

Azure Virtual Desktop:

guía de migración
a Servicios de
Escritorio remoto

Índice

Introducción 3

- ¿Por qué considerar una VDI en el cloud? 3
- ¿Por qué migrar a Azure Virtual Desktop? 4

Preparación de la migración 6

- Paso 1: Requisitos previos 7
- Paso 2: Configuración de Azure Migrate 7
- Paso 3: Detectar máquinas virtuales 8
- Paso 4: Revisar la evaluación 10

Creación del entorno de Azure Virtual Desktop 13

- Requisitos previos 13
- Consideraciones 15
- Optimizar el coste 16
- Directrices de red 17
- Directrices de administración de perfiles 18
- Windows 10 multisesión 18
- Convenciones de nomenclatura 19
- Orientación para la implementación 19
- Paso 5: Replicar máquinas virtuales 23
- Paso 6: Migración de prueba 23
- Paso 7: Migrar a producción 24

Prueba y preparación de la implementación de Azure Virtual Desktop 25

- Confirmación del estado de implementación de Azure Virtual Desktop 25
- Estado del grupo de hosts de Azure Virtual Desktop 26
- Instrucciones para probar las implementaciones de Azure Virtual Desktop 26
- Preparativos finales para la puesta en marcha 27

Pasos para la puesta en marcha e implementación posterior 28

- Confirmación del estado y el uso de Azure Virtual Desktop.. 28
- Consideraciones y pasos posteriores a la implementación 29
- Limpieza de una implementación de RDS 30

Orientación sobre las capacidades adicionales 31

- Escalado automático 31
- Acceso condicional 32
- Supervisión 33
- Automatización 34
- Azure Advisor 35
- Microsoft Teams 35
- Conexión de aplicaciones MSIX 36

Conclusión 37

- Resumen 37
- Recursos 37

Glosario 39

Acerca del autor 40

Introducción

¿Por qué considerar una VDI en el cloud?

A medida que las empresas se adaptan a las nuevas formas de trabajo y evalúan la manera de aportar resiliencia a sus negocios, cada vez es más importante permitir una experiencia de escritorio segura y remota a la que se pueda acceder desde cualquier lugar.

El enfoque de **infraestructura del escritorio virtual (VDI)** se aprovecha a menudo para ofrecer una experiencia de escritorio remoto a los empleados y a menudo se ofrece a través de **Servicios de Escritorio remoto (RDS)**. Sin embargo, como una solución on-premises, RDS no obtiene el valor total de la modernización o de las ventajas de una VDI en el cloud.

Azure Virtual Desktop es una solución administrada de entrega de VDI hospedada en Microsoft Azure, que te ofrece la escalabilidad del cloud. Azure Virtual Desktop no solo es compatible con Windows Server, sino que también proporciona Windows 10 Enterprise multisesión, combinando la experiencia de Windows 10 con la capacidad de ejecutar múltiples sesiones de usuario simultáneas que antes solo estaba disponible en Windows Server. También obtienes una experiencia optimizada para las aplicaciones de Microsoft 365, incluido Microsoft Teams y una mayor seguridad para los usuarios, las aplicaciones de la empresa y los datos. Además, con programas como [App Assure](#), podrás modernizar y reducir los costes asociados a tres pilares diferentes. En la *figura 1* se muestran estos pilares y se incluyen las diversas áreas en las que se pueden reducir los costes.

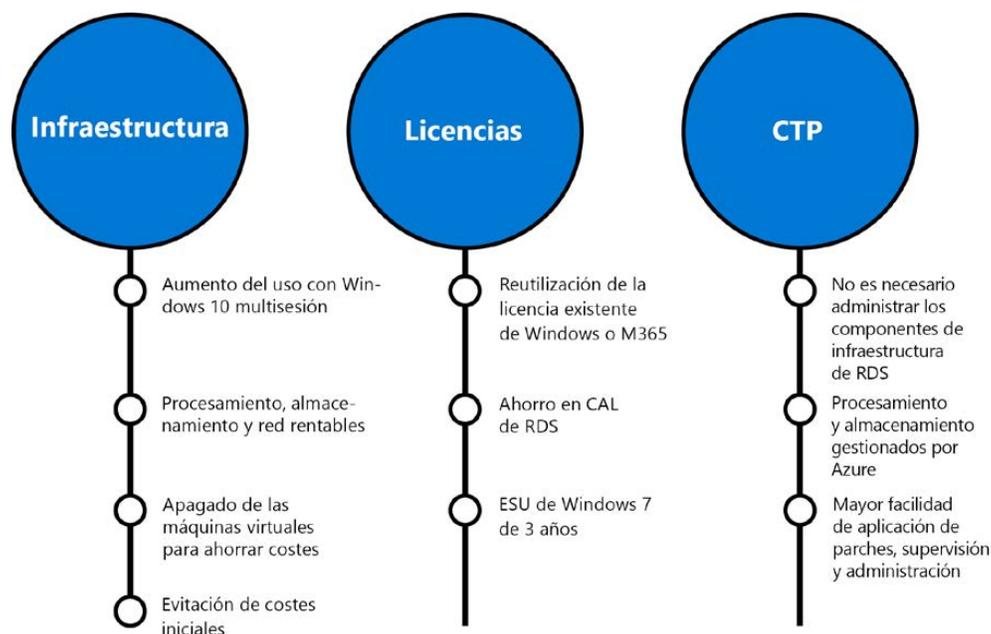


Figura 1: Los pilares del ahorro de costes de Azure Virtual Desktop

Además de permitir el trabajo remoto y el ahorro en infraestructura, licencias y **coste total de propiedad (TCO)**, Azure Virtual Desktop también aporta otras ventajas a tu empresa, como la administración de TI simplificada, las capacidades de seguridad que mantienen protegidos a tus usuarios, datos y organización, y protección contra interrupciones con las tecnologías integradas Azure Site Recovery y Azure Backup.

¿Por qué migrar a Azure Virtual Desktop?

Si tienes RDS y estás considerando la posibilidad de migrar a una solución de Microsoft, puedes migrar a un enfoque de **infraestructura como servicio (IaaS)** con Azure o migrar directamente a Azure Virtual Desktop.

Para entender las diferencias entre RDS on-premises, la migración a Azure y la migración a Azure Virtual Desktop, echa un vistazo a la *tabla 1*. Aunque RDS te proporciona flexibilidad, también incluye una enorme lista de responsabilidades. Con un entorno RDS, eres esencialmente responsable de la administración y el mantenimiento de todos los componentes necesarios. La migración a RDS aumenta la responsabilidad proporcionada por Microsoft; sin embargo, al migrar a Azure Virtual Desktop, Microsoft también administra automáticamente el plano de control de la virtualización. Esto te permite cambiar tu enfoque a lo que es realmente importante para ti: la experiencia de usuario final percibida.

Responsabilidad	RDS on-premises	RDS en Azure	Azure Virtual Desktop
Identidad	Cliente	Microsoft	Microsoft
Dispositivos de usuario final (móviles y PC)	Cliente	Microsoft	Microsoft
Seguridad de aplicaciones	Cliente	Microsoft	Microsoft
Sistema operativo del host de sesión	Cliente	Microsoft	Microsoft
Configuración de la implementación	Cliente	Microsoft	Microsoft
Controles de red	Cliente	Microsoft	Microsoft
Plano de control de virtualización	Cliente	Microsoft	Microsoft
Hosts físicos	Cliente	Microsoft	Microsoft
Red física	Cliente	Microsoft	Microsoft
Centro de datos físico	Cliente	Microsoft	Microsoft

Tabla 1: Responsabilidades

Este e-book es una guía para ayudar a las organizaciones a migrar las infraestructuras de RDS existentes a Azure Virtual Desktop. En él se describe cómo beneficiarse plenamente de Azure Virtual Desktop y de Azure en general, y se ofrece orientación sobre los siete pasos para migrar tus cargas de trabajo de RDS a Azure Virtual Desktop.

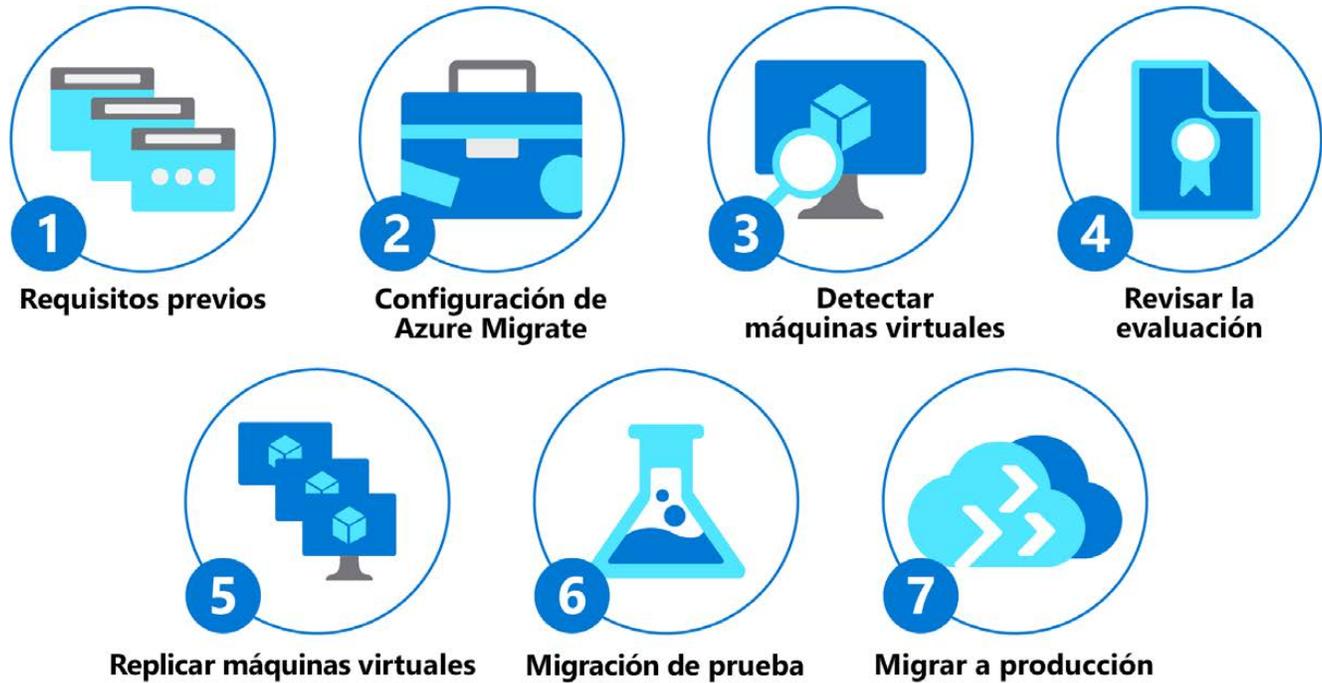


Figura 2: El plan de migración en siete etapas

En la *figura 2* se muestran los siete pasos aconsejados para permitir un proceso de migración sin problemas de RDS a Azure Virtual Desktop. Este e-book te guiará por este proceso de migración de siete pasos. En el próximo capítulo, veremos en detalle cómo implementar estos siete pasos.

Preparación de la migración

En el capítulo anterior, presentamos el enfoque de siete pasos para migrar tus cargas de trabajo de RDS a Azure Virtual Desktop. El paso 1 consiste en reunir los requisitos necesarios para empezar a migrar las cargas de trabajo a Azure Virtual Desktop. En el paso 2, se instala y configura Azure Migrate como la herramienta para migrar las cargas de trabajo existentes. Usando Azure, se detectan las **máquinas virtuales (MV)** en el paso 3. Esta detección lleva a una evaluación de revisión en el paso 4, que permite examinar los detalles de la replicación. Cuando se acepte la evaluación de la revisión, las MV se replicarán en Azure como parte del paso 5. Una vez replicadas, puedes empezar a probar tus cargas de trabajo en el paso 6. Después de una prueba correcta, migrarás y pondrás Azure Virtual Desktop en producción.

Este e-book te guiará por este proceso de migración de siete pasos. Estos pasos se basan en Azure Migrate, que puede utilizarse para migrar también otras cargas de trabajo on-premises a Azure. Azure Migrate ofrece muchas ventajas, incluidas evaluaciones para la preparación, el tamaño y la estimación de costes. También contiene una migración integrada que ofrece un tiempo de inactividad casi nulo. Se te ofrece una experiencia integrada con el seguimiento del progreso de principio a fin. Para obtener más información y orientación sobre Azure Migrate, visita [esta página](#).

En este capítulo, explicaremos los primeros cuatro pasos que forman parte del enfoque de siete pasos que presentamos antes para comenzar a migrar tus cargas de trabajo de RDS a Azure Virtual Desktop.



Figura 3: Los primeros cuatro pasos del proceso de migración



Paso 1: Requisitos previos

En primer lugar, se requiere una [suscripción a Azure](#). Si tu organización ya tiene una, asegúrate de tener el nivel correcto de permisos. Durante esta migración, necesitas permiso para trabajar con componentes de almacenamiento y redes, y, por supuesto, con máquinas virtuales. Asegúrate de que los servicios de dominio, como Active Directory o Azure Active Directory Domain Services, estén sincronizados con **Azure Active Directory (Azure AD)**. Asegúrate de que el servicio de dominio sea accesible desde la suscripción a Azure y la red virtual que se conectará donde se implementará Azure Virtual Desktop. Sigue la guía de [Azure AD Connect](#) para sincronizar Active Directory on-premises con Azure AD.



Paso 2: Configuración de Azure Migrate

Ahora podemos empezar a crear el proyecto de Azure Migrate. En el portal de Azure, hay un asistente dedicado que te permite configurar Azure Migrate para Azure Virtual Desktop. Se puede encontrar en la sección llamada **VDI**, como se muestra en la *figura 4*:

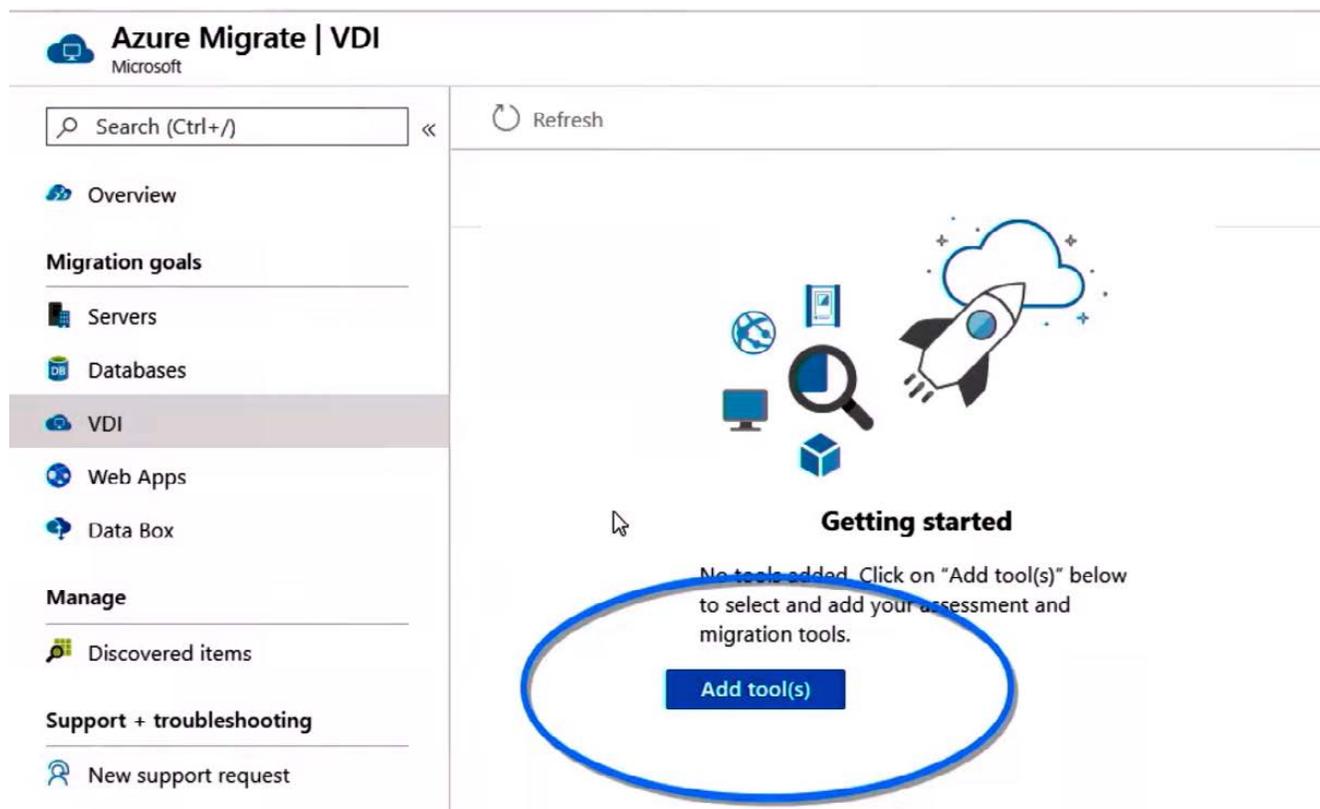


Figura 4: Iniciar el asistente de Azure Migrate

En este asistente, se configuran la suscripción, el grupo de recursos, el nombre del proyecto y la ubicación geográfica. Comienza la evaluación del entorno actual del RDS seleccionando **Registrar**.

En este paso, se crea un nuevo proyecto de Azure Migrate en la suscripción a Azure de destino. Esta suscripción debe cumplir los requisitos previos descritos en el paso 1. A continuación, selecciona la opción de evaluar y migrar servidores, selecciona **VDI** y añade una herramienta. Después de configurar los parámetros básicos, como la suscripción, el grupo de recursos y la ubicación, asegúrate de seleccionar **Azure Migrate: Migración de servidor** como herramienta de migración. El asistente de configuración también te permitirá seleccionar herramientas opcionales de partners del ecosistema que proporcionan ventajas adicionales además de la migración del servidor. Según el ejemplo, puedes seleccionar **Lakeside SysTrack** como la herramienta de evaluación, además de Azure Migrate como la herramienta de migración. Lakeside es un partner del ecosistema que se especializa en la evaluación de los entornos de RDS y VDI. Lakeside SysTrack proporciona un conocimiento profundo sobre tu carga de trabajo actual para ayudarte a determinar el tamaño y el uso. Además de RDS de Microsoft, también admite los entornos VMware y Citrix para ayudarte a evaluar dichos entornos para migrarlos a Azure. Después de conectar Azure Migrate y las herramientas opcionales de los partners del ecosistema y aceptar los permisos solicitados, comienza el proceso de detección.



Paso 3: Detectar máquinas virtuales

Durante esta fase, se detectará y evaluará el servidor host de sesión de Escritorio remoto de tu entorno actual. Durante este paso, vamos a recopilar mucha información sobre tu infraestructura actual. Si has seleccionado Lakeside SysTrack como tu herramienta de evaluación en el paso anterior, esto te ayudará a recopilar aún más información sobre tu actual carga de trabajo de RDS. Lakeside SysTrack requiere un agente que puedes instalar fácilmente con tus herramientas de implementación existentes. En la *figura 5* se muestra Lakeside SysTrack Visualizer, que facilita la ingesta de los inventarios de uso, consumo y aplicaciones actuales, y te ayuda a determinar el tamaño de tus máquinas virtuales de Azure Virtual Desktop, entre otras muchas cosas.



Figura 5: Ejemplo de Lakeside SysTrack Visualizer

Como parte de este paso, también se recopilan conocimientos sobre cualquier carga de trabajo back-end de la aplicación que tal vez quieras o no migrar a Azure. Normalmente, trasladar esos back-ends de aplicación a Azure garantiza el mejor rendimiento, porque, en ese escenario, el lado de cliente de la aplicación que se ejecuta en Azure Virtual Desktop estará más cerca del back-end de aplicación. Azure Migrate también puede ayudarte a migrar estas cargas de trabajo a Azure. Si decides no migrar algunos de estos recursos back-end, asegúrate de configurar la conectividad con tu entorno on-premises utilizando ExpressRoute o una VPN de sitio a sitio. Los pasos detallados sobre la detección se pueden encontrar [aquí](#).

📄 **Paso 4: Revisar la evaluación**

Cuando se obtiene una cantidad de datos suficiente, se pueden revisar los datos de evaluación para determinar la mejor ruta de migración. Estos datos de evaluación incluyen los datos de evaluación sin procesar del escritorio y los datos desglosados en diferentes roles de usuario. A medida que analizas los datos, puedes determinar el uso más rentable de los recursos de Azure Virtual Desktop tanto agrupados como personales. La información recopilada como parte del paso 3 está visible en tu Azure Portal. En la figura siguiente se muestra un ejemplo que contiene la información que se recopila. Se incluye información como la siguiente:

- El número de usuarios en cada rol
- Aplicaciones en uso por parte de los usuarios
- Consumo de recursos por usuario
- Medias de utilización de recursos por rol de usuario
- Datos de rendimiento del servidor VDI
- Informes de usuarios simultáneos
- Principales paquetes de software en uso

User name	User account	Devices used	Total application co...	OS Used	Multi user Windows...	Persona	Target Azure VM size	Is ready for migrati...	Target location	Target
User3	FAREAST\user3	UserVM-3.domain.org	4	Windows 10	No	Persona3	Standard_F2s_v2	Yes	West Central US	Standa
User11	FAREAST\user11	UserVM-11.domain...	4	Windows 10	No	Persona11	Standard_F2s_v2	Yes	West Central US	Standa
User10	FAREAST\user10	UserVM-10.domain...	4	Windows 10	No	Persona10	Standard_F2s_v2	Yes	West Central US	Standa
User1	FAREAST\user1	UserVM-1.domain.org	4	Windows 10	Yes	Persona1	Standard_F2s_v2	Yes	West Central US	Standa
User2	FAREAST\user2	UserVM-2.domain.org	4	Windows 10	No	Persona2	Standard_F2s_v2	Yes	West Central US	Standa
User14	FAREAST\user14	UserVM-14.domain...	4	Windows 10	Yes	Persona14	Standard_F2s_v2	Yes	West Central US	Standa
User4	FAREAST\user4	UserVM-4.domain.org	4	Windows 10	No	Persona4	Standard_F2s_v2	Yes	West Central US	Standa
User6	FAREAST\user6	UserVM-6.domain.org	4	Windows 7	No	Persona6	Standard_F2s_v2	Yes	West Central US	Standa
User13	FAREAST\user13	UserVM-13.domain...	4	Windows 7	No	Persona13	Standard_F2s_v2	Yes	West Central US	Standa
User5	FAREAST\user5	UserVM-5.domain.org	4	Windows 10	No	Persona5	Standard_F2s_v2	Yes	West Central US	Standa
User12	FAREAST\user12	UserVM-12.domain...	4	Windows 10	No	Persona12	Standard_F2s_v2	Yes	West Central US	Standa
User17	FAREAST\user17	UserVM-17.domain...	4	Windows 10	No	Persona17	Standard_F2s_v2	Yes	West Central US	Standa
User9	FAREAST\user9	UserVM-9.domain.org	4	Windows 10	No	Persona9	Standard_F2s_v2	Yes	West Central US	Standa
User28	FAREAST\user28	UserVM-28.domain...	4	Windows 10	Yes	Persona28	Standard_F2s_v2	Yes	West Central US	Standa
User7	FAREAST\user7	UserVM-7.domain.org	4	Windows 10	Yes	Persona7	Standard_F2s_v2	Yes	West Central US	Standa
User20	FAREAST\user20	UserVM-20.domain...	4	Windows 7	No	Persona20	Standard_F2s_v2	Yes	West Central US	Standa
User18	FAREAST\user18	UserVM-18.domain...	4	Windows 10	No	Persona18	Standard_F2s_v2	Yes	West Central US	Standa
User15	FAREAST\user15	UserVM-15.domain...	4	Windows 10	Yes	Persona15	Standard_F2s_v2	Yes	West Central US	Standa

Figura 6: Ejemplo de resultados de la evaluación

Se pueden encontrar los pasos detallados sobre la evaluación [aquí](#).

En cuanto a las máquinas virtuales de host de sesión, según los resultados que has analizado como parte de la evaluación y en función de si quieres beneficiarte de Windows 10 multisesión o seguir usando Windows Server, tienes dos opciones:

Puedes elegir migrar ("lift and shift") los servidores host de sesión de Escritorio remoto existentes on-premises a Azure y transformarlos en servidores host de sesión de Azure Virtual Desktop. En ese caso, se usa la opción **Detectar** en las herramientas de **Azure Migrate: Migración de servidor**. Esto permite convertir un dispositivo en su entorno, que va a administrar la replicación de las máquinas, a Azure Virtual Desktop. El proveedor de replicación se descarga, instala y registra en el proyecto de Azure Migrate para iniciar la replicación en Azure. Como la replicación de los hosts en Azure Blob Storage ya ha comenzado, puedes dejar que se realice la replicación hasta que se vayan a probar las MV y, después, migrarlas a producción. Cuando las máquinas empiecen a ejecutarse en Azure, asegúrate de instalar el agente de máquina virtual de Azure Virtual Desktop en cada servidor de sesión. Como parte de la instalación, debes introducir un token de registro para que el entorno de Azure Virtual Desktop asocie el servidor con el entorno correcto. Como último paso antes de la migración final, debes asignar usuarios y grupos a los grupos de aplicaciones apropiados.

También puedes crear una nueva plantilla de imagen basada en Windows 10 multisesión para aprovechar todas las ventajas que incluye el sistema operativo. Para la creación de una nueva plantilla, Windows 10 Enterprise multisesión está disponible en la galería de imágenes de Azure. Hay dos opciones para personalizar esta imagen:

- a. La primera opción es aprovisionar una máquina virtual en Azure y luego pasar a la [preparación e instalación del software](#).
- b. La segunda opción es crear la imagen localmente descargando la imagen, suministrando una máquina virtual de Hyper-V y personalizándola para que se ajuste a tus necesidades.

Para obtener una guía completa paso a paso sobre cómo preparar, crear e implementar imágenes de plantilla personalizadas para Azure Virtual Desktop, consulta [esta guía](#).

Antes de continuar con el paso 5, ha llegado el momento de empezar a crear tu entorno de Azure Virtual Desktop. En este paso, crearás los componentes de Azure Virtual Desktop y prepararás tu suscripción de Azure. En este paso se crearán tres objetos de Azure diferentes en tu suscripción a Azure: el grupo de hosts, el área de trabajo y el grupo de aplicaciones. Se explican a continuación:

- Los **grupos de hosts** son una colección de una o más máquinas virtuales idénticas en entornos de Azure Virtual Desktop. Cada grupo de hosts puede contener un grupo de aplicaciones, que a su vez contiene una aplicación o un escritorio con el que los usuarios pueden interactuar como lo harían en un escritorio físico.
- El proceso de configuración del grupo de hosts crea un grupo de aplicaciones de escritorio de forma predeterminada. Para que el grupo de hosts funcione del modo previsto, debes asignar este grupo de aplicaciones a usuarios o grupos de usuarios, y debes registrar el grupo de aplicaciones en un **área de trabajo**.
- El **grupo de aplicaciones** predeterminado creado para un nuevo grupo de hosts de Azure Virtual Desktop también publica el escritorio completo. Además, puedes crear uno o más grupos de aplicaciones RemoteApp para el grupo de hosts.

En el capítulo 3, hablamos de los requisitos previos y las consideraciones que es importante conocer antes de crear la implementación de Azure Virtual Desktop. En el capítulo 3, también explicaremos algo más sobre las opciones de implementación y te guiaremos por el proceso general de implementación.

Creación del entorno de Azure Virtual Desktop

Requisitos previos

Ahora que has seguido el proceso de migración como parte de los pasos descritos anteriormente, explicaremos la creación del entorno de Azure Virtual Desktop con mayor detalle. Antes de hacerlo, debes disponer de algunas cosas. En esta sección se examinan esos requisitos. Asegúrate de cumplir con estos requisitos antes de comenzar a implementar Azure Virtual Desktop y migrar tus cargas de trabajo de RDS.

En lo que respecta a los sistemas operativos para los servidores host de sesión como parte de los grupos de hosts de Azure Virtual Desktop, hay una lista de sistemas operativos compatibles. Dependiendo del sistema operativo que selecciones, también se requieren licencias apropiadas para los usuarios que se conecten a los escritorios y las aplicaciones. Asegúrate de que todos los usuarios a los que se les permite el acceso a cualquier recurso en Azure Virtual Desktop dispongan de la licencia necesaria. En la *tabla 2* se muestran las licencias necesarias para cada sistema operativo. [Aquí](#) puedes obtener más información sobre las licencias necesarias.

Sistema operativo	Licencia necesaria
Windows Server 2012 R2, 2016, 2019	Licencia de acceso de cliente (CAL) de RDS con Software Assurance
Windows 7 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 10 Enterprise multisesión o Windows 10 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5

Tabla 2: Sistemas operativos y licencias necesarias

Además, tu infraestructura necesita lo siguiente para admitir Azure Virtual Desktop:

- Debe haber una instancia de Azure AD.
- Una instancia de Windows Server AD que esté sincronizada con Azure AD. Puedes implementarla basada en Azure AD Connect (ideal para organizaciones híbridas) o en Azure AD Domain Services (ideal para organizaciones híbridas o en el cloud). En cuanto a los orígenes de identidad y la pertenencia al dominio de los servidores host de sesión de Azure Virtual Desktop, puedes seleccionar una de las siguientes opciones:
 - Puedes usar Windows Server AD sincronizado con Azure AD, en cuyo caso las cuentas de usuario se obtienen de Windows Server AD. La máquina virtual de host de sesión de Azure Virtual Desktop está unida al dominio de Windows Server AD.
 - Puedes usar Windows Server AD sincronizado con Azure AD, en cuyo caso las cuentas de usuario se obtienen de Windows Server AD. La máquina virtual de host de sesión de Azure Virtual Desktop está unida a Azure AD Domain Services.
 - Puedes usar el dominio de Azure AD Domain Services, en cuyo caso el usuario se obtiene de Azure AD. La máquina virtual de host de sesión de Azure Virtual Desktop está unida a un dominio de Azure AD Domain Services.
 - Se requiere una suscripción a Azure, que debe estar relacionada con el mismo inquilino de Azure AD que contiene la red virtual. La red virtual debe tener acceso a la instancia de Windows Server AD o Azure AD Domain Services.

El usuario que se conecte a Azure Virtual Desktop debe cumplir los siguientes requisitos:

- El usuario debe proceder del mismo AD que está conectado a Azure AD. Azure Virtual Desktop no admite cuentas B2B o MSA.
- El nombre principal de usuario (UPN) que utilizas para suscribirte a Azure Virtual Desktop debe existir en el dominio de AD al que está unida la máquina virtual.

- Las máquinas virtuales de host de sesión de Azure Virtual Desktop que creas como parte del grupo de hosts de Azure Virtual Desktop deben estar [unidas a un dominio estándar](#) o a un [AD híbrido](#). Las máquinas virtuales no pueden estar unidas solo a Azure AD por el momento. Está previsto que las máquinas virtuales de host de sesión de Azure Virtual Desktop unidas a Azure AD se admitan más adelante. Y, como se ha indicado antes, el servidor host de sesión de Azure Virtual Desktop debe ejecutar uno de los sistemas operativos compatibles:
 - Windows 10 Enterprise multisesión, versión 1809 o posterior
 - Windows 10 Enterprise, versión 1809 o posterior
 - Windows 7 Enterprise
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2

Azure Virtual Desktop no es compatible con las imágenes de los sistemas operativos x86 (32 bits), Windows 10 Enterprise N o Windows 10 Enterprise KN. Windows 7 tampoco es compatible con ninguna solución de perfil basada en discos duros virtuales (VHD) o VHDX hospedada en Azure Storage administrado. Las opciones de automatización e implementación disponibles dependen del sistema operativo y de la versión que elijas, como se indica en este artículo sobre los [sistemas operativos compatibles](#).

Si bloqueas de forma activa el tráfico saliente de los servidores host de sesión de Azure Virtual Desktop, deberás desbloquear direcciones URL específicas para que la implementación de Azure Virtual Desktop funcione correctamente. Las máquinas virtuales de Azure que crees para Azure Virtual Desktop deben tener acceso a las URL que aparecen en la [lista de URL seguras](#).

Consideraciones

Limitaciones

Al implementar Azure Virtual Desktop, hay un par de limitaciones técnicas que debes tener en cuenta. Evalúa y revisa estas limitaciones antes de implementar Azure Virtual Desktop en tu entorno. Una lista actualizada de estas limitaciones se puede encontrar [aquí](#).

Optimizar el coste

Para aprovechar al máximo Azure Virtual Desktop, te aconsejamos que consideres las diferentes formas de ahorrar costes. Encontrarás seis formas de ahorrar costes en la implementación de Azure Virtual Desktop en la siguiente lista:

- Usa Windows 10 multisesión como sistema operativo de tus servidores host de sesión de Azure Virtual Desktop. Al aprovechar una experiencia de escritorio multisesión para los usuarios que tienen idénticos requisitos de procesamiento, puedes permitir que más usuarios inicien sesión en una sola máquina virtual a la vez. Esto conlleva un considerable ahorro de costes de consumo de Azure para las MV que se están ejecutando. Las [preguntas frecuentes de Windows 10 Enterprise multisesión](#) contienen información más detallada si quieres obtener más indicaciones.
- Aprovecha Ventaja híbrida de Azure. Si tu organización tiene Microsoft Software Assurance, puedes usar Ventaja híbrida de Azure para Windows Server con el fin de ahorrar en el coste de tu infraestructura de Azure. Para obtener más información, visita [este enlace](#).
- Las **instancias reservadas (RI)** de Azure pueden reducir considerablemente los costes hasta un 72 % si se compara con los precios de pago por uso, con un compromiso de un año o tres años en las máquinas virtuales de Windows y Linux. Con las instancias reservadas, pagas por adelantado tu uso de máquinas virtuales. Lo ideal sería combinar las instancias reservadas con la Ventaja híbrida de Azure (como se ha indicado anteriormente) para ahorrar hasta un 80 % en los precios de lista.
- Puede reducir el coste total de implementación de Azure Virtual Desktop si escalas tus máquinas virtuales. Esto significa apagar y desasignar las máquinas virtuales de host de sesión durante las horas de menor uso y, después, volver a encenderlas y reasignarlas durante las horas de máximo uso. En el capítulo 6 se proporciona información más detallada.
- Al configurar las máquinas virtuales de host de sesión, considera las diferentes opciones de equilibrio de carga. El equilibrio de carga en amplitud es el modo predeterminado (y el más utilizado). El equilibrio de carga en amplitud reparte a los usuarios entre los servidores host de sesión en función del número de sesiones por host. El equilibrio de carga en modo de profundidad llena primero un servidor host de sesión con el máximo número de usuarios antes de pasar al siguiente servidor. Según el caso de uso, el equilibrio de carga en modo de profundidad puede conllevar un ahorro de costes adicional, pero en algunos casos podría no ser suficiente para hacer frente a las avalanchas de inicio de sesión de los usuarios. Puedes ajustar esta configuración para obtener el máximo ahorro de costes. Para obtener información más detallada sobre ambas opciones de equilibrio de carga, visita [este enlace](#).

Directrices de red

La recomendación general es diseñar la red de Azure usando una topología radial. Considera el concentrador como una **zona desmilitarizada (DMZ)** implementada con sus puertas de enlace de red virtual y otros dispositivos de seguridad/perímetro, como firewalls y demás, mientras que el radio actuará como la zona back-end en la que se implementan los servidores host de sesión y se empareja con el concentrador. Consulta a tu equipo de red durante esta fase para efectuar una implementación óptima.

El ancho de banda disponible del cliente local para los componentes de plano anterior de Azure Virtual Desktop, o más específicamente, el componente de puerta de enlace en Azure Virtual Desktop, desempeña un papel importante en la experiencia general percibida del usuario final. En la *tabla 3* se muestran los anchos de banda mínimos recomendados para una experiencia de usuario sin problemas.

Tipo de carga de trabajo	Ancho de banda recomendado
Ligera	1,5 Mbps
Media	3 Mbps
Pesada	5 Mbps
Potencia	15 Mbps

Tabla 3: Anchos de banda mínimos recomendados

Ten en cuenta que los factores externos también pueden aumentar el ancho de banda que se utiliza. Por ejemplo, si aumenta la velocidad de imágenes o la resolución de la pantalla, también aumentará el requisito de ancho de banda. Los anchos de banda de la *tabla 3* son valores recomendados y variarán según las aplicaciones consumidas y del caso de uso específico de Azure Virtual Desktop que implementes. Se aconseja realizar siempre evaluaciones comparativas y pruebas para confirmar los valores medios de la implementación de Azure Virtual Desktop.

La resolución de la pantalla que se utilice también afecta al ancho de banda disponible. La *tabla 4* contiene una lista de los anchos de banda recomendados para permitir una experiencia de usuario fluida, según una velocidad de 30 **imágenes por segundo (fps)**.

Resoluciones típicas de pantalla a 30 fps Ancho de banda recomendado	
Alrededor de 1024 × 768 píxeles	1,5 Mbps
Alrededor de 1280 × 720 píxeles	3 Mbps
Alrededor de 1920 × 1080 píxeles	5 Mbps
Alrededor de 3840 × 2160 píxeles (4K)	15 Mbps

Tabla 4: Resoluciones típicas de pantalla y anchos de banda recomendados

Directrices de administración de perfiles

Si tu implementación actual de RDS utiliza el **disco de perfil de usuario (UPD)** o los perfiles móviles como la solución de administración de perfiles, ten en cuenta que debes migrar o hacer una transición a los contenedores de perfiles FSLogix. Esto se debe a que UPD no es compatible con Azure Virtual Desktop. La migración de perfiles UPD a los contenedores de perfiles FSLogix puede realizarse manualmente o con el método que elijas, pero, para proporcionar una buena ruta de migración entre tu solución de perfiles existente y el contenedor de perfiles, hemos creado un [script de migración que está disponible actualmente como preview privada](#).*

Windows 10 multisesión

Si actualmente tienes una implementación de RDS que se ejecuta localmente que quieres migrar a Azure Virtual Desktop, estás utilizando una versión de Windows Server como sistema operativo para los servidores host de sesión de Escritorio remoto. Esto se debe a que Windows 10 multisesión no se admite fuera de Azure Virtual Desktop. Como parte de esta migración, puedes migrar tus servidores host de sesión de Escritorio remoto actuales. Windows Server 2012 R2 y cualquier versión posterior es compatible con Azure Virtual Desktop. Sin embargo, por varios motivos, como se indica en el capítulo 1, el uso de Windows 10 multisesión proporciona muchas ventajas adicionales, incluido un ahorro de costes, debido a que ya no se requiere una CAL de RDS. Para optimizar completamente Azure Virtual Desktop y Azure, te aconsejamos que vuelvas a crear las imágenes en Windows 10 multiusuario. [En este artículo](#) se explica cómo preparar una imagen maestra de **disco duro virtual (VHD)** para cargarla en Azure, incluido el modo de crear máquinas virtuales e instalar software en ellas. Sugerimos consultar este artículo para aprovechar al máximo las capacidades de Azure Virtual Desktop.

* La preview privada para la conversión de contenedores UPD a FSLogix para Azure Virtual Desktop se proporciona sin un acuerdo de nivel de servicio y no se recomienda para cargas de trabajo de producción. Ciertas funciones podrían no ser compatibles o podrían tener capacidades limitadas. Es posible que los contenedores de perfiles FSLogix no admitan toda la funcionalidad de los formatos que se convierten. Para obtener más información, consulta Términos suplementarios de uso para versiones preview de Microsoft Azure.

Convenciones de nomenclatura

Con cualquier suscripción a Azure, es importante tener una buena convención de nomenclatura. En la siguiente lista se incluyen consideraciones relativas a las convenciones de nomenclatura:

- Una convención de nomenclatura eficaz reúne los nombres de los recursos utilizando información importante de los recursos como parte del nombre de un recurso. Cuando crees tu convención de nomenclatura, identifica las piezas clave de información que quieres reflejar en un nombre de recurso.
- Cada carga de trabajo puede constar de muchos recursos y servicios individuales. La incorporación de prefijos de tipo de recurso en los nombres de recurso facilita la identificación visual de los componentes de aplicación o servicio.
- Cuando aplicas etiquetas de metadatos a los recursos del cloud, puedes incluir información sobre los activos que no se ha podido incluir en el nombre de recurso.

Sigue la guía de [este enlace](#) para mantener una convención de nomenclatura coherente en todos tus recursos si no tienes una convención de nomenclatura existente para tu suscripción.

Orientación para la implementación

Después de haber evaluado los requisitos previos y las consideraciones que se han descrito en las dos secciones anteriores, ya puedes implementar los objetos necesarios de Azure Virtual Desktop en tu suscripción de Azure.

Comienza con la implementación de un grupo de hosts. Los grupos de hosts son una colección de una o más máquinas virtuales idénticas en entornos de Azure Virtual Desktop. Para crear el grupo de hosts, elige un nombre único en un grupo de recursos y proporciona la región de Azure.

Create a host pool

[Basics](#)
[Virtual Machines](#)
[Workspace](#)
[Tags](#)
[Review + create](#)

Project details

Subscription * ⓘ

Resource group * ⓘ

[Create new](#)

Host pool name *

Location * ⓘ

Metadata will be stored in Azure geography associated with (US) East US

[Learn more](#)

Validation environment ⓘ No Yes

Host pool type

If you select pooled (shared), users will still be able to access their personalization and user data, using FSLogix.

Host pool type *

Figura 7: El asistente para crear un grupo de hosts en Azure Portal

La ubicación geográfica de Azure asociada con las regiones que has seleccionado es donde se almacenarán los metadatos de este grupo de hosts y sus objetos relacionados. Asegúrate de elegir las regiones en la ubicación geográfica en la que quieres que se almacenen los metadatos del servicio. En **Tipo de grupo de hosts**, selecciona si el grupo de hosts será **Personal** o **Agrupado**. Si eliges **Agrupado**, introduce un límite máximo de sesión y un algoritmo de equilibrio de carga. Antes de terminar la creación del grupo de hosts, puedes decidir crear nuevas máquinas virtuales basadas en una nueva imagen de plantilla, o decidir no crear una nueva máquina virtual todavía para migrarlas posteriormente desde tu implementación de RDS on-premises. Explicamos esta opción con más detalle en el capítulo 2. Para obtener una descripción técnica detallada de la implementación de grupos de hosts, visita [esta página](#).

El proceso de configuración del grupo de hosts crea un **grupo de aplicaciones** de escritorio de forma predeterminada. Para que el grupo de hosts funcione del modo previsto, debes asignar este grupo de aplicaciones a usuarios o grupos de usuarios, y debes registrar el grupo de aplicaciones en un área de trabajo.

Create a host pool

Basics Virtual Machines Workspace Tags Review + create

To save some time, you can register the default desktop application group from this host pool, with a new or pre-existing workspace.

Register desktop app group No Yes

Figura 8: Creación del grupo de aplicaciones

Si seleccionas *No*, puedes registrar el grupo de aplicaciones más tarde, pero te recomendamos que registres el área de trabajo lo antes posible para que tu grupo de hosts funcione correctamente. Elige si quieres crear una nueva **área de trabajo** o selecciona una de las áreas de trabajo existentes. Solo se podrán elegir áreas de trabajo creadas en el mismo lugar que el grupo de hosts para registrar el grupo de aplicaciones.

Create a host pool

Basics Virtual Machines Workspace Tags Review + create

To save some time, you can register the default desktop application group from this host pool, with a new or pre-existing workspace.

Register desktop app group No Yes

To this workspace ⓘ

[Create new](#)

Create new

Workspace name *

We will also create a display name for this workspace, which you can always edit later.

Figura 9: Creación del área de trabajo

Revisa la información sobre tu implementación para asegurarte de que todo se ve correcto. Cuando hayas terminado, selecciona **Crear**. Esto inicia el proceso de implementación, que crea los siguientes objetos:

- Un nuevo grupo de hosts.
- Un grupo de aplicaciones de escritorio.
- Un área de trabajo, si has elegido crearla.
- Si has elegido registrar el grupo de aplicaciones de escritorio, el registro se completará.
- Un enlace de descarga para una plantilla de administración de recursos de Azure basada en tu configuración.

Ahora que has creado tu grupo de hosts, puedes llenarlo con programas RemoteApp o un escritorio por grupo de hosts. El grupo de aplicaciones predeterminado creado para un nuevo grupo de hosts de Azure Virtual Desktop también publica el escritorio completo. Además, puedes crear uno o más grupos de aplicaciones RemoteApp para el grupo de hosts. Solo puedes crear 50 grupos de aplicaciones por cada inquilino de Azure AD. Añadimos este límite debido a las restricciones del servicio de recuperación de canales para nuestros usuarios. Para obtener una descripción técnica detallada de la implementación de grupos de aplicaciones, visita [este enlace](#).

Anteriormente, hemos completado los pasos del 1 al 4 y, en la sección anterior, hemos creado nuestra implementación de Azure Virtual Desktop. Ahora ya podemos empezar a replicar los servidores host de sesión de Escritorio remoto en Azure (paso 5) y convertirlos en parte de la implementación de Azure Virtual Desktop, realizar una migración de prueba (paso 6) y migrar a producción (paso 7).

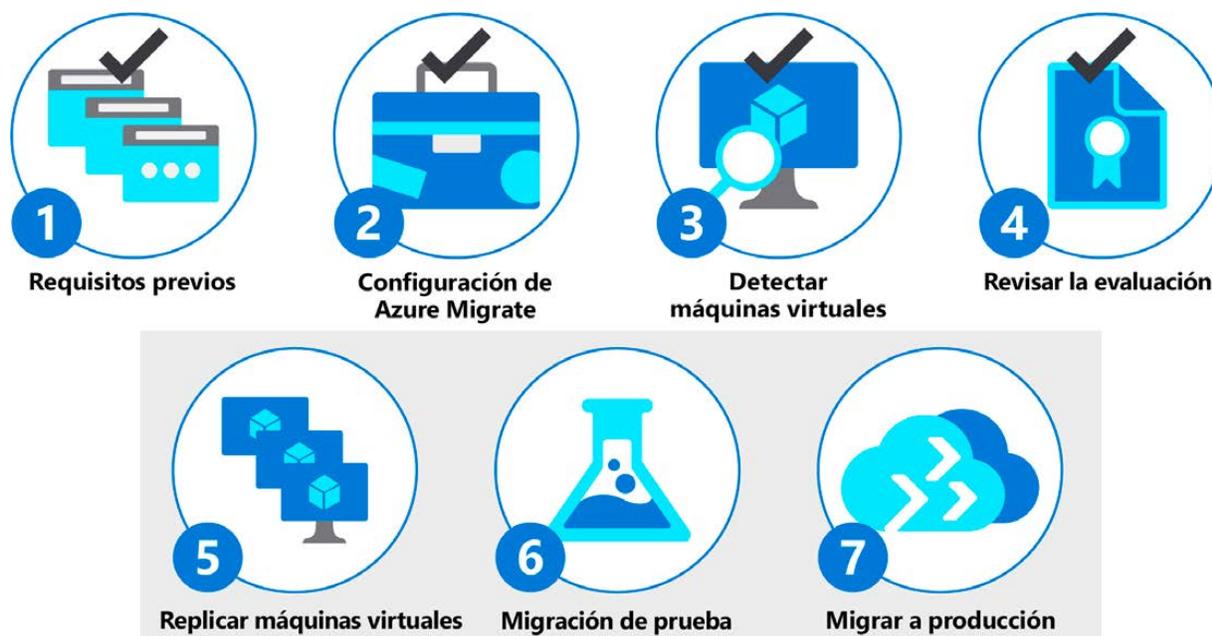


Figura 10: Paso 5, 6 y 7



Paso 5: Replicar máquinas virtuales

En este paso, replicaremos los servidores host de sesión de Escritorio remoto de on-premises a Azure para que podamos añadir los servidores replicados a nuestra implementación de Azure Virtual Desktop creada. Puedes comenzar la replicación de las máquinas virtuales en Azure. En el proyecto de Azure Migrate, haz clic en **Replicar** en **Migración de servidor**. Si has realizado una evaluación de las máquinas virtuales, puedes aplicar las recomendaciones de tamaño y tipo de disco (premium/estándar) a partir de los resultados de la evaluación. Busca las máquinas virtuales según sea necesario y marca cada una que quieras migrar. Activa la Ventaja híbrida de Azure si tienes máquinas de Windows Server que están cubiertas con una suscripción activa a Software Assurance o a Windows Server y quieres aplicar el beneficio a las máquinas que estás migrando. Después de que termine la replicación inicial, comienza la replicación delta. Los cambios incrementales en los discos on-premises se replican periódicamente en Azure. Puedes realizar el seguimiento del estado del trabajo en las notificaciones del portal.

Los pasos detallados sobre la replicación se pueden encontrar [aquí](#).

Como se ha mencionado anteriormente, en algunos escenarios es posible que no quieras migrar tus máquinas virtuales existentes, sino crear una nueva plantilla de máquina virtual; por ejemplo, si quieres aprovechar Windows 10 multisesión, que solo está disponible como parte de Azure Virtual Desktop. En [este artículo](#) se explica cómo preparar una nueva imagen maestra en su lugar. En este caso, la información recogida durante la fase de evaluación será de gran ayuda para informarte de cómo componer tus imágenes y configurar tu infraestructura de aplicaciones.



Paso 6: Migración de prueba

Cuando comience la replicación delta como parte del paso 6, puedes ejecutar una migración de prueba de las máquinas virtuales, antes de realizar una migración completa a Azure. Te recomendamos que lo hagas al menos una vez por cada servidor host de sesión de Escritorio remoto antes de migrarlo. La ejecución de una migración de prueba verifica que la migración funcionará como se espera, sin que se vean afectadas las máquinas on-premises, que siguen operativas y continúan replicándose. En **Objetivos de migración** selecciona **servidores**, selecciona **Azure Migrate y Migration de servidor** y haz clic en **Probar servidores migrados**. Supervisa el trabajo en las notificaciones del portal.

Los pasos detallados sobre la migración de prueba se pueden encontrar [aquí](#).

Paso 7: Migrar a producción

Una vez que hayas verificado que la migración de prueba funciona según lo previsto, puedes migrar los servidores de sesión host de sesión de Escritorio remoto on-premises. En el área **Replicación de máquinas**, haz clic con el botón derecho del ratón en la máquina virtual y haz clic en **Migrar**. De forma predeterminada, Azure Migrate apaga la máquina virtual on-premises y ejecuta una replicación bajo demanda para sincronizar cualquier cambio en la MV que haya ocurrido desde la última replicación. Esto garantiza que no haya pérdida de datos. Comienza un trabajo de migración para la MV. Realiza el seguimiento del trabajo en las notificaciones de Azure. Después de que termine el trabajo, puedes ver y administrar la MV desde la página **Máquinas virtuales**. Una vez terminada la migración, utiliza la opción **Detener migración**. Este proceso detiene la replicación de la máquina on-premises y quita la máquina del recuento de **Replicación de servidores** en Azure Migrate.

Los pasos detallados sobre la migración a producción se pueden encontrar [aquí](#).



Figura 11: Los siete pasos completados

Ya hemos completado el proceso de siete pasos de Azure Migrate. En el capítulo 4, continuaremos explicando cómo probar y preparar más a fondo tu entorno de Azure Virtual Desktop, seguido del capítulo 5, donde ofreceremos orientación sobre la puesta en marcha y sugeriremos pasos posteriores a dicha puesta en marcha.

Prueba y preparación de la implementación de Azure Virtual Desktop

Confirmación del estado de implementación de Azure Virtual Desktop

La región en la que te encuentras puede afectar a la experiencia del usuario tanto como las condiciones de la red. El cliente de Azure Virtual Desktop, basado en la información de DNS, siempre enrutará la conexión del usuario a la región de Azure más cercana que tenga componentes del plano anterior de Azure Virtual Desktop. Para determinar qué región de Azure funciona mejor para tu ubicación específica, busca el [Estimador de experiencia de Azure Virtual Desktop](#). Esto te permite estimar la calidad de la experiencia que tus usuarios recibirán al conectarse a Azure Virtual Desktop. Mide y calcula el **tiempo de ida y vuelta (RTT)** desde tu ubicación actual, a través del servicio de Azure Virtual Desktop, a cada región de Azure en la que puedes implementar máquinas virtuales como parte de tu grupo de hosts de Azure Virtual Desktop.

Azure Region*	Round Trip Time (ms)
Germany West Central	31
Switzerland North	37
France Central	39
West Europe	40
Germany North	40
Switzerland West	40
UK South	45
France South	47

Figura 12: Ejemplo de resultado del Estimador de experiencia de Azure Virtual Desktop

Se resalta la región de Azure con la conexión RTT más baja desde tu ubicación actual. Ten en cuenta que los tiempos que se muestran son estimaciones destinadas a ayudar a evaluar la calidad y la experiencia del usuario final percibida para la implementación de Azure Virtual Desktop. La experiencia real variará en función de otras condiciones, como otras especificaciones de la red, el dispositivo del usuario final y la configuración de las máquinas virtuales implementadas.

Estado del grupo de hosts de Azure Virtual Desktop

Azure Portal proporciona una forma fácil de determinar el estado de los grupos de hosts de Azure Virtual Desktop. Cuando estés en Azure Portal, navega a Azure Virtual Desktop, haz clic en **Grupos de hosts** y abre el grupo correspondiente. El estado de todos los servidores host de sesión de Azure Virtual Desktop individuales debe ser *Disponible* si se activa.

Home > Azure Virtual Desktop > NINJA-WE-P-RG-WVD-FB-APP-HOSTPOOL >

NINJA-WE-P-RG-WVD-FB-APP-HOSTPOOL - Session hosts

Host pool

+ Add Refresh Assign Export to CSV Turn drain mode on Turn drain mode off Remove

Filter by Name Status: 12 selected Drain mode: 2 selected

Name ↑↓	Status ↑↓	Drain mode ↑↓	Assigned User ↑↓	Active sessions ↑↓
<input type="checkbox"/> WVDFBAP2004-1-2.wvd.ninja	✔ Available	Off	-	0

Figura 13: El estado del servidor host de sesión de Azure Virtual Desktop es Disponible

Instrucciones para probar las implementaciones de Azure Virtual Desktop

Una vez que hayas confirmado el estado de tu entorno de Azure Virtual Desktop, puedes comenzar a probar la implementación.

Ahora que has creado tu grupo de hosts, puedes llenarlo con programas RemoteApp o un escritorio por grupo de hosts. El grupo de aplicaciones predeterminado creado para un nuevo grupo de hosts de Azure Virtual Desktop también publica el escritorio completo. Además, puedes crear uno o más grupos de aplicaciones RemoteApp para el grupo de hosts. Usa Azure Portal para personalizar la implementación de Azure Virtual Desktop [publicando aplicaciones](#), [asignando usuarios](#) y [configurando las opciones del grupo de hosts](#).

Puedes acceder a los recursos de Azure Virtual Desktop en dispositivos con Windows 7, Windows 10 y Windows 10 IoT Enterprise mediante el cliente de Escritorio de Windows. Además de la plataforma Windows, también puedes aprovechar los clientes Android, iOS, macOS y web. La siguiente lista contiene enlaces a los diferentes clientes y guías sobre la instalación, configuración y uso del cliente:

- [Conectar con el cliente de escritorio de Windows](#)
- [Conectar con el cliente web](#)
- [Conectar con el cliente de escritorio de Android](#)
- [Conectar con el cliente de MacOS](#)
- [Conectar con el cliente de iOS](#)

En la *figura 14* se muestra un ejemplo del cliente de Azure Virtual Desktop, que contiene escritorios publicados, así como aplicaciones remotas.

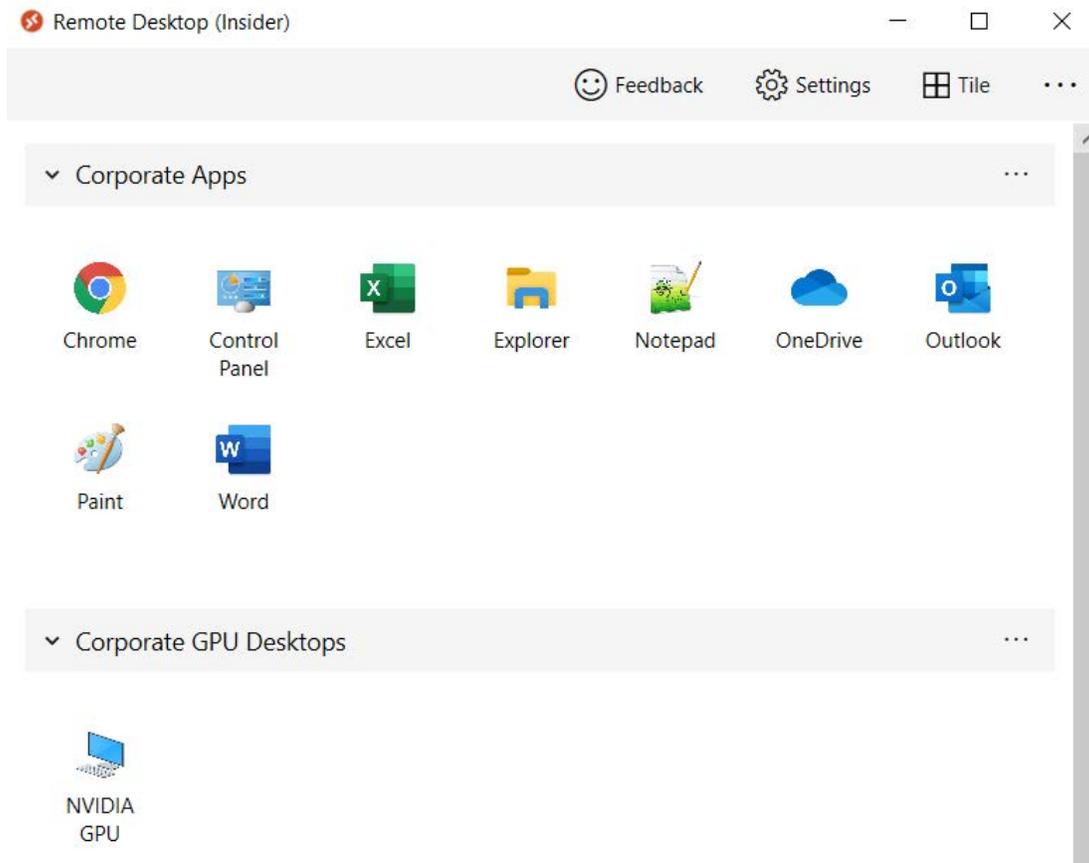


Figura 14: Ejemplo del cliente de Azure Virtual Desktop

Si tienes problemas de conexión en este momento, consulta [esta página](#), que contiene escenarios de error comunes, errores de administración y códigos de error de conexión externa.

Preparativos finales para la puesta en marcha

La adaptación del usuario es una parte clave de todo proyecto de TI que implique cambios para los usuarios finales. Aunque los usuarios podrán acceder a sus aplicaciones y escritorios publicados como antes, debes preparar minuciosamente la adopción de los usuarios de Azure Virtual Desktop. Los usuarios requieren formación, manuales y recursos al estilo de preguntas frecuentes para ayudarles a aprovechar al máximo el servicio de Azure Virtual Desktop. El acceso a las aplicaciones y escritorios de Azure Virtual Desktop es un poco diferente si se compara con RDS, ya que los usuarios deben efectuar un registro inicial único en su dispositivo. Asegúrate de que los usuarios tengan las instrucciones correctas e incorpora los enlaces a los diversos clientes de Azure Virtual Desktop como se indica en el capítulo anterior.

Pasos para la puesta en marcha e implementación posterior

Confirmación del estado y el uso de Azure Virtual Desktop

Después de haber migrado a Azure Virtual Desktop, investiga el uso y el estado de Azure Virtual Desktop en tu entorno. Durante la fase de preparación, hemos determinado qué tamaño de máquina virtual utilizar para las máquinas virtuales host de sesión e investigado el uso del entorno reuniendo datos de telemetría sobre los recursos que se han consumido; por ejemplo, mediante la implementación de Log Analytics, tal como se describe más adelante en la sección *Supervisión*. Esto te permite conocer el número de usuarios que utilizan las aplicaciones y los escritorios publicados de Azure Virtual Desktop y te proporciona datos de telemetría sobre el consumo de recursos. Usa esta información para reajustar tus servidores host de sesión según sea necesario.

Como se ha explicado en un capítulo anterior, el estado de todos los servidores de sesión individuales de Azure Virtual Desktop debe ser *Disponible*. Investiga el estado de todos los servidores host de sesión para asegurarte de que están conectados y funcionando correctamente. Ten en cuenta que si has implementado el escalado automático, como se explica en el capítulo 6, las máquinas virtuales actualmente reducidas aparecen como *No disponibles*, pero no requieren ninguna acción.

Recopila información sobre el número de usuarios que utilizan activamente Azure Virtual Desktop e información sobre el diagnóstico para conocer qué sesiones han provocado errores de conexión. Investiga estos errores y haz un seguimiento con las correcciones sugeridas.

Azure Advisor te proporciona información sobre el entorno de Azure Virtual Desktop y te guía por los procedimientos recomendados que puedes no haber realizado durante la implementación. Investiga atentamente las recomendaciones que contiene Azure Advisor y aplica los procedimientos recomendados sugeridos que se muestran.

En la *figura 15* se muestra un ejemplo de Azure Advisor que proporciona directrices para Azure Virtual Desktop.

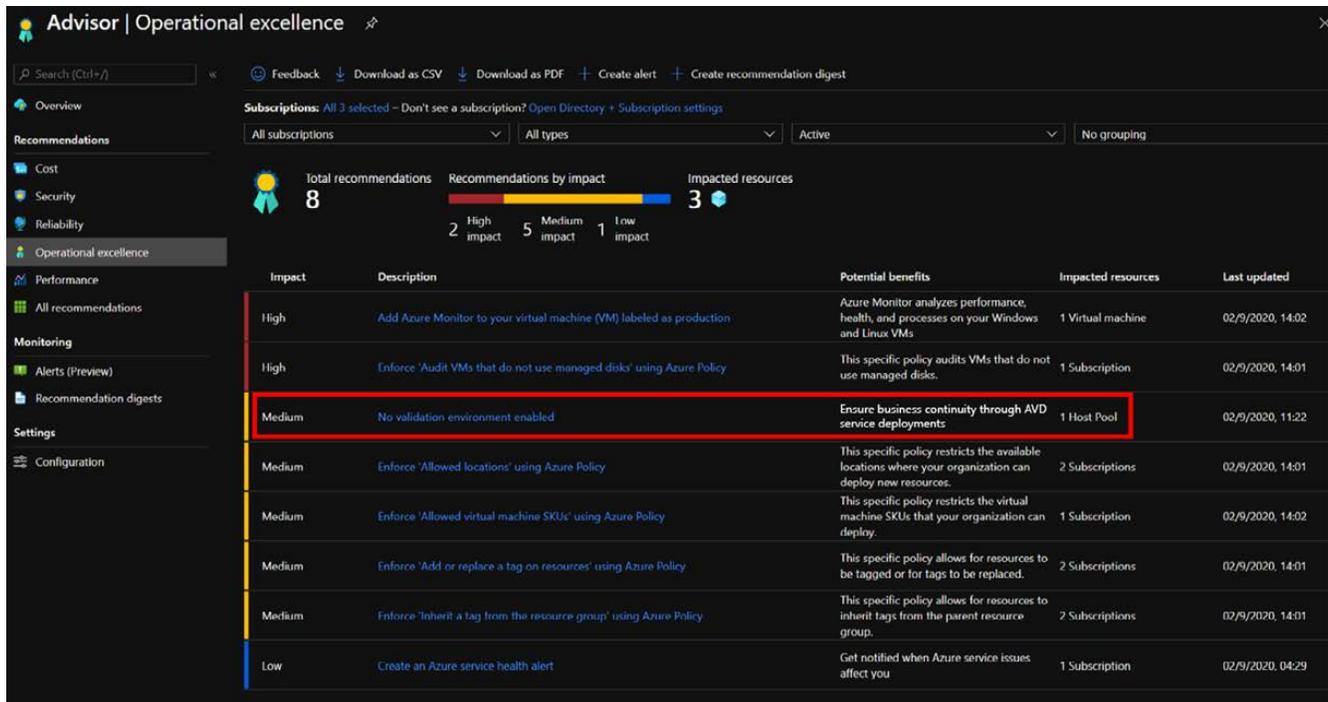


Figura 15: Ejemplo de Azure Advisor para Azure Virtual Desktop

Consideraciones y pasos posteriores a la implementación

Después de haber realizado la implementación de Azure Virtual Desktop en producción, es recomendable analizar y planificar los pasos posteriores a la implementación. En un paso anterior, has confirmado el estado y el uso de la implementación de Azure Virtual Desktop, pero es aconsejable supervisar ese estado de manera continua. Considera la posibilidad de implementar la supervisión basada en Azure Monitor y Log Analytics, tal como se describe en la sección *Supervisión* más adelante. La seguridad es una parte importante de Azure Virtual Desktop. Puede que hayas usado la **autenticación multifactor (MFA)** en tu implementación de RDS. Ahora es un buen momento para considerar la posibilidad de añadir el acceso condicional a tu implementación. Como Azure Virtual Desktop está basado en Azure AD, es una tarea relativamente fácil. Describimos esta tarea en la sección *Acceso condicional* más adelante. A medida que comiences a utilizar Azure Virtual Desktop, considera otros escenarios que puedan beneficiarse de esta implementación. Por ejemplo, podrías permitir a los administradores el acceso remoto a tu entorno para realizar tareas de mantenimiento. Puede que actualmente estés usando una solución VPN para eso. Tus administradores también pueden utilizar Azure Virtual Desktop al proporcionar acceso seguro a un servidor de administración central (host de salto). Es importante planificar el escalado automático continuo y las actualizaciones de las máquinas virtuales host de sesión como parte de tu grupo de hosts. Automatiza estas actualizaciones como se indica en la próxima sección *Escalado automático*.

Limpieza de una implementación de RDS

Después de haber migrado correctamente tu implementación de RDS a Azure Virtual Desktop, es aconsejable que también limpies tu implementación de RDS. Es importante investigar, planificar y ejecutar esta limpieza a fondo para asegurarte de que no queden componentes ni configuraciones. Hay un par de áreas en las que se aconseja la limpieza del entorno de RDS:

- Es evidente que las MV de tu implementación de RDS se pueden quitar. Las máquinas virtuales que ejecutan sus funciones de infraestructura de RDS, como Agente de conexión a Escritorio remoto, Acceso web de Escritorio remoto y Puerta de enlace de Escritorio remoto, ya no son necesarias. Las máquinas virtuales host de sesión de Escritorio remoto se han migrado a Azure como parte de la migración a Azure Virtual Desktop y también se pueden quitar. Es recomendable exportar las opciones de configuración de RDS, por ejemplo, las aplicaciones publicadas, las opciones de redireccionamiento, etc., para asegurarte de que dispones de esa información si quieres comparar la configuración de Azure Virtual Desktop en una fase posterior. También puede ser recomendable hacer una instantánea o una copia de seguridad de uno de tus host servidores de sesión de Escritorio remoto si se produce un comportamiento inesperado con las aplicaciones o con la configuración en los servidores host de sesión como parte de Azure Virtual Desktop en una etapa posterior y quieres comparar la configuración con la implementación de RDS anterior.
- Tu implementación de RDS también habrá utilizado varios registros de DNS y lo más probable es que estos se hayan creado en servicios DNS públicos y privados. Los registros de tipo A de DNS se han utilizado para acceder a los componentes Agente de conexión a Escritorio remoto, Puerta de enlace de Escritorio remoto y Acceso web de Escritorio remoto. Lo más probable es que también hayas utilizado los registros TXT de DNS para permitir que el applet del Panel de control **Conexiones de RemoteApp y Escritorio (RADDC)** configure automáticamente la URL del canal web basándose en la dirección de correo electrónico del usuario. Estos registros DNS ahora se pueden eliminar con seguridad ya que no son necesarios para Azure Virtual Desktop.
- Los componentes de infraestructura de la implementación de RDS, incluidos los servidores host de sesión de Escritorio remoto reales, son todos miembros de la instancia interna de AD Domain Services. Ya que hemos eliminado las máquinas virtuales de infraestructura, los correspondientes objetos de equipo de AD, incluidas sus entradas DNS, también se pueden eliminar ahora. El hecho de que puedas o no eliminar el objeto de equipo del servidor host de sesión de Escritorio remoto depende de la forma en que hayas migrado esas cargas de trabajo. Si has migrado las máquinas virtuales en sí, vas a reutilizar esos objetos de equipo y no deberías eliminarlas. Si has hecho la migración basándote en un nuevo conjunto de máquinas virtuales en Azure, por ejemplo, como parte de tu migración de Windows Server a Windows 10 multisesión, lo más probable es que también estés usando nuevos nombres y objetos de equipo, lo que significa que puedes eliminar los objetos antiguos.

Orientación sobre las capacidades adicionales

Escalado automático

Como se ha mencionado brevemente en el capítulo 3, al escalar automáticamente las máquinas virtuales de host de sesión, puedes reducir el coste total de implementación de Azure Virtual Desktop. El escalado automático de Azure Virtual Desktop garantiza que se apaguen y se desasignen las máquinas virtuales de host de sesión durante las horas de menor uso y que se vuelvan a encender y reasignar durante las horas de mayor uso. La herramienta de escalado te proporciona una opción de automatización de bajo coste para un escenario en el que quieres optimizar los costes de máquina virtual de host de sesión.

La herramienta de escalado automático que proporciona Microsoft te ayudará a automatizar y programar las máquinas virtuales de host de sesión para que se inicien y se detengan en función de las horas pico y no pico que definas como parámetros. Las dos acciones siguientes se llevarán a cabo después de que hayas configurado el escalado automático:

- La herramienta de escalado automático hará un escalado horizontal de las máquinas virtuales de los hosts de sesión según el número de sesiones por VCPU definidas como uno de los parámetros.
- La herramienta de escalado automático hará un escalado vertical de las máquinas virtuales durante las horas no pico, dejando el número mínimo de MV host de sesión en ejecución definido como uno de los parámetros.

En las siguientes secciones se ofrecen más detalles sobre las horas pico y las horas no pico.

Durante el tiempo de uso máximo, el trabajo comprueba el número actual de sesiones y la capacidad de máquinas virtuales del host de sesión en curso para cada grupo de hosts. Utiliza esta información para calcular si las máquinas virtuales de host de sesión en ejecución pueden admitir sesiones existentes basándose en el parámetro `SessionThresholdPerCPU`.

Durante el tiempo de uso fuera de las horas pico, el trabajo determina cuántas máquinas virtuales de host de sesión deben apagarse según el parámetro `MinimumNumberOfRDSH`. El trabajo notificará a cualquier usuario que haya iniciado la sesión para que guarde su trabajo, esperará el tiempo configurado y forzará a los usuarios a cerrar la sesión. Una vez que se han cerrado todas las sesiones de usuario en la máquina virtual de host de sesión, el trabajo apagará la MV. Después de que se apague la máquina virtual, el trabajo restablecerá su modo de drenaje de host de sesión.

En cualquier momento, el trabajo también tiene en cuenta el valor `MaxSessionLimit` del grupo de hosts para determinar si el número actual de sesiones es superior al 90 % de la capacidad máxima. El trabajo se ejecuta periódicamente según un intervalo de periodicidad establecido. Puedes personalizar este intervalo en función del tamaño de tu entorno de Azure Virtual Desktop. Ten en cuenta que el inicio y el apagado de las máquinas virtuales puede llevar algún tiempo, por lo que no te olvides de tener en cuenta este retraso. El intervalo de periodicidad recomendado es cada 15 minutos.

En la actualidad, la herramienta también tiene las siguientes limitaciones que debes conocer:

- La herramienta de escalado automático solo se aplica a las máquinas virtuales de host de sesión multisesión agrupadas. Los hosts de Azure Virtual Desktop asignados personales no se pueden escalar automáticamente con esta herramienta.
- La herramienta de escalado automático administra las máquinas virtuales de cualquier región; sin embargo, solo puede utilizarse en la misma suscripción que tu cuenta de Azure Automation y Azure Logic App (el objeto Azure del que consta la herramienta de escalado automático).
- Si el inicio o la detención de las máquinas virtuales en tu grupo de hosts tarda más de tres horas, se producirá un error en el trabajo.

Para empezar a usar el escalado automático, sigue [esta guía](#).

Acceso condicional

Tal como se ha mencionado brevemente en el capítulo 1, Azure Virtual Desktop se basa en Azure AD. Esto significa que Azure Virtual Desktop puede aprovechar de forma instantánea todas las características de seguridad de Azure AD. En la mayoría de los entornos de producción, aconsejamos configurar el acceso condicional para Azure Virtual Desktop. Esto te permite definir los requisitos de seguridad adicionales que la sesión de un usuario debe cumplir para acceder a los escritorios y las aplicaciones que se han publicado.

Un ejemplo común de acceso condicional es Azure MFA. Después de configurar Azure MFA, cuando un usuario inicia sesión, el cliente le pide su nombre de usuario y contraseña, seguido de una solicitud de Azure MFA. Al seleccionar **Recordarme**, los usuarios pueden iniciar sesión después de reiniciar el cliente sin necesidad de volver a introducir sus credenciales. Estas credenciales se almacenan en el administrador de credenciales local. Esto último se aplica al uso del cliente de Azure Virtual Desktop; otros clientes de Azure Virtual Desktop pueden mostrar una experiencia diferente según la plataforma y la versión del cliente. Aunque recordar las credenciales es cómodo, también puede provocar que las implementaciones para los escenarios de empresa o los dispositivos personales sean menos seguros. Para proteger a tus usuarios, tendrás que asegurarte de que el cliente siempre pida credenciales de Azure MFA. Puedes encontrar más información sobre la configuración de Azure MFA para Azure Virtual Desktop [aquí](#).

Supervisión

Como muchos otros servicios de Azure, Azure Virtual Desktop también puede utilizar Azure Monitor para la supervisión y las alertas. Esto permite a los administradores de Azure Virtual Desktop identificar los problemas a través de una interfaz y un panel de control consolidados. Azure Monitor y Log Analytics pueden recopilar registros de actividad tanto del usuario final como de las acciones administrativas. Cada registro de actividad capturado corresponde a una de las siguientes categorías:

- Actividades de administración
- Fuente
- Conexiones
- Registro de host
- Errores
- Puntos de control

Las conexiones que no llegan a Azure Virtual Desktop no aparecerán en los resultados del diagnóstico porque el servicio de rol de diagnóstico es parte de Azure Virtual Desktop. Los problemas de conexión de Azure Virtual Desktop pueden suceder cuando el usuario experimenta problemas de conectividad de red.

Azure Monitor te permite analizar la información consolidada de tu implementación de Azure Virtual Desktop, así como los datos de telemetría sobre las MV de host de sesión. Al definir los contadores de rendimiento, puedes crear un panel personalizado. Azure Monitor también permite a los administradores crear paneles personalizados y compartirlos con otros administradores de Azure. A estos paneles se puede acceder fácil y cómodamente desde Azure Portal.

En la siguiente captura de pantalla se muestra un ejemplo del resultado de Azure Monitor y Log Analytics para Azure Virtual Desktop.

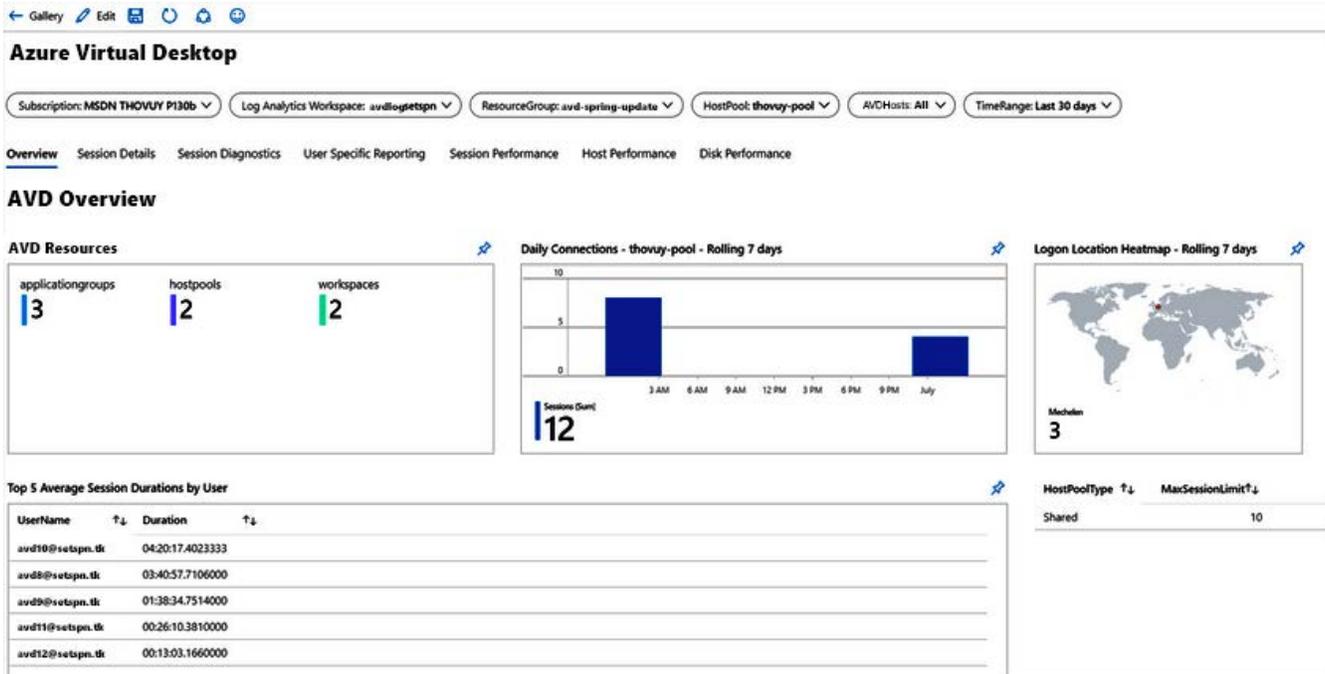


Figura 16: Ejemplo de Azure Monitor para Azure Virtual Desktop

Para empezar a usar Azure Monitor para Azure Virtual Desktop, usa [esta guía](#).

Automatización

Azure Virtual Desktop está totalmente basado en **Azure Resource Manager (ARM)**. Esto también significa que puedes aprovechar varias formas de automatizar la implementación y el mantenimiento de Azure Virtual Desktop. Para la automatización mediante ARM, Microsoft proporciona y mantiene una ubicación en GitHub, donde puedes recuperar scripts de automatización para varias tareas.

ARM te permite definir la infraestructura que se debe implementar en el código. El código de infraestructura se convierte en parte de tu proyecto. Al igual que el código de aplicación, el código de infraestructura se almacena en un repositorio de fuentes y se crean versiones de él. Cualquier miembro de tu equipo puede ejecutar el código e implementar entornos similares.

Para implementar la infraestructura como código para tus soluciones Azure, se utilizan plantillas de ARM. La plantilla es un archivo de **JavaScript Object Notation (JSON)** que define la infraestructura y la configuración de tu proyecto. La plantilla utiliza una sintaxis declarativa, que permite declarar lo que se piensa implementar sin tener que escribir la secuencia de comandos de programación para crearlo. En la plantilla, especifica los recursos que se implementarán y las propiedades de esos recursos. Puedes encontrar más información sobre las plantillas de ARM [aquí](#).

Hay plantillas de ARM disponibles para crear y actualizar grupos de hosts de Azure Virtual Desktop, para configurar el escalado automático y para muchas otras tareas. El repositorio principal de GitHub se encuentra [aquí](#).

Azure Advisor

Azure Advisor puede ayudar a los usuarios a resolver problemas comunes en Azure Virtual Desktop. Estas recomendaciones pueden reducir la necesidad de presentar solicitudes de ayuda, ahorrándote tiempo y costes. Azure Advisor analiza tu configuración y telemetría para ofrecer recomendaciones personalizadas con el fin de resolver problemas comunes. Con estas recomendaciones, puedes optimizar tus recursos de Azure para fiabilidad, seguridad, excelencia operativa, rendimiento y coste.

Asegúrate de consultar las recomendaciones con frecuencia, al menos una vez a la semana. Trata de resolver siempre los asuntos con el nivel de prioridad más alto en Azure Advisor. Si una recomendación parece menos importante, puedes descartarla o posponerla. Cuando observes un problema en Azure Virtual Desktop, siempre consulta primero Azure Advisor. Azure Advisor te dará instrucciones sobre cómo resolver el problema, o al menos te indicará un recurso que pueda ayudarte. Para obtener más información sobre cómo acceder y configurar Azure Advisor para Azure Virtual Desktop, visita [este enlace](#).

Microsoft Teams

Microsoft Teams en Azure Virtual Desktop admite el chat y la colaboración de forma predeterminada. Con optimizaciones de medios para Azure Virtual Desktop, también admite la funcionalidad de llamadas y reuniones. Con la optimización de medios instalada y configurada para Microsoft Teams, el cliente de escritorio de Windows gestiona el audio y el vídeo localmente para las llamadas y reuniones de Teams. Actualmente, las optimizaciones de medios se limitan únicamente al cliente de Azure Virtual Desktop. Sin embargo, puedes seguir usando Microsoft Teams en Azure Virtual Desktop con otros clientes sin necesidad de optimizar las llamadas y las reuniones. Las funciones de chat y colaboración de Teams son compatibles en todas las plataformas sin limitaciones. Para obtener más información sobre cómo activar y configurar las optimizaciones de medios, sigue [este enlace](#).

Hay un par de limitaciones actuales para usar el cliente de escritorio de Teams en entornos de Azure Virtual Desktop. Visita [este enlace](#) para conocer las limitaciones actuales.

Conexión de aplicaciones MSIX

Para mejorar la experiencia de empaquetado de todas las aplicaciones de Windows, se ha introducido MSIX como un nuevo formato de empaquetado que ofrece muchas y excelentes funciones. La conexión de aplicaciones MSIX es una forma de distribuir aplicaciones MSIX a máquinas físicas y virtuales. En una implementación de Azure Virtual Desktop, la conexión de aplicaciones MSIX crea una separación completa entre los datos del usuario, el sistema operativo y las aplicaciones mediante el uso de MSIX en un contenedor virtual. Elimina la necesidad de volver a empaquetar, porque puede aprovechar los paquetes MSIX existentes. El uso de la conexión de aplicaciones MSIX puede ponerse a disposición del servidor host de sesión de Azure Virtual Desktop y del usuario de forma rápida y eficiente. Tanto para el sistema operativo como para el usuario, una conexión de aplicaciones MSIX se trata como cualquier otra aplicación MSIX.

Hay algunas cosas que deben estar aplicadas para que puedas empezar con la conexión de aplicaciones MSIX:

- Es necesario tener al menos Windows 10 versión 2004 como sistema operativo del servidor host de sesión de Azure Virtual Desktop.
- Es necesario que haya una implementación de Azure Virtual Desktop que funcione.
- Preferiblemente, aprovecha la conexión de aplicaciones MSIX con las aplicaciones nativas MSIX que proporciona el proveedor de aplicaciones. Consulta al proveedor de aplicaciones para obtener más información. Si no se proporciona una aplicación nativa MSIX, también puedes utilizar la herramienta de empaquetado MSIX para transformar las aplicaciones existentes (MSI, EXE, etc.) en paquetes MSIX.
- Un recurso compartido de red en la implementación de Azure Virtual Desktop, donde se almacenará el paquete MSIX. Este recurso compartido de red puede estar basado en un servidor de archivos IaaS de Azure y Azure Files.

Puedes encontrar más información sobre la configuración de la conexión de aplicaciones MSIX para Azure Virtual Desktop [aquí](#).

Conclusión

Resumen

En el capítulo 1, presentamos las ventajas de aprovechar la VDI en el cloud para tu estrategia de teletrabajo y los motivos para migrar a Azure Virtual Desktop. Explicamos las ventajas desde la perspectiva de los costes y ofrecemos una introducción al servicio de Azure Virtual Desktop. Además, presentamos el plan de siete pasos para migrar RDS a Azure Virtual Desktop aprovechando Azure Migrate. En el capítulo 2, explicamos con mayor detalle los primeros cuatro pasos del plan de siete pasos y ofrecemos orientación para llevar a cabo estos pasos. En el capítulo 3 se explicó la creación de un entorno de Azure Virtual Desktop y los tres pasos restantes del plan. En el capítulo 4 se habló de probar el entorno de Azure Virtual Desktop y prepararse para la puesta en marcha. En el capítulo 5, explicamos la puesta en marcha y ofrecemos orientación sobre los pasos posteriores a la implementación. En el capítulo 6, ofrecemos orientación sobre las capacidades adicionales que debes tener en cuenta como parte de la implementación de Azure Virtual Desktop. Sigue leyendo para obtener recursos adicionales, instrucciones sobre funcionalidades adicionales, un glosario y más información sobre el autor de este e-book.

Recursos

Esperamos que hayas disfrutado del recorrido y que ahora te sientas más preparado para migrar a Azure Virtual Desktop. Hay muchos otros recursos y materiales de ayuda. Aquí tienes algunas referencias clave:

1. [Consulta](#) más documentación sobre Azure Virtual Desktop para obtener las últimas instrucciones técnicas.
2. [Realiza](#) un tutorial sobre cómo empezar a usar Azure Virtual Desktop.
3. [Ve](#) el vídeo de Microsoft Mechanics para obtener rápidamente información general sobre cómo migrar.
4. [Regístrate](#) en una cuenta gratuita de Azure para intentar implementar tus escritorios y aplicaciones de Windows virtualizados.
5. [Obtén orientación práctica para la implementación](#) si ya tienes una suscripción de Azure.
6. [Únete](#) al Programa de modernización y migración Azure para obtener instrucciones y ayuda de los expertos.
7. [Ponte en contacto con el departamento de ventas](#) para hablar de precios, requisitos técnicos y soluciones a corto y largo plazo para permitir un trabajo remoto seguro.

Si es necesario, usa los siguientes recursos para obtener información más detallada sobre los temas específicos mencionados en este e-book:

- [Instancias de máquina virtual reservadas \(RI\) de Azure](#)
- [Integraciones de partners de Azure Virtual Desktop](#)
- [¿Qué es Azure Virtual Desktop?](#)
- [Especificaciones del equipo de Windows 10 y requisitos de sistema](#)
- [SLA para Virtual Machines](#)
- [Servicios de escritorio remoto: aceleración de GPU](#)
- [Tamaños de máquinas virtual optimizados para GPU](#)
- [Serie de máquinas virtuales](#)
- [Integraciones de partners de Azure Virtual Desktop](#)
- [Acerca de Azure Migrate](#)
- [Preparar y personalizar una imagen de VHD maestra](#)
- [Módulo de vista previa de migración de FSLogix](#)
- [Precios de Azure Virtual Desktop](#)
- [Imágenes de SO de máquinas virtuales compatibles](#)
- [Lista de URL seguras](#)
- [Preguntas frecuentes de Windows 10 Enterprise multisesión](#)
- [Métodos de equilibrio de carga del grupo de hosts](#)
- [Convenciones recomendadas de nomenclatura y etiquetado](#)
- [Crear un grupo de hosts con Azure Portal](#)
- [Administrar grupos de aplicaciones con Azure Portal](#)
- [Estimador de experiencia de Azure Virtual Desktop](#)
- [Escalar hosts de sesión con Azure Automation](#)
- [Activar la autenticación multifactor de Azure para Azure Virtual Desktop](#)
- [Usar Log Analytics para la función de diagnóstico](#)
- [¿Qué son las plantillas de ARM?](#)
- [Plantillas de ARM de RDS/Azure Virtual Desktop](#)
- [Usar Azure Advisor con Azure Virtual Desktop](#)
- [Usar Microsoft Teams en Azure Virtual Desktop](#)
- [Configurar la conexión de aplicaciones MSIX](#)

Glosario

La tabla siguiente contiene un glosario de la terminología utilizada en este libro.

Término	Descripción
Active Directory Domain Services	Un directorio es una estructura jerárquica que almacena información sobre los objetos de la red. Un servicio de directorio, como Active Directory Domain Services (AD DS), proporciona los métodos para almacenar los datos del directorio y ponerlos a disposición de los usuarios y administradores de la red.
Grupo de aplicaciones	Un grupo de aplicaciones es una agrupación lógica de aplicaciones instaladas en los hosts de sesión en el grupo de hosts. Un grupo de aplicaciones puede ser de tipo Escritorio de aplicación remota.
Azure Active Directory (Azure AD)	Azure Active Directory (Azure AD) es el servicio de administración de identidades y acceso basado en el cloud de Microsoft, que ayuda a tus empleados a iniciar sesión y a acceder a los recursos.
Usuarios finales	Después de asignar los usuarios a sus grupos de aplicaciones, pueden conectarse a una implementación de Azure Virtual Desktop con cualquiera de los clientes de Azure Virtual Desktop.
FSLogix	FSLogix se ha diseñado para perfiles móviles en entornos informáticos remotos, como Azure Virtual Desktop. Almacena un perfil de usuario completo en un solo contenedor.
Grupo de hosts	Un grupo de hosts es una colección de máquinas virtuales de Azure que se registran en Azure Virtual Desktop como hosts de sesión cuando se ejecuta el agente de Azure Virtual Desktop.
MFA	La autenticación multifactor es un proceso en el que se pide al usuario, durante el proceso de inicio de sesión, que introduzca un código en su teléfono móvil o que proporcione un escaneo de sus huellas dactilares.
Conexión de aplicaciones MSIX	La conexión de aplicaciones MSIX es una forma de distribuir aplicaciones MSIX a máquinas físicas y virtuales.
RDS	Servicios de Escritorio remoto es la plataforma IaaS que crea soluciones de virtualización.
Windows 10 Enterprise multisesión	Windows 10 Enterprise multisesión, antes conocido como Windows 10 Enterprise para escritorios virtuales (EVD), es un nuevo host de sesión Escritorio remoto que permite varias sesiones interactivas a la vez.
Área de trabajo	Un área de trabajo es una agrupación lógica de grupos de aplicaciones en Azure Virtual Desktop.
Azure Virtual Desktop	Un servicio de virtualización de escritorios y aplicaciones que se ejecuta en Microsoft Azure.

Tabla 5: Glosario

Acerca del autor

Freek Berson es un arquitecto de soluciones en el cloud especializado en la entrega de aplicaciones y escritorios basados en la tecnología remota. Tiene una larga trayectoria en el espacio de RDS y ha sido premiado como el **profesional más valioso (MVP)** de Microsoft desde 2011.

Freek participa activamente en la comunidad. Interviene en varias conferencias por todo el mundo, incluido Microsoft Ignite, Microsoft Ignite | The Tour, Microsoft TechSummit, Microsoft TechDays, Azure Saturday, BriForum, E2EVC, ExpertsLive y muchos más eventos (online). También es autor de libros publicados.

Trabaja en Wortell, una empresa integradora del cloud con sede en los Países Bajos, donde se centra en la informática de usuario final, sobre todo en la plataforma de Microsoft con un fuerte enfoque en Azure. También es partner administrador de RDS Gurus.

Mantiene su blog personal en themicrosoftplatform.net, donde escribe artículos y entradas de blog relacionados con Azure Virtual Desktop, RDS, Azure, el cloud de Azure y otras tecnologías de Microsoft.

Puedes seguirlo en Twitter en @fberson y consultar sus aportaciones mediante [su cuenta de GitHub](#).