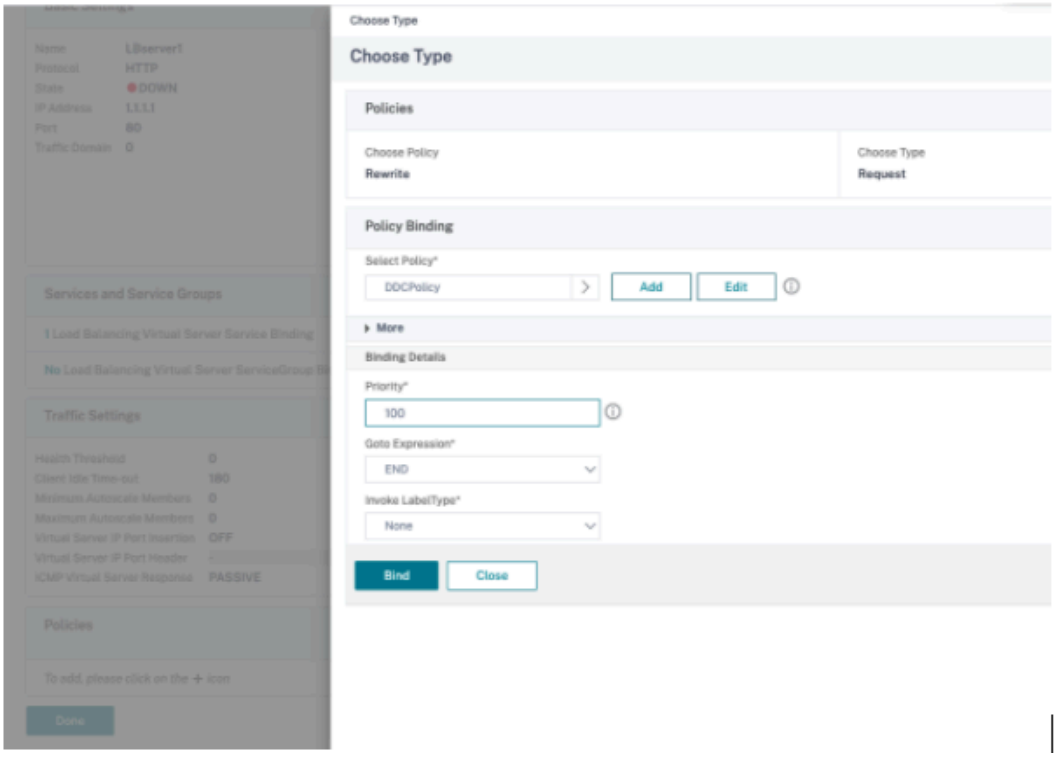



- En **Service Binding**, seleccione la instancia de Citrix DaaS creada anteriormente.
- Haga clic en **Bind**.

d) Vincule la directiva de reescritura creada anteriormente al servidor virtual.

- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Advanced Settings**, haga clic en **Policies,** y, a continuación, en la sección **Policies** haga clic en **+**.

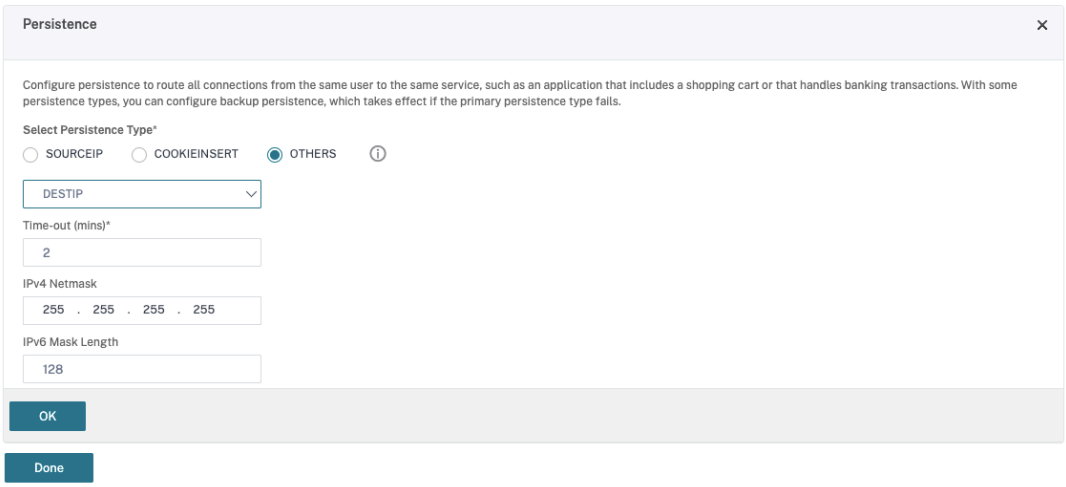
 




- En **Choose Policy**, seleccione **Rewrite** y, en **Choose Type**, seleccione **Request**.
- Haga clic en **Continuar**.
- En **Select Policy**, seleccione la directiva de reescritura creada anteriormente.
- Haga clic en **Bind**.
- Haga clic en **Listo**.

e) Configure la persistencia para el servidor virtual, si es necesario.

- Seleccione el servidor virtual creado anteriormente y haga clic en **Edit**.
- En **Advanced Settings**, haga clic en **Persistence**.




- Seleccione el tipo de persistencia **Others**.

- Seleccione **DESTIP** para crear sesiones de persistencia basadas en la dirección IP del servicio seleccionado por el servidor virtual (la dirección IP de destino)
- En **IPv4 Netmask**, agregue una máscara de red igual que la del Desktop Delivery Controller.
- Haga clic en **Aceptar**.

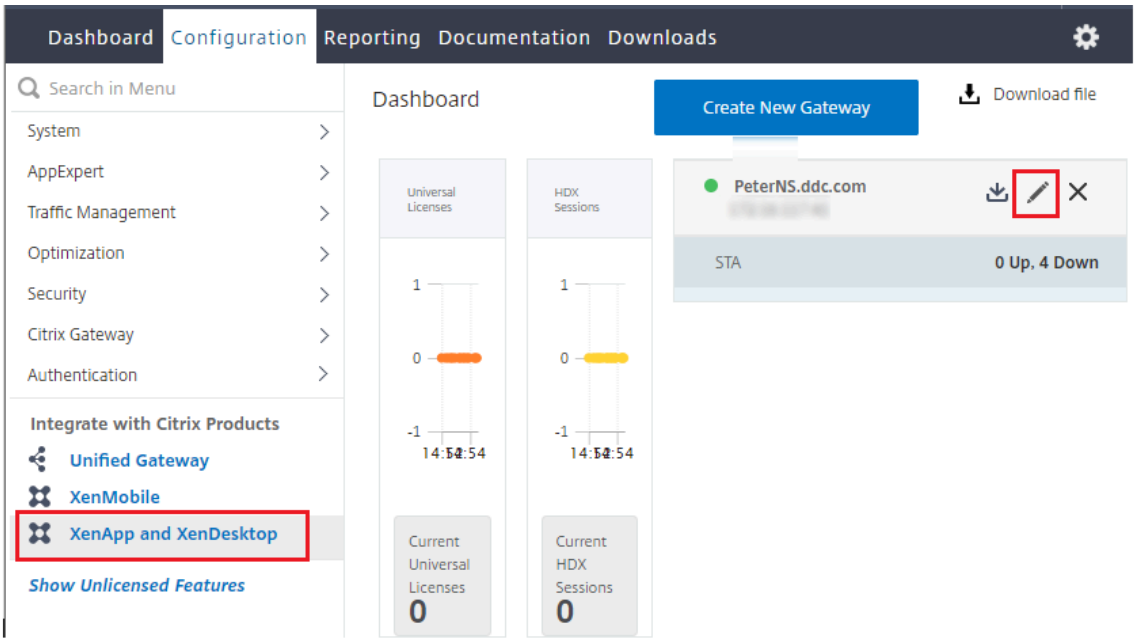
f) Repita estos pasos para el otro servidor virtual.

### La configuración cambia si el dispositivo Citrix ADC ya está configurado con Citrix DaaS

Si ya ha configurado el dispositivo Citrix ADC con Citrix DaaS, para utilizar la funcionalidad Secure XML, debe realizar los siguientes cambios de configuración.

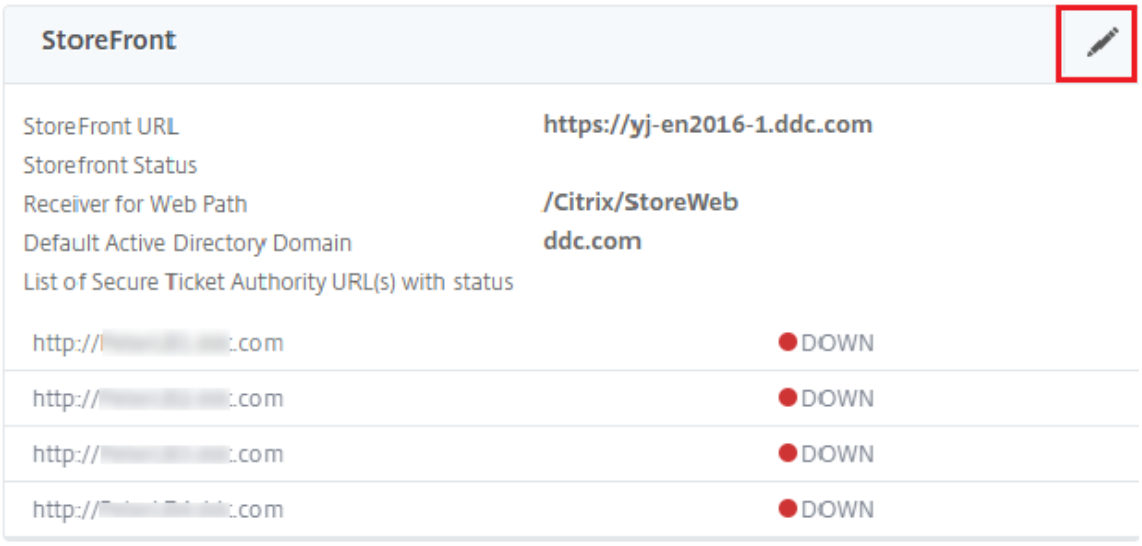
- Antes de iniciar la sesión, cambie la **URL de Secure Ticket Authority (STA)** de la puerta de enlace para que utilice utilizar los nombres de dominio completos (FQDN) de los servidores virtuales de equilibrio de carga.
- Compruebe que el parámetro `TrustRequestsSentToTheXmlServicePort` esté establecido en False. De forma predeterminada, el parámetro `TrustRequestsSentToTheXmlServicePort` se establece en False. Sin embargo, si el cliente ya ha configurado Citrix ADC para Citrix DaaS, `TrustRequestsSentToTheXmlServicePort` se establece en True.

1. En la GUI de Citrix ADC, vaya a **Configuration > Integrate with Citrix Products** y haga clic en **XenApp and XenDesktop**.
2. Seleccione la instancia de puerta de enlace y haga clic en el icono de modificación.




3. En el panel StoreFront, haga clic en el icono de modificación.

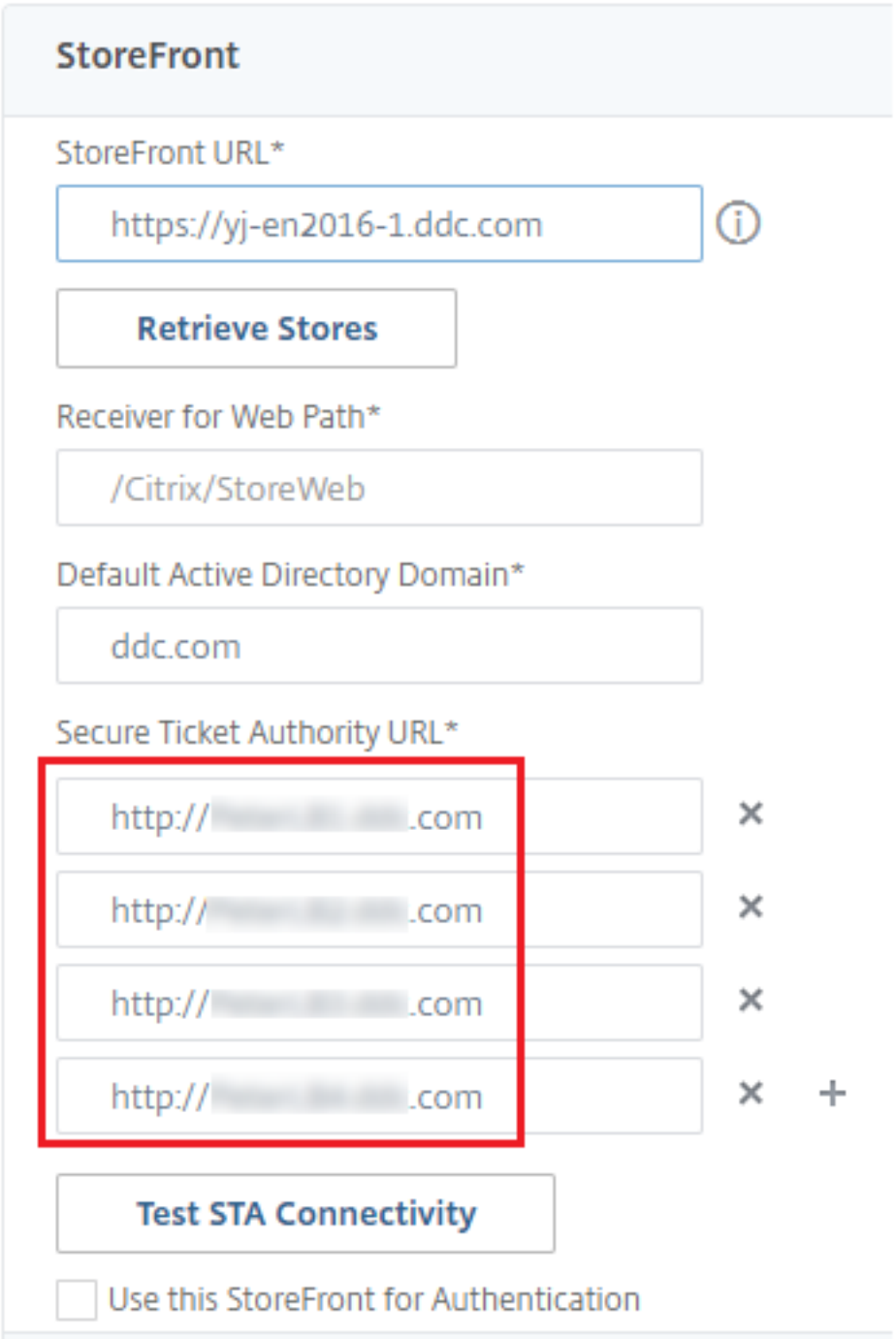
 




4. Agregue la **URL de Secure Ticket Authority**

   - Si la funcionalidad Secure XML está habilitada, la URL de STA debe ser la URL del servicio de equilibrio de carga.
   - Si la funcionalidad Secure XML está inhabilitada, la URL de STA debe ser la URL de STA (la dirección del Desktop Delivery Controller) y el parámetro TrustRequestsSentToTheXmlServicePort del Desktop Delivery Controller debe establecerse en True.




## Parámetros de resistencia de las sesiones

March 30, 2024

El mantenimiento de la actividad de las sesiones es fundamental para ofrecer la mejor experiencia

de uso. La pérdida de conectividad debido a redes poco fiables, a una latencia de red muy variable y a limitaciones del alcance de los dispositivos inalámbricos puede provocar frustración en el usuario. Poder cambiar rápidamente de una estación de trabajo a otra y acceder al mismo conjunto de aplicaciones cada vez que se inicie sesión es prioritario para muchos empleados móviles, como sería el caso de los empleados de un hospital.

Las funciones que se describen en este artículo optimizan la fiabilidad de las sesiones y reducen las molestias, los períodos de inactividad y la pérdida de productividad; con estas funciones, los usuarios móviles pueden trasladarse de unos equipos a otros fácil y rápidamente.

## Fiabilidad de la sesión

Cuando la conectividad de red se ve interrumpida, la fiabilidad de la sesión mantiene las sesiones activas y en la pantalla del usuario. Los usuarios siguen viendo la aplicación que están utilizando hasta que vuelve la conexión.

Esta función es especialmente útil para usuarios móviles con conexiones inalámbricas. Pensemos, por ejemplo, en un usuario con una conexión inalámbrica que se encuentra viajando en un tren y entra en un túnel, y pierde por un momento la conectividad. Por lo general, la sesión se desconecta y desaparece de la pantalla del usuario y después debe conectarse de nuevo. Con la función Fiabilidad de la sesión, la sesión permanece activa en la máquina. Para indicar que se ha perdido la conectividad, la pantalla del usuario se congela y el cursor se convierte en un reloj de arena giratorio hasta que se recupera la conectividad al salir del túnel. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red. La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Los usuarios de la aplicación Citrix Workspace no pueden anular la configuración de Controller.

Puede usar la función de fiabilidad de la sesión con Transport Layer Security (TLS). TLS cifra solo los datos enviados entre el dispositivo de usuario y Citrix Gateway.

Habilite y configure la fiabilidad de la sesión con las siguientes configuraciones de directiva:

- La configuración de directiva Conexiones de fiabilidad de la sesión permite o impide la fiabilidad de la sesión.
- La configuración de directiva Tiempo de espera de fiabilidad de la sesión tiene un tiempo predeterminado de 180 segundos, o tres minutos. Aunque puede ampliar la cantidad de tiempo que Fiabilidad de la sesión mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no pedirá a este que repita la autenticación. Si se prolonga el tiempo que una sesión se mantiene abierta, se incrementa el riesgo de que los usuarios se distraigan, se alejen del dispositivo y, con ello, se facilite a usuarios no autorizados el acceso a la sesión.

- Las conexiones entrantes de fiabilidad de la sesión utilizan el puerto 2598 a menos que usted cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.
- Si no desea que los usuarios se reconecten con sesiones interrumpidas sin tener que repetir la autenticación, use la función Reconexión automática de clientes. Puede definir la configuración de la directiva Autenticación para reconexión automática de clientes de manera que solicite a los usuarios que repitan la autenticación cuando vuelvan a conectarse a las sesiones interrumpidas.

Si usa tanto la fiabilidad de la sesión como la reconexión automática de clientes, las dos actúan de manera secuencial. La fiabilidad de la sesión cierra o desconecta la sesión de usuario después de trascurrido el tiempo que se especifica en la configuración de directiva Tiempo de espera de fiabilidad de la sesión. A continuación, se aplicará la configuración de directiva de Reconexión automática de clientes y se intentará reconectar al usuario con la sesión desconectada.

### Reconexión automática de clientes

Con la función de reconexión automática de clientes, la aplicación Citrix Workspace puede detectar desconexiones accidentales de las sesiones ICA y volver a conectar automáticamente a los usuarios de las sesiones afectadas. Cuando esta función está habilitada en el servidor, los usuarios no tienen que volver a conectarse de forma manual para continuar trabajando.

En sesiones de aplicación, la aplicación Citrix Workspace trata de reconectarse a la sesión hasta que lo logra o el usuario cancela el intento de reconexión.

En sesiones de escritorio, la aplicación Citrix Workspace intenta reconectarse a la sesión durante un período de tiempo especificado, a menos que lo logre o el usuario cancele el intento de reconexión. De forma predeterminada, este tiempo es de cinco minutos. Para cambiar este tiempo, modifique el Registro en el dispositivo del usuario:

```
HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds
; DWORD;<seconds>
```

Donde `seconds` es la cantidad de segundos después de los que no hay más intentos para volver a conectarse a la sesión.

Habilite y configure la Reconexión automática de clientes con las siguientes configuraciones de directiva:

- **Reconexión automática de clientes:** Habilita o inhabilita la reconexión automática de la aplicación Citrix Workspace cuando una sesión se ve interrumpida.
- **Autenticación para reconexión automática de clientes:** Habilita o inhabilita el requisito de autenticación del usuario después de la reconexión automática.

- **Registro de reconexión automática de clientes:** Habilita o inhabilita el registro de sucesos de reconexión en el registro de sucesos. El registro de sucesos está inhabilitado de forma predeterminada. Cuando se habilita, el Registro del sistema del servidor recopila información sobre los sucesos de reconexión automática correctos y fallidos. Cada servidor almacena información sobre los sucesos de reconexión en su propio registro de sistema. El sitio no proporciona los registros combinados de sucesos de reconexión que han tenido lugar en todos los servidores.

Reconexión automática de clientes incorpora un mecanismo de autenticación basado en credenciales de usuario cifradas. Cuando un usuario inicia una primera sesión, el servidor cifra y guarda en memoria las credenciales de usuario, y crea y envía a la aplicación Citrix Workspace una cookie que contiene la clave de cifrado. La aplicación Citrix Workspace envía la clave al servidor para la reconexión. El servidor descifra las credenciales y las envía al inicio de sesión de Windows para su autenticación. Cuando caducan las cookies, los usuarios deben repetir la autenticación para volver a conectarse a las sesiones.

Las cookies no se usan si se habilita la configuración Autenticación para reconexión automática de clientes. En este caso, en su lugar, los usuarios ven un cuadro de diálogo que les solicita sus credenciales cuando la aplicación Citrix Workspace intenta reconectarse automáticamente.

Para lograr la máxima protección de las credenciales y las sesiones del usuario, utilice el cifrado para todas las comunicaciones entre los clientes y el sitio.

Inhabilite la función Reconexión automática de clientes en la aplicación Citrix Workspace para Windows mediante el archivo icaclient.adm. Para obtener más información, consulte la documentación correspondiente a su versión de la aplicación Citrix Workspace para Windows.

Las configuraciones de las conexiones también influyen en la función de reconexión automática de clientes:

- De forma predeterminada, la reconexión automática de clientes se habilita a través de las configuraciones de directiva en el nivel del sitio, como se describe anteriormente. No es necesario repetir la autenticación de los usuarios. Sin embargo, si la conexión ICA TCP del servidor está configurada para restablecer sesiones con un vínculo de comunicación interrumpido, la reconexión automática no se produce. La reconexión automática de clientes solo funciona si el servidor desconecta sesiones cuando existe alguna conexión interrumpida o que ha superado el tiempo de espera. En este contexto, la conexión ICA TCP hace referencia a un puerto virtual del servidor (en lugar de una conexión de red real) que se utiliza para las sesiones en redes TCP/IP.
- De manera predeterminada, la conexión ICA TCP de un servidor está configurada para desconectar sesiones cuya conexión se haya interrumpido o haya superado el tiempo de espera. Las sesiones desconectadas permanecen intactas en la memoria del sistema y la aplicación Citrix Workspace puede volver a conectarse a ellas.
- La conexión se puede configurar para restablecer o cerrar sesiones cuya conexión se haya interrumpido o haya superado el tiempo de espera. Cuando una sesión se restablece, los intentos de

reconexión inician una nueva sesión. No obstante, en lugar de restaurar al usuario a la posición en que se encontraba en la aplicación en uso, la aplicación se reinicia.
- Si el servidor está configurado para restablecer sesiones, la reconexión automática de clientes crea una sesión. En este proceso, el usuario debe introducir sus credenciales para iniciar sesión en el servidor.
- Es posible que la reconexión automática no se lleve a cabo si la aplicación Citrix Workspace o el plugin envían una información de autenticación incorrecta; por ejemplo, durante un ataque o si el servidor determina que ha transcurrido demasiado tiempo desde que se detectó la interrupción de la conexión.

### ICA Keep-Alive

La habilitación de ICA Keep-Alive impide que las conexiones interrumpidas se desconecten. Cuando esta función está habilitada, si el servidor detecta que no hay actividad (por ejemplo, no hay cambios en el reloj, no hay movimientos del puntero ni actualizaciones de pantalla), esta función impide que Servicios de Escritorio remoto desconecte la sesión. El servidor envía paquetes de Keep-Alive cada pocos segundos a fin de detectar si la sesión está activa. Si la sesión ya no está activa, el servidor la marca como desconectada.

> **Importante:**
>
> La función ICA Keep-Alive solo funciona si no se usa la función Fiabilidad de la sesión. Fiabilidad de la sesión tiene su propio mecanismo para impedir que las conexiones interrumpidas se desconecten. Configure ICA Keep-Alive únicamente para las conexiones que no usen Fiabilidad de la sesión.

Los parámetros de ICA Keep-Alive sobrescriben los parámetros de Keep-Alive configurados en la directiva de grupo de Microsoft Windows.

Habilite y configure ICA Keep-Alive con las siguientes configuraciones de directiva:

- **Tiempo de espera de ICA Keep Alive:** Especifica el intervalo de envío de mensajes de ICA Keep-Alive (de 1 a 3600 segundos). No seleccione esta opción si desea que su software de supervisión de red cierre las conexiones inactivas en los entornos en los que las conexiones interrumpidas son tan poco frecuentes que permitir que los usuarios se vuelvan a conectar a las sesiones no es relevante.

  El intervalo predeterminado es 60 segundos: los paquetes de ICA Keep-Alive se envían a los dispositivos de usuario cada 60 segundos. Si un dispositivo del usuario no responde en 60 segundos, el estado de las sesiones ICA cambia a "Desconectado".
- **ICA Keep Alive:** Envía o impide el envío de mensajes de ICA Keep-Alive.

### Control del espacio de trabajo

Con el control del espacio de trabajo, los escritorios y las aplicaciones permanecen disponibles para el usuario cuando éste pasa de un dispositivo a otro. Esta capacidad para moverse entre dispositivos permite que un usuario pueda acceder a todos sus escritorios o aplicaciones abiertas, desde cualquier lugar, simplemente iniciando una sesión, sin tener que reiniciar dichos escritorios y aplicaciones cuando cambia de dispositivo. Por ejemplo: el control del espacio de trabajo puede ser muy útil para los trabajadores de un hospital, que se desplazan rápidamente entre estaciones de trabajo y necesitan acceder al mismo conjunto de aplicaciones cada vez que inician una sesión. Si configura las opciones de control del espacio de trabajo con este propósito, estos trabajadores pueden desconectarse de varias aplicaciones en un dispositivo cliente y reconectarse a las mismas en un dispositivo cliente distinto.

El control del espacio de trabajo afecta a las siguientes actividades:

- **Inicio de sesión:** De manera predeterminada, el control del espacio de trabajo permite a los usuarios reconectarse automáticamente a todos los escritorios y las aplicaciones que estén ejecutándose simplemente iniciando una sesión, sin tener que volver a abrirlos manualmente. Mediante el control del espacio de trabajo, los usuarios pueden abrir aplicaciones y escritorios desconectados, además de otros que estén activos en otro dispositivo cliente. Cuando el usuario se desconecta de una aplicación o de un escritorio, estos siguen ejecutándose en el servidor. Si hay usuarios móviles que deben mantener en ejecución ciertas aplicaciones o escritorios en un dispositivo cliente mientras se reconectan con un subconjunto de sus aplicaciones y escritorios en otro dispositivo cliente distinto, puede configurar el comportamiento de reconexión durante el inicio de sesión para que se abran solo los escritorios y aplicaciones de los que se haya desconectado el usuario anteriormente.
- **Reconexión:** Después de iniciar una sesión en el servidor, los usuarios pueden reconectarse a todos sus escritorios o aplicaciones en cualquier momento haciendo clic en Reconectar. De manera predeterminada, la función Reconectar abre los escritorios y aplicaciones desconectados, además de los que estén ejecutándose en ese momento en otro dispositivo cliente. Puede configurar la función Reconectar para que abra solo los escritorios y aplicaciones de los que se desconectó el usuario anteriormente.
- **Cierre de sesión:** En el caso de usuarios que abren aplicaciones o escritorios mediante StoreFront, puede configurar el comando Cerrar sesión para que el usuario cierre su sesión en StoreFront y en todas las sesiones activas conjuntamente, o bien para que solo cierre la sesión en StoreFront.
- **Desconexión:** Los usuarios se pueden desconectar de todos los escritorios y aplicaciones a la vez, sin necesidad de desconectarse de cada uno de ellos individualmente.

El control del espacio de trabajo está disponible para los usuarios que acceden a escritorios y aplicaciones a través de una conexión de Citrix StoreFront o mediante la aplicación Citrix Workspace. De

manera predeterminada, el control del espacio de trabajo está inhabilitado para las sesiones de escritorio virtual, pero está habilitado para las aplicaciones alojadas en servidores. El uso compartido de sesiones no se produce de manera predeterminada entre los escritorios publicados y las aplicaciones publicadas que se ejecutan en esos escritorios.

Las directivas de usuario, asignaciones de unidad cliente y configuraciones de impresora cambian según sea necesario al cambiar el usuario de dispositivo cliente. Las directivas y asignaciones se aplican según el dispositivo cliente donde el usuario haya iniciado sesión. Por ejemplo, si un trabajador cierra sesión en un dispositivo cliente en el área de Urgencias del hospital y luego inicia sesión en una estación de trabajo del Laboratorio de rayos X, las directivas, las asignaciones de impresora y las asignaciones de unidades del cliente apropiadas para la sesión en el Laboratorio de rayos X entran en efecto en el momento en que se inicia esa nueva sesión.

Puede personalizar qué impresoras se muestran a los usuarios cuando éstos cambian de ubicación. También puede controlar si los usuarios pueden imprimir en impresoras locales, cuánto ancho de banda pueden consumir cuando se conectan de forma remota, así como otros aspectos de la impresión.

Si desea más información sobre cómo habilitar y configurar el control del espacio de trabajo para los usuarios, consulte la documentación de StoreFront.

### Itinerancia de sesiones

> **Nota:**
>
> Esta información le guía para configurar la itinerancia de sesiones mediante PowerShell. En su lugar, puede utilizar la interfaz de administración de Configuración completa. Para obtener más información, consulte Administrar grupos de entrega.

De forma predeterminada, las sesiones se mueven con el usuario entre los diferentes dispositivos cliente. Cuando el usuario inicia una sesión y, más tarde, cambia de dispositivo, se utiliza la misma sesión y las aplicaciones están disponibles simultáneamente en ambos dispositivos. Puede ver las aplicaciones en varios dispositivos. Las aplicaciones se mueven, independientemente del dispositivo o de si las sesiones actuales existen. A menudo, las impresoras y otros recursos asignados a la aplicación también se mueven.

Aunque este comportamiento predeterminado ofrece muchas ventajas, es posible que no sea el mejor para todos los casos. Puede impedir la movilidad de sesión mediante el SDK de PowerShell.

Ejemplo 1. Un miembro del personal médico usa dos dispositivos: uno para completar un formulario del seguro en un equipo de escritorio y otro para consultar información sobre un paciente en una tableta.

- Si la movilidad de sesión está habilitada, ambas aplicaciones aparecerán en ambos dispositivos

(una aplicación iniciada en un dispositivo es visible en todos los dispositivos en uso). Es posible que este comportamiento no cumpla los requisitos de seguridad.
- Si se inhabilita la movilidad de sesión, el registro del paciente no aparecerá en el equipo de escritorio y el formulario del seguro no aparecerá en la tableta.

Ejemplo 2. Un director de producción inicia una aplicación en su equipo de oficina. La ubicación y el nombre del dispositivo determinan qué impresoras y otros recursos están disponibles para esa sesión. Más tarde en la misma jornada laboral, el director va a una oficina situada en el edificio contiguo con el objetivo de asistir a una reunión para la que necesitará usar una impresora.

- Si la movilidad de sesión está habilitada, posiblemente el director de producción no podrá acceder a las impresoras de la sala de la reunión porque las aplicaciones que inició antes, en su oficina, resultaron en la asignación de impresoras y otros recursos cercanos a esa ubicación.
- Si la movilidad de sesión está inhabilitada, cuando inicie sesión en otra máquina (con las mismas credenciales), se iniciará una nueva sesión y las impresoras y los recursos cercanos estarán disponibles.

#### Configurar la itinerancia de sesiones

Para configurar la movilidad de sesión, use los siguientes cmdlets de la regla de directiva de derechos con la propiedad "SessionReconnection". Opcionalmente, también puede especificar la propiedad "LeasingBehavior".

Para sesiones de escritorio:

```
Set-BrokerEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Para sesiones de aplicación:

```
Set-BrokerAppEntitlementPolicyRule <Delivery-Group-name> -SessionReconnection
 <value> -LeasingBehavior Allowed|Disallowed
```

Donde `value` puede ser uno de los siguientes valores:

- **Always:** Las sesiones siempre se mueven, independientemente del dispositivo cliente y si la sesión está conectada o desconectada. Este es el valor predeterminado.
- **DisconnectedOnly:** Reconectarse solo a sesiones que ya se han desconectado; de lo contrario, iniciar una nueva sesión. (Las sesiones pueden moverse entre dispositivos cliente primero desconectándolos, o bien mediante el control del espacio de trabajo para moverlas explícitamente.) Una sesión activa conectada desde otro dispositivo cliente no se utiliza nunca. En su lugar, se inicia una nueva sesión.
- **SameEndpointOnly:** El usuario obtiene una sesión única para cada dispositivo que use. Esto inhabilita completamente la movilidad. Los usuarios solo pueden volver a conectarse al mismo dispositivo que usaron anteriormente en la sesión.

La propiedad "LeasingBehavior"se describe más adelante.

**Efectos de otras opciones de configuración:**

La inhabilitación de la movilidad de sesión se ve afectada por el límite para aplicaciones "Permitir una sola instancia de aplicación por usuario"en las propiedades de aplicación, en el grupo de entrega.

- Si inhabilita la movilidad de sesión, inhabilite el límite para aplicaciones "Permitir una sola instancia de aplicación por usuario".
- Si habilita el límite para aplicaciones "Permitir una sola instancia de aplicación por usuario", no configure uno de los dos valores que permiten sesiones nuevas en dispositivos nuevos.

### Intervalo de inicio de sesión

Si una máquina virtual que contiene un escritorio VDA se cierra antes de que se complete el proceso de inicio de sesión, se puede asignar más tiempo al proceso. El valor predeterminado para 7.6 y versiones posteriores es de 180 segundos, mientras que el predeterminado para versiones de 7.0 a 7.5 es de 90 segundos.

En la máquina (o la imagen maestra utilizada en un catálogo de máquinas), defina la siguiente clave de Registro:

Clave: `HKLM\SOFTWARE\Citrix\PortICA`

- Valor: `AutoLogonTimeout`
- Tipo: `DWORD`
- Especifique un número decimal en segundos que vaya de 0 a 3600.

Si cambia la imagen maestra, implante la nueva imagen en el catálogo. Para obtener más información, consulte Cambiar la imagen maestra.

Esta configuración se aplica solo a las máquinas virtuales con agentes VDA de escritorio de sesión única (estaciones de trabajo). Microsoft controla el tiempo de espera de inicio de sesión en las máquinas con VDA de servidor multisesión.

## Etiquetas

November 17, 2023

### Introducción

Las etiquetas son cadenas que identifican elementos como, por ejemplo, máquinas, aplicaciones, escritorios, grupos de entrega, grupos de aplicaciones y directivas. Después de crear una etiqueta y

agregarla a un elemento, puede adaptar determinadas operaciones para que solo se apliquen a los elementos que tengan esa etiqueta concreta.

- Las búsquedas personalizadas se muestran en la interfaz de administración de Configuración completa.

  Por ejemplo: si quiere que solo se muestren las aplicaciones que se hayan optimizado de cara a evaluadores, cree una etiqueta llamada "evaluar"y agréguela (aplíquela) a esas aplicaciones. Entonces, podrá filtrar la búsqueda con la etiqueta "evaluar"(test).

- Publicar aplicaciones de un grupo de aplicaciones o escritorios concretos de un grupo de entrega, teniendo en cuenta solo un subconjunto de las máquinas en los grupos de entrega seleccionados. Esto se denomina una *restricción por etiquetas*.

  Con una restricción por etiquetas, puede usar las máquinas existentes para más de una tarea de publicación, con lo que se ahorran los costes asociados a la implementación y la administración de más máquinas. La restricción por etiquetas puede entenderse como una subdivisión (o partición) de las máquinas de un grupo de entrega. Su funcionalidad es similar (pero no idéntica) a los grupos de trabajo en las versiones de XenApp anteriores a 7.x.

  Usar un grupo de aplicaciones o escritorios con una restricción por etiquetas puede ser útil para aislar un subconjunto de las máquinas de un grupo de entrega y solucionar los problemas que presentan.

  Más adelante en este artículo, se muestran detalles y ejemplos del uso de una restricción por etiquetas.

- Programar reinicios periódicos para un subconjunto de las máquinas de un grupo de entrega.

  Una restricción por etiquetas en las máquinas permite utilizar los nuevos cmdlets de PowerShell para configurar varias programaciones de reinicios para subconjuntos de máquinas en un grupo de entrega. Para obtener más información, consulte Administrar grupos de entrega.

- Personalizar la aplicación (asignación) de las directivas de Citrix a máquinas de los grupos de entrega, tipos de grupos de entrega o unidades organizativas que contienen (o no) una etiqueta especificada.

  Por ejemplo: si quiere aplicar una directiva de Citrix solo a las estaciones de trabajo más potentes, agregue una etiqueta llamada "potencia alta"a esas máquinas. A continuación, en la página **Asignar directiva** del asistente para la creación de directivas, seleccione la etiqueta y marque la casilla **Habilitar**. También puede agregar una etiqueta a un grupo de entrega y, a continuación, aplicar una directiva de Citrix a ese grupo. Para obtener más información, consulte Crear directivas.

Puede aplicar etiquetas a:

- Máquinas

- Aplicaciones
- Catálogos de máquinas
- Grupos de entrega
- Grupos de aplicaciones

Puede configurar una restricción por etiquetas al crear o modificar lo siguiente en la interfaz de administración de Configuración completa:

- Un escritorio en un grupo de entrega compartido
- Un grupo de aplicaciones

## Restricciones por etiquetas para un grupo de escritorios o aplicaciones

Una restricción por etiquetas implica varios pasos:

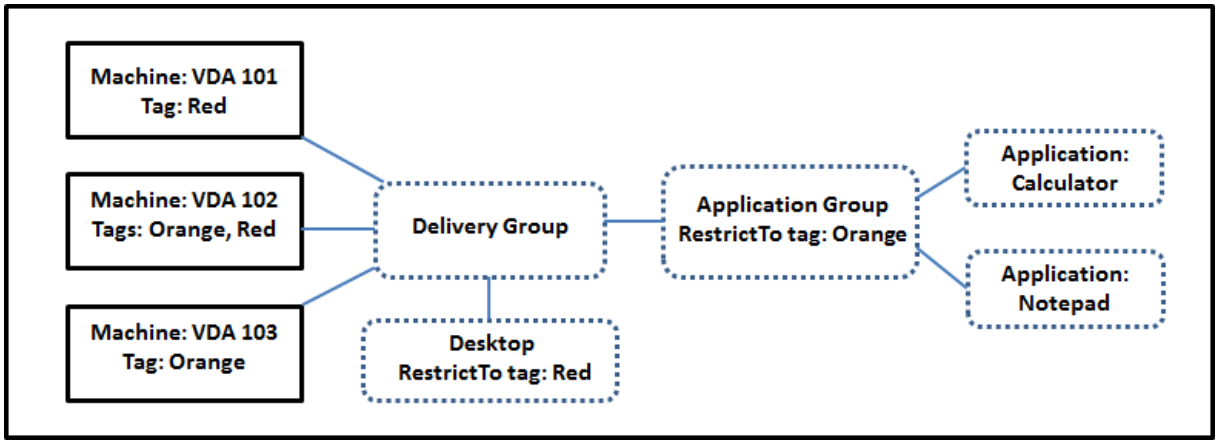
- Crear la etiqueta y, a continuación, agregarla (aplicarla) a las máquinas.
- Crear o modificar un grupo con la restricción por etiquetas (en otras palabras, restringir inicios a máquinas con la etiqueta *x*).

La restricción por etiquetas amplía el proceso de selección de máquinas del Controller. El Controller selecciona una máquina de un grupo de entrega asociado al que se aplican: la directiva de acceso, las listas de usuarios configurados, la preferencia de zonas, la disponibilidad de inicio y la restricción por etiquetas (si existe). Para las aplicaciones, el Controller recurre a otros grupos de entrega por orden de prioridad, aplica las mismas reglas de selección de máquinas para cada grupo de entrega que se tiene en cuenta.

### Ejemplo 1: Distribución sencilla

En este ejemplo, se presenta una distribución sencilla que usa restricciones por etiqueta para limitar las máquinas que se tienen en cuenta para ciertos inicios de aplicaciones y escritorios. Hay un grupo de entrega compartido, un escritorio publicado, y un grupo de aplicaciones configurado con dos aplicaciones.




- Se han agregado etiquetas a cada una de las tres máquinas (VDA 101, 102 y 103).
- El escritorio del grupo de entrega se creó con una restricción por etiquetas llamada `Red`. Por tanto, ese escritorio solo puede iniciarse en máquinas de ese grupo de entrega que tengan la etiqueta `Red`: VDA 101 y 102.
- El grupo de aplicaciones se creó con la restricción por etiquetas `Orange`. Por lo tanto, cada una de sus aplicaciones (`Calculator` y `Notepad`) solo se puede iniciar en máquinas de ese grupo de entrega que tengan la etiqueta `Orange`: VDA 102 y 103.

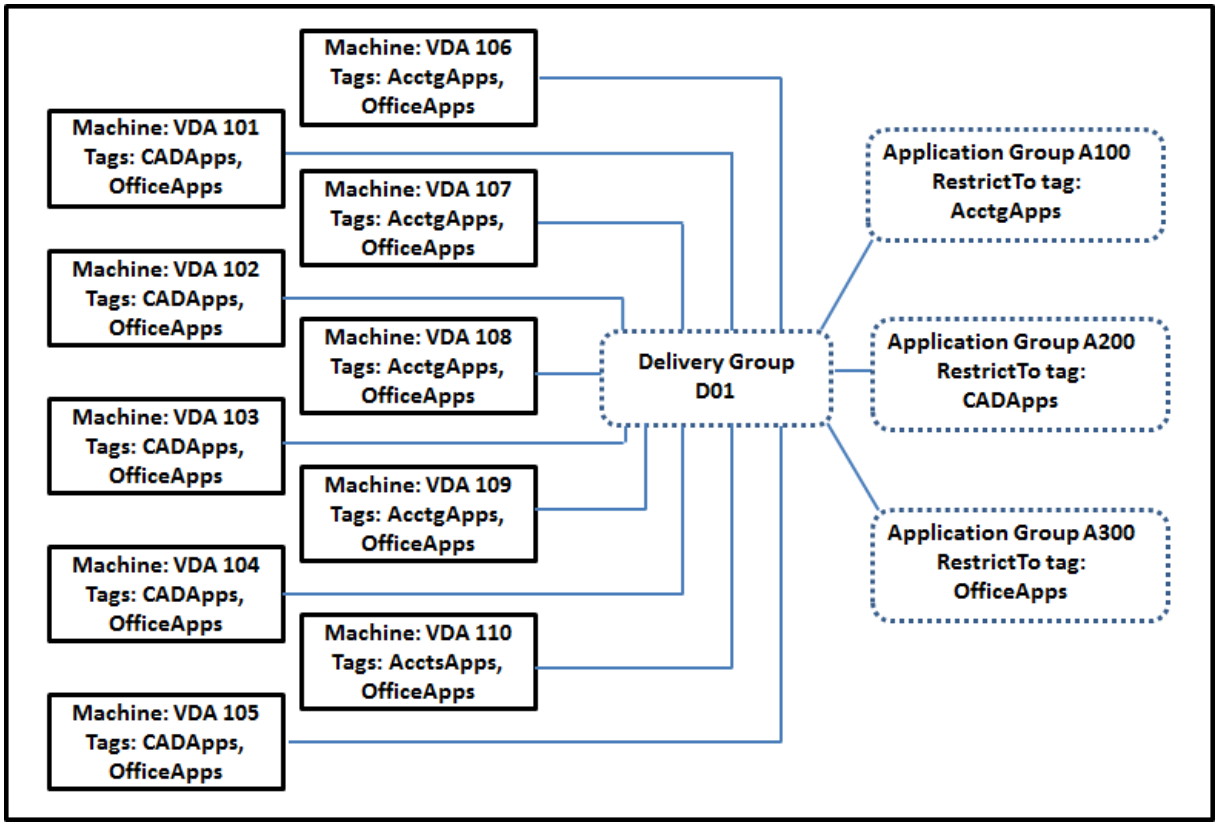
La máquina VDA 102 tiene ambas etiquetas (`Red` y `Orange`); por lo tanto, puede considerarse para iniciar las aplicaciones y el escritorio.

#### Ejemplo 2: Distribución más compleja

En este ejemplo, existen varios grupos de aplicaciones que se han creado con restricciones por etiqueta. Por eso, se pueden entregar más aplicaciones con menos máquinas de las que se necesitarían si solo se usaran grupos de entrega.

En Ejemplo 2: Cómo configurar, se describen los pasos que hay que seguir para crear, aplicar las etiquetas y configurar las restricciones de etiqueta de este ejemplo.




En este ejemplo se utilizan 10 máquinas (VDA 101-110), un grupo de entrega (`D01`) y tres grupos de aplicaciones (`A100`, `A200` y `A300`). Si aplica etiquetas a cada máquina y especifica las restricciones por etiqueta cuando cree cada grupo de aplicaciones:

- Los usuarios de Contabilidad del grupo pueden acceder a las aplicaciones que necesitan en cinco máquinas (VDA de 101 a 105)
- Los diseñadores de CAD del grupo pueden acceder a las aplicaciones que necesitan en cinco máquinas (VDA de 106 a 110)
- Los usuarios del grupo que necesitan las aplicaciones de Office pueden acceder a las aplicaciones Office en 10 máquinas (VDA de 101 a 110)

Solo se utilizan 10 máquinas, con un solo grupo de entrega. Usar solo grupos de entrega (sin grupos de aplicaciones) requeriría el doble de máquinas, porque una máquina solo puede pertenecer a un grupo de entrega.

### Administrar etiquetas y restricciones por etiqueta

Las etiquetas se crean, se agregan (se aplican), se modifican y se eliminan de los elementos seleccionados a través de la acción **Administrar etiquetas** de la interfaz de administración de Configuración completa.

[Excepción: Las etiquetas que se utilizan para las asignaciones de directiva se crean, se modifican y se eliminan mediante la acción **Administrar etiquetas**. Sin embargo, las etiquetas se aplican (asignan) cuando se crea la directiva. Consulte Crear directivas para obtener información detallada].

Las restricciones por etiqueta se configuran cuando crea o modifica los escritorios de los grupos de entrega, y cuando crea y modifica grupos de aplicaciones.

#### Usar la función Administrar etiquetas

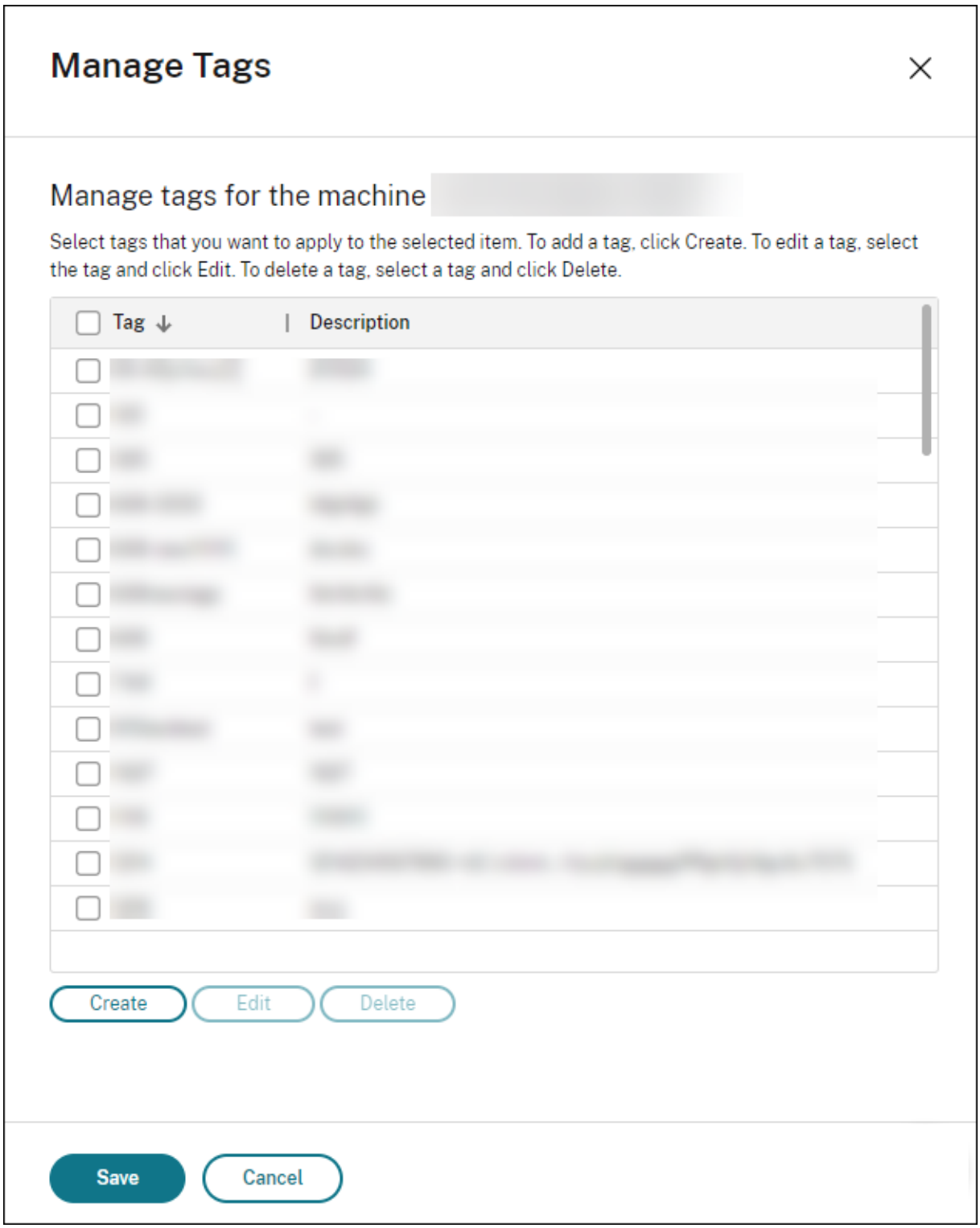
En **Administrar > Configuración completa**, seleccione los elementos a los que quiere aplicar una etiqueta. Los elementos pueden ser:

- Al menos una máquina
- Al menos una aplicación
- Un escritorio, un grupo de entrega o un grupo de aplicaciones
- Un catálogo de máquinas

A continuación, seleccione **Administrar etiquetas** en la barra de acciones. El cuadro de diálogo **Administrar etiquetas** muestra todas las etiquetas existentes, no solo las de los elementos seleccionados.

- Una casilla de verificación marcada indica que la etiqueta ya se ha agregado a los elementos seleccionados. (En la captura de pantalla siguiente, la máquina seleccionada tiene aplicada una etiqueta llamada “Tag1”.)
- Si selecciona más de un elemento, una casilla de verificación que contiene un guión indica que algunos elementos seleccionados (pero no todos) tienen agregada esa etiqueta.




Puede llevar a cabo estas acciones desde el cuadro de diálogo **Administrar etiquetas**. Revise Precauciones al trabajar con etiquetas.

- **Para crear una etiqueta:**

Seleccione **Crear.** Escriba un nombre y una descripción. Los nombres de etiqueta deben ser únicos; en ellos, no se distingue entre mayúsculas y minúsculas. A continuación, seleccione **Guardar**.

Crear una etiqueta no la aplica automáticamente a los elementos que haya seleccionado. Utilice las casillas de verificación para aplicar la etiqueta.

- **Para agregar (aplicar) una o varias etiquetas:**

  Marque la casilla de verificación situada junto al nombre de la etiqueta. Una casilla de verificación que contiene un guión indica que algunos elementos seleccionados (pero no todos) ya tienen aplicada la etiqueta. Cuando se seleccionan varios elementos y la casilla de verificación de una etiqueta tiene un guion, cambiarlo a una marca de verificación afecta a todas las máquinas seleccionadas.

  Si intenta agregar una etiqueta a las máquinas y resulta que esa etiqueta se usa como restricción en un grupo de aplicaciones, se le advierte que la acción puede provocar que esas máquinas estén disponibles para el inicio. Si es lo que quería hacer, continúe.

- **Para quitar una o varias etiquetas:**

  Desmarque la casilla de verificación situada junto al nombre de la etiqueta. Una casilla de verificación que contiene un guión indica que algunos elementos seleccionados (pero no todos) ya tienen aplicada la etiqueta. Cuando se seleccionan varios elementos y la casilla de verificación de una etiqueta tiene un guion, al desactivarla se quita la etiqueta de todas las máquinas seleccionadas.

  Si intenta quitar una restricción por etiquetas desde una máquina, se le advertirá de que la acción puede afectar a las máquinas que se tienen en cuenta para el inicio. Si es lo que quería hacer, continúe.

- **Para modificar una etiqueta:**

  Seleccione una etiqueta y, a continuación, seleccione **Modificar**. Introduzca un nuevo nombre, descripción o ambos. Solo puede modificar una etiqueta a la vez.

- **Para eliminar una o varias etiquetas:**

  Seleccione las etiquetas y, a continuación, seleccione **Eliminar**. El cuadro de diálogo **Eliminar etiqueta** indica la cantidad de elementos que usan en ese momento las etiquetas seleccionadas (por ejemplo, "2 máquinas"). Seleccione un elemento para mostrar más información (por ejemplo, los nombres de las dos máquinas que tienen aplicada la etiqueta). Confirme si quiere eliminar las etiquetas.

  No puede eliminar una etiqueta que se usa como una restricción. Primero, debe modificar el grupo de aplicaciones y quitar la restricción por etiquetas o seleccionar otra etiqueta.

Cuando haya terminado en el cuadro de diálogo **Administrar etiquetas**, seleccione **Guardar**.

Para ver si una máquina tiene etiquetas aplicadas: Seleccione **Grupos de entrega** en el panel de la izquierda. Seleccione un grupo de entrega y, a continuación, seleccione **Ver máquinas** en la barra de acciones. Seleccione una máquina y, a continuación, seleccione la ficha **Etiquetas** en el panel **Detalles**.

#### Administrar restricciones por etiqueta

Configurar una restricción por etiquetas es un proceso de varios pasos: Primero, debe crear la etiqueta y agregar o aplicarla a las máquinas. A continuación, debe agregar la restricción al grupo de aplicaciones o al escritorio.

- **Para crear y aplicar la etiqueta:**

  Cree la etiqueta y, a continuación, agréguela (aplíquela) a las máquinas que se verán afectadas por la restricción por etiquetas mediante las acciones de **Administrar etiquetas**.

- **Para agregar una restricción por etiquetas a un grupo de aplicaciones:**

  Cree o modifique el grupo de aplicaciones. En la página **Grupos de entrega**, seleccione **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en la lista.

- **Para cambiar o quitar una restricción por etiquetas de un grupo de aplicaciones:**

  Modifique el grupo. En la página **Grupos de entrega**, seleccione otra etiqueta en la lista o quite la restricción por etiquetas por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.

- **Para agregar una restricción por etiquetas a un escritorio:**

  Cree o modifique un grupo de entrega. Seleccione **Agregar** o **Modificar** en la página **Escritorios**. En el cuadro de diálogo **Agregar escritorio**, marque **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta en el menú.

- **Para cambiar o quitar la restricción por etiquetas de un grupo de entrega:**

  Modifique el grupo. En la página **Escritorios**, seleccione **Modificar**. En el cuadro de diálogo, seleccione otra etiqueta en la lista o quite la restricción por etiquetas por completo desmarcando **Restringir inicios a máquinas con la etiqueta**.

#### Precauciones al trabajar con etiquetas

Una etiqueta aplicada a un elemento puede utilizarse con distintos fines. Recuerde que agregar, quitar y eliminar una etiqueta puede tener efectos imprevistos. Puede utilizar una etiqueta para ordenar las pantallas de las máquinas al usar la búsqueda en la interfaz de administración de Configuración completa. Puede utilizar la misma etiqueta como restricción al configurar un grupo de aplicaciones

o un escritorio. Esa acción hará que solo se tengan en cuenta para inicio las máquinas de los grupos de entrega especificados que tengan esa etiqueta.

Si agrega una etiqueta a las máquinas después de que la etiqueta se haya configurado como una restricción por etiquetas para un escritorio o un grupo de aplicaciones, se le advertirá que esta acción podría provocar que las máquinas estén disponibles para iniciar otras aplicaciones o escritorios. Si es lo que quería hacer, continúe. Si no, cancele la operación.

Por ejemplo, supongamos que crea un grupo de aplicaciones con la restricción por etiquetas Red. Posteriormente, agrega otras máquinas a los mismos grupos de entrega que utiliza ese grupo de aplicaciones. Si, a continuación, intenta agregar la etiqueta Red a esas máquinas, aparecerá un mensaje similar a: "La etiqueta Red se utiliza como restricción en los siguientes grupos de aplicaciones. Agregar esta etiqueta puede hacer que las máquinas seleccionadas estén disponibles para iniciar las aplicaciones de este grupo de aplicaciones". Puede confirmar o cancelar la operación de agregar esa etiqueta a esas máquinas adicionales.

Del mismo modo, al utilizar una etiqueta en un grupo de aplicaciones para restringir inicios, no puede eliminar la etiqueta hasta que modifique el grupo y la quite como restricción (si pudiera eliminar esa etiqueta, es posible que se permita iniciar aplicaciones en todas las máquinas de los grupos de entrega asociados al grupo de aplicaciones). La misma prohibición de eliminar una etiqueta se aplica si esta se utiliza como una restricción para inicios de escritorio. Después de modificar el grupo de aplicaciones o escritorios en el grupo de entrega para quitar la restricción por etiquetas, puede eliminar la etiqueta.

Es posible que no todas las máquinas tengan el mismo conjunto de aplicaciones. Un usuario puede pertenecer a más de un grupo de aplicaciones, cada uno con una restricción por etiquetas diferente y conjuntos de máquinas diferentes o iguales de los grupos de entrega. En la tabla siguiente, se ofrece una lista de cómo se tienen en cuenta las máquinas.

| **Cuando una aplicación se ha agregado a** | **Estas máquinas de los grupos de entrega seleccionados se tienen en cuenta para el inicio** |
|---|---|
| Un grupo de aplicaciones sin restricción por etiquetas | Cualquier máquina |
| Un grupo de aplicaciones con una restricción por etiquetas A | Máquinas que tienen aplicada la etiqueta A |
| Dos grupos de aplicaciones: uno con una restricción por etiquetas A y otro con una restricción por etiquetas B | Máquinas que tienen las etiquetas A y B; si no hay ninguna disponible, máquinas que tienen la etiqueta A o B |
| Dos grupos de aplicaciones: uno con una restricción por etiquetas A y otro sin restricción por etiquetas | Máquinas que tienen la etiqueta A. Si no hay ninguna disponible, cualquier máquina |

Si ha utilizado una restricción por etiquetas en una programación de reinicios, los cambios que realice que afecten a las aplicaciones o las restricciones por etiqueta afectarán al próximo ciclo de reinicios. Lo que no afecta a los ciclos de reinicios en vigor mientras se realizan los cambios.

#### Ejemplo 2: Cómo configurar

En la siguiente secuencia, se muestran los pasos a seguir para crear y aplicar las etiquetas, así como para configurar las restricciones por etiqueta para los grupos de aplicaciones representados en el segundo ejemplo anterior.

Los agentes VDA y las aplicaciones ya se han instalado en las máquinas y el grupo de entrega se ha creado.

Crear etiquetas y aplicarlas a las máquinas:

1. En **Administrar > Configuración completa**, seleccione **Grupos de entrega** en el panel de la izquierda. Seleccione el grupo de entrega `D01` y, a continuación, seleccione **Ver máquinas** en la barra de acciones.
2. Seleccione las máquinas VDA de la 101 a la 105 y, a continuación, seleccione **Administrar etiquetas** en la barra de acciones.
3. En el cuadro de diálogo **Administrar etiquetas**, seleccione **Crear**. Cree una etiqueta llamada `CADApps`. Seleccione **OK**.
4. Seleccione **Crear** de nuevo y cree una etiqueta denominada `OfficeApps`. Seleccione **OK**.
5. Agregue (aplique) las etiquetas recién creadas a las máquinas seleccionadas marcando las casillas de verificación situadas junto al nombre de cada etiqueta (`CADApps` y `OfficeApps`). A continuación, cierre el cuadro de diálogo.
6. Seleccione el grupo de entrega `D01`. Seleccione **Ver máquinas** en la barra de acciones.
7. Seleccione las máquinas VDA de la 106 a la 110 y, a continuación, seleccione **Administrar etiquetas** en la barra de acciones.
8. En el cuadro de diálogo **Administrar etiquetas**, seleccione **Crear**. Cree una etiqueta llamada `AcctgApps`. Seleccione **OK**.
9. Para aplicar la etiqueta recién creada `AcctgApps` y la etiqueta `OfficeApps` a las máquinas seleccionadas, marque las casillas de verificación situadas junto al nombre de cada etiqueta. A continuación, cierre el cuadro de diálogo.

Cree los grupos de aplicaciones con restricciones por etiqueta.

1. En **Administrar > Configuración completa**, seleccione **Aplicaciones** en el panel de la izquierda.
2. Seleccione **Crear grupo de aplicaciones** en la barra de acciones. Se iniciará el asistente.
3. En la página **Grupos de entrega**, seleccione el grupo de entrega `D01`. Seleccione la opción **Restringir inicios a máquinas con la etiqueta** y, a continuación, seleccione la etiqueta

`AcctgApps` de la lista.

4. Para completar el asistente, especifique los usuarios y las aplicaciones de contabilidad (al agregar la aplicación, seleccione el origen **Desde el menú Inicio**, que busca la aplicación en las máquinas que tienen la etiqueta `AcctgApps`). En la página **Resumen**, especifique un nombre para el grupo `A100`.
5. Repita los pasos anteriores para crear el grupo de aplicaciones `A200`, en que especifique las máquinas que tienen la etiqueta `CADApps`, además de sus usuarios y aplicaciones pertinentes.
6. Repita estos pasos para crear el grupo de aplicaciones `A300`, en que especifique las máquinas que tienen la etiqueta `OfficeApps`, además de sus usuarios y aplicaciones pertinentes.

#### Aplicar etiquetas a catálogos de máquinas

Puede utilizar **Administrar > Configuración completa** o PowerShell para aplicar etiquetas a catálogos de máquinas.

- El uso de la interfaz de administración se describe en Administrar etiquetas. Las pantallas de los catálogos no indican si se han aplicado etiquetas.
- Para usar PowerShell, consulte Usar PowerShell para aplicar etiquetas a catálogos.

A continuación, se muestra un ejemplo de uso de etiquetas con catálogos:

- Un grupo de entrega contiene máquinas de varios catálogos, pero le interesa una operación (por ejemplo, una programación de reinicios) que afecte solamente a las máquinas de un catálogo específico. Al aplicar una etiqueta a ese catálogo, se cumple dicho objetivo.

#### Usar PowerShell para aplicar etiquetas a catálogos

Están disponibles los siguientes cmdlets de PowerShell:

- Puede pasar objetos de catálogo a cmdlets como `Add-BrokerTag` y `Remove-BrokerTag`.
- `Get-BrokerTagUsage` muestra cuántos catálogos contienen etiquetas.
- `Get-BrokerCatalog` tiene una propiedad llamada `Tags`.

Por ejemplo, estos cmdlets agregan una etiqueta que se creó anteriormente denominada `fy2018` al catálogo `acctg`: `Get-BrokerCatalog -Name acctg | Add-BrokerTag fy2018`.

Consulte la ayuda de los cmdlets de PowerShell para ver instrucciones y sintaxis.

### Etiquetas automáticas (Technical Preview)

El etiquetado automático permite a los administradores establecer etiquetas en varios objetos de DaaS automáticamente, o quitarlas, conforme a reglas personalizadas. Esta mejora elimina la necesi-

dad de mantener diferentes scripts que se ejecutan periódicamente para optimizar el entorno.

#### Casos de uso

Con el etiquetado automático, puede implementar reglas conforme a sus prioridades empresariales clave, como reducir los costes, optimizar la infraestructura e impulsar el consumo. A continuación, se indican algunos casos de uso:

- **Recuperar VDI no utilizados**: Para liberar las cargas de trabajo dedicadas que no se han utilizado durante más de un número de días preconfigurado.
- **Eliminar el desorden de aplicaciones**: Para reducir el desorden mediante la identificación de las aplicaciones que no se han utilizado durante más de un número de días preconfigurado.
- **Grupos de entrega con un nivel funcional inferior a X**: Para encontrar grupos de entrega con un nivel funcional inferior a uno específico.
- **Usuarios inactivos**: Para obtener los recursos de los usuarios que no han iniciado sesión durante más de un número de días preconfigurado.

#### Comandos de PowerShell

Puede crear etiquetas automáticas con los comandos de PowerShell. Una vez creada una regla de etiquetado automático, se evalúa con una frecuencia de 600 segundos. Para obtener más información, consulte New-BrokerAutoTagRule.

**Ejemplos** `New-BrokerAutoTagRule` utiliza el mismo tipo de objeto y los mismos parámetros de filtro que el cmdlet `Get-BrokerMachine`. Para obtener más información, consulte GetBrokerMachine.

1. Etiquete los VDI dedicados que no se hayan utilizado durante más de 30 días con un ID 123:

    a) Defina una etiqueta para etiquetar los VDI no usados, por ejemplo, **VDI-sin-usar**.

    - Nombre de etiqueta: VDI-sin-usar
    - ID de etiqueta : 123

    b) Cree la regla de etiquetado automático para etiquetar las máquinas no usadas. Defina los parámetros de regla:

    - Nombre : Nombre genérico de la regla.
    - Tipo de objeto: Máquina.
    - Texto de la regla : Máquinas estáticas asignadas cuya hora última de conexión es > 30 días o no tiene un valor.
    - UID de etiqueta : El identificador de etiqueta al que quiere asociar 123.

```
New-BrokerAutoTagRule -Name 'UnusedVdi' -ObjectType 'Machine' -
RuleText "-AllocationType Static -IsAssigned $true -Filter {
SummaryState -ne `"InUse`" -and ( LastConnectionTime -lt '-30'
 -or LastConnectionTime -eq `$null )} " -TagUid 123
```

c) Compruebe las máquinas marcadas con la etiqueta **VDI-sin-usar** y libérelas.

2. Para etiquetar grupos de entrega con un nivel funcional inferior a X (mediante**L7_20** como nivel funcional de umbral):

```
New-BrokerAutoTagRule -Name 'LowFL'-ObjectType 'DesktopGroup'-
RuleText "-Filter { MinimumFunctionalLevel -lt 'L7_20' } "-TagUid
 123
```

3. Para etiquetar aplicaciones visibles por el usuario publicadas sin una carpeta:

```
New-BrokerAutoTagRule -Name 'NoFolder'-ObjectType 'Application'-
RuleText "-Enabled $true -Filter { ClientFolder -eq $null )} "-
TagUid 123
```

### Más información

Entrada de blog: How to assign desktops to specific servers.

## Configuración de la zona horaria

March 6, 2024

Personalice el formato de fecha y hora en la consola de administración según sus preferencias.

> **Nota:**
>
> Este parámetro es específico para cada cuenta de usuario.

1. Vaya a **Configuración completa > Parámetros > Fecha y hora**.
2. Haga clic en **Modificar** para configurar los siguientes parámetros:
   - **Formato de hora:**
     - Seleccione esta opción para mostrar la hora con un reloj de 12 horas (por ejemplo, las 09:00 p. m.) o un reloj de 24 horas (por ejemplo, las 21:00).

> **Nota:**
>
> Seleccione la opción **Igual que local** si quiere que el formato se ajuste a la zona horaria de su explorador.

- **Formato de fecha:**
  - Configure el formato de fecha para que coincida con sus preferencias, como aaaa/MM/dd.

> **Nota:**
>
> Seleccione la opción **Igual que local** si quiere que el formato se ajuste a la zona horaria de su explorador.

- **Zona horaria:**
  - **UTC:** Muestra la fecha y la hora en UTC en toda la interfaz de usuario. Al pasar el mouse, se muestran la fecha y la hora locales de su zona horaria.
  - **Zona horaria local:** Muestra la fecha y la hora en su zona horaria local en toda la interfaz de usuario. Al pasar el mouse, se muestran la fecha y la hora en formato UTC.

## Solucionar problemas de registro de VDA e inicio de sesión

March 30, 2022

Ofrecemos una función de verificación que le permite comprobar el estado de los VDA. La función le permite identificar las posibles causas de problemas comunes de registro de VDA e inicio de sesión a través de la interfaz de administración de Configuración completa.

A diferencia de Comprobación de estado de Cloud, una herramienta independiente para medir el estado y la disponibilidad del sitio y sus otros componentes, la función está disponible como acción **Realizar comprobación de estado** en la interfaz de administración de Configuración completa.

La acción **Realizar comprobación de estado** puede ejecutar las mismas comprobaciones que Comprobación de estado de Cloud, excepto las siguientes:

- Para el registro de VDA:
  - Disponibilidad del puerto de comunicación en el VDA
- Para inicio de sesiones en VDA:
  - Disponibilidad del puerto de comunicación en el inicio de sesión
  - Ruta de inicio de aplicaciones en VDA

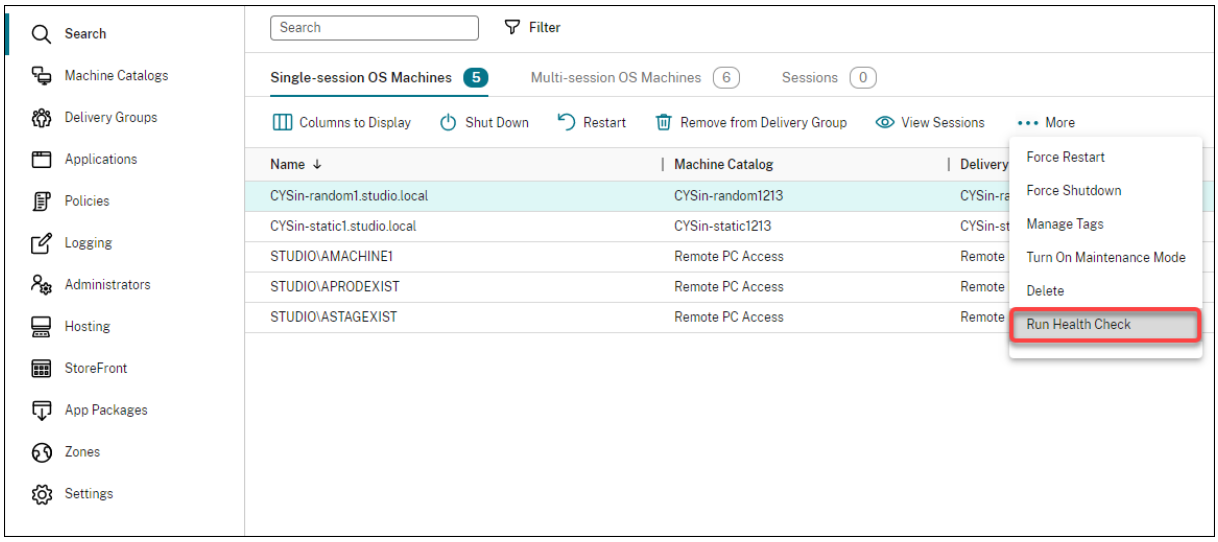
### Requisitos previos

Antes de usar la función, compruebe que cumple los siguientes requisitos previos:

- VDA de Windows
- VDA versión 2109 o posterior
- Los VDA están registrados

### Realizar comprobaciones de estado de los VDA

1. En la interfaz de administración de Configuración completa, vaya al nodo **Buscar**.
2. Seleccione una o más máquinas y, a continuación, seleccione **Realizar comprobación de estado** en la barra de acciones.




> **Nota:**
>
> Actualmente, solo puede realizar comprobaciones de estado de los VDA registrados. La acción **Realizar comprobación de estado** no está disponible para los VDA no registrados.

Al seleccionar **Realizar comprobación de estado**, aparece una ventana en la que se muestra el progreso de las comprobaciones. Espere hasta que se hayan completado las comprobaciones de estado o haga clic en **Cancelar** para cancelar las comprobaciones. Si es necesario, puede mover la ventana.

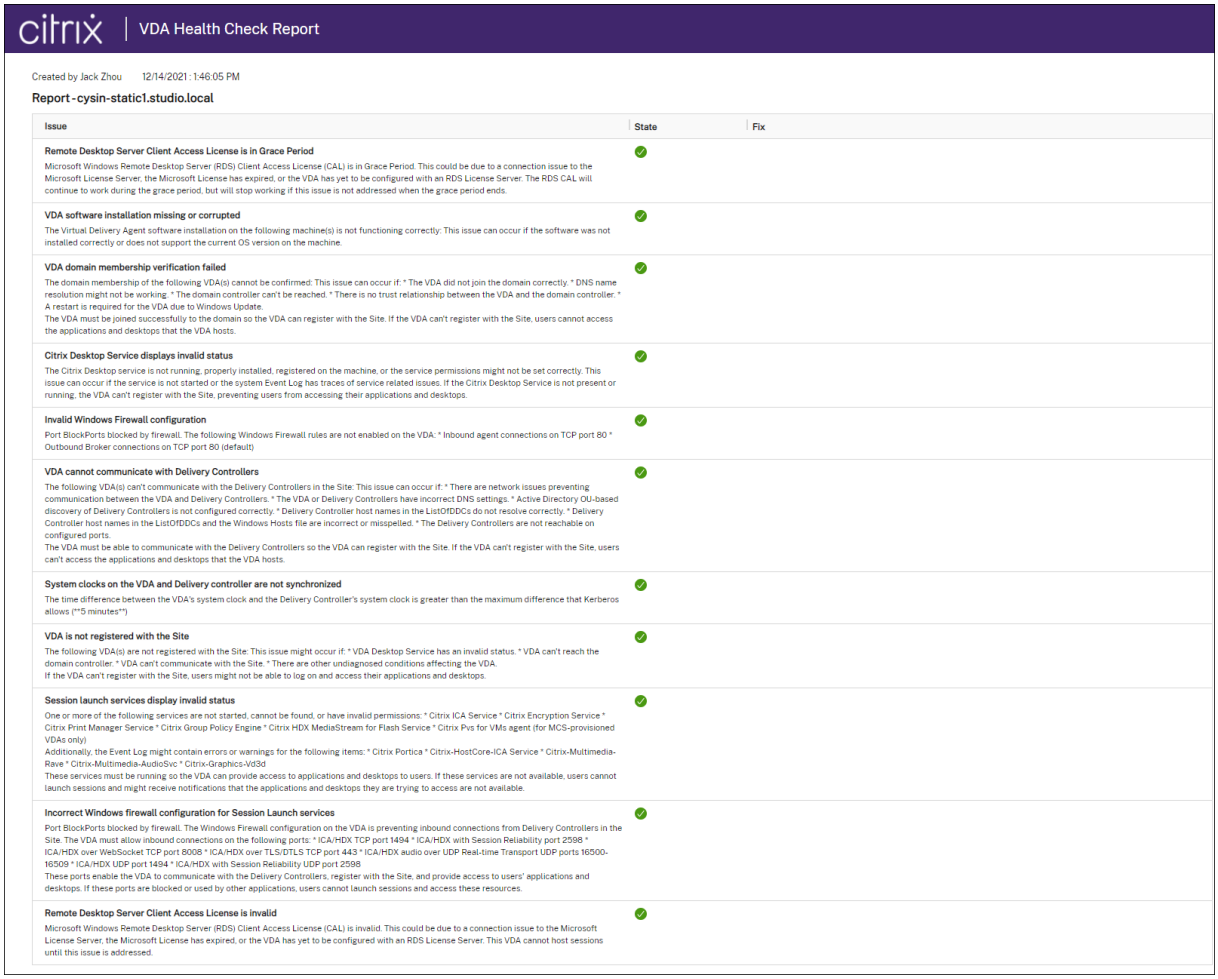
> **Nota:**
>
> En situaciones en las que ya existe una ventana de "comprobaciones de estado en curso", no puede realizar otras comprobaciones de estado adicionales hasta que se completen las primeras.

Una vez completadas las comprobaciones de estado, aparecerán los dos botones siguientes: **Ver informe** y **Cerrar**. Para ver los resultados de las comprobaciones de estado, haga clic en **Ver informe**.


El informe de comprobación de estado se abre en una nueva ficha de explorador. El informe contiene los siguientes elementos:

- Hora y fecha en que se generó el informe de resultados
- La persona que realizó los las comprobaciones de estado
- Comprobaciones realizadas en las máquinas de destino
- Problemas detectados, junto con recomendaciones para corrección



citrix | VDA Health Check Report

Created by Jack Zhou 12/14/2021 1:46:05 PM

Report - cysin-static1.studio.local

| Issue | State | Fix |
|---|---|---|
| **Remote Desktop Server Client Access License is in Grace Period**<br>Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is in Grace Period. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. The RDS CAL will continue to work during the grace period, but will stop working if this issue is not addressed when the grace period ends. | ✓ | |
| **VDA software installation missing or corrupted**<br>The Virtual Delivery Agent software installation on the following machine(s) is not functioning correctly: This issue can occur if the software was not installed correctly or does not support the current OS version on the machine. | ✓ | |
| **VDA domain membership verification failed**<br>The domain membership of the following VDA(s) cannot be confirmed: This issue can occur if: * The VDA did not join the domain correctly. * DNS name resolution might not be working. * The domain controller can't be reached. * There is no trust relationship between the VDA and the domain controller. * A restart is required for the VDA due to Windows Update.<br>The VDA must be joined successfully to the domain so the VDA can register with the Site. If the VDA can't register with the Site, users cannot access the applications and desktops that the VDA hosts. | ✓ | |
| **Citrix Desktop Service displays invalid status**<br>The Citrix Desktop service is not running, properly installed, registered on the machine, or the service permissions might not be set correctly. This issue can occur if the service is not started or the system Event Log has traces of service related issues. If the Citrix Desktop Service is not present or running, the VDA can't register with the Site, preventing users from accessing their applications and desktops. | ✓ | |
| **Invalid Windows Firewall configuration**<br>Port BlockPorts blocked by firewall. The following Windows Firewall rules are not enabled on the VDA: * Inbound agent connections on TCP port 80 * Outbound Broker connections on TCP port 80 (default) | ✓ | |
| **VDA cannot communicate with Delivery Controllers**<br>The following VDA(s) can't communicate with the Delivery Controllers in the Site: This issue can occur if: * There are network issues preventing communication between the VDA and Delivery Controllers. * The VDA or Delivery Controllers have incorrect DNS settings. * Active Directory OU-based discovery of Delivery Controllers is not configured correctly. * Delivery Controller host names in the ListOfDDCs do not resolve correctly. * Delivery Controller host names in the ListOfDDCs and the Windows Hosts file are incorrect or misspelled. * The Delivery Controllers are not reachable on configured ports.<br>The VDA must be able to communicate with the Delivery Controllers so the VDA can register with the Site. If the VDA can't register with the Site, users can't access the applications and desktops that the VDA hosts. | ✓ | |
| **System clocks on the VDA and Delivery controller are not synchronized**<br>The time difference between the VDA's system clock and the Delivery Controller's system clock is greater than the maximum difference that Kerberos allows (**5 minutes**) | ✓ | |
| **VDA is not registered with the Site**<br>The following VDA(s) are not registered with the Site: This issue might occur if: * VDA Desktop Service has an invalid status. * VDA can't reach the domain controller. * VDA can't communicate with the Site. * There are other undiagnosed conditions affecting the VDA.<br>If the VDA can't register with the Site, users might not be able to log on and access their applications and desktops. | ✓ | |
| **Session launch services display invalid status**<br>One or more of the following services are not started, cannot be found, or have invalid permissions: * Citrix ICA Service * Citrix Encryption Service * Citrix Print Manager Service * Citrix Group Policy Engine * Citrix HDX MediaStream for Flash Service * Citrix Pvs for VMs agent (for MCS-provisioned VDAs only)<br>Additionally, the Event Log might contain errors or warnings for the following items: * Citrix Portica * Citrix-HostCore-ICA Service * Citrix-Multimedia-Rave * Citrix-Multimedia-AudioSvc * Citrix-Graphics-Vd3d<br>These services must be running so the VDA can provide access to applications and desktops to users. If these services are not available, users cannot launch sessions and might receive notifications that the applications and desktops they are trying to access are not available. | ✓ | |
| **Incorrect Windows firewall configuration for Session Launch services**<br>Port BlockPorts blocked by firewall. The Windows Firewall configuration on the VDA is preventing inbound connections from Delivery Controllers in the Site. The VDA must allow inbound connections on the following ports: * ICA/HDX TCP port 1494 * ICA/HDX with Session Reliability port 2598 * ICA/HDX over WebSocket TCP port 8008 * ICA/HDX over TLS/DTLS TCP port 443 * ICA/HDX audio over UDP Real-time Transport UDP ports 16500-16509 * ICA/HDX UDP port 1494 * ICA/HDX with Session Reliability UDP port 2598<br>These ports enable the VDA to communicate with the Delivery Controllers, register with the Site, and provide access to users' applications and desktops. If these ports are blocked or used by other applications, users cannot launch sessions and access these resources. | ✓ | |
| **Remote Desktop Server Client Access License is invalid**<br>Microsoft Windows Remote Desktop Server (RDS) Client Access License (CAL) is invalid. This could be due to a connection issue to the Microsoft License Server, the Microsoft License has expired, or the VDA has yet to be configured with an RDS License Server. This VDA cannot host sessions until this issue is addressed. | ✓ | |

Puede realizar comprobaciones de estado de forma individual y en lotes.

> **Nota:**
>
> Al ejecutar comprobaciones de estado en lotes, no seleccione más de 10 máquinas. De lo contrario, la acción **Realizar comprobación de estado** no estará disponible.

## Acceso de usuarios

April 21, 2023

Hay dos componentes principales que proporcionan acceso a aplicaciones y escritorios en implementaciones de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service):

- **Plataforma Citrix Workspace**: La plataforma Citrix Workspace es una solución digital completa que le permite ofrecer acceso seguro a la información, las aplicaciones y otro contenido

relevante para el rol de una persona en su organización. Los usuarios se suscriben a los servicios que usted pone a su disposición, de modo que puedan acceder a ellos desde cualquier lugar y dispositivo. La plataforma Citrix Workspace le ayuda a organizar y automatizar los detalles más importantes que sus usuarios necesitan para colaborar, tomar decisiones óptimas y centrarse plenamente en su trabajo.

Implementar Citrix Workspace no supone ningún esfuerzo, y Citrix se encarga de mantenerlo en buen estado. La plataforma Citrix Workspace se recomienda para clientes nuevos y existentes, previsualizaciones y pruebas de concepto.

- **Almacén local de StoreFront:** Los clientes también pueden utilizar un almacén existente de StoreFront para agrupar escritorios y aplicaciones en Citrix Cloud. Este caso de uso ofrece mayor seguridad y la autenticación de dos factores, y evita que los usuarios introduzcan sus contraseñas en el servicio de la nube. También permite a los clientes personalizar sus nombres de dominio y sus direcciones URL. Este tipo de implementación se recomienda para todos los clientes de Citrix Virtual Apps and Desktops que ya tienen StoreFront implementado.

  Consulte también Caché de host local y StoreFront.

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

### Usar Citrix Workspace

A los espacios de trabajo se accede a través de `https://<customername>.cloud.com`. Si es necesario, puede personalizar la parte `<customername>` de la URL del espacio de trabajo. A continuación, puede configurar la conectividad para cada ubicación de recursos que quiera utilizar de modo que los usuarios finales puedan acceder a los recursos de sus espacios de trabajo. Los usuarios finales acceden a su espacio de trabajo mediante la versión más reciente de la aplicación Citrix Workspace.

Para obtener más información sobre el uso de Citrix Workspace, consulte:

- Configurar espacios de trabajo: Para configurar el acceso y las personalizaciones.
- Espacios de trabajo seguros: Para configurar la autenticación.
- Gestionar la experiencia en los espacios de trabajo: Para comprender cómo acceden los usuarios finales a sus espacios de trabajo y cómo se muestran estos.

Para proporcionar acceso remoto a los usuarios finales a través de Citrix Workspace, puede usar Citrix Gateway Service o su propio dispositivo Citrix Gateway.

- Para usar Citrix Gateway Service:

  1. En **Citrix Cloud > Ubicaciones de recursos**, seleccione **Gateway** para la ubicación de recursos que quiere utilizar.
  2. Seleccione **Gateway Service** y, a continuación, haga clic en **Guardar**.
  3. En **Citrix Cloud > Configuración de Workspace > Integraciones de servicios**, busque Gateway Service y seleccione **Habilitar** en el menú de tres puntos.

- Para usar su propio dispositivo Citrix Gateway:

  1. Configure Citrix Gateway como proxy de ICA (no se necesitan directivas de sesión ni autenticación).
  2. Configure una ubicación de recursos para usar Citrix Gateway:

     a) En **Citrix Cloud > Ubicaciones de recursos**, seleccione **Gateway** para la ubicación de recursos que quiere utilizar.
     b) Seleccione **Gateway tradicional** e introduzca el nombre FQDN externo. No agregue protocolo. Los puertos son optativos. Citrix Workspace no admite la combinación de acceso remoto e interno.

  3. Vincule Citrix Cloud Connectors como servidores Secure Ticket Authority (STA) a Citrix Gateway. Para obtener más información, consulte CTX232640.

     > **Nota:**
     >
     > Con Citrix Gateway, solo se admite el uso de máquinas Citrix Cloud Connector como servidores STA. No se admite el uso de otros conectores, como Connector Appliance, como servidores STA.

Para obtener más información sobre Citrix Gateway Service y sobre Citrix Gateway, consulte Citrix Gateway.

### Usar un almacén local de StoreFront

Para obtener información sobre cómo configurar un StoreFront local, consulte la documentación de StoreFront.

Una de las ventajas de utilizar un almacén existente de StoreFront es que el Citrix Cloud Connector proporciona el cifrado de las contraseñas de usuario. El Cloud Connector cifra las credenciales mediante AES-256 con una clave única generada aleatoriamente. Esta clave se devuelve directamente a la aplicación Citrix Workspace y nunca se envía a la nube. La aplicación Citrix Workspace la suministra al VDA durante el inicio de sesión para descifrar las credenciales y ofrecer una experiencia de inicio de sesión unificado (Single Sign-On) en Windows.

- Para el transporte, seleccione HTTP y el puerto 80. La máquina de StoreFront debe poder acceder directamente al Cloud Connector a través del nombre de dominio completo (FQDN) proporcionado. El Cloud Connector debe poder llegar a la URL de NFuse/STA de Cloud en `https://<customername\>.xendesktop.net/Scripts/wpnbr.dll` y `ctxsta.dll`.
- Agregue Cloud Connectors como Delivery Controllers para obtener alta disponibilidad.

Use la versión más reciente de StoreFront.

#### Acceso externo

Para proporcionar acceso externo a través de Citrix Gateway y StoreFront local ("on-premises"):

- Configure Citrix Gateway como de costumbre, con las directivas de sesión y autenticación. Para obtener información más detallada, consulte la documentación de Citrix Gateway.
- Apunte los Delivery Controllers del almacén local de StoreFront hacia los Citrix Cloud Connectors. Vincule los Cloud Connectors como servidores Secure Ticket Authority (STA) a Citrix Gateway.
- Citrix Gateway debe usar las mismas direcciones URL de STA que StoreFront. Si la puerta de enlace no está ya configurada para usar el STA de un entorno de Citrix Virtual Apps and Desktops existente, se pueden usar los Cloud Connectors como servidores STA.

#### Acceso interno

Para ofrecer acceso interno a través de un almacén local de StoreFront, apunte los Delivery Controllers de dicho almacén a los Citrix Cloud Connectors.

#### Acceso externo e interno

Para proporcionar acceso externo e interno a través de Citrix Gateway y StoreFront local:

- Configure Citrix Gateway como de costumbre, con las directivas de sesión y autenticación. Para obtener información más detallada, consulte la documentación de Citrix Gateway.
- Vincule los Cloud Connectors como servidores Secure Ticket Authority (STA) a Citrix Gateway.
- Apunte los Delivery Controllers del almacén local de StoreFront hacia los Cloud Connectors.

### Caché de host local y StoreFront

La caché de host local permite que la intermediación de las conexiones en una implementación de Citrix DaaS continúe cuando haya Cloud Connectors que no se pueden comunicar con Citrix Cloud.

La función de caché de host local funciona solo en ubicaciones de recursos que contienen un almacén local de StoreFront implementado por el cliente. Con Citrix Workspace, no se admite el uso de caché de host local.

Cada ubicación de recursos debe tener un StoreFront local implementado por el cliente. Verifique que la ubicación de recursos contiene un almacén local de StoreFront que apunta a todos los Cloud Connectors que se encuentran en esa ubicación de recursos.

Para obtener más información, consulte Caché de host local.

## IP virtual y bucle invertido virtual

March 30, 2022

> **Importante:**
>
> La multisesión de Windows 10 Enterprise no admite virtualización de IP de Escritorio remoto (IP virtual) y nosotros no admitimos IP virtual ni bucle invertido virtual en multisesión con Windows 10 Enterprise.

Las funciones de IP virtual y bucle invertido virtual se admiten en máquinas con Windows Server 2016. Sin embargo, no se aplican a las máquinas con SO de escritorio Windows.

La función de dirección IP virtual de Microsoft proporciona una dirección IP exclusiva a una aplicación publicada, asignada dinámicamente para cada sesión. La función de bucle invertido virtual de Citrix permite configurar aplicaciones que dependen de la comunicación con el host local (127.0.0.1 de forma predeterminada) para utilizar una dirección de bucle invertido virtual exclusiva en el intervalo de host local (127.*).

Algunas aplicaciones, como CRM y Computer Telephony Integration (CTI), utilizan una dirección IP para el direccionamiento, las licencias, la identificación y otros fines, y, por lo tanto, requieren una dirección IP exclusiva o una dirección de bucle invertido en las sesiones. Otras aplicaciones pueden enlazar con un puerto estático, por lo que, al intentar iniciar instancias adicionales de una aplicación en un entorno multiusuario, se producirá un error porque el puerto ya está en uso. Para que estas aplicaciones funcionen correctamente en un entorno Citrix Virtual Apps, se necesita una dirección IP exclusiva para cada dispositivo.

Las funciones de IP virtual y bucle invertido virtual son funciones independientes. Puede usar solo una de ellas o ambas.

Sinopsis de acciones de administrador:

- Para utilizar la dirección IP virtual de Microsoft, habilite y configure esta función en el servidor Windows. (No se necesitan configuraciones de directivas de Citrix).

- Para usar el bucle virtual de Citrix, configure dos parámetros en una directiva de Citrix.

## IP virtual

Cuando la función IP virtual está habilitada y configurada en el servidor Windows, cada una de las aplicaciones configuradas que se ejecutan en una sesión parece tener una dirección exclusiva. Los usuarios acceden a dichas aplicaciones en un servidor de Citrix Virtual Apps del mismo modo que acceden a cualquier otra aplicación publicada. Un proceso requiere IP virtual en cualquiera de los siguientes casos:

- El proceso utiliza un número de puerto TCP integrado en el código.
- El proceso utiliza Windows Sockets y requiere una dirección IP exclusiva o un número de puerto TCP específico.

Para determinar si una aplicación necesita utilizar direcciones IP virtuales:

1. Obtenga la herramienta TCPView de Microsoft. Esta herramienta muestra todas las aplicaciones que enlazan puertos y direcciones IP específicas.
2. Inhabilite la función de resolución de direcciones IP de forma que vea las direcciones en lugar de los nombres de host.
3. Ejecute la aplicación y con ayuda de TCPView consulte qué direcciones IP y puertos abre la aplicación y qué nombres de proceso abren estos puertos.
4. Configure los procesos que abren la dirección IP del servidor, 0.0.0.0 o 127.0.0.1.
5. Para asegurarse de que la aplicación no abre la misma dirección IP en otro puerto, ejecute otra instancia de la aplicación.

### Funcionamiento de la virtualización de IP de Escritorio remoto (RD) de Microsoft

- El uso de direcciones IP virtuales debe estar habilitado en el servidor de Microsoft.

  Por ejemplo, en un entorno de Windows Server 2016, desde el Administrador del servidor, expanda **Servicios de Escritorio remoto > Conexiones de host de sesión de Escritorio remoto** para activar la función Virtualización de IP de Escritorio remoto y configure los parámetros para asignar direcciones IP dinámicamente mediante el servidor DHCP (Dynamic Host Configuration Protocol) para cada sesión o cada programa. Consulte la documentación de Microsoft para obtener instrucciones.

- Después de habilitar la función, al comenzar una sesión, el servidor solicita al servidor DHCP las direcciones IP asignadas dinámicamente.

- La función de Virtualización de IP de Escritorio remoto asigna direcciones IP a las conexiones a escritorios remotos por sesión y por programa. Si se asignan direcciones IP para varios programas, éstos comparten una dirección IP por sesión.

- Después de asignar una dirección a una sesión, la sesión utiliza la dirección virtual en lugar de la dirección IP principal del sistema, siempre que se efectúan las siguientes llamadas: `bind`, `closesocket`, `connect`, `WSAConnect`, `WSAAccept`, `getpeername`, `getsockname`, `sendto`, `WSASendTo`, `WSASocketW`, `gethostbyaddr`, `getnameinfo`, `getaddrinfo`.

Con la función de virtualización de IP de Microsoft en la configuración de host de sesiones de Escritorio remoto, las aplicaciones se vinculan con direcciones IP específicas mediante la introducción de un componente de "filtro"entre la aplicación y las llamadas de función de Winsock. La aplicación solo ve entonces la dirección IP que debe usar. Cualquier intento de la aplicación de escuchar comunicaciones TCP o UDP se vincula inmediatamente a su dirección IP virtual asignada (o dirección de bucle invertido) y cualquier conexión de origen abierta por la aplicación se origina desde la dirección IP vinculada a la aplicación.

En funciones que devuelven una dirección, tales como `GetAddrInfo()` (que está controlada por una directiva de Windows), si se solicita la dirección IP local del host, la IP virtual examina la dirección IP devuelta y la cambia a la dirección IP virtual de la sesión. Las aplicaciones que intentan obtener la dirección IP del servidor local a través de dichas funciones de nombre solo ven la dirección IP virtual exclusiva asignada a dicha sesión. Esta dirección IP se utiliza con frecuencia en las posteriores llamadas de socket (tales como bind o connect). Para obtener más información acerca de las directivas de Windows, consulte Virtualización de IP de RDS en Windows Server.

A menudo una aplicación solicita vincularse a un puerto para escuchar en la dirección 0.0.0.0. En ese caso, si además la aplicación utiliza un puerto estático, no podrá ejecutar más de una instancia de la aplicación. La función de dirección IP virtual también busca 0.0.0.0 en estos tipos de llamada y cambia la llamada para escuchar en la dirección IP virtual específica, lo que permite que varias aplicaciones puedan escuchar en el mismo puerto en el mismo equipo, puesto que todas escuchan en diferentes direcciones. La llamada solo se cambia si se está en una sesión ICA y la función de dirección IP virtual está habilitada. Por ejemplo, si dos instancias de una aplicación que se ejecutan en distintas sesiones intentan vincularse a todas las interfaces (0.0.0.0) y un puerto específico, por ejemplo, el 9000, se vinculan a VIPAddress1:9000 y VIPAddress2:9000, por lo que no existen conflictos.

### Bucle invertido virtual

La habilitación de la configuración de directiva de Bucle invertido de IP virtual de Citrix permite que cada sesión disponga de su propia dirección de bucle invertido para las comunicaciones. Cuando una aplicación usa la dirección de host local (predeterminada = 127.0.0.1) en una llamada de Winsock, la función de bucle invertido virtual sencillamente sustituye 127.0.0.1 por 127.X.X.X, donde X.X.X es una representación del ID de sesión + 1. Por ejemplo, un ID de sesión de 7 es 127.0.0.8. En el caso improbable de que un ID de sesión fuera superior al cuarto octeto (más de 255), la dirección pasaría al octeto siguiente (127.0.1.0) hasta el máximo de 127.255.255.255.

Un proceso requiere el bucle invertido virtual en los siguientes casos:

- El proceso usa la dirección de bucle invertido de Windows Sockets del host local (127.0.0.1)
- El proceso utiliza un número de puerto TCP integrado en el código.

Use la configuración de directiva de bucle invertido para aplicaciones que usan una dirección de bucle invertido para la comunicación entre procesos. No se requiere ninguna configuración adicional. La función de bucle invertido virtual no depende de la dirección IP virtual, de modo que no es necesario configurar el servidor de Microsoft.

- Funcionalidad de bucle invertido de IP virtual. Cuando está habilitada, esta configuración de directiva permite que cada sesión tenga su propia dirección virtual de bucle invertido. Este parámetro está inhabilitado de forma predeterminada. La función solo se aplica a las aplicaciones especificadas en la configuración de directiva lista de programas para bucle invertido de IP virtual.
- Lista de programas para bucle invertido de IP virtual. Esta configuración de directiva especifica las aplicaciones que usan la función de bucle invertido de IP virtual. Esta configuración solo se aplica cuando está habilitada la configuración de directiva Funcionalidad de bucle invertido de IP virtual.

#### Funciones relacionadas

Se pueden usar los siguientes parámetros del Registro del sistema para garantizar que se da preferencia al bucle invertido sobre la IP virtual; esto se denomina bucle invertido preferido. Sin embargo, hay que actuar con precaución:

- Utilice el bucle invertido preferido solo cuando tanto IP virtual como Bucle invertido virtual están habilitados; en caso contrario, podría obtener resultados inesperados.
- Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Ejecute regedit en los servidores donde residen las aplicaciones.

- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP
- Nombre: PreferLoopback, Tipo: REG_DWORD, Datos: 1
- Nombre: PreferLoopbackProcesses, Tipo: REG_MULTI_SZ, Datos: <lista de procesos>

# Zonas

May 17, 2024

## Introducción

Las implementaciones de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) que incluyen ubicaciones muy alejadas entre sí, conectadas por una red WAN, pueden presentar problemas de fiabilidad y latencia de la red. El uso de zonas puede ayudar a los usuarios de regiones remotas a conectarse a recursos sin que las conexiones recorran necesariamente grandes segmentos de red WAN. En el entorno de Citrix DaaS, cada ubicación de recursos se considera una zona.

Las zonas pueden resultar útiles en implementaciones de todos los tamaños. Puede usar zonas para mantener las aplicaciones y los escritorios cerca de los usuarios, lo que mejora el rendimiento. Las zonas se pueden usar para: recuperación ante desastres, centros de datos geográficamente alejados, sucursales, una nube o una zona de disponibilidad de una nube.

En este artículo, el término "local"se refiere a la zona que se analiza. Por ejemplo, "un VDA se registra en un Cloud Connector local"significa que el VDA se registra en un Cloud Connector de la zona donde está situado el VDA.

### Diferencias de zonas en entornos locales de Citrix Virtual Apps and Desktops

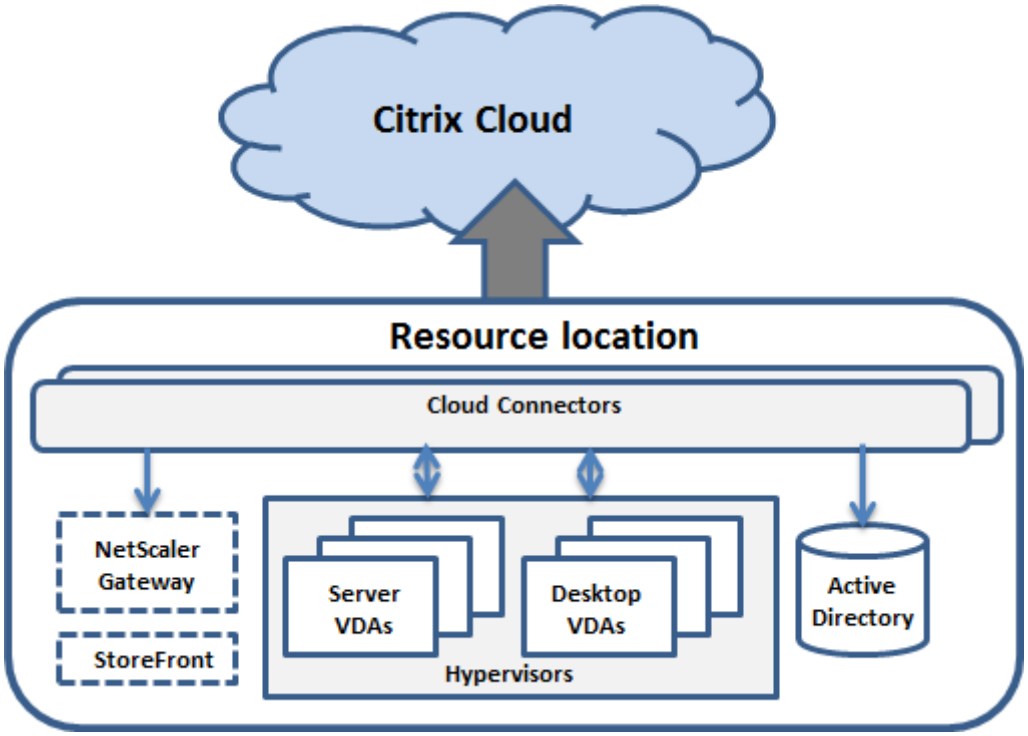
Las zonas de un entorno de Citrix DaaS son parecidas pero no idénticas a las zonas de una implementación local ("on-premises") de Citrix Virtual Apps and Desktops.

- En Citrix DaaS, las zonas se crean automáticamente cuando se crea una ubicación de recursos y se le agrega un Cloud Connector. A diferencia de una implementación "on-premises", un entorno de Citrix DaaS no clasifica las zonas como principales o satélite.
- En XenApp 6.5 y versiones anteriores, las zonas incluían recopiladores de datos. Citrix DaaS no utiliza recopiladores de datos para las zonas. Además, la conmutación por error y la preferencia de zona funcionan de otra manera.

### ¿Qué hay en una zona?

Una zona equivale a una ubicación de recursos. Cuando se crea una ubicación de recursos y se instala un Cloud Connector, se crea automáticamente una zona para usted. Cada zona puede contener un conjunto de recursos diferente, en función del entorno y las necesidades que usted tenga.




Cada zona debe tener al menos un Cloud Connector, pero es preferible tener dos o más, para permitir redundancia.

En una zona se pueden colocar catálogos de máquinas, hipervisores, conexiones de host, usuarios y aplicaciones. Una zona también puede contener servidores StoreFront y Citrix Gateway. Para usar la función Caché de host local, la zona debe tener un servidor StoreFront.

Las zonas son compatibles con Citrix Workspace y Citrix Gateway Service.

Colocar elementos en una zona afecta al modo en que Citrix DaaS interactúa con ellos y con otros objetos relacionados.

- Cuando se coloca una conexión de hipervisor en una zona, se presupone que todos los hipervisores administrados a través de esa conexión también residen en esa zona.
- Cuando se coloca un catálogo de máquinas en una zona, se presupone que todos los VDA de ese catálogo están en esa misma zona.
- Se pueden agregar instancias de Citrix Gateway a las zonas. Cuando se crea una ubicación de recursos, se ve la opción de agregar un Citrix Gateway. Cuando se asocia un Citrix Gateway a una zona, se utiliza preferentemente ese Citrix Gateway en conexiones a los VDA de esa zona.
- Preferiblemente, Citrix Gateway de una zona se usa para conexiones de usuario que llegan a esa zona provenientes de otras zonas o ubicaciones externas. También se puede usar para conexiones dentro de la zona.
- Después de crear más ubicaciones de recursos e instalar Cloud Connectors en ellas (lo que automáticamente crea más zonas), se pueden mover recursos entre las zonas. Esta flexibilidad conlleva el riesgo de separar elementos que funcionan mejor cuando están próximos. Por ejem-

plo: mover un catálogo de máquinas a otra zona distinta de la zona de la conexión (host) que crea las máquinas del catálogo podría afectar al rendimiento. Por lo tanto, tenga en mente los posibles efectos imprevistos antes de mover elementos entre zonas. Mantenga el catálogo y la conexión de host que este usa en la misma zona.

Si falla la conexión entre una zona y Citrix Cloud, la función Caché de host local permite que un Cloud Connector de la zona siga actuando como broker en las conexiones con los VDA de esa zona. (La zona debe tener StoreFront instalado). Por ejemplo, esto es efectivo en una oficina donde los trabajadores utilicen el sitio local de StoreFront para acceder a sus recursos locales, incluso aunque falle el enlace WAN que conecta su oficina a la red de la empresa. Para obtener más información, consulte Caché de host local.

### Dónde se registran los VDA

La versión de los VDA debe ser 7.7 como mínimo para poder usar estas funciones de registro de zona:

- Un VDA de una zona se registra en un Cloud Connector local.
  - Siempre y cuando ese Cloud Connector pueda comunicarse con Citrix Cloud, el funcionamiento continúa normalmente.
  - Si ese Cloud Connector está en funcionamiento, pero no se puede comunicar con Citrix Cloud (y esa zona tiene un almacén local de StoreFront), entra en el modo de interrupción de Caché de host local.
  - Si un Cloud Connector falla, los VDA de esa zona intentan registrarse con otros Cloud Connectors locales. Un VDA de una zona nunca intenta registrarse con un Cloud Connector de otra zona.
- Si se agrega o se quita un Cloud Connector de una zona (desde la consola de administración de Citrix Cloud) y la actualización automática está habilitada, los VDA de esa zona recibirán listas actualizadas de los Cloud Connectors que están disponibles, por lo que sabrán en qué conectores pueden registrarse y de cuáles pueden aceptar conexiones.
- Si mueve un catálogo de máquinas a otra zona (mediante la interfaz de administración de Configuración completa), los VDA de ese catálogo volverán a registrarse en los Cloud Connectors de la zona a la que haya movido el catálogo. Cuando mueva un catálogo, asegúrese de que también mueve a la misma zona las conexiones de host asociadas.
- Durante una interrupción (cuando los Cloud Connectors de una zona no se pueden comunicar con Citrix Cloud), solo están disponibles los recursos asociados con las máquinas que están registradas en esa zona.

## Preferencia de zonas

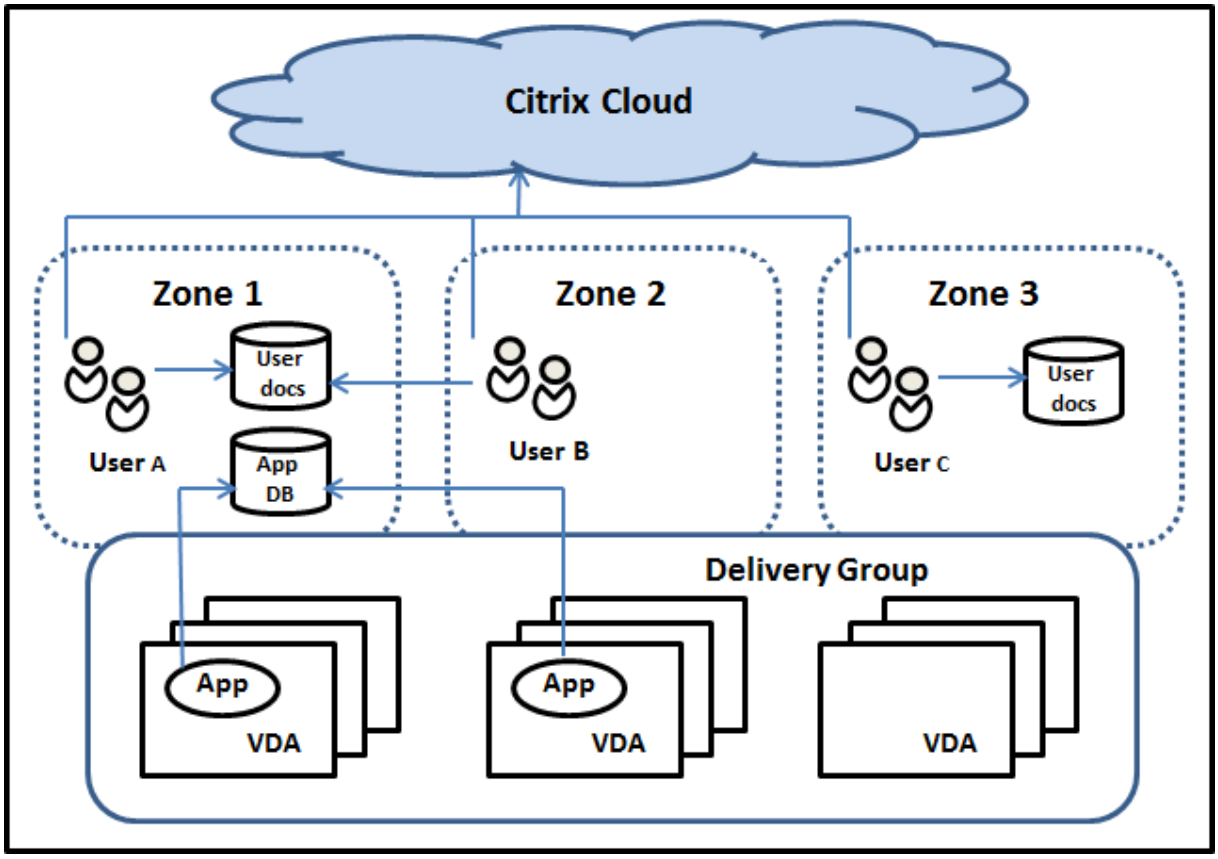
En un sitio de varias zonas, la función Preferencia de zonas ofrece más flexibilidad al administrador para controlar qué VDA se utiliza para iniciar una aplicación o un escritorio.

### Cómo funciona la preferencia de zonas

Existen tres preferencias distintas de zonas. Es posible que prefiera utilizar un VDA en una zona particular, en función de:

- Dónde se almacenan los datos de la aplicación. Esto se conoce como zona particular de la aplicación.
- La ubicación de los datos principales del usuario (por ejemplo, un perfil o un directorio particular en un recurso compartido de red). Esto se conoce como zona particular del usuario.
- La ubicación actual del usuario (dónde se está ejecutando la aplicación Citrix Workspace). Esto se conoce como ubicación del usuario. La ubicación de usuario requiere como mínimo StoreFront 3.7 y Citrix Gateway (antes NetScaler Gateway) 11.0-65.x.

En el gráfico siguiente, se muestra un ejemplo de configuración de varias zonas.




En este ejemplo, los VDA están distribuidos en tres zonas, pero pertenecen todos a un mismo grupo

de entrega. Por lo tanto, el intermediario (broker) de Citrix DaaS puede elegir qué VDA usar cuando un usuario lanza una solicitud de inicio. En este ejemplo se muestra cómo los usuarios pueden ejecutar sus dispositivos de punto final con la aplicación Citrix Workspace en diferentes ubicaciones. El usuario A está utilizando un dispositivo con la aplicación Citrix Workspace en la zona 1. El usuario B está utilizando un dispositivo en la zona 2. Del mismo modo, los documentos de un usuario se pueden almacenar en diferentes ubicaciones. Los usuarios A y B utilizan un recurso de red compartido ubicado en la zona 1. El usuario C utiliza un recurso de red compartido ubicado en la zona 3. Además, una de las aplicaciones publicadas utiliza una base de datos que se encuentra en la zona 1.

Para asociar un usuario o una aplicación a una zona, configure una zona particular específica para ese usuario o esa aplicación. A partir de ahí, el broker usa esas asociaciones para seleccionar la zona donde se lanzará la sesión, si los recursos están disponibles. Puede:

- Configurar la zona particular de un usuario agregándolo a una zona.
- Configurar la zona particular de una aplicación modificando las propiedades de la aplicación.

Un usuario o una aplicación pueden tener solo una zona particular en un momento dado. (Puede darse una excepción para los usuarios cuando se da el caso de que pertenecen a varias zonas debido a que son miembros de varios grupos de usuarios. Sin embargo, incluso en este caso, el broker utiliza una sola zona particular.)

Aunque se puedan configurar las preferencias de zonas para usuarios y aplicaciones, el broker selecciona una sola zona preferida para el inicio. El orden predeterminado de prioridad para seleccionar la zona preferida es: zona particular de la aplicación > zona particular del usuario > ubicación del usuario. Cuando un usuario inicia una aplicación:

- Si la aplicación tiene configurada una asociación de zona (es decir, una zona particular de la aplicación), entonces la zona preferida es la zona particular de esa aplicación.
- En cambio, si la aplicación no tiene configurada una asociación de zona pero el usuario sí la tiene (una zona particular de usuario), entonces la zona preferida es la zona particular del usuario.
- Si ni la aplicación ni el usuario tienen configurada una asociación de zona, entonces la zona preferida es la zona donde el usuario ejecuta la instancia de la aplicación Citrix Workspace (la ubicación del usuario). Si esa zona no está definida, se seleccionan un VDA y una zona aleatorios. El equilibrio de carga se aplica a todos los VDA de la zona preferida. Si no hay ninguna zona preferida, el equilibrio de carga se aplica a todos los VDA del grupo de entrega.

#### Adaptar la preferencia de zonas

Al configurar (o quitar) la zona particular de un usuario o de una aplicación, puede limitar aún más cómo se utilizará (o no) la preferencia de zonas.

- **Uso obligatorio de la zona particular del usuario:** En un grupo de entrega, puede especificar la opción "Iniciar sesión en la zona particular del usuario (si el usuario tiene una), sin conmutación por error a otra zona cuando los recursos no estén disponibles en esa zona particular". Esta restricción es útil para evitar el riesgo de copia de perfiles o archivos de datos grandes entre las zonas. En otras palabras, con esta opción se prefiere denegar el lanzamiento de una sesión a lanzarla en una zona diferente.
- **Uso obligatorio de la zona particular de la aplicación:** Del mismo modo, cuando se configura la zona particular de una aplicación, se puede especificar la opción para que la aplicación se lance "solo en esa zona, sin conmutación por error a otra zona cuando los recursos no estén disponibles en la zona particular de la aplicación".
- **Sin zona particular de aplicación, e ignorar la zona particular configurada del usuario:** Si no especifica ninguna zona particular para una aplicación, también puede especificar la opción para que no se tenga en cuenta ninguna zona de usuario configurada para lanzar esa aplicación. Por ejemplo, use la preferencia de zona de la ubicación del usuario si quiere que los usuarios ejecuten una aplicación concreta en un VDA cercano a la máquina que están usando, aunque algunos usuarios tengan otra zona particular.

#### Cómo afecta la preferencia de zonas al uso de sesiones

Cuando un usuario inicia una aplicación o un escritorio, el broker prefiere usar la zona preferida en lugar de usar una sesión existente.

Si el usuario que inicia la aplicación o escritorio ya tiene una sesión apropiada para el recurso que se va a iniciar (por ejemplo, puede usar la función de compartir sesiones para una aplicación, o bien una sesión que ya ejecuta el recurso que se va a iniciar), pero esa sesión está en un VDA que se encuentra en otra zona, no la preferida de la aplicación o el usuario, el sistema puede crear una nueva sesión. Con esta acción, el inicio se produce en la zona correcta (si tiene capacidad disponible), en vez de reconectarse a una sesión en una zona menos ventajosa para los requisitos de sesión del usuario.

Para que no exista una sesión "huérfana"con la que ya no se pueda establecer conexión, se permite volverse a conectar a las sesiones desconectadas incluso aunque estén en una zona no preferida.

El orden de preferencia para elegir una sesión para el inicio es:

1. Reconectarse a una sesión existente en la zona preferida.
2. Reconectarse a una sesión desconectada existente en una zona que no sea la preferida.
3. Iniciar una sesión nueva en la zona preferida.
4. Reconectarse una sesión conectada existente en una zona que no sea la preferida.
5. Iniciar una sesión nueva en una zona que no sea la preferida.

**Otras consideraciones de preferencia de zonas**

- Si configura la zona particular de un grupo de usuarios (por ejemplo, un grupo de seguridad), los usuarios de ese grupo (por pertenencia directa o indirecta) se asocian a la zona especificada. No obstante, un usuario puede pertenecer a varios grupos de seguridad y, por lo tanto, puede tener otras zonas particulares configuradas por pertenecer a otros grupos. En tales casos, la determinación de la zona particular de ese usuario puede ser ambigua.

  Si un usuario tiene configurada una zona particular que no adquirió por pertenecer a grupos, esa es la zona que se usa para la preferencia de zonas. Se ignoran las asociaciones de zona que se adquieran por pertenecer a grupos.

  Si el usuario tiene varias asociaciones de zonas que adquirió únicamente por pertenecer a grupos, el broker escoge una zona aleatoria de entre ellas. Una vez que el broker hace su elección, se utiliza la misma zona para los lanzamientos subsiguientes de sesión, hasta que cambie la pertenencia del usuario a los grupos.

- La preferencia de zona "ubicación del usuario"requiere que el Citrix Gateway a través del cual se conecta el dispositivo de punto final detecte la aplicación Citrix Workspace en ese dispositivo de punto final. Citrix Gateway debe estar configurado para asociar intervalos de direcciones IP a zonas concretas. La identidad de zona detectada se debe pasar a través de StoreFront a Citrix DaaS.

Aunque se escribió para el uso de zonas en implementaciones locales ("on-premise"), la publicación de blog Zone Preference Internals contiene información técnica relevante.

## Permisos para administrar zonas

Un administrador total puede realizar todas las tareas admitidas de administración de zonas. Mover elementos entre zonas no requiere permisos de zonas (excepto el permiso de lectura de zonas). Sin embargo, debe tener permiso para modificar los elementos que esté moviendo. Por ejemplo, para mover un catálogo de máquinas de una zona a otra, debe tener el permiso de modificar ese catálogo.

**Si utiliza Citrix Provisioning:** La consola de Citrix Provisioning actual no reconoce zonas, por lo que Citrix recomienda usar la interfaz de **Administrar > Configuración completa** para crear catálogos de máquinas que quiera colocar en zonas específicas. Después de crear el catálogo, puede utilizar la consola de Citrix Provisioning para aprovisionar máquinas de ese catálogo.

## Creación de zonas

Cuando se crea una ubicación de recursos en Citrix Cloud y se le agrega un Cloud Connector, Citrix DaaS automáticamente crea y da nombre a una zona. Opcionalmente, puede agregar una descripción

más tarde.

Después de crear otras ubicaciones de recursos (lo que automáticamente crea las zonas correspondientes), se pueden mover recursos de una zona a otra.

Las ubicaciones de recursos y zonas se sincronizan regularmente, por lo general cada cinco minutos aproximadamente. Por lo tanto, si cambia el nombre de una ubicación de recursos en Citrix Cloud, ese cambio se propaga a la zona asociada en los cinco minutos siguientes.

### Agregar o cambiar una descripción de zona

Aunque no puede cambiar el nombre de una zona, puede agregar o cambiar su descripción.

1. En **Administrar > Configuración completa**, seleccione **Zonas** en el panel de la izquierda.
2. Seleccione una zona en el panel central y, a continuación, seleccione **Modificar zona** en la barra de acciones.
3. Agregue o cambie la descripción de la zona.
4. Seleccione **Aceptar** o **Aplicar**.

### Mover recursos de una zona a otra

1. En **Administrar > Configuración completa**, seleccione **Zonas** en el panel de la izquierda.
2. Seleccione una zona en el panel central y, a continuación, seleccione uno o varios elementos.
3. Arrastre los elementos a la zona de destino o seleccione **Mover elementos** en la barra de acciones y, a continuación, especifique la zona a la que moverlos. (Aunque se pueden seleccionar Cloud Connectors, en realidad los conectores no pueden moverse a otra zona.)

Aparecerá un mensaje de confirmación con una lista de los elementos seleccionados y preguntará si quiere moverlos todos.

Recuerde: Si un catálogo de máquinas usa una conexión de host a un hipervisor o un servicio de nube, ambos (el catálogo y la conexión) deben estar en la misma zona. De lo contrario, el rendimiento puede verse afectado. Si mueve un elemento, mueva el otro.

### Eliminación de zonas

Las zonas no pueden eliminarse. Sin embargo, sí que puede eliminar una ubicación de recursos (después de quitar sus Cloud Connectors). Al eliminar la ubicación de recursos, la zona correspondiente se elimina automáticamente.

- Si la zona no contiene ningún elemento (como catálogos, conexiones, aplicaciones o usuarios), la zona se elimina durante la siguiente sincronización entre las zonas y las ubicaciones de recursos. La sincronización se produce cada cinco minutos.

- Si la zona contiene elementos, la zona se elimina automáticamente una vez que se han quitado todos ellos.

### Agregar una zona particular a un usuario

Configurar la zona particular de un usuario también se conoce como *agregar un usuario a una zona*.

1. En **Administrar > Configuración completa**, seleccione **Zonas** en el panel de la izquierda.
2. Seleccione una zona en el panel central y, a continuación, seleccione **Agregar usuarios a la zona** en la barra de acciones.
3. En el cuadro de diálogo **Agregar usuarios a la zona**, seleccione **Agregar** y, a continuación, seleccione los usuarios y los grupos de usuarios que quiera agregar a la zona. Si especifica usuarios que ya tienen su zona particular, aparecerá un mensaje con dos opciones: **Sí**, que equivale a agregar solo a los usuarios especificados que no tengan ninguna zona particular; **No**, que equivale a volver al diálogo de selección de usuarios.
4. Seleccione **OK**.

Para los usuarios que tengan una zona particular configurada, puede definir que las sesiones se inicien solo desde su zona particular correspondiente:

1. Cree o modifique un grupo de entrega.
2. En la página **Usuarios**, marque la casilla **Las sesiones deben iniciarse en la zona particular del usuario, si está configurada**.

Todas las sesiones que inicie un usuario de ese grupo de entrega deberán iniciarse desde las máquinas que se encuentren en la zona particular de ese usuario. Si un usuario del grupo de entrega no tiene configurada una zona particular, este parámetro no tiene ningún efecto.

### Eliminar la zona particular de un usuario

Este procedimiento también se conoce como quitar un usuario de una zona.

1. En **Administrar > Configuración completa**, seleccione **Zonas** en el panel de la izquierda.
2. Seleccione una zona en el panel central y, a continuación, seleccione **Quitar usuarios de la zona** en la barra de acciones.
3. En el cuadro de diálogo **Agregar usuarios a la zona**, seleccione **Quitar** y, a continuación, seleccione los usuarios y los grupos que quiera quitar de la zona. Esta acción solo quita los usuarios de la zona en cuestión. Esos usuarios siguen estando en los grupos de entrega a los que pertenecen.
4. Confirme la eliminación cuando se le solicite.

### Administrar zonas particulares de aplicaciones

Configurar la zona particular de una aplicación también se conoce como agregar una aplicación a una zona. De forma predeterminada, en un entorno de varias zonas, una aplicación no tiene ninguna zona particular.

La zona particular de una aplicación se especifica en las propiedades de la aplicación. Puede configurar las propiedades de una aplicación en el momento de agregarla a un grupo, o más adelante.

- Al crear un grupo de entrega o agregar aplicaciones a grupos existentes, seleccione **Propiedades** en la página **Aplicaciones** del asistente.
- Para cambiar las propiedades de una aplicación después de agregarla, seleccione **Zonas** en el panel de la izquierda. Seleccione una aplicación y, a continuación, seleccione **Propiedades** en la barra de acciones.

En la página **Zonas** de las propiedades o ajustes de la aplicación:

- Si quiere que la aplicación tenga una zona particular:
  - Marque la opción **Usar la zona seleccionada para determinar** donde se inicia esta aplicación y, a continuación, seleccione la zona.
  - Si quiere que la aplicación solo se inicie desde la zona seleccionada (ninguna otra), marque la casilla situada debajo de la selección de zonas.
- Si no quiere que la aplicación tenga una zona particular:
  - Seleccione la opción **No configurar una zona particular para esta aplicación**.
  - Si no quiere que el broker tenga en cuenta ninguna de las zonas de usuario configuradas cuando se inicie esta aplicación, marque la casilla situada bajo el botón de opción. En ese caso, no se utilizará ninguna zona particular de aplicación o de usuario para determinar dónde iniciar esta aplicación.

### Otras acciones que implican especificar zonas

Si tiene más de una zona, puede especificar una de ellas cuando agregue una conexión de host o cree un catálogo. Las zonas se enumeran alfabéticamente en las listas de selección. De forma predeterminada, se selecciona el primer nombre de la lista alfabética.

### Solución de problemas

Configuración completa le proporciona alertas proactivas para garantizar que la caché de host local y las zonas estén correctamente configuradas, de modo que pueda resolver los problemas a tiempo

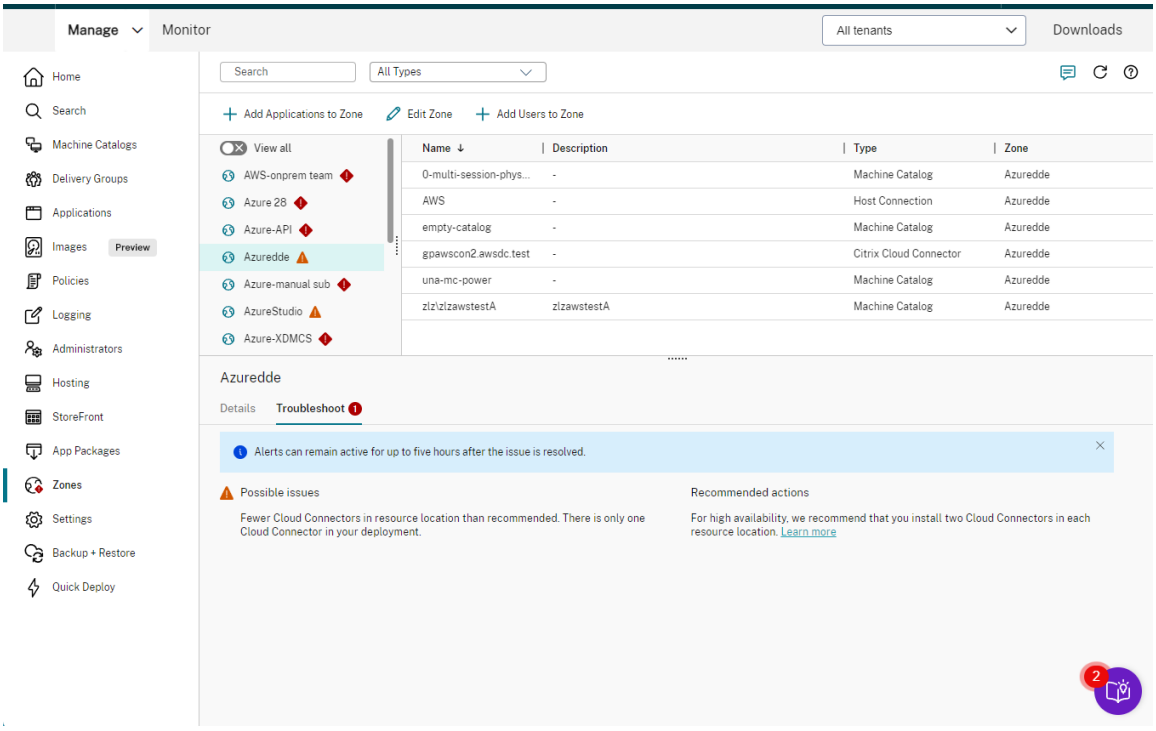
antes de que una interrupción afecte a sus usuarios. Esta función ayuda a mantener el acceso continuo de los usuarios a las cargas de trabajo críticas.

Aparece una ficha **Solucionar problemas** para cada zona con problemas.

Para comprobar los problemas relacionados con la zona, siga estos pasos:

1. Vaya a **Configuración completa > Zonas** y haga clic en la zona con el icono de advertencia.
2. Vaya a la ficha **Solucionar problemas** en el panel inferior y lea la información que aparece allí.

> **Nota:**
>
> Los diagnósticos se actualizan cada hora.
>
> Ejemplo de información de solución de problemas:




La siguiente tabla proporciona una lista completa de las advertencias y errores relacionados con la zona:

| Gravedad | Posibles problemas | Acciones recomendadas |
| --- | --- | --- |
| Advertencia | La ubicación de recursos contiene varios dominios. Con varios dominios en una ubicación de recursos, si las relaciones de confianza no están configuradas correctamente, los VDA pueden tardar más en registrarse. Además, es posible que los VDA no se registren en el modo de alta disponibilidad. | Asegúrese de que las relaciones de confianza entre los dominios de esta ubicación de recursos estén correctamente configuradas. Consulte Detalles técnicos de Citrix Cloud Connector. |
| Advertencia | Hay más conexiones de host en la ubicación de recursos de las recomendadas. Al superar el límite, es posible que el rendimiento se degrade, lo que afectaría a la experiencia del usuario. | Reduzca la cantidad de conexiones de host de esta ubicación de recursos para no superar el límite recomendado. Consulte Límites. |
| Advertencia | Hay menos procesadores de CPU lógicas que los recomendados. En el modo de alta disponibilidad, es posible que el rendimiento se degrade. | Compruebe que cada Cloud Connector cumpla con los requisitos mínimos de procesador de CPU lógica. Consulte Caché de host local. |
| Advertencia | Hay menos Cloud Connectors en la ubicación de recursos de lo recomendado. Solo hay un Cloud Connector en su implementación. | Para tener alta disponibilidad, se recomienda instalar dos Cloud Connectors en cada ubicación de recursos. Consulte Detalles técnicos de Citrix Cloud Connector. |
| Advertencia | Menos RAM de la recomendada en, al menos, un Cloud Connector. En el modo de alta disponibilidad, es posible que el rendimiento se degrade. | Asegúrese de que cada Cloud Connector cumpla con los requisitos mínimos de RAM. Consulte Consideraciones de escala y tamaño para los Cloud Connectors. |

| Gravedad | Posibles problemas | Acciones recomendadas |
| --- | --- | --- |
| Error | Hay más VDA en la ubicación de recursos de los recomendados. En el modo de alta disponibilidad, la caché de host local solo permite el registro de 10 000 VDA. No podrá registrar VDA adicionales. | Reduzca la cantidad de VDA de esta ubicación de recursos para no superar el límite recomendado. Consulte Límites. |
| Error | No se puede acceder a los Cloud Connectors de la zona. No se puede acceder a ninguno de los Cloud Connectors de la zona. Es posible que los VDA de esta ubicación de recursos no estén disponibles, a menos que la caché de host local o la continuidad del servicio estén configuradas para su implementación. | Revise la conectividad de los Cloud Connectors de la zona y consulte el registro para verificar si el modo de caché de host local (LHC) está forzado a través del registro. Si el registro no fuerza el modo LHC, considere la posibilidad de ejecutar la utilidad de comprobación de la conectividad de Cloud Connector. Si el problema persiste, abre un tíquet de asistencia. |

## Supervisar

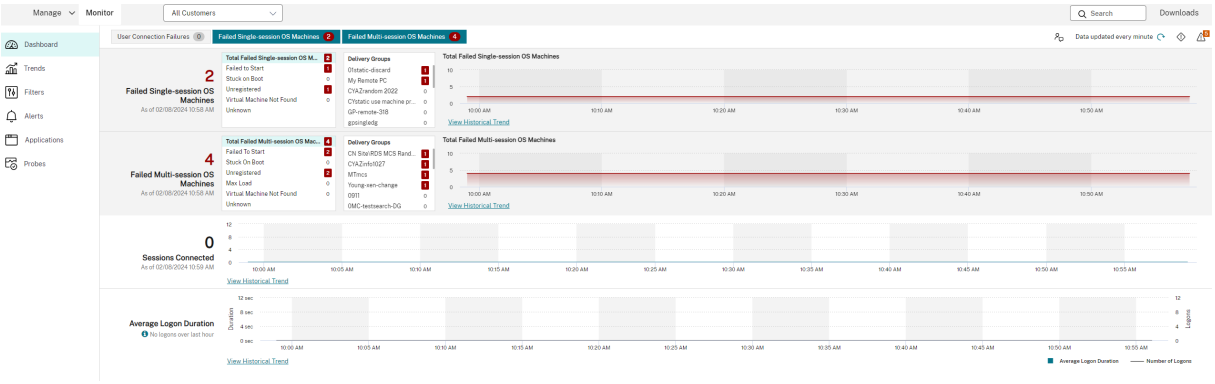
February 21, 2024

Los administradores y el personal de asistencia técnica pueden supervisar Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) desde **Supervisar**, la consola de supervisión y solución de problemas. La ficha **Supervisar** muestra un panel de mandos que ayuda a supervisar, solucionar problemas y realizar tareas de asistencia técnica para los suscriptores.

> **Nota:**
>
> Supervisar está disponible como la consola de Director para supervisar y solucionar problemas de implementación de Versión actual y LTSR de Citrix Virtual Apps and Desktops.

Para acceder a **Supervisar**, inicie sesión en Citrix Cloud. En el menú superior de la izquierda, seleccione **Mis servicios > DaaS**. Haga clic en **Supervisar**.




> **Nota:**
>
> La resolución de pantalla óptima recomendada para ver Supervisar de Citrix es de 1440 x 1024.

Supervisar proporciona:

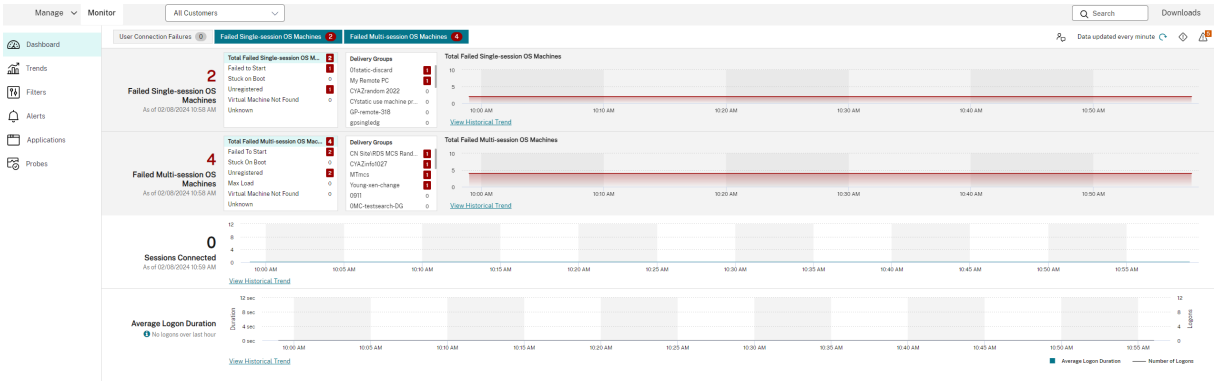
- Datos en tiempo real de Broker Agent mediante una consola unificada integrada con Analytics y Performance Manager.
- Analytics incluye la administración de rendimiento para garantizar el estado y la capacidad de la implementación y tendencias históricas con el fin de identificar cuellos de botella en el entorno de Citrix DaaS.
- Datos históricos almacenados en la base de datos de Supervisar para acceder a la base de datos de registros de configuración.
- Obtenga visibilidad sobre la experiencia de los usuarios finales en aplicaciones y escritorios virtuales de Citrix DaaS.
- Supervisar utiliza un panel de mandos para la solución de problemas que ofrece un historial de supervisión en tiempo real del estado de Citrix DaaS. Esta función permite ver los fallos en tiempo real, lo que proporciona una mejor idea de la experiencia del usuario final.

## Análisis de sitios

March 30, 2024

El panel de mandos de Supervisar ofrece una ubicación centralizada desde la que puede supervisar el estado y el uso de un sitio.




Si no hay fallos y no se han producido fallos en los últimos 60 minutos, los paneles permanecen contraídos. Cuando hay fallos, el panel de fallos específicos aparecerá automáticamente.

| Panel | Descripción |
| --- | --- |
| Fallos de conexión de usuario | Fallos de conexión en los últimos 60 minutos. Haga clic en las categorías junto al número total para ver las mediciones para ese tipo de fallo. En la tabla adyacente, ese número se clasifica además en función de cada grupo de entrega. Los fallos de conexión incluyen fallos provocados por haberse alcanzado el límite de las aplicaciones. Para obtener más información acerca de los límites para aplicaciones, consulte Aplicaciones. |
| Máquinas con SO de sesión única fallidas o Máquinas con SO multisesión fallidas | Total de fallos en los últimos 60 minutos clasificados por grupos de entrega. Fallos clasificados por tipos, incluidos los tipos “No se iniciaron”, “Atascadas en el arranque”y “Sin registrar”. Para máquinas con sistema operativo multisesión, los fallos también incluyen máquinas que alcanzan el máximo de carga. |
| Sesiones conectadas | Sesiones conectadas en todos los grupos de entrega durante los últimos 60 minutos. |

| Panel | Descripción |
| --- | --- |
| Promedio de duración de inicio de sesión | Datos de inicio de sesión durante los últimos 60 minutos. El número grande a la izquierda es el promedio de la duración de los inicios de sesión durante la última hora. Los datos de inicio de sesión de VDA anteriores a XenDesktop 7.0 no están incluidos en esta media. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios. |

> **Nota:**
>
> Cuando el tipo de host en uso no admite ninguna métrica en particular, no aparece ningún icono para esa métrica en particular. Por ejemplo: no hay información de estado disponible de los hosts de System Center Virtual Machine Manager (SCVMM), de Amazon Web Services ni de CloudStack.

Continúe solucionando problemas con estas opciones (que se documentan en las siguientes precedentes):

- Controlar la energía de la máquina del usuario
- Impedir conexiones a máquinas

### Supervisar sesiones

Si una sesión se desconecta, sigue activa y sus aplicaciones siguen ejecutándose. Sin embargo, el dispositivo de usuario ya no se comunica con el servidor.

| Acción | Descripción |
| --- | --- |
| Ver la máquina o sesión a la que está conectado un usuario | En las vistas Administrador de actividades y Detalles del usuario, se puede ver la máquina o la sesión a la que está conectado un usuario en ese momento. También se puede ver una lista de todas las máquinas y sesiones a las que tiene acceso ese usuario. Para tener acceso a esta lista, haga clic en el icono de cambio de sesión en la barra de título de usuario. Para obtener más información, consulte Restaurar sesiones. |

| Acción | Descripción |
| --- | --- |
| Ver la cantidad total de sesiones conectadas en todos los grupos de entrega | En el Panel de mandos, en el panel **Sesiones conectadas**, se puede ver la cantidad total de sesiones conectadas en todos los grupos de entrega durante los últimos 60 minutos. A continuación, haga clic en el número total grande para abrir la vista Filtros. Aquí puede mostrar datos gráficos de la sesión en función de los grupos e intervalos de entrega seleccionados y del uso en los distintos grupos de entrega. |
| Finalizar sesiones inactivas | La vista Filtros de sesiones muestra los datos relacionados con todas las sesiones activas. Puede filtrar las sesiones en función del usuario asociado, grupo de entrega, estado de la sesión y de un tiempo de inactividad mayor a un umbral de período de tiempo. En la lista filtrada, seleccione las sesiones a cerrar o desconectar. Para obtener más información, consulte Solucionar problemas de aplicaciones. |
| Ver datos para un período más largo | En la vista **Tendencias** , seleccione la ficha **Sesiones** para obtener datos de uso más específicos. Puede desglosar los datos de las sesiones conectadas y desconectadas durante un período de tiempo más prolongado. Puede ver los totales de las sesiones anteriores a los últimos 60 minutos. Para ver esta información, haga clic en **Ver tendencias históricas**. |

> **Nota:**
>
> Tenga en cuenta que un dispositivo de usuario se ejecuta en un Virtual Delivery Agent (VDA) antiguo, como un VDA anterior a la versión 7 o Linux VDA. En este caso, Supervisar no puede mostrar la información completa sobre la sesión. En vez de ello, aparece un mensaje donde se indica que la información no está disponible.

**Limitación de reglas de asignación de escritorios:**
La consola Administrar permite la asignación de varias reglas de asignación de escritorios (DAR) para distintos usuarios o grupos de usuarios a un solo VDA en el grupo de entrega. StoreFront muestra el escritorio asignado con el **nombre simplificado** correspondiente a las reglas DAR para el usuario que

ha iniciado sesión. Sin embargo, Supervisar no admite las reglas de asignación de escritorios y, por tanto, muestra el escritorio asignado que usa el nombre del grupo de entrega, sin tener en cuenta qué usuario está conectado a la sesión. Como resultado de ello, no se puede asignar un escritorio específico a una máquina en Supervisar.

Puede asignar el escritorio asignado que se muestra en StoreFront al nombre del grupo de entrega que se muestra en Supervisar. Para la asignación, use el siguiente comando de PowerShell:

```
Get-BrokerDesktopGroup | Where-Object {
  $_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

Ejecute el comando anterior de PowerShell mediante el SDK de PowerShell remoto como se describe en el blog.

#### Inhabilitar la visibilidad de las aplicaciones en ejecución en el Administrador de actividades

De forma predeterminada, el Administrador de actividades muestra una lista de todas las aplicaciones que haya en ejecución en la sesión del usuario. Todos los administradores que tienen acceso a la función Administrador de actividades pueden ver esta información. Para los roles de administrador delegado, esta vista incluye los roles de administrador total, administrador de grupos de entrega y administrador de asistencia técnica.

Para proteger la privacidad de los usuarios y las aplicaciones que estos ejecutan, puede configurar que la ficha **Aplicaciones** no muestre las aplicaciones en ejecución. Para ello, en el VDA, modifique la clave de Registro en HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. De forma predeterminada, el valor de la clave es 1. Cambie el valor a 0 para que la información no se recopile del VDA y, por tanto, no se muestre en el Administrador de actividades.

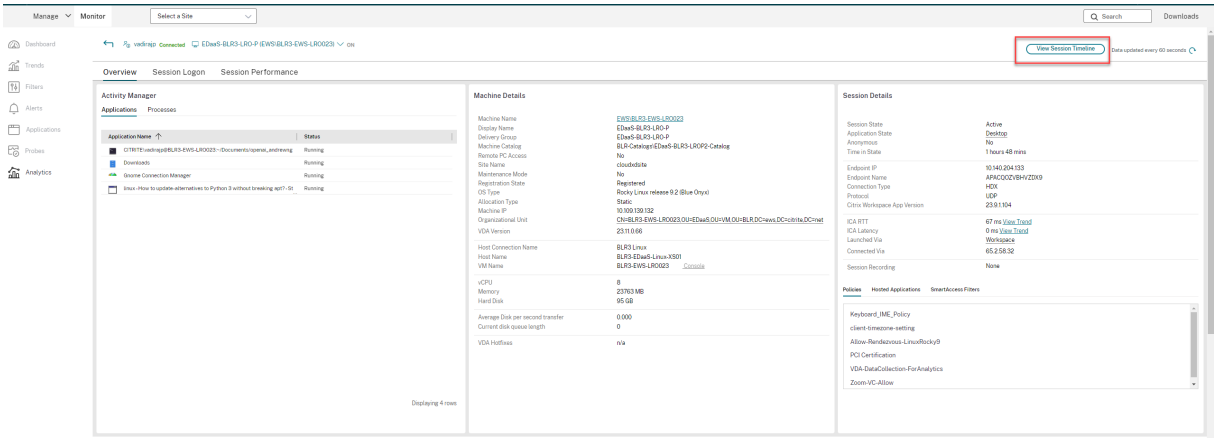
> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

#### Acceder a Citrix Analytics for Performance: Detalles de la sesión

Se puede acceder a la página Session Details de Citrix Analytics for Performance desde Supervisar. Al hacer clic en **View Session Timeline** en la sección de **detalles de las sesiones** del Administrador de

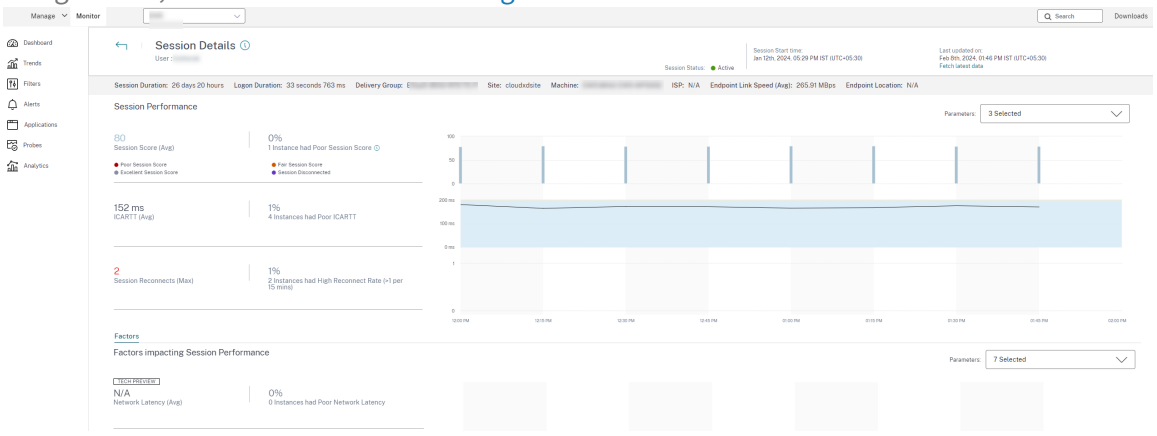
actividades, se abre la página de detalles de la sesión de Citrix Analytics for Performance en Supervisar.




**Nota:**

Esta función requiere que tenga derecho a usar Citrix Analytics for Performance.

Los detalles de la sesión están disponibles para las sesiones categorizadas como Excellent, Fair o Poor (excelente, media o mala, respectivamente) en Citrix Analytics for Performance. Para obtener más información sobre los motivos por los que es posible que una sesión no esté categorizada, consulte el artículo No categorizadas.



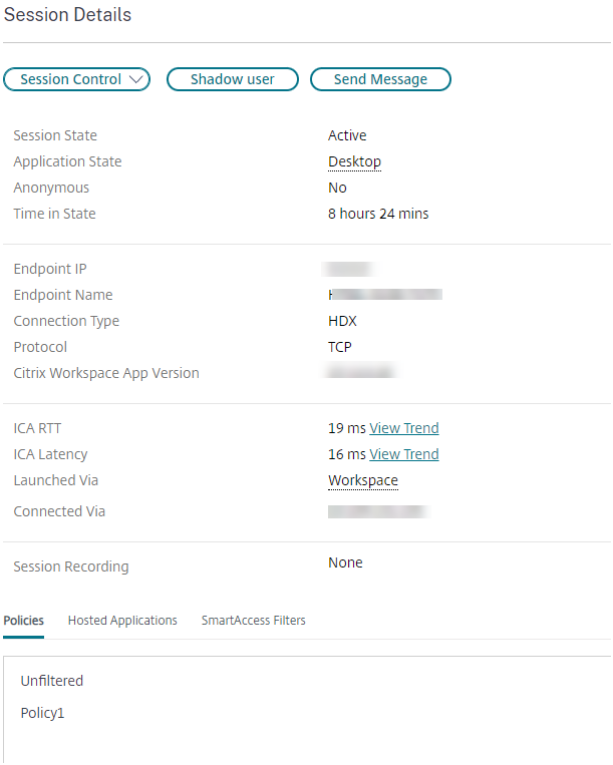

Puede ver una tendencia de la experiencia con respecto a la sesión durante los últimos tres días. Esta vista de tendencias también incluye los factores que contribuyen a dicha experiencia. Esta información complementa los datos en tiempo real disponibles en Supervisar, que el administrador del servicio de asistencia utiliza para solucionar problemas relacionados con la experiencia de la sesión.

Para obtener más información sobre la página Detalles de la sesión, consulte Detalles de la sesión.

### Protocolo de transporte en la sesión

El protocolo de transporte que se utiliza para el tipo de conexión HDX en la sesión actual aparece en el panel **Detalles de la sesión**. Esta información está disponible para las sesiones iniciadas en los VDA 7.13 o una versión posterior.




Utilice el menú desplegable **Control de sesión** en el panel **Detalles de la sesión** para cerrar o desconectar una sesión.

- Para el tipo de conexión **HDX**:
  - El protocolo que se muestra es **UDP** si se utiliza EDT para la conexión HDX.
  - El protocolo que se muestra es **TCP** si se utiliza TCP para la conexión HDX.
- Para el tipo de conexión **RDP**, el protocolo se muestra como **n/d**.

Cuando se configura el transporte adaptable, el protocolo de transporte de la sesión cambia dinámicamente entre EDT (sobre UDP) y TCP, según las condiciones de red. Si no se puede establecer la sesión HDX por el protocolo EDT, se recurre al protocolo TCP.

Para obtener más información sobre cómo configurar el transporte adaptable, consulte Transporte adaptable.

## Exportar informes

Puede exportar los datos de tendencias para generar informes de uso habitual y administración de capacidad. En la exportación, se admiten los formatos PDF, Excel y CSV. Los informes en formatos PDF o Excel incluyen datos de tendencias representados en gráficos y tablas. Los informes en formato CSV contienen datos tabulares que puede usar para generar vistas o archivarlos.

Para exportar un informe:

1. Vaya a la ficha **Tendencias**.
2. Establezca los criterios de filtrado, el período de tiempo y haga clic en **Aplicar**. La tabla y el gráfico de tendencias se rellenan con los datos.
3. Haga clic en **Exportar**, y escriba el nombre y el formato del informe.

Supervisar genera el informe en función de los criterios de filtrado que haya seleccionado. Si cambia los criterios de filtrado, haga clic en **Aplicar** antes de hacer clic en **Exportar**.

> **Nota:**
>
> La exportación de una gran cantidad de datos implica un aumento significativo en el consumo de memoria y de CPU en el servidor de Supervisar, el Delivery Controller y los servidores SQL. Se establecen límites predeterminados a la cantidad admitida de operaciones de exportación simultáneas y a la cantidad de datos que pueden exportarse con el fin de lograr un rendimiento óptimo de exportación.

### Límites de exportación admitidos

Los informes en PDF y Excel exportados contienen gráficos completos de los criterios de filtrado seleccionados. Sin embargo, los datos tabulares de todos los formatos de informe se truncan si superan los límites predeterminados de cantidad de filas o registros que haya en la tabla. La cantidad predeterminada de registros admitidos se define en función del formato de informe.

| Formato del informe | Cantidad predeterminada de registros admitidos |
|---|---|
| PDF | 500 |
| Excel | 100 000 |
| CSV | 100 000 (10 000 000 en la ficha **Sesiones**) |

### Gestión de errores

Errores que pueden producirse durante una operación de exportación:

- **Se agotó el tiempo de espera de Director:** Este error puede darse por problemas de red o por un consumo alto de recursos por parte de Monitor Service o en el servidor de Director.
- **Se agotó el tiempo de espera de Supervisar:** Este error puede darse por problemas de red o por un consumo alto de recursos por parte de Monitor Service o en SQL Server.
- **Cantidad máxima de operaciones simultáneas de exportación o vista previa en curso:** Solo puede haber una instancia activa de exportación o vista previa en un momento dado. Si recibe el error **Cantidad máxima de operaciones simultáneas de exportación o vista previa en curso**, vuelva a intentar más tarde la siguiente operación.

### Supervisar parches rápidos

Para ver los parches rápidos instalados en la máquina (física o VM) de un VDA concreto, elija la vista **Detalles de la máquina**.

### Controlar los estados de energía de la máquina del usuario

Para controlar el estado de las máquinas que selecciona en Supervisar, use las opciones de Control de energía. Estas opciones están disponibles para máquinas con SO de sesión única, pero podrían no estar disponibles para máquinas con SO multisesión.

> **Nota:**
>
> Esta función no está disponible para máquinas físicas ni para máquinas que usan el acceso con Remote PC.

| Comando | Función |
| --- | --- |
| **Reiniciar** | Realiza un apagado ordenado (suave) de la VM, y todos los procesos que se estén ejecutando se detienen uno por uno antes de reiniciar la VM. Por ejemplo, seleccione las máquinas que aparecen en Supervisar como “No se iniciaron”y use este comando para reiniciarlas. |
| **Forzar reinicio** | Reinicia la máquina virtual sin antes realizar un procedimiento de apagado. Este comando funciona igual que desenchufar un servidor físico y, a continuación, volverlo a enchufar y volverlo a iniciar. |

| Comando | Función |
| --- | --- |
| **Apagar** | Realiza un cierre ordenado (estable) de la VM, y todos los procesos que se estén ejecutando se detienen uno por uno. |
| **Forzar apagado** | Apaga la máquina virtual sin realizar un procedimiento de apagado ordenado. Este comando funciona igual que desenchufar un servidor físico. No siempre se cierran todos los procesos en ejecución, por lo que corre el riesgo de perder datos si apaga una VM de este modo. |
| **Suspender** | Suspende una VM en ejecución en su estado actual y guarda ese estado en el repositorio de almacenamiento predeterminado. Esta opción permite apagar el servidor host de la VM y más tarde, después de un reinicio, reanudar la VM devolviéndola al estado de ejecución en que estaba. |
| **Reanudar** | Reanuda una VM que fue suspendida, devolviéndola al estado de ejecución en el que se encontraba. |
| **Iniciar** | Inicia una VM cuando está desactivada (también llamado un inicio "en frío"). |

Si las acciones de control de energía fallan, pase el puntero sobre la alerta y aparecerá un mensaje emergente con información detallada sobre el fallo.

### Impedir conexiones a máquinas

Use el modo de mantenimiento para impedir nuevas conexiones temporalmente, mientras el administrador realiza tareas de mantenimiento en la imagen.

Cuando se habilita el modo de mantenimiento en las máquinas, no se permiten nuevas conexiones hasta que se inhabilita dicho modo. Si hay usuarios con sesiones ya iniciadas, el modo de mantenimiento entra en vigor cuando todos los usuarios cierran sus sesiones. Para los usuarios que no cierren sesión, envíeles un mensaje informándoles de que las máquinas se apagarán al cabo de cierto tiempo. Puede usar los controles de energía para forzar el apagado de las máquinas.

1. Seleccione la máquina en, por ejemplo, la vista Detalles del usuario o un grupo de máquinas en la vista Filtros.

2. Seleccione **Modo de mantenimiento** y active esta opción.

Si un usuario intenta conectarse a un escritorio asignado mientras este se encuentra en el modo de mantenimiento, aparecerá un mensaje para indicar que el escritorio no se encuentra disponible. No se pueden establecer nuevas conexiones hasta que se inhabilite el modo de mantenimiento.

### Análisis de aplicaciones

La ficha **Aplicaciones** muestra datos de análisis de aplicaciones en una vista única y consolidada, con el fin de ayudar a analizar y gestionar de forma eficiente el rendimiento de las aplicaciones. Puede obtener información valiosa sobre el estado y el uso de todas las aplicaciones publicadas en el sitio. Muestra métricas como estas:

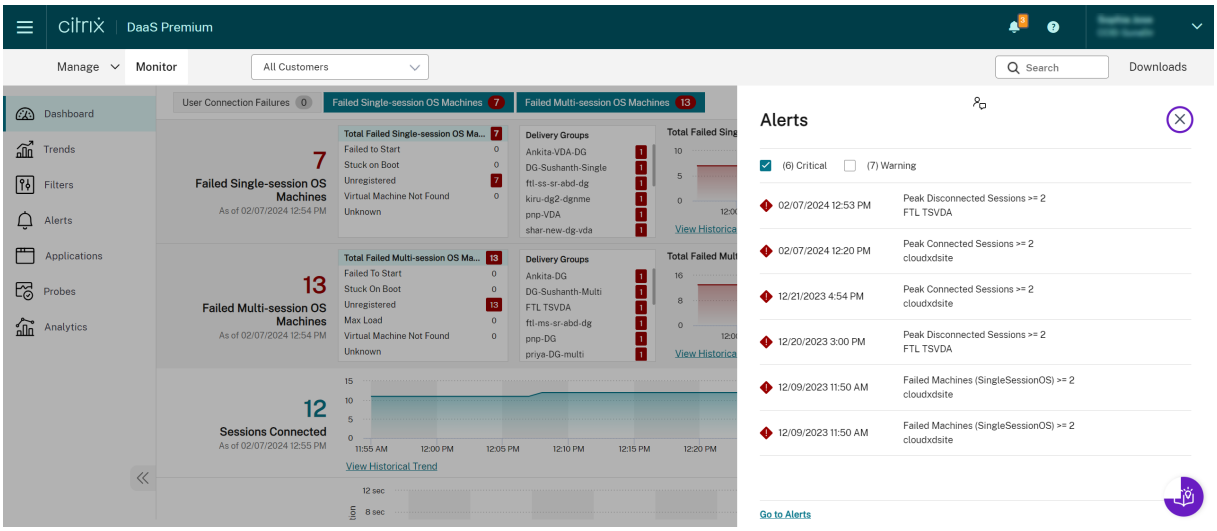
- Resultados del sondeo
- Cantidad de instancias por aplicación
- Fallos y errores asociados a las aplicaciones publicadas

Para obtener más información, consulte la sección Análisis de aplicaciones en **Solucionar problemas de aplicaciones**.

## Alertas y notificaciones

February 21, 2024

En Supervisar, las alertas se muestran en el panel de mandos y en otras vistas de alto nivel mediante símbolos de alertas críticas y advertencias. Las alertas se actualizan automáticamente cada minuto, aunque también se pueden actualizar a petición.



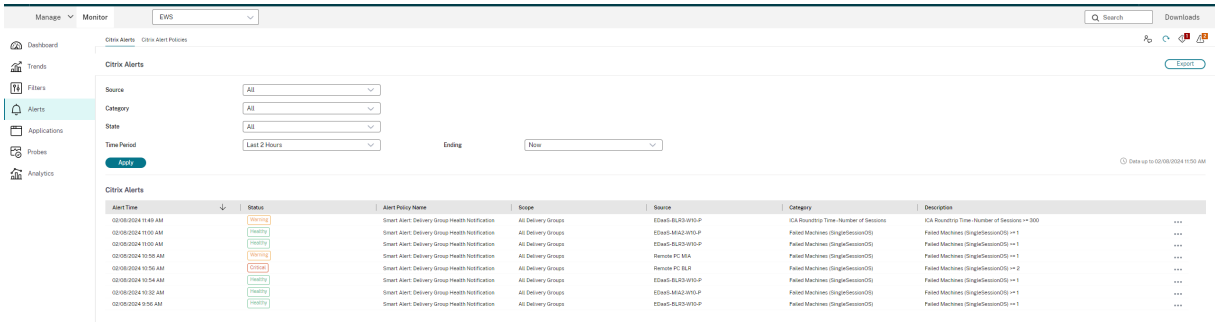

 

Una alerta de advertencia (un triángulo ámbar) indica que se ha alcanzado o superado el umbral de advertencia de una condición.

Una alerta crítica (un círculo rojo) indica que se ha alcanzado o superado el umbral crítico de una condición.

Puede acceder a información más detallada acerca de las alertas. Para ello, seleccione una alerta de la barra lateral, y haga clic en el enlace **Ir a Alertas** situado en la parte inferior de la barra lateral, o bien, seleccione **Alertas** en la parte superior de la página de Supervisar.

En la vista Alertas, puede filtrar y exportar alertas. Por ejemplo, puede ver las máquinas con sistema operativo multisesión pertenecientes a un grupo de entrega específico que han fallado durante el último mes, o bien puede ver todas las alertas de un usuario concreto. Para obtener más información, consulte Exportar informes.




## Alertas de Citrix

Las alertas de Citrix son las que se originan en componentes de Citrix. Puede configurar las alertas de Citrix desde Supervisar, en **Alertas** > **Directiva de alertas de Citrix**. Durante la configuración, puede definir las notificaciones que se enviarán por correo electrónico a usuarios y grupos cuando las alertas superen los umbrales que haya configurado. Para obtener más información sobre la configuración de alertas de Citrix, consulte Crear directivas de alertas.

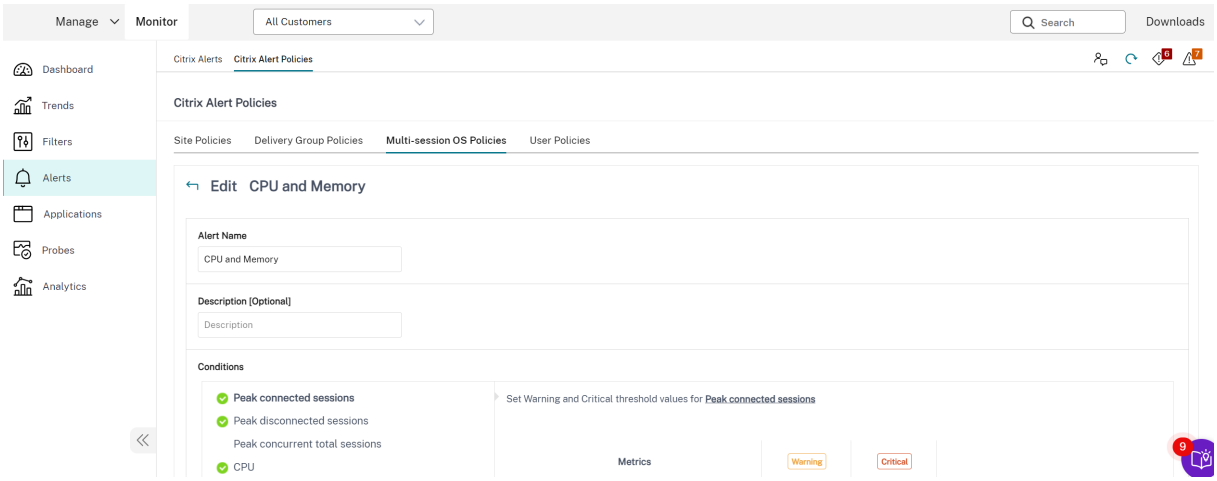
## Directivas de alertas inteligentes

Dispone de un conjunto de directivas de alertas integradas con valores de umbral predefinidos para el ámbito de grupos de entrega y el ámbito VDA con SO multisesión. Puede modificar los parámetros de umbral de las directivas de alertas integradas en **Alertas** > **Directiva de alertas de Citrix**.
Las directivas de alertas integradas se crean cuando hay al menos un objetivo de alerta: un grupo de entrega o un VDA de SO multisesión definido en el sitio. Además, estas alertas integradas se agregan automáticamente a un nuevo grupo de entrega o a un VDA de SO multisesión.

Las directivas de alertas integradas se crean solo si no existen reglas de alertas correspondientes en la base de datos de Supervisar.

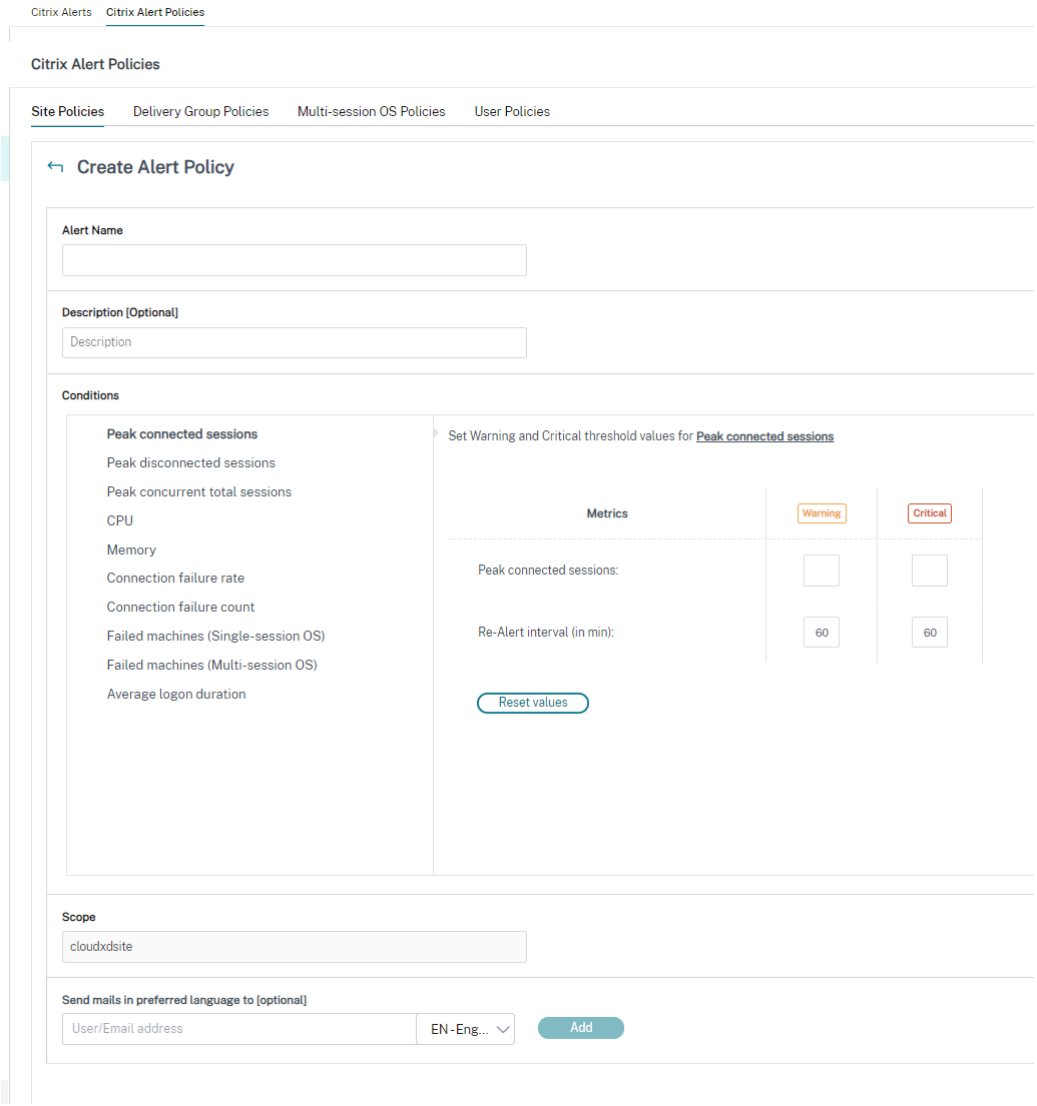
 

Para conocer los valores de umbral que tienen las directivas de alertas integradas, consulte la sección Condiciones para directivas de alertas.



## Crear directivas de alertas




Para crear una nueva directiva de alertas (por ejemplo, para que se genere una alerta cuando se cumple un conjunto concreto de criterios referentes al recuento de sesiones):

1. Vaya a **Alertas** > **Directiva de alertas de Citrix** y seleccione, por ejemplo, la directiva de SO multisesión.
2. Haga clic en **Crear**.
3. Denomine y describa la directiva. A continuación, establezca las condiciones que deben cumplirse para que se active la alerta. Por ejemplo: especifique recuentos críticos y de advertencia para el máximo de sesiones conectadas, el máximo de sesiones desconectadas y el máximo total de sesiones simultáneas. Los valores de advertencia no deben ser superiores a los valores críticos. Para obtener más información, consulte Condiciones para directivas de alertas.

4. Establezca el intervalo de Repetición de alerta. Si se siguen cumpliendo las condiciones de la alerta, esta se activa de nuevo en este intervalo de tiempo y, si lo define en la directiva de alertas, se generará un correo electrónico de notificación. Una alerta descartada no genera ninguna notificación por correo electrónico en el intervalo de repetición de alerta.
5. Establezca el Ámbito. Por ejemplo, defínala para un grupo de entrega determinado.
6. En las preferencias de notificación, especifique a quién debe notificarse por correo electrónico cuando se active la alerta. Las notificaciones por correo electrónico se envían a través de SendGrid. Asegúrese de que la dirección de correo electrónico `donotreplynotifications@citrix.com` aparece en la lista de direcciones permitidas en la configuración del correo electrónico.
7. Haga clic en **Guardar**.

Crear una directiva con 20 o más grupos de entrega definidos en el ámbito puede llevar aproximadamente 30 segundos en completar la configuración. Aparece un cursor giratorio durante este tiempo.

Crear más de 50 directivas para un máximo de 20 grupos de entrega distintos (1000 grupos de entrega de destino en total) puede hacer que aumente el tiempo de respuesta (más de 5 segundos).

Mover una máquina que contiene sesiones activas desde un grupo de entrega a otro puede provocar alertas de grupo de entrega erróneas, al estar definidas mediante parámetros de máquina.

> **Nota:**
> Después de eliminar una directiva de alertas, es posible que pasen hasta 30 minutos hasta que se detengan las notificaciones de alerta generadas por la directiva.

## Condiciones para directivas de alertas

A continuación, dispone de las categorías de alertas, las acciones recomendadas para mitigar la alerta y las condiciones de directiva integrada, si están definidas. Las directivas de alertas integradas se definen para alertar cada 60 minutos.

### Pico de sesiones conectadas

- En Supervisar, consulte la vista “Tendencias de sesiones”para ver la cantidad máxima de sesiones conectadas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.
- Agregue más máquinas, si fuera necesario.

**Pico de sesiones desconectadas**

- En Supervisar, consulte la vista "Tendencias de sesiones"para ver la cantidad máxima de sesiones desconectadas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.
- Agregue más máquinas, si fuera necesario.
- Cierre sesiones desconectadas, si fuera necesario.

**Pico de total de sesiones simultáneas**

- En Supervisar, consulte la vista "Tendencias de sesiones"para ver la cantidad máxima de sesiones simultáneas.
- Compruebe que haya capacidad suficiente para admitir la carga de las sesiones.
- Agregue más máquinas, si fuera necesario.
- Cierre sesiones desconectadas, si fuera necesario.

**CPU**

El porcentaje de uso de CPU indica el consumo general de CPU en el VDA, incluido el de los procesos. Puede obtener más información sobre la utilización de CPU por parte de procesos individuales en la página **Detalles de la máquina** del VDA correspondiente.

- Vaya a **Detalles de la máquina > Ver utilización histórica > 10 procesos principales** para identificar los procesos que consumen CPU. Compruebe que la directiva de supervisión de procesos esté habilitada para iniciar la recopilación de estadísticas de uso de recursos a nivel de procesos.
- Finalice el proceso, si fuera necesario.
- Finalizar el proceso provocará la pérdida de los datos que no se hayan guardado.
- Si todo funciona según lo previsto, agregue más recursos de CPU en el futuro.

  > **Nota:**
  >
  > De forma predeterminada, la configuración de directiva **Habilitar supervisión de recursos** está habilitada para supervisar los contadores de rendimiento de memoria y CPU en máquinas con agentes VDA. Si esta configuración de directiva está inhabilitada, las alertas que tengan condiciones de memoria y CPU no se activarán. Para obtener más información, consulte Configuraciones de directiva de Supervisión.

  **Condiciones para directivas inteligentes:**

  - **Ámbito:** Grupo de entrega, SO multisesión

- **Valores de umbral:** Advertencia (80%), Crítico (90%)

#### Memoria

El porcentaje de uso de memoria indica el consumo general de memoria en el VDA, incluido el de los procesos. Puede obtener más información sobre el uso de memoria por parte de procesos individuales en la página **Detalles de la máquina** del VDA correspondiente.

- Vaya a **Detalles de la máquina > Ver utilización histórica > 10 procesos principales** para identificar los procesos que consumen memoria. Compruebe que la directiva de supervisión de procesos esté habilitada para iniciar la recopilación de estadísticas de uso de recursos a nivel de procesos.
- Finalice el proceso, si fuera necesario.
- Finalizar el proceso provocará la pérdida de los datos que no se hayan guardado.
- Si todo funciona según lo previsto, agregue más capacidad de memoria en el futuro.

> **Nota:**
>
> De forma predeterminada, la configuración de directiva **Habilitar supervisión de recursos** está habilitada para supervisar los contadores de rendimiento de memoria y CPU en máquinas con agentes VDA. Si esta configuración de directiva está inhabilitada, las alertas que tengan condiciones de memoria y CPU no se activarán. Para obtener más información, consulte Configuraciones de directiva de Supervisión.

**Condiciones para directivas inteligentes:**

- **Ámbito:** Grupo de entrega, SO multisesión
- **Valores de umbral:** Advertencia (80%), Crítico (90%)

#### Tasa de fallos de conexión

Porcentaje de fallos de conexión durante la última hora.

- Se calcula a partir del total de fallos según el total de intentos de conexión.
- En Supervisar, consulte la vista "Tendencias de fallos de conexión"para ver eventos registrados en el registro de configuración.
- Determine si las aplicaciones o los escritorios son accesibles.

#### Recuento de fallos de conexión

Cantidad de fallos de conexión durante la última hora.

- En Supervisar, consulte la vista "Tendencias de fallos de conexión"para ver eventos registrados en el registro de configuración.
- Determine si las aplicaciones o los escritorios son accesibles.

#### RTT de ICA (promedio)

Tiempo medio de ida y vuelta del protocolo Independent Computing Architecture.

- Consulte Citrix ADM para ver un desglose del RTT de ICA para determinar la causa raíz. Para obtener más información, consulte la documentación de Citrix ADM.
- Si Citrix ADM no está disponible, consulte la vista "Detalles del usuario"de Supervisar para ver los tiempos de ida y vuelta (RTT) de ICA y la latencia, y determinar si se trata de un problema de red o de aplicaciones o escritorios.

#### RTT de ICA (n.º de sesiones)

Cantidad de sesiones que superan el umbral de tiempos de ida y vuelta (RTT) de ICA.

- Consulte Citrix ADM para ver la cantidad de sesiones que tienen tiempos RTT de ICA altos. Para obtener más información, consulte la documentación de Citrix ADM.
- Si Citrix ADM no está disponible, póngase en contacto con el equipo de red para determinar con ellos la causa del problema.

  **Condiciones para directivas inteligentes:**

  - **Ámbito:** Grupo de entrega, SO multisesión
  - **Valores de umbral:** Advertencia (300 ms para 5 sesiones o más), Crítico (400 ms para 10 sesiones o más)

#### RTT de ICA (% de sesiones)

Porcentaje de sesiones que superan el tiempo medio de ida y vuelta de ICA.

- Consulte Citrix ADM para ver la cantidad de sesiones que tienen tiempos RTT de ICA altos. Para obtener más información, consulte la documentación de Citrix ADM.
- Si Citrix ADM no está disponible, póngase en contacto con el equipo de red para determinar con ellos la causa del problema.

#### RTT de ICA (usuario)

El tiempo de ida y vuelta de ICA que se aplica a las sesiones iniciadas por el usuario especificado. La alerta se activa si el tiempo RTT de ICA supera el umbral en al menos una sesión.

#### Máquinas fallidas (SO de sesión única)

Cantidad de máquinas fallidas de SO de sesión única. Los errores pueden ocurrir por diversos motivos, como se muestra en las vistas Panel de mandos y Filtros de Supervisar.

- Ejecute diagnósticos de Citrix Scout para determinar la causa principal. Para obtener más información, consulte Solucionar problemas de usuarios.

  **Condiciones para directivas inteligentes:**

  - **Ámbito:** Grupo de entrega
  - **Valores de umbral:** Advertencia (1), Crítico (2)

#### Máquinas fallidas (SO multisesión)

Cantidad de máquinas fallidas de SO multisesión. Los errores pueden ocurrir por diversos motivos, como se muestra en las vistas Panel de mandos y Filtros de Supervisar.

- Ejecute diagnósticos de Citrix Scout para determinar la causa principal.

  **Condiciones para directivas inteligentes:**

  - **Ámbito:** Grupo de entrega, SO multisesión
  - **Valores de umbral:** Advertencia (1), Crítico (2)

#### Máquinas fallidas (en %)

Porcentaje de máquinas con sistema operativo de sesión única y multisesión que han fallado en un grupo de entrega en función del número de máquinas que han fallado Esta condición de alerta le permite configurar los umbrales de alerta como un porcentaje de máquinas fallidas de un grupo de entrega y se calcula cada 30 segundos.
Los errores pueden ocurrir por diversos motivos, como se muestra en las vistas Panel de mandos y Filtros de Director. Ejecute diagnósticos de Citrix Scout para determinar la causa principal. Para obtener más información, consulte Solucionar problemas de usuarios.

#### Promedio de duración de inicio de sesión

Duración media de los inicios de sesión que se han producido durante la última hora.

- Consulte el panel de mandos de Supervisar para obtener métricas actualizadas sobre la duración de los inicios de sesión. Si una gran cantidad de usuarios intenta iniciar sesión en un corto período de tiempo, el tiempo que tardan los inicios de sesión puede alargarse.

- Consulte la referencia y el desglose de los inicios de sesión para determinar la causa. Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

  **Condiciones para directivas inteligentes:**

  - **Ámbito:** Grupo de entrega, SO multisesión
  - **Valores de umbral:** Advertencia (45 segundos), Crítico (60 segundos)

#### Duración de inicio de sesión (Usuario)

La duración de los inicios de sesión de un usuario especificado que tuvieron lugar durante la pasada hora.

#### Índice de patrón de carga

Valor del Índice de patrón de carga en los últimos 5 minutos.

- Consulte Supervisar para ver las máquinas con sistema operativo multisesión que puedan tener un máximo de carga. Consulte el panel de mandos (para ver errores) y el informe de tendencias en el índice del patrón de carga.

  **Condiciones para directivas inteligentes:**

  - **Ámbito:** Grupo de entrega, SO multisesión
  - **Valores de umbral:** Advertencia (80%), Crítico (90%)

### Supervisar alertas de hipervisor

Supervisar muestra alertas para supervisar el estado del hipervisor. Las alertas de Citrix Hypervisor y VMware vSphere ayudan a supervisar los parámetros y estados del hipervisor. El estado de conexión al hipervisor también se supervisa, y se genera una alerta si el clúster o el grupo de hosts se reinicia o no está disponible.

Para recibir alertas de hipervisor, debe crear una conexión de alojamiento en la ficha Administrar. Para obtener más información, consulte Conexiones y recursos. Solo se supervisan estas conexiones para las alertas de hipervisor. En la tabla siguiente se describen los distintos parámetros y estados de las alertas de hipervisor.

| Alerta | Hipervisores compatibles | Desencadenada por | Condición | Configuración |
|---|---|---|---|---|
| Uso de CPU | Citrix Hypervisor, VMware vSphere | Hypervisor | Se alcanza o supera el umbral de alerta que tiene el consumo de CPU. | Los umbrales de alerta deben configurarse en el hipervisor. |
| Uso de memoria | Citrix Hypervisor, VMware vSphere | Hypervisor | Se alcanza o supera el umbral de alerta que tiene el consumo de memoria. | Los umbrales de alerta deben configurarse en el hipervisor. |
| Uso de la red | Citrix Hypervisor, VMware vSphere | Hypervisor | Se alcanza o supera el umbral de alerta que tiene el uso de la red. | Los umbrales de alerta deben configurarse en el hipervisor. |
| Uso del disco | VMware vSphere | Hypervisor | Se alcanza o supera el umbral de alerta que tiene el uso del disco. | Los umbrales de alerta deben configurarse en el hipervisor. |
| Conexión de host o estado de energía | VMware vSphere | Hypervisor | El host del hipervisor se ha reiniciado o no está disponible. | Las alertas están preintegradas en VMware vSphere. No se necesita ninguna configuración adicional. |

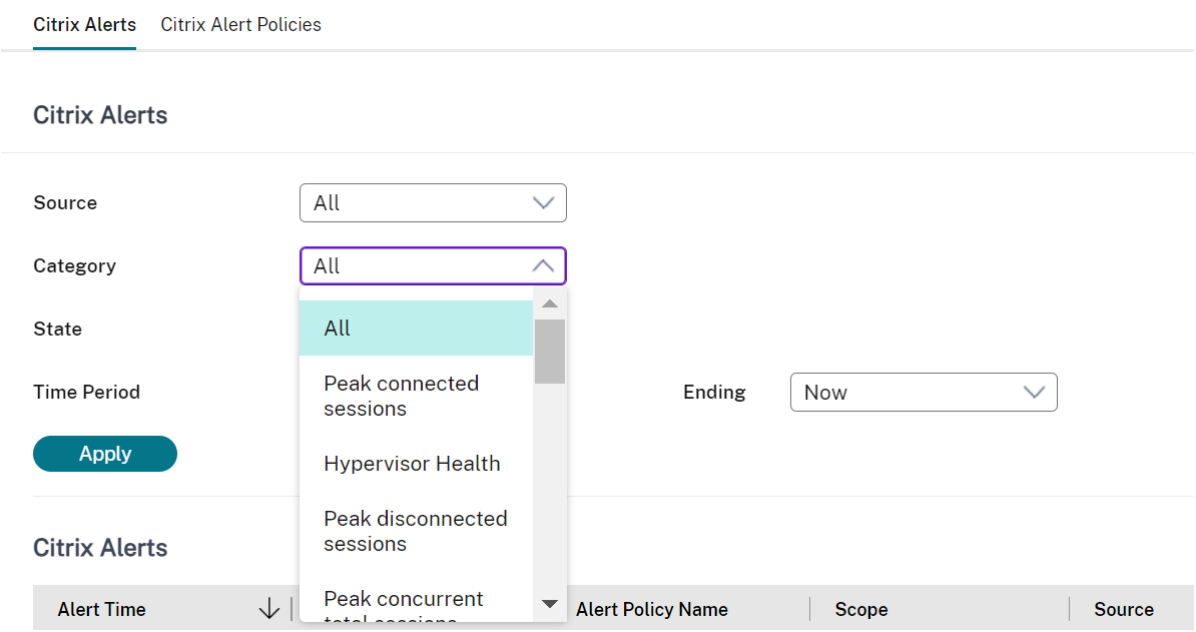
| Alerta | Hipervisores compatibles | Desencadenada por | Condición | Configuración |
|---|---|---|---|---|
| Conexión de hipervisor no disponible | Citrix Hypervisor, VMware vSphere | Delivery Controller | La conexión con el hipervisor (grupo o clúster) se pierde, se apaga o se reinicia. Esta alerta se genera cada hora mientras la conexión no esté disponible. | Las alertas están preintegradas en el Delivery Controller. No se necesita ninguna configuración adicional. |

> **Nota:**
>
> Para obtener más información sobre la configuración de alertas, consulte Alertas de Citrix XenCenter o la documentación sobre alertas de VMware vCenter.

La preferencia de notificación por correo electrónico se puede configurar en **Directiva de alertas de Citrix > Directiva de sitio > Estado del hipervisor**. Las condiciones de umbral para las directivas de alertas del hipervisor se pueden configurar, modificar, inhabilitar o eliminar únicamente desde el hipervisor, no desde Supervisar. Sin embargo, en Supervisar se pueden modificar las preferencias de correo electrónico y descartar alertas.

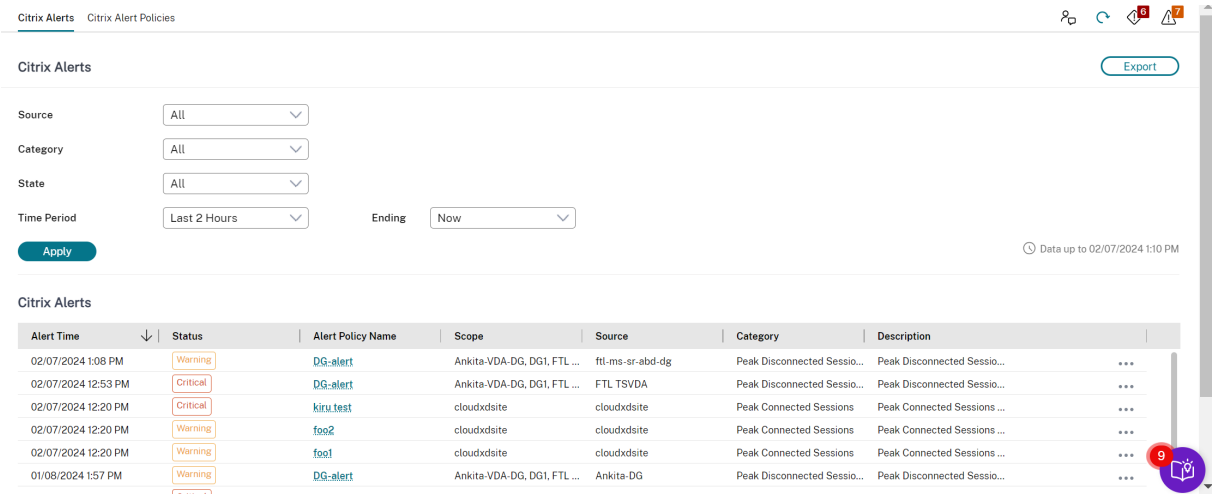
> **Importante:**
>
> - Todas las alertas de Hypervisor que tengan más de un día se descartan automáticamente.
> - Las alertas activadas por el hipervisor se obtienen y se muestran en Supervisar. Sin embargo, los cambios en el ciclo de vida o el estado de las alertas del hipervisor no se reflejan en Supervisar.
> - Las alertas que están en estado correcto o descartadas o inhabilitadas en la consola del hipervisor seguirán apareciendo en Supervisar y deberán descartarse explícitamente.
> - Las alertas que se descartan en Supervisar no se descartan automáticamente en la consola del hipervisor.




Se ha agregado una nueva categoría de alerta denominada **Estado del hipervisor** para habilitar el filtrado únicamente de las alertas del hipervisor. Estas alertas se muestran una vez que se alcanzan o superan los umbrales. Las alertas del hipervisor pueden ser:

- Crítico: Se ha alcanzado o superado el umbral crítico de la directiva de alertas del hipervisor.
- Advertencia: Se ha alcanzado o superado el umbral de advertencia de la directiva de alertas del hipervisor.
- Descartado: La alerta ya no se muestra como activa.



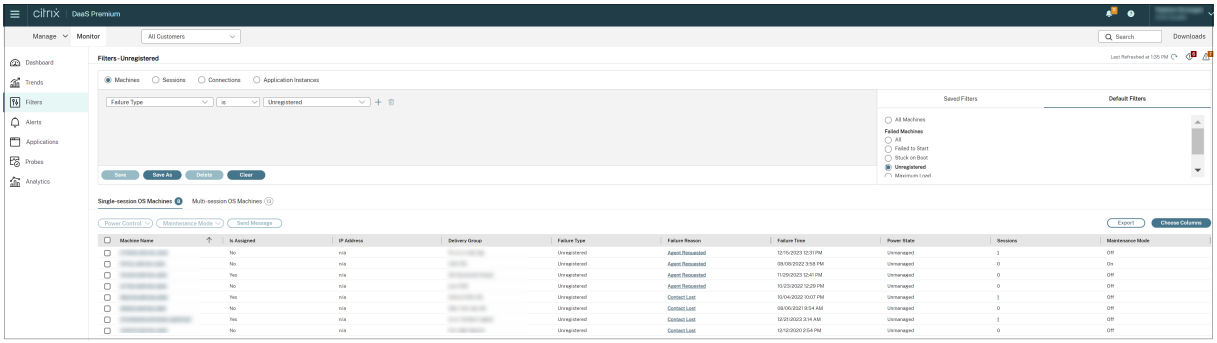

 

# Filtrar datos para solucionar fallos

August 15, 2023

Cuando haga clic en números en el panel de mandos o seleccione un filtro predefinido Predeterminado desde la ficha **Filtros**, la vista Filtros se abre y muestra los datos en función de la máquina seleccionada o del tipo de fallo.

Puede crear vistas con filtros personalizados de máquinas, conexiones, sesiones e instancias de aplicación en todos los grupos de entrega y guardar la búsqueda para acceder más adelante. Puede modificar un filtro predefinido y guardarlo como filtro guardado.



1. Seleccione una vista:

    - **Máquinas**. Seleccione Máquinas con SO de sesión única o Máquinas con SO multisesión. Estas vistas muestran la cantidad de máquinas configuradas. La ficha Máquinas con SO multisesión también incluye el índice del patrón de carga. Este índice indica la distribución de contadores de rendimiento, así como información sobre herramientas del recuento de sesiones si pasa el puntero sobre el vínculo.
    - **Sesiones**. También puede ver el recuento de sesiones desde la vista Sesiones. Use las mediciones del tiempo de inactividad para identificar las sesiones que estén inactivas transcurrido un cierto período de tiempo. Haga clic en el **Usuario asociado** para abrir el Administrador de actividades del usuario. Al hacer clic en el nombre del **dispositivo de punto final**, se abre el Administrador de actividades del dispositivo de punto final. Al hacer clic en **Ver detalles**, se abre la página **Detalles del usuario** o **Detalles del dispositivo de punto final**, respectivamente. Para obtener más información, consulte Detalles del usuario.
    - **Conexiones**. Filtre conexiones por distintos períodos de tiempo, incluidos los últimos 60 minutos, las últimas 24 horas o los últimos 7 días.
    - **Instancias de aplicación**. Esta vista muestra las propiedades de todas las instancias de aplicación que haya en los VDA de SO de sesión única y multisesión. Las métricas del tiempo de inactividad de la sesión están disponibles para las instancias de aplicación en los VDA de SO multisesión.

2. Seleccione un filtro de la lista de filtros guardados o predeterminados.
3. Utilice las listas desplegables para seleccionar otros criterios de filtro.
4. Seleccione columnas adicionales, si es necesario, para solucionar problemas más complejos.
5. Guarde el filtro y cámbiele el nombre.
6. Para abrir el filtro más adelante, en la vista Filtros, seleccione Ver (Máquinas, Sesiones, Conexiones o Instancias de aplicaciones) y, a continuación, el filtro guardado.
7. Haga clic en **Exportar** para exportar los datos a archivos en formato CSV. Se pueden exportar datos de hasta 100 000 registros.
8. Si es necesario, para las vistas **Máquinas** o **Conexiones**, use los controles de energía para todas las máquinas que seleccione en la lista filtrada. Para la vista Sesiones, utilice los controles de sesión u opciones para enviar mensajes.
9. En las vistas **Máquinas** y **Conexiones**, haga clic en **Motivo del fallo** de la máquina o conexión donde se ha producido el error para obtener una descripción detallada del error y las acciones recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para fallos de máquinas y conexiones están disponibles en Citrix Director Failure Reasons Troubleshooting Guide.
10. En la vista **Máquinas**, haga clic en un enlace del nombre de la máquina para ir a la página **Detalles de la máquina** correspondiente. Esta página muestra los datos de la máquina, ofrece controles de alimentación, y muestra gráficos de CPU, memoria, supervisión de disco y supervisión de GPU. Además, puede hacer clic en **Ver utilización histórica** para ver las tendencias de utilización de los recursos en la máquina. Para obtener más información, consulte Solucionar problemas de máquinas.
11. En la vista **Instancias de aplicación**, ordene o filtre en función del **Tiempo de inactividad** superior al período de tiempo del umbral. Seleccione las instancias de aplicación inactivas que quiere finalizar. Cerrar o desconectar una instancia de aplicación finaliza todas las instancias de aplicación activas que haya en la misma sesión. Para obtener más información, consulte Solucionar problemas de aplicaciones. La página de filtro "Instancias de aplicación"y las mediciones del tiempo de inactividad en la página de filtro "Sesiones"están disponibles si los agentes VDA son de la versión 7.13 o una posterior.

> **Nota:**
>
> La consola Administrar permite la asignación de varias reglas de asignación de escritorios (DAR) para distintos usuarios o grupos de usuarios a un solo VDA en el grupo de entrega. StoreFront muestra el escritorio asignado con el nombre simplificado correspondiente a las reglas DAR para el usuario que ha iniciado sesión. Sin embargo, Supervisar no admite las reglas de asignación de escritorios y, por tanto, muestra el escritorio asignado que usa el nombre del grupo de entrega,

> sin tener en cuenta qué usuario está conectado a la sesión. Como resultado de ello, no se puede asignar un escritorio específico a una máquina en Supervisar. Para asignar el escritorio asignado que se muestra en StoreFront al nombre del grupo de entrega que se muestra en Supervisar, use el siguiente comando de PowerShell. Ejecute el comando de PowerShell mediante el SDK de PowerShell remoto como se describe en el blog.

```
Get-BrokerDesktopGroup | Where-Object {
  $\_.Uid -eq (Get-BrokerAssignmentPolicyRule | Where-Object {
  $\_.PublishedName -eq "<Name on StoreFront>"  }
 ).DesktopGroupUid  }
  | Select-Object -Property Name, Uid
<!--NeedCopy-->
```

## Supervisar tendencias históricas en un sitio

January 24, 2024

En la vista "Tendencias", se accede a información histórica sobre tendencias de cada sitio con relación a los siguientes parámetros:

- sesiones
- fallos de conexión
- fallos de máquinas
- rendimiento de los inicios de sesión
- patrones de carga
- administración de la capacidad
- uso de máquinas
- utilización de recursos

Para buscar esta información, haga clic en el menú **Tendencias**.

La función de consulta detallada de datos permite navegar entre los gráficos de tendencias, acercar el gráfico para ver en detalle un período de tiempo concreto (haciendo clic en un punto de datos en el gráfico) y consultar los detalles asociados a la tendencia. Esta función permite comprender mejor qué o quién se ve afectado por las tendencias que se muestran.

Para cambiar el ámbito predeterminado de cada gráfico, aplique un filtro distinto a los datos.

> **Nota:**
>
> - La información de tendencias referentes a sesiones, fallos y rendimiento de inicios de sesión está representada en gráficos y tablas cuando el período de tiempo seleccionado es "Último mes"(**hasta el día de hoy**) o menos. Cuando el período de tiempo es "Último

> mes"(con una fecha de finalización personalizada) o "Último año", la información de tendencias se representa en gráficos, pero no en tablas.
> - Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service) admite la retención de datos históricos solo durante 90 días. Por lo tanto, las tendencias e informes de un año en Supervisar muestran los últimos 90 días de datos.

### Tendencias disponibles

**Ver tendencias de sesiones:** En la ficha Sesiones, seleccione el grupo de entrega y el período de tiempo para ver información más detallada sobre el recuento de sesiones simultáneas.

La columna **Reconexión automática de sesión** muestra la cantidad de reconexiones automáticas en una sesión. La reconexión automática se habilita cuando las directivas de fiabilidad de la sesión o de reconexión automática del cliente están activas. Cuando hay una interrupción de la red en el dispositivo de punto final, entran en vigor las siguientes directivas:

- La fiabilidad de la sesión se activa (de forma predeterminada durante 3 minutos) cuando la aplicación Citrix Receiver o Citrix Workspace intenta conectarse al VDA.
- La reconexión automática del cliente surte efecto entre 3 y 5 minutos cuando el cliente intenta conectarse al VDA.

Ambas reconexiones se capturan y se muestran al usuario. Esta información puede tardar un tiempo máximo de 5 minutos en aparecer en la interfaz de usuario de Director después de que se haya producido la reconexión.

La información de reconexión automática le ayuda a ver y solucionar problemas de conexión de red que sufren interrupciones, así como a analizar las redes que tienen una experiencia fluida y sin problemas. Puede ver la cantidad de reconexiones de un grupo de entrega específico o un período de tiempo que haya seleccionado en los filtros.

Un desglose proporciona información adicional, como la fiabilidad de la sesión o la reconexión automática del cliente, las marcas de tiempo, la dirección IP del dispositivo de punto final o el nombre de la máquina de punto final en la que está instalada la aplicación Workspace.

De forma predeterminada, los registros se ordenan por las marcas de tiempo del evento en orden descendente. Esta función está disponible para la aplicación Citrix Workspace para Windows, la aplicación Citrix Workspace para Mac, Citrix Receiver para Windows y Citrix Receiver para Mac. Esta función requiere agentes VDA con la versión 1906 o una posterior.

Para obtener más información acerca de la reconexión de sesiones, consulte Sesiones. Para obtener más información, consulte Configuraciones de directiva de Reconexión automática de clientes y Configuraciones de directiva de Fiabilidad de la sesión.

A veces, es posible que los datos de reconexión automática no aparezcan en Supervisar por los siguientes motivos:

- La aplicación Workspace no envía los datos de reconexión automática al VDA.
- El VDA no envía datos al servicio Supervisar.

> **Nota:**
>
> A veces, es posible que la dirección IP del cliente no se obtenga correctamente si se establecen ciertas directivas de Citrix Gateway.

**Ver tendencias de fallos de conexión:** En la ficha "Fallos", seleccione la conexión, el tipo de máquina, el tipo de fallo, el grupo de entrega y el período de tiempo, para ver un gráfico con información más detallada sobre los fallos de conexión de los usuarios en el sitio.

**Ver tendencias de fallos de máquinas:** En la ficha "Fallos de máquina con SO de sesión única"o en la ficha "Fallos de máquina con SO multisesión", seleccione el tipo de fallo, el grupo de entrega y el período de tiempo, para ver un gráfico con información más detallada sobre los fallos de máquinas en el sitio.

**Ver tendencias del rendimiento de los inicios de sesión:** En la ficha "Rendimiento de inicio de sesión", seleccione el grupo de entrega y el período de tiempo para ver un gráfico con información más detallada sobre cuánto tardan los inicios de sesión de los usuarios en el sitio, y si la cantidad de inicios de sesión afecta al rendimiento. En esta vista, también se puede ver el promedio de duración de las fases de inicio de sesión, tales como la duración de la intermediación y la hora de inicio de la VM.
Estos datos son específicos para inicios de sesión de usuario y no incluyen a los usuarios que intentan volver a conectarse a sesiones desconectadas.
La tabla que aparece debajo del gráfico muestra la Duración de inicio de sesión por sesión de usuario. Usted puede elegir las columnas que quiere mostrar y ordenar el informe por cualquiera de las columnas.
Para obtener más información, consulte Diagnosticar problemas de inicio de sesión de los usuarios.

**Ver tendencias de evaluación de carga:** En la ficha Índice de patrón de carga, dispone de un gráfico con información detallada sobre la carga que se distribuye entre las máquinas con SO multisesión. Las opciones de filtro para este gráfico incluyen: grupo de entrega o máquina con SO multisesión en un grupo de entrega, máquina con SO multisesión (disponible solo si se selecciona Máquina con SO multisesión en un grupo de entrega) y un intervalo. El índice del patrón de carga se muestra como porcentajes de la CPU total, la memoria, el disco o las sesiones, y se compara con la cantidad de usuarios conectados en el último intervalo.

**Ver uso de aplicaciones alojadas:** En la ficha "Administración de capacidad", seleccione la ficha "Uso de aplicaciones alojadas", el grupo de entrega y el período de tiempo para ver un gráfico con el uso simultáneo en las horas punta y una tabla que muestra el uso de las aplicaciones. Desde la tabla

de Uso basado en aplicaciones, puede elegir una aplicación específica para ver más detalles y una lista de usuarios que están utilizando, o han usado, la aplicación.

**Ver el uso de SO de sesión única y multisesión:** La vista "Tendencias"muestra el uso del SO de sesión única por sitio y por grupo de entrega. Al seleccionar un sitio, se muestra el uso por grupo de entrega. Cuando se selecciona un grupo de entrega, se muestra el uso por usuario.
La vista Tendencias muestra también el uso del SO multisesión por sitio, por máquina y por grupo de entrega. Al seleccionar un sitio, se muestra el uso por grupo de entrega. Cuando se selecciona un grupo de entrega, se muestra el uso por máquina y por usuario. Cuando se selecciona una máquina, se muestra el uso por usuario.

**Ver uso de máquinas virtuales:** En la ficha "Uso de máquinas", seleccione "Máquinas con SO de sesión única"o "Máquinas con SO multisesión"para obtener una vista en tiempo real del uso de las máquinas virtuales. La página muestra la cantidad de máquinas encendidas con SO de sesión única y SO multisesión con Autoscale habilitado para un grupo de entrega y un período de tiempo determinados. También está disponible una estimación del ahorro logrado al habilitar Autoscale en el grupo de entrega seleccionado, cuyo porcentaje se calcula mediante los costes por máquina.

Las tendencias de uso de las máquinas con Autoscale habilitado indican el uso real de las máquinas, lo que le permite evaluar rápidamente las necesidades de capacidad de su sitio.

- Disponibilidad de SO de sesión única: Muestra el estado actual de las máquinas con SO de sesión única (VDI) por disponibilidad, para el sitio entero o para un grupo de entrega específico.
- Disponibilidad de SO multisesión: Muestra el estado actual de las máquinas con SO multisesión por disponibilidad, para el sitio entero o para un grupo de entrega específico.

> **Nota:**
>
> La tabla situada debajo del gráfico muestra en tiempo real los datos de uso de la máquina por grupo de entrega. Los datos incluyen la disponibilidad de todas las máquinas independientemente de si Autoscale está habilitado o no. La cantidad de máquinas que se indica en la columna "Contadores disponibles"de la matriz incluye máquinas en modo de mantenimiento.

La consolidación de los datos de supervisión depende del período de tiempo que seleccione.

- Los datos de supervisión de los períodos de un día y una semana se consolidan por hora.
- Los datos de supervisión del período de un mes se consolidan por día.

El estado de la máquina se lee en el momento de la consolidación, y cualquier cambio que se produzca mientras tanto no se tiene en cuenta. Para obtener información sobre el período de consolidación, consulte la documentación de la API de Supervisar.

Para obtener más información sobre la supervisión de máquinas con AutoScale habilitado, consulte el artículo AutoScale.

**Ver utilización de recursos:** Para una planificación más precisa de la capacidad, vaya a la ficha "Utilización de recursos"y seleccione máquinas con SO de sesión única o multisesión para obtener información detallada sobre tendencias históricas de uso de CPU, memoria, IOPS y latencia de disco en cada máquina VDI.
Esta función requiere agentes VDA con la **versión 7.11** o una posterior.
Los gráficos muestran datos sobre el promedio de CPU, el promedio de memoria, el promedio de E/S por segundo, la latencia de disco y el máximo de sesiones simultáneas. Puede explorar en profundidad una máquina para ver datos y gráficos sobre los 10 procesos que consumen más CPU. Asimismo, puede filtrar por grupo de entrega y período de tiempo. Los gráficos de CPU, consumo de memoria y pico de sesiones simultáneas están disponibles para las últimas 2 horas, 24 horas, 7 días, mes y año. Los gráficos del promedio de E/S por segundo y la latencia de disco están disponibles para las últimas 24 horas, el último mes y el último año.

> **Nota:**
>
> - La configuración de la directiva de Supervisión Habilitar supervisión de procesos debe estar establecida en "Permitida"para recopilar y mostrar datos en la tabla "10 procesos principales"de la página "Utilización histórica de máquinas". De forma predeterminada, la directiva está establecida en "Prohibida". De forma predeterminada, se recopilan los datos referentes al uso de recursos. Se pueden inhabilitar mediante la directiva Habilitar supervisión de recursos. La tabla situada bajo los gráficos muestra los datos de utilización de recursos por máquina.
> - El Promedio de E/S por segundo muestra los promedios diarios. Para indicar el pico de E/S por segundo, se calcula la mayor de las E/S medias para el intervalo de tiempo seleccionado. (Un promedio de E/S por segundo son las operaciones medias de E/S por segundo recopiladas durante una hora en el VDA.)
> - El desglose de las máquinas muestra procesos con el uso medio de CPU o de memoria que sea superior al 1 %, lo que podría significar que, a veces, aparecen menos de 10 procesos en la lista.

**Ver fallos de las aplicaciones:** La ficha Fallos y errores de aplicación muestra los fallos asociados a las aplicaciones publicadas en los VDA.

Esta función requiere agentes VDA con la **versión 7.15** o una posterior. Se admiten los VDA de SO de sesión única con Windows Vista o posterior y los VDA de SO multisesión con Windows Server 2008 o posterior.
Para obtener más información, consulte Supervisar fallos históricos de aplicaciones.

De forma predeterminada, solo se muestran los fallos de aplicaciones en los VDA de SO multisesión. Puede configurar la supervisión de los fallos de aplicación mediante las directivas de Supervisión. Para obtener más información, consulte Configuraciones de directiva de Supervisión.

**Crear informes personalizados:** La ficha "Informes personalizados"ofrece una interfaz de usuario

para generar informes personalizados que contienen datos históricos y en tiempo real obtenidos de la base de datos de supervisión en formato tabular.

Desde la lista de las consultas de "Informe personalizado"previamente guardadas, puede hacer clic en **Ejecutar y descargar** para exportar un informe en formato CSV, y hacer clic en **Copiar OData** para copiar y compartir la consulta de OData correspondiente, o hacer clic en **Modificar** para modificarla. Puede crear una consulta de informe personalizado en función de las máquinas, las conexiones, las sesiones o las instancias de aplicación. Especifique las condiciones de filtro, que pueden establecerse en función de campos como la máquina, el grupo de entrega o el período de tiempo. Especifique las columnas adicionales necesarias en el informe personalizado. La vista previa muestra un ejemplo de los datos del informe. Si guarda la consulta del informe personalizado, esta se agrega a la lista de consultas guardadas.

Puede crear una consulta de informe personalizado a partir de una consulta de OData copiada. Para ello, seleccione la opción de consulta de OData y pegue la consulta de OData copiada. Puede guardar la consulta resultante para ejecutarla más adelante.

> **Nota:**
>
> Los nombres de las columnas en el informe de vista previa y exportación que se generan mediante consultas de OData no están localizados, aparecen en inglés.

Los iconos de marcas del gráfico indican acciones o sucesos significativos para un intervalo de tiempo concreto. Pase el puntero sobre el marcador y haga clic en la lista de sucesos o acciones.

> **Nota:**
>
> - Los datos de inicio de sesión de conexiones HDX no se recopilan para versiones del VDA anteriores a 7. Para los VDA anteriores, los datos gráficos se muestran como 0.
> - Los grupos de entrega eliminados en la consola Administrar pueden seleccionarse en los filtros de tendencias hasta que los datos relacionados con ellos se hayan limpiado y eliminado. Si se selecciona un grupo de entrega eliminado se muestran gráficos para los datos disponibles durante el período de retención. Sin embargo, las tablas no mostrarán datos.
> - Al mover una máquina que contiene sesiones activas de un grupo de entrega a otro, las tablas de **Utilización de recursos e Índice de patrón de carga** del nuevo grupo de entrega muestran métricas consolidadas de ambos grupos de entrega, el antiguo y el nuevo.

## Supervisar máquinas administradas con Autoscale

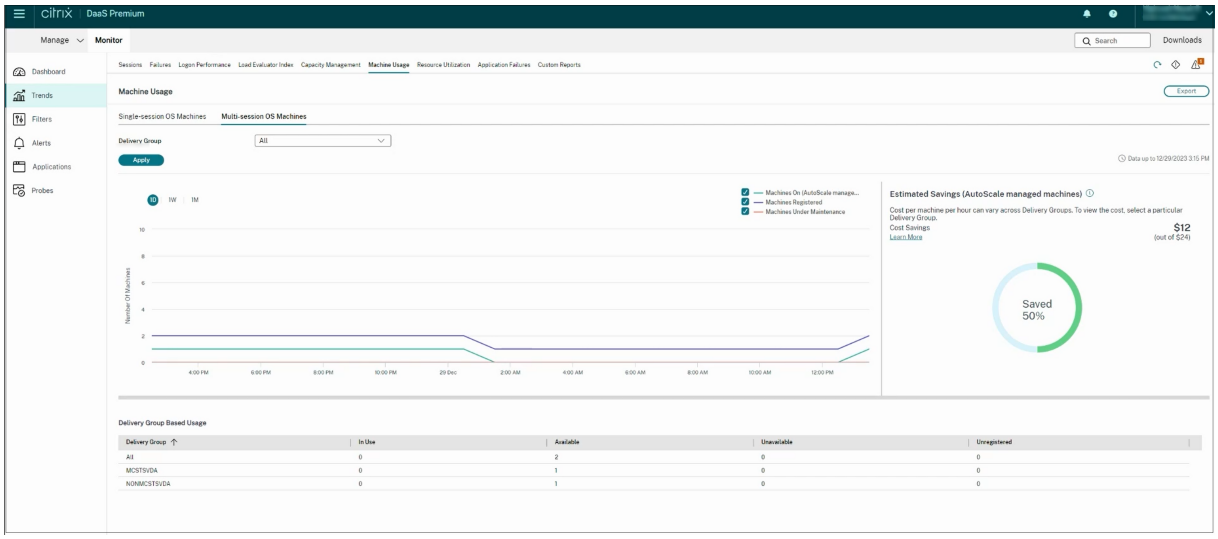
March 30, 2022

Autoscale es una función de administración de energía que permite administrar de forma proactiva la energía de todas las máquinas de SO de sesión única y de SO multisesión registradas en un grupo de entrega. Puede configurar Autoscale para un grupo de entrega concreto desde la ficha **Administrar**. Para obtener más información, consulte Autoscale.
Puede supervisar las métricas clave de las máquinas con Autoscale habilitado desde la ficha **Supervisar**.

## Uso de máquinas

La página **Supervisar** > **Tendencias** > **Uso de máquinas** muestra la cantidad total de máquinas encendidas con SO de sesión única y SO multisesión con Autoscale habilitado para un grupo de entrega y un período de tiempo determinados. Esta métrica indica el uso real de las máquinas que hay en el grupo de entrega.
En la ficha **Máquinas con SO de sesión única** o en la ficha **Máquinas con SO multisesión**, seleccione el grupo de entrega y el período de tiempo.



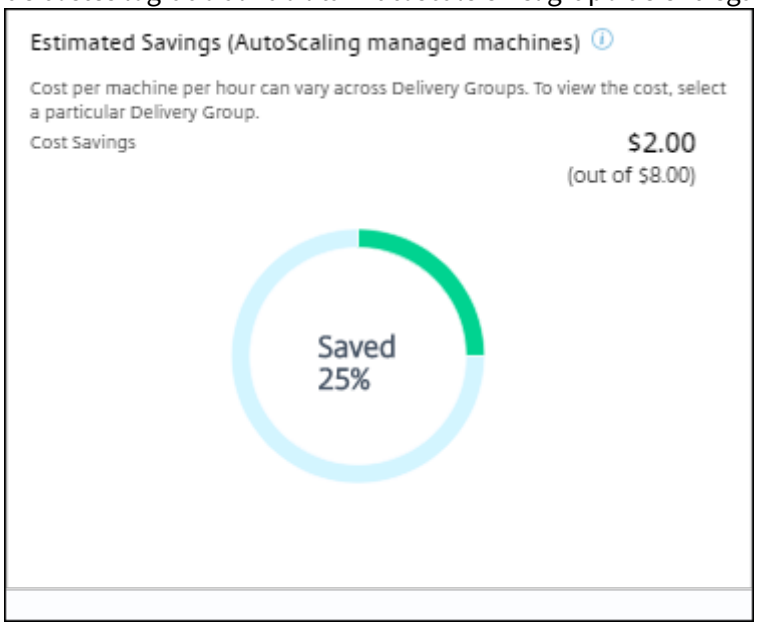

El gráfico indica las siguientes métricas:

- **Máquinas encendidas**: La cantidad de máquinas con Autoscale habilitado que están encendidas.
- **Máquinas registradas**: La cantidad de máquinas de SO de sesión única o de SO multisesión registradas.
- **Máquinas en mantenimiento**: La cantidad de máquinas de SO de sesión única o de SO multisesión con el modo de mantenimiento activado.

### Ahorro estimado

La página **Supervisar** > **Tendencias** > **Uso de máquinas** también muestra una estimación del ahorro de costes logrado al habilitar Autoscale en el grupo de entrega seleccionado.




El ahorro estimado se calcula como el porcentaje de ahorro por máquina y hora (en USD) configurado en **Administrar** > **Modificar grupo de entrega** > **Autoscale**. Para obtener más información sobre cómo configurar los ahorros por máquina, consulte Autoscale.

Al seleccionar todos los grupos de entrega, se muestra el valor medio del ahorro estimado para todos los grupos de entrega.
El ahorro estimado ayuda a los administradores a consolidar la infraestructura existente y a planificar la capacidad para maximizar el ahorro y el uso.

### Notificaciones de alerta para máquinas y sesiones

El panel de mandos Supervisar muestra notificaciones de alerta que se pueden detallar más. La información detallada de las alertas aparece en la página **Supervisar** > **Alertas**.

- Para crear una directiva de alerta en un grupo de entrega, vaya a **Supervisar** > **Alertas** > **Directiva de alertas de Citrix** > **Directiva de grupo de entrega**.
- Aquí puede establecer los siguientes umbrales de advertencia y aviso crítico:
  - Máquinas fallidas (SO de sesión única) y Máquinas fallidas (SO multisesión),
  - Máximo de sesiones conectadas, máximo de sesiones desconectadas y máximo total de sesiones simultáneas en el grupo de entrega.

- Las alertas se generan cuando la métrica correspondiente del grupo de entrega alcanza el umbral.

Para obtener información detallada sobre las condiciones de la directiva de alertas y la creación de directivas de alerta, consulte Alertas y notificaciones.

### Estado de la máquina

- **Supervisar** > **Filtros** > **Máquinas** muestra el estado de energía de todas las máquinas en formato tabular. Puede filtrar por un grupo de entrega específico.
- **Supervisar** > **Filtros** > **Sesiones** muestra un filtro por el nombre de la máquina para ver las sesiones asociadas y su estado en tiempo real.
- En **Supervisar** > **Tendencias** > **Sesiones**, seleccione el grupo de entrega y el período de tiempo para ver la tendencia de las sesiones y sus métricas asociadas.

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

### Tendencias de los patrones de carga

La página **Supervisar** > **Tendencias** > **Índice de patrón de carga** muestra un gráfico con información detallada sobre la carga que se distribuye entre las máquinas de SO multisesión. Las opciones de filtro para este gráfico incluyen: grupo de entrega o máquina con SO multisesión en un grupo de entrega, máquina con SO multisesión (disponible solo si se selecciona Máquina con SO multisesión en un grupo de entrega) y un intervalo. El índice del patrón de carga se muestra como porcentajes de la CPU total, la memoria, el disco o las sesiones, y se compara con la cantidad de usuarios conectados en el último intervalo.

## Solucionar problemas de implementaciones

March 30, 2024

Como administrador del servicio de asistencia técnica, puede buscar al usuario que informa de un problema. Y, a continuación, mostrar los detalles de las sesiones o aplicaciones asociadas a ese usuario.

Del mismo modo, puede buscar máquinas o dispositivos de punto final donde se han producido problemas. Los problemas se pueden resolver rápidamente supervisando las métricas relevantes y realizando las acciones correspondientes.

Las siguientes acciones están disponibles:

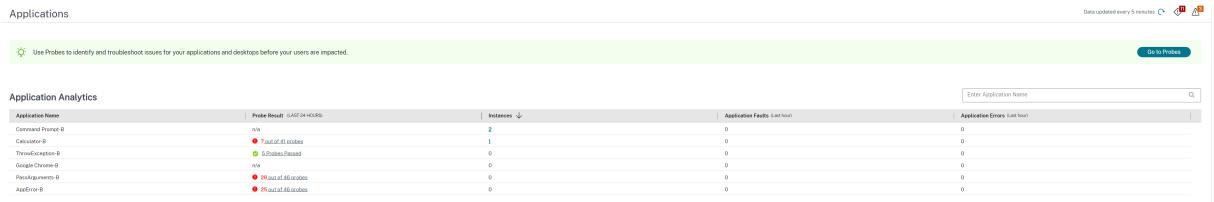
- finalizar una aplicación o un proceso que no responde
- remedar operaciones en la máquina del usuario
- cerrar una sesión que no responde
- reiniciar la máquina
- colocar una máquina en modo de mantenimiento
- restablecer el perfil de usuario

## Solucionar problemas de aplicaciones

July 24, 2023

### Análisis de aplicaciones

La vista **Aplicaciones** muestra datos de análisis de aplicaciones en una vista única y consolidada a fin de ayudar a analizar y administrar de forma eficiente el rendimiento de las aplicaciones. Puede obtener información valiosa sobre el estado y el uso de todas las aplicaciones publicadas en el sitio. La vista predeterminada ayuda a identificar las aplicaciones que se ejecutan con mayor frecuencia. Esta función requiere agentes VDA con la versión 7.15 o una posterior.




En la columna **Resultado del sondeo**, se muestra el resultado del sondeo de aplicaciones ejecutado en las últimas 24 horas. Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias** > **Resultados del sondeo**. Para obtener más información sobre cómo configurar los sondeos de aplicaciones, consulte Sondeo de aplicaciones y escritorios.

La columna **Instancias** muestra el uso de las aplicaciones. Indica la cantidad de instancias de aplicación que se ejecutan en ese momento (instancias conectadas y desconectadas). Para solucionar problemas complejos, haga clic en el campo **Instancias** para ver la página de filtros de **Instancias de aplicación** correspondientes. En ella, puede seleccionar las instancias de aplicación que se van a cerrar o desconectar.

> **Nota:**
>
> Para los administradores con ámbito personalizado, Supervisar no muestra las instancias de aplicación creadas en los grupos de aplicaciones. Para ver todas las instancias de aplicación, debe

> ser administrador total. Para obtener más información, consulte el artículo CTX256001 de Knowledge Center.

Puede supervisar el estado de las aplicaciones publicadas en el sitio con las columnas **Fallos de aplicación** y **Errores de aplicación**. Esas columnas muestran la cantidad total de fallos y errores que se han producido mientras se iniciaba la aplicación en cuestión durante la última hora. Haga clic en el campo **Fallos de aplicación** o **Errores de aplicación** para ver datos sobre los fallos y errores en la página **Tendencias** > **Fallos y errores de aplicación** que corresponde a la aplicación seleccionada.

La disponibilidad y la presentación de los fallos y los errores se define con las configuraciones de directiva de fallos de aplicación. Para obtener más información sobre las directivas y cómo modificarlas, consulte Directivas para supervisar fallos de aplicación en las configuraciones de la directiva Supervisión.

### Supervisar aplicaciones en tiempo real

Puede solucionar las aplicaciones y las sesiones con la ayuda de métricas de inactividad para identificar las instancias que llevan inactivas más de un límite de tiempo concreto.

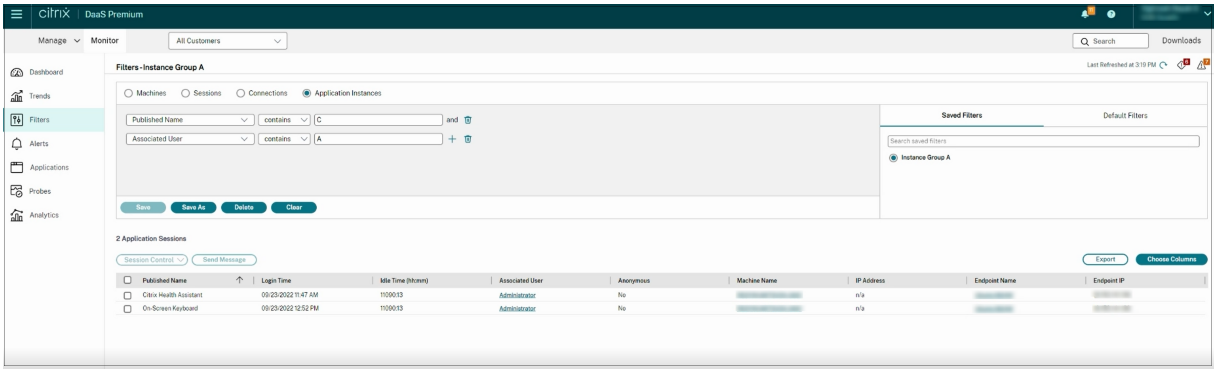
Los casos típicos donde solucionar problemas de aplicaciones pertenecen al sector de la asistencia médica, donde los empleados comparten licencias de aplicación. Allí, debe finalizar las sesiones inactivas y las instancias de aplicación inactivas para purgar el entorno de Citrix Virtual Apps and Desktops, para reconfigurar los servidores de bajo rendimiento o para mantener y actualizar aplicaciones.

La página de filtros **Instancias de aplicación** ofrece una lista de todas las instancias de aplicación que están presentes en los VDA de SO multisesión y SO de sesión única. Se muestran las métricas del tiempo de inactividad asociadas a las instancias de aplicación en los VDA de SO multisesión que hayan estado inactivas durante al menos 10 minutos.

> **Nota:**
>
> Las métricas de instancias de aplicación están disponibles en los sitios de todas las ediciones de licencias.

Utilice esta información para identificar las instancias de aplicación que estén inactivas transcurrido un período de tiempo concreto con el objetivo de cerrarles o desconectarlas, según corresponda. Para ello, seleccione **Filtros > Instancias de aplicación**. A continuación, seleccione un filtro guardado previamente o elija **Todas las instancias de aplicación** y cree su propio filtro.

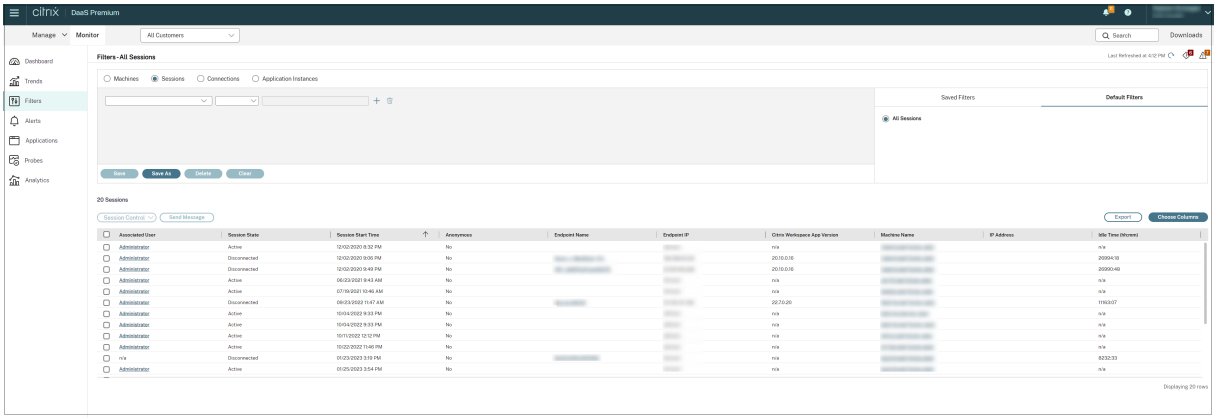
 




A continuación, se ofrece un filtro de ejemplo. Como criterio **Filtrar por**, elija **Nombre publicado** (de la aplicación) y **Tiempo de inactividad**. A continuación, establezca **Tiempo de inactividad** en **mayor o igual que** un límite de tiempo concreto y guarde el filtro si quiere volver a utilizarlo en el futuro. En la lista filtrada, seleccione las instancias de aplicación. Seleccione la opción para enviar mensajes o, desde la lista desplegable **Control de sesión**, elija **Cerrar sesión** o **Desconectar** para finalizar las instancias.

> **Nota:**
>
> Cerrar la sesión o desconectar una instancia de aplicación cierra o desconecta la sesión actual, lo que finaliza todas las instancias de aplicación que pertenezcan a la misma sesión.

Puede identificar las sesiones inactivas desde la página de filtro **Sesiones** si utiliza el estado de la sesión y la métrica del tiempo de inactividad de la sesión. Ordene por la columna **Tiempo de inactividad** o defina un filtro para identificar las sesiones que estén inactivas transcurrido un tiempo específico. Se muestra el tiempo de inactividad de las sesiones en los VDA de SO multisesión que hayan estado inactivas durante al menos 10 minutos.




El **Tiempo de inactividad** se muestra como **N/D** cuando la instancia de aplicación o sesión

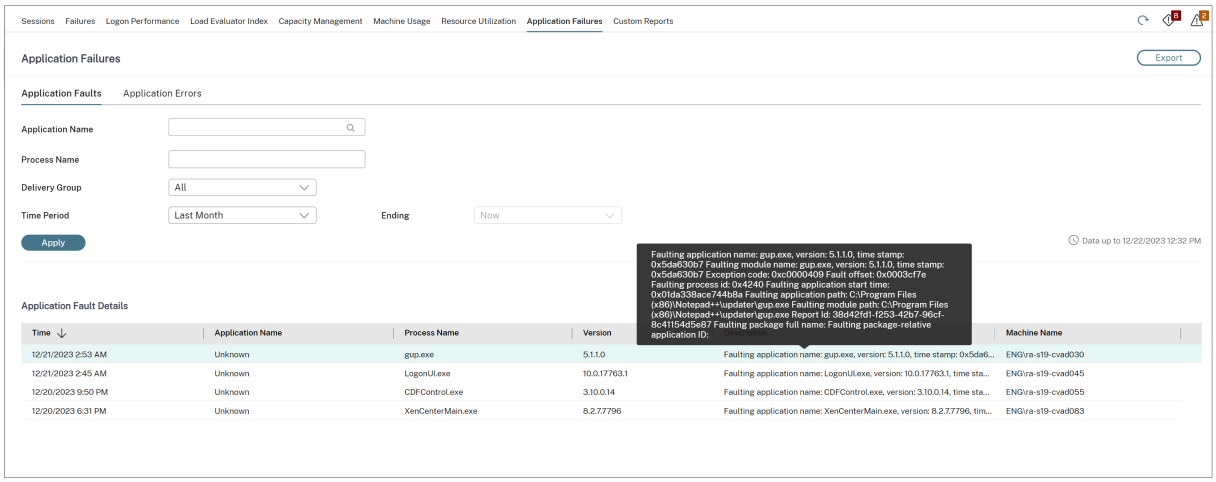
- no ha estado inactiva durante más de 10 minutos,
- se ha iniciado en un VDA de SO de sesión única o
- se ha iniciado en un VDA que ejecuta la versión 7.12 o una versión anterior.

## Supervisar fallos históricos de aplicaciones

La ficha **Tendencias** > **Fallos y errores de aplicación** muestra los fallos y los errores asociados a las aplicaciones publicadas en los VDA.

Para obtener más información sobre la disponibilidad de las tendencias de errores de las aplicaciones, consulte el artículo Granularidad y retención de datos. Se supervisan aquellos fallos de aplicaciones que se registran en el Visor de eventos con el origen "Errores de aplicación". Haga clic en **Exportar** para generar informes en formato CSV, Excel o PDF.




Los fallos se muestran como **Fallos de aplicación** o **Errores de aplicación** en función de su gravedad. La ficha "Fallos de aplicación"muestra fallos asociados a la pérdida de datos o de funcionalidad. En cambio, "Errores de aplicación"indica problemas que no son inmediatamente relevantes; representan condiciones que pueden provocar problemas en el futuro.

Puede filtrar los fallos en función del **Nombre de la aplicación publicada**, **Nombre del proceso** o **Grupo de entrega** y **Período de tiempo**. La tabla muestra el código del error o del fallo junto con una breve descripción de este. La descripción detallada de errores y fallos se muestra como un cuadro de información.

> **Nota:**
>
> El "Nombre de la aplicación publicada"aparece como "Desconocido"cuando no se puede deducir el nombre de la aplicación correspondiente. Esto ocurre normalmente cuando falla una aplicación iniciada en una sesión de escritorio, o bien cuando falla debido a una excepción no controlada ocasionada por un archivo ejecutable de dependencia.

De forma predeterminada, se supervisan solo los fallos de las aplicaciones alojadas en agentes VDA de SO multisesión. Puede modificar los parámetros de supervisión desde las directivas de grupo de supervisión (Habilitar supervisión de fallos de aplicación, Habilitar supervisión de fallos de aplicación en VDA de SO de sesión única y Lista de aplicaciones excluidas de la supervisión de fallos). Para obtener

más información, consulte Directivas para supervisar fallos de aplicación en "Configuraciones de directiva de Supervisión".

En la página **Tendencias** > **Resultados del sondeo de aplicaciones**, se muestran los resultados de los sondeos de aplicaciones ejecutados en el sitio en las últimas 24 horas y los últimos 7 días. Para obtener más información sobre cómo configurar los sondeos de aplicaciones, consulte Sondeo de aplicaciones.

## Sondeo de aplicaciones

January 17, 2023

El sondeo de aplicaciones automatiza las comprobaciones de estado de las aplicaciones de Citrix Virtual Apps publicadas en un sitio. Los resultados del sondeo de aplicaciones están disponibles en la ficha **Supervisar** de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service). Citrix Probe Agent admite sitios alojados en planos de control de Citrix Cloud Japan y Citrix Cloud Government.

Asegúrese de que las máquinas de punto final que ejecutan Probe Agents son máquinas de Windows con Citrix Receiver para Windows versión 4.8 o posterior, o la aplicación Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) versión 1808 o posterior. No se admite la aplicación Workspace para UWP.

Requisitos:

- Las máquinas de punto final con Probe Agents son máquinas Windows con la versión 4.8 de Citrix Receiver para Windows o una posterior, o versión 1906 de la aplicación Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) o una posterior. No se admite la aplicación Workspace para UWP.
- Citrix Probe Agent permite la autenticación predeterminada basada en formularios, tal y como la permite Citrix Workspace. Citrix Probe Agent no permite otros métodos de autenticación, como Single Sign-On (SSO) o la autenticación de varios factores (MFA). Del mismo modo, Citrix Probe Agent solo funciona cuando no hay un servidor proxy o un equilibrador de carga implementados, como Citrix Gateway o Citrix ADC.
- Asegúrese de que la versión 4.7.2 de Microsoft .NET Framework o una posterior está instalada en la máquina de punto final donde quiere instalar Probe Agent.
- Para usar el agente de sondeos en el plano de control de Citrix Cloud Japan, establezca el valor del Registro en la ruta "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\regi en 2. Para usar el agente de sondeos en el plano de control de Citrix Cloud Government, establezca el valor del Registro en la ruta "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAg en 3.

Las cuentas de usuario o permisos requeridos para ejecutar el sondeo de aplicaciones son las siguientes:

- Un usuario único de Workspace para sondear aplicaciones en cada máquina de punto final. No es necesario que el usuario de Workspace sea un administrador; los sondeos pueden ejecutarse en un contexto no administrativo.
- Cuentas de usuario con permisos de administrador de Windows para instalar y configurar Citrix Probe Agent en las máquinas de punto final
- Una cuenta de administrador total con los siguientes permisos. Si reutiliza cuentas de usuarios existentes para el sondeo de aplicaciones, podrían cerrarse las sesiones activas de esos usuarios.
  - Permisos de grupo de entrega:
    - Solo lectura
  - Permisos de Director:
    - Crear, modificar y eliminar configuraciones de sondeo
    - Ver página Configuraciones
    - Ver página Tendencias

### Configurar el sondeo de aplicaciones

Programe los sondeos de aplicaciones para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar problemas relacionados con las aplicaciones aprovisionadas, las máquinas de host o las conexiones antes de que los usuarios los experimenten.

Citrix Probe Agent versión 2103 es compatible con la agregación de sitios. Las aplicaciones y los escritorios se pueden enumerar e iniciar desde sitios agregados. Cuando configure el agente de sondeo, seleccione la opción **Agregación de sitios de Workspace (StoreFront) habilitada** para habilitar la enumeración de aplicaciones y escritorios desde sitios agregados. Se admiten las siguientes combinaciones de sitios:

- Varios sitios locales que tengan una URL de StoreFront.
- Sitios locales y en la nube que tengan una URL de StoreFront o Workspace.
- Varios sitios en la nube que tengan una URL de Workspace.

> **Nota:**
>
> Deberá crear administradores o usuarios independientes para configurar sondeos que tengan acceso a un solo sitio.

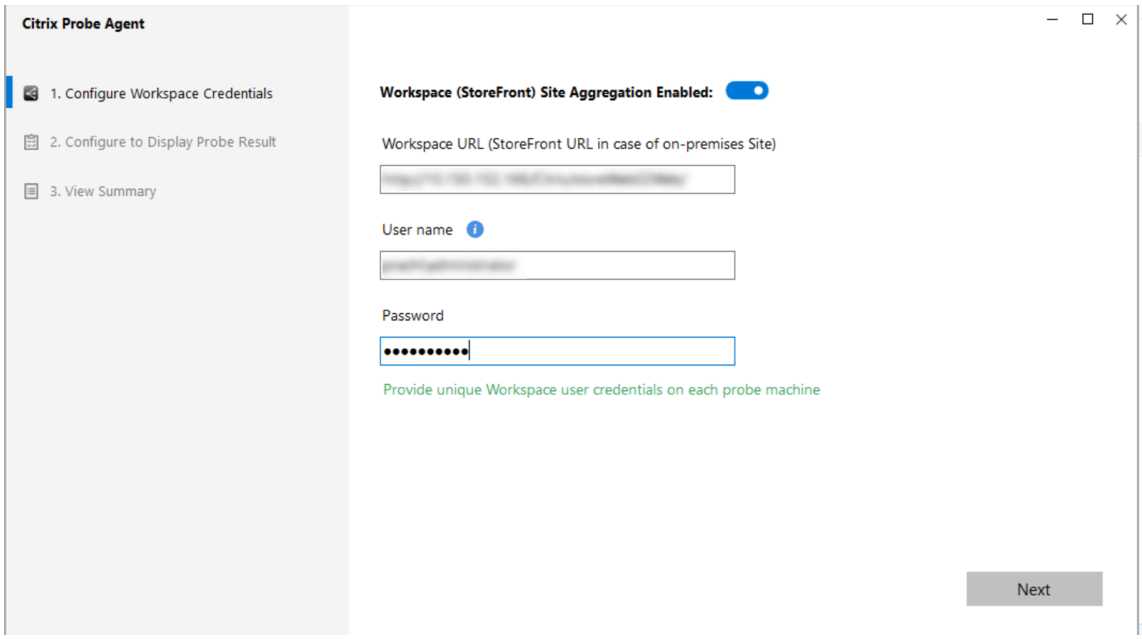
 

### Paso 1: Instale y configure el Citrix Probe Agent

Citrix Probe Agent es un ejecutable de Windows que simula el inicio de la aplicación por parte del usuario a través de Citrix Workspace. Prueba los inicios de las aplicaciones siguiendo las pautas configuradas en Supervisar e informa de los resultados a Supervisar.

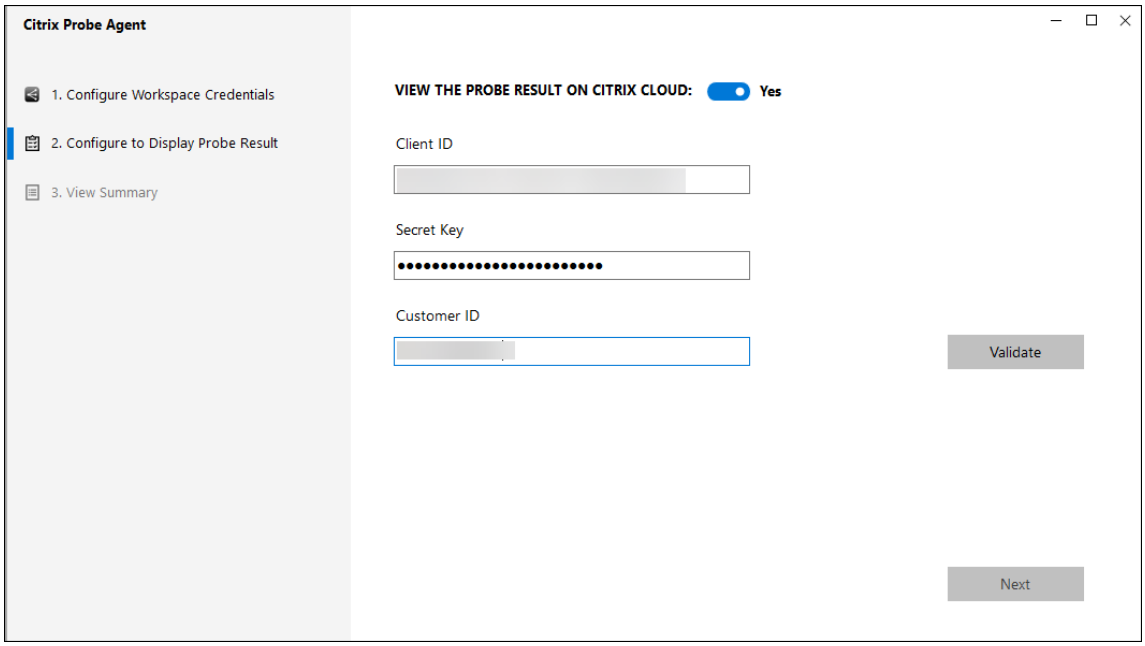
1. Identifique las máquinas de punto final desde donde ejecutar el sondeo de aplicaciones.
2. Los usuarios con privilegios administrativos pueden instalar y configurar Citrix Probe Agent en la máquina de punto final. Descargue el ejecutable de Citrix Probe Agent disponible en https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie el agente y configure las credenciales de Citrix Workspace. Configure un usuario único de Workspace en cada máquina de punto final. Las credenciales se cifran y se almacenan de forma segura.

   > **Notas:**
   >
   > - Para acceder al sitio que va a sondear desde fuera de la red, escriba la URL de inicio de sesión de Citrix Gateway en el campo **URL de Workspace**. Citrix Gateway enruta automáticamente la solicitud a la URL de Workspace del sitio correspondiente.
   > - Utilice NetBIOS como el nombre de dominio en el campo del nombre de usuario. Por ejemplo, NetBIOS/nombredeusuario.
   > - El sondeo de aplicaciones admite el uso de Citrix Content Collaboration Service mediante la autenticación de Workspace (solo AD).



4. En la ficha **Configurar para mostrar el resultado del sondeo**, introduzca las credenciales para acceder a Citrix DaaS. Encontrará el nombre del cliente, el ID del cliente y la clave secreta en la página Acceso a API en la consola de Citrix Cloud.




**Paso 2: Configure el sondeo de aplicaciones en la ficha Supervisar**

1. En Citrix DaaS, vaya a **Configuración** > **Configuración del sondeo** > **Sondeo de aplicaciones** y haga clic en **Crear sondeo**:
2. En la página **Crear sondeo**, introduzca el nombre del sondeo.
3. Seleccione la programación:

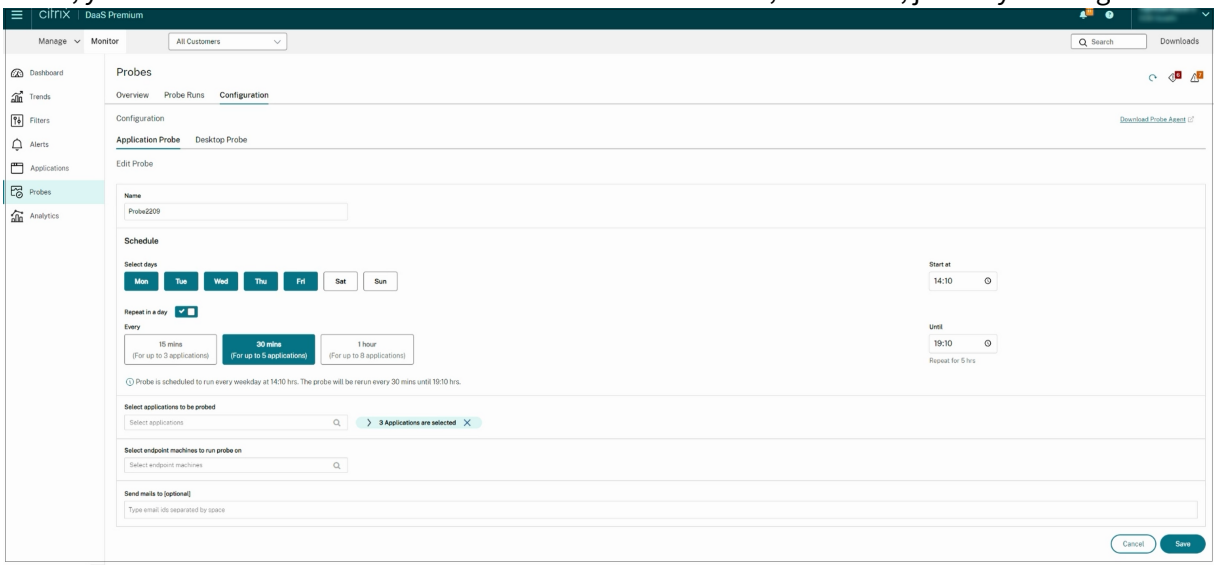
    a) Elija los días de la semana en los que quiere que se realice el sondeo.
    b) Introduzca la hora de inicio del sondeo.
    c) Además, puede elegir la opción **Repetir dentro de un día**. Introduzca la hora de finalización y el intervalo en el que quiere que el sondeo se repita dentro de un día. Por ejemplo, la siguiente configuración ayuda a ejecutar sondeos de aplicaciones desde las 12:08 horas hasta las 16:34 horas, que se repiten cada 30 minutos todos los lunes, miércoles, jueves y domingos.

4. Seleccione el número recomendado de aplicaciones que se van a sondear en función del intervalo.
5. Seleccione las máquinas de punto final en las que debe llevarse a cabo el sondeo.
6. Introduzca las direcciones de correo electrónico a las que se envían los resultados de errores en el sondeo y haga clic en **Guardar**.

En esta configuración, las sesiones de aplicaciones se inician a las 12:08 horas, 12:38 horas, 13:08

horas, y así sucesivamente hasta las 16:08 horas todos los lunes, miércoles, jueves y domingos.




**Nota:**

- Configure su servidor de correo electrónico en **Alertas** > **Configuración del servidor de correo electrónico**.
- Tras la configuración en la ficha **Supervisar**, el agente ejecuta los sondeos configurados a partir de la hora siguiente.
- Los sondeos que se configuraron antes de que se introdujera la opción **Repetir dentro de un día** siguen realizándose a la hora programada. De manera predeterminada, tienen inhabilitada la opción **Repetir dentro de un día**.

### Paso 3: Ejecute el sondeo

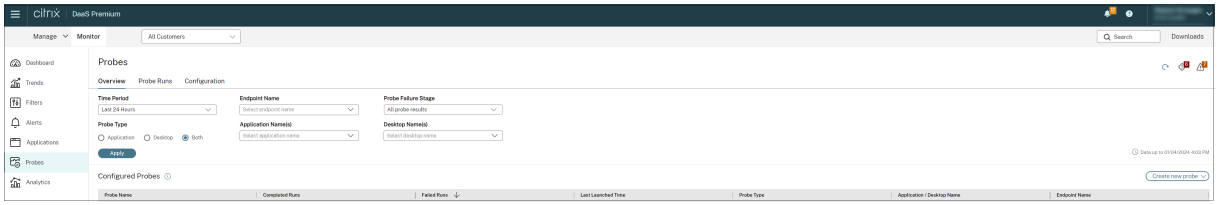
El agente ejecuta el sondeo de aplicaciones según esté configurado cada sondeo (la configuración se obtiene de Supervisar cada hora). Inicia las aplicaciones seleccionadas en serie mediante Workspace. El agente informa de los resultados a Supervisar a través de la base de datos de Supervisar. Los fallos se informan en cinco etapas específicas:

- **Accesibilidad de Workspace**: La URL configurada de Workspace no es accesible.
- **Autenticación de Workspace**: Las credenciales configuradas de Workspace no son válidas.
- **Enumeración de Workspace:** La lista de aplicaciones en Workspace no contiene la aplicación que quiere sondear.
- **Descarga de ICA:** El archivo ICA no está disponible.
- **Inicio de aplicación:** La aplicación no se ha podido iniciar.

**Paso 4: Consulte los resultados del sondeo**

Los resultados del último sondeo se encuentran en la página Citrix DaaS > **Aplicaciones**.




Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias** > **Resultados del sondeo de aplicaciones**.

En esta página, están disponibles los resultados completos de los sondeos realizados durante las últimas 24 horas o los últimos 7 días. Puede ver la etapa en la que falló el sondeo. Asimismo, puede filtrar la tabla para ver la aplicación específica, la etapa exacta del fallo del sondeo o la máquina de punto final concreta.

## Sondeo de escritorios

February 9, 2023

El sondeo de escritorios automatiza las comprobaciones de estado de las aplicaciones de Citrix Virtual Desktops publicadas en un sitio. Los resultados del sondeo de escritorios están disponibles en Supervisar. Ahora, Citrix Probe Agent admite sitios alojados en planos de control de Citrix Cloud Japan y Citrix Cloud Government.

En la página Configuración de Supervisar, configure los escritorios que se sondearán, las máquinas de punto final en las que se ejecutará el sondeo y el tiempo dedicado al sondeo. El agente prueba el inicio de los escritorios seleccionados mediante Workspace e informa de los resultados en Supervisar. Los resultados del sondeo se muestran en la interfaz de usuario de Supervisar: los datos de las últimas 24 horas en la página Aplicaciones, y los datos históricos del sondeo en la página **Tendencias > Resultados del sondeo > Resultados del sondeo de escritorios**.

Aquí verá la etapa en la que falló el sondeo: Accesibilidad de Workspace, Autenticación de Workspace, Enumeración de Workspace, Descarga de ICA o Inicio de escritorio. El informe de errores se envía a las direcciones de correo configuradas.

Puede programar los sondeos de escritorios para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar proactivamente los problemas relacionados con los escritorios aprovisionados, las máquinas de host o las conexiones, entre otros, antes de que los usuarios los experimenten.

Esta función requiere Probe Agent 1903 o una versión posterior.

Requisitos:

- Las máquinas de punto final con Probe Agents son máquinas Windows con la versión 4.8 de Citrix Receiver para Windows o una posterior, o versión 1906 de la aplicación Citrix Workspace para Windows (anteriormente Citrix Receiver para Windows) o una posterior. No se admite la aplicación Workspace para UWP.
- Citrix Probe Agent permite la autenticación predeterminada basada en formularios, tal y como la permiten StoreFront y Citrix Workspace. Citrix Probe Agent no permite otros métodos de autenticación, como Single Sign-On (SSO) o la autenticación de varios factores (MFA). Del mismo modo, Citrix Probe Agent solo funciona cuando no hay un servidor proxy o un equilibrador de carga implementados, como Citrix Gateway o Citrix ADC.
- Asegúrese de que la versión 4.7.2 de Microsoft .NET Framework o una posterior está instalada en la máquina de punto final donde quiere instalar Probe Agent.
- Para usar el agente de sondeos en el plano de control de Citrix Cloud Japan, establezca el valor del Registro en la ruta "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAgent\AGENT\regi en 2. Para usar el agente de sondeos en el plano de control de Citrix Cloud Government, establezca el valor del Registro en la ruta "\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ProbeAg en 3.

Cuentas de usuario o permisos requeridos para ejecutar el sondeo de escritorios:

- Un usuario único de Workspace para sondear aplicaciones en cada máquina de punto final. No es necesario que el usuario de Workspace sea un administrador; los sondeos pueden ejecutarse en un contexto no administrativo.
- Cuentas de usuario con permisos de administrador de Windows para instalar y configurar Citrix Probe Agent en las máquinas de punto final
- Una cuenta de administrador total o un rol personalizado con los siguientes permisos. Si reutiliza cuentas de usuarios normales para el sondeo de escritorios, podrían cerrarse las sesiones activas de esos usuarios.
  - Permisos de grupo de entrega:
    - Solo lectura
  - Permisos de supervisión:
    - Crear, modificar y eliminar la configuración del servidor de correo electrónico de alertas (si el servidor de correo electrónico aún no está configurado)
    - Crear, modificar y eliminar configuraciones de sondeo
    - Ver página Configuraciones
    - Ver página Tendencias

## Configurar sondeo de escritorios

Puede programar los sondeos de escritorios para que se ejecuten durante las horas de menor actividad en varios puntos geográficos. Unos resultados exhaustivos pueden ayudar a solucionar problemas relacionados con los escritorios aprovisionados, las máquinas de host o las conexiones antes de que los usuarios los experimenten.

Citrix Probe Agent versión 2103 es compatible con la agregación de sitios. Las aplicaciones y los escritorios se pueden enumerar e iniciar desde sitios agregados. Cuando configure el agente de sondeo, seleccione la opción **Agregación de sitios de Workspace (StoreFront) habilitada** para habilitar la enumeración de aplicaciones y escritorios desde sitios agregados. Se admiten las siguientes combinaciones de sitios:

- Varios sitios locales que tengan una URL de StoreFront.
- Sitios locales y en la nube que tengan una URL de StoreFront o Workspace.
- Varios sitios en la nube que tengan una URL de Workspace.

> **Nota:**
>
> Deberá crear administradores o usuarios independientes para configurar sondeos que tengan acceso a un solo sitio.

### Paso 1: Instale y configure el Citrix Probe Agent

Citrix Probe Agent es un ejecutable de Windows que simula el inicio del escritorio por parte del usuario a través de Workspace. Prueba los inicios de los escritorios siguiendo las pautas configuradas en Supervisar e informa de los resultados a Supervisar.

1. Identifique las máquinas de punto final desde donde ejecutar el sondeo de escritorios.
2. Los usuarios con privilegios administrativos pueden instalar y configurar Citrix Probe Agent en la máquina de punto final. Descargue el ejecutable de Citrix Probe Agent disponible en https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/components/app-probe-agent.html
3. Inicie el agente y configure sus credenciales de Workspace y Receiver para Web. Configure un usuario único de Workspace en cada máquina de punto final. Las credenciales se cifran y se almacenan de forma segura.

   > **Notas:**
   >
   > - Para acceder al sitio que va a sondear desde fuera de la red, escriba la URL de la página de inicio de sesión de Citrix Gateway en el campo URL de Workspace. Citrix Gateway enruta automáticamente la solicitud a la URL de Workspace del sitio correspondiente.

> Esta función está disponible a partir de la versión 12.1 de Citrix Gateway.
> - Utilice NetBIOS como el nombre de dominio en el campo del nombre de usuario. Por ejemplo, NetBIOS/nombredeusuario.
> - El sondeo de escritorios admite el uso de Citrix Content Collaboration Service mediante la autenticación de Workspace (solo AD).
> - Debe habilitar el inicio de sesión interactivo para el usuario único de StoreFront configurado.

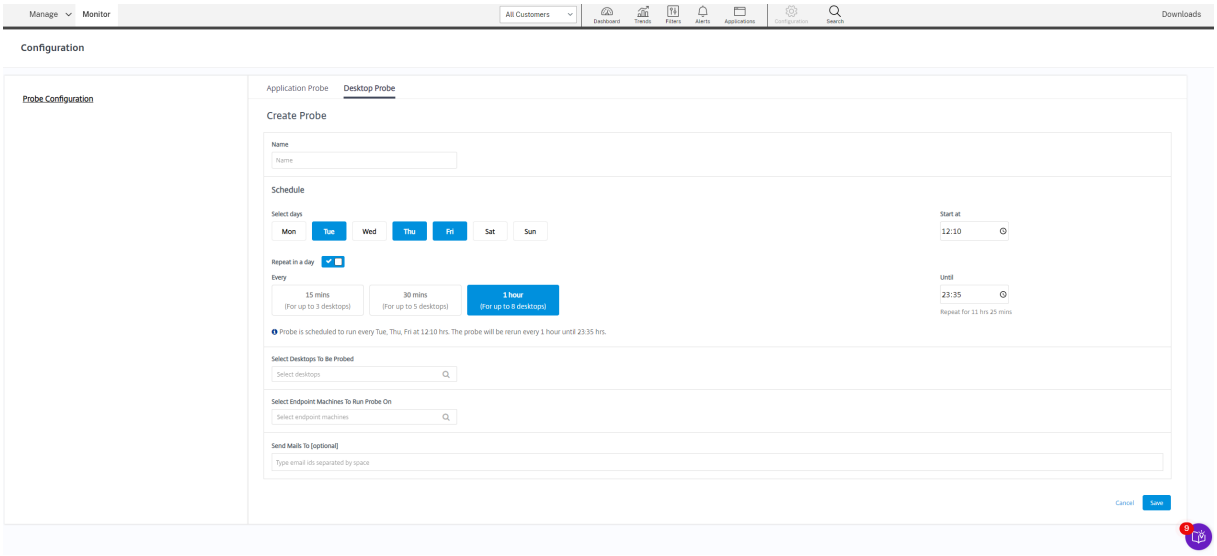
4. En la ficha **Configurar para mostrar el resultado del sondeo**, introduzca sus credenciales de Supervisar. Encontrará el nombre del cliente, el ID del cliente y la clave secreta en la página Acceso a API en la consola de Citrix Cloud.

**Paso 2: Configure el sondeo de escritorios en Supervisar**

1. En Citrix DaaS, vaya a **Configuración** > **Configuración del sondeo** > **Sondeo de aplicaciones** y haga clic en **Crear sondeo**:
2. En la página **Crear sondeo**, introduzca el nombre del sondeo.
3. Seleccione la programación:
   a) Elija los días de la semana en los que quiere que se realice el sondeo.
   b) Introduzca la hora de inicio del sondeo.
   c) Además, puede elegir la opción **Repetir dentro de un día**. Introduzca la hora de finalización y el intervalo en el que quiere que el sondeo se repita dentro de un día. Por ejemplo, la siguiente configuración ayuda a ejecutar sondeos de escritorios desde las 12:10 horas hasta las 23:35 horas, repitiéndose cada hora los martes, jueves y viernes.
4. Seleccione la cantidad recomendada de escritorios que se van a sondear en función del intervalo.
5. Seleccione las máquinas de punto final en las que debe llevarse a cabo el sondeo.
6. Introduzca las direcciones de correo electrónico a las que se envían los resultados de errores en el sondeo y haga clic en **Guardar**.

En esta configuración, las sesiones de escritorio se inician a las 12:10 horas, 13:10 horas, 14:10 horas, y así sucesivamente hasta las 23:10 horas todos los martes, jueves y viernes.




> **Nota:**
>
> - Configure su servidor de correo electrónico en **Alertas** > **Configuración del servidor de correo electrónico**.
> - Una vez finalizada la configuración del sondeo de escritorios, el agente ejecuta los sondeos configurados a partir de la hora siguiente.
> - Los sondeos que se configuraron antes de que se introdujera la opción **Repetir dentro de un día** siguen realizándose a la hora programada. De manera predeterminada, tienen inhabilitada la opción **Repetir dentro de un día**.

### Paso 3: Ejecute el sondeo

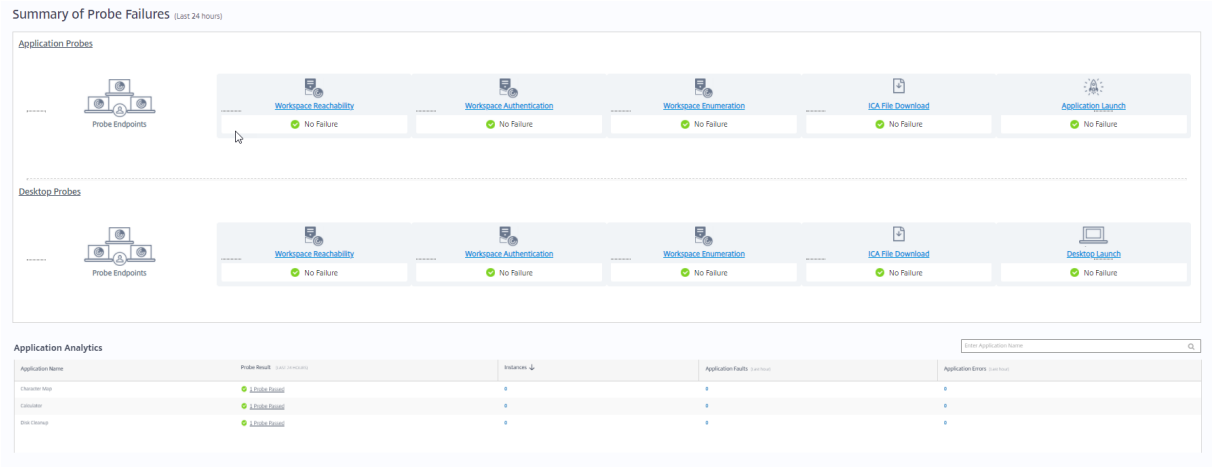
El agente ejecuta el sondeo de escritorios según la configuración de cada sondeo (esta se obtiene de Supervisar periódicamente). Inicia los escritorios seleccionados en serie mediante Workspace. El agente informa de los resultados a Supervisar a través de la base de datos de Supervisar. Los fallos se informan en cinco etapas específicas:

- **Accesibilidad de Workspace**: La URL configurada de Workspace no es accesible.
- **Autenticación de Workspace**: Las credenciales configuradas de Workspace no son válidas.
- **Enumeración de Workspace:** La lista de escritorios en Workspace no contiene el escritorio que quiere sondear.
- **Descarga de ICA:** El archivo ICA no está disponible.
- **Inicio del escritorio**: No se puede iniciar el escritorio.

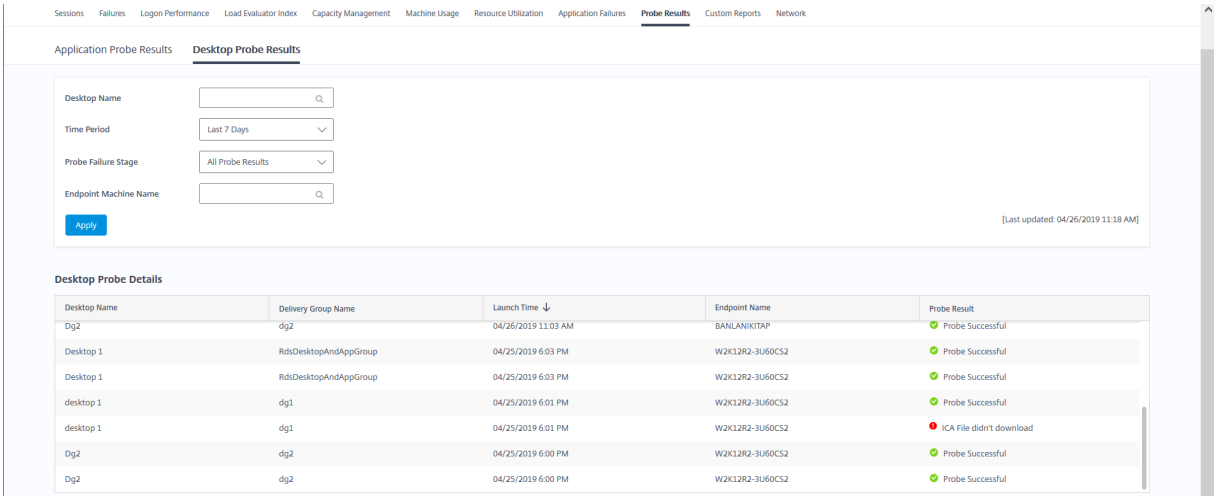
### Paso 4: Consulte los resultados del sondeo

Los resultados del último sondeo se encuentran en la página **Escritorios**.




Haga clic en el enlace de resultados del sondeo para ver más datos en la página **Tendencias** > **Resultados del sondeo** > **Resultados del sondeo de escritorios**.




En esta página, están disponibles los resultados completos de los sondeos realizados durante las últimas 24 horas o los últimos 7 días. Puede ver la etapa en la que falló el sondeo. Asimismo, puede filtrar la tabla para ver el escritorio específico, la etapa exacta del fallo del sondeo o la máquina de punto final concreta.

## Solucionar problemas de máquinas

May 17, 2024

> **Nota:**
>
> **Citrix Health Assistant** es una herramienta para solucionar problemas técnicos de configuración en VDA no registrados. La herramienta automatiza una serie de comprobaciones de

> estado para identificar las posibles causas de problemas en el registro de los VDA, el inicio de sesión y la configuración de la redirección de zonas horarias. Dispone de las instrucciones de descarga y uso de la herramienta **Citrix Health Assistant** en el artículo Citrix Health Assistant - Troubleshoot VDA Registration and Session Launch de Citrix Knowledge Center.

La vista **Filtros > Máquinas** en la consola de la ficha Supervisar muestra las máquinas configuradas en el sitio. La ficha Máquinas con SO multisesión incluye el índice del patrón de carga. Este índice indica la distribución de contadores de rendimiento, así como texto de ayuda sobre el recuento de sesiones si pasa el puntero sobre el vínculo.

Haga clic en la columna **Motivo del fallo** de la máquina donde se ha producido el fallo para obtener una descripción detallada de este y las acciones recomendadas para solucionarlo. Los motivos de los errores y las acciones recomendadas para fallos de máquinas y conexiones están disponibles en Citrix Director Failure Reasons Troubleshooting Guide.

Haga clic en el enlace del nombre de máquina para ir a la página **Detalles de la máquina**.

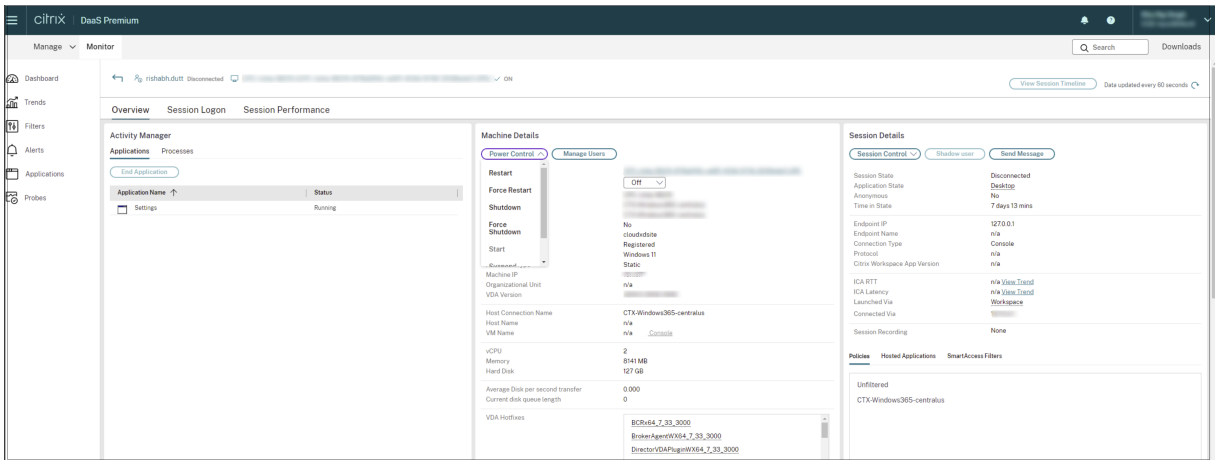
La página "Detalles de la máquina"muestra datos de la máquina, de la infraestructura y de los parches rápidos que se hayan aplicado a la máquina.

**Compatibilidad con los PC en la nube con HDX Plus para Windows 365 y Azure Virtual Desktop:**

> **Nota:**
>
> Para los PC en la nube con HDX Plus para Windows 365, solo están disponibles las opciones de Control de energía Reiniciar y Forzar reinicio. Para Azure Virtual Desktops (AVD) están disponibles todas las opciones de Control de energía.

Puede ver las opciones de Control de energía disponibles mediante uno de los métodos siguientes:

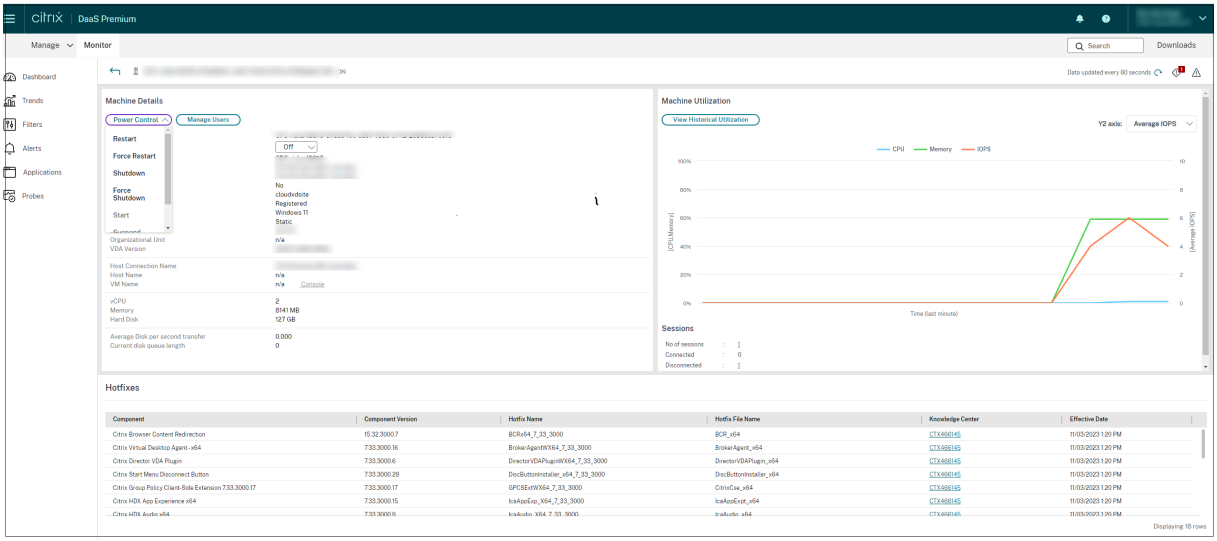
Haga clic en la lista desplegable **Filtros** > **Sesiones** > **Ver detalles** > **Detalles de la máquina** > **Control de energía** y seleccione una opción para asignar la opción de control de energía requerida a una máquina.



O bien:

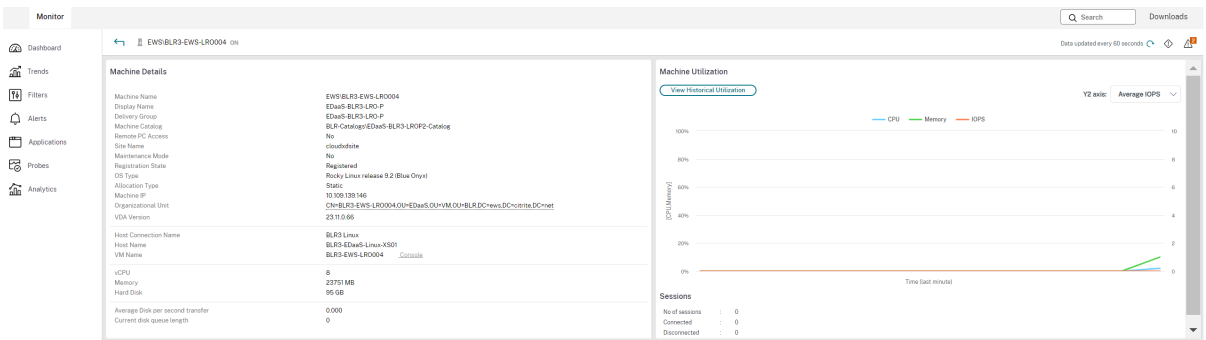
Haga clic en la lista desplegable **Filtros** > **Máquina** > **Detalles de la máquina** > **Control de energía** y seleccione una opción para asignar la opción de control de energía requerida a una máquina.




## Usar recursos en tiempo real en cada máquina

El panel **Utilización de máquinas** muestra gráficos del uso en tiempo real de la CPU y la memoria. Además, dispone de gráficos de supervisión del disco y la GPU para aquellos sitios que tengan agentes VDA con la versión 7.14 o una posterior.

Los gráficos de supervisión de disco, la latencia de disco y el promedio IOPS son métricas de rendimiento importantes que le ayudan a supervisar y solucionar problemas relacionados con los discos VDA. El gráfico de IOPS medias muestra la cantidad media de lecturas y escrituras en un disco. Seleccione **Latencia de disco** para ver un gráfico de la demora entre una solicitud de datos y su retorno desde el disco, medida en milésimas de segundo.



### Utilización de GPU

Seleccione **Utilización de GPU** para ver, en porcentajes, el uso de la GPU, la memoria de la GPU y del codificador y el decodificador para solucionar problemas relacionados con la GPU en los agentes VDA de SO de sesión única o multisesión.

**Versiones de GPU compatibles:**

- Versión 369.17 de las GPU de NVIDIA Tesla M60 con controlador de pantalla o una posterior. Para obtener más información, consulte NVIDIA vGPU Software.
- Las GPU de AMD Radeon Instinct MI25 y las CPU AMD EPYC 7V12 (Rome). Para obtener más información, consulte AMD Drivers and Support.

**Controladores:**

Los controladores o extensiones adecuados deben estar instalados en los VDA.

- Para las GPU de NVIDIA, instale los controladores GRID manualmente o mediante extensiones. Para obtener más información, consulte NVIDIA vGPU Software.
  - Tenga en cuenta que NVIDIA solo admite controladores GRID. Los controladores CUDA no funcionan con la serie NVadsA10 v5 y no son compatibles.
  - Para ver un ejemplo del proceso de instalación de controladores GRID de GPU de NVIDIA mediante extensiones en máquinas basadas en Azure, consulte Controladores GRID de NVIDIA. Extensión del controlador de GPU de NVIDIA - Máquinas virtuales de Azure Windows - Máquinas virtuales de Azure.
  - Para ver un ejemplo del proceso de instalación manual de controladores GRID de GPU de NVIDIA, consulte Instalación de controladores de GPU de NVIDIA en VM de la serie N con Windows - Máquinas virtuales de Azure.
- Para las GPU de AMD, instale los controladores de gráficos AMD manualmente o mediante extensiones. Para obtener más información, consulte AMD Drivers and Support.
  - Para ver un ejemplo del proceso de instalación de controladores de GPU de AMD mediante extensiones en máquinas basadas en Azure, consulte Extensión del controlador de GPU de AMD - Máquinas virtuales Windows de Azure - Máquinas virtuales de Azure.
  - Para ver un ejemplo del proceso de instalación manual de los controladores de GPU de AMD en máquinas de Azure, consulte Instalación de controladores de GPU de AMD en máquinas virtuales de la serie N con Windows.

**Notas de uso:**

- Los gráficos de Utilización de GPU solo están disponibles para los VDA con Windows de 64 bits.
- Los gráficos de Utilización de GPU de AMD solo están disponibles para los VDA que ejecutan Citrix Virtual Apps and Desktops 7 2212 o versiones posteriores.

- Los VDA deben tener HDX 3D Pro habilitado para proporcionar la aceleración de GPU. Para obtener más información, consulte Aceleración de GPU para sistemas operativos de sesión única Windows y Aceleración de GPU para sistemas operativos multisesión Windows.
- Cuando el VDA accede a más de una GPU, el gráfico de uso muestra el promedio de las métricas de GPU recopiladas a partir de las GPU individuales. Las métricas de la GPU se recopilan del VDA entero, no de procesos individuales.
- Para AMD, el uso del codificador y del decodificador no se permite por separado. Cualquier carga de trabajo de codificación/decodificación que utilice la GPU se registrará como la carga 3D general del uso de la GPU.
- Asegúrese de instalar la WMI de NVIDIA durante la instalación. Esta ventana solo está disponible durante la instalación manual.
- Si los controladores están instalados, pero Director no detecta la GPU
  - Compruebe el Administrador de tareas. Si los controladores están instalados correctamente, la GPU debería aparecer en el Administrador de tareas.
  - Compruebe que la máquina esté registrada. A veces, las máquinas pueden tardar un tiempo en detectarse que están conectadas.
- Si el uso de la GPU no muestra actividad en Director, asegúrese de que la carga de trabajo activa utilice la GPU. Para las cargas de trabajo gráficas, puede habilitar esto desde Configuración > Sistema > Pantalla > Configuración gráfica > Elija la aplicación para configurar las preferencias. Asegúrese de activar Alto rendimiento. A veces, Windows utiliza de forma predeterminada la CPU para cargas de trabajo gráficas cuando está configurada como predeterminada del sistema o para ahorrar energía, según otros parámetros.
- Los datos se actualizan cada minuto y la visualización de los datos comienza un minuto después de seleccionar **Utilización de la GPU**.

### Usar recursos históricos en cada máquina

En el panel **Utilización de máquinas**, haga clic en **Ver utilización histórica** para ver el historial del uso de los recursos en la máquina seleccionada.
Los gráficos de utilización contienen contadores de rendimiento de la CPU, la memoria, el pico de sesiones simultáneas, el promedio de IOPS y la latencia de disco.

> **Nota:**
>
> La configuración de la directiva de Supervisión **Habilitar supervisión de procesos** debe estar establecida en "Permitida"para recopilar y mostrar datos en la tabla "10 procesos principales" de la página "Utilización histórica de máquinas". La recopilación de datos está inhabilitada de forma predeterminada.

De forma predeterminada, se recopilan los datos referentes al uso de la CPU, la memoria, el promedio

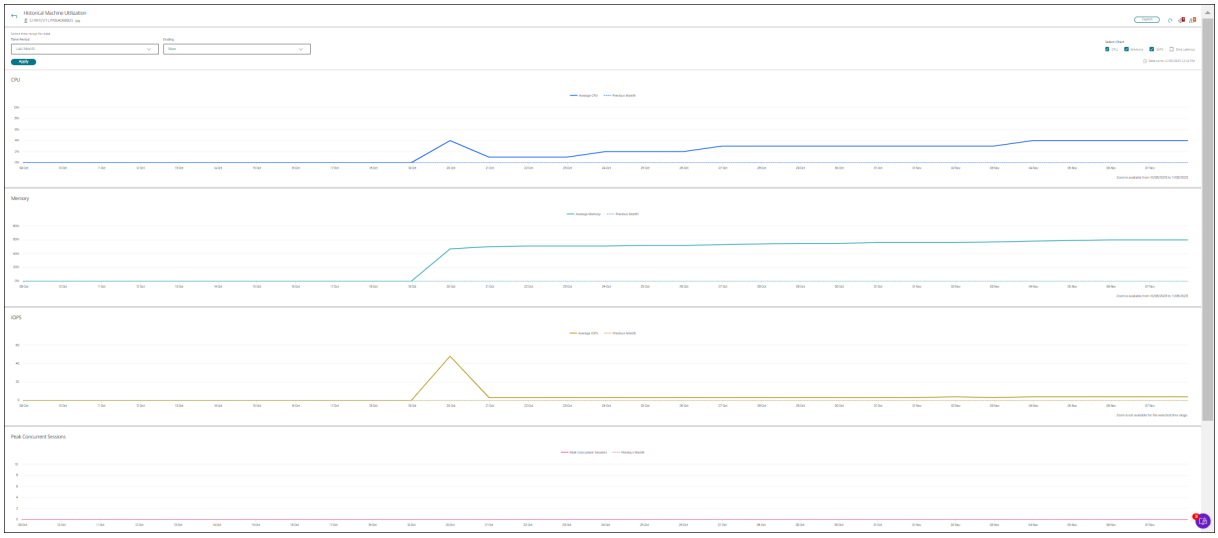
de IOPS y la latencia de disco. Puede inhabilitar la recopilación mediante la configuración de directiva **Habilitar supervisión de recursos**.


1. En el panel **Utilización de máquinas** de la vista **Detalles de la máquina**, seleccione **Ver utilización histórica**.
2. En la página **Utilización histórica de máquinas**, establezca el **Período de tiempo** para ver las últimas 2 horas, 24 horas, 7 días, o bien el último mes o año.

   > **Nota:**
   >
   > Los datos de uso del promedio de IOPS y la latencia de disco están disponibles solamente para las últimas 24 horas, el último mes y el último año contando hasta el momento actual. No se admite establecer un tiempo de finalización personalizado.

3. Haga clic en **Aplicar** y seleccione los gráficos necesarios.
4. Pase el cursor sobre las diferentes secciones del gráfico para ver más información sobre un período de tiempo seleccionado.



Por ejemplo: si selecciona **Últimas 2 horas**, el período de referencia será de 2 horas antes del intervalo de tiempo seleccionado. Verá las tendencias de uso de la CPU, la memoria y la sesión entre las últimas 2 horas y el punto de referencia. Si selecciona **Último mes**, el período de referencia será el mes anterior. Seleccione esta opción para ver la latencia de disco y el promedio de IOPS entre el último mes y el punto de referencia.

1. Haga clic en **Exportar** para exportar los datos de utilización de recursos durante el período seleccionado. Para obtener más información, consulte la sección Exportar informes en "Supervisar implementaciones".
2. Debajo de los gráficos, en la tabla, aparecen los 10 procesos principales que consumen más CPU o memoria. Puede ordenarla por cualquiera de las columnas: Nombre de la aplicación, Nombre de usuario, ID de sesión, Promedio de CPU, Pico de CPU, Promedio de memoria y Pico de memoria durante el intervalo de tiempo seleccionado. Las columnas IOPS y Latencia de disco no se pueden ordenar.

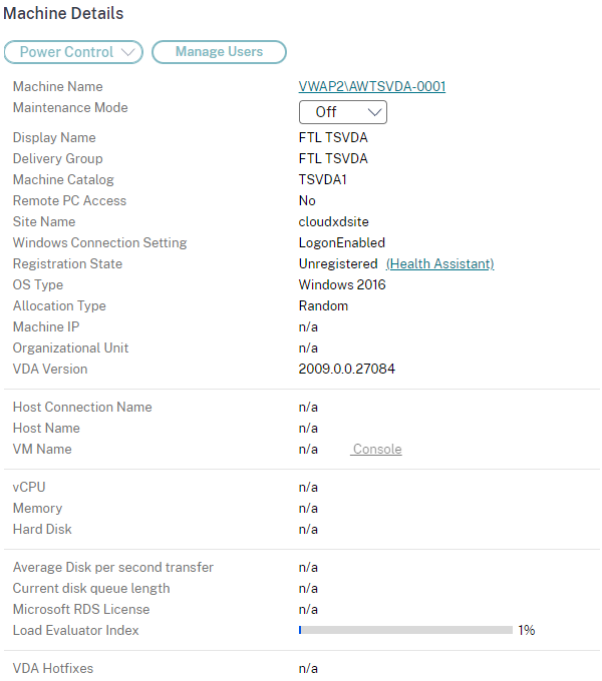
   > **Nota:**
   >
   > - El ID de sesión aparece como "0000"para los procesos del sistema.
   > - Si un sitio que pertenece al plano Citrix Cloud Japan o Citrix Cloud Government contiene más de 5000 máquinas, los datos de proceso solo están disponibles para un máximo de 2000 máquinas. La directiva de supervisión de procesos debe estar habilitada en estas máquinas.

3. Para ver la tendencia histórica en el consumo de recursos de un proceso concreto, consulte los detalles de cualquiera de los diez procesos principales.

### Acceso a la consola de la máquina

Puede acceder a las consolas de las máquinas de sistema operativo de escritorio y multisesión alojadas en XenServer 7.3 y posterior directamente desde Supervisar. De esta manera, no necesita XenCenter para solucionar problemas en los VDA alojados en XenServer. Para que esta función esté disponible, el servidor XenServer que aloja la máquina debe tener la versión 7.3 o una posterior, y debe poder accederse a él desde Supervisar.




Para solucionar un problema en una máquina, haga clic en el enlace **Consola** en el panel "Detalles de la máquina"en la máquina correspondiente. Después de la autenticación de las credenciales de host que proporcione, la consola de la máquina se abrirá en otra ficha mediante noVNC, un cliente web VNC. Ahora tiene acceso por teclado y mouse a la consola.

> **Nota:**
>
> - Esta función no es compatible con Internet Explorer 11.
> - Si la posición del puntero en la consola no coincide con la posición del puntero en la máquina, consulte CTX230727 para conocer los pasos para solucionar el problema.
> - El acceso a la consola se inicia en una nueva ficha; por eso, su explorador web debe permitir las ventanas emergentes.
> - Por razones de seguridad, Citrix recomienda instalar certificados SSL en su explorador web.

### Inspeccionar las máquinas con acciones de energía recientes

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

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

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

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

En la ficha **Filtros** -> **Máquinas**. En este caso, las columnas **Hora de acción de energía** y **Resultado de la acción de energía** están visibles de forma predeterminada. También puede seleccionar qué columnas quiere hacer visibles.

En la ficha **Optimización de costes**. En este caso, el filtro predeterminado **Acción de energía desencadenada por** está configurado en *Autoscale* y el valor de **Resultado de la acción de energía** está establecido en *Fallido*.

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

Se agregan estos filtros para ver el estado de la acción de energía:

| Filtro | Descripción |
| --- | --- |
| Resultado de la acción de energía | Muestra el resultado de la acción de energía. Los valores de filtro posibles son correcto y fallido. |
| Acción de energía desencadenada por | Muestra quién o qué desencadenó la acción de energía. Los valores de filtro posibles son los siguientes<br>• Autoscale: Este valor aparece cuando lo que desencadena una acción de energía es lo siguiente<br>• Cuando el administrador apaga una VM para limpiar su disco de SO y devolverlo a su estado inicial |

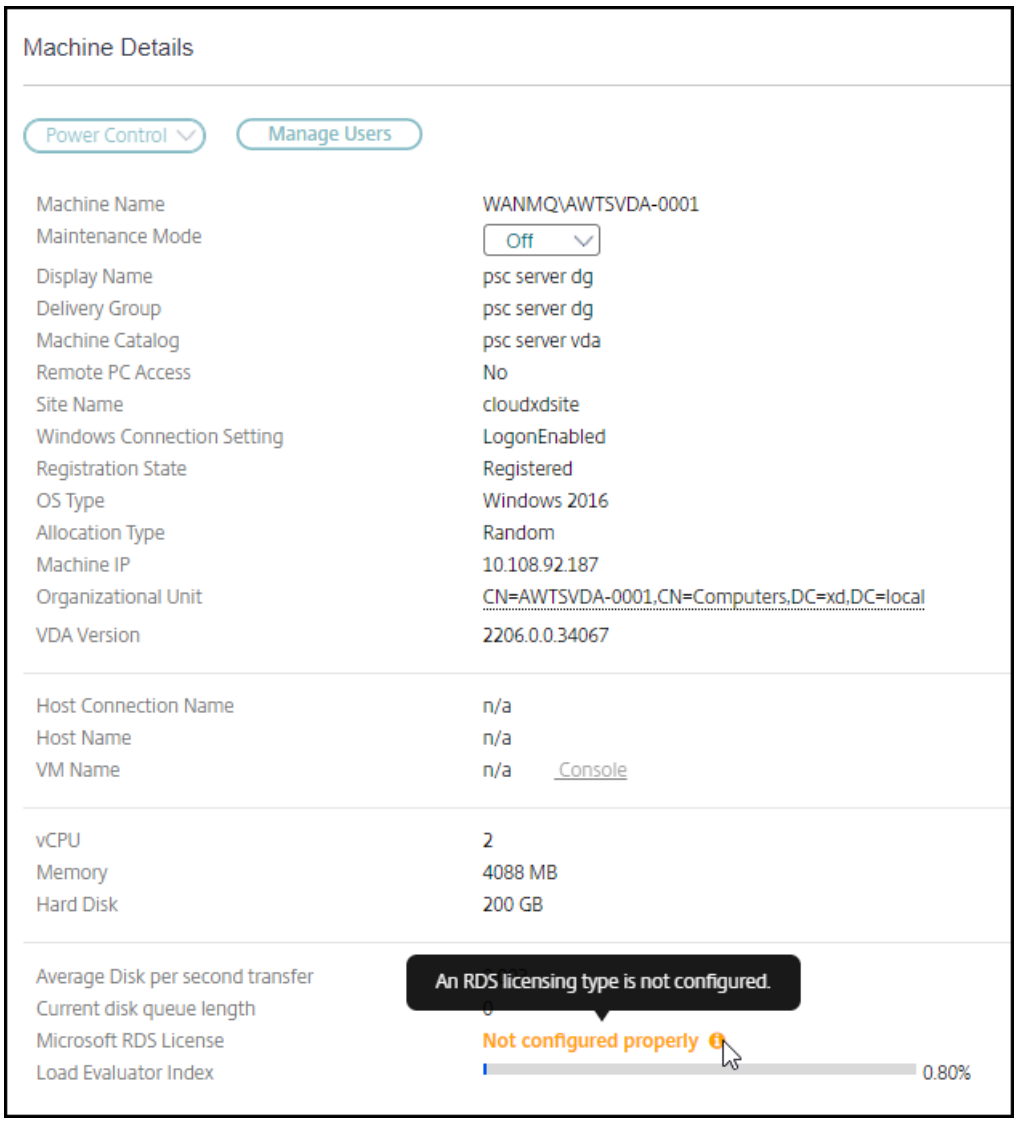
 

| Filtro | Descripción |
| --- | --- |
| | • Cuando una VM se apaga o suspende en función de las directivas establecidas<br>• Cuando una VM se hace disponible en función de la configuración del tamaño de la agrupación o el tamaño del búfer<br>• Administrador: Este valor aparece cuando un administrador desencadena una acción de energía. Los posibles ejemplos son cuando el administrador solicita apagar, encender, suspender, reanudar o reiniciar una VM.<br>• Usuario: Este valor aparece cuando un usuario desencadena una acción de energía. Los ejemplos son cuando un usuario restablece, inicia o reanuda el trabajo en la máquina virtual.<br>• Otros: Este valor aparece cuando se desencadena una acción de energía por motivos de programación y desconocidos. |
| Última acción de energía | Muestra la acción exacta de energía que tuvo lugar en la máquina, como encender, apagar, apagar, reiniciar, restablecer, reanudar, etc. |
| Hora de acción de energía | El momento en que se completa la acción de energía. Los valores de filtro posibles son última hora, últimos 5 minutos, últimos 30 minutos, última hora, hoy, últimas 24 horas y ayer. |
| Motivo del fallo de la acción de energía | Muestra el motivo del fallo. Los valores de filtro posibles son fallo notificado por hipervisor, se ha superado el límite de frecuencia del hipervisor, error desconocido y ninguno. Si la acción se ha realizado correctamente, aparece "Ninguno". |

### Estado de licencias RDS de Microsoft

El estado de la licencia RDS (Servicios de Escritorio remoto) de Microsoft aparece en el panel "Detalles" de la página **Detalles de la máquina** y **Detalles del usuario** para las máquinas de SO multisesión.




Se muestra uno de los siguientes mensajes:

- Licencia disponible
- No se ha configurado correctamente (advertencia)
- Error de licencia (error)
- Versión incompatible de VDA (error)

> **Nota:**
>
> En el estado de la licencia RDS para máquinas en período de gracia con una licencia válida, se muestra el mensaje **Licencia disponible** en color verde. Renueve la licencia antes de que caduque.

Cuando se trata de mensajes de advertencia y de error, coloque el puntero sobre el icono de información para ver información adicional como se indica en la tabla siguiente.

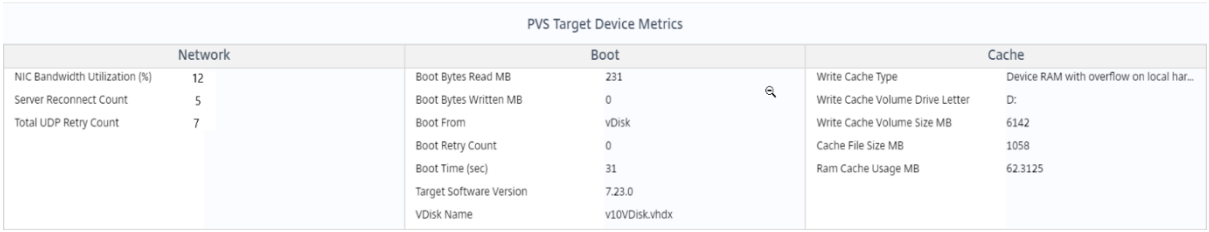
| Tipo de mensaje | Mensajes en Supervisar |
| --- | --- |
| Error | Disponible para VDA 7.16 y posterior. |
| Error | No se permiten nuevas conexiones RDS. |
| Error | La licencia RDS ha excedido su período de gracia. |
| Error | Hay un servidor de licencias que no está configurado para el nivel de SO requerido con el tipo de licencia de acceso de cliente por dispositivo. |
| Error | El servidor de licencias configurado no es compatible con el nivel de SO del host RDS con el tipo de licencia de acceso de cliente por dispositivo. |
| Advertencia | Una licencia de Terminal Server temporal no es un tipo de licencia RDS válido en una implementación de Citrix Virtual Apps and Desktops. |
| Advertencia | El escritorio remoto para administración no es un tipo de licencia válido en una implementación de Citrix Virtual Apps and Desktops. |
| Advertencia | No hay ningún tipo de licencia RDS configurado. |
| Advertencia | No se puede acceder al controlador de dominio o al servidor de licencias con el tipo de licencia RDS de acceso de cliente por dispositivo. |
| Advertencia | Con el tipo de licencia de acceso de cliente por dispositivo, la licencia del dispositivo de cliente no se pudo determinar, ya que no se puede acceder al servidor de licencias para el nivel de SO que se requiere. |

> **Nota:**
>
> Esta función solo se aplica a Microsoft RDS CAL (Licencia de acceso de cliente).

### Métricas de dispositivo de destino de PVS

Puede ver el estado de los dispositivos de destino de PVS para máquinas con sistema operativo de sesión única y multisesión en la página **Detalles de la máquina** en Supervisar. En este panel, hay disponibles varias métricas de **Red**, **Arranque** y **Caché**. Estas métricas le ayudan a supervisar y solucionar problemas en los dispositivos de destino de PVS para asegurarse de que funcionen correctamente.




**Red:**

- Uso del ancho de banda de NIC: Utilización media del ancho de banda en todas las NIC.
- Recuento de reconexiones del servidor: Número de veces que el servidor se ha vuelto a conectar debido a problemas de red o reequilibrio de servidores, o bien a apagado y reinicio de Citrix Provisioning Stream Service.
- Recuento total de reintentos de UDP: Número de veces que el dispositivo de destino de Provisioning ha intentado volver a conectarse al servidor de Provisioning mediante UDP. Esta métrica le permite saber si hay algún problema de red en Citrix Provisioning Stream Service (por ejemplo, configuraciones de conmutación incorrectas).

**Arranque:**

- Lectura de bytes de arranque en MB: Bytes leídos durante el arranque.
- Escritura de bytes de arranque en MB: Bytes escritos durante el arranque.
- Arranque desde: Medio de arranque (vDisk, disco local, etc.).
- Recuento de reintentos de arranque: Número de reintentos para arrancar la máquina.
- Tiempo de arranque: Tiempo que tarda en arrancar la máquina, en segundos. De forma predeterminada, hay una demora de 5 segundos entre reintentos. Si esta demora alcanza o supera 10 segundos, hay un aumento significativo en el tiempo de arranque. Compruebe la configuración de Provisioning para resolver este problema.
- Versión de software de destino: Versión del software del dispositivo de destino de Provisioning.
- Nombre de vDisk: Disco virtual desde el que se inicia el dispositivo de destino de Provisioning.

**Caché:**

- Tipo de caché de escritura: vDisk se puede establecer en diferentes tipos de caché. Para obtener más información, consulte el artículo CTX119469 de Knowledge Center.
- Letra de la unidad del volumen de caché de escritura: Letra de la unidad para los tipos de caché de escritura que implican unidades.
- Tamaño de volumen de caché de escritura en MB: Tamaño total del volumen configurado para caché de escritura.
- Tamaño del archivo de caché en MB: Tamaño actual del archivo de caché (caché en la memoria RAM del dispositivo con desbordamiento en el disco duro).
- Uso de caché de RAM en MB: Tamaño actual de caché de RAM (caché en la memoria RAM del dispositivo con desbordamiento en el disco duro). Use el desbordamiento en disco solo si es necesario. Esta métrica es útil para configurar u optimizar el tamaño de caché de RAM.

Para obtener más información, consulte Usar la herramienta Status Tray en un dispositivo de destino.

Las métricas de dispositivos de destino de Provisioning solo están disponible en:

- Máquinas de Provisioning
- Dispositivos de destino de Provisioning 7.19 y versiones posteriores.
- VDA 2003 y versiones posteriores.

> **Nota:**
>
> Las métricas de Recuento de reconexiones del servidor y el Recuento de reintentos UDP solo están disponibles para la versión de destino de Provisioning 1912 CU2 y versiones posteriores.

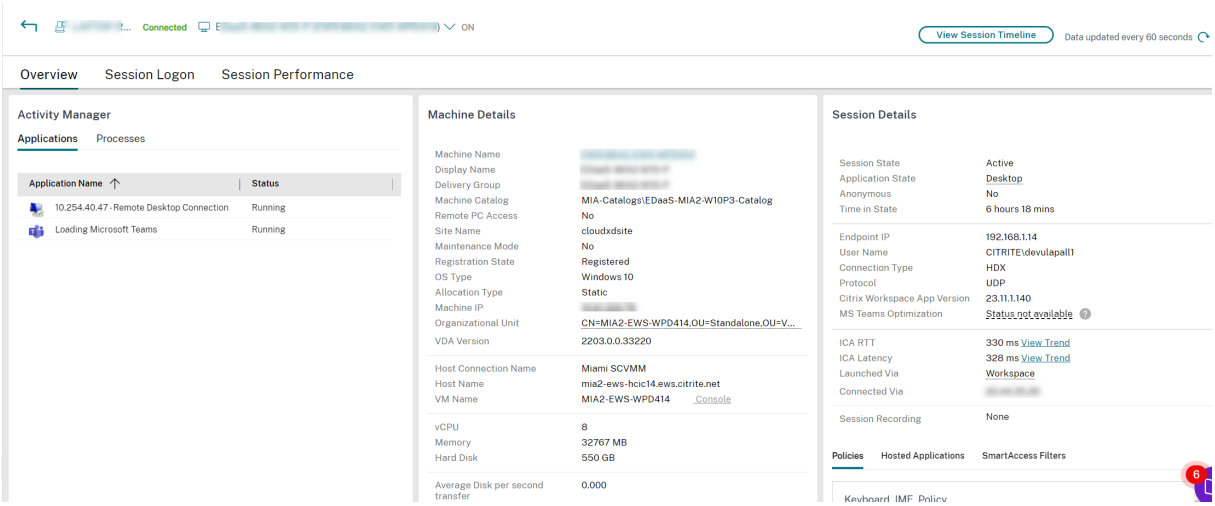
## Solucionar problemas de usuarios

May 17, 2024

Use el **Servicio de asistencia** de Supervisar (página **Administrador de actividades**) para ver información sobre el usuario o el dispositivo de punto final:

Al hacer clic en **Ver detalles** en el Administrador de actividades del usuario, se abre la página **Detalles del usuario**.
Al hacer clic en **Ver detalles** en el Administrador de actividades del dispositivo de punto final, se abre la página **Detalles del dispositivo de punto final**.




Si el usuario ha iniciado más de una sesión, se muestra el selector de sesiones.


Elija una sesión para ver los detalles.

- Consulte los detalles de la sesión, la experiencia de inicio de sesión del usuario, el inicio de la sesión, la conexión y las aplicaciones.
- puede reflejar la máquina del usuario.
- Solucione el problema con las acciones recomendadas en la tabla siguiente y, si es necesario, remita el problema al administrador que corresponda.

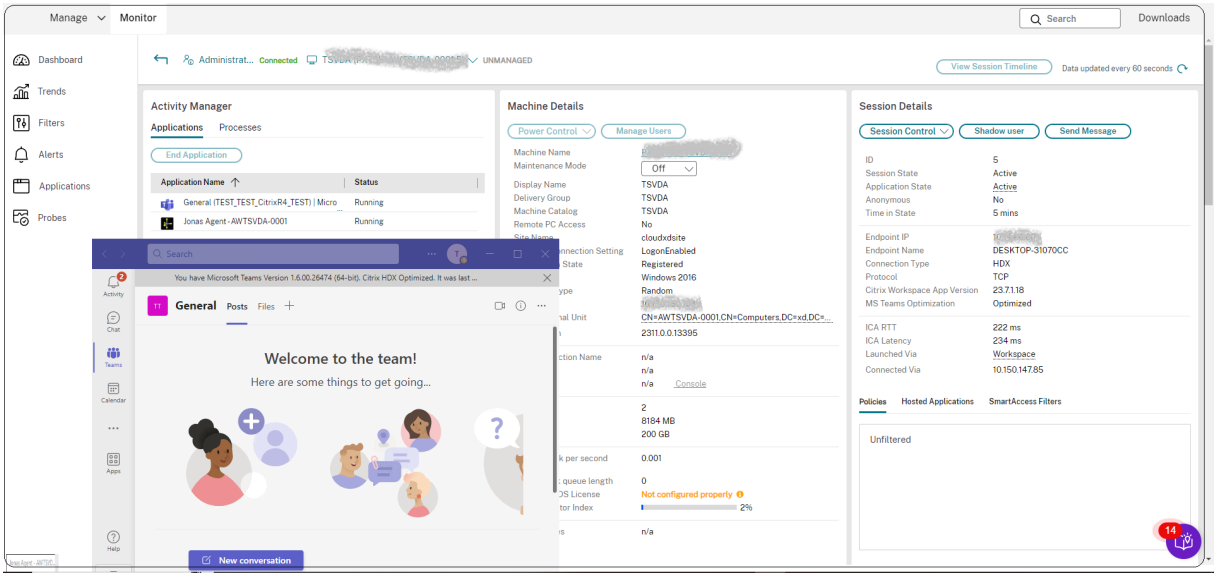
### Estado de optimización de Microsoft Teams

Citrix Monitor muestra el estado de optimización de Microsoft Teams para las sesiones de HDX en la página **Detalles del usuario** > panel **Detalles de la sesión** > campo **Optimización de MS Teams**. La optimización de Microsoft Teams es fundamental para una mejor experiencia de usuario, como audio y vídeo nítidos. La visibilidad del estado de optimización de Microsoft Teams es útil para reducir el tiempo necesario para resolver los tíquets y ayuda a los administradores a identificar las métricas importantes durante la solución de problemas.

> **Nota:**
>
> Supervisar de Citrix es compatible con la versión 2.1 o anterior de Microsoft Teams.

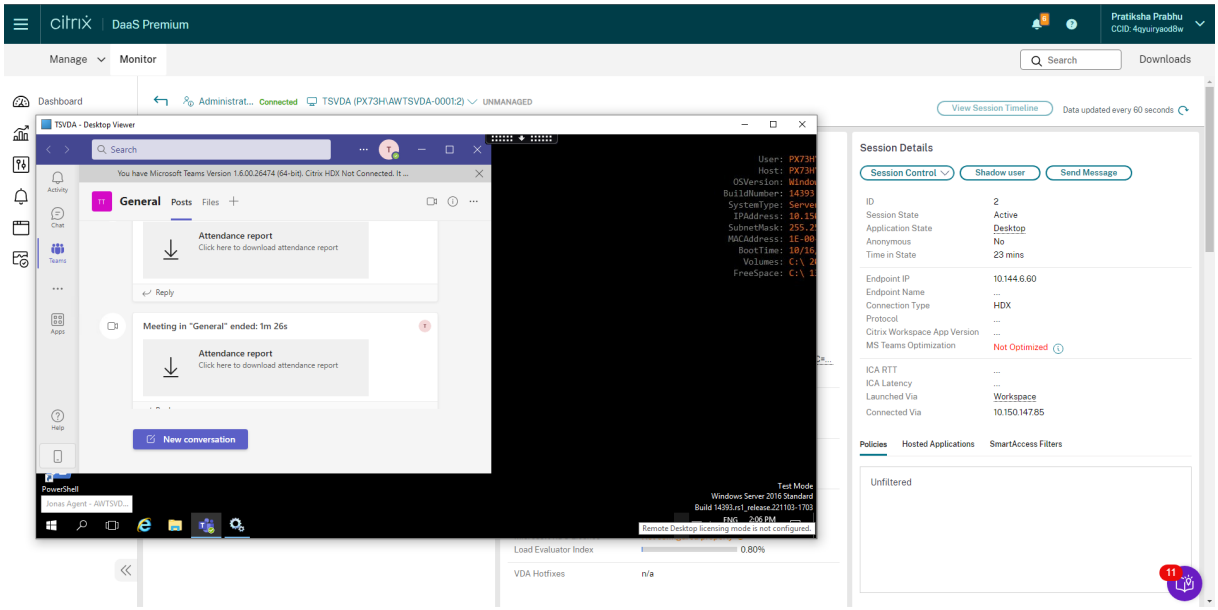
Requisitos previos:

- Las versiones de la aplicación Citrix Workspace compatibles se enumeran en Optimización para Microsoft Teams.
- Microsoft Teams se ejecuta como una aplicación publicada o dentro de un escritorio publicado.
- Se están ejecutando servicios cruciales, como el servicio de redirección de vídeo HTML5 de Citrix HDX.




Si los MS Teams no están optimizados, el texto de ayuda proporciona un enlace a un artículo externo en directo de resolución de problemas de HDX que contiene consejos para optimizar Microsoft Teams. Solución de problemas de optimización de HDX.




## Sugerencias para solucionar problemas

| Problema de los usuarios | Sugerencias |
|---|---|
| El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente | Diagnosticar problemas de inicio de sesión de los usuarios |
| El inicio de sesión tarda mucho tiempo o falla de forma intermitente o repetidamente | Diagnosticar problemas de inicio de sesión |
| Identificar los componentes involucrados en el establecimiento de la sesión | Analizar la vista de topología de sesión |
| La respuesta de la sesión es lenta o inexistente | Diagnosticar problemas de rendimiento de sesión |
| La aplicación es lenta o no responde | Resolver fallos de aplicaciones |
| La conexión falló | Restaurar conexiones de escritorio |
| La sesión es lenta o no responde | Restaurar sesiones |
| El vídeo es lento o de poca calidad | Generar informes del sistema de canales HDX |

> **Nota:**
>
> Para comprobar que la máquina no está en modo de mantenimiento, en la vista "Detalles del usuario", consulte el panel "Detalles de la máquina".

### Rendimiento de sesión

La ficha **Rendimiento de sesión** cuenta con flujos de trabajo de solución de problemas mejorados, empezando por la capacidad de correlacionar métricas en tiempo real para identificar problemas dentro de las sesiones de los usuarios. El panel **Topología de sesión** proporciona una representación visual de la ruta de las sesiones de HDX conectadas. El panel de **Métricas de rendimiento** ofrece tendencias para las métricas de sesión como ICARTT, la latencia de ICA, los fotogramas por segundo, el ancho de banda de salida disponible y el ancho de banda de salida consumido, ayudan a indicar el rendimiento de estas métricas a lo largo del tiempo. Para obtener más información, consulte Diagnosticar problemas de rendimiento.

### Sugerencias para la búsqueda

La búsqueda de nombre de usuario se realiza en todas las instancias de Active Directory configuradas.

Al escribir el nombre de una máquina multiusuario en el campo Buscar, se muestran los detalles de la máquina especificada.

Al escribir el nombre de un dispositivo de punto final en el campo Buscar, se muestran las sesiones sin autenticar (anónimas) y las sesiones autenticadas que están conectadas a un punto final específico. Esta lista habilita la solución de problemas para sesiones no autenticadas. Asegúrese de que los nombres de los dispositivos de punto final son exclusivos para poder resolver problemas de sesiones no autenticadas.

Los resultados de la búsqueda incluyen también usuarios que no están utilizando máquinas en ese momento o no tienen asignada ninguna.

- Las búsquedas no distinguen el uso de mayúsculas y minúsculas.
- Las entradas parciales generan una lista de posibles coincidencias.
- Después de escribir unas pocas letras de un nombre que tiene dos partes, separadas por un espacio, los resultados incluyen coincidencias para ambas cadenas. Los ejemplos de nombres que constan de dos partes son el nombre de usuario, el apellido y el nombre, o el nombre para mostrar. Por ejemplo: si escribe “ju rod”, los resultados pueden incluir cadenas como “Juan Rodríguez”o “Rodrigo Juárez”.

Para volver a la página inicial, haga clic en la ficha **Supervisar**.

## Diagnóstico de problemas de inicio de sesión

February 21, 2024

Además de las fases del proceso de inicio de sesión mencionadas en la sección Diagnosticar problemas de inicio de sesión de los usuarios, Supervisar muestra la duración del inicio de la sesión. Esta duración se divide en la duración de Inicio de sesión en la aplicación Workspace e Inicio de sesión en VDA, en las páginas **Detalles del usuario** y **Detalles de la máquina**. Estas dos duraciones contienen más fases individuales cuyas duraciones de inicio también se muestran. Estos datos le ayudan a comprender y solucionar problemas con una duración elevada para iniciar las sesiones. Además, la duración de cada fase involucrada en el inicio de las sesiones ayuda a solucionar problemas asociados a fases individuales. Por ejemplo: si el tiempo de asignación de unidades es elevado, puede comprobar si todas las unidades válidas se asignan correctamente en el objeto de directiva de grupo o en el script.

### Requisitos previos

Debe cumplir los siguientes requisitos previos para que se muestren los datos de duración de inicio de sesión:

- VDA 1903 o una versión posterior.
- El servicio Citrix End User Experience Monitoring (EUEM) debe ejecutarse en el VDA.

### Limitaciones

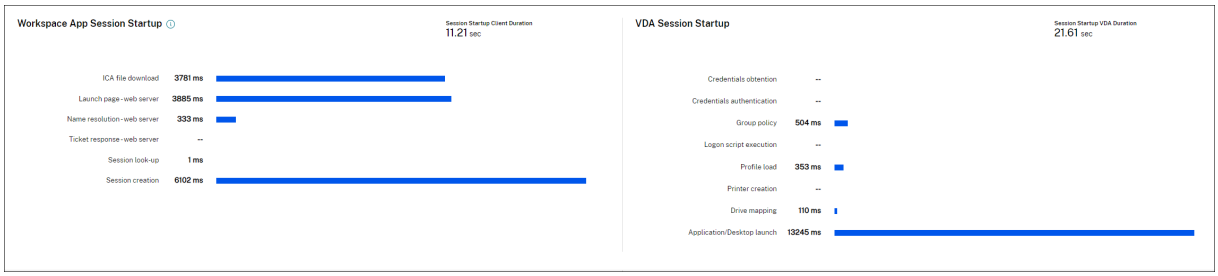
Las siguientes limitaciones se aplican cuando Supervisar muestra los datos de duración de inicio de sesión.

- La duración de inicio de sesión solo está disponible para sesiones HDX.
- Para el inicio de sesiones desde los sistemas operativos iOS y Android, solo está disponible la duración de inicio en VDA.
- IFDCD solo está disponible cuando se detecta la aplicación Workspace al llevar a cabo el inicio desde un explorador.
- Para el inicio de sesiones desde macOS, IFDCD solo está disponible para la aplicación Workspace 1902 y versiones posteriores.
- Para el inicio de sesiones desde el sistema operativo Windows, IFDCD está disponible para la aplicación Workspace 1902 y versiones posteriores. Para las versiones anteriores, IFDCD solo se muestra para el inicio de aplicaciones desde un explorador con la aplicación Workspace detectada.

> **Notas:**
>
> - Si tiene problemas en la pantalla de duración de inicio de sesiones una vez que se hayan cumplido los requisitos previos, consulte los registros del servidor de Supervisar y de VDA, tal y como se describe en CTX130320.

> Para las sesiones compartidas (varias aplicaciones iniciadas en la misma sesión), se muestran las métricas de inicio de la aplicación Workspace para la conexión más reciente o el inicio más reciente de la aplicación.
> - Algunas métricas del inicio de sesión en VDA no son aplicables en las reconexiones. En tales casos, se muestra un mensaje.




## Fases del inicio de sesión de la aplicación Workspace

### Duración del inicio de sesión en el cliente (SSCD)

Cuando esta métrica es elevada, indica un problema del lado del cliente que está alargando los tiempos de inicio. Revise las métricas siguientes para determinar la raíz probable del problema. SSCD comienza lo más cerca posible del momento de la solicitud (clic del mouse) y finaliza cuando se ha establecido la conexión ICA entre el dispositivo cliente y el VDA. En una sesión compartida, esta duración es mucho menor, ya que no se incurre en gran parte de los costes de instalación asociados a la creación de una nueva conexión con el servidor. En el siguiente nivel, más abajo, hay varias métricas detalladas disponibles.

### Duración de la descarga de archivos ICA (IFDCD)

IFDCD es el tiempo que tarda el cliente en descargar el archivo ICA del servidor. El proceso general es el siguiente:

1. El usuario hace clic en un recurso (aplicación o escritorio) de la aplicación de Workspace.
2. Una solicitud del usuario se envía a StoreFront a través de Citrix Gateway (si está configurado), que envía la solicitud al Delivery Controller.
3. El Delivery Controller busca una máquina disponible para la solicitud y envía la información de la máquina y otros detalles a StoreFront. Además, StoreFront solicita y recibe un tíquet único de Secure Ticket Authority.
4. StoreFront genera un archivo ICA y lo envía al usuario a través de Citrix Gateway (si está configurado).

IFDCD representa el tiempo que tarda todo el proceso (del paso 1 al 4). La duración de IFDCD deja de contar cuando el cliente recibe el archivo ICA.

LPWD es el componente de StoreFront del proceso.

Si el valor de IFDCD es elevado (pero el de LPWD es normal), el procesamiento del lado del servidor del inicio se ha realizado correctamente, pero se han producido problemas de comunicación entre el dispositivo cliente y StoreFront. Esto se debe a problemas de red entre las dos máquinas. Por lo tanto, primero puede solucionar problemas potenciales de red.

#### Duración de la carga de páginas en el servidor web (LPWD)

Este es el tiempo que se tarda en procesar la carga de páginas (launch.aspx) en StoreFront. Si el valor de LPWD es elevado, puede haber un cuello de botella en StoreFront.

He aquí las posibles causas:

- Carga elevada en StoreFront. Intente identificar la causa de la desaceleración; para ello, compruebe los registros de Internet Information Services (IIS) y las herramientas de supervisión, el Administrador de tareas, el Monitor de rendimiento, etc.
- StoreFront tiene problemas para comunicarse con otros componentes, como Delivery Controller. Compruebe si la conexión de red entre StoreFront y Delivery Controller es lenta o hay Delivery Controllers desconectados o sobrecargados.

#### Duración de la resolución de nombres en el servidor web (NRWD)

Este es el tiempo que tarda el Delivery Controller en resolver el nombre de una aplicación o escritorio publicados en la dirección IP de una máquina VDA.

Cuando esta métrica es elevada, indica que el Delivery Controller tarda mucho tiempo en resolver el nombre de una aplicación publicada en una dirección IP. He aquí las posibles causas:

- un problema en el cliente
- problemas con el Delivery Controller, como, por ejemplo, que el Delivery Controller esté sobrecargado, o un problema con el enlace de red que los une

#### Duración de respuestas a tíquets en el servidor web (TRWD)

Esta duración indica el tiempo que se tarda en obtener un tíquet (si es necesario) del servidor Secure Ticket Authority (STA) o de Delivery Controller. Cuando esta duración es elevada, indica que el servidor STA o el Delivery Controller están sobrecargados.

#### Duración de la búsqueda de sesiones en el cliente (SLCD)

Esta duración representa el tiempo que se tarda en enviar una consulta a cada sesión para alojar la aplicación publicada solicitada. La comprobación se realiza en el cliente para determinar si una sesión existente puede gestionar la solicitud de inicio de la aplicación. El método utilizado depende de si la sesión es nueva o compartida.

#### Duración de la creación de sesiones en el cliente (SCCD)

Esta duración representa el tiempo que se tarda en crear una sesión, desde el momento en que se inicia wfica32.exe (o un archivo equivalente similar) hasta el momento en que se establece la conexión.

### Fases de inicio de sesión en VDA

#### Duración del inicio de sesión en el VDA (SSVD)

Esta duración es la métrica de alto nivel relacionada con el inicio de conexiones del lado del servidor que indica el tiempo que tarda VDA en realizar toda la operación de inicio. Cuando esta métrica es elevada, indica que hay un problema en VDA que alarga los tiempos de inicio de sesión. Esto incluye el tiempo dedicado en el VDA a realizar toda la operación de inicio.

#### Duración de la obtención de credenciales en el VDA (COVD)

Tiempo que tarda el VDA en obtener las credenciales de usuario.

Esta duración se puede inflar artificialmente si un usuario no proporciona las credenciales a tiempo y, por lo tanto, no se incluye en la duración de inicio en VDA. Es probable que este tiempo sea importante solo si se está utilizando el inicio de sesión manual y se muestra el cuadro de diálogo de credenciales del lado del servidor (o si se muestra un aviso legal antes de iniciar el inicio de sesión).

#### Duración de la autenticación de credenciales en el VDA (CAVD)

Este es el tiempo que tarda el VDA en autenticar las credenciales del usuario en el proveedor de autenticación, que puede ser Kerberos, Active Directory o una interfaz del proveedor de compatibilidad para seguridad (SSPI).

#### Duración de directivas de grupo en el VDA (GPVD)

Esta duración es el tiempo que se tarda en aplicar objetos de directiva de grupo durante el inicio de sesión.

#### Duración de scripts de inicio de sesión en el VDA (LSVD)

Este es el tiempo que tarda el VDA en ejecutar los scripts de inicio de sesión del usuario.

Puede hacer asíncronos los scripts de inicio de sesión del usuario o grupo. Optimice cualquier script de compatibilidad con aplicaciones o, en su lugar, utilice variables de entorno.

#### Duración de carga de perfil en el VDA (PLVD)

Este es el tiempo que tarda el VDA en cargar el perfil del usuario.

Si esta duración es elevada, revise la configuración de su perfil de usuario. El tamaño y la ubicación del perfil de itinerancia contribuyen a ralentizar el inicio de sesión. Cuando un usuario inicia una sesión en la que los perfiles de itinerancia y las carpetas principales de Terminal Services están habilitados, el contenido del perfil de itinerancia y el acceso a esa carpeta se asignan durante el inicio de sesión, lo que consume recursos adicionales. A veces, esto equivale a una parte importante de la CPU. Para mitigar este problema, utilice las carpetas **principales de Terminal Services** con carpetas personales redirigidas. De manera general, utilice Citrix Profile Management para administrar perfiles de usuario en entornos Citrix. Si utiliza Citrix Profile Management y tiene tiempos de inicio de sesión lentos, compruebe si el software antivirus está bloqueando la herramienta Citrix Profile Management.

#### Duración de la creación de impresoras en el VDA (PCVD)

Este es el tiempo que tarda el VDA en asignar de forma sincrónica las impresoras cliente del usuario. Si se establece la configuración para que la creación de impresoras se realice de forma asíncrona, no se registra ningún valor para PCVD, ya que no afecta a la finalización del inicio de la sesión.

El tiempo excesivo dedicado a la asignación de impresoras suele ser el resultado de la configuración de la directiva de creación automática de impresoras. La cantidad de impresoras agregadas localmente en los dispositivos cliente de los usuarios y la configuración de impresión pueden afectar directamente a los tiempos de inicio de sesión. Cuando se inicia una sesión, Citrix Virtual Apps and Desktops tiene que crear todas las impresoras asignadas localmente en el dispositivo cliente. Vuelva a configurar las directivas de impresión para reducir la cantidad de impresoras que se crean, concretamente cuando los usuarios tienen muchas impresoras locales. Para ello, modifique la directiva de creación automática de impresoras en Delivery Controller y Citrix Virtual Apps and Desktops.

#### Duración de la asignación de unidades en el VDA (DMVD)

Este es el tiempo que tarda el VDA en asignar las unidades, los dispositivos y los puertos cliente del usuario.

Compruebe que las directivas base incluyen configuraciones para inhabilitar los canales virtuales no utilizados, como la asignación de puertos COM o audio, para optimizar el protocolo ICA y mejorar el rendimiento general de la sesión.

#### Duración de inicio de aplicaciones/escritorios en el VDA (ALVD/DLVD)

Esta fase es una combinación de la duración de userinit y de Shell. Cuando un usuario inicia sesión en una máquina con Windows, Winlogon ejecuta userinit.exe. Usernit.exe ejecuta scripts de inicio de sesión, restablece las conexiones de red y, a continuación, inicia explorer.exe, la interfaz de usuario de Windows. Userinit representa la duración entre el inicio de userinit.exe y el inicio de la interfaz de usuario para el escritorio o la aplicación virtuales. La duración de Shell es el tiempo que transcurre entre la inicialización de la interfaz de usuario y el momento en que el usuario recibe el control del teclado y del mouse.

#### Duración de la creación de sesiones en el VDA (SCVD)

Este tiempo incluye varios retrasos en la creación de sesiones en VDA.

## Diagnosticar problemas de inicio de sesión de los usuarios

November 17, 2023

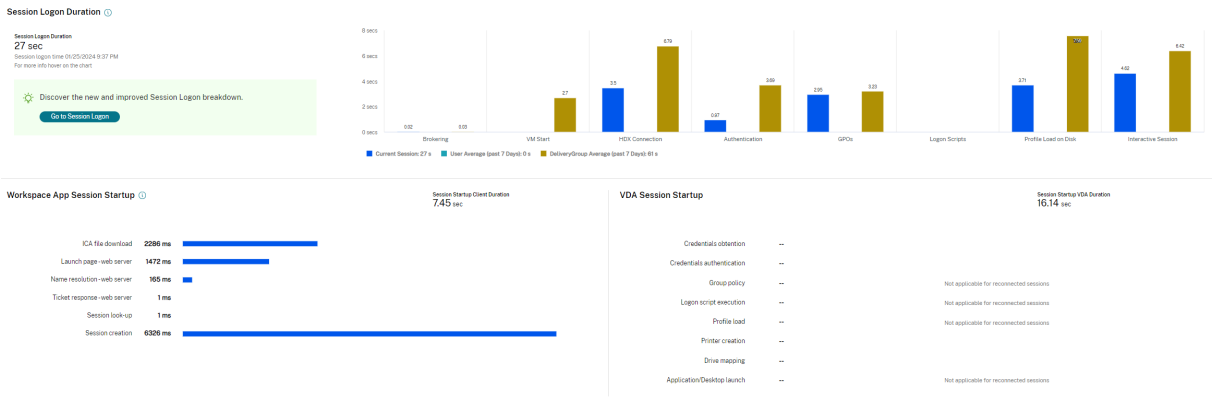
Use los datos de Duración de inicio de sesión para solucionar problemas de inicio de sesión.

La duración del inicio de sesión se mide solo para las conexiones iniciales a un escritorio o aplicación que usa HDX. Esta información no incluye a los usuarios que intentan conectarse con el protocolo de escritorio remoto (RDP) o que se vuelven a conectar desde sesiones desconectadas. Específicamente, la duración del inicio de sesión no se mide cuando un usuario se conecta inicialmente mediante un protocolo que no es HDX y vuelve a conectarse por HDX.

En la vista "Detalles del usuario", la duración se muestra como un valor numérico; debajo se muestra la hora en que se produjo el inicio de sesión y un gráfico de las fases de ese inicio.

A medida que los usuarios inician sesión en Citrix Virtual Apps and Desktops, Monitor Service supervisa las fases del proceso de inicio de sesión desde el momento en que el usuario se conecta desde la aplicación Citrix Workspace al momento en que el escritorio está listo para usarse.




El número elevado de la parte izquierda es el tiempo total de inicio de sesión. Se calcula sumando el tiempo que se tarda en establecer la conexión y en obtener un escritorio desde Delivery Controller al tiempo que se tarda en autenticarse e iniciar sesión en un escritorio virtual. La información de duración se presenta en segundos (o fracciones de segundo).

## Requisitos previos

Deben cumplirse los siguientes requisitos previos para que aparezcan los datos de duración del inicio de sesión y los resultados detallados:

1. Instale **Citrix User Profile Manager** y **Citrix User Profile Manager WMI Plugin** en el VDA.
2. Compruebe que el servicio de Citrix Profile Management se esté ejecutando.
3. Para los sitios de XenApp y XenDesktop 7.15 y versiones anteriores, inhabilite la configuración de GPO llamada **No procesar la lista de ejecución antigua**.
4. La auditoría del seguimiento de procesos debe estar habilitada para obtener el desglose de la sesión interactiva.
5. Para obtener el desglose del GPO, aumente el tamaño de los registros de operaciones de las directivas de grupo.

> **Nota:**
>
> La duración del inicio de sesión solo se admite en el shell predeterminado de Windows (explorer.exe), no en los shells personalizados.

## Pasos para solucionar problemas en el inicio de sesión de los usuarios

1. En la vista **Detalles del usuario**, puede resolver problemas del estado de inicio de sesión desde el panel "Duración de inicio de sesión".
    - Si el usuario está iniciando una sesión, esta vista refleja dicho proceso.

- Si el usuario tiene una sesión ya iniciada, el panel "Duración de inicio de sesión"muestra el tiempo que tardó el inicio de sesión del usuario.

2. Examine las fases del proceso de inicio de sesión.

## Fases del proceso de inicio de sesión

### Intermediación con broker

Cuánto tiempo se tardó en decidir qué escritorio asignar al usuario.

### Inicio de la VM

Si la sesión requería el inicio de una máquina virtual, este es el tiempo que tardó en iniciarse la máquina.

### Conexión HDX

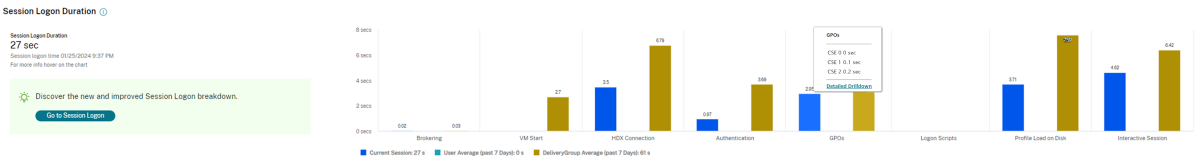
Tiempo que se tardó en completar los pasos requeridos para configurar la conexión HDX desde el cliente a la máquina virtual.

### Autenticación

Tiempo que se tardó en completar la autenticación en la sesión remota.

### Objetos de directiva de grupo (GPO)

Si había configuraciones de directiva de grupo habilitadas en las máquinas virtuales, este es el tiempo que se tardó en aplicar los objetos de directiva de grupo durante el inicio de sesión. El desglose del tiempo necesario para aplicar cada directiva por cada CSE (extensión del lado del cliente) está disponible como texto de ayuda cuando pasa el cursor sobre la barra de GPO.




Haga clic en **Desglose detallado** para ver una tabla con el estado de la directiva y el nombre del GPO correspondiente. Las duraciones del desglose representan solo el tiempo de procesamiento de CSE, no se suman al tiempo total de GPO. Puede copiar la tabla de detalles para resolver problemas o utilizarla en los informes. El tiempo de GPO para las directivas se obtiene de los registros del

Visor de eventos. Los registros se pueden sobrescribir dependiendo de la memoria asignada para los registros de operaciones (el tamaño predeterminado es 4 MB). Para obtener más información sobre cómo aumentar el tamaño del registro para los registros de operaciones, consulte el artículo https://docs.microsoft.com/en-us/previous-versions/tn-archive/dd277416(v=technet.10) de Microsoft TechNet.

### Scripts de inicio de sesión

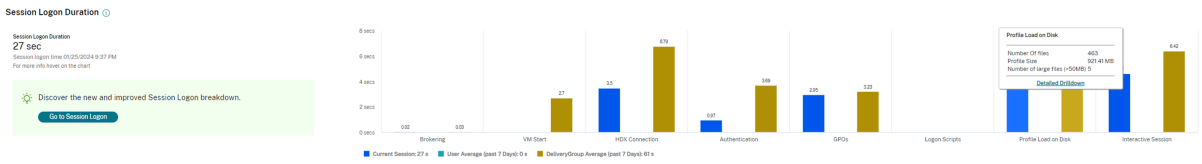
Si había scripts de inicio de sesión configurados para la sesión, este es el tiempo que se tardó en ejecutarlos.

### Carga de perfil

Si había parámetros de perfil configurados para el usuario o para la máquina virtual, este es el tiempo que tardó el perfil en cargarse.

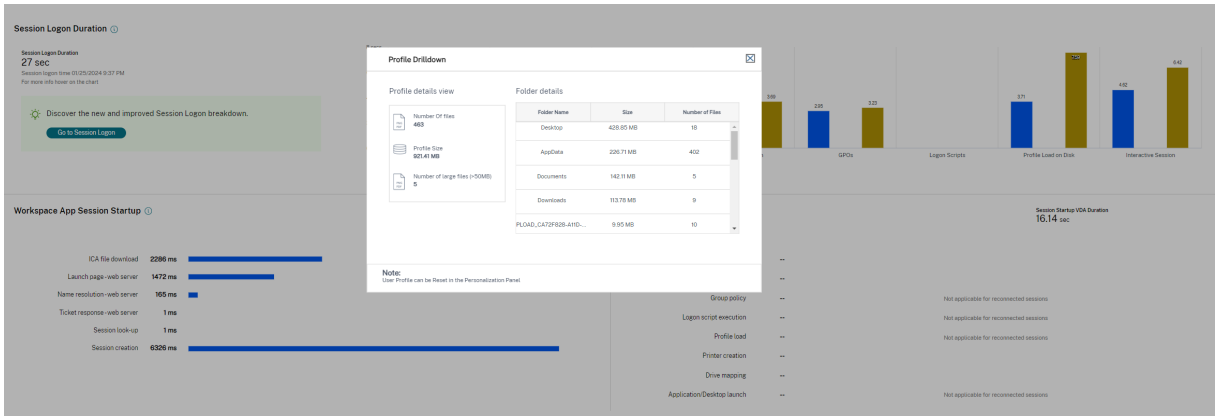
Si Citrix Profile Management está configurado, la barra Carga de perfil indica el tiempo que Citrix Profile Management tarda en procesar perfiles de usuario. Esta información ayuda a los administradores a solucionar problemas con la duración elevada de cargas de perfil. Cuando se configura Profile Management, la barra Carga de perfil muestra una duración mayor. Este aumento se debe a esta mejora y no refleja ninguna degradación del rendimiento. Esta mejora está disponible en VDA 1903 y en versiones posteriores.

Al pasar el cursor sobre la barra Carga de perfil, aparece un texto de ayuda que muestra datos del perfil del usuario de la sesión actual. Esta información adicional puede ayudar a solucionar problemas de cargas largas de perfiles.




Hacer clic en **Desglose detallado** para ver cada carpeta individual que hubiera en la carpeta raíz del perfil (por ejemplo, C:/Usuarios/nombre de usuario), su tamaño y la cantidad de archivos (incluidos los archivos dentro de las carpetas anidadas).




El desglose de perfiles está disponible en VDA 1811 y versiones posteriores. Con la información desglosada del perfil, puede resolver problemas de tiempos de carga largos para los perfiles. Puede hacer lo siguiente:

- Restablecer el perfil de usuario
- Optimizar el perfil eliminando archivos de gran tamaño no deseados
- Reducir la cantidad de archivos para reducir la carga de la red
- Usar streaming de perfiles

De forma predeterminada, se ven los nombres de todas las carpetas. Para ocultar los nombres de las carpetas, modifique los valores de Registro en la máquina VDA siguiendo estos pasos:

> **Advertencia:**
>
> Si se modifica el Registro o se le agregan valores de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no garantiza que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el VDA, agregue el nuevo valor de Registro **ProfileFoldersNameHidden** a HKEY_LOCAL_MACHINE\Softwa
2. Establezca el valor en 1. Este debe ser un valor DWORD (32 bits). La visibilidad de los nombres de las carpetas está ahora inhabilitada.
3. Para volver a ver los nombres de las carpetas, establezca el valor en 0.

> **Nota:**
>
> Puede usar GPO o PowerShell para aplicar el cambio de valor del Registro a varias máquinas. Para obtener más información sobre el uso de GPO para implementar cambios en el Registro, consulte el blog.

### Información adicional

- En el desglose de perfil no se tienen en cuenta las carpetas redirigidas.

- Puede que los usuarios finales no vean los archivos ntuser.dat de la carpeta raíz. Sin embargo, están incluidos en el desglose de perfil y se muestran en la lista de archivos de la **Carpeta raíz**.
- Hay algunos archivos ocultos en la carpeta AppData que no se incluyen en el desglose de perfil.
- El número de archivos y los datos de tamaño de perfil podrían no coincidir con los datos del panel de Personalización, debido a ciertas limitaciones de Windows.

#### Sesión interactiva

Este es el tiempo que se tardó en entregar el control del teclado y del mouse al usuario después de cargar el perfil de usuario. Suele ser la fase más larga de todas las fases de inicio de sesión y se calcula de este modo: **Duración de la sesión interactiva = Marca de hora del evento en el escritorio preparado (EventId 1000 en el VDA) - Marca de hora en el evento de perfil de usuario cargado (EventId 2 en el VDA)**. La fase Sesión interactiva está compuesta de tres subfases: Pre-userinit, Userinit y Shell. Al pasar el mouse sobre la sesión interactiva, se muestra lo siguiente:

- subfases
- tiempo empleado para cada subfase
- tiempo total de demora acumulada entre estas subfases

> **Nota:**
>
> Esta función solamente está disponible en agentes VDA 1811 y versiones posteriores. Si ha iniciado sesiones en sitios cuya versión es anterior a la 7.18 y, a continuación, la ha actualizado a la 7.18, aparecerá el mensaje "El desglose no está disponible debido a un error del servidor". Sin embargo, si ha iniciado alguna sesión después de actualizar la versión, no se muestra ningún mensaje de error.

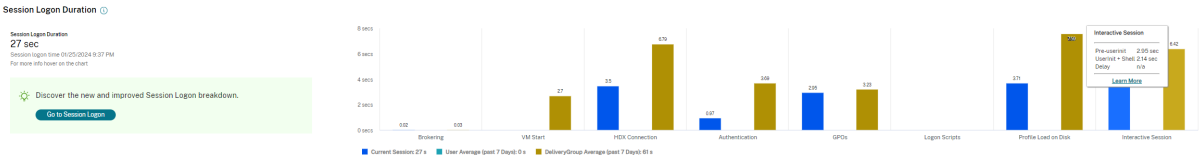
Para ver la duración de cada subfase, habilite la opción "Auditar el seguimiento de procesos"en la VM (VDA). Cuando la opción "Auditar el seguimiento de procesos"está inhabilitada (predeterminado), se muestra la duración de Pre-userinit y la duración combinada de Userinit y Shell. Puede habilitar la opción "Auditar el seguimiento de procesos"a través de un objeto de directiva de grupo (GPO) de la siguiente manera:

1. Cree un GPO y modifíquelo con el editor de GPO.
2. Vaya a **Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Directiva de auditoría**.
3. En el panel de la derecha, haga doble clic en **Auditar el seguimiento de procesos**.
4. Seleccione **Correcto** y haga clic en "Aceptar".
5. Aplique este GPO a los VDA o grupos requeridos.

Para obtener más información sobre la auditoría del seguimiento de procesos y cómo habilitarla o inhabilitarla, consulte https://docs.microsoft.com/en-us/previous-versions/ms813609(v=msdn.10)

en la documentación de Microsoft.




Panel "Duración de inicio de sesión"en la vista "Detalles del usuario".

- **Sesión interactiva: Pre-userinit:** Este es el segmento de Sesión Interactiva que se superpone con los scripts y los objetos de directivas de grupo. Esta subfase se puede reducir optimizando los GPO y los scripts.
- **Sesión interactiva: Userinit:** Cuando un usuario inicia sesión en una máquina con Windows, Winlogon ejecuta userinit.exe. Userinit.exe ejecuta scripts de inicio de sesión, restablece las conexiones de red y luego inicia Explorer.exe, la interfaz de usuario de Windows. Esta subfase de Sesión interactiva representa la duración entre el inicio de Userinit.exe y el inicio de la interfaz de usuario para el escritorio o la aplicación virtual.
- **Sesión interactiva: Shell:** En la fase previa, Userinit comienza a inicializar la interfaz de usuario de Windows. La subfase Shell captura la duración entre la inicialización de la interfaz de usuario y la hora en que el usuario recibe el control del teclado y del mouse.
- **Demora:** Este es el tiempo de demora que se haya acumulado entre las subfases **Pre-userinit y Userinit** y las subfases **Userinit y Shell**.

El tiempo total de inicio de sesión no es exactamente la suma de esas fases. Por ejemplo, algunas fases se dan simultáneamente y, en otras fases, se llevan a cabo otros procesos que pueden llevar a una duración de inicio de sesión más larga que la suma de las fases.
El tiempo total del inicio de sesión no incluye el tiempo de inactividad de ICA; es decir, el tiempo transcurrido entre la descarga del archivo ICA y el inicio del archivo ICA para una aplicación.
Para habilitar la apertura automática del archivo ICA en el inicio de la aplicación, configure el explorador para que abra automáticamente el archivo ICA tras descargarlo. Para obtener más información, consulte CTX804493.

> **Nota:**
>
> El gráfico de Duración de inicio de sesión muestra las fases de inicio de sesión en segundos. Los valores por debajo de un segundo se muestran en valores inferiores al segundo. Los valores por encima de 1 segundo se redondean al medio (0,5) segundo más cercano. El gráfico se ha diseñado para mostrar el valor más alto del eje Y como 200 segundos. Cualquier valor por encima de los 200 segundos se muestra con el valor real mostrado encima de la barra.

### Sugerencias para solucionar problemas

Para identificar valores poco habituales o inesperados en el gráfico, compare el tiempo tomado en cada fase de la sesión actual con los valores promedio para este usuario correspondientes a los últi-

mos siete días, y los valores promedio para todos los usuarios del grupo de entrega, también correspondientes a los últimos siete días.

Si observa algún problema, remita la cuestión a otros administradores según sea necesario. Por ejemplo: si el inicio de la VM es lento, el problema puede estar en el hipervisor. En ese caso, contacte con el administrador del hipervisor. O bien, si la intermediación del broker es lenta, se puede remitir el problema al administrador del sitio para que compruebe el equilibrio de carga en el Delivery Controller.

Examine diferencias inusuales, como:

- Cuando falten barras de inicios de sesión (actuales)
- Discrepancias importantes entre los valores de duración actual y de duración promedio para un usuario. Las causas pueden ser:
  - Se ha instalado una nueva aplicación.
  - Se ha actualizado el sistema operativo.
  - Se realizaron cambios en la configuración.
  - El tamaño del perfil del usuario es muy grande. En este caso el valor de Carga del perfil es alto.
- Discrepancias importantes entre los valores de inicios de sesión del usuario (duración actual y duración promedio) y el valor de duración promedio del grupo de entrega.

Si fuera necesario, haga clic en **Reiniciar** para observar el proceso de inicio de sesión del usuario y, así, solucionar problemas de intermediación con broker o inicio de VM.

## Remedar usuarios

November 17, 2022

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

El remedo se inicia en una ficha nueva, por lo que debe actualizar los parámetros del explorador web para permitir elementos emergentes provenientes de la URL de Citrix Cloud.

Acceda a la función de remedo desde la vista **Detalles de usuario**. Seleccione la sesión del usuario y haga clic en **Remedar** en la vista "Administrador de actividades"o el panel "Detalles de la sesión".

### Remedar agentes Linux VDA

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

> **Nota:**
>
> - 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 VDA para el remedo.

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

### Remedar agentes Windows VDA

Las sesiones de Windows VDA se remedan mediante la Asistencia remota de Windows. Habilite la función Asistencia remota de Windows en la máquina del usuario durante la instalación del VDA. Para obtener más información, consulte Habilitar o inhabilitar funciones.

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

#### Optimizar exploradores Microsoft Internet Explorer para el remedo

Configure Microsoft Internet Explorer para que abra automáticamente el archivo descargado de Asistencia remota de Microsoft (.msra) con el cliente de Asistencia remota.

Para ello, debe habilitar la configuración Pedir intervención del usuario automática para descargas de archivo en el Editor de directivas de grupo:

Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página Seguridad > Zona Internet > Pedir intervención del usuario automática para descargas de archivo.

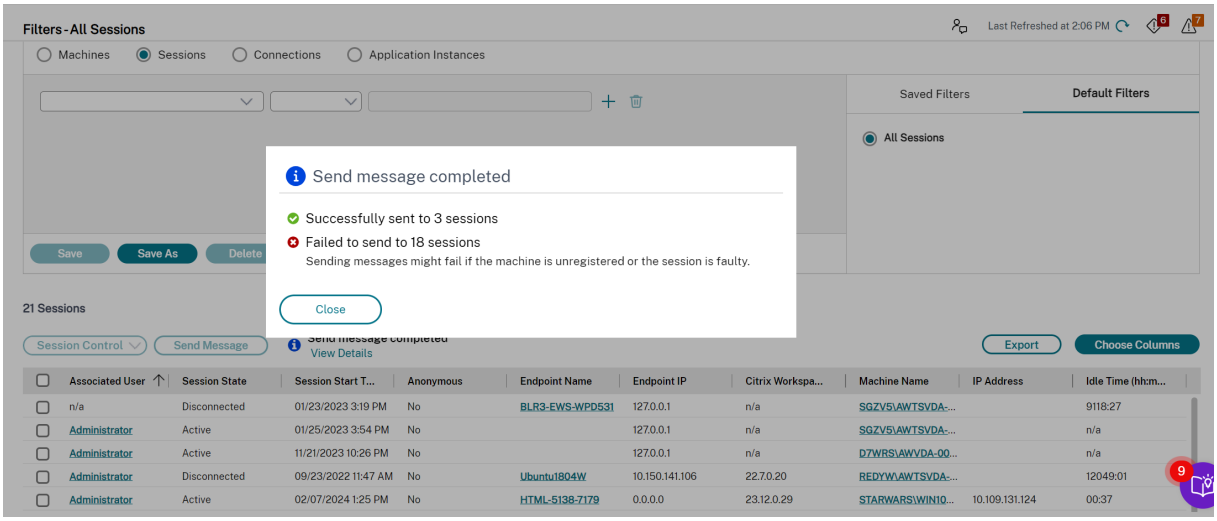
## Enviar mensajes a usuarios

January 24, 2024

Desde Supervisar, puede enviar un mensaje a un usuario que está conectado a una o varias máquinas. Por ejemplo, puede usar esta función para enviar notificaciones inmediatas acerca de acciones administrativas, tales como unas operaciones de mantenimiento de escritorios que están a punto de tener lugar, cierres de sesión y reinicios de máquinas y restablecimientos de perfiles.

Para enviar un mensaje a un usuario, siga estos pasos:

1. Vaya a **Supervisar** > **Filtros** > **Máquinas** > **Todas las máquinas**.
2. Seleccione una máquina a la que desee enviar un mensaje y haga clic en **Enviar mensaje**.
3. Escriba el mensaje y haga clic en **Enviar**.




El envío de mensajes puede fallar si las máquinas no están registradas o si las sesiones presentan fallos.

Si el mensaje se envió correctamente, aparece un mensaje de confirmación. Si la máquina del usuario está conectada, aparece el mensaje allí.

Si el mensaje no se envió correctamente, aparece un mensaje de error. Solucione el problema de acuerdo con el mensaje de error. Cuando haya terminado, escriba de nuevo el asunto y el texto del mensaje, y haga clic en la opción **Reintentar**.

Si elige enviar mensajes en bloque a todas las sesiones conectadas, el progreso de la operación se muestra en porcentaje. Una vez finalizada la operación, se muestran la cantidad de mensajes que se enviaron correctamente y la cantidad de mensajes en que falló el envío. El estado del envío del mensaje es especialmente útil cuando se administran sitios de gran tamaño. Ayuda a entender si es necesario reenviar el mensaje a ciertos usuarios.

## Resolver fallos de aplicación

February 9, 2023

En la vista **Administrador de actividades**, haga clic en la ficha **Aplicaciones**. Puede ver todas las aplicaciones de todas las máquinas a las que el usuario tiene acceso, incluidas las aplicaciones locales y las alojadas para la máquina conectada actualmente, y el estado de cada una de ellas.

La lista incluye solo las aplicaciones que se han iniciado en la sesión.

Para máquinas con sistema operativo de sesión única o multisesión, se muestran las aplicaciones para cada sesión desconectada. Si el usuario no está conectado, no se muestra ninguna aplicación.

| Acción | Descripción |
| --- | --- |
| Finalizar una aplicación que dejó de responder | Elija la aplicación que no responde, y haga clic en **Finalizar aplicación**. Una vez que la aplicación haya finalizado, solicite al usuario que la abra de nuevo. |
| Finalizar procesos que dejaron de responder | Si dispone de los permisos necesarios, haga clic en la ficha **Procesos**. Seleccione un proceso que está relacionado con la aplicación o el que está utilizando una gran cantidad de recursos de la CPU o la memoria y haga clic en **Finalizar proceso**. No obstante, si no dispone de los permisos necesarios para finalizar el proceso, los intentos de finalizarlo fallan. |

| Acción | Descripción |
| --- | --- |
| Reiniciar la máquina del usuario | Si se trata solo de máquinas con sistema operativo de sesión única, para la sesión seleccionada, haga clic en **Reiniciar**. Como alternativa, en la vista "Detalles de la máquina", use los controles de energía para reiniciar o apagar la máquina. Pida al usuario que vuelva a iniciar la sesión para poder comprobar de nuevo la aplicación. Si se trata de máquinas con sistema operativo multisesión, la opción de reinicio no está disponible. En su lugar, cierre la sesión del usuario y permita que el usuario inicie sesión de nuevo. |
| Colocar la máquina en modo de mantenimiento | Si la imagen de la máquina necesita mantenimiento (por ejemplo, instalar una revisión o actualización de software), colóquela en modo de mantenimiento. Desde la vista Detalles de la máquina, haga clic en **Detalles** y active el modo de mantenimiento. Remita la cuestión al administrador que corresponda. |

### Inhabilitar la visibilidad de aplicaciones en ejecución

De forma predeterminada, el Administrador de actividades muestra una lista de todas las aplicaciones que haya en ejecución en la sesión del usuario. Esta información pueden verla todos los administradores que tengan acceso a la función del Administrador de actividades. Para los roles de administrador delegado, esto incluye los roles de administrador total, administrador de grupos de entrega y administrador de asistencia técnica.

Para proteger la privacidad de los usuarios y las aplicaciones que estos ejecutan, puede configurar que la ficha Aplicaciones no muestre las aplicaciones en ejecución. Para ello, en el VDA, modifique la clave de Registro en HKEY_LOCAL_MACHINE\Software\Citrix\Director\TaskManagerDataDisplayed. De forma predeterminada, el valor de la clave es 1. Cambie el valor a 0 para que la información no se recopile del VDA y, por tanto, no se muestre en el Administrador de actividades.

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

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

## Restaurar conexiones de escritorio

March 30, 2022

Desde Supervisar, compruebe el estado de conexión del usuario a la máquina actual en la barra de título del usuario.

Si ha fallado la conexión de escritorio, se mostrará el error que hizo que fallara la conexión, lo que puede ayudarle a solucionar el problema.

| Acción | Descripción |
| --- | --- |
| Comprobar que la máquina no está en modo de mantenimiento | En la página Detalles del usuario, asegúrese de que el modo de mantenimiento está desactivado. |
| Reiniciar la máquina del usuario | Seleccione la máquina y haga clic en **Reiniciar**. Utilice esta opción si la máquina del usuario no responde o no puede conectarse a ella porque, por ejemplo, está utilizando una cantidad inusualmente alta de recursos de la CPU, lo que puede inutilizar la CPU. |

## Restaurar sesiones

March 30, 2022

Si una sesión se desconecta, la sesión permanece activa y sus aplicaciones siguen ejecutándose, pero el dispositivo de usuario ya no se comunica con el servidor.

En la vista Detalles del usuario, se pueden solucionar fallos de sesión en el panel **Detalles de la sesión**. Puede ver los detalles de la sesión actual, indicada por el ID de sesión.

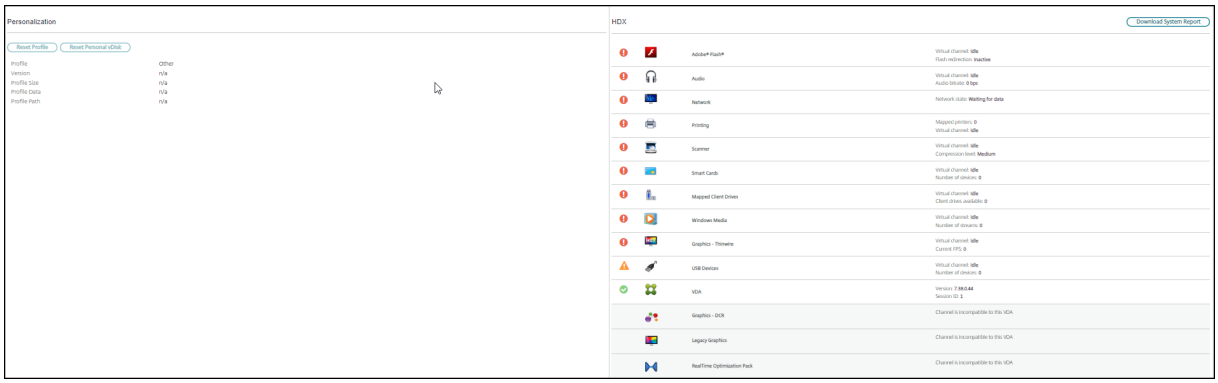
| Acción | Descripción |
| --- | --- |
| Finalizar aplicaciones o procesos que dejaron de responder | Haga clic en la ficha **Aplicaciones**. Elija la aplicación que no responde y haga clic en **Finalizar aplicación**. Del mismo modo, seleccione los procesos correspondientes que no respondan y haga clic en **Finalizar proceso**. Además de eso, finalice los procesos que estén consumiendo una cantidad inusualmente alta de memoria o de recursos de la CPU, lo que puede inutilizar la CPU. |
| Desconectar la sesión de Windows | Haga clic en **Control de sesión** y seleccione **Desconectar**. Esta opción solo está disponible para las máquinas con sistema operativo multisesión intermediario. En caso de sesiones sin intermediarios, la opción está inhabilitada. |
| Cerrar la sesión de un usuario | Haga clic en **Control de sesión** y seleccione **Cerrar sesión**. |

Para probar la sesión, el usuario puede intentar volver a iniciar la sesión. También puede remedar al usuario para supervisar más de cerca esta sesión.

## Generar informes del sistema de canales HDX

November 17, 2023

En la vista **Detalles del usuario**, se puede comprobar el estado de los canales HDX en la máquina del usuario en el panel HDX. Este panel solo está disponible si la máquina del usuario está conectada mediante HDX.



Si aparece un mensaje que indica que la información no está disponible actualmente, espere un minuto para que se actualice la página o haga clic en el botón **Actualizar**. Los datos de HDX tardan un poco más que otros datos en actualizarse.

Haga clic en el icono de advertencia o error para obtener más información.

> Sugerencia:
>
> Puede ver información acerca de otros canales en el mismo cuadro de diálogo. Para ello, haga clic en las flechas izquierda y derecha situadas en la esquina izquierda de la barra de título.

Citrix Support es quien suele utilizar los informes del sistema de canales HDX para solucionar problemas más complejos. Para hacer esto, en el panel HDX, haga clic en **Descargar informe del sistema**.

## Restablecer un perfil de usuario

April 14, 2022

> **Precaución:**
>
> Cuando se restablece un perfil, aunque las carpetas y los archivos del usuario se guarden y se copian al nuevo perfil, la mayor parte de los datos del perfil se eliminan (por ejemplo, el Registro se restablece y los parámetros de aplicaciones podrían eliminarse).

1. Desde Supervisar, busque al usuario cuyo perfil quiere restablecer y seleccione la sesión de ese usuario.
2. Haga clic en **Restablecer perfil**.
3. Indique al usuario que cierre todas las sesiones.
4. Indique al usuario que vuelva a iniciar sesión. Las carpetas y archivos del perfil de usuario que se guardaron se copian en el nuevo perfil.

   > **Importante:**
   >
   > Si el usuario tiene perfiles en varias plataformas (por ejemplo, en Windows 8 y en Windows 7), indíquele que inicie sesión primero en el mismo escritorio o aplicación que notificó como un problema. Esto garantiza el restablecimiento del perfil adecuado. Para un perfil de usuario de Citrix, se habrá restablecido cuando aparezca el escritorio del usuario. Para un perfil móvil de Microsoft, es posible que la restauración de carpetas aún esté en curso durante unos momentos. El usuario puede permanecer conectado hasta que se complete la restauración.

En los pasos anteriores, se presupone que está utilizando Citrix Virtual Desktops (VDA de escritorio). Si está utilizando Citrix Virtual Desktops (VDA de servidor) necesitará tener una sesión iniciada para realizar el restablecimiento del perfil. El usuario tiene que cerrar la sesión y volver a iniciarla para completar el restablecimiento del perfil.

Si el perfil no se restablece correctamente (por ejemplo, el usuario no puede volver a iniciar la sesión en la máquina o faltan algunos archivos), debe restaurar manualmente el perfil original.

Las carpetas (y sus archivos) del perfil del usuario se guardan y se copian en el nuevo perfil. Se copian por este orden:

- Escritorio
- Cookies
- Favoritos
- Documentos
- Imágenes
- Música
- Vídeos

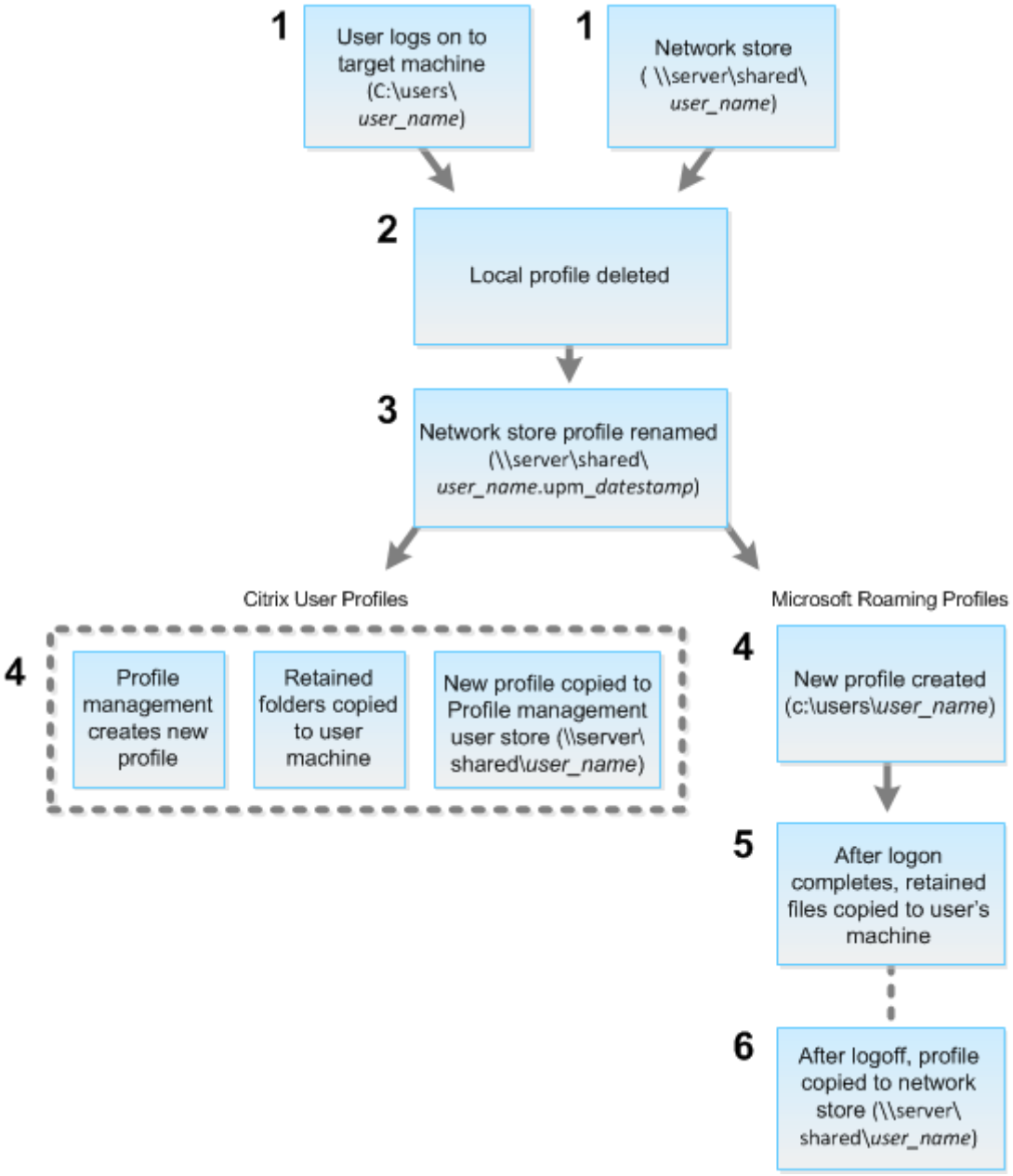
> **Nota:**
>
> En Windows 8 y versiones posteriores, las cookies no se copian cuando los perfiles se restablecen.

### Cómo se procesan los perfiles restablecidos

Es posible restablecer cualquier perfil de usuario de Citrix o perfil itinerante de Microsoft. Después de que el usuario cierra la sesión y se selecciona el comando para restablecer (ya sea en Supervisar o en el SDK de PowerShell), Supervisar primero identifica el perfil de usuario en uso y emite un comando de restablecimiento apropiado. Supervisar recibe la información a través de Profile Management, incluida la información sobre el tamaño del perfil, el tipo de perfil y los tiempos de inicio de sesión.

Este diagrama ilustra el proceso que tiene lugar después de que el usuario inicie sesión tras restablecerse el perfil.




El comando de restablecimiento emitido por Supervisar especifica el tipo de perfil. Después, el servicio de Profile Management intenta restablecer un perfil de ese tipo y busca el recurso compartido de red (el almacén de usuarios). Si Profile Management procesa el usuario, pero recibe un comando de perfil móvil (itinerante), se rechaza (o viceversa).

1. Si hay un perfil local está presente, se elimina.
2. El perfil de red se cambia de nombre.
3. La siguiente acción depende de si el perfil que se restablece es un perfil de usuario de Citrix o un perfil itinerante de Microsoft.

Para los perfiles de usuario de Citrix, el nuevo perfil se crea mediante las reglas de importación de Profile Management, y las carpetas se copian de vuelta en el perfil de red, y el usuario puede iniciar una sesión como lo hace normalmente. Si se usa un perfil itinerante para el restablecimiento, los parámetros de Registro en el perfil itinerante se conservan en el perfil restablecido. Si es necesario, puede configurar Profile Management para que un perfil de plantilla sobrescriba el perfil itinerante.

Para los perfiles móviles de Microsoft, Windows crea un perfil y, cuando el usuario inicia sesión, las carpetas se copian de nuevo en el dispositivo del usuario. Cuando el usuario cierra la sesión de nuevo, el nuevo perfil se copia en el almacén de la red.

### Para restablecer un perfil manualmente después de un error de restablecimiento

1. Indique al usuario que cierre todas las sesiones.
2. Elimine el perfil local si existe.
3. Busque la carpeta archivada en el recurso compartido de red que contiene la fecha y hora junto con el nombre de la carpeta, la carpeta con la extensión .upm_fechayhora.
4. Elimine el nombre del perfil actual. Es decir, el que no tiene la extensión upm_datestamp.
5. Cambie el nombre de la carpeta archivada mediante el nombre del perfil original; es decir, elimine la extensión de fecha y hora. Con ello, habrá devuelto el perfil a su estado original, prerrestablecido.

## Grabar sesiones

February 21, 2024

En Supervisar puede grabar sesiones ICA mediante los controles de la función Grabación de sesiones, desde las pantallas **Detalles del usuario** y **Detalles de la máquina**. Esta función está disponible para los clientes de los sitios con licencia **Premium**.

### Grabación dinámica de sesiones

Puede grabar la sesión activa actual mediante los controles de grabación de sesiones de la pantalla **Detalles del usuario**. Para obtener más información sobre la grabación dinámica de sesiones, consulte el artículo Servicio de grabación de sesiones.

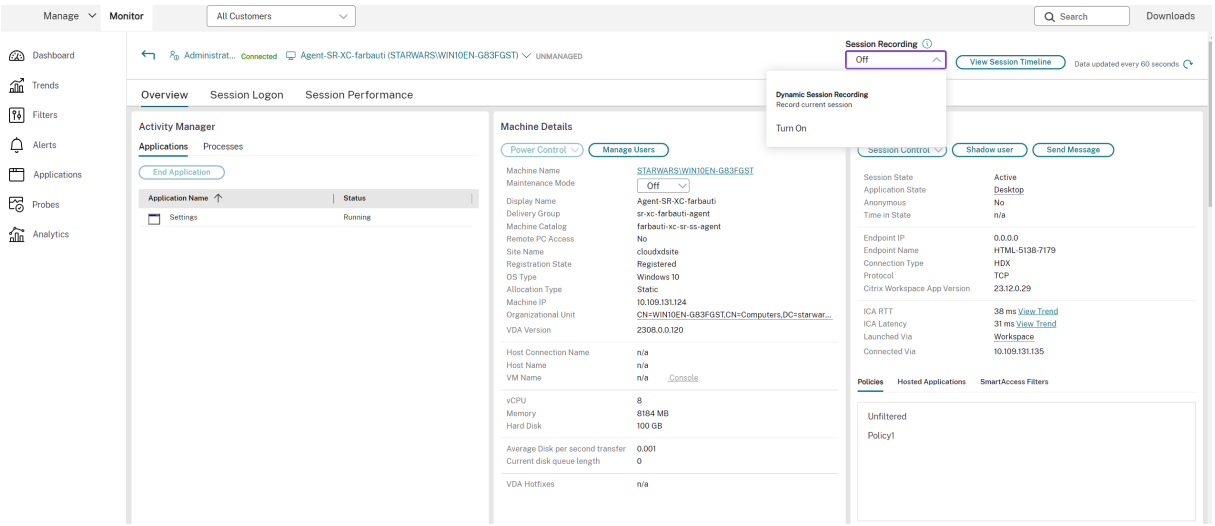
 

### Controles de grabación de sesiones en Supervisar

Puede usar las acciones **Detalles del usuario** > **Grabación de sesiones** para grabar las sesiones actuales o posteriores.

- Habilite la grabación dinámica de sesiones: se graba la sesión actual.
- Desactivar: Inhabilitar la grabación de las sesiones del usuario.

El nombre de la directiva activa de Grabación de sesiones aparece en el panel **Directivas**.




El panel **Detalles de la máquina** muestra el estado de la directiva Grabación de sesiones de la máquina.

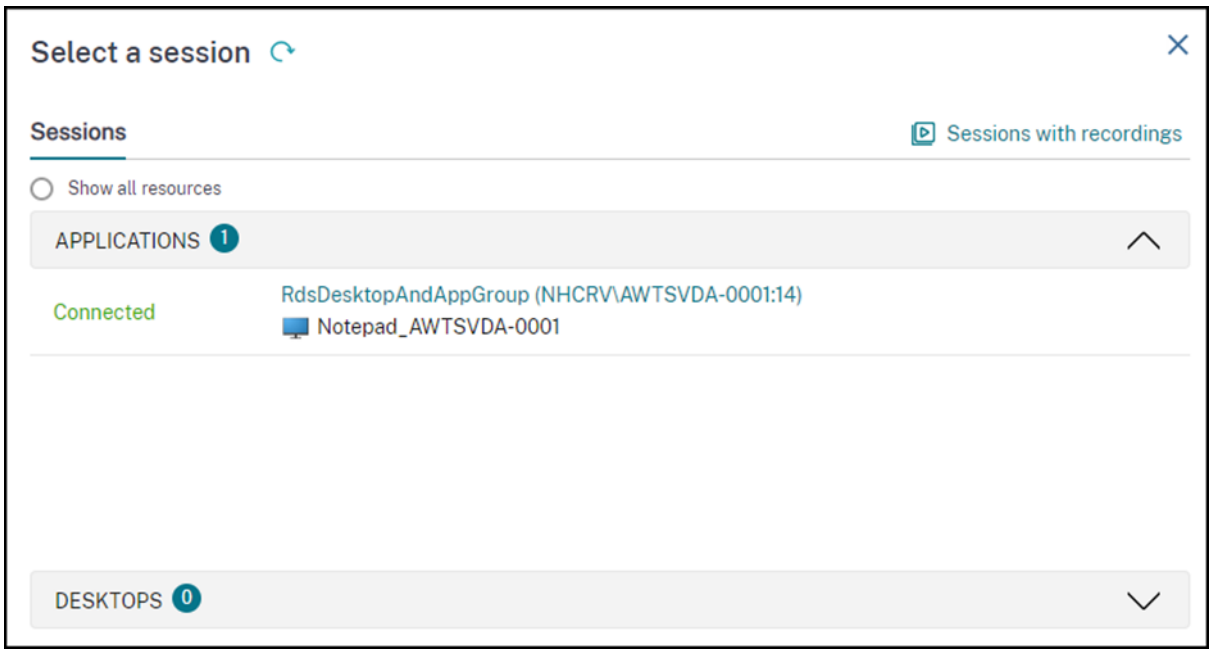
#### Reproducir sesiones grabadas y en directo

Puede reproducir sesiones de usuario grabadas y en directo para entender los problemas a los que se enfrenta el usuario. El fácil acceso a las grabaciones y a las métricas relacionadas con las sesiones en la consola Supervisar elimina la necesidad de buscar grabaciones en varios servidores de grabación de sesiones o buscar aplicaciones de terceros para ver las grabaciones. Ayuda a correlacionar los problemas descubiertos en las grabaciones con las métricas de rendimiento.

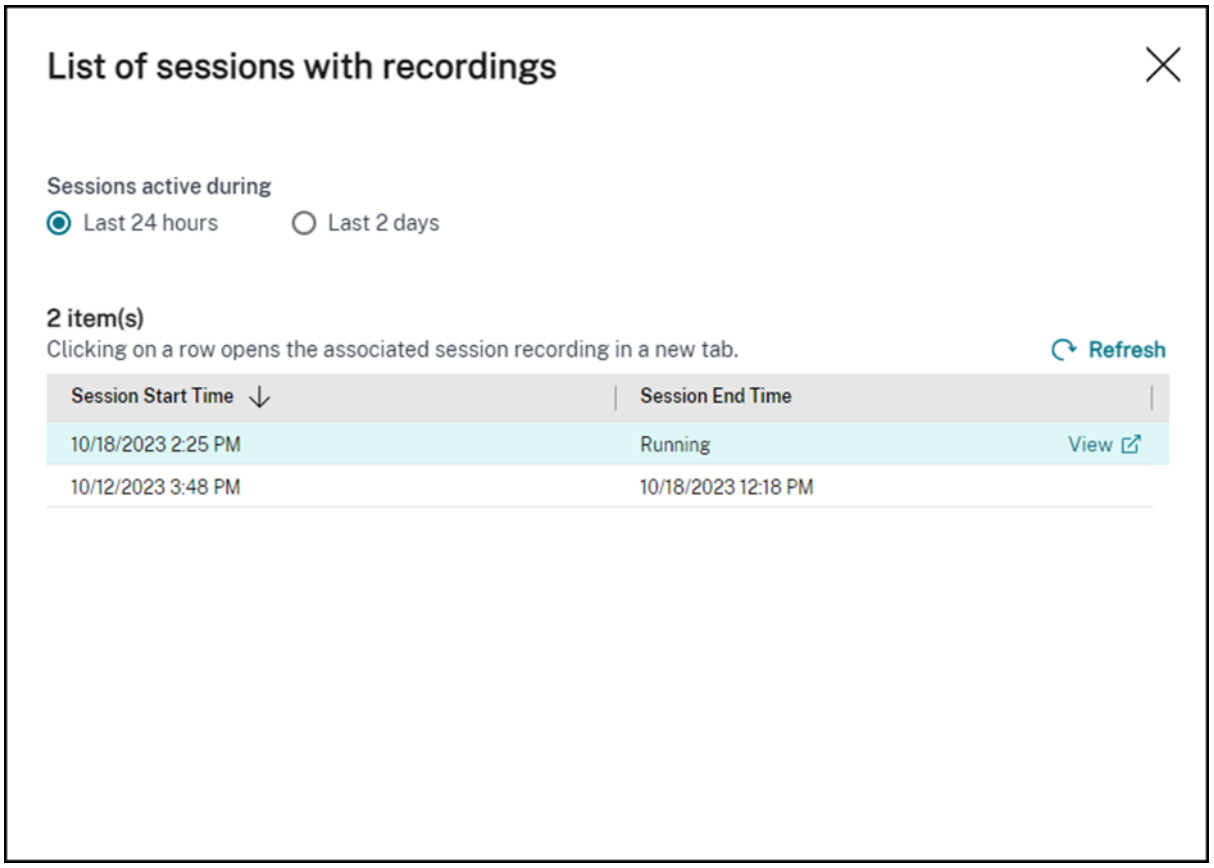
Esta función requiere un VDA y los servidores de grabación de sesiones de la versión 2308 o posteriores.

Supervisar almacena las grabaciones de las sesiones en un repositorio centralizado. La lista de grabaciones que pertenecen al usuario se muestra al hacer clic en el enlace modal **Selector de sesiones** > **Sesiones con grabaciones**.




Puede elegir ver las grabaciones de las sesiones que estuvieron activas durante las últimas 24 horas o los últimos 2 días. Las grabaciones en directo de las sesiones actualmente activas se marcan con la **hora de finalización de la sesión** como **En curso**.




Haga clic en el enlace **Ver** para reproducir la grabación en una ficha nueva mediante el servidor de

reproducción de grabación de sesiones de Citrix.

## Tabla de compatibilidad de funciones

June 12, 2024

Citrix Monitor admite tres ediciones de Citrix DaaS (antes, Citrix Virtual Apps and Desktops Service). Estas son **Premium**, **Citrix DaaS Advanced** y **Citrix DaaS Advanced Plus**. Las funciones específicas de Citrix Monitor, las versiones de VDA, los componentes dependientes y sus respectivas ediciones de licencia se indican en la tabla siguiente.

| Función | Dependencias: Versión mínima requerida | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Utilización de GPU en tiempo real disponible para las GPU de AMD | VDA 7 2212 con Windows de 64 bits | Sí | Sí | Sí |
| Acceder a Citrix Analytics for Performance: Detalles de la sesión | Derecho de uso de Citrix Analytics for Performance | Sí | Sí | Sí |
| Reconexión automática de sesión | VDA 1906 | Sí | Sí | Sí |
| Duración de inicio de sesión | VDA 1903 | Sí | Sí | Sí |
| Sondeo de escritorios | Citrix Probe Agent 1903 | Sí | No | No |
| Duración de Citrix Profile Management en la carga de perfil | VDA 1903 | Sí | Sí | Sí |
| Desglose de perfil | VDA 1811 | Sí | Sí | Sí |

| Función | Dependencias: Versión mínima requerida | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Supervisar alertas de hipervisor | Ninguno | Sí | No | No |
| Sondeo de aplicaciones | Citrix Application Probe Agent 1811 | Sí | No | No |
| Estado de licencias RDS de Microsoft | VDA 7.16 | Sí | Sí | Sí |
| Acceder a la consola de la máquina desde Supervisar | XenServer Hypervisor 7.3 | Sí | Sí | Sí |
| Exportación de datos de filtros | Ninguno | Sí | Sí | Sí |
| Desglose de la sesión interactiva | VDA 1808 | Sí | Sí | Sí |
| Desglose de GPO | VDA 1808 | Sí | Sí | Sí |
| Datos históricos disponibles de la máquina mediante la API de OData | Ninguno | Sí | Sí | Sí |
| Directivas de alertas inteligentes | Ninguno | Sí | No | No |
| Enlace de Health Assistant | Ninguno | Sí | Sí | Sí |
| Desglose de la sesión interactiva | Ninguno | Sí | Sí | Sí |
| Análisis de aplicaciones | VDA 7.15 | Sí | Sí | Sí |
| API de OData 4 | Ninguno | Sí | Sí | Sí |

| Función | Dependencias: Versión mínima requerida | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Remedo de usuarios en Linux VDA | VDA 7.16 | Sí | Sí | Sí |
| Acceso a la consola de la máquina | Ninguno | Sí | Sí | Sí |
| Supervisión de fallos de aplicación | VDA 7.15 | Sí | Sí | Sí |
| Solución de problemas de aplicación | VDA 7.13 | Sí | Sí | Sí |
| Supervisar discos | VDA 7.14 | Sí | Sí | Sí |
| Supervisar GPU | VDA 7.14 | Sí | Sí | Sí |
| Protocolo de transporte en el panel “Detalles de la sesión” | VDA 7.13 | Sí | Sí | Sí |
| Descripciones claras de los errores de conexión y de máquina | VDA 7.x | Sí | Sí | Sí |
| Retención de datos históricos | VDA 7.x | Sí | No | No |
| Informes personalizados | VDA 7.x | Sí | No | No |
| Informes de utilización de recursos | VDA 7.11 | Sí | Sí | Sí |

| Función | Dependencias: Versión mínima requerida | Premium | Citrix DaaS Advanced | Citrix DaaS Advanced Plus |
|---|---|---|---|---|
| Alertas extendidas para condiciones de CPU, memoria y RTT de ICA | VDA 7.11 | Sí | No | No |
| Mejoras en la exportación de informes | VDA 7.x | Sí | Sí | Sí |
| Desglose de la duración del inicio de sesión | VDA 7.x | Sí | Sí | Sí |
| Supervisión y alertas mejoradas | VDA 7.x | Sí | No | No |
| Uso de aplicaciones alojadas | VDA 7.x | Sí | No | No |
| Uso de SO de sesión única y SO multisesión | VDA 7.x | Sí | No | No |
| Compatibilidad con canal virtual Framehawk | VDA 7.6 | Sí | Sí | Sí |

## Administración delegada y supervisión

March 30, 2022

La administración delegada utiliza tres conceptos: los administradores, los roles y los ámbitos. Los permisos se basan en un rol de administrador y en el ámbito de este rol. Por ejemplo, a un administrador se le puede asignar un rol de administrador de asistencia técnica en el que el ámbito implica la responsabilidad de usuarios finales en un único sitio.

Los permisos administrativos determinan la interfaz de supervisión que ven los administradores y las tareas que estos pueden realizar. Los permisos determinan:

- Las vistas a las que los administradores pueden acceder, denominadas conjuntamente como una vista.
- Los escritorios, las máquinas y las sesiones que el administrador puede ver y con las que puede interactuar.
- Los comandos que el administrador puede ejecutar, como el remedo de la sesión de un usuario o habilitar el modo de mantenimiento.

Ahora en la supervisión se admiten roles de administrador delegado que permiten asignar roles personalizados o integrados a los administradores. El rol determina los permisos disponibles y, por lo tanto, determina cómo utiliza un administrador la supervisión. También puede definir el ámbito aplicable a esos roles. El ámbito define los objetos para los que se aplica el rol.

Para obtener información sobre cómo crear administradores delegados, consulte el artículo principal de Administración delegada.

Los roles y permisos integrados determinan cómo los administradores usan **Supervisar**:

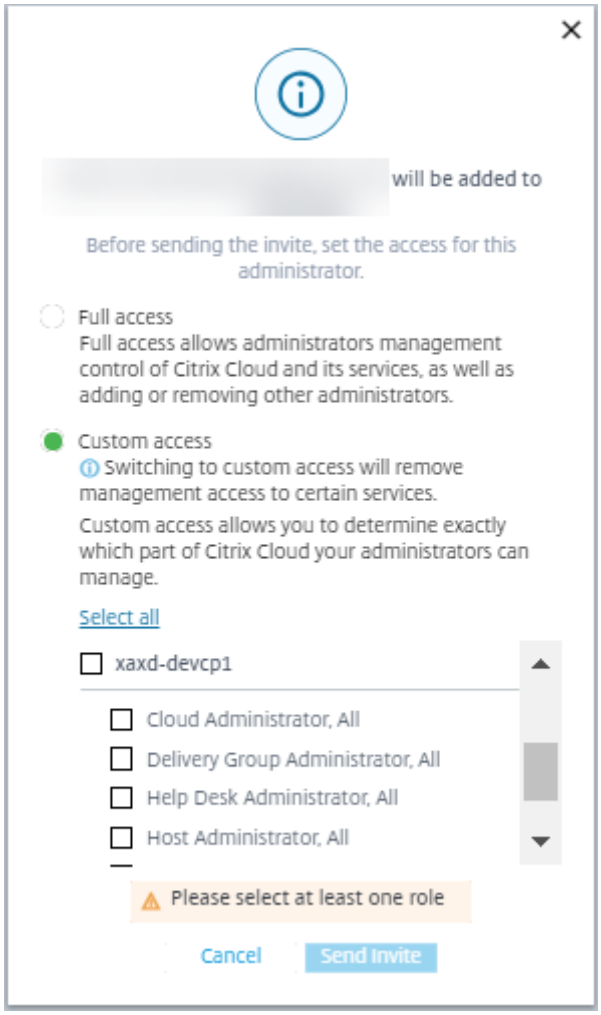
| Rol de administrador | Permisos en Supervisar |
|---|---|
| Administrador total | Cuenta con acceso completo a todas las vistas y puede ejecutar todos los comandos, incluidos remedar la sesión de un usuario, habilitar el modo de mantenimiento y exportar los datos de tendencias. |
| Administrador de grupos de entrega | Cuenta con acceso completo a todas las vistas y puede ejecutar todos los comandos, incluidos remedar la sesión de un usuario, habilitar el modo de mantenimiento y exportar los datos de tendencias. |
| Administrador de solo lectura | Puede acceder a todas las vistas y ver todos los objetos en los ámbitos especificados, además de información global. Puede descargar informes de canales HDX y puede exportar datos de tendencias mediante la opción de exportación en la vista Tendencias. No puede ejecutar ningún otro comando ni cambiar nada en las vistas. |

| Rol de administrador | Permisos en Supervisar |
| --- | --- |
| Administrador de asistencia técnica | Puede acceder únicamente a las vistas del Servicio de asistencia y de los Detalles del usuario y solo puede ver los objetos que le han sido delegados para que los administre. Puede remedar la sesión de un usuario y ejecutar comandos para ese usuario. Puede realizar operaciones en modo de mantenimiento. Puede utilizar las opciones de control de energía para las máquinas con sistema operativo de sesión única. No puede acceder a las vistas de Panel de mandos, Tendencias, Alertas ni Filtros. No puede utilizar las opciones de control de energía para las máquinas con sistema operativo multisesión. |
| Administrador de catálogos de máquinas | Solo puede acceder a la página "Detalles de la máquina"(búsqueda por máquinas). |
| Administrador de host | Sin acceso. Este administrador no es compatible en Supervisar y no puede ver datos. |
| Administrador de Probe Agent | Acceso de solo lectura a la página Aplicaciones, no puede acceder a ninguna otra vista. Diseñado para ejecutar Citrix Probe Agent en máquinas de punto final. |
| Administrador total de supervisión | Tiene pleno acceso a todas las vistas y comandos de la ficha **Supervisar**. |
| Administrador de sesiones | Puede ver los grupos de entrega y administrar sus sesiones y máquinas asociadas en la página **Filtros** de la ficha **Supervisar**. |

Para asignar un rol integrado o personalizado a un usuario, desde el menú Citrix Cloud vaya a **Administración de acceso e identidad** > **Administradores**. Una vez aquí, al agregar o modificar el acceso de un administrador, puede seleccionar **Acceso personalizado** y uno de los roles que se enumeran.

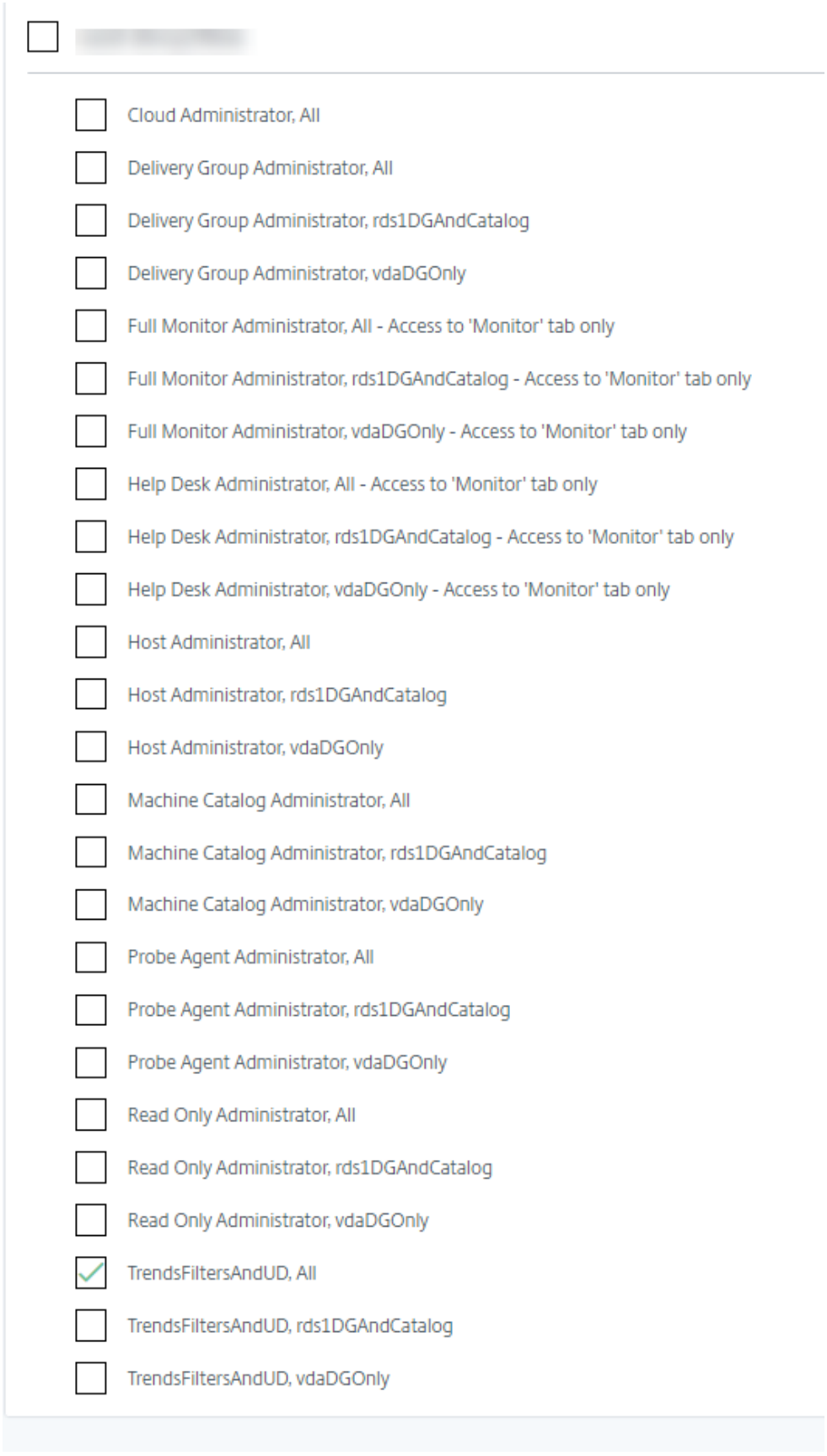
 




Puede definir roles y ámbitos personalizados en **Configuración completa > Administradores > Administradores**.

Los roles integrados y los roles personalizados se enumeran para su selección con un ámbito personalizado.



# Granularidad y retención de datos

January 17, 2023

## Agregar valores de datos

Monitor Service recopila diferentes datos, incluidos el uso de las sesiones de usuario, la información del rendimiento de los inicios de sesión de usuario, la información del equilibrio de carga de las sesiones y la información de fallos de conexión y de las máquinas. Los datos se agregan de forma diferente en función de la categoría. Para interpretar los datos, es fundamental comprender la agregación de los valores de los datos presentados mediante las API de Método de OData. Por ejemplo:

- Los errores de máquinas y sesiones conectadas se producen durante un período. Por lo tanto, se exponen como máximos a lo largo de un período de tiempo.
- La duración del inicio de sesión es una medida de tiempo, por lo que se expone como el promedio en las métricas tomadas a lo largo de un período de tiempo.
- Los recuentos de inicio de sesión y los fallos de conexión son el número de casos a lo largo de un período, por lo que se exponen como sumas para un período de tiempo.

## Evaluar datos simultáneos

Las sesiones deben superponerse para considerarse simultáneas. Sin embargo, cuando el intervalo temporal es de 1 minuto, todas las sesiones de ese minuto (tanto si se superponen como si no) se consideran simultáneas. El tamaño del intervalo es tan pequeño que la sobrecarga de rendimiento que implica el cálculo con precisión no compensa el valor agregado. Si las sesiones se producen en la misma hora, pero no en el mismo minuto, no se consideran superpuestas.

## Correlacionar tablas de resumen con datos sin procesar

El modelo de datos representa las métricas de dos maneras diferentes:

- Las tablas de resumen representan vistas agregadas de las métricas por minuto, por hora y por día.
- Los datos sin procesar representan eventos individuales o de estado actual de seguimiento de una sesión, conexión, aplicación y otros objetos.

Al intentar establecer una correlación entre las llamadas de la API o en el modelo de datos mismo, es importante comprender los conceptos y las limitaciones siguientes:

- **No hay datos de resumen para intervalos parciales.** Los resúmenes de métricas están diseñados para satisfacer las necesidades de tendencias históricas en períodos prolongados. Estas métricas se agregan en la tabla de resumen para intervalos completos. No hay datos de resumen para un intervalo parcial al comienzo (en los datos más antiguos) de la recopilación de datos ni al final de esta. Cuando se consultan los datos agregados de un día (Intervalo=1440), esto significa que los días incompletos al principio y los más recientes no tienen datos. Aunque podrían existir datos sin formato para esos intervalos parciales, estos datos no se resumirán. Para determinar el intervalo combinado más antiguo y reciente para una granularidad de datos en particular, utilice la fecha de resumen (SummaryDate) máxima y mínima de una tabla de resumen. La columna SummaryDate representa el inicio del intervalo. El valor de la columna Granularity representa la duración del intervalo para los datos agregados.
- **Correlación por tiempo.** Las métricas se agregan en la tabla de resumen para intervalos completos, como se describe en la sección anterior. Se pueden usar para descubrir tendencias históricas, pero los eventos sin procesar podrían ser más actualizados en los datos de estado que lo que se resumió para el análisis de tendencias. En cualquier comparación basada en el tiempo entre datos de resumen y datos sin procesar, se debe tener en cuenta que no hay datos de resumen para intervalos parciales que puedan ocurrir ni para el comienzo ni para el final del período de tiempo en cuestión.
- **Eventos latentes y perdidos.** Las métricas agregadas en tablas de resumen podrían ser ligeramente inexactas si hay eventos perdidos o latentes en el período de agregación. Aunque Monitor Service intenta mantener un alto nivel de precisión del estado actual, no vuelve atrás en el tiempo para recalcular la agregación en las tablas de resumen para eventos perdidos o latentes.
- **Alta disponibilidad de conexiones.** Durante la alta disponibilidad de conexiones, hay huecos en los datos de resumen sobre los recuentos de las conexiones actuales, pero las instancias de sesión siguen ejecutándose en los datos sin procesar.
- **Períodos de retención de datos.** Los datos de las tablas de resumen se conservan siguiendo una programación de limpieza distinta de la programación para datos de eventos sin procesar. Podrían faltar datos porque se hayan limpiado las tablas de resumen y de datos sin procesar. Los períodos de retención también podrían diferir según las distintas granularidades de los datos de resumen. Una granularidad de datos menor (minutos) se limpia más rápidamente que una granularidad de datos mayor (días). Si faltan datos de una granularidad debido a una limpieza, es posible que los que encuentre en una granularidad mayor. Puesto que las llamadas de API solo devuelven la granularidad solicitada, si no se reciben datos para una granularidad, eso no significa que los datos no existan en una granularidad mayor para el mismo período de tiempo.
- **Zonas horarias.** Las métricas se guardan con marcas de hora UTC. Las tablas de resumen se agregan en límites de una hora de la zona horaria. Para las zonas horarias que no caen en límites de una hora, podría haber una discrepancia en cuanto a dónde se agregan los datos.

### Granularidad y retención

La granularidad de los datos agregados obtenida por Supervisar es una función del intervalo de tiempo (T) solicitado. Las reglas son las siguientes:

- 0 < T <= 30 días; se utiliza una granularidad por horas
- T > 31 días; se utiliza una granularidad por días

Los datos solicitados que no provienen de datos agregados provienen de la información sin procesar sobre sesiones y conexiones. Estos datos tienden a aumentar rápidamente y, por lo tanto, tienen su propia configuración de limpieza. La limpieza de la base de datos garantiza que solo se conserven los datos que sean relevantes a largo plazo. Esto garantiza un mejor rendimiento, al tiempo que se mantiene la granularidad necesaria para crear informes.

| | Nombre del parámetro | Limpieza afectada | Días de retención para Premium | Días de retención para Advanced |
|---|---|---|---|---|
| 1 | GroomSessionsRetentionDays | Retención de registros de conexión y de sesión después de cerrar la sesión | 90 | 31 |
| 2 | GroomFailuresRetentionDays | Registros de MachineFail-ureLog y Connection-FailureLog | 90 | 31 |
| 3 | GroomLoadIndexesRetentionDays | Registros de LoadIndex | 90 | 31 |

| | | Nombre del parámetro | Limpieza afectada | Días de retención para Premium | Días de retención para Advanced |
|---|---|---|---|---|---|
| | 4 | GroomDeletedRetentionDays | Entidades de máquina, catálogo de máquinas, grupo de escritorios e hipervisor cuyo estado de ciclo de vida (LifecycleState) es “Eliminado” (Deleted). Esta acción también elimina los registros de Session, SessionDetail, Summary, Failure o LoadIndex relacionados. | 90 | 31 |
| | 5 | GroomSummariesRetentionDays | Registros de DesktopGroupSummary, FailureLogSummary y LoadIndexSummary. Datos agregados: granularidad diaria | 365 | 31 |

| | Nombre del parámetro | Limpieza afectada | Días de retención para Premium | Días de retención para Advanced |
|---|---|---|---|---|
| 6 | GroomMachineHotfixLogRetentionDays | Registros de rápidos aplicados a las máquinas de VDA y Controllers | 90 | 31 |
| 7 | GroomHourlyRetentionDays | Datos agregados: granularidad horaria | 32 | 31 |
| 8 | GroomApplicationInstanceRetentionDays | Historial de instancias de aplicación | 90 | No aplicable |
| 9 | GroomNotificationLogRetentionDays | Registro del registro de notificaciones | 90 | No aplicable |
| 10 | GroomResourceUsageRawDataRetentionDays | Datos sin procesar utilización de recursos: datos sin procesar | 3 | 3 |
| 11 | GroomResourceUsageHourDataRetentionDays | Datos resumidos de utilización de recursos: granularidad de hora | 30 | 30 |
| 12 | GroomResourceUsageDayDataRetentionDays | Datos resumidos de utilización de recursos: granularidad de día | 365 | 31 |

| | Nombre del parámetro | Limpieza afectada | Días de retención para Premium | Días de retención para Advanced |
|---|---|---|---|---|
| 13 | GroomProcessUsageRawDataRetentionDays | Datos de utilización de procesos: datos sin procesar | 1 | 1 |
| 14 | GroomProcessUsageHourlyDataRetentionDays | Datos de utilización de procesos: granularidad horaria | 7 | 7 |
| 15 | GroomProcessUsageDailyDataRetentionDays | Datos de utilización de procesos: granularidad diaria | 30 | 30 |
| 16 | GroomSessionMetricsDataRetentionDays | Datos de métricas de sesiones | 1 | 1 |
| 17 | GroomMachineMetricsDataRetentionDays | Datos de métricas de máquinas | 3 | 3 |
| 18 | GroomMachineMetricsDaySummaryDataRetentionDays | Datos resumidos de métricas de máquinas | 365 | 31 |
| 19 | GroomApplicationErrorsDataRetentionDays | Datos de errores de aplicaciones | 1 | 1 |
| 20 | GroomApplicationFaultsDataRetentionDays | Datos de fallos de aplicaciones | 1 | 1 |

> **Precaución:**

> No se pueden modificar los valores de la base de datos de Supervisar servicio.

La retención de datos durante largos períodos de tiempo tiene las implicaciones siguientes en los tamaños de las tablas:

- **Datos por hora.** Si se conservan datos por hora en la base de datos durante dos años, un sitio con 1000 grupos de entrega puede hacer que la base de datos crezca así:

  1000 grupos de entrega x 24 horas/día x 365 días/año x 2 años = 17 520 000 filas de datos. El impacto que esta gran cantidad de datos tiene en el rendimiento de las tablas agregadas es importante. Puesto que los datos de panel de mandos se sacan de esta tabla, los requisitos del servidor de la base de datos podrían ser altos. Si la cantidad de datos es excesiva, el impacto en el rendimiento puede resultar significativo.

- **Datos de sesiones y eventos.** Estos datos se recopilan cada vez que comienza una sesión y se realiza una conexión o reconexión. En sitios grandes (100 000 usuarios), estos datos crecen rápidamente. Por ejemplo, las tablas correspondientes a dos años recopilarían más de un TB de datos, para lo cual se necesitaría una base de datos de nivel empresarial de gama alta.

## Diagnóstico de inicio de sesión

March 30, 2024

> **Nota:**
>
> El diagnóstico de inicio de sesión está actualmente en versión Tech Preview.

Los inicios de sesión involucran a diferentes componentes de Citrix. Para diagnosticar errores de inicio de sesión, utilice Supervisar de Citrix (es decir, el servicio Citrix Director) para localizar el componente y la etapa exactos en los que se produjo el problema. Aplique las acciones recomendadas para resolver el problema. La aplicación Citrix Workspace genera un ID de transacción de 32 dígitos (8-4-4-4-12) que sirve para diagnosticar errores de inicio de sesión.

> **Nota:**
>
> Esta función solo está disponible para clientes de la nube en las regiones de EE. UU., AP-S y UE. No está disponible en Japón ni en las regiones gubernamentales.

### Requisitos previos

Si usa Citrix DaaS, la incorporación es automática. Los clientes de la nube que utilizan StoreFront local deben asegurarse de que se incorpore una versión compatible de StoreFront.

- Si usa Citrix Analytics for Performance, consulte Orígenes de datos para conocer los pasos de incorporación de StoreFront local.
- Si no usa Citrix Analytics for Performance:

  1. Vaya a `https://analytics.cloud.com/unified-datasources/perf/Citrix%20Virtual%20Apps%20and%20Desktops/site-details`.
  2. Haga clic en **Connect to StoreFront deployment**, introduzca los detalles y descargue el archivo de configuración. Para obtener más información, consulte Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante StoreFront.

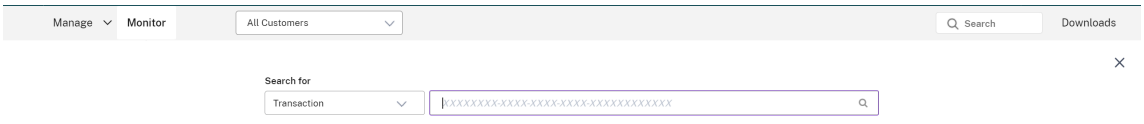
  > **Nota:**
  >
  > Los administradores con roles de Administrador de Cloud pueden incorporar las implementaciones de StoreFront, mientras que los administradores con roles de Administrador total de Supervisar solo pueden verlas.

Las versiones mínimas admitidas de otros componentes son las siguientes:

- Aplicación Citrix Workspace para Windows 2109
- Aplicación Citrix Workspace para Mac 2112
- Aplicación Citrix Workspace para Linux 2112
- Aplicación Citrix Workspace para HTML5 2110
- Aplicación Citrix Workspace para Chrome 2110
- Aplicación Citrix Workspace para Android 2110
- VDA de Citrix Virtual Apps and Desktops versión 2112
- Citrix StoreFront 1912 LTSR CU4

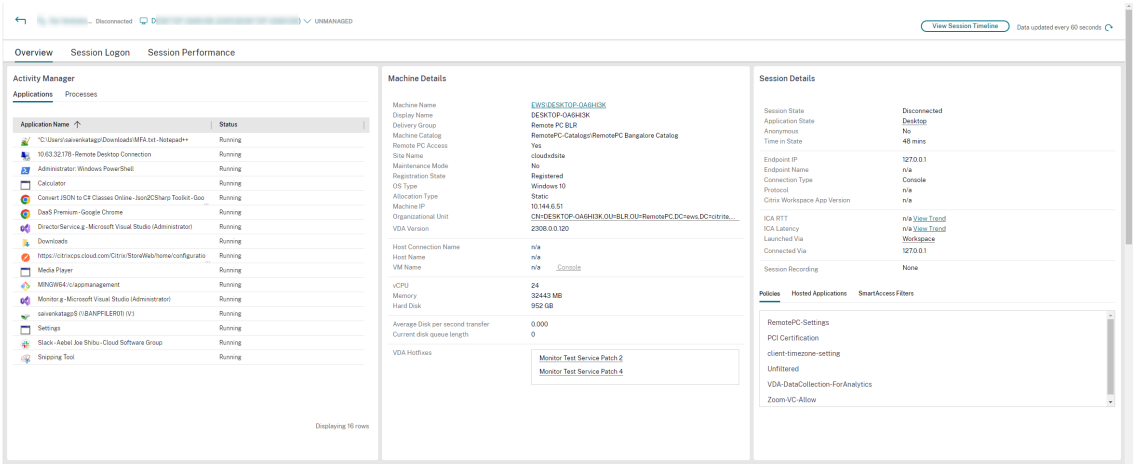
### Pasos para diagnosticar un error en el inicio

1. Copie el ID de transacción del inicio de sesión fallido desde la aplicación Citrix Workspace.
2. En la interfaz de usuario de Supervisar, busque el ID de transacción de 32 dígitos y haga clic en **Detalles**.

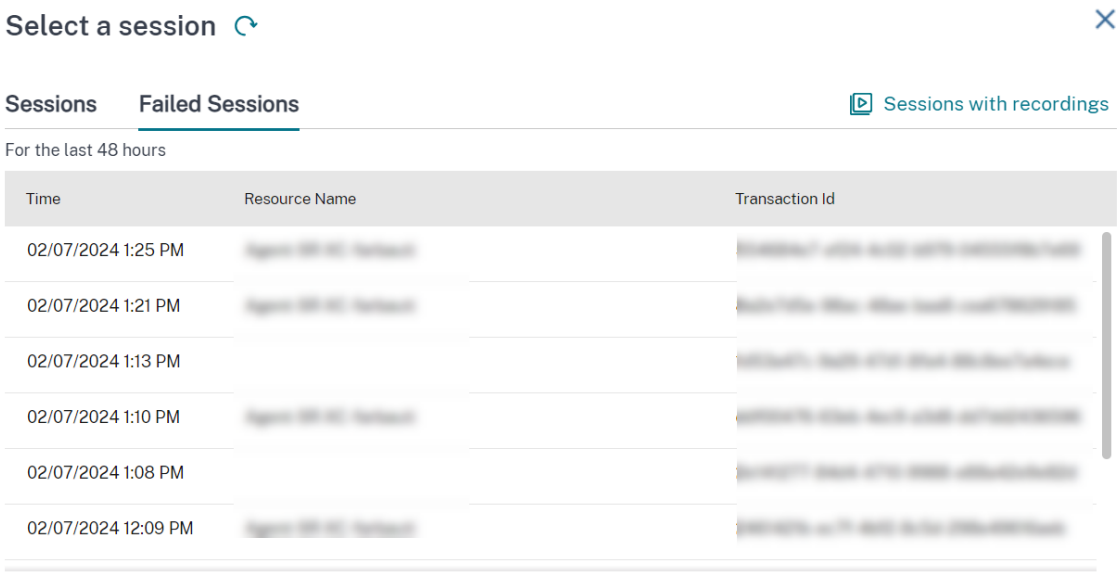



3. Si el ID de transacción no está disponible, busque con el nombre de usuario. Se muestra el Administrador de actividades del usuario.

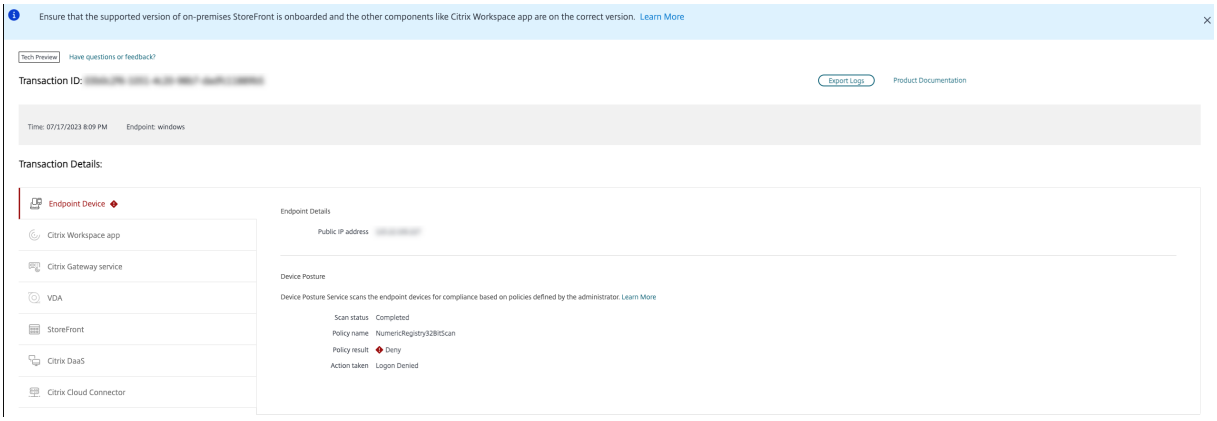



4. Haga clic en el selector de sesión. Vaya a la ficha **Sesiones fallidas**. Se muestra una lista de las sesiones que han fallado durante las últimas 48 horas. Haga clic en la sesión seleccionada.




5. Supervisar de Citrix muestra información clave sobre la transacción, como el nombre de usuario, la marca de hora y la aplicación o el escritorio en los que se produjo el error.
6. El panel Detalles de la transacción contiene una lista de componentes que indican la aparición del error.
7. Haga clic en **Dispositivo de punto final** en la lista de componentes para ver el estado del escaneo de Postura del dispositivo. Device Posture Service analiza el dispositivo de punto final para comprobar su conformidad en función de directivas definidas por el administrador.




Se muestran el estado del escaneo, el nombre de la directiva, el resultado de la directiva y la acción realizada. Asegúrese de que Device Posture Service esté configurado con DaaS tal y como se describe en el artículo Postura de dispositivos. Los errores registrados por Postura de dispositivos se describen en Registros de errores de Postura de dispositivos.

1. Haga clic en los otros nombres de componentes para comprobar los detalles del componente y los detalles del último error conocido.
2. Se muestran el motivo del fallo y el código de error. Haga clic en el enlace **Más información sobre el error** para ver el código de error específico en la sección Códigos de error que contiene la descripción detallada y la acción recomendada.
3. Puede exportar los registros para verlos. El archivo de registros enumera los pasos del inicio de la sesión en orden cronológico y muestra el componente y la etapa exactos en los que se produjo el error.
4. En caso de que se haya producido más de un error en los componentes, solo se muestran los detalles del último error conocido en la página Transacción. Los registros exportados contienen los detalles de todos los errores relacionados con la transacción.

> **Nota:**
>
> Los códigos de error y la información de diagnóstico del lado del cliente solo están disponibles cuando Citrix StoreFront se ha incorporado y envía datos. Para obtener más información sobre la incorporación de StoreFront, consulte Requisitos previos.

## Broker Agent

### bka.prepare.session.failure.validation

- Descripción: No se pudo validar la solicitud de preparación de sesión.
- Acción recomendada: Reintentar acción. Si el error se repite, compruebe que los conectores estén en buen estado.

**bka.prepare.session.failure.rejected**

- Descripción: El VDA no puede aceptar la solicitud de inicio.
- Acción recomendada: Reiniciar el servicio Citrix Delivery Agent en el VDA o reiniciar el VDA.

**bka.hdx.prepare.failure.general**

- Descripción: Error de preparación de HDX.
- Acción recomendada: Reiniciar el VDA.

**bka.hdx.validate.failure.ticket_not_found**

- Descripción: El tíquet o inicio referenciado no está en la caché de inicio.
- Acción recomendada: Comprobar que el VDA puede comunicarse con el conector.

**bka.ticketing.validate.failure.unlicensed**

- Descripción: No se puede verificar la licencia para el inicio.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**bka.ticketing.validate.failure.general**

- Descripción: Error genérico al validar un tíquet.
- Acción recomendada: Recopilar registros en el VDA y ponerse en contacto con Asistencia técnica de Citrix.

**bka.set.configuration.failure.policy**

- Descripción: Se produjo un error durante la configuración de las directivas.
- Acción recomendada: Reiniciar el servicio Citrix Delivery Agent en el VDA o reiniciar el VDA.

**bka.set.configuration.failure**

- Descripción: Se produjo un error durante la configuración de los parámetros.
- Acción recomendada: Reiniciar el servicio Citrix Delivery Agent en el VDA o reiniciar el VDA.

## Intermediario

### brk.validate.credentials.failure.invalid

- Descripción: No se pudieron validar las credenciales debido a algún problema. La razón se puede ampliar en el parámetro del mensaje.
- Acción recomendada: Reintentar acción. Si el error se repite, compruebe que los conectores estén en buen estado.

### brk.resolve.machine.failure.general

- Descripción: No se pudo enumerar o resolver el empleado. La razón se puede ampliar en el parámetro del mensaje.
- Acción recomendada: Comprobar que las máquinas capaces de iniciar esta aplicación estén registradas en el Broker. Asegúrese de que todas las máquinas disponibles no hayan alcanzado su capacidad.

### brk.license.check.failure.constraints

- Descripción: Restricciones de licencia impidieron iniciar la sesión.
- Acción recomendada: Comprobar que haya licencias disponibles para este tipo de aplicación o escritorio.

### brk.resolve.machine.failure.timeout

- Descripción: El broker agotó el tiempo de espera al contactar con la base de datos
- Acción recomendada: Problemas de comunicación con la base de datos del sitio. Contacte con la asistencia técnica de Citrix.

### brk.poweron.forlaunch.queued.failure.general

- Descripción: No se pudo poner en cola la acción de energía.
- Acción recomendada: Problemas de comunicación con la base de datos del sitio. Contacte con la asistencia técnica de Citrix.

### brk.set.configuration.failure.general

- Descripción: Error no especificado al establecer la configuración en el VDA de destino.
- Acción recomendada: Reiniciar el servicio Citrix Delivery Agent en el VDA o reiniciar el VDA.

**brk.prepare.session.failure.host_unreachable**

- Descripción: No se pudo comunicar con el VDA.
- Acción recomendada: Reiniciar el servicio Citrix Delivery Agent en el VDA o reiniciar el VDA.

**brk.prepare.session.failure.general**

- Descripción: No se pudo preparar la sesión en el VDA o errores UnsupportedClientType o ConnectionRefused.
- Acción recomendada: Reiniciar el servicio Citrix Delivery Agent en el VDA o reiniciar el VDA.

**brk.validate.ticket.failure.license**

- Descripción: No se pudo obtener una licencia válida para esta sesión.
- Acción recomendada: Comprobar el estado del sitio y asegurarse de que todos los conectores y el Desktop Delivery Controller de Citrix sean operativos.

**brk.validate.ticket.failure.general**

- Descripción: Llamada de generación de tíquets no válida.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**brk.reverse.prepare.failure.general**

- Descripción: Error genérico durante el inicio de la sesión.
- Acción recomendada: Comprobar el estado del sitio y asegurarse de que todos los conectores y el Desktop Delivery Controller de Citrix sean operativos.

**brk.reverse.prepare.failure.lease_revoked**

- Descripción: Se ha revocado la concesión de esta sesión.
- Acción recomendada: Reintentar la acción; si el error se repite, compruebe que los conectores estén en buen estado.

**brk.reverse.prepare.failure.resource_unavailable**

- Descripción: El recurso ya está en uso o no está disponible temporalmente.
- Acción recomendada: Reintentar la acción; si el error se repite, compruebe que los conectores estén en buen estado.

#### brk.reverse.prepare.failure.app_protection

- Descripción: Falta App Protection y es necesaria para esta sesión.
- Acción recomendada: Comprobar que App Protection está habilitada en este VDA o suprimir el requisito de protección de la aplicación.

### HDX VDA Linux

#### VDA_LINUX_ERR_RECONNECT_PRE_LOGOFF

- Descripción: No se permite reconectarse a una sesión en estado previo al cierre de sesión.
- Acción recomendada: Intentarlo de nuevo más tarde, ya que deja tiempo para que la sesión se cierre.

#### VDA_LINUX_ERR_RECONNECT_NO_SESSION

- Descripción: Reconectarse a una sesión no existente.
- Acción recomendada: Volver a intentarlo más tarde. Si sigue fallando, póngase en contacto con Asistencia técnica de Citrix.

#### VDA_LINUX_ERR_SAME_KEY

- Descripción: En preparación para una conexión, pero hay una sesión existente con la misma clave de sesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VDA_LINUX_ERR_GET_FQDN

- Descripción: No se pudo obtener el nombre de dominio completo de este VDA.
- Acción recomendada: Comprobar que la configuración de DNS en el VDA es correcta

#### VDA_LINUX_ERR_NO_CGP_LISTENER

- Descripción: No hay ninguna escucha de CGP en ejecución.
- Acción recomendada: Comprobar que la directiva de **conexiones de fiabilidad de la sesión** está habilitada. Compruebe que la escucha de CGP se dirige al puerto previsto del VDA (el puerto predeterminado es 2598, se puede cambiar mediante la directiva de **número de puerto de fiabilidad de la sesión**).

#### VDA_LINUX_ERR_DTLS_CONNECT

- Descripción: No se pudo establecer una conexión DTLS con Gateway Service.
- Acción recomendada: Comprobar que el nombre de dominio completo de Gateway Service está disponible desde el VDA. Compruebe que la ruta `/var/xdl/keystore/cacerts` existe en el VDA. Elimine `/var/xdl/keystore` y ejecute `/var/xdl/split_ca_bundle.sh` para regenerar los certificados de CA. Compruebe que el VDA confíe en el nombre de dominio completo de Gateway Service.

#### VDA_LINUX_ERR_ACCEPT_EDT_CONNECT

- Descripción: No se aceptó la negociación con EDT del cliente.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VDA_LINUX_ERR_TCP_CONNECT

- Descripción: No se pudo establecer una conexión TCP con Gateway Service.
- Acción recomendada: Comprobar que el nombre de dominio completo de Gateway Service está disponible desde el VDA.

#### VDA_LINUX_ERR_TLS_CONNECT

- Descripción: No se pudo establecer una negociación con TLS con Gateway Service.
- Acción recomendada: Comprobar que existe la ruta `/var/xdl/keystore/cacerts` en el VDA. Elimine `/var/xdl/keystore` y ejecute `/var/xdl/split_ca_bundle.sh` para regenerar los certificados de CA. Compruebe que el nombre de dominio completo de Gateway Service sea de confianza.

#### VDA_LINUX_ERR_RDVZ_HANDSHAKE

- Descripción: No se pudo establecer una negociación con Rendezvous con Gateway Service.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VDA_LINUX_ERR_ACCEPT_ICA_CONNECT

- Descripción: No se aceptó una conexión ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_RECONNECT_TO_ANON_SESSION_NOT_ALLOWED**

- Descripción: No se permite reconectarse a una sesión anónima.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_CONN_NOT_ALLOWED**

- Descripción: Conexión no autorizada.
- Acción recomendada: Si el código de resultado es 3, verificar que la licencia no haya caducado; de lo contrario, volver a intentarlo más tarde. Si no puede resolverlo, póngase en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_CONN_GENERAL**

- Descripción: No se pudo validar la conexión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_USER_CANCELLED_LOGIN**

- Descripción: El usuario final canceló el inicio de sesión.
- Acción recomendada: Se prevé este error cuando SSO está inhabilitado y el usuario final hace clic en el botón "Cancelar"del cuadro de inicio de sesión; de lo contrario, póngase en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_GET_TARGET**

- Descripción: No se pudo obtener la sesión de destino.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_START_LOGON_TIMERS**

- Descripción: No se pudieron iniciar los temporizadores de inicio de sesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**VDA_LINUX_ERR_SEND_CMD_TO_TARGET**

- Descripción: No se pudo enviar el comando a la sesión de destino.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VDA_LINUX_ERR_POST_RECONNECT_EVENT

- Descripción: No se pudo publicar un evento de reconexión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VDA_LINUX_ERR_RECONNECT_TIMEOUT

- Descripción: Se agotó el tiempo de espera de reconexión a la sesión de usuario.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### HDX VDA Windows

#### RENDEZVOUS_CONNECT_FAILED_TCP

- Descripción: Error en un intento de conexión de transporte de Rendezvous saliente a través de TCP.
- Acción recomendada: Pueden producirse fallos esporádicos debido a malas condiciones de la red. Esto es algo que se prevé. Compruebe la configuración de los VDA si esto ocurre con frecuencia y, a continuación, póngase en contacto con Asistencia técnica de Citrix.

#### RENDEZVOUS_CONNECT_FAILED_EDT

- Descripción: Error en un intento de conexión de transporte de Rendezvous saliente a través de TCP.
- Acción recomendada: Pueden producirse fallos esporádicos debido a malas condiciones de la red. Esto es algo que se prevé. Compruebe la configuración de los VDA si esto ocurre con frecuencia y, a continuación, póngase en contacto con Asistencia técnica de Citrix.

#### RENDEZVOUS_CONNECT_FAILED_PROXY

- Descripción: Se produjo un error en un intento de conexión de transporte de Rendezvous saliente debido a una configuración de proxy no válida.
- Acción recomendada: Comprobar la configuración de proxy de Rendezvous y ponerse en contacto con Asistencia técnica de Citrix.

#### RENDEZVOUS_CONNECT_FAILED_DTLS

- Descripción: Error en un intento de conexión de transporte de Rendezvous saliente debido a un error de negociación de transporte seguro.

- Acción recomendada: Comprobar la configuración de Rendezvous, verificar la configuración de cifrado. Contacte con la asistencia técnica de Citrix.

#### RENDEZVOUS_CONNECT_FAILED_TLS

- Descripción: Error en un intento de conexión de transporte de Rendezvous saliente debido a un error de negociación de transporte seguro.
- Acción recomendada: Comprobar la configuración de Rendezvous, verificar la configuración de cifrado y ponerse en contacto con Asistencia técnica de Citrix.

#### RENDEZVOUS_CONNECT_FAILED_CGP

- Descripción: Error en un intento de conexión de transporte de Rendezvous saliente debido a un problema de configuración de CGP.
- Acción recomendada: Comprobar que CGP (Fiabilidad de la sesión) está habilitada y que se escucha a los puertos CGP; ponerse en contacto con Asistencia técnica de Citrix.

#### CGP_SR_SUSPEND_RESUME_FAILED_TIMEOUT

- Descripción: La interrupción de red no se resolvió debido a que se agotó el tiempo de espera; fiabilidad de la sesión no pudo reanudar la conexión.
- Acción recomendada: Pueden producirse fallos esporádicos debido a malas condiciones de la red. Esto es algo que se prevé.

#### CGP_SR_SUSPEND_RESUME_FAILED

- Descripción: La interrupción de red no se resolvió debido a un error imprevisto; fiabilidad de la sesión no pudo reanudar la conexión.
- Acción recomendada: Pueden producirse fallos esporádicos debido a malas condiciones de la red. Esto es algo que se prevé.

#### PREPARE_RECONNECT_REJECTED

- Descripción: El VDA rechazó una solicitud de reconexión de una conexión ICA entrante debido a una clave de sesión no válida.
- Acción recomendada: Comprobar la configuración del VDA y ponerse en contacto con Asistencia técnica de Citrix.

**Error: PREPARE_REJECTED**

- Descripción: El VDA rechazó una solicitud de conexión de una conexión ICA entrante debido a una clave de sesión no válida.
- Acción recomendada: Comprobar la configuración del VDA y ponerse en contacto con Asistencia técnica de Citrix.

**PREPARE_LISTENING_FAILED**

- Descripción: El VDA no pudo iniciar las escuchas de la conexión ICA entrante.
- Acción recomendada: Comprobar la configuración de red, verificar que otras aplicaciones no estén utilizando los puertos de escucha, ponerse en contacto con Asistencia técnica de Citrix.

**RENDEZVOUSCONNECTIONREQ_FAILED**

- Descripción: El VDA no pudo notificar a la pila ICA que iniciara una conexión de Rendezvous saliente.
- Acción recomendada: Comprobar la configuración de Rendezvous, verificar la configuración de proxy de Rendezvous, verificar la configuración de CGP (fiabilidad de la sesión) y ponerse en contacto con Asistencia técnica de Citrix.

**RENDEZVOUSCONNECTIONREQ_FAILED_PROXYCONFIG**

- Descripción: El VDA no pudo solicitar a la pila ICA que iniciara una conexión Rendezvous saliente debido a un error de configuración de proxy.
- Acción recomendada: Comprobar la configuración de proxy de Rendezvous y ponerse en contacto con Asistencia técnica de Citrix.

**ESTABLISH_SESSION_FAILED**

- Descripción: El VDA no pudo crear una sesión para la conexión ICA entrante o no pudo conectarse a una sesión existente.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**ICA_ESTABLISH_FAILED**

- Descripción: Error en aceptación o negociación de las conexiones ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VALIDATE_FAILED

- Descripción: El agente no pudo validar una solicitud de conexión ICA entrante del VDA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### VALIDATE_TICKETING_FAILED

- Descripción: El broker no pudo validar una solicitud de conexión ICA entrante del VDA debido a un problema de generación de tíquets.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### MCS

#### brk.poweron.forlaunch.execution.generalfailure

- Descripción: Errores generales.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### brk.poweron.forlaunch.execution.insufficientresourcefailure

- Descripción: No se puede completar una operación de hipervisor porque este no tiene recursos suficientes.
- Acción recomendada: Comprobar la cuota de recursos en el hipervisor. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

#### brk.poweron.forlaunch.execution.nosuchmanagedmachine

- Descripción: No existe un ID de máquina.
- Acción recomendada: Comprobar el ID de máquina en el hipervisor. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

#### brk.poweron.forlaunch.execution.hypervisorconnectionfailure

- Descripción: No se puede establecer una conexión con el hipervisor. Por ejemplo, no se encontró la dirección de la infraestructura de alojamiento.
- Acción recomendada: Comprobar que la dirección de la infraestructura de alojamiento es correcta. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.invalidcredentialsfailure**

- Descripción: Credenciales no válidas.
- Acción recomendada: Comprobar las credenciales de la conexión de hipervisor. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.authorizationfailure**

- Descripción: Privilegios o credenciales insuficientes.
- Acción recomendada: Comprobar el permiso asignado a las credenciales para la conexión de hipervisor. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.sslcertauthfailure**

- Descripción: No se puede establecer una conexión debido a un problema de autenticación SSL.
- Acción recomendada: Comprobar el certificado de conexión del hipervisor. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.ratelimitedfailure**

- Descripción: La conexión a la nube informa de limitación del tráfico.
- Acción recomendada: Reintentar la conexión más tarde si la solicitud está bloqueada debido a limitación de tráfico del hipervisor. Si no puede encontrar una solución, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.connectorconnectionfailure**

- Descripción: Existen errores en el conector de nube. Por ejemplo, se agota el tiempo de espera de la conexión. Una vez que se alcanza el tiempo de espera, el conector de nube se desconecta.
- Acción recomendada: Reiniciar el conector de nube. Si no funciona, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.remotehclserverconnectionfailure**

- Descripción: No se encontraron errores en el plug-in HCL/proxy remoto o en el dispositivo de punto final al configurar la conexión al plug-in.
- Acción recomendada: Reiniciar el conector. Si no funciona, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.expiredcredentialsfailure**

- Descripción: Se proporcionó una credencial caducada.
- Acción recomendada: Actualizar las credenciales caducadas que utiliza la conexión del hipervisor.

**brk.poweron.forlaunch.execution.mcsmachinemanagementcustomfailure**

- Descripción: Errores durante la creación de máquinas.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.detachdiskfailed**

- Descripción: No se pudo desconectar el disco utilizado por la máquina virtual.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.createclonefailed**

- Descripción: Error al crear disco clonado en el hipervisor.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.provisionedvmnotfound**

- Descripción: No se encontró la VM aprovisionada.
- Acción recomendada: Quitar la máquina virtual aprovisionada del catálogo. Si no funciona, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.invalidvmstate**

- Descripción: La operación no puede continuar debido a un estado de VM no válido.
- Acción recomendada: Reiniciar primero la VM y volver a intentar la operación.

**brk.poweron.forlaunch.execution.insufficientresources**

- Descripción: Recursos insuficientes durante la operación.
- Acción recomendada: Comprobar la cuota de recursos que utiliza el hipervisor.

**brk.poweron.forlaunch.execution.hypervisorinmaintenancemode**

- Descripción: La operación no puede continuar porque el hipervisor está en modo de mantenimiento.
- Acción recomendada: Comprobar si el hipervisor está en modo de mantenimiento.

**brk.poweron.forlaunch.execution.delayed**

- Descripción: La operación está en cola.
- Acción recomendada: Esperar a que se complete el proceso. Si la operación, póngase en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.recreatevmfailed**

- Descripción: No se pudo volver a crear la máquina virtual.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.unknownvirtualmachine**

- Descripción: Máquina virtual desconocida.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**brk.poweron.forlaunch.execution.ratelimitexceed**

- Descripción: Limitación de tráfico en la conexión a la nube.
- Acción recomendada: Reintentar la conexión más tarde si la solicitud estaba bloqueada debido a limitación de tráfico del hipervisor.

**brk.poweron.forlaunch.execution.virtualdisknotyetonstorage**

- Descripción: No se almacena el disco virtual.
- Acción recomendada: Volver a intentarlo más tarde. Si no funciona, póngase en contacto con Asistencia técnica de Citrix.

## Profile Management

### xendesktop.upm.userprofile.error.failure

- Descripción: Citrix Profile Management no pudo procesar el perfil de usuario. En su lugar, utilizar un perfil temporal.
- Acción recomendada: Este error no provoca un error de inicio de sesión. En su lugar, Citrix Profile Management utiliza un perfil temporal. Para solucionar el error, consulte los registros de eventos de Windows.

### xendesktop.upm.userprofile.error.timeout

- Descripción: Citrix Profile Management no pudo procesar el perfil de usuario en el tiempo especificado.
- Acción recomendada: Este error no provoca un error de inicio de sesión. Citrix Profile Management continúa procesando el perfil de usuario. Para solucionar el error, consulte los registros de Citrix Profile Management.

## Agente de WEM

### wem.agent.userpolicy.error.failure

- Descripción: El agente de Workspace Environment Management (WEM) no pudo procesar las directivas de grupo del usuario. El inicio de sesión de usuario continúa.
- Acción recomendada: El error no provoca errores de inicio de sesión. Para obtener más información, consulte la documentación de producto de WEM y los registros de servicio del agente de WEM.

### wem.agent.userpolicy.error.timeout

- Descripción: El agente de Workspace Environment Management (WEM) no pudo procesar las directivas de grupo del usuario en el tiempo especificado. El inicio de sesión de usuario continúa.
- Acción recomendada: El error no provoca errores de inicio de sesión. Para obtener más información, consulte la documentación de producto de WEM y los registros de servicio del agente de WEM.

## Android posterior al inicio

### SessionManager.Launch.EngineLoadFailed

- Descripción: No se pudo cargar o inicializar el motor ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### SessionManager.Launch.ConnectionFailed

- Descripción: Motor cancelado antes de conectar.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### SessionManager.Launch.LogonFailed

- Descripción: Sesión desconectada sin completarse el inicio de sesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### SessionManager.LeaseResolution.Failed

- Descripción: No se puede intentar iniciar la concesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### SessionManager.clxmtp.SoftDeny

- Descripción: Error en la negociación del servicio CLXMTP del motor (denegación de software).
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### SessionManager.clxmtp.SoftDeny_Implicit

- Descripción: Error en la conexión del servicio CLXMTP del motor (denegación de software implícita).
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### Transport.Connect.NoCGP_Fail

- Descripción: Error de conexión (CGP inhabilitado).
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### Transport.Connect.FallbackFail

- Descripción: Error de conexión. Probada la reserva ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### Transport.Connect.Fail

- Descripción: La conexión no está disponible.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### Android previo al inicio

#### CWA-ICADOWNLOAD_ERR_00001

- Descripción: El tipo de solicitud ICA de envío es incorrecto.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00002

- Descripción: La solicitud de ICA no es válida.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00003

- Descripción: El almacén es nulo para la solicitud ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00004

- Descripción: La URL del almacén es nula para la solicitud ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00005

- Descripción: El parámetro de recurso es nulo para la solicitud ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00006**

- Descripción: El parámetro de recurso proporcionado para la solicitud ICA no es un tipo de recurso válido.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00007**

- Descripción: El parámetro de recurso proporcionado para la solicitud ICA es nulo para la URL de inicio de ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00008**

- Descripción: La solicitud ICA es nula con los parámetros de Authentication Manager.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00009**

- Descripción: El cuerpo de la solicitud ICA es nulo.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000010**

- Descripción: No se pudo crear una entidad HTTP a partir del cuerpo de la solicitud ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000011**

- Descripción: No se pudo descargar el archivo ICA debido a una excepción al crear la solicitud de Authentication Manager.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000012**

- Descripción: No se pudo descargar el archivo ICA debido a una excepción al ejecutar la solicitud de Authentication Manager.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000013**

- Descripción: No se pudo descargar el archivo ICA debido a una respuesta inesperada de la solicitud de Authentication Manager.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000014**

- Descripción: No se pudo descargar el archivo ICA al copiar el valor de inputStream de la respuesta de Authentication Manager.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000015**

- Descripción: No se pudo analizar el documento ICA con el valor de inputStream de la respuesta de Authentication Manager.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000016**

- Descripción: El documento ICA descargado es nulo sin excepción alguna.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000017**

- Descripción: No se pudo descargar el archivo ICA debido a una respuesta incorrecta.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000018**

- Descripción: El recurso no está disponible.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_000019**

- Descripción: El recurso que se va a iniciar no existe, no está habilitado o no es visible para el usuario.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000020

- Descripción: No hay más sesiones activas.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000021

- Descripción: El servidor no tiene la licencia requerida para realizar la actividad solicitada.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000022

- Descripción: No hay estaciones de trabajo disponibles.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000023

- Descripción: No se puede conectar con la estación de trabajo. El servidor ha rechazado la conexión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000024

- Descripción: La estación de trabajo está en modo de mantenimiento y no está disponible para uso.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000025

- Descripción: No se puede iniciar el recurso debido a un error `resourceerror` en el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000026

- Descripción: No se puede iniciar el recurso debido a un error `generalapplauncherror` en el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000027

- Descripción: No se puede iniciar el recurso debido a un error desconocido en el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000028

- Descripción: No se puede iniciar el recurso debido a un error de reinicio en el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000029

- Descripción: No se puede iniciar el recurso debido a un error de reanudación en el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000030

- Descripción: No se puede iniciar el recurso debido a un error indefinido en el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_000031

- Descripción: No se puede descargar el archivo ICA. Sin embargo, el código de error no se encuentra en el mapa definido.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### Linux posterior al inicio

#### SessionManager.Launch.EngineLoadFailed

- Descripción: No se pudo cargar el motor ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### SessionManager.Launch.Failed

- Descripción: No se pudo iniciar la sesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**SessionManager.Launch.ConnectionFailed**

- Descripción: Motor cancelado antes de conectar.
- Acción recomendada: Buscar otros errores asociados al intento de inicio.

**SessionManager.Launch.LogonFailed**

- Descripción: Sesión desconectada sin completarse el inicio de sesión.
- Acción recomendada: Este error indica un fallo en el inicio de sesión, que posiblemente incluya que el usuario no ha introducido las credenciales manualmente. Investigue de qué modo intentó el usuario iniciar sesión en el VDA remoto.

**SessionManager.LeaseResolution.Failed**

- Descripción: No se puede intentar iniciar la concesión.
- Acción recomendada: Comprobar que las concesiones se han sincronizado con la máquina cliente y que siguen siendo válidas. El usuario puede iniciar sesión en Citrix Workspace en modo en línea para activar la (re)sincronización de concesiones. Busque errores emitidos por componentes de Gateway o Cloud Connector. Estos errores pueden indicar los motivos del fallo.

**Transport.Connect.NoCGP_Fail**

- Descripción: Error de conexión (CGP inhabilitado).
- Acción recomendada: Investigar por qué el cliente no puede conectar con un VDA a través de TCP o EDT.

**Transport.Connect.FallbackFail**

- Descripción: Error de conexión. Probada la reserva ICA.
- Acción recomendada: Investigar por qué el cliente no puede conectar con una instancia de Gateway, Connector o VDA a través de TCP o EDT.

**Transport.Connect.Fail**

- Descripción: La aplicación Citrix Workspace no pudo conectar con una instancia de Gateway, Connector o VDA a través de TCP, EDT o UDP.
- Acción recomendada: Investigar por qué el cliente no puede conectar con la instancia de Gateway, Connector o VDA a través de TCP, EDT o UDP. Es posible que el firewall entre el cliente y el host no admita los protocolos (UDP/TCP) o los puertos requeridos.

#### SessionManager.clxmtp.SoftDeny

- Descripción: Error en la negociación del servicio CLXMTP del motor (denegación de software).
- Acción recomendada: Este error no indica que el inicio deba fallar. Indica que el motor no funciona a través de una ruta de red específica. Busque errores emitidos por componentes de Gateway o Cloud Connector. Estos errores pueden indicar los motivos del fallo.

#### SessionManager.clxmtp.SoftDeny_Implicit

- Descripción: Error en la conexión del servicio CLXMTP del motor (denegación de software implícita).
- Acción recomendada: Este error no indica que el inicio deba fallar. Indica que el motor no funciona a través de una ruta de red específica. Investigue por qué el cliente no puede conectar con una instancia de Connector o Gateway. Se podría esperar que ese host no fuera accesible debido a la topología de red o a restricciones de firewall.

### Linux previo al inicio

#### CWA-ICADOWNLOAD_ERR_00001

- Descripción: No se puede conectar con el almacén debido a que la aplicación Citrix Workspace no responde.
- Acción recomendada: Comprobar si Citrix Workspace o StoreFront están inactivos. Verificar también la conectividad a Internet.

#### CWA-ICADOWNLOAD_ERR_00002

- Descripción: El usuario canceló el inicio de sesión.
- Acción recomendada: Reiniciar la sesión después de algún tiempo.

#### CWA-ICADOWNLOAD_ERR_00003

- Descripción: No se puede conectar con el almacén. Compruebe que los certificados del servidor son válidos.
- Acción recomendada: Comprobar que los certificados del servidor están instalados y activos.

**CWA-ICADOWNLOAD_ERR_00004**

- Descripción: El recurso que se va a iniciar no existe, no está habilitado o no es visible para el usuario.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00005**

- Descripción: Las estaciones de trabajo no están disponibles para esta solicitud.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00006**

- Descripción: El servidor no tiene la licencia requerida para realizar la actividad solicitada.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00007**

- Descripción: El servidor rechazó la conexión a la estación de trabajo.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00008**

- Descripción: La estación de trabajo solicitada está en modo de mantenimiento y no está disponible para uso.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00009**

- Descripción: Se ha alcanzado el límite máximo de sesiones.
- Acción recomendada: Se alcanzó el límite máximo de sesiones configurado por un administrador. Reinicie la sesión.

**CWA-ICADOWNLOAD_ERR_000010**

- Descripción: Error general que no se puede especificar con más detalle.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

## Mac posterior al inicio

### No se pudo iniciar el escritorio

- Descripción: El escritorio "nombre del escritorio"no se pudo iniciar. ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

### No se pudo iniciar el visor

- Descripción: No se pudo iniciar el visor. ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

### No se pudo iniciar el escritorio

- Descripción: El escritorio "nombre del escritorio"se encuentra en modo de mantenimiento planificado. ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

### No se pudo iniciar la aplicación

- Descripción: No se pudo iniciar "nombre de la aplicación".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

### No se pudo iniciar la aplicación

- Descripción: No se pudo iniciar "nombre de la aplicación". ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

### No se pudo iniciar el escritorio

- Descripción: El escritorio "nombre del escritorio"no se pudo iniciar.

- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**No se pudo iniciar el escritorio**

- Descripción: El escritorio "nombre del escritorio"no se pudo iniciar. ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**No se pudo iniciar el visor**

- Descripción: El visor no pudo abrir "nombre de la aplicación". ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**No se pudo iniciar el visor**

- Descripción: El visor no pudo abrir el escritorio "nombre del escritorio". ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**No se pudo iniciar el escritorio**

- Descripción: El escritorio "nombre del escritorio"se encuentra en modo de mantenimiento planificado.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**No se pudo iniciar el escritorio**

- Descripción: El escritorio "nombre del escritorio"se encuentra en modo de mantenimiento planificado. ID de transacción: "ID de transacción".
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

#### No se puede conectar al escritorio

- Descripción: No se puede acceder al escritorio "nombre del escritorio". ID de transacción: "ID de transacción". Inténtelo de nuevo más tarde.
- Acción recomendada: Si el problema persiste, ponerse en contacto con el administrador y facilitarle los detalles del error

### Mac previo al inicio

#### CWA-ICADOWNLOAD_ERR_00001

- Descripción: El archivo ICA no es válido.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00002

- Descripción: Se agotó el tiempo de espera de la solicitud de inicio.
- Acción recomendada: Comprobar la conexión a Internet o ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00003

- Descripción: El servidor no respondió.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00004

- Descripción: El recurso que se va a iniciar no existe, no está habilitado o no es visible para el usuario.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CWA-ICADOWNLOAD_ERR_00005

- Descripción: No se puede acceder al servidor.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00006**

- Descripción: Error al iniciar el visor.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00007**

- Descripción: No se pudo iniciar un evento abierto de Apple.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00008**

- Descripción: No se puede acceder a la ruta del visor.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CWA-ICADOWNLOAD_ERR_00009**

- Descripción: El usuario canceló la autenticación.
- Acción recomendada: Pedir al usuario que vuelva a iniciar el recurso.

**CWA-ICADOWNLOAD_ERR_000010**

- Descripción: El usuario canceló la ventana de LSI.
- Acción recomendada: Pedir al usuario que vuelva a iniciar el recurso.

**CWA-ICADOWNLOAD_ERR_000011**

- Descripción: La estación de trabajo solicitada está en modo de mantenimiento y no está disponible para uso.
- Acción recomendada: Pedir al usuario que lo intente una vez finalizado el mantenimiento, cuando la estación de trabajo esté disponible para uso.

**CWA-ICADOWNLOAD_ERR_000012**

- Descripción: Se deben cambiar las credenciales de inicio de sesión del usuario.
- Acción recomendada: Pedir al usuario que cambie las credenciales de inicio de sesión.

#### CWA-ICADOWNLOAD_ERR_000013

- Descripción: La sesión que conecta el recurso ya no está activa.
- Acción recomendada: Pedir al usuario que lo intente de nuevo o ponerse en contacto con Asistencia técnica de Citrix para obtener más ayuda.

#### CWA-ICADOWNLOAD_ERR_000014

- Descripción: No se pudo descargar el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### Windows posterior al inicio

#### SessionManager.Launch.EngineLoadFailed

- Descripción: Los componentes principales para establecer una conexión a una aplicación o escritorio remoto no se cargaron o inicializaron correctamente. Es posible que se incluyan detalles adicionales en el mensaje de error.
- Acción recomendada: La aplicación Citrix Workspace no funciona de la manera prevista. Es posible que una DLL de canal virtual de terceros (no de Citrix) u otro componente del sistema esté causando este problema. Podría ser necesario recopilar y enviar seguimientos CDF para determinar el tipo de fallo.

#### SessionManager.Launch.ConnectionFailed

- Descripción: Se trata de un error genérico que indica que un intento de inicio ha fallado. Otros errores emitidos pueden indicar la causa.
- Acción recomendada: Buscar otros errores asociados al intento de inicio.

#### SessionManager.Launch.LogonFailed

- Descripción: Este error indica que se estableció una conexión con una aplicación o escritorio remoto. Sin embargo, la sesión se desconectó sin completar el inicio de sesión de Windows (u otro sistema operativo).
- Acción recomendada: Este error indica un fallo en el inicio de sesión, que posiblemente incluya que el usuario no ha introducido las credenciales manualmente. Investigue de qué modo intentó el usuario iniciar sesión en el VDA remoto.

**SessionManager.Launch.Cancelled**

- Descripción: Se canceló el intento de conexión del motor Citrix, muy probablemente por acción del usuario.
- Acción recomendada: Este error indica por qué una conexión no se estableció correctamente, pero probablemente indica un comportamiento correcto.

**SessionManager.LeaseResolution.Failed**

- Descripción: Indica que un inicio de sesión sin conexión (lo que también se denomina "basado en concesión") ha fallado. Este error se debe a que no se encontró una concesión válida y obligatoria para el recurso en la máquina cliente. Además, Gateway o Cloud Connector rechazaron la solicitud de inicio, o bien esta no era válida.
- Acción recomendada: Comprobar que las concesiones se han sincronizado con la máquina cliente y que siguen siendo válidas. El usuario puede iniciar sesión en Citrix Workspace en modo en línea para activar la (re)sincronización de concesiones. Busque errores emitidos por componentes de Gateway o Cloud Connector. Estos errores pueden indicar los motivos del fallo.

**SessionManager.clxmtp.SoftDeny**

- Descripción: Se intentó iniciar una concesión y una instancia de Connector o Gateway informó al cliente de que no podía completar el proceso solicitado. Sin embargo, otras instancias de Connector o Gateway pueden ayudar con el inicio.
- Acción recomendada: Este error no indica que el inicio deba fallar. Indica que el motor no funciona a través de una ruta de red específica. Busque errores emitidos por componentes de Gateway o Cloud Connector. Estos errores pueden indicar los motivos del fallo.

**SessionManager.clxmtp.SoftDeny_Implicit**

- Descripción: Se intentó iniciar una concesión y no se pudo acceder a una instancia de Connector o Gateway. Sin embargo, otras instancias de Connector o Gateway pueden ayudar con el inicio.
- Acción recomendada: Este error no indica que el inicio deba fallar. Indica que el motor no funciona a través de una ruta de red específica. Investigue por qué el cliente no puede conectar con una instancia de Connector o Gateway. Se podría esperar que ese host no fuera accesible debido a la topología de red o a restricciones de firewall.

#### Transport.Connect.NoCGP_Fail

- Descripción: Los componentes principales (motor) de la aplicación Citrix Workspace no pudieron conectarse a un host de VDA a través del protocolo ICA (puerto 1494). Si se ha enviado este evento, no tuvieron lugar los intentos de conectarse a una puerta de enlace o VDA a través del protocolo CGP.
- Acción recomendada: Investigar por qué el cliente no puede conectar con un VDA a través de TCP o EDT.

#### Transport.Connect.FallbackFail

- Descripción: Los componentes principales (motor) de la aplicación Citrix Workspace no pudieron conectarse a un host de VDA a través del protocolo ICA (puerto 1494). Después de este error, la aplicación Citrix Workspace no se conecta a una instancia de Gateway o VDA a través del protocolo CGP (puerto 2598).
- Acción recomendada: Investigar por qué el cliente no puede conectar con una instancia de Gateway, Connector o VDA a través de TCP o EDT.

#### Transport.Connect.Fail

- Descripción: Los componentes principales (motor) de la aplicación Citrix Workspace no pudieron conectarse a una instancia de Gateway o VDA a través del protocolo CGP (puerto 2598). Si se ha emitido este evento, no tuvieron lugar los intentos de conectarse a un VDA a través del protocolo ICA.
- Acción recomendada: Investigar por qué el cliente no puede conectar con una instancia de Gateway, Connector o VDA a través de TCP o EDT.

### Windows previo al inicio

#### CWA-ICADOWNLOAD_ERR_00001

- Descripción: No se puede conectar con el almacén debido a que la aplicación Citrix Workspace no responde.
- Acción recomendada: Comprobar si Citrix Workspace o StoreFront están inactivos. Verificar también la conectividad a Internet.

#### CWA-ICADOWNLOAD_ERR_00002

- Descripción: El usuario canceló el inicio de sesión.

- Acción recomendada: Reiniciar la sesión después de algún tiempo.

**CWA-ICADOWNLOAD_ERR_00003**

- Descripción: No se puede conectar con el almacén. Compruebe que los certificados del servidor son válidos.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**CWA-ICADOWNLOAD_ERR_00004**

- Descripción: El recurso que se va a iniciar no existe, no está habilitado o no es visible para el usuario.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**CWA-ICADOWNLOAD_ERR_00005**

- Descripción: Las estaciones de trabajo no están disponibles para esta solicitud.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**CWA-ICADOWNLOAD_ERR_00006**

- Descripción: El servidor no tiene la licencia requerida para realizar la actividad solicitada.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**CWA-ICADOWNLOAD_ERR_00007**

- Descripción: El servidor rechazó la conexión a la estación de trabajo.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

**CWA-ICADOWNLOAD_ERR_00008**

- Descripción: La estación de trabajo solicitada está en modo de mantenimiento y no está disponible para uso.

- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

#### CWA-ICADOWNLOAD_ERR_00009

- Descripción: Se ha alcanzado el límite máximo de sesiones.
- Acción recomendada: Se alcanzó el límite máximo de sesiones configurado por un administrador. Reinicie la sesión.

#### CWA-ICADOWNLOAD_ERR_000010

- Descripción: Error general que no se puede especificar con más detalle.
- Acción recomendada: Ponerse en contacto con el administrador de TI y facilitarle los detalles del error.

### Workspace

#### StoreLaunchIcaEndpoint.LaunchFailed

- Descripción: Se ha producido un error durante el inicio.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

#### StoreLaunchSessionEndpoint.BadRequest

- Descripción: Los parámetros de la solicitud de inicio no eran válidos o estaban en blanco.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### StoreLaunchSessionEndpoint.FarmUnavailable

- Descripción: No había comunidades disponibles para el inicio.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops.

#### StoreLaunchSessionEndpoint.Error

- Descripción: Se ha producido un error interno durante el inicio.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**StoreGetIcaFileEndpoint.BadRequest**

- Descripción: No se proporcionó ningún tíquet de inicio en la solicitud.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**StoreGetIcaFileEndpoint.RetrieveIcaFileForTicketFailed**

- Descripción: Workspace no pudo obtener el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**StoreGetIcaFileEndpoint.Error**

- Descripción: Workspace no pudo obtener el archivo ICA.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**WebProxyGetLaunchStatusEndPoint.DSAuthFailure**

- Descripción: Hubo un problema de autenticación.
- Acción recomendada: Reintentar la autenticación. Contacte con la asistencia técnica de Citrix.

**WebProxyGetLaunchStatusEndPoint.LaunchFailed**

- Descripción: Se produjo un error interno al iniciar la aplicación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**WebProxyGetLaunchStatusEndPoint.ResourceNotFound**

- Descripción: El inicio falló porque no se encontró la aplicación.
- Acción recomendada: Comprobar la configuración de la aplicación y los registros de Citrix Virtual Apps and Desktops.

**WebProxyLaunchIcaEndpoint.DSAuthFailure**

- Descripción: Hubo un problema de autenticación.
- Acción recomendada: Reintentar la autenticación. Contacte con la asistencia técnica de Citrix.

**WebProxyLaunchIcaEndpoint.LaunchFailed**

- Descripción: Se produjo un error interno al iniciar la aplicación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**WebProxyLaunchIcaEndpoint.ResourceNotFound**

- Descripción: El inicio falló porque no se encontró la aplicación.
- Acción recomendada: Comprobar la configuración de la aplicación y los registros de Citrix Virtual Apps and Desktops.

**WebProxySessionsLaunchIcaEndpoint.SessionNotFound**

- Descripción: Workspace no pudo reconectarse a la sesión HDX existente. Es posible que la sesión finalice.
- Acción recomendada: Volver a iniciar la aplicación.

**WebProxySessionsLaunchIcaEndpoint.DSAuthFailure**

- Descripción: Hubo un problema de autenticación.
- Acción recomendada: Reintentar la autenticación. Contacte con la asistencia técnica de Citrix.

**WebProxySessionsLaunchIcaEndpoint.ReconnectSessionFailed**

- Descripción: Workspace no pudo reconectarse a la sesión HDX existente. Es posible que la sesión finalice.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**WebProxySessionsLaunchIcaEndpoint.Error**

- Descripción: Se produjo un error interno al reconectarse a la sesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**WebProxySessionsGetLaunchStatusEndpoint.DSAuthFailure**

- Descripción: Hubo un problema de autenticación.
- Acción recomendada: Reintentar la autenticación. Contacte con la asistencia técnica de Citrix.

**WebProxySessionsGetLaunchStatusEndpoint.ReconnectSessionFailed**

- Descripción: Workspace no pudo reconectarse a la sesión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**WebProxySessionsGetLaunchStatusEndpoint.Error**

- Descripción: Se produjo un error interno al reconectarse a la sesión.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**DetermineGateway.Error**

- Descripción: Workspace no pudo determinar a qué puerta de enlace conectarse.
- Acción recomendada: Comprobar la configuración de puerta de enlace. Contacte con la asistencia técnica de Citrix.

**ConnectionRoutingProviderLaunch.Error**

- Descripción: Workspace no pudo determinar a qué puerta de enlace conectarse.
- Acción recomendada: Comprobar la configuración de puerta de enlace. Contacte con la asistencia técnica de Citrix.

**BrokerGetAddressCall.AnonymousPrelaunchNotSupported**

- Descripción: Workspace no puede iniciar la aplicación porque la comunidad no admite inicios anónimos.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**BrokerGetAddressCall.LeasingError**

- Descripción: Workspace recibió un error del broker de Citrix Virtual Apps and Desktops.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**BrokerGetAddressCall.ServiceConnectionError**

- Descripción: Workspace no pudo ponerse en contacto con ningún broker de Citrix Virtual Apps and Desktops de la comunidad.

- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**BrokerGetAddressCall.BrokerError**

- Descripción: Workspace recibió un error de un broker de Citrix Virtual Apps and Desktops.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**BrokerGetAddressCall.LicensingError**

- Descripción: Workspace no pudo iniciar la aplicación debido a un error de licencia.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**BrokerGetAddressCall.Error**

- Descripción: Workspace no puede obtener los detalles del VDA del broker de Citrix Virtual Apps and Desktops.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**GetLaunchReference.NoAccessToken**

- Descripción: Workspace no puede conectar con el VDA.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**GetLaunchReference.BrokerError**

- Descripción: Workspace no puede conectar con el VDA.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**GetLaunchReference.Error**

- Descripción: Workspace no puede conectar con el VDA.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**GenerateIcaFile.InvalidIcaSetting**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**StoreIcaFileAndGetTicket.StoreIcaFileAndCreateTicketFailed**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**StoreIcaFileAndGetTicket.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetFasVdaLogonTicket.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GenerateSTATicket.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetVdaAddress.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetTicket.NoAccessToken**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetTicket.BrokerError**

- Descripción: El broker de Citrix Virtual Apps and Desktops no pudo iniciar la sesión HDX.
- Acción recomendada: Comprobar el ID en el mensaje de error y los registros de Citrix Virtual Apps and Desktops.

**GetTicket.ServiceConnectionError**

- Descripción: Workspace no puede conectar con un broker de Citrix Virtual Apps and Desktops.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetTicket.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetNetscalerConfigurationByCustomer.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**DiscoverMPSServerCapabilities.Error**

- Descripción: Hubo un problema al hacer una solicitud al broker de Citrix Virtual Apps and Desktops.
- Acción recomendada: Comprobar los registros de Citrix Virtual Apps and Desktops. Contacte con la asistencia técnica de Citrix.

**GetResourceLocationNetScalerConfig.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**GetCustomerResourceLocations.Error**

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### GetResourceLocationFromResourceProvider.Error

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### GetNetScalerGatewayInfo.Error

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### GetCustomerEntitlements.Error

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### GetResourceLocationForServerFeed.Error

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### GetResourceInformation.Error

- Descripción: Se produjo un error interno al establecer una conexión HDX.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

### Citrix Gateway como servicio

#### CGS-ICASN_ERR_00001

- Descripción: No se pudo iniciar la aplicación debido a un error de análisis de la solicitud.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### CGS-ICASN_ERR_00002

- Descripción: No se pudo validar el tíquet de autenticación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS-ICASN_ERR_00003**

- Descripción: No se pudo validar el tíquet de autenticación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS-ICASN_ERR_00004**

- Descripción: No se pudo validar el tíquet de autenticación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS-ICASN_ERR_00005**

- Descripción: No se pudo establecer la conexión con Connector.
- Acción recomendada: Comprobar el estado del conector. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00006**

- Descripción: Se agotó el tiempo de espera de la solicitud de conexión a Connector.
- Acción recomendada: Comprobar el estado del conector. Compruebe si alguna configuración de proxy bloquea el tráfico entre el conector/VDA y NGS. Compruebe la conectividad entre el VDA y Connector. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00007**

- Descripción: La aplicación Citrix Workspace cerró la conexión.
- Acción recomendada: Comprobar que la conectividad de red del lado del cliente es estable. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00008**

- Descripción: El back-end cerró la conexión.
- Acción recomendada: Comprobar el estado del conector. Verifique la estabilidad de la red desde Connector/VDA a la red pública (NGS). Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00009**

- Descripción: Error al establecer una conexión de VDA a NGS (Rendezvous).
- Acción recomendada: Comprobar el estado del conector. El VDA debe poder comunicarse con el servicio NGS. Compruebe la conectividad entre el VDA y Connector. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00010**

- Descripción: Cambio de EDT a TCP. Verifique el requisito previo para EDT.
- Acción recomendada: Rendezvous debe estar habilitado y el VDA debe poder comunicarse con el servicio NGS a través de UDP. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00011**

- Descripción: Fallo en el servicio interno de NGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00012**

- Descripción: Fallo en el servicio interno de NGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00013**

- Descripción: Error en la validación de GCT.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00014**

- Descripción: Error en la validación de GCT.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00015**

- Descripción: Fallo en el servicio interno de NGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00016**

- Descripción: Fallo en el servicio interno de NGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00017**

- Descripción: Fallo en el servicio interno de NGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00018**

- Descripción: No se pudo validar el tíquet de autenticación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00019**

- Descripción: No se pudo validar el tíquet de autenticación.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00020**

- Descripción: Error en la licencia interna de CGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00021**

- Descripción: Cambio a Rendezvous v2 debido a marca de función inhabilitada.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00022**

- Descripción: Fallo en el servicio interno de NGS.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00023**

- Descripción: Error de tiempo de espera en intercambio CLXMTP.
- Acción recomendada: Comprobar que los conectores están en buen estado y que se pueda acceder al servicio NGS. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00024**

- Descripción: Error en la validación VSR de CLXMTP.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00025**

- Descripción: Error en la validación VSR de CLXMTP.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**CGS_ICASN_ERR_00026**

- Descripción: Connector no está disponible en CLXMTP.
- Acción recomendada: Comprobar que el conector está en buen estado para la ubicación de recursos. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

**CGS_ICASN_ERR_00027**

- Descripción: La redirección de CLXMTP a Connector falló tras la cantidad máxima de intentos.
- Acción recomendada: Comprobar que el conector está en buen estado para la ubicación de recursos. Compruebe que el servicio `Citrix ClxMtp Service` se esté ejecutando en todos los conectores. Contacte con la asistencia técnica de Citrix.

**CGS_ICASN_ERR_00028**

- Descripción: No se pudo comunicar con Controller.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

**Success: CGS_ICASN_SUCCESS_00001**

- Descripción: Se recibió una solicitud de inicio de sesión.
- Acción recomendada: No procede

#### Success: CGS_ICASN_SUCCESS_00002

- Descripción: Se completó la solicitud de inicio de sesión.
- Acción recomendada: No procede

### Proxy XAXD

#### XDPXY_INF_00001

- Descripción: El broker envía una solicitud al VDA para que se prepare para las conexiones entrantes.
- Acción recomendada: No procede

#### XDPXY_INF_00002

- Descripción: El VDA confirma la solicitud de conexión del broker.
- Acción recomendada: No procede

#### XDPXY_ERR_00001

- Descripción: No se pudo comunicar con el VDA.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Reinicie el servicio Citrix Delivery Agent en el VDA o reinicie el VDA.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00002

- Descripción: Se agotó el tiempo de espera de XaxdProxy en espera de una respuesta del VDA.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Reinicie el servicio Citrix Delivery Agent en el VDA o reinicie el VDA.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00003

- Descripción: Se ha encontrado un error o una excepción de WCF al intentar hacer la solicitud.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Reinicie el servicio Citrix Delivery Agent en el VDA o reinicie el VDA.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_INF_00003

- Descripción: La pila realiza una solicitud de validación de una conexión ICA o RDP entrante.
- Acción recomendada: No procede

#### XDPXY_INF_00004

- Descripción: Se establece la validación de la conexión ICA o RDP entrante.
- Acción recomendada: No procede

#### XDPXY_ERR_00001

- Descripción: No se pudo comunicar con el proxy del VDA.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Reinicie el servicio Citrix Delivery Agent en el VDA o reinicie el VDA.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00002

- Descripción: Se agotó el tiempo de espera de XaxdProxy en espera de una respuesta del proxy del VDA.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Reinicie el servicio Citrix Delivery Agent en el VDA o reinicie el VDA.

  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00003

- Descripción: Se ha encontrado una excepción al intentar hacer la solicitud.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Reinicie el servicio Citrix Delivery Agent en el VDA o reinicie el VDA.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_INF_00005

- Descripción: Se ha hecho una solicitud de tráfico de sesión HDX dirigida al VDA.
- Acción recomendada: No procede

#### XDPXY_INF_00006

- Descripción: El VDA establece una conexión directa con el plano de control de Citrix Cloud para el tráfico de sesiones HDX.
- Acción recomendada: No procede

#### XDPXY_INF_00007

- Descripción: El cliente envía una solicitud de conexión a StoreFront local para obtener un recurso.
- Acción recomendada: No procede

#### XDPXY_INF_00008

- Descripción: StoreFront local acepta la solicitud de conexión del cliente relativa al recurso.
- Acción recomendada: No procede

#### XDPXY_ERR_00004

- Descripción: XaxdProxy recibió una respuesta de error HTTP al intentar conectar.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Compruebe la estabilidad de la red desde Connector a la red pública.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00006

- Descripción: La solicitud XML tiene un formato no válido.
- Acción recomendada: Ponerse en contacto con Asistencia técnica de Citrix.

#### XDPXY_ERR_00007

- Descripción: La solicitud XML tiene formato o encabezados de credenciales no válidos.
- Acción recomendada: Cerrar sesión, volver a iniciar sesión y volver a intentar la acción. Si el problema persiste, póngase en contacto con Asistencia técnica de Citrix

#### XDPXY_INF_00011

- Descripción: El usuario solicita el inicio de la continuidad del servicio a través de WSA.
- Acción recomendada: No procede

#### XDPXY_INF_00012

- Descripción: El usuario solicita el inicio de la continuidad del servicio a través de WSA.
- Acción recomendada: No procede

#### XDPXY_ERR_00004

- Descripción: XaxdProxy dio con un error de HTTP al intentar conectarse.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.

  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00008

- Descripción: No se pudo iniciar la continuidad del servicio porque se agotó el tiempo de espera de XaxdProxy en espera de una respuesta.
- Acción recomendada: Comprobar el estado de Connector. Para obtener más información, consulte Citrix Cloud Connector y CTX224133.
  - Si tiene un proxy web entre Connector y el broker, asegúrese de que esté configurado correctamente.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

#### XDPXY_ERR_00009

- Descripción: No se pudo iniciar la continuidad del servicio debido a que la concesión se bloqueó o revocó.
- Acción recomendada: Ponerse en contacto con el administrador de Citrix Cloud y facilitarle los detalles del error. Para obtener más información, consulte la documentación de Continuidad del servicio.
  - Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix.

## Citrix DaaS para Citrix Service Providers

February 12, 2024

En este artículo se describe cómo **Citrix Service Providers (CSP)** puede configurar Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) para 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.

## Limitaciones y problemas conocidos

### Limitaciones

- Los cambios de nombre de arrendatario tardan hasta 24 horas en aplicarse a todas las interfaces.
- Al crear un arrendatario, la dirección de correo electrónico debe ser única.
- El filtrado en **Administrar > Configuración completa** por ámbito (similar a Supervisar) no está disponible. Para ver los recursos asociados a un ámbito, seleccione **Administradores** en el panel de la izquierda. En la ficha **Ámbitos**, seleccione el ámbito y, a continuación, seleccione **Modificar ámbito** en el panel Acción.

### Problemas conocidos

- Una vez asignados los ámbitos a un recurso, no se puede utilizar la consola de administración para quitarlos o cancelar su asignación. Esas tareas solo se admiten a través de PowerShell.
- **Administrar > Configuración completa** no aplica ámbitos. Usted es responsable de seleccionar el ámbito adecuado al crear catálogos de máquinas, grupos de entrega y grupos de aplicaciones.
- Cuando se crean más de 15 ámbitos (automáticamente y personalizados), la información de acceso personalizado a Citrix Cloud de un administrador (**Administración de acceso e identidad > Administradores**) no se muestra correctamente. Solución temporal: Limite los ámbitos a 15 o menos.

## Agregar un cliente

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. Seleccione **Clientes** en el menú superior de la izquierda.
2. En el panel de mandos de clientes, seleccione **Invitar o Agregar**. Proporcione la información solicitada.
3. 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.
4. 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 las consolas **Administrar** y **Supervisar**.

### Agregar Citrix DaaS a un cliente

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. Seleccione **Clientes** en el menú superior de la izquierda.
2. En el panel de mandos de clientes, en el menú de tres puntos del cliente, seleccione **Agregar servicio**.
3. En **Seleccione un servicio para agregar**, seleccione **Virtual Apps and Desktops**.
4. Seleccione **Continue**.

Después de completar este procedimiento, el cliente se incorpora a su suscripción de Citrix DaaS.

Una vez completada la incorporación, se crea automáticamente un ámbito de cliente en Citrix DaaS. El ámbito está visible en la pantalla **Administrar > Configuración completa**. Este ámbito es exclusivo de ese cliente. Puede cambiar el nombre del ámbito, pero no puede eliminarlo.

Utilice este ámbito para adaptar el acceso de otros administradores. Supongamos, por ejemplo, que tiene 10 clientes y dos administradores. Con el ámbito exclusivo, puede restringir el acceso de un administrador a solo tres de los clientes. El otro administrador puede acceder a uno de esos tres clientes, además de otros dos clientes. Para obtener información más detallada, consulte Controlar el acceso de administrador a los clientes

### Configurar una ubicación de recursos

Una ubicación de recursos contiene las máquinas que entregan las aplicaciones y escritorios de los clientes, y componentes de infraestructura, como Citrix Cloud Connectors. Para obtener más información, consulte Conectarse a Citrix Cloud.

### Configurar catálogos y grupos para entrega de aplicaciones y escritorios

> **Nota:**
>
> Para administrar DaaS para un cliente arrendatario, debe cambiar a la cuenta del cliente de CSP. Para hacerlo, haga clic en el nombre del cliente en el menú superior derecho y haga clic en **Cambiar cliente**.

Un catálogo es un grupo de máquinas virtuales idénticas. Al crear un catálogo, se utiliza una imagen (con otros parámetros) como plantilla para crear las máquinas. Para obtener más información, consulte Crear catálogos de máquinas.

Un grupo de entrega es un conjunto de máquinas seleccionadas de uno o varios catálogos de máquinas. El grupo de entrega especifica los usuarios que pueden usar esas máquinas, además de las aplicaciones o los escritorios disponibles para esos usuarios. Para obtener información detallada, consulte Crear grupos de entrega.

Los grupos de aplicaciones permiten administrar colecciones de aplicaciones. Puede crear grupos de aplicaciones para las aplicaciones compartidas entre varios grupos de entrega o que son utilizadas por un subconjunto de usuarios dentro de un grupo de entrega. Para obtener más información, consulte Crear grupos de aplicaciones.

Al configurar grupos, asegúrese de que:

- El ámbito del grupo de entrega es un subconjunto del ámbito del catálogo de máquinas. Por ejemplo, supongamos que el ámbito del catálogo es A y B. El ámbito del grupo de entrega puede ser A o B, o A y B.
- El ámbito del grupo de aplicaciones es un subconjunto del ámbito del grupo de entrega. Por ejemplo, supongamos que los grupos de entrega asociados a un grupo de aplicaciones tienen el ámbito A y B. El ámbito del grupo de aplicaciones puede ser A o B, o A y B.

## 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. Esto le permite proporcionar espacios de trabajo dedicados a sus clientes, a los que los usuarios de dichos clientes pueden acceder mediante una URL de espacio de trabajo personalizada (por ejemplo, customer.cloud.com), mientras que la ubicación de los recursos sigue estando 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 que los clientes puedan acceder a su espacio de trabajo dedicado, debe agregarlos a los dominios correspondientes que administre. Después de configurar el espacio de trabajo en Configuración de Workspace, los usuarios de los clientes pueden iniciar sesión en su espacio de trabajo y acceder a las aplicaciones y escritorios que haya puesto a disposición.

### Agregar un cliente a un dominio

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. Seleccione **Clientes** en el menú superior de la izquierda.
2. En el panel de mandos de clientes, seleccione **Administración de acceso e identidad** en el menú superior de la izquierda.

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. Seleccione el signo más que hay junto al nombre del cliente. El cliente seleccionado aparecerá ahora en la columna de **clientes federados**. Repita esta operación para agregar otros clientes. Cuando haya terminado, seleccione **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. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Dominios**.
2. Busque el dominio que quiere administrar y seleccione el botón de tres puntos. Seleccione **Administrar el dominio federado**.
3. En la lista de clientes federados, busque los clientes que quiere quitar y seleccione el botón X. Seleccione **Quitar todos** para quitar del dominio todos los clientes de la lista. Los clientes seleccionados pasan a la lista de clientes disponibles.
4. Seleccione **Aplicar**.
5. Revise los clientes seleccionados y seleccione **Quitar clientes**.

### Controlar el acceso de administrador a los clientes

Puede controlar el acceso de administrador a los clientes mediante el ámbito exclusivo que se creó al agregar Citrix DaaS al cliente. Puede configurar el acceso al agregar un administrador o más tarde.

Para obtener información sobre cómo restringir el acceso mediante roles y ámbitos en Citrix DaaS, consulte Administración delegada.

#### Agregar un administrador con acceso restringido

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. Seleccione **Clientes** en el menú superior de la izquierda.
2. En el panel de mandos de clientes, seleccione **Administración de acceso e identidad** en el menú superior de la izquierda.
3. En la ficha **Administradores**, seleccione **Agregar administradores desde** y, a continuación, seleccione **Identidad de Citrix**.
4. Escriba la dirección de correo electrónico de la persona que va a agregar como administrador y, a continuación, seleccione **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. Después de seleccionar **Acceso personalizado**, seleccione uno o más pares de roles y ámbitos para Citrix DaaS, según sea necesario. Asegúrese de habilitar solo las entradas que contengan el ámbito exclusivo que se creó para el cliente.
7. Cuando haya terminado de seleccionar los pares de roles y ámbitos, seleccione **Enviar invitación**.

Cuando el administrador acepte la invitación, tendrá el acceso que le ha asignado.

#### Modificar permisos de administración delegada para administradores

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. Seleccione **Clientes** en el menú superior de la izquierda.
2. En el panel de mandos de clientes, seleccione **Administración de acceso e identidad** en el menú superior de la izquierda.
3. En la ficha **Administradores**, seleccione **Modificar acceso** en el menú de tres puntos del administrador.
4. Seleccione y borre los pares de roles y ámbitos para Citrix DaaS según sea necesario. Asegúrese de habilitar solo las entradas que contengan el ámbito exclusivo que se creó para el cliente.
5. Seleccione **Guardar**.

#### Ver administradores de clientes y sus roles y ámbitos asignados

1. Inicie sesión en Citrix Cloud con sus credenciales de CSP. Seleccione **Clientes** en el menú superior de la izquierda.
2. En el panel de mandos del cliente, seleccione **Mis servicios > DaaS** en el menú superior de la izquierda.
3. En Citrix DaaS, seleccione **Administrar > Configuración completa**.
4. Seleccione **Administradores** en el panel de la izquierda.

Hay información disponible en tres fichas:

- La ficha **Administradores** muestra los administradores que se han creado, además de sus roles y ámbitos.
- La ficha **Roles** muestra todos los roles. Para ver información detallada de un rol, selecciónelo en el panel central. La parte inferior de ese panel muestra los tipos de objetos y los permisos asociados al rol. Seleccione la ficha **Administradores** en el panel inferior para ver una lista de los administradores que actualmente tienen ese rol.

- La ficha **Ámbitos** muestra todos los ámbitos, incluidos aquellos generados para los clientes de los socios de Citrix (Citrix Partners).

### Configurar espacios de trabajo

El cliente tiene su propio espacio de trabajo con una URL `customer.cloud.com` única. Este espacio de trabajo es donde los usuarios del cliente acceden a sus aplicaciones y escritorios publicados.

La URL del espacio de trabajo se muestra en dos lugares:

- En el panel de mandos de clientes, seleccione **Configuración de Workspace** en el menú de la esquina superior izquierda.
- En la página de **bienvenida** de Citrix DaaS (la ficha **Vista general**), la URL del espacio de trabajo aparece en la parte inferior de la página.

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 mandos **Supervisar** de un entorno de CSP es esencialmente el mismo que el de un entorno que no es de 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**.

Recuerde que la capacidad de ver las pantallas Supervisar de un cliente se controla mediante el acceso configurado para el administrador. El acceso debe incluir un par de rol y ámbito que incluya el ámbito exclusivo del cliente.

Si ha utilizado roles integrados para configurar el acceso: Los roles integrados determinan si el administrador puede ver las pantallas **Administrar** y **Supervisar**. Si selecciona solamente pares de rol y ámbito de cliente que no incluyen visibilidad de la ficha **Supervisar**, ese administrador no puede ver la ficha **Supervisar** de ninguno de los clientes seleccionados. Por ejemplo, si proporciona a un administrador acceso de **solo lectura para el cliente ABC**, ese administrador no puede ver la ficha **Supervisar** correspondiente al cliente ABC, ya que los administradores de solo lectura no tienen acceso a las pantallas Supervisar.

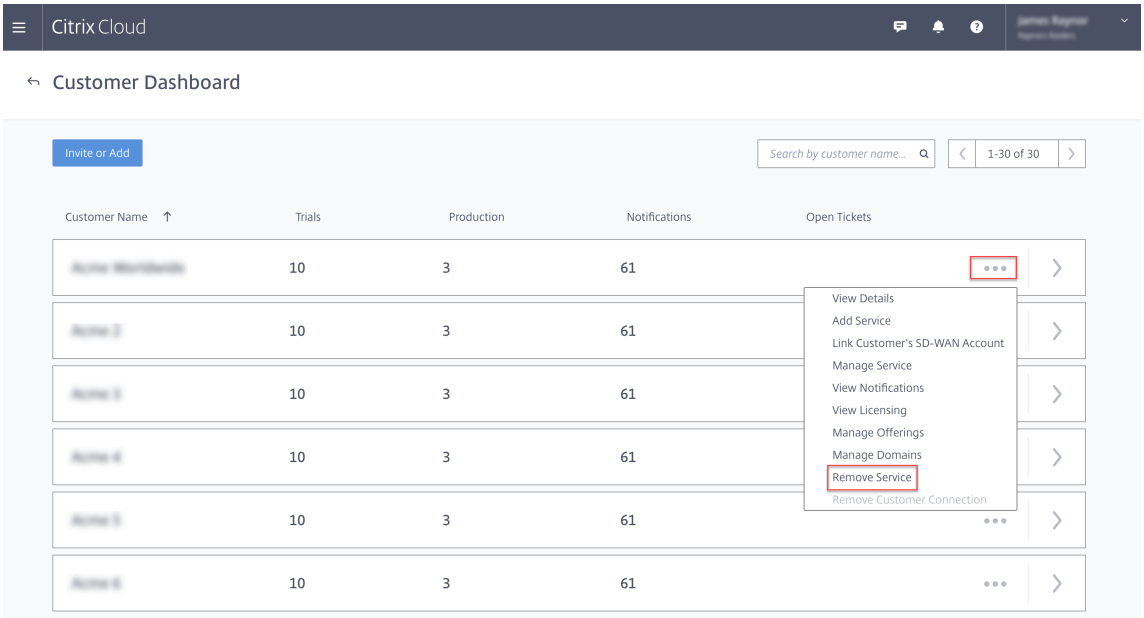
 

## Quitar un servicio

### Requisitos previos

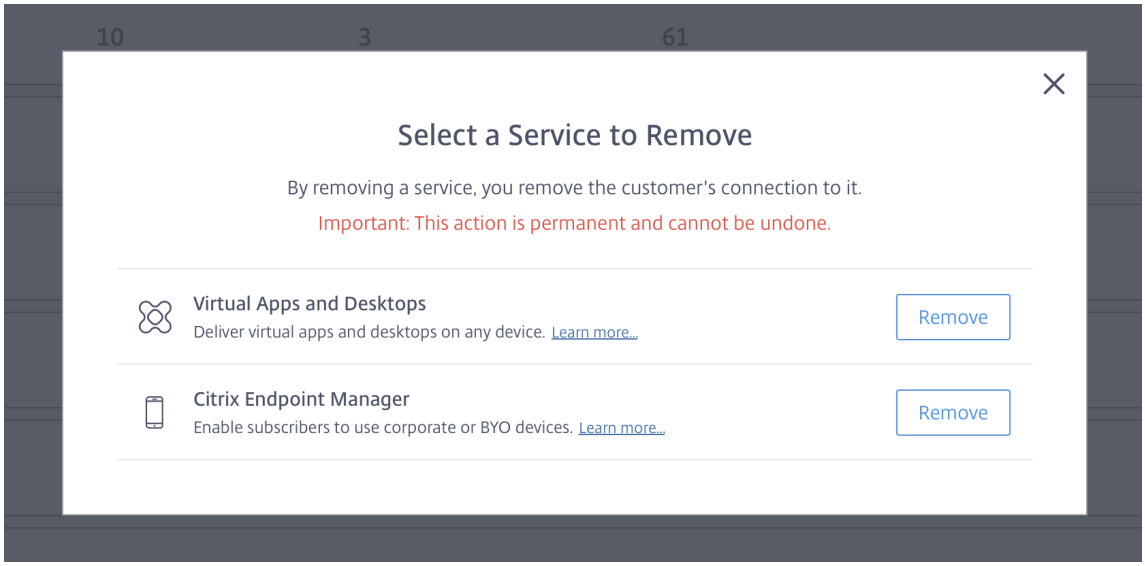
- Asegúrese de que el ámbito del cliente no esté vinculado a ningún objeto de Citrix DaaS. Si están vinculados, no puede quitar el servicio. Para desvincular ámbitos, vaya a **Citrix Studio > Administradores > Ámbitos** y modifique el ámbito.
- Para conocer el ámbito de su cliente y administrarlo, consulte Crear y gestionar ámbitos.

1. Inicie sesión en Citrix Cloud con sus credenciales de Citrix Service Provider.
2. En el **panel de mandos de clientes**, haga clic en el menú de **puntos suspensivos** (…) del cliente del que desea quitar un servicio y seleccione **Quitar servicio**.

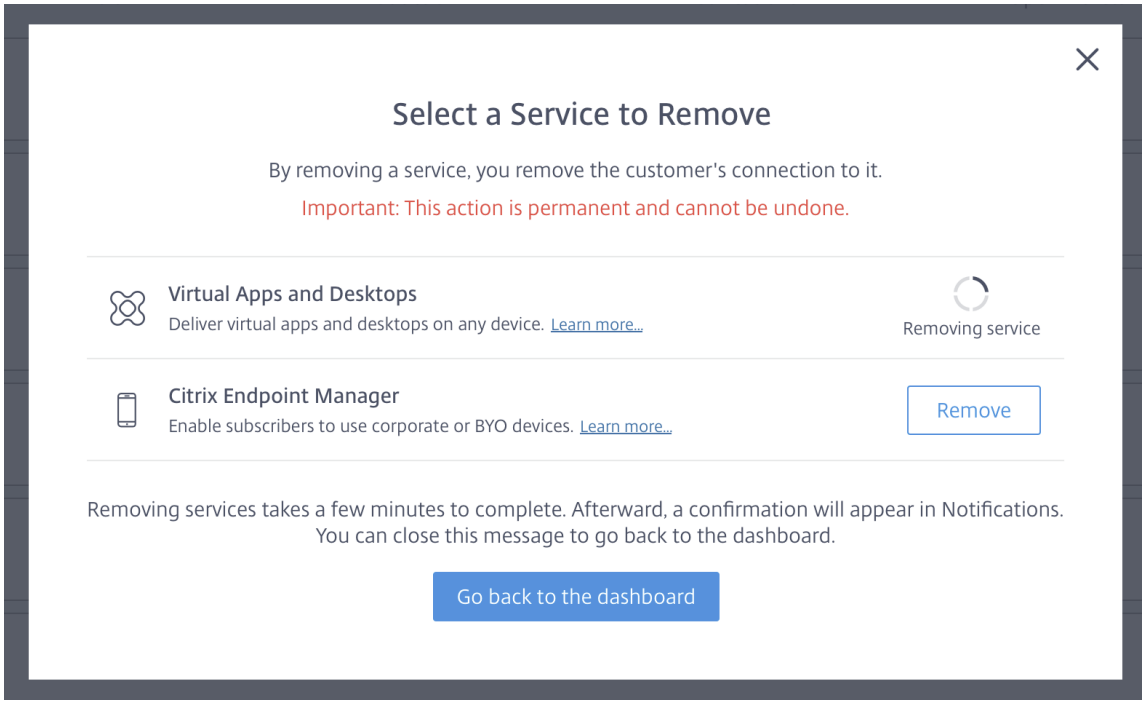



Aparecerá la página **Servicio que quitar**.




3. Haga clic en **Quitar** para quitar el servicio.




## Citrix Gateway service

December 7, 2022

Citrix Gateway proporciona a los usuarios acceso seguro a aplicaciones de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

Citrix Gateway Service permite un acceso remoto seguro a las aplicaciones, sin tener que implementar Citrix Gateway en la zona DMZ ni volver a configurar el firewall. La sobrecarga que provoca en la infraestructura el uso de Citrix Gateway pasa a Citrix Cloud.

Para obtener más información sobre Citrix Gateway Service, consulte la documentación del producto. Ese contenido incluye cómo habilitar Citrix Gateway Service y los problemas conocidos de la versión que esté usando.

Citrix ADC es un controlador de entrega de aplicaciones que analiza el tráfico específico de cada aplicación para distribuir, optimizar y proteger el tráfico de red de Layer 4-Layer 7 (L4–L7) de forma inteligente para aplicaciones web. El dispositivo virtual Citrix ADC VPX se puede alojar en varias plataformas de virtualización y nube. Para obtener información detallada, consulte Implementar una instancia de Citrix ADC VPX.

## SDK y API

December 14, 2023

### SDK de PowerShell remoto de Citrix DaaS

El SDK de PowerShell remoto automatiza las tareas repetitivas y complejas. Proporciona el mecanismo para configurar y administrar el entorno de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) sin utilizar la interfaz de usuario de **Administrar**.

- Los detalles de los cmdlets se proporcionan en Citrix DaaS SDK.
- Los módulos compatibles se detallan en Funciones disponibles y limitaciones. Esa sección también ofrece una lista de los cmdlets que están inhabilitados en el SDK.
- El SDK de PowerShell remoto está disponible para descarga en el sitio web de Citrix.

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

### Qué diferencias hay entre este SDK y el SDK para implementaciones administradas por el cliente

En una implementación de Citrix Virtual Apps and Desktops instalada y administrada por los administradores del cliente, esos administradores ejecutan cmdlets y scripts en un sitio que contiene los VDA y los Delivery Controllers dentro de una estructura de dominio común. En cambio, Citrix DaaS separa los agentes VDA y los Controllers en una ubicación de recursos y el plano de control, respectivamente. Esta división significa que el SDK de PowerShell de Citrix Virtual Apps and Desktops original no

funciona en entornos de Citrix DaaS. No puede cruzar el límite seguro desde la ubicación de recursos hasta el plano de control.

La solución es el SDK de PowerShell remoto de Citrix DaaS. Al ejecutarse en la ubicación de recursos, el SDK de PowerShell remoto accede al plano de control como si fuera local. Esto proporciona la misma funcionalidad que un único sitio de Citrix Virtual Apps and Desktops. Solo existe una capa de comunicación no visible, la más baja, mejorada para funcionar en un solo sitio local o en el entorno de nube. Los cmdlets son los mismos y la mayoría de los scripts no cambian.

El cmdlet `Get-XdAuthentication` proporciona la autorización para cruzar la frontera entre la ubicación de recursos segura y el plano de control. De forma predeterminada, `Get-XdAuthentication` pide a los usuarios las credenciales de CAS. Este cmdlet solo debe utilizarse una vez por sesión de PowerShell. Como alternativa, el usuario puede definir un perfil de autenticación mediante una API de acceso seguro al cliente, creada en la consola de Citrix Cloud. En ambos casos, la información de seguridad se conserva para usarla en llamadas posteriores del SDK de PowerShell. Si este cmdlet no se ejecuta explícitamente, lo llama el primer cmdlet del SDK de PowerShell.

#### Requisitos previos

Para usar Citrix DaaS Remote Powershell SDK, incluya en la lista blanca las siguientes URL:

#### Comerciales

- `https://accounts.cloud.com`
- `https://[service].citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

#### Japón

- `https://accounts.citrixcloud.jp`
- `https://[service].citrixworkspacesapi.jp/[customerid]`
- `https://[customerid].apps.citrixworkspacesapi.jp:443`

#### Gobierno

- `https://accounts.cloud.us`
- `https://[service].citrixworkspacesapi.us/[customerid]`
- `https://[customerid].xendesktop.us:443`

### Instalar y utilizar el SDK de PowerShell remoto

Requisitos y consideraciones:

> **Nota:**
>
> No instale el SDK de PowerShell remoto en una máquina con Citrix Cloud Connector. Se puede instalar en cualquier máquina unida a un dominio dentro de la misma ubicación de recursos.
>
> Citrix no admite la ejecución de los cmdlets de este SDK en Cloud Connectors. La operación del SDK no concierne a los Cloud Connectors.
>
> Si también tiene una implementación de Citrix Virtual Apps and Desktops (además de la implementación de Citrix DaaS), no instale el SDK de PowerShell remoto en ninguna máquina local con Delivery Controllers.

- Instale **Microsoft Edge WebView2**.
- Compruebe que PowerShell 3.0, 4.0 o 5.0 está disponible en la máquina.
- El instalador del SDK descarga e instala .NET Framework 4.8 si no está instalado (o una versión posterior compatible).
- Si la máquina ya tiene instalado el SDK de Citrix Virtual Apps and Desktops, quite ese SDK (de la sección Programas y características de Windows) antes de instalar el SDK de PowerShell remoto.
- En un entorno automatizado, utilice el parámetro `-quiet` para instalar el SDK sin intervención del usuario.

Para instalar el SDK de PowerShell remoto:

1. En la página de descargas, descargue el SDK de PowerShell remoto de Virtual Apps and Desktops.
2. Instale el SDK y ejecútelo.

Los registros de instalación se crean en `%TEMP%\CitrixLogs\CitrixPoshSdk`. Los registros pueden ayudar a resolver problemas de instalación.

Ejecute el SDK en un equipo unido a un dominio dentro de esa ubicación de recursos:

- Abra una ventana de símbolo del sistema de PowerShell. No es necesario ejecutarla como administrador.
- Si quiere utilizar el complemento (en lugar del módulo), agréguelo mediante el cmdlet `Add-PSSnapin` (o `asnp`).
- Puede autenticarse explícitamente mediante el cmdlet `Get-XdAuthentication`. Si no, también puede ejecutar el primer comando del SDK de PowerShell remoto, que le solicitará la misma autenticación que `Get-XdAuthentication`. Si usa un proxy, debe autenticarse en el proxy para poder usar el cmdlet `Get-XdAuthentication`. Para obtener más información, consulte Usar el SDK de PowerShell remoto con un proxy.

- Para omitir la solicitud de autenticación, puede usar el cmdlet `Set-XdCredentials` y crear un perfil de autenticación predeterminado, que accederá mediante un cliente seguro creado en la consola de Citrix Cloud.
- Continúe ejecutando cmdlets del SDK de PowerShell o scripts de automatización del SDK de PowerShell. Aquí tiene un ejemplo.

Para desinstalar el SDK de PowerShell remoto, desde la función de Windows para quitar o cambiar programas, seleccione **Citrix Virtual Apps and Desktops Remote PowerShell SDK**. Haga clic con el botón secundario y seleccione **Desinstalar**. Siga el cuadro de diálogo.

**Usar el SDK de PowerShell remoto con un proxy** Si usa un proxy, es posible que no pueda usar el cmdlet `Get-xdAuthentication` porque el proxy bloquea las solicitudes HTTP que realiza el cmdlet.

Hay dos formas de autenticarse en el proxy. Puede utilizar el parámetro `ProxyUseDefault` o los parámetros `ProxyUsername` y `ProxyPassword`:

- El parámetro `ProxyUseDefault` permite la autenticación en el proxy mediante las credenciales de proxy predeterminadas. Por ejemplo:

```
1 Get-XdAuthentication -ProxyUseDefault
2 <!--NeedCopy-->
```

- Los parámetros `ProxyUsername` y `ProxyPassword` permiten la autenticación en el proxy dentro de la sesión de PowerShell. Por ejemplo:

```
1 $secureString = ConvertTo-SecureString -String "password" -
     AsPlainText -Force
2
3 Get-XdAuthentication -ProxyUsername user1 -ProxyPassword
     $secureString
4 <!--NeedCopy-->
```

#### Actividades de ejemplo

Por actividades comunes, se entiende la configuración de catálogos de máquinas, aplicaciones y usuarios. A continuación, se muestra un script de ejemplo.

```
1     $users = "xd.local\Domain Users"
2
3     $TSVDACatalogName = "TSVDA"
4
5     $TSVDADGName = "TSVDA"
6
7     $TSVDAMachineName = "xd\ds-tsvda2"
8
```

```
    #Create TSVDA Catalog

    $brokerUsers = New-BrokerUser -Name $users

    $catalog = New-BrokerCatalog -Name $TSVDACatalogName -
        AllocationType "Random" -Description $TSVDACatalogName -
        PersistUserChanges "OnLocal" -ProvisioningType "Manual" -
        SessionSupport "MultiSession" -MachinesArePhysical $true

    #Add TSVDA Machine to Catalog

    $BrokeredMachine = New-BrokerMachine -MachineName $TSVDAMachineName
         -CatalogUid $catalog.uid

    #Create new desktops & applications delivery group

    $dg = New-BrokerDesktopGroup -Name $TSVDADGName -PublishedName
        $TSVDADGName -DesktopKind "Shared" -SessionSupport "MultiSession
        " -DeliveryType DesktopsAndApps -Description $TSVDADGName

    #Create notepad application

    New-BrokerApplication -ApplicationType HostedOnDesktop -Name "
        Notepad" -CommandLineExecutable "notepad.exe" -DesktopGroup $dg

    #Assign users to desktops and applications

    New-BrokerEntitlementPolicyRule -Name $TSVDADGName -DesktopGroupUid
         $dg.Uid -IncludedUsers $brokerUsers -description $TSVDADGName

    New-BrokerAccessPolicyRule -Name $TSVDADGName -
        IncludedUserFilterEnabled $true -IncludedUsers $brokerUsers -
        DesktopGroupUid $dg.Uid -AllowedProtocols @("HDX","RDP")

    New-BrokerAppEntitlementPolicyRule -Name $TSVDADGName -
        DesktopGroupUid $dg.Uid -IncludedUsers $brokerUsers -description
         $TSVDADGName

    #Add machine to delivery group

    Add-BrokerMachine -MachineName $TSVDAMachineName -DesktopGroup $dg
<!--NeedCopy-->
```

### Funciones disponibles y limitaciones

El SDK de PowerShell remoto admite los siguientes sistemas operativos:

- Windows 11
- Windows 10
- Windows 10 IoT Enterprise LTSC x32 2019

- Windows 10 IoT Enterprise LTSC x64 2019
- Windows 10 IoT Enterprise 21h1 x64
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

En esta versión, se admiten estos módulos de PowerShell para Citrix Virtual Apps and Desktops:

- Intermediario
- Identidad de Active Directory (AD)
- Creación de máquinas
- Configuración
- Registro de configuraciones
- Host
- Administración delegada
- Análisis

Para obtener información detallada sobre los cmdlets, consulte Citrix Virtual Apps and Desktops SDK.

Tras la autenticación, el acceso remoto será válido en la sesión actual de PowerShell durante 24 horas. Transcurrido ese tiempo, deberá introducir sus credenciales.

El SDK de PowerShell remoto debe ejecutarse en un equipo de la ubicación de recursos.

Los siguientes cmdlets están inhabilitados en las operaciones remotas para mantener la integridad y la seguridad del plano de control de Citrix Cloud.

**Citrix.ADIdentity.Admin.V2:**

- Copy-AcctIdentityPool
- Get-AcctDBConnection
- Get-AcctDBSchema
- Get-AcctDBVersionChangeScript
- Get-AcctInstalledDBVersion
- Remove-AcctServiceMetadata
- Reset-AcctServiceGroupMembership
- Set-AcctDBConnection
- Set-AcctServiceMetadata
- Set-AcctADAccountUserCert
- Test-AcctDBConnection

**Citrix.Analytics.Admin.V1:**

- Get-AnalyticsDBConnection

- Get-AnalyticsDBSchema
- Get-AnalyticsDBVersionChangeScript
- Get-AnalyticsInstalledDBVersion
- Import-AnalyticsDataDefinition
- Remove-AnalyticsServiceMetadata
- Reset-AnalyticsServiceGroupMembership
- Set-AnalyticsDBConnection
- Set-AnalyticsServiceMetadata
- Set-AnalyticsSite
- Set-AnalyticsDBConnection

**Citrix.DelegatedAdmin.Admin.V1:**

- Add-AdminRight
- Get-AdminDBConnection
- Get-AdminDBSchema
- Get-AdminDBVersionChangeScript
- Get-AdminInstalledDBVersion
- Import-AdminRoleConfiguration
- New-AdminAdministrator
- Remove-AdminAdministrator
- Remove-AdminAdministratorMetadata
- Remove-AdminRight
- Remove-AdminServiceMetadata
- Reset-AdminServiceGroupMembership
- Set-AdminAdministrator
- Set-AdminAdministratorMetadata
- Set-AdminDBConnection
- Set-AdminServiceMetadata
- Test-AdminDBConnection

**Citrix.Broker.Admin.V2:**

- Get-BrokerDBConnection
- Get-BrokerDBSchema
- Get-BrokerDBVersionChangeScript
- Get-BrokerInstalledDBVersion
- Get-BrokerLease
- Get-BrokerController
- New-BrokerMachineConfiguration
- Remove-BrokerControllerMetadata
- Remove-BrokerLease

- Remove-BrokerLeaseMetadata
- Remove-BrokerMachineConfigurationMetadata
- Remove-BrokerMachineConfiguration
- Remove-BrokerSiteMetadata
- Remove-BrokerUserFromApplication
- Reset-BrokerLicensingConnection
- Reset-BrokerServiceGroupMembership
- Set-BrokerControllerMetadata
- Set-BrokerDBConnection
- Set-BrokerLeaseMetadata
- Set-BrokerMachineConfiguration
- Set-BrokerMachineConfigurationMetadata
- Set-BrokerSiteMetadata
- Test-BrokerDBConnection
- Test-BrokerLicenseServer
- Update-BrokerBrokerLocalLeaseCache

**Citrix.Configuration.Admin.V2:**

- Export-ConfigFeatureTable
- Get-ConfigDBConnection
- Get-ConfigDBSchema
- Get-ConfigDBVersionChangeScript
- Get-ConfigInstalledDBVersion
- Get-ConfigServiceGroup
- Import-ConfigFeatureTable
- Register-ConfigServiceInstance
- Remove-ConfigRegisteredServiceInstanceMetadata
- Remove-ConfigServiceGroup
- Remove-ConfigServiceGroupMetadata
- Remove-ConfigServiceMetadata
- Remove-ConfigSiteMetadata
- Reset-ConfigServiceGroupMembership
- Set-ConfigDBConnection
- Set-ConfigRegisteredServiceInstance
- Set-ConfigRegisteredServiceInstanceMetadata
- Set-ConfigServiceGroupMetadata
- Set-ConfigServiceMetadata
- Set-ConfigSite
- Set-ConfigSiteMetadata
- Test-ConfigDBConnection

- Unregister-ConfigRegisteredServiceInstance

**Citrix.Host.Admin.V2:**

- Get-HypDBConnection
- Get-HypDBSchema
- Get-HypDBVersionChangeScript
- Get-HypInstalledDBVersion
- Remove-HypServiceMetadata
- Reset-HypServiceGroupMembership
- Set-HypDBConnection
- Set-HypServiceMetadata
- Test-HypDBConnection

**Citrix.ConfigurationLogging.Admin.V1:**

- Get-LogDBConnection
- Get-LogDBSchema
- Get-LogDBVersionChangeScript
- Get-LogInstalledDBVersion
- Remove-LogOperation
- Remove-LogServiceMetadata
- Remove-LogSiteMetadata
- Reset-LogDataStore
- Reset-LogServiceGroupMembership
- Set-LogDBConnection
- Set-LogServiceMetadata
- Set-LogSite
- Set-LogSiteMetadata
- Test-LogDBConnection

**Citrix.MachineCreation.Admin.V2:**

- Get-ProvDBConnection
- Get-ProvDBSchema
- Get-ProvDBVersionChangeScript
- Get-ProvInstalledDBVersion
- Get-ProvServiceConfigurationData
- Remove-ProvServiceConfigurationData
- Remove-ProvServiceMetadata
- Reset-ProvServiceGroupMembership
- Set-ProvDBConnection
- Set-ProvServiceMetadata

- Test-ProvDBConnection

**Citrix.EnvTest.Admin.V1:**

- Get-EnvTestDBConnection
- Get-EnvTestDBSchema
- Get-EnvTestDBVersionChangeScript
- Get-EnvTestInstalledDBVersion
- Remove-EnvTestServiceMetadata
- Reset-EnvTestServiceGroupMembership
- Set-EnvTestDBConnection
- Set-EnvTestServiceMetadata
- Test-EnvTestDBConnection

**Citrix.Monitor.Admin.V1:**

- Get-MonitorConfiguration
- Get-MonitorDBConnection
- Get-MonitorDBSchema
- Get-MonitorDBVersionChangeScript
- Get-MonitorDataStore
- Get-MonitorDataStore
- Get-MonitorInstalledDBVersion
- Remove-MonitorServiceMetadata
- Reset-MonitorDataStore
- Reset-MonitorServiceGroupMembership
- Set-MonitorConfiguration
- Set-MonitorDBConnection
- Set-MonitorServiceMetadata
- Test-MonitorDBConnection

**Citrix.Storefront.Admin.V1:**

- Build-SfCluster
- Get-SfClusters
- Get-SfDBConnection
- Get-SfDBSchema
- Get-SfDBVersionChangeScript
- Get-SfInstalledDBVersion

## Módulo de detección de Citrix DaaS para paquetes y servidores de App-V

Citrix DaaS puede entregar aplicaciones contenidas en paquetes de App-V a sus dispositivos de punto final con uno de estos métodos:

- Método de administración única (acceso a paquetes desde un recurso compartido de red)
- Método de administración dual (acceso a paquetes desde un servidor de administración de Microsoft App-V)

El proceso de registro de paquetes de App-V y servidores de publicación y de administración de Microsoft App-V con la biblioteca de aplicaciones mediante Citrix DaaS difiere ligeramente del registro de paquetes mediante una implementación local. Sin embargo, el proceso de asignar aplicaciones a los usuarios e iniciarlas en el dispositivo de punto final de un usuario es idéntico.

La consola de administración de Citrix DaaS que hay Citrix Cloud no puede ver archivos en una ubicación de recursos. Además, no puede detectar directamente paquetes de App-V o servidores de Microsoft App-V en su infraestructura. El módulo de detección proporciona funciones que detectan la información de los paquetes de App-V en la infraestructura local y cargan la información de los paquetes en Citrix DaaS. La información de los paquetes incluye paquetes de App-V, servidores de Microsoft App-V y las aplicaciones que contienen los paquetes.

El módulo de detección utiliza el SDK de PowerShell remoto de Virtual Apps and Desktops. Puede detectar información de paquetes de un recurso compartido de red o de un servidor de administración de Microsoft App-V. Utilice el módulo de detección en una máquina de su ubicación de recursos.

Requisitos previos para utilizar el módulo de detección:

- Compruebe que PowerShell 3.0 o posterior está disponible en la máquina.
- Compruebe que el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops está instalado en la máquina.
- Compruebe que tiene acceso al recurso compartido de red que contiene los paquetes App-V.
- Compruebe que tiene acceso al servidor donde están instalados los Citrix Cloud Connectors y donde se aloja el servidor de administración de Microsoft App-V.

### Agregar paquetes de App-V a la biblioteca de aplicaciones en Citrix Cloud

Este procedimiento es válido para agregar paquetes de App-V desde recursos compartidos de red (administración única) y para agregar todos los paquetes de App-V publicados desde el servidor de administración de Microsoft App-V (administración dual). Con el método de administración dual, debe administrar los paquetes de App-V agregados al igual que cuando utiliza el método de administración única.

1. Descargue el módulo de detección de la página de descargas de Citrix DaaS: https://www.citrix.com/downloads/citrix-cloud/product-software/xenapp-and-xendesktop-service.html. Extraiga el archivo zip `Citrix.Cloud.AppLibrary.Admin.v1.psm1` en una carpeta.

   > **Nota:**
   >
   > Este archivo también se encuentra en la ISO de Citrix Virtual Apps and Desktops en `Support\Tools\Scripts`. Puede copiarlo localmente o hacer referencia a él directamente desde la unidad de CD.

2. Compruebe que el SDK de PowerShell remoto de Citrix Virtual Apps and Desktops está instalado en la máquina.
3. Vaya a la carpeta que contiene el módulo de detección. En la ventana de PowerShell, introduzca la ruta de acceso completa de la carpeta que contiene el módulo de detección y, a continuación, presione **Entrar**.
4. Importe el módulo de detección con el comando `Import-Module .\Citrix.Cloud.AppLibrary.Admin.v1.psm1`.
5. Agregue los paquetes de App-V a la biblioteca de aplicaciones de Citrix Cloud con uno de los métodos siguientes.

   - Para agregar paquetes de App-V desde un recurso compartido de red, ejecute el cmdlet de PowerShell: `Import-AppVPackageToCloud`.

     Por ejemplo: `Import-AppVPackageToCloud –PackagePath \\AppVSrv\share\Notepad++.appv`

     Para obtener ayuda sobre el cmdlet, escriba `Get-Help Import-AppVPackageToCloud`.

   - Para agregar paquetes de App-V desde un servidor de administración de Microsoft App-V, ejecute el cmdlet de PowerShell: `Import-AppVPackagesFromManagementServerToCloud`

     Por ejemplo: `Import-AppVPackagesFromManagementServerToCloud –ManagementSrvFQDN AppVMngSrv.domain.local`

     Para obtener ayuda sobre el cmdlet, escriba `Get-Help Import-AppVPackagesFromManageme`.

     Este comando importa todos los paquetes de App-V publicados desde el servidor de administración de Microsoft App-V en Citrix Cloud.

     Después de agregar los paquetes de App-V a Citrix Cloud, debe administrarlos como lo haría con el método de administración única.

6. Inicie sesión en Citrix Cloud. Seleccione el cliente de destino. Una vez ejecutado correctamente el script, los paquetes de App-V se agregan a la biblioteca de aplicaciones en Citrix Cloud.

#### Funciones de alto nivel de PowerShell

El módulo contiene las siguientes funciones de alto nivel que puede llamar desde su propio script de PowerShell:

- `Import-AppVPackageToCloud -PackagePath <Full UNC path to App-V package>`

  Detecta y carga en Citrix DaaS toda la información necesaria para publicar aplicaciones desde un único paquete de App-V.

- `Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN <FQDN of a Microsoft App-V Management Server>`

  Descubre las rutas UNC de los paquetes publicados por el servidor de administración y llama a **Import-AppVPackageToCloud** para cada paquete.

  Los paquetes detectados de esta manera se cargan en Citrix DaaS mediante el método de administración única. Citrix DaaS no puede entregar paquetes con el método de administración dual.

- `Import-AppVDualAdminToCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Detecta servidores de publicación y de administración de Microsoft App-V e importa el contenido a la biblioteca de aplicaciones. Este cmdlet importa todos los paquetes administrados mediante el servidor de administración de Microsoft App-V e información relacionada. Los servidores se pueden agregar y quitar a través de PowerShell.

  Este cmdlet agrega paquetes de App-V en el modo de administración dual. Solo se importan los paquetes de App-V que se publican en el servidor de administración de Microsoft App-V y que tienen grupos de AD agregados. Si hace cambios en el servidor de administración de Microsoft App-V, vuelva a ejecutar este cmdlet para sincronizar la biblioteca de aplicaciones con el servidor de administración de Microsoft App-V.

- `Remove-AppVServerFromCloud -ManagementSrvUrl <URL of a Microsoft App-V Management Server> -PublishingServerUrl <URL of a Microsoft App-V Publishing Server>`

  Quita los servidores de publicación y de administración de Microsoft App-V agregados a la biblioteca de aplicaciones.

Este cmdlet quita los servidores de publicación y de administración de Microsoft App-V especificados, además de todos los paquetes de App-V asociados.

Ejecute el módulo de detección para paquetes y servidores de App-V en un equipo unido a un dominio dentro de esa ubicación de recursos: Siga las instrucciones de Instalar y utilizar el SDK de PowerShell remoto para empezar. Continúe ejecutando cmdlets o scripts de PowerShell. Consulte los siguientes ejemplos.

### Actividades de ejemplo

Importe el módulo de detección de paquetes de App-V de Citrix DaaS.

```
import-module "D:\Support\Tools\Scripts\Citrix.Cloud.AppLibrary.Admin.v1.psm1"
<!--NeedCopy-->
```

Recorrer el directorio del almacén de paquetes de App-V y cargar cada paquete.

```
Get-ChildItem -Path "\FileServer.domain.net\App-V Packages" -Filter *.appv |
Foreach-Object{

    Import-AppVPackageToCloud -PackagePath $_.FullName
 }

<!--NeedCopy-->
```

Detectar y cargar paquetes registrados con un servidor de administración de Microsoft App-V.

```
Import-AppVPackagesFromManagementServerToCloud -ManagementSrvFQDN AppVManagementServer.domain.net
<!--NeedCopy-->
```

Detectar los servidores de publicación y de administración de Microsoft App-V y agregar la configuración a la biblioteca de aplicaciones. Esto también importa todos los paquetes administrados por el servidor de administración de Microsoft App-V en el modo de administración dual.

```
Import-AppVDualAdminCloud -ManagementSrvUrl http://AppVManagementServer.domain.net  – PublishingServerUrl http://AppVManagementServer.domain.net:8001
<!--NeedCopy-->
```

Consultar la documentación de ayuda de PowerShell incluida en el módulo.

```
Get-Help Import-AppVPackageToCloud
<!--NeedCopy-->
```

### Limitaciones

- No puede detectar paquetes de App-V en la infraestructura de la ubicación de recursos directamente desde la consola de administración de Citrix DaaS que hay en Citrix Cloud. Para obtener más información sobre Citrix Cloud, consulte la documentación de Citrix Cloud.
- La consola de administración de Citrix DaaS que hay en Citrix Cloud no tiene una conexión activa con el servidor de administración de App-V de Microsoft. Los cambios en los paquetes y otra configuración en el servidor de administración de App-V de Microsoft no se reflejan en la consola de administración de Citrix DaaS hasta que `Import-AppVDualAdminCloud` se ejecuta de nuevo.

## API de OData para Monitor Service

Además de utilizar las funciones de Monitor para mostrar datos históricos, puede consultar datos mediante la API de Monitor Service. Utilice la API para:

- Analizar tendencias históricas para planificaciones
- Realizar informes de error detallados sobre problemas de máquina y conexión
- Extraer información para insertarla en otras herramientas y procesos; por ejemplo, mediante las tablas de PowerPivot de Microsoft Excel para mostrar los datos de diferentes formas
- Generar una interfaz de usuario personalizada en la parte superior de los datos que proporciona la API

Para obtener más información, consulte API OData de Monitor Service. Para acceder a la API de Monitor Service, consulte Access Monitor Service data using the OData v4 endpoint in Citrix Cloud.

## Las API de Citrix DaaS

Las API de Citrix DaaS están disponibles en https://developer.cloud.com/citrixworkspace/citrix-daas.

## Renuncia de responsabilidades

Este software o código de muestra se proporciona "tal cual", sin ningún tipo de declaración, garantía ni condición. Puede utilizarlo, modificarlo y distribuirlo bajo su propio riesgo. CITRIX RENUNCIA A TODAS LAS GARANTÍAS, EXPRESAS, IMPLÍCITAS, ESCRITAS, ORALES O LEGALES, INCLUIDAS, ENTRE OTRAS, GARANTÍAS DE COMERCIABILIDAD, IDONEIDAD PARA UN PROPÓSITO PARTICULAR, TÍTULO Y NO INFRACCIÓN. Sin limitar el carácter general de lo anteriormente expuesto, Ud. reconoce y acepta (a) que el software o código de muestra puede presentar errores, fallos de diseño o cualquier otro problema, que pueden provocar una pérdida de datos o daños materiales; (b) que puede que no sea

posible hacer funcionar por completo el software o código de muestra; y (c) que sin previo aviso y sin responsabilidad respecto a Ud., Citrix puede dejar de poner a su disposición la versión actual o las versiones futuras de este software o código de muestra. El software o código de muestra no debe utilizarse en ningún caso para dar apoyo a actividades de riesgo extremo, incluidas, a título enunciativo, actividades de explosión o de soporte vital. NI CITRIX NI SUS AFILIADOS O AGENTES SERÁN RESPONSABLES, POR INCUMPLIMIENTO DE CONTRATO O CUALQUIER OTRO PRINCIPIO DE RESPONSABILIDAD, DE CUALQUIER DAÑO QUE SE PRODUZCA DEL USO DEL SOFTWARE/CÓDIGO DE MUESTRA, INCLUIDOS PERO SIN LIMITACIÓN, DAÑOS DIRECTOS, ESPECIALES, INCIDENTALES, PUNITIVOS, CONSECUENTES O DE OTRO TIPO, AUNQUE SE INFORME DE LA POSIBILIDAD DE TALES DAÑOS. Ud. acepta indemnizar y defender a Citrix contra cualquier tipo de reclamación relativa al uso, modificación o distribución del código.