



Microsoft Azure Architect Technologies

Exam Ref AZ-303

Mike Pfeiffer • Derek Schauland
Nicole Stevens • Gurvinder Singh

Ref. De examen AZ-303 Tecnologías de Microsoft Azure Architect

Mike Pfeiffer
Derek Schauland
Gurvinder Singh
Nicole Stevens



Microsoft

Contenido de un vistazo

Expresiones de gratitud

Sobre los autores

Introducción

Capítulo 1 Implementar y monitorear una infraestructura de Azure

Capítulo 2 Implementar soluciones de gestión y seguridad

Capítulo 3 Implementar soluciones para aplicaciones

Capítulo 4 Implementar y administrar plataformas de datos

Índice

Contenido

Introducción

Organización de este libro

Preparándose para el examen

Certificaciones de Microsoft

Acceso rápido a referencias en línea

Erratas, actualizaciones y asistencia para libros

Mantente en contacto

Capítulo 1 Implementar y monitorear una infraestructura de Azure

Habilidad 1.1: Implementar el monitoreo de la infraestructura en la nube

Supervisar la seguridad

Monitorear el desempeño

Supervisar el estado y la disponibilidad

Monitorear el costo

Configurar el registro avanzado

Configurar el registro para cargas de trabajo

Inicie respuestas automáticas mediante el uso de grupos de acción

Configurar y administrar alertas avanzadas

Habilidad 1.2: Implementar cuentas de almacenamiento

Seleccione las opciones de la cuenta de almacenamiento según un caso de uso

Configurar Azure Files y Blob Storage

Administrar claves de acceso

Configurar el acceso de red a la cuenta de almacenamiento

Implementar firmas de acceso compartido y políticas de acceso

Implementar la autenticación de Azure AD para el almacenamiento

Implementar la replicación de Azure Storage

Implementar la conmutación por error de la cuenta de Azure Storage

Habilidad 1.3: Implementar máquinas virtuales para Windows y Linux

Seleccione el tamaño de la máquina virtual

Configurar el almacenamiento para máquinas virtuales

Configurar el cifrado de disco de Azure

Configurar alta disponibilidad

Implementar y configurar conjuntos de escalas

Implementar hosts dedicados de Azure

Habilidad 1.4: Automatizar la implementación y configuración de recursos

Guardar una implementación como plantilla de Azure Resource Manager

Modificar la plantilla de Azure Resource Manager

Evaluar la ubicación de nuevos recursos.

Implementar desde una plantilla

Configurar una plantilla de disco virtual

Administrar una biblioteca de plantillas

Crear y ejecutar un runbook de automatización

Habilidad 1.5: Implementar redes virtuales

Implementar conexiones de red virtual a red virtual

Implementar emparejamiento de redes virtuales

Habilidad 1.6: Implementar Azure Active Directory

Agregar dominios personalizados

Administrar varios directorios

Implementar el restablecimiento de contraseña de autoservicio

Configurar cuentas de usuario para MFA

Configurar alertas de fraude

Configurar opciones de derivación

Configurar direcciones IP confiables

Configurar métodos de verificación

Implementar y administrar cuentas de invitados

Configurar la protección de identidad de Azure AD

Implementar el acceso condicional, incluido MFA

Habilidad 1.7: Implementar y administrar identidades híbridas

Instalar y configurar Azure AD Connect

Opciones de sincronización de identidad

Configurar y administrar la sincronización y la escritura diferida de contraseñas

Configurar el inicio de sesión único

Utilice Azure AD Connect Health

Resumen del capítulo

Experimento mental

Respuestas del experimento mental

Capítulo 2 Implementar soluciones de gestión y seguridad

Habilidad 2.1: Administrar cargas de trabajo en Azure

Configurar los componentes de Azure Migrate

Habilidad 2.2: implementar la recuperación ante desastres mediante Azure Site Recovery

Configurar componentes de Azure de Site Recovery

Configurar componentes locales de Site Recovery

Replica datos en Azure

Migrar mediante Azure Site Recovery

Habilidad 2.3: Implementar la infraestructura de la aplicación

Crea una aplicación lógica simple

Administrador funciones de Azure

Administrador Azure Event Grid

Administrador Azure Service Bus

Habilidad 2.4: Gestionar la seguridad de las aplicaciones

Uso de Azure Key Vault para almacenar y administrar secretos de aplicaciones

Uso de la identidad administrada de Azure Active Directory

Registro de la aplicación de Azure Active Directory

Creación de secretos de aplicación para aplicaciones registradas

Habilidad 2.5: Implementar el equilibrio de carga y la seguridad de la red

Configurar Application Gateway y reglas de equilibrio de carga
Implementar configuraciones de IP de front-end
Administrar el equilibrio de carga de la aplicación
Implementar Azure Load Balancer
Configurar y administrar Azure Firewall
Configurar y administrar Azure Front Door
Implementar Azure Traffic Manager
Administrar y configurar grupos de seguridad de aplicaciones y redes
Grupos de seguridad de red
Grupos de seguridad de aplicaciones
Implementar Azure Bastion
Habilidad 2.6: Integrar una red virtual de Azure y una red local
Crear y configurar Azure VPN Gateway
Crear y configurar VPN de sitio a sitio
Verificar la conectividad local
Administrar la conectividad local con Azure
Configurar ExpressRoute
Habilidad 2.7: implementar y administrar soluciones de gobernanza de Azure
Implementar la política de Azure
Implementación de Azure Blueprint
Implementar y aprovechar los grupos de administración
Habilidad 2.8: Gestionar el control de acceso basado en roles (RBAC)
Crea un rol personalizado
Configurar el acceso a los recursos asignando roles
Configurar el acceso de administración a Azure
Solucionar problemas de RBAC
Resumen del capítulo
Experimento mental
Respuestas del experimento mental

Capítulo 3 Implementar soluciones para aplicaciones

Habilidad 3.1: Implementar una infraestructura de aplicaciones

Crear y configurar Azure App Service

Crear una aplicación web de App Service para contenedores

Configurar redes para un servicio de aplicaciones

Crear y administrar ranuras de implementación

Implementar aplicaciones lógicas

Implementar funciones de Azure

Habilidad 3.2: Implementar aplicaciones basadas en contenedores

Crea una imagen de contenedor

Publicar y automatizar la implementación de imágenes en Azure

Container Registry

Implementar una aplicación que se ejecute en una instancia de contenedor de Azure

Administrar la configuración del contenedor usando código

Configurar el servicio Azure Kubernetes

Resumen del capítulo

Experimento mental

Respuestas del experimento mental

Capítulo 4 Implementar y administrar plataformas de datos

Habilidad 4.1: Implementar bases de datos NoSQL

Configurar tablas de cuentas de almacenamiento

Modelo de datos subyacente del servicio de almacenamiento de tablas de Azure

Crear un servicio de almacenamiento de Azure Table

Configurar el acceso a los datos de almacenamiento de tablas

Elija entre el servicio de almacenamiento de tablas de Azure y la API de tablas de CosmosDB

Azure Cosmos DB

Seleccione las API de Cosmos DB adecuadas

Configurar réplicas en Cosmos DB

Habilidad 4.2: Implementar bases de datos SQL de Azure

Aprovisionar y configurar bases de datos relacionales

[Configuración de la configuración de la base de datos SQL de Azure](#)

[Implementar una instancia administrada de Azure SQL Database](#)

[Configurar HA para una base de datos SQL de Azure](#)

[Publicar una base de datos SQL de Azure](#)

[Resumen del capítulo](#)

[Experimento mental](#)

[Respuestas del experimento mental](#)

Índice

Sobre los autores

Mike Pfeiffer Mike Pfeiffer es un veterano de la industria tecnológica de 20 años que ha trabajado para algunas de las empresas de tecnología más grandes del mundo, incluidas Microsoft y Amazon Web Services (AWS). Es el fundador y tecnólogo jefe de CloudSkills.io, una empresa de consultoría y capacitación en la nube. Mike es autor de Pluralsight, conferencista internacional, Microsoft Azure MVP y presentador del podcast CloudSkills.fm.

Derek Schauland Derek Schauland es un profesional de TI con 20 años de experiencia. Actualmente se especializa en tecnologías en la nube. Pasó 10 años de su carrera como MVP de Microsoft, primero en el almacenamiento del sistema de archivos y luego en la gestión de la nube y del centro de datos. Además de escribir sobre tecnologías en la nube, es coautor de otros tres libros e innumerables artículos y blogs. Fuera del espacio tecnológico, le gusta hacer barbacoas con familiares y amigos.

Gurvinder Singh Gurvinder Singh es un arquitecto de soluciones Azure certificado por Microsoft con 13 años de experiencia diversificada en el desarrollo de software. Tiene una sólida formación en programación y experiencia práctica en .NET y C#. Desde los últimos años, Gurvinder ha estado guiando a las grandes empresas en la transformación de aplicaciones heredadas en una arquitectura nativa de la nube con un enfoque en la migración a Microsoft Azure. Es un apasionado de la tecnología, especialmente con la plataforma Microsoft Azure (PaaS, IaaS y Serverless).

Nicole Stevens Nicole Stevens es directora técnica de un proveedor de software independiente (ISV) en el Reino Unido. Nicole tiene 20 años de experiencia en desarrollo de software, comenzando como un administrador de bases de datos de Oracle en la resolución de problemas de rendimiento, diseño e integración para grandes empresas en EMEA (Europa, Medio Oriente y África). El cambio a una puesta en marcha de ISV trajo nuevos desafíos, con un rol que abarcaba profesionales de TI, consultoría técnica e ingeniero de DevOps. El enfoque actual de Nicole es diseñar soluciones nativas en la nube

mientras ayuda en la refactorización de soluciones de software heredadas para clientes en Azure.

Introducción

El propósito del examen de certificación AZ-303 es probar su comprensión de la arquitectura de soluciones de Microsoft Azure. El examen valida su capacidad para reconocer qué servicios de Azure comprenden una solución en particular y valida su conocimiento de los escenarios de diseño del mundo real y la arquitectura de las soluciones de Microsoft Azure. Este libro proporciona una amplia comprensión de Microsoft Azure que permite a las pequeñas, medianas y grandes empresas que desean adoptar estrategias integrales de innovación y modernización de aplicaciones utilizando las herramientas y servicios de su elección.

Si bien hemos hecho todo lo posible para que la información de este libro sea precisa, Azure está evolucionando rápidamente y existe la posibilidad de que algunas de las pantallas del portal de Azure sean ligeramente diferentes ahora de lo que eran cuando se escribió este libro. También es posible que se hayan producido otros cambios menores, como cambios de nombre, etc.

Azure admite una amplia gama de lenguajes de programación, marcos, bases de datos y servicios. En consecuencia, los profesionales de TI deben aprender rápidamente una amplia gama de temas técnicos. Hay una sobreabundancia de contenido educativo disponible, lo que dificulta encontrar el material adecuado. Este libro corta el contenido superfluo y proporciona la información que necesita para prepararse para el examen.

Este libro cubre todas las áreas temáticas principales que se encuentran en el examen, pero no cubre todas las preguntas del examen. Solo el equipo de examen de Microsoft tiene acceso a las preguntas del examen, y Microsoft agrega periódicamente nuevas preguntas al examen, lo que hace imposible cubrir preguntas específicas. Le recomendamos que considere este libro como un complemento de su experiencia relevante en el mundo real y otros materiales de estudio. Si encuentra un tema en este libro con el que no se siente completamente cómodo, use la opción "¿Necesita más revisión?" enlaces en el texto para encontrar más información y tomarse el tiempo para investigar y estudiar el tema. Hay gran información disponible en la documentación de Microsoft Azure

(<https://docs.microsoft.com/azure>) y Microsoft Learn (<https://microsoft.com/learn>).

ORGANIZACIÓN DE ESTE LIBRO

Este libro está organizado por la lista de "Habilidades medidas" publicada para el examen. La lista "Habilidades medidas" está disponible para cada examen en el sitio web de Microsoft Learn: <http://aka.ms/examlist>. Cada capítulo de este libro corresponde a un área temática principal de la lista, y las tareas técnicas de cada área temática determinan la organización de un capítulo. Si un examen cubre seis áreas temáticas principales, por ejemplo, el libro contendrá seis capítulos.

PREPARÁNDOSE PARA EL EXAMEN

Los exámenes de certificación de Microsoft son una excelente manera de crear su currículum y dejar que el mundo conozca su nivel de experiencia. Los exámenes de certificación validan su experiencia en el trabajo y su conocimiento del producto. Aunque no hay sustituto para la experiencia en el trabajo, la preparación a través del estudio y la práctica pueden ayudarlo a prepararse para el examen. Este libro *no* está diseñado para enseñarle nuevas habilidades.

Le recomendamos que amplíe su plan de preparación para el examen utilizando una combinación de cursos y materiales de estudio disponibles. Por ejemplo, puede usar la Referencia de examen y otra guía de estudio para su preparación "en casa" y tomar un curso del plan de estudios oficial de Microsoft para la experiencia en el aula. Elija la combinación que crea que funciona mejor para usted. Obtenga más información sobre la capacitación presencial disponible y encuentre cursos en línea gratuitos y eventos en vivo en <http://microsoft.com/learn>. Las pruebas de práctica oficiales de Microsoft están disponibles para muchos exámenes en <http://aka.ms/practicetests>.

Tenga en cuenta que esta referencia de examen se basa en información disponible públicamente sobre el examen y la experiencia del autor. Para salvaguardar la integridad del examen, los autores no tienen acceso al examen en vivo.

CERTIFICACIONES DE MICROSOFT

Las certificaciones de Microsoft lo distinguen al demostrar su dominio de un amplio conjunto de habilidades y experiencia con los productos y tecnologías actuales de Microsoft. Los exámenes y las certificaciones correspondientes se desarrollan para validar su dominio de las competencias críticas a medida que diseña y desarrolla, o implementa y brinda soporte, soluciones con productos y tecnologías de Microsoft tanto en las instalaciones como en la nube. La certificación aporta una variedad de beneficios para el individuo y para los empleadores y las organizaciones.

Más información Todas las certificaciones de Microsoft

Para obtener información sobre las certificaciones de Microsoft, incluida una lista completa de las certificaciones disponibles, visite <http://www.microsoft.com/learn>.

ACCESO RÁPIDO A REFERENCIAS EN LÍNEA

A lo largo de este libro hay direcciones de páginas web que el autor le ha recomendado que visite para obtener más información. Algunos de estos enlaces pueden ser muy largos y laboriosos de escribir, por lo que los hemos reducido para que sea más fácil visitarlos. También los hemos compilado en una sola lista a la que los lectores de la edición impresa pueden consultar mientras leen.

Descargue la lista en MicrosoftPressStore.com/ExamRefAZ303/downloads

Las URL están organizadas por capítulo y encabezado. Cada vez que encuentre una URL en el libro, busque el hipervínculo en la lista para ir directamente a la página web.

ERRATAS, ACTUALIZACIONES Y ASISTENCIA PARA LIBROS

Hemos hecho todo lo posible para garantizar la precisión de este libro y su contenido complementario. Puede acceder a las actualizaciones de este

libro, en forma de lista de erratas enviadas y sus correcciones relacionadas, en:

MicrosoftPressStore.com/ExamRefAZ303/errata

Si descubre un error que aún no está en la lista, envíenoslo en la misma página.

Para obtener ayuda e información adicional sobre libros, visite *<http://www.MicrosoftPressStore.com/Support>*.

Tenga en cuenta que el soporte de productos para software y hardware de Microsoft no se ofrece a través de las direcciones anteriores. Para obtener ayuda con el software o hardware de Microsoft, vaya a *<http://support.microsoft.com>*.

MANTENTE EN CONTACTO

¡Sigamos con la conversación! Estamos en Twitter: *<http://twitter.com/MicrosoftPress>*.

Capítulo 1

Implementar y monitorear una infraestructura de Azure

Trabajando como arquitecto de soluciones en la nube de Microsoft Azure, diseñará soluciones y se relacionará con profesionales de TI que implementarán su diseño. Entonces, ¿por qué el examen de certificación AZ-303 requiere que sepa cómo implementar y configurar recursos? Como arquitecto, debe comprender cómo se vinculan los recursos para crear una solución que cumpla con los requisitos de sus clientes, al tiempo que se adhiere a los pilares de una gran arquitectura:

- ■ Optimización de costos
- ■ Excelencia operativa
- ■ Eficiencia en el desempeño
- ■ Fiabilidad
- ■ Seguridad

Para lograr esto, se requiere una comprensión profunda de cómo se implementa y configura cada recurso subyacente. El examen AZ-303 espera que demuestre este conocimiento a través de laboratorios prácticos, tanto a través del portal de Azure como en la línea de comandos.

Una vez que su diseño se implementa y comienza a moverse por las etapas de desarrollo y prueba, necesita comentarios para asegurarse de que se mantengan estos pilares. No tiene mucho sentido tener una solución en producción que sea cara, que falle constantemente y sea insegura. La supervisión de la infraestructura durante el desarrollo, las pruebas y la producción proporciona una retroalimentación continua en cada etapa y garantiza que su producto no falle ni se vuelva inseguro.

Cada recurso en Azure se puede configurar para que la supervisión envíe comentarios a ubicaciones centralizadas. El examen de certificación AZ-303 espera que demuestre una sólida comprensión del monitoreo. Debe saber cómo configurar sus recursos para el

monitoreo, cómo recopilar los datos y cómo se pueden visualizar para identificar posibles problemas y fallas.

La certificación Azure Solution Architect es un título de nivel experto, por lo que se espera que tenga al menos capacidades de configuración de Azure de nivel intermedio. También se espera que tenga conocimientos básicos de creación de scripts con la CLI de Azure y los módulos de Azure PowerShell.

Habilidades cubiertas en este capítulo:

- ■ [Habilidad 1.1: Implementar el monitoreo de la infraestructura en la nube.](#)
- ■ [Habilidad 1.2: Implementar cuentas de almacenamiento](#)
- ■ [Habilidad 1.3: implementar máquinas virtuales para Windows y Linux](#)
- ■ [Habilidad 1.4: Automatizar la implementación y configuración de recursos.](#)
- ■ [Habilidad 1.5: Implementar redes virtuales](#)
- ■ [Habilidad 1.6: Implementar Azure Active Directory](#)
- ■ [Habilidad 1.7: implementar y administrar identidades híbridas](#)

HABILIDAD 1.1: IMPLEMENTAR EL MONITOREO DE LA INFRAESTRUCTURA EN LA NUBE

La supervisión continua de las aplicaciones y la infraestructura permitirá a sus clientes responder con más rapidez a los problemas y cambios. Las respuestas a las alertas generadas por un sistema bien supervisado se pueden automatizar, lo que significa que, en algunas circunstancias, una aplicación puede recuperarse automáticamente. Hay muchas soluciones de monitoreo dentro de Azure, cada una con sus propios casos de uso y configurabilidad. Como arquitecto de soluciones, necesita una excelente comprensión de qué solución de monitoreo se adapta a cada caso de uso. Esta habilidad analiza algunas de las opciones de supervisión disponibles para usted, lo que supervisan y cómo configurarlas.

Esta habilidad cubre cómo:

- ■ Supervisar la seguridad
- ■ Supervisar el rendimiento
- ■ Supervisar el estado y la disponibilidad
- ■ Supervisar el costo
- ■ Configurar el registro avanzado
- ■ Configurar el registro para cargas de trabajo
- ■ Iniciar respuestas automáticas mediante el uso de grupos de acción.
- ■ Configurar y administrar alertas avanzadas

Supervisar la seguridad

La reputación de sus clientes está vinculada a la seguridad de sus sistemas; por lo tanto, como arquitecto, debe saber diseñar sistemas seguros. Esta es solo una parte del rompecabezas; no puede asumir que su diseño es a prueba de balas. También debe poder instruir a sus clientes sobre cómo monitorear los sistemas continuamente para detectar posibles ataques y mitigar las amenazas antes de que los datos se pongan en riesgo.

Hay varios exámenes de seguridad disponibles para Azure, aunque para este examen, debe conocer las opciones disponibles para monitorear la seguridad y sus casos de uso de alto nivel.

Centro de seguridad de Azure

Al diseñar soluciones en Azure, existe una responsabilidad compartida entre el cliente y Azure para garantizar que los recursos se mantengan seguros. Azure Security Center es un sistema de administración de seguridad de la infraestructura diseñado para ayudar a mitigar los desafíos de seguridad que conlleva el traslado de cargas de trabajo a la nube:

- ■ **Falta de habilidades de seguridad.** Es posible que sus clientes no cuenten con las habilidades internas tradicionales y el capital necesario para asegurar una infraestructura compleja.

- ■ **Aumento de la sofisticación de los ataques.** Los ataques son cada vez más sofisticados, ya sea que sus cargas de trabajo estén en la nube, en las instalaciones o sean parte de una nube híbrida y una configuración local.
- ■ **Infraestructura que cambia con frecuencia.** Debido a la flexibilidad de la nube, la arquitectura puede cambiar rápidamente, generando vectores de ataque en constante movimiento.

El centro de seguridad viene en dos niveles: gratuito y estándar:

- ■ **Nivel gratuito.** El nivel gratuito está habilitado de forma predeterminada y proporciona recomendaciones de seguridad en las máquinas virtuales de Azure y los servicios de aplicaciones.
- ■ **Nivel estándar.** El nivel estándar aumenta la supervisión de cualquier VM en la nube y cargas de trabajo de VM híbridas. El nivel estándar también incluye algunos de los servicios PaaS más utilizados, como datos, almacenamiento y contenedores.

Cuando activa Security Center para cualquiera de los niveles, se requiere un agente de supervisión para la mayoría de las evaluaciones de seguridad. Puede configurar Security Center para implementar automáticamente el agente de Log Analytics en máquinas virtuales de Azure, aunque los servicios PaaS (plataforma como servicio) no requieren configuración adicional. Para máquinas virtuales locales y en la nube, el agente de Log Analytics debe instalarse manualmente. Una vez que los agentes están instalados y configurados, Security Center comienza a evaluar el estado de seguridad de todas sus máquinas virtuales, redes, aplicaciones y datos. El motor de análisis de Security Center analiza los datos devueltos por los agentes para proporcionar un resumen de seguridad, como se muestra en la [Figura 1-1](#).

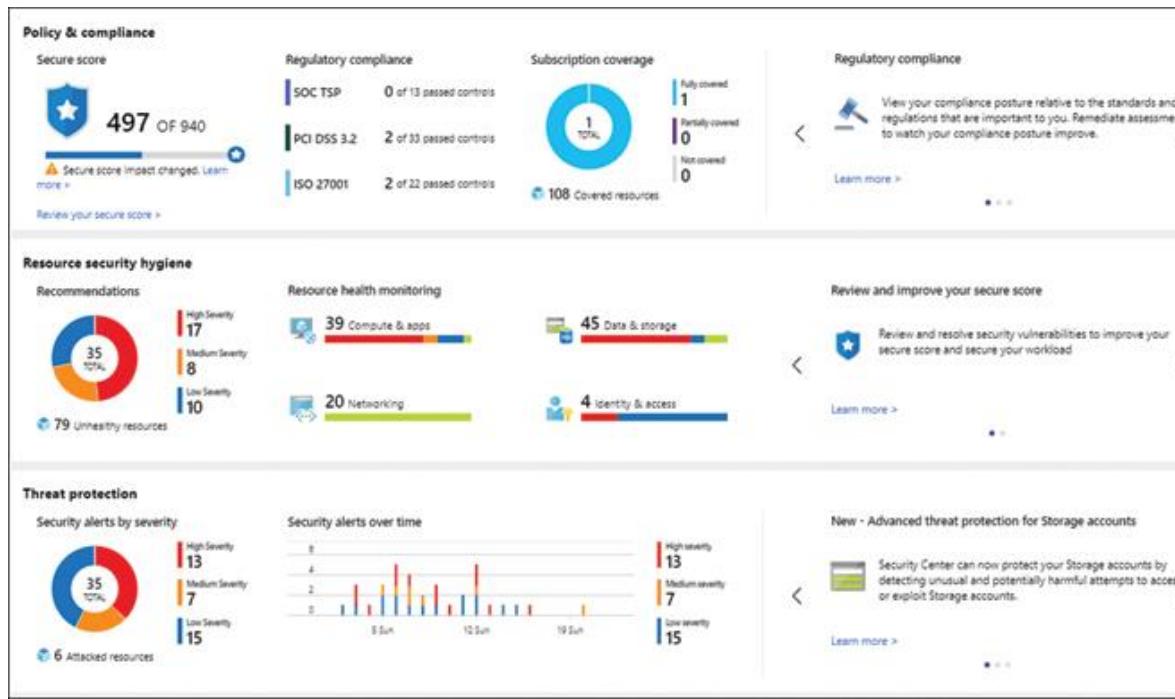


FIGURA 1-1 Hoja de descripción general del centro de seguridad

La Figura 1-1 proporciona una excelente descripción general de las características principales del nivel estándar de Security Center:

- **Política y cumplimiento.** Esta sección incluye la puntuación segura, que es un indicador clave de cómo está protegida su infraestructura. Security Center evalúa los recursos de sus suscripciones y organización para detectar problemas de seguridad. Secure Score es una agregación de problemas de seguridad identificados y sus correspondientes niveles de riesgo. Cuanto mayor sea la puntuación de seguridad, menor será el riesgo. La sección de cumplimiento rastrea si se están siguiendo las regulaciones para estándares como ISO 27001 y PCI DSS.
- **Higiene de seguridad de recursos.** Esta sección proporciona recomendaciones sobre recursos y redes. Explore los menús para ver recomendaciones y corregirlas para mejorar su postura de seguridad y la puntuación segura.
- **Protección contra amenazas.** Los registros de los recursos informáticos y de datos se pasan a través de algoritmos para el análisis del comportamiento, la detección de anomalías y

la inteligencia de amenazas integrada para buscar posibles amenazas. Las alertas se crean según la gravedad.

El nivel estándar también incluye acceso justo a tiempo (JIT) para máquinas virtuales de Azure. Con el acceso JIT habilitado en una máquina virtual, un administrador puede solicitar acceso desde un rango de IP durante un período de tiempo específico. Si el administrador tiene los permisos de RBAC correctos, Azure crea una regla de red y se le concede acceso al administrador. Una vez transcurrido el tiempo especificado, Azure quita la regla de red para revocar el acceso.

Centinela azur

Azure Sentinel es una solución de gestión de eventos e información de seguridad (SIEM) orquestada por la seguridad y respuesta automatizada (SOAR). Security Center se utiliza para recopilar datos y detectar vulnerabilidades de seguridad. Azure Sentinel se extiende más allá al incorporar herramientas para ayudar a sus clientes a buscar amenazas y luego investigarlas y responder a ellas, todo a escala empresarial:

- ■ **Recopila datos a escala de la nube.** Los datos recopilados incluyen otros datos en la nube, locales, Microsoft 365 y Advanced Threat Protection.
- ■ **Detecte amenazas no detectadas.** Las amenazas se detectan mediante análisis e inteligencia de amenazas de Microsoft.
- ■ **Investigue amenazas con IA.** Puede buscar actividades sospechosas a gran escala.
- ■ **Responder a incidentes.** Azure Sentinel incluye orquestación y automatización integradas de tareas comunes.

Azure Sentinel requiere un área de trabajo de Log Analytics cuando está habilitado y se factura en función de la cantidad de datos ingeridos desde el área de trabajo.

Monitorear el desempeño

Una vez que las aplicaciones que han diseñado sus clientes entran en producción, es probable que el tiempo de respuesta sea uno de los principales KPI en los que estén interesados sus usuarios. El rendimiento debe ser monitoreado para que sus clientes conozcan los problemas

potenciales antes que los usuarios de la aplicación. En esta sección se analiza cómo configurar recursos para la supervisión del rendimiento y cómo Azure Monitor puede usar estos datos para buscar problemas de rendimiento.

Configurar la configuración de diagnóstico en los recursos

Azure genera automáticamente información de auditoría y diagnóstico en toda la plataforma en forma de registros de la plataforma. Los registros de plataforma son invaluables para un arquitecto porque contienen información generada en diferentes capas de Azure:

- ■ **Registro de actividad.** Todas las operaciones de escritura (PUT, POST, DELETE) en un recurso (el plano de gestión). Con seguimiento a nivel de suscripción, este registro contiene quién realizó el cambio, desde dónde se realizó un cambio y cuándo se realizó un cambio.
- ■ **Registro de Azure Active Directory.** Este es un tren de auditoría completo y seguimiento de la actividad de inicio de sesión para Azure Active Directory.
- ■ **Registros de recursos.** Los registros de recursos están disponibles para las operaciones que se realizaron dentro de un recurso (el plano de datos). Por ejemplo, se pueden registrar una solicitud en una aplicación web o el número de veces que se ha ejecutado una aplicación lógica. El detalle del registro de recursos varía según el tipo de recurso porque cada recurso ofrece un servicio diferente.

Esta información le da al arquitecto una vista de lo que está sucediendo actualmente en la (s) aplicación (es) de sus clientes y lo que sucedió anteriormente.

El registro de actividad y el registro de Azure Active Directory están disponibles automáticamente para verlos en el portal de Azure. Los registros de recursos deben configurarse a nivel de recursos a través de la configuración de diagnóstico antes de que se puedan ver. La configuración de los parámetros de diagnóstico tiene los mismos pasos genéricos, independientemente del tipo de recurso.

Plataforma como servicio (PaaS)

Siga estos pasos en un recurso de plataforma como servicio (PaaS) para habilitar la configuración de diagnóstico:

1. Vaya a la hoja de menú de un recurso de PaaS en Azure Portal. Desplácese hacia abajo hasta **Supervisión** y haga clic en **Configuración de diagnóstico**. Se abre la hoja **Configuración de diagnóstico**, que muestra una lista de configuraciones que se pueden transmitir a otros destinos. Haga clic en **Agregar configuración de diagnóstico** para configurar la recopilación de datos.
2. Al hacer clic en **Agregar**, se abre la hoja **Configuración de configuración de diagnóstico**, como se muestra en la [Figura 1-2](#).

The screenshot shows the 'Diagnostics setting' configuration page. At the top, there are buttons for Save, Discard, Delete, and Provide feedback. Below this, a descriptive text explains that a diagnostic setting specifies categories of logs and metrics to collect from a resource and send to a destination. A note states that normal usage charges apply for the destination log.

The main area is divided into 'Category details' and 'Destination details'.

Category details:

- log:** WorkflowRuntime is selected with a retention of 7 days.
- metric:** AllMetrics is selected with a retention of 7 days.

Destination details:

- Send to Log Analytics:** Checked.
- Subscription:** Free Trial.
- Log Analytics workspace:** az303la (uksouth).
- Archive to a storage account:** Checked.
- Location:** UK South.
- Subscription:** Free Trial.
- Storage account:** 112diagsettingsssa.
- Stream to an event hub:** Unchecked.

Informational notes provide details about retention policy and storage account charges.

FIGURA 1-2 Configure los ajustes de diagnóstico

3. En el campo **Nombre de configuración de diagnóstico**, agregue un nombre exclusivo para esta configuración de diagnóstico en el recurso.
4. En **Detalles de la categoría**, seleccione todas las categorías de datos que desee recopilar:
 1. **■ Registro.** Estos son los registros de recursos. Las categorías de registro diferirán según el tipo de recurso elegido. Esta captura de pantalla es de una aplicación lógica.
 2. **■ Métrica.** Al elegir esta opción, se transmitirán datos métricos numéricos en un formato de serie temporal sobre este recurso.
5. En **Detalles del destino**, seleccione al menos un destino para las categorías elegidas para transmitir a:
 0. **■ Log Analytics.** Marque esto para transmitir datos a un espacio de trabajo de Log Analytics. Para obtener más información sobre Log Analytics, consulte "Configurar un espacio de trabajo de Log Analytics", más adelante en este capítulo. Si se selecciona **Log Analytics**, es obligatorio seleccionar la **Suscripción y el Espacio de trabajo de Log Analytics**, que recibirá los datos, como se muestra en la [Figura 1-2](#).
 1. **■ Archivar en una cuenta de almacenamiento.** Marque esto para archivar las categorías elegidas en una cuenta de almacenamiento; esta opción es más útil si se requiere una auditoría futura del recurso. Una vez que haya elegido esta opción, el punto de entrada **Retención (Días)** se habilita con un valor de 0 para cada categoría seleccionada, como se muestra anteriormente en la [Figura 1-2](#). Edite este valor numérico para establecer el número de días que debe conservarse cada categoría. Si cambia este valor más tarde, solo tendrá efecto en los nuevos registros y métricas almacenados. Las métricas y los registros antiguos se conservarán durante el período de retención original. Si se selecciona **Archivar en cuenta de almacenamiento**, una **Cuenta de suscripción y almacenamiento** debe seleccionarse de los menús desplegables respectivos, como se muestra anteriormente en la [Figura 1-2](#).

2. ■ **Transmitir a un centro de eventos.** Seleccione esta opción para enviar datos de diagnóstico a un centro de eventos. El envío de datos a un centro de eventos permite la transmisión de datos fuera de Azure a aplicaciones de terceros, como el software de administración de eventos e información de seguridad (SIEM). Si se selecciona **Transmitir a un centro de eventos**, se deben completar los campos **Suscripción** y **Espacio de nombres del centro de eventos**.
6. Una vez elegida la configuración de diagnóstico, haga clic en **Guardar** en la parte superior izquierda para guardar las opciones. Las categorías y destinos seleccionados ahora se muestran en la hoja **Configuración de diagnóstico** y los datos se enviarán automáticamente a los destinos elegidos.

La configuración de diagnóstico también se puede administrar en la línea de comandos a través de PowerShell mediante el cmdlet `Set-AzDiagnosticSetting` o el comando de la CLI de Azure `az monitor diagnostic-settings`. Por ejemplo, para habilitar categorías de registro específicas para una base de datos de Azure SQL, ejecute este comando en PowerShell:

[Haga clic aquí para ver la imagen del código](#)

```
Set-AzDiagnosticSetting -Name sqldb112-diagsettings '  
-ResourceId $ dbResource.ResourceId '  
-Categoría QueryStoreRuntimeStatistics,  
QueryStoreWaitStatistics, Errores,  
DatabaseWaitStatistics, Deadlocks -Enabled $ true '  
-StorageAccountId $ storageResource.ResourceId '  
-WorkspaceId $ workspaceResource.ResourceId
```

Máquinas virtuales de Azure

Las máquinas virtuales de Azure no forman parte de PaaS. En cambio, forman parte de la oferta de infraestructura como servicio (IaaS) de Azure y usted las administra. Para que una máquina virtual de Azure

registre datos, se debe instalar la extensión de diagnóstico de Azure. Al hacerlo, se configura un agente de Azure Monitor en la máquina virtual. La extensión de diagnóstico es una extensión de máquina virtual de Azure, lo que significa que se puede instalar a través de una plantilla ARM o en la línea de comandos. También se puede instalar a través del portal de Azure. El nombre de la extensión varía según el sistema operativo. Para Windows, es la extensión de diagnóstico de Windows Azure (WAD); para Linux, es la extensión de diagnóstico de Linux (LAD). Para instalar cualquiera de las extensiones a través de Azure Portal, navegue hasta el elemento de menú **Configuración de diagnóstico** de cualquier máquina virtual de Azure. Tendrás la opción de elegir **Habilite la supervisión a nivel de invitado** si la extensión de diagnóstico aún no se ha instalado. Una vez instaladas, las pestañas para métricas y registro se habilitan dentro de la hoja **Configuración de diagnóstico**. La cantidad de pestañas y su contenido configurable dependen del sistema operativo de la VM. Para una máquina virtual de Windows, se muestran estas pestañas:

- ■ **Descripción general.** Esta es una página de resumen que muestra las opciones seleccionadas en las otras pestañas.
- ■ **Contadores de rendimiento.** Elija **Básico** para elegir entre grupos de contadores que se recopilarán, como **CPU**, **Memoria** y **Disco**. Elija **Personalizado** para elegir contadores específicos.
- ■ **Registros.** Elija **Básico** para elegir entre agrupaciones de registros de **aplicaciones**, **seguridad** y **sistema** que se recopilarán, o elija **Personalizado** para seleccionar registros y niveles específicos mediante una expresión XPath, registros IIS, registros de aplicaciones .Net y seguimiento de eventos para Windows (ETW). también se seleccionará para la colección.
- ■ **Volcados accidentales.** Recopile volcados completos o mini para procesos seleccionados.
- ■ **Fregaderos.** Opcionalmente, puede enviar datos a Azure Monitor o Application Insights.
- ■ **Agente.** Si el agente de diagnóstico no funciona correctamente, se puede quitar de esta pestaña y luego volver a instalarlo. También puede editar el **nivel de registro**, el espacio

máximo en disco local (**cuota de disco**) y la **cuenta de almacenamiento** para el agente.

Si ha creado una máquina virtual Linux, verá las siguientes pestañas:

- ■ **Descripción general.** Esta es una página de resumen que muestra las opciones seleccionadas de las otras pestañas.
- ■ **Métricas.** Elija **Básico** para elegir entre grupos de métricas que se recopilarán, como **Procesador**, **Memoria** y **Red**, y sus frecuencias de muestreo. Si elige **Personalizado**, A continuación, puede elegir **Agregar nueva métrica** o **Eliminar** métricas específicas, y puede establecer frecuencias de muestreo individuales.
- ■ **Syslog.** En esta pestaña, puede elegir qué servicios de syslog recopilar y el nivel de gravedad en el que desea recopilarlos.
- ■ **Agente.** Si el agente de diagnóstico no funciona correctamente, se puede quitar de esta pestaña y luego volver a instalarlo. Además, puede **elegir una cuenta de almacenamiento** para el agente.

Nota Configuración de diagnóstico y extensión de diagnóstico

No todos los servicios tienen el elemento de menú **Configuración de diagnóstico** en sus hojas de menú. Cuando falta la opción **Configuración de diagnóstico**, navegue hasta el grupo de recursos y haga clic en **Configuración de diagnóstico**. Si se puede habilitar la **Configuración de diagnóstico** para el servicio, aparecerá en la lista. Por ejemplo, las puertas de enlace VPN deben configurarse de esta manera. Si planea usar la extensión de Log Analytics en una máquina virtual Linux, debe instalarla antes que la extensión de diagnóstico.

Cree una línea de base de rendimiento para los recursos

Los recursos de base le brindan a sus clientes una visión de cómo es el comportamiento esperado de los recursos. Cuando ocurre una degradación del rendimiento, sus clientes pueden utilizar sus líneas de base de recursos para ayudar en sus análisis y resolución de fallas.

Azure Monitor recopila dos tipos principales de datos:

- **Métricas.** Series de tiempo y valores o recuentos medidos numéricamente, como el uso de la CPU o las esperas
- **Registros.** Eventos y archivos de seguimiento

Las métricas en Azure Monitor forman la línea de base, brindando una vista de series temporales de sus recursos. Puede ver una vista de métricas para la mayoría de los recursos individuales eligiendo el menú **Métricas** con el recurso en sí. Puede usar esto para crear una vista de cómo se está desempeñando su recurso. A continuación, se muestra un ejemplo de una máquina virtual de Azure:

1. En Azure Portal, navegue a cualquier máquina virtual y haga clic en **Métricas** en la hoja de menú **Máquina virtual**.
2. Ahora debe elegir las métricas para agregar al gráfico. El alcance ya ha sido seleccionado para usted: es la VM. Seleccione una métrica en el menú **Métricas** y luego seleccione una agregación en el menú **Agregación**. Haga clic fuera de la métrica y se agregará al gráfico.
3. Para agregar una nueva métrica, haga clic en **Agregar métrica** y repita el paso 2. Repita este proceso hasta que todas las métricas que necesita estén presentes en el gráfico.

La Figura 1-3 muestra un gráfico de métricas, con el rendimiento de la CPU durante las últimas 24 horas, lo que sugiere que es posible que esta VM deba ampliarse.

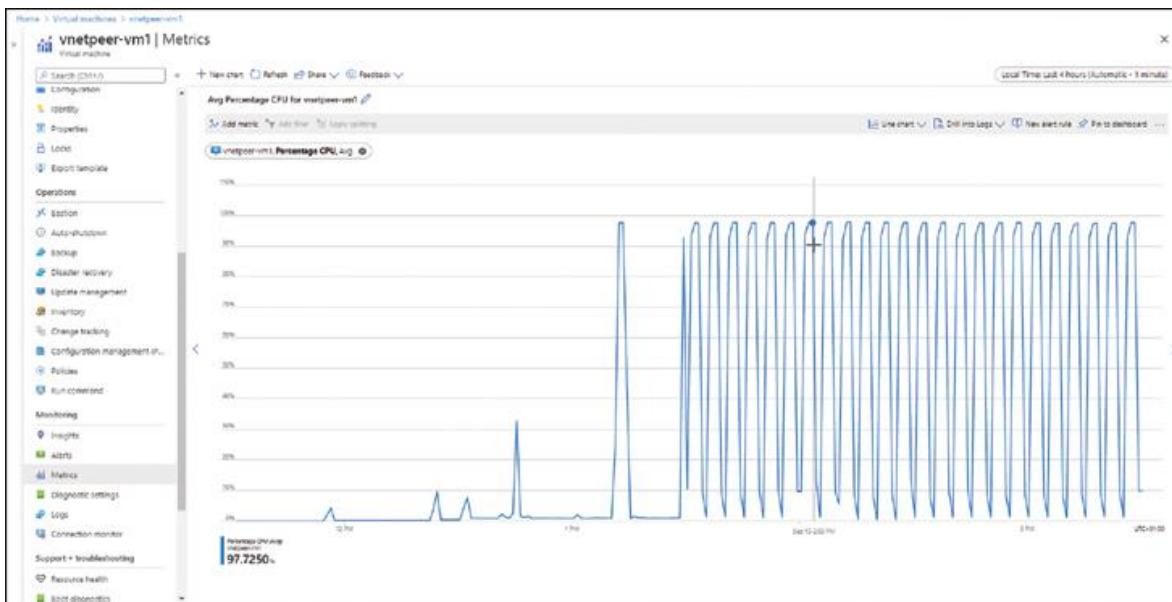


FIGURA 1-3 Cuadro de métricas para el uso de CPU de VM

4. Una vez completado, puede optar por agregar el gráfico a su panel de Azure Portal haciendo clic en **Anclar al panel**. Para navegar a una página de panel, haga clic en el ícono de menú en la parte superior izquierda de cualquier página de Azure, haga clic en **Panel** y elija el nombre del panel al que agregó el gráfico.

Supervisar los recursos no utilizados

Debido a la flexibilidad de Azure, puede ser fácil para sus clientes tener recursos no utilizados o infrautilizados ocultos dentro de sus suscripciones. Con la facturación de pago por minuto o por hora, el costo de un recurso no utilizado podría afectar el gasto considerablemente. Azure Advisor contiene recomendaciones de costos que cubren lo siguiente:

- ■ **VM infrautilizadas.** Estas son máquinas virtuales que pueden reducirse o desasignarse.
- ■ **Orígenes de bases de datos de tamaño adecuado.** Se puede reducir el tamaño de Azure SQL, MySQL o MariaDB.
- ■ **Puertas de enlace de red inactivas.** Estas son puertas de enlace de redes virtuales que no se han utilizado durante 90 días o más y podrían eliminarse.
- ■ **Instancias reservadas de VM / PaaS.** Puede comprar capacidad por adelantado para ahorrar costos según el uso de PaaS (plataforma como servicio) y VM.

Las recomendaciones de Azure Advisor son gratuitas y puede acceder a Azure Advisor a través del portal de Azure:

1. Busque **Azure Advisor** en la barra de recursos de búsqueda en Azure Portal. Seleccione **Azure Advisor** en el menú desplegable que se abre en la barra de búsqueda mientras escribe el nombre del recurso. Se carga la página de descripción general de **Azure Advisor**, como se muestra en la Figura 1-4; el resumen de **costos** se muestra en la parte superior izquierda.

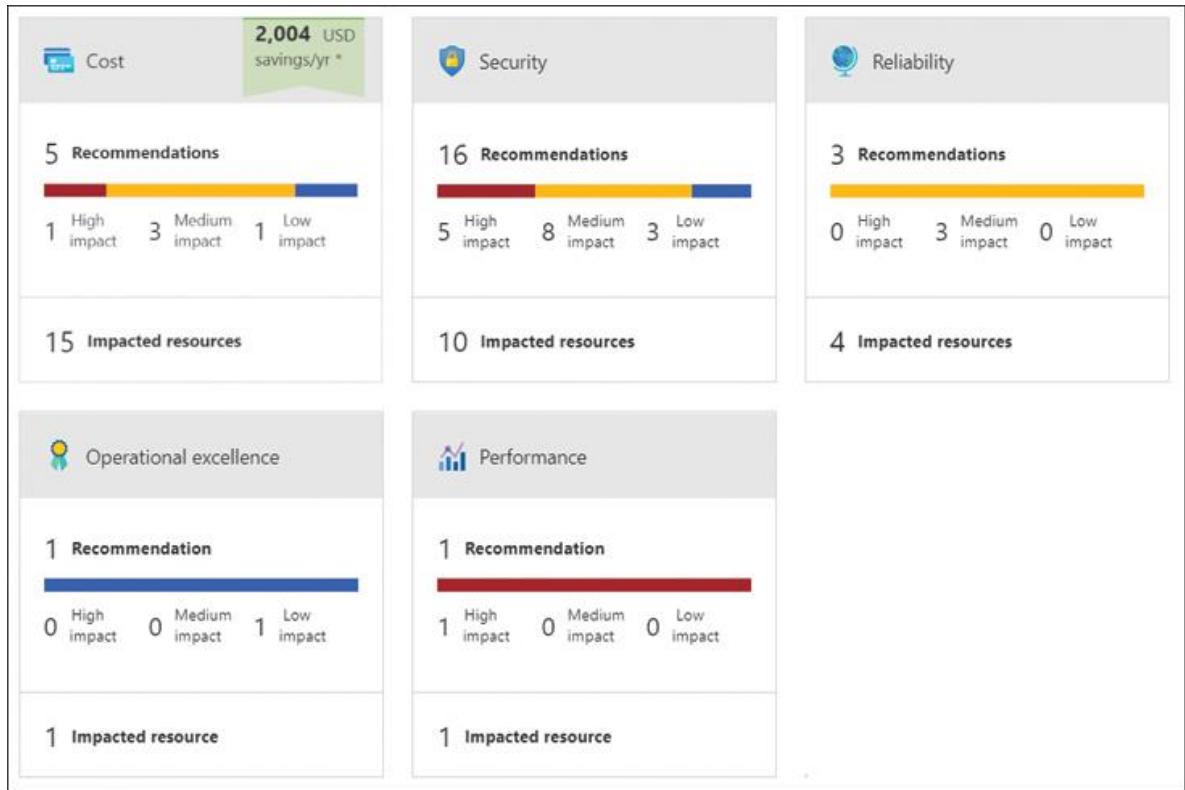


FIGURA 1-4 Hoja de descripción general de Azure Advisor

2. Haga clic en el cuadro **Costo** para profundizar en las recomendaciones. Cada recomendación se muestra como **Impacto alto**, **Impacto medio** o **Impacto bajo**, y la cantidad y el tipo de **Recursos afectados** se muestran en la parte inferior de cada recomendación. Los posibles ahorros de costos anuales se muestran en la parte superior derecha del cuadro **Costos**.

Supervisar la capacidad de rendimiento

Azure Monitor puede recopilar datos de muchas fuentes diferentes a través de una variedad de agentes. En un entorno híbrido, sus clientes necesitarán una vista única de toda su organización. Para ofrecer esta funcionalidad, sus clientes deberán combinar las métricas de carga de trabajo local con las de Azure. El agente de diagnóstico para máquinas virtuales solo recopilará datos de máquinas virtuales de Azure; no admite máquinas virtuales locales.

El agente de Log Analytics recopilará datos de máquinas virtuales de Azure, máquinas virtuales locales y máquinas virtuales administradas por System Center Operations Manager (SCOM). El Agente de Log Analytics

también se conoce como "Agente de OMS Linux" o "Agente de supervisión de Microsoft (Windows)". El agente de Log Analytics se puede instalar en una máquina virtual de Azure desde la sección **Máquinas virtuales** de un área de trabajo de **Log Analytics**. La instalación en una máquina local requiere que el agente se descargue e instale desde la línea de comandos.

Los datos de la máquina virtual recopilados por el agente de Log Analytics se pueden ver en el registro de Azure Monitor. Azure Monitor Log usa KQL (Kusto Query Language) para crear informes sobre los datos mediante consultas. Azure Monitor Log viene con consultas integradas para ayudarlo a comenzar. Para ver sus datos mediante estas consultas, inicie sesión en Azure Portal y siga estos pasos:

1. Busque **Monitor** en la barra de recursos de búsqueda en la parte superior de Azure Portal. (Tenga en cuenta que Azure Monitor aparece en Azure Portal como **Monitor**). Seleccione **Monitor** en el menú desplegable que se abre en la barra de búsqueda mientras escribe el nombre del recurso.
2. Elija **Registros** en el panel izquierdo. Los registros de Azure Monitor se abren con la página **Consultas de ejemplo**. Desplácese por la sección **Todas las consultas**, donde puede ver la lista de recursos de Azure que tienen consultas de ejemplo.
3. Desplácese hasta la parte inferior y elija **Otro > Uso de memoria y CPU**. El KQL de ejemplo se carga en el panel de consultas. Haga clic en **Ejecutar** para ejecutar la consulta y ver los resultados.
4. Haga clic en **Seleccionar alcance**, que se encuentra a la izquierda de **Ejecutar**. Aquí, puede elegir el alcance en el que se ejecutará su consulta. Seleccione un grupo de recursos que contenga máquinas virtuales que envían datos a Log Analytics. Haga clic en **Aplicar**; volverá al Editor de consultas, donde el ámbito seleccionado se encuentra ahora a la izquierda de **Seleccionar ámbito**. Haga clic en **Ejecutar**; los datos devueltos están restringidos al alcance seleccionado, que es el grupo de recursos que acaba de seleccionar.
5. Ahora modifique el KQL editándolo directamente. En la Figura 1-5, el KQL se ha editado a partir del seleccionado en el Paso 3 anterior. El filtro de predicado `TimeGenerated > ago (2h)` se ha establecido en 2 horas y el resumen de los valores devueltos, `bin (TimeGenerated, 2m)`, se agrupa en 2 minutos.



FIGURA 1-5 Capacidad de visualización a través de registros de Azure Monitor



Consejo de examen KQL

Es importante tener un conocimiento básico del lenguaje KQL para el examen, aunque esto puede ser difícil sin acceso a la infraestructura que está creando datos para consultar. Microsoft proporciona una base de datos de tutoriales y un portal de análisis de registros de demostración. Se puede acceder a estos para practicar en <https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/tutorial> y <https://portal.loganalytics.io/demo>.

¿Necesita más revisión? Registros de Azure Monitor

El ejemplo de la [Figura 1-5](#) muestra un caso de uso único para los registros de Azure Monitor. Para obtener más información sobre la gran cantidad de servicios cuyos datos se pueden extraer a través de registros y métricas, visite <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-logs>.

Visualice los datos de diagnóstico con Azure Monitor

Azure Monitor puede recopilar datos de muchas fuentes diferentes a través de una variedad de agentes. Sus clientes encontrarán la gran cantidad de datos casi imposible de analizar sin una representación

gráfica de los datos. Ya ha visto cómo Azure Monitor puede anclar gráficos a su panel, pero puede tener más capacidades de visualización mediante el uso de libros de trabajo de Azure Monitor, que leen métricas y registros de Log Analytics para crear visualizaciones de datos en múltiples fuentes. Azure Monitor viene precargado con plantillas de libros de trabajo, que permiten a sus clientes ver información sobre sus recursos, como identificar máquinas virtuales con poca memoria o uso de CPU alto o ver la capacidad de almacenamiento de sus cuentas de almacenamiento. Todas las plantillas pueden informar a través de una suscripción. Para ver la plantilla de libro de análisis de rendimiento en Azure Monitor, siga estos pasos:

1. Busque **monitor** en la barra de recursos de búsqueda en la parte superior de Azure Portal. (Tenga en cuenta que Azure Monitor aparece en Azure Portal como **Monitor**). Seleccione **Monitor** en el menú desplegable que se abre en la barra de búsqueda mientras escribe el nombre del recurso.
2. En el menú de Azure Monitor, haga clic en **Libros** y, en la **Galería**, en **Máquinas virtuales** , haga clic en **Métricas clave** .
3. Elija la suscripción que desea ver y el espacio de trabajo de Log Analytics en el que sus máquinas virtuales registran métricas. Elija un **intervalo de tiempo** para filtrar aún más los datos. La visualización del libro de trabajo se carga con la pestaña **Descripción general** seleccionada. La pestaña **Descripción general** muestra el uso de CPU para todas las máquinas virtuales en la suscripción seleccionada.
4. Haga clic en la pestaña **Métricas clave** para ver las métricas clave del uso de la CPU, el disco y la red en un formato tabular, como se muestra en la [Figura 1-6](#) .

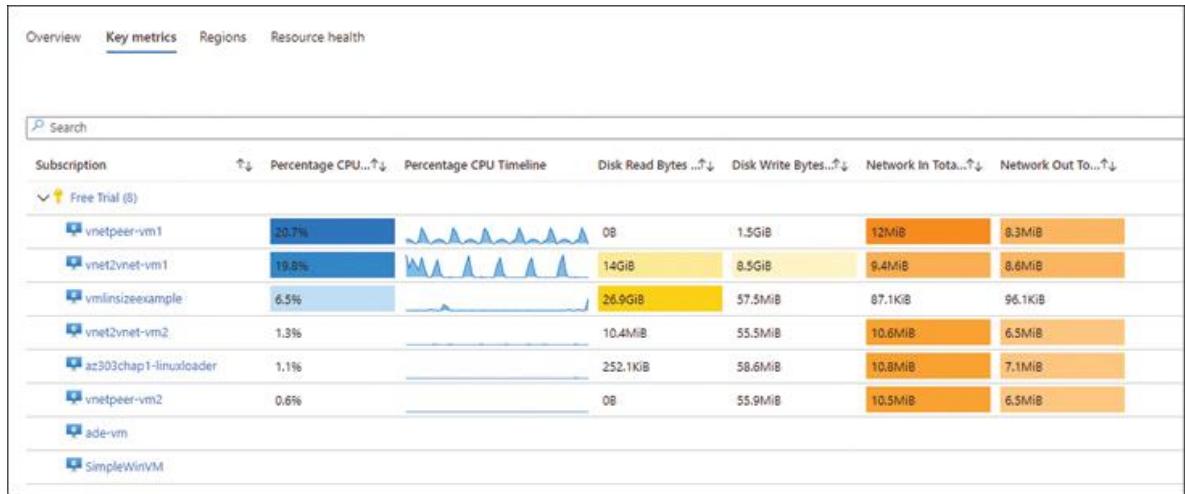


FIGURA 1-6 Plantilla de libro de trabajo de métricas clave que muestra el uso de CPU, disco y red para máquinas virtuales

5. Haga clic en las otras pestañas. La pestaña **Regiones** muestra el mayor uso de CPU en cada región de Azure donde la suscripción contiene una máquina virtual. La pestaña **Resource Health** muestra el estado de cada máquina virtual en la suscripción. Al hacer clic en la máquina virtual en la pestaña **Estado de recursos**, se accederá a la hoja **Estado de recursos** de la máquina virtual.
6. Regrese a la **Galería** a la que navegó en el Paso 2 y explore los otros libros de trabajo disponibles para máquinas virtuales.

Si sus gráficos no se cargan, es porque las estadísticas de VM no se han configurado para las VM. Esto también se indica mediante un signo de exclamación rojo y un **No incorporado que** aparece a la derecha del menú desplegable **Intervalo de tiempo**. Para configurar conocimientos de VM, consulte "Configurar el registro para cargas de trabajo", más adelante en este capítulo. Regrese a la **Galería** para explorar las otras plantillas disponibles para usted.

Azure Monitor también puede enviar datos de registro y métricas a otras fuentes para su análisis, como Power BI, donde se pueden combinar más fuentes de datos para crear informes comerciales. Los paneles operativos se pueden crear con Grafana. (Puede hacerlo instalando el complemento Azure Monitor desde Grafana). Grafana es una plataforma de código abierto que se utiliza principalmente para detectar y clasificar incidentes de operaciones.

Supervisar el estado y la disponibilidad

Comprender cómo monitorear el estado de la infraestructura de aplicaciones de sus clientes es clave para detectar problemas potenciales y reducir el tiempo de inactividad. Debido a que la infraestructura de aplicaciones de sus clientes usa servicios de Azure y estos servicios pueden verse afectados por el tiempo de inactividad relacionado con el servicio, sus clientes pueden requerir alertas si un servicio subyacente deja de estar disponible. Esta sección analiza los métodos para hacer precisamente eso.

Supervisar el estado del servicio

Azure Service Health realiza un seguimiento del estado de los servicios de Azure en todo el mundo, informando el estado de los recursos en las regiones donde los usa. Azure Service Health es un servicio gratuito que realiza un seguimiento automático de los eventos que pueden afectar a los recursos.

Para ver el estado del servicio de Azure, inicie sesión en el portal de Azure y busque el estado del **servicio** en la barra de recursos de búsqueda en la parte superior del portal. Seleccione la opción de menú **Service Health**, que se mostrará como una opción en el menú desplegable a medida que escribe el nombre del recurso. Las opciones de menú en el lado izquierdo debajo de **Eventos activos** corresponden al tipo de eventos, que se rastrean en Azure Service Health:

- ■ **Problemas de servicio.** Servicios de Azure con problemas actuales en sus regiones
- ■ **Mantenimiento planificado.** Eventos de mantenimiento que pueden afectar sus recursos en el futuro
- ■ **Avisos de salud.** Notificación de depreciación de funciones o requisitos de actualización que utiliza
- ■ **Avisos de seguridad.** Notificaciones y violaciones de seguridad para los servicios de Azure que está usando

Al elegir **Historial de salud** en el menú **Estado del servicio**, se enumeran todos los eventos de salud históricos que han ocurrido en las regiones que usa durante un período de tiempo específico.

Al seleccionar la opción de menú **Resource Health**, se enumeran los recursos por tipo de recurso y se muestra dónde los problemas de servicio están afectando a sus recursos. Puede hacer clic en el recurso enumerado para profundizar en el historial de salud del recurso o para leer más sobre un problema actual que afecta al recurso.

Al volver al menú **Estado del servicio**, puede crear una alerta para **los** eventos del **Estado del servicio** en **Alertas de estado**. **Alertas de Salud** supervisa el registro de la actividad y envía una alerta si Azure emite un **Servicio de Salud** de notificación. Por lo tanto, los registros de diagnóstico deben configurarse en el nivel de suscripción para incluir el estado del **servicio**; de lo contrario, **las alertas de salud** no se configurarán.

Monitorear redes

La supervisión del estado de la red para los productos IaaS se realiza con Azure Network Watcher. Azure Network Watcher tiene herramientas para ver métricas, habilitar el registro y diagnosticar y monitorear los recursos conectados a una red virtual de Azure (VNet). Azure Network Watcher se activa automáticamente para una región tan pronto como se crea una red virtual en su suscripción. Para comprender las capacidades de supervisión de Azure Network Watcher, debe explorar tres herramientas: Topología de Network Watcher, Monitor de conexión y Monitor de rendimiento de red.

Topología

La topología de Azure Network Watcher ofrece una descripción general de todas las redes virtuales y sus recursos conectados dentro de un grupo de recursos. Para ver una topología, abra el portal de Azure y la búsqueda de **vigilante de la red** en la barra de recursos de búsqueda en la parte superior de la página, seleccione Red Vigía en el menú desplegable que aparece al escribir el nombre del recurso. **La topología** se puede seleccionar en el menú del lado izquierdo del portal en el menú **Network Watcher**. Seleccione una **suscripción** y un **grupo de recursos** que contenga al menos una red virtual. La topología se cargará automáticamente, como se muestra en la Figura 1-7.

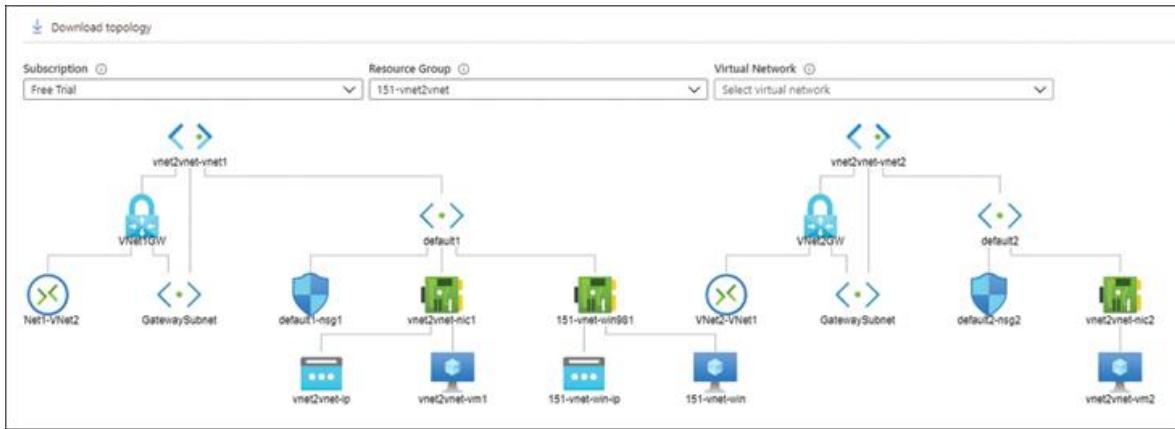


FIGURA 1-7 Topología de Network Watcher para un grupo de recursos específico

La figura 1-7 muestra dos redes virtuales: vnet2vnet-vnet1 y vnet2vnet2. Esta es la topología de red de la infraestructura creada en "Implementar conexiones de red virtual a red virtual", más adelante en este capítulo. También se ha agregado una máquina virtual adicional (151-vnet-win) a la subred predeterminada1. Puede ver las subredes de puerta de enlace obligatorias, sus puertas de enlace VPN (VNetGW1, VNetGW2) y las conexiones para cada puerta de enlace VPN (VNet1-VNet2 y VNet2-Vnet1).

Monitor de conexión

El Monitor de conexión se usa generalmente para ver la latencia; puede proporcionar la latencia mínima, media y máxima observada a lo largo del tiempo o en un momento determinado. Estos datos se pueden usar para supervisar si mover recursos de Azure a nuevas regiones puede disminuir la latencia. **Connection Monitor** también puede monitorear los cambios de topología que pueden afectar la comunicación entre una máquina virtual y un punto final. Si un punto final se vuelve inalcanzable, la función de resolución de **problemas de conexión** de **Network Watcher** puede identificar el motivo como resolución de DNS, capacidad de VM, firewall o problemas de enrutamiento.

Monitor de rendimiento de red

Network Performance Monitor (NPM) supervisa el rendimiento de la red entre puntos de su infraestructura. NPM detecta problemas de red y se

puede configurar para generar alertas según los umbrales establecidos para un enlace de red. NPM tiene las siguientes capacidades:

- ■ **Monitor de rendimiento.** Detecte problemas de red en sus entornos híbridos y en la nube
- ■ **Monitor de conectividad del servicio.** Identifique cuellos de botella e interrupciones entre sus usuarios y sus servicios
- ■ **Monitor ExpressRoute.** Supervisar la conectividad de un extremo a otro a través de Azure ExpressRoute

Para usar el Monitor de rendimiento en Azure, al menos una máquina virtual en su red requerirá que se instale el Agente de Log Analytics. El Monitor de rendimiento de red está habilitado en Network Watcher.

¿Necesita más revisión? Vigilante de la red

Para obtener más información sobre la supervisión de redes IaaS mediante Network Watcher, consulte <https://docs.microsoft.com/en-us/azure/network-watcher/>.

Monitorear el costo

Azure cobra a sus clientes por los recursos y tecnologías que usan y los datos que fluyen entre los recursos y sus usuarios. En la mayoría de los casos, tan pronto como se crea un recurso, a sus clientes se les comenzará a cobrar por el recurso. ¡Sin controlar y monitorear el gasto, sus clientes podrían recibir una factura impactante a fin de mes! Las características de administración de costos de Azure Cost Management and Billing permiten a sus clientes controlar los costos al analizar el gasto y recibir alertas según los umbrales de gasto.

Monitorear el gasto

Azure Cost Management usa presupuestos para controlar los costos y alertar a sus clientes cuando los presupuestos están a punto de romperse. Cuando se está a punto de incumplir un presupuesto, la gestión de costes y la facturación pueden generar una alerta para permitir que sus clientes actúen. Para crear un presupuesto, use Administración de costos en Azure Portal y siga estos pasos:

1. Abra Azure Portal y busque administración de costos en la barra de recursos de búsqueda en la parte superior de Azure

Portal. Seleccione **Administración de costos + Facturación** en el menú desplegable que se abre cuando comienza a escribir el nombre del recurso.

2. Seleccione **Gestión de costes** en el menú de la izquierda. La **gestión de costes** de menú ahora carga. Elija **Presupuestos** en la sección **Administración de costos** del menú **Administración de costos**.
3. Si tiene presupuestos, aparecerán en la hoja **Presupuestos** que ahora se muestra. Haga clic en **Agregar** en la parte superior izquierda para agregar un presupuesto.
4. Se abre la pestaña **Crear presupuesto**, que tiene las secciones de configuración en la siguiente lista. Una vez que haya elegido sus opciones, su presupuesto debería aparecer como se muestra en la Figura 1-8.

The screenshot shows the 'Create a budget' configuration page. At the top, there are two tabs: 'Create a budget' (selected) and 'Set alerts'. Below the tabs, a sub-header reads 'Create a budget and set alerts to help you monitor your costs.' Under the 'Budget scoping' section, it says 'The budget you create will be assigned to the selected scope. Use additional filters like resource groups to have your budget monitor with more granularity as needed.' It shows a 'Scope' dropdown set to 'Free Trial' with a 'Change scope' link and an 'Add filter' button. The 'Budget Details' section asks for a unique name, time window, creation date, and expiration date. The 'Name' field is filled with 'check100'. The 'Reset period' is set to 'Billing month'. The 'Creation date' is set to '2020 September 4'. The 'Expiration date' is set to '2022 September 3'. In the 'Budget Amount' section, it asks for a budget amount threshold, with 'Amount (£)' set to '1000'. A note at the bottom states 'Suggested budget: £2,462 based on forecast.'

FIGURA 1-8 Creación de un presupuesto en la gestión de costos

1. ■ **Alcance.** Puede establecer un presupuesto a nivel de grupo de administración, suscripción o grupo de recursos. Por ejemplo, establezca el **ámbito** en el nivel de suscripción.
 2. ■ **Filtro.** Esto se usa a menudo para filtrar a una etiqueta taxonómica, como un departamento, para proporcionar vistas presupuestarias entre organizaciones. Para este ejemplo, no agregue un filtro.
 3. ■ **Nombre.** Ingrese un **nombre** para su presupuesto.
 4. ■ **Período de reinicio.** Elija el período durante el cual se restablece su período presupuestario interno. Para este ejemplo, establezca el **Período de reinicio** en **Mes de facturación**.
 5. ■ **Fecha de creación.** Esta es la fecha para iniciar el presupuesto. Puede elegir opciones desde el inicio del mes de facturación actual u opciones que se extienden hacia el futuro. Para este ejemplo, deje la configuración predeterminada.
 6. ■ **Fecha de vencimiento.** Aquí es cuando terminará el presupuesto. Para este ejemplo, déjelo como la configuración predeterminada.
 7. ■ **Monto presupuestado.** El límite que debe establecer para el presupuesto. Estará en la moneda de su suscripción, que puede diferir de su moneda local. Ingrese un valor que esté justo por encima de su gasto actual. Haga clic en **Siguiente** en la parte inferior de la página.
5. La pestaña **Establecer alertas** ahora está activa, que es donde puede configurar una alerta en su presupuesto. Para una alerta de presupuesto, tiene las siguientes opciones de configuración:
- 0.■ **Condiciones de alerta.** Ingrese el **% del presupuesto** sobre el que desea que se active la alerta. Sus clientes deberán establecer esto en un valor que les dé tiempo para remediar un posible gasto excesivo antes de que se supere el límite. Para este ejemplo, elija **75%**. Deje

el **grupo de acción** vacío, ya que explorará los grupos de acción más adelante en este capítulo en "Iniciar respuestas automáticas mediante el uso de grupos de acción".

- 1.■ **Destinatarios de alertas.** Ingrese las direcciones de correo electrónico de las personas que requieren este informe.
6. Haga clic en **Crear**; se crea el presupuesto junto con su correspondiente alerta.

Cuando se activa una alerta de costo, se activan las notificaciones y se crea una alerta activa para el presupuesto. Las alertas se pueden ver en la opción de menú **Alertas de costos** que se muestra a la izquierda de **Administración de costos**. En **Alertas de costos**, tiene la opción de descartar las alertas o reactivar una alerta descartada.

Informe sobre gasto

Azure Cost Management también es el mejor lugar para informar sobre el gasto. Vuelva al menú **Administración de costos** en Azure Portal y elija **Análisis de costos**. La hoja **Análisis de costos** está preconfigurada con un panel de resumen de su gasto actual y pasado, como se muestra en la [Figura 1-9](#).



FIGURA 1-9 Análisis de costos para informar sobre el gasto en Azure Cost Management

La Figura 1-9 muestra el gasto en el mes de facturación actual, con los costos acumulados desglosados en servicios, ubicaciones y grupos de recursos. Puede cambiar el ámbito a grupo de administración, suscripción o grupo de recursos. La capacidad de filtrar por etiqueta se considera una mejor práctica y es una de las características clave del análisis de costos. Por ejemplo, si etiqueta por departamento, puede producir un análisis del gasto de cada departamento. Haga clic en **Descargar** en la parte superior de la página para descargar manualmente los datos del gráfico o programar los datos de gastos para extraerlos a una cuenta de almacenamiento.

Configurar el registro avanzado

La supervisión avanzada en Azure Monitor se realiza a través de Insights, que forma parte de Azure Monitor. Insights proporciona a su cliente una experiencia de supervisión especializada para sus aplicaciones y

servicios. Insights aprovecha los registros de Azure Monitor que se encuentran en un área de trabajo de Log Analytics. Por lo tanto, antes de explorar Insights, deberá crear y configurar un espacio de trabajo.

Configurar un espacio de trabajo de Log Analytics

Para crear un área de trabajo de Log Analytics en el portal, busque **el análisis de registros** en la barra de recursos de búsqueda en la parte superior de Azure Portal. Seleccione **Espacios de trabajo de Log Analytics** en el menú desplegable que se abre a medida que escribe el nombre del recurso. Para agregar y configurar un espacio de trabajo, siga estos pasos:

1. Haga clic en **Agregar** en la parte superior izquierda de la hoja **Espacios de trabajo**. Ingrese un nombre para el espacio de trabajo, elija un grupo de recursos y seleccione la región donde necesita que resida su espacio de trabajo. Haga clic en **Revisar + Crear** y luego en **Crear** para crear el espacio de trabajo.
2. Una vez creado, su nuevo espacio de trabajo aparece en la lista. Haga clic en el nombre del espacio de trabajo para ver las opciones de configuración.
3. En el menú de la izquierda, en **Configuración**, seleccione **Administración de agentes**. En la parte superior de la página se encuentran las pestañas **Servidores Windows y Servidores Linux**. Para incorporar manualmente una máquina virtual para registrarAnalytics, necesitará el ID y las claves de estas pestañas. Explorará las máquinas virtuales integradas en "Configurar el registro para cargas de trabajo", más adelante en esta habilidad.
4. En el menú **Espacios de trabajo de Log Analytics**, elija **Configuración avanzada**. La sección **Datos** es donde puede configurar qué contadores y archivos de registro se recopilan para sus recursos. Por ejemplo, haga clic en **Datos > Contadores de rendimiento de Windows**. Se enumeran los contadores disponibles, pero hasta que seleccione **Agregar los contadores de rendimiento seleccionados**, los datos no se recopilarán para ninguna VM de Windows conectada a este espacio de trabajo. Una

vez seleccionada, la pantalla se actualiza, como se muestra en la Figura 1-10.

The screenshot shows the Log Analytics workspace configuration interface. On the left, there's a sidebar with options like Connected Sources, Data, Computer Groups, Windows Event Logs, Windows Performance Counters (which is selected), Linux Performance Counters, IIS Logs, Custom Fields, Custom Logs, and Syslog. On the right, there's a table titled 'Collect the following performance counters' with columns for 'COUNTER NAME', 'SAMPLE INTERVAL', and 'Remove'. The table lists various Windows performance counters with a sample interval of 10 seconds. Each row has a 'Remove' button.

COUNTER NAME	SAMPLE INTERVAL	
LogicalDisk("0")% Free Space	10 seconds	Remove
LogicalDisk("0")Avg. Disk sec/Read	10 seconds	Remove
LogicalDisk("0")Avg. Disk sec/Write	10 seconds	Remove
LogicalDisk("0")Current Disk Queue Length	10 seconds	Remove
LogicalDisk("0")Disk Reads/sec	10 seconds	Remove
LogicalDisk("0")Disk Transfers/sec	10 seconds	Remove
LogicalDisk("0")Disk Writes/sec	10 seconds	Remove
LogicalDisk("0")Free Megabytes	10 seconds	Remove
Memory("0")% Committed Bytes In Use	10 seconds	Remove
Memory("0")Available Mbytes	10 seconds	Remove
Network Adapter("0")Bytes Received/sec	10 seconds	Remove
Network Adapter("0")Bytes Sent/sec	10 seconds	Remove
Network Interface("0")Bytes Total/sec	10 seconds	Remove
Processor(_Total)% Processor Time	10 seconds	Remove
System("0")Processor Queue Length	10 seconds	Remove

FIGURA 1-10 Configuración del espacio de trabajo de Log Analytics para recopilar contadores de rendimiento de Windows

Cuando los agentes de VM Log Analytics actualizan sus configuraciones, los agentes recogen las nuevas configuraciones de contador y envían los datos seleccionados al espacio de trabajo de Log Analytics.

5. Deberá repetir este ejercicio para los registros de eventos, los contadores de rendimiento de Linux y otras fuentes de datos que necesite.

6. Permaneciendo en el espacio de trabajo de Log Analytics que acaba de crear, haga clic en **Máquinas virtuales** en el menú del lado izquierdo. Se muestra una tabla que enumera las máquinas virtuales que podrían estar conectadas al espacio de trabajo de Log Analytics que acaba de crear. La configuración del contador de rendimiento que realizó en los pasos 3 a 5 solo afectará a las máquinas virtuales enumeradas como **Conectadas** en esta tabla.

Implementar y configurar la información de Azure Monitor, incluida la información de la aplicación, las redes y los contenedores.

Las aplicaciones modernas alojadas en la nube suelen ser complejas y combinan varios servicios PaaS e IaaS. Monitorear, mantener y diagnosticar tales aplicaciones puede ser una tarea casi imposible si no se implementan herramientas para analizar los datos de la aplicación y alertar sobre métricas clave. Azure Monitor proporciona Insights, que brinda una observabilidad de pila completa en todas las aplicaciones e infraestructura, lo que permite capacidades de diagnóstico y alertas profundas. En esta sección, se analizan las perspectivas disponibles para aplicaciones, redes y contenedores en Azure Monitor.

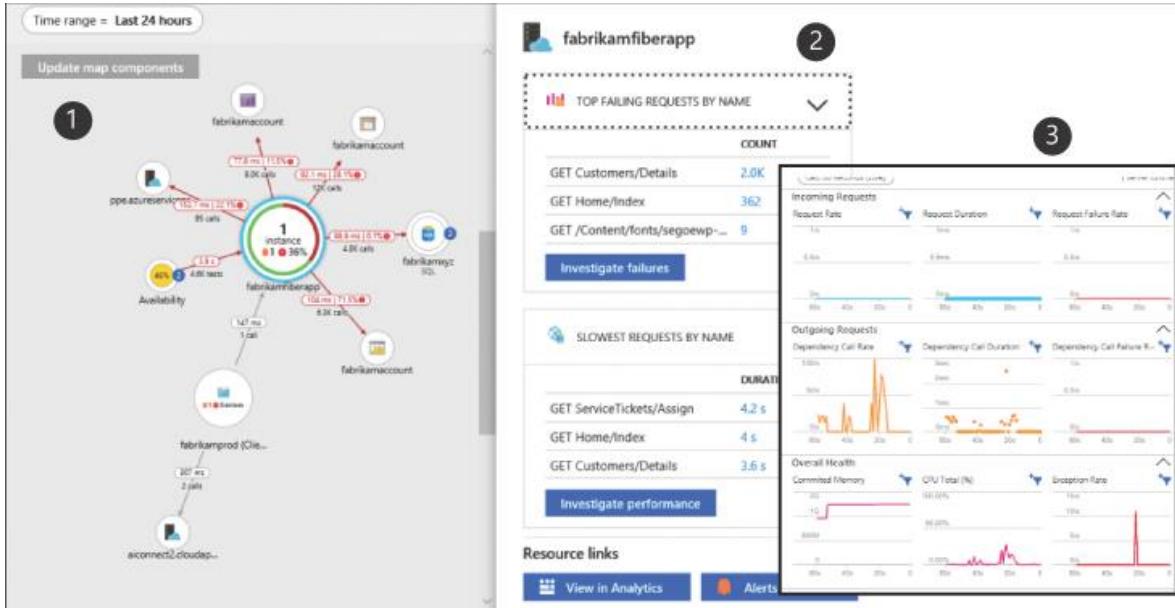
Perspectivas de la aplicación

Application Insights es un servicio de Application Performance Management (APM) para que los desarrolladores monitorean sus aplicaciones en vivo. La información de las aplicaciones detectará automáticamente anomalías en aplicaciones híbridas, locales o en la nube pública donde lo necesite.

- Analizar y abordar problemas y problemas que afectan el estado de su aplicación.
- Mejore el ciclo de vida de desarrollo de su aplicación
- Analizar las actividades de los usuarios para ayudar a comprenderlos mejor.

Para integrar Application Insights con sus aplicaciones, debe configurar un recurso de **Application Insights** en Azure Portal. Para hacer esto, navegue hasta **Application Insights** en el portal y haga clic en **Agregar**. Elija un nombre, grupo de recursos y región para crear el recurso. Una vez que se crea el recurso, hay una **clave de instrumentación** disponible en la página **Descripción general**. Tus clientes dan esta clave a sus desarrolladores. Los desarrolladores utilizan un kit de desarrollo de software (SDK) para agregar un paquete de instrumentación a sus aplicaciones. El paquete de instrumentación utiliza la clave de instrumentación de Application Insights para enrutar la telemetría al recurso de Application Insights para su análisis.

Una vez que la telemetría fluye hacia Application Insights, hay visualizaciones integradas que le permiten analizar su entorno. [La Figura 1-11](#) muestra dos de las visualizaciones: mapa de la aplicación y métricas en vivo.



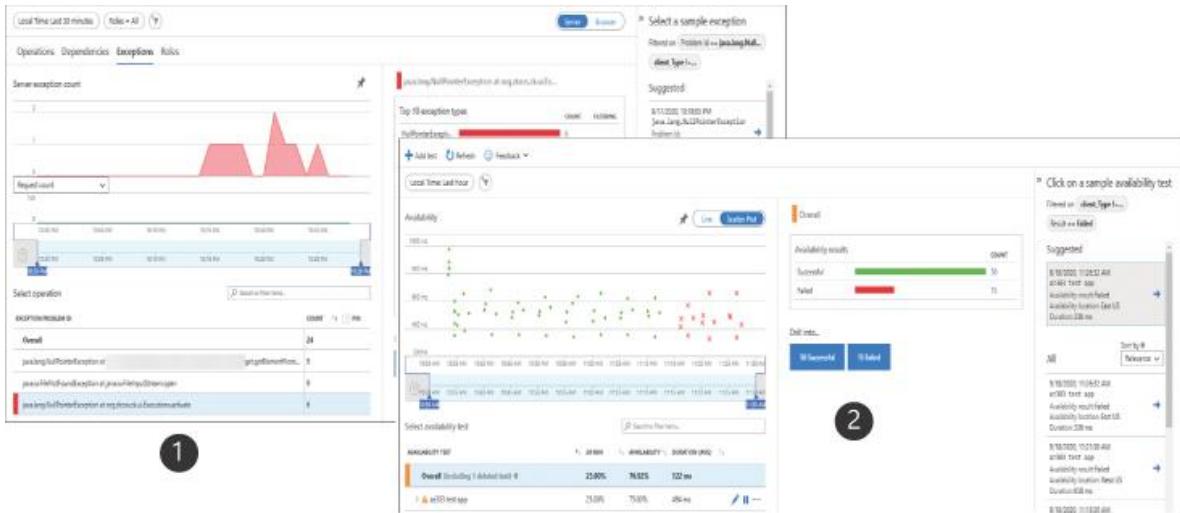
1. Application Map
2. Live Metrics
3. Live Metrics drill through

FIGURA 1-11 El mapa de la aplicación y las métricas en vivo, que forman parte de Application Insights

Application Map muestra una descripción general de su aplicación, donde cada nodo es un componente de la aplicación. Los vínculos entre los nodos son las dependencias. El mapa de aplicaciones muestra los KPI de salud y los estados de alerta en cada nodo, en los que puede profundizar para obtener análisis detallados.

Live Metrics proporciona una vista en tiempo real de su aplicación sin tener que configurar ajustes, lo que podría afectar la disponibilidad. Puede trazar contadores de métricas en vivo y puede profundizar en solicitudes fallidas y excepciones.

Otros dos conocimientos de uso común son Disponibilidad y Fallos; La salida de ejemplo para ambos se muestra en la [Figura 1-12](#).



1. Failures
2. Availability

FIGURA 1-12 Información sobre fallas y disponibilidad

Las fallas se muestran en la parte superior izquierda de la [Figura 1-12](#). Las fallas se trazan en un rango de tiempo y se agrupan por tipo. Puede hacer clic en los **exitosos** y **fallidos** botones debajo de los **agujeros en** investigar la operación, la dependencia, y excepciones.

La disponibilidad debe configurarse agregando una prueba de disponibilidad a la página Disponibilidad de Application Insights. Usted ingresa la URL del punto final que desea monitorear y Azure prueba la disponibilidad desde cinco ubicaciones diferentes. También puede configurar la prueba de disponibilidad para verificar el tiempo de respuesta para descargar dependencias de página, como imágenes, hojas de estilo y scripts. Azure traza las respuestas en los gráficos de la página de disponibilidad, que incluyen la latencia. Puede configurar alertas de las pruebas de disponibilidad para la notificación inmediata de un posible tiempo de inactividad.

Perspectivas de la red

Network Insights proporciona una descripción general completa de su inventario de red sin ninguna configuración. Puede ver el estado y las métricas de todos los recursos de red e identificar sus dependencias. Las siguientes perspectivas están disponibles a través de Network Insights:

- **Búsqueda y filtrado.** Puede tener miles de recursos de red. Ver los datos de análisis de un solo recurso puede resultar complicado. Con **Búsqueda y filtrado**, puede ingresar un solo nombre de recurso y se devolverá el recurso junto con sus dependencias.
- **Alertas.** Esto muestra todas las alertas generadas para los recursos seleccionados en todas las suscripciones.
- **Métrica de recursos y salud.** Agrupados por tipo de recurso, esta es una vista de resumen de los componentes seleccionados. Los resúmenes se muestran como mosaicos.
- **Vista de dependencia.** Explore los mosaicos de estado y métricas para ver dependencias y métricas para el tipo de recurso elegido, como se muestra en la [Figura 1-13](#) para dos puertas de enlace de red virtual en una configuración de red virtual a red virtual.

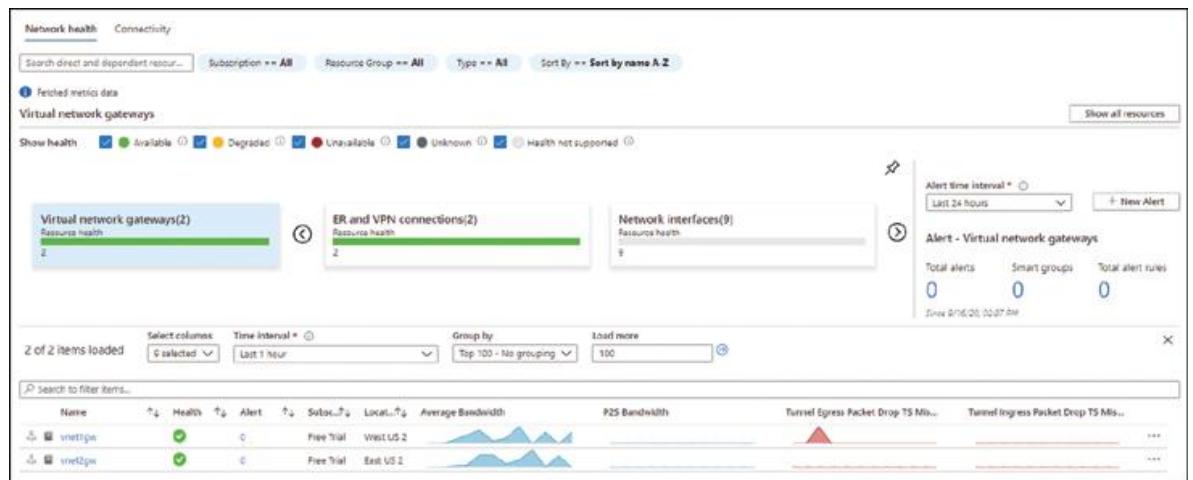


FIGURA 1-13 La vista de dependencia de dos puertas de enlace de red virtual en una configuración de red virtual a red virtual en Network Insights

Azure Monitor para contenedores

Cuando está diseñando soluciones con contenedores, monitorearlas es fundamental. Azure Monitor para contenedores recopila métricas de memoria y procesador de cargas de trabajo de contenedor. Las cargas de trabajo se pueden implementar localmente en Kubernetes en Azure Stack, o se pueden implementar en Azure Kubernetes Service (AKS), Azure

Container Instances (ACI) u otros orquestadores de contenedores de terceros basados en Azure.

Cuando está habilitada, la API de métricas de Kubernetes envía métricas para controladores, nodos y contenedores. También se recogen registros de contenedores. La métrica y los datos de registro se envían a un área de trabajo de Log Analytics, que es un requisito de Azure Monitor para contenedores. El método para habilitar Azure Monitor para contenedores varía según el servicio en el que se habilitará. A continuación, se muestra un comando de ejemplo para crear un clúster de AKS con la CLI de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
az aks create --resource-group $ resourceGroupName --name myAKSCluster --node-count 1  
--enable-addons monitoring --generate-ssh-keys
```

La opción de supervisión `--enable-addons` habilita Azure Monitor para contenedores. Si desea utilizar un espacio de trabajo de Log Analytics existente, debe pasarle el ID del espacio de trabajo con `--workspace-resource-id`; de lo contrario, se creará un espacio de trabajo de Log Analytics para usted. También puede habilitar la supervisión en un clúster existente mediante el siguiente comando de la CLI de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
az aks enable-addons --addons monitoring --name myAKSCluster  
--resource-group  
$ resourceGroupName
```

El `--workspace-resource-id` se puede especificar para usar un espacio de trabajo existente. Una vez que se recopilan las métricas y los registros, puede acceder a los datos desde el menú **Insights** del clúster de AKS o a través del menú **Contenedores** de Azure Monitor. Si usa Azure Monitor, deberá seleccionar la pestaña **Clústeres supervisados** en la parte superior de la ventana y luego seleccionar el clúster que desea ver. La vista **Clúster** es un resumen de los contadores del clúster, como se muestra en la [Figura 1-14](#).

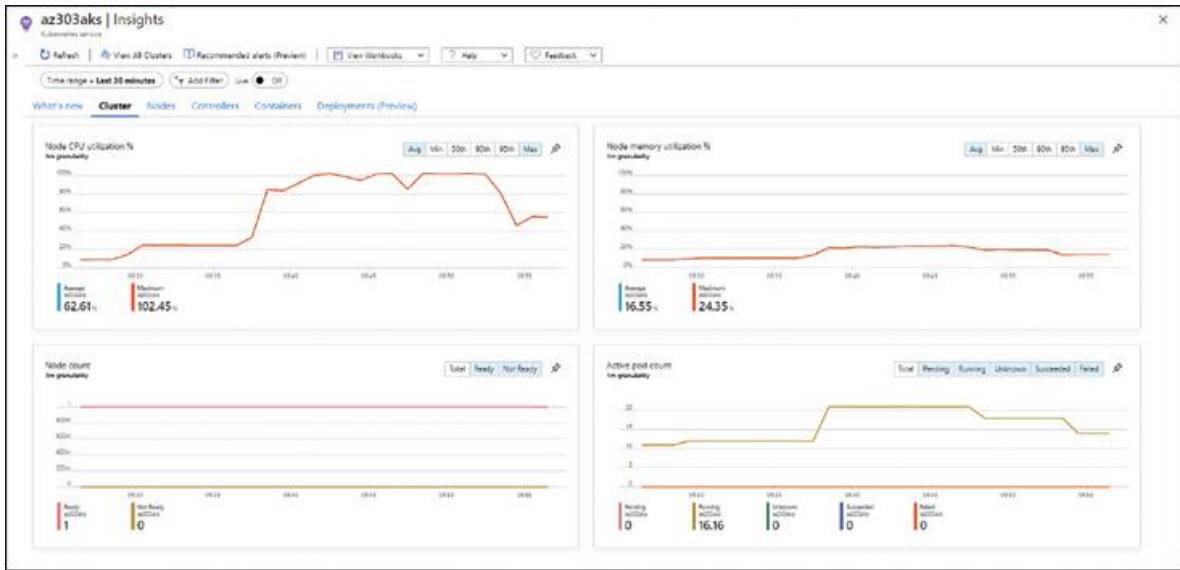


FIGURA 1-14 Vista de resumen de clúster para AKS en Azure Monitor para contenedores

En la [Figura 1-14](#), el gráfico superior izquierdo muestra el **% de utilización de CPU del nodo** del clúster. La aplicación que se ejecuta en AKS en este ejemplo contiene un front-end HTML (azure-vote-front) con una instancia de Redis en el back-end (azure-vote-back). Para implementar esta infraestructura, siga la guía de inicio rápido de Azure: <https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>. Cuando se implementa la aplicación, hay una réplica de azure-vote-front que está siendo estresada por múltiples solicitudes concurrentes. En la parte superior de la ventana hay seis pestañas: Novedades, Clúster, Nodos, Controladores, Contenedores e Implementaciones (vista previa). En la [Figura 1-15](#), se ha seleccionado la pestaña **Nodos**. El nodo superior enumerado en la tabla en [La figura 1-15](#) se denomina frente de voto azul. La columna **Tendencia 95%** muestra una pequeña barra verde; ocho barras rojas de altura completa, lo que sugiere un gran aumento en el tráfico de aplicaciones.

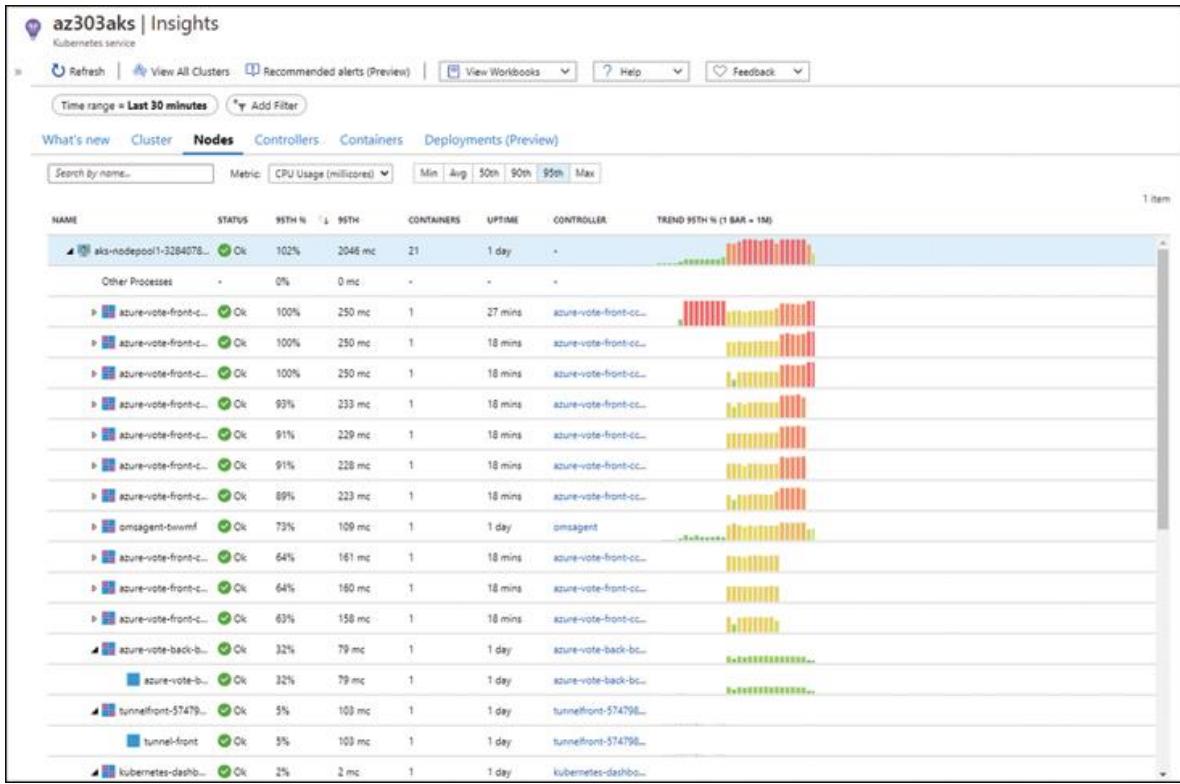


FIGURA 1-15 Nodos en Azure Monitor para contenedores

- El número de réplicas de `azure-vote-front` se incrementa a diez. Esto se puede ver en los nueve listados de `azure-vote-front` debajo del nodo original. No hay datos para estos nodos mientras el nodo superior de la tabla está a plena capacidad. Las barras amarillas para los nuevos nodos y el nodo original muestran que la carga se ha distribuido por igual entre cada uno de los 10 nodos. Mirando hacia atrás a la [Figura 1-14](#), la escala manual a 10 nodos del frente de voto azul corresponde bastante bien al gráfico de la parte inferior derecha, **Active Pod Count**. También puede ver el aumento de la demanda de CPU de los 10 nodos que se muestran en el gráfico de **porcentaje de utilización de CPU de nodo**. Volviendo a la [Figura 1-15](#), el número de nodos de front-end azul se reduce a 7 y, poco después, se escala a 3. Esto corresponde a la parada en los datos de los 3 nodos de front-end de votos azules inferiores en la columna **Trend 95th%**, y luego corresponde a la parada en los datos para todos menos los tres nodos superiores. También puede ver el aumento de la tensión en los 3 nodos superiores a medida que las barras de la

columna **Trend 95th%** aumentan de tamaño y pasan de amarillo a naranja a rojo.

¿Necesita más revisión? Perspectivas de Azure Monitor

Insights es una herramienta inmensa; para obtener más información, visite <https://docs.microsoft.com/en-us/azure/azure-monitor/insights/insights-overview> .

Configurar el registro para cargas de trabajo

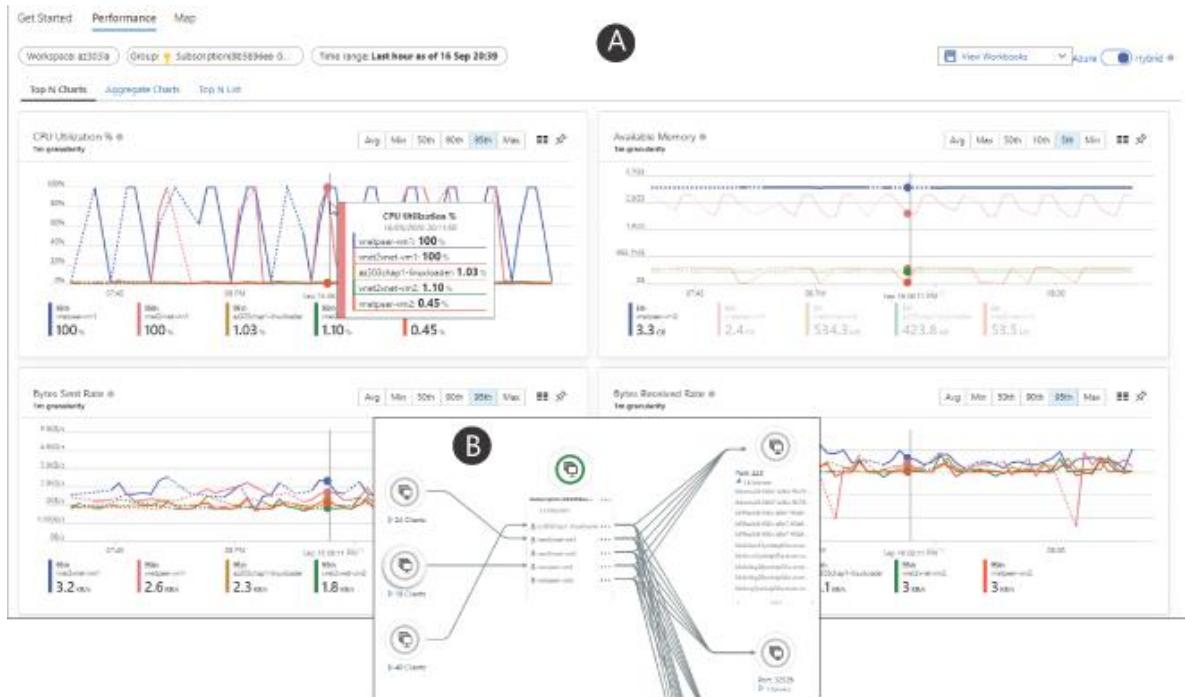
Al diseñar VM a escala, monitorear sus cargas de trabajo y recursos dependientes ha sido históricamente complejo. Azure Monitor para máquinas virtuales está diseñado para escalar y analiza las máquinas virtuales de Windows y Linux y los conjuntos de escalado de máquinas virtuales a través de sus métricas de estado y rendimiento. Azure Monitor para máquinas virtuales supervisa las máquinas virtuales y las dependencias de las aplicaciones en cargas de trabajo que se encuentran en Azure, en las instalaciones o en otras nubes.

La incorporación de una máquina virtual en Azure se puede realizar de una en una en el portal de Azure navegando a una máquina virtual, desplazándose hacia abajo en el menú de **Azure**

Monitor hasta **Supervisión**, eligiendo **Insights** y haciendo clic en **Habilitar**. Azure Portal envía una solicitud de implementación a la máquina virtual para instalar los agentes de Log Analytics y Dependency. El agente de dependencia es necesario para mapear dependencias y el agente de Log Analytics para recopilar datos de registro y rendimiento. Azure Monitor para VM está diseñado para monitorear cargas de trabajo a escala; si está implementando para clientes de VM, deberá automatizar la tarea. Azure Policy se puede configurar para implementar los agentes, informar sobre el cumplimiento y corregir las máquinas virtuales que no cumplen. Para máquinas virtuales locales y en la nube, los agentes pueden implementarse manualmente o enviarse a través de una herramienta de administración de estado diseñada.

Una vez que se recopilan los datos, se pueden ver en la hoja **Insights** de una sola máquina virtual o para obtener una vista agregada acumulada en el nivel de suscripción desde Azure Monitor. Para ver los datos agregados y explorar el resultado en Azure Portal, siga estos pasos:

1. Busque **azure monitor** en la barra de recursos de búsqueda en la parte superior de Azure Portal. Elija **Monitor** en el menú desplegable que se muestra una vez que comienza a escribir el nombre del recurso.
2. En el menú **Insights**, haga clic en **Virtual Machines**.
3. Se muestra la pestaña **Getting Started** para VM Insights. Desde esta pestaña, se muestran las siguientes opciones de configuración:
 1. ■ **Supervisado.** Esta opción muestra las máquinas que supervisa Azure Monitor para máquinas virtuales. Puede elegir ver los datos a nivel de suscripción, grupo de recursos y una sola máquina virtual haciendo clic en los nombres enumerados.
 2. ■ **No supervisado.** Esta opción enumera las máquinas virtuales de sus suscripciones que no están supervisadas. Desde aquí, puede habilitar las VM.
 3. ■ **Configuración del área de trabajo** Desde aquí, puede configurar los espacios de trabajo de Log Analytics que se han habilitado para Azure Monitor para máquinas virtuales.
4. Haga clic en el nombre de la suscripción para ver el rendimiento de todas las máquinas virtuales habilitadas. Esta vista incluye métricas de CPU, memoria, red y disco. Justo debajo de la pestaña **Rendimiento** hay más pestañas de vista de análisis; haga clic en ellos para ver las tablas y listas agregadas (vea la imagen A de la [Figura 1-16](#)).



A. Virtual Machines Performance tab

B. Virtual Machines Map tab

FIGURA 1-16 Azure Monitor para máquinas virtuales con las pestañas Rendimiento y Mapa

- Vuelva a la pestaña **Introducción** y elija un grupo de recursos con varias máquinas virtuales. A continuación, haga clic en **Mapa** para ver las dependencias de la aplicación, como se muestra en la parte insertada (B) de la [Figura 1-16](#).

¿Necesita más revisión? Azure Monitor para máquinas virtuales

Para obtener más información sobre la supervisión de cargas de trabajo a escala, visite <https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-overview>.

Inicie respuestas automáticas mediante el uso de grupos de acción

A lo largo de este capítulo, se ha hecho referencia a las alertas y se han configurado especificando cuentas de correo electrónico únicas. Para las implementaciones de sus clientes, es muy poco probable que una sola persona sea responsable de una alerta o un conjunto de alertas. Además, es posible que un correo electrónico no garantice una respuesta lo

suficientemente rápida a un problema. Cuando busque mitigar las respuestas lentas a una alerta, debe recomendar la configuración de grupos de acción. Un grupo de acciones es una colección de notificaciones y tareas de automatización que se activan cuando se activa una alerta. Puede configurar varios grupos de acción que notifiquen a diferentes grupos o activen diferentes respuestas, según la alerta. Para examinar las opciones disponibles en un grupo de acciones, siga estos pasos para crear un grupo de acciones en Azure Portal. Tenga en cuenta que los grupos de acciones también se pueden crear en la línea de comandos y con una plantilla ARM.

1. Navegue a Azure **Monitor** mediante la barra de recursos de búsqueda en la parte superior de Azure Portal. Elija **Monitor** en el menú desplegable que se muestra una vez que comienza a escribir el nombre del recurso.
2. Haga clic en **Alertas** en el menú **Monitor** y luego haga clic en **Administrar acciones** en la parte superior de la hoja **Alertas**. Se abrirá la hoja **Acción administrada**.
3. Si tiene grupos de acciones, aparecerán en la hoja **Administrar acciones**. Haga clic en **Agregar grupo de acciones** en la parte superior derecha para agregar una nueva acción.
4. Se muestra la página de configuración **Crear grupo de acciones** con la pestaña **Conceptos básicos** abierta. Haga clic en **Siguiente: Notificaciones>** en la parte inferior de la página. A continuación, se muestran las opciones que se muestran en la pestaña **Conceptos básicos** :
 1. ■ **Suscripción.** Elija la suscripción en la que desea guardar el grupo de acciones.
 2. ■ **Grupo de recursos.** Elija un grupo de recursos de la suscripción o cree un nuevo grupo de recursos predeterminado para grupos de acción.
 3. ■ **Nombre del grupo de acciones.** Este es el nombre del grupo de acciones y debe ser exclusivo dentro del grupo de recursos.
 4. ■ **Nombre para mostrar.** Esto se incluye en los mensajes de correo electrónico y SMS.

5. La página **Crear grupo de acciones** cambia a la pestaña **Notificaciones**. Aquí, puede configurar cómo se alerta a los usuarios si se activa el **grupo de acción**:

0.■ **Tipo de notificación.** Este es el tipo de notificación que se enviará al receptor. Puede elegir entre:

- 1.■ **Envíe un correo electrónico al rol de administrador de recursos de Azure.** Al elegir esta opción, se envía un correo electrónico a todos los miembros de suscripción del rol.
- 2.■ **Correo electrónico / mensaje SMS / Push / Voice.** Se enviará una notificación de inserción a la aplicación de Azure que está vinculada a una cuenta de Azure AD, Voice llama a un número, incluido un teléfono fijo. Hay límites para estas acciones: 1 SMS cada 5 minutos, 1 Voz cada 5 minutos y 100 correos electrónicos por hora.

1.■ **Nombre.** El nombre de la notificación. Debe ser exclusivo de otros nombres de notificación y de nombres de acciones.

6. Haga clic en **Siguiente: Acciones>** en la parte inferior de la página.

7. La página **Crear grupo de acciones** cambia a la pestaña **Acciones**. Aquí, puede configurar acciones automatizadas si se activa el **Grupo de acción**:

0.■ **Tipo de acción.** Esta es la acción automatizada que se realizará cuando se active el grupo de acciones:

0. ■ **ITSM.** Registre automáticamente un ticket en un software de administración de servicios de TI (ITSM) específico.
1. ■ **Aplicación lógica.** Cree un flujo lógico para automatizar una respuesta, como publicar un mensaje en Microsoft Teams.
2. ■ **Webhook / Webhook seguro.** Esta opción envía una carga útil JSON a una API REST externa.
3. ■ **Runbook de Azure Automation.** Use esta opción para crear un runbook para ejecutar código

en respuesta a una alerta, como detener una máquina virtual de Azure después de un incumplimiento presupuestario.

4. ■ **Función Azure.** Use esta opción para invocar una función de Azure para que se ejecute en respuesta a una alerta, como iniciar una máquina virtual que se haya detenido.

1. ■ **Nombre.** El nombre de la acción. Debe ser exclusivo de otros nombres de acción y de nombres de notificación.

2. ■ **Configurar.** Esta opción se activa una vez que se elige el **tipo de acción**. Aquí, ingresa los detalles de la notificación, la **URL del webhook**, el **nombre de la aplicación lógica** o el **nombre de la aplicación de función**. También puede habilitar el esquema de alerta común, que proporciona la siguiente funcionalidad:

0. ■ **SMS.** Esto crea una plantilla coherente para todas las alertas.
 1. ■ **Correo electrónico.** Esto crea una plantilla de correo electrónico coherente para todas las alertas.
 2. ■ **JSON.** Esto crea un esquema JSON coherente para integraciones con webhooks, aplicaciones lógicas, funciones de Azure y runbooks de automatización.
8. Una vez que esté satisfecho con la configuración del grupo de acciones, haga clic en **Revisar + Crear** para agregar el grupo de acciones.

Configurar y administrar alertas avanzadas

A lo largo de esta habilidad, ha explorado cómo monitorear los recursos para una amplia gama de problemas y anomalías. La gran escala de los datos que se pueden producir mientras se monitorean las soluciones diseñadas en la nube pública e híbrida es enorme. Esto significa que tratar de examinar los datos manualmente para detectar problemas será casi imposible o requerirá una cantidad de trabajo excesiva y costosa. La creación de alertas basadas en la métrica subyacente y los datos de registro automatizará algunas de estas tareas para sus clientes.

Recopile alertas y métricas en varias suscripciones

Las alertas de Azure Monitor le brindan la capacidad de activar alertas sobre recursos para una suscripción. La experiencia de alerta está unificada para los tres tipos de alerta: métrica, registro y registro de actividad. Por ejemplo, es posible que desee saber cuándo se detiene una máquina virtual en su suscripción de producción, para poder intentar reiniciarla. Siga estas instrucciones para crear la alerta de ejemplo de máquina virtual detenida en Azure Portal:

1. Vaya a Azure Monitor, elija **Alertas** en el menú del lado izquierdo. En la parte superior de la página, haga clic en **Nueva regla de alerta**.
2. Se carga la hoja **Crear regla de alerta**, que le permite seleccionar una suscripción, un grupo de recursos, un recurso o un conjunto de recursos. Elija todas las máquinas virtuales de su suscripción mediante el filtro de **máquinas virtuales** y una única ubicación.
3. Ahora, para seleccionar todas las VM en la misma ubicación, seleccione la suscripción (como se muestra en la [Figura 1-17](#)). En la parte inferior derecha, puede ver los tipos de señales disponibles, que son recursos dentro de la misma ubicación; Tanto la métrica como el registro de actividad están disponibles.

The screenshot shows the 'Select a resource' dialog box. At the top, there's a header 'Select a resource' and a close button 'X'. Below the header, a message says: 'Select the resource(s) you want to monitor. Available signal types for your selection will show up on the bottom right.' There are three filter sections: 'Filter by subscription *' (set to 'Free Trial'), 'Filter by resource type' (set to 'Virtual machines'), and 'Filter by location' (set to 'UK South'). A search bar 'Search to filter items...' is also present. The main area displays a table of resources:

Resource	Resource type	Location
✓ Free Trial	Subscription	UK South
✓ az303chap1_3-rg	Resource group	UK South
✓ ade-vm	Virtual machine	UK South
✓ vmLinSizeExample	Virtual machine	UK South
✓ az303chap1_4-rg	Resource group	UK South
✓ SimpleWinVM	Virtual machine	UK South

FIGURA 1-17 Seleccione el alcance de destino en alertas unificadas

4. Ahora, cambie **Filtrar por tipo de recurso** y **Filtrar por ubicación** a **Todo** y seleccione la suscripción una vez más. Tenga en cuenta que los tipos de señales disponibles ahora son solo **Registro de actividad** porque la **métrica** no se puede usar para alertas en todas las regiones. Haz clic en **Listo**.
5. Haga clic en **Seleccionar condición**, que abre la página **Configurar lógica de señal**. Los tipos de señales disponibles dependerán del **osciloscopio** seleccionado en el paso anterior:
 1. **Tronco.** Cree una consulta KQL para datos en análisis de registros; si la consulta devuelve filas, se activa la alerta.
 2. **Métrico.** Establezca un valor de umbral frente a una métrica, como "mayor que un promedio de X". Si se traspasa el umbral, se dispara la alerta.
 3. **Registro de actividades.** Si se crea un tipo de registro de actividad coincidente en el registro de actividad de la suscripción, se activa la alerta.
- El tipo de señal disponible en el nivel de suscripción es Registro de actividad. Ingrese **máquina virtual** en el cuadro de búsqueda para filtrar los datos. Desplácese hacia abajo en la misma hoja y seleccione **Desasignar máquina virtual (Microsoft.ClassicCompute / virtualMachines)**. Deje **Alert Logic** configurado en **Todos**. Haz clic en **Listo**.
6. Haga clic en **Grupo de acciones** para elegir un grupo de acciones. Recuerde de la sección anterior que se trata de una agrupación de notificaciones y respuestas automáticas. Para este ejemplo, cree un grupo de acción que le envíe un correo electrónico.
7. Introduzca un **nombre** y una **descripción de la regla de alerta** y, a continuación, seleccione un **grupo de recursos** para guardarlo.
8. Haga clic en **Crear regla de alerta** para crear la regla de alerta.
9. Pruebe la alerta deteniendo una máquina virtual dentro de su suscripción seleccionada.
10. Si necesita recopilar alertas en varias suscripciones, puede automatizar el proceso utilizando plantillas ARM para implementar una configuración de alerta en cada suscripción.

Ver alertas en los registros de Azure Monitor

Todas las alertas que se han desencadenado, independientemente de dónde estén configuradas, se pueden ver en la experiencia de alertas unificadas en Azure Monitor. Para acceder a esta información, vaya a Azure Monitor y haga clic en **Alertas** en el menú de la izquierda. Se muestra la hoja **Alertas con** una lista de todas las alertas de las últimas 24 horas. Las alertas están agrupadas por gravedad. Por ejemplo, todas las alertas de gravedad 0 se agrupan en una línea de gravedad titulada **Sev 0**. Al hacer clic en la línea de una gravedad, se profundizará en las alertas que se incluyen dentro de esa clasificación de gravedad. La elección de una alerta específica en la vista detallada le brinda la opción de cambiar el estado de una alerta a reconocida.

Una vista similar de los datos está disponible a través de **Azure Monitor Logs**, dentro de **Workbooks**. En Azure Monitor, seleccione **Libros de trabajo** en el menú de la izquierda. Desplácese hacia abajo en la **Galería de libros** y seleccione la plantilla de libro de **alertas** en **Recursos de Azure**. Se muestra una vista similar a la de la experiencia de alertas unificadas. Usted tiene la opción de filtrar por **suscripciones**, **los grupos de recursos**, **tipos de recursos**, **Recursos**, **rango de tiempo**, y **Estado**. Al hacer clic en una alerta en la lista **Resumen de alertas**, se accede a **Detalles de la alerta**, como se muestra en la [Figura 1-18](#).

The screenshot shows the Azure Monitor Alerts interface. At the top, there are dropdown menus for Subscriptions (All), Resource groups (All), Resource types (All), and Resources (All). Below these are filters for Time Range (Last 24 hours) and State (All).

The main area is titled "Alert Summary". It displays a table with columns: Severity, Count, New, Acknowledged, and Closed. Two rows are shown: one for "Sev 1" with 2 new alerts, and one for "Sev 4" with 12 new alerts. The "Sev 1" row is highlighted with a blue background.

Below the summary is a tab labeled "Alert Details" which is currently selected. It shows "2 'Sev1' Alerts". A search bar is present above the alert log table.

The final section is a table titled "Alerts by Region" with columns: StartTime, Severity, State, Name, and TargetResource. It lists two entries: one from 6/16/2020 at 1:08:11 AM and another from 6/15/2020 at 2:28:37 PM, both for "ds-availability-az303ai".

FIGURA 1-18 La plantilla del libro de trabajo de alertas para los registros de Azure Monitor

HABILIDAD 1.2: IMPLEMENTAR CUENTAS DE ALMACENAMIENTO

Azure Storage es un almacén de datos administrado. Es seguro, duradero, enormemente escalable y de alta disponibilidad listo para usar. Puede configurar Azure Storage para resistir una interrupción local o un desastre natural mediante la replicación. Azure Storage puede adaptarse a una amplia variedad de casos de uso de datos en sus servicios principales y es accesible en todo el mundo. Como arquitecto de Azure, necesita saber cómo se pueden configurar una cuenta de almacenamiento y sus servicios principales para adaptarse a los requisitos de sus clientes.

Esta habilidad cubre cómo:

- ■ Seleccione las opciones de la cuenta de almacenamiento según un caso de uso
- ■ Configurar Azure Files y Blob Storage
- ■ Administrar claves de acceso
- ■ Configurar el acceso de red a la cuenta de almacenamiento
- ■ Implementar firmas de acceso compartido y políticas de acceso.
- ■ Implementar la autenticación de Azure AD para el almacenamiento
- ■ Implementar la replicación de Azure Storage
- ■ Implementar la conmutación por error de la cuenta de Azure Storage

Seleccione las opciones de la cuenta de almacenamiento según un caso de uso

La configuración de una cuenta de almacenamiento durante el proceso de creación determina las funciones que están disponibles para su uso. Esta configuración rige qué servicios básicos, niveles de rendimiento y niveles de acceso son accesibles después de la creación de la cuenta. Por lo tanto,

al diseñar la arquitectura del almacenamiento para sus aplicaciones, se debe prestar especial atención a las opciones de la cuenta de almacenamiento.

Todas las cuentas de almacenamiento se cifran en reposo mediante claves de cifrado administradas por Microsoft y cifrado del servicio de almacenamiento (SSE) para los datos en reposo.

Servicios principales

Para explorar más las cuentas de almacenamiento, es importante comprender los servicios principales disponibles en Azure Storage y cómo se pueden usar:

- ■ **Blobs de Azure.** Los blobs de Azure están optimizados para almacenar cantidades masivas de datos no estructurados, ya sean binarios o basados en texto. Los blobs de Azure se pueden usar para imágenes, documentos, archivos de respaldo, transmisión de video y audio. Las manchas vienen en tres tipos:
 - ■ **Bloquear blobs.** Datos binarios y de prueba, hasta 4,7 TB.
 - ■ **Anexar blobs.** Blobs de bloques optimizados para anexos y buenos para el registro.
 - ■ **Blobs en la página.** Blobs de lectura / escritura aleatorios que se utilizan para discos o archivos VM VHD y pueden tener hasta 8 TB.
- ■ **Archivos de Azure.** Servicio de archivos compartidos basado en Server Message Block (SMB). Úselo como reemplazo de un recurso compartido de archivos local tradicional o comparta archivos de configuración entre varias cargas de trabajo de Azure. Azure Files se puede sincronizar con un servidor local para escenarios de uso compartido de archivos híbridos.
- ■ **Colas de Azure.** Almacena mensajes de hasta 64K. Normalmente se utiliza para escenarios de procesamiento asincrónico primero en entrar, primero en salir (FIFO).
- ■ **Tablas de Azure.** Un servicio de datos estructurado NoSQL. Es un almacén de clave / valor que tiene un diseño sin

esquema, que puede usarse para almacenar grandes cantidades de datos flexibles. (Se recomienda Azure Cosmos DB para todos los datos flexibles no estructurados).

- ■ **Discos de Azure.** Discos para máquinas virtuales. Aunque figura como un servicio principal, no se puede configurar; en su lugar, está completamente administrado por Azure.

Tipo de cuenta de almacenamiento

Los servicios básicos disponibles para su uso dependen del tipo de cuenta de almacenamiento elegido. El tipo predeterminado para una cuenta de almacenamiento en el momento de la creación es General-Purpose V2, que es el tipo de cuenta de almacenamiento recomendado por Microsoft y es compatible con todos los servicios principales enumerados en la sección anterior.

El siguiente comando de la CLI de Azure crea una cuenta V2 de uso general denominada az303defaultsa .

[Haga clic aquí para ver la imagen del código](#)

```
Crear cuenta de almacenamiento az --name az303defaultsa --  
resource-group $ resourceGroupName
```

Para cambiar el tipo de cuenta de almacenamiento, agregue el parámetro --kind , que tiene las siguientes opciones:

- ■ **StorageV2.** También conocido como **V2 de uso general** , este es el valor predeterminado para una cuenta de almacenamiento y el tipo de cuenta recomendado por Microsoft. El acceso a todos los servicios básicos y sus niveles de rendimiento asociados y niveles de acceso está disponible.
- ■ **Almacenamiento.** También conocido como **V1 de propósito general** , se proporciona para el soporte heredado de implementaciones más antiguas. El acceso a todos los servicios básicos y niveles de rendimiento está disponible, pero no hay niveles de acceso disponibles para seleccionar. Es posible actualizar de V1 a V2 usando la línea de comando.
- ■ **Almacenamiento de blobs.** Esto se proporciona para compatibilidad heredada con blobs. Todos los niveles de acceso

están disponibles, pero solo se puede seleccionar el rendimiento estándar. Utilice **V2 de uso general en lugar de Blob Storage** cuando sea posible.

- **BlockBlobStorage.** Almacenamiento de baja latencia para blobs con altas tasas de transacción, rendimiento superior sin niveles de acceso.
- **Sólo** archivos de **almacenamiento de archivos**, rendimiento superior y niveles sin acceso. Esta opción se puede configurar específicamente para mejoras de rendimiento relacionadas con archivos, como la ráfaga de IOPS.

El siguiente comando CLI Azure crea una **BlockBlobStorage cuenta** llamada `az303blockblob`:

[Haga clic aquí para ver la imagen del código](#)

```
Crear cuenta de almacenamiento az --name az303blockblob --  
resource-group $ resourceGroupName  
- kind BlockBlobStorage
```

Nivel de acceso

Los blobs admiten tres niveles de acceso, Hot, Cool y Archive. Los niveles de acceso están optimizados para patrones específicos de uso de datos. Estos patrones corresponden a la frecuencia de acceso a los datos subyacentes. Esto significa que al seleccionar cuidadosamente su nivel de acceso, puede reducir sus costos. Examinando esto más a fondo:

- **Nivel caliente.** Costos de almacenamiento más altos, costos de acceso más bajos. Se utiliza para los datos a los que se accede con frecuencia y es el nivel predeterminado.
- **Nivel fresco.** Costos de almacenamiento más bajos que costos de acceso más altos y en caliente. Úselo para los datos que se almacenarán "tal cual" y no se accederá a ellos durante al menos 30 días.
- **Nivel de archivo.** Esto es solo a nivel de blob. Costos de almacenamiento más bajos, costos de acceso más altos. Úselo únicamente para los datos que permanecerán "como están" a los que no se accederá durante al menos 180 días y que pueden

soportar una alta latencia de recuperación de varias horas. Excelente para copias de seguridad a largo plazo y datos de archivo.

[Haga clic aquí para ver la imagen del código](#)

```
Crear cuenta de almacenamiento az --name az303blobaccesstier  
--resource-group $ resourceGroupName  
  
-Kind StorageV2 -access-tier hot
```

El comando de la CLI de Azure anterior crea una cuenta V2 de uso general denominada `az303blobaccesstier` con un nivel de acceso activo .

[Haga clic aquí para ver la imagen del código](#)

```
Crear cuenta de almacenamiento az --name az303blobaccesstier  
--resource-group $ resourceGroupName  
  
--kind StorageV2 - nivel de acceso caliente
```

Un nivel de acceso se puede cambiar en cualquier momento mediante la línea de comandos o Azure Portal. Para cambiar `az303blobaccesstier` al nivel Cool en la CLI de Azure, emita el siguiente comando:

[Haga clic aquí para ver la imagen del código](#)

```
actualización de la cuenta de almacenamiento az --name  
az303blobaccesstier --resource-group $ resourceGroupName  
  
--kind StorageV2 --access-tier cool
```

Tenga en cuenta la penalización por eliminación anticipada

Cambiar el nivel de Archive o Cool antes de los períodos respectivos de 180 o 30 días incurrirá en una penalización por eliminación anticipada equivalente al costo de los días restantes del almacenamiento.



Sugerencia de examen Configuración de almacenamiento de Azure

Comprender qué servicios básicos, niveles de acceso y niveles de rendimiento están disponibles para los tipos de cuentas de almacenamiento es un área importante para esta certificación. Consulte <https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview#types-of-storage-accounts> para una revisión más detallada .

Configurar Azure Files y Blob Storage

Una vez que haya elegido las opciones de su cuenta de almacenamiento, debe configurar "contenedores" específicos de casos de uso para sus datos. Estos son los servicios principales de Azure Storage, como se enumeró anteriormente. El método de creación de estos cambios de contenedores depende del servicio principal que esté configurando. La certificación AZ-303 requiere que comprenda la configuración de Azure Files y Blob Storage.

Archivos de Azure

Azure Files se puede configurar en la línea de comandos y dentro de Azure Portal. Siga estos pasos para configurar Azure Files mediante la ejecución de cmdlets en PowerShell:

1. Utilice estos cmdlets para crear una cuenta de almacenamiento:

Haga clic aquí para ver la imagen del código

```
$ resourceGroupName = "12almacenamiento"

$ ubicación = "noreste de Europa"

$ storageAccountName = "az303fsdemosa"

New-AzResourceGroup -Name $ resourceGroupName -Location
$ location '

    -Tag @ {departamento = "desarrollo"; env = "dev"}

$ sacc = New-AzStorageAccount ' 

    -ResourceGroupName $ resourceGroupName ' 

    -Name $ storageAccountName '
```

```
-Ubicación $ ubicación '
-Kind StorageV2 '
-SkuName Standard_LRS '
-EnableLargeFileShare
```

Estos cmdlets de PowerShell crean una cuenta de almacenamiento denominada `az303fsdemosa` que admite el servicio principal de Azure Files. Si compara estos cmdlets con el comando de la CLI de Azure de la sección "Niveles de acceso", es algo similar, excepto por el cmdlet `-EnableLargeFileShare`. Este cmdlet indica a Azure que habilite archivos compartidos de más de 5 TB en esta cuenta de almacenamiento. El objeto de la cuenta de almacenamiento se almacena en una variable `$ sacc`, que le permite utilizar el contexto de la cuenta de almacenamiento más adelante en su configuración sin tener que recuperarlo nuevamente. Explorará los contextos de las cuentas de almacenamiento en "Administrar claves de acceso", más adelante en este capítulo.

2. Cree un recurso compartido de archivos denominado `az303share` y establezca un tamaño máximo de 1 TB con `-QuotaGB` en este cmdlet de PowerShell:

Haga clic aquí para ver la imagen del código

```
$ shareName = "az303share"

New-AzRmStorageShare '
-StorageAccount $ sacc '
-Nombre $ shareName '
-QuotaGiB 1024
```

Nota Cambio de cuotas

Las cuotas se pueden cambiar con `Update-AzRmStorageShare`.

3. En este punto, puede comenzar a cargar archivos en su recurso compartido una vez que haya creado una estructura de carpetas que se denomina "estructura de directorio" en Azure

Files. Ejecute los siguientes comandos en PowerShell para crear una carpeta denominada `topLevelDir`:

Haga clic aquí para ver la imagen del código

```
$ dirName = "topLevelDir"  
  
New-AzStorageDirectory '  
    -Contexto $ sacc.Context '  
    -ShareName $ shareName '  
    -Ruta $ dirName
```

PowerShell devuelve la URL del directorio, como se muestra en el siguiente resultado:

Haga clic aquí para ver la imagen del código

```
-Directorio:  
https://az303fsdemos.afile.core.windows.net/az303share
```

Tipo	Longitud	Nombre
Directorio	0	<code>topLevelDir</code>

Esta URL se puede utilizar desde el interior de una aplicación para acceder al directorio desde cualquier lugar, siempre que la aplicación esté autenticada y autorizada para hacerlo.

4. Aún debe tener el contexto de la cuenta de almacenamiento en su sesión de PowerShell. Ahora puede usar esto en lugar de la URL del directorio para cargar un archivo en su nuevo directorio. Ejecute este cmdlet para cargar un archivo llamado `file.txt`:

Haga clic aquí para ver la imagen del código

```
"Ejemplo de recurso compartido de AZ-303 Azure Files" |  
out-file -FilePath "file.txt" -Force  
  
Set-AzStorageFileContent '
```

```
-Contexto $ sacc.Context  
-ShareName $ shareName '  
-Fuente "file.txt" '  
-Ruta "$ ($ dirName) \ file.txt"
```

Utilice Azure Portal para explorar el recurso compartido de archivos de la cuenta de almacenamiento y comprobar la existencia del archivo.

Almacenamiento de blobs

Las gotas se almacenan en un contenedor; puede pensar en un contenedor como una agrupación de blobs. Un contenedor funciona para blobs de la misma manera que una carpeta para archivos. Como se mencionó anteriormente, una cuenta de Azure Storage puede admitir varios servicios principales. Por lo tanto, para este ejemplo, la cuenta de almacenamiento az303fsdemosa se actualizará para permitir que se almacenen blobs. Siga los pasos a continuación, ejecutando los comandos en PowerShell, para configurar un contenedor de blobs, cargar un archivo y explorar más a fondo las opciones de configuración de blobs. Este ejemplo supone que continúa desde el paso 4 en la sección anterior ("Archivos de Azure") con el contexto de la cuenta de almacenamiento disponible en \$ saccobjeto. Si este no es el caso, lea la sección "Administrar claves de acceso" más adelante en este capítulo para aprender cómo obtener el contexto de la cuenta de almacenamiento:

1. En PowerShell, ejecute el siguiente cmdlet para crear un contenedor de blobs denominado imágenes :

[Haga clic aquí para ver la imagen del código](#)

```
$ containerName = "imágenes"  
  
New-AzStorageContainer '  
-Nombre $ containerName '  
-Contexto $ sacc.Context '  
-Blob de permiso
```

Tenga en cuenta el parámetro `-Permission`, que establece el nivel de acceso público del blob; hay tres valores para este parámetro:

1. ■ **Ninguno.** Este parámetro significa que no se permite el acceso público; los contenedores con este parámetro son privados. Para utilizar este contenedor, un servicio debe autenticarse y estar autorizado para hacerlo.
 2. ■ **Blob.** Este parámetro otorga acceso de lectura a los blobs en el contenedor cuando se accede directamente. No se puede acceder al contenido del contenedor u otros datos sin autenticación y autorización.
 3. ■ **Contenedor.** Este parámetro otorga acceso de lectura a los blobs y al contenedor. Se puede enumerar el contenido del recipiente.
2. Ahora puede usar el contexto de la cuenta de almacenamiento para cargar archivos en el contenedor. Ejecute los siguientes comandos en PowerShell para cargar un archivo en el contenedor de imágenes creado anteriormente.

Haga clic aquí para ver la imagen del código

```
Set-AzStorageBlobContent -File "D:\az303files\uploadTest.jpg" '  
-Container $ containerName '  
-Blob "uploadTest.jpg" '  
-Contexto $ sacc.Context
```

Nota Editar el bloque de código

Deberá editar este bloque de código para establecer el parámetro `-File` en un archivo de imagen que exista en su cliente. Es posible que también desee cambiar el parámetro `-Blob` para que los nombres de archivo coincidan después de la carga.

3. Abra Azure Portal y navegue hasta la cuenta de almacenamiento `az303fsdemosa`. En el menú **Cuenta de almacenamiento**, en **Servicio de blob**, elija **Contenedores**. Haga

clic en el nombre del contenedor **Imágenes** para ver el archivo almacenado en él.

4. En el menú **Cuenta de almacenamiento**, haga clic en **Protección de datos**. Aquí, puede configurar **Blob Soft Delete**, que habilita un mecanismo para recuperar Blobs eliminados accidentalmente. La política de retención es de 7 a 365 días. **Blob Soft Delete** es una propiedad de nivel de cuenta de almacenamiento que afecta a todos los contenedores de blobs. Para habilitar **Blob Soft Delete** con PowerShell, establezca una política de retención en el objeto de la cuenta de almacenamiento con el siguiente comando:

Haga clic aquí para ver la imagen del código

```
$ sacc | Enable-AzStorageDeleteRetentionPolicy -  
RetentionDays 7
```

5. Vuelva a Azure Portal y haga clic en las otras opciones del servicio BLOB para examinarlas más a fondo:

- 0.■ **Gestión del ciclo de vida.** Esta opción le permite establecer reglas para la transición automática de blobs a través de los niveles Cool y Archive hasta una posible eliminación después de un número específico de días desde la modificación.
- 1.■ **Dominio personalizado.** El almacenamiento de blobs se puede configurar para utilizar nombres de dominio personalizados.
- 2.■ **Azure CDN.** Esta opción proporciona integración a Azure CDN para brindar una latencia constante para el acceso en cualquier parte del mundo.
- 3.■ **Búsqueda de Azure.** Esta opción agrega la búsqueda de texto completo a los blobs mediante Azure Cognitive Search.

Administrar claves de acceso

Cuando crea una cuenta de almacenamiento, Azure también crea dos claves de acceso, que se pueden usar para acceder a la cuenta mediante programación. Por ejemplo, en la sección "Archivos de Azure", se mencionó el "contexto" en múltiples ocasiones. Un objeto de contexto de Azure PowerShell contiene información de autenticación, lo que le

permite ejecutar cmdlets de PowerShell en los recursos. En la sección "Archivos de Azure", el contexto es un contexto de almacenamiento, que le permite ejecutar cmdlets de almacenamiento en un recurso de cuenta de almacenamiento que requiere un contexto. Para recuperar el contexto de la cuenta en PowerShell, primero debe recuperar la clave de acceso para la cuenta de almacenamiento. El contexto se recupera usando la clave. Por ejemplo, en la cuenta `az303fsdemos` utilizada en la sección "Archivos de Azure", usaría este código:

[Haga clic aquí para ver la imagen del código](#)

```
$ clave1 = (Get-AzStorageAccountKey '  
    -name $ storageAccountName '  
    -ResourceGroupName $ resourceGroupName '  
) .value [0]  
  
$ key1  
  
$ ctx = New-AzStorageContext '  
-StorageAccountName $ storageAccountName '  
-StorageAccountKey $ key1  
  
$ key1 almacena la clave de acceso principal y el contexto de  
almacenamiento está en $ ctx. El contexto se puede utilizar para  
administrar la configuración de la cuenta de almacenamiento y acceder a  
los datos almacenados.
```

Microsoft recomienda que las claves de acceso se rotén con regularidad. La rotación de las claves ayuda a mantener seguras las cuentas de almacenamiento al invalidar las claves antiguas. Para rotar manualmente las llaves, se debe seguir el siguiente proceso:

1. Modifique las conexiones de servicio para usar la clave secundaria.
2. Gire la clave principal en Azure Portal o en la línea de comandos. Por ejemplo, para rotar `key1` para la cuenta de almacenamiento `az303fsdemos` en PowerShell, ejecute los siguientes comandos:

Haga clic aquí para ver la imagen del código

```
New-AzStorageAccountKey  
    -ResourceGroupName $ resourceGroupName  
    -Name $ storageAccountName  
    -KeyName key1
```

3. Modifique las conexiones de servicio para volver a utilizar la clave principal.
4. Gire la llave secundaria utilizando el mismo método que se muestra en el paso 2.

El cambio entre primaria y secundaria en este proceso es la razón por la que Microsoft recomienda que todos los servicios utilicen solo las claves primarias o secundarias de forma predeterminada. De lo contrario, las conexiones a las cuentas de almacenamiento se perderán cuando gire las claves.

¿Necesita más revisión? Administrar claves de acceso

Para obtener información sobre el uso de Azure Key Vault para administrar las claves de acceso, consulte <https://docs.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage>.

Configurar el acceso de red a la cuenta de almacenamiento

Los servicios principales configurables son puntos finales vinculados y cada uno tiene una dirección única basada en un URI conocido:

- ■ **Blob.** *http://<nombre-cuenta-almacenamiento>.blob.core.windows.net*
- ■ **Archivo.** *http://<nombre-de-cuenta-de-almacenamiento>.file.core.windows.net*
- ■ **Mesa.** *http://<nombre-de-cuenta-de-almacenamiento>.table.core.windows.net*

- **Cola.** `http://<nombre-de-cuenta-de-almacenamiento>.queue.core.windows.net`

Los puntos finales son públicos y, de forma predeterminada, la cuenta de almacenamiento está configurada para aceptar todo el tráfico a los puntos finales públicos, incluso el tráfico de Internet. Sin embargo, no puede obtener acceso a un punto de conexión sin la autorización adecuada mediante una clave de acceso, un token de firma de acceso compartido (SAS) o Azure AD. Es probable que los casos de uso de sus clientes requieran que el punto final público esté protegido a un rango de direcciones IP o a una red virtual específica. Esto se configura usando cortafuegos de almacenamiento y redes virtuales. Puede usar la línea de comandos o el portal de Azure para configurar el acceso a la red. Para explorar la configuración en Azure Portal, siga estos pasos:

1. Con Azure Portal, busque **la cuenta de almacenamiento** en la barra de recursos de búsqueda. Seleccione **Cuentas de almacenamiento** en el menú desplegable que se muestra a medida que escribe el nombre del recurso en la búsqueda. Seleccione **12storage** de la lista de cuentas de almacenamiento. Este paso asume que todavía tiene disponible la cuenta de almacenamiento que creó anteriormente en este capítulo. De lo contrario, elija cualquier cuenta de almacenamiento recién creada.
2. En el menú **Cuenta de almacenamiento**, desplácese hacia abajo y haga clic en **Cortafuegos y redes virtuales** para abrir la hoja.
3. Se selecciona la configuración predeterminada de **Todas las redes**. Como se discutió, esto significa que todo el tráfico, incluso el tráfico de Internet, puede acceder al punto final. Elija **redes seleccionadas**. Las opciones de configuración para redes virtuales y el firewall de la cuenta de almacenamiento se muestran en la Figura 1-19.

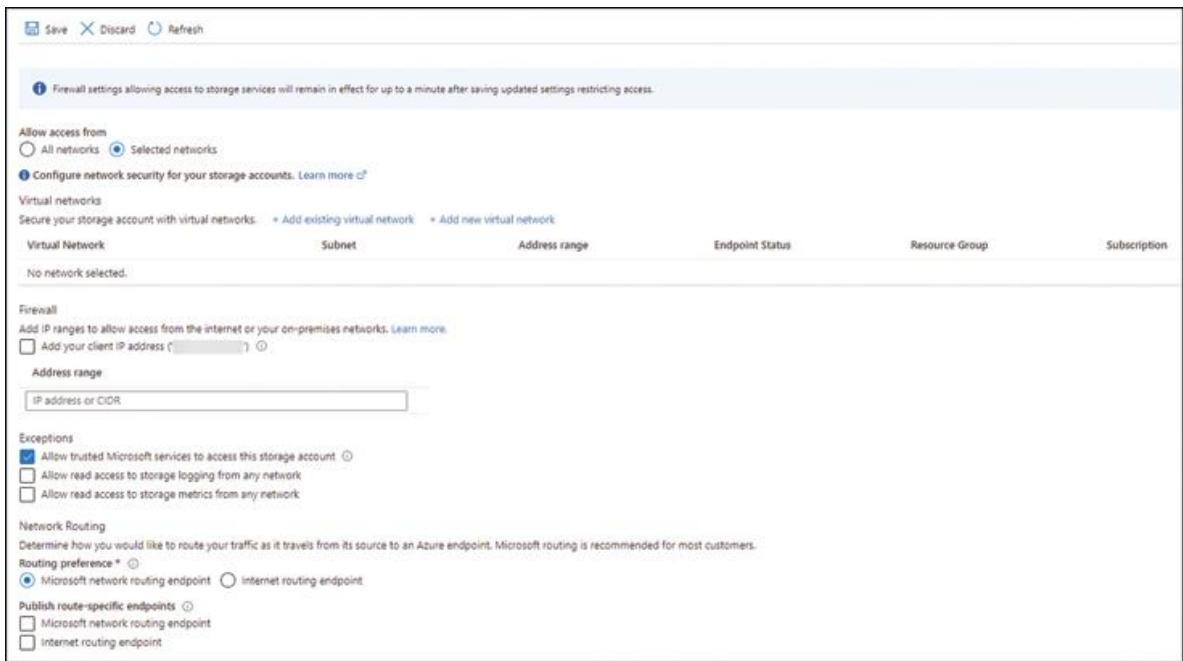


FIGURA 1-19 Configure el firewall de la cuenta de almacenamiento y las redes virtuales

4. Al elegir **Redes seleccionadas**, la regla de red ahora se establece en "denegar", lo que significa que no se permite el acceso de tráfico a los puntos finales privados de la cuenta de almacenamiento de forma predeterminada. Para permitir el acceso a sus servicios, se deben agregar reglas específicas en las secciones **Cortafuegos** o **Redes virtuales** de la hoja **Cortafuegos y redes virtuales**.
5. La sección **Firewall** gobierna qué rangos de direcciones IP públicas pueden tener acceso a la cuenta de almacenamiento. Tiene la opción de configurar los siguientes ajustes:
 1. **Agregue la dirección IP de su cliente.** El portal de Azure recoge su dirección IP pública de acceso a Internet de su navegador. Si elige esta opción, su cliente se agregará a la lista de acceso. Para esta demostración, deje esta opción sin marcar.
 2. **Rango de direcciones.** Se pueden agregar direcciones IP individuales, como las direcciones IP públicas estáticas orientadas a Internet de sus clientes o un rango de direcciones en notación CIDR.

6. El acceso a la cuenta de almacenamiento se puede asegurar a subredes específicas dentro de una red virtual, lo que aísla aún más el acceso a su cuenta de almacenamiento. La red virtual puede estar en una suscripción diferente. Desde la sección **Redes virtuales** en la misma hoja, tiene las siguientes opciones:
 - 0.■ **Suscripción.** Aquí es donde elige la suscripción en la que reside su red virtual.
 - 1.■ **Redes virtuales.** Aquí es donde elige una red virtual, aunque solo se enumerarán las redes dentro del par regional de cuentas de almacenamiento.
 - 2.■ **Subredes.** Aquí es donde elige las subredes de la red virtual elegida que requieren acceso.
7. Haga clic en **Habilitar**. Esto creará un punto final de servicio para el almacenamiento en la red virtual.
8. Haga clic en **Agregar**. Esto le permite agregar la red virtual y la subred seleccionada para acceder a la cuenta de almacenamiento.
9. Las opciones que se muestran en la sección **Excepciones** cubren el acceso a los servicios de Azure que no se pueden aislar a través de las reglas de acceso a la red virtual o al firewall:
 - 0.■ **Permitir que los servicios de confianza de Microsoft accedan a esta cuenta de almacenamiento.** Deje esta opción seleccionada para permitir el registro, los servicios de respaldo y los servicios específicos a los que se les otorga acceso mediante una identidad administrada por el sistema.
 - 1.■ **Permitir acceso de lectura al registro de almacenamiento desde cualquier red.** Seleccionar esto permite acceder a registros y tablas para análisis de almacenamiento.
 - 2.■ **Permitir acceso de lectura a métricas de almacenamiento desde cualquier red.** La selección de esta opción permite métricas de acceso para análisis de almacenamiento.
10. Una vez que se complete la configuración, haga clic en **Guardar**.

11. Para probar la configuración actualizada, vuelva a PowerShell. Utilice los cmdlets de la sección "Administrar claves de acceso" anteriormente en este capítulo para recuperar el contexto. Ahora vuelva a ejecutar el comando para agregar un blob que discutimos en la sección "Configurar archivos de Azure y Blob Storage" de esta habilidad:

Haga clic aquí para ver la imagen del código

```
Set-AzStorageBlobContent -File "D:\az303files\uploadTest.jpg" '  
-Container $containerName '  
-Blob "uploadTest.png" '  
-Contexto $ctx  
  
Set-AzStorageBlobContent: esta solicitud no está autorizada para realizar esto  
  
operación. Código de estado HTTP: 403 - Mensaje de error HTTP: Esta solicitud no es  
  
autorizado para realizar esta operación.
```

Su dirección IP pública no forma parte de la lista de acceso, por lo que recibirá el error 403 anterior. Regrese a Azure Portal y seleccione **Agregar su dirección IP de cliente**, siga los pasos del paso 4 anterior y haga clic en **Guardar**. Espere un poco de tiempo (en promedio, alrededor de un par de minutos) y luego vuelva a ejecutar el cmdlet para agregar un blob. El blob se agregará porque su dirección IP ahora está en la lista de permitidos. Realice el mismo ejercicio desde una máquina virtual que forma parte de la subred agregada en el paso 5. Debería poder agregar el blob sin errores.

Punto final privado

Los terminales privados son una adición relativamente reciente a las opciones de configuración para el acceso a la red de la cuenta de almacenamiento. Los puntos de conexión privados brindan a las máquinas virtuales de una red virtual un enlace privado para acceder de forma segura a la cuenta de almacenamiento. El tráfico entre la máquina

virtual y la cuenta de almacenamiento fluye desde el cliente hasta el punto final privado de la red virtual y a través de la red troncal de Microsoft hasta la cuenta de almacenamiento. Este método de acceso tiene los siguientes beneficios:

- Bloquear la exfiltración de datos de la red virtual asegurando el tráfico al enlace privado
- Conecte de forma segura redes locales a una cuenta de almacenamiento mediante una puerta de enlace VPN o ExpressRoute a la red virtual con el enlace privado.
- Configure el firewall de la cuenta de almacenamiento para deshabilitar todas las conexiones al punto final público.

Cuando crea el punto final privado, debe especificar qué servicio principal de la cuenta de almacenamiento requiere acceso. Luego, Azure crea una zona DNS privada que permite que la URL del punto de conexión de almacenamiento original se resuelva en la dirección del punto de conexión privado, que tiene un alias con un subdominio de enlace privado .

¿Necesita más revisión? Configurar el acceso de red a la cuenta de almacenamiento

Para obtener más información sobre cómo configurar el acceso a la red a una cuenta de almacenamiento y puntos finales privados para el almacenamiento azul, consulte <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security> y <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints> .

Implementar firmas de acceso compartido y políticas de acceso

La clave de acceso de una cuenta de almacenamiento otorga al titular autorización para todos los recursos de la cuenta de almacenamiento. Es poco probable que este método de autorización siga el principio de privilegio mínimo para sus casos de uso. Una firma de acceso compartido (SAS) para una cuenta de almacenamiento otorga acceso restringido, servicios con derechos específicos, lo que permite un control granular sobre cómo el titular de un SAS puede acceder a los datos. Para explorar

cómo se configura SAS para una cuenta de almacenamiento y ver cómo se usa un SAS, siga estos pasos:

1. En Azure Portal, ingrese **la cuenta de almacenamiento** en la barra de recursos de búsqueda y elija **Cuenta de almacenamiento** en el menú desplegable que se muestra a medida que escribe el nombre del recurso. En la lista de cuentas de almacenamiento, seleccione la cuenta de almacenamiento `az303fsdemosa` utilizada en las secciones anteriores de la lista. Si esto no existe, seleccione cualquier otra cuenta de almacenamiento con un contenedor de blobs y blob.
2. En el menú **Cuenta de almacenamiento** a la izquierda, seleccione **Firma de acceso compartido** en **Configuración**. La hoja de **firma de acceso compartido** donde se puede configurar el SAS se abre a la derecha. La Figura 1-20 muestra un ejemplo de configuración:

The screenshot shows the 'Shared access signature' configuration page for a storage account. It includes sections for Allowed services (Blob checked), Allowed resource types (Container and Object checked), Allowed permissions (Read checked), Blob versioning permissions (Enables deletion of versions checked), Start and expiry date/time (Start: 09/05/2020 at 9:00:00 AM, End: 09/12/2020 at 9:00:00 AM), Allowed IP addresses (example: 168.1.5.65 or 168.1.5.65-168.1.5.70), Allowed protocols (HTTPS only selected), Preferred routing tier (Basic (default) selected), and a note about routing options being disabled because endpoints are not published. At the bottom, there is a 'Generate SAS and connection string' button.

FIGURA 1-20 Creación de una firma de acceso compartido (SAS) en Azure Portal

3. La configuración que se muestra crea un SAS para acceder a los contenedores de blobs. Cada ajuste de configuración define la granularidad de la autorización:
 1. ■ **Servicios permitidos.** Los servicios principales a los que puede acceder SAS.
 2. ■ **Tipos de recursos permitidos.** Acceso a los niveles de API bajo el servicio permitido:
 - 1.■ **Servicio.** API de nivel de servicio, como contenedores de listas, colas, tablas o recursos compartidos.
 - 2.■ **Contenedor.** API a nivel de contenedor, como API para crear o eliminar contenedores, crear o eliminar colas, crear o eliminar tablas o crear o eliminar recursos compartidos.
 - 3.■ **Objeto.** API de nivel de objeto, como Put Blob, Query Entity, Get Messages, Create File, etc.
 3. ■ **Permisos** permitidos Los permisos definidos por tipo de recurso.
 0. ■ **Leer / Escribir.** Válido para todo tipo de recursos.
 1. ■ **Eliminar.** Válido para tipos de contenedor y objeto.
 2. ■ **Otras opciones.** Todas las demás opciones son válidas para los tipos de objeto.
 4. ■ **Habilita la eliminación de versiones.** Cuando el permiso permitido está configurado para eliminar (las viñetas anteriores), SAS otorga permiso para eliminar versiones de blob.
 5. ■ **Fecha / hora de inicio y vencimiento.** El tiempo de boxeo para el SAS, el SAS no funcionará fuera de este rango de datos.
 6. ■ **Direcciones IP permitidas.** Direcciones únicas o rangos en notación CIDR. Déjelo en blanco para cualquier dirección IP.

7. ■ **Protocolos permitidos.** HTTPS o HTTPS y HTTP.
8. ■ **Nivel de enrutamiento preferido.** **Básico**. Si se han especificado puntos finales en la configuración de firewalls y redes virtuales para la cuenta de almacenamiento, también puede seleccionar los tipos de enrutamiento para los puntos finales.
9. ■ **Clave de firma.** La clave de acceso utilizada para firmar el SAS. Tenga en cuenta que si rota sus claves, su SAS también debe regenerarse.

Con la información anterior y mirando la [Figura 1-20](#), puede deducir el acceso otorgado por este SAS a los recursos de la cuenta de almacenamiento. Otorgará acceso al servicio de blob a nivel de contenedor y objeto. El acceso de nivel de lectura permite la lista de blobs almacenados en un contenedor y la lectura de blobs dentro del contenedor. La casilla de verificación **Habilita la eliminación de versiones** se puede ignorar porque la eliminación a nivel de objeto no es un permiso otorgado. El SAS será válido desde las 9 a. M. Del 12 de junio hasta las 9 a. M. Del 19 de junio y se puede acceder a él a través de HTTPS.

4. Haga clic en **Generar SAS y cadena de conexión como se muestra** en la [Figura 1-20](#). El token SAS y la URL se crean y se muestran debajo del botón **Generar SAS y cadena de conexión**. El formato de las cadenas se muestra en la [Figura 1-21](#).

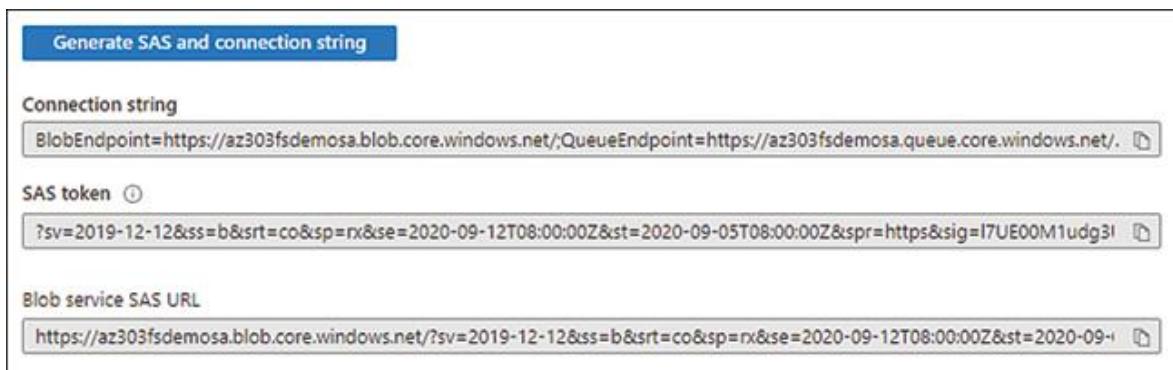


FIGURA 1-21 Cadena de conexión SAS, token SAS y URL SAS de Blob Service generados, como se muestra en Azure Portal

Si observa la URL SAS de SAS Token and Blob Service en la [Figura 1-21](#), los parámetros directamente después de ? son las opciones elegidas en la

pantalla de creación de SAS. La cadena grande después de `& sig =` es la firma digital utilizada para verificar y autorizar el acceso solicitado.

Muchos lenguajes de programación pueden utilizar tokens SAS, URL y cadenas de conexión a través de sus kits de desarrollo de software (SDK) para acceder a los datos de la cuenta de almacenamiento. Para ver esto en acción, aquí está el resultado de PowerShell de la sección "Administrar claves de acceso" de anteriormente en este capítulo, que se actualizó para usar el token SAS generado desde Azure Portal:

[Haga clic aquí para ver la imagen del código](#)

```
$ resourceGroupName = "12almacenamiento"

$ storageAccountName = "az303fsdemos"

$ SASToken = "? Sv = 2019-10-10 & ss = b & srt = co & sp = rx
& se = 2020-06-19T08: 00: 00Z & st = 2020-06-12T08: 0
0: 00Z & spr = https & sig =
ceDhRXv2uu937OcRaCrtVdrHd1WDy8gLqNboZkqxwxM% 3D "

$ containerName = "imágenes"

$ ctx = New-AzStorageContext '
-StorageAccountName $ storageAccountName '
-SasToken $ SASToken
```

Ejecute los comandos anteriores en una terminal de PowerShell para establecer el contexto utilizando el token SAS pasado al parámetro `-SasToken`. El token SAS otorga acceso de lectura, por lo que se puede usar para obtener un blob de un contenedor. Para obtener el blob, ejecute los siguientes comandos en PowerShell:

[Haga clic aquí para ver la imagen del código](#)

```
Get-AzStorageBlobContent '
-Container $ containerName '
```

```
-Blob "uploadTest.png" '
-Destino "d:\ az303files \"'
-Contexto $ ctx

Contenedor Uri:
https://az303fsdemosa.blob.core.windows.net/images
```

Nombre BlobType Longitud ContentType

Última modificación de AccessTier SnapshotTime IsDeleted

uploadTest.png BlockBlob 592021 imagen / png

2020-06-11 23: 44: 18Z Desconocido Falso

No olvide asegurarse de que el cliente desde el que está ejecutando PowerShell tenga acceso de red a la cuenta de almacenamiento; de lo contrario, el cmdlet anterior generará un error.

Si ahora intentó ejecutar el cmdlet add blob de la sección "Configurar Azure Files y Blob Storage" anteriormente en este capítulo, se producirá un error porque el token SAS está creando un contexto que solo tiene acceso de lectura. Para probar esto, ejecute los siguientes comandos en PowerShell:

Haga clic aquí para ver la imagen del código

```
Set-AzStorageBlobContent -File "D:\ az303files \
uploadTestSAS.png" '
-Container $ containerName '
-Blob "uploadTestSAS.png" '
-Contexto $ ctx

Set-AzStorageBlobContent: esta solicitud no está autorizada
para realizar esta operación

usando este permiso. Código de estado HTTP: 403 - Mensaje de
error HTTP: Esta solicitud no es
```

autorizado para realizar esta operación utilizando este permiso.

ErrorCode: AuthorizationPermissionMismatch

ErrorMessage: esta solicitud no está autorizada para realizar esta operación utilizando este permiso.

Implementar la autenticación de Azure AD para el almacenamiento

Los tokens de acceso a la cuenta de Azure Storage y los tokens SAS deben compartirse para poder usarse. Aunque los tokens compartidos se pueden almacenar de forma segura en Azure Key Vault para minimizar el riesgo, aún existe la posibilidad de que un token se almacene en el control de código fuente o se transmita de manera insegura. Esta es una posible vulnerabilidad de seguridad y, como arquitecto de Azure, es parte de su función minimizar las posibles vulnerabilidades de seguridad.

Azure Active Directory (Azure AD) se puede usar para crear una entidad de seguridad en forma de usuario, grupo o aplicación. A la entidad de seguridad se le pueden otorgar permisos para colas y blobs de Azure Storage mediante el control de acceso basado en roles (RBAC). En este modelo, la entidad de seguridad se autentica en Azure AD y se devuelve un token de OAuth. Luego, el token se usa para autorizar solicitudes contra Azure Storage. No se comparten credenciales con la autenticación de Azure AD; por este motivo, Microsoft recomienda utilizar Azure AD para la autorización de una cuenta de almacenamiento siempre que sea posible.

Con la cuenta de almacenamiento de ejemplo `az303fsdemosa` que ha estado explorando a lo largo de esta habilidad, puede probar el acceso principal del usuario. Si ya no tiene esta cuenta de almacenamiento, sustituya las variables `$ storageAccountName` y `$ containerName` por las que existen en su suscripción. Para este ejemplo, deberá colocar un archivo de texto en la variable `$ containerName`. Los siguientes fragmentos de código utilizan un mosaico de texto denominado `storage-az303demo.txt`.

Abra una terminal de PowerShell e inicie sesión como el usuario que creó la cuenta de almacenamiento. Ejecute los siguientes cmdlets para establecer el contexto con Azure AD e intente recuperar el blob de prueba:

[Haga clic aquí para ver la imagen del código](#)

```
$ resourceGroupName = "12almacenamiento"  
$ storageAccountName = "az303fsdemos"  
$ containerName = "imágenes"  
  
$ ctx = New-AzStorageContext '  
-StorageAccountName $ storageAccountName '  
-UseConnectedAccount  
  
Get-AzStorageBlobContent '  
-Container $ containerName '  
-Blob "almacenamiento-az303demo.txt" '  
-Destino "d: \ az303files \"  
-Contexto $ ctx
```

Tenga en cuenta el parámetro `-UseConnectedAccount` de `New-AzStorageContext` anterior. Esto indica al cmdlet que use la autenticación OAuth para recuperar un token de acceso para la cuenta que inició sesión. Este token de OAuth se usa luego para obtener los permisos para la cuenta de almacenamiento, que se convierte en parte del contexto de almacenamiento.

El cmdlet `Get-AzStorageBlobContent` fallará con un error 403: solicitud no autorizada. La cuenta con la que inició sesión creó la cuenta de almacenamiento; se le asignó automáticamente el rol de propietario a la cuenta de almacenamiento. El rol de propietario es para el "plano de

administración" de un recurso de Azure y la cuenta tiene acceso completo para administrar la configuración de la cuenta de almacenamiento. El rol de propietario no tiene permisos en el "plano de datos"; por lo tanto, no puede leer, escribir, actualizar ni eliminar datos. La línea de comandos o el portal de Azure se pueden usar para otorgar los permisos necesarios a través de RBAC. Abra Azure Portal y siga estos pasos para otorgar permiso de lectura a Blob Storage:

1. En la barra de recursos de búsqueda en la parte superior del portal, ingrese **la cuenta de almacenamiento**, luego elija **Cuenta de almacenamiento** en el menú desplegable que se muestra mientras escribe el nombre del recurso. De la lista de cuentas de almacenamiento, seleccione la cuenta de almacenamiento `az303fsdemosa` o la cuenta utilizada en la sección anterior de la lista.
2. Haga clic en **Control de acceso (IAM)** en el menú. Aquí es donde se asignan los permisos a través de RBAC. Haga clic en la pestaña **Asignaciones de roles**. Si ha estado siguiendo esta habilidad, no verá ningún usuario en la lista. Esta pestaña muestra todas las asignaciones de roles concedidas que afectan a este recurso; estos pueden estar a nivel de recursos o pueden heredarse de un ámbito principal.
3. Haga clic en **Agregar** en la parte superior y elija **Agregar asignación de funciones**. En el menú desplegable superior, elija **Storage Blob Data Reader**. Esto otorgará permiso de solo lectura al servicio de blob de la cuenta de almacenamiento. Deje **Asignar acceso para establecer como usuario, grupo o entidad de servicio de Azure AD**. Ahora puede buscar un usuario, grupo o entidad de servicio. Busque el usuario que no pudo ejecutar el cmdlet de PowerShell anterior y selecciónelo. La hoja **Agregar asignación de funciones** debe tener el aspecto que se muestra en la [Figura 1-22](#).



FIGURA 1-22 Asignación del rol de lector de datos de Storage Blob a un usuario de Azure AD

Haga clic en **Guardar** en la parte inferior de la tarea para asignar el permiso, que lo llevará de regreso a la lista de **asignaciones de roles**. Si se desplaza hacia abajo hasta la parte inferior, se ha agregado la función Lector de datos de Storage Blob.

4. Vuelva a la terminal de PowerShell y vuelva a ejecutar los cmdlets desde el principio de esta sección. El cmdlet `Get-AzStorageBlobContent` ya no genera errores y se recupera el blob.

Este ejemplo explica cómo otorgar permisos a un usuario o grupo, pero ¿qué pasa con una aplicación? Es más probable que, como arquitecto, diseñe una solución en la que una aplicación acceda a los recursos de almacenamiento. Una aplicación requiere una entidad de servicio o una identidad administrada, a las que se les otorgan los permisos para acceder al recurso. Puede pensar en una entidad de servicio o una identidad administrada como equivalente a una cuenta de servicio en un Active Directory local. Microsoft recomienda usar una identidad administrada siempre que sea posible. Los pasos siguientes usan una combinación de la CLI de Azure y una función de Azure como ejemplo:

1. Cree una función de Azure con un disparador HTTP. Para obtener ayuda con esto, consulte "Implementar funciones de Azure" en la habilidad "Implementar soluciones para aplicaciones" en el [Capítulo 3](#).
2. En Azure Portal, busque la **función de aplicación** en la barra de recursos de búsqueda en la parte superior. Seleccione **Aplicación de función** y haga clic en el nombre de la función que creó en el paso 1.

3. Seleccione **Funciones** en el menú de la izquierda y luego elija **HttpTrigger1** de la lista de funciones en la hoja **Funciones**.
4. En el lado izquierdo, elija **Código + Prueba**. Copie el código que se enumera a continuación y péguelo en la edición de PowerShell reemplazando el código que se muestra. Haga clic en **Guardar**.

Haga clic aquí para ver la imagen del código

```
usando el espacio de nombres System.Net

# Los enlaces de entrada se pasan a través del bloque
de parámetros.

param ($ Solicitud, $ TriggerMetadata)

# Escriba en el flujo de registro de Azure Functions.

Write-Host "La función de activación HTTP de PowerShell
procesó una solicitud".

$ resourceGroupName = "12almacenamiento"

$ storageAccountName = "az303fsdemosa"

$ containerName = "imágenes"

$ ctx = New-AzStorageContext ' 

-StorageAccountName $ storageAccountName ' 

-UseConnectedAccount

$ blob = Get-AzStorageBlobContent ' 

-Container $ containerName ' 

-Blob "almacenamiento-az303demo.txt" ' 

-Contexto $ ctx ' 

-Fuerza

$ cuerpo = $ blob.ICloudBlob.DownloadText ()
```

```

# Asociar valores a enlaces de salida llamando a 'Push-
OutputBinding'.

Push-OutputBinding -Name Response -Value
([HttpResponseContext] @ {

    StatusCode = [HttpStatusCode] :: Aceptar

    Cuerpo = $ cuerpo

})

```

En el fragmento de código anterior, verá que la sección central es casi idéntica a los cmdlets ejecutados para leer el blob con una entidad de seguridad de usuario. El contexto se recupera mediante `-UseConnectedAccount` y se pasa a `Get-StorageBlobContent`. El destino se ha eliminado para que la función de Azure almacene el archivo en `wwwroot`. – Se agrega `fuerza` para que el archivo se sobrescriba cada vez que se ejecuta la función. El texto del blob se extrae en `$ body` y se envía a la respuesta de la función. Tenga en cuenta que este ejemplo ha sido diseñado para su uso con un archivo de texto.

Haga clic en **Probar / Ejutar > Ejecutar** para ejecutar la función. Fallará con la siguiente salida al registro de funciones, como se muestra en la [Figura 1-23](#). En este ejemplo, la función no se ejecuta en una cuenta de Azure AD, lo que significa que `-UseConnectedAccount` no se puede autenticar y el contexto es nulo. Se debe asignar una identidad administrada a la función de Azure para la autenticación.



```

Connected!
2020-09-05T14:55:43.063 [Error] ERROR: Context cannot be null. Please log in using Connect-AzAccount.Exception
System.InvalidOperationExceptionTargetSite :Name      : CreateOAuthTokenDeclaringType :
Microsoft.WindowsAzure.Commands.Storage.Common.Cmdlet.NewAzureStorageContextMemberType   : MethodModule      :
Microsoft.Azure.PowerShell.Cmdlets.Storage.dllStackTrace :at
Microsoft.WindowsAzure.Commands.Storage.Common.Cmdlet.NewAzureStorageContext.CreateOAuthToken()at
Microsoft.WindowsAzure.Commands.Storage.Common.Cmdlet.NewAzureStorageContext.GetStorageAccountByOAuth(String storageAc
storageEndpoint)at Microsoft.WindowsAzure.Commands.Storage.Common.Cmdlet.NewAzureStorageContext.ExecuteCmdlet()at
Microsoft.WindowsAzure.Commands.Utilities.Common.CmdletExtensions.<>c`1.<ExecuteSyncNonnull>vOrAsinh>`1.B/T c)at

```

FIGURA 1-23 Error de ejecución de la función de contexto nulo

5. Para asignar una identidad, haga clic en el nombre de la función en la ruta de navegación en la parte superior de Azure Portal. Desplácese hacia abajo por el menú y haga clic en **Identidad**. Deje la pestaña en **Sistema asignado** y cambie

el **Estado** a **Activado**. Haga clic en **Guardar**. La función ahora tiene una identidad administrada por el sistema. Una identidad administrada por el sistema es una identidad que sigue el ciclo de vida del recurso al que está asignada; si se elimina el recurso, también se elimina la identidad. Cuando se crea una identidad administrada en una función de Azure, se crean dos variables de entorno: `MSI_ENDPOINT` y `MSI_SECRET`. Los desarrolladores pueden usarlos dentro del código para recuperar el token de OAuth para la identidad administrada. Luego, se pasa al recurso de Azure como parte de una solicitud para que se pueda autorizar la solicitud. En este ejemplo, `Get-NewAzContext` envuelve este proceso por usted, por lo que no tiene que estar codificado específicamente.

6. Haga clic en **Funciones** en el menú de la izquierda, seleccione **HttpTrigger1 > Código + Prueba** y luego ejecute la función nuevamente. El error ha cambiado a 403: error de autorización. La función ahora está recuperando el contexto de la identidad administrada, pero la identidad no tiene permiso para leer el blob.
7. La asignación de roles RBAC a una identidad administrada es casi idéntica a la de un usuario. Navegue hasta la cuenta de almacenamiento que está usando para este tutorial: `az303fsdemosa`. Haga clic en **Control de acceso (IAM)** en el menú de la izquierda y luego haga clic en **Agregar** en la parte superior. Haga clic en **Agregar asignación de funciones**. En **Rol**, seleccione **Lector de datos de Storage Blob**. En **Asignar acceso**, haga clic en **Aplicación de función**, que aparece en **Identidad administrada asignada por el sistema**. Aparecerá el nombre de la aplicación de función que ha estado usando para este tutorial. Haga clic en el nombre de la aplicación de función; la hoja de asignación de funciones se verá como se muestra en la [Figura 1-24](#). Haga clic en **Guardar**.

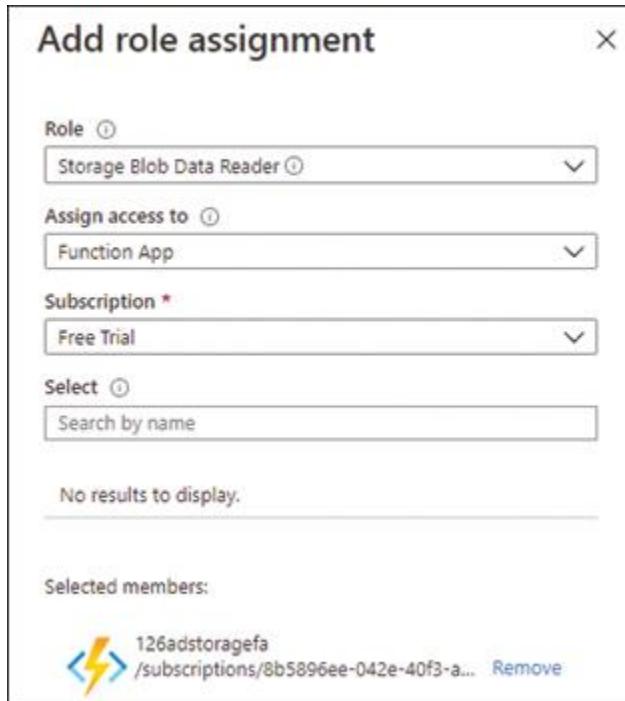


FIGURA 1-24 Asignación de acceso de lectura en un servicio BLOB a una identidad administrada por el sistema

8. Vuelva a la aplicación de función y utilice el mismo proceso que se describe en el paso 7 para ejecutar la aplicación de función nuevamente. El código se ejecutará ahora sin errores y el contenido del archivo se mostrará en la ventana de salida. Tenga en cuenta que seguirá recibiendo un error 403 si su aplicación de función no tiene acceso de red a la cuenta de almacenamiento.

Implementar la replicación de Azure Storage

Azure replica automáticamente sus datos de almacenamiento tres veces dentro del centro de datos en el que está almacenado, lo que protege contra fallas de hardware físico subyacentes. Hay más opciones de alta disponibilidad para Azure Storage, cada una con su propio caso de uso:

- ■ **Almacenamiento con redundancia local (LRS).** Azure realiza tres copias de la cuenta de almacenamiento y las distribuye a través de un único centro de datos en su región de origen. Aquí, tiene protección contra la falla de una matriz de almacenamiento.

- **Almacenamiento con redundancia de zona (ZRS).** Azure realiza tres copias de la cuenta de almacenamiento y las distribuye en varios centros de datos de su región de origen. Aquí, tiene protección contra fallas a nivel de centro de datos. Tenga en cuenta que solo las cuentas de almacenamiento de uso general V2 pueden usar la opción de replicación de ZRS.
- **Almacenamiento con redundancia geográfica (GRS).** Azure realiza tres copias de la cuenta de almacenamiento en la región de origen y tres copias en una segunda región emparejada. Las regiones emparejadas son geográficamente lo suficientemente cerca como para tener conectividad de alta velocidad para reducir o eliminar la latencia. Aquí, tiene protección contra fallas regionales.
- **Almacenamiento con redundancia de zona geográfica (GZRS).** Azure crea copias dentro de las zonas de disponibilidad de la región principal y luego replica los datos en la región secundaria. Este es el nivel de replicación recomendado por Microsoft que abarca los niveles más altos de durabilidad, disponibilidad y rendimiento.
- **Almacenamiento con redundancia geográfica con acceso de lectura (RA-GRS).** Es lo mismo que GRS con la excepción de que puede acceder a la cuenta de almacenamiento en la región secundaria; la ruta de la URL base es `https://<nombre-cuenta>-secondary.<servicio>.windows.net`.
- **Almacenamiento con redundancia de zona geográfica con acceso de lectura (RA-GZRS).** Es lo mismo que RA-GRS, pero Azure también copia datos en las zonas de disponibilidad de la región principal.

También debe considerar el costo; cuanto más se replican los datos, mayor es el SLA y mayor el costo.



Acuerdos de nivel de servicio de la cuenta de almacenamiento de punta de examen

Puede resultar beneficioso comprender los SLA para cada tipo de redundancia. Consulte <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy> para obtener más información .

El tipo de replicación se especifica cuando se crea la cuenta de almacenamiento. En la sección "Seleccionar opciones de cuenta de almacenamiento según un caso de uso" de este capítulo, creó una cuenta de almacenamiento con la CLI de Azure. Se omitió el parámetro `--sku`; el parámetro `sku` es donde se selecciona el tipo de replicación. El `sku` consta de dos partes: el nivel de rendimiento (Estándar o Premium) y el tipo de replicación (LRS, ZRS, GRS o RAGRS). Solo LRS y ZRS pueden tener un nivel de rendimiento superior. Ejecute el siguiente comando para crear una cuenta de almacenamiento con redundancia geográfica de acceso de lectura en la CLI de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
resourceGroupName = "12storage"

storageAccountName = "az303ragrs"

crear una cuenta de almacenamiento az \
    --name $ storageAccountName \
    --resource-group $ resourceGroupName \
    - kind StorageV2 \
    --sku Standard_RAGRS
```

El JSON devuelto por el cmdlet anterior contiene esta sección:

[Haga clic aquí para ver la imagen del código](#)

```
"secundariosEndpoints": {
    "blob": "https://az303ragrs-
secondary.blob.core.windows.net/",
    "dfs": "https://az303ragrs-
secondary.dfs.core.windows.net/",
```

Estos son URL (puntos finales) para la región secundaria.

¿Necesita más revisión? Redundancia de datos

Para obtener más información sobre la redundancia de datos para cuentas de almacenamiento, visite <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy> .

Implementar la conmutación por error de la cuenta de Azure Storage

Las cuentas de almacenamiento configuradas para la replicación geográfica pueden conmutarse manualmente a los puntos finales secundarios si hay una interrupción en el principal. También debe recomendar que sus clientes realicen conmutaciones por error de prueba como parte de sus planes de recuperación ante desastres. Para iniciar una conmutación por error, puede usar la línea de comandos o Azure Portal. Inicie sesión en Azure Portal y siga estos pasos. Utilizará la cuenta de almacenamiento con redundancia geográfica az303ragrs que creó en la sección anterior:

1. En la barra de recursos de búsqueda en la parte superior del portal, ingrese **la cuenta de almacenamiento** y luego elija **Cuenta de almacenamiento** en el menú desplegable que se muestra cuando comienza a escribir el nombre del recurso. En la lista de cuentas de almacenamiento, seleccione la cuenta de almacenamiento az303ragrs o la cuenta utilizada en la sección anterior ("Implementar la replicación de Azure Storage").
2. El menú se abre en la hoja **Descripción general**. Mire el campo **Estado** que dice: "Principal: disponible, secundario: disponible". El campo **Ubicación** mostrará la región emparejada seleccionada. El primario está en la primera ubicación; el secundario está en el segundo.
3. Desplácese hacia abajo en el menú y haga clic en **Replicación geográfica**. El mapa muestra la ubicación de sus puntos finales primarios y secundarios. Desplácese hasta la parte inferior del mapa y haga clic en **Prepararse para la conmutación por error**. La hoja de **conmutación por error** indica cuándo se sincronizaron por última vez el primario y el secundario y que perderá datos después de este punto. Además, tenga en cuenta el párrafo que establece que cuando el secundario se convierte en el primario, el nuevo primario se convertirá en almacenamiento con redundancia local (LRS). Debe actualizar la cuenta de

almacenamiento para volver al almacenamiento con redundancia geográfica después de la conmutación por error. Esto se puede realizar mediante Azure Portal, Azure CLI o PowerShell. Escriba **sí** en el cuadro **Confirmar conmutación por error** y haga clic en **Comutación por error**.

¿Necesita más revisión? Comutación por error de la cuenta de almacenamiento

Para obtener más información sobre la recuperación ante desastres y la conmutación por error para cuentas de almacenamiento, visite <https://docs.microsoft.com/en-us/azure/storage/common/storage-disaster-recovery-guidance>.

HABILIDAD 1.3: IMPLEMENTAR MÁQUINAS VIRTUALES PARA WINDOWS Y LINUX

Como arquitecto, puede parecer inusual que una habilidad para el examen implique implementar y configurar máquinas virtuales (VM). Sin embargo, las operaciones de elevación y cambio suelen ser el pan y la mantequilla de un arquitecto de nube en una gran empresa. Esta habilidad analizará las opciones de configuración para una máquina virtual y cómo diseñar para escala y disponibilidad.

Esta es una certificación de nivel experto, por lo que existe la expectativa de que su conjunto de habilidades ya incluya la creación de máquinas virtuales Linux y Windows en Azure Portal. También se espera que posea habilidades básicas de scripting en Bash y PowerShell.

Esta habilidad cubre cómo:

- ■ [Seleccionar el tamaño de la máquina virtual](#)
- ■ [Configurar el almacenamiento para máquinas virtuales](#)
- ■ [Configurar Azure Disk Encryption](#)
- ■ [Configurar alta disponibilidad](#)
- ■ [Implementar y configurar conjuntos de escalas](#)
- ■ [Implementar hosts dedicados de Azure](#)

Seleccione el tamaño de la máquina virtual

Es muy probable que se encuentre con muchos proyectos como arquitecto que impliquen la elevación y el traslado de máquinas virtuales (VM) locales a la nube. Una parte esencial de esta tarea es evaluar la carga de trabajo de cada máquina virtual local y dimensionar una máquina virtual adecuada en Azure. Hay muchos tamaños de máquina virtual disponibles en Azure y todos están optimizados para cargas de trabajo específicas. Debe tener una buena comprensión de estas optimizaciones y dónde aplicarlas. Consulte la [Tabla 1-1](#).

TABLA 1-1 Resumen de tamaños y tipos de máquinas virtuales

Tipo de VM	Tamaños	Descripción y uso
Propósito general	A, B, D	CPU equilibrada a la memoria. Aplicaciones de desarrollo y prueba, bases de datos de tamaño mediano y servidores de aplicaciones
Computación optimizada	F	Gran cantidad de CPU a memoria. Servidores de aplicaciones, dispositivos de red y lotes
Memoria optimizada	E, M, DSv2m Dv2	Gran cantidad de memoria a CPU. Servidores de datos y grandes procesos de almacenamiento caché / en memoria
Almacenamiento optimizado	L	Alto rendimiento del disco. Para big data y almacenes de datos
GPU	norte	Procesamiento de gráficos pesados y aprendizaje automático
Computación de alto rendimiento	H A8-11 (dejará de estar disponible el 3/2021)	Las CPU de mayor potencia disponibles. Los tamaños también pueden tener interfaz de acceso directo a memoria aleatoria (RDMA)

La tabla anterior proporciona una descripción general amplia de cómo las letras al comienzo del tamaño de una máquina virtual denotan el tipo de máquina virtual. Cada letra puede tener múltiples configuraciones de núcleos de CPU, tamaños de memoria y capacidades de almacenamiento.

Para ver las opciones en el portal, elija agregar un recurso de máquina virtual, desplácese hacia abajo hasta **Tamaño** y haga clic en **Cambiar tamaño**. Esto mostrará las opciones disponibles para usted. Las opciones de tamaño disponibles para usted cambian entre regiones y puede enumerar los tamaños de máquina virtual disponibles en cada ubicación mediante PowerShell o, en este ejemplo, con la CLI de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
az vm lista-tamaños - ubicación uksouth --tabla de salida
```

La salida del comando anterior enumera todos los tamaños de VM disponibles para la ubicación dada, `-location uksouth`. Puede usar operadores Bash o PowerShell para filtrar sus resultados. Por ejemplo, emita el siguiente comando en PowerShell para mostrar todas las máquinas virtuales disponibles en una región con ocho núcleos:

[Haga clic aquí para ver la imagen del código](#)

```
Get-AzVMSize -Location uksouth | Donde NumberOfCores -EQ '8'
```

Para crear una máquina virtual fuera del portal, debe especificar el tamaño como parte del comando de creación. La columna `Nombre` de la salida del comando anterior es el valor que debe pasarse al comando de creación:

[Haga clic aquí para ver la imagen del código](#)

```
az vm create --name vmLinSizeExample \
--resource-group $ resourceGroupName \
--imagen UbuntuLTS \
--tamaño Standard_B1s \
--generate-ssh-key
```

Si la carga de trabajo en una máquina virtual se altera o si tenía un tamaño incorrecto en el momento de la creación, deberá cambiar el tamaño de su máquina virtual. Puede cambiar el tamaño de una máquina virtual mientras aún está asignada, pero solo puede cambiar su tamaño a un tamaño disponible en el clúster en el que se creó. Para verificar los tamaños disponibles para usted, ejecute este comando:

[Haga clic aquí para ver la imagen del código](#)

```
az vm list-vm-resize-options --resource-group $  
resourceGroupName --name vmLinSizeExample  
  
--tabla de salida
```

Si el tamaño que necesita no aparece en `az vm list-vm-resize-options` pero sí en `az vm list-size`, debe desasignar la máquina virtual antes de cambiar el tamaño. Luego, Azure volverá a crear la máquina virtual en un nuevo clúster:

[Haga clic aquí para ver la imagen del código](#)

```
az vm resize --resource-group $ resourceGroupName --name  
vmLinSizeExample --size  
  
Standard_DS2_v2
```

¿Necesita más revisión? Dimensionamiento de la máquina virtual

Para conocer las opciones disponibles para el tamaño de la máquina virtual, visite el artículo de Microsoft Docs “Tamaños para máquinas virtuales Linux en Azure” en <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes>. Asegúrese de explorar la descripción de cada tipo. Esta página también incluye un enlace a más información sobre las máquinas virtuales de Windows.

Configurar el almacenamiento para máquinas virtuales

El almacenamiento de la máquina virtual puede administrarse o no administrarse, aunque se administra el modo recomendado. Con un disco

administrado, la cuenta de almacenamiento, los límites de almacenamiento subyacentes y el cifrado están a cargo de usted.

Hay cuatro tipos de disco disponibles en Azure y cada tipo de disco tiene límites diferentes y, por lo tanto, diferentes casos de uso específicos, como se muestra en la Tabla 1-2.

TABLA 1-2 Tipo de disco

Tipo de disco	Caso de uso	tamaño máximo	Rendimiento máximo
Ultra discos	IO intensivo Bases de datos de primer nivel y cargas de trabajo con muchas transacciones	65G	2000 MB / s
SSD premium	Aplicaciones de producción Cargas de trabajo de rendimiento	32G	900 MB / s
SSD estándar	Servidores de desarrollo y prueba Aplicaciones de uso ligero y servidores web	32G	750 MB / s
HDD estándar	No crítico y de respaldo	32G	500 MB / s

El costo de cada tipo de disco aumenta a medida que se mueve entre los diferentes tipos de disco, siendo los ultra discos los que tienen el costo más alto.

Originalmente, todas las máquinas virtuales de Azure se creaban con discos no administrados. Puede convertir los discos no administrados en administrados mediante Azure Portal o la línea de comandos. Primero, debe desasignar la máquina virtual y luego convertirla. Por ejemplo, el siguiente comando muestra cómo desasignar una máquina virtual en la CLI de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
az vm deallocate --resource-group $ resourceGroupName --name  
vmLinSizeExample  
  
az vm convert --resource-group $ resourceGroupName --name  
vmLinSizeExample  
  
az vm start --resource-group $ resourceGroupName --name  
vmLinSizeExample
```

¿Necesita más revisión? Discos administrados

Para obtener información sobre los discos administrados y los tipos de discos disponibles para IaaS en Azure, visite el artículo de Microsoft Docs "Introducción a los discos administrados de Azure" en <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/managed-disk-general>. Le recomendamos que revise todas las secciones de Conceptos de almacenamiento en disco y la sección SELECCIONAR UN TIPO DE DISCO PARA IAAS VMS.

Una máquina virtual usa discos en tres roles: discos de SO, discos temporales y discos de datos. Los discos del sistema operativo almacenan los archivos para el sistema operativo seleccionado cuando se creó la máquina virtual. Los discos del sistema operativo no pueden utilizar un disco ultra. Sin embargo, si está utilizando ultra discos para sus discos de datos, se recomienda que utilice SSD premium para su disco de sistema operativo. Los discos de SO también pueden utilizar un disco de SO efímero. Los datos de los discos de SO efímeros se almacenan en el almacenamiento de la máquina virtual local y no en Azure Storage. El almacenamiento local proporciona operaciones de lectura y escritura con una latencia mucho menor y acelera el proceso de creación de imágenes. Almacenar los datos localmente en el host significa que los discos efímeros no incurren en ningún costo; sin embargo, si falla una máquina virtual individual, es probable que se pierdan todos los datos del disco efímero. Los discos de SO efímeros son excelentes para aplicaciones sin estado, donde falla una máquina virtual no afectará a la aplicación porque el tráfico se pondrá en cola o se redirigirá. Se elige un disco de sistema operativo efímero en Azure Portal en la sección **Avanzado** de la pestaña **Discos** para crear una máquina virtual en Azure Portal o en la línea de comandos. Por ejemplo, en la CLI de Azure, use la marca --ephemeral-os-disk true :

Haga clic aquí para ver la imagen del código

```
az vm create \  
    --resource-group $ resourceGroupName \  
    --nombre vmEphemOSDisk \  
    --imagen UbuntuLTS \  
    --ephemeral-os-disk true \  
    --os-disk-caching ReadOnly \  
    --admin-username azureadmin \  
    --generate-ssh-keys
```

¿Necesita más revisión? Discos de SO efímeros

Para obtener más información sobre los discos de SO efímeros, visite el artículo de Microsoft Docs "Discos de SO efímeros para máquinas virtuales de Azure" en <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/ephemeral-os-disks>.

Los discos temporales contienen datos que se pueden perder durante un evento de mantenimiento o la desasignación de una máquina virtual. Por lo tanto, no coloque datos críticos en un disco temporal. Sin embargo, los datos persisten en un disco temporal después de un reinicio normal.

Los discos de datos contienen datos, páginas web o código de aplicación personalizado. Se pueden agregar varios discos de datos a una máquina virtual; la cantidad máxima depende del tamaño de la máquina virtual. Vio la columna MaxDataDiskCount al ejecutar el comando az vm list-size en la sección "Seleccionar un tamaño de máquina virtual", anteriormente en este capítulo. La cifra máxima de discos de datos también se incluyó en la vista de Azure Portal. Los discos de datos admiten todos los tipos de discos de Azure.

No es obligatorio crear discos de datos cuando crea una máquina virtual, a menos que haya elegido una imagen que requiera discos de datos. Puede agregar uno o más discos de datos una vez que se haya creado una máquina virtual. Para agregar un disco de datos, puede usar

Azure Portal y la línea de comandos. Por ejemplo, use este código para adjuntar un disco de datos en PowerShell:

[Haga clic aquí para ver la imagen del código](#)

```
$ diskConfig = New-AzDiskConfig -SkuName Premium_LRS -  
Location uksouth  
  
-CreateOption Vacío -DiskSizeGB 128  
  
$ disk1 = New-AzDisk -DiskName dataDisk1 -Disk $ diskConfig -  
ResourceGroupName  
  
resourceGroupName  
  
$ vm = Get-AzVM -Name vmName -ResourceGroupName  
resourceGroupName  
  
$ vm = Add-AzVMDataDisk -VM $ vm -Name dataDisk1 -  
CreateOption Attach  
  
-ManagedDiskId $ disk1.Id -Lun 1  
  
Update-AzVM -VM $ vm -ResourceGroupName resourceGroupName
```

Tenga en cuenta el parámetro `-CreateOption Empty` en la primera línea para `New-AzDiskConfig`. Este parámetro crea un nuevo disco vacío para adjuntarlo a su VM. Los discos vacíos deben inicializarse una vez conectados mediante la administración de discos en Windows o los comandos de partición y montaje en Linux. Se pueden usar extensiones de script personalizadas para automatizar esta tarea a escala.

El parámetro `-CreateOption` también toma `Upload` como entrada. La opción `Cargar` se usa para crear una configuración de disco en Azure Storage y luego cargar un VHD directamente en él. Las cargas pueden ser para discos locales o para copiar discos entre regiones. Tenga en cuenta que los archivos VHDX deben convertirse primero a VHD. El valor final de `-CreateOption` es `FromImage`. Usted crea su máquina virtual personalizada, la prepara para la generalización con sysprep y luego usa la imagen resultante para crear una o más máquinas virtuales de Azure.

¿Necesita más revisión? Agregar discos

Para obtener más información sobre cómo agregar discos, visite el artículo de Microsoft Docs "Agregar un disco a una máquina virtual Linux" en <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/add-disk>. Además, le recomendamos que revise todas las páginas de la sección Administrar almacenamiento de las guías prácticas en la documentación de la máquina virtual.

Configurar el cifrado de disco de Azure

Azure protege a los clientes del improbable caso de que un atacante obtenga acceso a los medios físicos cifrando los datos en reposo. De forma predeterminada, los discos se cifran en reposo con cifrado del lado del servidor (SSE) mediante claves administradas por Microsoft. La naturaleza automática y transparente del cifrado del disco significa que no se requieren cambios en el código de la aplicación para utilizarlo. El cifrado por SSE es compatible con FIPS 140-2; sin embargo, para algunos casos de uso, es posible que esto no se ajuste a sus requisitos normativos y de cumplimiento. Si se copia un VHD de la cuenta de almacenamiento en la que se encuentra, se descifrará. La posibilidad de descifrado fuera del límite de almacenamiento es la razón por la que Azure Security Center marcará las máquinas virtuales que no tienen Azure Disk Encryption (ADE) habilitado.

ADE se realiza en el nivel del sistema operativo de la VM, lo que agrega una capa adicional de seguridad para la VM. Las funciones BitLocker (Windows) y DM-Crypt (Linux) de un sistema operativo proporcionan cifrado de volumen del sistema operativo y los discos de datos. Debido a que esta es una característica del sistema operativo, no todas las versiones del sistema operativo son compatibles. Azure Disk Encryption usa una clave de cifrado de datos (DEK) para cifrar los datos; luego tiene la opción de usar una clave de cifrado de clave (KEK) para cifrar la DEK para mayor seguridad. Cifrar la DEK con una KEK se conoce como "cifrado de sobre". La DEK y la KEK deben almacenarse en Azure Key Vault, lo que significa que el sistema operativo debe tener acceso al key vault.

Azure Disk Encryption se realiza en máquinas virtuales que ya se han creado. El cifrado solo se puede realizar desde la línea de comandos. Siga los pasos a continuación para cifrar los discos en una máquina virtual de Windows existente \$ vmName mediante la CLI de Azure:

1. Realice una instantánea de los discos VM que se van a cifrar; Esto se hace con fines de restauración en caso de que se produzca un error durante el cifrado. También puede ejecutar este comando para verificar que Azure Disk Encryption no esté habilitado en la máquina virtual:

Haga clic aquí para ver la imagen del código

```
resourceGroupName = "az303chap1_3-rg"  
  
ubicación = "uksouth"  
  
vmName = "ade-vm"  
  
vaultName = "ade-vk"  
  
  
keyName = "ade-kek"  
  
  
  
az vm encryption show --resource-group $  
resourceGroupName --name $ vmName  
  
Azure Disk Encryption no está habilitado
```

2. Cree una bóveda de claves con el siguiente comando. Este almacén de claves debe estar en la misma región que las máquinas virtuales que desea cifrar. Tenga en cuenta el parámetro `-enabled-for-encryption`, que habilita el almacén de claves para el cifrado de disco; sin esto, el cifrado del paso 3 fallará.

Haga clic aquí para ver la imagen del código

```
habilitación de cifrado az vm --resource-group $  
resourceGroupName --name $ vmName  
  
--disk-encryption-keyvault $ vaultName
```

3. Cifre la máquina virtual con este comando, que crea la DEK por usted en el conjunto de almacén de claves especificado: `-disk-encryption-keyvault $ vaultName`. Tenga en cuenta el parámetro `ALL` de tipo de volumen. `ALL` instruye al proceso de cifrado para cifrar todos los discos de datos y sistemas

operativos. También puede reemplazar TODOS con SO o DATA para cifrar solo esos tipos.

Haga clic aquí para ver la imagen del código

```
habilitación de cifrado az vm --resource-group $  
resourceGroupName --name $ vmName  
  
--disk-encryption-keyvault $ vaultName --tipo de  
volumen TODOS
```

4. Verifique el estado del cifrado del disco en la máquina virtual una vez más. Si se desplaza por la salida JSON del siguiente comando, puede ver el estado de cifrado de cada disco como EncryptionState / encrypted como se muestra en la Figura 1-25.

Haga clic aquí para ver la imagen del código

```
az vm encryption show --resource-group $  
resourceGroupName --name $ vmName
```

```
az303@Ubuntu: az vm encryption show --resource-group $resourceGroupName --name $vmName  
{  
  "disks": [  
    {  
      "encryptionSettings": [  
        {  
          "diskEncryptionKey": {  
            "secretUrl": "https://ade-vk.vault.azure.net/secrets/00F924D9-92A1-4267-BEE6-5610AE86DBDD/d2ab64ad775c4dc6a6  
80e03d500ad1a9",  
            "sourceVault": {  
              "id": "/subscriptions/8b5896ee-042e-40f3-a274-e7bbec8133d7/resourceGroups/az303chap1_3-rg/providers/Micros  
oft.KeyVault/vaults/ade-vk"  
            }  
          },  
          "enabled": true,  
          "keyEncryptionKey": null  
        }  
      ],  
      "name": "ade-vm_disk1_823ef6ea0e004cc9853503c8867339a7",  
      "statuses": [  
        {  
          "code": "EncryptionState/encrypted",  
          "displayStatus": "Encryption is enabled on disk",  
          "level": "Info",  
          "message": null,  
          "time": null  
        }  
      ]  
    ]  
},  
  "status": "Success",  
  "statusMessage": "The command completed successfully."}
```



FIGURA 1-25 Verifique que los discos estén cifrados en la CLI de Azure

- Para verificar que el disco del sistema operativo está encriptado desde dentro de la VM, RDP en la VM y abra el Explorador de Windows. Haga clic en **Esta PC** en el panel de navegación izquierdo. Los candados de la unidad C: y D: verifican que estén protegidos por BitLocker, como se muestra en la [Figura 1-26](#).



FIGURA 1-26 Verifique que los discos estén protegidos por BitLocker en el Explorador de Windows

Los primeros tres pasos anteriores son los mínimos necesarios para cifrar una máquina virtual con Azure Disk Encryption. Para explorar más el proceso de cifrado en el paso 3, puede mostrar todos los secretos que ahora están almacenados en el almacén de claves \$ vaultName mediante el siguiente comando en la CLI de Azure; la salida se muestra en la [Figura 1-27](#):

[Haga clic aquí para ver la imagen del código](#)

```
az keyvault secret list - nombre de la bóveda $ vaultName
```

```
az303@Ubuntu: az keyvault secret list --vault-name $vaultName
[
  {
    "attributes": {
      "created": "2020-09-05T16:04:08+00:00",
      "enabled": true,
      "expires": null,
      "notBefore": null,
      "recoveryLevel": "Recoverable+Purgeable",
      "updated": "2020-09-05T16:04:08+00:00"
    },
    "contentType": "BEK",
    "id": "https://ade-vk.vault.azure.net/secrets/0DF924D9-92A1-4267-BEE6-5610AE86DBDD",
    "managed": null,
    "name": "0DF924D9-92A1-4267-BEE6-5610AE86DBDD",
    "tags": {
      "DiskEncryptionKeyFileName": "0DF924D9-92A1-4267-BEE6-5610AE86DBDD.BEK",
      "MachineName": "ade-vm",
      "VolumeLabel": "Windows",
      "VolumeLetter": "C:\\"
    }
  }
]
az303@Ubuntu:
```

FIGURA 1-27 Secreto de Azure Key Vault después del cifrado de disco

Si observa la mitad de la salida en la [Figura 1-27](#), puede ver la línea "contentType": "" BEK ". BEK significa clave de cifrado de BitLocker. BEK es la clave de cifrado de datos (DEK), como se describe en Al comienzo de esta sección. Cuando se emitió el comando de cifrado, Azure creó el BEK automáticamente y almacenó la clave en el almacén de claves. Si existiera más de un volumen para la VM, se habría creado un BEK para cada uno.

Si debe utilizar sus propias claves de cifrado con fines reglamentarios, deberá cifrar el BEK generado con una clave de cifrado de claves (KEK). Para cifrar con su propia KEK, debe importar su clave en el almacén de claves y luego volver a emitir el comando de cifrado, como se muestra en este comando de la CLI de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
az keyvault key import --name $ keyName --vault-name $  
vaultName --pem-file ./keys/ade-  
  
kek.pem --pem-contraseña $ contraseña  
  
az vm encryption enable --resource-group $ resourceGroupName  
--name $ vmName --disk-  
  
encryption-keyvault $ vaultName --volume-type ALL --key-  
encryption-key $ keyName
```

Vuelva a ejecutar el comando de la [Figura 1-25](#) anterior para verificar el estado de cifrado nuevamente:

[Haga clic aquí para ver la imagen del código](#)

```
az vm encryption show --resource-group $ resourceGroupName --  
name $ vmName
```

Tenga en cuenta la adición de la sección `keyEncryptionKey`, que detalla dónde se almacena la KEK.

¿Necesita más revisión? Cifrado de disco de Azure

Para obtener más información sobre cómo configurar Azure Disk Encryption, visite el artículo de Microsoft Docs "Azure Disk Encryption para máquinas virtuales"

en <https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms -vmss> .

Configurar alta disponibilidad

Hasta ahora, en esta habilidad, ha estado explorando configuraciones en una sola máquina virtual. Una sola máquina virtual en Azure tiene un SLA del 99,9 por ciento, pero solo cuando se usan discos SSD Premium o ultra para todos los discos de datos y SO. Si no se utilizan SSD Premium, la VM no tiene SLA. Un SLA es un acuerdo de nivel de servicio, que es la cantidad mínima de tiempo que Microsoft garantiza que un servicio estará disponible.

Un SLA del 99,9 por ciento garantiza que el tiempo de inactividad en una sola máquina virtual no superará los 43 minutos al mes. Puede que esto no parezca mucho tiempo, pero ¿y si fuera durante la hora pico de operaciones del mes de un cliente? El uso de máquinas virtuales individuales para una aplicación presenta un único punto de falla. Hay tres situaciones en las que una máquina virtual de Azure podría verse afectada:

- ■ **Mantenimiento planificado.** Las máquinas virtuales deben actualizarse para garantizar la confiabilidad, el rendimiento y la seguridad. Cuando las actualizaciones requieren el reinicio de una máquina virtual, se lo contacta para que elija una ventana de mantenimiento a través del mantenimiento planificado de Azure.
- ■ **Mantenimiento de hardware no planificado.** Azure predice que el hardware subyacente está a punto de fallar y migra en vivo las máquinas virtuales afectadas al hardware en buen estado. Una migración en vivo detiene la máquina virtual para mantener las conexiones de red, la memoria y el acceso a los archivos, pero es probable que el rendimiento se reduzca en algún momento de la migración.
- ■ **Tiempo de inactividad inesperado.** Esto ocurre cuando el hardware o la infraestructura física fallan sin previo aviso. Puede ser una falla de red, disco u otra falla a nivel de rack. Cuando Azure detecta un tiempo de inactividad inesperado, Azure migra la máquina virtual y la reinicia para repararla; el reinicio provoca tiempo de inactividad. El tiempo de inactividad también se

producirá en el caso poco probable de que se produzca una interrupción completa del centro de datos.

Como arquitecto, debe diseñar para eliminar puntos únicos de falla, lo que se puede lograr mediante la arquitectura de soluciones de alta disponibilidad (HA). Para diseñar una solución basada en VM de alta disponibilidad en Azure, debe comprender las zonas de disponibilidad y los conjuntos de disponibilidad.

Conjuntos de disponibilidad

Los conjuntos de disponibilidad en Azure se utilizan para mitigar los efectos de una falla de hardware en el nivel de rack y el mantenimiento programado en las máquinas virtuales. Cuando coloca sus máquinas virtuales en un conjunto de disponibilidad, Azure distribuye la carga de trabajo en varios dominios de actualización y dominios de error. Un dominio de actualización es un grupo lógico de hardware subyacente que puede reiniciarse o someterse a mantenimiento al mismo tiempo. Cuando se implementan los parches, solo un dominio de actualización se verá afectado a la vez. Un dominio de error es una sección física del centro de datos; cada sección tiene su propia infraestructura de red, energía y refrigeración. Si se produce una falla de hardware en un dominio de falla, solo algunas de las VM de su conjunto de disponibilidad se verán afectadas. Los conceptos lógicos y físicos de cómo los dominios de falla y actualización permiten la alta disponibilidad se muestran en la [Figura 1-28](#).

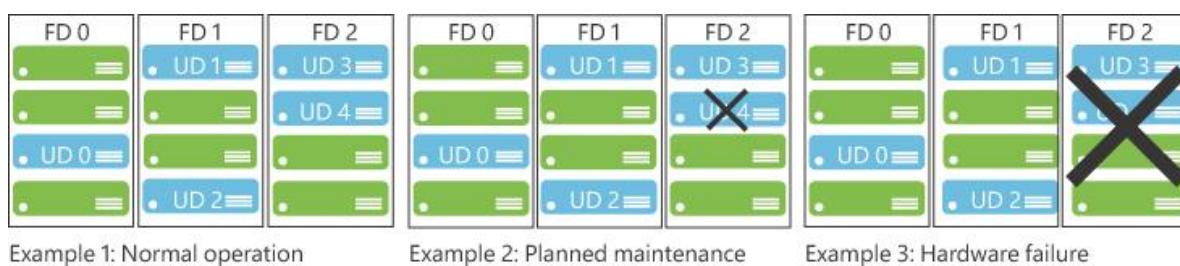


FIGURA 1-28 Actualización del conjunto de disponibilidad y ejemplos de dominio de fallas

Cada uno de los tres ejemplos de la [figura 1-28](#) representa un centro de datos de Azure distribuido en dominios de actualización (UD) y entre dominios de error (FD) para un conjunto de disponibilidad. En el Ejemplo 1, la operación es normal y las VM se distribuyen en el valor

predeterminado de tres dominios de falla y cinco dominios de actualización. Puede tener un máximo de tres dominios de error, aunque los dominios de actualización se pueden aumentar a 20. Cuando el número de máquinas virtuales en el conjunto supera las cinco, Azure aumentará secuencialmente las máquinas virtuales en cada dominio de actualización en una. UD 0 aumentará a dos VM, UD 1 aumentará a dos VM, y así sucesivamente. Para estos ejemplos, suponga que hay una máquina virtual en cada uno de los cinco dominios de actualización.

El ejemplo 2 de la [Figura 1-28](#) representa un evento de mantenimiento planificado. Azure inicia el proceso de parcheo al parchear y reiniciar UD 4. Azure repite el proceso de parche y reinicio en cada dominio de actualización a su vez. Si tiene cinco máquinas virtuales en su conjunto de disponibilidad, hay cuatro máquinas virtuales disponibles en cada punto del proceso de parcheo.

El ejemplo 3 de la [Figura 1-28](#) representa una falla de hardware en FD 2. Los dominios de actualización UD 3 y UD 4 se desactivan, pero UD 0, UD 1 y UD 2 están disponibles, que son tres VM. Si se produce un evento de mantenimiento planificado mientras las VM en UD 3 y UD 4 se mueven y reparan, hay dos VM disponibles.

El uso de conjuntos de disponibilidad garantiza que al menos una máquina virtual estará disponible durante un evento de mantenimiento planificado o no planificado. Esto aumenta el SLA para las máquinas virtuales dentro de una disponibilidad establecida en 99,95 por ciento o aproximadamente 22 minutos de tiempo de inactividad al mes. Para configurar un conjunto de disponibilidad para máquinas virtuales, comience por crear el conjunto de disponibilidad. En el portal, escriba el **conjunto de disponibilidad** en la barra de recursos de búsqueda en la parte superior del portal, elija **Conjuntos de disponibilidad** cuando se muestre el menú desplegable mientras escribe el nombre del recurso. Una vez que se cargue la pantalla **Conjuntos de disponibilidad**, haga clic en **Agregar**. [La Figura 1-29](#) muestra un ejemplo de una página de **creación de conjunto de disponibilidad** completada .

Create availability set

Basics Advanced Tags Review + create

An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions. [Learn more about availability sets.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Free Trial

Resource group * ⓘ

az303chap1_3-rg

Create new

Instance details

Name * ⓘ

az303chap1-as

Region * ⓘ

(Europe) UK South

Fault domains ⓘ

2

ⓘ The maximum platform fault domain count in the selected subscription and location is 2.

Update domains ⓘ

5

Use managed disks ⓘ

No (Classic) Yes (Aligned)

Review + create

< Previous

Next : Advanced >

FIGURA 1-29 Página de creación de un conjunto de disponibilidad completo

Para que una máquina virtual se agregue a un conjunto de disponibilidad, debe existir en la misma región que el conjunto de disponibilidad. Mirando a la figura 1-29 también se puede ver la lectura de advertencia: El dominio máxima de la plataforma de fallos contar en el Seleccionado suscripción y la ubicación es 2 . Esto se debe a que la región, Reino Unido Sur, solo proporciona dos

dominios de error. Cambiar esto a otra región, como Europa Occidental, permitiría tres dominios. Puede consultar el recuento máximo de dominios de fallas para una región desde la línea de comandos. Si configura la opción **Usar discos administrados** en **Sí (alineado)**, los discos de VM se distribuirán entre dominios de fallas de almacenamiento, evitando puntos únicos de falla para los discos de su VM. Si no utiliza discos administrados, deberá crear manualmente una cuenta de almacenamiento para cada máquina virtual en un conjunto de disponibilidad.

Una vez que se crea el conjunto de disponibilidad, puede asignar VM en el portal o en la línea de comando; por ejemplo, en la CLI de Azure, especifica el parámetro `--availability-set`, como se muestra a continuación:

[Haga clic aquí para ver la imagen del código](#)

```
az vm create \  
    --resource-group $ resourceGroup \  
    --nombre $ vmNamei \  
    --disponibilidad-set az303chap1-ag \  
    --tamaño Standard_DS1_v2 \  
    --nombre-vnet $ nombreVnet \  
    --subnet $ subnetName \  
    --imagen UbuntuLTS \  
    --admin-username azureuser \  
    --generate-ssh-keys
```

Solo puede agregar una máquina virtual a un conjunto de disponibilidad en el momento de la creación de la máquina virtual. Si necesita asignar una máquina virtual a un conjunto de disponibilidad después de la creación, la máquina virtual se debe eliminar y volver a crear. Una vez que se crea el conjunto de disponibilidad y se implementan las VM, agrega un equilibrador de carga para distribuir el tráfico entre las VM disponibles.

Si la solución que está creando es para una aplicación de varios niveles, debe crear un conjunto de disponibilidad para cada nivel al diseñar la arquitectura para una alta disponibilidad.

Zonas de disponibilidad

Una zona de disponibilidad se compone de uno o más centros de datos, y cada zona tiene su propia red, alimentación y refrigeración. Las zonas están separadas físicamente, por lo que el uso de zonas de disponibilidad lo protegerá de las fallas del centro de datos. Cada zona de disponibilidad tiene un dominio de falla y actualización, y estos funcionan de la misma manera que se describe para los conjuntos de disponibilidad. Tenga en cuenta que no puede combinar conjuntos de disponibilidad y zonas de disponibilidad. Las zonas de disponibilidad no están disponibles en todas las regiones y no todas las SKU de VM están disponibles en una zona de disponibilidad. Puede comprobar lo que está disponible en la línea de comandos. Por ejemplo, en la CLI de Azure, ejecutaría este comando:

[Haga clic aquí para ver la imagen del código](#)

```
az vm list-skus -l uksouth --zone --output tsv
```

El parámetro `--zone` en `az vm list-skus` enumerará las máquinas virtuales que están disponibles para su uso en una zona de disponibilidad. Si cambió la ubicación anterior a `uknorth`, no se incluirán SKU. En el momento de escribir este artículo, `uknorth` no tiene zonas de disponibilidad. Para agregar una máquina virtual a una zona de disponibilidad, especifique la zona como parte de la configuración de la máquina virtual; por ejemplo, puede ejecutar este comando en PowerShell con el parámetro `-Zone`:

[Haga clic aquí para ver la imagen del código](#)

```
New-AzVMConfig -VMName $ vmName -VMSize Standard_DS1_v2 -Zone 2
```

Para lograr un SLA del 99,99 por ciento para una zona de disponibilidad, también debe asegurarse de que la conectividad de red y el almacenamiento para la máquina virtual estén dentro de la misma zona. Si el proceso de agregar VM está creando discos administrados y

el parámetro `-Zone` está configurado, el almacenamiento se colocará automáticamente en la zona correcta.

Si su solución requiere alta disponibilidad en todas las regiones, las zonas de disponibilidad no serán adecuadas. Deberá diseñar una solución multirregional con el tráfico equilibrado en todas las regiones. En la [Figura 1-30](#) se muestra un ejemplo de arquitectura multirregional .

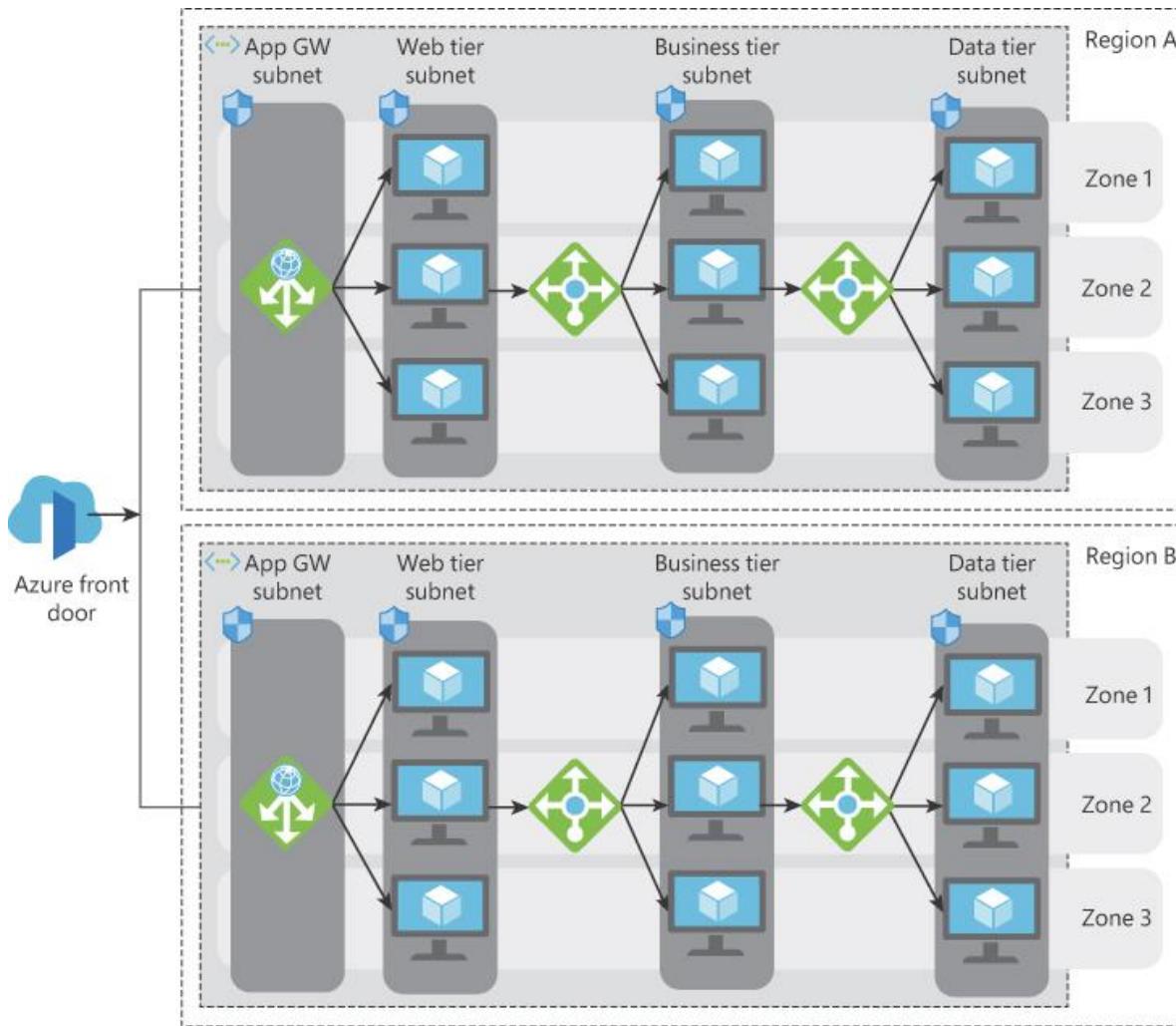


FIGURA 1-30 Alta disponibilidad multirregional para IaaS con una interfaz web



Sugerencia de examen SLA de máquina virtual de Azure
Conozca bien los porcentajes de SLA para una máquina virtual de instancia única, las máquinas virtuales en un conjunto de

disponibilidad y las máquinas virtuales en las zonas de disponibilidad.

¿Necesita más revisión? Alta disponibilidad para máquinas virtuales

Para conocer las configuraciones de disponibilidad disponibles para las máquinas virtuales, visite el artículo de Microsoft Docs "Administrar la disponibilidad de las máquinas virtuales de Windows en Azure" en <https://docs.microsoft.com/en-gb/azure/virtual-machines/windows/administrar-la-disponibilidad>.

Implementar y configurar conjuntos de escalas

Un problema histórico con la configuración del centro de datos local es tener que comprar hardware con anticipación para hacer frente a la carga prevista en el futuro. Un conjunto de escalado de máquinas virtuales (VMSS) en Azure le permite implementar un conjunto de máquinas virtuales idénticas y con equilibrio de carga. Estas máquinas virtuales se pueden escalar vertical u horizontalmente para satisfacer la demanda. El equilibrador de carga distribuye la carga de trabajo entrante entre las VM del conjunto de escalado. Si la sonda de estado del balanceador de carga detecta que una VM no responde, el balanceador de carga deja de enviar tráfico a esa VM. Un conjunto de básculas puede aportar un nivel de redundancia y la distribución de la carga puede ayudar con el rendimiento de la aplicación. Para agregar un conjunto de escalado de máquina virtual, puede usar Azure Portal o la línea de comandos. Por ejemplo, para agregar un conjunto de escalas en la CLI de Azure, ejecute los siguientes comandos:

[Haga clic aquí para ver la imagen del código](#)

```
az vmss create \
    --resource-group $ resourceName \
    --nombre myScaleSet \
    --imagen UbuntuLTS \
    --upgrade-policy-mode automático \
    --admin-username $ adminUser \
```

```
--generate-ssh-keys
```

El comando `az vmss create` anterior agrega un conjunto de escalado de VM para VM basadas en Ubuntu. Tenga en cuenta que puede usar el parámetro `--zones` para colocar un conjunto de básculas en una zona o zonas para aumentar la disponibilidad. También puede utilizar imágenes personalizadas en un conjunto de escalas; estas deben ser máquinas virtuales que se desasignan y generalizan primero.

Una vez que haya agregado un conjunto de escalas, puede usar Azure Portal para explorar la configuración del conjunto de escalas. En la parte superior del portal, ingrese el **conjunto de escalas** en la barra de búsqueda de recursos y presione Entrar. Seleccione su conjunto de escalas, haga clic en **Instancias** en la hoja del menú y observe que se han creado dos instancias. Una instancia es una máquina virtual en un conjunto de escalas. De forma predeterminada, el comando `az vmss create` tiene dos máquinas virtuales y un equilibrador de carga. También puede especificar un balanceador de carga existente o una puerta de enlace de aplicaciones al crear un conjunto de escalado. En este ejemplo, el equilibrador de carga se crea automáticamente sin reglas de enrutamiento, por lo que debe agregarlas. Por ejemplo, en la CLI de Azure, este comando enrutaría el tráfico HTTP a las máquinas virtuales:

[Haga clic aquí para ver la imagen del código](#)

```
creación de regla lb de red az \
--resource-group $ resourceName \
--nombre myLoadBalancerRuleWeb \
--lb-name myScaleSetLB \
--backend-pool-name myScaleSetLBEPool \
--puerto de backend 80 \
--frontend-ip-name loadBalancerFrontEnd \
--frontend-port 80 \
--protocolo tcp
```

También debe agregar una sonda de estado al balanceador de carga si necesita verificar la disponibilidad de las VM subyacentes.

Vuelva a Azure Portal y abra la hoja **Instancias**. Seleccione una instancia y observe la hoja **Descripción general**. Las máquinas virtuales de un conjunto de escalado no tienen una dirección IP pública. Si se requiere mantenimiento para una instancia, se debe configurar un Jumpbox para RDP o SSH en la instancia. Vuelva a la hoja de conjunto de escalas y haga clic en **Escala**. La configuración predeterminada para el escalado es **Manual**, pero en Azure Portal, puede arrastrar el control deslizante hacia arriba o hacia abajo para escalar el número de instancias hacia adentro o hacia afuera. Para realizar el escalado en la línea de comandos, como en la CLI de Azure, ejecute `az vmss scale` y especifique el parámetro `--new-capacity`, como se muestra aquí:

[Haga clic aquí para ver la imagen del código](#)

```
az vmss scale --name myScaleSet --new-capacity 3 --resource-group $ resourceGroupName
```

El autoescalamiento es el verdadero poder en los conjuntos de escalas. Vuelva a Azure Portal y haga clic en **Escala automática personalizada** en la hoja **Escalado**. Se muestra la condición de escala predeterminada; desplácese hasta la parte inferior y haga clic en **Agregar una condición de escala**. Se pueden agregar múltiples condiciones. [La Figura 1-31](#) muestra ejemplos de condiciones de escala para cargas predecibles e impredecibles.

The figure consists of two side-by-side screenshots of the Azure portal's scaling rules configuration interface.

Screenshot 1: Predicted load

This screenshot shows a scaling rule for "Predicted - Every Friday at 9AM scale to 3". The "Scale mode" is set to "Scale based on a metric". The "Instance count" is set to 3. The "Schedule" section shows "Repeat every Friday". The "Start time" is set to 09:00 and the "End time" is set to 11:00. A circled number "1" is overlaid on this screenshot.

Screenshot 2: Unpredictable load

This screenshot shows a scaling rule for "Unpredictable - Scale based on CPU above 70 percent". It includes two "Scale out" rules: one for "When average Percentage CPU > 70" (scale by 1) and another for "When average Percentage CPU < 40" (scale by 1). The "Instance limits" section shows a maximum of 2 instances. The "Schedule" section shows "Specify start/end dates" with a start date of 09/09/2020 and an end date of 09/09/2021. A circled number "2" is overlaid on this screenshot.

1. Predicted load
2. Unpredictable load

FIGURA 1-31 Condiciones de escala de carga previstas e impredecibles

El ejemplo de condición de escala de carga predecible en la [Figura 1-31](#) se muestra a la izquierda. El **Modo de escala** se establece en **la Escala Para un recuento de instancia específica** y el **número de instancias** puede escalar a cabo un recuento de instancia específica de 3 . El **programa** se establece en **Repetir días específicos** y **Repetir cada** se establece en **viernes** . Por último, la **hora de inicio** y la **hora de finalización** son las **09:00** y las **11:00** , respectivamente.

La condición de escala de carga impredecible en la [Figura 1-31](#) aparece a la derecha. El **Modo de escala** se establece en **Escalar según una métrica** . La primera regla de métrica se establece en **Aumentar el recuento en 1** y los **créditos de CPU (promedio) consumidos > 70** (la carga de CPU promedio en todas las instancias es superior al 70 por ciento durante al menos 10 minutos). La segunda regla de métrica está configurada para **Disminuir el recuento en 1** y el **porcentaje (promedio) de CPU <40** (la carga promedio de CPU en todas las instancias es menos del 40 por ciento durante 10 minutos). **Los límites de instancias** garantizan que la condición de escala no supere las 5 instancias.

El escalado hacia adentro y hacia afuera no se limita a las métricas de instancias de VM; haga clic en **Agregar una regla** en una condición de conjunto de escalas y vea que las colas de **Storage** y **Service Bus** están disponibles en **Metric Source** . Por lo tanto, si las colas de su VMSS son grandes, puede escalar horizontalmente para reducir la cola.

Mientras aún está en el panel **Regla de escala** , desplácese hacia abajo hasta **Acciones** . Aquí es donde puede aumentar o disminuir sus instancias.

¿Necesita más revisión? Conjuntos de escalas de máquinas virtuales

Para obtener más información sobre los conjuntos de escalado de máquinas virtuales, visite el artículo de Microsoft Docs "Documentación de conjuntos de escalado de máquinas virtuales" en <https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/> .

Implementar hosts dedicados de Azure

Las máquinas virtuales que ha examinado hasta ahora en esta habilidad se han estado ejecutando en una infraestructura física compartida

subyacente. Tiene poco control sobre dónde se ha colocado su VM, más allá de especificar una región o zona de disponibilidad. No tiene control sobre las cargas de trabajo con las que comparte la infraestructura. En muchos casos de uso, esto no es un problema, aunque algunos requisitos regulatorios y de cumplimiento deben tener una infraestructura física aislada. Los hosts dedicados de Azure abordan estos requisitos al proporcionar las siguientes características:

- ■ **Servidores físicos de un solo inquilino.** Solo las máquinas virtuales que elija se colocan en sus hosts. Esto se logra mediante el aislamiento de hardware a nivel de servidor físico.
- ■ **Control de eventos de mantenimiento.** Esto le permite elegir las ventanas de mantenimiento para su (s) host (s).
- ■ **Beneficio híbrido de Azure.** Puede traer sus propias licencias de Windows Server y SQL para reducir costos.

Los hosts dedicados de Azure se agrupan dentro de un grupo de hosts. Al crear un grupo de hosts, puede especificar cuántos dominios de error utilizar. Si especifica más de un dominio de fallas, elige en qué dominio de fallas se agrega un host. Las máquinas virtuales recogen automáticamente este dominio de error del host. Esta característica es la razón por la que los conjuntos de disponibilidad no son compatibles con los hosts dedicados de Azure. En un grupo de hosts, tiene la opción de especificar una zona de disponibilidad. Debe crear varios grupos de hosts en las zonas de disponibilidad si necesita una alta disponibilidad en todas las zonas. Un host requiere la elección de una familia del tamaño de SKU de la serie VM y las generaciones de hardware admitidas en la región de su grupo de host.

Cuando se agrega una máquina virtual a un host dedicado de Azure, debe coincidir con la región del host y la familia de tamaños. Se pueden agregar máquinas virtuales existentes, aunque deben cumplir los mismos requisitos y, en primer lugar, deben detenerse o desasignarse.

¿Necesita más revisión? Hosts dedicados de Azure

Para obtener información sobre la implementación de hosts dedicados de Azure en el portal, visite el artículo de Microsoft Docs "Implementar máquinas virtuales en hosts dedicados mediante el portal" en <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/dedicated-hosts-portal>.

HABILIDAD 1.4: AUTOMATIZAR LA IMPLEMENTACIÓN Y CONFIGURACIÓN DE RECURSOS

La velocidad de los negocios se ha vuelto mucho más rápida y las organizaciones están implementando cambios y soluciones en la nube utilizando metodologías ágiles. Como arquitecto, debe comprender cómo automatizar la implementación de sus soluciones, asegurando que la infraestructura subyacente sea confiable desde la primera hasta la enésima vez que se implementa. Estas implementaciones aprovechan la infraestructura como código (IaC). En Azure, IaC se realiza mediante una plantilla de Azure Resource Manager (ARM), que es una estructura basada en JSON (Javascript Object Notation) en la que declaras cuál será el estado final de tus recursos en JSON.

Una vez que se ha implementado una solución, es posible que requiera alguna configuración. Esto también se puede programar y se conoce como "Configuración como código". La configuración como código ayuda a la deriva de la configuración, donde la configuración de un servidor se altera con el tiempo debido a intervenciones manuales. En esta sección, explorará el uso de plantillas ARM para la implementación y la configuración y el uso de un runbook de automatización de Azure para la configuración del estado.

Esta habilidad cubre cómo:

- ■ [Guardar una implementación como una plantilla de Azure Resource Manager](#)
- ■ [Modificar la plantilla de Azure Resource Manager](#)
- ■ [Evaluar la ubicación de nuevos recursos](#)
- ■ [Implementar desde una plantilla](#)
- ■ [Configurar una plantilla de disco virtual](#)
- ■ [Administrar una biblioteca de plantillas](#)
- ■ [Crear y ejecutar un runbook de automatización.](#)

¿Necesita más revisión? Plantillas ARM

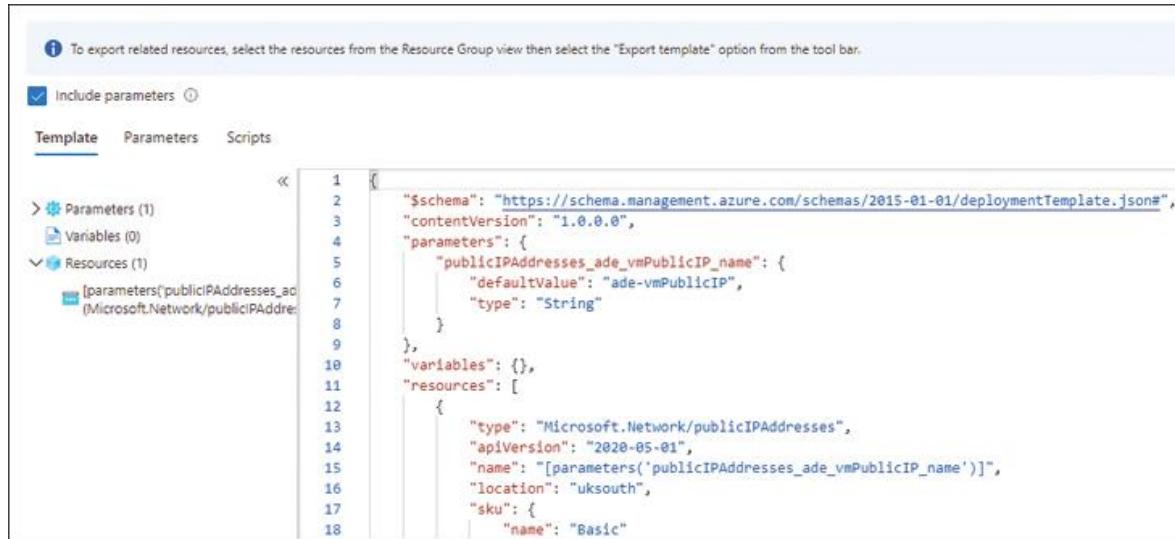
Para obtener más información sobre las plantillas ARM, visite el artículo de Microsoft Docs en <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/>.

Guardar una implementación como plantilla de Azure Resource Manager

Azure Portal ofrece la posibilidad de exportar implementaciones a una plantilla ARM. Esto puede resultar especialmente útil cuando empiece a utilizar plantillas ARM. Puede exportar un entorno con el que está acostumbrado a trabajar y luego explorar el JSON exportado. Azure Portal tiene dos formas de exportar una plantilla:

- **De un recurso o grupo de recursos.** Genera una plantilla ARM basada en un recurso o grupo de recursos existente.
- **Antes de una implementación o de una implementación histórica.** Extrae la plantilla ARM utilizada para una implementación.

Exportar desde un recurso específico es, en general, el mismo proceso independientemente del recurso. En Azure Portal, haga clic en cualquier recurso, desplácese hacia abajo en la hoja del menú de recursos hasta **Configuración** y luego elija **Exportar plantilla**, que abre la hoja **Exportar plantilla**, como se muestra en la [Figura 1-32](#).



The screenshot shows the 'Export template' dialog in the Azure portal. At the top, there's a note: 'To export related resources, select the resources from the Resource Group view then select the "Export template" option from the tool bar.' Below this, there's a checked checkbox for 'Include parameters'. The tabs at the bottom are 'Template', 'Parameters', and 'Scripts', with 'Template' selected. On the left, there's a tree view showing 'Parameters (1)', 'Variables (0)', and 'Resources (1)'. Under 'Resources (1)', it lists '[parameters('publicIPAddresses_ade')]' and '(Microsoft.Network/publicIPAddresses_ade)'. The main area displays the JSON template code, with line numbers 1 through 18 visible on the left. The code defines a schema, content version, parameters (including a public IP address parameter), variables, and a single resource (a public IP address).

```
1  {
2      "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3      "contentVersion": "1.0.0.0",
4      "parameters": {
5          "publicIPAddresses_ade_vmPublicIP_name": {
6              "defaultValue": "ade-vmPublicIP",
7              "type": "String"
8          }
9      },
10     "variables": {},
11     "resources": [
12         {
13             "type": "Microsoft.Network/publicIPAddresses",
14             "apiVersion": "2020-05-01",
15             "name": "[parameters('publicIPAddresses_ade_vmPublicIP_name')]",
16             "location": "uksouth",
17             "sku": {
18                 "name": "Basic"
19             }
20         }
21     ]
22 }
```

FIGURA 1-32 Exportación de una plantilla desde un recurso en Azure Portal

La Figura 1-32 muestra un ejemplo de exportación de un solo recurso. Es la IP pública de un controlador de dominio al que se hace referencia en la habilidad 1.7 de este libro. Como se muestra en la Figura 1-32, la hoja **Exportar plantilla** muestra las siguientes opciones:

- ■ **Descarga.** Descarga una copia comprimida de la plantilla.
- ■ **Agregar a la biblioteca.** Guarda la plantilla en una biblioteca para su uso posterior. La biblioteca de plantillas se analiza en la sección "Administrar una plantilla desde una biblioteca" más adelante en este capítulo.
- ■ **Implementar.** Implementa la plantilla como se muestra en el editor.
- ■ **Incluir parámetros.** Incluye la sección de parámetros de la plantilla. Si esta opción no está seleccionada, la sección de parámetros se convierte en un objeto vacío— {}.
- ■ **Estructura de la plantilla.** El lado izquierdo del panel inferior define el contorno de la estructura JSON de la plantilla.
- ■ **Editor de plantillas.** El lado derecho del panel inferior permite la edición en vivo de la exportación.

Haga clic en **Descargar**. El archivo zip resultante contiene dos archivos JSON: el archivo `template.json` contiene la definición de sus recursos y el archivo `parameters.json` se usa para pasar parámetros al archivo `template.json` para una implementación.

Exportar un grupo de recursos es similar, como muestra la captura de pantalla de la Figura 1-33.

The screenshot shows the Azure Portal's 'Essentials' blade. At the top, it displays 'Subscription (change) : Free Trial', 'Subscription ID : [REDACTED]', and 'Tags (change) : Usage : az303chap1'. Below this, there are filters for 'Type == all' and 'Location == all'. A message indicates 'Showing 1 to 10 of 10 records.' and an option to 'Show hidden types'. On the right, there are dropdowns for 'No grouping' and 'List view'. The main area lists 10 resources with checkboxes:

Name	Type	Location
ade-vk	Key vault	UK South
ade-vm	Virtual machine	UK South
ade-vm_disk1_823ef6ea0e004cc9853503c8867339a7	Disk	UK South
ade-vmNSG	Network security group	UK South
ade-vmPublicIP	Public IP address	UK South
ade-vmVMNIC	Network interface	UK South
ade-vmVNET	Virtual network	UK South
vmScSet	Virtual machine scale set	UK South
vmScSetLB	Load balancer	UK South
vmScSetLBPublicIP	Public IP address	UK South

FIGURA 1-33 Selección de recursos para exportar desde un grupo de recursos en Azure Portal

Al hacer clic en el enlace **Exportar plantilla** en la parte superior derecha, se exportarán todos los recursos de su grupo de recursos, a menos que seleccione específicamente los recursos que desea exportar.

Modificar la plantilla de Azure Resource Manager

Las plantillas ARM son archivos JSON y pueden modificarse con cualquier editor de texto y almacenarse junto con el código de su empresa en el control de fuente. El editor de código fuente multiplataforma de Microsoft, Visual Studio Code (VS Code), tiene algunas extensiones excelentes para ayudar con la edición de plantillas ARM. (Consulte <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/use-vs-code-to-create-template>). El uso del editor no es parte del examen, pero las extensiones harán que sea más fácil ver las secciones clave de una plantilla ARM y aprender a modificar esas secciones.

Para comenzar a modificar una plantilla, puede exportar una plantilla desde el portal como se discutió en la sección anterior. Además, el repositorio de GitHub de plantillas de inicio rápido de Azure ARM tiene cientos de plantillas listas para usar para ayudar con el aprendizaje de ARM. La complejidad de estas plantillas varía desde plantillas de recursos individuales más pequeñas hasta plantillas grandes que contienen arquitecturas de múltiples niveles de mejores prácticas con seguridad,

cumplimiento, resiliencia y redundancia integradas. Las plantillas de 100 niveles son las plantillas introductorias. (Consulte <https://github.com/Azure/azure-quickstart-templates/tree/master/100-blank-template>). Copie el contenido del archivo `azuredeploy.json` en VS Code como se muestra en la [Figura 1-34](#).



```
1 azuredeploy.json X
1.4 - Automation > 1.4.2 - Modifying a bank template > (1) azuredeploy.json > ...
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {},
5 },
6   "variables": {},
7 },
8   "resources": [
9     ],
10  "outputs": {}
11 }
12 }
```

FIGURA 1-34 Estructura de la plantilla ARM en blanco

La plantilla ARM en blanco que se muestra en la [Figura 1-34](#) muestra una vista clara de la estructura de la plantilla:

- **\$ esquema (obligatorio).** Esta es la ubicación de la definición de esquema JSON para una plantilla ARM. Esto no cambia a menos que se actualice el esquema.
- **contentVersion (obligatorio).** Se utiliza para el control de la fuente y puede tener cualquier formato.
- **Parámetros.** Los parámetros se pasan a la plantilla para personalizar la implementación.
- **Variables.** Las variables son valores calculados a partir de parámetros, otras variables o recursos en la plantilla y luego se utilizan en la implementación.
- **Recursos (requerido).** Se deben definir los recursos para el despliegue.
- **Salidas.** Estos son los resultados de las implementaciones de recursos, como una dirección IP o un punto final de servicio.

La plantilla en blanco se puede implementar en Azure; no hará nada, pero es una plantilla válida.

La Figura 1-35 muestra una versión adaptada de la plantilla de inicio rápido 101-storage-account-create desde el repositorio de GitHub. La plantilla se ha separado en las siguientes cuatro imágenes para que pueda ver claramente la estructura definida anteriormente.

```
1.4 - Automation > 1.4.2 - Modifying a storage account > [ ] azuredeploy.json > [ ] resources > {} 0
1 {
2   "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3   "contentVersion": "1.0.0.0",
4   "parameters": {
5     "storageAccountName": { A
6       "type": "string",
7       "metadata": {
8         "description": "Specifies the name of the Azure Storage account." B
9       }
10    },
11    "storageAccountType": {
12      "type": "string",
13      "defaultValue": "Standard_LRS",
14      "allowedValues": [ C
15        "Standard_LRS",
16        "Standard_GRS",
17        "Standard_ZRS",
18        "Premium_LRS"
19      ],
20      "metadata": {
21        "description": "Storage Account type"
22      }
23    },
24    "location": {
25      "type": "string",
26      "defaultValue": "uksouth",
27      "metadata": {
28        "description": "The location in which the Azure Storage resources should be deployed." D
29      }
30    }
31  },
32}
```

FIGURA 1-35 Parámetros de la plantilla ARM

La Figura 1-35 muestra la sección de parámetros de la plantilla; cada parámetro se define de una manera ligeramente diferente:

1. Cada parámetro tiene un nombre; el primero es `storageAccountName`. Este nombre es cómo se hará referencia al parámetro en la plantilla.
2. los metadatos se pueden configurar en toda la plantilla ARM; en la mayoría de los casos, se ignora. Para un parámetro, la configuración de metadatos con la descripción del nombre se puede ver durante la implementación y se usa principalmente como un mecanismo de ayuda.
3. `allowValues` utiliza una configuración de menú desplegable. Solo se pueden elegir los valores especificados en `allowedValues`.

4. `defaultValue`, si se especifica, significa que no es necesario pasar un valor al parámetro con el que se especifica cuando se implementa la plantilla. Para los parámetros anteriores, siempre se debe proporcionar `storageAccountName` cuando se implementa la plantilla, ya que no hay `defaultValue`.

La siguiente sección de la plantilla (ver [Figura 1-36](#)) define una variable.

```
32 "variables": {  
33   "uniqueAccountName": "[concat(parameters('storageAccountName'), uniquestring(resourceGroup().id))]"  
34 },
```

FIGURA 1-36 Definición de una variable en una plantilla ARM

En la [Figura 1-36](#), los parámetros ('`storageAccountName`') es un ejemplo de cómo usar un parámetro en una plantilla ARM; devolverá el valor ingresado para el parámetro `storageAccountName`. Las plantillas ARM tienen muchas funciones integradas disponibles. Por ejemplo, `concat` es una función de cadena que concatena dos cadenas. En el ejemplo anterior, está concatenando `storageAccountName` a otra función que devuelve una cadena única que se basa en el grupo de recursos.

La sección de recursos suele ser la más complicada; [La figura 1-37](#) muestra un solo recurso: una cuenta de almacenamiento.

```
35 "resources": [  
36   {  
37     "type": "Microsoft.Storage/storageAccounts",  
38     "apiVersion": "2019-04-01",  
39     "name": "[variables('uniqueAccountName')]",  
40     "location": "[parameters('location')]",  
41     "sku": {  
42       "name": "[parameters('storageAccountType')]"  
43     },  
44     "kind": "StorageV2",  
45     "properties": {}  
46   },  
47 ],  
48   "outputs": {}  
49 }
```

FIGURA 1-37 Definición de cuenta de almacenamiento para un recurso

Cada recurso implementado requiere las siguientes propiedades:

- ■ **tipo.** Esto establece el tipo de recurso. Es el espacio de nombres del proveedor de recursos, que en este caso es algo así

```
como Microsoft.Storage/storageAccounts, Microsoft.Compute /  
virtualMachines o Microsoft.Network/virtualNetworks.
```

- ■ **apiVersion.** Esta es la versión de la API REST utilizada para crear el recurso. Cada proveedor tiene su propia versión de API.
- ■ **Nombre.** Este es el nombre del recurso.

La mayoría de los recursos también requieren una ubicación. En la [Figura 1-37](#), también puede ver el parámetro `storageAccountType` que se usa para el SKU. Este es un buen caso de uso para `allowedValues` porque los SKU los define Microsoft y, por lo tanto, tienen un conjunto fijo de valores. Otro buen caso de uso para esto es limitar las SKU disponibles para una máquina virtual.

La sección de salidas de esta plantilla está vacía.



Plantillas de brazo de punta de examen

Se espera que pueda leer y comprender las plantillas ARM y sus estructuras JSON. Utilice las 101 plantillas de inicio rápido para recursos de uso frecuente, como máquinas virtuales, redes y almacenamiento, para desarrollar sus conocimientos.

Evaluar la ubicación de nuevos recursos.

Los valores de la plantilla ARM se pueden ampliar mediante expresiones. Una expresión de plantilla ARM se evalúa en tiempo de ejecución y, a menudo, contiene una función. En la [Figura 1-37](#), usamos una expresión para crear el nombre de cuenta único: `[reference(variables('uniqueAccountName')).PrimaryEndpoints]`, que solo se puede evaluar en tiempo de ejecución. Hasta el tiempo de ejecución, la plantilla no sabe qué La función `resourceGroup()` volverá.

La sección de salida de la plantilla ARM descrita en la sección anterior podría haber contenido una expresión para ser evaluada. Para una cuenta de almacenamiento, es posible que desee devolver los puntos finales creados, como se muestra en la [Figura 1-38](#).

```
45     "outputs": {
46       "endPoints": {
47         "type": "object",
48         "value": "[reference(variables('uniqueAccountName')).primaryEndpoints]"
49       }
50     }
51 }
```

FIGURA 1-38 Salida de información para un recurso recién creado a partir de una plantilla ARM

El código que se muestra en la [Figura 1-38](#) habría devuelto la siguiente salida JSON si se le hubiera dado un parámetro de az303arm para storageAccountName :

[Haga clic aquí para ver la imagen del código](#)

```
"salidas": {

  "endPoints": {

    "type": "Objeto",

    "valor": {

      "blob": "https://az303armfrs1x5kksdvcu.blob.core.windows.net/",

      "dfs": "https://az303armfrs1x5kksdvcu.dfs.core.windows.net/",

      "archivo": "https://az303armfrs1x5kksdvcu.file.core.windows.net/",

      "cola": "https://az303armfrs1x5kksdvcu.queue.core.windows.net/",

      "tabla": "https://az303armfrs1x5kksdvcu.table.core.windows.net/",

      "web": "https://az303armfrs1x5kksdvcu.z33.web.core.windows.net/"

    }

  }

}
```

},

Otra expresión común es usar la función incorporada de `resourceGroup()` para devolver la ubicación del grupo de recursos en el que se está implementando la plantilla ARM. Como se mostró anteriormente en la [Figura 1-35](#), la definición del parámetro de ubicación cambiaría para incluir la expresión que se muestra en la [Figura 1-39](#).

```
24 |     "location": {  
25 |         "type": "string",  
26 |         "defaultValue": "[resourceGroup().location]"  
27 |     }
```

FIGURA 1-39 Evaluación de la ubicación del recurso dentro de la plantilla

La propiedad `.location` devuelve la ubicación del grupo de recursos proporcionado. Todos los recursos de la plantilla utilizan este parámetro, lo que garantiza que todos los recursos estén en la misma ubicación. Tener todos los recursos en la misma ubicación que el grupo de recursos al que pertenecen aplica las mejores prácticas.

Implementar desde una plantilla

Ahora que ha configurado una plantilla, es hora de implementar sus recursos en Azure. Hay algunas opciones para esto, y en esta sección, exploraremos las opciones más utilizadas: Azure Portal, PowerShell y Azure CLI.

Una plantilla ARM se puede implementar en varios ámbitos, inquilinos, grupos de administración, suscripciones y grupos de recursos. Los primeros tres ámbitos se utilizan generalmente para implementaciones de políticas de Azure y RBAC. La implementación del grupo de recursos es la forma en que se implementan la mayoría de los recursos y es el foco del examen. La implementación de un grupo de recursos requiere un grupo de recursos existente para implementar; puede explorar la implementación en un grupo de recursos mediante Azure Portal:

Plantilla de nota ARM para tutorial

Cada una de las implementaciones de este ejemplo utiliza la plantilla 101-simple-vm-windows de las plantillas de inicio rápido de Azure (<https://github.com/Azure/azure-quickstart-templates/tree/master/101-vm-simple-windows>) . En el momento de

redactar este documento, esta plantilla fue creada por un empleado de Microsoft. Sin embargo, no todos lo son, así que verifique lo que está implementando.

1. En Azure Portal, ingrese **implementar** en el campo en la parte superior de Azure Portal. Elija **Implementar una plantilla personalizada** en la parte superior del menú desplegable que se muestra a medida que escribe el nombre del recurso.
2. La implementación de plantillas personalizadas le permite pegar su plantilla en **Construya su propia plantilla en el editor**; cree recursos a partir de **plantillas comunes** o **cargue una plantilla de inicio rápido de GitHub**. Elija **Cargar una plantilla de inicio rápido de GitHub**. Filtre el texto "simple" y seleccione **101-vm-simple-windows**. Haga clic en **Seleccionar plantilla**.
3. Tenga en cuenta que la pantalla de **Implementación personalizada** ([Figura 1-40](#)) es muy similar a las pantallas del portal para agregar cualquier recurso. Si abre el archivo `azuredeploy.json` desde el repositorio de [inicio rápido 101-vm-simple-windows](#) y compara los parámetros, cada parámetro en `azuredeploy.json` tiene un cuadro de entrada en esta página. Los cuadros de entrada vacíos corresponden a los parámetros sin valor predeterminado. Seleccione el menú desplegable **2016-Datacenter**; las opciones disponibles para usted son los valores permitidos definidos para el parámetro.
4. Ingrese los valores apropiados para la implementación de la máquina virtual y seleccione **Revisar + Crear**. Finalmente, haz clic en **Crear**. Su máquina virtual está implementada.

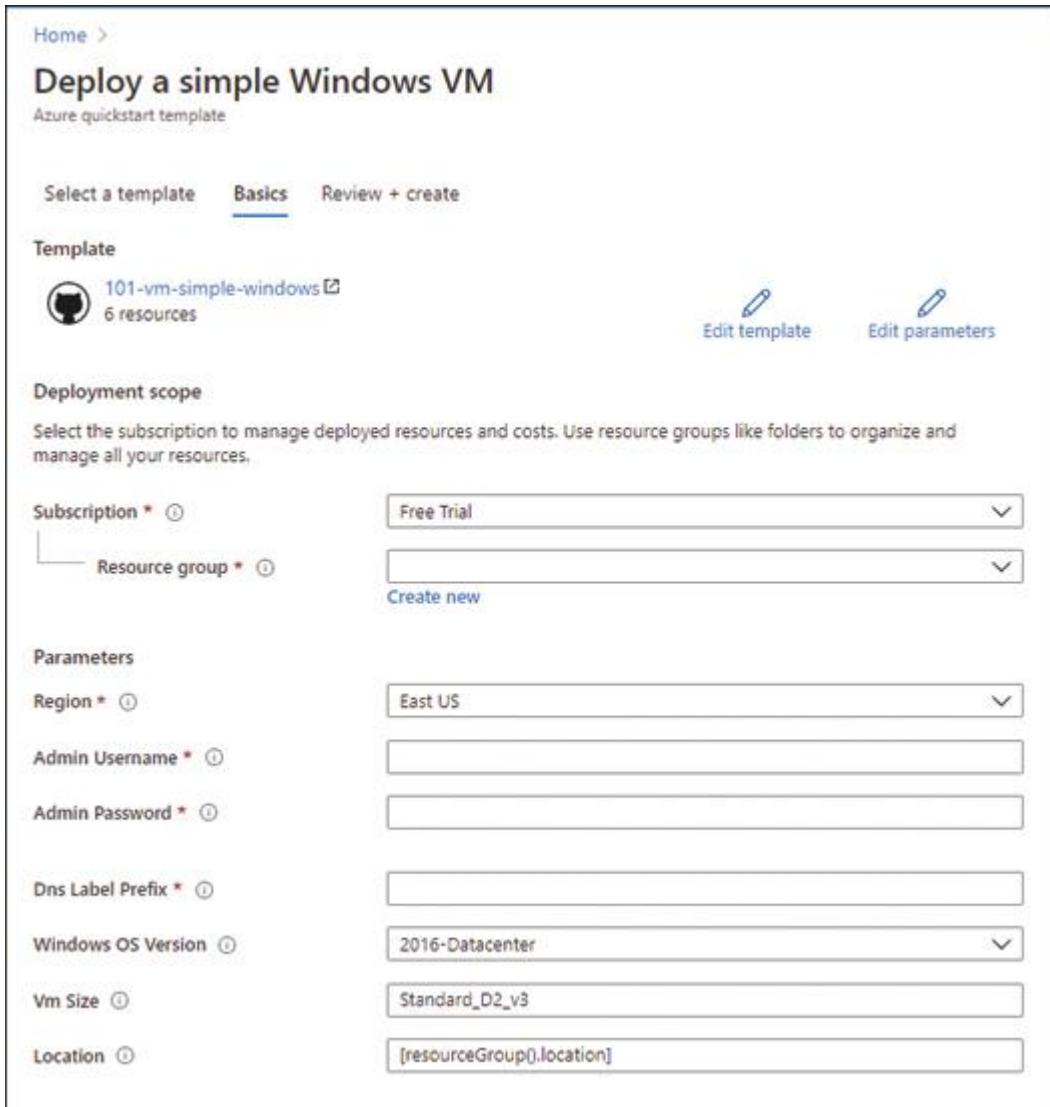


FIGURA 1-40 Implementación de la plantilla ARM 101-vm-simple-windows en Azure Portal

Como arquitecto que desea utilizar IaC para acelerar sus implementaciones a través de la automatización, es poco probable que utilice Azure Portal para implementar sus recursos. Aquí es donde entra en juego la implementación con script en PowerShell o la CLI de Azure. Necesitará un grupo de recursos y deberá establecer sus parámetros. Los parámetros se pueden pasar directamente a la plantilla en la línea de comandos con la CLI de Azure, como se muestra en el siguiente código:

[Haga clic aquí para ver la imagen del código](#)

```
#! / bin / bash
```

```
resourceGroupName = "az303chap1_4-rg"
deploymentName = "simpleWinVM"
templateUri = "https://raw.githubusercontent.com/Azure/azure-
quickstart-templates/
master / 101-vm-simple-windows / azuredeploy.json "
adminUsername = "adminuser"
adminPassword = "secretP @ ssw0rd"
dnsLabelPrefix = "az303depvm"

az deployment group create --resource-group $resourceGroupName \
--name $ deploymentName \
--template-uri $ templateUri \
--parámetros "adminUsername = $ adminUsername" \
"adminPassword = $ adminPassword" \
"dnsLabelPrefix = $ dnsLabelPrefix"
```

La Figura 1-41 muestra el bloque de código anterior que se ejecuta a través de VS Code:

```
deploy.sh > 1.4 - Automation > 1.4.4 - Deploy params in script > deploy.sh
1  #!/bin/bash
2
3  resourceName="az303chap1_4-rg"
4
5  deploymentName="simpleWinVM"
6  templateUri="https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json"
7  adminUsername="adminuser"
8  adminPassword="secretP@ssw0rd"
9  dnsLabelPrefix="az303depvm"
10
11 az deployment group create --resource-group $resourceName \
12   --name $deploymentName \
13   --template-uri $templateUri \
14   --parameters "adminUsername=$adminUsername" \
15     "adminPassword=$adminPassword" \
16     "dnsLabelPrefix=$dnsLabelPrefix"

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE

MINGW64 /d/git/personal/az303-chap1/1.4 - Automation/1.4.4 - Deploy params in script (master)
$ ./deploy.sh
[]- Running ..
```

FIGURA 1-41 Implementación de 101-vm-simple-windows con la CLI de Azure

Los parámetros de la [Figura 1-41](#) están configurados de modo que solo aquellos que no tienen un valor predeterminado se pasen a la plantilla. Tenga en cuenta que el argumento `templateUri` toma la URL del archivo `azuredeploy.json` directamente de GitHub. El argumento `templateUri` usa `raw.githubusercontent.com`, que pasa el contenido sin procesar del archivo; sin este cambio en la URL, la plantilla generará un error.

Si recuerda haber exportado un recurso de la sección anterior titulada "Guardar una implementación como una plantilla de Azure Resource Manager", el archivo zip contenía un archivo `parameters.json`. Este archivo se utiliza para pasar parámetros a la plantilla durante la implementación. Se hace referencia a él como parte del comando de implementación para la CLI de Azure y en el ejemplo que se muestra en la [Figura 1-42](#), con PowerShell.

The screenshot shows a code editor with an open file named `azuredeploy.parameters.json`. The file contains JSON configuration for an Azure deployment, including parameters for an administrator user, password, DNS label prefix, and VM size. To the right of the code editor is a terminal window showing PowerShell commands. The commands are:

```

1.4 - Automation > 1.4.4 - Deploy parameters in JSON > deploy.ps1
1 $resourceGroupName="az303chap1_4-rg"
2 $templateFile="azuredeploy.json"
3 $templateParameterFile="azuredeploy.parameters.json"
4
5 New-AzResourceGroupDeployment -ResourceGroupName $resourceGroupName ` 
6 -TemplateFile $templateFile ` 
7 -TemplateParameterFile $templateParameterFile ` 
8 -Mode Complete ` 
9 -Force

```

Below the terminal window, the file system is listed:

```

PS D:\git\personal\az303-chap1\1.4 - Automation> Get-ChildItem

Directory: D:\git\personal\az303-chap1\1.4 - Automation\1.4.4 - Deploy parameters in JSON

Mode                LastWriteTime      Length Name
----                -----        7230  azuredeploy.json
-a---       07/06/2020 10:39          405  azuredeploy.parameters.json
-a---       07/06/2020 10:39          299  deploy.ps1

```

At the bottom of the terminal window, the command `./deploy.ps1` is shown.

FIGURA 1-42 Implementación de una plantilla local con PowerShell

En la [Figura 1-42](#), el código de la derecha muestra la secuencia de comandos de PowerShell, y la ventana de terminal a continuación muestra el comando para llamar a la secuencia de comandos. La plantilla y los parámetros de la plantilla se almacenan localmente, por lo que se usa el argumento `TemplateFile` en lugar del URI. Para este ejemplo, `101-vm-simple-windows` `azuredeploy.json` y `azuredeploy.parameters.json` se copiaron en el directorio desde el que se ejecuta el script. Tenga en cuenta el parámetro `-Mode`; una plantilla ARM que se ejecuta en un grupo de recursos que ya tiene recursos se puede ejecutar en dos modos:

- **Incremental.** Este es el modo predeterminado en el que permanecen todos los recursos que existen en el grupo de recursos pero no en la plantilla. Los recursos especificados en la plantilla se crean o actualizan.
- **Completo.** Todos los recursos del grupo de recursos se eliminan y se vuelven a crear.

El modo se define como completo. Cuando se ejecuta este script de PowerShell, todos los recursos del grupo de recursos definido se eliminan y se vuelven a crear desde cero. Esto podría ser un movimiento bastante destructivo, por lo que PowerShell le preguntará si está seguro, aunque puede omitir esta verificación con la opción `-Force`.

En el lado izquierdo de la [Figura 1-42](#), puede ver el archivo de parámetros que pasa el comando de PowerShell. Los tres parámetros principales son los mismos que se pasaron directamente en el ejemplo anterior de la [Figura 1-41](#) con la CLI de Azure. En el ejemplo de la [Figura 1-42](#), hay un cuarto parámetro, `vmSize`, que tiene un valor predeterminado dentro de la plantilla ARM. La especificación de un parámetro en el archivo de parámetros anulará un valor predeterminado en la plantilla ARM.



Implementación de la plantilla del brazo de la punta del examen
Se espera que comprenda cómo ejecutar implementaciones desde el portal y la línea de comandos. Tener una buena comprensión de las opciones en torno a estas implementaciones podría ser beneficioso.

Configurar una plantilla de disco virtual

El mercado de Azure Portal tiene muchas imágenes de sistemas operativos; sin embargo, es posible que estos no siempre sean el mejor punto de partida para crear sus máquinas virtuales en Azure. Es posible que deba crear su propia imagen base o migrar una imagen base desde las instalaciones. Hay muchas formas de lograr esto, como copiar un disco virtual (VHD) de la imagen en Azure Storage y hacer referencia a él como parte de una plantilla ARM. Para hacer referencia a un VHD en una plantilla ARM, el `storageProfile` debe establecerse para que apunte al VHD. Consulte el `StorageProfile` de la plantilla de inicio rápido de Azure 101-vm-simple-linux como se muestra en la [figura 1-43](#):

```

217     "storageProfile": {
218         "osDisk": {
219             "createOption": "fromImage",
220             "managedDisk": {
221                 "storageAccountType": "[variables('osDiskType')]"
222             }
223         },
224         "imageReference": {
225             "publisher": "Canonical",
226             "offer": "UbuntuServer",
227             "sku": "[parameters('ubuntuOSVersion')]",
228             "version": "latest"
229         }
230     },

```

FIGURA 1-43 Almacenamiento de plantilla ARM Perfil para un disco de sistema operativo administrado

La Figura 1-43 muestra la definición de un disco administrado. La sección `osDisk` significa que el disco se creará a partir de una imagen y lo administrará Azure en el almacenamiento `Standard_LRS`, que se establece en la variable `osDiskType` en la parte superior de la plantilla ARM. La sección `imageReference` determina qué imagen se utilizará para el disco.

La configuración de la plantilla ARM para usar una copia de un VHD de Azure Storage cambia la sección `storageProfile` a la que se muestra en la Figura 1-44.

```

203     "storageProfile": {
204         "osDisk": {
205             "name": "[concat(parameters('vmName'),'-osDisk')]",
206             "osType": "[parameters('osType')]",
207             "caching": "ReadWrite",
208             "image": {
209                 "uri": "[parameters('vhndl')]"
210             },
211             "vhd": {
212                 "uri": "[variables('osDiskVhdName')]"
213             },
214             "createOption": "FromImage"
215         }
216     },

```

FIGURA 1-44 Perfil de almacenamiento de plantilla ARM para un VHD no administrado

La sección `osDisk` (Figura 1-44) se ha expandido porque se trata de un disco no administrado. La plantilla ahora establece el nombre del disco

administrado como `osType` (Establecer en linux en los parámetros) y el mecanismo de almacenamiento en caché. La parte clave de esta sección es la imagen; aquí es donde se copiará el VHD. El `vhdUrl` se pasa como un parámetro, que es la dirección URL completa del VHD en Azure Storage. No hay una sección `imageReference`; el sistema operativo ya está en el VHD, por lo que no es necesario seleccionarlo. La sección `vhd` define dónde se almacenará el nuevo VHD. Se establece en la sección de variables y es una cuenta de almacenamiento en la misma región que la VM.

Administrar una biblioteca de plantillas

Azure Portal tiene una biblioteca de plantillas donde puede almacenar e implementar plantillas. Abra Azure Portal y busque **plantillas** en el cuadro de búsqueda de nombre de recurso en la parte superior de Azure Portal. Elija **Plantillas** en el menú desplegable que se muestra a medida que escribe el nombre del recurso y presiona Entrar. La página que se carga es la biblioteca de plantillas. Siga estos pasos para explorar la funcionalidad de la biblioteca:

1. Haga clic en **Agregar** en la parte superior izquierda. Este proceso agregará una plantilla a la biblioteca. Introduzca un **nombre** y una **descripción** (ambos obligatorios). Haga clic en **Aceptar**. Ahora puede crear una plantilla desde cero en el editor a la derecha de la página para agregar o pegar la suya propia. Pegue una copia de `azuredeploy.json` de <https://github.com/Azure/azure-quickstart-templates/blob/master/101-vm-simple-linux/azuredeploy.json>. Haga clic en **Aceptar** y luego en **AÑADIR**.
2. Su plantilla ahora está almacenada en el portal. Haga clic en el nombre de la plantilla almacenada en el portal. Tenga en cuenta que es posible que deba hacer clic en **Actualizar** en la parte superior de la página **Plantillas** para ver la nueva plantilla en la lista.
3. Como se muestra en la [Figura 1-45](#), las siguientes opciones están disponibles:
 1. ■ **Editar.** Edite la plantilla en el editor en línea o pegue otra versión en la parte superior. La descripción de la plantilla también se puede editar, aunque el nombre es fijo.

2. ■ **Eliminar.** Elimina la plantilla.
3. ■ **Comparta.** RBAC para la plantilla seleccionada.
4. ■ **Implementar.** Abre la plantilla en la ventana **Implementación personalizada**. Consulte "Implementar desde una plantilla", anteriormente en este capítulo, para obtener más información.
5. ■ **Ver plantilla.** Abre una vista de solo lectura de la plantilla.

```

1  {
2      "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
3      "contentVersion": "1.0.0.0",
4      "parameters": {
5          "vmName": {
6              "type": "string",
7              "defaultValue": "simpleLinuxVM",
8              "metadata": {
9                  "description": "The name of your Virtual Machine."
10             }
11         },
12         "adminUsername": {
13             "type": "string",
14             "metadata": {
15                 "description": "Username for the Virtual Machine."
16             }
17         },
18         "authenticationType": {
19             "type": "string",
20             "defaultValue": "password"
21         }
22     }
  
```

FIGURA 1-45 Características de la biblioteca de plantillas de Azure Portal

Biblioteca de plantillas de *notas*

La gestión de una biblioteca de plantillas es parte de la especificación del examen. Sin embargo, al guardar una plantilla en la biblioteca, se sobrescribe la versión anterior. Por lo tanto, la biblioteca no está controlada por versiones. Como arquitecto, debe recomendar la mejor práctica, que es el control de versiones para almacenar Infraestructura como código (IaC).

Crear y ejecutar un runbook de automatización

La automatización de Azure permite la automatización y configuración de entornos locales y en la nube. La automatización de Azure funciona en Windows y Linux y ofrece una forma coherente de implementar, configurar y administrar recursos. La automatización de Azure tiene tres capacidades principales:

- ■ **Gestión de la configuración.** Puede administrar configuraciones mediante la configuración de estado deseado (DSC) de PowerShell, actualizar la configuración o detener el

cambio de configuración aplicando configuraciones extraídas de Azure.

- ■ **Gestión de actualizaciones.** Puede organizar la instalación de la actualización a través de ventanas de mantenimiento.
- ■ **Automatización de procesos.** Puede automatizar tareas que consumen mucho tiempo, son frecuentes y, a veces, propensas a errores a través de runbooks.

Se utiliza un runbook de automatización para la automatización de procesos. El runbook se puede crear con PowerShell o Python, o se puede crear gráficamente mediante la función de arrastrar y soltar en Azure Portal. Un runbook se puede ejecutar en Azure o localmente en un trabajador de runbook híbrido. Al ejecutar el runbook, la automatización de Azure crea un trabajo que ejecuta la lógica tal como se define en el runbook.

Antes de que se pueda crear o ejecutar un runbook de automatización, se debe crear una cuenta de automatización. Esto se puede realizar en la línea de comandos o, como se muestra en este ejemplo, se puede crear en Azure Portal:

1. En Azure Portal, busque **automatización** en la barra de búsqueda de nombres de recursos en la parte superior de Azure Portal y haga clic en **Cuentas de automatización**.
2. Haga clic en **Agregar** para agregar una cuenta de automatización. [La Figura 1-46](#) muestra la pantalla **Agregar cuenta de automatización**, donde puede establecer las opciones de configuración para la cuenta:
 1. ■ **Nombre.** Este es el nombre de la cuenta de automatización.
 2. ■ **Grupo de recursos.** Este es el grupo de recursos donde reside la cuenta de automatización.
 3. ■ **Ubicación.** Esta es la ubicación de la cuenta de automatización.
 4. ■ **Cree una cuenta de ejecución de Azure.** Cuando se establece en **Sí**, esta opción crea una entidad de servicio, que tiene el rol de Colaborador en el nivel de suscripción. Se

utiliza para acceder a los recursos y gestionarlos. Para este ejemplo, deje esto configurado en **Sí**.

Home > Automation Accounts >

Add Automation Account

Name * ⓘ
az303aa

Subscription *
Free Trial

Resource group *
az303chap1_4-rg
Create new

Location *
UK South

Create Azure Run As account * ⓘ
 Yes No

i This will create Azure Run As account in the Automation account which are useful for authenticating with Azure to manage Azure resources from Automation runbooks. Note that the creation of Azure Run As account may affect the security of the subscription.[Learn more](#)

i Learn more about Automation pricing.

Create

FIGURA 1-46 Agregar cuenta de automatización

3. Una vez que haya seleccionado los valores apropiados, al hacer clic en **Crear** se creará la cuenta de automatización. Volverá a la página Cuentas de automatización.
4. Actualice la página **Cuentas de automatización** y verá la cuenta recién creada en la lista. Para agregar un runbook a la cuenta de automatización, haga clic en el nombre de la cuenta de automatización. La pantalla que se carga es el menú Cuenta de automatización. Desplácese hacia abajo y haga clic en **Runbooks**. Los runbooks enumerados se crearon automáticamente cuando agregó la cuenta de automatización. Para agregar un runbook, haga clic en **Create A Runbook** y complete los siguientes parámetros:
 - 0.■ **Nombre.** Este es el nombre del runbook; para este ejemplo, ingrese **cleanDevResources**.
 - 1.■ **Tipo de Runbook.** En el menú desplegable, puede elegir los tipos **PowerShell**, **Python 2**, **Gráfico** o **Basado en flujo de trabajo**. Para este ejemplo, elija **PowerShell**.
 - 2.■ **Descripción.** Tiene la opción de ingresar una descripción para la naturaleza del runbook.

5. Haga clic en **Aceptar**.

El runbook se abrirá con el editor que eligió en **Tipo de Runbook**. En este caso, estamos usando PowerShell. Puede escribir su secuencia de comandos de PowerShell en línea o puede pegarla desde otro editor. El caso de uso de un runbook es la automatización de procesos. El ejemplo de PowerShell en el Runbook de la [Figura 1-47](#) elimina todos los recursos en grupos de recursos con una etiqueta específica. Este proceso podría usarse para limpiar los recursos de desarrollo al final del día.

```

1 $conn = "AzureRunAsConnection"
2 try
3 {
4     # Get the connection "AzureRunAsConnection "
5     $sPConnection=Get-AutomationConnection -Name $conn
6
7     Connect-AzAccount ` 
8         -ServicePrincipal ` 
9         -Tenant $sPConnection.TenantId ` 
10        -ApplicationId $sPConnection.ApplicationId ` 
11        -CertificateThumbprint $sPConnection.CertificateThumbprint
12 }
13 catch {
14     if (!$sPConnection)
15     {
16         $ErrorMsg = "$conn not found."
17         throw $ErrorMsg
18     } else{
19         Write-Error -Message $_.Exception
20         throw $_.Exception
21     }
22 }
23
24 # Set the tag for AZ303 Chapter 1 resource removal
25 $rgTag = "az303Chap1"
26
27 $toCleanResources = (Get-AzResourceGroup -Tag @{ Usage=$rgTag })
28
29 Foreach ($resourceGroup in $toCleanResources) {
30     Write-Host "=> $($resourceGroup.ResourceGroupName) is for az303chap1. Deleting it..."
31     Remove-AzResourceGroup -Name $resourceGroup.ResourceGroupName -Force
32 }

```

FIGURA 1-47 Script de PowerShell para eliminar todos los grupos de recursos con una etiqueta determinada

La lista de códigos para este ejemplo se encuentra a continuación:

[Haga clic aquí para ver la imagen del código](#)

```

$ conn = "AzureRunAsConnection"

intentar

{

    # Obtenga la conexión "AzureRunAsConnection"

    $ sPConnection = Get-AutomationConnection -Name $ conn

    Connect-AzAccount '

```

```

    -ServicePrincipal '
    -Tenant $ sPConnection.TenantId '
    -ApplicationId $ sPConnection.ApplicationId '
    -CertificateThumbprint $ sPConnection.CertificateThumbprint
}

captura {
    si (! $ sPConnection)
    {
        $ ErrorMsg = "$ conn no encontrado".
        lanzar $ ErrorMsg
    } demás{
        Write-Error -Message $ _. Excepción
        lanzar $ _. Excepción
    }
}

```

```

# Establecer la etiqueta para la eliminación de recursos del
Capítulo 1 de AZ303

$ rgTag = "az303chap1"

$ toCleanResources = (Get-AzResourceGroup -Tag @ {Uso = $ rgTag})

```

```

Foreach ($ resourceGroup en $ toCleanResources) {

```

```
Write-Host "==> $ ($resourceGroup.ResourceGroupName) es  
para az303chap1. Eliminándolo ..."  
  
Remove-AzResourceGroup -Name $  
resourceGroup.ResourceGroupName -Force  
  
}
```

Una vez que se haya agregado la secuencia de comandos, haga clic en **Guardar**. Seleccione **Panel de prueba** en la parte superior de la pantalla, que ejecuta la versión editada del runbook para probar los resultados. Esto es útil si no está listo para publicar su runbook. La publicación de un runbook sobrescribe la copia en vivo. Haga clic en **Iniciar** para iniciar la prueba.

En este ejemplo, el runbook generará un error; PowerShell no reconoce `Connect-AzAccount`. Esto se debe a que la cuenta de automatización tiene los módulos heredados de `AzureRM` PowerShell cargados de forma predeterminada, pero no los módulos `Az`. Debe cargar los módulos `Az`; para hacer esto, regrese a la hoja de menú **Cuenta de Automatización** y elija **Módulos**. Los módulos que se cargan de forma predeterminada se muestran en la hoja **Módulos**. En este ejemplo, solo están disponibles los módulos de `AzureRM`. Haga clic en **Examinar galería**, busque `Az`, elija `Az.Accounts` y haga clic en **Importar**. A continuación, elija **Examinar galería**, busque `Az` y elija `Az.Resources`. (Debe hacer esto porque PowerShell en el runbook de ejemplo usa cmdlets de ambos módulos).

Una vez que los módulos se muestran como importados en la hoja del **módulo**, vuelva a la hoja **Runbook** y seleccione `cleanDevResources`, el nombre del runbook del paso 4 anterior. Haga clic en **Editar > panel de prueba > Start** para probar la runbook una vez más. El runbook debería ejecutarse ahora correctamente.

Se ha verificado que el runbook funciona, por lo que ahora seleccione **Publicar** para que el runbook esté disponible para ejecutarse. Volverá a la hoja de **runbook** para `cleanDevResources`. Hay tres formas de ejecutar un runbook:

- ■ **Manualmente.** Si elige **Iniciar** en la parte superior de la página del runbook, se ejecutará el runbook.

- **Webhook.** Activa el runbook mediante HTTP POST a una URL.
- **Programación.** Programa la ejecución del runbook.

El caso de uso de este ejemplo es eliminar los recursos del desarrollador al final del día. Por lo tanto, haga clic en **Programaciones** en la hoja de menú **Runbook** y luego elija **Agregar una programación** para agregar una programación para el Runbook, que abre la página **Programar Runbook**, como se muestra en la [Figura 1-48](#).

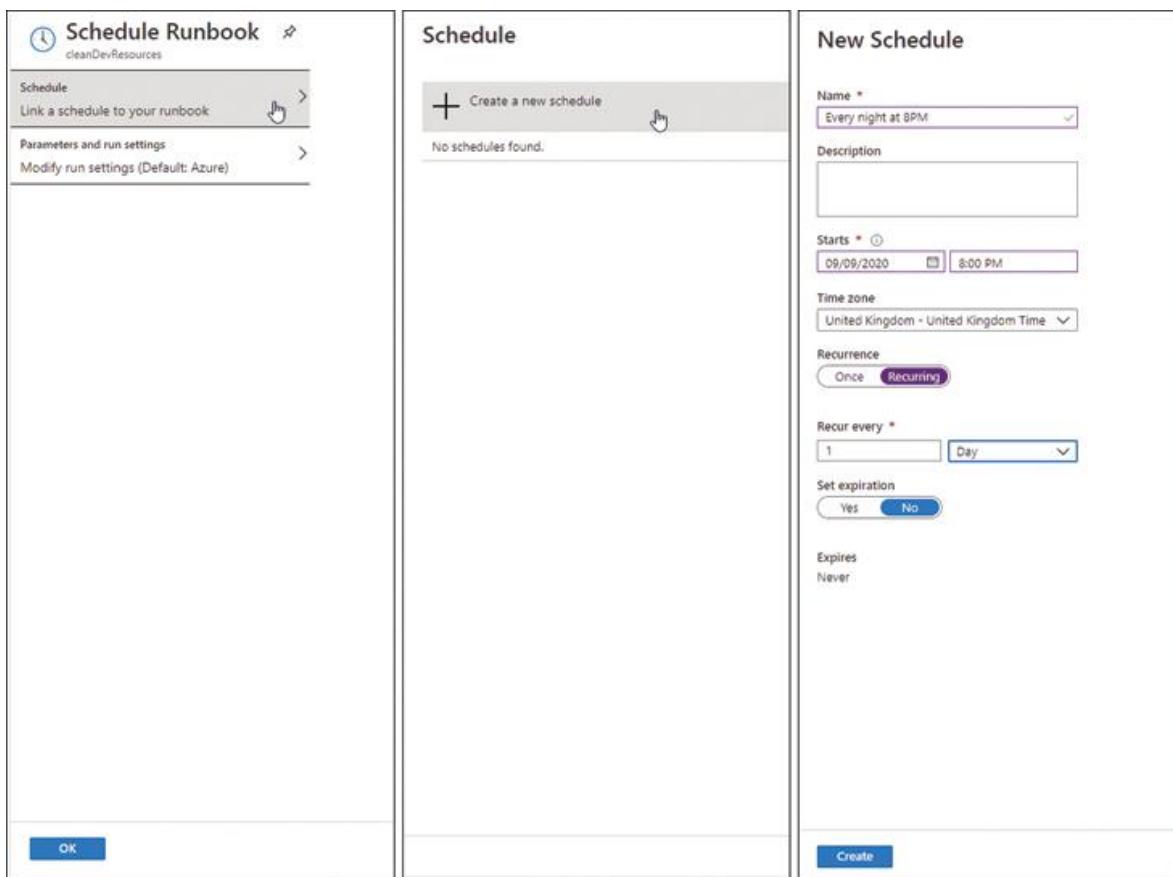


FIGURA 1-48 Programación de un runbook en Azure Portal

Puede configurar las siguientes opciones: **Inicio** , **Recurrencia** , **Repetir cada** y **Establecer vencimiento** . En el ejemplo que se muestra en la [Figura 1-48](#) , el runbook está configurado para ejecutarse todas las noches a las 8 p.m. El runbook se creará cuando haga clic en **Crear** .

¿Necesita más revisión? Automatización de Azure

Para obtener más información sobre Azure Automation en el portal, visite el artículo de Microsoft Docs "Introducción a Azure Automation" en <https://docs.microsoft.com/en-us/azure/automation/automation-intro>. En particular, debe leer las secciones de Configuración del estado deseado.

HABILIDAD 1.5: IMPLEMENTAR REDES VIRTUALES

Debido a que AZ-303 es una certificación de expertos, se espera que ya posea conocimientos sobre cómo se usan las redes virtuales para habilitar la comunicación segura entre recursos en Azure. Además, se espera que sepa cómo crear y mantener redes virtuales y comprender la notación CIDR. Esta habilidad requiere que comprenda cómo conectar redes virtuales para construir su red privada dentro de Azure, así como los requisitos que impulsan cada método de conexión.

Esta habilidad cubre cómo:

- ■ Implementar conexiones de red virtual a red virtual
- ■ Implementar el emparejamiento de redes virtuales

Implementar conexiones de red virtual a red virtual

Cuando el tráfico cifrado aparece como un requisito de seguridad o de cumplimiento para la comunicación a través de redes virtuales en una red virtual, deberá implementar una conexión de puerta de enlace VPN de red virtual a red virtual. Cuando se crea una conexión de red virtual a red virtual, es como una conexión VPN de sitio a sitio; todo el tráfico entre las redes virtuales fluye a través de un túnel IPsec / IKE seguro. El túnel se crea entre dos direcciones IP públicas que se asignan dinámicamente a las puertas de enlace VPN en el momento de la creación. La figura 1-49 muestra un diagrama de una implementación de ejemplo para conexiones de red virtual a red virtual.

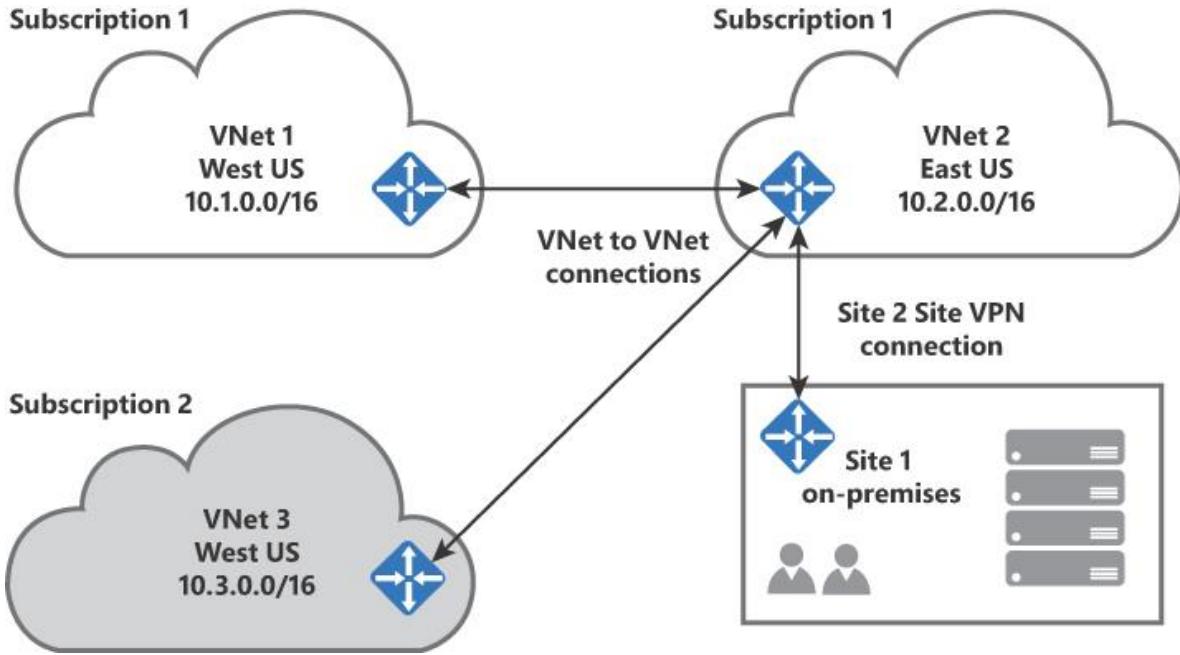


FIGURA 1-49 Conexiones de red virtual a red virtual entre suscripciones y regiones

Solo se permite una puerta de enlace VPN por red virtual. Sin embargo, una puerta de enlace VPN puede conectarse a varias redes virtuales y VPN de sitio a sitio. Las conexiones de red virtual a red virtual pueden estar en todas las regiones y suscripciones. En la [Figura 1-49](#), VNet 3 está en el oeste de EE. UU. Y es parte de la Suscripción 2. VNet 3 también conectado a VNet 2 en el este de EE. UU., que es parte de la suscripción 1. Para conectar dos redes virtuales, no debe haber cruces en los rangos de direcciones de las subredes.

Siga estos pasos para configurar la conexión para VNet 1 y VNet 2 dentro de la misma suscripción pero en todas las regiones.

1. Cree dos máquinas virtuales (VM) Linux Azure, una en la red virtual 1 y otra en la red virtual 2 con espacios de direcciones, como se muestra en la [figura 1-49](#). Asegúrese de que la VM en VNet 1 esté en una subred de 10.1.0.0/24 y que VNet 2 esté en una subred de 10.2.0.0/24. Esto asegurará que no haya superposición en las subredes existentes, que es un requisito del diseño de la puerta de enlace VPN. Asegúrese de que la máquina virtual en la red virtual 1 tenga una dirección IP pública. Para ayudar a crear esta arquitectura, use la plantilla ARM de inicio rápido de Azure en <https://github.com/Azure/azure-quickstart-templates>

[*templates/tree/master/101-vm-sshkey*](#). Deberá editar la dirección y los prefijos de subred en consecuencia.

2. Inicie sesión en Azure Portal y, en la barra de búsqueda de nombre de recurso en la parte superior, escriba **puerta de enlace de red virtual**. Seleccione **Puerta de enlace de red virtual** en el menú desplegable que se muestra a medida que escribe el nombre del recurso. Se abre la página Virtual Network Gateways. Haga clic en **Agregar** para crear una puerta de enlace de red virtual.
3. Como se muestra en la [Figura 1-49](#), cree la puerta de enlace VPN para VNet1 con los siguientes valores:
 1. ■ **Suscripción.** Seleccione la misma suscripción utilizada para crear las redes virtuales y las máquinas virtuales en el paso 1.
 2. ■ **Grupo de recursos.** Se completa automáticamente cuando se selecciona la red virtual.
 3. ■ **Nombre.** Este es un nombre único para la puerta de enlace VPN; para este ejemplo, ingrese **VNet1GW**.
 4. ■ **Región.** Seleccione la región utilizada para VNet 1; en la [Figura 1-49](#), este es el oeste de EE. UU.
 5. ■ **Tipo de puerta de enlace.** Para una puerta de enlace VPN, debe ser VPN.
 6. ■ **Tipo de VPN.** Elija **Basado en ruta**. Las VPN basadas en rutas cifran todo el tráfico que pasa a través de la VPN, mientras que la elección **de las basadas en políticas** cifra parte del tráfico según lo define la política.
 7. ■ **SKU.** Elija **Básico**. Los SKU para una puerta de enlace VPN se diferencian por las cargas de trabajo, el rendimiento, las funciones y los SLA. (Cuanto mayor sea el rendimiento, mayor será el costo).
 1. ■ **Básico.** Destinado a pruebas de concepto (POC) o cargas de trabajo de desarrollo.
 2. ■ **VpnGw1-3.** Admite BGP, hasta 30 conexiones VPN de sitio a sitio y un rendimiento de hasta 10 gigabits por segundo (Gbps) para el SKU Gw3 cuando se combina con la Generación 2.

3. ■ **VpnGw1-3AZ.** Estos SKU tienen el mismo conjunto de características que VPNGw1-3, pero son conscientes de la zona de disponibilidad.
8. ■ **Generación.** Elija **Generación 1**. La combinación de Generation y SKU admite varios rendimientos. Un SKU básico solo es compatible con la Generación 1.
9. ■ **Red virtual.** Elija VNet 1. Debería aparecer como disponible si seleccionó la **Región** correcta en el Paso 3d.
10. ■ **Intervalo de direcciones de subred de la puerta de enlace.** Esto se completará automáticamente una vez que se seleccione la red virtual. El rango de la subred se completa con / 24; sin embargo, Microsoft recomienda un rango / 27 o / 26, pero no menor que un rango / 28. Introduzca **10.1.1.0/27**.
11. ■ **Dirección IP pública.** Elija esta opción para crear una nueva dirección IP pública.
12. ■ **Nombre de la dirección IP pública.** Ingrese un nombre único; en este caso, use **VNet1GW-ip**.
13. ■ **Habilite el modo activo-activo.** Deje esta opción configurada como **Desactivada**. El modo activo-activo se utiliza para la conectividad VNet a VNet de alta disponibilidad.
14. ■ **Configure BGP ASN.** Deje esta opción configurada como **Desactivada**. El Border Gateway Protocol (BGP) se utiliza para intercambiar información de enrutamiento entre dos o más redes.
15. ■ **Haga clic en Revisar + Crear.** Una vez que haya pasado la validación, haga clic en **Crear**. El proceso de validación puede llevar algún tiempo.
4. Mientras se crea VNet1GW, siga los mismos pasos para crear una VNet denominada **VNet2GW**. Una vez más, seleccione agregar una puerta de enlace VPN en el portal siguiendo las mismas instrucciones del paso 2. Con la Figura 1-49 como guía, ingrese la configuración requerida para VNet2GW:

- 0.■ **Suscripción.** Seleccione la misma suscripción utilizada para crear las redes virtuales y las máquinas virtuales en el paso 1.
 - 1.■ **Grupo de recursos.** Se completa automáticamente cuando se selecciona la red virtual.
 - 2.■ **Nombre.** Este es un nombre único para la puerta de enlace VPN; para este ejemplo, ingrese **VNet2GW**.
 - 3.■ **Región.** En la Figura 1-49, este es el este de EE. UU.
 - 4.■ **Tipo de puerta de enlace.** Elija **VPN**.
 - 5.■ **Tipo de VPN.** Elija **Basado en ruta**.
 - 6.■ **SKU.** Elija **Básico**.
 - 7.■ **Generación.** Elija **Generación 1**.
 - 8.■ **Red virtual.** Elija **VNet2**.
 - 9.■ **Intervalo de direcciones de subred de la puerta de enlace.** Ingrese **10.2.1.0/27**.
 10. ■ **Dirección IP pública.** Elija crear una nueva dirección IP pública.
 11. ■ **Nombre de la dirección IP pública.** Ingrese un nombre único para la dirección IP pública; para este ejemplo, ingrese **VNet2GW-ip**.
 12. ■ **Habilite el modo activo-activo.** Deje esto configurado en **Desactivado**.
 13. ■ **Configure BGP ASN.** Deje esto configurado en **Desactivado**.
5. Haga clic en **Revisar + Crear**. Una vez que haya pasado la validación, haga clic en **Crear**.
 6. Una vez que se crean las dos puertas de enlace VPN, deben conectarse entre sí antes de que se pueda crear un túnel y el tráfico pueda fluir. Navegue de regreso a Virtual Network Gateways ingresando **Virtual Network Gateway** en el cuadro de búsqueda de nombre de recurso en la parte superior de Azure Portal, luego seleccione **Virtual Network Gateways** en el menú desplegable que se abre cuando comienza a escribir. Se abre la página Puertas de enlace de red virtual y se enumerarán las dos puertas de enlace

VPN nuevas. Haga clic en el nombre dado a la primera puerta de enlace VPN que creó; en este ejemplo, es VNet1GW. En la hoja de menú VNet1GW, haga clic en **Conexiones > Agregar** para comenzar a crear la conexión. Complete estas opciones:

- 0.■ **Nombre.** Ingrese un nombre único para la conexión; para este ejemplo, ingrese **VNet1-VNet2**.
- 1.■ **Tipo de conexión.** Deje este conjunto como **VNet-To-VNet**. Las otras dos opciones cubren soluciones locales a Azure.
- 2.■ **Segunda puerta de enlace de red virtual.** Seleccione **VNet2GW**.
- 3.■ **Clave compartida (PSK).** Se trata de una cadena aleatoria de letras y números que se utiliza para cifrar la conexión.
- 4.■ **Protocolo IKE.** Deje este conjunto como IKEv2 para VNet-to-VNet. IKEv1 puede ser necesario para algunas conexiones de sitio a sitio locales.
7. Haga **clic en Aceptar** para agregar la conexión.
8. Ahora debe crear una segunda conexión de VNet2 a VNet1 mediante el proceso descrito en el paso 6, esta vez eligiendo **VNetGW2**.
9. Navegue a la opción de menú **Conexiones** en VNet1GW. Compruebe que el **estado** de ambas conexiones esté **conectado**. Esto puede tardar un poco. Una vez que ambos están conectados, la conexión está lista para probar.
10. SSH a la VM en VNet 1 con la dirección IP pública. Ahora debería poder hacer ping a la máquina virtual en la red virtual 2. Si utilizó la plantilla ARM en el paso 1 de esta guía, el puerto 22 se abrirá para la red virtual 2 para probar SSH entre las dos máquinas virtuales. Este es un punto clave: los grupos de seguridad de red (NSG) definidos en la interfaz de red (NIC) o la subred seguirán funcionando a través de una conexión de red virtual a red virtual. Por lo tanto, es posible que deba configurar reglas de NSG para permitir que su tráfico fluya.

Nota Conexiones de puerta de enlace VPN

Azure Portal solo se puede usar para crear conexiones entre puertas de enlace VPN en la misma suscripción. Para conectar dos puertas de enlace VPN en diferentes suscripciones, use PowerShell; consulte <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-vnet-vnet-rm-ps>. Además, puede utilizar la CLI de Azure; consulte <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal>.

Implementar emparejamiento de redes virtuales

La ejecución de dos puertas de enlace VPN para conectar redes virtuales puede resultar bastante costosa, ya que cada puerta de enlace VPN se factura por hora junto con el tráfico de salida. Las conexiones de la puerta de enlace VPN también limitan el ancho de banda disponible, ya que todo el tráfico debe fluir a través de la puerta de enlace. El emparejamiento de redes virtuales es equivalente a una conexión de red virtual a redes virtuales mediante puertas de enlace VPN porque el emparejamiento también permite la comunicación de recursos entre redes virtuales. Sin embargo, con un emparejamiento de redes virtuales, el tráfico se enruta a través de direcciones IP privadas en la red troncal de Azure. Esto significa que el emparejamiento de redes virtuales ofrece una latencia más baja, una mayoropción de ancho de banda en comparación con VNet-to-VNet utilizando puertas de enlace VPN. Cuando el emparejamiento está dentro de la misma región, la latencia es la misma que dentro de una única red virtual. El emparejamiento de redes virtuales también es una opción de menor costo, ya que no se acumulan costos de puerta de enlace VPN; solo se acumulan las tarifas de entrada y salida. El emparejamiento de redes virtuales también puede conectar redes virtuales en regiones de Azure; esto se conoce como emparejamiento de redes virtuales globales.

La figura 1-50 muestra un patrón de arquitectura común (una topología de red de concentrador y radio) disponible para un arquitecto de Azure mediante la implementación del emparejamiento de redes virtuales.

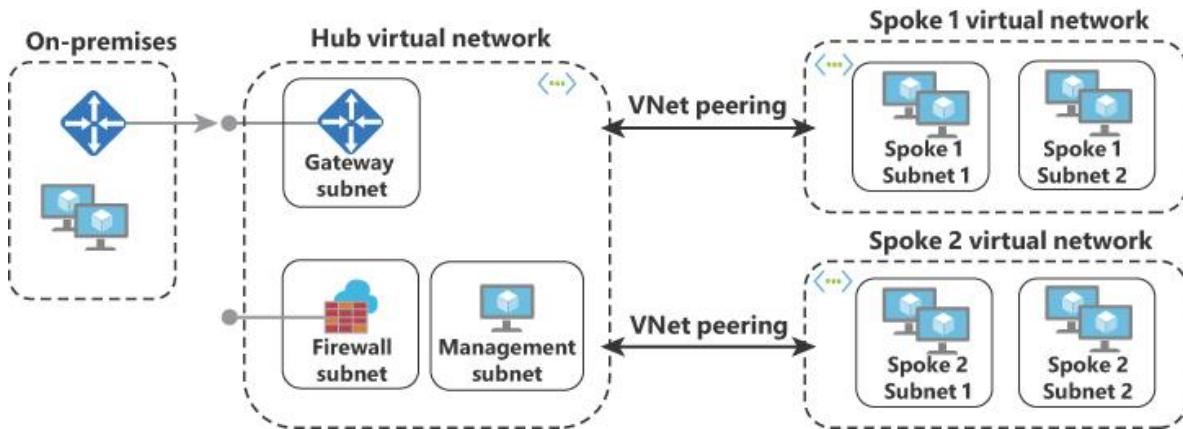


FIGURA 1-50 Emparejamiento de redes virtuales para crear una topología de red de concentrador y radio

En una topología de concentrador y radio, el concentrador es una red virtual y es el punto central; el concentrador contiene la conexión a su red local. La conexión desde las instalaciones al concentrador se puede realizar a través de una puerta de enlace de VPN o ExpressRoute. Un hub se utiliza a menudo para agrupar servicios compartidos que pueden ser utilizados por más de una carga de trabajo, como DNS o un dispositivo de seguridad (NVA).

Cada radio se conecta al concentrador mediante emparejamiento de redes virtuales; un radio puede estar en una suscripción diferente a la del concentrador. El intercambio de tráfico entre varias suscripciones se puede utilizar para superar los límites de suscripción. El intercambio de tráfico aísla las cargas de trabajo. Como se muestra en la [Figura 1-50](#), si Spoke 1 fuera para su departamento de desarrollo y Spoke 2 fuera para su departamento de producción, se aislarían y podrían administrarse por separado. Configurar radios de esta manera permite otra práctica arquitectónica: la separación de preocupaciones. [La Figura 1-50](#) muestra cómo los radios pueden comunicarse con el concentrador para usar servicios compartidos, pero no entre ellos.

Para ver parte de esta topología en acción, siga los siguientes pasos en Azure Portal para crear un emparejamiento de redes virtuales entre dos redes virtuales:

1. Cree dos máquinas virtuales (VM) Linux Azure, una en cada una de las siguientes configuraciones de redes virtuales y subredes:

1. ■ VNet1: 10.3.0.0/24 - subred 10.3.0.0/16

2. ■ VNet2: 10.4.0.0/24 - subred 10.4.0.0/16

Esta configuración garantiza que no haya superposición en los espacios de direcciones de VNet existentes, que es un requisito del emparejamiento de VNet. Asegúrese de que la máquina virtual en VNet1 tenga una dirección IP pública. Para ayudar a crear esta arquitectura, use la plantilla ARM de inicio rápido de Azure en <https://github.com/Azure/azure-quickstart-templates/tree/master/101-vm-sshkey>. Deberá editar la dirección y los prefijos de subred en consecuencia.

2. En Azure Portal, busque **vnet** en la barra de búsqueda en la parte superior y seleccione **Redes virtuales** en el menú desplegable que se muestra cuando comienza a escribir VNet. En la lista de redes virtuales que se muestra en la página **Redes virtuales**, seleccione **VNet1**.
3. Ahora puede configurar VNet1; en la hoja de menú a la izquierda de la hoja **Descripción general** que está abierta, desplácese hacia abajo, seleccione **Peerings** y haga clic en **Agregar**. Ahora debe ingresar los siguientes ajustes de configuración de emparejamiento:
 - 0.■ **Nombre del emparejamiento desde VNet1 a la red virtual remota.** Ingrese un nombre para su intercambio de tráfico; en este ejemplo, ingrese **Vnet1peerVNet2**.
 - 1.■ **Modelo de implementación de redes virtuales.** Elija **Resource Manager**. En el paso 1, creó una nueva red virtual con ARM o el portal; en este paso, está creando el modelo de Resource Manager.
 - 2.■ **Sé mi identificación de recurso.** Deje esto sin seleccionar. Si conoce el ID de recurso de la **red virtual a la que está emparejando**, puede seleccionar este cuadro e ingresar el ID en lugar de seleccionar la **suscripción** y la **red virtual**.
 - 3.■ **Suscripción.** Seleccione la suscripción en la que creó VNet2.
 - 4.■ **Red virtual.** Seleccione **VNet2**.
 - 5.■ **Nombre del emparejamiento de VNet1 a VNet2.** Ingrese **Vnet2peerVNet1**.

- 6.■ **Configure las opciones de acceso a la red virtual.** Deje ambos interruptores configurados en **Habilitado**. Esto permite que el tráfico fluya entre las dos redes virtuales.
 - 7.■ **Configure los ajustes del tráfico reenviado.** Deje ambos interruptores configurados en **Desactivado**. Esto bloquea el tráfico que no se origina desde dentro de la red virtual a la que se está emparejando para que no ingrese a la red virtual desde la que se origina el emparejamiento. Así es como se aísla el tráfico en los radios.
 - 8.■ **Permitir Gateway Transit.** Seleccione esta opción si la red virtual desde la que se está interconectando contiene una puerta de enlace VPN y desea usarla.
4. Haga clic en **Aceptar** para crear el emparejamiento.
 5. Cuando hace clic en **Aceptar**, vuelve a la hoja **Peering**s en el portal. Una vez que el **estado** de emparejamiento del emparejamiento que acaba de crear muestra **Conectado**, estará listo para probar la conexión.
 6. SSH a la VM en VNet 1 con la dirección IP pública. Ahora debería poder hacer ping a la máquina virtual en la red virtual 2. Si usó la plantilla ARM en el paso 1 de esta guía, el puerto 22 se abrirá para la red virtual 2 para probar SSH entre las dos máquinas virtuales. Este es un punto clave: los grupos de seguridad de red (NSG) definidos en la interfaz de red (NIC) o la subred seguirán funcionando a través de una conexión de red virtual a red virtual. Por lo tanto, es posible que deba configurar las reglas de NSG para permitir que su tráfico fluya.

HABILIDAD 1.6: IMPLEMENTAR AZURE ACTIVE DIRECTORY

Azure Active Directory (Azure AD) es la plataforma de identidad y gestión de acceso basada en la nube de Microsoft. En un nivel básico, Azure AD registra a los usuarios en Microsoft 365, Azure Portal y muchas otras aplicaciones Microsoft SaaS. Azure AD también puede iniciar sesión en las aplicaciones que ha creado en las instalaciones y en la nube.

Esta habilidad cubre cómo:

- [Agregar dominios personalizados](#)
- [Administrar varios directorios](#)
- [Implementar el restablecimiento de contraseña de autoservicio](#)
- [Configurar cuentas de usuario para MFA](#)
- [Configurar alertas de fraude](#)
- [Configurar opciones de derivación](#)
- [Configurar direcciones IP confiables](#)
- [Configurar métodos de verificación](#)
- [Implementar y administrar cuentas de invitados](#)
- [Configurar la protección de identidad de Azure AD](#)
- [Implementar el acceso condicional, incluido MFA](#)

La primera vez que un usuario de su organización se registra en un servicio Microsoft SaaS, se crea una instancia de Azure AD para su organización. Una instancia de Azure AD se denomina inquilino de Azure. Un inquilino de Azure tiene una relación de uno a varios con las suscripciones de Azure.

Azure AD viene en tres niveles y las características que se describen en esta habilidad pueden requerir el uso de los dos niveles premium, como se muestra en la [Tabla 1-3](#).

TABLA 1-3 Resumen de características de la capa de anuncios de Azure

	Libre	Premium P1
<i>Dominios personalizados</i>	sí	sí
<i>Usuarios invitados</i>	sí	sí
<i>Varios directorios</i>	sí	sí

	Libre	Premium P1
<i>Autenticación multifactor (MFA)</i>	Sí (para administradores)	sí
<i>Acceso condicional (con MFA)</i>		sí
<i>Autoservicio de restablecimiento de contraseñas: usuarios híbridos y en la nube</i>		sí
<i>Reseñas de acceso de invitados</i>		
<i>Protección de identidad de Azure</i>		
<i>Gestión de identidad privilegiada</i>		



La sugerencia del examen está aquí

Será beneficioso saber cuáles de las características descritas a lo largo de esta habilidad son gratuitas, las características P1 y P2.

Como arquitecto, debe tener una excelente comprensión de las características de Azure AD y cómo se pueden configurar. En esta habilidad, explorará estas configuraciones.

Agregar dominios personalizados

Cuando se crea el inquilino de Azure de una organización, se le asigna un nombre DNS público con el formato `tenantname.onmicrosoft.com`. El nombre del inquilino es generalmente el nombre de dominio de la organización; por ejemplo, `contoso.com` se convertiría en `contoso.onmicrosoft.com`. Aunque el nombre de dominio de su organización es parte del nombre DNS público, no es uno que sus empleados o sus clientes reconozcan como parte de su marca. Para asociar su dominio con su inquilino de Azure, deberá agregar un nombre de dominio personalizado. Puede agregar un nombre de dominio personalizado en Azure Portal. Siga estos pasos para probarlo:

1. Inicie sesión en Azure Portal y busque Azure **Active Directory** en la barra de búsqueda de recursos en la parte superior. Seleccione **Azure Active Directory** en los resultados de la búsqueda que se muestran en el menú desplegable mientras escribe el nombre del recurso. Ahora haga clic en **Nombres de dominio personalizados** en el menú a la izquierda de la página de **Azure Active Directory**. Aquí se enumeran los nombres de dominio asociados con su inquilino de Azure. Verá el `tenantname.onmicrosoft.com` en la lista.
2. Seleccione **Agregar dominio personalizado** en la parte superior de la página **Nombres de dominio personalizados**. Se le pedirá que ingrese un nombre de dominio. Este nombre de dominio debe ser uno que ya posea a través de un registrador de dominios; se muestra un ejemplo en la [Figura 1-51](#). Haz clic en **Agregar dominio**.
3. Ahora se muestran los ajustes necesarios para verificar su dominio. Debe agregar el registro TXT o MX al archivo de zona DNS. Si no tiene acceso a su registrador, puede elegir **Compartir estas configuraciones por correo electrónico**. Debe utilizar los valores exactos para que Microsoft pueda verificar que es el propietario del dominio. En la [Figura 1-51](#) se muestra un ejemplo. Una vez que se agrega el registro DNS en el registrador, haga clic en **Verificar**.
4. La página **Verificación exitosa** debería aparecer como se muestra en la [Figura 1-51](#). Si recibe un error, es posible que deba esperar a que se propaguen los cambios en el registro DNS antes de intentarlo una vez más. Si desea que este dominio recién agregado sea el predeterminado cuando se agreguen nuevos usuarios, haga clic en **Hacer principal** en la parte superior de la página de verificación exitosa. Su dominio ahora aparece en la página **Nombres de dominio personalizados** en Azure Portal.

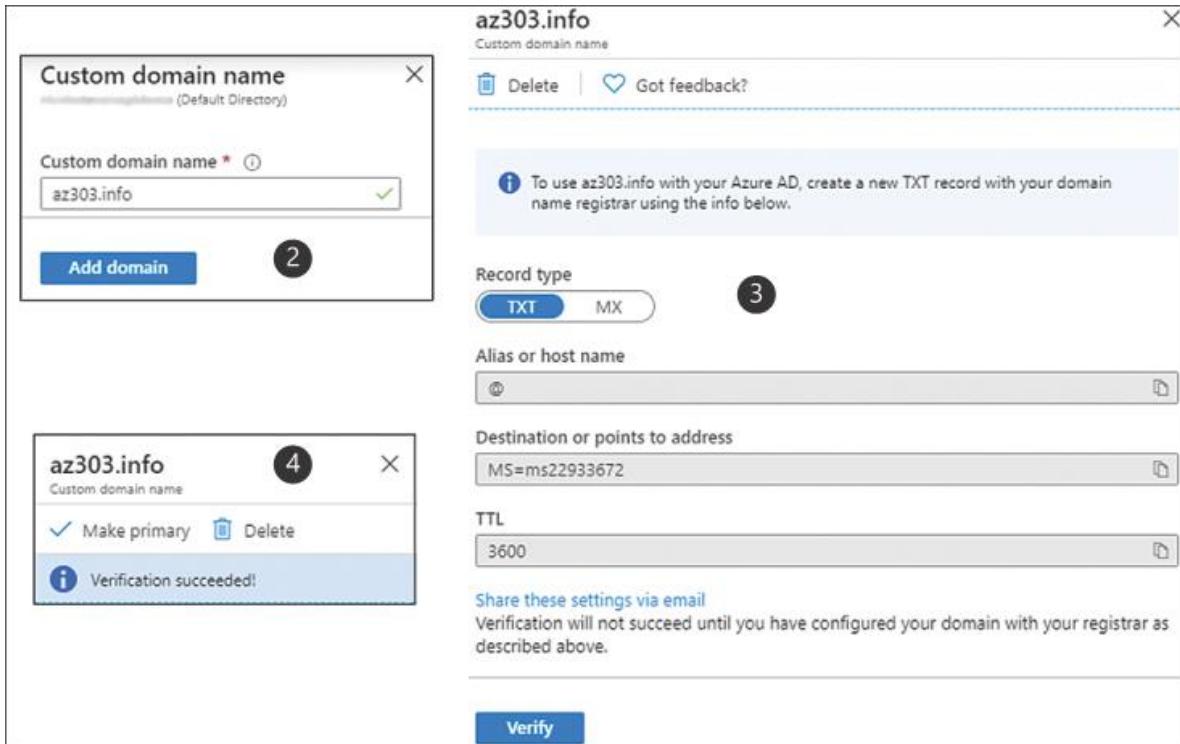


FIGURA 1-51 Los pasos para crear un dominio personalizado

Administrar varios directorios

Azure AD es un entorno multiusuario. Cada inquilino puede tener varias suscripciones y varios dominios, pero los inquilinos pueden tener solo un directorio. Un directorio es el servicio de Azure AD, que puede tener uno o más dominios. A un directorio se le pueden asignar varias suscripciones, pero nunca se puede asociar con más de un inquilino. Esta relación de uno a uno entre un inquilino y un directorio puede generar confusión con las palabras "inquilino" y "directorio" que se usan indistintamente sin explicación en la documentación y en el portal de Azure.

Puede tener varios directorios y una identidad puede tener permisos para acceder a varios directorios. Cada directorio es independiente de otro, incluido el acceso administrativo a directorios específicos. Si es administrador en un directorio, no tendrá privilegios de administrador en otro directorio a menos que se le otorguen. Puede utilizar varios directorios para separar su directorio activo de un directorio de prueba que se utiliza para explorar nuevas funciones o configuraciones.

Para crear un nuevo directorio, deberá crear un nuevo inquilino y buscar Azure **Active Directory** en la barra de búsqueda de nombre de

recurso en la parte superior de Azure Portal. Seleccione **Azure Active Directory** en el menú desplegable que se muestra a medida que escribe el nombre del recurso. Después de ingresar a **Azure Active Directory**, la **descripción general** se muestra de forma predeterminada en la hoja de menú. En la parte superior de Descripción general, haga clic en **Crear un inquilino**. Se le dirige a la página **Crear un inquilino**. Deje la opción **Tipo de directorio** en su configuración predeterminada de **Azure Active Directory** y haga clic en **Configuración** pestaña. Se muestra la Configuración del directorio, como se muestra en la Figura 1-52.

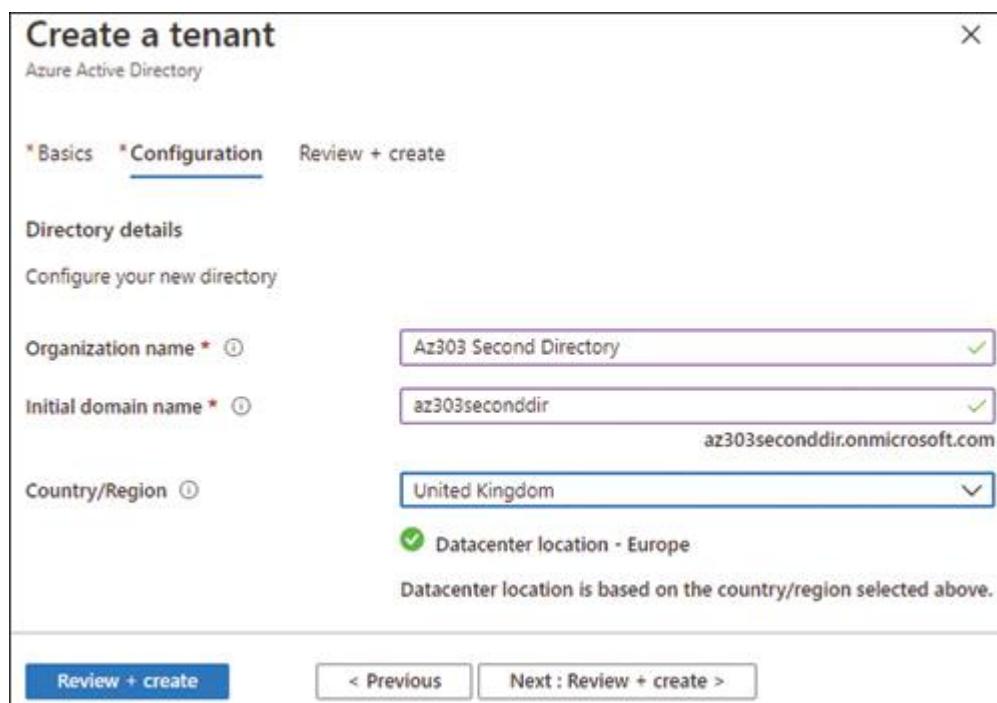


FIGURA 1-52 Configuración de un nuevo inquilino

Ingrese el **nombre de su organización** y un **nombre de dominio inicial**. Tenga en cuenta que el nombre de dominio está agregado. `.onmicrosoft.com`, como se describe en "Aregar dominios personalizados" anteriormente en este capítulo. La configuración de **Ubicación del centro de datos** tiene una importancia adicional si la información del usuario en este directorio está sujeta a la legislación local, por lo que la selección de **País / Región** debe reflejar esto. Haga clic en **Revisar + Crear** para crear el nuevo inquilino.

Su identidad de inicio de sesión ha creado el nuevo inquilino y, por lo tanto, un nuevo directorio. Azure también ha asignado automáticamente sus derechos de administrador global de identidad para el nuevo directorio como la identidad que creó el inquilino. Para acceder al nuevo directorio, deberá cambiar a él. Vaya a la hoja **Descripción general** de Azure Active Directory y haga clic en **Cambiar inquilino** en la parte superior. Esto abre la hoja **Cambiar inquilino**, que le brinda la opción de cambiar a un nuevo inquilino haciendo clic en él o de establecer inquilinos como favoritos.

También puede cambiar de directorio haciendo clic en el avatar de su identidad en la parte superior derecha del portal y eligiendo **Cambiar de directorio**. Esto abre la hoja **Directorio + Suscripción**, que tiene las siguientes opciones:

- ■ Seleccione un directorio al que cambiar
- ■ Establecer un directorio de Azure AD predeterminado
- ■ Establecer directorios favoritos, haciéndolos más fáciles de encontrar si administra varios inquilinos de Azure AD

Implementar el restablecimiento de contraseña de autoservicio

Cualquier arquitecto que haya trabajado en una mesa de soporte sabrá que las llamadas para restablecer las contraseñas de los usuarios en las instalaciones pueden llevar bastante tiempo. Se estima que el restablecimiento de contraseña representa el 20 por ciento del gasto en TI de una organización. Al diseñar soluciones para la cantidad de usuarios a los que se les podría dar acceso a una aplicación en la nube, querrá que los usuarios restablecer sus propias contraseñas. El restablecimiento de contraseña de autoservicio (SSPR) permite a los usuarios restablecer sus propias contraseñas sin tener que ponerse en contacto con una función de soporte. Un usuario puede cambiar su contraseña con cualquier nivel de Azure AD. Sin embargo, el uso de SSPR requiere un nivel premium o la activación de una prueba. Una vez que se haya activado un nivel premium, siga estos pasos para habilitar SSPR en Azure Portal:

1. Busque **Azure Active Directory** en la barra de búsqueda de nombres de recursos en la parte superior de Azure Portal. Tenga en cuenta que en la página **Información general**, el **inquilino** ahora

es Azure AD Premium P1 o P2 . Haga clic en **Restablecer contraseña** en la hoja del menú.

2. La opción **Restablecimiento de contraseña de autoservicio habilitado** tiene el valor predeterminado **Ninguno** . Ningún usuario del directorio puede utilizar SSPR. Si cambia esto a **Seleccionado** , los administradores pueden especificar qué grupos de usuarios pueden usar SSPR. Si elige **Todo** , SSPR se habilitará para todos los usuarios del directorio.

3. Haga clic en **Guardar** .

Una vez que SSPR esté ahora habilitado, Azure asignará valores predeterminados a la configuración de SSPR. Como arquitecto, debe comprender cómo los valores predeterminados afectan las experiencias de sus usuarios. En la hoja de menú **Restablecimiento de contraseña** , elija **Métodos de autenticación** .

Tenga en cuenta que se seleccionan **Correo electrónico y Teléfono móvil** porque son los métodos de autenticación que estarán disponibles para sus usuarios. Además, puede elegir **Aplicación móvil** o **Teléfono de oficina** , y puede configurar **Preguntas de seguridad** . Ahora haga clic en **Registro** . El control deslizante para **Requerir que los usuarios se registren antes de iniciar sesión** se estableció en **Sí** cuando SSPR estaba habilitado. Esta configuración obliga a los usuarios a configurar SSPR por sí mismos en sus primeros inicios de sesión. El **número de días antes de que se solicite a los usuarios que vuelvan a confirmar su información de autenticación** El ajuste predeterminado es 180 días. Este es el número de días antes de que se le solicite al usuario que vuelva a confirmar su información SSPR. Haga clic en **Notificaciones** . La **Notificar a los usuarios sobre el restablecimiento de contraseña** tiene el valor predeterminado **Sí** . Esta configuración enviará un correo electrónico a los usuarios cuando restablezcan sus propias contraseñas. ¿Si elige **Notificar a todos los administradores cuando otros administradores restablezcan su contraseña**? Se enviará un correo electrónico a todos los administradores cuando un administrador restablezca su propia contraseña.

La última opción en el menú de **restablecimiento de contraseña** es **Integración local** . Esto se usa junto con identidades híbridas. Explorará esto en "Habilidad 1.7: Implementar y administrar identidades híbridas".

Nota SSPR y Azure AD Premium

Se requiere Azure AD Premium para el usuario SSPR. De forma predeterminada, los administradores están habilitados para SSPR en todos los niveles de Azure AD.

Sus usuarios pueden configurar el restablecimiento de contraseña de autoservicio a través del portal Mis aplicaciones. Para ver el proceso SSPR, agregue un nuevo usuario al directorio en el que acaba de habilitar SSPR. Asegúrese de que el usuario tenga establecida una ubicación de uso, que es un requisito para la asignación de una licencia de Azure AD Premium. Asigne una licencia AD Premium al usuario y utilice el nuevo usuario para iniciar sesión en el portal de Mis aplicaciones (<https://myapps.microsoft.com>). Ahora, siga estos pasos (que también son los pasos que comunicaría a sus usuarios):

1. En la esquina superior derecha del portal **Mis aplicaciones**, haga clic en el avatar y luego seleccione **Perfil > Configurar el restablecimiento de contraseña de autoservicio**.
2. Tiene la opción de configurar un número de teléfono o una dirección de correo electrónico para restablecer la contraseña. Elija **Configurar ahora** junto a **Autenticación El teléfono no está configurado** para configurar el restablecimiento de contraseña basado en el teléfono.
3. Elija el país donde está registrado su teléfono e ingrese su número de teléfono.
4. Haz clic en **Envíame un mensaje de texto** o **Llámame** para elegir un método de verificación.
5. Microsoft te enviará un mensaje de texto o te llamará con un código de verificación, según el método elegido en el Paso 4. Ingresa este código de verificación en el cuadro junto a **Verificar** y luego **haz clic en Verificar**.
6. Opcionalmente, puede optar por verificar una dirección de correo electrónico. Sus usuarios solo necesitan utilizar uno de los métodos de verificación que elijan.
7. Haga clic en **Finalizar**.

Nota MY Portal de aplicaciones

Microsoft ha lanzado un nuevo portal de Mis aplicaciones al que se puede acceder a través de (<https://myapplications.microsoft.com>). Se accede a SSPR mediante Ver cuenta, a la que se puede acceder a través del avatar del usuario en el portal de mi aplicación. El restablecimiento de la contraseña es como se describe anteriormente, ya que el nuevo portal redirige al usuario a las mismas páginas.

Cuando sus usuarios inicien sesión en una aplicación protegida por Azure AD, ahora verán **Mi contraseña olvidada** en el campo **Contraseña**. Si el usuario ha completado los pasos de configuración anteriores y se le ha asignado una licencia premium, el usuario podrá restablecer su propia contraseña. Los pasos para restablecer una contraseña se muestran en la [Figura 1-53](#).

¿Necesita más revisión? Restablecimiento de contraseña de autoservicio (SSPR)

Para obtener información sobre cómo habilitar e implementar el restablecimiento de contraseña de autoservicio, visite el artículo de Microsoft Docs "Cómo funciona: restablecimiento de contraseña de autoservicio de Azure AD" en <https://docs.microsoft.com/en-us/azure/active-directory/autentication/concepto-sspr-howitworks>. Para obtener más información, también debe revisar las secciones de restablecimiento de contraseña.

Nota SSPR y almacenamiento en caché del navegador

Si los usuarios no recogen los cambios en el nivel de Azure AD y las asignaciones de licencias, es probable que su navegador esté almacenando en caché tokens antiguos. Borre su historial y vuelva a intentarlo.

Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

User ID:
suptest@az303.info
Example: user@contoso.onmicrosoft.com or user@contoso.com

Enter the characters in the picture or the words in the audio.

HG SVH

Next Cancel

1

Microsoft

Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

Send a text to my mobile phone number
 Call my mobile phone number

In order to protect your account, we need you to enter your complete mobile phone number (+*****37) below. You will then receive a text message with a verification code which can be used to reset your password.

+ +37

Text Cancel

2

Microsoft

Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

Send a text to my mobile phone number
 Call my mobile phone number

We've sent a text message to your phone number containing a verification code.

014000

Next Try again Contact your administrator Cancel

3

Microsoft

Get back into your account

verification step 1 > choose a new password

* Enter new password:

strong

* Confirm new password:

Finish Cancel

4

FIGURA 1-53 Pasos para restablecer la contraseña de autoservicio del usuario

1. El inicio de sesión del usuario se copia en el campo **ID de usuario**. El usuario debe ingresar el texto CAPTCHA. Haga clic en **Siguiente**.
2. El restablecimiento de contraseña para un número de teléfono se habilitó en la sección anterior. El usuario puede elegir ser llamado o recibir un código de verificación por mensaje de texto. Si también se hubiera habilitado la verificación por correo electrónico, vería una opción para eso. Deje esto configurado como **Enviar un mensaje de texto** e ingrese el número de teléfono que se verificó previamente. Haz clic en **Texto**.

3. Microsoft envía un código de verificación; intodúzcalo en el cuadro y haga clic en **Siguiente**.
4. El usuario ahora puede elegir una nueva contraseña. El usuario hará clic en **Finalizar** una vez que se complete el restablecimiento de la contraseña.



Punta de examen SSPR

Asegúrese de tener un buen conocimiento de los métodos de autenticación SSPR, el registro y las notificaciones.

Configurar cuentas de usuario para MFA

Sus usuarios viven en un mundo multiplataforma y multidispositivo. Pueden conectarse a aplicaciones dentro y fuera de la red de su organización con teléfonos, tabletas y PC, a menudo desde múltiples plataformas. Esta flexibilidad significa que el uso de contraseñas ya no es suficiente para proteger las cuentas de sus usuarios. La autenticación multifactor de Azure (MFA) proporciona una capa adicional de seguridad en forma de un método de autenticación secundario conocido como verificación en dos pasos. Este método secundario requiere que el usuario proporcione "algo que tiene", que a menudo tiene la forma de un token proporcionado por SMS o una aplicación de autenticación.

Como arquitecto, debe saber cómo habilitar MFA en Azure AD y cómo configurar la configuración de MFA para su caso de uso. Hay cuatro formas principales de habilitar MFA para un usuario en Azure AD:

- ■ **Habilitar cambiando de estado.** Los usuarios deben realizar MFA cada vez que inician sesión.
- ■ **Habilitar por valores predeterminados de seguridad.** Ajustes de seguridad preconfigurados por Microsoft, incluido MFA.
- ■ **Habilitar mediante la política de acceso condicional.** Este es un método más flexible y de dos pasos que se requiere para ciertas condiciones. Este método requiere licencias premium de Azure AD.

- **Habilitado por Azure AD Identity Protection.** Se requieren dos pasos según el riesgo de inicio de sesión. Este método requiere licencias premium P2 Azure AD.

En esta sección, verá la habilitación cambiando el estado y la habilitación mediante los métodos predeterminados de seguridad. Los demás se tratan más adelante en esta habilidad. Tenga en cuenta que el método de habilitación por cambio de estado también se conoce como "MFA por usuario". Para habilitar la MFA por usuario, navegue hasta la parte superior de Azure Portal y busque **Azure Active Directory** en la barra de búsqueda de nombres de recursos en la parte superior de Azure Portal. Seleccione **Azure Active Directory** en el menú desplegable que se muestra a medida que escribe el nombre del recurso y, a continuación, siga estos pasos para configurar MFA por usuario cambiando el estado de un usuario:

1. Azure AD se abre con **Descripción general** seleccionada en el menú de **Azure Active Directory**. Haz clic en **Usuarios**.
2. Hacia la parte superior de la hoja **Todos los usuarios** se encuentra el menú **Gestión de usuarios**. Haga clic en los puntos suspensivos a la derecha de este menú y elija **Autenticación multifactor**.
3. Seleccione los usuarios para los que desea habilitar MFA. Si hay muchos usuarios para los que necesita habilitar o deshabilitar MFA al mismo tiempo, puede usar la función **Bulk Update** para cargar un archivo CSV de usuarios para habilitar / deshabilitar, como se muestra en la [Figura 1-54](#).

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
AZ303 82B	az303.b2b@gmail.com	Disabled
AZ303 Guest	az303.guest@protonmail.com	Disabled
globaladmin	globaladmin@az303.info	Disabled
<input checked="" type="checkbox"/> MFA Test	mfatatest@az303.info	Disabled
<input type="checkbox"/> Power User	poweruser@az303.info	Disabled
<input checked="" type="checkbox"/> SSPR Test	ssprtest@az303.info	Disabled

FIGURA 1-54 Habilitación de MFA para usuarios finales

4. En la sección **Pasos rápidos**, haga clic en **Habilitar** y luego en **Habilitar autenticación multifactor** en la ventana emergente.
5. Volverá a la lista de usuarios; el **Estado de autenticación multifactor** para los usuarios que habilitó ahora está configurado como **Habilitado**. Hay tres estados de usuario para MFA:
 1. ■ **Discapacitado.** No se ha habilitado MFA.
 2. ■ **Habilitado.** MFA está habilitado, pero el usuario no se ha registrado.
 3. ■ **Cumplida.** MFA está habilitado y el usuario se ha registrado.

MFA ahora está configurado y, en el próximo inicio de sesión del usuario habilitado, se le pedirá que se registre en MFA.

El uso del método descrito anteriormente para cambiar el estado de un usuario para administrar MFA tiene algunos inconvenientes. Si tú estudias [Figura 1-54](#), puede que esta pantalla no se haya integrado con el portal de Azure. Por tanto, la experiencia administrativa es diferente, lo que puede resultar confuso. La falta de integración con Azure Portal también significa que no puede usar el control de acceso basado en roles para otorgar acceso para administrar MFA por usuario. Solo los administradores globales pueden acceder a MFA por usuario, y es poco probable que esto se adhiera al principio de privilegio mínimo en la mayoría de las organizaciones. La habilitación de MFA por usuario también habilita las contraseñas de aplicaciones, que son una forma heredada de autenticación en la que la contraseña de la aplicación se almacena de forma segura en el dispositivo que utiliza la aplicación. Las contraseñas de aplicaciones se utilizan para aplicaciones heredadas que no pueden admitir MFA, donde la aplicación devuelve la contraseña de la aplicación al servicio en la nube de Microsoft y se omite MFA.

- ■ Si su organización no tiene licencias de Azure AD de nivel premium y la MFA por usuario no se ajusta a los requisitos de su organización, también tiene la opción de usar el método habilitar por valores predeterminados de seguridad. Microsoft ha creado un conjunto de configuraciones de seguridad preconfiguradas para proteger a las organizaciones contra ataques como suplantación de identidad (phishing), rociado de contraseñas y

reproducción. Estas configuraciones están agrupadas con los valores predeterminados de seguridad:

- Todos los administradores de Azure AD con acceso privilegiado deben realizar MFA en cada inicio de sesión. Esto incluye las siguientes funciones administrativas: Global, SharePoint, Exchange, Acceso condicional, Seguridad, Helpdesk, Facturación, Usuario y Autenticación.
- Todos los usuarios deben registrarse para MFA. La MFA para usuarios no administrativos se realiza cuando es necesario, como acceder a un servicio a través de un nuevo dispositivo o cuando caduca el token de actualización del usuario.
- Se requiere MFA para cualquier usuario que acceda a la API de Azure Resource Manager a través de Azure Portal, PowerShell o CLI.
- Los protocolos de autenticación heredados, como las contraseñas de aplicaciones, están bloqueados.

Una vez habilitados, todos los valores predeterminados de seguridad enumerados anteriormente se aplican automáticamente al inquilino y no puede elegir un subconjunto de ellos. Los valores predeterminados están completamente administrados por Microsoft, lo que significa que también pueden estar sujetos a cambios.

Para habilitar los valores predeterminados de seguridad, navegue hasta la parte superior de Azure Portal y busque Azure **Active Directory** en la barra de búsqueda de nombres de recursos en la parte superior de la página. Seleccione **Azure Active Directory** en el menú desplegable que se muestra mientras escribe el nombre del recurso y siga estos pasos para habilitar los valores predeterminados de seguridad:

1. Azure AD se abre con **Descripción general** seleccionada en el menú de **Azure Active Directory**. En el mismo menú, haga clic en **Propiedades**.
2. En la parte inferior de la página **Propiedades**, haga clic en **Administrar valores predeterminados de seguridad**. Los **Permitir valores predeterminados de seguridad** de la cuchilla aparece.
3. En la hoja **Habilitar valores predeterminados de seguridad**, habilite **Habilitar valores predeterminados de**

seguridad moviendo el control deslizante a **Sí** y haga clic en **Guardar**.

Tenga en cuenta los valores predeterminados de seguridad

Si su inquilino se creó después de octubre de 2019, es posible que los valores predeterminados de seguridad ya estén habilitados para su inquilino. Los valores predeterminados de seguridad no se pueden habilitar si su inquilino tiene habilitada al menos una política de acceso condicional. Consulte "Implementar el acceso condicional, incluido MFA", más adelante en este capítulo para obtener información sobre las políticas de acceso condicional.

¿Necesita más revisión? Autenticación multifactor de Azure

Para obtener información sobre cómo habilitar e implementar Azure Multi-Factor Authentication, visite el artículo de Microsoft Docs "**¿Qué son los valores predeterminados de seguridad?**" En <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults> y "**Configure Azure Multi-Factor Authentication**" en <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>. Tenga en cuenta que el segundo artículo también se recomienda para las siguientes cuatro secciones.

Configurar alertas de fraude

Si se accede de forma fraudulenta a una cuenta de usuario protegida por MFA, se contactará a los usuarios a través de sus métodos de verificación, aunque no hayan iniciado el acceso. Esto permite a los usuarios saber que se está produciendo un intento de inicio de sesión fraudulento. Al configurar las alertas de fraude, permite a los usuarios informar automáticamente sobre intentos fraudulentos y bloquear sus cuentas para evitar más intentos de acceso. Para configurar alertas de fraude, abra Azure Portal y siga estos pasos:

1. Buscar **Azure Active Directory** en el buscador nombre del recurso en la parte superior del portal y pulse ENTER para seleccionar **Azure Active Directory** desde el menú desplegable que aparece al escribir el nombre del recurso.

2. Haga clic en **Seguridad** en la hoja de menú y luego haga clic en **MFA** en la hoja de **Seguridad**. Haga clic en **Alerta de fraude** en la hoja **MFA**.
3. Se abre la hoja **Alerta de fraude**, como se muestra en la Figura 1-55. Para habilitar las alertas de fraude, configure **Permitir a los usuarios enviar alertas de fraude** en **Activado**.

The screenshot shows the 'Fraud alert' configuration page in the Azure portal. The left sidebar lists various MFA-related options like 'Getting started', 'Diagnose and solve problems', 'Settings' (which is selected), 'Account lockout', 'Block/unblock users', 'Fraud alert' (which is also selected), 'Notifications', 'OATH tokens', 'Phone call settings', 'Providers', 'Manage MFA Server', 'Server settings', 'One-time bypass', 'Caching rules', 'Server status', 'Reports', 'Activity report', 'Troubleshooting + Support', and 'New support request'. The main content area is titled 'Fraud alert' and contains the following settings:

- Fraud alert**: A description stating "Allow your users to report fraud if they receive a two-step verification request that they didn't initiate."
- Allow users to submit fraud alerts**: A toggle switch set to **On**.
- Automatically block users who report fraud**: A toggle switch set to **On**.
- Code to report fraud during initial greeting**: A text input field containing "Default fraud code is 0".

FIGURA 1-55 Habilitación de alertas de fraude para MFA en Azure Portal

4. **Bloquear automáticamente usuarios que informan Fraude** se establece en **On** por defecto. Esto bloqueará la cuenta del usuario durante 90 días o hasta que un administrador pueda desbloquearla.
5. **El código para informar fraude durante el saludo inicial** está configurado en 0 de forma predeterminada. Esto permite que los usuarios que utilizan la verificación de llamadas denuncien fraudes.

6. Haga clic en **Guardar** en la parte superior de la página **Alerta de fraude**. Las alertas de fraude ahora están configuradas.

El usuario puede activar la alerta de fraude cuando utiliza la aplicación Authenticator (consulte “Configurar métodos de verificación” más adelante en este capítulo) o mediante la verificación de llamada. Si la cuenta de un usuario se bloquea al activar una alerta de fraude, un administrador debe desbloquear al usuario antes de que pueda iniciar sesión nuevamente. Para desbloquear a un usuario, siga estos pasos:

1. Buscar **azul directorio activo** en la barra de búsqueda de nombre de recurso en la parte superior del portal y pulse Enter para seleccionar **Azure Active Directory**.
2. Haga clic en **Seguridad** en la hoja **Menú** y luego haga clic en **MFA** en la hoja **Seguridad**. En la hoja **MFA**, haga clic en **Bloquear / Desbloquear usuarios**. En la [Figura 1-56](#) se muestra una lista de usuarios bloqueados .

The screenshot shows a table titled 'Blocked users' with the following data:

User	Reason	Date	Action
mfatest@az303.info	User blocked their account from the mobile app	09/10/2020, 8:57:09 AM	Unblock

FIGURA 1-56 Desbloqueo de un usuario cuyo inicio de sesión fue bloqueado después de activar una alerta de fraude

3. Haga clic en **Desbloquear**, ingrese una **Razón para desbloquear** y haga clic en **Aceptar**. El usuario ahora está desbloqueado.

Si un usuario activa una alerta de fraude, se envía una notificación por correo electrónico a todas las direcciones de correo electrónico que se han agregado a la sección de configuración de **Notificaciones** de la página **Autenticación** multifactor. Esta sección se encuentra en el elemento **del menú Seguridad** para **Azure Active Directory**.

Configurar opciones de derivación

La verificación en dos pasos depende en gran medida de que el usuario pueda recibir la notificación del código a través de mensajes SMS o llamadas telefónicas. Es posible que estas notificaciones no sean posibles, por ejemplo, si una de las instalaciones de su organización está bajo tierra o si el usuario ha perdido su teléfono. En este caso, debe recomendar una forma segura de omitir MFA. En Azure MFA, esto se logra con una omisión única que permite a un administrador configurar una breve ventana durante la cual un usuario puede iniciar sesión solo con su contraseña. Para ver esta característica en acción, siga estos pasos en Azure Portal:

1. Busque **Azure Active Directory** en el cuadro de búsqueda de nombre de recurso en la parte superior del portal y presione Entrar para seleccionar Azure Active Directory.
2. Haga clic en **Seguridad** en la hoja de menú y luego haga clic en **MFA** en la hoja de **Seguridad**. Haga clic en **Omisión única** en la hoja **MFA**.
3. Tenga en cuenta que los **segundos de omisión únicos predeterminados** están configurados en **300**, lo que significa que cada usuario tiene 5 minutos para completar su inicio de sesión.
4. Haga clic en **Agregar**.
5. En el campo **Usuario**, agregue la dirección de correo electrónico del usuario que se está utilizando para iniciar sesión. Puede anular el tiempo de omisión en el cuadro **Segundos** (posiblemente a algo más corto). En **Razón**, proporcione una razón para el desvío, como "Trabajar bajo tierra".
6. Haga clic en **Aceptar**. El usuario al que se le otorgó una omisión única se agrega a la lista **Usuarios omitidos**, como se muestra en la Figura 1-57.

The screenshot shows the 'Multi-Factor Authentication | One-time bypass' page in the Azure portal. On the left, there's a sidebar with various navigation links like 'Getting started', 'Diagnose and solve problems', 'Settings', 'Account lockout', etc. The main content area has a heading 'One-time bypass' with a description: 'Allow a user to authenticate without performing two-step verification for a limited time. The bypass goes into effect immediately, and expires after the specified number of seconds. This feature only applies to MFA Server deployment.' Below this is a section 'Default one-time bypass seconds' with a input field set to '300'. Underneath is a table titled 'Bypassed users' showing one entry: 'User: mfatatest@az303.info, Reason: Underground working, Date: 09/10/2020, 9:11:31 AM, Seconds: 300, Action: Cancel'.

FIGURA 1-57 La cuchilla de derivación de una sola vez

Tenga en cuenta que un administrador también puede cancelar la solicitud antes de que expire el tiempo, como se muestra en la [Figura 1-57](#).

Configurar direcciones IP confiables

A lo largo de las últimas tres secciones, ha estado explorando la configuración de Azure MFA mediante el método enable by change state. Este método requiere que el usuario verifique en dos pasos cada inicio de sesión que realice. Si un usuario inicia sesión desde una estación de trabajo dentro de la intranet de su organización, es muy probable que este sea un intento de acceso válido. Si configura una IP confiable para esta ubicación, se omitirá la verificación de dos pasos para cada inicio de sesión iniciado desde esa IP. Para habilitar direcciones IP de confianza mediante la configuración del servicio Azure MFA, siga los siguientes pasos en Azure Portal:

1. Buscar **Azure Active Directory** en el buscador nombre del recurso en la parte superior del portal y pulse Enter para seleccionar **Azure Active Directory**.
2. Haga clic en **Usuarios** en la hoja del menú y luego haga clic en los puntos suspensivos en el menú superior. Haga clic en **Autenticación multifactor** en el menú desplegable.
3. Se abre la página **Autenticación multifactor** en la pestaña **Usuarios**. Haga clic en la pestaña **Configuración del servicio** para abrir

la página **Configuración del servicio**, como se muestra en la Figura 1-58.

The screenshot shows the 'multi-factor authentication' section of the 'users service settings' page. It includes options for 'app passwords', 'trusted ips', 'verification options', and 'remember multi-factor authentication'. A 'save' button and links for 'Manage advanced settings and view reports' and 'Go to the portal' are at the bottom.

multi-factor authentication

users service settings

app passwords (learn more)

Allow users to create app passwords to sign in to non-browser apps
 Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets:
40.126.9.98/32

verification options (learn more)

Methods available to users:

Call to phone
 Text message to phone
 Notification through mobile app
 Verification code from mobile app or hardware token

remember multi-factor authentication (learn more)

Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-365):

save

Manage advanced settings and view reports Go to the portal

FIGURA 1-58 Configuración de IP confiables para MFA en la página Configuración del servicio

4. En el cuadro **IP de confianza**, agregue la dirección IP o el rango de direcciones utilizando la notación CIDR. El ejemplo de la Figura 1-58 establece una única dirección IP. El **Saltar multi-factor de autenticación para las peticiones de los Federados Originario de usuarios desde Mi Intranet** es que las organizaciones que utilizan inicio de sesión único (SSO) a través de Active Directory Federation Services (AD FS).

5. Haga clic en **Guardar** y luego en **Cerrar** en la pantalla **Actualizaciones exitosas**. La IP de confianza ahora está configurada.

Tenga en cuenta las direcciones IP de confianza

Este método de IP confiables solo es compatible con IPv4.



Sugerencia para el examen MFA e IP de confianza

Este método para configurar direcciones IP confiables no es el método recomendado por Microsoft. La configuración recomendada se describe en la sección "Implementar el acceso condicional, incluido MFA", más adelante en este capítulo. Por lo tanto, si una pregunta involucra direcciones IP confiables, es probable que se trate de acceso condicional.

Configurar métodos de verificación

Hasta ahora, en esta habilidad, ha visto los SMS y las llamadas telefónicas como los métodos principales para la segunda parte de la verificación en dos pasos. Estos son los valores predeterminados que se dan a los usuarios cuando se registran en MFA. Sin embargo, hay cuatro métodos de verificación disponibles para un usuario:

- **Llamar al teléfono.** Una llamada telefónica automatizada. El usuario presiona # en el teclado para verificar el inicio de sesión.
- **Mensaje de texto al teléfono.** Envía un código de verificación en un mensaje de texto. El usuario ingresa el código en la pantalla de inicio de sesión cuando se le solicita que verifique el inicio de sesión.
- **Notificación a través de la aplicación móvil.** Envía una notificación de inserción a la aplicación Microsoft Authenticator en el móvil del usuario. El usuario elige **Verificar** en la notificación.
- **Código de verificación de la aplicación móvil o token de hardware.** Se genera un código OATH en la aplicación Microsoft Authenticator cada 30 segundos. El usuario ingresa

este código en la pantalla de inicio de sesión cuando se le solicita que verifique el inicio de sesión.

De forma predeterminada, los cuatro métodos de verificación están disponibles para un usuario cuando MFA está habilitado. Sin embargo, un usuario debe optar por habilitar específicamente el uso de la aplicación Microsoft Authenticator a través del portal Mis aplicaciones. Para ver cómo funciona este proceso, agregue un usuario a Azure AD y use las credenciales de este usuario para iniciar sesión en el portal de Mis aplicaciones (<https://myapplication.microsoft.com>). Ahora siga estas instrucciones dentro de Mis aplicaciones:

1. Haga clic en el avatar en la parte superior derecha y luego seleccione **Ver cuenta**.
2. Se muestra la página **Perfil** para el usuario que inició sesión. Haga clic en **Verificación de seguridad adicional** en el widget de **información de seguridad** de la parte superior derecha.
3. Se le pedirá al usuario que inicie sesión nuevamente como medida de seguridad adicional.
4. El usuario puede configurar su método de verificación preferido en la parte superior de la página. En la sección **Cómo le gustaría responder**, el usuario puede seleccionar entre los métodos de verificación que se han habilitado para MFA.
5. Una vez que el usuario haya completado sus elecciones, haga clic en **Guardar** y se le pedirá que inicie sesión y verifique una vez más para guardar los cambios.

Para configurar los métodos de verificación disponibles para un usuario, siga estos pasos en Azure Portal:

1. Buscar **azul directorio activo** en la barra de búsqueda de nombre de recurso en la parte superior del portal y pulse Enter para seleccionar **Azure Active Directory**.
2. Haga clic en **Usuarios** en la hoja del menú y luego haga clic en los puntos suspensivos en el menú superior. Haga clic en **Autenticación multifactor** en el menú desplegable.
3. Se abre la página **Autenticación** multifactor en la pestaña **Usuarios**. Haga clic en **Configuración del servicio** para abrir la página **Configuración del servicio**.

4. El cuadro **Opciones de verificación** en la pestaña **Configuración del servicio** muestra los métodos de verificación disponibles. Seleccione o anule la selección de las opciones según sea necesario.
5. Haga clic en Guardar y luego en **Cerrar** en la pantalla **Actualizaciones exitosas**. Los métodos de verificación actualizados ahora están configurados.

Implementar y administrar cuentas de invitados

Azure AD brinda acceso de invitado a su inquilino con la colaboración de empresa a empresa (B2B) de Azure AD. A través de Azure AD B2B, el acceso a servicios y aplicaciones se puede compartir de forma segura. Los usuarios externos no tienen que ser parte de Azure AD; pueden utilizar sus propias soluciones de identidad, lo que significa que no hay gastos generales para los equipos de TI de su organización. La adición de usuarios invitados a Azure AD se realiza mediante invitación a través de Azure Portal. Para explorar cómo funciona esto, siga estos pasos:

1. Buscar **azul directorio activo** en la barra de búsqueda de nombre de recurso en la parte superior del portal y pulse Enter para seleccionar **Azure Active Directory**.
2. En la hoja de menú de **Azure AD**, haga clic en **Usuarios > Nuevo usuario invitado**.
3. Ahora puede ingresar la información del usuario invitado:
 1. ■ **Nombre.** El nombre y apellido del usuario invitado.
 2. ■ **Dirección de correo electrónico (obligatorio).** La dirección de correo electrónico del usuario invitado. Aquí es donde se envía la invitación.
 3. ■ **Mensaje personal.** Incluya un mensaje de bienvenida personal para el usuario invitado.
 4. ■ **Grupos.** Puede agregar el usuario invitado a cualquier grupo de Azure AD existente.
 5. ■ **Rol de directorio.** Asignación directa de permisos administrativos si es necesario.
4. Una vez que esté satisfecho de que las credenciales de invitado sean correctas, haga clic en **Invitar**.

5. Volverá a la lista de todos los usuarios de su inquilino. Mire la fila del usuario invitado que acaba de agregar. El **Tipo de usuario** se establece en **Invitado** y el **Origen** se establece en **Usuario invitado**, como puede ver en la Figura 1-59. En este ejemplo, el usuario invitado invitado es az303.guest@protonmail.com. En la columna **Fuente** que se muestra en la Figura 1-60, se muestra un valor de **Usuario invitado**, que muestra que el usuario aún no ha aceptado la invitación y no ha iniciado sesión.
6. El usuario recibe un correo electrónico de invitación con un enlace **Comenzar**. El usuario inicia sesión con las credenciales de la cuenta de Microsoft del mismo nombre de usuario o se le solicita que cree una nueva cuenta.
7. El usuario debe otorgar acceso al directorio para leer una cantidad mínima de datos del usuario, como se muestra en la Figura 1-59. Una vez que el usuario hace clic en **Aceptar**, la cuenta se agrega al directorio.

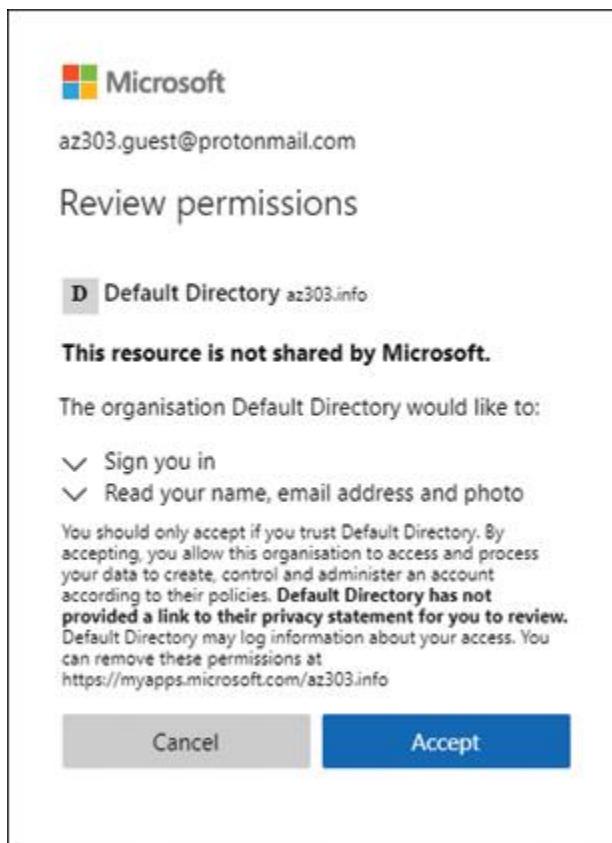


FIGURA 1-59 Revise los permisos de un usuario que acepta una invitación para ser invitado

0.■ La fuente del usuario ahora aparecerá como **Cuenta Microsoft**. En la Figura 1-60 se muestra un ejemplo de esto para el usuario az303.b2b@gmail.com.

The screenshot shows the 'Users | All users (Preview)' page in the Azure Active Directory portal. The left sidebar includes options like 'All users (Preview)', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity' (with 'Sign-ins', 'Audit logs', and 'Bulk operation results'), and 'Troubleshooting + Support'. The main area displays a table of users with columns for 'Name', 'User name', 'User type', and 'Source'. The table includes the following data:

Name	User name	User type	Source
AZ303 B2B	az303.b2b@gmail.com	Guest	Microsoft Account
AZ303 Guest	az303.guest@protonmail.com	Guest	Invited user
globaladmin	globaladmin@az303.info	Member	Azure Active Directory
MFA Test	mftest@az303.info	Member	Azure Active Directory
Power User	poweruser@az303.info	Member	Azure Active Directory
SSPR Test	ssprtest@az303.info	Member	Azure Active Directory
testadmin1	testadmin1@az303.info	Member	Windows Server AD
testadmin2	testadmin2@az303.info	Member	Windows Server AD
testadmin3	testadmin3@az303.info	Member	Windows Server AD

FIGURA 1-60 Tipos de origen de usuario invitado de Azure AD

Nota Federación B2B

En el procedimiento anterior, el paso 6 requiere que el usuario invitado tenga una cuenta de Microsoft para iniciar sesión. Es posible federar su Azure AD a Google u otros proveedores externos a través de la federación directa (vista previa), que permite al usuario tener el mismo nombre de usuario y contraseña. Esta configuración está más allá del alcance del examen, aunque es algo a tener en cuenta.

La administración de invitados dentro de Azure AD se puede realizar con revisiones de acceso de Azure AD. Las revisiones de acceso forman parte de Identity Governance, que es un conjunto de características que forman parte de la SKU de pago de Azure AD Premium P2. Las revisiones de Azure AD Access cubren las membresías y las aplicaciones de grupos. Las revisiones de acceso basadas en roles y recursos forman parte de Azure AD Privileged Identity Management (PIM).

Las revisiones de acceso de Azure AD garantizan que cada usuario revisado aún requiera su acceso. Esto se hace preguntando al usuario o al responsable de la toma de decisiones si el acceso sigue siendo apropiado. Dado que la revisión se realiza en un grupo o aplicación de Azure AD, las revisiones de acceso no son solo para el acceso de invitados. El usuario que crea la revisión de acceso debe tener asignada una licencia Premium P2 y ser un administrador global.

Para explorar las revisiones de acceso de Azure AD para administrar usuarios invitados, siga el siguiente proceso en Azure Portal. Nota para este tutorial, ya se ha creado un grupo de Azure AD que contiene dos usuarios invitados:

1. Buscar **Azure Active Directory** en el buscador nombre del recurso en la parte superior del portal y pulse Enter para seleccionar **Azure Active Directory**. Haga clic en **Gobierno de identidad** en el menú de **Azure Active Directory**, que abre el menú **Gobierno de identidad**.
2. En el menú **Control de identidad**, es posible que la sección **Revisiones de acceso** no esté disponible. Para habilitar **las revisiones de acceso**, debe hacer clic en **Integrado** en el menú de **Gobierno de identidad**. Si tiene más de un directorio con licencias Premium P2, puede elegir el directorio a bordo. Haga clic en **Onboard Now** para permitir el uso de revisiones de acceso en el directorio seleccionado. Tenga en cuenta que si no está a bordo, recibirá un mensaje que indica que no tiene acceso para crear una revisión de acceso y para ponerse en contacto con su administrador global.
3. Vuelva a Azure Portal y haga clic en **Identity Governance** en la hoja de menú.
4. Se abre la hoja **Getting Started**. A la derecha de esta hoja, haga clic en **Crear una revisión de acceso**. Las opciones para crear una revisión de acceso se muestran en la [Figura 1-61](#).

Create an access review

Review name * ✓

Description

Start date * !

Frequency ▼

Duration (in days) ○

End ○

Number of times

End date * !

Users

Users to review ▼

Scope

*Group >
Guest User Group

i The most recent review 'Guest Access Review' for the Group 'Guest User Group' ended on 14/04/2020. Click to view.

Reviewers

Reviewers ▼

Programs

Link to program >
Default Program

^ Upon completion settings

Auto apply results to resource Enable Disable

If reviewers don't respond Remove access ▼

^ Advanced settings

Show recommendations ○	Enable Disable
Require reason on approval ○	Enable Disable
Mail notifications ○	Enable Disable
Reminders ○	Enable Disable

(Preview) Additional content for reviewer email ○

Start

FIGURA 1-61 Creación de una revisión de acceso de administración de invitados

1. ■ **Revise el nombre.** Nombre obligatorio para la revisión.
2. ■ **Descripción.** Una breve descripción de la revisión.
3. ■ **Fecha de inicio.** Fecha de inicio obligatoria de la revisión.
4. ■ **Frecuencia.** Se puede elegir entre **una sola vez , semanal , mensual , trimestral o anual** opiniones. Elija **una vez** .
5. ■ **Duración y finalización.** Si la frecuencia no es anual, elija cuándo finalizar una revisión periódica.
6. ■ **Usuarios para revisar.** Asignado a una aplicación o miembros de un grupo. Para esta explicación, elija **Miembros de un grupo.**
7. ■ **Alcance.** Esta es la clave para administrar usuarios invitados; puede elegir entre todos los usuarios del grupo o la aplicación, o simplemente puede elegir usuarios invitados. Elija **Solo usuarios invitados** .
8. ■ **Grupo.** Elija el grupo para revisar. Si **Usuarios a revisar** se ha establecido en **Asignado a la aplicación** , en su lugar aparecerá un selector de nombre de aplicación. Seleccione el grupo de Azure AD que creó para este tutorial y elija algunos usuarios invitados. Si había creado una revisión para este grupo anteriormente, un banner que lo indica se muestra debajo del grupo, como se muestra en la [Figura 1-61](#) .
9. ■ **Revisores.** Menú desplegable de opciones:
 1. ■ **Propietarios de grupos.** El propietario del grupo que revisa en nombre de los miembros.
 2. ■ **Usuarios seleccionados.** Usuarios seleccionados dentro del grupo.
 3. ■ **Miembros (propios).** Los propios miembros del grupo.
5. Elija **Miembros (yo mismo)**. Esto activará un correo electrónico a los usuarios del grupo para que revisen su propio acceso.
- 0.■ **Programas.** Le permite crear programas para recopilar datos para requisitos de cumplimiento específicos. Deje esta configuración en la configuración predeterminada.

1.■ Al finalizar la configuración. Opciones para acciones automatizadas al completar una revisión:

0. ■ **Aplicar automáticamente los resultados al recurso.** Si una revisión devuelve que un usuario ya no necesita acceso, se eliminará automáticamente.
1. ■ **Si los revisores no responden.** Puede optar por eliminar o aprobar el acceso, o puede dejar su configuración de acceso como está. Elija **Quitar acceso**.
6. Una vez que haya configurado las opciones de revisión de acceso, haga clic en **Iniciar**. Volverá a la hoja **Revisiones de acceso** y su nueva revisión aparecerá como **No iniciada**. Puede hacer clic en la revisión de acceso enumerada para editar la configuración, eliminarla o ver el estado de la revisión de cada usuario.

La revisión de acceso permanecerá como **No iniciada** hasta que se alcance la fecha de inicio. El Estado de revisión cambiará a **Inicializando** cuando Azure envíe correos electrónicos de notificación de revisión a los seleccionados como revisores. Una vez que se envían las notificaciones, el estado cambia a **Activo**.

Cuando se reciba el correo electrónico de notificación, verá un enlace **Revisar acceso**. Cuando hace clic en el enlace, el usuario o revisor seleccionado inicia sesión y puede revisar su acceso o el acceso de otros en el grupo. Si la revisión es una autoevaluación, se le pregunta al usuario si aún necesita acceso al grupo o la aplicación. El usuario elige **Sí** o **No** y completa una razón por la que se necesita el acceso, que se refleja en los **Resultados de la revisión de acceso**, como se muestra en la [Figura 1-62](#).

The screenshot shows the 'Guest Access Review | Results' page in the Azure portal. The left sidebar has 'Overview' selected under 'Manage'. The main area displays two review items:

User	Review status	Reason	Reviewed by	Applied by	Apply result	Recommended action
az213322 az213322@gmail.com	Not reviewed					Deny Last signed in more than 30 days ago
az213322 Owner az213322@gmail.com	Denied	I no longer need this job function	az213322 Owner az213322@gmail.com	az213322 Owner az213322@gmail.com	Approve Last signed in less than 30 days ago (5/1/2020)	

FIGURA 1-62 Revisión de los resultados de la revisión de acceso en Azure Portal

En este ejemplo, el usuario az303.guest ha seleccionado que ya no necesita acceso y se le ha denegado automáticamente el acceso según la selección. El usuario az303.b2b no ha iniciado sesión durante 30 días, por lo tanto, el acceso se denegará automáticamente. Si el usuario az303.b2b responde dentro del período de revisión indicando que aún requiere acceso, se restablece el acceso.

Nota Acceso condicional

Microsoft recomienda utilizar el acceso condicional con MFA para el inicio de sesión de un usuario B2B. Esto se puede realizar seleccionando Todos los usuarios invitados en la sección Asignaciones . Para obtener más detalles, consulte "Configurar métodos de verificación", anteriormente en este capítulo.

Configurar la protección de identidad de Azure AD

Microsoft se ocupa de millones de inicios de sesión desde Azure AD, cuentas de Microsoft y Xbox todos los días. El aprendizaje automático proporciona puntuaciones de riesgo para cada inicio de sesión y estas señales de riesgo se introducen en Azure AD Identity Protection para proporcionar tres informes clave:

- ■ **Usuarios riesgosos.** La probabilidad de que la cuenta se haya visto comprometida.
- ■ **Inicios de sesión arriesgados.** La probabilidad de que el inicio de sesión no haya sido autorizado por el propietario de la cuenta.
- ■ **Detecciones de riesgos.** Esto se muestra cuando no hay una licencia P2 disponible para mostrar que se ha activado alguno de los dos riesgos anteriores.

Azure AD Identity Protection proporciona datos en tiempo real en forma de una descripción general de seguridad en Azure Portal. Para acceder a la descripción general de seguridad, vaya a **Azure AD > Seguridad > Identity Protect** en el portal, como se muestra en la figura 1-63.

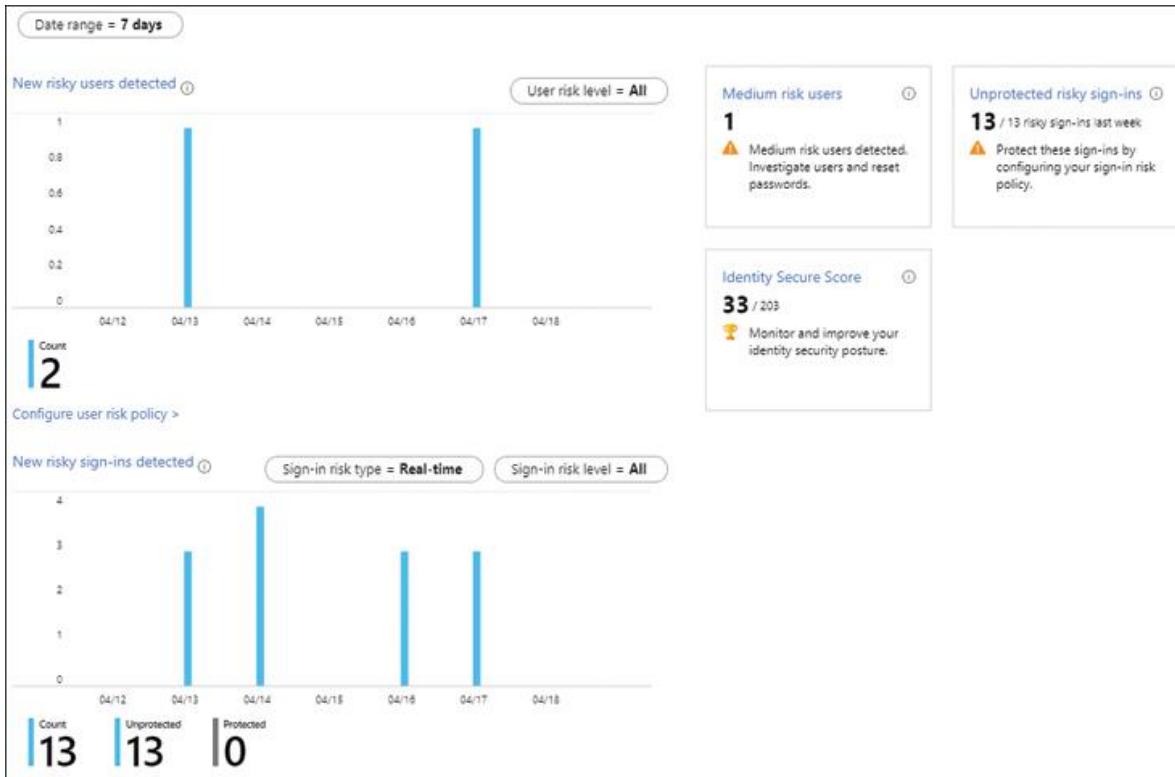


FIGURA 1-63 Resumen de información general sobre Identity Protection de Azure Portal

Este es un nuevo inquilino con escasa cantidad de datos. La documentación indica que Azure AD requiere aproximadamente 14 días de aprendizaje inicial para crear un modelo del comportamiento de su usuario. El gráfico superior de la [Figura 1-63](#) muestra los usuarios que han sido identificados como de riesgo. El gráfico inferior muestra el número de inicios de sesión riesgosos por día. También se puede acceder a esta información a través de las API de protección de identidad de Azure AD de Microsoft Graph.

En la hoja del menú **Protección de identidad**, desplácese hacia abajo hasta **Notificar**. Aquí, puede configurar dos tipos de notificación por correo electrónico:

- **Usuarios en riesgo detectados.** Configure uno o más administradores (todos los administradores globales agregados de forma predeterminada) para recibir una alerta por correo electrónico basada en el nivel de riesgo de alerta bajo, medio o alto.

- **Correo electrónico de resumen semanal.** Este es un resumen de usuarios en riesgo, actividades sospechosas y vulnerabilidades detectadas.

El correo electrónico de los usuarios en riesgo contiene un enlace al informe de usuarios en riesgo; un administrador puede acceder a este informe directamente en **Azure AD > Seguridad > Protección de identidad > Usuarios riesgosos**. Como se muestra en la Figura 1-64, el informe muestra una lista de usuarios de riesgo, así como sus estados y niveles de riesgo.

The screenshot shows the Azure AD Identity Protection Risky Users report interface. At the top, there are filters for 'Show dates as: Local', 'Risk state: 2 selected' (with 'At risk' checked), 'Status: Active', and 'Add filters'. Below the filters is a table with columns: User, Risk state, Risk level, and Risk last updated. A single row is selected for 'AZ303 Guest', showing 'At risk' status, 'Medium' risk level, and last updated on '4/15/2020, 9:46:10 AM'. There is also a 'Details' button next to the row. Below the table, there are links for 'User's sign-ins', 'User's risky sign-ins', 'User's risk detections', 'Reset password', 'Confirm user compromised', 'Dismiss user risk', and an ellipsis. Under the 'Basic Info' tab, detailed user information is shown: User (AZ303 Guest), Roles (User), Username (az303.guest_protonmail.com#EXT#@onmicrosoft.com), User ID (0821270a-d412-484d-8b7b-92da22aaea8d), Risk state (At risk), Risk level (Medium), Details (empty), and Risk last updated (4/15/2020, 9:46:10 AM). Other tabs include 'Recent risky sign-ins', 'Detections not linked to a sign-in', and 'Risk history'.

FIGURA 1-64 Informe de usuarios riesgosos de Azure AD Identification Protection

Tenga en cuenta que en la Figura 1-64, las acciones que se pueden realizar directamente desde el informe: **Restablecer contraseña**, **Confirmar usuario comprometido** y **Descartar riesgo de usuario**. Estos le permiten proporcionar comentarios sobre las evaluaciones de riesgos de Azure AD Identity Protection.

En la parte superior de la hoja de menú de Azure AD Identity Protection en Azure Portal, hay tres políticas predeterminadas que se pueden habilitar para admitir Identity Protection:

- **Política de riesgo del usuario.** Esto depende del nivel de riesgo del usuario (**bajo**, **medio** o **alto**). El nivel de riesgo de una Política de riesgo del usuario es la condición. Puede optar por bloquear o permitir el acceso según la condición. Si está permitiendo el acceso, tiene la opción de hacer cumplir MFA.

- **Política de riesgo de inicio de sesión.** Esto depende del nivel de riesgo de inicio de sesión del usuario (**bajo**, **medio** o **alto**). El nivel de riesgo de una política de riesgo de inicio de sesión es la condición. Puede optar por bloquear o permitir el acceso según la condición. Si está permitiendo el acceso, tiene la opción de hacer cumplir MFA.
- **Política de registro de MFA.** Cuando está habilitada, esta directiva obliga a los usuarios o grupos seleccionados a usar la autenticación multifactor de Azure AD.

Cada una de estas políticas se puede establecer para un subconjunto de usuarios, para grupos o para todos los usuarios. Estas políticas tienen una personalización limitada. Si necesita más control, puede utilizar una política de acceso condicional. Las políticas de acceso condicional se tratan en la siguiente sección.

Implementar el acceso condicional, incluido MFA

Hasta ahora, nuestra discusión sobre la configuración de MFA se ha concentrado en MFA que se habilita por usuario al cambiar el estado del usuario, o contra una característica específica como el riesgo de inicio de sesión. Esto puede ser inflexible porque requiere que se fuerce un segundo paso de verificación en cada inicio de sesión, independientemente del nivel de riesgo de la información a la que se accede. El acceso condicional le brinda un marco para diseñar una estrategia de acceso para las aplicaciones y los recursos que utiliza su organización, adaptándola para satisfacer las necesidades de acceso a los recursos de su organización.

El acceso condicional es una característica de P2 Premium Azure AD, que se puede encontrar en **Azure Active Directory** en la sección **Seguridad** de la hoja de menú de **Azure AD**. Cuando observe el acceso condicional por primera vez, verá que se muestra un conjunto de políticas. Estas son las políticas de base; son políticas heredadas y deben ignorarse. Debe crear sus políticas desde cero.

El acceso condicional es altamente configurable. Para ver qué tan configurable, el siguiente ejemplo analiza la configuración de MFA condicional. El caso de uso de este ejemplo es: "Si el inicio de sesión de un usuario de un grupo específico está fuera de la oficina central, se requiere un MFA, una máquina unida a un dominio o un dispositivo compatible de

Microsoft Intune". Explorará las otras opciones de acceso condicional disponibles en cada hoja.

Nota Acceso condicional

Si aún tiene MFA por usuario configurado en la sección anterior, deberá deshabilitarlo. El acceso condicional se reemplaza por el MFA por usuario.

En este ejemplo, antes de crear una política de acceso condicional, primero debe crear una ubicación con nombre para simular su oficina central. En la hoja de menú **Acceso condicional** del portal, haga clic en **Ubicaciones con nombre** y luego siga estos pasos:

1. Haga clic en **Agregar ubicación con nombre**.
2. Ingrese un **nombre** para la ubicación; para este ejemplo, ingrese **Head Office**.
3. Seleccione **Marcar como ubicación de confianza**, que automáticamente reducirá el riesgo de inicio de sesión para los usuarios que inicien sesión desde esta ubicación. Explorará esto más adelante en esta sección.
4. En el campo **IP Ranges**, ingrese la notación CIDR para la dirección IP que está utilizando actualmente. Haga clic en **Crear**.

La ubicación nombrada se crea y está lista para ser seleccionada en la política de acceso condicional. Para crear la directiva, permanezca en Azure Portal y seleccione **Acceso condicional** en la hoja del menú **Seguridad**. Siga este tutorial para crear la política de casos de uso y explorar las opciones en los blades, como se muestra en la [Figura 1-65](#).

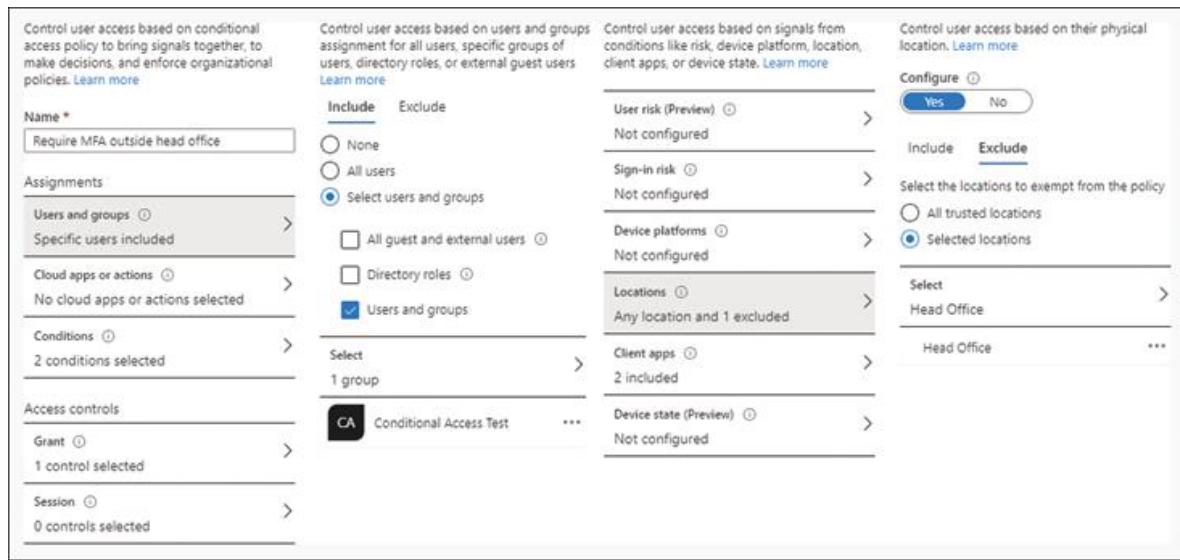


FIGURA 1-65 Los blades de acceso condicional para asignaciones en Azure Portal

1. Haga clic en **Nueva política**; la primera hoja de la [Figura 1-65](#) se muestra con cada sección configurada en 0 selecciones.
2. Haga clic en **Usuarios y grupos**. En esta hoja (consulte la [Figura 1-65](#)), se muestran los usuarios que se incluirán o excluirán. Por ejemplo, el caso de uso es: "Incluir usuarios que forman parte de un grupo específico". Haga clic en **Seleccionar usuarios y grupos** para seleccionar el grupo. Haz clic en **Listo**.
3. Haga clic en **Aplicaciones o acciones en la nube**. Aquí, se pueden seleccionar aplicaciones de Microsoft, como Microsoft 365, sus propias aplicaciones o aplicaciones de terceros que se han integrado con Azure AD. El caso de uso indica "cualquier inicio de sesión" y no se refiere a aplicaciones específicas, así que seleccione todas las aplicaciones en la nube y haga clic en **Listo**.
4. Haga clic en **Condiciones**. La información sobre las condiciones de inicio de sesión que se utilizan se transmite desde Azure:
 1. **Riesgo de inicio de sesión**. Filtro de **baja**, **media** o **alta** (como se describe anteriormente en este capítulo en "Configurar Azure AD protección de la identidad"). Para este ejemplo, dejar **Configurar conjunto de n**.

2. ■ **Plataformas de dispositivos.** Incluir o excluir según el tipo de sistema operativo: Android, iOS, Windows o macOS. Para este ejemplo, deje **Configurar conjunto de n** .
 3. ■ **Ubicación.** Incluya o excluya ubicaciones con nombre y / o de confianza. Parte del caso de uso es excluir la oficina central. Establezca la **ubicación** para excluir la oficina central. (Creó la ubicación de la oficina central en el conjunto de pasos anterior).
 4. ■ **Aplicaciones cliente (vista previa).** Incluir o excluir según el tipo de aplicación cliente que se utiliza para el inicio de sesión. Para este ejemplo, deje **Configurar conjunto de n** .
 5. ■ **Estado del dispositivo.** Puede optar por excluir dispositivos unidos a un dominio o de Microsoft Intune que estén marcados como compatibles. Para este ejemplo, deje **Configurar conjunto de n** .
5. Se pueden combinar varias condiciones para filtrar a un conjunto específico de circunstancias. Haz clic en **Listo** .
 6. En la hoja **Nueva** , ahora debe configurar los controles de acceso y hacer clic en **Otorgar** . Los botones de opción **Block Access** y **Grant Access** aparecen en la parte superior de **Grant hoja** , comose muestra en la Figura 1-66 . El caso de uso es otorgar acceso a un usuario fuera de la oficina central si aprueba MFA o tiene un dispositivo compatible. Para configurar los ajustes de la política de **subvenciones** para cumplir con este caso de uso, deberá configurar lo siguiente:
 - 0.■ **Requerir autenticación multifactor.** Requiere que un usuario realice la autenticación multifactor. Seleccione esta casilla de verificación para cumplir con el requisito de caso de uso de "requerir MFA".
 - 1.■ **Requerir que el dispositivo se marque como compatible.** Requiere que el dispositivo del usuario cumpla con los requisitos de cumplimiento configurados por Microsoft Intune. Seleccione esta casilla de verificación para cumplir con el requisito de caso de uso de "un dispositivo compatible de Microsoft Intune".

2.■ Requerir un dispositivo unido a Azure AD

híbrido. Seleccione esta casilla de verificación para cumplir con el requisito de caso de uso de "un dispositivo unido a un dominio".

3.■ Requerir aplicación de cliente aprobada. Requiere que la aplicación a la que accede el usuario sea una de las aplicaciones cliente aprobadas por Microsoft. Deje esta casilla sin marcar, ya que no forma parte del requisito del caso de uso.

4.■ Requerir política de protección de

aplicaciones. Requiere que la aplicación a la que accede el usuario tenga una política de protección de aplicaciones obligatoria. Deje esta casilla sin seleccionar, ya que no forma parte del requisito del caso de uso.

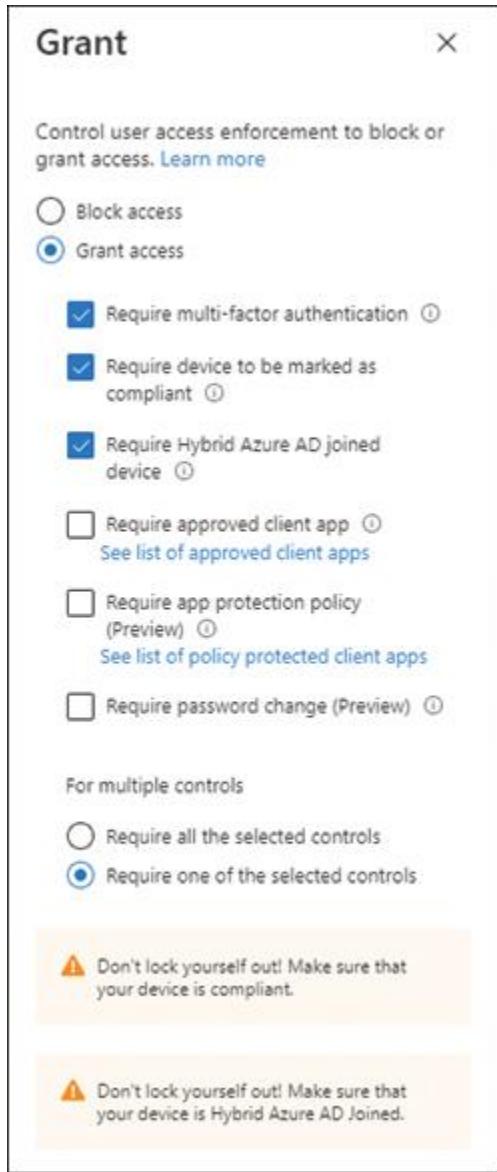


FIGURA 1-66 La hoja Grant para crear una política de acceso condicional

7. El caso de uso establece que solo se debe cumplir uno de los controles; por lo tanto, configure **Múltiples controles para requerir uno de los controles seleccionados**. Haga clic en **Seleccionar**.
8. Haga clic en **Sesión**. Esto limita el acceso dentro de las aplicaciones específicas de Microsoft 365. Esto no es necesario para el caso de uso. Cierre la hoja de **sesión**.
9. El requisito del caso de uso ahora se cumple; haga clic en **Crear** para crear la política de acceso.

10. La nueva política se enumera en la hoja **Políticas**. Para probar la política, inicie sesión en Mis aplicaciones (<https://myapplications.microsoft.com>) desde la dirección IP establecida en la ubicación indicada. Deberá realizar este inicio de sesión como uno de los usuarios que forma parte del grupo seleccionado en el paso 2 de este tutorial. Ha iniciado sesión correctamente porque esto simula el inicio de sesión desde la oficina central.
11. Ahora intente iniciar sesión desde su teléfono con datos móviles; Se le pedirá que verifique usando MFA porque el acceso condicional marca el inicio de sesión como proveniente de fuera de la oficina.

Para ayudar a solucionar problemas de políticas de acceso condicional, haga clic en el botón **Y si ...** en la hoja **Acceso condicional**. Aquí puede ver qué políticas de acceso condicional se aplicarán en diversas condiciones.

¿Necesita más revisión? Acceso condicional

Para obtener más información sobre cómo implementar el acceso condicional, incluido MFA, visite el artículo de Microsoft Docs “Documentación de acceso condicional” en <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/>.

HABILIDAD 1.7: IMPLEMENTAR Y ADMINISTRAR IDENTIDADES HÍBRIDAS

La mayoría de las organizaciones tendrán una solución de identidad local en la que las aplicaciones abarcan recursos locales y en la nube. Administrar a los usuarios que acceden a estas aplicaciones puede ser un desafío. Como arquitecto, debe buscar soluciones que permitan a sus usuarios tener un conjunto de credenciales independientemente de dónde estén alojadas sus aplicaciones. Las soluciones de identidad de Microsoft tienen capacidades locales y basadas en la nube. Esto crea una identidad híbrida, que es una única identidad común para la autenticación y autorización en todas las ubicaciones. Active Directory en Windows Server es el proveedor de identidad local de Microsoft. Las identidades

dentro de Active Directory se pueden sincronizar con Azure AD mediante Azure AD Connect, que crea una identidad común para la autenticación y autorización de todos los recursos, en todas las ubicaciones.

Esta habilidad cubre cómo:

- Instalar y configurar Azure AD Connect
- Opciones de sincronización de identidad
- Configurar y administrar la sincronización y la escritura diferida de contraseñas
- Configurar el inicio de sesión único
- Utilice Azure AD Connect Health

Los tutoriales de esta habilidad requieren un controlador de dominio para que se pueda configurar una sincronización de Active Directory a Azure AD. Si no tiene experiencia previa trabajando con Azure AD Connect, le recomendamos que configure un entorno para trabajar durante el proceso. Esto puede parecer abrumador, pero a un alto nivel, se puede lograr en Azure con tres pasos:

1. Compre un nombre de dominio y siga las instrucciones en Skill 1.6 para agregar un nombre de dominio personalizado y convertirlo en el dominio principal en su inquilino de Azure AD.
2. Use la plantilla de inicio rápido de Azure para crear un controlador de dominio en Azure (<https://github.com/Azure/azure-quickstart-templates/tree/master/active-directory-new-domain>) . Haga clic en **Implementar en Azure** y luego use los siguientes parámetros:
 - **Conceptos básicos.** Ingrese un nombre de grupo de recursos y elija una ubicación.
 - **Configuración.** Elija un nombre de usuario y contraseña de administrador. Para **Nombre de dominio**, ingrese el nombre de dominio que compró en el paso 1. Para **Prefijo DNS**, ingrese algo que sea único. Deje todo lo demás configurado en los valores predeterminados.
3. Haga clic en **Comprar**.
4. Una vez implementado, RDP a la IP pública del balanceador de carga. Inicie sesión como el usuario administrador que creó en el paso 2. El Administrador del servidor se abrirá

automáticamente. Haga clic en **Herramientas > Usuarios y equipos de Active Directory** y cree algunos usuarios. Es posible que desee crear una nueva unidad organizativa (OU) en la que pueda colocar a sus usuarios de prueba cuando explore el filtrado de Azure AD Connect en la siguiente sección. Asegúrese de que uno de los usuarios sea un administrador de empresa.

Su controlador de dominio en Azure actuará como si fuera local.

Instalar y configurar Azure AD Connect

Azure AD Connect es una herramienta que proporciona sincronización de datos de identidad desde controladores de dominio locales a Azure AD. Es un agente ligero que se puede instalar en Windows Server 2012 o superior. Azure AD Connect puede incluso instalarse en el propio controlador de dominio, aunque esta no es la práctica recomendada. Azure AD Connect funciona a través de una conexión a Internet estándar y no es necesario configurar una VPN de sitio a sitio o una ruta rápida. Para explorar más la configuración, siga estos pasos:

1. Abrir el portal Azure, buscar **azul directorio activo** en la barra de búsqueda de nombre de recurso en la parte superior del portal, y pulsar Enter para seleccionar **Azure Active Directory**. Haga clic en **Azure AD Connect** en la hoja de menú. En la hoja de **Azure AD Connect**, haga clic en **Descargar Azure AD Connect**; este es el agente de Azure AD Connect. Copie el archivo `AzureADConnect.msi` descargado en el servidor desde el que realizará la instalación. Para este tutorial, instalará en el controlador de dominio.
2. Haga doble clic en el archivo `AzureADConnect.msi` que acaba de copiar en el servidor para iniciar la instalación. Acepte los términos de la licencia y haga clic en **Continuar**.
3. La instalación predeterminada de Express Settings se muestra en la [Figura 1-67](#). Este proceso es automático e instalará **Azure AD Connect** con los valores predeterminados. Haga clic en **Personalizar**, lo que le dará un control total sobre el proceso de instalación, incluido el método de sincronización.

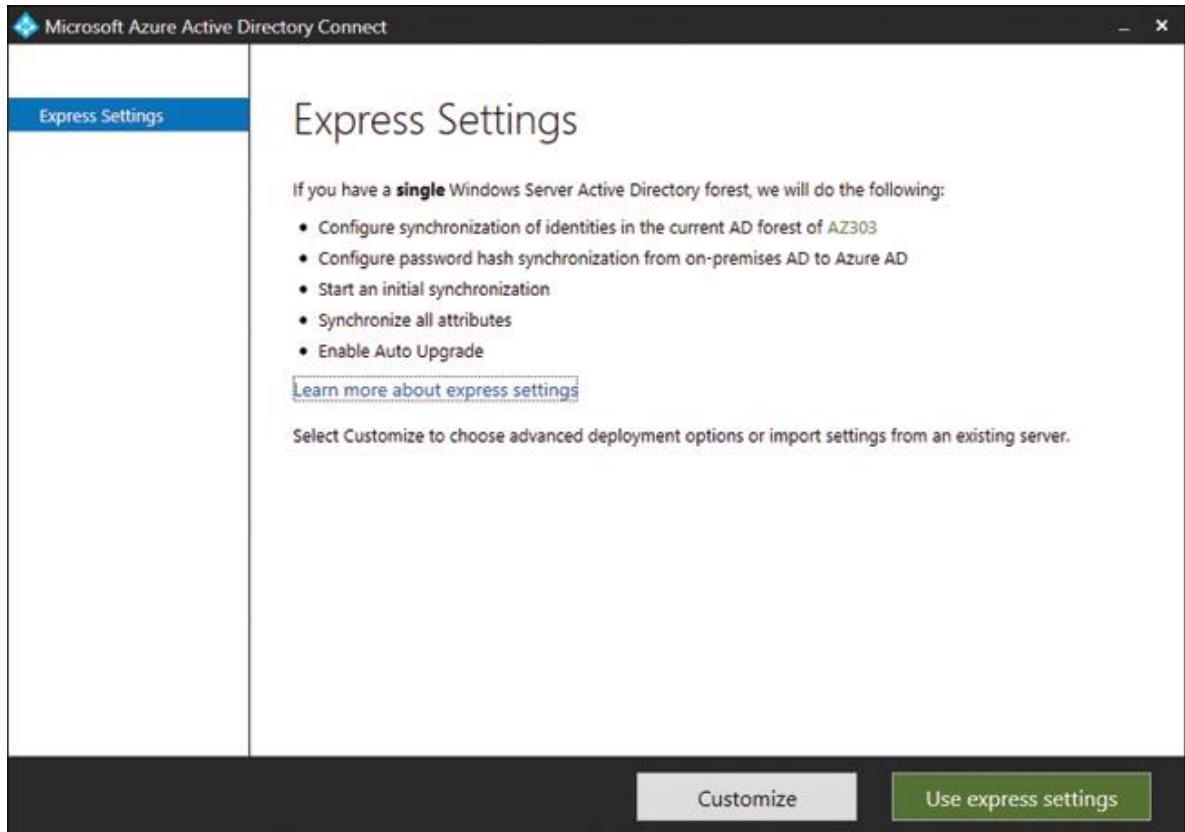


FIGURA 1-67 El proceso de instalación automática para Express Settings en Azure AD Connect

4. La pantalla **Componentes requeridos** le ofrece la opción de utilizar componentes instalados previamente. Déjelos configurados con sus valores predeterminados (no seleccionados). Haga clic en **Instalar**. Ahora se instalarán los componentes necesarios.
1. ■ **Ubicación de instalación personalizada.** Elija dónde se instalarán los archivos del agente de Azure AD Connect.
2. ■ **SQL Server existente.** Puede especificar un servidor de base de datos para albergar la base de datos de Azure AD Connect si ya tiene una instalación de SQL.
3. ■ **Cuenta de servicio.** Es posible que ya tenga configurada una cuenta de servicio, aunque requerirá el permiso Iniciar sesión como servicio y que sea un administrador del sistema en el servidor SQL elegido.
4. ■ **Grupos de sincronización personalizados.** Grupos locales al servidor.

5. La pantalla de inicio de sesión del usuario enumera las opciones de sincronización disponibles, como se muestra en la Figura 1-68. Los explorará en "Opciones de sincronización de identidad", más adelante en este capítulo. Deje la **Sincronización de hash de contraseña** habilitada. La configuración **Habilitar el inicio de sesión único** también se explorará en "Configurar el inicio de sesión único", más adelante en este capítulo. Por ahora, no haga clic en esta opción. Haga clic en **Siguiente**.

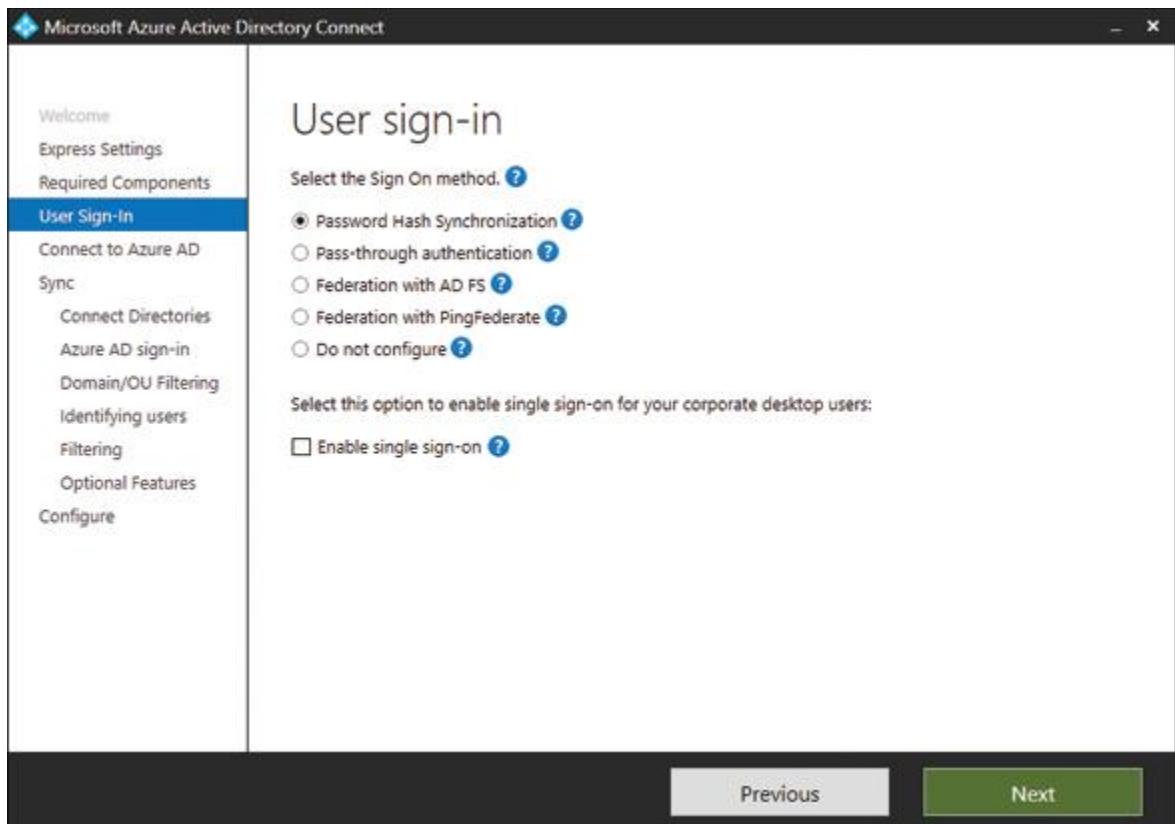


FIGURA 1-68 Elección del método de inicio de sesión para usuarios en Azure AD Connect

6. La conexión a Azure AD requiere credenciales de administrador global. Ingrese estas credenciales y haga clic en **Siguiente**.
7. La pantalla **Conectar a Azure AD** le permite elegir el tipo de directorio al que desea conectarse. Elija el bosque y haga clic en **Agregar directorio**, como se muestra en la Figura 1-69. Ahora necesita crear una cuenta con permisos para sincronizar periódicamente su Active Directory. En **Seleccionar opción de cuenta**, deje **seleccionada la opción Crear nueva cuenta AD e**

ingrese las credenciales de administrador de la empresa. Este proceso se muestra en la [Figura 1-69](#). Haga clic en **Aceptar**.

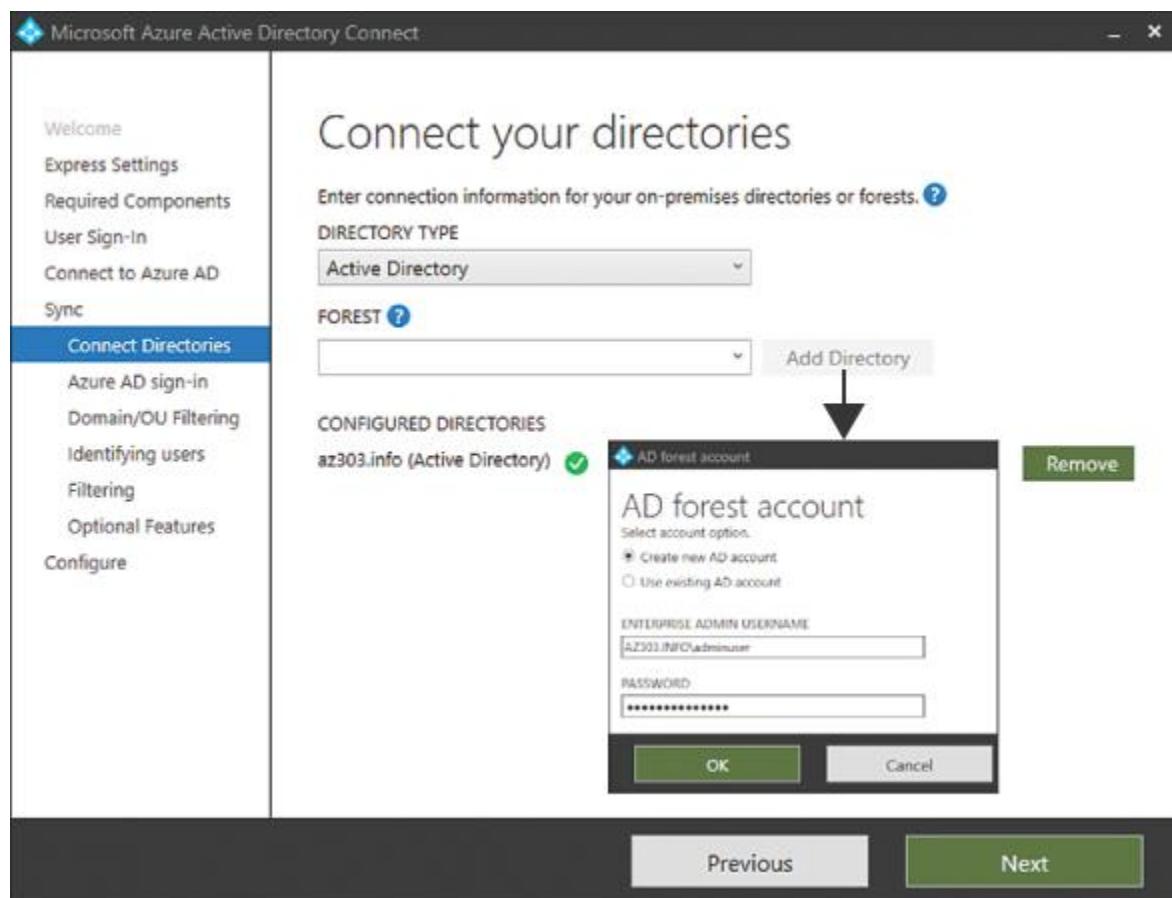


FIGURA 1-69 Conexión de directorio de Azure AD Connect e inicio de sesión de administrador empresarial

8. Volverá a la pantalla **Conectar sus directorios**, como se muestra en la [Figura 1-70](#). El directorio que acaba de agregar aparece en **Directorios configurados**. Haga clic en **Siguiente**.
9. Azure AD Connect ahora enumerará los **sufijos UPN** de su Active Directory local, como se muestra en la [Figura 1-70](#). Para que un usuario inicie sesión sin errores, el dominio personalizado en Azure AD debe coincidir con un sufijo UPN en el entorno local. No puede usar el nombre de dominio predeterminado * .onmicrosoft.com del inquilino. Cuando un sufijo UPN y un dominio de Azure AD coinciden, se marca como **verificado** en la columna **Dominio de Azure AD** (consulte la [figura 1-70](#)).

En el pasado, muchos directorios activos se configuraban con .local como dominio. Si su Active Directory está configurado de esta

manera, debe agregar un sufijo UPN a su bosque, que debe coincidir con el dominio personalizado en Azure AD. Esto también puede significar que el selector de **Nombre principal de usuario (UPN)** es incorrecto. El UPN se tomará como el nombre de usuario para el inicio de sesión de Azure. El UPN debe tener un sufijo como se verifica en la lista de la [Figura 1-70](#); de lo contrario, los usuarios no podrán iniciar sesión. Si el **sufijo UPN de Active Directory y el dominio de Azure AD** no coinciden, por ejemplo, de un archivo dominio, es posible que deba usar un atributo diferente, como la dirección de correo electrónico, para su nombre principal de usuario. Hacer clic histórico .local **Siguiente**.

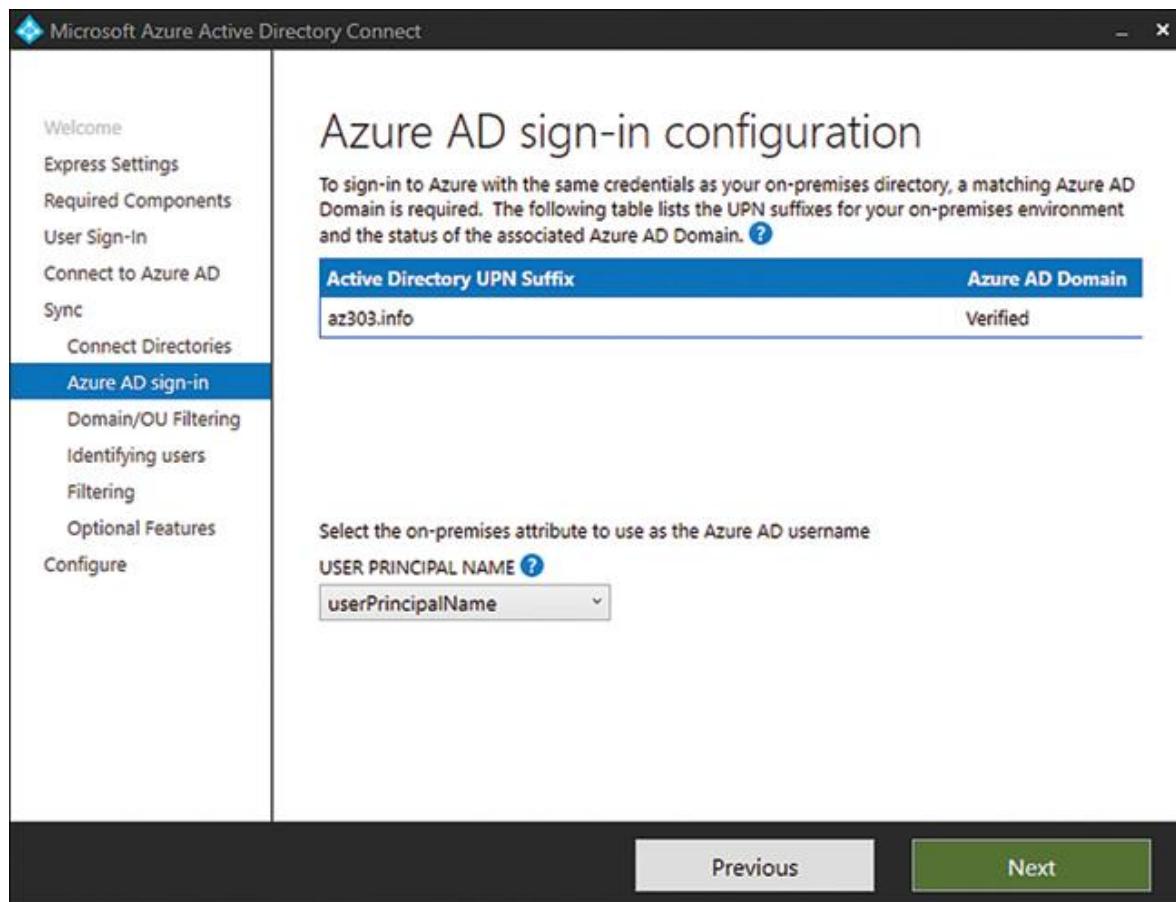


FIGURA 1-70 Verificación de la configuración de inicio de sesión de Azure AD Connect

10. Ahora puedes elegir qué partes de su directorio sincronizar. El valor predeterminado es seleccionar todos los dominios y unidades organizativas. Sin embargo, debes filtrar por dos razones:

1. ■ No desea desperdiciar costosas licencias de Azure AD en cuentas que no son de usuario.
 2. ■ No desea sincronizar cuentas de servicio o cuentas con privilegios elevados con Azure AD a menos que sea necesario.
11. Elija **Sincronizar dominios seleccionados y unidades organizativas**, y luego seleccione las unidades organizativas donde residen sus usuarios, como se muestra en la Figura 1-71. Haga clic en **Siguiente**.

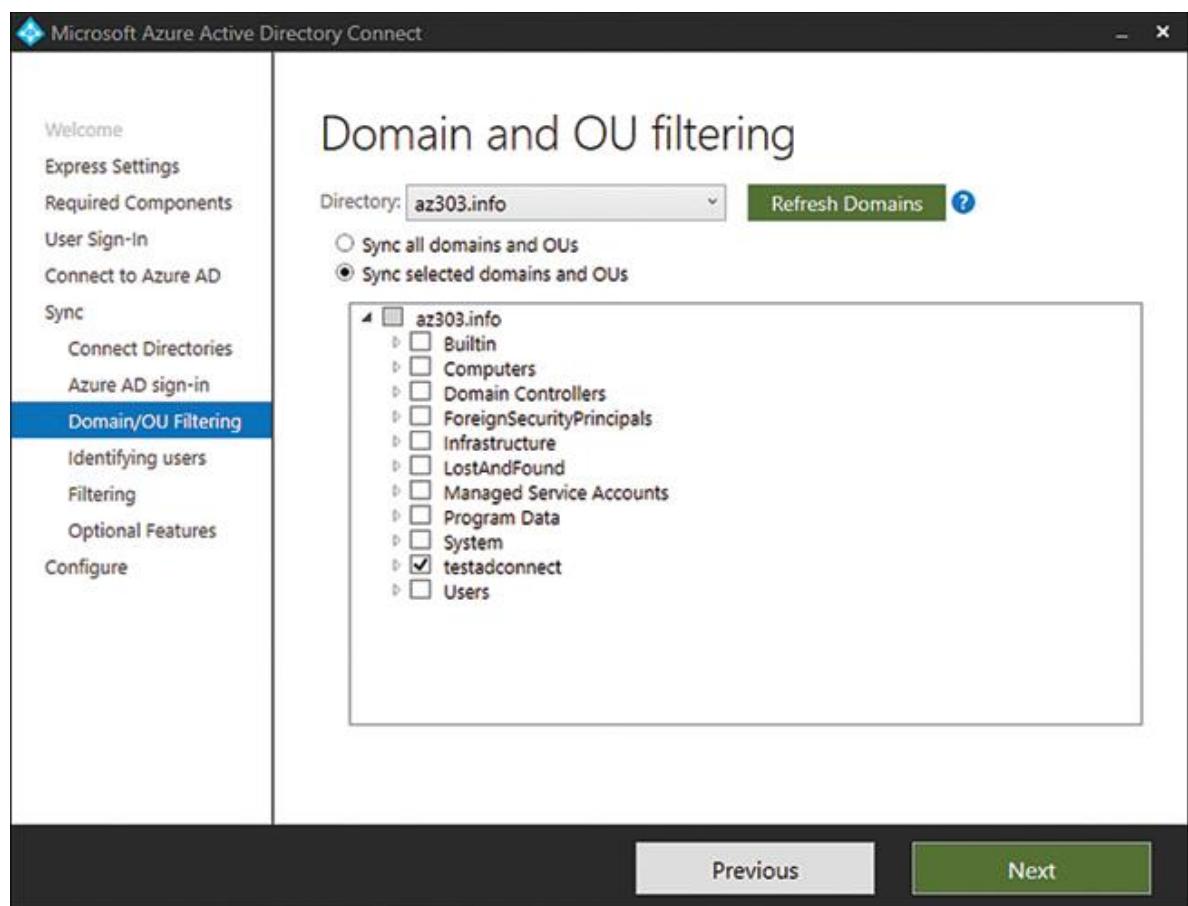


FIGURA 1-71 Dominio de Azure AD Connect y filtrado de unidades organizativas

12. En la pantalla **Identificación exclusiva de sus usuarios**, haga clic en **Siguiente** para continuar. De forma predeterminada, Azure AD Connect usa el atributo UPN para identificar sus cuentas de AD locales de forma individual. En organizaciones más grandes que planean sincronizar usuarios en dominios y bosques de AD, es posible que deba elegir otro

atributo de esquema de AD para resolver los conflictos de nombres de cuentas.

13. **Filtrar usuarios y dispositivos** se usa para una fase piloto de Azure AD Connect. Si desea probar un subconjunto de usuarios, cree un grupo en su AD local e ingrese el nombre del grupo en este punto. Deje esta selección configurada para **Sincronizar todos los usuarios y dispositivos**. Haga clic en **Siguiente**.

14. En la pantalla **Funciones opcionales**, haga clic en **Siguiente**. Explorará estas características en las siguientes cuatro secciones de esta habilidad.

15. La pantalla **Listo para configurar que se muestra en la Figura 1-72** muestra la sincronización que se ha configurado en su servidor. Si elige **Iniciar el proceso de sincronización cuando se complete la configuración**, se iniciará la sincronización tan pronto como se complete la configuración.

16. Si selecciona **Habilitar modo de ensayo: cuando se selecciona, la sincronización no exportará ningún dato a AD o Azure AD**, los cambios en Azure AD Connect se importarán y sincronizarán, pero no se exportarán a Azure AD. Esto significa que puede obtener una vista previa de sus cambios antes de realizar la sincronización en vivo. Una vez instalado, dejarmodo de ensayo, deberá editar la configuración de Azure AD Connect y desactivar el modo de ensayo, que iniciará la sincronización. Haga clic en **Instalar**. Azure AD Connect ahora se instalará y comenzará a sincronizar sus usuarios con Azure AD.

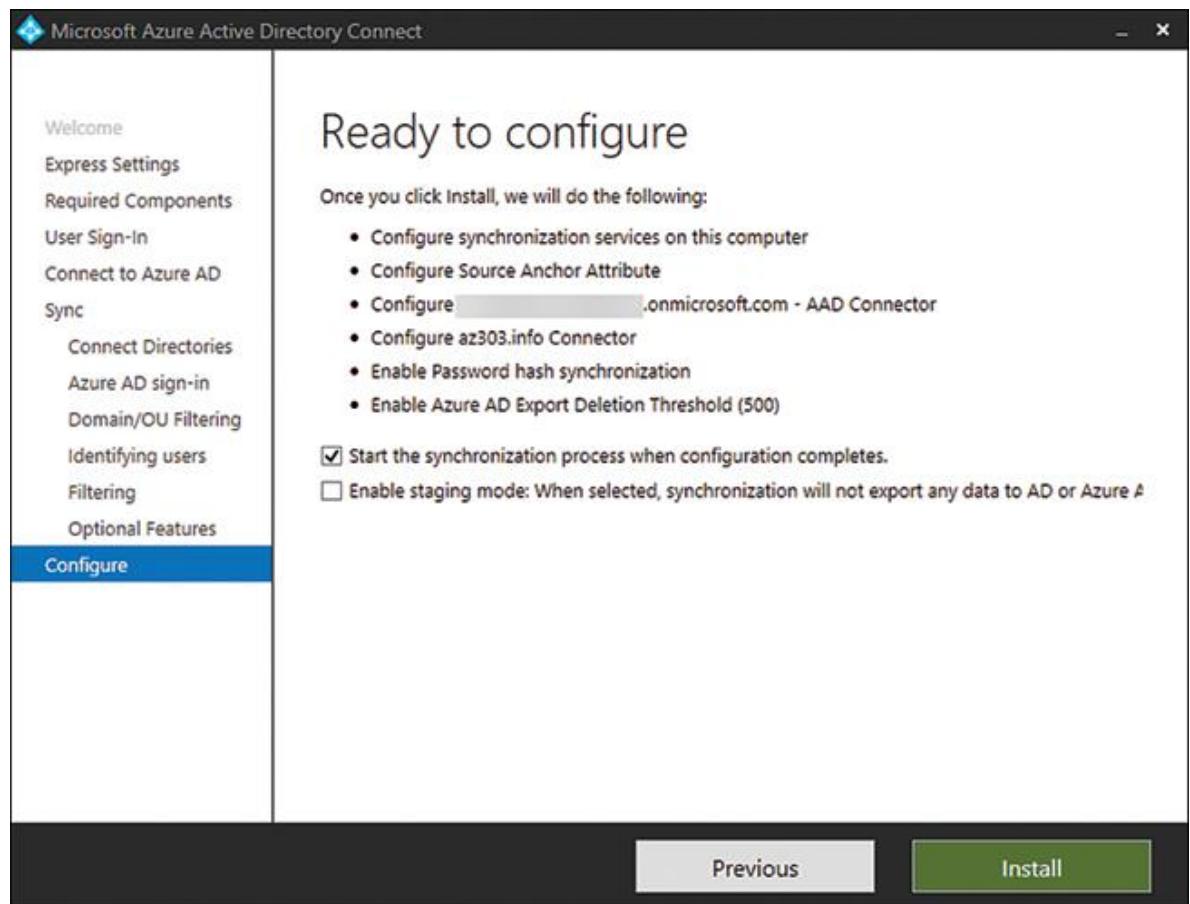


FIGURA 1-72 Azure AD Connect listo para configurar

Ahora puede verificar que sus usuarios se hayan sincronizado con Azure AD cambiando a Azure Portal. Busque el **directorio activo azul** en la barra de búsqueda de nombres de recursos en la parte superior del portal. Después de hacer clic en **Usuarios** en la hoja del menú, ahora debería ver a sus usuarios en la lista, como se muestra en la [Figura 1-73](#). En la columna **Fuente**, los usuarios sincronizados se muestran con **Windows Server AD**.

User Management				
Search users		Actions		
Name	User name	User type	Source	
<input type="checkbox"/> SSP Test	ssptest@az303.info	Member	Azure Active Directory	
<input type="checkbox"/> MFA Test	mfastest@az303.info	Member	Azure Active Directory	
<input type="checkbox"/> globaladmin	globaladmin@az303.info	Member	Azure Active Directory	
<input type="checkbox"/> testaadc1	testaadc1@az303.info	Member	Windows Server AD	
<input type="checkbox"/> testaadc2	testaadc2@az303.info	Member	Windows Server AD	
<input type="checkbox"/> testaadc3	testaadc3@az303.info	Member	Windows Server AD	

FIGURA 1-73 Los usuarios sincronizados se identifican con Windows Server AD.

Haga clic en cualquiera de los usuarios que se hayan sincronizado desde un Active Directory local. Puede ver en la [Figura 1-74](#) que la mayoría de los detalles no se pueden editar porque no están disponibles. Solo están disponibles los elementos que se utilizan en la nube, como la **ubicación de uso**. El Active Directory de Windows Server es el directorio maestro. Si se van a realizar ediciones, deben realizarse en las instalaciones.

The screenshot shows the Azure portal's user management interface. At the top, it displays the user's name, email, and a placeholder for a profile picture. Below this, there are tabs for 'User Sign-ins' and 'Group memberships'. Under 'Identity', it lists the user's name, user principal name, object ID, first name, and last name. In the 'Job info' section, it shows the job title as 'Manager' and the department as 'United Kingdom'. The 'Settings' section includes a toggle for 'Block sign in' set to 'No' and a dropdown for 'Usage location' set to 'United Kingdom'.

FIGURA 1-74 Solo se pueden editar los elementos de la nube.



Privilegios de usuario de la sugerencia del examen para Azure AD Connect

Es posible que deba explicar los tipos de privilegios de usuario necesarios para configurar Azure AD Connect (administrador global y administrador empresarial).

¿Necesita más revisión? Instalar AD Connect

Para obtener información sobre la instalación de Azure AD Connect, visite el artículo de Microsoft Docs "Instalación personalizada de Azure AD Connect" en [https://docs.microsoft.com/en-](https://docs.microsoft.com/en)

[us/azure/active-directory/hybrid/how-to-connect-instalar-personalizado](#).

Opciones de sincronización de identidad

En la sección anterior, aprendió cómo instalar y configurar Azure AD Connect. Establece **Sincronización de hash de contraseña** como la opción de sincronización. Sin embargo, había otras cinco opciones disponibles. Cada una de estas opciones tiene diferentes ventajas y, por lo tanto, diferentes casos de uso. Como arquitecto, debe comprender cuándo se debe utilizar cada opción.

- ■ **No configurar.** Los usuarios pueden iniciar sesión con un inicio de sesión federado que no está administrado por Azure AD Connect. Estos inicios de sesión no utilizan la misma contraseña, solo el mismo nombre de usuario. Esto debe elegirse cuando ya existe un servidor de federación de terceros.
- ■ **Sincronización de hash de contraseña.** Los usuarios pueden iniciar sesión en Office 365 y otros servicios en la nube de Microsoft con la misma contraseña que usan localmente. Azure AD Connect sincroniza un hash de la contraseña con Azure AD y la autenticación se produce dentro de la nube. Este método solo debe usarse cuando se almacena el hash de la contraseña de un usuario en el cloud cumple con los requisitos de cumplimiento de su organización. También es importante recordar que debido a que Azure AD realiza la autenticación, no se seguirán todas las políticas de Active Directory. Por ejemplo, si una cuenta ha caducado pero la cuenta aún está activa, Azure AD aún se autenticará. La sincronización de hash de contraseña admite el inicio de sesión único sin problemas.
- ■ **Autenticación de paso a través.** Los usuarios pueden iniciar sesión en los servicios en la nube de Microsoft con sus propias contraseñas. Sin embargo, con la autenticación PassThrough, la autenticación se realiza en el Active Directory local. El beneficio clave de la autenticación PassThrough es que no se almacenan contraseñas en la nube, lo que puede ser un requisito de cumplimiento para muchas organizaciones. Debido a que la autenticación se realiza en el Active Directory local, las

políticas de contraseña y seguridad de AD también se pueden aplicar.

- ■ **Federación con AD FS.** La federación es una colección de dominios que han establecido confianza entre ellos. La confianza puede contener autenticación y autorización. Históricamente, la federación se utilizó para establecer la confianza entre organizaciones para los recursos compartidos. Azure AD se puede federar con AD FS local, lo que permite a los usuarios usar sus propias contraseñas y usar el inicio de sesión único (SSO). La federación con AD FS se autentica en el servidor de AD FS local, por lo que no se almacenan contraseñas ni hashes de contraseñas en la nube. AD FS con Azure AD Connect debe usarse cuando las aplicaciones de terceros lo requieran y cuando AD FS ya está en uso.
- ■ **Federación con PingFederate.** Esta es una alternativa de terceros a AD FS. Esta opción debe seleccionarse para empresas que ya usan PingFederate para SSO basado en tokens.



Consejo de examen AD FS

Microsoft recomienda que los clientes pasen de la federación con AD FS a la autenticación PassThrough con SSO transparente siempre que sea posible. Tenga esto en cuenta si se le pregunta sobre los métodos de contraseña en la nube y el inicio de sesión único.

Configurar y administrar la sincronización y la escritura diferida de contraseñas

Con el restablecimiento de contraseña de autoservicio de Azure AD habilitado, los usuarios pueden desbloquear sus cuentas y actualizar sus contraseñas desde aplicaciones basadas en la nube. Si estos usuarios son miembros de su Active Directory local que se sincroniza mediante Azure AD Connect a Azure AD, es posible que sus usuarios descubran que sus contraseñas no están sincronizadas.

La escritura diferida de contraseña es una característica de Azure AD Connect que escribe los cambios de contraseña en tiempo real en un directorio local. La escritura diferida de contraseña es compatible con la sincronización de hash de contraseña, la autenticación de paso a través y

ADFS. La escritura diferida de la contraseña no requiere ningún cambio en el cortafuegos; utiliza un relé de bus de servicio de Azure a través del canal de comunicación de Azure AD Connect.

La escritura diferida de contraseñas es una característica paga que requiere al menos una licencia premium P1 para ser asignada a sus usuarios en Azure AD. La reescritura de contraseña debe configurarse en el Active Directory local y en Azure AD. Para configurar el Active Directory local, siga estos pasos a través de una sesión RDP en el servidor en el que deberá iniciar sesión como administrador de dominio:

1. Abra Azure AD Connect, que ya se ha instalado y haga clic en **Configurar > Ver configuración actual**. La configuración actual de Azure AD Connect se muestra en la [figura 1-75](#).

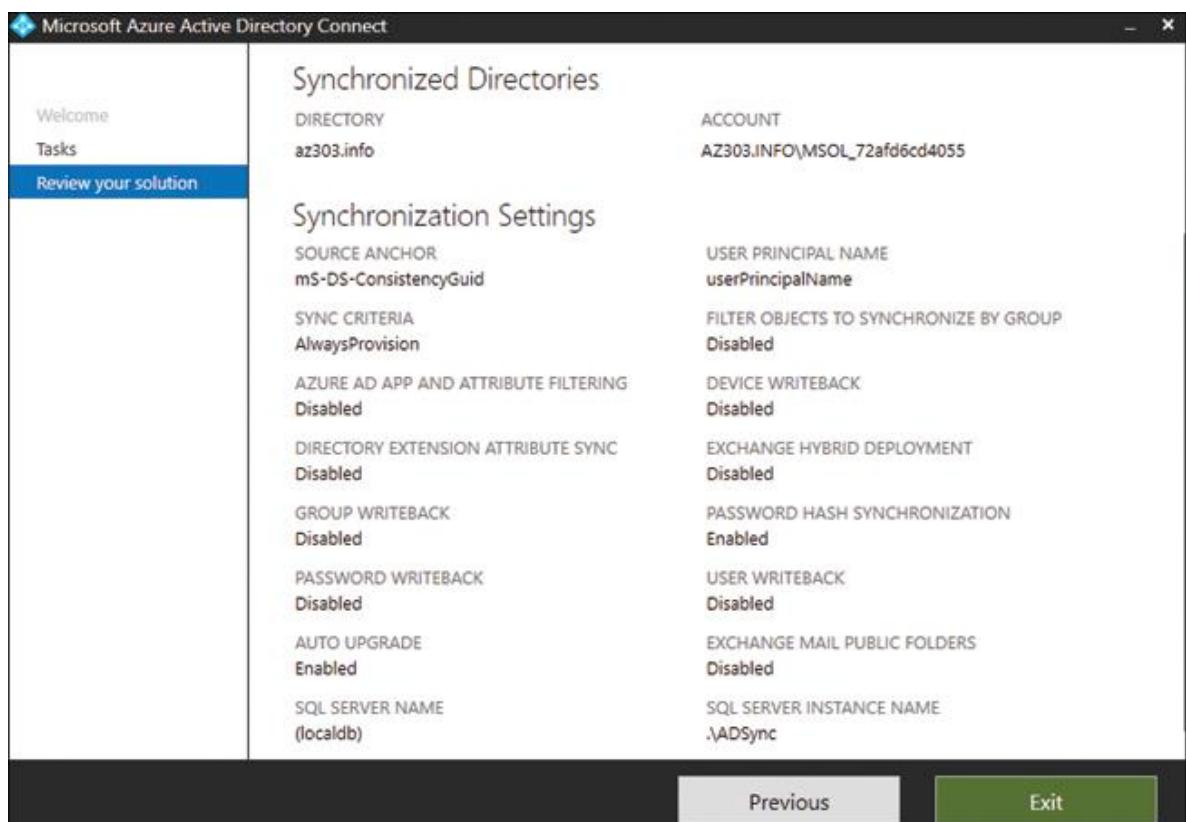


FIGURA 1-75 Configuración actual de la sincronización de Azure AD Connect

2. Tenga en cuenta la cuenta que se muestra en la parte superior derecha. Esta es la cuenta de servicio creada por Azure AD Connect para el proceso de sincronización. Esta cuenta debe tener los

siguientes permisos agregados para la escritura diferida de contraseñas:

1. ■ Restablecer contraseña
2. ■ Escribir permisos en `lockoutTime`
3. ■ Escribir permisos en `pwdLastSet`
4. ■ Derechos ampliados para la contraseña sin expirar en
 1. ■ El objeto raíz de cada dominio de ese bosque
 2. ■ Las unidades organizativas (OU) de usuario que desea que estén incluidas en el ámbito de SSPR
3. Abra **Usuarios y equipos de Active Directory**. En **Ver** en la parte superior, elija **Funciones avanzadas**. Haga clic con el botón derecho en la raíz del dominio y elija **Propiedades**.
4. Haga clic en la pestaña **Seguridad** en la parte superior y luego haga clic en **Avanzado**. Haga clic en **Agregar**. Los primeros tres permisos deben aparecer en la columna **Acceso** del panel de **Entrada de permisos** para la cuenta anotada en el paso 2. El nombre de la cuenta de la Figura 1-75 debe seleccionarse en **Principal**. Si falta alguno, agréguelos.
5. El último permiso enumerado en el Paso 2 se logra estableciendo la **Antigüedad mínima de la contraseña** en **0** en la Política de grupo. Abra el **Administrador del servidor**, haga clic en **Herramientas** en la parte superior derecha y luego haga clic en **Administración de políticas de grupo**.
6. Edite la política relevante para el alcance de OU de sus usuarios. La **antigüedad mínima de la contraseña** se encuentra seleccionando **Configuración del equipo > Políticas > Configuración de Windows > Configuración de seguridad > Políticas de cuenta**. Haga clic en **Aceptar**, cierre **Administración de políticas de grupo** y ejecute `gpupdate / force` en la línea de comando para forzar la actualización de la política.
7. Vuelva a Azure AD Connect y haga clic en **Anterior > Personalizar opciones de sincronización**. Ingrese las credenciales de un administrador global y haga clic en **Siguiente**.

8. Haga clic en **Siguiente** dos veces para acceder a la página **Funciones opcionales**. Seleccione **Reescritura de contraseña**, como se muestra en la Figura 1-76, haga clic en **Siguiente** y luego en **Configurar**.

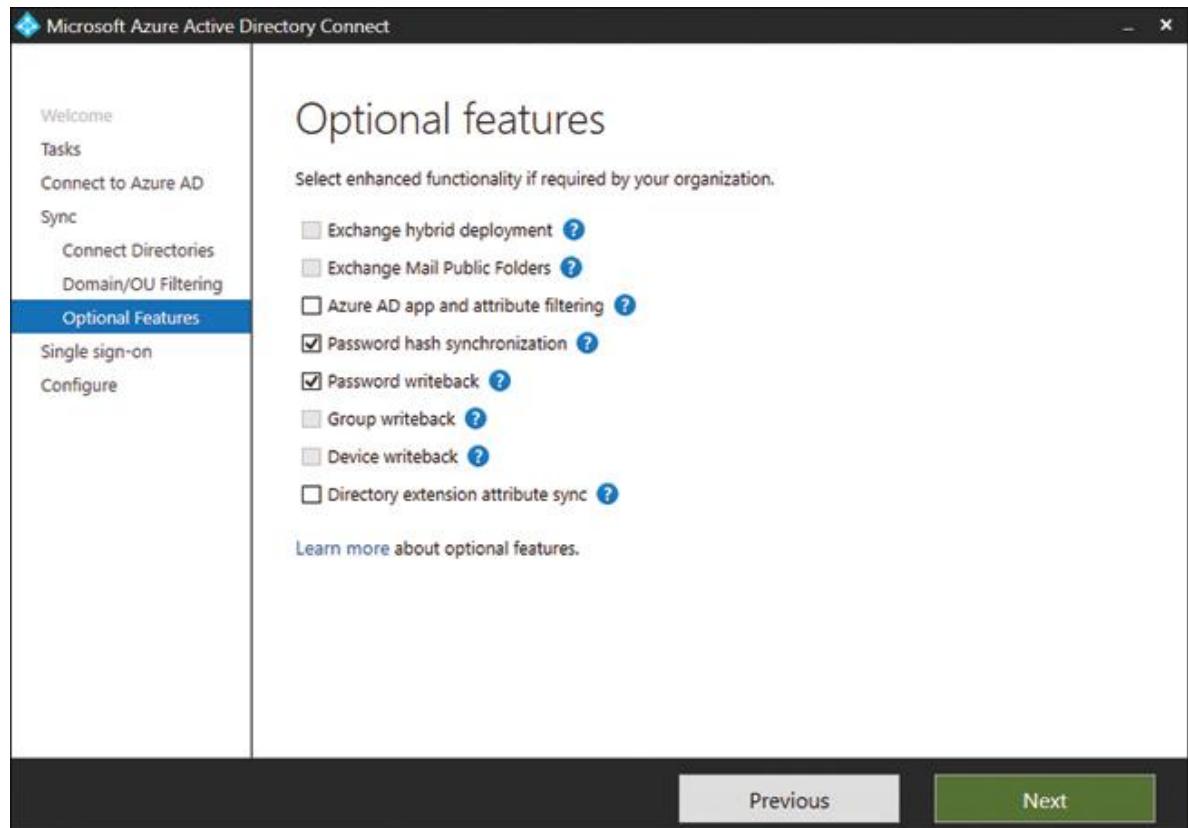


FIGURA 1-76 Selección de escritura diferida de contraseña en las características opcionales de Azure AD Connect

Azure AD Connect ahora habilitará la escritura diferida de contraseñas y configurará los servicios adecuados en el servidor local.

La parte final es configurar el restablecimiento de contraseña de autoservicio (SSPR) para escribir los cambios de contraseña en el controlador de dominio. Se asume que SSPR ya se ha configurado, pero si no lo ha habilitado, consulte “Implementar el restablecimiento de contraseña de autoservicio” anteriormente en este capítulo. Para configurar la escritura diferida de contraseñas con SSPR, inicie sesión en Azure Portal como administrador global:

1. Abra Azure Portal y busque **Azure Active Directory** en el cuadro de recursos de búsqueda en la parte superior del portal. Presione

Entrar para seleccionar **Azure Active Directory** y luego seleccione **Restablecer contraseña** en la hoja de menú.

2. Seleccione **Integración local** en la hoja de menú **Restablecimiento de contraseña**. Los pasos anteriores 1 a 8 de la última sección para habilitar la escritura diferida de contraseñas han configurado **Escritura diferida ¿Contraseñas para su directorio local? a sí**. El mensaje **Your On-Premises Client Is Up And Running** se muestra en la Figura 1-77.
3. Opcionalmente, puede cambiar la opción **¿ Permitir a los usuarios desbloquear cuentas sin restablecer su contraseña?** el establecimiento de **n**.

The screenshot shows the 'Password reset | On-premises integration' page in the Azure Active Directory portal. The 'On-premises integration' section is highlighted. A green checkmark icon indicates that the 'Your on-premises writeback client is up and running.' message is displayed. There are two configuration options with 'Yes' selected: 'Write back passwords to your on-premises directory?' and 'Allow users to unlock accounts without resetting their password?'. The 'Save' button is visible at the top right.

FIGURA 1-77 Habilitación de la escritura diferida de contraseñas para Azure AD SSPR

4. Haga clic en **Guardar**.

La escritura diferida de contraseña ahora está habilitada. Puede probar esto restableciendo la contraseña de un usuario usando Mis aplicaciones

(<https://myapps.microsoft.com>) y luego registrando al usuario en un servidor o estación de trabajo en su dominio.

¿Necesita más revisión? Configurar la escritura diferida de la contraseña

Para obtener información sobre cómo configurar la sincronización y la escritura diferida de contraseñas, visite el artículo de Microsoft Docs "Tutorial: Habilite la escritura diferida de restablecimiento de contraseña de autoservicio de Azure Active Directory en un entorno local" en <https://docs.microsoft.com/en-us/azure/directory-active-authentication/concept-sspr-writeback>.

Configurar el inicio de sesión único

Sus usuarios ahora pueden usar las mismas credenciales en aplicaciones locales y en la nube; sin embargo, deben ingresar sus credenciales en cada inicio de sesión. El inicio de sesión único sin interrupciones de Azure AD (SSO sin interrupciones de Azure AD) es una característica de Azure AD que registra automáticamente a un usuario en sus aplicaciones en la nube sin que el usuario tenga que escribir la contraseña.

Azure AD Seamless SSO se habilita a través de una configuración en Azure AD Connect. Cuando está habilitado, se crea una cuenta de computadora llamada AZUREADSSOACC en el Active Directory local. Esta cuenta de equipo representa Azure AD y la contraseña de la cuenta se almacena de forma segura con Azure AD. Cuando los usuarios ingresan sus nombres de usuario en una página de inicio de sesión de Azure AD, se ejecuta un script JavaScript en segundo plano para que el usuario acceda a AZUREADSSOACC. El Active Directory local devuelve un vale de Kerberos al navegador, que está encriptado con el secreto de la cuenta. El vale de Kerberos se pasa de forma segura a Azure AD, que lo descifra. El ticket de Kerberos incluye la identidad del usuario que inició sesión en el dispositivo. Azure AD evalúa el ticket y devuelve un token de autenticación a la aplicación o solicita MFA. En caso de éxito, el usuario inicia sesión en la aplicación.

El SSO transparente de Azure AD requiere que el dispositivo en el que el usuario inició sesión esté unido al dominio. También requería que el método de inicio de sesión fuera sincronización de hash de contraseña o

autenticación de paso. El SSO integrado de Azure AD no es compatible con ADFS.

Para habilitar el SSO transparente de Azure AD en un Azure AD Connect ya instalado y configurado, siga estos pasos:

1. RDP al servidor donde está instalado Azure AD Connect. Abra Azure AD Connect y haga clic en **Configurar**.
2. Haga clic en **Cambiar inicio de sesión de usuario** en la página **Tareas adicionales**. Ingrese las credenciales para una cuenta de administrador global de Azure AD. Haga clic en **Siguiente**.
3. Se muestra la página de inicio de **sesión del usuario**, que es idéntica a la que se muestra en la [Figura 1-68](#) en "Configurar y administrar la sincronización y la escritura diferida de contraseñas". Seleccione **Habilitar inicio de sesión único**. Nota **Habilitar inicio de sesión único** solo está disponible si se seleccionan **Sincronización de hash de contraseña** o **Autenticación de paso a través**, ya que estas son las opciones admitidas. Haga clic en **Siguiente**.
4. La **Habilitar inicio de sesión único** aparece la página, como se muestra en [la figura 1-78](#). Haga clic en **Ingresar credenciales** e ingrese las credenciales de un usuario con privilegios de administrador de dominio. Haga clic en **Aceptar**. Estas credenciales se utilizarán para configurar Active Directory para el inicio de sesión único.
5. Volverá a la página **Habilitar inicio de sesión único**. Ahora debe seleccionar **Ingresar credenciales**. Haga clic en **Siguiente** y luego en **Configurar**.

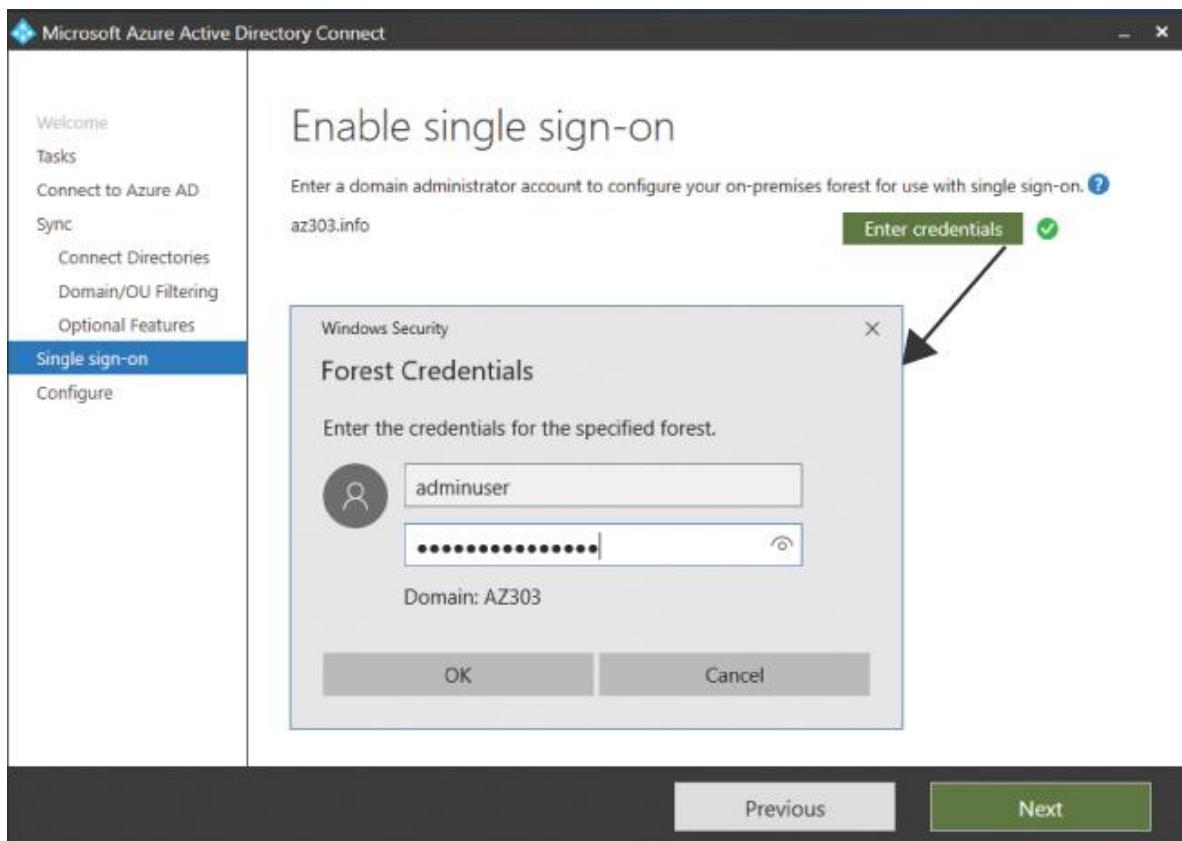


FIGURA 1-78 Introducción de credenciales de administrador de dominio para habilitar el inicio de sesión único en Active Directory para Azure AD Connect.

Azure AD Seamless SSO ahora está habilitado. Para verificar este cambio a Azure Portal, busque **Azure Active Directory** en la barra de recursos de búsqueda en la parte superior del portal. En la hoja de menú, seleccione **Azure AD Connect**. La página **Azure AD Connect** ahora debería mostrar que el inicio de sesión único sin interrupciones está habilitado, como se muestra en la [figura 1-79](#).

On-Premises Domain Name	Key Creation Date (UTC)	Status
az303.info	8/26/2020	(green checkmark)

FIGURA 1-79 Verificación de que el inicio de sesión único transparente está habilitado para local en Azure AD.

Aunque Azure Seamless SSO ahora está habilitado, si inició sesión como uno de sus usuarios en un dispositivo unido a un dominio, aún se le pedirá la contraseña. Esto se debe al vale de Kerberos; un navegador no enviará el ticket a un punto final en la nube a menos que sea parte de la zona de intranet del usuario. Esto significa que el ticket se está generando correctamente, pero no llega a Azure AD para ser evaluado. Para permitir que el ticket se pase a Azure AD, debe agregar el punto de conexión a la zona de intranet de cada usuario. Además, debe permitir el JavaScript que devuelve elPermiso de token de Kerberos para enviarlo al punto de conexión de Azure AD. Para lograr esto, debe editar la política de grupo en el controlador de dominio local, lo que también significa que puede implementar gradualmente esta función. Para editar la política de grupo, haga lo siguiente en su controlador de dominio:

1. Abra el **Administrador del servidor**, haga clic en **Herramientas** en la parte superior derecha y haga clic en **Administración de políticas de grupo**.
2. Edite la política adecuada para sus usuarios. Vaya a **Configuración de usuario > Política > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página de seguridad**. Luego seleccione **Lista de asignación de sitio a zona**.
3. Habilite la política y luego haga clic en **Mostrar** en las **asignaciones de zona**. Configure lo siguiente:
 1. ■ **Nombre del valor** : <https://autologon.microsoftazuread-sso.com>
 2. ■ **Valor - 1**
4. Haga clic en **Aceptar** y luego en **Aceptar** una vez más.
5. Permaneciendo en el editor de políticas, vaya a **Configuración de usuario > Política > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página de seguridad > Zona de intranet**, y luego seleccione **Permitir actualizaciones a la barra de estado a través de un script**.
6. Habilite la política y luego haga **clic en Aceptar**.

Para determinar que Azure AD Seamless SSO funciona correctamente, puede iniciar sesión en (<http://myapps.microsoft.com>) . Asegúrese de haber borrado la memoria caché de su navegador y de ejecutar primero `gpupdate` en un símbolo del sistema. Si los pasos de esta sección se han seguido correctamente, solo necesitará ingresar su nombre de usuario pero no su contraseña. En su lugar, verá la página **Intentando** iniciar **sesión** antes de iniciar sesión en MyApps.

Si ha configurado un controlador de dominio de prueba en Azure para esta habilidad, puede agregar una máquina virtual de Windows 10 a su red virtual y unirla a su controlador de dominio. Entonces podrá completar esta prueba.

Utilice Azure AD Connect Health

Ahora que ha configurado Azure AD Connect, debe asegurarse de que el servicio sea confiable. Azure AD Connect Health supervisa la sincronización de la identidad de Azure AD Connect y usa agentes para registrar las métricas. Si usa la sincronización de hash de contraseña o la autenticación PassThrough, el agente se instala como parte de Azure AD Connect. Si usa ADFS, deberá descargar un agente de Azure AD. Las métricas devueltas a Azure AD Connect Health se muestran como componentes del panel en el portal de Azure AD Connect Health. Estos componentes del tablero cubren el uso, el rendimiento y las alertas. Azure AD Connect Health es una característica premium de Azure AD, por lo que requiere una SKU comprada.

Puede explorar las características de Azure AD Connect Health en Azure Portal. Busque el **directorio activo azul** en la barra de búsqueda del nombre del recurso en la parte superior del portal y presione Entrar. Ingresará a **Azure Active Directory** en la hoja **Descripción general**. En la parte superior de la hoja de descripción general se encuentra el widget de panel de **Azure AD Connect Health**, que proporciona un resumen rápido de si la sincronización de Azure AD Connect es correcta. Haga clic en el widget y se abre la hoja de **Azure AD Connect**. En la parte inferior, haga clic en **Azure AD Connect Health** en la sección **Health And Analytics**.

Haga clic en **Errores de sincronización** en la hoja de menú **Azure AD Connect Health**. Al hacerlo, se muestran resúmenes de los widgets del panel de control de los errores de sincronización de Azure AD Connect,

como los atributos duplicados y las discrepancias de datos. Si los errores se enumeran aquí, puede hacer clic en el widget y profundizar para investigar más.

Ahora haga clic en **Servicios de sincronización** en la hoja de menú de **Azure AD Connect Health**. Los servicios de sincronización enumeran los servicios que se sincronizan en este inquilino de Azure AD. La columna **Estado** muestra si el servicio está en buen estado o no, como se muestra en la [Figura 1-80](#). Al hacer clic en la línea de servicio, se profundizará en los servidores que componen el servicio, como se muestra en la [Figura 1-80](#).

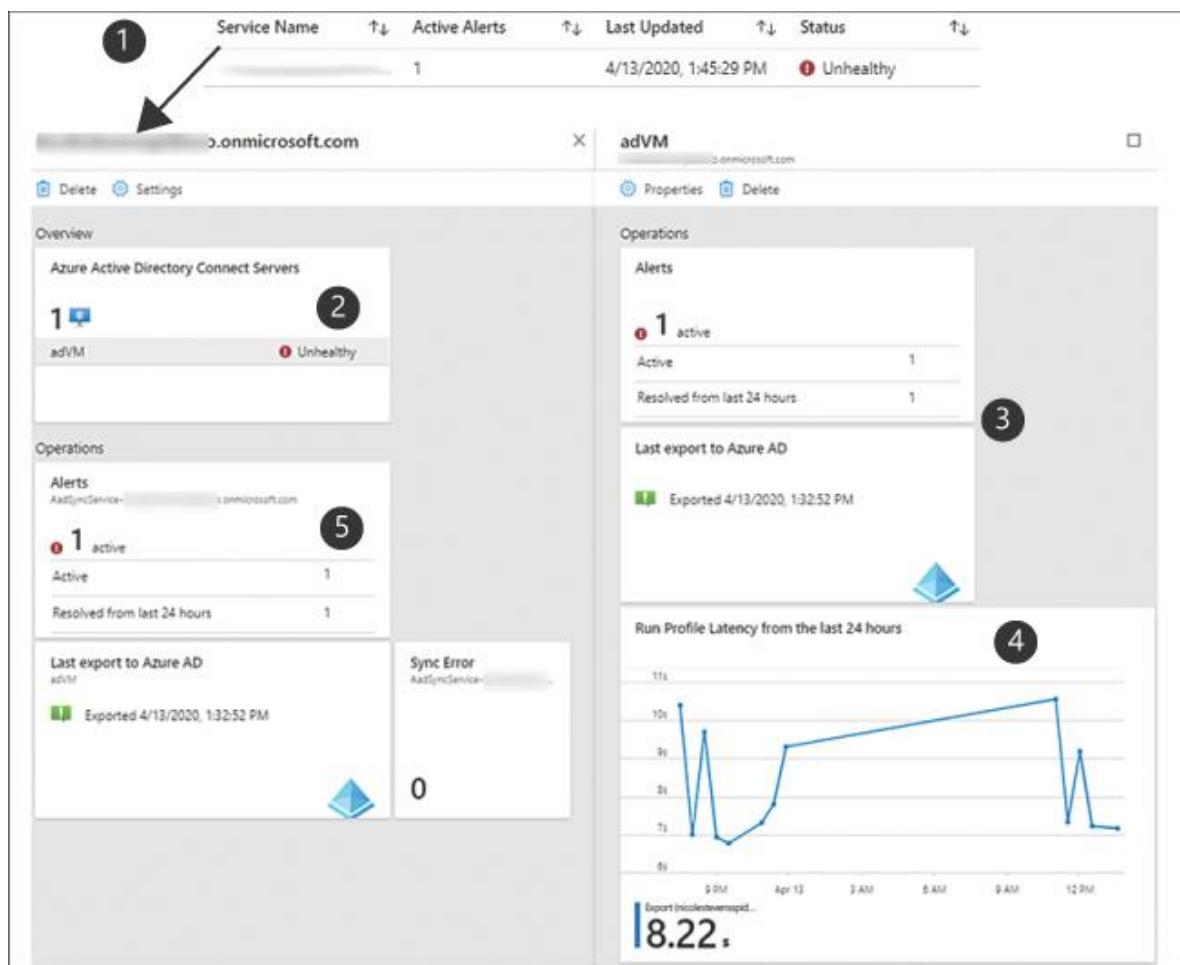
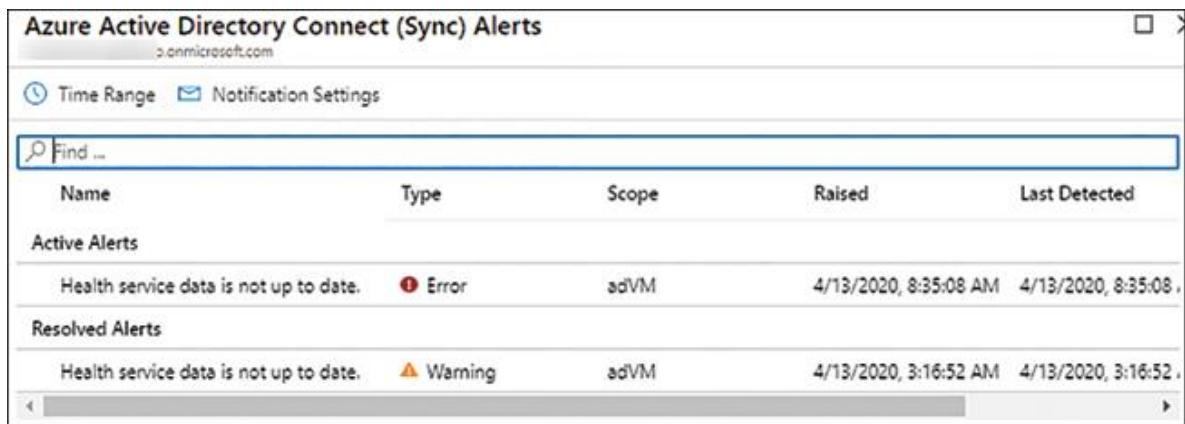


FIGURA 1-80 Métricas de servicios de sincronización de Azure AD Connect Health

A continuación se muestra una breve descripción general del widget de panel numerado de la [Figura 1-80](#):

1. Servicios de sincronización de Azure AD Health Connect.
2. Esta es una lista de servidores conectados al servicio a través de Azure AD Connect. La lista muestra si la sincronización de los servidores es correcta. Al seleccionar una máquina virtual en la lista, se mostrará una vista detallada, que se muestra a la derecha en la [Figura 1-80](#).
3. Esto se muestra cuando se explora desde la selección del mosaico 2. Esta es una lista de todas las alertas y el estado de exportación de la última exportación desde un Active Directory local a Azure AD.
4. Perforado desde la selección del segundo mosaico. De forma predeterminada, esta es la latencia de la exportación desde un Active Directory local a Azure AD. Puede hacer clic en este gráfico y editarla para mostrar otros conectores. Tenga en cuenta la falta de puntos métricos durante las horas nocturnas del 13 de abril. Esto muestra una sincronización incorrecta durante este período de tiempo. Esto se simuló al desasignar el controlador de dominio.
5. Alertas actuales de los servidores conectados. Haga clic en el widget de **Alertas** para obtener más información, como se muestra en la [Figura 1-81](#).



The screenshot shows a table titled "Azure Active Directory Connect (Sync) Alerts" with the URL "3.onmicrosoft.com". The table has columns: Name, Type, Scope, Raised, and Last Detected. It displays two rows under "Active Alerts": "Health service data is not up to date." (Error, adVM, 4/13/2020, 8:35:08 AM, 4/13/2020, 8:35:08) and "Health service data is not up to date." (Warning, adVM, 4/13/2020, 3:16:52 AM, 4/13/2020, 3:16:52). There is also a section for "Resolved Alerts" which is currently empty.

Name	Type	Scope	Raised	Last Detected
Active Alerts				
Health service data is not up to date.	Error	adVM	4/13/2020, 8:35:08 AM	4/13/2020, 8:35:08
Resolved Alerts				
Health service data is not up to date.	Warning	adVM	4/13/2020, 3:16:52 AM	4/13/2020, 3:16:52

FIGURA 1-81 Alertas de sincronización de estado de Azure AD Connect

Haga clic en una alerta para ver los detalles completos de la alerta y los enlaces sugeridos para ayudar a solucionar el problema. En la parte superior de la página de **Alertas de Azure Active Directory Connect (Syncs)** hay un vínculo de **configuración de notificaciones** (consulte la [figura 1-81](#)). De forma predeterminada, las alertas se envían por

correo electrónico a todos los administradores globales. Haga clic en este enlace para configurar los ajustes de notificación.

RESUMEN DEL CAPÍTULO

- ■ Azure Security Center y Azure Sentinel le brindan la capacidad de monitorear la seguridad de su infraestructura.
- ■ Puede implementar Log Analytics como un almacén centralizado para el registro y las métricas de sus servicios. Puede informar desde Log Analytics mediante Workbooks, KQL y Metrics Explorer a través de Azure Monitor.
- ■ Se debe utilizar Azure Monitor para obtener información cuando necesite información detallada sobre el rendimiento de las máquinas virtuales, las aplicaciones, las redes y los contenedores.
- ■ Azure Storage se puede configurar para proporcionar múltiples niveles de respaldo de datos y alta disponibilidad de datos. Azure Storage debe protegerse mediante la autenticación de Azure AD siempre que sea posible.
- ■ Azure Storage tiene límites en la cantidad de IOPS que puede proporcionar cada cuenta. Por lo tanto, al configurar el almacenamiento para máquinas virtuales, debe verificar las IOPS requeridas y distribuir los discos entre las cuentas de almacenamiento cuando sea necesario.
- ■ El emparejamiento de redes virtuales permite la comunicación entre redes en Azure sin necesidad de una VPN con emparejamiento de redes virtuales global que conecta redes virtuales entre regiones. Cuando se requieren comunicaciones cifradas entre redes en Azure, debe considerar una VPN de red virtual a red virtual.
- ■ Las identidades híbridas brindan a sus usuarios una identidad de usuario común para la autenticación y autorización tanto en la nube como en las instalaciones. Si desea utilizar el inicio de sesión único con identidades híbridas, pero no puede almacenar contraseñas en la nube, utilice la autenticación de paso.

- Azure AD Identity Protection es una función de Azure AD Premium P2 que utiliza Intelligent Security Graph de Microsoft para detectar posibles vulnerabilidades con sus identidades de usuario.
- Utilice la autenticación multifactor para evitar que los agentes malintencionados accedan a las cuentas mediante el uso de un segundo factor de autenticación. Al implementar la autenticación multifactor, utilice el acceso condicional para cumplir con los requisitos de las mejores prácticas.
- Infraestructura como código utilizando plantillas de Azure ARM le brinda la capacidad de automatizar las implementaciones de su infraestructura, haciéndolas repetibles. Al implementar recursos utilizando la infraestructura como código para almacenar sus secretos en Azure Key Vault.

EXPERIMENTO MENTAL

En este experimento mental, demuestre sus habilidades y conocimiento de los temas cubiertos en este capítulo. Puede encontrar las respuestas a las preguntas del experimento mental en la siguiente sección, "Respuestas al experimento mental".

Usted es un arquitecto de soluciones de Azure contratado por Wide World Importers para ayudar con una migración de "elevación y cambio" de sus máquinas virtuales locales a Azure. Wide World Importers actualmente no tiene infraestructura en ninguna nube privada; sin embargo, tiene uso de Microsoft 365 en toda la empresa. Durante las conversaciones con Wide World Importers, los siguientes elementos se identifican como requisitos:

Las cargas de trabajo que se ejecutan en la nube deben estar aisladas para que la comunicación sea privada para cada carga de trabajo. Las cargas de trabajo se gestionarán desde un punto central. Cinco de las cargas de trabajo tienen una infraestructura idéntica que respalda el proceso de desarrollo de la aplicación de seguimiento de inventario inteligente de Wide World Importers. Estas cargas de trabajo deben eliminarse y recrearse con el mínimo esfuerzo.

Wide World Importers ha estado recibiendo informes de que los usuarios de su aplicación de seguimiento de inventario inteligente basada en .Net

han experimentado frecuentes períodos de inactividad y excepciones. Los desarrolladores de la aplicación de seguimiento de inventario inteligente están luchando por encontrar una solución.

El inicio de sesión único se utiliza para la autenticación de aplicaciones internas. Este requisito debe llevarse a cabo, pero la seguridad de las credenciales es una preocupación.

Los usuarios de nivel de administrador en Azure deben usar contraseñas seguras y otro nivel de autenticación. Todos los administradores son usuarios de teléfonos inteligentes. Todos los usuarios de aplicaciones internas que no se encuentran en la oficina deben utilizar más de un método de autenticación al iniciar sesión.

Teniendo en cuenta los requisitos descubiertos, responda las siguientes preguntas:

1. 1. ¿Qué recomendaría para el despliegue de la infraestructura y el aislamiento de la comunicación?
2. 2. ¿Qué herramienta de supervisión sería la más adecuada para ayudar a los desarrolladores a solucionar los problemas de las excepciones de sus aplicaciones y realizar un seguimiento de la disponibilidad?
3. 3. ¿Qué solución abordará las inquietudes sobre las credenciales de Wide World Importers mientras continúa brindando capacidades de inicio de sesión único?
4. 4. ¿Cómo se pueden cumplir los requisitos administrativos y de seguridad de las cuentas de usuario?

RESPUESTAS DEL EXPERIMENTO MENTAL

Esta sección contiene la solución al experimento mental de este capítulo. Tenga en cuenta que puede haber otras formas de lograr el resultado deseado. Cada respuesta explica por qué la respuesta es correcta.

1. Es una buena práctica implementar la infraestructura en Azure utilizando la infraestructura como código (IaC). Las plantillas de Azure Resource Manager (ARM) son el método recomendado para implementar en Azure mediante IaC. Una plantilla ARM se puede

reutilizar para múltiples entornos utilizando parámetros, que cumplen los criterios para ser reutilizable con un esfuerzo mínimo. Las redes virtuales aislan el tráfico de red dentro de Azure. Al implementar el emparejamiento de redes virtuales mediante una topología de concentrador y radio, los importadores de Wide World pueden aislar el tráfico de cargas de trabajo mientras mantienen un concentrador central para el mantenimiento.

2. Los puntos clave aquí son el uso singular de la palabra herramienta y los tipos de problemas que los desarrolladores necesitan ayuda para rectificar. Application Insights es un servicio de gestión del rendimiento de las aplicaciones (APM) que analiza una aplicación en tiempo real. Application Insights admite dotnet, lo que significa que los desarrolladores pueden usarlo para la instrumentación de la aplicación para ver las excepciones. Los conocimientos de las aplicaciones también incluyen el seguimiento y las alertas de la disponibilidad de las aplicaciones, lo que permite a los equipos de desarrollo y operaciones responder a los eventos con mayor rapidez.
3. Había una pequeña pista aquí en el resumen en la parte superior de la página anterior. Si los importadores de Wide World ya usan Microsoft 365, es posible que Azure AD Connect ya se esté usando para sincronizar las identidades de los usuarios con Azure AD. Azure AD Connect con autenticación PassThrough proporciona una capacidad de inicio de sesión único sin problemas. Con la autenticación PassThrough, no se almacenan contraseñas en la nube, lo que resuelve los problemas de seguridad de credenciales de Wide World Importers.
4. Azure AD viene con capacidad de autenticación multifactor (MFA) para administradores de Azure. Sin embargo, las políticas de acceso condicional son la forma recomendada por Microsoft de implementar MFA. Las políticas de acceso condicional se pueden utilizar para cumplir con los requisitos de usuario administrativo y fuera de la oficina para Wide World Importers. El acceso condicional requiere un nivel de Azure AD Premium P1; por lo tanto, es posible que sea necesario actualizar las licencias de AD de Wide World Importers.

Capítulo 2

Implementar soluciones de gestión y seguridad

Las organizaciones aún están trabajando en los detalles para llegar a la nube. Con todo el hardware y los servidores que se ejecutan en centros de datos y espacios de coubicación, mudarse a la nube aún requiere un poco de esfuerzo.

La arquitectura de soluciones en Azure no es solo el desarrollo o la gestión de la infraestructura en la nube. Es mucho más que eso, y debe comprender cómo los recursos de Azure que una organización necesita para operar a veces se centrarán en el desarrollo y, a veces, en la infraestructura. Depende de usted saber lo suficiente sobre estos temas.

Este capítulo le ayuda a comprender cómo puede llevar sus cargas de trabajo existentes a Azure al permitir el uso de algunos recursos familiares (máquinas virtuales IaaS) y otros que pueden ser nuevos (como la informática sin servidor) en su entorno. Además, el uso de la autenticación multifactor (MFA) se trata aquí para garantizar que su entorno en la nube sea lo más seguro posible. Un arquitecto de soluciones de Azure puede enfrentarse a todas estas situaciones en la vida laboral diaria y debe estar preparado para cada una de ellas.

Habilidades cubiertas en este capítulo:

- ■ [Habilidad 2.1: administrar cargas de trabajo en Azure](#)
- ■ [Habilidad 2.2: implementar la recuperación ante desastres mediante Azure Site Recovery](#)
- ■ [Habilidad 2.3: Implementar la infraestructura de aplicaciones](#)
- ■ [Habilidad 2.4: administrar la seguridad de las aplicaciones](#)
- ■ [Habilidad 2.5: Implementar el equilibrio de carga de las aplicaciones y la seguridad de la red](#)
- ■ [Habilidad 2.6: Integrar una red virtual de Azure y una red local](#)

- ■ Habilidad 2.7: implementar y administrar soluciones de gobernanza de Azure
- ■ Habilidad 2.8: Implementar la autenticación multifactor (MFA)

HABILIDAD 2.1: ADMINISTRAR CARGAS DE TRABAJO EN AZURE

Debido a que la mayoría de las organizaciones han estado operando con una infraestructura que se ejecuta internamente, existe una gran oportunidad para ayudarlas a migrar estas cargas de trabajo a Azure, lo que podría ahorrar algunos costos y brindar eficiencias para estos servidores que sus centros de datos podrían no tener. También, es posible que algunas organizaciones quieran explorar la posibilidad de salir del negocio de los centros de datos. ¿Cómo puede ayudar a su organización o cliente a pasar de un centro de datos a la nube de Azure?

La herramienta recomendada para esto es Azure Migrate, que ofrece diferentes opciones según el tipo de carga de trabajo que esté migrando (física o virtual). Azure Site Recovery no ha desaparecido, aunque se usa principalmente para escenarios de recuperación ante desastres en los que Azure es el objetivo de la recuperación ante desastres. Consulte la Habilidad 2-2, "Implementar la recuperación ante desastres mediante Azure Site Recovery", para obtener más información.

Esta habilidad cubre:

- ■ Configurar los componentes de Azure Migrate
- ■ Migrar máquinas virtuales a Azure
- ■ Migrar datos a Azure
- ■ Migrar aplicaciones web
- ■ Configurar los componentes necesarios para migrar bases de datos a Azure SQL o una instancia administrada por Azure SQL

Configurar los componentes de Azure Migrate

Azure Migrate usa proyectos de migración para evaluar y administrar cualquier migración entrante de cargas de trabajo a Azure. Para crear un proyecto de migración y comenzar, siga estos pasos:

1. Determine el tipo de carga de trabajo para migrar:
 1. ■ **Servidores.** Servidores virtuales o físicos
 2. ■ **Bases de datos.** Bases de datos locales
 3. ■ **VDI.** Infraestructura de escritorio virtual
 4. ■ **Aplicaciones web.** Aplicaciones basadas en web
 5. ■ **Cuadro de datos.** Migración de datos sin conexión a Azure
2. Agregue las herramientas para la migración seleccionada para crear un proyecto de migración
3. Realizar una migración de las cargas de trabajo seleccionadas a Azure

Herramientas de evaluación de Azure Migrate

Antes de ejecutar la migración de cualquier carga de trabajo a Azure, con la excepción de una migración de Data Box, la evaluación del estado actual de los recursos locales ayudará a determinar el tipo de recursos de Azure necesarios, así como el costo de migrarlos a Azure..

Hay dos herramientas de evaluación para migrar servidores a Azure:

- ■ **Evaluación del servidor de Azure Migrate.** Este servicio ha sido la herramienta de evaluación incorporada durante algún tiempo y tiene sus raíces en Site Recovery. Descubrirá y revisará VMware, Hyper-V y servidores físicos para determinar si están listos y pueden realizar la transición a Azure.
- ■ **Mover.** Esta herramienta de evaluación fue una empresa de terceros hasta finales de 2019, que fue adquirida por Microsoft para ampliar las herramientas disponibles para obtener recursos en Azure. Con las evaluaciones realizadas por Movere, se carga un agente dentro del entorno local y se realizan análisis para determinar el volumen de servidores en el entorno. Movere

también proporciona información adicional, incluidas las instancias de SQL Server, las instancias de SharePoint y otras aplicaciones.

Además de las evaluaciones del servidor, Azure Migrate tiene herramientas para revisar las aplicaciones web existentes con Web App Migration Assistant y las bases de datos locales de SQL Server con el Servicio de migración de bases de datos. La evaluación de SQL Server también revisará el ajuste de las bases de datos descubiertas dentro de las tres ofertas de Azure para SQL Server: Azure SQL Database, Managed Instance SQL y SQL Server que se ejecutan en máquinas virtuales en Azure.

Nota Es posible que se requieran correcciones adicionales de Azure SQL

Al migrar bases de datos SQL, puede haber pasos adicionales identificados por la evaluación que deben corregirse en función de la implementación de destino del SQL elegido. En nuestra experiencia, Azure SQL Database tendrá la mayor cantidad de elementos para revisar porque es la opción más diferente (y potencialmente restringida por funciones).

Herramienta de evaluación del servidor de Azure Migrate

La herramienta de evaluación del servidor proporciona la siguiente información para ayudar a su organización a tomar las mejores decisiones al prepararse para mover recursos a Azure:

- **Preparación de Azure.** Esta herramienta determina si los servidores detectados localmente son buenos candidatos para migrar a Azure.
- **Dimensionamiento de Azure.** Esta herramienta estima el tamaño de una máquina virtual una vez que ha migrado a Azure, según las especificaciones existentes del servidor local.
- **Estimación de costos de Azure.** Esta herramienta de evaluación del servidor ayudará a estimar la tasa de ejecución de las máquinas que se migran a Azure.

La herramienta de evaluación del servidor no requiere agentes. La evaluación del servidor se configura como un dispositivo y se ejecuta en

una máquina virtual dedicada o un servidor físico en el entorno que se está evaluando.

Una vez que se ha escaneado un entorno para su evaluación, los administradores pueden revisar los resultados de la herramienta y los servidores de grupo para proyectos o ciclos de vida específicos. (La agrupación de servidores se realiza después de la evaluación). Luego, los grupos de servidores se pueden evaluar para la migración a Azure.

Al revisar los grupos de servidores para la migración, asegúrese de considerar aspectos como la conectividad a Azure y cualquier dependencia que puedan tener las aplicaciones o los servidores que se están moviendo.

Para completar una evaluación del entorno del servidor, realice los siguientes pasos:

1. Busque Azure Migrate en Azure Portal.
2. Cree un recurso de Azure Migrate desde Azure Portal seleccionando **Evaluar y migrar servidores** en la hoja **Información general**, como se muestra en la [Figura 2-1](#).

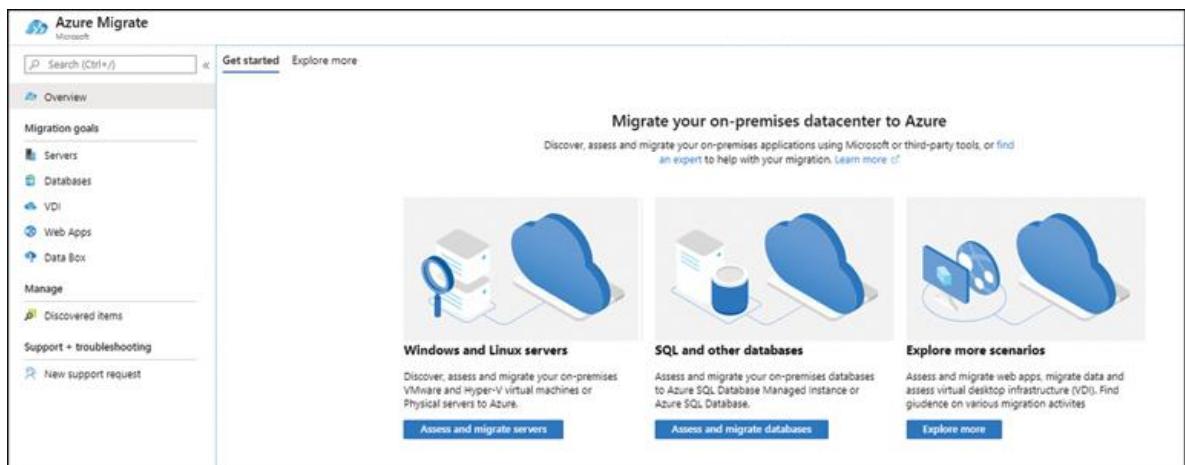


FIGURA 2-1 Elección de Evaluar y migrar servidores

3. Seleccione **Agregar herramienta (s)** para crear un proyecto y seleccione herramientas de evaluación y migración, como se muestra en la [Figura 2-2](#).

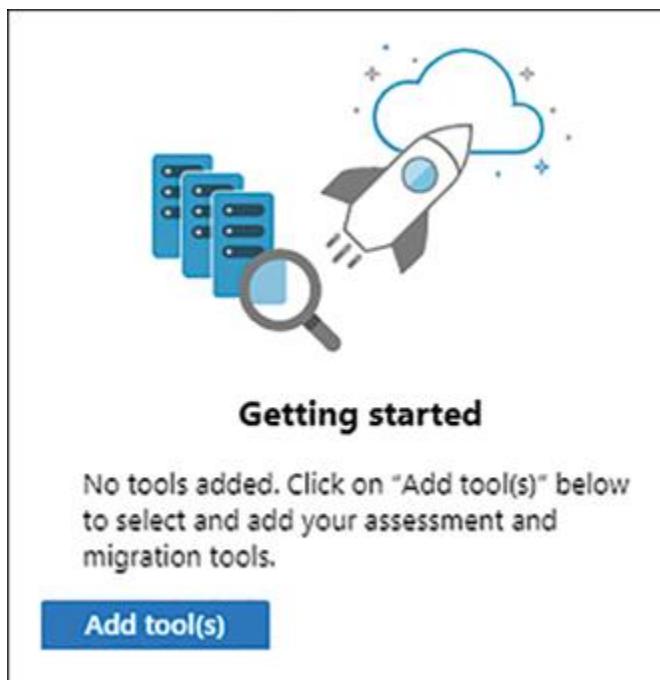


FIGURA 2-2 Selección de herramientas de evaluación y migración

4. Ingrese los detalles requeridos para el proyecto de migración para servidores, como se muestra en la Figura 2-3.

Add a tool

Migrate project Select assessment tool Select migration tool Review + add tool(s)

An Azure Migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ azure-migrate

Create new

PROJECT DETAILS

Specify the name of the migrate project and the preferred geography.

Migrate project * ⓘ Enter migrate project name.

Geography * ⓘ United States

FIGURA 2-3 Detalles para la configuración del proyecto de migración del servidor

5. Seleccione una **suscripción** .
6. Seleccione un **grupo de recursos** .
7. Ingrese un nombre para el proyecto de Azure Migrate.
8. Seleccione la herramienta **Azure Migrate: Server Assessment** y haga clic en **Siguiente** , como se muestra en la Figura 2-4 .

Add a tool

Migrate project Select assessment tool Select migration tool Review + add tool(s)

Start by choosing a server discovery and assessment tool. We recommend that you discover and assess your datacenter to determine migration readiness.

Tool	Pricing	Supported Workloads	Features	Learn more
 Azure Migrate: Server Assessment	View	VMware and Hyper-V virtual machines Import-based Assessments (Preview) Physical machines (preview)	Agentless discovery Cost planning and optimal right sizing Discovery of installed applications (preview) Application dependency analysis Cloud migration planning	Learn more
 Cloudmizer: Cloud Assessment	View	VMware and Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Corent Tech: SurPaaS MaaS	View	VMware and Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Device42: Device42	View	VMware and Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Application workload grouping	Learn more
 Turbonomic: Turbonomic	View	VMware and Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 UnityCloud: CloudRecon	View	VMware and Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Movere: Movere	View	VMware, Hyper-V and Xen virtual machines Physical machines Workstations (including VDI) Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more

[Previous](#) [Next](#)

FIGURA 2-4 Herramientas para la evaluación del servidor en Azure

9. Seleccione la casilla de verificación **Omitir agregar una herramienta de migración por ahora** y haga clic en **Siguiente** , como se muestra en la Figura 2-5 .

Add a tool

Migrate project Select assessment tool **Select migration tool** Review + add tool(s)

Choose a tool to migrate your on-premises servers to Azure.

Tool	Pricing	Supported Workloads	Features	Learn more
 Azure Migrate: Server Migration	View	VMware and Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agentless or agent-based migration Cutover in seconds Minimal application downtime	Learn more
 Carbonite: Carbonite Migrate	View	VMware and Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agent-based migration Cutover in seconds Minimal application downtime	Learn more
 Corent Tech: SurPaaS MaaS	View	VMware and Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows, Linux, Unix Agent-based migration Cutover in seconds Minimal application downtime	Learn more
 RackWare: Cloud Migration	View	VMware, Hyper-V, Xen and KVM virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agentless migration Cutover in seconds Minimal application downtime	Learn more

Note: Visit the ISV tools website to learn more about tool capabilities.
Don't see a tool that you are looking for? We are continuously adding support for more ISV tools. [Learn more](#).

Skip adding a migration tool for now

[Previous](#) [Next](#)

FIGURA 2-5 Herramientas de migración del servidor

- Revise las selecciones de evaluación realizadas y haga clic en **Agregar herramienta (s)**, como se muestra en la [Figura 2-6](#).

Add a tool

Migrate project Select assessment tool **Select migration tool** [Review + add tool\(s\)](#)

Settings

Subscription	Azure subscription 1
Resource group	azure-migrate
Geography	United States
Assessment tool	Azure Migrate: Server Assessment
Migration tool	-
Migrate project	(new) server-migration

[Add tool\(s\)](#) [Previous](#)

FIGURA 2-6 Revise las opciones y continúe

- Una vez que se ha elegido la herramienta de evaluación en Azure, es necesaria una configuración adicional del dispositivo.

12. Haga clic en **Descubrir** en **Herramientas de evaluación**. El cuadro de diálogo **Azure Migrate: Server Assessment** que se muestra en la Figura 2-7 a continuación.

The screenshot shows the Azure Migrate | Servers dashboard. On the left, there's a sidebar with 'Migration goals' (Servers, Databases, VDI, Web Apps, Data Box) and 'Manage' (Discovered items). Below that are 'Support + troubleshooting' sections for New support request and Discovered items. The main area is titled 'Assessment tools' and contains a box for 'Azure Migrate: Server Assessment'. It has tabs for Discover, Assess, and Overview, with 'Discover' selected. It includes a 'Quick start' section with steps 1: Discover (Discover your on-premises machines by using an appliance or importing in a CSV format. Click 'Discover' to get started.) and 2: Assess (Click 'Assess' to assess the discovered machines.). At the bottom of this box is a link 'Add more assessment tools? Click here.' To the right of this is another box titled 'Migration tools' for 'Azure Migrate: Server Migration', which also has tabs for Discover, Replicate, Migrate, and Overview, with 'Discover' selected. It includes a 'Quick start' section with steps 1: Discover (Click "Discover" to start discovering your on-premises machines.), 2: Replicate (Once your on-premises machines are discovered, click "Replicate" to start replicating the discovered machines.), and 3: Migrate (Once your machines have replicated, click "Migrate" to migrate your machines.).

FIGURA 2-7 Detección de servidores para la migración a Azure

13. Para usar un dispositivo, seleccione **Descubrir usando dispositivo**, como se muestra en la Figura 2-8.



FIGURA 2-8 Descubrimiento de servidores mediante un dispositivo autohospedado

14. Elija el tipo de hipervisor utilizado en el entorno: **Hyper-V, VMware o servidores físicos**.
15. Descargue el dispositivo e instálelo en el entorno.
16. Con un navegador, visite la dirección IP del dispositivo, configúrelo para llegar al proyecto de Azure Migrate y luego inicie el descubrimiento.

Después de aproximadamente 15 minutos, las máquinas que se detecten comenzarán a aparecer en Azure Migrate Discovery Dashboard.

También puede completar una plantilla CSV, que proporciona los detalles de su entorno, y luego cargarla en el proyecto de Azure Migrate si prefiere no usar el dispositivo de descubrimiento. Esto se muestra en la [Figura 2-9](#).

The screenshot shows the 'Discover machines' page in the Azure Migrate service. At the top, there are three tabs: 'Discover using appliance', 'Import using CSV' (which is selected), and 'Help me choose'. Below the tabs, a heading says 'Import your on-premises server inventory using a CSV file. You can use the imported inventory to create a quick assessment for migration to Azure VM or AVS.' A note below it says 'Use CSV import to get a quick assessment on cost and compatibility. For accurate assessments, use appliance-based discovery and profiling. [Learn more](#)'. The main content area is titled 'Steps to import using CSV.' It lists three steps: 1. Download CSV template, 2. Add server inventory data in the CSV file, and 3. Import the CSV file. Step 1 has a note about downloading the template and a 'Download .CSV file' button. Step 2 has a note about populating the CSV template with server inventory data. Step 3 has a note about the file being reviewed for errors and servers being added to the project. Below these steps is a 'Upload the CSV file' section with a 'Select a file' input field and a 'Import' button. To the right of the input field is a small 'Import' icon. On the left side of the import form, there's a 'Import details' section with dropdown menus for 'Import status', 'Records inserted', and 'Time of import'. At the bottom of the page, a note says 'You can start with creating assessments 10 minutes after the import is complete.'

FIGURA 2-9 Descarga de la plantilla CSV para proporcionar información sobre el medio ambiente

Evaluación y migración de *notas* : mejor juntos

La evaluación y la migración se analizan juntas aquí porque se usa la misma herramienta para ambas operaciones.

Para completar una evaluación y migración de una aplicación web, complete los siguientes pasos:

1. Dentro del proyecto de Azure Migrate existente, seleccione **Aplicaciones web** en la sección **Objetivos de migración** de la barra de navegación.
2. Seleccione **Agregar herramienta (s)** y elija **Azure Migrate: herramienta de evaluación de aplicaciones web**, como se muestra en la [Figura 2-10](#).

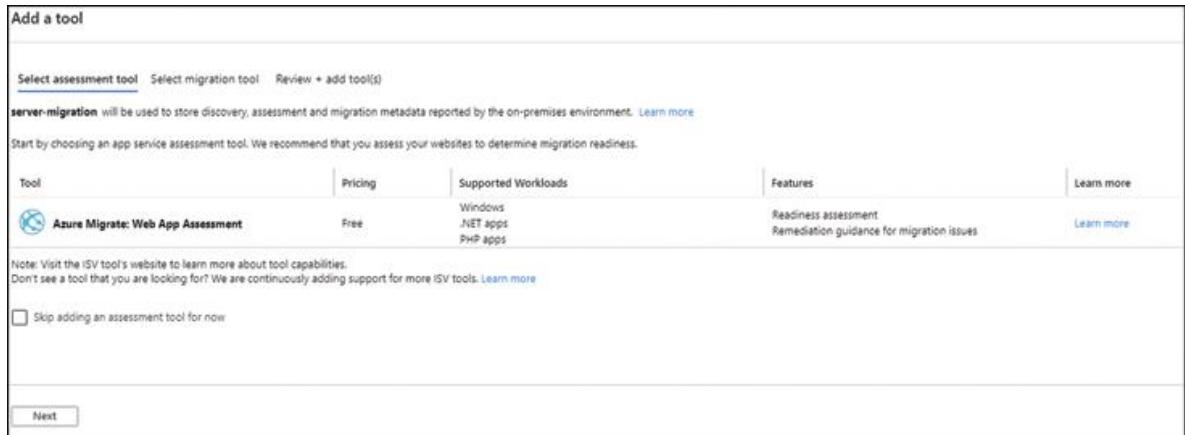


FIGURA 2-10 Adición de Azure Migrate: herramienta de evaluación de aplicaciones web

3. Haga clic en **Siguiente**.
4. Seleccione la casilla de verificación **Omitir agregar una herramienta de migración** y haga clic en **Siguiente**.
5. Después de revisar la configuración, haga clic en **Agregar herramienta (s)**.
6. Una vez que se haya agregado la herramienta de evaluación de aplicaciones web, descargue Azure App Service Migration Assistant para evaluar las aplicaciones web internas. Si la aplicación tiene una URL pública, se puede escanear a través de la Internet pública.
7. Instale la herramienta de evaluación en cualquier servidor web que contenga aplicaciones para la migración. IIS 7.5 y el acceso de administrador en los servidores son los requisitos mínimos para completar una evaluación. Actualmente, las aplicaciones PHP y .NET son compatibles con la migración, y pronto habrá más tipos de aplicaciones.
8. La herramienta de migración determinará si los sitios web seleccionados están listos para migrar a Azure, como se muestra en la [Figura 2-11](#).

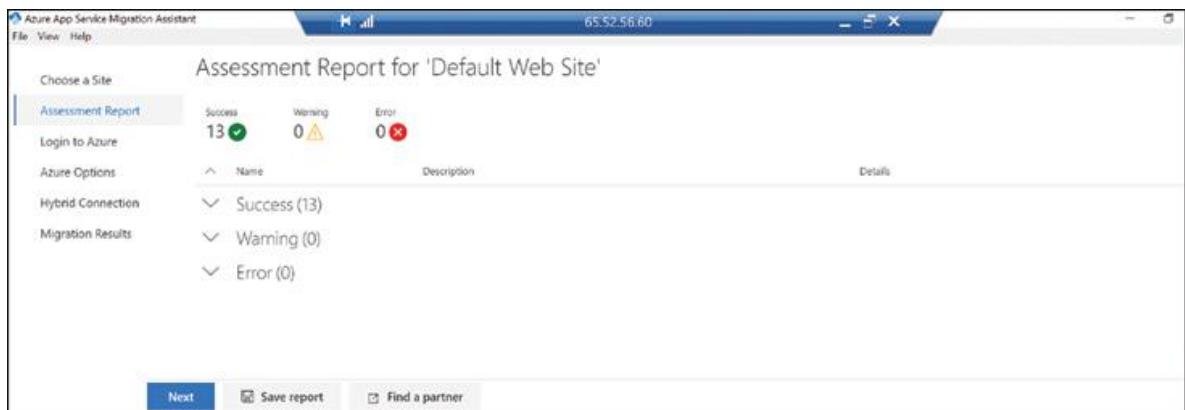


FIGURA 2-11 Evaluación del sitio web para la migración a Azure App Services

- Una vez que la herramienta de evaluación haya revisado las aplicaciones web elegidas, haga clic en **Siguiente** para iniciar sesión en Azure con el código de dispositivo proporcionado y el vínculo proporcionado en el asistente, que se muestran en la [Figura 2-12](#).

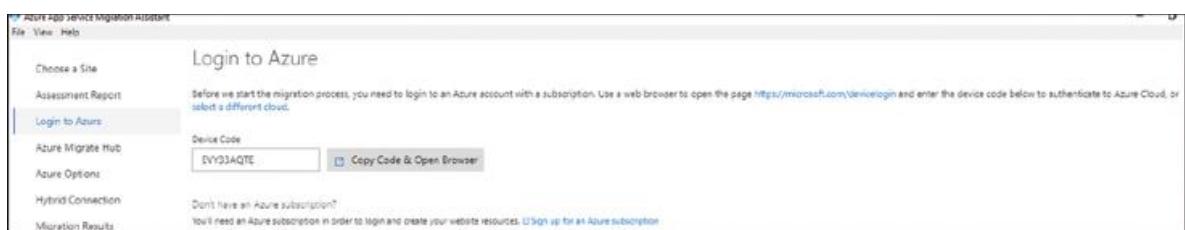


FIGURA 2-12 Utilice el vínculo proporcionado para abrir un explorador e iniciar sesión en su proyecto de Azure Migrate

- Haga clic en Opciones de Azure en el panel de navegación del lado izquierdo y configure las opciones **Suscripción**, **Grupo de recursos**, **Nombre del sitio de destino**, **Plan de servicio de aplicaciones**, **Región**, **Proyecto de migración de Azure** y **Bases de datos**, como se muestra en la [Figura 2-13](#).

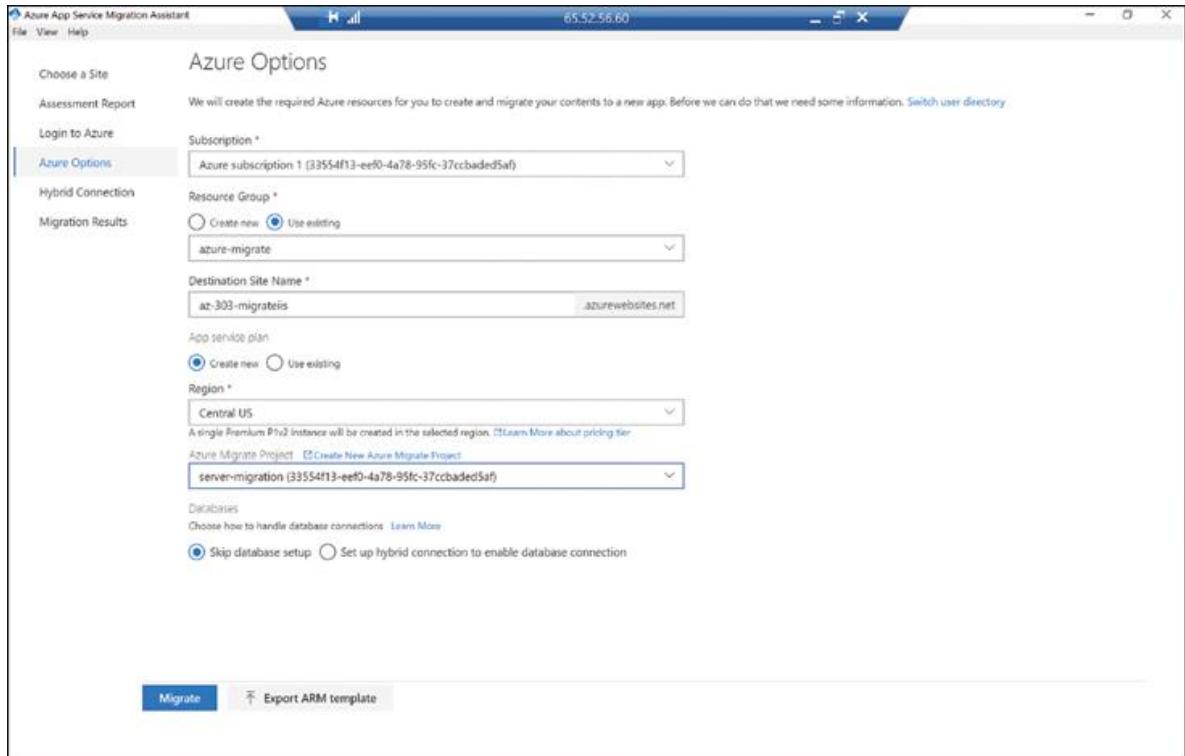


FIGURA 2-13 Opciones para la utilidad de aplicación web Azure Migrate

11. Si su aplicación tiene un back-end de base de datos, seleccione la opción **Configurar conexión híbrida para habilitar la conexión de base de datos** e ingrese el nombre del servidor de base de datos local y el puerto en el que conectarse en el campo Servidor de base de datos local que se muestra cuando la opción está seleccionado.
12. Haga clic en **Migrar** para migrar la aplicación tal cual o haga clic en el botón **Exportar plantilla ARM** en la pantalla **Opciones de Azure** para producir la plantilla ARM basada en JSON para la aplicación para su posterior implementación en Azure.
13. El progreso de la migración se muestra en la [Figura 2-14](#). También podrá ver los recursos una vez que se hayan migrado en Azure Portal.

Migration in Progress

Please wait while migration is in progress. This may take a few minutes. Once the migration is complete, we will take you to the next step.

- Sending server discovery data to Azure Migrate (step 1 of 1)
- Sending site assessment data to Azure Migrate (step 1 of 1)
- Sending site migration data to Azure Migrate (step 2 of 3)
- Creating site resources (step 1 of 3)
- Publishing site content (step 0 of 3)

FIGURA 2-14 Migración en proceso

Complete una evaluación y migración de la base de datos SQL mediante los siguientes pasos:

1. Dentro del proyecto de Azure Migrate, seleccione **Bases de datos > Agregar herramientas**.
2. Seleccione la herramienta **Azure Migrate: Database Assessment** y haga clic en **Next**, como se muestra en la [Figura 2-15](#).

The screenshot shows the 'Add a tool' interface. At the top, there are three tabs: 'Select assessment tool' (which is selected), 'Select migration tool', and 'Review + add tool(s)'. Below the tabs, a note states that 'server-migration' will be used to store discovery, assessment and migration metadata reported by the on-premises environment. It also recommends assessing your datacenter to determine migration readiness. The main area displays two tools: 'Azure Migrate: Database Assessment' and 'UnityCloud: CloudPilot'. Both tools are listed under the 'Pricing' column as 'Free'. Under 'Supported Workloads', both are listed as 'SQL Server 2005 - 2017'. The 'Features' column lists 'Target and size', 'Readiness assessment', 'Compatibility analysis', and 'Schema conversion' for both. There is a 'Learn more' link for each. A note at the bottom says to visit the ISV tool's website for more capabilities and to skip adding an assessment tool now. A 'Next' button is at the bottom.

FIGURA 2-15 Selección de la herramienta de evaluación de la base de datos en Azure Migrate

3. Para continuar con una migración si la evaluación produce el resultado esperado, seleccione la herramienta **Azure Migrate: Database Migration**.
4. Si está evaluando cargas de trabajo de producción y / o bases de datos extremadamente grandes, seleccione la casilla de verificación **Omitir agregar una herramienta de migración por**

ahora para permitir una revisión adicional de la evaluación para corregir cualquier problema encontrado.

5. Una vez que se hayan agregado las herramientas al proyecto de migración, como se muestra en la Figura 2-16, haga clic en el enlace **Descargar** para descargar la herramienta Evaluación de migración de la base de datos para comenzar la evaluación.

The screenshot shows the Azure Migrate | Databases interface. On the left, there is a navigation sidebar with the following items:

- Search (Ctrl+I)
- Overview
- Migration goals
 - Servers
 - Databases
 - VDI
 - Web Apps
 - Data Box
- Manage
 - Discovered items
 - Support + troubleshooting
 - New support request

In the center, there is a "Assessment tools" section. It features a "Azure Migrate: Database Assessment" card with a "Assess" button. Below this, there is a "Quick start" section with two steps:

- 1: Download DMA**
Download the Data Migration Assessment tool from [here](#)
- 2: Assess using DMA**
Once you have downloaded DMA, install it on a machine and assess your databases by following the steps mentioned [here](#)

At the bottom of the "Assessment tools" section, there is a link: "Add more assessment tools? Click here."

FIGURA 2-16 Herramientas de migración y evaluación de bases de datos

6. Instale y ejecute la herramienta Asistente de migración de datos en los servidores SQL que se migrarán a Azure.
7. En la herramienta Asistente de migración de datos, como se muestra en la Figura 2-17, haga clic en **Nuevo** para agregar un nuevo proyecto.

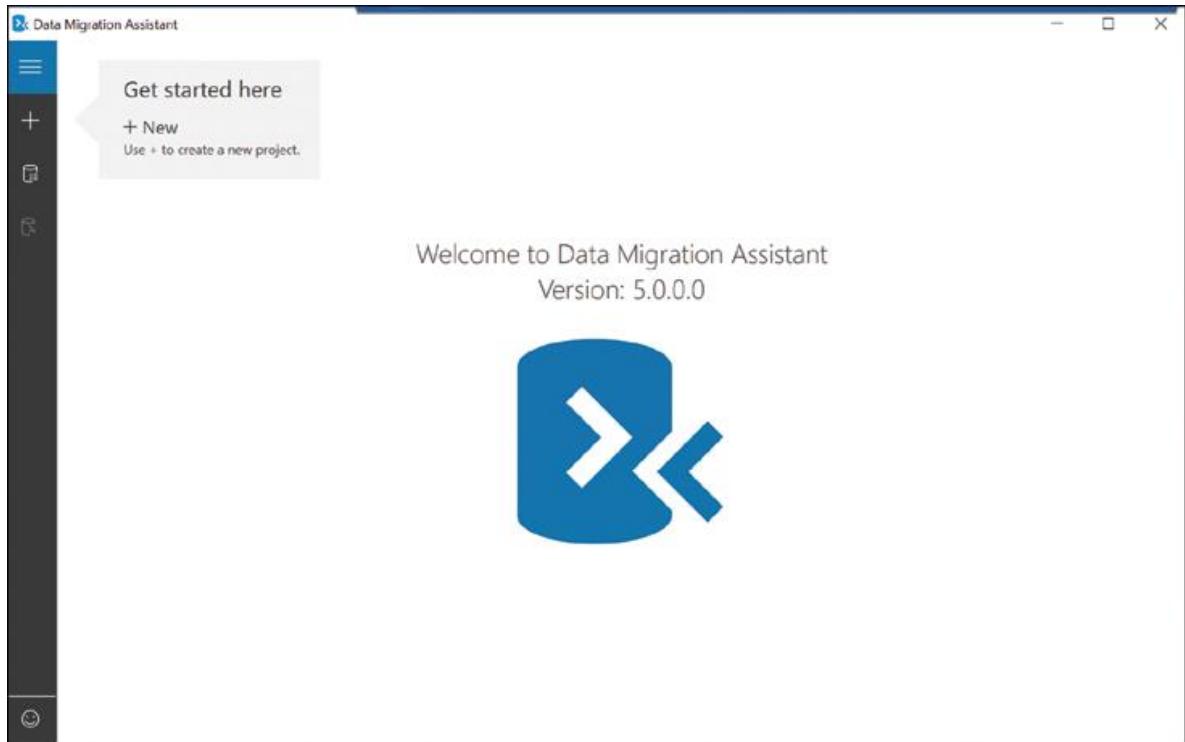


FIGURA 2-17 Asistente de migración de Azure

8. Ingrese un nombre para el proyecto y seleccione lo siguiente para los datos del servidor SQL que se migran:
 1. **Tipo de evaluación.** Elija motor de base de datos o servicios de integración.
 2. **Tipo de servidor de origen.** Elija SQL Server o AWS RDS para SQL Server.
 3. **Tipo de servidor de destino.** Elija entre Azure SQL Database, Azure SQL Database Managed Instance, SQL Server en Azure Virtual Machines o SQL Server.
9. En la pantalla **Opciones** dentro del proyecto creado, las siguientes son las opciones seleccionadas (y predeterminadas):
 0. **Verifique la compatibilidad de la base de datos.** Esto comprobará una base de datos existente en busca de problemas que impidan que se ejecute en Azure SQL.
 1. **Compruebe la paridad de funciones.** Esta opción busca funciones no compatibles en la base de datos de origen.

10. Seleccione los servidores SQL y elija los métodos de autenticación adecuados para el servidor SQL:
- 0.■ **Autenticación de Windows.** Utilice las credenciales de Windows con la sesión iniciada actualmente para conectarse.
 - 1.■ **Autenticación de SQL Server.** Utilice credenciales específicas almacenadas en el servidor SQL para conectarse.
 - 2.■ **Autenticación integrada de Active Directory.** Utilice el usuario de Active Directory que inició sesión para la autenticación.
 - 3.■ **Autenticación de contraseña de Active Directory.** Utilice una cuenta de servicio o un usuario de Active Directory específico para autenticarse.
11. Seleccione las propiedades para la conexión:
- 0.■ **Encriptar la conexión.** Marque esta casilla si SQL Server (y / o el equipo de seguridad de la información de su organización) requiere que las conexiones estén encriptadas.
 - 1.■ **Certificado de servidor de confianza.** Si SQL Server utiliza certificados, el Asistente de migración de datos puede confiar en estos certificados para simplificar las conexiones futuras.
12. Haga clic en **Conectar**.
13. De la lista de bases de datos encontradas, seleccione cualquiera que deba incluirse en la evaluación, como se muestra en la Figura 2-18.

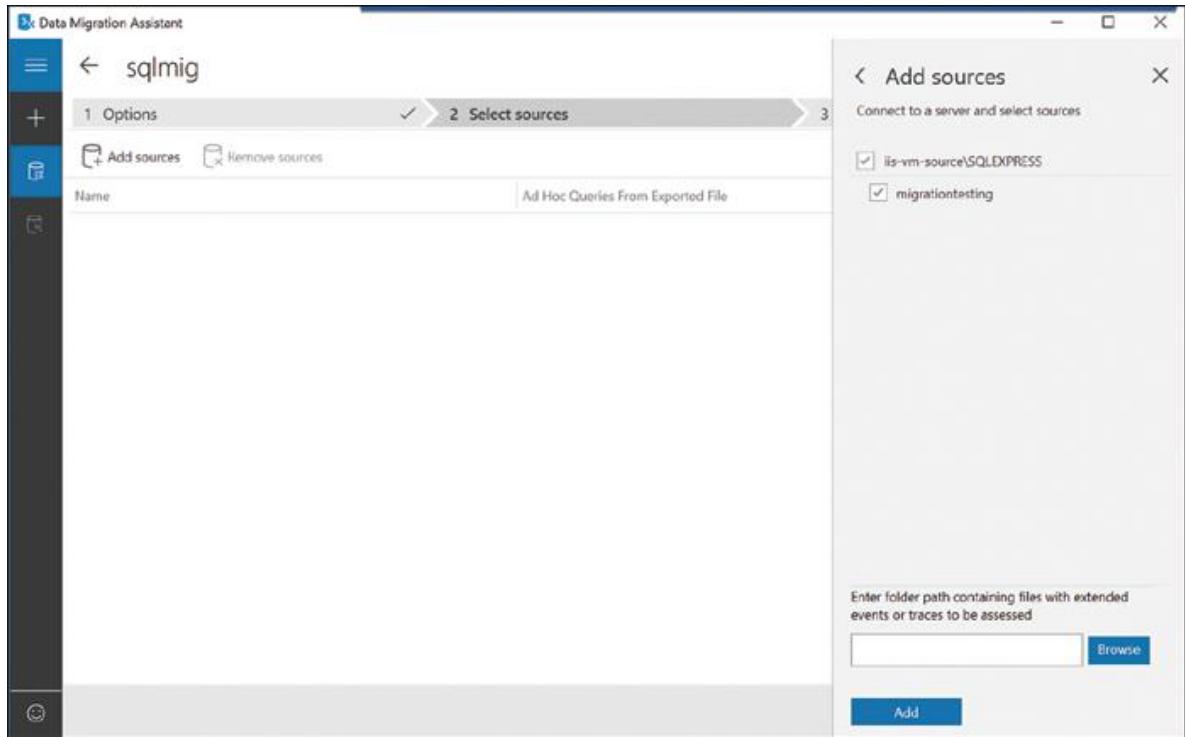


FIGURA 2-18 Incluir bases de datos seleccionadas en la evaluación

14. Haga clic en **Agregar**.
15. Una vez que las bases de datos se agregan a la evaluación, si hay archivos de registro o eventos extendidos para incluir, haga clic en **Examinar** para ubicarlos e incluirlos, como se muestra en la [Figura 2-19](#).

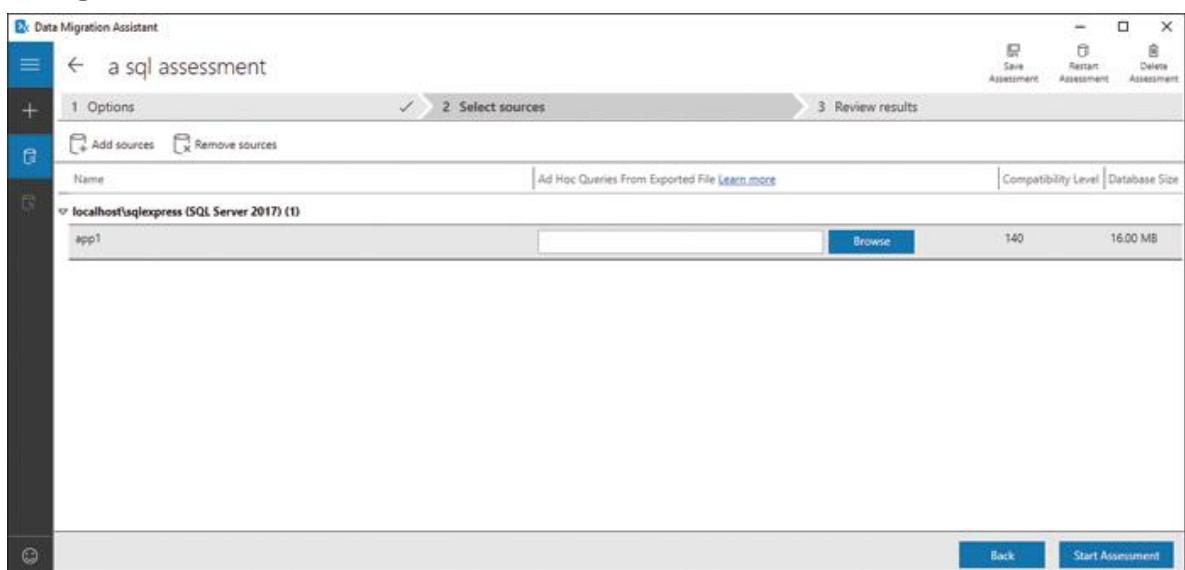


FIGURA 2-19 Incluya archivos de registro o eventos extendidos

16. Revise la evaluación tanto para la paridad de funciones como para la compatibilidad y solucione los problemas encontrados. Si hay discrepancias, deberán resolverse antes de que pueda continuar la migración.

Nota: algunos elementos pueden requerir trabajo adicional

La evaluación devolverá elementos que no son compatibles con Azure SQL pero que están en uso en las bases de datos de origen. También encontrará problemas de compatibilidad dentro de los datos de la base de datos de origen. Estos elementos deberán solucionarse antes de migrar los datos a Azure SQL.

17. Haga clic en **Cargar en Azure**.
18. Se le pedirá que inicie sesión si aún no lo ha hecho en la computadora donde se está ejecutando la evaluación.
19. Seleccione **Suscripción y grupo de recursos** y luego haga clic en **Cargar**.

La migración de información también es sencilla, aunque debe haber una base de datos SQL de Azure existente en la que migrar los datos SQL. Debe crear esta base de datos de Azure SQL de antemano porque las herramientas no compilarán Azure SQL u otros tipos de SQL en Azure como parte del proceso.

Para completar una migración después de la evaluación de las bases de datos SQL, complete los siguientes pasos:

1. En la herramienta Evaluación de migración de datos, seleccione la opción **Migraciones**.
2. Especifique la instancia de SQL de origen y el método de inicio de sesión.
3. Especifique el nombre y las credenciales de Azure SQL Server de destino y, a continuación, haga clic en **Conectar**.

Nota Acceso necesario para continuar

Deberá asegurarse de que el sistema donde se está ejecutando la migración tenga acceso a la base de datos SQL de Azure al

permitir el acceso desde la dirección IP del cliente dentro de los detalles de red de Azure SQL Server.

4. Seleccione la base de datos para migrar y haga clic en **Siguiente**, como se muestra en la Figura 2-20.

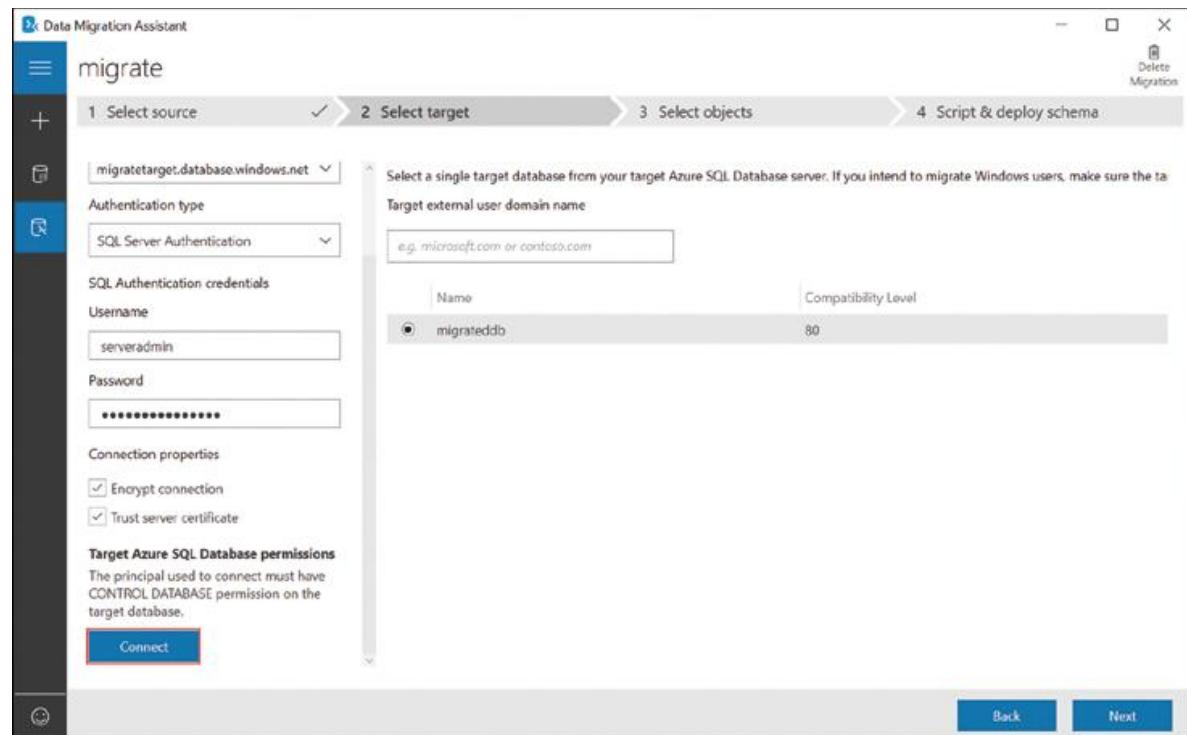


FIGURA 2-20 Conéctese a Azure para migrar datos de origen a Azure SQL Database

5. Una vez que se complete la preparación y se haya revisado, haga clic en **Generar secuencia de comandos SQL** para crear una secuencia de comandos. Un script generado se muestra en la Figura 2-21.

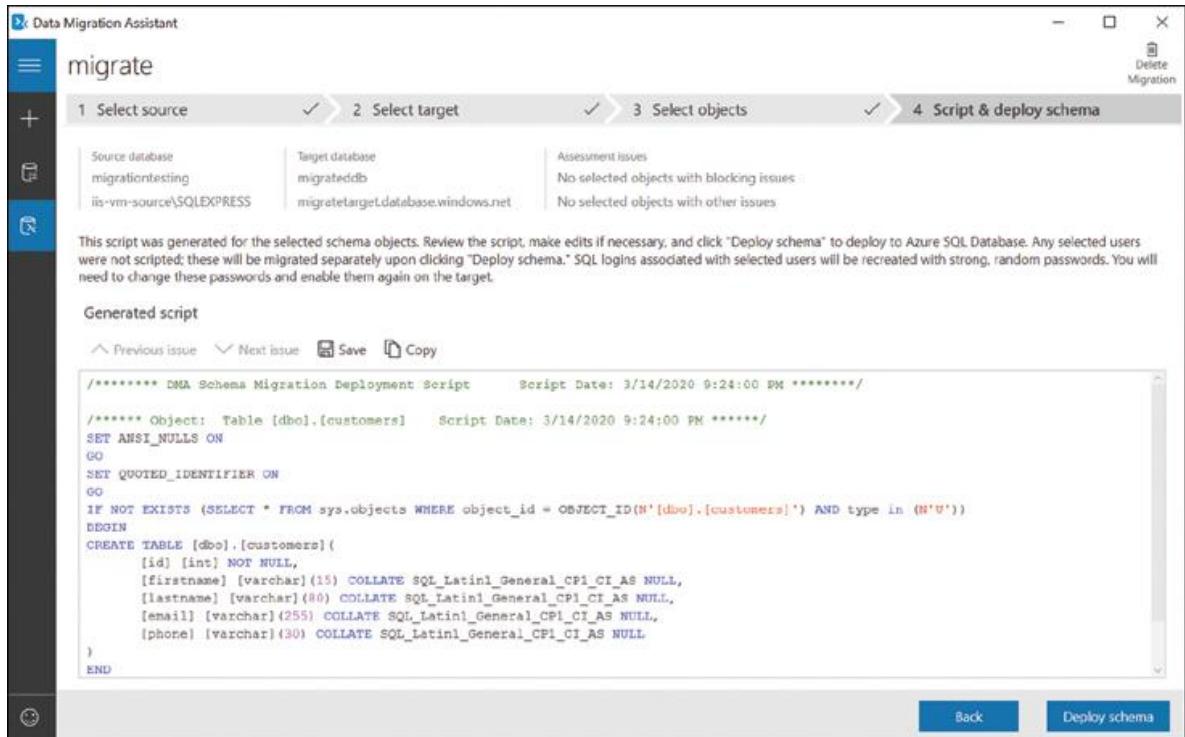


FIGURA 2-21 Un script SQL generado para el trabajo de migración

6. Para enviar estos datos a una instancia específica de Azure SQL Database mediante el Asistente de migración de datos, haga clic en **Implementar esquema** .

Migre la infraestructura de escritorio virtual a Azure

Azure Migrate también le permite llevar la infraestructura de escritorio virtual (VDI) a Azure. La evaluación de VDI requiere el uso de Lakeside: Systrack, una herramienta de terceros, para completar la evaluación de entornos VDI. Sin embargo, el proceso de migración sigue el mismo camino que una migración de servidor, lo que permite migrar cargas de trabajo de VMware o Hyper-V.

Azure Data Box permite la migración sin conexión de datos existentes a Azure. El Data Box en sí es un NAS reforzado que es capaz de almacenar hasta 100 TB de datos con cifrado AES 256 para transportar sus datos físicamente a los centros de datos de Azure para su ingestión.

Para completar una migración sin conexión de Data Box de cargas de trabajo a Azure, complete los pasos siguientes:

1. Desde dentro de un proyecto de Azure Migrate, seleccione **Cuadro de datos** como el **objetivo de migración**.
2. Proporcione los siguientes detalles sobre los datos que se están ingiriendo:
 - Suscripción.** Seleccione el nombre de la suscripción de Azure a la que se transferirán los datos.
 - Grupo de recursos.** Seleccione el grupo de recursos donde se transferirán los datos.
 - Tipo de transferencia.** Seleccione el tipo de transferencia que se está realizando.
 - País / región de origen.** Seleccione el país o la región donde residen los datos hoy.
 - Región de destino de Azure.** Seleccione la región en Azure donde deben residir los datos después de la transferencia.
3. Haga clic en **Aplicar**.
4. Seleccione la opción de Cuadro de datos adecuada para su migración, como se muestra en la Figura 2-22.

The screenshot shows the 'Data Box' section of the Azure Migrate migration target configuration interface. At the top, there are dropdown menus for Transfer type (Import to Azure), Subscription (Azure subscription 1), Resource group (site-recovery), Source country (United States), and Destination Azure region (North Central US). An 'Apply' button is also present. Below these, four data box options are listed:

- Data Box Disk (40 TB):** Total capacity per order. Options include: 35 TB usable capacity, Up to 5 disks per order, Supports Azure Blobs, Files, Managed Disks and ADLS Gen2 accounts, Copy data to 1 storage account, USB 3.1/SATA interface, and Refer pricing page for details. A 'Select' button is available.
- Data Box (100 TB):** Total capacity per order. Options include: 80 TB usable capacity, 10 day use at no extra cost, Supports Azure Blobs, Files, Managed Disks and ADLS Gen2 accounts, Copy data across 10 storage accounts, 1x1/10 Gbps RJ45, 2x10 Gbps SFP+ interface, and Refer pricing page for details. A 'Select' button is available.
- Data Box Heavy (1000 TB):** Total capacity per order. Options include: 800 TB usable capacity, 20 day use at no extra cost, Supports Azure Blobs, Files, Managed Disks and ADLS Gen2 accounts, Copy data across 10 storage accounts, 4x1 Gbps, 4x40 Gbps interface, and For preview pricing, refer to the pricing page. A 'Select' button is available.
- Send your own disks (1 TB onwards):** Options include: Send up to 10 disks per order, Supports SATA/SSD disks, Supports Azure Blobs and Files, Copy data to 1 storage account, SATA II/III interface, and a 'More' link. A 'Select' button is available.

FIGURA 2-22 Seleccione el tamaño de cuadro de datos apropiado para su migración

Tenga en cuenta que los discos Data Box proporcionados por Microsoft solo están permitidos con las siguientes ofertas de suscripción:

- 0.■ **EA.** Convenio de empresa
- 1.■ **CSP.** Asociación de proveedores de soluciones en la nube
- 2.■ **Red de socios de Microsoft.** Organizaciones asociadas
- 3.■ **Patrocinio.** Una oferta limitada de suscripción de Azure solo por invitación proporcionada por Microsoft

Si no tiene una oferta vinculada a su suscripción de Azure que cumpla con los requisitos anteriores para usar un cuadro de datos proporcionado, puede enviar datos en sus propios discos. Si proporciona su propio disco, se aplican los siguientes requisitos:

- 4.■ Hasta 10 discos por pedido
- 5.■ 1 TB por disco
- 6.■ Copiar datos a una cuenta de almacenamiento
- 7.■ \$ 80 por tarifa de importación de disco

Estas opciones de Data Box son para transferencias sin conexión a Azure. El uso de Data Box Gateway, un dispositivo virtual dentro de su entorno, realizará una migración de datos en línea a Azure.

5. Una vez que haya seleccionado una opción de disco, podrá configurar las opciones para su entorno (consulte la [Figura 2-22](#)). Elegirás las siguientes opciones que se muestran en la figura 2-23:

Create import/export job

Create import/export job

Basics Job details Shipping Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * site-recovery Create new

Name * importsfordatabox

Type Import into Azure Export from Azure

Review + create < Previous Next : Job details >

FIGURA 2-23 Opciones de configuración para el entorno de migración

0. **Escriba.** Importar o exportar desde Azure.
1. **Nombre.** El nombre del trabajo para identificarlo en Azure.
2. **Suscripción.** Seleccione la suscripción para el trabajo.
3. **Grupo de recursos.** Seleccione un grupo de recursos existente o cree uno nuevo para el trabajo.
6. Después de hacer clic en **Siguiente: Detalles del trabajo**, proporcionará la siguiente información, que se muestra en la Figura 2-24 :

Create import/export job

Create import/export job

Basics Job details Shipping Tags Review + create

⚠ Download the latest WAImportExport tool to generate the .jm file

Data source

Upload journal files ⓘ Select a file

Drive ID Journal file

Import destination:

Destination Azure region * North Central US

Storage account * databoximportaz303

Drop-off location North Central US

Save verbose log in the 'waimportexport' blob container

Review + create < Previous Next : Shipping >

FIGURA 2-24 Proporcione detalles del trabajo

0. **Cargar archivos de diario.** Especifique la ruta al archivo de diario para cada unidad que se utiliza para la importación.
1. **Destino de importación.** Especifique una cuenta de almacenamiento para consumir los datos ingeridos y la región en la que se almacenarán los datos.
2. **Proporcione información de envío de devolución.** Especifique los detalles del nombre y la dirección para permitir que su disco sea devuelto junto con la información del operador, como se muestra en la Figura 2-24.

Revise y confirme sus opciones.

Si ha enviado sus propias unidades para este proceso, deberá proporcionar la información de devolución.

Opción de solo nota

Proporcionar sus propias unidades es la única opción disponible para algunos tipos de suscripción de Azure.

Como se mencionó anteriormente, si no está usando una suscripción de EA, CSP, Partner, Patrocinio en Azure o una con una designación de oferta especial, es posible que deba usar su (s) propia (s) unidad (es) con Data Box. Si ese es el caso, se requiere la información de envío de devolución, como se muestra en la Figura 2-25.

Create import/export job

Create import/export job

Basics Job details * Shipping Tags Review + create *

Return carrier

Carrier name * Blue Dart

Carrier account number * 123454321

Return address

Contact name * Derek

Phone * 12345678

Email * email@databox.azure.com

Street address 1 * 123 Any Street

Street address 2 (optional)

City * Cloudville

State/Province IN

Zip code * 12345

Country/Region * US

Save return address as default.

Review + create < Previous Next : Tags >

FIGURA 2-25 Información de envío de devolución

Existen otras herramientas de evaluación y migración como Movere u otras herramientas de terceros. Estas herramientas pueden requerir un gasto adicional para evaluar su entorno. Movere es gratuito y se puede

utilizar como parte de este proceso porque fue adquirido por Microsoft, pero este libro se centra en las herramientas de Azure para la evaluación y la migración.

Implementación de Azure Update Management

Una organización que busca trasladar cargas de trabajo a la nube probablemente (con suerte) ya se está asegurando de que estos servidores se revisen con regularidad y se mantengan tan cerca de la verdadera actualización como lo permitan sus organizaciones de control de la información y seguridad. Migrar un servidor a Azure no necesariamente elimine esta carga de los equipos de administración del servidor. Lo último que se debe cubrir en esta sección sobre la administración y migración de la carga de trabajo es la administración de actualizaciones en la nube. Como era de esperar, Azure tiene un método para eso, y aquí veremos la implementación de este conjunto de características.

Nota Si está funcionando, tal vez debería seguir funcionando

El hecho de que Azure lleve una herramienta de administración de actualizaciones a la fiesta no significa que será la mejor estrategia de administración de parches para su organización. En el caso de que su organización tenga principalmente sistemas unidos a un dominio de Windows o una estrategia bien aceitada para parchear Linux, es posible que no haya razón para que cambie la forma en que están las cosas. Claro, debe evaluar la situación, pero asegúrese de que las nuevas herramientas se adapten a las necesidades de su organización.

Para configurar Azure Update Management, complete los pasos siguientes:

1. Inicie sesión en Azure Portal y navegue hasta una máquina virtual en ejecución.
2. En la sección **Operaciones** del menú de navegación izquierdo de la VM, seleccione **Gestión de actualizaciones**.
3. Proporcione la siguiente información:
 1. **Ubicación del espacio de trabajo de Log Analytics.** Seleccione la región de la cuenta.

2. ■ **Espacio de trabajo de Log Analytics.** Elija (o cree) un espacio de trabajo de análisis de registros.
 3. ■ **Suscripción a la cuenta de automatización.** Seleccione la suscripción de Azure para albergar este recurso.
 4. ■ **Cuenta de automatización.** Elija o cree una cuenta de automatización para la Gestión de actualizaciones.
4. Haga clic en **Habilitar** y espere a que se complete la implementación (entre 5 y 15 minutos).

Tenga en cuenta que sea paciente con la recopilación de datos

Una vez que la solución está habilitada, la solución deberá recopilar datos sobre su (s) sistema (s) para ayudar a garantizar el mejor plan de gestión de actualizaciones. Esto puede tardar varias horas en completarse. El cuadro de diálogo de Azure Portal recomienda permitir que esto se ejecute durante la noche.

5. Una vez que la solución haya terminado de incorporar las máquinas virtuales, al volver a visitar la hoja de **administración de actualizaciones** para una o más máquinas virtuales, se mostrará la información a medida que esté disponible.
6. La selección del solucionador de problemas de disponibilidad del **agente de actualización** ayudará a determinar qué elementos pueden interferir con el uso de la solución de administración de actualizaciones (consulte la [Figura 2-26](#)).

 Troubleshoot Update Agent
server-to-dr

Click the button below to run a troubleshooting utility in the Azure VM. [This uses the RunCommand API.](#)
The results will be available in about a minute.

Run checks

Troubleshooting documentation

Prerequisite Checks

Operating system ⓘ	Passed	Operating system version is supported.
.Net Framework 4.5+ ⓘ	Passed	.NET Framework version 4.5+ is found.
WMF 5.1 ⓘ	Passed	Detected Windows Management Framework version: 5.1.14393.3471.
TLS 1.2 ⓘ	Passed	TLS 1.2 is enabled by default on the operating system.

Connectivity Checks

Registration endpoint ⓘ	Passed	TCP test for 5ac509ad-1b73-4c40-8ebf-184009c6ba2a.agentsvc.azure-automation.net (port 443) succeeded.
Operations endpoint ⓘ	Passed	TCP test for eus2-jobruntimedata-prod-su1.azure-automation.net (port 443) succeeded.

Monitoring Agent Service Health Checks

Monitoring Agent service status ⓘ	Passed	Microsoft Monitoring Agent service (HealthService) is running.
Monitoring Agent service events ⓘ	Passed	Microsoft Monitoring Agent service Event Log (Operations Manager) does not have Error event 4502 logged in the last 24 hours.

Access Permission Checks

MachineKeys folder access ⓘ	Passed	Permissions exist to access C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
-----------------------------	--------	--

Machine Update Settings

Automatically reboot after install ⓘ	Passed	Windows Update reboot registry keys are not set to automatically reboot
WSUS Server Configuration ⓘ	Passed	Windows Updates are downloading from the default Windows Update location. Ensure the server has access to the Windows Update service
Automatically download and install ⓘ	⚠ Passed with warning	Auto Update is enabled on the machine and will interfere with Update management Solution

FIGURA 2-26 Configuración de la preparación del agente de actualización

- Si su máquina virtual está ejecutando Windows Auto Update, querrá deshabilitarla antes de continuar con la administración de actualizaciones en Azure.

Una vez que se haya completado el proceso de incorporación y después de esperar a que se complete la configuración, visite la hoja de **administración de actualizaciones** para una máquina virtual para ver las **actualizaciones que faltan** para el sistema, que están desglosadas por **crítica , seguridad y otros** , como se muestra en la [figura 2-27](#) .

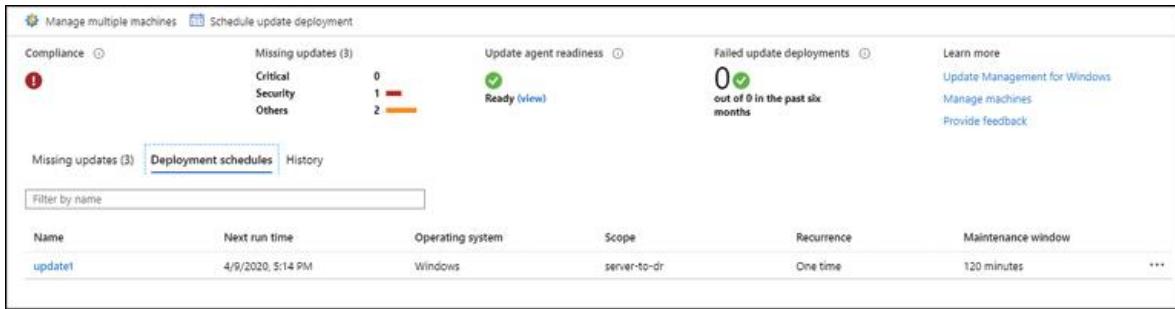


FIGURA 2-27 Correcciones de seguridad necesarias antes de que pueda continuar la migración

Al seleccionar una actualización de la lista **Actualizaciones perdidas**, se abrirá Log Analytics e insertará una consulta en busca de esa actualización; ejecutar la consulta mostrará la actualización como resultado.

Cuando un servidor se ha incorporado a Update Management, se puede parchear configurando un programa para la implementación de actualizaciones. Para hacer eso, complete los siguientes pasos:

1. En la hoja **Administración de actualizaciones**, haga clic en **Programar implementación de actualizaciones**.
2. Ingrese la siguiente información sobre el horario:
 1. **Nombre.** Un nombre para la implementación.
 2. **Actualizar clasificación.** Los tipos de actualización que se incluirán.
 3. **Incluir / excluir actualizaciones.** Opcionalmente, seleccione las actualizaciones para incluir o excluir.
 4. **Configuración de programación.** Cuándo debería ocurrir la implementación.
 5. **Guiones previos y posteriores.** Cualquier script que deba ejecutarse antes o después de la implementación.
 6. **Ventana de mantenimiento.** Especifique la duración de la ventana de mantenimiento para implementar actualizaciones.
 7. **Opciones de reinicio.** Elija las opciones de reinicio para las actualizaciones.

3. Haga clic en **Crear** en el programa de implementación de actualizaciones.

La implementación que se ha programado aparecerá en la pestaña **Programa de implementación**. Además, cualquier implementación se establecerá de forma predeterminada en 30 minutos después de la hora actual para permitir que la programación se envíe a Azure.

Una vez configurados estos elementos, las actualizaciones se aplicarán según el cronograma que se haya configurado.

Esta sección presentó una descripción general de alto nivel que cubre los diversos tipos de migraciones a Azure mediante herramientas integradas de Azure. A medida que esta tecnología cambie y Azure evolucione, seguramente se expandirá.

¿Necesita más revisión? Azure Migrate

Consulte estos recursos:

- **Directrices de migración de Azure para Hyper-V.** <https://docs.microsoft.com/en-us/azure/migrate/migrate-support-matrix-Hyper-V#assessment-appliance-requirements>
- **Descripción general de Azure Migrate.** <https://docs.microsoft.com/en-us/azure/migrate/>
- **Update Management Solution en Azure.** <https://docs.microsoft.com/en-us/azure/automation/update-management/overview>
- **Una descripción general de Azure VM Backup.** <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction>

HABILIDAD 2.2: IMPLEMENTAR LA RECUPERACIÓN ANTE DESASTRES MEDIANTE AZURE SITE RECOVERY

Con el creciente número de organizaciones que se mudan a Azure, una de las primeras cosas que me viene a la mente es aprovechar la nube como objetivo para la recuperación ante desastres. Si una organización tiene una ubicación conjunta existente para los datos de recuperación ante desastres, Azure puede proporcionar algunos o todos los servicios necesarios para reemplazar estos centros de datos secundarios (o múltiples secundarios). En esta sección, se tratan el uso y la configuración de Azure Site Recovery.

Nota Antes de que existiera Migrate, existía Site Recovery

Antes de Azure Migrate, Azure Site Recovery era la solución de Microsoft tanto para la recuperación ante desastres como para la migración de servidores a Azure.

Esta habilidad cubre:

- ■ [Configurar componentes de Azure de Site Recovery](#)
- ■ [Configurar componentes locales de Site Recovery](#)
- ■ [Replicar datos en Azure](#)
- ■ [Migrar mediante Azure Site Recovery](#)

Configurar componentes de Azure de Site Recovery

Azure Site Recovery proporciona una forma de aprovechar la escala de Azure y, al mismo tiempo, permitir que los recursos vuelvan a su centro de datos local en caso de que surja la necesidad como parte de un escenario de continuidad empresarial y recuperación ante desastres (BCDR). Desde la introducción de Azure Migrate y las cargas de trabajo adicionales tratadas anteriormente en este capítulo, Site Recovery se ha convertido en la principal herramienta de recuperación ante desastres para usar con Azure.

Siga estos pasos para configurar los recursos de Azure para usar Site Recovery for DR en Azure:

Nota Consideré la posibilidad de crear primero los recursos de Azure

La creación de los recursos de Azure prepara primero el destino y garantiza que no se pierda nada. Debido a que el proceso mueve archivos a Azure, esto puede minimizar los problemas cuando comienza la transferencia porque los recursos de destino se identificarán por adelantado.

1. Inicie sesión en su suscripción de Azure.
2. Cree un grupo de recursos para almacenar su Azure Backup Vault.
3. Cree un nuevo recurso y seleccione **Copia de seguridad y recuperación del sitio** en la agrupación **Almacenamiento** en Azure Marketplace , como se muestra en la Figura 2-28 .

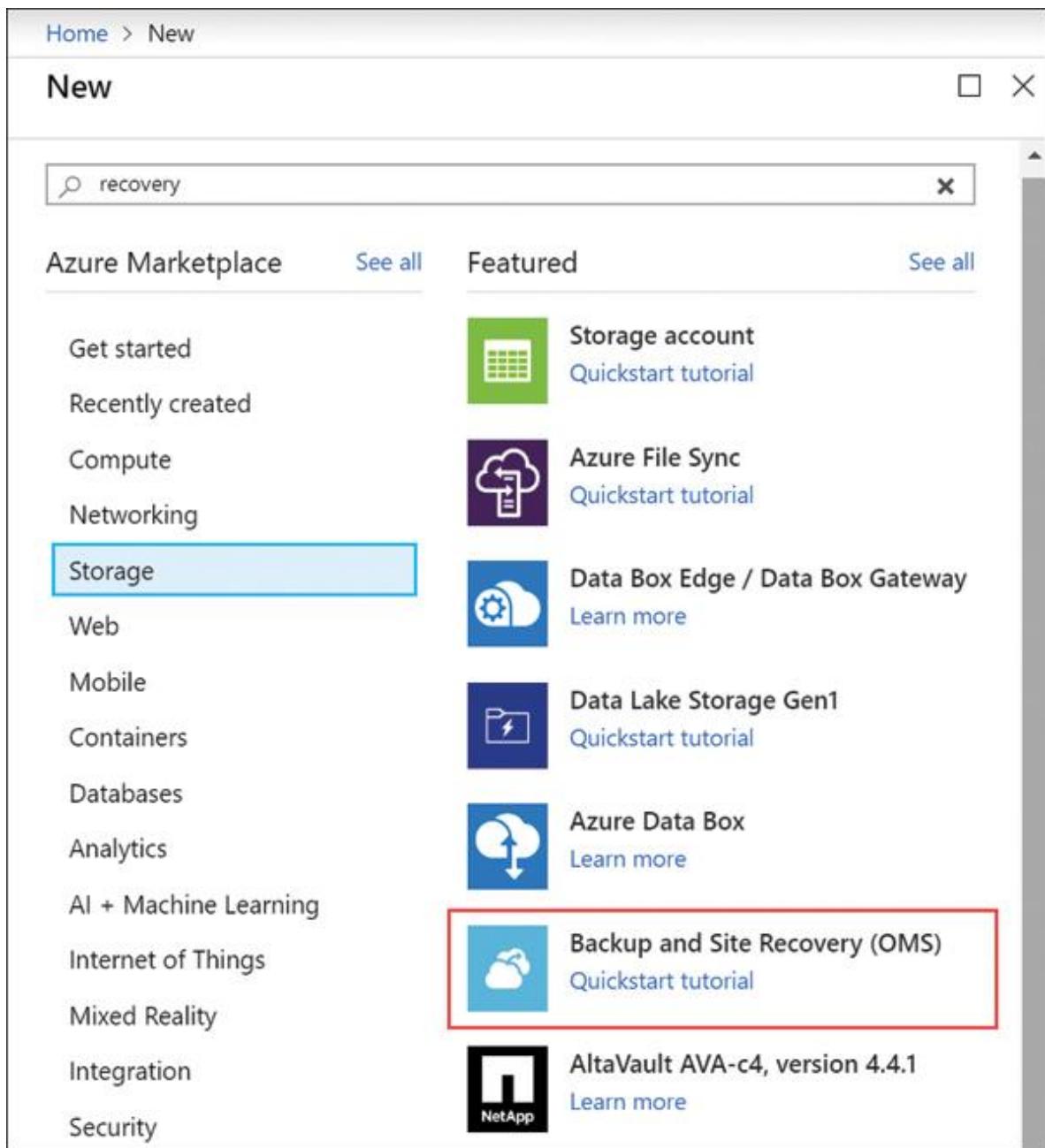


FIGURA 2-28 Creación de una bóveda de recuperación de sitios y copias de seguridad

4. En la hoja **Creación del almacén de Recovery Services** que se muestra en la Figura 2-29, complete el formulario:

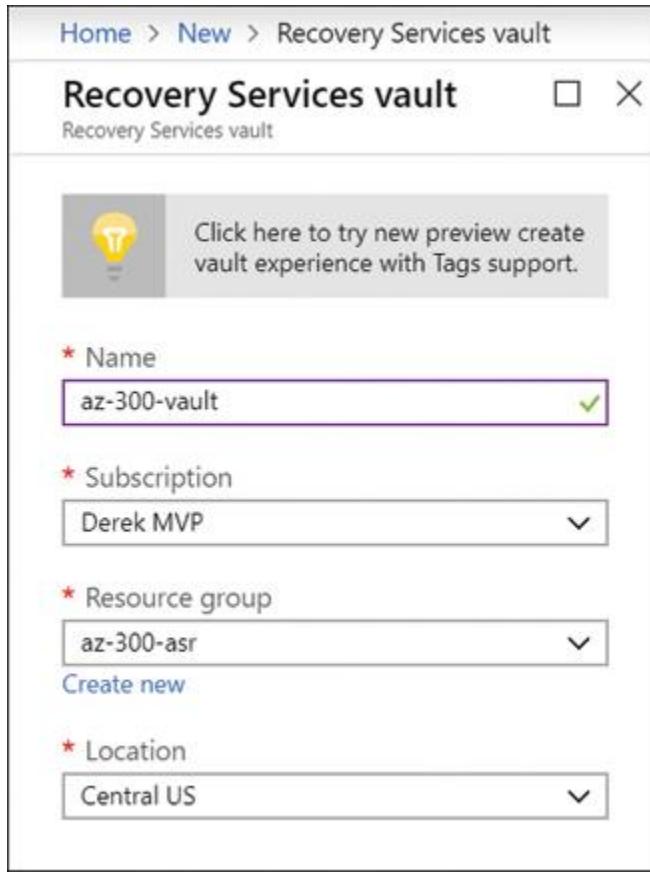


FIGURA 2-29 Creación de una bóveda de Recovery Services

1. ■ **Suscripción.** Especifique una suscripción de Azure activa.
2. ■ **Grupo de recursos.** Cree un nuevo grupo de recursos o seleccione un grupo de recursos existente para el almacén de Recovery Services.
3. ■ **Nombre.** Elija un nombre único para su bóveda de Recovery Services.
4. ■ **Ubicación.** Seleccione la región que se usará para la bóveda de Recovery Services.
5. Haga clic en el botón **Crear** para crear el recurso, que puede tardar unos minutos en completarse.

Nota: los cambios en el nombre de la función también ocurren a la velocidad de la nube

Backup and Site Recovery es el nuevo nombre del recurso de la bóveda de Recovery Services. Al momento de escribir este artículo, los nombres no se han actualizado en todo el portal.

Una vez que la bóveda de Recovery Services esté lista, abra la página **Descripción general** haciendo clic en el recurso dentro del grupo de recursos. Esta página proporciona información de alto nivel, incluidas las novedades relacionadas con la bóveda de Recovery Services.

Configurar componentes locales de Site Recovery

Siga los siguientes pasos para comenzar con la recuperación del sitio (migración en este caso):

1. Haga clic en el enlace **Site Recovery** en **Getting Started** en el panel de **Configuración**, como se muestra en la [Figura 2-30](#).

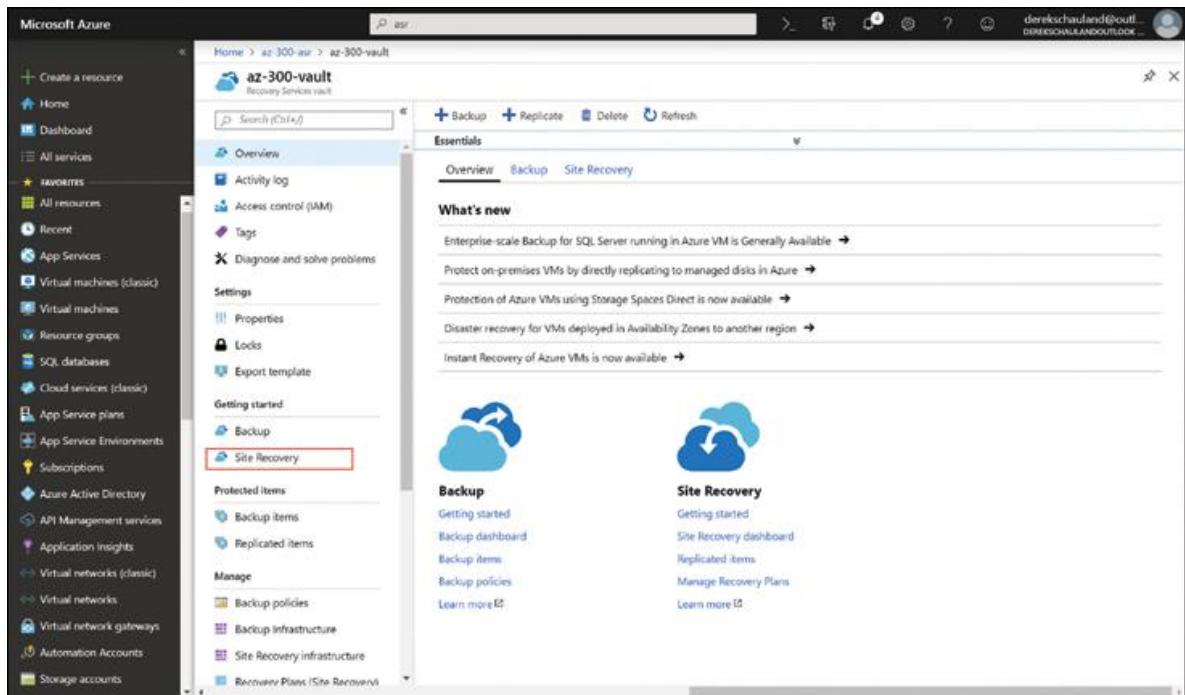


FIGURA 2-30 Introducción a Site Recovery

2. Seleccione el enlace **Preparar infraestructura** para comenzar a preparar las máquinas locales.
3. Complete los pasos de **Preparar la infraestructura** (que se muestran en la [Figura 2-31](#)):

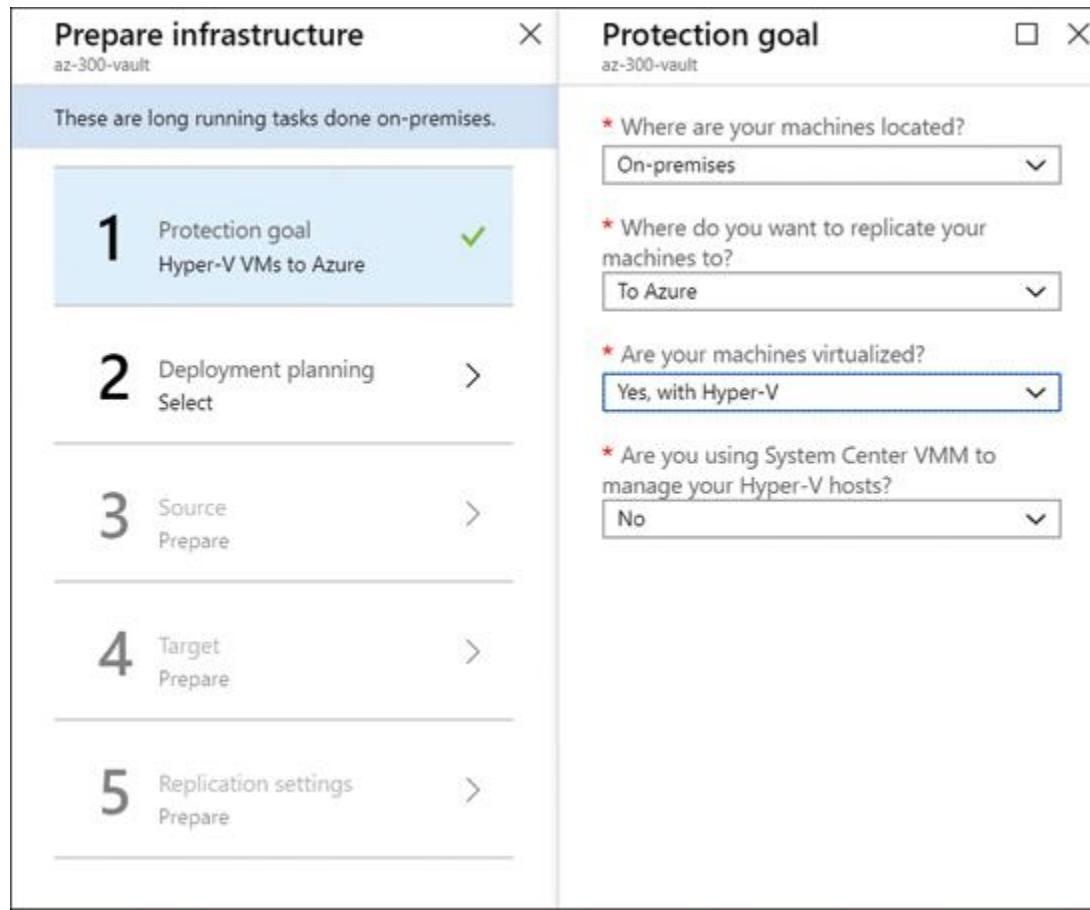


FIGURA 2-31 Configurar objetivos de protección

1. ■ **¿Dónde están ubicadas sus máquinas?** Elija en las instalaciones .
2. ■ **¿Dónde desea replicar sus máquinas?** Elija A Azure .
3. ■ **¿Está realizando una migración?** Seleccione Sí o No .
4. ■ **¿Están virtualizadas sus máquinas?** Seleccione la respuesta adecuada:
 - 1.■ **Sí, con VMware .**
 - 2.■ **Sí, con Hyper-V .**
 - 3.■ **Otro / No virtualizado .**

Nota sobre los servidores físicos

La migración de servidores físicos mediante P2V, que se trata más adelante en este capítulo, utiliza la opción Físico / Otro de la configuración de Azure Site Recovery que se menciona aquí. Aparte de este paso, la configuración de Azure es la misma que se describe aquí.

Nota sobre Hyper-V

Si selecciona Hyper-V como plataforma de virtualización, también deberá indicar si está utilizando System Center VMM para administrar las máquinas virtuales.

4. Haga clic en **Aceptar** para completar el formulario **Objetivo de protección**.

El paso 2 de la preparación de la infraestructura es la planificación de la implementación, que ayuda a garantizar que tenga suficiente ancho de banda para completar la transferencia de cargas de trabajo virtualizadas a Azure. El asistente calculará el tiempo necesario para transferir completamente las cargas de trabajo a Azure en función de las máquinas que se encuentran en su entorno.

Haga clic en el enlace **Descargar** del planificador de implementación, ubicado en el panel central del paso de planificación de la implementación, para descargar un archivo zip y comenzar.

Este archivo zip incluye una plantilla que ayudará a recopilar información sobre el entorno virtualizado, así como una herramienta de línea de comandos para escanear el entorno virtualizado y determinar una línea de base para la migración. La herramienta requiere acceso de red al entorno de Hyper-V o VMware (o acceso directo a los hosts de VM donde se ejecutan las VM). La herramienta de línea de comandos proporciona un informe sobre el rendimiento disponible para ayudar a determinar el tiempo que tomaría mover los recursos escaneados a Azure.

Nota Asegúrese de que RDP esté habilitado antes de la migración

Asegurarse de que el sistema local esté configurado para permitir conexiones de escritorio remoto antes de migrarlo a Azure vale la pena las comprobaciones previas. Habrá un trabajo considerable por hacer, incluida la configuración de un Jumpbox que sea local a la red virtual de la VM migrada, si estos pasos no se realizan antes de la

migración. Es probable que esto ya esté configurado, pero nunca es una mala idea volver a verificar.

Una vez que se haya ejecutado la herramienta, en Azure Portal, especifique que el planificador de implementación se ha completado y haga clic en Aceptar .

A continuación, el entorno de virtualización se proporcionará a Azure agregando el sitio y los servidores de Hyper-V.

Tenga en cuenta que todos los hipervisores son bienvenidos

En el momento de escribir este artículo, el laboratorio utilizado para los ejemplos consiste en la infraestructura Hyper-V. Los ejemplos proporcionados utilizarán Hyper-V como fuente local, pero ASR también es compatible con VMware.

Para agregar un servidor Hyper-V, descargue Azure Site Recovery Provider y la clave de registro del almacén (consulte la Figura 2-32) e instálelos en el servidor Hyper-V. La información de registro de la bóveda es necesaria porque ASR necesita saber a qué bóveda de recuperación pertenecen las máquinas virtuales una vez que estén listas para migrar a Azure.

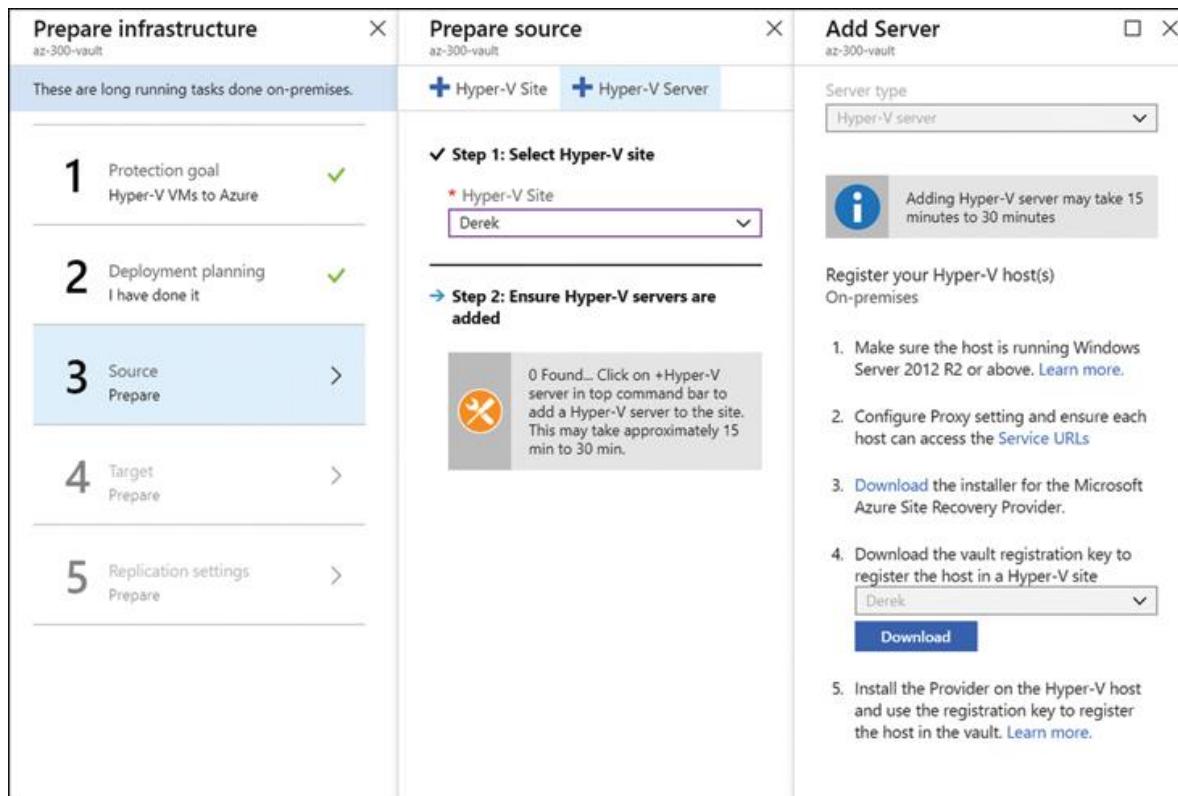


FIGURA 2-32 Preparación del entorno de virtualización de origen

Si está utilizando Hyper-V, instale Site Recovery Provider en el host de virtualización, como se muestra en la [Figura 2-33](#).

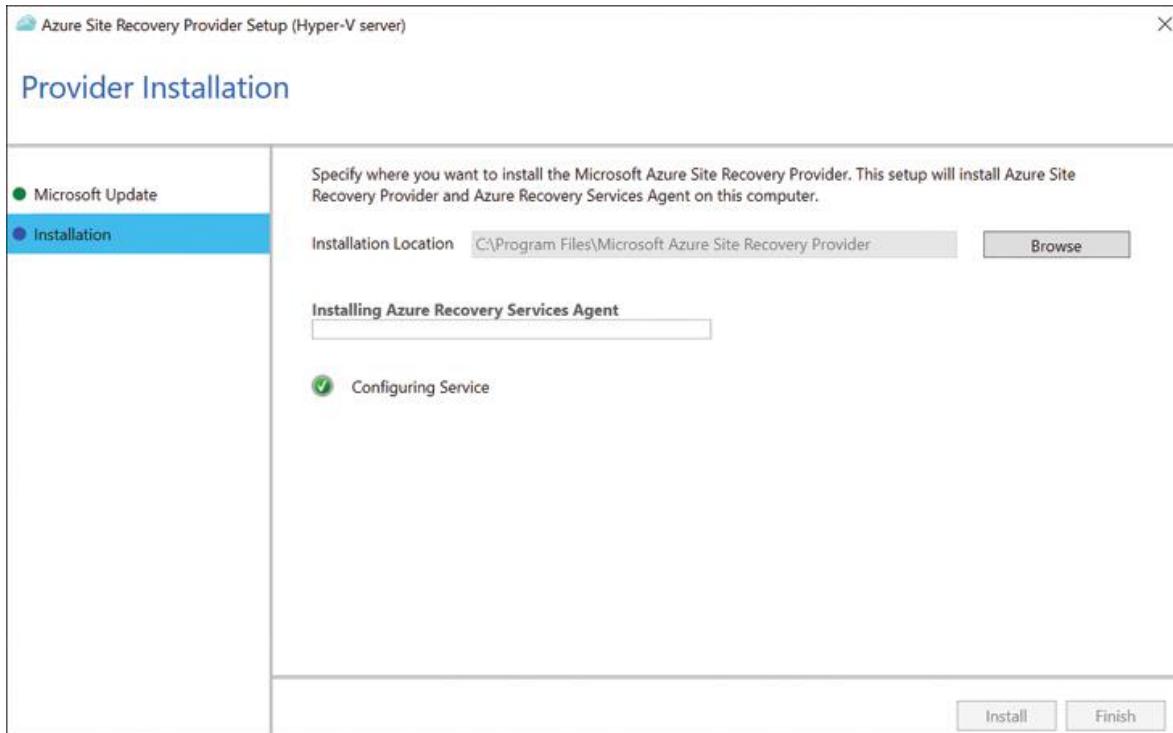


FIGURA 2-33 Instalación de Site Recovery Provider

Después de la instalación y el registro, es posible que Azure tarde un poco en encontrar el servidor que se ha registrado en el almacén de Site Recovery.

Continúe con la preparación de la infraestructura completando la sección **Destino** del asistente, como se muestra en la [Figura 2-34](#).

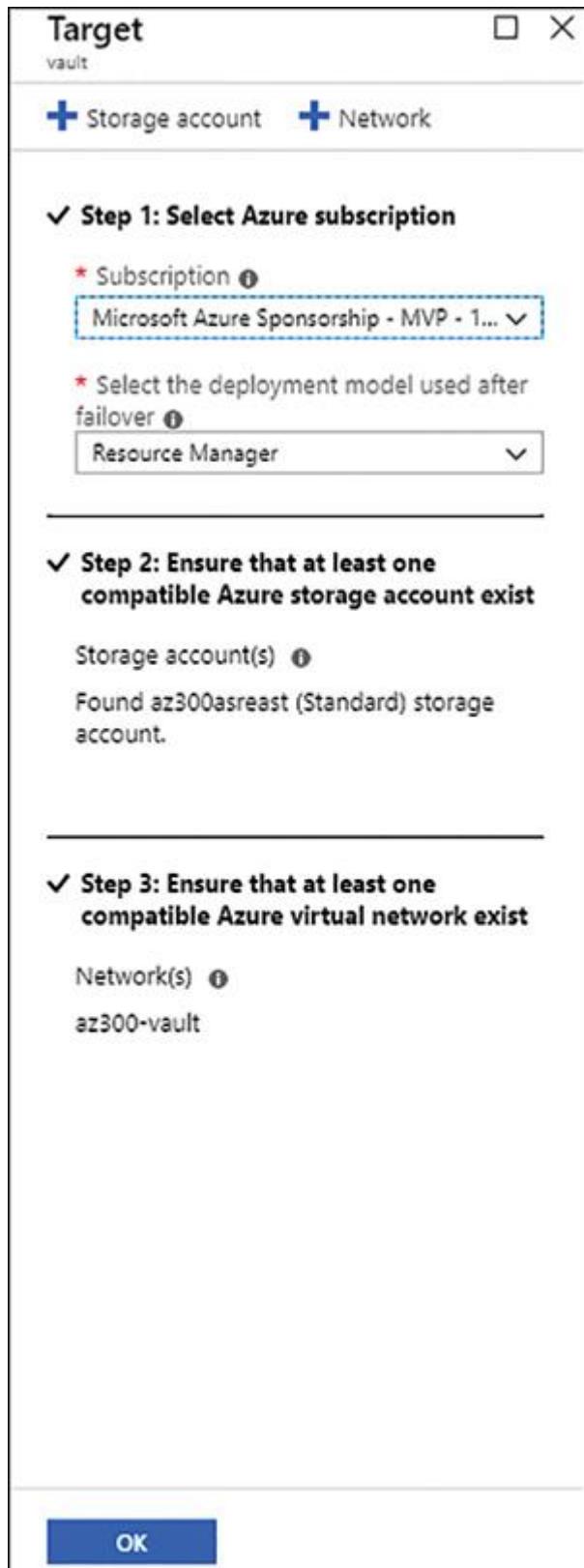


FIGURA 2-34 Preparación del destino de Azure

Seleccione la **suscripción** y el **modelo de implementación** utilizados. (Generalmente, el **modelo de implementación** será el **administrador de recursos**).

Nota Asegúrese de que el almacenamiento y las redes estén disponibles

Se necesitan una cuenta de almacenamiento y una red dentro de la suscripción especificada en la misma región de Azure que el almacén de Recovery Services. Si esto existe cuando llegue a este paso, puede seleccionar los recursos. Si la cuenta de almacenamiento y la red no existen, puede crearlas en este paso.

Haga clic en el botón **Cuenta de almacenamiento** en la parte superior de la hoja **Destino** para agregar una cuenta de almacenamiento.

Proporcione los siguientes detalles de la cuenta de almacenamiento:

- ■ Nombre de la cuenta de almacenamiento
- ■ Configuración de replicación
- ■ Tipo de cuenta de almacenamiento

Cuando se crea esta cuenta de almacenamiento, se colocará en la misma región que la bóveda de servicios de replicación.

Si no se encuentra una red en la misma región que la bóveda, puede hacer clic en el botón **Agregar red** en la parte superior de la hoja **destino** para crear una. Al igual que el almacenamiento, la región de la red coincidirá con la bóveda. Otras configuraciones, incluidos el **rango de direcciones** y el **nombre**, estarán disponibles para la configuración.

El último requisito para preparar la infraestructura es configurar una política de replicación. Complete los siguientes pasos para crear una política de replicación:

1. Haga clic en **Crear y asociar** en la parte superior de la hoja **Política de replicación**. Ingrese la siguiente información:
 1. ■ **Nombre** El nombre de la política de replicación.
 2. ■ **Tipo de fuente** Debe llenarse previamente en función de la configuración anterior.
 3. ■ **Tipo de destino** Debe llenarse previamente en función de la configuración anterior.

4. ■ **Frecuencia de copia** Introduzca la frecuencia de replicación para que se capturen las copias posteriores.
 5. ■ **Retención del punto de recuperación en horas** Cuánta retención se necesita para este servidor.
 6. ■ **Frecuencia de instantáneas coherentes con la aplicación en horas** Frecuencia con la que se capturará una instantánea coherente con la aplicación.
 7. ■ **Hora de inicio de la replicación inicial** Introduzca una hora para que comience la replicación inicial.
 8. ■ **Sitio de Hyper-V asociado completado** en función de la configuración anterior.
2. Haga clic en **Aceptar** para crear la directiva y Azure compilará y asociará esta configuración con el entorno local especificado.

Replica datos en Azure

Después de completar la configuración local, regresa a la hoja de **Site Recovery** para continuar con la configuración.

Para habilitar la replicación, complete los siguientes pasos:

1. Seleccione el origen de la replicación : **local** , en este caso.
2. Seleccione la ubicación de **origen** : el servidor Hyper-V configurado dentro de su entorno.
3. Haga clic en **Aceptar** para continuar con la configuración de destino.
4. Seleccione la **suscripción** que se utilizará con esta replicación.
5. Proporcione un grupo de recursos posterior a la conmutación por error, que es un grupo de recursos para la máquina virtual con conmutación por error.
6. Elija el modelo de implementación para la máquina virtual de conmutación por error.
7. Seleccione o cree la cuenta de almacenamiento que se utilizará para almacenar discos para las máquinas virtuales a las que se realiza la conmutación por error.

8. Seleccione la opción para cuándo se debe configurar la red de Azure: **ahora** o más tarde .
9. Si seleccionó **Ahora** , seleccione o cree la red para usar después de la conmutación por error.
10. Seleccione la subred que utilizarán estas máquinas virtuales de la lista de subredes disponibles para la red elegida.
11. Haga clic en **Aceptar** .
12. Seleccione las máquinas virtuales para la conmutación por error como parte de Azure Site Recovery.
13. Especifique las siguientes propiedades predeterminadas y las propiedades de las máquinas virtuales seleccionadas:
 1. ■ **Tipo de SO** Si el SO es Linux o Windows (disponible como predeterminado y por VM).
 2. ■ **Disco del SO** Seleccione el nombre del Disco del SO para la VM (disponible por VM).
 3. ■ **Discos** para replicar Seleccione los discos conectados a la VM para replicar (disponibles por VM).
14. Haga clic en **Aceptar** .
15. Revise la configuración de la política de replicación para esta replicación. Coincidirán con la configuración de la política de replicación configurada en el paso 5 del asistente **Preparar infraestructura** , pero puede seleccionar otras políticas si existen.
16. Haga clic en Aceptar.
17. Haga clic en Habilitar replicación.

Con las opciones de replicación configuradas, la última parte de la configuración para completar es el plan de recuperación. Para configurar el plan de recuperación, siga los siguientes pasos:

1. En la hoja **Site Recovery** , seleccione **Paso 2: Administrar planes de recuperación** y haga clic en el botón **Agregar plan de recuperación** en la parte superior de la pantalla.
2. Proporcione un nombre para el plan de recuperación y seleccione el modelo de implementación para los elementos que se recuperarán.
3. Seleccione los elementos para un plan de recuperación. Aquí elegirá las máquinas virtuales que se incluirán en la recuperación.

4. Haga clic en **Aceptar** para finalizar el plan de recuperación.
5. Una vez que los elementos están protegidos y listos para la conmutación por error a Azure, puede probar la conmutación por error seleccionando el recurso de la bóveda de **Site Recovery** y eligiendo **Recovery Plans (Site Recovery)** en la sección **Administrar** del panel de navegación.
6. Seleccione el plan de recuperación adecuado para esta conmutación por error. Esta pantalla de descripción general muestra la cantidad de elementos en el plan de recuperación tanto en el origen como en el destino, como se muestra en la [Figura 2-35](#).

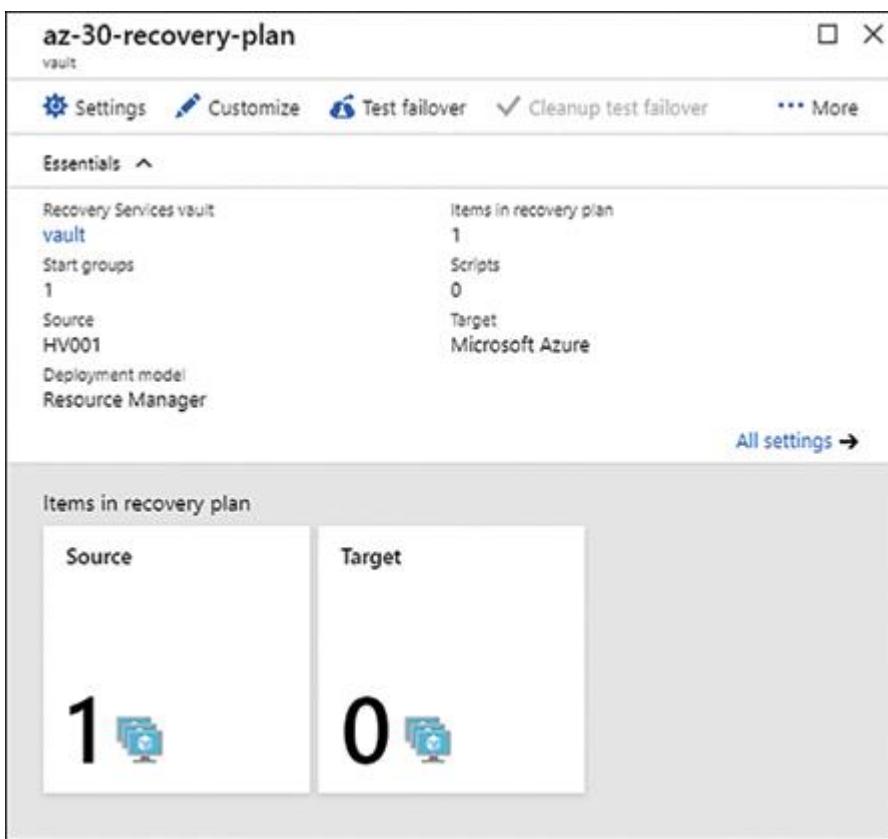


FIGURA 2-35 Descripción general del plan de recuperación del sitio

Para probar la configuración, haga clic en el botón **Probar conmutación por error** en la parte superior de la hoja **Plan de recuperación del sitio** y complete los siguientes pasos:

1. Seleccione el punto de recuperación que se utilizará para la prueba.
2. Seleccione la **red virtual de Azure** para la máquina virtual replicada.

3. Haga clic en **Aceptar** para iniciar la prueba de conmutación por error.

Una vez que se completa la conmutación por error, la máquina virtual debe aparecer en el grupo de recursos que se especificó para el uso posterior a la conmutación por error, como se muestra en la [Figura 2-36](#).

NAME	TYPE	LOCATION	RESOURCE ACTION (TAG)
ipConfigServer001-test9fa42940...	Public IP address	East US 2	
Server001-test	Virtual machine	East US 2	
Server001-test9fa42940-34e8-41...	Network interface	East US 2	

FIGURA 2-36 Recursos después de la ejecución de la conmutación por error en Azure

Migrar mediante Azure Site Recovery

Una vez que se ha completado la conmutación por error de prueba, su máquina virtual se está ejecutando en Azure y puede ver que todo es como se esperaba. Cuando esté satisfecho con el resultado de la máquina virtual en ejecución, puede completar una limpieza de la prueba, que eliminará los recursos creados como parte de la conmutación por error de la prueba. Seleccione los elementos en la lista **Elementos replicados** y elija el botón de **conmutación por error de prueba de limpieza** que se muestra anteriormente en la parte superior de la hoja del plan de recuperación (consulte la [Figura 2-35](#)). Cuando esté listo para migrar, utilice una conmutación por error real completando los siguientes pasos:

1. Seleccione **Elementos replicados** en la sección **Elementos protegidos de ASR Vault**.
2. Elija el elemento a replicar de la lista.
3. Una vez que el elemento se haya sincronizado, haga clic en el botón **Conmutación por error** para enviar la máquina virtual a Azure.

Después de la conmutación por error de la máquina virtual a Azure, el entorno local se limpia como parte de la finalización de la migración a Azure. Esto garantiza que los puntos de restauración de la máquina virtual migrada se limpien y que la máquina de origen se pueda eliminar porque quedará desprotegida una vez que se hayan completado estas tareas.

Es posible que deba modificar la configuración para optimizar el rendimiento y asegurarse de que la administración remota esté configurada una vez que el sistema haya aterrizado (lo que significa que se ha migrado a Azure), como cambiar a discos administrados; los discos que se usan en una conmutación por error son discos estándar.

Es posible que haya algunas consideraciones de red después de migrar la máquina virtual. La conectividad externa puede requerir grupos de seguridad de red para garantizar que RDP o SSH estén activos para permitir conexiones. Recuerde que las reglas de firewall que se configuraron localmente no se configurarán necesariamente después de la migración en Azure.

Después de verificar que el recurso migrado funciona según sea necesario, el último paso de la migración es eliminar los recursos locales. En términos de Azure, los recursos todavía se encuentran en un estado de conmutación por error porque el proceso debía conmutarlos por error con la intención de devolverlos a una ubicación local.

Aunque la migración a Azure con Site Recovery todavía funciona mediante el proceso de transición y limpieza, Azure Migrate es una versión más reciente de esta herramienta que se usa específicamente para mover cargas de trabajo (VM, bases de datos, etc.) a Azure. Azure Migrate se trató anteriormente en este capítulo.

¿Necesita más revisión? Recursos de recuperación ante desastres de Azure

Para obtener material adicional, consulte "Preparar recursos de Azure para la recuperación ante desastres de máquinas locales" en <https://docs.microsoft.com/en-us/azure/site-recovery/tutorial-prepare-azure> .

HABILIDAD 2.3: IMPLEMENTAR LA INFRAESTRUCTURA DE LA APLICACIÓN

En la era de la nube, incluso el uso de servidores se considera tecnología heredada en algunos casos porque existen servicios basados en plataformas que ejecutarán el código proporcionado en lugar de implementar aplicaciones, funciones u otras unidades de trabajo en un servidor. El proveedor de la nube, Azure, en este caso, se encarga del funcionamiento bajo el capó y el cliente solo debe preocuparse por el código que se ejecutará.

Hay más de unos pocos recursos en Azure que se ejecutan sin infraestructura o sin servidor:

- ■ Almacenamiento de Azure
- ■ Funciones de Azure
- ■ Azure Cosmos DB
- ■ Azure Active Directory
- ■ Azure Key Vault

Estos son solo algunos de los servicios que están disponibles para la computación sin servidor. Los recursos sin servidor son los servicios administrados de Azure. No son exactamente una plataforma como servicio (PaaS), pero tampoco son todos software como servicio (SaaS). Están en algún punto intermedio.

Los objetos sin servidor son los recursos sin servidor que se utilizarán en una arquitectura. Estos son los componentes básicos que se utilizan en una solución y se crearán varios tipos, según la solución que se presente.

Dos de las tecnologías sin servidor más populares admitidas por Azure son las aplicaciones lógicas y las aplicaciones funcionales. Los detalles de la configuración de estos se discuten en el texto que sigue.

Una aplicación lógica es un componente sin servidor que maneja la lógica empresarial y las integraciones entre componentes, al igual que Microsoft Flow, pero con personalización y desarrollo completos disponibles.

Esta habilidad cubre:

- ■ Cree una aplicación lógica simple

- ■ [Administrar las funciones de Azure](#)
- ■ [Administrar Azure Event Grid](#)

Crea una aplicación lógica simple

Para crear una aplicación lógica simple que busque archivos en una carpeta de OneDrive y envíe un correo electrónico cuando se encuentren, complete los siguientes pasos:

1. Seleccione **Crear un recurso** en el menú de navegación de Azure.
2. Escriba **Logic Apps** en la búsqueda del mercado y seleccione el recurso Logic App.
3. Haga clic en **Crear** en la descripción de la aplicación lógica.
4. Complete el formulario **Crear aplicación lógica** y haga clic en **Crear**.
 1. ■ **Nombre.** Proporcione un nombre para la aplicación lógica.
 2. ■ **Suscripción.** Elija la suscripción donde se debe crear el recurso.
 3. ■ **Grupo de recursos.** Seleccione **Crear o Usar existente** para elegir el grupo de recursos donde se debe crear la aplicación lógica. Si selecciona **Usar existente**, elija el grupo de recursos apropiado en el menú desplegable.
 4. ■ **Ubicación.** Seleccione la región donde se debe crear la aplicación lógica.
 5. ■ **Log Analytics.** Establezca **Log Analytics** en **Activado** o **Desactivado** para este recurso.

Nota Se requiere el espacio de trabajo de Log Analytics

Para habilitar la función de análisis de registros para una aplicación lógica, asegúrese de que el espacio de trabajo de análisis de registros que recopilará la información exista de antemano.

Una vez que existe un recurso de aplicación lógica, puede aplicar el código para que actúe sobre los recursos a través de plantillas predefinidas, plantillas personalizadas o usando una aplicación en blanco y agregando código para realizar acciones para la aplicación.

Para agregar código para copiar blobs de almacenamiento de Azure de una cuenta a otra, complete los pasos siguientes:

1. Abra el grupo de recursos especificado cuando creó el recurso de la aplicación lógica.
2. Seleccione el nombre de la aplicación lógica. La página de la **aplicación lógica** se abre para que pueda agregar plantillas, acciones y código personalizado a la aplicación lógica (consulte la [Figura 2-37](#)).

Logic App

Create

* Name
logicapp2

* Subscription
Derek MVP

* Resource group ⓘ
 Create new Use existing
az-300-serverless

* Location
Central US

Log Analytics ⓘ
On Off

* Log Analytics workspace
loganalyticsaz3001

i You can add triggers and actions to your Logic App after creation.

Create Automation options

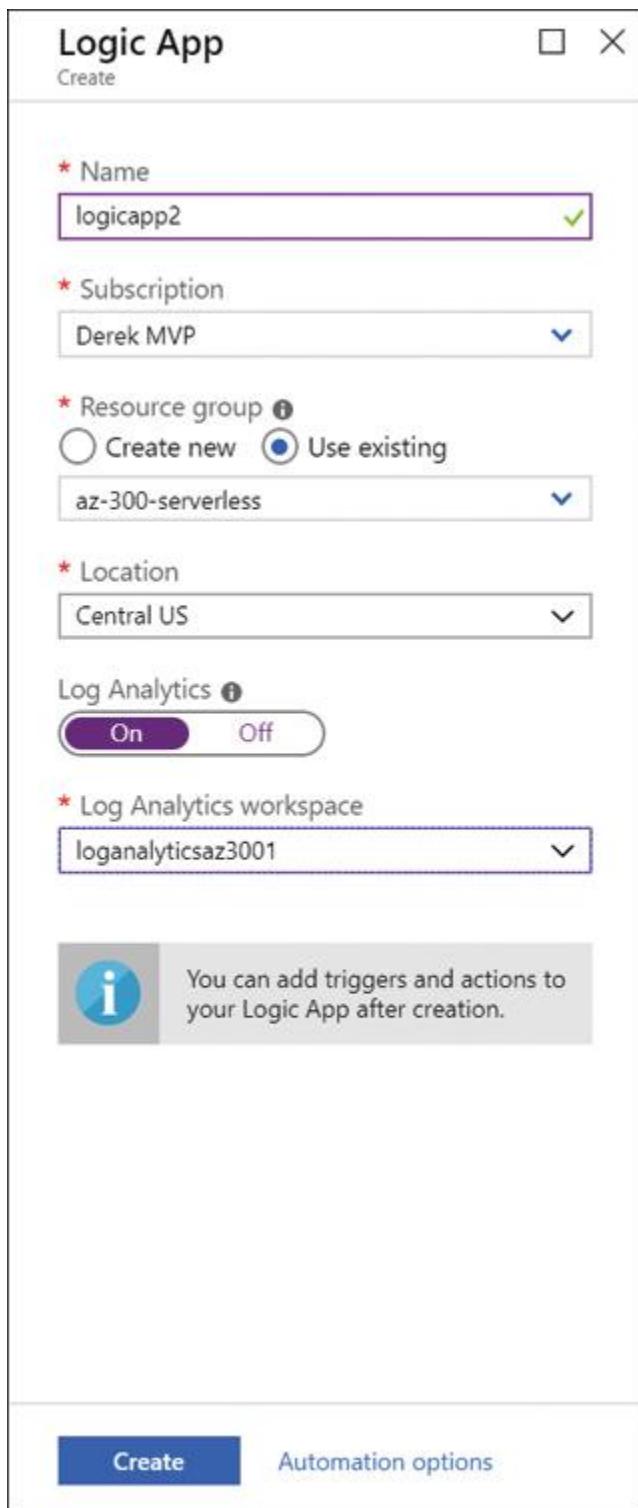


FIGURA 2-37 Creación de un recurso de aplicación lógica

3. Desde la página del diseñador inicial, seleccione el desencadenador común **Cuando se crea un nuevo archivo en OneDrive**, como se muestra en la Figura 2-38.

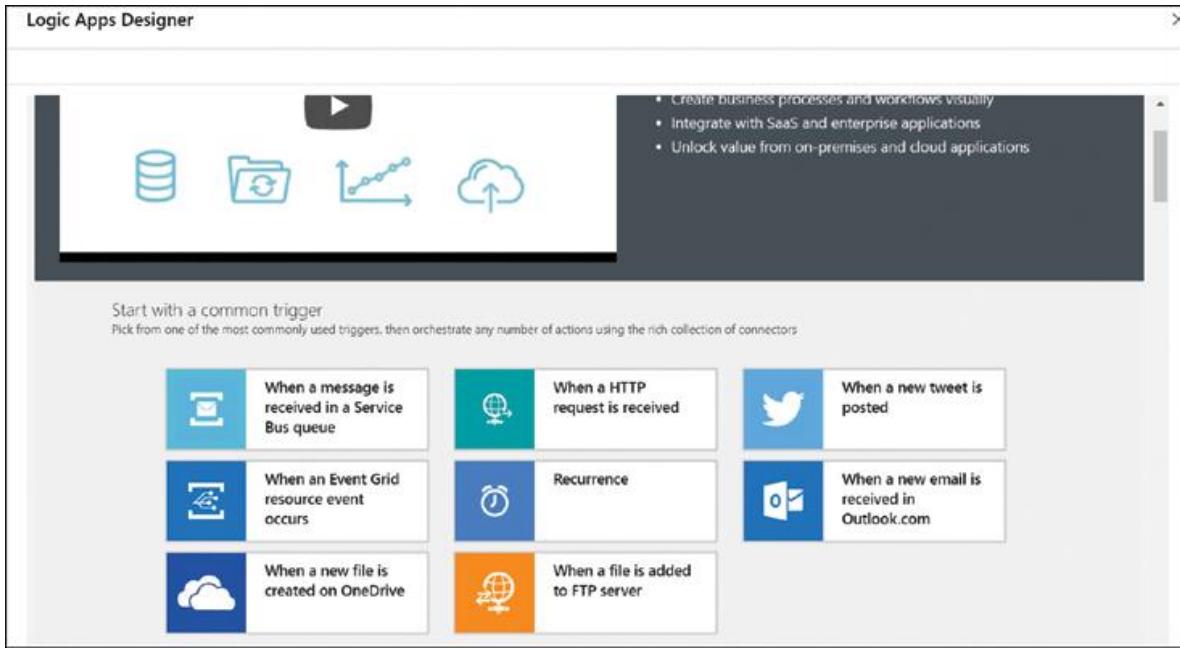


FIGURA 2-38 Logic Apps Designer con plantillas comunes

En este ejemplo, la aplicación lógica busca nuevos archivos en OneDrive y envía un correo electrónico cuando se aterriza un nuevo archivo. Es muy simple, pero está diseñado para mostrar las herramientas disponibles para trabajar con aplicaciones lógicas.

Nota Conectarse a OneDrive

Se necesitará una conexión a OneDrive para usar esta plantilla; elegir conectar una cuenta de OneDrive le pedirá que inicie sesión en la cuenta.

4. Especifique las credenciales de la cuenta para que OneDrive sea supervisado en busca de archivos y haga clic en **Continuar**.
5. Especifique la carpeta que se supervisará y el intervalo de la frecuencia con la que la aplicación lógica debe verificar la carpeta, como se muestra en la [Figura 2-39](#).

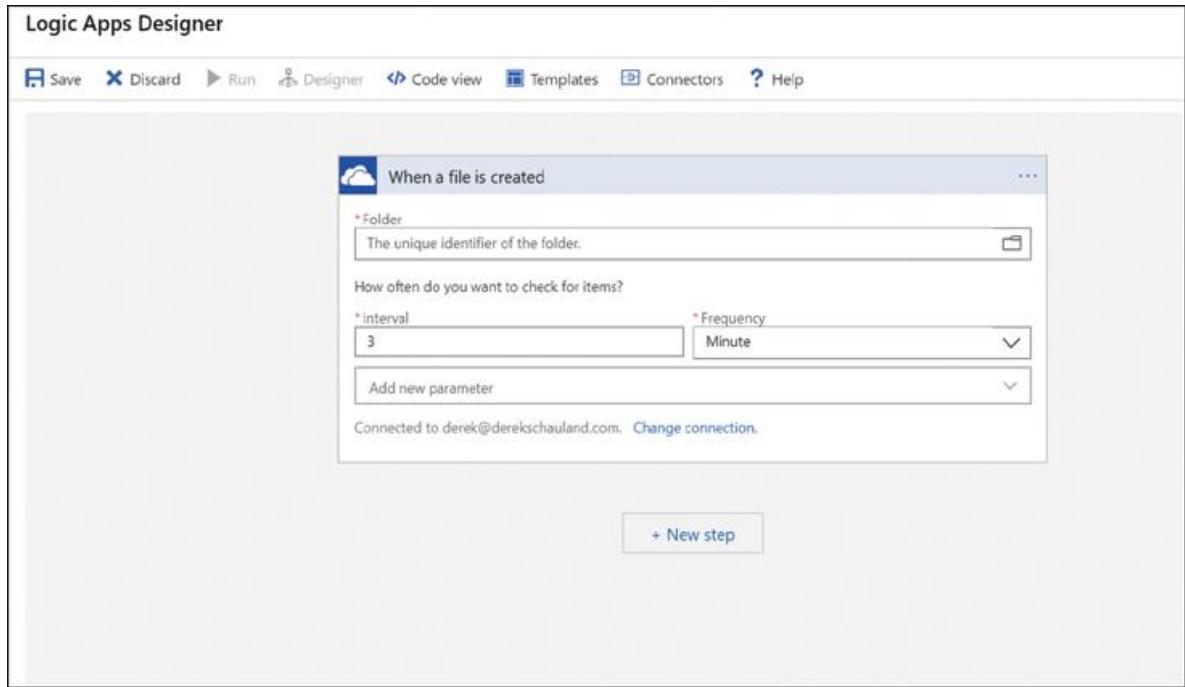


FIGURA 2-39 Especificación de la carpeta de OneDrive que se supervisará en busca de archivos nuevos

6. Elija una carpeta para monitorear haciendo clic en el ícono de carpeta al final del cuadro de texto de la carpeta y eligiendo la carpeta raíz.
7. Establezca un **intervalo**. El valor predeterminado es de 3 minutos.
8. Haga clic en **Nuevo paso** para agregar una acción a la aplicación lógica.
9. Seleccione **la plantilla de Office 365 Outlook**.
 10. Elija la opción **Enviar un correo electrónico**.
 11. Inicie sesión en Office 365.
 12. Especifique **Para**, **Asunto** y **Cuerpo** del correo electrónico, como se muestra en la Figura 2-40.

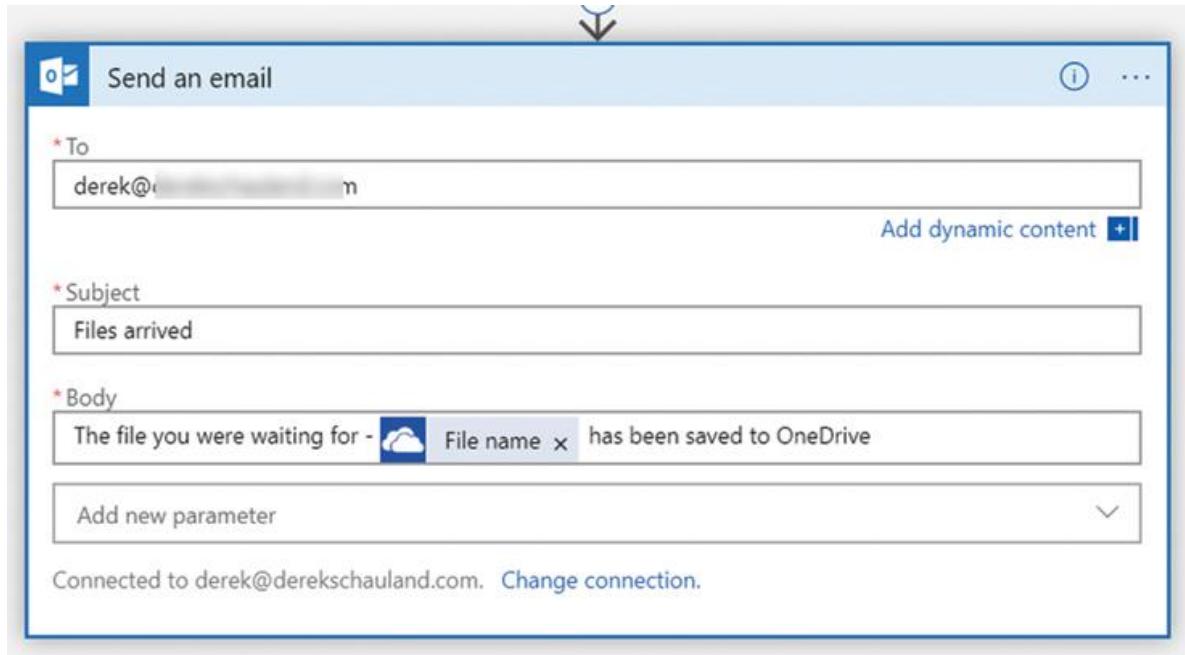


FIGURA 2-40 Configuración de una acción para enviar un correo electrónico desde una aplicación lógica

13. Haga clic en **Guardar** en la parte superior de la ventana del **Diseñador de aplicaciones lógicas** para asegurarse de que los cambios realizados en la aplicación lógica no se pierdan.
14. Haga clic en el botón **Ejecutar** en Logic Apps Designer para que la aplicación comience a buscar archivos.
15. Coloque un nuevo archivo en la carpeta que está supervisando la aplicación lógica.
16. El diseñador de aplicaciones lógicas debe mostrar el progreso de la aplicación y que todos los pasos para encontrar el archivo y enviar el mensaje de correo se hayan completado correctamente.

Administrar funciones de Azure

Azure Functions permite la ejecución de código bajo demanda, sin infraestructura que aprovisionar. Mientras que las aplicaciones lógicas brindan integración entre servicios, las aplicaciones de funciones ejecutan cualquier fragmento de código a pedido. La forma en que se activan puede ser tan versátil como las funciones mismas.

En el momento de redactar este documento, Azure Functions admite los siguientes entornos de tiempo de ejecución:

- ■ .NET
- ■ JavaScript
- ■ Java
- ■ PowerShell (que se encuentra actualmente en versión preliminar)

Para crear una aplicación de función, complete los siguientes pasos:

1. Seleccione el vínculo **Crear un recurso** en la barra de navegación de Azure Portal.
2. Escriba **aplicaciones de función** en el cuadro de búsqueda del mercado y seleccione **Aplicaciones de función**.
3. En el centro de información general de **Function Apps**, haga clic en el botón **Crear**.
4. Complete el formulario **Crear aplicación de función que se muestra en la Figura 2-41**:

Function App

Create

★ App name

az-300-function 

.azurewebsites.net

★ Subscription

Derek MVP ★ Resource Group  Create new Use existingaz-300-function 

★ OS

 Windows Linux★ Hosting Plan Consumption Plan 

★ Location

Central US 

★ Runtime Stack

PowerShell (Preview) ★ Storage  Create new Use existingaz300function862e Application Insights 

Disabled

Automation options

FIGURA 2-41 Creación de una función

1. ■ **Nombre de la aplicación.** Ingrese el nombre de la aplicación de la función.
2. ■ **Suscripción.** Ingrese la suscripción que albergará el recurso.
3. ■ **Grupo de recursos.** Cree o seleccione el grupo de recursos que contendrá este recurso.
4. ■ **SO.** Seleccione el sistema operativo que utilizará la función (Windows o Linux).
5. ■ **Plan de alojamiento.** Seleccione el modelo de precios utilizado para la aplicación: **consumo** (pago por uso) o **servicio de aplicaciones** (servicio de aplicaciones de tamaño específico).

Tenga en cuenta el nuevo plan de servicio de aplicaciones si es necesario

Si selecciona el plan de alojamiento de App Service, se agregará un mensaje para seleccionarlo / crearlo.

6. ■ **Ubicación.** Seleccione la región de Azure donde se ubicará el recurso.
 7. ■ **Pila de tiempo de ejecución.** Seleccione el entorno de ejecución para la aplicación de funciones.
 8. ■ **Almacenamiento.** Cree o seleccione la cuenta de almacenamiento que utilizará la aplicación de función.
 9. ■ **Información sobre aplicaciones.** Cree o seleccione un recurso de Application Insights para realizar un seguimiento del uso y otras estadísticas sobre esta aplicación de función.
5. Haga clic en **Crear** para crear la aplicación de funciones.

En el Grupo de recursos donde creó la aplicación de función, seleccione la función para ver la configuración y las opciones de administración para ella.

La hoja **Descripción general** de la aplicación de la función proporciona la URL, el servicio de la aplicación y la información de suscripción junto con el estado de la función (consulte la [Figura 2-42](#)).

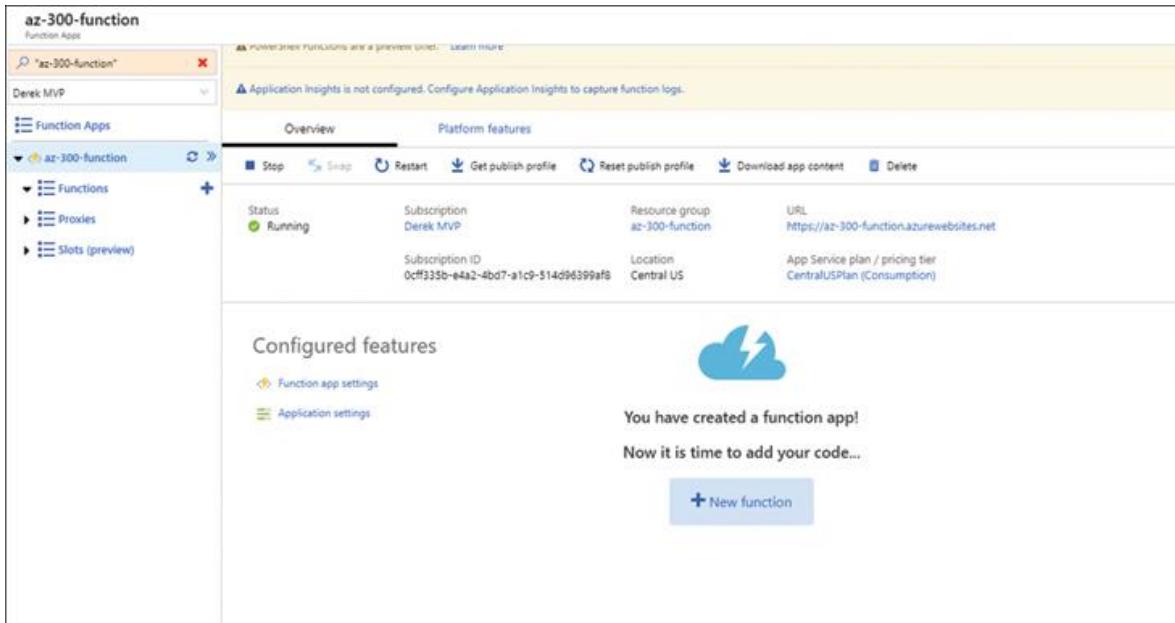


FIGURA 2-42 La hoja de información general para una función de Azure

Las aplicaciones de función están diseñadas para escuchar eventos que inician la ejecución del código. Algunos de los eventos que las funciones escuchan son

- ■ Activador HTTP
- ■ Disparador del temporizador
- ■ Almacenamiento en cola de Azure
- ■ Activador de cola de Azure Service Bus
- ■ Activador de tema de Azure Service Bus

Importante Se pueden realizar varios tipos de autenticación

Al configurar una función para el desencadenante HTTP, debe elegir el nivel de autorización para determinar si se necesitará una clave API para permitir la ejecución. Si se usa otro desencadenador de servicio de Azure, es posible que necesite una extensión para permitir que la función se comunique con otros recursos de Azure.

Además de la hoja **Información general**, hay una hoja **Características de la plataforma**, que muestra los elementos de configuración para el plan de App Service y otras partes de la configuración sin servidor de Azure para esta función. Aquí, configura cosas como redes, SSL, escalado y dominios personalizados, como se muestra en la [Figura 2-43](#).

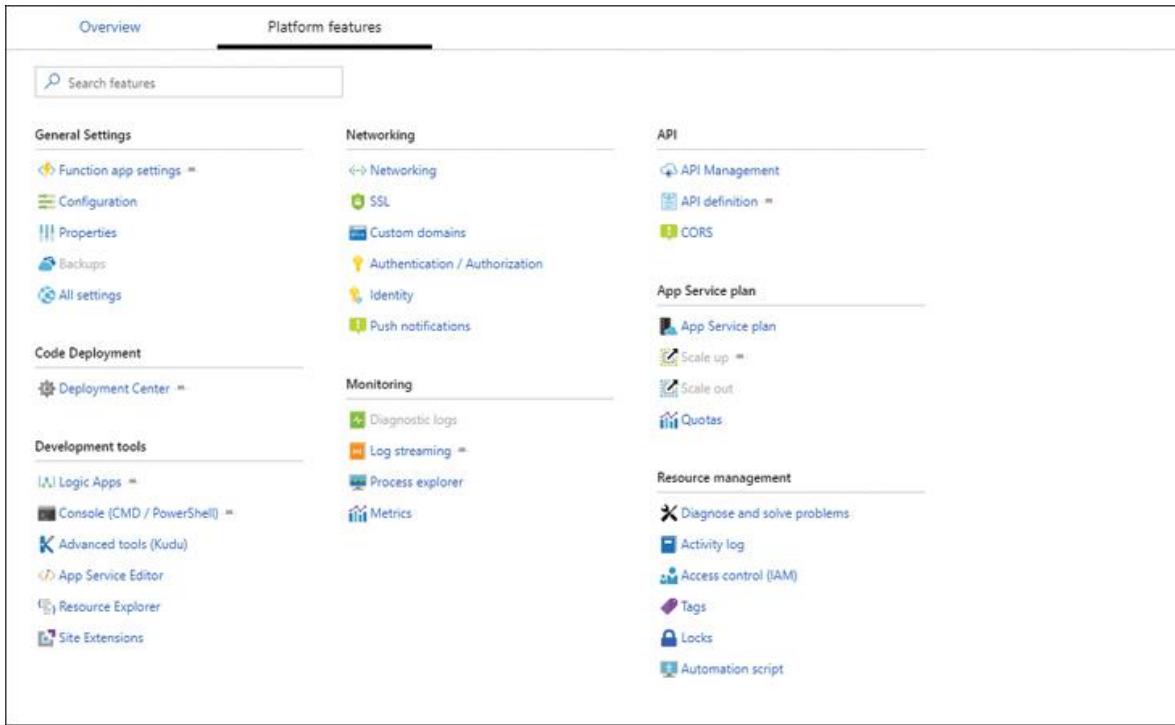


FIGURA 2-43 Hoja de características de la plataforma para una aplicación de función de Azure

Dentro de la hoja **Configuración de la aplicación** para las aplicaciones de función se encuentra la consola Kudu, que se muestra como **Herramientas avanzadas (Kudu)**. Esta consola funciona de manera muy parecida a estar conectado al sistema o al back-end de la aplicación. Debido a que esta es una aplicación sin servidor, no hay un back-end que administrar; esta herramienta se utiliza para solucionar problemas de una aplicación de función que no funciona como es necesario. La Figura 2-44 muestra el back-end de Kudu.

wiki'."/>

Kudu Environment Debug console Process explorer Tools Site extensions

Environment

Build	81.10329.3844.0 (14d700a964)
Azure App Service	82.0.7.22 (master-eb6da2b3974)
Site up time	00:00:22:23
Site folder	D:\home
Temp folder	D:\localTemp

REST API (works best when using a JSON viewer extension)

- App Settings
- Deployments
- Source control info
- Files
- Log streaming (use curl, not browser!)
- Processes and mini-dumps
- Runtime versions
- Site Extensions: installed | feed
- Web hooks
- WebJobs: all | triggered | continuous
- Functions: list | host config

More information about Kudu can be found on the [wiki](#).

FIGURA 2-44 La consola de resolución de problemas de Kudu para una aplicación de función

Nota Azure tiene una consola personalizada para solucionar problemas

Puede acceder a la consola Kudu insertando `.scm`. en la URL de la función de

Azure. <https://myfunction.azurewebsites.net> sería <https://myfunction.scm.azurewebsites.net>.

¿Necesitas más revisión? Creación y solución de problemas de Azure Functions

Para obtener información adicional, consulte

- ■ “Uso de Kudu e implementación de aplicaciones en Azure”
en https://blogs.msdn.microsoft.com/uk_faculty_connection/2017/05/15/using-kudu-and-deploying-apps-into-azure/
- ■ “Documentación de Azure Functions”
en <https://docs.microsoft.com/en-us/azure/azure-functions/>
- ■ “Ejecutar una función de Azure con desencadenadores”
en <https://docs.microsoft.com/en-us/learn/modules/execute-azure-function-with-triggers/>

Administrar Azure Event Grid

Event Grid es un servicio de consumo de eventos que se basa en la publicación / suscripción (pub / sub) para pasar información entre servicios. Supongamos que tengo una aplicación local que genera datos de registro y una función de Azure que está esperando saber qué datos de registro ha creado la aplicación local. La aplicación local publicaría los datos de registro en un tema en Azure Event Grid. La aplicación de funciones de Azure se suscribirá al tema para recibir una notificación cuando la información llegue a Event Grid.

El objetivo de Event Grid es acoplar libremente los servicios, lo que les permite comunicarse mediante una cola intermedia que se puede verificar en busca de nuevos datos según sea necesario. La aplicación de consumidor escucha la cola y no está conectada directamente a la aplicación de publicación.

Para comenzar con Event Grid, complete los siguientes pasos:

1. Abra la hoja **Suscripciones** en Azure Portal.
2. Seleccione **Proveedores de recursos** en Configuración.
3. Filtre la lista de proveedores ingresando **Event Grid** en el cuadro **Filtrar por nombre**.
4. Haga clic en el proveedor de recursos **Microsoft.EventGrid** y luego haga clic en **Registrarse** en la parte superior de la página.

Una vez que se completa el registro, puede comenzar a usar Event Grid navegando a los servicios de **Event Grid Topics** en el portal, como se muestra en la [Figura 2-45](#).

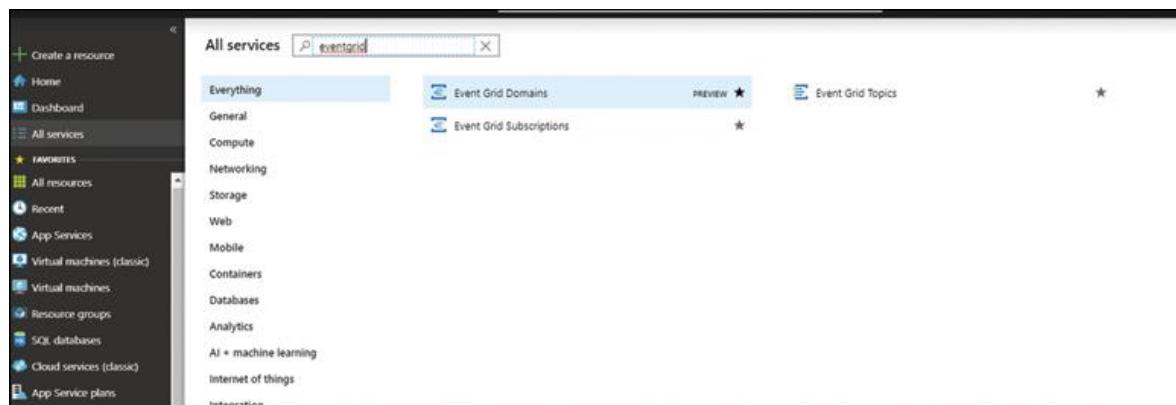


FIGURA 2-45 Temas de la cuadrícula de eventos

Una vez que una suscripción tiene temas creados, cada tema tendrá propiedades específicas relacionadas con la suscripción. Haga clic en la suscripción a la cuadrícula de eventos de la lista. En la hoja **Descripción general** del tema, están disponibles la URL del punto final del tema, el estado y la información general de la suscripción. Puede gestionar los siguientes elementos desde este punto:

- **Control de acceso.** La configuración basada en roles / IAM de Azure para la que los usuarios de Azure pueden leer, editar y actualizar el tema. El control de acceso se analiza más adelante en este capítulo.
- **Teclas de acceso.** Llaves de seguridad utilizadas para autenticar aplicaciones que publican eventos en este tema.

Asegurarse de que las aplicaciones que envían información a este tema tengan una clave para hacerlo garantizará que se controle la cantidad de ruido enviado al tema. Si la aplicación envía una cantidad de información demasiado habladora, es posible que el ruido no se reduzca.

Elemento de seguridad *importante*

Para garantizar que las claves de acceso de un tema estén protegidas y se mantengan seguras, considere colocarlas en un Key Vault como secretos. De esta manera, la aplicación que los necesita puede referirse al punto final secreto y evitar almacenar las claves de la aplicación para el tema en cualquier código. Esto evita que las claves sean visibles en texto sin formato y solo las pone a disposición de la aplicación en tiempo de ejecución.

Una vez que se ha creado un tema y se está recopilando información, los servicios consumidores que requieren esta información deben suscribirse a estos eventos y un punto final para la suscripción. En este caso, un punto final es un servicio de aplicación con una URL a la que accederán los servicios de suscriptor para interactuar con el tema.

Las suscripciones a eventos pueden recopilar toda la información enviada a un tema, o se pueden filtrar de las siguientes maneras:

- **Por tema.** Permite filtrar por el asunto de los mensajes enviados al tema, por ejemplo, solo mensajes con .jpg imágenes en ellos

- ■ **Filtro avanzado.** Un par clave-valor de un nivel de profundidad

Tenga en cuenta las limitaciones de los filtros avanzados

Estos están limitados a cinco filtros avanzados por suscripción.

Además de filtrar la información para recopilar para una suscripción, cuando selecciona la pestaña **Funciones adicionales** cuando está creando una suscripción a un evento, se muestran funciones configurables adicionales, incluidas las siguientes:

- ■ **Intentos** máximos de **entrega de eventos** Cuántos reintentos habrá.
- ■ **Tiempo de vida del evento.** La cantidad de días, horas, minutos y segundos que se reintentará el evento.
- ■ **Letras muertas.** Seleccione si los mensajes que no se pueden entregar deben almacenarse.
- ■ **Hora de vencimiento de la suscripción al evento.** Cuando la suscripción caducará automáticamente.
- ■ **Etiquetas.** Cualquier etiqueta que pueda ayudar a identificar la suscripción.

¿Necesitas más revisión? Trabajar con Event Grid

Consulte los artículos en las siguientes URL para obtener información adicional:

- ■ "Conceptos en Azure Event Grid"
en <https://docs.microsoft.com/en-us/azure/event-grid/concepts>
- ■ "Comprender el filtrado de eventos para las suscripciones a Event Grid"
en <https://docs.microsoft.com/en-us/azure/event-grid/event-filtering>
- ■ "Fuentes de eventos en Azure Event Grid"
en <https://docs.microsoft.com/en-us/azure/event-grid/event-sources>

Administrar Azure Service Bus

Azure Service Bus es un servicio de mensajería asincrónica de varios inquilinos que puede funcionar con la cola primero en entrar, primero en salir (FIFO) o el intercambio de información de publicación / suscripción. Usando colas, el servicio de bus de mensajes intercambiará mensajes con un servicio asociado. Si está utilizando el modelo de publicación / suscripción (pub / sub), el remitente puede enviar información a cualquier número de servicios suscritos.

Un espacio de nombres de bus de servicio tiene varias propiedades y opciones que se pueden administrar para cada instancia:

- **Políticas de acceso compartido.** Las claves y cadenas de conexión disponibles para acceder al recurso. El nivel de permisos, administrar, enviar y escuchar se configuran aquí porque forman parte de la cadena de conexión.
- **Escala.** El nivel de servicio utilizado por el servicio de mensajería: Básico o Estándar.

Nota Una nota sobre SKU

Se puede configurar un espacio de nombres con un SKU premium, que permite la recuperación geográfica en caso de un desastre en la región donde existe el bus de servicio. La selección de un SKU premium solo está disponible en el momento de la creación.

- **Recuperación geográfica.** Configuraciones de recuperación ante desastres que están disponibles con un espacio de nombres Premium.
- **Exportar plantilla.** Una plantilla de automatización ARM para el recurso de bus de servicio.
- **Colas.** Las colas de mensajería utilizadas por el bus de servicio.

Cada cola configurada muestra la URL de la cola, el tamaño máximo y los recuentos actuales sobre los siguientes tipos de mensajes:

- **Mensajes activos.** Mensajes actualmente en cola.
- **Mensajes programados.** Estos mensajes se envían a la cola mediante trabajos programados o en un horario general.

- **Mensajes de letra muerta.** Los mensajes de letra muerta no se pueden entregar a ningún receptor.
- **Transferir mensajes.** Mensajes pendientes de transferencia a otra cola.
- **Transferir mensajes de letra muerta.** Mensajes que no se pudieron transferir a otra cola.

Además de ver la cantidad de mensajes en la cola, puede crear permisos de acceso compartido para la cola. Esto permitirá que se asignen permisos de administración, envío y escucha. Además, esto proporciona una cadena de conexión que aprovecha los permisos asignados que la aplicación de escucha utilizará como punto final al recopilar información de la cola.

En la hoja **Descripción general** de la cola de mensajes seleccionada, se pueden actualizar las siguientes configuraciones:

- **Mensaje Time to Live**
- **Duración del bloqueo de mensajes**
- **Historial de detección duplicado**
- **Recuento máximo de entregas**
- **Tamaño máximo**
- **Letras muertas**
- **Reenviar mensajes a**

La configuración de una cola de mensajes es similar a las descritas anteriormente en la sección "Administrar Azure Event Grid" porque tienen un propósito similar para las colas configuradas.

¿Necesitas más revisión? Mensajería de bus de servicio

Consulte los artículos en las siguientes URL para obtener información adicional:

- "[¿Qué es Azure Service Bus?](https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview)" en <https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview>
- "Elija entre los servicios de mensajería de Azure: Event Grid, Event Hubs y Service Bus" en <https://docs.microsoft.com/en-us/azure/event-grid/choose-between-service-bus-event-grid-and-event-hubs>

[grid/compare-messaging-services?toc=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fservice-bus-messaging%2FTOC.json & bc = https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fbread%2Ftoc.json](https://docs.microsoft.com/en-us/azure/service-bus-messaging/TOC.json)

- “Elija un modelo de mensajería en Azure para conectar libremente sus servicios” en <https://docs.microsoft.com/en-us/learn/modules/choose-a-messaging-model-in-azure-to-connect-your-servicios>

HABILIDAD 2.4: GESTIONAR LA SEGURIDAD DE LAS APLICACIONES

Azure Active Directory está disponible para registrar aplicaciones y usuarios para acceder a servicios y aplicaciones. En esta sección se explica cómo se registran las aplicaciones y otros recursos de Azure en Azure Active Directory y cómo se administran los valores confidenciales mediante un servicio llamado Azure Key Vault.

Esta habilidad cubre:

- [Uso de Azure Key Vault para almacenar y administrar secretos de aplicaciones](#)
- [Uso de la identidad administrada de Azure Active Directory](#)
- [Registro de la aplicación de Azure Active Directory](#)

Uso de Azure Key Vault para almacenar y administrar secretos de aplicaciones

Las aplicaciones necesitan acceso a recursos fuera de lo que se está desarrollando. Colocar credenciales, claves de API u otra información potencialmente confidencial en el código es algo que puede hacer que los desarrolladores se reúnan con InfoSec, lo que podría significar problemas. Azure tiene un servicio que puede resolver este problema: Key Vault.

Azure Key Vault es un servicio de almacenamiento cifrado creado específicamente para almacenar los siguientes elementos:

- ■ Llaves
- ■ Secretos
- ■ Certificados

Todos estos elementos están cifrados en reposo y solo son visibles para las cuentas de usuario, los principales de servicio (aplicaciones registradas) o las identidades administradas a las que se les concede acceso para usarlos.

Key Vault, como todos los demás recursos, puede tener acceso controlado por IAM, que en este caso, significa la capacidad del usuario o grupo para ver o acceder al recurso Key Vault. Esto no se aplica a los elementos contenidos en Key Vault. Para acceder a secretos, claves y certificados, el usuario o la aplicación deberán estar identificados en una política de acceso específica para el Key Vault particular que contiene estos elementos.

Para crear el recurso de Key Vault, siga estos pasos:

1. Inicie sesión en el portal de Azure <https://portal.azure.com> .
2. Seleccione el botón **Crear un recurso** en la pantalla de inicio.
3. Busque **Key Vault** en la hoja **Nuevos recursos** .
4. En la hoja del mercado de **Key Vault** , haga clic en **Crear** .
5. Seleccione la **suscripción** que albergará el recurso de Key Vault.
6. Seleccione un **grupo de recursos** (o cree uno) que se utilizará para administrar el recurso de Key Vault.
7. Ingrese un **nombre** para el recurso de Key Vault.
8. Seleccione una **región** para el recurso de Key Vault.
9. Elija un **nivel de precios** :
 1. ■ **Estándar.** Solución de gestión de claves basada únicamente en software
 2. ■ **Premium.** Módulo de seguridad de software y hardware (HSM): solución de gestión de claves respaldada

Tenga en cuenta cuándo elegir Premium

Elija los precios premium de Key Vault solo si necesita datos respaldados por HSM. Ésta es la única diferencia entre los dos

niveles; todos los demás precios son los mismos. Si necesita las funciones de HSM, el precio aumenta un poco.

10. Habilite **Soft Delete**.
11. Determine el período de retención si **Soft Delete** está habilitado.
12. Habilite la **protección de purga**.
13. Haga clic en **Siguiente** para crear una política de acceso.

Soft Delete marca un valor o almacén de claves para su eliminación después de un número configurado de días antes de eliminar los elementos almacenados de forma permanente. La cantidad de días está determinada por el período de retención elegido cuando se crea Key Vault.

Nota solo una vez

Cuando se establece un valor de retención, no se puede cambiar ni eliminar de Key Vault. Lo mismo ocurre con la protección de purga; una vez que se establece en verdadero, los elementos guardados en Key Vault se guardan durante 90 días antes de ser eliminados permanentemente.

Una política de acceso gestiona la seguridad de los elementos contenidos en un Key Vault. Un Key Vault puede tener varias políticas de acceso.

Crear una política de acceso, completando los siguientes pasos mientras se hace referencia a las figuras 2-46 y 2-47.

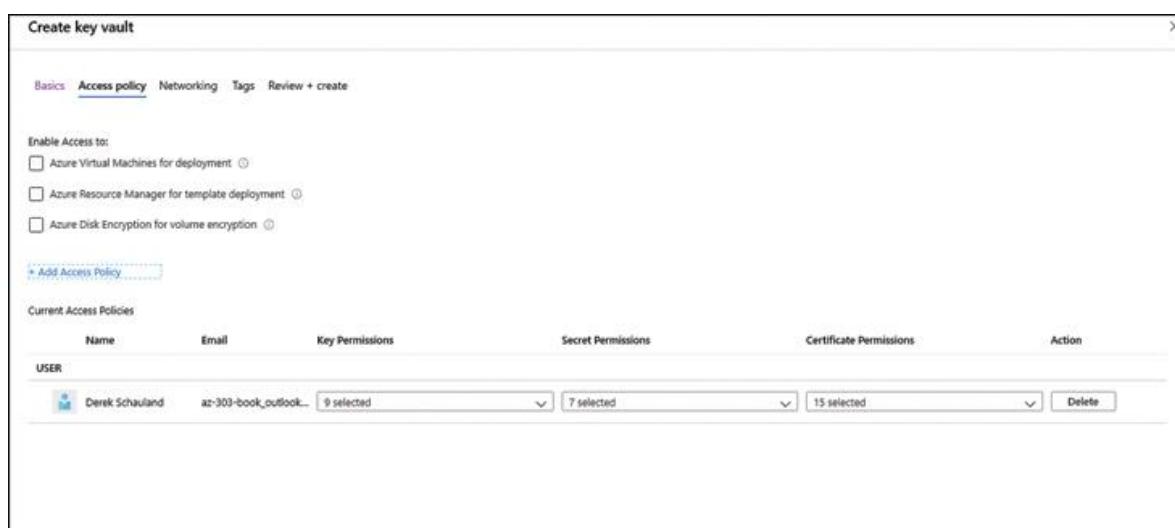


FIGURA 2-46 Creación de una política de acceso de Azure Key Vault

Add access policy

Add access policy

Configure from template (optional)

Key permissions

0 selected

Secret permissions

0 selected

Certificate permissions

0 selected

Select principal

*

None selected >

Authorized application ⓘ

None selected

Add

FIGURA 2-47 Configurar la clave, el secreto y el certificado con una directiva de acceso de Azure Key Vault

1. En la hoja de recursos de **Key Vault** en Azure Portal, seleccione **Directiva de acceso** en la lista de navegación.
2. Especifique si este Key Vault se puede utilizar para la implementación de VM.
3. Especifique si las plantillas de implementación pueden utilizar este Key Vault durante la implementación; piense en el almacenamiento de credenciales administrativas.
4. Especifique si este Key Vault debe usarse para la información de Azure Disk Encryption.
5. Haga clic en el enlace **Agregar política de acceso**.
6. Si lo desea, seleccione una plantilla para configurar una política de acceso.
7. Seleccione los permisos para los valores clave almacenados en este almacén de claves:

Operaciones de gestión de claves

- ■ **Obtener.** Recuperar valores clave
- ■ **Lista.** Lista de claves contenidas en Key Vault
- ■ **Actualización.** Modificar valores clave existentes
- ■ **Crear.** Crea nuevas claves
- ■ **Importar.** Importar valores clave
- ■ **Eliminar.** Quitar llaves
- ■ **Recuperarse.** Recuperar claves eliminadas
- ■ **Copia de seguridad.** Claves de respaldo
- ■ **Restaurar.** Restaurar copias de seguridad de claves

Operaciones criptográficas

- ■ **Descifrar.** Descifrar datos almacenados criptográficamente
- ■ **Encriptar.** Cifrar datos para almacenar
- ■ **Desenvolver llave.** Descifrar datos de claves simétricas
- ■ **Llave de envoltura.** Cifrar datos de claves simétricas
- ■ **Verificar.** Proporciona verificación de datos clave almacenados en Key Vault
- ■ **Firmar.** Utiliza datos clave almacenados para firmar aplicaciones y recursos.

Operaciones clave privilegiadas

- ■ **Purgar.** Eliminar datos clave de Key Vault de forma permanente
8. Seleccione los permisos para los secretos almacenados en este Key Vault:
1. ■ **Obtener.** Permite el acceso a valores secretos.
 2. ■ **Lista.** Permite el acceso para ver qué secretos se almacenan en Key Vault
 3. ■ **Establecer.** Escribir un secreto y su valor en Key Vault

4. ■ **Eliminar.** Eliminar un secreto de Key Vault
5. ■ **Recuperarse.** Devolver un secreto eliminado a Key Vault
6. ■ **Copia de seguridad.** Capture una copia externa de un secreto almacenado en Key Vault
7. ■ **Restaurar.** Importar una copia externa de un secreto a Key Vault
8. ■ **Purgar.** Eliminar de forma permanente un secreto de Key Vault después del período de retención configurado
9. Seleccione los permisos para los certificados almacenados en Key Vault:
 - 0.■ **Obtener.** Permitir el acceso a los valores del certificado
 - 1.■ **Lista.** Permitir el acceso para ver qué certificados están almacenados en Key Vault
 - 2.■ **Actualización.** Permitir que se actualicen los valores de certificado existentes almacenados
 - 3.■ **Crear.** Agregar nuevos certificados a Key Vault desde el portal
 - 4.■ **Importar.** Importar certificados existentes a Key Vault
 - 5.■ **Eliminar.** Quitar un certificado de Key Vault
 - 6.■ **Recuperarse.** Devolver un certificado eliminado a Key Vault
 - 7.■ **Copia de seguridad.** Crear una copia de seguridad de un archivo externo de un certificado
 - 8.■ **Restaurar.** Cree un valor de certificado en Key Vault a partir de una copia de seguridad externa
 - 9.■ **Administrar contactos.** Agregar o editar contactos asociados con un certificado almacenado
 10. ■ **Gestionar autoridades de certificación.** Agregar, editar o eliminar autoridades de certificación para los certificados almacenados en Key Vault

11. ■ **Obtenga autoridades de certificación.** Revise la información de la autoridad de certificación existente en Key Vault
 12. ■ **Enumere las autoridades de certificación.** Lista de las autoridades de certificación almacenadas en Key Vault
 13. ■ **Establecer autoridades de certificación.** Actualizar / crear datos de la autoridad de certificación almacenados en Key Vault
 14. ■ **Eliminar autoridades de certificación.** Eliminar los datos de la autoridad de certificación almacenados en Key Vault
 15. ■ **Purgar.** Elimine permanentemente los datos del certificado almacenados en Key Vault según los días de retención establecidos para el recurso de Key Vault
10. Seleccione el principal de la política de acceso: el usuario, el grupo o la aplicación a la que se aplica esta política.
- 0.■ Busque el usuario o grupo necesario y haga clic en **Seleccionar**.
 11. Especifique las aplicaciones autorizadas que pueden acceder a este Key Vault a través de esta política de acceso. (Esta opción generalmente está bloqueada y no está disponible para su selección).
 12. Haga clic en **Agregar** para crear la política.

Tenga en cuenta que algunas cosas son mejores juntas

Cuando esté buscando asignar permisos de lectura, considere mantener el acceso a la lista y la obtención juntos dentro de una política de acceso. Es más fácil seleccionar el extremo secreto correcto cuando se pueden enumerar todos los secretos.

Nota sobre las bóvedas de claves

Un Key Vault es una excelente manera de almacenar información confidencial, pero también tiene una desventaja. Cuando configura una política de acceso, ese acceso se asigna al almacén de claves. No es específico de un registro individual dentro de Key Vault. Si puede

ver un secreto, puede verlos todos, algo que debe tener en cuenta al usar un Key Vault.

Una vez asignados los permisos a través de una política de acceso, no olvide hacer clic en el botón **Guardar** dentro del recurso para escribir las políticas en Key Vault.

Accediendo a un endpoint

Una vez que un valor se almacena dentro de un Key Vault, se le asigna un punto final HTTPS para permitir el acceso. Si la entidad que accede al punto final aparece en una política de acceso con permiso para usar el valor, el valor se usa en lugar del punto final. Un Key Vault es una excelente manera de mantener la información confidencial solo accesible para las aplicaciones o los usuarios que la necesitan. Vive dentro de Azure y no requiere suscripciones o servicios de terceros para administrar esta información para una organización.

Uso de la identidad administrada de Azure Active Directory

Azure Active Directory es una excelente manera de autenticar cuentas de usuario y proporcionar servicios como el inicio de sesión único para aplicaciones. Managed Identity extiende estas características a otros recursos de Azure, incluidos, entre otros,

- ■ Servicios de aplicaciones
- ■ Aplicaciones de función
- ■ Máquinas virtuales

Los ejemplos anteriores son servicios a los que se les puede asignar una identidad administrada que permite la interacción con otros servicios de Azure. Azure permite dos tipos de identidades administradas: asignadas por el sistema y asignadas por el usuario:

- ■ **Identidad administrada asignada por el sistema.** Este tipo de identidad administrada está habilitado en una instancia de servicio en Azure, y la identidad para el servicio se crea en Azure Active Directory y es de confianza para la suscripción que contiene la instancia del servicio. El ciclo de vida de las credenciales de la instancia de servicio está directamente

vinculado al ciclo de vida de la instancia de servicio sin necesidad de una administración adicional de las credenciales asignadas.

- ■ **Identidad administrada asignada por el usuario.** Este tipo de identidad administrada se crea como un recurso independiente dentro de Azure y se le asigna una entidad de servicio dentro de Azure Active Directory. Una vez que se crea la entidad de servicio, se puede asignar a una o más aplicaciones o instancias de Azure. El ciclo de vida de una identidad asignada por el usuario se gestiona independientemente de los recursos a los que está asignada.

A menos que su organización tenga requisitos específicos para administrar estas identidades, las identidades administradas asignadas por el sistema reducen la sobrecarga de administración y brindan el mismo nivel de seguridad y acceso que las identidades administradas asignadas por el usuario.

Por ejemplo, una bóveda de claves puede contener información confidencial y permitir que otros recursos accedan a esa información. Si, por ejemplo, mi aplicación necesita conectarse a una base de datos, necesitará una cadena de conexión para hacerlo. La cadena de conexión probablemente contiene un ID de usuario y una contraseña o clave que proporciona a la base de datos una forma de verificar que la aplicación que solicita el acceso debe poder conectarse. Debido a que la cadena de conexión es una información confidencial, almacenarla en Key Vault tiene sentido porque estará encriptada y solo será accesible para aquellos que tengan políticas de acceso asignadas.

Como administrador de Key Vault, el usuario Derek podría agregar la cadena de conexión como un secreto y verla una vez agregada. Sin embargo, Derek no es la aplicación, por lo que si la aplicación llamaba a un punto final para la cadena de conexión, la conexión fallaría o devolvería un error sobre una identidad no válida.

La asignación de una identidad administrada a la aplicación proporciona un registro en Azure Active Directory y devuelve las siguientes credenciales para la aplicación:

- ■ **ID de cliente.** Este es un identificador dentro de Azure Active Directory para la aplicación y su entidad de servicio (identidad administrada).

- ■ **Identificación principal.** Este es el `objectID` de la aplicación dentro de Azure Active Directory para la aplicación.
- ■ **Servicio de metadatos de instancia de Azure.** Este es un punto de conexión de descanso al que solo se puede acceder desde los recursos de la máquina virtual de Azure Resource Manager en una dirección IP conocida y no enrutable (169.254.169.254).

Una vez que se asigna una identidad administrada, a la aplicación se le puede asignar acceso basado en roles a los recursos en Azure y, al igual que la cuenta de usuario, a Derek se le pueden asignar estos permisos. Además, en el caso de un Key Vault, la aplicación puede tener asignada una política de acceso. Esto otorgará los permisos establecidos en la política de acceso a todos los elementos dentro de Key Vault.

Con Managed Identity habilitado para la aplicación y con una política de acceso configurada, el código de la aplicación puede hacer referencia a la cadena de conexión para las bases de datos necesarias simplemente llamando al punto final secreto.

Para habilitar la identidad administrada para un servicio de aplicaciones de Azure, siga estos pasos:

1. Inicie sesión en Azure Portal.
2. Busque el recurso del servicio de aplicaciones al que se asignará la identidad administrada.
3. En el panel de navegación que se muestra en la [Figura 2-48](#), seleccione **Identidad** en la sección **Configuración**.

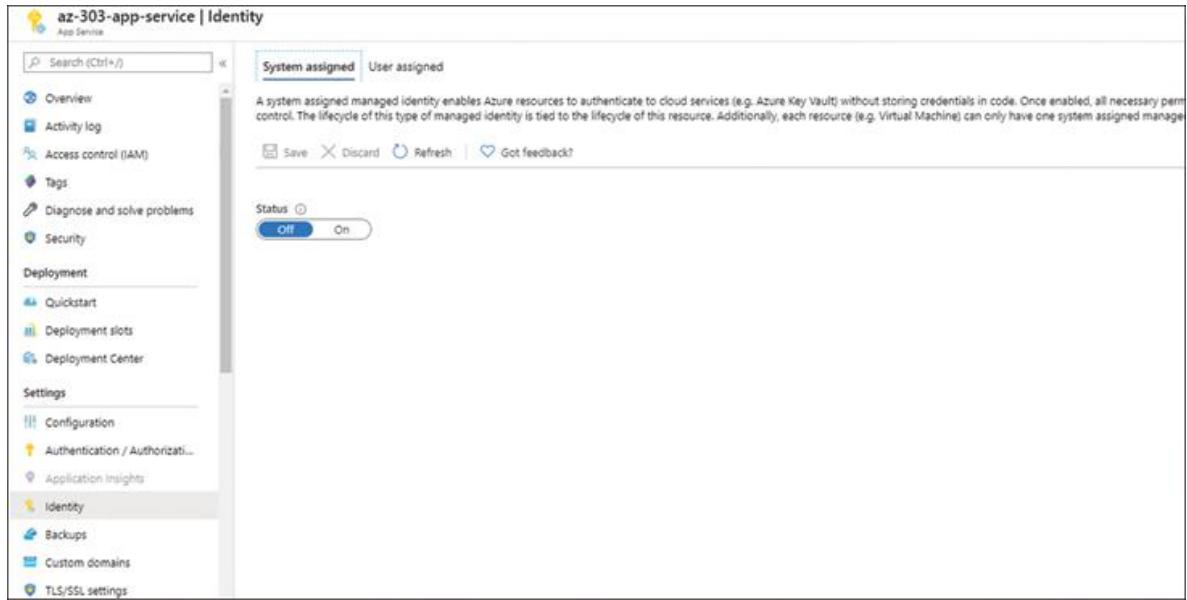


FIGURA 2-48 Identidad administrada para App Service

4. En la pestaña **Asignado por el sistema**, cambie el **Estado** a **Activado** y haga clic en **Guardar** para usar una identidad asignada por el sistema.
5. Para usar una identidad asignada por el **usuario**, seleccione la pestaña **Asignado por el usuario** y haga clic en **Agregar**.
6. Seleccione la identidad administrada asignada por el usuario que desea asignar a esta aplicación.

Aplicaciones y credenciales de Azure Manage

Una vez que se asigna la identidad administrada, no es necesario que conozca o administre el secreto del cliente (contraseña). Esta contraseña está completamente administrada por Azure y la aplicación.

Para los servicios que admiten la habilitación de la opción de identidad administrada, la identidad administrada crea un registro de aplicación para el recurso donde está habilitada la función; al menos en parte, lo hace mediante la creación de una entidad de servicio dentro de Azure Active Directory. Los registros de aplicaciones se tratan en detalle en la siguiente sección, "Registro de aplicaciones de Azure Active Directory".

Registro de la aplicación de Azure Active Directory

Al igual que las identidades administradas, los registros de aplicaciones en Azure Active Directory son un método que se usa para identificar las aplicaciones y permitirles el acceso y la asignación de roles. Se puede crear una aplicación o registro de aplicación para aplicaciones creadas por su organización o para aplicaciones de terceros que podrían estar aprovechando las capacidades de inicio de sesión único proporcionadas por Azure Active Directory.

Para crear un registro de aplicación en Azure Active Directory mediante Azure Portal, complete los siguientes pasos y consulte la Figura 2-49:

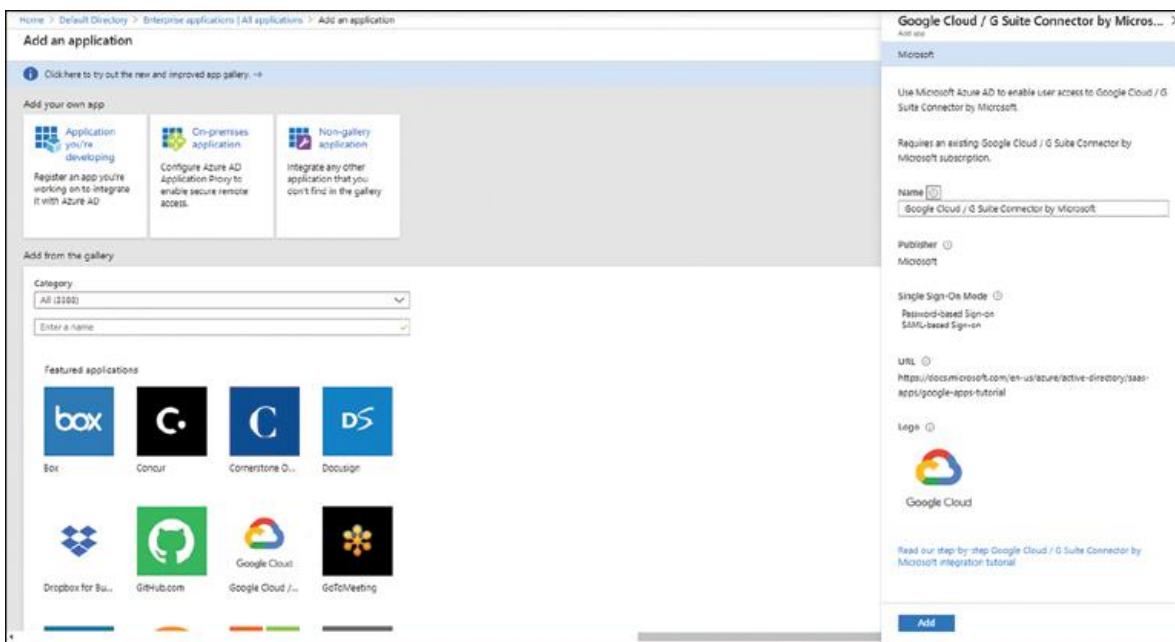


FIGURA 2-49 Registro de una aplicación empresarial / galería

1. En el menú de navegación de Azure Portal, seleccione **Azure Active Directory**.
2. Asegúrese de que esté seleccionado el inquilino adecuado de Azure Active Directory. Muchas organizaciones solo tienen un inquilino, pero se permite más de un inquilino de Azure Active Directory.
3. Seleccione **Aplicaciones empresariales**.
4. Seleccione **Nueva aplicación**.
5. Elija el tipo de aplicación para registrarse:

1. ■ Una aplicación que está desarrollando.
 2. ■ Una aplicación local a través de un proxy de aplicación.
 3. ■ Una aplicación que no es de galería, que es cualquier otra aplicación que no esté en la galería.
 4. ■ Una aplicación de galería (mercado). Al momento de escribir estas líneas, hay 3.388 aplicaciones en la galería.
6. Para una aplicación de galería, seleccione o busque la aplicación y haga clic en la galería para registrarse.
 7. Ingrese un nombre y otros detalles para el registro, si es necesario, y haga clic en **Agregar**.

Para una aplicación en la que su organización está trabajando, complete los siguientes pasos y consulte la Figura 2-50:

The screenshot shows the 'Register an application' form. The 'Name' field is filled with 'my registered application'. Under 'Supported account types', the first option ('Accounts in this organizational directory only') is selected. The 'Redirect URI (optional)' dropdown is set to 'Web' and contains the value 'https://localhost'. At the bottom, there is a link to 'Microsoft Platform Policies' and a blue 'Register' button.

Register an application

* Name
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Web

By proceeding, you agree to the Microsoft Platform Policies [\[?\]](#)

Register

FIGURA 2-50 Registro de una aplicación desarrollada internamente

1. En el menú de navegación de Azure Active Directory, seleccione **Registros de aplicaciones** .
2. Haga clic en **Registrar una aplicación** .
3. Proporcione un **nombre** para la aplicación.
4. Seleccione el contexto en el que estará disponible la aplicación:
 1. **Cuentas en este directorio organizativo únicamente (directorio predeterminado Solo - inquilino individual)**
 2. **Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: Multiarrendatario)**
 3. **Cuentas en cualquier directorio organizativo (cualquier directorio de Azure AD: Cuentas de Microsoft personales y de múltiples inquilinos, como Skype o Xbox)**
5. Ingrese un **URI de redireccionamiento** opcional .
6. Haga clic en **Registrarse** .

La tenencia de la aplicación determina

- **Si solo su organización puede utilizar el registro de la aplicación.**
- **Si cualquier otro inquilino de Azure Active Directory puede usar el registro de la aplicación.**
- **Si además de cualquier inquilino de Azure Active Directory, cualquier servicio de cuenta personal de Microsoft (Xbox o Skype) puede acceder a la aplicación.**

El tipo de aplicación que se está registrando y / o la política de la empresa pueden dictar esta selección.

El URI de redireccionamiento es opcional y se puede completar como <https://localhost> si no hay un URI de redireccionamiento requerido por la aplicación. Este URI determina dónde se enviará la respuesta de autenticación.

Para crear un registro de aplicación en Azure Active Directory con PowerShell, ejecute el siguiente código:

[Haga clic aquí para ver la imagen del código](#)

```

Connect-AzureAD -tenantid <su ID de inquilino de anuncios de
Azure> Connect-AzureAD -tenantid <your azure ad tenant id>

$ applicationName = "mi última aplicación"

$ AppURI = "https://myapp.azurewebsites.net"

If (! ($ Myapp = get-azureadapplication -filter "DisplayName
-eq '$ ($ applicationName)'"))

{
    $ myapp = new-azureadapplication -displayname $ applicationName -identifierUris

    $ appURI
}

```

Deberá tener instalado el módulo de Azure AD para registrar una aplicación a través de PowerShell.

Este código especifica el nombre y la URL de la aplicación para la aplicación y luego verifica Azure AD para asegurarse de que la aplicación que se está registrando no esté ya registrada en el inquilino. Si no se encuentra la aplicación, se registra en Azure AD.

Creación de secretos de aplicación para aplicaciones registradas

Ahora que la próxima gran aplicación se ha registrado en Azure Active Directory, tiene un ID de aplicación (cliente) al igual que el ID de aplicación mencionado anteriormente para identidades administradas y se puede encontrar en Azure AD. Todavía no tiene un secreto de cliente configurado porque el proceso manual de registro de la aplicación requiere que el administrador cree también el secreto.

Nota Dos ID de un solo uso

La identificación de la aplicación y la identificación del cliente para las aplicaciones registradas son las mismas; sin embargo, Microsoft generalmente ha tenido dos nomenclaturas para este valor.

Para agregar un secreto de cliente para el registro de su aplicación, complete los siguientes pasos:

1. Dentro de Azure Active Directory, seleccione **Registros de aplicaciones**.
2. Busque y seleccione su aplicación registrada.
3. En el menú de navegación, seleccione **Certificados y secretos**.
4. Haga clic en **Nuevo secreto de cliente** para crear un valor secreto para esta aplicación y establecer la información de vencimiento.
5. Ingrese una descripción para el secreto y seleccione una caducidad.
6. Haga clic en **Agregar**.

Nota: los secretos son secretos

Al agregar un nuevo secreto, el valor se muestra en el portal solo mientras está en la pantalla donde se muestra el secreto por primera vez. Debería desaparecer si navega fuera de esta pantalla y no se puede recuperar una vez descartado. Asegúrese de copiar el valor en algún lugar para mantenerlo a salvo antes de salir de la pantalla. Un Key Vault es un gran lugar para almacenar estos valores.

Si está agregando un secreto de cliente a través de PowerShell, puede elegir la fecha de vencimiento que desee; por ejemplo, puede establecer esto en 5 años. También puede recopilar el secreto del cliente de PowerShell para el registro de una aplicación existente después del hecho. Para agregar un secreto de cliente en PowerShell, ejecute el siguiente código:

[Haga clic aquí para ver la imagen del código](#)

```
$ application = get-azureadapplication  
$ secretStartDate = obtener-fecha  
$ secretExpireDate = (obtener-fecha) .addyears (5)
```

```
$ aadClientSecret = new-azureadapplicationpasswordcredential  
-objectid $ aplicación.  
  
objectid -customkeyidentifier "App Secret" -startdate $  
secretStartDate -enddate  
  
$ secretEndDate
```

Nota Revise Powershell antes de copiarlo de Internet

Asegúrese de comprender cómo funciona este PowerShell y de haberlo examinado. Además, los valores de las variables enumerados aquí generalmente no funcionarán a menos que los edite para usarlos en su entorno.

¿Necesitas más revisión? Más información sobre la seguridad de las aplicaciones de Azure

Consulte los artículos en las siguientes URL para obtener información adicional:

- “Conceptos básicos de Azure Key Vault” en <https://docs.microsoft.com/en-us/azure/key-vault/basic-concepts>
- “¿Qué son las identidades administradas para los recursos de Azure?” en <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>
- “Registro de su aplicación en Azure AD” en <https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/registrationinazureactivedirectory>

HABILIDAD 2.5: IMPLEMENTAR EL EQUILIBRIO DE CARGA Y LA SEGURIDAD DE LA RED

Azure tiene un par de opciones diferentes para el equilibrio de carga: el equilibrador de carga de Azure que opera en la capa de transporte de la pila de red y la puerta de enlace de la aplicación que se suma al

equilibrador de carga en la capa 4 y agrega el equilibrio de carga de la capa 7 (HTTP) encima de esta configuración usando reglas adicionales. Con algunas adiciones recientes al espacio de seguridad, se están agregando recursos adicionales constantemente para mejorar la postura de seguridad de los clientes que utilizan los servicios de Azure. Los nuevos servicios incluyen

- ■ Cortafuegos de Azure
- ■ Puerta de entrada azul
- ■ Administrador de tráfico de Azure
- ■ Grupos de seguridad de redes y aplicaciones
- ■ Bastión Azure

Esta habilidad cubre cómo:

- ■ [Configurar Application Gateway y reglas de equilibrio de carga](#)
- ■ [Implementar configuraciones de IP de front-end](#)
- ■ [Administrar el equilibrio de carga de la aplicación](#)
- ■ [Configurar y administrar Azure Firewall](#)
- ■ [Configurar y administrar Azure Front Door](#)
- ■ [Implementar Azure Traffic Manager](#)
- ■ [Implementar grupos de seguridad de redes y aplicaciones](#)

Configurar Application Gateway y reglas de equilibrio de carga

Una puerta de enlace de aplicaciones tiene la siguiente configuración que puede configurar para ajustar el recurso a las necesidades de una organización:

- ■ **Configuración.** Configuración para actualizar el nivel, el SKU y el recuento de instancias; indicar si HTTP / 2 está habilitado.
- ■ **Cortafuegos de aplicaciones web.** Permite el ajuste del nivel de firewall para el dispositivo (estándar o WAF) y si la configuración del firewall para la puerta de enlace está habilitada o deshabilitada.

- Al habilitar WAF en una puerta de enlace, el recurso en sí se establece de forma predeterminada en un nivel **Medio**.
- Si el **estado del firewall** está habilitado, la puerta de enlace evalúa todo el tráfico excepto los elementos excluidos en una lista definida (consulte la [Figura 2-51](#)). La configuración del firewall / WAF permite que la puerta de enlace se configure solo para detección (registro) o prevención.

FIGURA 2-51 Configuración de WAF en una puerta de enlace de aplicaciones

Nota La auditoría en el cortafuegos requiere diagnósticos

Cuando se utiliza la configuración del cortafuegos en el modo WAF, habilitar el modo de detección requiere que se habiliten los diagnósticos para revisar la configuración registrada.

- **Grupos de back-end** Los nodos o aplicaciones a los que la puerta de enlace de aplicaciones enviará tráfico.

Nota: cualquier cosa puede ser un grupo de back-end

Los grupos se pueden agregar mediante FQDN o dirección IP, máquina virtual, VMSS y servicios de aplicaciones. Para los nodos de destino no hospedados en Azure, el método de dirección IP / FQDN permite servicios de back-end externos.

- ■ **Configuración de HTTP.** Éstas son las configuraciones de puerto para los grupos de back-end. Si configuró la puerta de enlace con HTTPS y certificados durante la instalación, este valor predeterminado es 443; de lo contrario, comienza con el puerto 80. Otras configuraciones relacionadas con HTTP que se administran aquí son las siguientes:
 - ■ Afinidad basada en cookies (sesiones adhesivas)
 - ■ Conexión de drenaje, que garantiza que las sesiones en vuelo en el momento en que se elimina un servicio de back-end podrán completarse
 - ■ Anular rutas para servicios de back-end, que permiten que los directorios o servicios especificados se redireccionen a medida que pasan a través de la puerta de enlace.
- ■ **Oyentes.** Estos determinan qué direcciones IP se utilizan para los servicios de front-end administrados por esta puerta de enlace. El tráfico llega al extremo frontal de la puerta de enlace y se procesa mediante reglas configuradas a medida que se mueve a través de la puerta de enlace de la aplicación. Los oyentes están configurados para direcciones IP y emparejamientos de puertos.
- ■ **Reglas.** Las reglas para la puerta de enlace conectan a los escuchas con los grupos de back-end, lo que permite que la puerta de enlace enrute el tráfico que aterriza en un escucha específico a un grupo de back-end utilizando la configuración HTTP especificada.

Aunque cada uno de estos elementos se configura por separado en la puerta de enlace de la aplicación, las reglas unen estos elementos para garantizar que el tráfico se enrute como se espera para un servicio de aplicación.

Las sondas de estado se utilizan para garantizar que los servicios administrados por la puerta de enlace estén en línea. Si hay problemas con uno de los servicios de back-end configurados, la puerta de enlace de

la aplicación elimina el recurso del back-end de la puerta de enlace. Esto asegura que el servicio de back-end que utiliza la puerta de enlace tendrá menos probabilidades de mostrar páginas con errores para los recursos que pueden estar inactivos.

Importante Se necesita al menos un servicio de back-end

Si todos los servicios de back-end no están en buen estado, la puerta de enlace de la aplicación no puede solucionar el problema.

El intervalo en el que se evalúan las sondas de estado, el período de tiempo de espera y el umbral de reintento se pueden configurar para adaptarse a las necesidades de las aplicaciones de back-end, como se muestra en la [Figura 2-52](#).

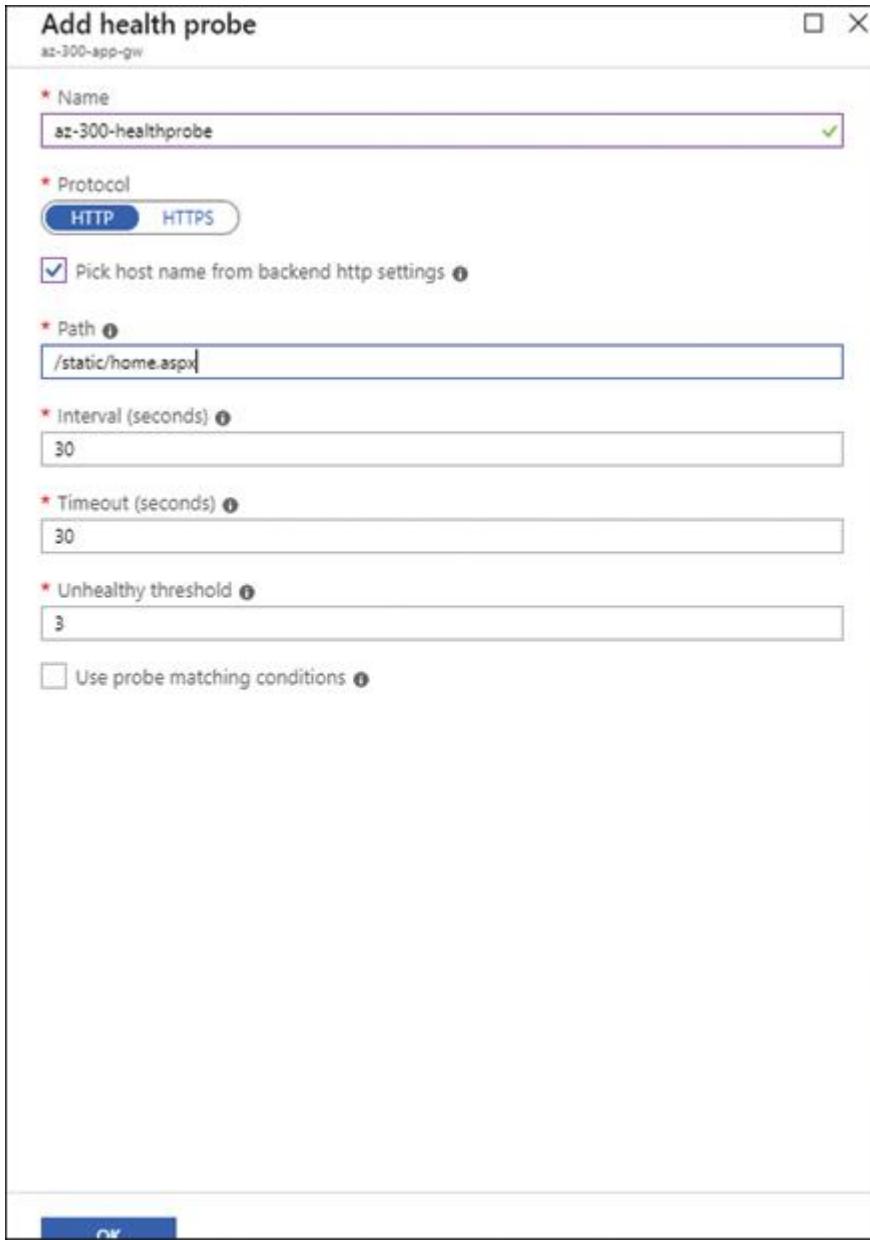


FIGURA 2-52 Configuración de una nueva prueba de salud



Sugerencia de examen Varias opciones disponibles para el equilibrio de carga

Azure admite diferentes tipos de servicios de equilibrio de carga que se pueden usar en conjunto. Asegúrese de comprender cuándo usar una puerta de enlace de aplicaciones y cuándo usar un equilibrador de carga de red.

Implementar configuraciones de IP de front-end

Una puerta de enlace de aplicaciones tiene de forma predeterminada una configuración de front-end que utiliza una dirección IP pública, pero puede configurarla para que utilice una dirección IP privada para el front-end. Esto podría ser útil en unconfiguración de aplicaciones de varios niveles. El uso de una puerta de enlace de aplicaciones para dirigir el tráfico de Internet a una puerta de enlace "interna" que tiene una configuración de front-end privada puede ser una configuración útil en algunos escenarios.

La configuración de direcciones IP virtuales (VIP) ocurre en la configuración de la puerta de enlace de la aplicación en la sección **Configuración de IP de front-end**, que se muestra en la Figura 2-53 .



FIGURA 2-53 La configuración de front-end para una puerta de enlace de aplicaciones

Cuando establece la configuración de front-end, la configuración pública predeterminada incluye un oyente configurado. Cada configuración necesita un escucha que le permita distribuir correctamente el tráfico a los recursos de back-end.

La configuración de la interfaz de usuario privada requiere que se especifique un nombre y una dirección IP privada si el encabezado original se modificará a un valor de IP conocido.

Nota Puede que se requiera tiempo de actualización

Al guardar la configuración en algunas áreas del recurso de la puerta de enlace de la aplicación, el tiempo de actualización puede demorar más de lo esperado.

Administrar el equilibrio de carga de la aplicación

La puerta de enlace de aplicaciones maneja el equilibrio de carga en la capa 7 (la capa de aplicación) del modelo OSI. Esto significa que maneja técnicas de balanceo de carga usando los siguientes métodos:

- **Afinidad basada en cookies.** Esto siempre enrutará el tráfico durante una sesión a la misma aplicación de back-end donde comenzó la sesión. El método basado en cookies funciona bien si hay información basada en el estado que debe mantenerse durante una sesión. Para que las computadoras cliente aprovechen este tipo de equilibrio de carga, el navegador utilizado debe permitir las cookies.

La administración de afinidad basada en cookies se realiza en la hoja **Configuración HTTP / Configuración HTTP de backend** del recurso (consulte la [Figura 2-54](#)).

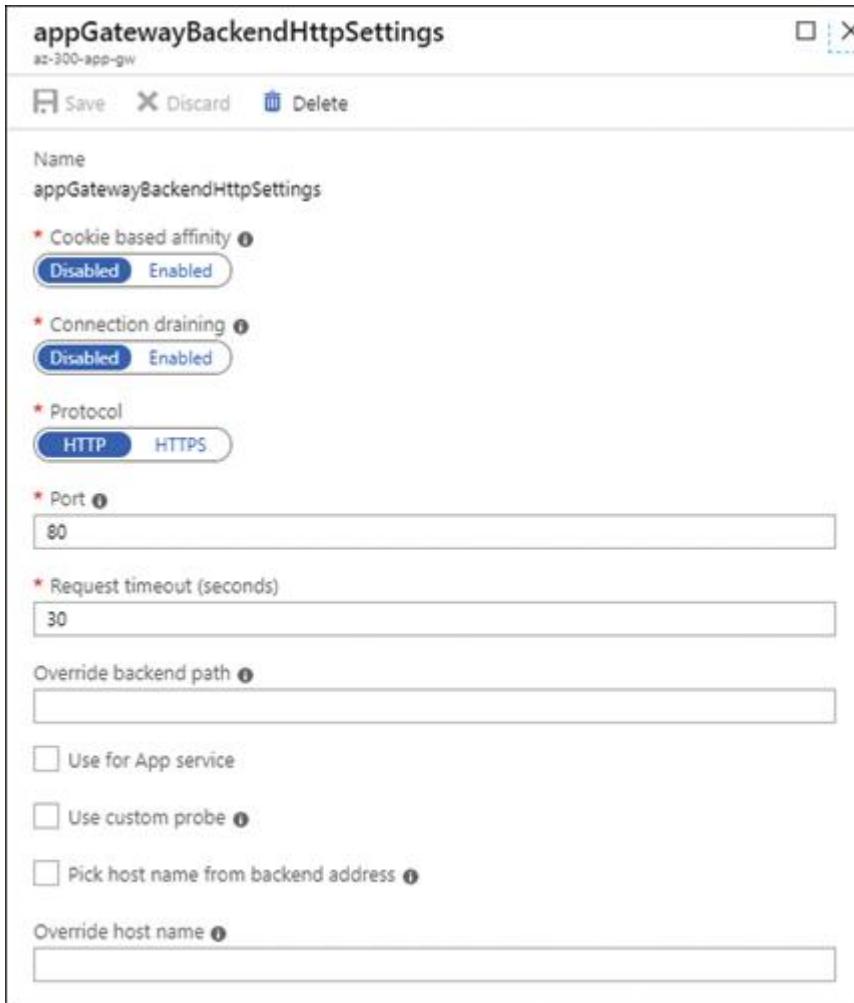


FIGURA 2-54 Configuración de HTTP

- **Conexión de drenaje.** Habilite esta configuración para asegurarse de que todas las conexiones que se enrutan a un recurso se completen antes de que el recurso se elimine de un grupo de back-end. Además, ingrese la cantidad de segundos para esperar a que se agote el tiempo de espera de la conexión.
- **Protocolo.** Configure HTTP o HTTPS aquí. Si elige HTTPS, debe cargar un certificado en la puerta de enlace de la aplicación.

Enrutamiento basado en ruta de URL

El enrutamiento basado en rutas de URL utiliza una configuración denominada mapa de rutas de URL para controlar qué solicitudes entrantes que llegan a la puerta de enlace se envían a qué recursos de

back-end. Hay algunos componentes dentro de Application Gateway necesarios para aprovechar el enrutamiento basado en rutas de URL:

- ■ **Mapa de ruta de URL.** El mapeo de solicitudes a recursos de back-end
- ■ **Escucha de backend.** Especifica la configuración de IP de front-end y el puerto que observarán las reglas de enrutamiento
- ■ **Reglas de enrutamiento.** Las reglas asocian el mapa de ruta de URL y el oyente para garantizar que las solicitudes específicas se enruten al grupo de back-end correcto.

PowerShell es necesario para agregar las configuraciones a una puerta de enlace de aplicaciones para la configuración necesaria para el enrutamiento basado en rutas de URL.



Sugerencia para el examen

Es recomendable aprovechar los ejemplos para ayudar a crear un script de PowerShell que funcione en su entorno. Cuando revise el código proporcionado por otros, asegúrese de consultarla en un editor que admita el lenguaje, como Visual Studio Code, para ayudarlo a comprender lo que hace el código antes de ejecutarlo en su entorno.

Un ejemplo útil del siguiente código se encuentra en <https://docs.microsoft.com/en-us/azure/application-gateway/tutorial-url-route-powershell>:

Haga clic aquí para ver la imagen del código

```
#Configurar grupos de backend de imágenes y videos  
$puerta de enlace = Get-AzApplicationGateway '  
    -ResourceGroupName Az-300-RG-Gateway '  
    -Nombre AppGateway  
  
Add-AzApplicationGatewayBackendAddressPool '  
    -ApplicationGateway $gateway '  
    -Nombre imagesPool
```

```

Add-AzApplicationGatewayBackendAddressPool '
    -ApplicationGateway $ gateway '
    -Nombre videoPool


Add-AzApplicationGatewayFrontendPort '
    -ApplicationGateway $ gateway '
    -Nombre InboundBEPort '
    -Puerto 8080

$ backendPort = Get-AzApplicationGatewayFrontendPort '
    -ApplicationGateway $ gateway '
    -Nombre bport

#configurar un escucha de backend

$ fipconfig = Get-AzApplicationGatewayFrontendIPConfig '
    -ApplicationGateway $ puerta de enlace


Add-AzApplicationGatewayHttpListener '
    -ApplicationGateway $ gateway '
    -Nombre backendListener '
    -Protocolo Http '
    -FrontendIPConfiguration $ fipconfig '
    -FrontendPort $ backendPort

#Configure el mapeo de URL

$ poolSettings = Get-AzApplicationGatewayBackendHttpSettings
'

```

```
-ApplicationGateway $ gateway '  
-Nombre myPoolSettings  
  
  
$ imagePool = Get-AzApplicationGatewayBackendAddressPool '  
-ApplicationGateway $ gateway '  
-Nombre imágenesBackendPool  
  
  
$ videoPool = Get-AzApplicationGatewayBackendAddressPool '  
-ApplicationGateway $ gateway '  
-Nombre videoBackendPool  
  
  
$ defaultPool = Get-AzApplicationGatewayBackendAddressPool '  
-ApplicationGateway $ puerta de enlace  
-Nombre appGatewayBackendPool  
  
  
$ imagePathRule = New-AzApplicationGatewayPathRuleConfig '  
-Nombre imagePathRule '  
-Rutas "/ images / *" '  
-BackendAddressPool $ imagePool '  
-BackendHttpSettings $ poolSettings  
  
  
$ videoPathRule = New-AzApplicationGatewayPathRuleConfig '  
-Name videoPathRule '
```

```
-Rutas "/ video / *" '
-BackendAddressPool $ videoPool '
-BackendHttpSettings $ poolSettings

Add-AzApplicationGatewayUrlPathMapConfig '
-ApplicationGateway $ gateway '
-Nombre urlpathmap '
-PathRules $ imagePathRule, $ videoPathRule '
-DefaultBackendAddressPool $ defaultPool '
-DefaultBackendHttpSettings $ poolSettings

#Añadir la (s) regla (s) de enrutamiento
$ backendlistener = Get-AzApplicationGatewayHttpListener '
-ApplicationGateway $ gateway '
-Nombre backendListener

$ urlPathMap = Get-AzApplicationGatewayUrlPathMapConfig '
-ApplicationGateway $ gateway '
-Nombre urlpathmap

Add-AzApplicationGatewayRequestRoutingRule '
-ApplicationGateway $ gateway '
-Nombre regla2 '
```

```
-RuleType PathBasedRouting  
-HttpListener $ backendlistener  
-UrlPathMap $ urlPathMap
```

#Actualice la puerta de enlace de la aplicación

```
Set-AzApplicationGateway -ApplicationGateway $ gateway
```

Importante Tenga paciencia al actualizar Application Gateway

Una actualización de la puerta de enlace de la aplicación puede tardar hasta 20 minutos.



Consejo para el examen Dedique algo de tiempo a la CLI

Recuerde trabajar con la interfaz de línea de comandos (CLI) de Azure para comprender cómo funcionan los comandos y en qué se diferencian de PowerShell. Aunque PowerShell puede manejar el trabajo de la línea de comandos en Azure, puede haber algunos elementos importantes de la CLI de Azure en el examen, y es bueno saber cómo hacerlo.

Una vez que el mapa de URL está configurado y aplicado a la puerta de enlace, el tráfico se enruta a los grupos de ejemplo (imágenes y videos) a medida que llega. Este no es el equilibrio de carga tradicional en el que el tráfico se enrutaría en función de la carga del dispositivo; un cierto porcentaje del tráfico va al grupo uno y el resto al grupo dos. En este caso, el tipo de contenido ayuda a impulsar el tráfico entrante.

Implementar Azure Load Balancer

Application Gateway incluye capacidades de equilibrio de carga de capa 7 (HTTP o HTTPS) para garantizar un mayor rendimiento de los sitios web o aplicaciones web en los entornos de Azure de una organización. Habrá ocasiones en las que surjan requisitos para una solución de equilibrio de carga de capa 4 más tradicional y Azure Load Balancer lo tiene cubierto.

Note Layer 4 y Layer 7

Las capas mencionadas anteriormente señalan el posicionamiento en el modelo de red OSI. La capa 7 es la capa superior y funciona a nivel de aplicación y navegador. La capa 4 es una capa intermedia que se ocupa del transporte de comunicaciones, el área TCP. Una discusión sobre lo que aportan estas capas está más allá del alcance de este texto. Puede encontrar más información en <https://osimodel.com> .

Azure Load Balancer funciona para manejar TCP y otras comunicaciones basadas en protocolos y garantizar que las solicitudes se manejen de manera adecuada.

Para configurar Azure Load Balancer, complete los siguientes pasos (que se muestran en la figura 2-55):

Create load balancer

Basics Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription *

Resource group *
[Create new](#)

Instance details

Name *

Region *

Type * Internal Public

SKU * Basic Standard

Public IP address

Public IP address * Create new Use existing

Public IP address name *

Public IP address SKU

Assignment * Dynamic Static

Add a public IPv6 address No Yes

Review + create [**< Previous**](#) [**Next : Tags >**](#) [Download a template for automation](#)

FIGURA 2-55 Creación de un equilibrador de carga de Azure

1. Inicie sesión en Azure Portal.
2. Haga clic en **Crear un recurso** y busque **Load Balancer** para comenzar a crear el balanceador de carga.
3. Haga clic en **Crear**.
4. Proporcione los siguientes elementos para crear un balanceador de carga:

1. ■ **Suscripción.** Seleccione la suscripción de Azure para usar con este recurso.
2. ■ **Grupo de recursos.** Seleccione o cree el grupo de recursos para el balanceador de carga.
3. ■ **Nombre.** Ingrese un nombre para el recurso que cumpla con los estándares de nomenclatura de la organización.
4. ■ **Región.** Seleccione la región para el balanceador de carga.
5. ■ **Escriba.** Seleccione el tipo:
 - 1.■ **Interna.** Se utiliza para proporcionar conectividad para máquinas virtuales dentro de su red virtual al VMS de front-end según sea necesario.
 - 2.■ **Público.** Proporciona conexiones salientes para las máquinas virtuales en una red virtual a través de la traducción de direcciones.
6. ■ **SKU.** Seleccione el SKU de precios para el balanceador de carga:
7. ■ **Básico.** Se ofrece sin cargo, pero es limitado y no tiene SLA.
8. ■ **Estándar.** Se utiliza para grandes grupos de objetivos o para funciones adicionales.
9. ■ **Dirección IP pública.** Seleccione una IP pública existente o cree una nueva.
10. ■ **Nombre de la dirección IP pública.** Nombre el recurso de dirección IP pública.
11. ■ **Cesión.** Seleccione el tipo de asignación para la IP pública.
 - 0.■ **Dinámico.** Se asigna cuando el balanceador de carga está en línea y se libera si el balanceador de carga desaparece.
 - 1.■ **Estático.** Asignado de forma permanente para su uso dentro de Azure.
12. ■ **Agregar una dirección pública .** Elija habilitar IPv6 si es necesario.

5. Haga clic en **Siguiente** para agregar etiquetas.
6. Haga clic en **Revisar + Crear** para revisar la configuración y crear el equilibrador de carga.



Etiquetas de consejos de examen y organización

El uso de etiquetas es una buena manera de garantizar que se capture cierta información para los recursos que se están creando. Azure mantiene cierta información en el Registro de actividad, pero estos datos se depuran con regularidad. Si se eliminó la información y necesita ver quién creó un recurso o la fecha en que se agregó, es posible que no tenga suerte. Aquí es donde las etiquetas son útiles y pueden ahorrar mucha frustración con los recursos en Azure. También hay otros usos para ellos, pero este es el uso principal que hemos encontrado para las etiquetas.

Una vez que el equilibrador de carga existe en Azure, necesita alguna configuración para que funcione correctamente en su entorno. Específicamente, es necesario configurar los siguientes elementos:

- ■ **Configuración de IP frontend.** La dirección IP pública y el punto final externo del recurso.
- ■ **Sondas de salud.** Método (s) para garantizar que el back-end esté en buen estado y en línea para que el equilibrador de carga sepa cuándo cambiar el tráfico.
- ■ **Grupos de backend.** Los recursos se equilibran en la carga.
- ■ **Reglas.** Esto expresa cómo se debe enrutar el tráfico a través del balanceador de carga.

La configuración de IP de front-end es la parte más sencilla de un equilibrador de carga simple. La IP se asignó durante la creación de recursos y no requiere más cambios para funcionar correctamente. Se pueden agregar direcciones IP adicionales al balanceador de carga si lo requiere una organización.

Los grupos de back-end son los recursos a los que se dirigen los usuarios y el equilibrador de carga. Aquí es donde se dirigen los que necesitan acceso a las cosas. Una nota sobre las agrupaciones de back-end es que están diseñadas para ser extremadamente similares. Por ejemplo, colocar tres servidores que ejecutan su aplicación detrás de un equilibrador de

carga sería un grupo de backend. Las solicitudes recibidas recibirían el mismo resultado sin importar a qué recurso se dirigieran.

Para configurar un grupo de back-end, complete los siguientes pasos:

1. En el **recurso Load Balancer** en Azure, seleccione **Grupos de backend** en la sección **Configuración** del panel de navegación.
2. Haga clic en **Agregar**.
3. Proporcione el **nombre** de la piscina.
4. Suministrar la **red virtual** que se debe utilizar para los recursos.
5. Seleccione la **versión de IP**. (Generalmente, se utilizará IPv4).
6. Seleccione la asociación para el grupo de back-end:
 1. **Máquina virtual única**
 2. **Conjunto de escala de máquina virtual**
7. Seleccione la máquina virtual (o conjunto de escalas) con la que asociarse.
8. Seleccione la dirección IP del recurso de back-end que se utilizará.
9. Haga clic en **Agregar** para crear el grupo.

Tenga en cuenta las regiones

Al configurar un balanceador de carga, debe existir en la misma región que la red virtual que se usará para su grupo de backend. El acceso a redes virtuales en todas las regiones no funcionará de forma nativa.

Con el front-end configurado y el grupo de back-end en línea, el siguiente elemento en el orden de operaciones son las sondas de salud. Antes de que comencemos a inundar el grupo de back-end con tráfico, los recursos deben estar en buen estado. Para configurar una sonda de salud, complete los siguientes pasos:

1. Seleccione sondas de estado de la lista de configuración en el menú de navegación para el balanceador de carga.
2. Haga clic en **Agregar** para crear una sonda de salud y proporcione lo siguiente:
 1. **Nombre.** El nombre de la sonda de salud.
 2. **Protocolo.** Seleccione el protocolo que debe utilizar la sonda.

3. ■ **Puerto.** Especifique el puerto a vigilar; asegúrese de que el puerto esté abierto o esté escuchando en la máquina virtual.
4. ■ **Intervalo.** El número de segundos entre comprobaciones.
5. ■ **Umbral insalubre.** La cantidad de fallas consecutivas antes de que el grupo se considere insalubre.

3. Haga clic en **Aceptar**.

Con un grupo de back-end saludable listo para funcionar, el último paso es configurar las reglas necesarias para mover el tráfico entre el front-end y el back-end. Según el tipo de equilibrio de carga que realizará, hay dos tipos de reglas que debe tener en cuenta:

- ■ **Reglas de equilibrio de carga.** Esto garantiza que el tráfico se enrute a recursos o grupos en buen estado.
- ■ **Reglas de NAT entrante.** Reenvía el tráfico desde un puerto de origen en el front-end a un puerto de destino en el grupo de back-end.

Complete los siguientes pasos para configurar una regla de equilibrio de carga:

1. Seleccione la hoja **Reglas de equilibrio de carga** en **Configuración** y haga clic en **Agregar**.
2. Proporcione la siguiente información para la regla:
 1. ■ **Nombre.** Un nombre para la regla.
 2. ■ **Versión de IP.** Si la regla debe usarse con IPv4 o IPv6.
 3. ■ **Protocolo.** Seleccione TCP o UDP.
 4. ■ **Puerto.** Especifique el puerto que debe aprovechar la regla.
 5. ■ **Grupo de backend.** Elija un grupo de back-end.
 6. ■ **Sonda de salud.** Elija una sonda de salud.
 7. ■ **Persistencia de la sesión.** Esto ayuda a garantizar que el servidor al que se conectó mantendrá su sesión durante toda su duración.

8. ■ **Tiempo de espera inactivo.** Especifique la cantidad de minutos que debe esperar antes de que se agote el tiempo.

9. ■ **IP flotante (retorno directo del servidor).** Seleccione si se debe utilizar una IP flotante. A menos que esté configurando SQL AlwaysOn u otros recursos sensibles, una IP flotante no es necesaria.

3. Haga clic en **Aceptar**.

Complete los siguientes pasos para configurar una regla de NAT entrante:

1. En la sección **Configuración** del panel de navegación, seleccione **Reglas NAT entrantes**.

2. Haga clic en **Agregar**.

3. Proporcione la siguiente información:

1. ■ **Nombre.** Un nombre para la regla NAT.

2. ■ **Dirección IP de la interfaz.** Seleccione la interfaz del equilibrador de carga que se utilizará.

3. ■ **Servicio.** El servicio que se utilizará con NAT.

4. ■ **Protocolo.** El protocolo del servicio (**TCP** o **UDP**).

5. ■ **Tiempo de espera inactivo.** La cantidad de minutos que la sesión debe permanecer inactiva.

6. ■ **Configuración de IP de red.** Seleccione el recurso que se utilizará con NAT.

7. ■ **Mapeo de puertos.** Elija usar el puerto predeterminado o un puerto personalizado con NAT.

4. Haga clic en **Aceptar**.

Con el balanceador de carga configurado, acceder a los recursos permitidos usando la dirección IP del balanceador de carga funciona de la misma manera que usando la dirección IP del propio recurso. Esto permite que cualquier dirección IP pública adjunta directamente se elimine de los recursos en un grupo de back-end. Antes de realizar este paso, asegúrese de que todo lo que utilice esas direcciones IP se haya trasladado a la IP del equilibrador de carga.

Nota sobre el uso de puertos específicos

El uso de reglas de NAT de entrada puede ayudar a garantizar que los puertos conocidos para determinadas cargas de trabajo no estén expuestos a Internet. Por ejemplo, puede configurar un puerto de front-end 2020 para enviar tráfico 3389 en su red interna para ocultar dónde está sucediendo RDP. Tenga en cuenta que 2020 fue solo un número de puerto aleatorio seleccionado como ejemplo.

El balanceador de carga configurado para este texto era un balanceador de carga básico. Visite la documentación de precios de Azure para el recurso Load Balancer para obtener más información sobre los SLA y las características adicionales proporcionadas por otras SKU del equilibrador de carga. Consulte <https://azure.microsoft.com/en-us/pricing/details/load-balancer/>.

Configurar y administrar Azure Firewall

Azure Firewall es un servicio de firewall de próxima generación con estado que se puede configurar en una red virtual. Cuando Azure Firewall está habilitado, el modo predeterminado es denegar el tráfico a los recursos en la misma red virtual. Solo después de que se configuren las reglas se permitirá el acceso a los recursos. Tenga esto en cuenta si agrega Azure Firewall a una red virtual existente.

Para que Azure Firewall se ejecute en una red virtual, complete los siguientes pasos:

1. Inicie sesión en Azure Portal y busque el recurso de red virtual al que se agregaría Azure Firewall.
2. Con la red virtual seleccionada, elija **Firewall** en **Configuración**.
3. Haga clic en el enlace Haga **clic aquí** para agregar un nuevo firewall para agregar un nuevo firewall y proporcionar la siguiente información:
 1. ■ **Suscripción.** Esta debe ser la misma suscripción que contiene la red virtual seleccionada anteriormente.
 2. ■ **Grupo de recursos.** El grupo de recursos debe ser el grupo de recursos predeterminado para la red virtual.
 3. ■ **Nombre.** El nombre de la instancia de Azure Firewall.
 4. ■ **Región.** La región de la instancia de Azure Firewall, que también debe coincidir con la región de la red virtual.

5. ■ **Elija una red virtual.** Cree o seleccione una red virtual existente.
 6. ■ **Nombre de la red virtual.** El nombre de una nueva red virtual si eligió crear una.
 7. ■ **Espacio de direcciones.** El espacio de direcciones de la nueva red virtual.
 8. ■ **Subred.** Esto se completará como `AzureFirewallSubnet` y no se puede cambiar. Si elige una red virtual existente, esta subred deberá existir antes de crear la instancia de firewall de Azure.
 9. ■ **Espacio de direcciones de subred.** El rango de direcciones IP para `AzureFirewallSubnet`.
 10. ■ **Dirección IP pública del cortafuegos.** La dirección IP pública (requerida) para usar con Azure Firewall.
 11. ■ **Túneles forzados (vista previa).** Esta función obligará a que todo el tráfico fluya a través del cortafuegos; está en vista previa en el momento de escribir este artículo.
4. Haga clic en **Revisar + crear** para revisar la configuración seleccionada.
 5. Haga clic en **Crear** para implementar Azure Firewall.

Nota Configuración adicional de túnel forzado

Si elige habilitar el túnel forzado, se requerirá una dirección IP de administración (pública) para garantizar que siempre se pueda acceder al firewall para la configuración y para garantizar que el tráfico de administración se maneje por separado del tráfico que pasa y se ve afectado por el firewall.



Plantillas integradas de consejos de examen

A medida que trabaje en la creación de estos recursos, se crearán plantillas en segundo plano para la implementación basada en ARM. La descarga de las plantillas para su revisión lo ayudará a mejorar su comprensión de las plantillas y lo preparará para la automatización de la implementación de recursos en Azure. Además, no creará ni intentará crear plantillas ARM desde cero.

Una vez que se haya completado la implementación, se necesitará una configuración adicional para garantizar que los recursos detrás del

firewall estén disponibles. De forma predeterminada, no se podrá acceder a nada detrás del firewall hasta que existan reglas que lo permitan.

Configuración de reglas para Azure Firewall

Para configurar reglas para Azure Firewall, complete los siguientes pasos:

1. En la hoja de recursos de **Azure Firewall**, seleccione **Reglas** en la sección **Configuración** del panel de navegación que se muestra en la Figura 2-56.

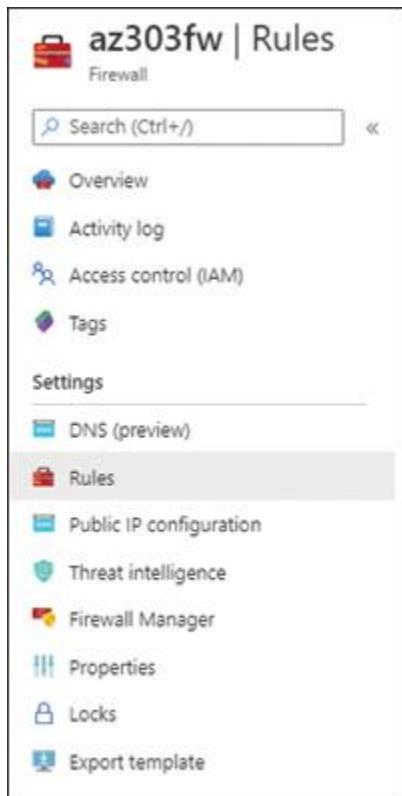


FIGURA 2-56 Configuración o adición de reglas a Azure Firewall

2. Seleccione uno de los siguientes tipos de reglas para configurar:
 1. ■ **Colección de reglas NAT.** Se trata de una colección de reglas que se utilizan para compartir una única dirección IP entrante con muchos recursos internos, según el puerto elegido. Microsoft podría referirse a esto como traducción de Azure de red de destino (DNAT).
 2. ■ **Colección de reglas de red.** Esta es una colección de reglas de salida para permitir la conexión a recursos externos según la dirección IP y / o el puerto.

3. ■ **Colección de reglas de aplicación.** Se trata de una colección de reglas de salida destinadas a apuntar a recursos FQDN externos, como google.com, y permitir o denegar el tráfico hacia los objetivos especificados según el puerto y el FQDN.



Las reglas de consejos de examen tienen orden de procesamiento
Cuando se utilizan, las reglas de red se procesan en orden de prioridad asignada. Si no se encuentran coincidencias para la solicitud de salida, se comprueban las reglas de la aplicación en busca de coincidencias. Una vez que se encuentra una coincidencia, no se intenta procesar más reglas.

3. Haga clic en **Agregar regla NAT** y proporcione la siguiente información:

1. ■ **Nombre.** El primer nombre es para la colección de reglas; Se pueden agregar tipos similares de reglas a la misma colección.
2. ■ **Prioridad.** Ésta es la prioridad de la colección; manténgalos adecuadamente espaciados si está utilizando más de un tipo de colección de reglas para dejar espacio para la expansión de reglas.
3. ■ **Nombre.** Este es el nombre de la regla individual que se está configurando (por ejemplo, RDP).
4. ■ **Protocolo.** Seleccione **TCP** o **UDP** (o ambos) para la regla.
5. ■ **Tipo de fuente.** Seleccione **Dirección IP** para una única dirección de origen o **Grupo de direcciones IP** para un grupo de direcciones de origen con equilibrio de carga.
6. ■ **Fuente.** Ingrese la dirección IP (o * para cualquiera) si el tipo de fuente es una dirección IP, o seleccione el grupo de direcciones IP con nombre si el tipo de fuente es un grupo de direcciones IP.
7. ■ **Dirección de destino.** Para una regla de NAT, debe ser la dirección IP pública del recurso de firewall de Azure.

8. ■ **Puertos de destino.** Los puertos de red esperados en el exterior del firewall, si se usa ofuscación; aquí es donde se debe utilizar el número de puerto personalizado.
 9. ■ **Dirección traducida.** Esta es la dirección IP interna del recurso al que apunta la regla; esta dirección debe estar dentro de la red virtual donde está configurado el firewall.
 10. ■ **Puerto traducido.** Este es el puerto de destino para el servicio utilizado por la regla; por ejemplo, RDP usa el puerto 3389.
4. Repita esta información para agregar reglas adicionales a la colección.
5. Haga clic en **Agregar**.
6. Haga clic en la pestaña **Colección** de reglas de red para crear reglas de red.
7. Proporcione la siguiente información para una colección de reglas de red:
- 0.■ **Nombre.** El nombre de la colección de reglas.
 - 1.■ **Prioridad.** La prioridad para la evaluación.
 - 2.■ **Acción.** Elija **Permitir** o **Denegar**.
 - 3.■ **Nombre.** El nombre de la regla.
 - 4.■ **Protocolo.** Seleccione **TCP**, **UDP** o ambos.
 - 5.■ **Tipo de fuente.** Una dirección IP o un grupo de direcciones IP.
 - 6.■ **Fuente.** Ingrese una dirección IP (* para cualquiera) o seleccione un grupo de direcciones IP.
 - 7.■ **Tipo de destino.** Una dirección IP o un grupo de direcciones IP.
 - 8.■ **Dirección de destino.** Ingrese una dirección IP (* para cualquiera) o seleccione un grupo de direcciones IP.
 - 9.■ **Puertos de destino.** Especifique el puerto que debe coincidir para que se aplique la regla.

Las etiquetas de servicio también se pueden configurar en conjuntos de reglas de red; se utilizan para indicar los servicios designados de Azure como el destino de la regla de red; se configuran como reglas individuales dentro de un conjunto de reglas.

1. Haga clic en **Agregar** para crear las reglas y el conjunto de reglas.
2. Para crear una colección de reglas de aplicación, proporcione la siguiente información:
 1. ■ **Nombre.** El nombre de la colección de reglas de la aplicación.
 2. ■ **Prioridad.** La prioridad de la colección de reglas.
 3. ■ **Acción.** Elija **Permitir** o **Denegar**.
 4. ■ **Etiquetas FQDN.** Estos permiten el acceso saliente a servicios basados en Azure, como Windows Update:
 - 1.■ **Nombre.** El nombre de la regla de etiqueta FQDN.
 - 2.■ **Tipo de fuente.** Dirección IP o un grupo de direcciones IP.
 - 3.■ **Fuente.** Ingrese la dirección IP (ingrese * para cualquiera) o seleccione grupos de direcciones IP.
 - 4.■ **Etiquetas FQDN.** Seleccione los servicios a los que se debe aplicar esta regla.
 5. ■ FQDN de destino. Nombres de dominio externos que deben permitirse (o denegarse) de esta colección de reglas.
 0. ■ **Nombre.** El nombre de la regla.
 1. ■ **Tipo de fuente.** Dirección IP o un grupo de direcciones IP.
 2. ■ **Fuente.** Ingrese la dirección IP (ingrese * para cualquiera) o seleccione grupos de direcciones IP.
 3. ■ **Protocolo: puerto.** Especifique un protocolo o protocolo conocido y un número de puerto para permitir el acceso saliente.

4. ■ **FQDN de destino.** especifique una lista de FQDN separados por comas a los que permitir el acceso saliente.

3. Haga clic en **Agregar** para crear las reglas y colecciones de firewall.

Con las reglas configuradas, el tráfico comenzará a fluir a través de Azure Firewall (si está permitido). Sin reglas, la acción predeterminada de Azure Firewall es denegar cualquier solicitud.

Una vez que se ha configurado un firewall, puede tener sentido bloquear el recurso para que no se pueda eliminar por accidente. En la hoja **Descripción general** del recurso de firewall, haga clic en la opción **Bloquear** para bloquear el recurso. Una vez habilitado, hacer clic en la opción **Desbloquear** eliminará el bloqueo de una instancia de Azure Firewall.

Configurar la inteligencia de amenazas

Microsoft realiza constantemente ataques de red y otras amenazas en Azure y otras propiedades que administra. Estos datos se agregan para permitir que los clientes trabajen con los datos recopilados y administrados por Microsoft. Tenga en cuenta que esto no significa que su entorno esté expuesto a ninguno de estos ataques o amenazas; en cambio, significa que cuando se configura, la inteligencia de amenazas puede prevenirlas.

Los datos de telemetría de toda esta agregación están disponibles dentro de Azure Firewall para permitir que los elementos sean alertados o que los elementos sean alertados y rechazados por una instancia de Azure Firewall.

Para configurar la inteligencia sobre amenazas, elija una de las siguientes opciones de la hoja **Configuración de inteligencia sobre amenazas** :

- ■ **Apagado.** Desactive la inteligencia sobre amenazas.
- ■ **Solo alerta (predeterminado).** Reciba alertas de alta confianza para el tráfico enrutado a través de una instancia de Azure Firewall en su entorno que va hacia o desde direcciones IP o dominios maliciosos conocidos.
- ■ **Alerta y denegación.** Además de alertar sobre estos eventos, se bloqueará el tráfico de esta naturaleza.

Azure Firewall Manager (versión preliminar)

Microsoft ha introducido un servicio de administración de firewall basado en políticas para Azure Firewall, que se encuentra en versión preliminar en el momento de escribir este artículo. Este servicio permitirá compartir reglas y configuraciones entre varias instancias de Azure Firewall. Esta característica no se trata en detalle porque está en vista previa.

Configurar y administrar Azure Front Door

Azure Front Door reúne la supervisión, la administración y el enrutamiento del tráfico HTTP y HTTPS entrante a un entorno al permitir que los usuarios se conecten a los puntos de presencia (POP) más cercanos a su ubicación para aprovechar las configuraciones de red y backplane de Azure para brindar la mejor experiencia y acceso a las aplicaciones de su organización.

Piense en Front Door como el servicio que combina el equilibrio de carga, Traffic Manager y la puerta de enlace de aplicaciones en una única oferta para los clientes que desean aprovecharla.

Para comenzar con Azure Front Door, complete los siguientes pasos:

1. Inicie sesión en Azure Portal (<https://portal.azure.com>).
2. Seleccione **Crear un recurso** en el menú de navegación de Azure.
3. En el cuadro de texto **Search The Marketplace** , ingrese **Front Door** para ubicar Azure Front Door.
4. Haga clic en **Crear** .
5. Proporcione la siguiente información para la configuración:
 1. ■ **Suscripción.** Seleccione la suscripción que albergará su implementación de Azure Front Door.
 2. ■ **Grupo de recursos.** Cree o seleccione un grupo de recursos existente para albergar su implementación de Azure Front Door.
6. Haga clic en **Siguiente: Configuración** .
7. Complete el asistente de configuración, como se muestra en la [Figura 2-57](#) .

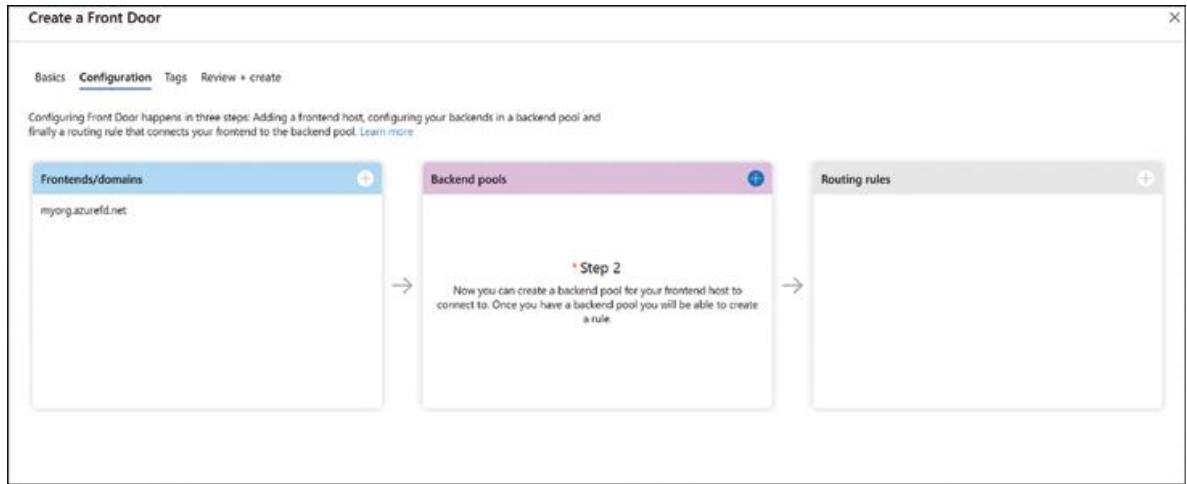


FIGURA 2-57 Configuración de Azure Front Door

- 0.■ Configurar frontends / dominios.
1. ■ Ingrese el nombre de host.
2. ■ Seleccione para habilitar o deshabilitar la afinidad de sesiones.
3. ■ Seleccione para habilitar o deshabilitar el firewall de la aplicación web.
4. ■ Haga clic en **Agregar** .
 - 1.■ Configurar grupos de back-end.
 0. ■ Ingrese un nombre para el grupo de back-end.
 1. ■ Haga clic en **Agregar un backend** para configurar un host dentro del grupo de backend.
 2. ■ Especifique una ruta para la sonda de estado para este grupo de back-end. Considere una aplicación o página estática para asegurarse de que la ruta no cambie.
 3. ■ Especifique el protocolo: **HTTP o HTTPS** .
 4. ■ Especifique el método de sondeo para el sondeo de salud (**Head o Get**).
 5. ■ Defina el intervalo en segundos para la frecuencia del sondeo.
 6. ■ Especifique un tamaño de muestra de equilibrio de carga.

7. ■ Especifique las muestras exitosas requeridas.
 8. ■ Especifique la sensibilidad a la latencia.
8. Haga clic en **Agregar**.
- 0.■ Definir las reglas de enrutamiento para determinar qué tráfico se distribuye a qué grupo de back-end.
 0. ■ Especifique un nombre para la regla.
 1. ■ Seleccione el protocolo que se aceptará.
 2. ■ Especifique los dominios frontales (configurados previamente).
 3. ■ Especifique patrones para que coincidan. Esto determinará qué tráfico es enruteado por esta regla.
 4. ■ Seleccione un tipo de ruta para la regla (**Reenviar** o **Redirigir**).
 5. ■ Seleccione el grupo de back-end al que pasar el tráfico.
 6. ■ Seleccione el protocolo de reenvío (**HTTPS**, **HTTP** o **Solicitud de coincidencia**).
 7. ■ Seleccione para habilitar o deshabilitar la reescritura de URL.
 8. ■ Seleccione para habilitar o deshabilitar el almacenamiento en caché.

9. Haga clic en **Agregar**.

- 0.■ Haga clic en **Revisar + Crear** .
- 1.■ Haga clic en **Crear** para implementar Azure Front Door .

Una vez que Front Door esté en línea y en funcionamiento, puede ver el diseñador de Front Door para agregar interfaces, back-end y reglas de enrutamiento adicionales. Esto seguirá el mismo proceso descrito anteriormente.

Además de estas opciones de configuración, puede habilitar y configurar las opciones de Firewall de aplicaciones web para Front Door por separado.

Dentro del recurso Azure Front Door, seleccione **Web Application Firewall** y luego seleccione la interfaz configurada a la que desea asignar una política. Las políticas son específicas de las configuraciones de front-end, por lo que pueden ser diferentes para cada front-end configurado.

Las políticas de firewall de aplicaciones web son entidades independientes de Front Door y deben existir dentro de la suscripción donde se implementa Front Door. En la barra de búsqueda en la parte superior de Azure Portal, busque **Web Application Firewall** para ver las políticas de Web Application Firewall (WAF), que se muestran en la Figura 2-58.

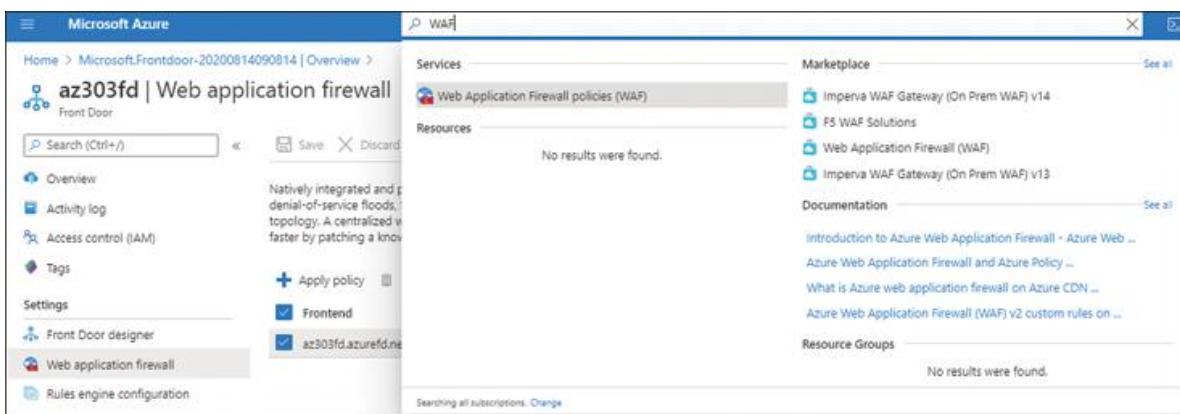


FIGURA 2-58 Adición de elementos de política de firewall de aplicaciones web

Nota ¿Por qué crear políticas WAF?

Front Door admite políticas para permitir la gestión centralizada de los ajustes de configuración de un entorno. Estos pueden personalizarse y crearse para seguir la política de seguridad de una organización (que debe crearse) y / o pueden usar políticas de Azure creadas previamente, que tienen en cuenta las cosas que se han detectado y han ocurrido en la nube de Azure. El uso de elementos de ambos le permitirá ajustar las políticas y reducir la cantidad de cosas que se deben considerar / incluir dentro de la política personalizada.

Para crear una política WAF personalizada, complete los siguientes pasos:

1. Proporcione detalles del proyecto sobre lo que cubrirá esta póliza.
2. Seleccione dónde se aplicará la política:

- WAF global (puerta de entrada de Azure)
- WAF regional (puerta de enlace de aplicaciones)
- Azure CDN (versión preliminar en el momento de escribir este artículo)
 - Seleccione una suscripción y un grupo de recursos para la política.
 - Proporcione un nombre de instancia para la política y elija si la política está habilitada o deshabilitada.

Nota Consideración de configuración

Recomendamos comenzar con las políticas deshabilitadas para garantizar que todas las opciones necesarias estén configuradas y documentadas según lo requiera su organización antes de habilitarlas. Habilitar esta configuración podría hacer que se rechace el tráfico a su entorno.

- Haga clic en **Siguiente: Configuración de la política** para definir lo siguiente sobre la política.
 - Modo.** Seleccione si la política evitirá (bloqueará) el tráfico o solo detectará (auditará).
 - Redirigir URL.** Esta es la URL que se utiliza para redirigir las solicitudes si está configurada.
 - Código de estado de respuesta de bloque.** Este es el código de error que se devuelve cuando se bloquea una solicitud.
 - Cuerpo de estado de respuesta de bloque.** El mensaje para volver al navegador cuando se bloquea una solicitud.
- Haga clic en **Siguiente: Reglas administradas** para configurar los elementos administrados por Azure.
 - Seleccione el conjunto de reglas administradas para aplicar o elija **Ninguno** para omitir las reglas administradas.
- Haga clic en **Siguiente: Reglas personalizadas** para agregar reglas específicas para una organización.
 - Haga clic en **Agregar regla personalizada**.

1.■ Proporcione la siguiente información para configurar una regla personalizada:

- 1.■ **Nombre de la regla.** El nombre de la regla.
- 2.■ **Estado.** Habilitado o deshabilitado.
- 3.■ **Tipo de regla.** Seleccione Coincidir para hacer coincidir patrones específicos o Límite de frecuencia para activar la regla en función de las solicitudes entrantes.
- 4.■ **Prioridad.** Especifique la prioridad de la regla, los números más bajos procesan primero.

8. Configure las condiciones para la regla:

- 0.■ Especifique un tipo de coincidencia y valores con los que comparar.
- 1.■ Especifique la condición entonces. Esto especifica qué hacer cuando se encuentra una coincidencia para las condiciones: **Permitir** , **Denegar** , **Registrar** o **Redirigir** .
- 2.■ Cuando se hayan agregado todas las condiciones necesarias para una regla, haga clic en **Agregar** .

9. Haga clic en **Siguiente: Asociación** para asociar esta política con un entorno.

- 0.■ Haga clic en **Agregar un host de front-end** .
- 1.■ Seleccione la instancia de Front Door y luego elija de la lista de hosts de front-end configurados para asociar la política.
- 2.■ Haga clic en **Revisar + Crear** para continuar.
- 3.■ Haga clic en **Crear** para crear la política configurada y asignarla.

Nota Simple, personalizado y preconfigurado con Azure

Al definir la política, es una buena idea configurar una política que contenga solo reglas preconfiguradas de Azure y otra que contenga solo reglas personalizadas. De esta manera, cuando los esté administrando más tarde, solo se debe administrar un conjunto de elementos a la vez. Esto también significa que no tendrá que

atravesar una combinación de reglas personalizadas y reglas proporcionadas por Azure.

- Como cualquier otro firewall o configuración de reglas, mantener las reglas dentro de una política que contenga elementos relacionados es una buena idea para la política WAF. Se pueden crear más políticas para generar más reglas, pero mantener juntas las reglas para ciertos tipos de tráfico puede facilitar la resolución de problemas.
- Recuerde: Azure Front Door es una ventanilla única para aplicaciones y recursos dentro de un entorno, y la aplicación de políticas individuales a las configuraciones de front-end dentro de Front Door elimina la necesidad de configurar varias instancias del servicio Front Door.



Sugerencias sobre revisiones periódicas de políticas

Al aprovechar servicios como Azure Front Door, es una buena idea revisar periódicamente la configuración del servicio, específicamente las políticas y reglas asociadas, para asegurarse de que aún se apliquen a su organización y que sigan brindando el resultado deseado. Si no es así, debe ajustarlos en consecuencia.

Implementar Azure Traffic Manager

Azure Traffic Manager es un equilibrador de carga de DNS que permite enviar tráfico basado en DNS a hosts configurados para garantizar que no se sobrecarguen hosts específicos. De manera similar a la forma en que un equilibrador de carga tradicional garantiza que el tráfico que va a la dirección IP 1.2.3.4 se distribuya uniformemente en un grupo de recursos, Traffic Manager hace lo mismo con el tráfico basado en DNS. También es posible equilibrar el tráfico en las regiones de Azure mediante los perfiles de Traffic Manager, lo que puede convertirlo en un componente clave de una solución de conmutación por error de servicio, lo que elimina la necesidad de actualizar los registros DNS durante un escenario de conmutación por error.

Para configurar Azure Traffic Manager, complete los siguientes pasos:

1. Inicie sesión en Azure Portal (<https://portal.azure.com>).
2. En el panel de navegación, seleccione **Crear un recurso**.

3. Busque **Perfil de Traffic Manager** y haga clic en **Crear**.
4. Proporcione la siguiente información para configurar un perfil de Traffic Manager:
 1. ■ **Nombre.** Este es el nombre del recurso, que obtendrá un nombre DNS de Azure de <name>.trafficmanager.net.
 2. ■ **Método de enrutamiento.** Elija el método para enrutar el tráfico:
 - 1.■ **Rendimiento.** Utilice esta ruta cuando los recursos estén dispersos geográficamente y desee enviar al usuario al punto final más cercano a su ubicación.
 - 2.■ **ponderado.** Úselo para distribuir el tráfico entre los nodos de manera uniforme o según el peso que especifique.
 - 3.■ **Prioridad.** Utilice esto para seleccionar un punto final como principal y especificar recursos adicionales como copias de seguridad.
 - 4.■ **Geográfico.** Utilice este enrutamiento para enviar usuarios específicos a una ubicación geográfica definida según el origen de la consulta de DNS.
 - 5.■ **MultiValue.** Use esto para perfiles donde solo las direcciones IPv4 o IPv6 pueden ser puntos finales. Cuando se consulta, se devolverán todos los valores.
 3. ■ **Subred.** Utilice esto para asignar conjuntos de rangos de direcciones IP de usuario a un punto final de Traffic Manager específico.
 4. ■ **Suscripción.** Seleccione la suscripción que albergará el perfil de Traffic Manager.
 5. ■ **Grupo de recursos.** Seleccione o cree el grupo de recursos que albergará el perfil de Traffic Manager.
 6. ■ **Ubicación del grupo de recursos.** Seleccione la región donde se ubicará el grupo de recursos.
 7. ■ Haga clic en **Crear**.

La configuración de Traffic Manager coloca el recurso en una región de Azure inicialmente. Sin embargo, Traffic Manager es un recurso global que existe en todas las regiones y no solo opera en centros de datos específicos.

Después de la configuración e implementación inicial, Traffic Manager estará habilitado y listo para su uso, pero no contiene ningún punto final de fábrica. Esto significa que cualquier cosa que se envíe al Traffic Manager no tiene adónde ir. Esto deberá configurarse proporcionando puntos finales al servicio. Para hacer esto, complete lo siguiente:

1. Desde el recurso Traffic Manager, seleccione **Endpoints** en el área **Configuración** del panel de navegación.
2. Haga clic en **Agregar** para agregar un punto final y proporcionar la siguiente información:
 1. **Escriba.** El tipo de recurso de este punto final es:
 1. **Azure Endpoint.** Un recurso que se ejecuta en Azure.
 2. **Punto final externo.** Un recurso que se ejecuta en otra nube o en un centro de datos corporativo.
 3. **Extremo anidado.** Aprovecha otra instancia de Traffic Manager como punto final.
 2. **Nombre.** El nombre del punto final.
 3. **Tipo de recurso de destino.** El tipo de servicio al que apunta este punto final:
 0. **Servicio en la nube.** Servicios en la nube PaaS que se ejecutan en Azure.
 1. **Servicio de aplicaciones.** Aplicaciones web que se ejecutan en Azure.
 2. **Ranura del servicio de aplicaciones.** Ranuras específicas de aplicaciones web que se ejecutan en Azure.
 3. **Dirección IP pública.** Especifique un equilibrador de carga o el nombre DNS de una

dirección IP vinculada a una máquina virtual que se ejecuta en Azure.

4. ■ **Recurso objetivo.** Si el punto de conexión es un punto de conexión de Azure, el destino se puede seleccionar de una lista de recursos disponibles.
5. ■ **Configuración de encabezado personalizado.** Información de encabezado que el objetivo podría estar esperando.
6. ■ **Agregar como deshabilitado.** Si se marca esta opción, el punto final no estará disponible para recibir tráfico tan pronto como se implemente.

3. Haga clic en **Aceptar** para agregar el punto final.

Capas de *notas* y capas de tráfico

Una nueva adición a los puntos finales de Traffic Manager es el punto final anidado. Esto permite que un administrador de tráfico haga referencia a otra instancia como un punto final al que puede enrutar el tráfico. Por ejemplo, es posible que una aplicación ubicada detrás de DNS en www.contoso.com deba enviar tráfico a apac.contoso.com, y es posible que este sitio deba equilibrarse la carga entre dos puntos de conexión específicos de Asia Pacífico. Con un punto final anidado, esto es fácil de configurar.

Configurar ajustes adicionales

Además de los puntos finales, Traffic Manager debe configurarse para garantizar que los puntos finales se supervisen correctamente. Sin configurar el monitoreo para Traffic Manager, o al menos sin revisarlo para asegurarse de que se implementen las configuraciones correctas, esto podría afectar el uso del endpoint. Si Traffic Manager no puede monitorear o alcanzar un punto final, se marcará como inactivo y no disponible para su uso.

Los siguientes elementos están disponibles dentro de los ajustes de configuración de Traffic Manager:

- ■ **Método de enrutamiento.** Seleccione el método de enrutamiento utilizado por Traffic Manager en general.

- **Tiempo de vida de DNS (TTL).** La cantidad de segundos que el cliente debe almacenar en caché un registro antes de volver a consultar Traffic Manager para obtener información actualizada.
- **Configuración del monitor de punto final:**
 - **Protocolo.** ¿Deben monitorearse los puntos finales a través de HTTP, HTTPS o TCP?
 - **Puerto.** El puerto utilizado para la monitorización.
 - **Ruta.** La ruta en el punto final que se usa para el monitoreo. Si hay una página de estado que debe usarse en lugar de la ruta raíz, ingrese la ruta relativa aquí.
- **Configuración de encabezado personalizada.** Cualquier información de encabezado personalizada que deba aplicarse a todos los puntos finales.
- **Código de estado esperado.** Configure los rangos de códigos de estado que se deben considerar durante la evaluación de un punto final. Por ejemplo, se puede configurar un rango de código de estado si un punto final no regresa 200 como un mensaje de éxito o si espera que el punto final esté inactivo en lugar de activo.
- **Intervalo de palpado.** Con qué frecuencia se debe verificar un punto final.
- **Número tolerado de fallas.** Cuántas fallas consecutivas están bien antes de que un punto final se considere inactivo.
- **Tiempo de espera de la sonda.** Número de segundos antes de que se agote el tiempo de espera de una sonda al comprobar un punto final.

Traffic Manager tiene dos opciones de monitoreo de tráfico fuera de las opciones de monitoreo de punto final que se usan para enrutar el tráfico que pueden ser útiles para ver cómo va el movimiento del tráfico: mediciones de usuarios reales y vista del tráfico.

Medidas reales de usuario

Para habilitar las mediciones de usuarios reales, seleccione el elemento **Mediciones de usuarios reales** de la sección de

configuración del panel de navegación dentro del recurso del administrador de tráfico, luego haga clic en el botón **Generar clave** e incluya la clave en su aplicación, al igual que una clave de instrumentación en Application Insights. Una vez configuradas, las medidas de latencia entre un explorador de cliente y Azure Traffic Manager ayudan a controlar la latencia experimentada por el usuario.

Vista de tráfico

Cuando se configura la vista de tráfico, puede recopilar datos sobre la latencia de las conexiones de los usuarios a los puntos finales detrás de Traffic Manager. Seleccione el elemento **Vista de tráfico** de la sección de configuración del panel de navegación dentro del recurso del administrador de tráfico, luego haga clic en **Habilitar Vista de tráfico** para activarlo. La habilitación inicial puede tardar hasta 24 horas en completar el mapa de calor y mostrar datos sobre las conexiones de los usuarios.

Nota se aplica a todas las instancias

Cuando se crea la clave de medidas de usuario real, se aplica a todas las instancias de Traffic Manager dentro de una suscripción, no solo a la instancia donde se hizo clic en el botón Generar clave.

Administrar y configurar grupos de seguridad de aplicaciones y redes

La seguridad en la nube es algo que debe tenerse en cuenta en cada paso del proceso. Microsoft aprovecha los grupos de seguridad de red (NSG) para proporcionar un método para permitir y denegar el tráfico destinado a los recursos de Azure. Los grupos de seguridad de aplicaciones llevan esto un paso más allá al permitir que una agrupación de recursos similares sea el objetivo de las reglas de NSG. El uso de estos recursos puede simplificar la seguridad y aprovechar la tecnología nativa de la nube que crecerá a medida que Azure continúe evolucionando.

Grupos de seguridad de red

Los grupos de seguridad de red son muy parecidos a las listas de control de acceso (ACL) utilizadas en los primeros dispositivos de

firewall. Permiten el tráfico a través de un recurso o segmento de red específico a través de un puerto o conjunto de puertos específico. En un nivel alto, los grupos de seguridad de red proporcionan un método de control permitido / denegado para el tráfico que entra o sale de los recursos a los que se aplican.

Para agregar un grupo de seguridad de red para una máquina virtual, complete los siguientes pasos:

1. Inicie sesión en Azure Portal (<https://portal.azure.com>).
2. Navegue hasta el grupo de recursos que contiene la máquina virtual que cubrirá el NSG.
3. Seleccione el botón **Agregar** en la parte superior de la página **Grupo de recursos** y busque y seleccione **Grupo de seguridad de red**. Haga clic en **Crear** para comenzar a crear el recurso.
4. Especifique la **suscripción** y el **grupo de recursos** que albergará el NSG.
5. Proporcione el **nombre** del NSG.
6. Elija la **región** para el recurso.
7. Haga clic en **Siguiente: Etiquetas** .
8. Especifique las etiquetas utilizadas por su organización agregando el nombre de la etiqueta y su valor en los campos correspondientes. Si ha utilizado una etiqueta anteriormente, su nombre y valor se podrán seleccionar una vez que ingrese a cada campo. Esto limita la necesidad de mantener una lista de etiquetas usadas fuera de Azure.

Nota solo texto

Las etiquetas son solo texto. Si el plan es crear una etiqueta para el nombre de usuario, el valor puede ser cualquier cosa: las etiquetas no admiten ninguna lógica.

9. Haga clic en **Revisar + Crear** para revisar las opciones de recursos que se enviarán para su implementación.
10. Haga clic en **Crear** para construir el recurso.

Nota Colocación de recursos de NSG

Decidir si colocar los recursos NSG cerca de la red o cerca del recurso depende de si el NSG se asociará a la red oa una o más subredes. Si el NSG se asociará a la tarjeta de interfaz de red de una máquina virtual, colóquelo con la máquina. Si se asociará con una o más subredes, colóquelo con el recurso de red virtual. Recuerde, esto es arbitrario y puede que no funcione para todos, pero es un buen lugar para comenzar.



Sugerencia para el examen

Al asignar un grupo de seguridad de red, incluso si solo hay una máquina virtual en un segmento de red, el uso de una asociación de subred para el grupo de seguridad de red reducirá significativamente la cantidad de lugares donde el grupo no está configurado cuando es necesario solucionar problemas.

Una vez que se crea el grupo de seguridad de red, necesitará alguna configuración para que sea útil. Con el nuevo recurso seleccionado, las reglas iniciales disponibles son:

- ■ **Permitir VnetInBound.** Se permite la entrada de todo el tráfico de recursos en la misma red virtual.
- ■ **AllowAzureLoadBalancerInBound.** Se permite la entrada de cualquier tráfico de Azure Load Balancer.
- ■ **DenyAllInBound.** Se deniega el tráfico entrante que no cumpla con otra regla.
- ■ **Permitir VnetOutBound.** Se permite la salida de todo el tráfico a otros recursos en la misma red virtual.
- ■ **AllowInternetOutBound.** Se permite la salida de todo el tráfico destinado a Internet.
- ■ **DenyAllOutBound.** Se deniega cualquier tráfico saliente que no cumpla con otra regla.

Puede notar que la prioridad en estas reglas es 65,000 o más, colocándolas al final de la lista. El número de prioridad es cómo se evalúan las reglas dentro de un NSG, primero los números más bajos. Las reglas predeterminadas creadas dentro de un entorno se evalúan en último lugar y cualquier regla agregada se alcanzaría antes que ellas. Estas son reglas generales para garantizar que la mayor parte del

tráfico no se bloquee tan pronto como se configura el recurso. La configuración inicial de un NSG se muestra en la [Figura 2-59](#).

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanceInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65500	DenyAllOutbound	Any	Any	Any	Any	Deny

FIGURA 2-59 Configuración del grupo de seguridad de red

Para agregar reglas al NSG, complete los siguientes pasos:

1. Seleccione **Reglas de seguridad** de entrada en el menú de navegación del grupo de **seguridad** de red.
2. Haga clic en **Agregar** y proporcione la siguiente información:
 1. ■ **Fuente.** Seleccione **Dirección IP**, **Etiqueta de servicio de Azure**, **Grupo de seguridad de la aplicación** o **Cualquiera**.
 - 1.■ **Dirección IP.** Una dirección IP de recurso específica.
 - 2.■ **Red virtual.** El nombre de una red virtual existente.
 - 3.■ **Grupo de seguridad de aplicaciones.** El nombre de un grupo de seguridad de aplicaciones existente.
 - 4.■ **Cualquiera.** Cualquier recurso que exista en la red donde está configurado este NSG.
 2. ■ **Rangos de puertos de origen.** Los números de puerto a los que se aplicará esta regla.

3. ■ **Destino.** Los recursos a los que se dirigirá esta regla:
 0. ■ **Dirección IP.** Una dirección IP de recurso específica.
 1. ■ **Red virtual.** El nombre de una red virtual existente.
 2. ■ **Grupo de seguridad de aplicaciones.** El nombre de un grupo de seguridad de aplicaciones existente.
 3. ■ **Cualquiera.** Cualquier recurso que exista en la red donde está configurado este NSG.
4. ■ **Rangos de puertos de destino.** Los puertos en el interior de este NSG que se verán afectados por esta regla; no es necesario que coincidan con los puertos de origen, a menos que exista una razón para hacerlo.
5. ■ **Protocolo.** Especifique el protocolo al que afectará esta regla.
6. ■ **Acción.** Especifique si la regla permitirá o denegará el acceso cuando se active esta regla.
7. ■ **Prioridad.** Especifique en qué lugar de la lista de reglas se debe procesar una regla. Los números más bajos se evaluarán en la parte superior.
8. ■ **Nombre.** Especifique un nombre para la regla NSG.
9. ■ **Descripción.** Especifique una descripción opcional.

3. Haga clic en **Agregar** para crear la regla.

Recuerde, las reglas en un NSG son unidireccionales, ya sea de entrada o de salida. Para agregar una regla de seguridad saliente, seleccione la opción **Reglas de seguridad saliente** en el menú de navegación del grupo de **seguridad** de red y repita el proceso anterior.

Con algunas reglas establecidas para controlar el tráfico, el NSG debe estar asociado con recursos para controlar el tráfico. Para asignarlo a una subred, haga clic en la opción **Subredes** en el menú de navegación, haga

clic en **Asociar** y elija la red virtual (y subred) donde se debe usar este grupo.



Sugerencia de examen Se requiere la misma región

Los grupos de seguridad de red asociados con subredes deben estar en la misma región que la red virtual donde existe la subred. Si no es así, no habrá redes disponibles para asociarse.

La asociación con una interfaz de red es como una asociación de subred: seleccione la opción **Interfaces de red** en el menú de navegación, haga clic en **Asociar** y seleccione los recursos de la interfaz de red con los que se debe utilizar esta regla.

Eso es todo lo que hay que hacer para configurar NSG, aunque esto no significa que no sea necesario solucionar problemas o revisar las reglas a medida que las cosas crecen, pero el proceso de configuración es sencillo.

Una cosa más sobre las NSG

Para revisar las reglas de seguridad efectivas aplicadas por un grupo, complete los siguientes pasos:

1. Seleccione la opción **Reglas de seguridad efectivas** en el menú de navegación del NSG.
2. Seleccione la máquina virtual (si está asociada con una máquina virtual) o la red virtual (si está asociada con una red virtual).
3. Se mostrarán las reglas que están actualmente en vigor en los recursos seleccionados.

Grupos de seguridad de aplicaciones

Los grupos de seguridad de aplicaciones (ASG) se utilizan como objetivos dentro de los NSG para garantizar que se permita que el tráfico correcto llegue a los recursos dentro de un ASG. No permiten ni niegan específicamente el tráfico, pero proporcionan una forma de mantener los recursos de un determinado tipo (servidores web, por ejemplo) agrupados para que todo el tráfico que ingresa por los puertos 80 o 443 pueda enrutarse a un destino y llegar a todos y cada uno de los servidores web configurados.

Para crear un ASG, complete los siguientes pasos:

1. Inicie sesión en Azure Portal (<https://portal.azure.com>).
2. En el menú de navegación, haga clic en el botón **Crear un recurso**, busque **Grupo de seguridad de la aplicación**, seleccione **Grupo de seguridad de la aplicación** en los resultados y haga clic en **Crear**.
3. Especifique la suscripción y el grupo de recursos que albergará el ASG.
4. Proporcione un nombre para el ASG y seleccione la región apropiada.
5. Si su organización utiliza etiquetas, haga clic en **Siguiente: Etiquetas** para agregarlas; si no es así, omita este paso.
6. Haga clic en **Revisar + Crear** para revisar las opciones de recursos que se enviarán para su implementación.
7. Haga clic en **Crear** para construir el recurso.

Al igual que los grupos de seguridad de red, los grupos de seguridad de aplicaciones necesitarán alguna configuración adicional una vez creados. Debido a que estos grupos ayudan a unir servidores que realizan tareas similares, la adición de miembros a un grupo de seguridad de aplicaciones ocurre desde dentro de las máquinas virtuales que se están configurando.

Para agregar un servidor virtual como miembro de un ASG, complete los siguientes pasos y consulte la [Figura 2-60](#) :

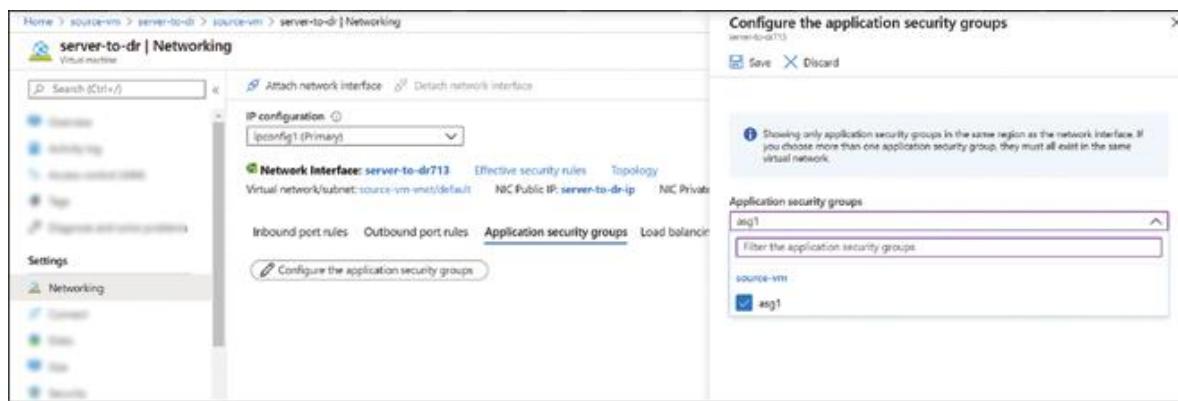


FIGURA 2-60 Configuración del grupo de seguridad de la aplicación

1. Navegue hasta el recurso de la máquina virtual que se está agregando.

2. Seleccione la opción **Redes** en el menú de navegación.
3. Seleccione la pestaña **Grupos de seguridad de aplicaciones**.
4. Haga clic en **Configurar los grupos de seguridad de la aplicación**.
5. Seleccione el ASG al que esta VM se convertirá en miembro.
6. Haga clic en **Guardar**.

Una vez que el ASG tiene miembros asignados, se puede utilizar para ayudar a simplificar los NSG y las reglas que se utilizan para definir el flujo de tráfico dentro de un entorno.

Debido a que es probable que los ASG sean bastante ambiguos al principio, en gran parte porque no tienen opciones de configuración individuales, es una práctica ideal asegurarse de que los nombres de los grupos sean muy específicos de las acciones para las que se utilizarán..

Por ejemplo, si existe el requisito de configurar una regla para permitir el acceso a una base de datos pero solo desde servidores específicos, podría tener sentido especificar un ASG como fuente de la regla. Esto significa que solo los servidores de ese grupo podrían acceder al recurso de la base de datos.

Implementar Azure Bastion

Azure Bastion es el servicio de Azure equivalente a un host de salto o bastión. El uso de estas máquinas para acceder a recursos en redes específicas permite aplicar más seguridad al objetivo.ambiente. Por ejemplo, mi organización podría necesitar una red específica para estar completamente aislada de Internet, lo que eliminaría cualquier dirección IP pública o acceso de otras redes conectadas a Internet. Cuando se configura en el mismo entorno, Azure Bastion permitirá el acceso de administración sin requerir una máquina virtual de host múltiple o acceso público a los servidores de destino.

Para poner en funcionamiento Azure Bastion, complete los siguientes pasos:

1. Inicie sesión en Azure Portal (<https://portal.azure.com>).
2. En el menú de navegación, seleccione **Crear un recurso**.
3. En el cuadro de búsqueda de nuevos recursos, escriba **Bastión**, seleccione la opción **Bastión** y haga clic en **Crear**.

4. Proporcione la siguiente información para configurar Azure Bastion en su entorno:
 1. ■ **Suscripción.** Seleccione la suscripción que albergará el recurso Bastión.
 2. ■ **Grupo de recursos.** Seleccione o cree un grupo de recursos para el recurso Bastión.



Ubicación de la sugerencia, ubicación, ubicación

Mantenga el servicio Bastion cerca de la red a la que dará servicio. Si lo coloca en el mismo grupo de recursos que la red virtual, se asegurará de que se encuentre en la región requerida.

3. ■ **Nombre.** El nombre de la instancia de Azure Bastion que se está configurando.
4. ■ **Región.** Especifique la región para el recurso Bastión.
5. ■ **Red virtual.** Seleccione o cree una red virtual para usar con Azure Bastion.
6. ■ **Subred.** Azure Bastion requiere una subred nombrada `AzureBastionSubnet` para existir o crearse en la red virtual utilizada. Si esta subred existe, se selecciona automáticamente.
7. ■ **Dirección IP pública.** Seleccione una dirección IP pública existente o cree una nueva para Azure Bastion.
5. Haga clic en **Siguiente: Etiquetas** para continuar y agregar etiquetas a la instancia de Azure Bastion.
6. Una vez que se hayan agregado las etiquetas, haga clic en **Siguiente: Revisar + Crear** para revisar sus selecciones.
7. Haga clic en **Crear** para aprovisionar Azure Bastion.

Una instancia de Azure Bastion implementada proporciona conectividad basada en navegador para Windows (a través de RDP) y Linux (a través de SSH) para administración y uso general. El uso de Azure Bastion no requiere que estos sistemas tengan una dirección IP de acceso público o una dirección IP privada accesible desde una estación de administración. El servicio Bastion maneja la conexión al sistema de destino.

Dos cosas a tener en cuenta:

- Azure Bastion, cuando se usa solo para acciones administrativas, no requiere una licencia de acceso de cliente para el sistema de destino.
- Además, actualmente existe un límite en la cantidad de hosts a los que Bastion puede conectarse simultáneamente. Para las sesiones de RDP, esto es 25 y para SSH 50, ambos dependiendo del número de otras sesiones que lleguen a los sistemas de destino.

Para conectarse a un servidor mediante Azure Bastion, complete los siguientes pasos:

1. Inicie sesión en Azure Portal.
2. Busque la máquina virtual a la que desea conectarse y selecciónela para ver sus opciones.
3. Haga clic en la opción **Conectar** en la sección **Configuración** del menú de navegación.
4. Seleccione **Bastion** como tipo de conexión.
5. Ingrese el nombre de usuario y la contraseña y haga clic en **Conectar**, como se muestra en la [Figura 2-61](#).

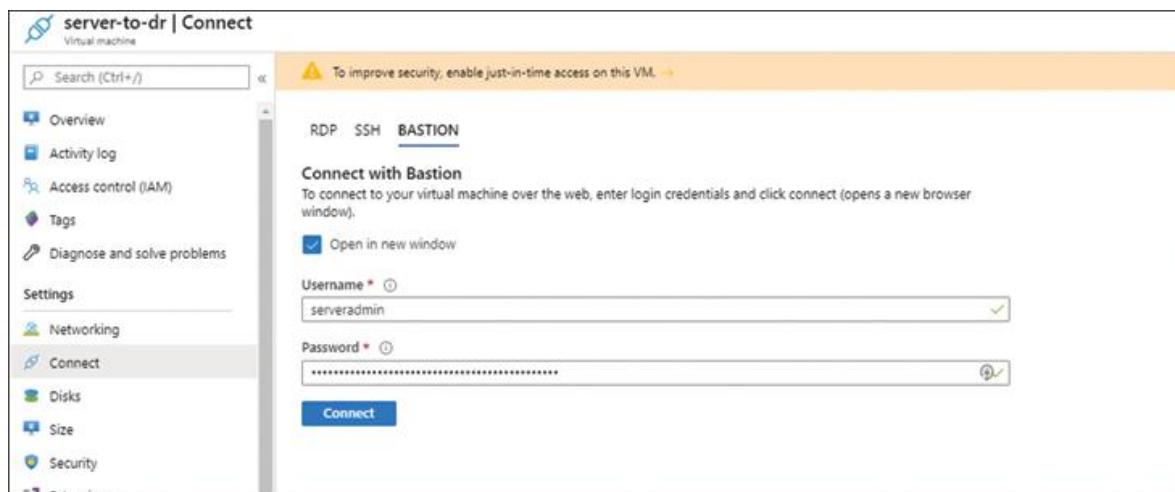


FIGURA 2-61 Información de conexión de Azure Bastion

De forma predeterminada, la conexión Bastion se abre en una nueva pestaña, que a veces está bloqueada por bloqueadores de ventanas emergentes.

Una vez conectado, la vista a través de Bastion es la misma que con las herramientas de conexión estándar. Simplemente ocurre en una pestaña del navegador en lugar de en aplicaciones externas (consulte la Figura 2-62).

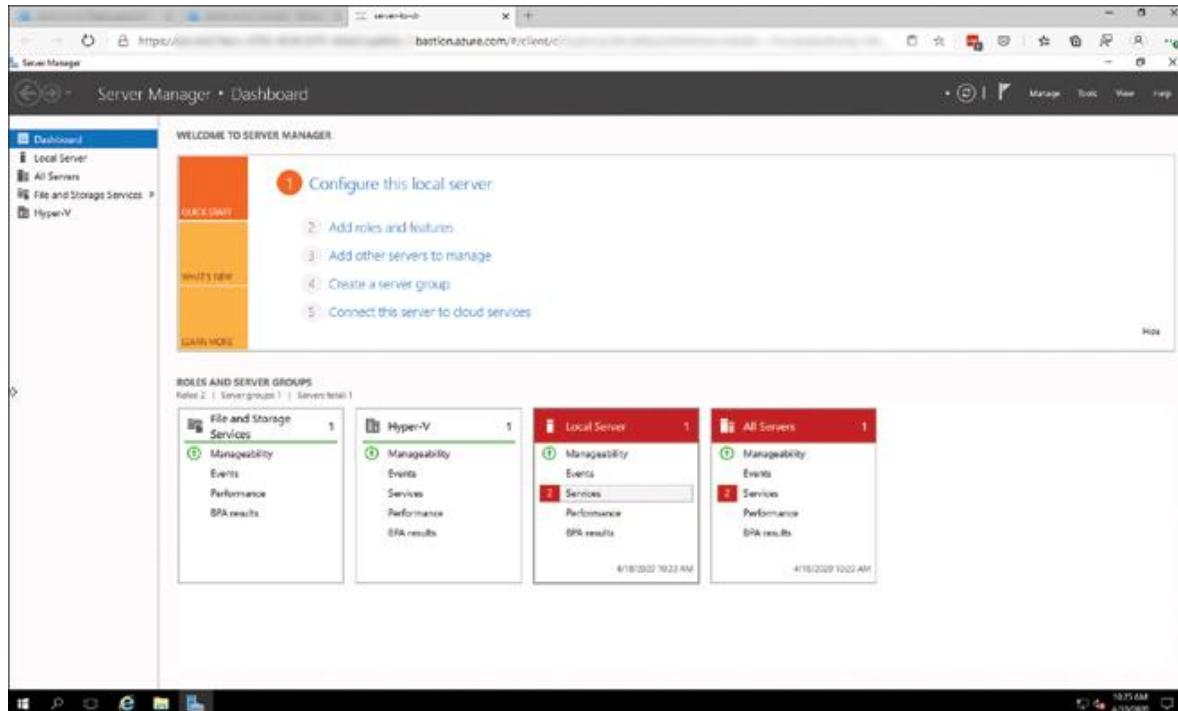


FIGURA 2-62 Conectado a una máquina virtual de Azure mediante Azure Bastion

El uso de este método de conexión elimina la necesidad de administrar el acceso a través de NSG y evita la adición de otro host para parchear y administrar. En un escenario de host de Bastion tradicional, el propio host de Bastion requeriría mantenimiento y parches, pero como Azure Bastion es un servicio PaaS, no requiere ningún mantenimiento adicional.

¿Necesitas más revisión? Recursos adicionales para las opciones de equilibrio de carga

Consulte los artículos en las siguientes URL para obtener información adicional:

- "¿Qué es Azure Application Gateway?" <https://docs.microsoft.com/en-us/azure/application-gateway/overview>

- "¿Qué es Azure Load Balancer?" <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>
- "¿Qué es Azure Firewall ?" <https://docs.microsoft.com/en-us/azure/firewall/overview>
- "¿Qué es Traffic Manager ?" <https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>
- "Descripción general de los grupos de seguridad de red" <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>
- "Ejemplos de grupos de seguridad de aplicaciones" <https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>
- "¿Qué es Azure Bastion?" <https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>

También puede revisar la documentación de la CLI de Azure en <https://docs.microsoft.com/en-us/cli/azure/get-started-with-azure-cli?view=azure-cli-latest>.

HABILIDAD 2.6: INTEGRAR UNA RED VIRTUAL DE AZURE Y UNA RED LOCAL

Azure admite la conectividad a redes externas o locales a través de dos métodos:

- **VPN** Una conexión encriptada entre dos redes a través de la Internet pública.
- **ExpressRoute** Una conexión basada en circuitos privados entre la red de una organización y Azure

Tenga en cuenta los detalles de seguridad

La conexión realizada por ExpressRoute se ejecuta a través de circuitos privados entre una organización y Azure. Ningún otro tráfico atraviesa estos circuitos, pero el tráfico no está encriptado en

el cable de forma predeterminada. Algunas organizaciones pueden optar por cifrar este tráfico con una VPN o tener que hacerlo.

Esta habilidad cubre cómo:

- ■ [Crear y configurar Azure VPN Gateway](#)
- ■ [Crear y configurar VPN de sitio a sitio](#)
- ■ [Verificar la conectividad local](#)
- ■ [Administrar la conectividad local con Azure](#)
- ■ [Configurar ExpressRoute](#)

Crear y configurar Azure VPN Gateway

La puerta de enlace de red virtual es un punto final de enrutador diseñado específicamente para administrar conexiones privadas entrantes. El recurso requiere la existencia de una subred dedicada, denominada subred de puerta de enlace, para que la utilice la VPN.

Para agregar una subred de puerta de enlace a una red virtual, complete los siguientes pasos:

1. Seleccione la red virtual que se utilizará con la puerta de enlace de red virtual.
2. Abra la hoja **Subredes** del recurso de red.
3. Haga clic en **Gateway Subred** en la parte superior de la hoja **Subredes** .
4. Especifique el rango de direcciones de la subred. Debido a que está dedicado a la conexión de VPN, la subred puede ser pequeña según la cantidad de dispositivos que se conectarán.
5. Edite la tabla de rutas según sea necesario (no es necesario de forma predeterminada).
6. Elija los servicios que utilizarán esta subred.
7. Seleccione los servicios a los que se dedicará esta red.
8. Haga clic en **Aceptar** .

Importante sobre las redes

Tenga en cuenta el espacio de direcciones utilizado para las redes virtuales creadas como subredes, incluida la subred de la puerta de

enlace; deben caber dentro del espacio de direcciones y no deben superponerse.

Para crear una puerta de enlace de red virtual, complete los siguientes pasos:

1. En Azure Portal, seleccione o cree el grupo de recursos que contendrá la puerta de enlace de red virtual.
2. Haga clic en **Agregar vínculo** en la parte superior de la hoja **Grupo de recursos**.
3. Ingrese **la puerta de enlace de red virtual** en el cuadro de búsqueda de recursos. Seleccione **Puerta de enlace de red virtual** en los resultados de la búsqueda.
4. Haga clic en el botón **Crear** para comenzar a crear el recurso.
5. Complete el formulario **Crear puerta de enlace de red virtual que se muestra en la Figura 2-63 :**

Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more.](#)

PROJECT DETAILS

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription

Resource group

INSTANCE DETAILS

* Name

* Region

* Gateway type VPN ExpressRoute

* VPN type Route-based Policy-based

* SKU

Only virtual networks in the currently selected subscription and region are listed.

VIRTUAL NETWORK

* Virtual network

Gateway subnet address range

PUBLIC IP ADDRESS

* Public IP address Create new Use existing

* Public IP address name

Public IP address SKU Basic

* Assignment Dynamic Static

* Enable active-active mode Enabled Disabled

* Configure BGP ASN Enabled Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

FIGURA 2-63 Creación de una puerta de enlace de red virtual

1. ■ **Suscripción.** La suscripción de Azure que contendrá el recurso de puerta de enlace de red virtual.
2. ■ **Nombre.** El nombre de la puerta de enlace de la red virtual.

3. ■ **Región.** La región de la puerta de enlace de la red virtual. Debe haber una red virtual en la región donde se crea la puerta de enlace de la red virtual.
 4. ■ **Tipo de puerta de enlace.** Elija ExpressRoute o VPN .
 5. ■ **Tipo de VPN.** Elija Basado en ruta o Basado en políticas .
 6. ■ **SKU.** El tamaño del recurso y el precio de la puerta de enlace.
 7. ■ **Red virtual.** La red a la que se conectará la puerta de enlace.
 8. ■ **Dirección IP pública.** La dirección IP externa de la puerta de enlace (nueva o existente).
 9. ■ **Habilite el modo activo-activo.** Permitir la gestión de conexiones activa / activa.
 10. ■ **Habilite BGP / ASN.** Permita la difusión de la ruta BGP para esta puerta de enlace.
6. Haga clic en **Revisar + Crear** para revisar la configuración.
 7. Haga clic en **Crear** para comenzar a aprovisionar la puerta de enlace.

Anote el tiempo de aprovisionamiento

Las puertas de enlace de red virtuales pueden tardar entre 15 y 45 minutos en crearse. Además, cualquier actualización de la puerta de enlace también puede tardar entre 15 y 45 minutos en completarse.

Importante sobre los recursos de redes

Cuando configura los recursos de red, no hay forma de desaprovisionarlos. Las máquinas virtuales se pueden apagar, pero los recursos de red siempre están encendidos y se facturan si existen.

Crear y configurar VPN de sitio a sitio

Una vez configuradas las puertas de enlace de la red virtual, puede comenzar a configurar la conexión entre ellas o entre una puerta de enlace y un dispositivo local.

Hay tres tipos de conexiones disponibles mediante el recurso de conexión en Azure:

- **VNet a VNet.** Conectar dos redes virtuales en Azure, quizás entre regiones
- **Sitio a sitio.** Un túnel IPSec entre dos sitios: un centro de datos local y Azure
- **ExpressRoute.** Una conexión basada en circuitos dedicada a Azure, que discutiremos más adelante en este capítulo.

Para una configuración de sitio a sitio, complete los siguientes pasos:

1. En Azure Portal, abra el grupo de recursos que contiene la puerta de enlace de red virtual y la red virtual que se usarán en esta configuración.
2. Recopile la dirección IP pública y el espacio de direcciones internas para las redes locales que se conectan a Azure y la dirección IP pública y el espacio de direcciones de la puerta de enlace de la red virtual.
3. Cree una clave previamente compartida para usar en el establecimiento de la conexión.
4. Agregue un recurso de conexión en el mismo grupo de recursos que la puerta de enlace de red virtual.
5. Elija el tipo de conexión para la VPN, de sitio a sitio, la suscripción, el grupo de recursos y la ubicación del recurso.

Importante Manténgalo unido

El grupo de recursos y la suscripción para las conexiones y otros recursos relacionados deben ser los mismos que la configuración de la puerta de enlace de la red virtual.

6. Configure las configuraciones para la VPN como se muestra en la Figura 2-64 :

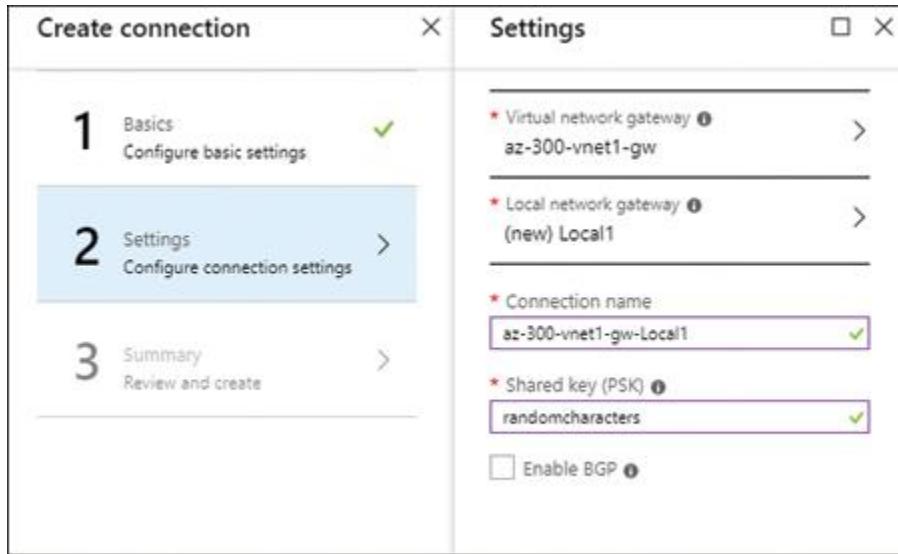


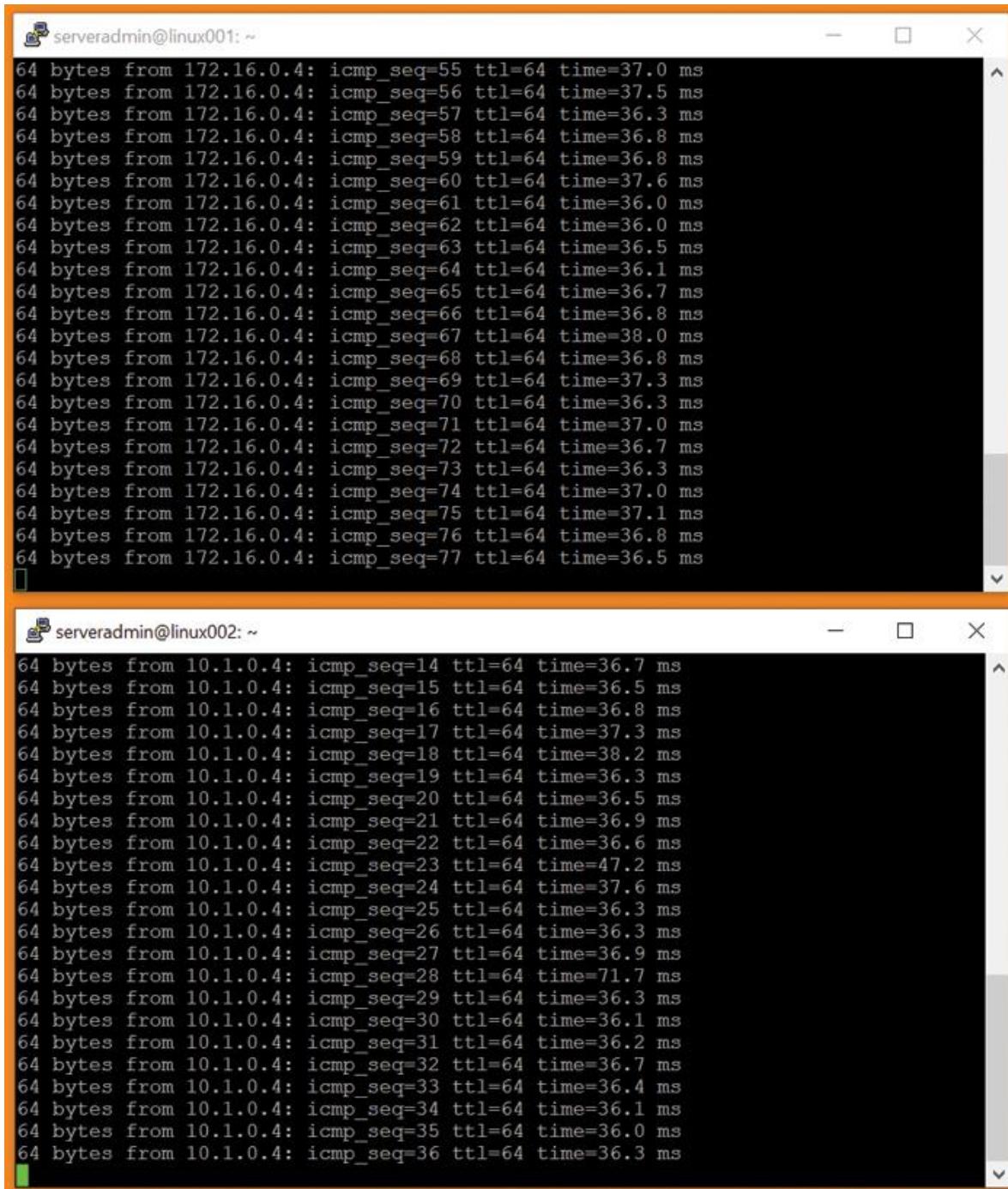
FIGURA 2-64 Configuración de la configuración de una VPN de sitio a sitio

1. ■ **Puerta de enlace de red virtual.** Elija la puerta de enlace de red virtual disponible según la suscripción y la configuración del grupo de recursos ya seleccionada.
2. ■ **Puerta de enlace de red local.** Seleccione o cree una puerta de enlace de red local. Este será el punto final para cualquier dispositivo local que se conecte a esta VPN.
7. Nombra la puerta de enlace de la red local.
8. Ingrese la dirección IP pública (externa) del dispositivo local utilizado.
9. Ingrese el espacio de direcciones para la red interna local. Se permite más de un rango de direcciones.
10. El **nombre de la conexión** se completa en función de los recursos involucrados, pero puede cambiarlo si necesita que se ajuste a una convención de nomenclatura.
11. Ingrese la **clave compartida (PSK)** para la conexión.
12. Habilite BGP si es necesario para la conexión. Esto requerirá al menos un SKU estándar para la puerta de enlace de red virtual.
13. Revise la información resumida de los recursos que se están creando y haga **clic en Aceptar**.

Verificar la conectividad local

Una vez que se haya completado la configuración de VPN de sitio a sitio, la verificación de la conexión funcionará o no. Si tiene todo configurado correctamente, acceder a los recursos en Azure debería funcionar como acceder a otros recursos locales.

La conexión a las máquinas conectadas a la red virtual de Azure mediante direcciones IP locales debe confirmar que la VPN está conectada, como muestra la prueba de ping en la [Figura 2-65](#).



The image displays two terminal windows side-by-side, both titled "serveradmin@linux001: ~" and "serveradmin@linux002: ~". Each window shows a list of ICMP echo requests (pings) sent from one machine to another. The top window (linux001) shows pings to 172.16.0.4, and the bottom window (linux002) shows pings to 10.1.0.4. Both lists include the byte count (64), source IP (either 172.16.0.4 or 10.1.0.4), sequence number (icmp_seq), TTL (64), and time taken (in ms). The traffic is bidirectional, with each machine sending a series of pings to the other.

```
64 bytes from 172.16.0.4: icmp_seq=55 ttl=64 time=37.0 ms
64 bytes from 172.16.0.4: icmp_seq=56 ttl=64 time=37.5 ms
64 bytes from 172.16.0.4: icmp_seq=57 ttl=64 time=36.3 ms
64 bytes from 172.16.0.4: icmp_seq=58 ttl=64 time=36.8 ms
64 bytes from 172.16.0.4: icmp_seq=59 ttl=64 time=36.8 ms
64 bytes from 172.16.0.4: icmp_seq=60 ttl=64 time=37.6 ms
64 bytes from 172.16.0.4: icmp_seq=61 ttl=64 time=36.0 ms
64 bytes from 172.16.0.4: icmp_seq=62 ttl=64 time=36.0 ms
64 bytes from 172.16.0.4: icmp_seq=63 ttl=64 time=36.5 ms
64 bytes from 172.16.0.4: icmp_seq=64 ttl=64 time=36.1 ms
64 bytes from 172.16.0.4: icmp_seq=65 ttl=64 time=36.7 ms
64 bytes from 172.16.0.4: icmp_seq=66 ttl=64 time=36.8 ms
64 bytes from 172.16.0.4: icmp_seq=67 ttl=64 time=38.0 ms
64 bytes from 172.16.0.4: icmp_seq=68 ttl=64 time=36.8 ms
64 bytes from 172.16.0.4: icmp_seq=69 ttl=64 time=37.3 ms
64 bytes from 172.16.0.4: icmp_seq=70 ttl=64 time=36.3 ms
64 bytes from 172.16.0.4: icmp_seq=71 ttl=64 time=37.0 ms
64 bytes from 172.16.0.4: icmp_seq=72 ttl=64 time=36.7 ms
64 bytes from 172.16.0.4: icmp_seq=73 ttl=64 time=36.3 ms
64 bytes from 172.16.0.4: icmp_seq=74 ttl=64 time=37.0 ms
64 bytes from 172.16.0.4: icmp_seq=75 ttl=64 time=37.1 ms
64 bytes from 172.16.0.4: icmp_seq=76 ttl=64 time=36.8 ms
64 bytes from 172.16.0.4: icmp_seq=77 ttl=64 time=36.5 ms

64 bytes from 10.1.0.4: icmp_seq=14 ttl=64 time=36.7 ms
64 bytes from 10.1.0.4: icmp_seq=15 ttl=64 time=36.5 ms
64 bytes from 10.1.0.4: icmp_seq=16 ttl=64 time=36.8 ms
64 bytes from 10.1.0.4: icmp_seq=17 ttl=64 time=37.3 ms
64 bytes from 10.1.0.4: icmp_seq=18 ttl=64 time=38.2 ms
64 bytes from 10.1.0.4: icmp_seq=19 ttl=64 time=36.3 ms
64 bytes from 10.1.0.4: icmp_seq=20 ttl=64 time=36.5 ms
64 bytes from 10.1.0.4: icmp_seq=21 ttl=64 time=36.9 ms
64 bytes from 10.1.0.4: icmp_seq=22 ttl=64 time=36.6 ms
64 bytes from 10.1.0.4: icmp_seq=23 ttl=64 time=47.2 ms
64 bytes from 10.1.0.4: icmp_seq=24 ttl=64 time=37.6 ms
64 bytes from 10.1.0.4: icmp_seq=25 ttl=64 time=36.3 ms
64 bytes from 10.1.0.4: icmp_seq=26 ttl=64 time=36.3 ms
64 bytes from 10.1.0.4: icmp_seq=27 ttl=64 time=36.9 ms
64 bytes from 10.1.0.4: icmp_seq=28 ttl=64 time=71.7 ms
64 bytes from 10.1.0.4: icmp_seq=29 ttl=64 time=36.3 ms
64 bytes from 10.1.0.4: icmp_seq=30 ttl=64 time=36.1 ms
64 bytes from 10.1.0.4: icmp_seq=31 ttl=64 time=36.2 ms
64 bytes from 10.1.0.4: icmp_seq=32 ttl=64 time=36.7 ms
64 bytes from 10.1.0.4: icmp_seq=33 ttl=64 time=36.4 ms
64 bytes from 10.1.0.4: icmp_seq=34 ttl=64 time=36.1 ms
64 bytes from 10.1.0.4: icmp_seq=35 ttl=64 time=36.0 ms
64 bytes from 10.1.0.4: icmp_seq=36 ttl=64 time=36.3 ms
```

FIGURA 2-65 Tráfico entre direcciones IP locales a través de la VPN

Además de las pruebas de ping y las conexiones entre sistemas en estas redes, la hoja **Resumen** para la conexión local en Azure muestra el tráfico a través de la VPN. Esto se muestra en la [Figura 2-66](#).



FIGURA 2-66 Una conexión VPN activa en Azure Portal

Administrar la conectividad local con Azure

En muchos casos, las conexiones VPN a Azure requerirán poco mantenimiento una vez que estén conectadas y en uso. Sin embargo, puede haber ocasiones en las que cierta conectividad requiera restricciones, por ejemplo, si se debe acceder a un servidor en Azure a través de un equilibrador de carga o solo desde la red local.

Azure permite que estos recursos se creen sin direcciones IP públicas, lo que los hace accesibles solo a través de la VPN. Esto es parte de la gestión de estos recursos; simplemente eliminar la IP pública saca la máquina de Internet, pero una organización puede tener requisitos adicionales en el sentido de que los sistemas en un entorno de producción no pueden comunicarse directamente con los sistemas en un entorno que no es de producción. La segregación se puede manejar a través de grupos de seguridad de red y entradas de la tabla de enrutamiento.

Un grupo de seguridad de red sirve como una lista de ACL para el acceso (o denegación) a los recursos, por lo que ayudaría a abrir o bloquear puertos hacia y desde ciertas máquinas.

La Figura 2-67 muestra un grupo de seguridad de red simple donde el puerto 22 está permitido pero solo desde una fuente etiquetada como red virtual. Esto permite que otros recursos de las redes virtuales de Azure lleguen al dispositivo, pero nada de Internet puede conectarse directamente.

Inbound security rules						
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	⚠ Port_22	22	Any	VirtualNetwork	10.1.0.4	🟢 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	🟢 Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	🟢 Allow
65500	DenyAllInBound	Any	Any	Any	Any	🔴 Deny
Outbound security rules						
PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	🟢 Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	🟢 Allow
65500	DenyAllOutBound	Any	Any	Any	Any	🔴 Deny

FIGURA 2-67 Grupos de seguridad de red

Puede utilizar grupos de seguridad de red en el nivel de interfaz de red para una máquina virtual o en el nivel de subred.



Sugerencia para el examen Simplifique la configuración a nivel de subred

La configuración de grupos de seguridad de red a nivel de subred garantiza un comportamiento uniforme de las reglas en todos los dispositivos de la subred planificada y hace que la administración de la conectividad sea mucho menos complicada.

Nota de seguridad

Si su organización tiene requisitos para el acceso y la conectividad uno a uno, es posible que sea necesario un grupo de seguridad de red configurado en el nivel de interfaz para la máquina virtual para garantizar el acceso restringido de un host a otro.

Los grupos de seguridad de red también permiten la recopilación de registros de flujo que capturan información sobre el tráfico que ingresa y sale de la red a través de grupos de seguridad de red configurados. Para habilitar esto, necesita dos recursos adicionales para todas las funciones, como se muestra en la [Figura 2-68](#) :

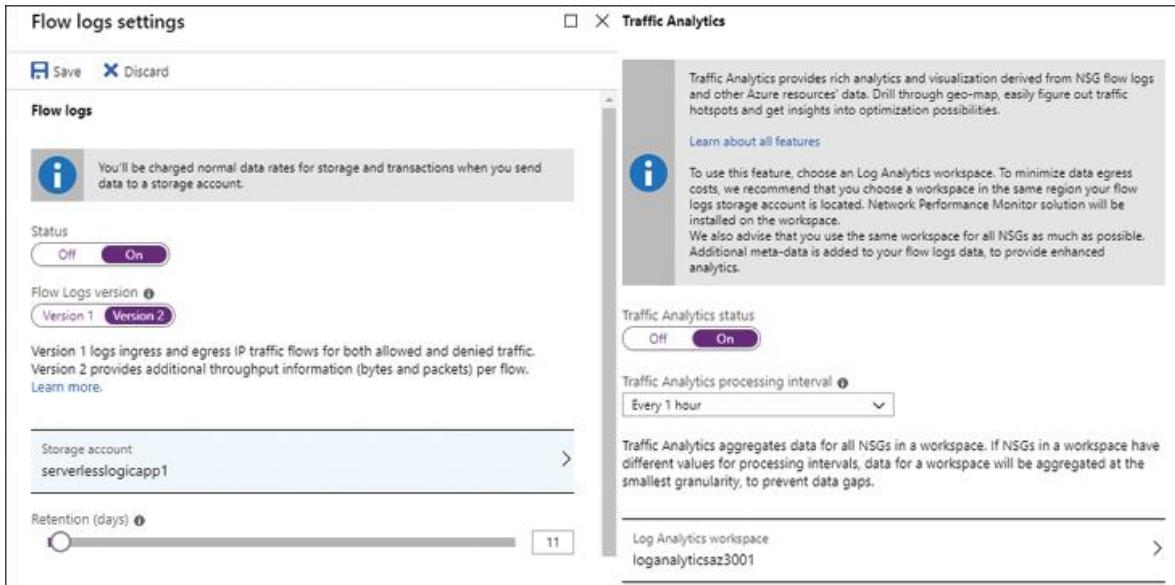


FIGURA 2-68 Configuración de análisis de tráfico y registro de flujo

- Una cuenta de almacenamiento para recopilar los datos del registro de flujo.
- Un espacio de trabajo de Log Analytics para el análisis del tráfico.

Además de los grupos de seguridad de la red, las entradas de la tabla de rutas se pueden utilizar para controlar el flujo de tráfico entre los recursos de la red. Con una entrada de tabla de rutas, puede forzar que todo el tráfico entre subredes pase a través de una red específica o dispositivo de red virtual que maneja todas las reglas y controles de acceso. Hay arquitecturas de referencia para este tipo de configuración en la documentación de Azure que explican cómo configurar este tipo de topología de red.

Configurar ExpressRoute

Antes de poder usar ExpressRoute como un tipo de conexión VPN, debe configurarlo y prepararlo como un recurso de Azure. Complete los siguientes pasos para configurar el recurso del circuito ExpressRoute en Azure:

1. En Azure Portal, haga clic en **Crear un recurso**.
2. Seleccione **ExpressRoute** en la categoría **Redes**.

3. En la página **Crear circuito ExpressRoute**, seleccione crear un circuito nuevo en lugar de importar desde una configuración clásica. Para completar la configuración de ExpressRoute, proporcione la siguiente información:
 1. **Nombre del circuito.** El nombre del recurso del circuito.
 2. **Proveedor.** Seleccione el nombre del proveedor que entrega el circuito.
 3. **Ubicación de intercambio de tráfico.** La ubicación donde termina su circuito; si está utilizando un socio como Equinix en su ubicación de Chicago, usaría Chicago para la ubicación de intercambio de tráfico.
 4. **Ancho de banda.** El ancho de banda proporcionado por el proveedor para esta conexión.
 5. **SKU.** Esto determina el nivel de ExpressRoute que está aprovisionando.
 6. **Medición de datos.** Esto es para el nivel de facturación y se puede actualizar de medido a ilimitado, pero no de ilimitado a medido.
 7. **Suscripción.** La suscripción de Azure asociada a este recurso.
 8. **Grupo de recursos.** El grupo de recursos de Azure asociado con este recurso.
 9. **Ubicación.** La región de Azure asociada a este recurso; esto es diferente de la ubicación de emparejamiento.
4. Haga clic en **Crear** el recurso.

Anote los costos y la facturación

Cuando configura ExpressRoute en Azure, recibe una clave de servicio. Cuando Azure emite la clave de servicio, comienza la facturación del circuito. Espere a configurar esto hasta que su proveedor de servicios esté preparado con el circuito que se emparejará con ExpressRoute para evitar cargos mientras espera otros componentes.

Una vez que se emite la clave de servicio y un proveedor ha proporcionado su circuito, usted proporciona la clave al operador para completar el proceso. Es necesario configurar el emparejamiento privado y permitir BGP para que ExpressRoute funcione.

ExpressRoute también requiere que se configure la puerta de enlace de red virtual. Para hacer esto, al crear una puerta de enlace de red virtual, seleccione **ExpressRoute** como el **Tipo de puerta de enlace** (como se muestra en la Figura 2-69).

The screenshot shows the 'Create Virtual Network Gateway' wizard in the Azure portal. The 'INSTANCE DETAILS' section is highlighted, specifically the 'Gateway type' dropdown. The 'ExpressRoute' option is selected, indicated by a red arrow pointing to the radio button. Other fields in this section include 'Name' (az-300-er-vnet-gw), 'Region' (US Central US), and 'SKU' (Standard). The 'Virtual NETWORK' section shows 'Virtual network' (az-300-er-net) and 'Gateway subnet address range' (10.1.1.0/24). The 'PUBLIC IP ADDRESS' section shows 'Public IP address' (Create new) and 'Public IP address name' (az-300-er-pip). The 'PROJECT DETAILS' section at the top shows the subscription (Microsoft Azure Sponsorship - MVP - 12k) and resource group (az-300-expressroute).

FIGURA 2-69 Configuración de una puerta de enlace de red virtual para ExpressRoute

La configuración de las opciones de emparejamiento para ExpressRoute se realiza desde la configuración de ExpressRoute una vez que se ha configurado el circuito en Azure. A partir de ahí, verá tres tipos de peerings:

- **Público de Azure.** Esto ha quedado obsoleto; utilice el emparejamiento de Microsoft en su lugar.
- **Azure Private.** Peering con redes virtuales dentro de las suscripciones administradas por su organización.
- **Microsoft.** Peering directo con Microsoft para el uso de servicios públicos como Dynamics y Office 365.

Debe cumplir los siguientes requisitos para el intercambio de tráfico:

- Subred A / 30 para el enlace principal.
- Subred A / 30 para el enlace secundario.
- Una ID de VLAN válida para construir el intercambio de tráfico; ninguna otra conexión basada en circuitos puede usar esta ID de VLAN. Los enlaces primario y secundario para ExpressRoute deben usar este ID de VLAN.
- Un número AS para peering (se permiten 2 bytes y 4 bytes).
- Prefijos anunciados, que es una lista de todos los prefijos que se anunciarán a través de BGP.
- Opcionalmente, puede proporcionar un ASN de cliente si se utilizan prefijos que no le pertenecen, un nombre de registro de enrutamiento si el número de AS no está registrado como propiedad suya y un hash MD5.

Revise la información de emparejamiento y complete los siguientes pasos para terminar de configurar ExpressRoute:

1. Seleccione el tipo de emparejamiento necesario y proporcione la información mencionada anteriormente.
2. Guarde la conexión.

Validación importante

Microsoft puede solicitarle que especifique una prueba de propiedad. Si ve que se necesita validación en la conexión, debe abrir un ticket con soporte para proporcionar la información necesaria antes de que se pueda establecer el par. Puede hacerlo desde el portal.

3. Una vez que haya configurado correctamente la conexión, la pantalla de detalles muestra un estado de `configured`.

4. Vincular (o crear una conexión a) ExpressRoute también ocurre desde dentro del recurso ExpressRoute. Elija la opción **Conexiones** dentro de la configuración de ExpressRoute y proporcione lo siguiente:

1. ■ **Nombre.** El nombre de la conexión.
2. ■ **Tipo de conexión.** ExpressRoute.
3. ■ **Puerta de enlace de red virtual.** Seleccione la puerta de enlace con la que vincular ExpressRoute.
4. ■ **Círculo ExpressRoute.** Seleccione el círculo configurado con el que conectarse.
5. ■ **Suscripción.** Seleccione la suscripción que contiene los recursos utilizados en esta conexión.
6. ■ **Grupo de recursos.** Seleccione el grupo de recursos que contiene los recursos utilizados en esta conexión.
7. ■ **Ubicación.** Seleccione la región de Azure donde se encuentran los recursos usados en esta conexión.

Es como crear una conexión de sitio a sitio, como se describió anteriormente, pero utiliza diferentes recursos como parte de la conexión.



Sugerencia para el examen

ExpressRoute es una conexión privada a Azure desde una ubicación determinada y requiere conectividad de gama alta. Gran parte de la discusión sobre ExpressRoute presentada aquí se basa en la documentación de Microsoft porque actualmente no tenemos acceso a un círculo ExpressRoute.

Los ajustes y configuraciones discutidos son de alto nivel, pero proporcionamos una descripción general de los conceptos de ExpressRoute para el examen.

HABILIDAD 2.7: IMPLEMENTAR Y ADMINISTRAR SOLUCIONES DE GOBERNANZA DE AZURE

La gobernanza dentro de un entorno de nube juega un papel cada vez más importante en la capacidad de las organizaciones para migrar a la nube y mantenerse al día con las tecnologías en constante cambio. Azure trae soluciones centradas en la gobernanza a la vanguardia para ayudar a las organizaciones de todos los tamaños a administrar el acceso a los recursos y garantizar que las cargas de trabajo se implementen y mantengan de manera adecuada.

Esta habilidad cubre cómo:

- [Implementar la política de Azure](#)
- [Configurar Azure Blueprint](#)
- [Implementar y aprovechar los grupos de gestión](#)

Implementar la política de Azure

Azure Policy proporciona una forma de hacer cumplir y auditar los estándares y la gobernanza en un entorno de Azure. El uso de esta configuración implica dos pasos de nivel superior:

1. Crear o seleccionar una definición de política existente
2. Asignar esta definición de política a un alcance de recursos

El uso de políticas puede optimizar la auditoría y el cumplimiento dentro de un entorno de Azure. Sin embargo, también puede evitar que se creen determinados recursos en función de la configuración de definición de políticas.

Importante Recuerde comunicarse

Aunque la intención podría ser garantizar, por ejemplo, que todos los recursos se creen en una región específica dentro de Azure, recuerde comunicar en exceso cualquier cambio de cumplimiento a quienes usan Azure. La aplicación de la política generalmente ocurre cuando se hace clic en el botón Crear , no cuando se descubre que el recurso se encuentra en una región no admitida.

Las colecciones de definiciones de políticas, llamadas *iniciativas*, se utilizan para agrupar definiciones de políticas similares para ayudar a lograr un objetivo más amplio de gobernanza en lugar de asignar diez definiciones de políticas por separado. Para alcanzar este objetivo, se pueden agrupar en una iniciativa.

Para asignar una política, complete los siguientes pasos:

1. En el panel de **navegación** de Azure Portal, seleccione **Todos los servicios**.
2. Busque la **política**.
3. Haga clic en la estrella junto al nombre del servicio. (Esto será útil en el futuro).
4. Haga clic en el nombre del servicio de políticas para ir al recurso.
5. En la hoja **Descripción general de políticas**, se mostrará la información de cumplimiento (100% compatible si aún no está en uso).
6. Seleccione el elemento **Tareas**.
7. En la hoja **Asignaciones de políticas**, que se muestra en la [Figura 2-70](#), haga clic en **Asignar política**.

The screenshot shows the 'Policy - Assignments' blade in the Azure portal. On the left, there's a navigation menu with items like Overview, Getting started, Join Preview, Compliance, Remediation, Authoring, and a selected 'Assignments' item under the Authoring section. The main area displays three summary metrics: 'Total Assignments' (0), 'Initiative Assignments' (0), and 'Policy Assignments' (0). Below these metrics is a table with columns for NAME, SCOPE, TYPE, and POLICIES. A message at the top of the table says 'No assignments to display within the given scope'.

FIGURA 2-70 Asignaciones de políticas de Azure

8. Complete la siguiente información en la pantalla Asignar política:
 1. ■ **Alcance.** Seleccione el alcance en el que se configurará la política elegida.

2. ■ **Exclusiones.** Seleccione los recursos que estarán exentos de la asignación de política.
 3. ■ **Definición de políticas.** Seleccione la definición de política que se asignará.
 4. ■ **Nombre de la asignación.** Ingrese el nombre para esta asignación de política.
 5. ■ **Descripción.** Ingrese una descripción del resultado esperado de la asignación de la política.
 6. ■ **Asignado por.** Aparecerá el nombre del usuario que inició sesión en Azure y que está asignando la directiva.
9. Haga clic en **Asignar** para guardar esta configuración.

Al seleccionar de la lista de definiciones disponibles, que se muestra en la [Figura 2-71](#), preste atención al nombre de la política. Las políticas de auditoría se utilizan para capturar información sobre lo que sucedería si se hiciera cumplir la política. Estos no introducirán cambios importantes. Las políticas que no están etiquetadas como auditoría pueden introducir cambios importantes.

Available Definitions

Type All types Search Filter by name or id...

Policy Definitions (171)

Audit virtual machines without disaster recovery configured
Built-in
Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit <https://aka.ms/asr-doc>.

[Preview]: Deploy Log Analytics Agent for Linux VMs
Built-in
Deploy Log Analytics Agent for Linux VMs if the VM Image (OS) is in the list defined and the agent is not installed.

Audit enabling of diagnostic logs in Azure Data Lake Store
Built-in
Audit enabling of diagnostic logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised

Audit VMs that do not use managed disks
Built-in
This policy audits VMs that do not use managed disks

Audit CORS resource access restrictions for a Function App
Built-in
Cross origin Resource Sharing (CORS) should not allow all domains to access your Function app. Allow only required domains to interact with your Function app.

[Preview]: Deploy Log Analytics Agent for Windows VMs
Built-in
Deploy Log Analytics Agent for Windows VMs if the VM Image (OS) is in the list defined and the agent is not installed. The list of OS images will be updated over time as support is updated.

Monitor Internet-facing virtual machines for Network Security Group traffic hardening recommendations
Built-in
Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface

Select Cancel

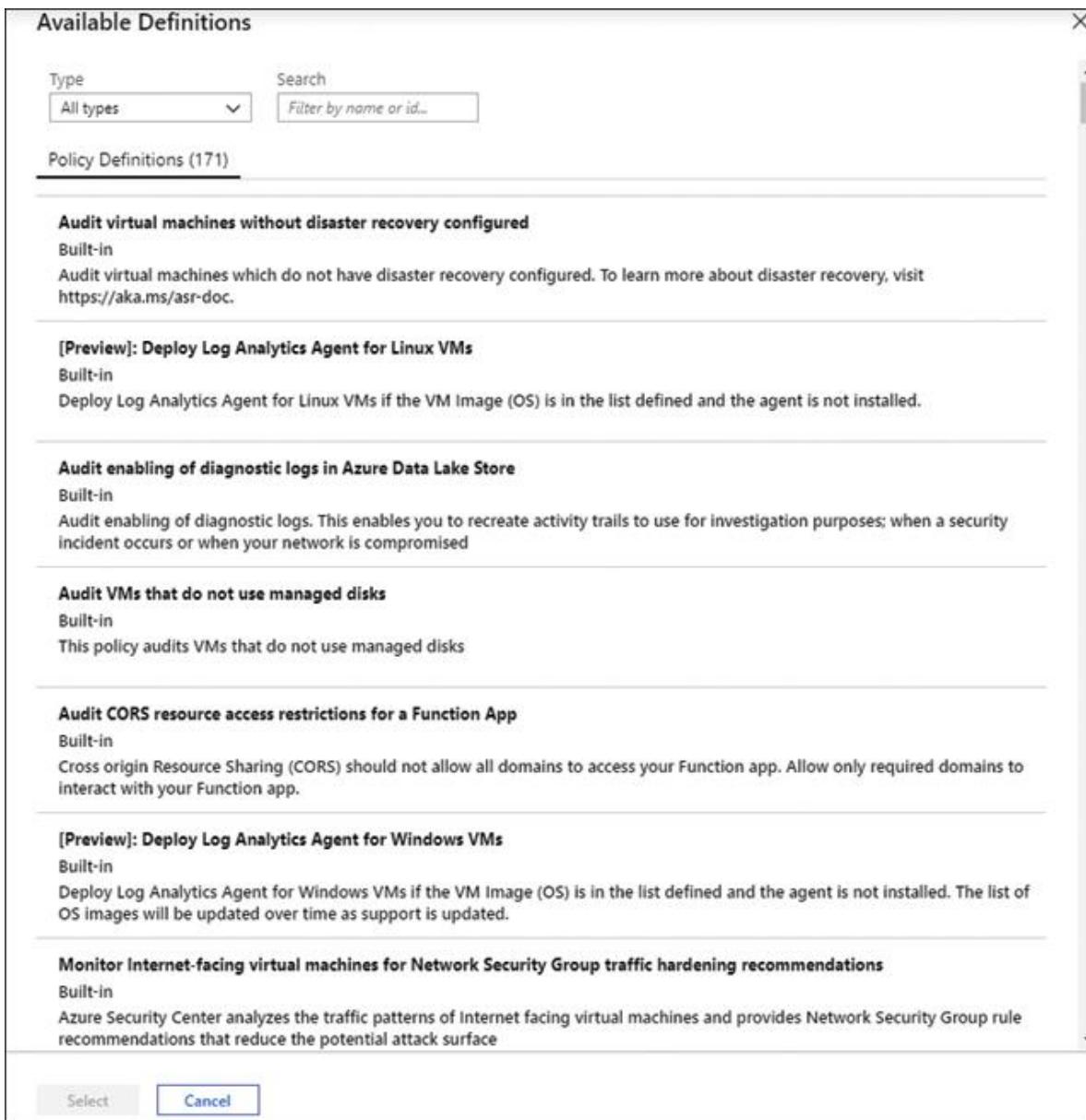


FIGURA 2-71 Definiciones de políticas

Una vez que se ha asignado una política, su estado de cumplimiento puede mostrarse como **No iniciado** porque la política es nueva y aún no se ha evaluado con respecto a los recursos. Haga clic en **Actualizar** para monitorear el estado de cumplimiento. Podría llevar algún tiempo reflejar el cambio de estado.

Si una política se ejecuta en un ámbito y encuentra elementos en incumplimiento, es posible que sea necesario realizar tareas de corrección. Estas tareas se enumeran en la sección **Corrección** de

la hoja **Política** y solo se aplican a las políticas que implementarán recursos si no se encuentran.

Kubernetes también obtiene política

En actualizaciones recientes del marco de políticas de Azure, Azure Kubernetes Service (AKS) se ha integrado con los servicios de políticas. Esto permite aplicar la política durante el proceso de escalado horizontal o vertical de un entorno de contenedor para garantizar que las cargas de trabajo en contenedor sigan las mismas reglas que otros servicios utilizados en el entorno de Azure de una organización.

Poder auditar la creación de cosas como máquinas virtuales y otros recursos de Azure de primera línea y asegurarse de que solo estén permitidos dentro de ciertas regiones fue un gran comienzo, pero si los recursos implementados dentro de un contenedor en AKS pudieran moverse a cualquier región en Azure, esto podría plantear un problema de cumplimiento para los administradores de Azure. Mediante el uso de herramientas de código abierto existentes para incluir AKS en Azure Policy, incluso las cargas de trabajo en contenedores están sujetas a la política de gobierno de la organización.

Aviso de alerta de vista previa limitada

La política de AKS se encuentra en versión preliminar limitada al momento de escribir este artículo. Solo admite las definiciones de políticas integradas, pero a medida que esto continúa avanzando hacia la disponibilidad general, es probable que surjan más opciones para el viaje.

Para habilitar la política de servicio de Azure Kubernetes, complete los siguientes pasos:

1. Para participar en la versión preliminar, registre los proveedores de recursos `Microsoft.ContainerService` y `Microsoft.PolicyInsights` en Azure Portal.
2. Vaya a **Azure Policy**.
3. Seleccione la opción para unirse a la vista previa.
4. Elija las suscripciones que se incluirán en la vista previa marcando las casillas de cada una.
5. Haga clic en el botón **Opt-In**.

Una vez que se haya completado la suscripción para la vista previa, queda trabajo por completar para instalar el agente de la política. Instale el complemento de Azure Policy completando los siguientes pasos:

1. Desde la CLI de Azure, instale la extensión de vista previa con este código:

Haga clic aquí para ver la imagen del código

Lista de az aks

Agregar extensión az --name aks-preview

#verifique la versión de la extensión

**Mostrar extensión az --name aks-preview --query
[versión]**

2. Una vez configurada la extensión de vista previa, instale el complemento AKS en el clúster que será controlado (o auditado) por la política:

1. ■ Desde el portal, ubique y seleccione el servicio Kubernetes.
2. ■ Seleccione cualquiera de los clústeres de AKS enumerados (o cree uno si no hay ninguno).
3. ■ Seleccione **Políticas (vista previa)** en el menú de navegación.
4. ■ Haga clic en el botón **Activar complemento** en la sección principal de la página.

El complemento de política se registrará en AKS una vez cada cinco minutos mediante un análisis completo de los clústeres habilitados. Una vez que este análisis completa, los detalles del análisis y los datos recopilados se devolverán a Azure Policy y se incluirán en los informes de detalles de cumplimiento proporcionados.

Implementación de Azure Blueprint

Azure Blueprint es una forma de crear repetibilidad dentro de un entorno de nube que se adhiere a los estándares que la organización ha configurado. Azure Blueprint es un recurso de orquestación declarativa para ayudar a crear mejores entornos de Azure.

Nota Mejor no significa Mejor

En este caso, mejor tenía la intención de especificar más organizado y repetible. No se requiere Blueprint para mantener las cosas repetibles. Azure se adapta muy bien a cualquier método de automatización y desarrollo.

Una de las ventajas de Blueprint es el back-end de Cosmos DB. Esto hace que los objetos utilizados dentro de Blueprint estén disponibles en todas las regiones debido a la operación distribuida globalmente de Cosmos DB. Mantener los objetos disponibles en Azure garantiza una implementación de baja latencia de los recursos, independientemente de la región en la que se implementen. Si una organización mantiene los recursos locales dentro de West US 2, Blueprint estará allí y no será necesario contactarlo desde una región diferente para su uso.

Para comenzar y configurar Blueprint, complete los siguientes pasos (que se muestran en la Figura 2-72 a continuación):

Create blueprint

Choose a blueprint sample

You can start with a blank blueprint or pick one of our pre-defined samples to help you get started quickly

Blank Blueprint

An empty blueprint with no initial properties or artifacts.

Start with blank blueprint

Other Samples

Name	Description
Basic Networking (VNET)	Configures a virtual network with a subnet and an NSG.
CAF Foundation	Microsoft Cloud Adoption Framework for Azure – Configure Foundational best practices Learn more
CAF Migration landing zone	Microsoft Cloud Adoption Framework for Azure – Migrations landing zone Learn more
Canada Federal PBMM	Assigns policies to address Canada Federal PBMM controls. Learn more
CIS Microsoft Azure Foundations Bench...	Assigns policies to address specific recommendations from the CIS Microsoft Azure Foundations Benchmark v1.1...
Common Policies	A set of popular policies to apply to a subscription

FIGURA 2-72 Configurar Azure Blueprint

1. Inicie sesión en Azure Portal y seleccione **Blueprints** en la lista de servicios (o busque si es más rápido).

2. Seleccione **Definiciones de planos** en la lista de navegación de la izquierda.
3. En la pantalla principal, seleccione **Crear plano**.
4. Hay algunos Blueprints predefinidos disponibles para elegir, que incluyen, entre otros:
 1. ■ Políticas de HIPAA
 2. ■ Grupos de recursos con RBAC
 3. ■ Redes básicas
5. Seleccione un Blueprint integrado o elija comenzar con uno en blanco.
6. Proporcione lo siguiente para el recurso Blueprint (que se muestra en la Figura 2-73):

Assign blueprint

networking-resources

Resource Group: Name	RG-blueprint-1
Resource Group: Location	West US 2

[User group or application name] : Contributor

[User group or application name] ([User group or application name] : Contributor)	Derek Schauland (az-303-book_outlook.com...)
---	--

Adaptive Network Hardening recommendations should be applied...

Effect (Policy: Adaptive Network Hardening recommendations should be applied on internet facing virtual machines)	AuditIfNotExists
---	------------------

Network ARM

location (Network ARM)	northcentralus
virtualNetworkName (Network ARM)	vnet1
resourceGroup (Network ARM)	rg-vnet1
addressSpaces (Network ARM)	["10.0.0.0/16"]
ipv6Enabled (Network ARM)	false
subnetCount (Network ARM)	1
subnet0_name (Network ARM)	subnet1
subnet0_addressRange (Network ARM)	10.0.1.0/24
ddosProtectionPlanEnabled (Network ARM)	false
firewallEnabled (Network ARM)	false
bastionEnabled (Network ARM)	false

Buttons: Assign | Cancel

FIGURA 2-73 Asignación de planos

- 0.■ **Nombre del plano.** Un nombre para el recurso Blueprint
 - 1.■ **Descripción del plano.** ¿Qué hace este Blueprint?
 - 2.■ **Definición Ubicación.** Dónde se guardará / tendrá el alcance el Blueprint
7. Agregue los artefactos que creará este plano; los tipos de recursos disponibles incluyen:
- 0.■ **Grupos de recursos.** Para la organización y RBAC en el momento de la construcción
 - 1.■ **Plantillas ARM.** Los archivos de configuración y las variables que se utilizan para crear recursos.
 - 2.■ **Políticas.** Las políticas de control asignadas a los recursos creados por este Blueprint
 - 3.■ **Roles de RBAC.** Roles asignados a los recursos creados por este Blueprint
8. Guarde el borrador del Blueprint.
9. Haga clic en el borrador guardado y luego haga clic en **Publicar** para que el Blueprint esté disponible para su asignación.
10. Cuando todo esté listo para su uso, haga clic en el Blueprint recién publicado y haga clic en **Assign Blueprint**, y luego proporcione lo siguiente:
- 0.■ **Nombre de la asignación.** El nombre de la tarea
 - 1.■ **Ubicación.** Elija la ubicación predeterminada
 - 2.■ **Versión de definición de plano.** El número de versión de este Blueprint
 - 3.■ **Bloquear asignación.** ¿Debería bloquearse este plano? De lo contrario, los usuarios o directores de servicio con el permiso apropiado pueden modificar el Blueprint.
 - 4.■ **Identidad administrada.** La identidad utilizada por el Blueprint
11. Haga clic en **Asignar**.

Al decidir si una asignación de Blueprint debe bloquearse, considere dónde están destinados a terminar los recursos. Si esto apunta a los recursos de nivel de producción, entonces bloquear la asignación puede tener sentido para garantizar que los recursos no se eliminan intencionalmente o por accidente.

Si el proceso de asignación no puede recopilar valores predeterminados de las plantillas de recursos proporcionadas en el Plan, es posible que le pida (con tinta roja) que lo ayude a proporcionar variables para la asignación. Si eso sucede, proporcione la información necesaria y haga clic en **Asignar** para continuar.

Una vez que la asignación tenga éxito, se aprovisionarán los recursos solicitados como parte del Blueprint.

Nota JSON se valida durante la creación

Al guardar la definición de Blueprint, se validará el JSON de cualquier archivo de plantilla incluido; si no pasa, el guardado fallará.

¿Debería utilizarse Blueprint en lugar de las plantillas de Resource Manager?

El uso de Blueprint incluye la implementación de recursos con plantillas ARM para crear o reconstruir elementos en Azure. Además, también se pueden incluir los aspectos de seguridad de Azure Policy y la configuración del control de acceso mediante grupos de administración o RBAC. Esto permite que Azure Blueprint cubra toda la implementación de un entorno en una configuración general.

Por ejemplo, si mi organización planea construir una aplicación que aproveche cosas como bus de servicio, DNS de Azure, servicios de aplicaciones y APIM, ciertamente puedo manejar esos recursos con plantillas ARM y canalizaciones de automatización. Sin embargo, también tendré que tener en cuenta la seguridad y la configuración de acceso. En lugar de depender de plantillas y configuraciones separadas, la creación de un Blueprint de Azure de toda la configuración no solo reunirá todas las soluciones necesarias en una configuración, sino que permitirá que todo se repita sin necesidad de volver a ensamblar todas las plantillas ARM individuales necesarias. archivos.

Si algunas de las plantillas ARM ya existen, Blueprints puede aprovecharlas para reducir la reinención de los recursos necesarios.

Recuerde, al final, un Blueprint asignado desplegará (o actualizará) todos los recursos asociados definidos dentro de él. Si varios elementos relacionados se administrarán juntos y se implementarán juntos, un Blueprint podría ser la opción lógica. Para implementaciones más pequeñas o únicas, una plantilla ARM podría ser una mejor opción.

Implementar y aprovechar los grupos de administración

Un grupo de administración en Azure es un recurso que puede cruzar los límites de las suscripciones y permitir un único punto de administración entre las suscripciones.

Si una organización tiene varias suscripciones, pueden usar grupos de administración para controlar el acceso a las suscripciones que pueden tener necesidades de acceso similares. Por ejemplo, si hay tres proyectos en marcha dentro de una organización que tienen necesidades de facturación claramente diferentes, cada una administrada por diferentes departamentos, el acceso a estas suscripciones puede ser manejado por grupos de administración, lo que permite que las tres suscripciones se administren juntas con menos esfuerzo y administración. gastos generales.

Los grupos de administración permiten que las configuraciones de RBAC crucen los límites de la suscripción. El uso del alcance de un grupo de administración para el acceso administrativo de alto nivel consolidará la visibilidad de múltiples suscripciones sin necesidad de configurar los ajustes de RBAC en cada una de las muchas suscripciones. De esta manera, al grupo de administradores se le puede asignar acceso de propietario en un grupo de administración que contiene todas las suscripciones para una organización, simplificando un poco más la configuración, como se muestra en la [Figura 2-74](#).

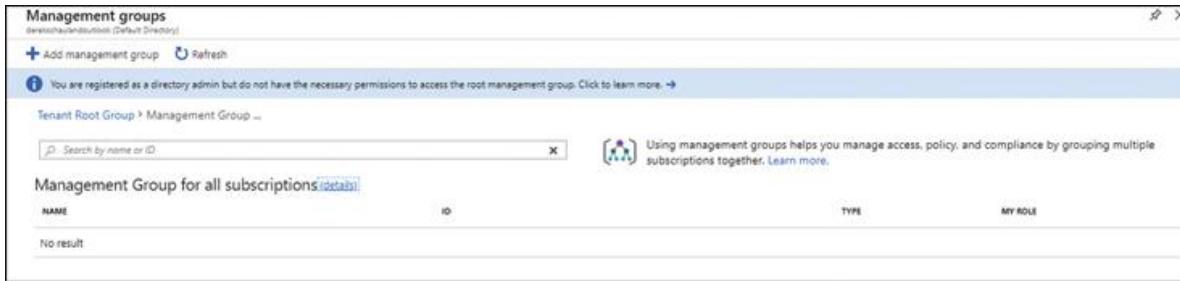


FIGURA 2-74 Los grupos de administración se pueden usar entre suscripciones para acceder

Los grupos de administración de acceso de nivel superior tienen un grupo raíz de nivel superior en el ámbito del inquilino de Azure AD. Los usuarios administrativos no pueden ver esto con los permisos RBAC administrativos o de propietario habituales. Para permitir esta visibilidad, asigne el rol de Administrador de acceso de usuario al grupo que trabajará con los grupos de administración.

Para agregar suscripciones o grupos de administración a un grupo de administración, complete los siguientes pasos:

1. Inicie sesión en Azure Portal.
2. Seleccione **Grupos de administración** de la lista **Todos los servicios** en el panel de navegación.
3. Si no existe ningún grupo de administración, haga clic en **Agregar grupo de administración**.
 1. ■ Ingrese la ID del nuevo grupo de administración. (Esto no se puede cambiar).
 2. ■ Ingrese el nombre para mostrar del grupo de administración.
 4. Haga clic en **Guardar**.
 5. Haga clic en el nombre del grupo de administración al que se agregarán los elementos. Es probable que haya muy poca información visible al ver un grupo de administración. Haga clic en el enlace **Detalles** junto al nombre del grupo para ver más información y tomar medidas en el grupo de administración, incluida la adición de grupos de administración y suscripciones.
 6. Para suscripciones, haga clic en **Agregar suscripción**.
 7. Seleccione la suscripción que administrará este grupo.

8. Haga clic en **Guardar**.
9. Para los grupos de administración, haga clic en **Agregar grupo de administración**.
10. Seleccione para crear un nuevo grupo de administración o utilizar un grupo existente.

Los grupos de administración se pueden anidar para consolidar la administración de recursos. Esto debe usarse con cuidado porque hacerlo puede complicar la administración de suscripciones y recursos más de lo necesario.

11. Seleccione un grupo de administración para incluir y haga clic en **Guardar**.

Importante El cambio de grupos de administración puede requerir revisión de permisos

Al mover elementos de un grupo de administración a otro, los permisos pueden verse afectados negativamente. Asegúrese de comprender el efecto de los cambios antes de realizarlos para evitar eliminar el acceso necesario a los recursos de Azure.

¿Necesitas más revisión? Recursos adicionales para opciones de gobernanza

Consulte los artículos en las siguientes URL para obtener información adicional:

- ■ "¿Qué es Azure Policy?" en <https://docs.microsoft.com/en-us/azure/governance/policy/overview>
- ■ "Comprender la política de Azure para los clústeres de Kubernetes" en <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/rego-for-aks>
- ■ "¿Qué son los grupos de administración de Azure?" en <https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>
- ■ "¿Qué es Azure Blueprints?" en <https://docs.microsoft.com/en-us/azure/governance/Blueprints/overview>

También puede revisar la documentación de la CLI de Azure en <https://docs.microsoft.com/en-us/cli/azure/get-started-with-azure-cli?view=azure-cli-latest> .

HABILIDAD 2.8: GESTIONAR EL CONTROL DE ACCESO BASADO EN ROLES (RBAC)

El control de acceso basado en roles (RBAC) proporciona una forma manejable de asignar acceso a los recursos en Azure al permitir que los permisos se asignen entre los roles de trabajo. Si es un operador de servidor, es posible que pueda iniciar y reiniciar las máquinas virtuales, pero no apagarlas ni eliminarlas. Dado que todos los recursos de Azure están permitidos y requieren acceso, la consolidación de permisos en roles puede ayudar a mantener las cosas organizadas.

Esta habilidad cubre cómo:

- ■ [Crear un rol personalizado](#)
- ■ [Configurar el acceso a los recursos mediante la asignación de roles](#)
- ■ [Configurar el acceso de administración a Azure](#)
- ■ [Solucionar problemas de RBAC](#)

Crea un rol personalizado

Si bien Azure proporciona roles para ciertas actividades, como colaborador y lector, que brindan acceso de edición y lectura respectivamente, puede haber roles de trabajo dentro de una organización que no encajan muy bien en estos elementos predefinidos. Se pueden crear roles personalizados para adaptarse mejor a las necesidades de una organización. Para crear un rol personalizado, complete los siguientes pasos:

1. Inicie sesión en Azure Portal y seleccione el grupo de recursos que contiene los elementos para los que se personalizará el acceso.
2. En la lista de navegación del grupo de recursos, seleccione **Control de acceso (IAM)** .

3. La hoja **IAM** aparece como se muestra en la [Figura 2-75](#) con la pestaña **Verificar acceso** seleccionada.

The screenshot shows the 'az300-vault - Access control (IAM)' blade in the Azure portal. The left sidebar lists various management categories like Overview, Activity log, and Cost Management. The 'Access control (IAM)' section is selected. The main content area has a header 'Check access' with tabs for 'Role assignments', 'Deny assignments', 'Classic administrators', and 'Roles'. Below this, there's a search bar for 'Find' (set to 'Azure AD user, group, or service principal') and a search input field. To the right, three cards provide options: 'Add a role assignment' (with a 'Add' button), 'View role assignments' (with a 'View' button), and 'View deny assignments' (with a 'View' button). The entire interface is titled 'az300-vault - Access control (IAM)' at the top left.

FIGURA 2-75 Compruebe el acceso a los recursos de Azure

4. Antes de crear un rol personalizado, es una buena idea verificar el acceso del usuario o grupo que incluirá el rol personalizado. Además de determinar la necesidad de un rol personalizado, esta verificación ayuda a garantizar que se conozca el acceso existente y que se pueda actualizar después de que se creen los roles personalizados.

5. En la hoja de **IAM**, seleccione **Roles** en la parte superior derecha para ver una lista del acceso que ya tiene un rol predefinido.

6. Haga clic en un rol que pueda tener algunos de los accesos que necesitará su rol personalizado para revisar sus permisos.

La creación de roles personalizados se realiza a través de la CLI de Azure o Azure PowerShell porque no existe un método basado en el portal para crear roles al momento de escribir este artículo. Para crear un rol personalizado con PowerShell, complete los siguientes pasos:

1. Abra una consola de PowerShell y conéctese a su suscripción de Azure.
2. Use el siguiente comando de PowerShell para recopilar el rol con el que comenzará:

Haga clic aquí para ver la imagen del código

```
$ CustomRole = Get-AZRoleDefinition | donde {$_.name -eq "Máquina virtual Contribuyente"}
```

3. Para ver las acciones que ya tiene este rol, muestre la `Actions` propiedad:

```
$ CustomRole.Actions
```

Para que la creación de roles personalizados sea bastante simple, cree un rol para los operadores de VM que puedan administrar y acceder a las máquinas virtuales. El rol mencionado anteriormente puede administrar pero no acceder a las máquinas. La función de inicio de sesión de administrador de máquina virtual permite iniciar sesión pero no administrar la máquina.

Haga clic aquí para ver la imagen del código

```
$ AdminRole = get-azroledefinition | donde {$_.name -eq "Máquina virtual Administrador Iniciar sesión"}
```

En este punto, la `$CustomRole` variable debe contener un objeto para el rol de Colaborador de la máquina virtual y `$AdminRole` debe contener un objeto para el rol de inicio de sesión del administrador de la máquina virtual.

Como puede ver en la [Figura 2-76](#), las acciones que permiten el acceso a las VM faltan en el rol de colaborador de la máquina virtual.

```

PS C:\> $customRole = Get-AzRoleDefinition | where {$_.name -eq "Virtual Machine Contributor"}
PS C:\> $customRole.actions
Microsoft.Authorization/*/read
Microsoft.Compute/availabilitySets/*
Microsoft.Compute/locations/*
Microsoft.Compute/virtualMachines/*
Microsoft.Compute/virtualMachineScaleSets/*
Microsoft.DevTestLab/schedules/*
Microsoft.Insights/alertRules/*
Microsoft.Network/applicationGateways/backendsAddressPools/join/action
Microsoft.Network/loadBalancers/backendsAddressPools/join/action
Microsoft.Network/networkInterfaces/inboundNatPools/join/action
Microsoft.Network/loadBalancers/inboundNatRules/join/action
Microsoft.Network/loadBalancers/probes/join/action
Microsoft.Network/loadBalancers/read
Microsoft.Network/locations/*
Microsoft.Network/networkInterfaces/*
Microsoft.Network/networkSecurityGroups/join/action
Microsoft.Network/publicIPAddresses/read
Microsoft.Network/publicIPAddresses/join/action
Microsoft.Network/publicIPAddresses/read
Microsoft.Network/virtualInterfaces/read
Microsoft.Network/virtualNetworks/read
Microsoft.Network/virtualNetworks/subnets/join/action
Microsoft.RecoveryServices/vaults/backupFabrics/backupProtectionItem/write
Microsoft.RecoveryServices/vaults/backupFabrics/protectedContainers/protectedItems/*/read
Microsoft.RecoveryServices/vaults/backupFabrics/protectedContainers/protectedItems/read
Microsoft.RecoveryServices/vaults/backupFabrics/protectedContainers/protectedItems/write
Microsoft.RecoveryServices/vaults/backupPolicies/read
Microsoft.RecoveryServices/vaults/backupPolicies/write
Microsoft.RecoveryServices/vaults/read
Microsoft.RecoveryServices/vaults/usages/read
Microsoft.Resources/deletedAvailabilityStatuses/read
Microsoft.Resources/deployments/*
Microsoft.Resources/subscriptions/resourceGroups/read
Microsoft.SqlVirtualMachine/*
Microsoft.Storage/storageAccounts/listKeys/action
Microsoft.Storage/storageAccounts/read
Microsoft.Support/*
PS C:\>

```

FIGURA 2-76 Permisos faltantes entre roles integrados

4. Para completar la función personalizada, agregue el permiso de administrador que falta al objeto \$ customRole:

[Haga clic aquí para ver la imagen del código](#)

```

$ customRole = get-azroledefinition | donde {$_.name
-eq "Máquina virtual
Colaborador "}

$ customRole.id = $ null

$ customRole.name = "Personalizado - Administrador de
máquina virtual"

$ Customrole.Description = "Puede administrar y
acceder a máquinas virtuales"

$ customRole.Actions.Add ("Microsoft.Compute /
VirtualMachines / * / read")

$ customRole.AssignableScopes.Clear ()

$ CustomRole.AssignableScopes = "/ subscriptions / <id
de su suscripción> /
resourceGroups / <Grupo de recursos para el rol> "

New-AzRoleDefinition -role $ CustomRole

```

Esto creará un rol personalizado llamado Personalizado: Administrador de máquina virtual y asignará todos los roles del Rol de colaborador de

máquina virtual más la capacidad de iniciar sesión en Azure Virtual Machines.

El rol tendrá como alcance el ID de recurso proporcionado para el grupo de recursos elegido. De esta manera, los permisos agregados son aplicables solo a los grupos de recursos que los necesitan, tal vez el grupo de recursos de Servidores.

La Figura 2-77 muestra el resultado del comando para crear este rol personalizado, con información confidencial censurada.

```
PS C:\> $customRole.id = $null
PS C:\> $customRole.name = "Custom - Virtual Machine Administrator"
PS C:\> $customRole.Description = "Can manage and access virtual machines"
PS C:\> $customRole.Actions.Add("Microsoft.Compute/VirtualMachines/*/read")
PS C:\> $customRole.AssignableScopes.Clear()
PS C:\> ##$customRole.AssignableScopes = "/subscriptions/<your subscription id>/resourceGroups/<Resource Group for role>"
PS C:\> $customRole.AssignableScopes = "/subscriptions/38b97161-b529-4733-969d-61f1aeaefac4/resourceGroups/az300-vault"
PS C:\>
PS C:\> New-AzRoleDefinition -role $CustomRole

Name          : Custom - Virtual Machine Administrator
Id            : 0c41319c-7e7b-4ac9-8c4c-010a691a47b2
IsCustom      : True
Description   : Can manage and access virtual machines
Actions       : {Microsoft.Authorization/*/read, Microsoft.Compute/availabilitySets/*, Microsoft.Compute/locations/*,
               Microsoft.Compute/virtualMachines/*...}
NotActions    : {}
DataActions   : {}
NotDataActions: {}
AssignableScopes : {/subscriptions/38b97161-b529-4733-969d-61f1aeaefac4/resourceGroups/az300-vault}

PS C:\>
```

FIGURA 2-77 Rol personalizado recién creado

Configurar el acceso a los recursos asignando roles

Anteriormente, se creaba un rol personalizado para permitir la administración y el acceso a las máquinas virtuales dentro de un grupo de recursos de Azure. Debido a que el rol personalizado se estableció en el nivel del grupo de recursos, solo se podrá asignar a los grupos de recursos.

Para hacer uso del rol personalizado y los roles integrados, los roles deben asignarse a usuarios o grupos, lo que les permite aprovechar estos derechos de acceso.

Para asignar el rol personalizado recién creado a un grupo, complete los siguientes pasos:

1. En Azure Portal, busque el grupo de recursos al que se asignó el rol personalizado.
2. Haga clic en el enlace **Control de acceso (IAM)** en el panel de navegación.
3. Haga clic en **Agregar** y seleccione **Agregar asignación de funciones**.
4. En el cuadro **Seleccionar un rol**, ingrese el nombre del rol personalizado "Personalizado -" y haga clic en el nombre del rol.

Tenga en cuenta la denominación de roles personalizados

Aunque el tipo de roles personalizados se establece en CustomRole cuando se agregan roles, hemos descubierto que anteponer la palabra "Personalizado -" al principio del nombre o seguir un estándar de nomenclatura predefinido por su organización puede hacer que los roles personalizados sean más fáciles de encontrar cuando buscándolos en un momento posterior.

5. El menú desplegable **Asignar acceso a** muestra los tipos de identidades a las que se puede asignar acceso:

1. ■ Usuario, grupo o entidad de servicio de Azure AD
2. ■ Identidad administrada asignada por el usuario
3. ■ Identidad administrada asignada por el sistema
4. ■ Servicio de aplicaciones
5. ■ Instancia de contenedor
6. ■ Aplicación de función
7. ■ Aplicación lógica
8. ■ Máquina virtual
9. ■ Conjunto de escala de máquina virtual

Dado que los administradores de máquinas virtuales suelen ser personas, mantenga seleccionado el usuario, el grupo o la entidad de servicio de Azure AD.

6. En el cuadro **Seleccionar**, ingrese el nombre del usuario o grupo al que se le debe asignar este nuevo rol.

7. Haga clic en el nombre de usuario o grupo resultante para seleccionarlos.

Importante acerca de los grupos

Tenga en cuenta que el uso de un grupo para la asignación de roles requiere un mantenimiento mucho menor que la asignación individual de usuarios a roles.

8. Haga clic en **Guardar** para completar la asignación de funciones.

Al usuario (o usuarios si se asignó un grupo) se le asignó un nuevo acceso y es posible que deba cerrar sesión en el portal o PowerShell y volver a iniciar sesión o volver a conectarse para ver los nuevos derechos de acceso.

Configurar el acceso de administración a Azure

Al igual que el acceso a los recursos que se ejecutan en Azure, el acceso a la propia plataforma se controla mediante RBAC. Hay algunos roles dedicados a la administración de recursos de Azure a un nivel muy alto: piense en grupos de administración y suscripciones.

Cuando usa roles RBAC, el método para asignar acceso a suscripciones o grupos de administración es el mismo que para otros recursos, pero los roles específicos de administración y dónde están asignados son diferentes. Estos se establecerían a nivel de suscripción o grupo de administración.

Importante acumulativo por defecto

El acceso RBAC es acumulativo de forma predeterminada, lo que significa que el acceso de los contribuyentes a nivel de suscripción lo heredan los grupos de recursos y los recursos alojados dentro de una suscripción. La herencia no es necesaria porque el permiso se puede otorgar en niveles inferiores dentro de una suscripción hasta el nivel de recurso específico. Además, el permiso también se puede denegar a cualquier nivel; al hacerlo, se evita el acceso a los recursos donde se denegó el permiso. Si la denegación de permisos ocurre en un nivel de recurso principal, cualquier recurso debajo del padre heredará la denegación.

Siempre habrá una entidad en Azure que sea el administrador o propietario de la suscripción general. Por lo general, esta es la cuenta que

creó la suscripción, pero puede (y debe) cambiarse a un grupo para garantizar que más de una persona tenga acceso de nivel superior a la suscripción. Además, este cambio tendrá en cuenta los cambios de trabajo, la rotación del personal y reducirá la probabilidad de que alguien se olvide del acceso a Azure durante estas situaciones.

Para configurar el acceso a Azure a nivel de suscripción, complete los siguientes pasos:

1. Inicie sesión en Azure Portal y seleccione **Suscripciones**.
2. Haga clic en la suscripción que desea administrar.
3. Haga clic en el elemento de navegación **Control de acceso (IAM)**.
4. En la hoja de **IAM**, seleccione **Asignaciones de funciones**.

Se muestran los usuarios o grupos que tienen asignados roles específicos. A nivel de suscripción, debería haber pocos roles asignados, como se muestra en la [Figura 2-78](#). La mayor parte del acceso ocurre en el grupo de recursos o en el nivel de recursos.

The screenshot shows the 'Role assignments' tab in the Azure IAM interface. It displays a list of role assignments for a specific scope. The table has columns for NAME, TYPE, ROLE, and SCOPE. The data is categorized into three groups: CONTRIBUTOR, OWNER, and READER.

	NAME	TYPE	ROLE	SCOPE
CONTRIBUTOR	AzureAuto_7q3XcW/kq0. App	App	Contributor	This resource
	OMS-east-testing_sNVw. App	App	Contributor	This resource
	Site-reco-asr-automatior App	App	Contributor	This resource
OWNER	DerekAdmin derek@*****.onmicrosoft.com	User	Owner	This resource
READER	CloudynAzureCollector App	App	Reader	This resource

FIGURA 2-78 Roles asignados a nivel de suscripción

5. Haga clic en **Agregar** en la parte superior de la hoja de **IAM**.
6. Seleccione **Agregar asignación de rol**.
7. Elija el **rol de propietario**.
8. Deje el menú desplegable **Asignar acceso a** configurado en **Usuario, grupo o entidad de servicio de Azure AD**.
9. Seleccione un grupo para asignar al rol de propietario buscando el grupo y luego haciendo clic en él en los resultados.
10. Hacer clic **Guardar**.

El grupo tiene acceso de propietario a nivel de suscripción. Este acceso permite a los miembros del grupo crear, modificar y eliminar cualquier recurso dentro de la suscripción seleccionada.

Nota Agregar un coadministrador

Esto solo es necesario si se utilizan implementaciones clásicas (el portal clásico). La asignación de derechos de propietario RBAC en el portal de administración de recursos logra el mismo resultado.

Solucionar problemas de RBAC

Identificar la causa de los problemas con RBAC puede requerir un poco de investigación para comprender por qué un usuario no puede realizar una acción. Cuando asigne acceso a través de RBAC, asegúrese de mantener un grupo de usuarios configurado para el acceso de propietario. Además de un grupo, considere habilitar un usuario solo en línea como propietario. De esta forma, si hay un problema con Active Directory, no todas las cuentas de usuario no podrán acceder a Azure.

Dado que el control de acceso basado en roles (RBAC) es fundamental para el acceso a los recursos en Azure, usar RBAC con cuidado es fundamental para trabajar con Azure. Al igual que los permisos en Windows antes, Azure RBAC trae una buena cantidad de prueba y error a la mesa al asignar acceso. Además, debido a que Azure está en constante evolución, puede haber ocasiones en las que un permiso simplemente no funcione como se indica.

El panel principal del **IAM** hoja ha mejorado considerablemente en los últimos tiempos al proporcionar una forma rápida de verificar el acceso desde el frente. Si alguien está cuestionando su acceso, un administrador u otro miembro del equipo puede ingresar fácilmente el nombre de usuario o el nombre del grupo donde se está cuestionando el acceso y ver qué asignaciones de roles se encuentran actualmente. Ya no es necesario examinar la lista de asignaciones de funciones para determinar si Fred tiene acceso de colaborador o de espectador al nuevo grupo de recursos. Esta es una de las herramientas clave en la resolución de problemas: poder ver quién tiene qué nivel de acceso.

Durante los momentos en que Fred debería tener acceso a un recurso en particular, pero afirma que no tiene acceso mientras Azure muestra las asignaciones de roles correctas, la pestaña **Roles** en la hoja de **IAM que**

se muestra en la [Figura 2-79](#) puede ayudar a determinar si todos los permisos necesarios están disponibles . A veces no lo serán.

The screenshot shows the 'Check access' blade in the Azure portal. At the top, there are buttons for 'Add', 'Edit columns', 'Refresh', and 'Remove'. Below these are tabs for 'Check access', 'Role assignments', 'Deny assignments', 'Classic administrators', and 'Roles'. The 'Roles' tab is selected. A note below the tabs states: 'A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more'.

Name	Type	Users	Groups	...
Owner	BuiltinRole	1	0	...
Contributor	BuiltinRole	4	0	...
Reader	BuiltinRole	1	0	...
AcrDelete	BuiltinRole	0	0	...
AcrImageSigner	BuiltinRole	0	0	...
AcrPull	BuiltinRole	0	0	...
AcrPush	BuiltinRole	0	0	...
AcrQuarantineReader	BuiltinRole	0	0	...
AcrQuarantineWriter	BuiltinRole	0	0	...
API Management Service Contributor	BuiltinRole	0	0	...
API Management Service Operator Role	BuiltinRole	0	0	...
API Management Service Reader Role	BuiltinRole	0	0	...

FIGURA 2-79 Revisión de asignaciones de roles para grupos y usuarios

Mirar la lista de roles es solo algo útil. Si Fred afirma que no puede leer un recurso, pero figura en la lista con el rol de lector del recurso, es probable que haya algo detrás del rol. Para ver los permisos asignados al rol listado, haga clic en el nombre del rol.

En la parte superior de la página de asignaciones enumeradas para el rol, haga clic en **Permisos** para ver la lista de permisos que componen el rol.

Verá, como se muestra en la [Figura 2-80](#), la lista de proveedores de recursos que cumple el rol y si tienen acceso parcial o total al proveedor, así como qué acceso a datos para un proveedor tiene el rol.

Permissions (preview)		
Reader	MANAGEMENT	DATA
RESOURCE PROVIDER		
84codes.CloudAMQP	Partial	--
Azure Data Box	Partial	--
Azure Database Migration Service	Partial	--
Azure IoT Central	Partial	--
Azure Log Analytics	Partial	--
Azure Stack Resource Provider	Partial	--
Bot Service Resource Provider	Partial	--
CloudSimple Private Cloud IaaS	Partial	--
Cnexlink MyCloudIT	Partial	--
Crypteron DataSecurity	Partial	--
Domain Services Resource Provider	Partial	--
FriendlyRpNamespace	Partial	--
LiveArena.Broadcast	Partial	--
Machine Learning Services Resource Provider	Partial	None

FIGURA 2-80 Permisos del proveedor de recursos dentro de un rol

Al seleccionar un nombre de proveedor en esta vista, se muestran los componentes que usa este rol dentro de un proveedor determinado y los permisos asignados, como se muestra para el proveedor de Azure Data Box en la [Figura 2-81](#).

Azure Data Box Permissions - Reader (Preview)			
RESOURCE TYPE (MANAGEMENT)	READ	WRITE	DELETE
▼ Azure Data Box			
Orders	✓		
Validate Address			
Operation Results	✓		

FIGURA 2-81 Permisos dentro del rol de lector para Azure Data Box

Además de investigar qué permisos se asignan con ciertos roles, cambiar los roles para ciertos usuarios o grupos para ver cómo cambia el acceso es otro método que es útil para resolver los problemas de acceso.

También puede haber ocasiones en las que los cambios en RBAC se almacenan en caché, cuando los cambios de configuración simplemente no aparecen una vez realizados. En Azure Portal, los cambios realizados pueden tardar hasta 30 minutos en reflejarse. En la CLI de Azure o una consola de PowerShell, el proceso de cerrar sesión y volver a iniciar sesión forzará la actualización de la configuración al realizar cambios en RBAC. De manera similar, cuando se utilizan las API de Rest para

administrar los permisos, la actualización del token de acceso actual actualizará los permisos.

También hay ocasiones en las que ciertos recursos pueden requerir permisos superiores a los establecidos; por ejemplo, trabajar en un servicio de aplicaciones puede requerir permiso de escritura en la cuenta de almacenamiento subyacente para garantizar que la supervisión del rendimiento sea visible; de lo contrario, devuelve un error. En casos como este, quizás el acceso elevado (contribuyente en este caso) podría ser preferible por un tiempo para permitir el monitoreo. De esta manera, los desarrolladores obtienen acceso a los elementos que necesitan, pero tal vez el acceso no permanezca asignado a largo plazo.

RESUMEN DEL CAPÍTULO

- ■ Las máquinas virtuales de los centros de datos locales u otros entornos en la nube, así como los servidores físicos, se pueden migrar a Azure.
- ■ Azure Bastion elimina la necesidad de recursos de IaaS dedicados que se utilizan para administrar máquinas dentro de una red virtual. Además, dado que Bastion es una oferta de plataforma como servicio, el usuario no debe realizar parches ni actualizaciones.
- ■ El equilibrio de carga de la aplicación y el equilibrio de carga de la red funcionan en conjunto para garantizar una solución completa.
- ■ Los recursos de plataforma como servicio y computación sin servidor trasladan la administración de la infraestructura más al proveedor de la nube que tener todos los recursos administrados por el personal de TI de una organización. Esto puede ahorrar dinero a largo plazo.
- ■ Azure Traffic Manager se puede usar para enrutar el tráfico entre regiones para ayudar a mejorar la alta disponibilidad de los recursos que se ejecutan en Azure y en otros lugares.
- ■ Logic Apps realiza integraciones personalizadas entre aplicaciones y servicios tanto dentro como fuera de Azure.

- El emparejamiento de redes virtuales permite la comunicación entre redes en Azure sin necesidad de una VPN, mientras que las VPN de sitio a sitio conectan Azure a redes locales existentes y ExpressRoute proporciona conexiones completamente privadas a los servicios de Microsoft desde un entorno local.
- Azure Firewall es una solución de firewall nativa de la nube que existe actualmente por red virtual. Las políticas de firewall se pueden enviar a varias instancias de Azure Firewall para una configuración más uniforme.
- El control de acceso basado en roles alinea el acceso de los usuarios a los recursos de Azure más estrechamente con los roles de trabajo. Tenga en cuenta que esta alineación no siempre es perfecta y que pueden ser necesarios varios roles para proporcionar el acceso correcto.
- Las políticas en Azure ayudan a garantizar que los recursos puedan ser auditados para el cumplimiento y la implementación controlada según lo requiera la organización.
- Managed Identity Services permitirá que las aplicaciones se registren en Azure Active Directory. El uso de tokens completamente administrados para estas aplicaciones mantiene las credenciales fuera del código de la aplicación y brinda acceso sin problemas a otros recursos de Azure.
- Azure Key Vault permite el acceso administrado a la identidad para un acceso seguro a secretos, claves y certificados con muy poca sobrecarga.
- Azure Blueprint proporciona la creación de recursos completamente basada en plantillas, incluida la política y el acceso basado en roles a los nuevos recursos. Aprovechar estos para una implementación repetible puede mejorar la velocidad y la eficiencia de la implementación.

EXPERIMENTO MENTAL

En este experimento mental, demuestre sus habilidades y conocimiento de los temas cubiertos en este capítulo. Puede encontrar las respuestas a las preguntas de los experimentos mentales en la siguiente sección.

Usted es un arquitecto de Azure contratado por Fabrikam para ayudarlos a configurar las redes de Azure y el acceso a los recursos dentro de su entorno mientras se mueven de un centro de datos local a Azure.

Las reuniones han sido productivas en su mayor parte al revisar lo que tienen en Azure hoy, pero al investigar el entorno, hace las siguientes recomendaciones / requisitos:

Las conexiones entre redes virtuales están incurriendo en un costo significativo: esto debería reducirse si es posible.

Las cargas de trabajo de IaaS en Azure tienen acceso abierto a RDP para permitir el mantenimiento y están expuestas a Internet en direcciones IP públicas. Para mejorar la seguridad, la IP pública debe eliminarse sin dejar de permitir el acceso para la administración del servidor.

Otros miembros de la organización han solicitado una aplicación web para problemas de alta disponibilidad. Esto es algo que debe hacerse lo antes posible; en este momento, no hay necesidad de preocuparse por las fronteras regionales.

Teniendo en cuenta los requisitos descubiertos, responda las siguientes preguntas:

1. 1. ¿Cómo reduciría el costo de las conexiones de red virtual dentro de Azure?
2. 2. ¿Qué soluciones de Azure podrían permitirle eliminar direcciones IP públicas de máquinas virtuales y seguir accediendo a ellas para tareas de administración?
3. 3. ¿Qué podría utilizar para asegurarse de que la aplicación web se transfiera a otro sitio en caso de una interrupción?

RESPUESTAS DEL EXPERIMENTO MENTAL

Esta sección contiene la solución al experimento mental de este capítulo. Tenga en cuenta que puede haber otras formas de lograr el resultado deseado. Cada respuesta explica por qué la respuesta es correcta.

1. 1. Las conexiones entre redes virtuales en Azure se pueden realizar mediante VNet Peering. La creación de dos pares unidireccionales entre dos redes virtuales debería reducir el costo de las conexiones

porque no es necesario pagar por los recursos de puerta de enlace de red virtual en cada red virtual. Dado que los pares también pueden cruzar los límites de las regiones, también mantendrán conexiones entre las regiones.

2. Las direcciones IP públicas pueden ser un recurso necesario para garantizar que sus clientes puedan acceder a sus aplicaciones. Hay varias soluciones posibles aquí, dado que el requisito es el acceso de administración a los servidores y no las direcciones IP públicas, el método con menos gastos generales sería configurar Azure Bastion en la red virtual que aloja los servidores y usarlo para el acceso. De esta forma se podrían eliminar las direcciones IP públicas. Si los servidores están unidos a un dominio de Active Directory y están disponibles a través de una VPN de sitio a sitio, RDP seguirá funcionando y no se necesitará una IP pública.
3. Asegurar una alta disponibilidad para las aplicaciones web también puede tomar múltiples caminos. Aprovechar una puerta de enlace de aplicaciones proporcionaría un punto final público regional al que sus clientes podrían acceder. Esto también enviaría el tráfico entrante a uno o varios recursos de backend para proporcionar alta disponibilidad en caso de que un recurso no esté disponible o necesite mantenimiento. Para trabajar en todas las regiones, se necesitaría una configuración duplicada para Application Gateway y cualquier servicio de aplicación necesario. Luego, se implementaría un administrador de tráfico frente a las puertas de enlace de aplicaciones para dirigir el tráfico entrante basado en DNS a la puerta de enlace de aplicaciones deseada

Capítulo 3

Implementar soluciones para aplicaciones

Azure App Service es una plataforma administrada que se utiliza para crear, implementar y escalar rápidamente aplicaciones web en la nube. App Service admite aplicaciones creadas con marcos comunes como .NET, .NET Core, Node.js, Java, PHP, Ruby o Python. Una de las mayores ventajas de usar App Service es la capacidad de lograr instantáneamente desempeño, seguridad y cumplimiento de nivel empresarial sin tener que preocuparse por el mantenimiento de rutina y las tareas operativas.

En este capítulo, aprenderá a crear e implementar aplicaciones web que se ejecutan en el entorno de Azure App Service y comprenderá los patrones y las prácticas modernas que se utilizan para crear e implementar aplicaciones en contenedores.

Habilidades cubiertas en este capítulo:

- 3.1: Implementar una infraestructura de aplicaciones
- 3.2: Implementar aplicaciones basadas en contenedores

HABILIDAD 3.1: IMPLEMENTAR UNA INFRAESTRUCTURA DE APLICACIONES

Azure App Service le brinda la capacidad de crear y alojar aplicaciones web, backends móviles y API RESTful sin atascarse en las profundidades de la administración de la infraestructura tradicional. Descargar el trabajo pesado del mantenimiento del servidor, la aplicación de parches y las copias de seguridad le brinda la libertad de concentrarse en su aplicación. App Service incluye las mejores prácticas de Microsoft para alta disponibilidad y equilibrio de carga como parte de esta oferta de servicio administrado. Puede habilitar y configurar fácilmente el ajuste de escala automático e implementar aplicaciones basadas en Windows o

Linux desde fuentes de implementación comunes como GitHub, Azure DevOps o cualquier repositorio de Git local.

Esta habilidad cubre cómo:

- Crear y configurar Azure App Service
- Crear una aplicación web de App Service para contenedores.
- Configurar redes para un servicio de aplicaciones
- Crear y administrar ranuras de implementación
- Implementar aplicaciones lógicas
- Implementar funciones de Azure

Crear y configurar Azure App Service

Microsoft ofrece una variedad de métodos para implementar aplicaciones web en Azure App Service. El término *aplicación web* simplemente se refiere a una aplicación administrada que se ejecuta en App Service. Puede usar Azure Portal para crear una aplicación web y también puede usar la CLI de Azure, PowerShell y otras herramientas basadas en IDE, como Visual Studio, que brindan integración con la plataforma Azure.

1. Para crear una aplicación web de Azure App Service, comience por iniciar sesión en Azure Portal y use el siguiente procedimiento:
Navegue hasta el marcador de **App Services** en el lado izquierdo de Azure Portal.
2. Haga clic en **Agregar** para crear una nueva aplicación web.
3. En la pantalla de la **aplicación web** (consulte la Figura 3-1), configure las siguientes opciones y luego haga clic en **Revisar y crear** :
 1. ■ **Suscripción.** Seleccione la suscripción adecuada para el recurso de la aplicación web. Puede tener diferentes suscripciones en su empresa que estén dedicadas a entornos de desarrollo o producción o que estén dedicadas para que las utilicen equipos específicos de su organización.
 2. ■ **Grupo de recursos.** Seleccione un grupo de recursos nuevo o existente donde residirá la aplicación web. Recuerde que puede implementar varios recursos en

un grupo y delegar el control de acceso al nivel del grupo de recursos si es necesario.

3. ■ **Nombre.** Ingrese un nombre de host único a nivel mundial para su aplicación web en *azurewebsites.net*. Esto puede requerir varios intentos porque ya se están usando muchos nombres de host. Ingrese el nombre de su aplicación web en minúsculas. Debe tener entre 3 y 24 caracteres.

4. ■ **Publicar.** Seleccione **Código** como la opción **Publicar**, a menos que esté implementando una aplicación web empaquetada en una imagen de contenedor de Docker.

5. ■ **Pila de tiempo de ejecución.** Seleccione la pila de tiempo de ejecución adecuada para su aplicación. Se admiten varios tiempos de ejecución en App Service, incluidos .NET Core, ASP.NET, Java, Node y Python.

6. ■ **Región.** Elija la región adecuada para alojar su aplicación web. Tenga en cuenta que la proximidad entre los usuarios y la infraestructura de la aplicación puede ser muy sensible, según el tipo de aplicación web que esté implementando. Es una práctica común alojar recursos en la nube en las regiones más cercanas a los usuarios.

7. ■ **Plan de servicio de aplicaciones.** Seleccione un plan de servicio de aplicaciones nuevo o existente, que es la infraestructura administrada que aloja sus aplicaciones web. Hay varios niveles de precios disponibles que brindan todo, desde capacidades básicas hasta capacidades muy avanzadas. El plan Standard S1 es el nivel de precio mínimo recomendado para las aplicaciones web de producción.

Home > App Services > Web App

Web App

Create

* Basics * Monitoring Tags Review and create

App Service Web Apps lets you quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. Meet rigorous performance, scalability, security and compliance requirements while using a fully managed platform to perform infrastructure maintenance. [Learn more](#)

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription [?](#) Microsoft Partner Network

* Resource Group [?](#) (New) MyWebApps

Create new

Instance Details

* Name mywebapp943 .azurewebsites.net

* Publish [Code](#) Docker Image

* Runtime stack .NET Core 2.2

* Operating System Linux Windows

* Region Central US

App Service Plan

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. [Learn more](#)

* Windows Plan (Central US) [?](#) (New) ASP-MyWebApps-9ba0

Create new

* Sku and size Standard S1
100 total ACU, 1.75 GB memory [Change size](#)

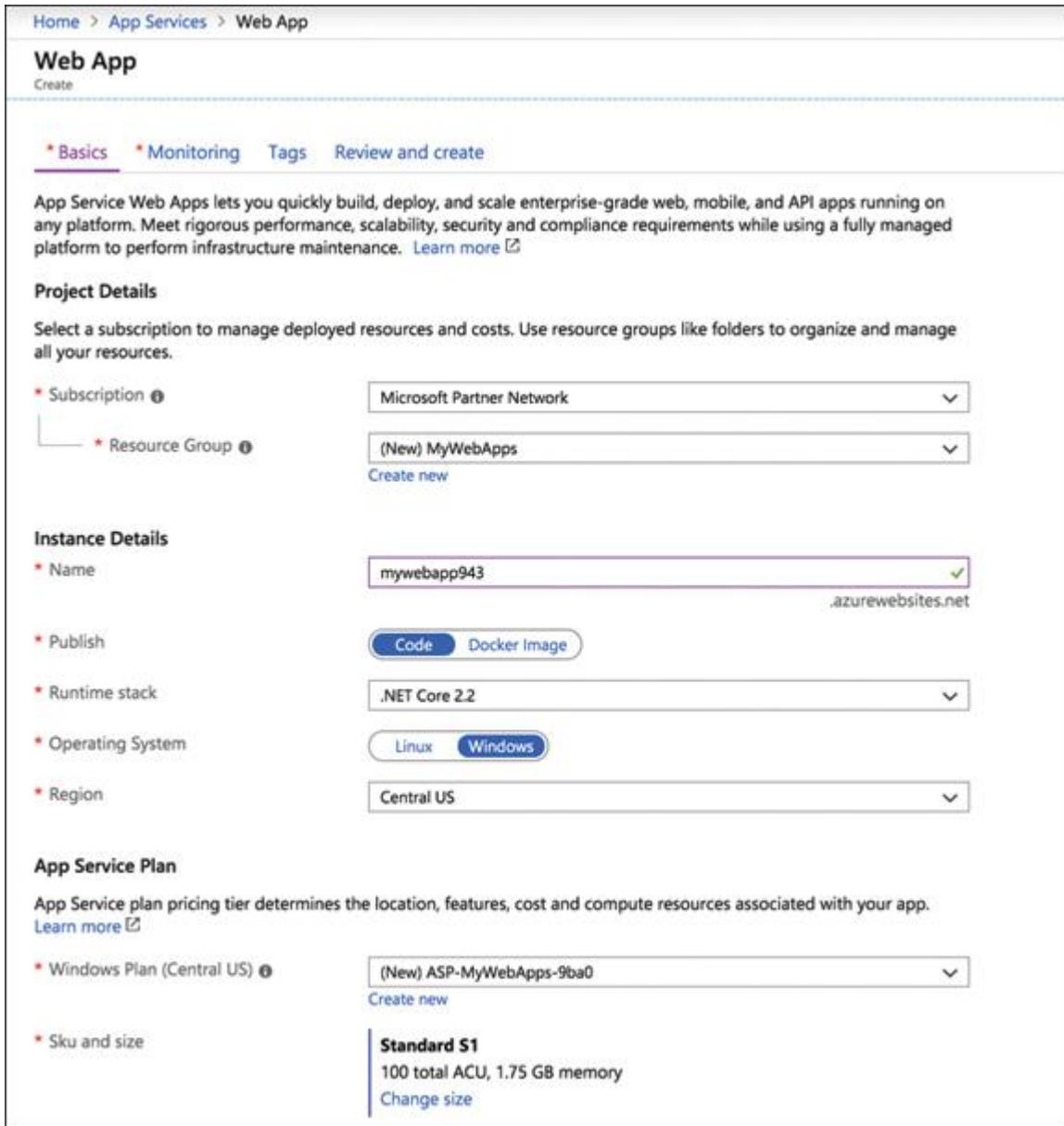


FIGURA 3-1 Creación de una aplicación web de App Service



Sugerencia para el examen

También puede utilizar la línea de comandos para implementar sus aplicaciones web. Por ejemplo, use el comando `az webapp create` con la CLI de Azure para realizar esta tarea desde su terminal local o instancia de Azure Cloud Shell.

Crear una aplicación web de App Service para contenedores

La facilidad de Azure App Service hace que la implementación de aplicaciones web basadas en contenedores de Windows o Linux sea un proceso simple. Puede extraer imágenes de contenedor de Docker alojadas en Docker Hub o usar su propio Azure Container Registry privado. Uno de los mayores beneficios de este enfoque es que puede incluir todas las dependencias que necesita para su aplicación dentro de las imágenes de su contenedor. Microsoft se encargará del parcheo, la alta disponibilidad y el equilibrio de carga que alimenta la infraestructura subyacente.

La creación de una aplicación web para contenedores es un proceso similar a la creación de una aplicación web estándar. Use el siguiente procedimiento en Azure Portal para crear una aplicación web en contenedores en App Services:



Sugerencia para el examen

Azure PowerShell es una alternativa de línea de comandos común que se usa para implementar aplicaciones web. Puede usar el cmdlet New-AzWebApp para crear un script para la implementación de aplicaciones web estándar o en contenedores en App Service.

1. Navegue hasta el marcador de **App Services** en el lado izquierdo de Azure Portal.
2. Haga clic en **Agregar** para crear una nueva aplicación web.
3. Proporcione todos los detalles necesarios para su aplicación web y asegúrese de configurar la opción **Publicar en Imagen de Docker** ; luego haga clic en **Siguiente** .
4. Ingrese los siguientes detalles para la imagen de su contenedor Docker, como se muestra en la Figura 3-2 , y luego haga clic en **Revisar y crear** :
 1. ■ **Opciones.** Seleccionar **contenedor único** es la opción más común. La compatibilidad con varios contenedores con Docker Compose está actualmente prevista para una versión futura.

2. ■ **Fuente de imagen.** Docker Hub es el registro de contenedores predeterminado para imágenes públicas. También puede seleccionar su propio registro privado o un recurso de Azure Container Registry.
3. ■ **Tipo de acceso.** Las imágenes públicas son el tipo de acceso predeterminado para Docker Hub; sin embargo, las imágenes privadas también son compatibles con las aplicaciones web de App Service. Si selecciona **Privado** para su tipo de acceso, se le pedirá que ingrese sus credenciales de registro.
4. ■ **Imagen y etiqueta.** Ingrese el nombre de la imagen de su contenedor y la etiqueta correspondiente (opcional).
5. ■ **Comando de inicio.** Se admiten scripts o comandos de inicio opcionales. Esto suele ser innecesario porque las imágenes de contenedor se pueden crear para usar un comando de inicio específico de forma predeterminada.

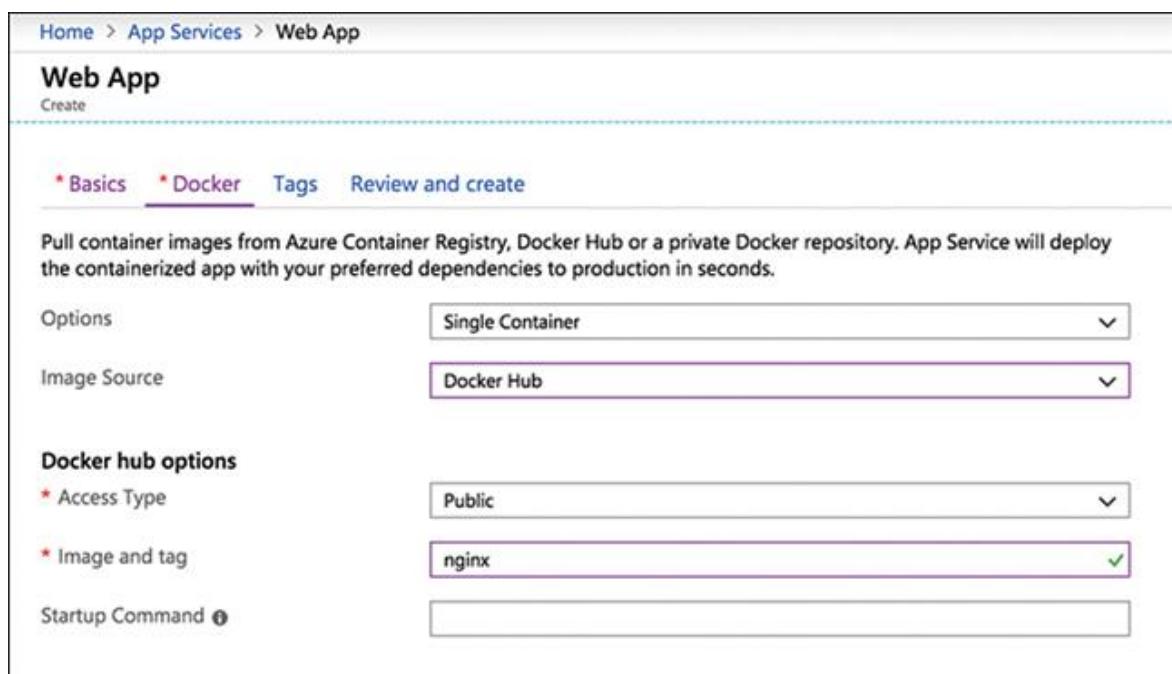


FIGURA 3-2 Configuración de la imagen de Docker

¿Necesita más revisión? Descripción general del servicio de aplicaciones

Para revisar más detalles sobre Azure App Service, consulte la documentación de Microsoft Azure en <https://docs.microsoft.com/en-us/azure/app-service/overview> .

Configurar redes para un servicio de aplicaciones

Las redes virtuales de Azure (VNets) le permiten colocar muchos recursos de Azure en una red virtual privada y completamente aislada que se usa para alojar máquinas virtuales, equilibradores de carga y más. Azure App Service proporciona una característica de integración de VNet que permite que sus aplicaciones accedan a recursos dentro de una VNet.

Por ejemplo, imagine que aloja una base de datos de Microsoft SQL en una máquina virtual de Azure. Puede usar la integración de VNet para permitir que su App Service se comunique con el servidor SQL, sin enviar ese tráfico a través de la Internet pública.

Es importante tener en cuenta que la funcionalidad de integración de VNet es un mecanismo que permite que sus aplicaciones accedan a recursos de red aislados. No coloca el servicio de aplicaciones dentro de la red virtual.

Si desea hacer cumplir el acceso a la red privada para sus aplicaciones de App Service, entonces debe elegir el plan de servicio App Service Environments (ASE) que ofrece redes totalmente aisladas y dedicadas para App Service. ASE coloca sus recursos de App Service dentro de su Azure VNet.

Si no está utilizando ASE, puede seguir el proceso para otorgar acceso a sus servicios de aplicaciones a los recursos de su red virtual mediante el siguiente procedimiento:

1. Vaya a la **interfaz de usuario de redes** en el portal de **App Service** . En **Integración de VNet** , seleccione **Haga clic aquí para configurar** .
2. Seleccione **Agregar red virtual** , como se muestra en la Figura 3-3 .

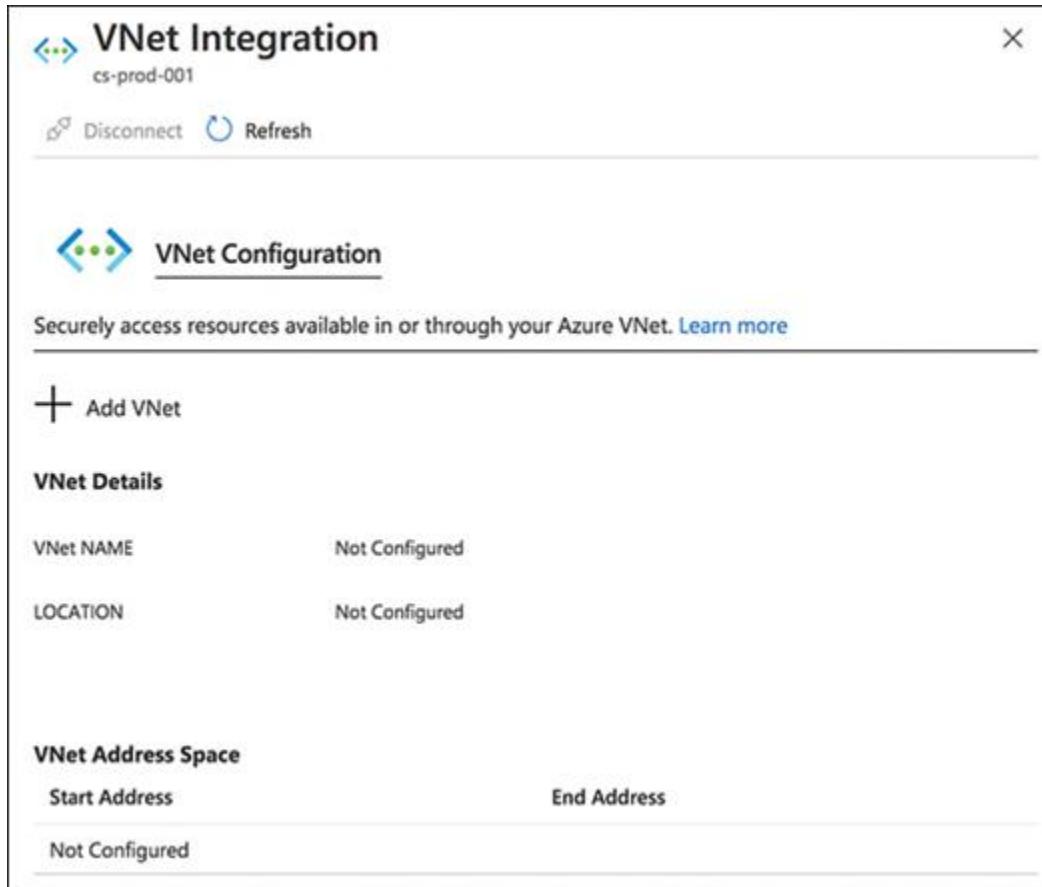


FIGURA 3-3 Habilitación de la integración de redes virtuales en App Service

3. El menú desplegable **Red virtual** contiene todas las redes virtuales de Azure Resource Manager en su suscripción en la misma región. Seleccione la red virtual con la que desea integrarse, como se muestra en la Figura 3-4 .

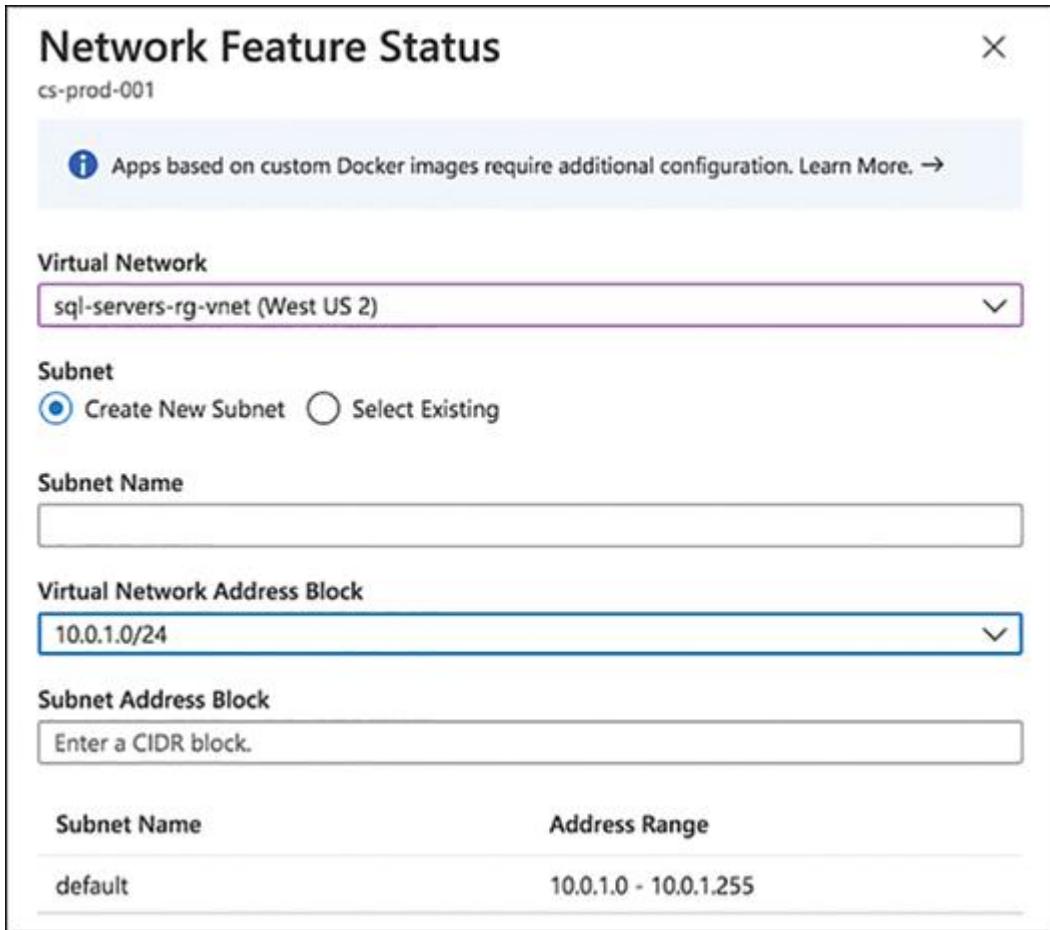


FIGURA 3-4 Selección de una red virtual y una subred para la integración de la red virtual de App Service

Crear y administrar ranuras de implementación

Los servicios de aplicaciones de Azure que se ejecutan en los niveles del plan de servicio de aplicaciones estándar, premium o aislado admiten el concepto de ranuras de implementación, que le permiten ejecutar diferentes aplicaciones en vivo con sus propios nombres de host. Las ranuras de implementación se utilizan generalmente para preparar nuevas versiones de su aplicación y, en última instancia, intercambiar nuevas versiones en producción.

Cada nivel del plan de App Service de nivel de producción admite una cantidad diferente de ranuras de implementación. Siempre hay un espacio de producción implícito.

La implementación de su aplicación en una ranura que no es de producción le permite validar los cambios de la aplicación en una ranura de prueba antes de cambiarla a una ranura de producción.

Utilice el siguiente procedimiento para agregar una ranura e intercambiar el código en su entorno de producción:

1. Vaya a las propiedades de una aplicación web existente en Azure Portal.
2. Desplácese hacia abajo en el lado izquierdo y seleccione **Deployment Slots**.
3. Despues de hacer clic en el botón **Agregar ranura**, asigne un nombre a la ranura y elija la configuración de clonación predeterminada en el menú **Configuración de clonación desde**, como se muestra en la Figura 3-5. Luego, puede implementar nuevas versiones de su aplicación en esta nueva ranura.



FIGURA 3-5 Creación de una ranura de implementación del servicio de aplicaciones

4. Finalmente, puede traer una nueva versión de su aplicación a producción, como se muestra en la Figura 3-6 .

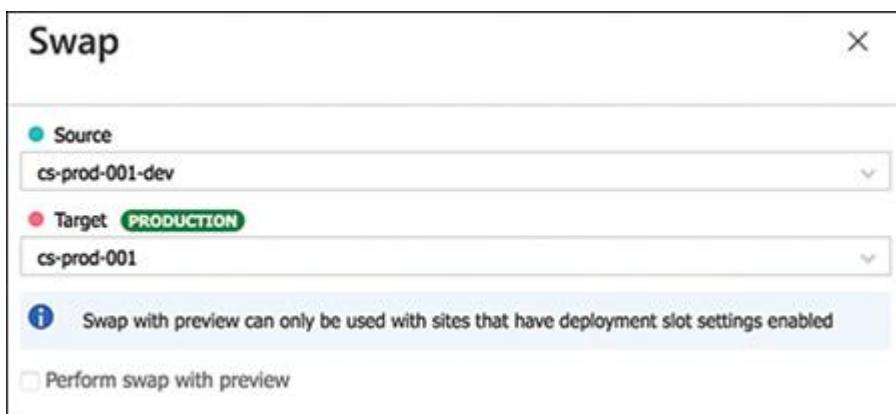


FIGURA 3-6 Creación de una ranura de implementación de App Service

Cuando intercambia dos ranuras (generalmente de una ranura de ensayo a la ranura de producción), App Service garantiza que la ranura de destino no experimente tiempo de inactividad.

Implementar aplicaciones lógicas

Azure Logic Apps lo ayuda a programar, automatizar y organizar tareas, procesos comerciales y flujos de trabajo. Puede utilizar Logic Apps para integrar aplicaciones, datos, sistemas y servicios en empresas u organizaciones.

Cada flujo de trabajo de una aplicación lógica comienza con un disparador, que se activa cuando ocurre un evento específico. Cada vez que se activa el desencadenador, el motor de Logic Apps crea una instancia de aplicación lógica que ejecuta las acciones en el flujo de trabajo. Estas acciones también pueden incluir conversiones de datos y controles de flujo de trabajo, como declaraciones condicionales, declaraciones de cambio, bucles y ramificaciones.

Por ejemplo, puede usar Logic Apps para enviar notificaciones por correo electrónico con Office 365 cuando los eventos tienen lugar en diferentes aplicaciones y servicios. O puede mover archivos cargados a través de SFTP a Azure Storage. Otro patrón de flujo de trabajo común sería monitorear las redes sociales para analizar el sentimiento de los tweets y crear alertas o tareas para los elementos que deben revisarse.

Complete los siguientes pasos para crear su primera aplicación Azure Logic:

1. En Azure Portal, en el cuadro de búsqueda, busque y seleccione **Logic Apps**.
2. En la página **Logic Apps**, seleccione **Agregar**.
3. En el panel **Aplicación lógica**, proporcione detalles sobre su aplicación lógica. Una vez que haya terminado, seleccione **Crear**.
4. Despues de que Azure implemente su aplicación, en la barra de herramientas de Azure, seleccione **Notificaciones > Ir al recurso** para su aplicación lógica implementada.
5. El Diseñador de aplicaciones lógicas se abre y muestra una página con un video de introducción y activadores de uso

común. En **Plantillas**, seleccione **Aplicación lógica en blanco**. Esto lo llevará a un lienzo en blanco en el diseñador de aplicaciones lógicas, como se muestra en la Figura 3-7.

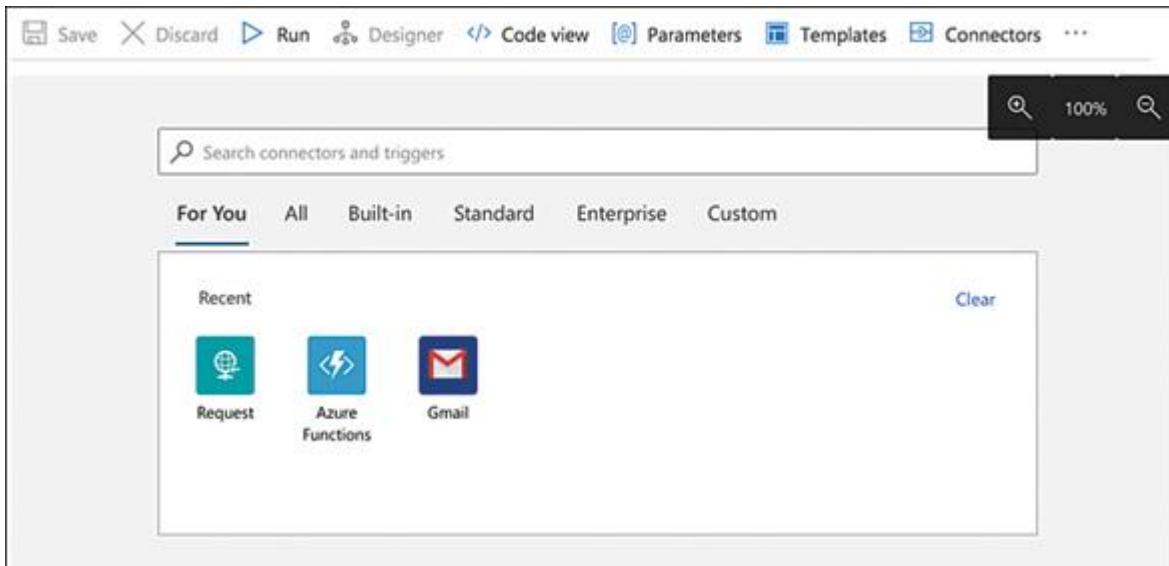


FIGURA 3-7 Creación de una aplicación lógica en blanco



Sugerencia para el examen

Asegúrese de comprender el proceso para crear una aplicación lógica en blanco, junto con cómo crear un disparador y una acción para una aplicación lógica, como enviar nuevos elementos RSS por correo electrónico.

Una vez que tenga una aplicación lógica en blanco, cree un disparador y una acción mediante el siguiente proceso. Este ejemplo explica cómo enviar nuevos elementos de fuente RSS por correo electrónico:

6. Con el diseñador de aplicaciones lógicas, dentro del cuadro de búsqueda, ingrese **rss** para encontrar el conector RSS. En la lista **Desencadenadores**, seleccione el **desencadenador Cuando se publica un elemento de noticias en tiempo real**.
7. Proporcione la **URL de la fuente RSS** y defina la frecuencia con la que desea buscar nuevos elementos estableciendo un valor en **¿Con qué frecuencia desea verificar los elementos?**, como se muestra en la Figura 3-8.

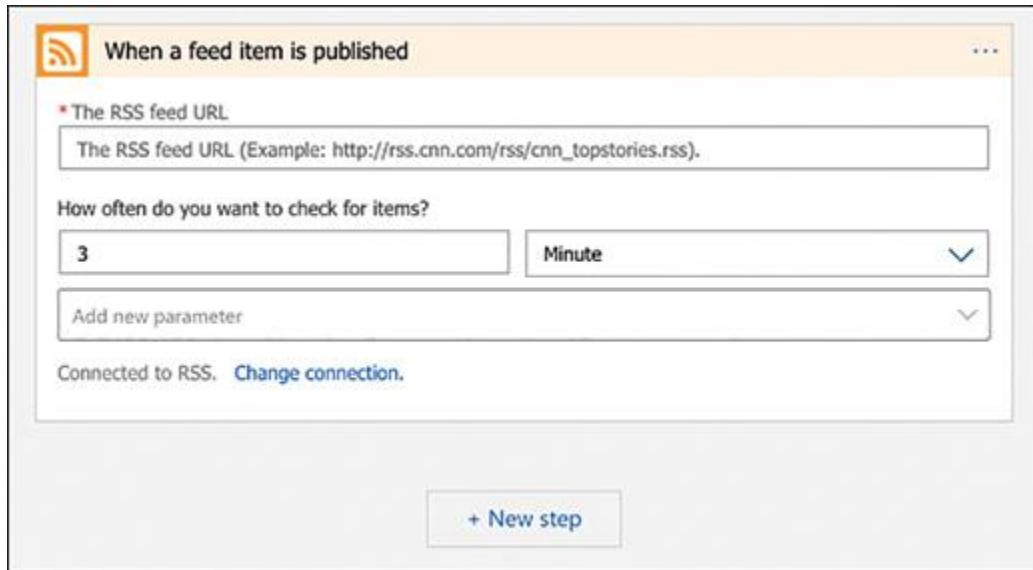


FIGURA 3-8 Creación de un disparador RSS para una aplicación lógica

8. Ahora agregue una acción que envíe un correo electrónico cuando aparezca un nuevo elemento en la fuente RSS. En el desencadenador **Cuando se publica un elemento de feed**, seleccione **Nuevo paso**.
9. En **Elija una acción** y el cuadro de búsqueda, seleccione **Todo**.
10. En el cuadro de búsqueda, ingrese enviar un correo electrónico para buscar conectores que ofrezcan esta acción. En la lista **Acciones**, seleccione la acción **Enviar un correo electrónico** para el servicio de correo electrónico que desea utilizar, como se muestra en la Figura 3-9 .

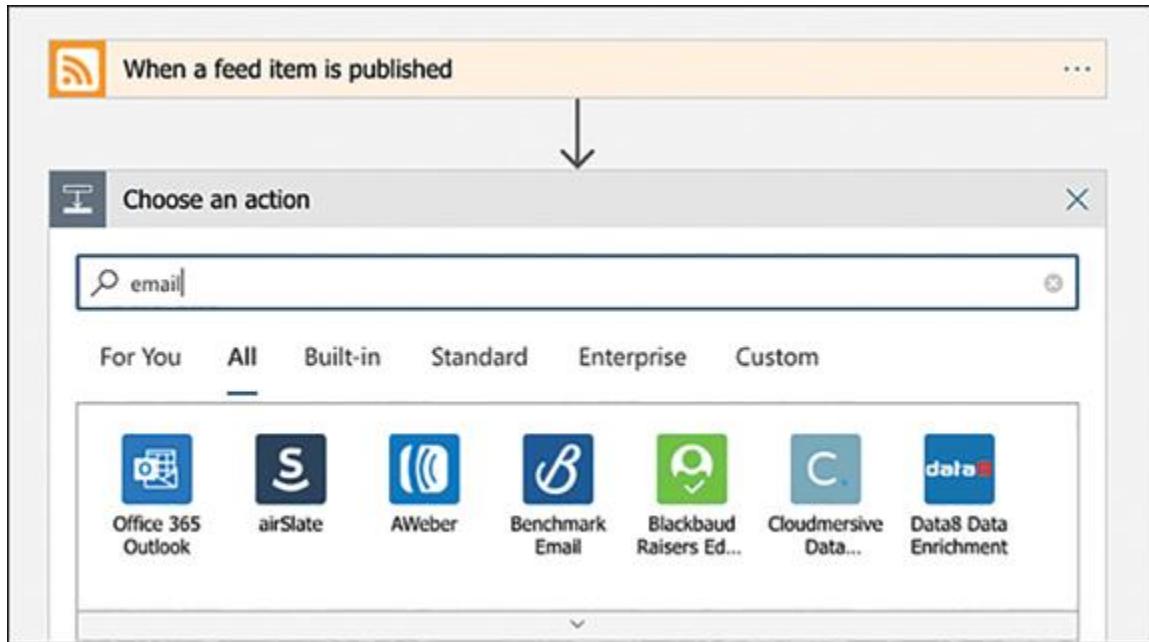


FIGURA 3-9 Creación de una acción de correo electrónico para una aplicación lógica

11. Si el conector de correo electrónico seleccionado le solicita que autentique su identidad, complete ese paso ahora para crear una conexión entre su aplicación lógica y su servicio de correo electrónico.
12. Guarde su aplicación lógica. Para iniciar manualmente su aplicación lógica, en la barra de la barra de herramientas del diseñador, seleccione **Ejecutar**.

Inicio rápido de *Note Logic Apps*

Aprenda a crear su primer flujo de trabajo con Azure Logic Apps, como crear una aplicación lógica en blanco, agregar un disparador y una acción, y luego probar su aplicación lógica en <http://docs.microsoft.com/en-us/azure/logic-apps/quickstart-create-first-logic-app-workflow> .

Implementar funciones de Azure

Azure Functions le permite concentrarse en el código sin preocuparse por la infraestructura de la aplicación. Con Azure Functions, la infraestructura en la nube proporciona el entorno informático que necesita para mantener su aplicación en ejecución a cualquier escala.

Las funciones se "activan" por un tipo específico de evento, que incluye activadores que responden a cambios en los datos, responden a mensajes, se ejecutan en un horario o como resultado de un Solicitud HTTP. La integración con otros servicios se simplifica mediante el uso de enlaces. Los enlaces le brindan acceso declarativo a una amplia variedad de servicios de Azure y de terceros.

Las funciones son una gran solución para procesar datos masivos, integrar sistemas, trabajar con Internet de las cosas (IoT) y crear API y microservicios simples.

Complete los siguientes pasos para crear su primera aplicación de función de Azure y función sin servidor:

1. Vaya a **Aplicación de funciones** en el lado izquierdo de Azure Portal.
2. Haga clic en **Crear aplicación de función**.
3. Complete los campos del formulario para definir el **grupo de recursos**, el **nombre de la aplicación de función** y la **pila de tiempo de ejecución** deseados para su aplicación, como se muestra en la Figura 3-10, y luego haga clic en **Siguiente**. Estos son los marcos de lenguaje disponibles que se pueden usar para desarrollar y ejecutar sus funciones.
 1. ■ .NET Core
 2. ■ Java
 3. ■ Python
 4. ■ PowerShell Core

Function App

Basics Hosting Monitoring Tags Review + create

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Pay-As-You-Go"/>
Resource Group *	<input type="text" value="(New) serverless"/> Create new

Instance Details

Function App name *	<input type="text" value="az303"/> .azurewebsites.net
Publish *	<input checked="" type="radio"/> Code <input type="radio"/> Docker Container
Runtime stack *	<input type="text" value=".NET Core"/>
Version *	<input type="text" value="3.1"/>
Region *	<input type="text" value="Central US"/>

FIGURA 3-10 Creación de una aplicación de función de Azure

4. Seleccione el **tipo de plan** de precios apropiado y haga clic en **Crear** para crear su aplicación de función, como se muestra en la Figura 3-11 . Estas son las opciones de **Tipo de plan** :

0. ■ **Plan de consumo.** Cuando usa el plan de consumo, las instancias del host de Azure Functions se agregan y eliminan dinámicamente según la cantidad de eventos entrantes. Este plan sin servidor se escala automáticamente y solo se le cobra por los recursos informáticos cuando sus funciones están en ejecución. En un plan de consumo, la ejecución de una función expira después de un período de tiempo configurable.

1. ■ **Plan Premium.** Cuando usa el plan Premium, las instancias del host de Azure Functions se agregan y eliminan

según la cantidad de eventos entrantes, al igual que el plan de consumo.

2. ■ **Plan dedicado (servicio de aplicaciones).** Sus aplicaciones de función también pueden ejecutarse en las mismas máquinas virtuales dedicadas que otras aplicaciones de App Service (SKU básicas, estándar, premium y aisladas). Considere un plan de App Service cuando tenga máquinas virtuales infrautilizadas existentes que ya estén ejecutando otras instancias de App Service.

The screenshot shows the 'Hosting' tab selected in the top navigation bar. Under 'Storage', it says: 'When creating a function app, you must create or link to a general-purpose Azure Storage account that supports Blobs, Queue, and Table storage.' A dropdown menu shows '(New) storageaccountserveb2ac' with a 'Create new' button below it. Under 'Operating system', it says: 'The Operating System has been recommended for you based on your selection of runtime stack.' A radio button for 'Windows' is selected. Under 'Plan', it says: 'The plan you choose dictates how your app scales, what features are enabled, and how it is priced.' A dropdown menu shows 'Consumption (Serverless)'.

FIGURA 3-11 Configuración de las opciones de hospedaje de la aplicación de función de Azure



Sugerencia para el examen

Asegúrese de comprender que puede publicar código directamente en una aplicación de función desde herramientas de desarrollo como Visual Studio Code y Visual Studio, o desde sistemas de entrega continua como Azure DevOps.

Después de tener una aplicación de función en funcionamiento, puede completar los siguientes pasos para crear su primera función:

1. Navegue a su aplicación de función en el portal de Azure.

2. Haga clic en **Funciones > Agregar** .
3. Seleccione una plantilla para activar su función. En este ejemplo, seleccionaremos **HTTP Trigger** .

Nota **Plantilla de activador HTTP**

La plantilla HTTP Trigger crea una función que acepta la entrada de una operación de publicación HTTP. La función busca específicamente una clave de "nombre" en la cadena de consulta o en el cuerpo de la solicitud. Este código se puede reemplazar con cualquier lógica que tenga sentido para su aplicación.

4. Asigne un nombre a su función, establezca su nivel de autorización y haga clic en **Crear función** .
5. Haga clic en la opción **Código + Prueba** para abrir el editor de código.
6. Haga clic en **Prueba / Ejecutar** para invocar su función con un parámetro de cadena de consulta para una tecla "Nombre", como se muestra en la Figura 3-12 .

The screenshot shows the 'Input' tab of the Azure Function Test blade. It includes fields for 'HTTP method' (set to POST), 'Key' (set to master (Host key)), and a 'Query' table with a single entry: 'name' with a value of 'AZ303'. A link '+ Add parameter' is visible at the bottom of the table.

FIGURA 3-12 Configuración de entradas de prueba para una función de Azure en el portal

7. Revise la salida en el portal, como se muestra en la Figura 3-13 .



The screenshot shows the Azure portal interface with the 'Output' tab selected. Under 'HTTP response code', it says '200 OK'. Under 'HTTP response content', there is a box containing the text 'Hello, AZ303. This HTTP triggered function executed successfully.'

FIGURA 3-13 Revisión del resultado de una función de Azure en el portal

Nota Crear funciones de Azure con Visual Studio Code

Aprenda a usar Visual Studio Code para crear una función basada en biblioteca de clase C # que responda a solicitudes HTTP en <http://docs.microsoft.com/en-us/azure/azure-functions/functions-create-first-function-vs-código> .

HABILIDAD 3.2: IMPLEMENTAR APLICACIONES BASADAS EN CONTENEDORES

La contenerización ha interrumpido por completo la industria de TI durante los últimos años y no hay señales de que la tendencia se desacelere. El equipo de Azure comprende esto y ha hecho todo lo posible para que sea increíblemente sencillo implementar aplicaciones en contenedores en App Service.

Esta habilidad cubre cómo:

- Cree una imagen de contenedor
- Publicar y automatizar la implementación de imágenes en Azure Container Registry.
- Publicar una solución en una instancia de contenedor de Azure
- Configurar el servicio Azure Kubernetes

Crea una imagen de contenedor

Las imágenes de contenedores son los artefactos que hacen posible implementar aplicaciones modernas a velocidades nunca antes vistas. Las aplicaciones se ejecutan dentro de contenedores, que se inician desde imágenes de contenedores. Piense en las imágenes de contenedores como plantillas que se pueden utilizar para iniciar contenedores. Usamos imágenes de contenedor para empaquetar nuestro código y las dependencias de la aplicación, y luego podemos invocar instancias en ejecución de estas imágenes para crear contenedores. El conjunto de herramientas de Docker se ha convertido en el estándar de oro para gestionar todo este proceso.

Debe estar familiarizado con el siguiente procedimiento para crear imágenes de contenedor de Docker:

1. Cree un nuevo archivo de texto llamado `Dockerfile` (asegúrese de no agregar una extensión de archivo).
2. Agregue comandos, como los que se muestran en la Figura 3-14 , para automatizar el proceso de compilación de una aplicación Node.js empaquetada en una imagen de contenedor. Cada instrucción en el Dockerfile agrega una capa de solo lectura a la imagen del contenedor.

```
1 FROM node:alpine
2
3 WORKDIR /usr/app
4
5 COPY . .
6 RUN npm install
7
8 CMD ["npm", "start"]
```

FIGURA 3-14 Escribiendo un Dockerfile

1. ■ **DESDE.** Cree una capa utilizando la imagen de contenedor oficial de Node.js basada en Alpine Linux.

2. ■ **WORKDIR**. Establezca el directorio de trabajo de la aplicación.
 3. ■ **COPIA**. Agregue archivos de la máquina del desarrollador a la imagen de Docker.
 4. ■ **EJECUTAR**. Instale todos los paquetes `npm` necesarios que necesitará la aplicación.
 5. ■ **CMD**. Úselo para especificar el comando que se ejecutará cuando se inicie el contenedor.
3. El paso final es usar el cliente de Docker para crear su imagen de contenedor. Millones de desarrolladores utilizan Docker Desktop, que se ejecuta en Mac y Windows, para desarrollar aplicaciones localmente con Docker. Puede usar el comando `Docker Build` después de haber instalado Docker Desktop para crear una imagen de contenedor usando su Dockerfile, como se muestra en la Figura 3-15 .

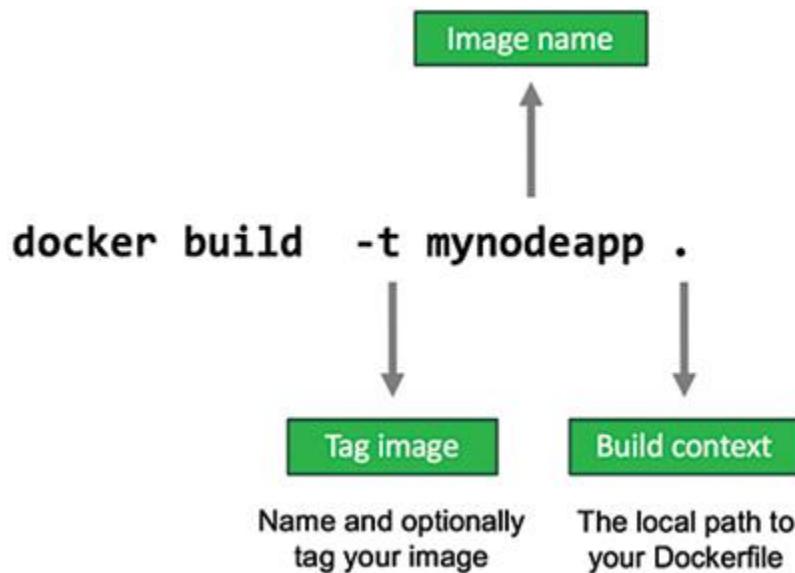


FIGURA 3-15 Ejecución de una compilación de Docker
Nota Referencia de Dockerfile

El proceso de creación de imágenes de Docker es increíblemente versátil. Para obtener más información sobre cómo escribir su propio Dockerfile, visite la referencia oficial de Docker en <https://docs.docker.com/engine/reference/builder/> .

Publicar y automatizar la implementación de imágenes en Azure Container Registry

Los servicios de registro de contenedores se utilizan como ubicación central para almacenar imágenes de contenedores. Azure Container Registry (ACR) es un servicio de registro de Docker completamente administrado basado en el Docker Registry de código abierto. Puede crear un recurso ACR e integrar una variedad de servicios de Azure con su registro de contenedores. Esto es útil para mantener las imágenes cerca de la infraestructura de la aplicación, y puede usar controles de seguridad nativos en Azure para permitir o denegar el acceso a ACR.

Una vez que haya creado sus propias imágenes de contenedor, puede enviarlas a una instancia de ACR. Complete los pasos del siguiente procedimiento para crear un recurso ACR para almacenar las imágenes de su contenedor:

1. Inicie sesión en Azure Portal y haga clic en **Crear un nuevo recurso**.
2. Seleccione **Contenedores** en **Azure Marketplace** y haga clic en **Container Registry**.
3. Ingrese los detalles del registro, como se muestra en la Figura 3-16 , y haga clic en **Crear** .



FIGURA 3-16 Creación de un recurso ACR

1. **Nombre de registro.** Ingrese un nombre de host globalmente único en `azurecr.io`. Siga las reglas de nomenclatura estándar de DNS y utilice únicamente caracteres alfanuméricos.
2. **Usuario administrador.** Habilite el uso de un nombre de usuario y una contraseña específicos de ACR para iniciar sesión en el registro mediante herramientas como la CLI de Docker.
3. **SKU.** Seleccione el nivel de precios. El nivel que seleccione dicta el rendimiento y la escalabilidad de su recurso ACR.
4. Navegue a las propiedades de su recurso ACR después de que se haya completado el aprovisionamiento. Haga clic en **Claves de acceso** en **Configuración** para recuperar los detalles del servidor de inicio de sesión y la contraseña para su cuenta de usuario administrador de ACR.

5. Inicie sesión en su instancia de ACR utilizando el cliente de Docker (por ejemplo, inicio de sesión de Docker <su nombre de ACR>.azurecr.io).
6. Despues de iniciar sesión en ACR, puede publicar imágenes mediante la CLI de Docker, como se muestra en la Figura 3-17 .

```
$ docker tag mynodeapp contoso.azurecr.io/mynodeapp
$ 
$ 
$ docker push contoso.azurecr.io/mynodeapp
The push refers to repository [contoso.azurecr.io/mynodeapp]
27036f822fba: Pushed
9adffa35f891: Pushed
2edfc06ca0f7: Pushed
662f8f5a2b7a: Pushed
00210cd15c5c: Pushed
ffa1cdbe8bf7: Pushed
f1b5933fe4b5: Pushed
```

FIGURA 3-17 Etiquetado y envío de una imagen de contenedor a ACR

- 0.■ **etiqueta de la ventana acoplable.** Utilice el comando de etiqueta de la ventana acoplable para etiquetar su imagen con el nombre de ACR en el formato de <nombre de host de ACR> / <su nombre de imagen>. Tenga en cuenta que esto también se puede hacer durante el tiempo de compilación al crear la imagen con docker build.
- 1.■ **empuje de la ventana acoplable.** Publique la imagen en ACR utilizando el nombre de host del registro incluido como parte del nombre de la imagen.



Sugerencia para el examen

Puede usar una entidad de servicio de Azure AD para delegar el acceso a su recurso ACR además de un usuario administrador.

Implementar una aplicación que se ejecute en una instancia de contenedor de Azure

La capacidad de poner en marcha rápidamente aplicaciones dentro de contenedores abre numerosas posibilidades. Además de ejecutar contenedores en App Service, también puede aprovechar un modelo que proporciona contenedores como servicio. Las instancias de contenedor de Azure (ACI) son una oferta de servicios que le permite activar contenedores a pedido, sin ninguna infraestructura existente, como máquinas virtuales o incluso planes de servicio de aplicaciones. ACI le permite diseñar e implementar sus aplicaciones en lugar de administrar la infraestructura que las ejecuta.

Use el siguiente procedimiento para crear una instancia de contenedor de Azure:

1. Inicie sesión en Azure Portal y haga clic en **Crear un nuevo recurso**.
2. Seleccione **Contenedores** en **Azure Marketplace** y haga clic en **Instancias de contenedor**.
3. Ingrese los detalles de ACI, como se muestra en la Figura 3-18 , y haga clic en **Crear** . Estas entradas proporcionan los detalles sobre su instancia de contenedor, incluido el nombre, el tipo de imagen y la ubicación.
 1. ■ **Nombre del contenedor.** Ingrese un nombre significativo para su contenedor.
 2. ■ **Tipo de imagen.** Seleccione **Público** si su imagen está alojada en un registro público. De lo contrario, elija **Privado** para habilitar las opciones para incluir los detalles de inicio de sesión de su registro.
 3. ■ **Nombre de la imagen.** Ingrese el nombre exacto de la imagen de su contenedor.
 4. ■ **Servidor de inicio de sesión de registro de imágenes.** Proporcione el nombre de dominio completo de su servidor de inicio de sesión. Si está utilizando ACR, este será el nombre de su servidor de inicio de sesión de ACR.

5. ■ **Nombre de usuario del registro de imágenes.** Ingrese el nombre de usuario de su registro.
6. ■ **Contraseña de registro de imágenes.** Proporcione su contraseña de registro.
7. ■ **Tipo de SO.** ACI admite contenedores basados en Linux y Windows. Seleccione el tipo de sistema operativo apropiado de la lista.
8. ■ **Tamaño.** ACI requiere que establezca límites de recursos para cada instancia de su aplicación. Esto también controla el precio del recurso ACI y puede cambiar el tamaño en cualquier momento después de que se haya aprovisionado el recurso ACI.

Home > New > Create container instance

Create container instance

Basics Networking Advanced Tags Review + create

Azure Container Instances (ACI) allows you to quickly and easily run containers on Azure without managing servers or having to learn new tools. ACI offers per-second billing to minimize the cost of running containers on the cloud. [Learn more about Azure Container Instances](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription * Resource group [Create new](#)

Container details

* Container name * Region * Image type Public Private
* Image name * Image registry login server * Image registry user name
* Image registry password * OS type Linux Windows
* Size [Change size](#)

FIGURA 3-18 Creación de una instancia de contenedor de Azure



Sugerencia para el examen

ACI es una gran solución para aplicaciones básicas y automatización de tareas. Para escenarios de producción que requieren una orquestación completa, Microsoft recomienda ejecutar contenedores en Azure Kubernetes Service (AKS).

Administrar la configuración del contenedor usando código

La plataforma Azure brinda acceso a numerosos SDK y herramientas específicos de cada idioma que puede usar para administrar su infraestructura mediante programación. Los desarrolladores pueden usar .NET, Java, Node.js, PHP, Python y Go para crear aplicaciones que interactúen con sus recursos de Azure.

Además de los SDK, Microsoft ofrece soporte para PowerShell y la CLI de Azure para la creación de scripts operativos y para ejecutar comandos de administración ad-hoc localmente o en el Cloud Shell interactivo.

Se espera que los arquitectos de soluciones de Azure comprendan cómo aprovechar estas capacidades de automatización para administrar la configuración del contenedor mediante código. Esto es cierto tanto si el código es parte de una aplicación robusta creada por desarrolladores como si se utiliza en scripts de aprovisionamiento creados por el equipo de DevOps. Dado que los SDK y las herramientas de línea de comandos aprovechan las API RESTful de Azure en segundo plano, los arquitectos de soluciones de Azure pueden aprovechar cualquier herramienta de su elección para realizar el trabajo.

Use el siguiente procedimiento con la CLI de Azure para descubrir los comandos que puede usar para administrar la configuración del contenedor mediante código:

1. Navegue a *shell.azure.com* en su navegador web e inicie una nueva instancia de Cloud Shell.
2. Ejecute el siguiente comando para revisar todos los subcomandos disponibles para administrar sus instancias de Azure Container Registry (ACR):

```
az acr --ayuda
```

3. Ejecute el siguiente comando para revisar todos los subcomandos disponibles para administrar sus Azure Container Instances (ACI):

```
contenedor az --help
```

4. Para crear un recurso, como una instancia de contenedor de Azure (ACI), use el comando `az container create`:

Haga clic aquí para ver la imagen del código

```
az container create \  
    --infraestructura central del grupo de recursos \  
    --nombre mynodeapp \  
    --image mynodeapp: última \  
    --cpu 1 \  
    --memoria 1
```

5. Una vez que tenga una instancia ACI en ejecución, puede administrar la configuración y el ciclo de vida de la instancia mediante el código, como se muestra en el siguiente comando que reinicia la instancia:

```
reinicio del contenedor az --name mynodeapp
```



Sugerencia para el examen

Microsoft puede poner a prueba sus conocimientos mediante tareas prácticas basadas en el rendimiento que deben completarse en Azure Portal. Esté preparado para usar Cloud Shell para obtener acceso a la CLI de Azure o PowerShell, y asegúrese de comprender cómo usar el sistema de ayuda para descubrir comandos y la sintaxis adecuada para completar la tarea.

Configurar el servicio Azure Kubernetes

Para aplicaciones de nivel de producción, Microsoft recomienda ejecutar contenedores utilizando Azure Kubernetes Service (AKS) totalmente administrado, lo que hace que sea rápido y fácil de implementar y administrar aplicaciones en contenedores. AKS elimina la carga de las operaciones y el mantenimiento continuo que se requieren al administrar su propia implementación de Kubernetes. Como servicio alojado, Azure maneja tareas críticas de Kubernetes como el monitoreo y el mantenimiento del estado, y AKS es de uso gratuito. Solo paga por los nodos de agentes dentro de sus clústeres, no por los nodos maestros que controlan sus clústeres.

Use el siguiente procedimiento para crear un clúster de Azure Kubernetes Service (AKS) mediante la CLI de Azure:

1. Navegue a shell.azure.com en su navegador web e inicie una nueva instancia de Cloud Shell.
2. Cree un nuevo grupo de recursos con el siguiente comando de la CLI de Azure:

Haga clic aquí para ver la imagen del código

```
az group create \
    --nombre AKS \
    - ubicación Eastus
```

3. Cree un nuevo clúster de AKS con el siguiente comando de la CLI de Azure:

Haga clic aquí para ver la imagen del código

```
az aks create \
    - grupo de recursos AKS \
    --nombre AKSCluster01 \
    --nodos-recuento 1 \
    --enable-addons monitoring \
    --generate-ssh-keys
```

4. Una vez creado el clúster de AKS, puede conectarse y administrar el clúster desde la línea de comandos. Primero, instale la CLI de AKS dentro de su instancia de shell de nube con el siguiente comando:

```
az aks install-cli
```

5. Descargue sus credenciales de AKS y configure la CLI de AKS para usarlas dentro de su sesión de shell:

Haga clic aquí para ver la imagen del código

```
az aks get-credentials \
```

```
- grupo de recursos AKS \
--nombre AKSCluster01
```

6. Verifique que su conexión al clúster de AKS funcione correctamente mediante el comando kubectl para recuperar una lista de nodos del clúster.

```
kubectl obtener nodos
```

Nota Azure Container Service (ACS)

Antes de lanzar Azure Kubernetes Service (AKS), Microsoft ofreció Azure Container Service (ACS) como una solución administrada que proporcionaba múltiples sistemas de orquestación como servicio, incluidos Kubernetes, Docker Swarm y DC / OS. ACS ha quedado obsoleto y los clientes actuales de ACS deberán migrar a AKS.

RESUMEN DEL CAPÍTULO

- Azure App Service le brinda la capacidad de crear y alojar aplicaciones web, backends móviles y API RESTful sin tener que administrar el servidor, la red y la infraestructura de almacenamiento.
- App Service admite aplicaciones creadas con marcos comunes como .NET, .NET Core, Node.js, Java, PHP, Ruby o Python.
- Puede implementar aplicaciones web mediante Azure Portal, CLI, PowerShell o cualquiera de los SDK disponibles proporcionados por Microsoft.
- App Service es compatible con aplicaciones de Windows y Linux, incluidos los contenedores de Docker.
- Las aplicaciones web de Azure son instancias de un servicio de aplicaciones que se ejecutan dentro de un plan de servicio de aplicaciones.
- Las instancias de contenedor de Azure no dependen de un plan de servicio de aplicaciones.

- Azure proporciona un soporte completo para los contenedores de Docker y las imágenes se pueden crear y almacenar en Azure Container Registry (ACR).
- Azure Kubernetes Service (AKS) es un sistema de orquestación de contenedores totalmente administrado que facilita a los equipos la ejecución de contenedores en producción.

EXPERIMENTO MENTAL

En este experimento mental, demuestre sus habilidades y conocimiento de los temas cubiertos en este capítulo. Puede encontrar respuestas a este experimento mental en la siguiente sección.

Es un arquitecto de Azure para Contoso Ltd. Se le solicitó que diseñe e implemente una solución para ejecutar una colección de aplicaciones de línea de negocio en la nube de Azure. Responda las siguientes preguntas sobre cómo aprovechar Azure App Service para implementar su solución para Contoso.

1. Necesita mover una aplicación web a Azure que el departamento de Recursos Humanos usa para capacitar a los empleados corporativos en la sucursal de Los Ángeles. La aplicación web implementa un reproductor de video integrado que ofrece contenido de capacitación en video a cada usuario. Todos los videos se producen con la mejor calidad posible. ¿Cómo debe diseñar la solución para reducir la latencia entre los usuarios y la infraestructura de la aplicación?
2. Se le asignó la tarea de refactorizar una aplicación web local para que se ejecute dentro de un contenedor de Docker en Azure App Service. Debe asegurarse de que solo ciertos miembros del personal de TI puedan acceder a las imágenes del contenedor. ¿Cómo puede lograr esto con la menor cantidad de esfuerzo administrativo?
3. Actualmente tiene una tarea nocturna que ejecuta un script de PowerShell en un servidor Windows local. El proceso genera un informe y envía el resultado al personal de soporte de TI en la sede de Contoso. Debe mover este proceso como parte de la migración de Contoso a Azure, pero debe hacerlo utilizando la menor cantidad de esfuerzo administrativo. Ya tiene planes para implementar

varios sitios web en Azure App Service. ¿Qué debe hacer para ejecutar el proceso nocturno en Azure?

RESPUESTAS DEL EXPERIMENTO MENTAL

Esta sección contiene la solución al experimento mental. Cada respuesta explica por qué la opción de respuesta es correcta.

1. 1. Implemente la infraestructura de App Service en una región de Azure basada en la costa oeste. Esto pondrá la infraestructura muy cerca de los usuarios en la sucursal de Los Ángeles. Para aplicaciones globales, considere usar el servicio Azure CDN para distribuir contenido estático a ubicaciones de borde disponibles en toda la infraestructura global de Azure.
2. 2. Implemente un recurso de Azure Container Registry (ACR) dentro de su suscripción de Azure. Des habilite el acceso de administrador y delegue el control al recurso ACR mediante el control de acceso basado en roles (RBAC).
3. 3. Cree un WebJob de Azure dentro de uno de los recursos de aplicaciones web existentes que se ejecutan en su suscripción de Azure. Cargue el script de PowerShell y configure un WebJob activado que se ejecute en una programación diaria.

Capítulo 4

Implementar y administrar plataformas de datos

En la era actual de desarrollo de aplicaciones modernas en la nube, la estrategia para almacenar datos de aplicaciones en la nube es fundamental para el éxito de cualquier aplicación. Las aplicaciones nativas de la nube requieren que se adapte a nuevos enfoques y diversas herramientas y servicios modernos para administrar los datos en la nube de manera segura y eficiente.

La plataforma Microsoft Azure proporciona un amplio conjunto de soluciones de almacenamiento de datos diseñadas específicamente para diferentes requisitos de clasificación de datos de su aplicación en la nube.

El examen AZ-303 espera que conozca las diferentes soluciones de almacenamiento de la plataforma de datos y elija la solución óptima según la clasificación de los datos de la aplicación, su patrón de uso y los requisitos de rendimiento.

Habilidades cubiertas en este capítulo:

- ■ [Habilidad 4.1: Implementar bases de datos NoSQL](#)
- ■ [Habilidad 4.2: Implementar bases de datos SQL de Azure.](#)

HABILIDAD 4.1: IMPLEMENTAR BASES DE DATOS NOSQL

Hoy en día, los datos generados y consumidos por las aplicaciones, incluida una amplia variedad de dispositivos IoT, sitios de redes sociales, son enormes. El manejo de datos tan masivos con los sistemas tradicionales de administración de bases de datos relacionales (RDBMS) a veces se vuelve abrumador e ineficiente. La heterogeneidad y complejidad de los datos (también conocidos como Big Data) emitidos por numerosos dispositivos conectados también es difícil de administrar utilizando soluciones tradicionales de almacenamiento de bases de datos.

Para manejar de manera eficiente un volumen tan grande de datos, entra en juego el concepto de bases de datos NoSQL. Las bases de datos NoSQL son bases de datos no relacionales que ofrecen escalabilidad horizontal y son rentables en comparación con los sistemas de bases de datos relacionales. Las bases de datos NoSQL también proporcionan modelos de datos más flexibles y patrones de acceso a datos optimizados para conjuntos de datos grandes y complejos. Las bases de datos NoSQL ofrecen los siguientes modelos de datos:

- ■ **Bases de datos de valores clave** . Una base de datos clave-valor es una base de datos no relacional que utiliza un método de par clave-valor para almacenar datos. La clave representa un identificador único para una colección determinada de valores de datos que le permite ejecutar comandos simples como GET , PUT o DELETE . Las bases de datos de valores clave son altamente particionables y admiten el escalado horizontal a gran escala. La plataforma Microsoft Azure proporciona las siguientes visualizaciones populares de bases de datos de valores clave:
 - ■ Almacenamiento de tablas de Azure
 - ■ API de tabla de Azure Cosmos DB
 - ■ Azure Cache para Redis
- ■ **Bases de datos de documentos.** Un modelo de base de datos de documentos nos permite almacenar datos usando un lenguaje de marcado como XML, JSON y YAML o incluso usar texto sin formato. Las bases de datos de documentos son independientes del esquema y no requieren que todos los documentos tengan la misma estructura. Azure Cosmos DB es una base de datos de documentos popular que admite una amplia variedad de API, SDK de software e idiomas potentes e intuitivos para administrar un gran volumen de datos semiestructurados.
- ■ **Bases de datos de gráficos.** Las bases de datos de gráficos suelen estar diseñadas para almacenar y visualizar la relación entre entidades de datos. Una base de datos gráfica tiene dos tipos de información: nodos y bordes. Los nodos denotan un cuerpo y los bordes indican la relación entre entidades.

- **Bases de datos de familias de columnas.** Las bases de datos de familias de columnas tienen un aspecto similar a las bases de datos relacionales, con datos almacenados en filas y columnas. Las bases de datos de familias de columnas le permiten agrupar columnas en función de entidades relacionadas lógicamente para formar una familia de columnas, en la que cada columna contiene los datos de todas las entidades agrupadas. Apache HBase es una base de datos de familias de columnas.

Esta habilidad cubre cómo:

- Configurar tablas de cuentas de almacenamiento
- Seleccione las API de Cosmos DB adecuadas
- Configurar réplicas en Cosmos DB

Configurar tablas de cuentas de almacenamiento

El servicio de almacenamiento de Azure Table proporciona una opción de almacenamiento de datos escalable masivamente para el almacenamiento de datos estructurados, NoSQL y de valor clave. Azure Table Storage es un almacenamiento sin esquema que almacena valores de datos en una entidad que puede cambiar con el tiempo a medida que evolucionan los datos de la aplicación. El servicio proporciona API REST para interactuar con los datos para operaciones de inserción, actualización, eliminación y consulta mediante el protocolo OData y consultas LINQ mediante bibliotecas .NET. A continuación, se muestran algunos casos de uso comunes para el almacenamiento de tablas de Azure:

- Necesita un almacenamiento rentable para manejar terabytes (TB) de datos estructurados que se escalen a gran escala y bajo demanda.
- Su aplicación almacena un conjunto de datos masivo y necesita un alto rendimiento y baja latencia.
- Los datos de su aplicación deben protegerse con recuperación ante desastres, estrategia de respaldo confiable, balanceo de carga, replicación y alta disponibilidad.

En la siguiente sección, aprenderá el modelo de datos subyacente del servicio de almacenamiento de Azure Table.

Modelo de datos subyacente del servicio de almacenamiento de tablas de Azure

Como aprendimos en la sección anterior, el servicio de almacenamiento de Azure Table le permite almacenar conjuntos de datos NoSQL estructurados mediante un diseño sin esquema. La figura 4-1 muestra el modelo de datos subyacente del servicio de almacenamiento de tablas de Azure.

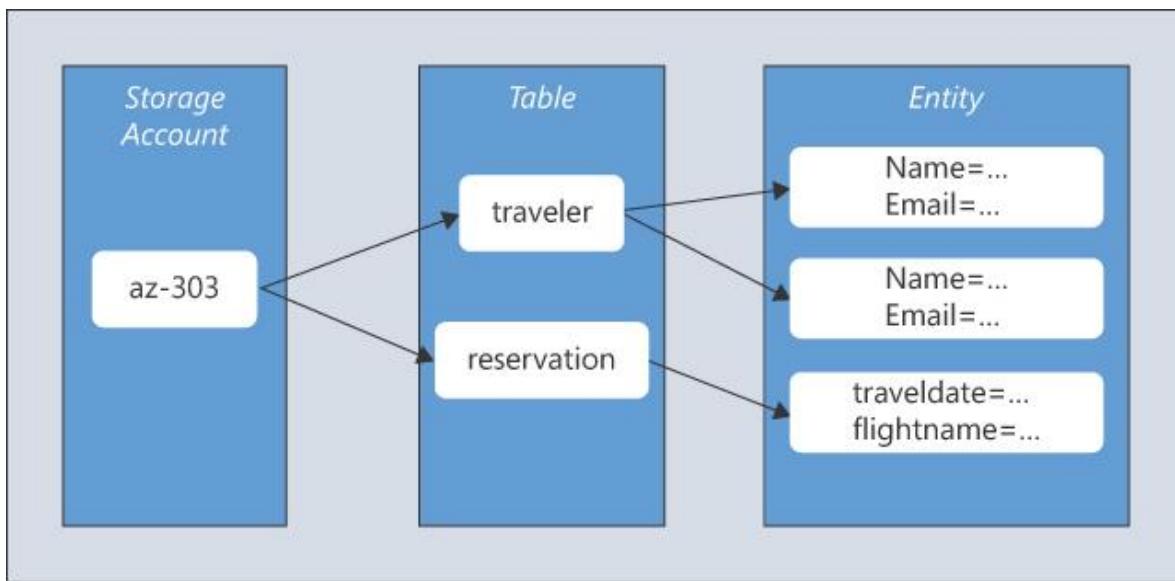


FIGURA 4-1 Modelo de datos de almacenamiento de Azure Table

Los siguientes son los elementos clave de Azure Table Storage como se ve en la figura anterior 4-1.

- **Cuenta de almacenamiento.** El nombre de la cuenta de almacenamiento es un identificador único global que sirve como espacio de nombres principal para un servicio de tabla. La autenticación y autorización en el servicio Table se realiza en el nivel de la cuenta de almacenamiento. Puede crear una o varias tablas dentro de la cuenta de almacenamiento. Por ejemplo, en la figura 4-1 anterior, tenemos dos tablas separadas: **viajero** y **reserva** para almacenar la información respectiva. Todas las tablas que cree debajo de la cuenta de almacenamiento obtendrán un URI base único para interactuar con el servicio mediante las API REST, PowerShell o la CLI de Azure. Un ejemplo de URI base es <https://<storage-account>>

.table.core.windows.net / . La cuenta de almacenamiento viene con dos SKU de la siguiente manera:

- ■ **Uso general V2** . Microsoft recomienda usar General-Purpose V2 para aprovechar las funciones más recientes de Azure Storage.
- ■ **Uso general V1** . Este tipo es el SKU heredado y se mantiene por compatibilidad con versiones anteriores de implementaciones. General-Purpose V1 no admite los nuevos niveles de acceso Hot, Cool o Archive ni la replicación a nivel de zona.
- ■ **Tabla, entidades y propiedades.** La tabla dentro de la cuenta de almacenamiento almacena una colección de entidades en filas. Las entidades tienen una colección de propiedades con un par clave-valor similar a una columna. Una entidad en la cuenta de almacenamiento puede almacenar hasta 1 MB de datos e incluir hasta 252 propiedades. Cada entidad tiene tres propiedades definidas por el sistema, como se menciona a continuación.
 - ■ **PartitionKey.** Una clave de partición es un identificador único para una determinada partición de datos dentro de una tabla. Está diseñado para admitir el equilibrio de carga en diferentes nodos de almacenamiento para un mejor rendimiento y rendimiento. La clave de partición es la primera parte del índice agrupado y está indexada de forma predeterminada para una búsqueda más rápida. El nombre de la clave de partición puede ser una cadena de hasta 1 KB de tamaño.
 - ■ **RowKey** . Una clave de fila es un identificador único dentro de una partición y está diseñada para formar una segunda parte del índice agrupado de una entidad determinada. Debe especificar una clave de fila y una clave de partición mientras realiza la operación CRUD para una entidad dentro de una tabla. Al igual que la clave de partición, una clave de fila es una columna de índice con un límite de tamaño de 1 KB.

- **Marca de tiempo.** La propiedad Timestamp es un valor de atributo derivado del sistema de fecha y hora que se aplica automáticamente en el lado del servidor para registrar la hora en que se modificó por última vez una entidad. El servicio de almacenamiento de Azure Table no le permite establecer un valor externamente y usa la marca de tiempo (LTM) modificada anteriormente internamente para administrar la simultaneidad optimista.

La API REST le permite interactuar con las tablas dentro de una cuenta de almacenamiento y realizar operaciones de inserción, actualización y eliminación en las entidades.

Haga clic aquí para ver la imagen del código

```
https://<cuenta-almacenamiento>.table.core.windows.net/<nombre de la tabla>
```

El diseño simple del servicio de almacenamiento de Azure Table se muestra en la [Figura 4-2](#).

PartitionKey	RowKey	Timestamp	Fname	Flightname	Lname	LeavesTaken	TotalEmployeesCount	TravelExpense
ORD-NY	Flight1	2020-03-20T13:10:51.567Z	Gurvinder	Airways-ABC	Singh	null	null	null
payroll	Flight1	2020-03-20T13:12:14.545Z	null	null	null	56	12345	456

Edit Entity

Property Name	Type	Value
PartitionKey	String	ORD-NY
RowKey	String	Flight1
Timestamp	Date/Time	2020-03-20T13:12:14.545Z
LeavesTaken	String	56
TotalEmployeesCount	Int64	12345
TravelExpense	String	456

FIGURA 4-2 Un diseño de mesa simple

Como puede ver en la [Figura 4-2](#), la naturaleza sin esquema de la tabla le permite almacenar entidades con un conjunto diferente de propiedades dentro de la misma tabla.

Las propiedades personalizadas definidas por el usuario para cada una de las entidades independientes pueden tener un tipo de datos, como una cadena o un número entero. De forma predeterminada, las propiedades tienen el tipo de datos de cadena a menos que especifique lo contrario. El servicio de almacenamiento de Azure Table también permite almacenar

tipos de datos complejos en las propiedades utilizando un formato serializado diferente, como JSON o XML.

¿Más información? Diseñar una partición escalable

Si bien el almacenamiento de Azure es enormemente escalable, es crucial diseñar particiones de tabla para aprovechar el escalado automático y el equilibrio de carga en diferentes nodos de servidor. Consulte la documentación completa de Microsoft "Diseñe una estrategia de partición escalable para Azure Table Storage" en [#gdft](https://docs.microsoft.com/en-us/rest/api/storageservices/designing-a-scalable-partitioning-strategy-for-azure-table-storage).

Crear un servicio de almacenamiento de Azure Table

Como se indicó en la sección anterior, antes de crear un servicio de almacenamiento de Azure Table, necesita una cuenta de almacenamiento como unidad base. Puede lograr esto mediante Azure Portal, Azure PowerShell o la CLI de Azure.



Sugerencia para el examen

El examen AZ-303 espera que tenga al menos conocimientos básicos del módulo az de PowerShell o la CLI de Azure (interfaz de línea de comandos multiplataforma) para interactuar con los servicios de Azure. La lista completa de comandos de la CLI de PowerShell y Azure para administrar el servicio de almacenamiento de Azure Table se publica en <https://docs.microsoft.com/en-us/cli/azure/storage/table?view=azure-cli-latest#az-almacenamiento-tabla-crear>.

¿Más información? Más información sobre la CLI de Azure

Para obtener más información sobre los comandos de la CLI de Azure y los diferentes SDK de clientes ligeros nativos para plataformas cruzadas, visite la documentación de Microsoft en <https://docs.microsoft.com/en-us/cli/azure/?view=azure-cli-latest>.

Este fragmento de código es un ejemplo de un comando de la CLI de Azure para crear un servicio de almacenamiento de tabla de Azure dentro de una cuenta de almacenamiento de Azure:

[Haga clic aquí para ver la imagen del código](#)

```
Crear tabla de almacenamiento az --name [--account-key] [--account-name]
```

- ■ - **nombre** El nombre es un parámetro obligatorio que representa el nombre exclusivo de la tabla que se creará. Debe contener solo caracteres alfanuméricos y no puede comenzar con un carácter numérico. No distingue entre mayúsculas y minúsculas y debe tener entre 3 y 63 caracteres.
- ■ - **account-key** Esta es una clave de cuenta de almacenamiento segura.
- ■ - **nombre-cuenta** Esto representa un nombre de cuenta de almacenamiento.

Siga estos pasos para crear un almacenamiento de tabla de Azure con Azure Cloud Shell. Los pasos asumen que ya tiene una suscripción de Azure y una cuenta de almacenamiento. De lo contrario, visite <https://azure.microsoft.com/en-in/free/> para crear uno.

1. Inicie sesión en Azure Portal en <https://portal.azure.com/> con sus credenciales de suscripción.
2. En la esquina superior derecha, debajo de la información del usuario, haga clic en el botón Cloud Shell, como se muestra en la [Figura 4-3](#).



FIGURA 4-3 Icono de Azure Portal para abrir Cloud Shell

3. Elija el tiempo de ejecución de bash y ejecute el siguiente comando en el shell de nube, como se muestra en la [Figura 4-4](#).

[Haga clic aquí para ver la imagen del código](#)

```

az storage table create --name az303table --account-key
cMwq9LmP06vGxxxxxxxxxxxxxx

xxxxxxxxxalUDpKJ7irIjLdZe8o + 1H38c8ZKIlTsT5pu / y /
YCupazeNGgA == --nombre-cuenta sgaz303

```

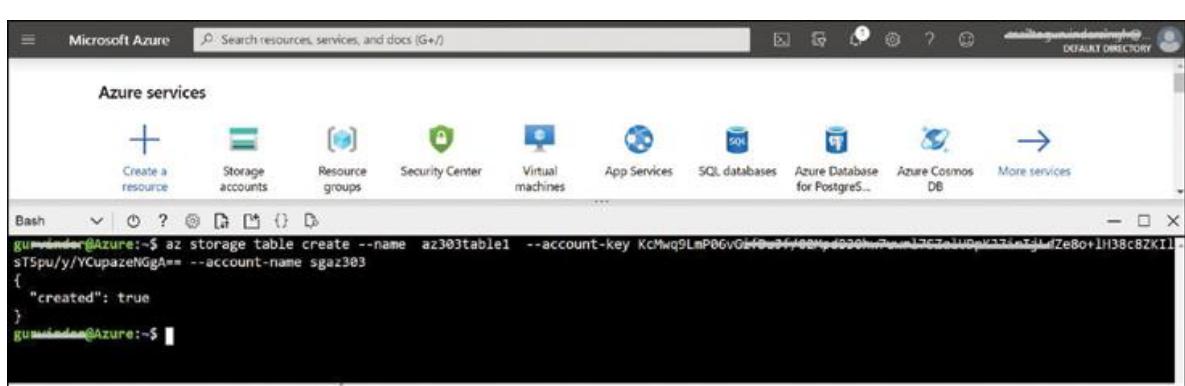


FIGURA 4-4 Consola de shell de Azure Cloud

Una vez que se ejecuta el comando, verá un mensaje `creado: verdadero`, como se muestra en la [Figura 4-4](#). El mensaje indica que se ha creado la tabla. Puede ver la tabla navegando a la cuenta de almacenamiento dentro de Azure Portal, como se muestra en la [Figura 4-5](#).

The screenshot shows the 'Tables' section of the 'sgaz303' storage account in the Azure Portal. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area has a search bar, a refresh button, and a delete button. A message encourages using the premium Table experience with Azure Cosmos DB. Below that is a 'Search tables by prefix' input field. A table named 'az303table' is listed with its URL: <https://sgaz303.table.core.windows.net/az303table>.

FIGURA 4-5 Hoja de almacenamiento Azure Table

Configurar el acceso a los datos de almacenamiento de tablas

Puede usar las claves de la cuenta de almacenamiento que genera Azure cuando activa una cuenta de almacenamiento. El uso de las claves de almacenamiento nativas o la exposición de estas claves a los desarrolladores puede no ser una buena práctica desde el punto de vista de la seguridad. Además, el uso de claves no le daría la capacidad de configurar el acceso granular y con límite de tiempo a uno o más servicios

de cuenta de almacenamiento ni le permitiría revocar acceso a los servicios cuando sea necesario. Aquí es donde entran en juego la firma de acceso compartido (SAS) y las políticas de acceso almacenado:

- ■ **Firma de acceso compartido.** La firma de acceso compartido (SAS) en la cuenta de almacenamiento le permite configurar el acceso delegado y granular a los servicios de la cuenta de almacenamiento. Una firma de acceso compartido está disponible en los siguientes tipos:
 - ■ **SAS de delegación de usuarios.** Este tipo está protegido mediante Azure AD (AAD) y solo se aplica al almacenamiento de blobs.
 - ■ **Servicio SAS.** Se trata de un servicio SAS que está protegido por una clave de cuenta de almacenamiento y normalmente se usa para delegar el acceso a solo uno de los servicios de almacenamiento de Azure.
 - ■ **Cuenta SAS.** La cuenta SAS también está protegida por una clave de cuenta de almacenamiento y se utiliza para delegar el acceso a uno o más servicios de cuenta de almacenamiento simultáneamente.
 - ■ **Política de acceso almacenado.** La política de acceso almacenado es un nivel adicional de control granular en el nivel de servicio SAS. Cuando utiliza un servicio SAS con una política de acceso almacenada, le permite revocar o cambiar los parámetros de acceso del SAS, como la hora de inicio, la hora de vencimiento y los permisos sobre la firma después de que se haya emitido el SAS.

Los siguientes pasos muestran cómo configurar una directiva de acceso almacenado en el servicio de almacenamiento de Azure Table mediante la CLI de Azure.

1. Inicie sesión en Azure Portal en <https://portal.azure.com/> con sus credenciales de suscripción.
2. Abra el shell en la nube basado en el navegador y siga el conjunto de pasos anterior.
3. Ejecute el siguiente comando de la CLI, cuyos componentes se explican a continuación del comando:

Haga clic aquí para ver la imagen del código

```
política de tabla de almacenamiento az crear --nombre
readupdateonly --nombre de tabla az303table

--account-name sgaz303 --account-key <la clave de la
cuenta va aquí> --expiry

2020-12-30'T'16: 23: 00'Z '--start 2020-3-01'T'16: 23:
00'Z' --permission ru
```

1. ■ **--name** Especifica el nombre de la política.
2. ■ **--table-name** Especifica el **nombre de** la tabla en la que se crea la política.
3. ■ **--account-name** El **nombre de** la cuenta de almacenamiento.
4. ■ **--account-key** Una clave de cuenta de almacenamiento segura.
5. ■ **--expiry** Caducidad fecha y hora UTC en (Ym-d'T'H: M: S'Z ').
6. ■ **--start** hora de inicio de fecha y hora en UTC en (YM-d'T'H: M: S'Z ')
7. ■ **--permission** Especifica las operaciones permitidas. En este ejemplo, permitimos solo operaciones de lectura y actualización. Los valores permitidos son los siguientes:
 1. ■ (r) para lectura / consulta
 2. ■ (a) para agregar
 3. ■ (u) para actualizar
 4. ■ (d) para eliminar

Después de ejecutar el comando en el shell de la nube, verá una política de acceso almacenada creada en el servicio de cuenta de Azure Table, como se muestra en la [Figura 4-6](#).

Identifier	Start time	Expiry time	Permissions
readupdate...	3/1/2020, 10:23:00 AM	12/30/2020, 10:23:00 AM	ru

FIGURA 4-6 Política de acceso almacenado en Azure Table Storage

Elija entre el servicio de almacenamiento de tablas de Azure y la API de tablas de Cosmos DB

Azure Cosmos DB Table API es la última oferta de base de datos NoSQL futurista de la familia de productos Azure Cosmos DB. Microsoft recomienda que utilice Cosmos DB Table API para nuevas aplicaciones, de modo que aproveche las funciones más recientes del producto, como compatibilidad con bases de datos multimodelo, distribución global llave en mano, commutación por error automática e indexación automática para un mejor rendimiento.

Cosmos DB Table API y Azure Table Storage usan el mismo modelo de datos para las operaciones CRUD. Por lo tanto, para las aplicaciones existentes, puede migrar sin problemas desde Azure Table Storage a Azure Cosmos DB sin cambiar el código de la aplicación. En la próxima sección, obtendrá información detallada sobre Azure Cosmos DB y sus API compatibles.

Azure Cosmos DB

En esta sección, aprenderá qué es Cosmos DB, por qué ha sido una base de datos tan popular para aplicaciones de nivel empresarial y qué herramientas, lenguajes y API estándar de la industria admite.

¿Qué es Cosmos DB?

Azure Cosmos DB es la base de datos multimodelo distribuida globalmente de Microsoft. Azure Cosmos DB le permite escalar de forma elástica e independiente el rendimiento y el almacenamiento en todo el mundo con rendimiento garantizado, baja latencia y alta disponibilidad.

Cosmos DB ofrece los siguientes beneficios:

- ■ **Rendimiento garantizado.** Cosmos DB garantiza el rendimiento y el rendimiento con carga máxima. El nivel de rendimiento de Cosmos DB se puede escalar elásticamente estableciendo Unidades de solicitud (RU).
- ■ **Distribución global.** Con la capacidad de tener réplicas multamaestro a nivel mundial y la capacidad incorporada para invocar la conmutación por error, Cosmos DB permite una disponibilidad de lectura / escritura del 99,999 por ciento en cada centro de datos donde Azure tiene presencia. La *API de alojamiento múltiple* de Cosmos DB es una función adicional para configurar la aplicación para que apunte al centro de datos más cercano para obtener una latencia baja y un mejor rendimiento.
- ■ **Modelo de consulta múltiple o API de consulta múltiple.** El soporte de base de datos de múltiples modelos le permite almacenar datos en el formato deseado, como un documento, gráfico o un modelo de datos de valor clave.
- ■ **Opciones de modos de coherencia.** El protocolo de replicación de Azure Cosmos DB ofrece cinco modelos de coherencia intuitivos, prácticos y bien definidos. Cada modelo tiene una compensación entre consistencia, rendimiento y latencia.
- ■ **Sin gestión de índices o esquemas.** El motor de la base de datos es completamente independiente del esquema. Cosmos DB indexa automáticamente todos los datos para una respuesta más rápida a las consultas.

Comprender la cuenta de Cosmos

La cuenta de Azure Cosmos es una construcción lógica que tiene un nombre DNS único a nivel mundial. Para una alta disponibilidad, puede agregar o eliminar regiones a su cuenta de Cosmos en cualquier momento con la capacidad de configurar múltiples maestros / escribir réplicas en diferentes regiones.

Puede administrar la cuenta de Cosmos en una suscripción de Azure mediante el portal de Azure, la CLI de Azure, el módulo AZ PowerShell o mediante diferentes SDK específicos del idioma. En esta sección se

describen los conceptos y la mecánica fundamentales esenciales de una cuenta de Azure Cosmos.

En el momento de redactar este libro, puede crear un máximo de 100 cuentas de Azure Cosmos con una suscripción de Azure. En la cuenta de Cosmos, puede crear una o más bases de datos de Cosmos y, dentro de la base de datos, puede crear uno o más contenedores. En el contenedor, coloca sus datos en forma de documentos, entidades de valor-clave, datos de familias de columnas o datos de gráficos al elegir las API adecuadas. [La figura 4-7](#) le ofrece una vista visual de lo que hemos compartido sobre la cuenta de Cosmos hasta ahora.

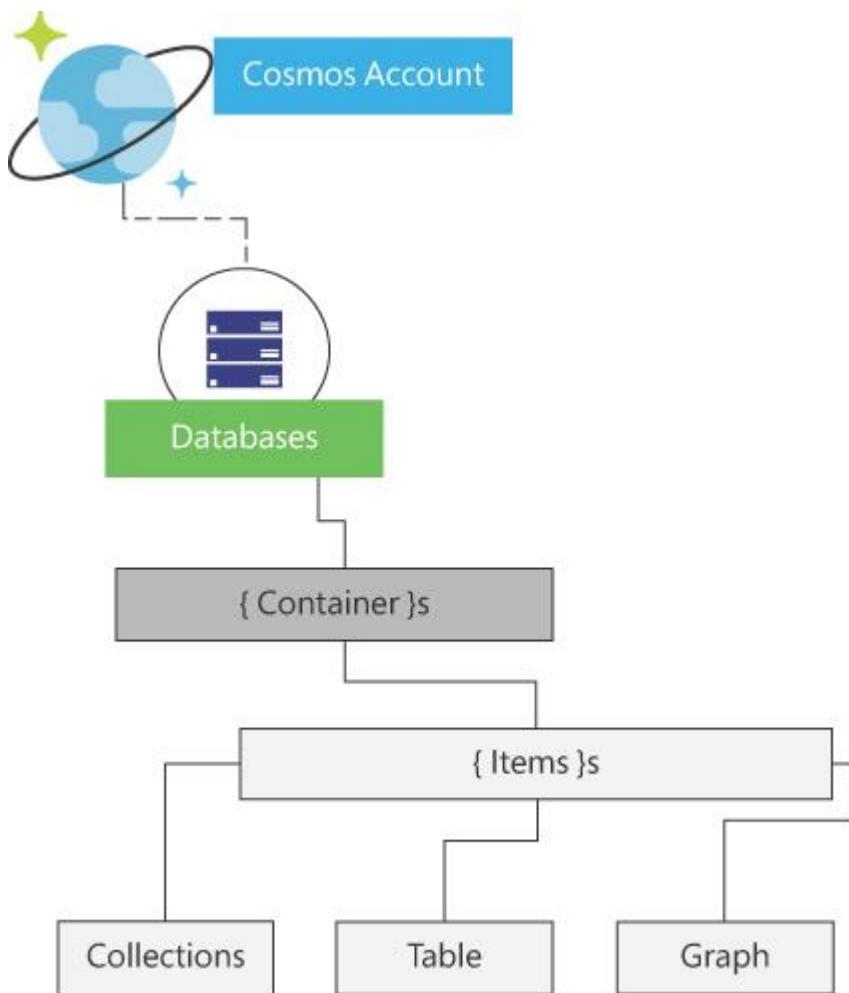


FIGURA 4-7 Entidades de cuenta de Azure Cosmos

Crea una cuenta Cosmos

Para configurar una cuenta de Cosmos mediante Azure Portal, siga los pasos siguientes:

1. Inicie sesión en el portal de Azure <https://portal.azure.com> .
2. Debajo de su suscripción en la esquina superior izquierda, seleccione **Crear un recurso** y busque **Cosmos DB** .
3. Haga clic en **Crear** (consulte la [Figura 4-8](#)).

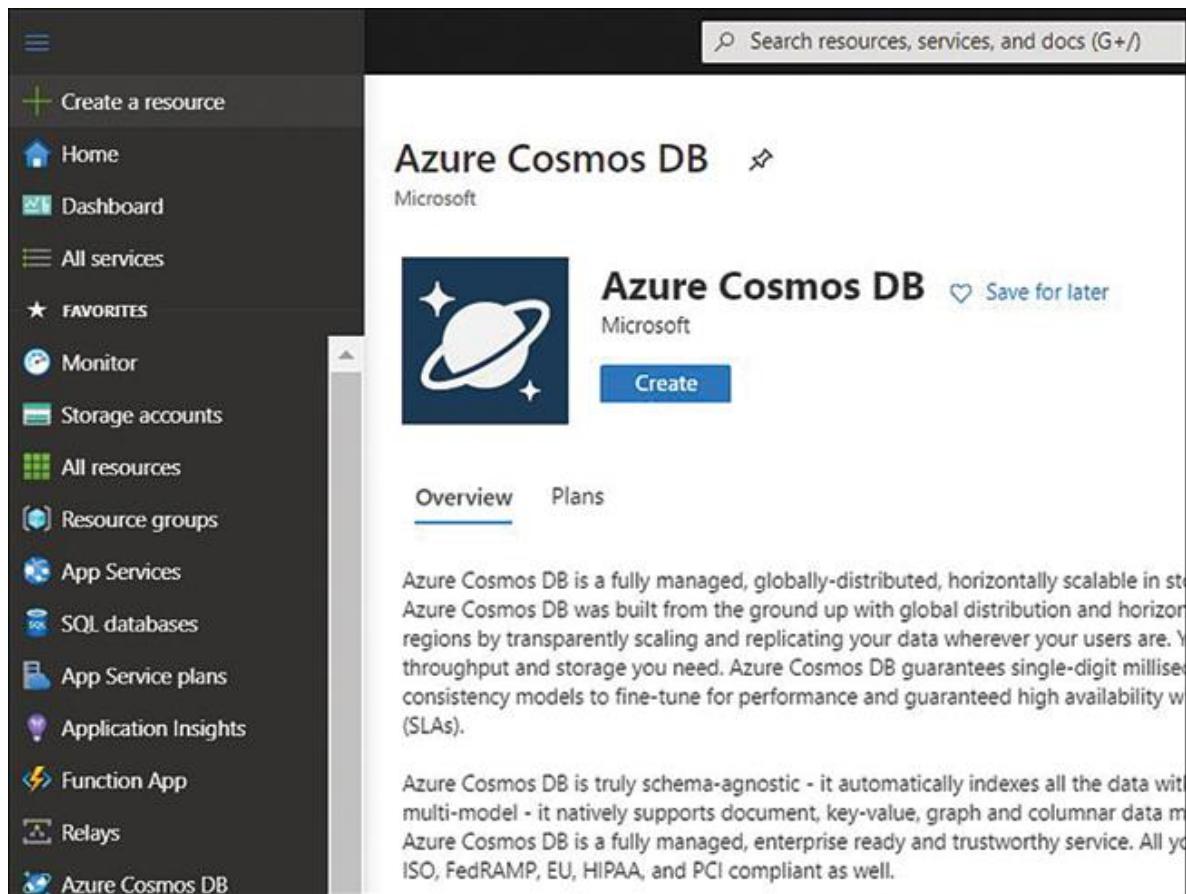


FIGURA 4-8 Creación de una cuenta de Azure Cosmos

4. En la página **Crear cuenta de Cosmos DB** , proporcione la información básica obligatoria, como se muestra en la [Figura 4-9](#) .
 1. ■ **Suscripción.** La suscripción de Azure con la que necesita crear una cuenta.
 2. ■ **Grupo de recursos.** Seleccione existente o cree un nuevo grupo de recursos.

3. ■ **Nombre de cuenta.** Ingrese el nombre de la nueva cuenta de Cosmos. Azure agrega documents.azure.com al nombre para construir un URI único.
4. ■ **API.** La API determina el tipo de cuenta que se creará. Veremos las API compatibles en la próxima sección.
5. ■ **Ubicación.** Elija la ubicación geográfica que necesita para alojar su cuenta de Cosmos.
6. ■ **Capacidad** En la opción de capacidad, mantenga la capacidad seleccionada predeterminada como **Rendimiento aprovisionado**, que está en disponibilidad general (GA). Puede configurar el rendimiento a nivel de contenedor o de base de datos. El rendimiento aprovisionado se puede configurar por adelantado o puede optar por el escalado automático.
7. ■ **Aplicar nivel gratuito:** el nivel le ofrece 5 GB de almacenamiento de datos y las primeras 400 RU (unidades de solicitud) gratuitas para siempre.
8. ■ **Tipo de cuenta** Bastante entendido, debe seleccionar **Producción** para la carga de trabajo de producción y **No** producción para la carga de trabajo de declaración o Desarrollo / Prueba.
9. ■ Puede omitir la sección Red y ETIQUETA y hacer clic en **Revisar + Crear**. La implementación tarda unos minutos en completarse. Puede ver la cuenta de Cosmos creada navegando a los **recursos del Grupo de recursos**.

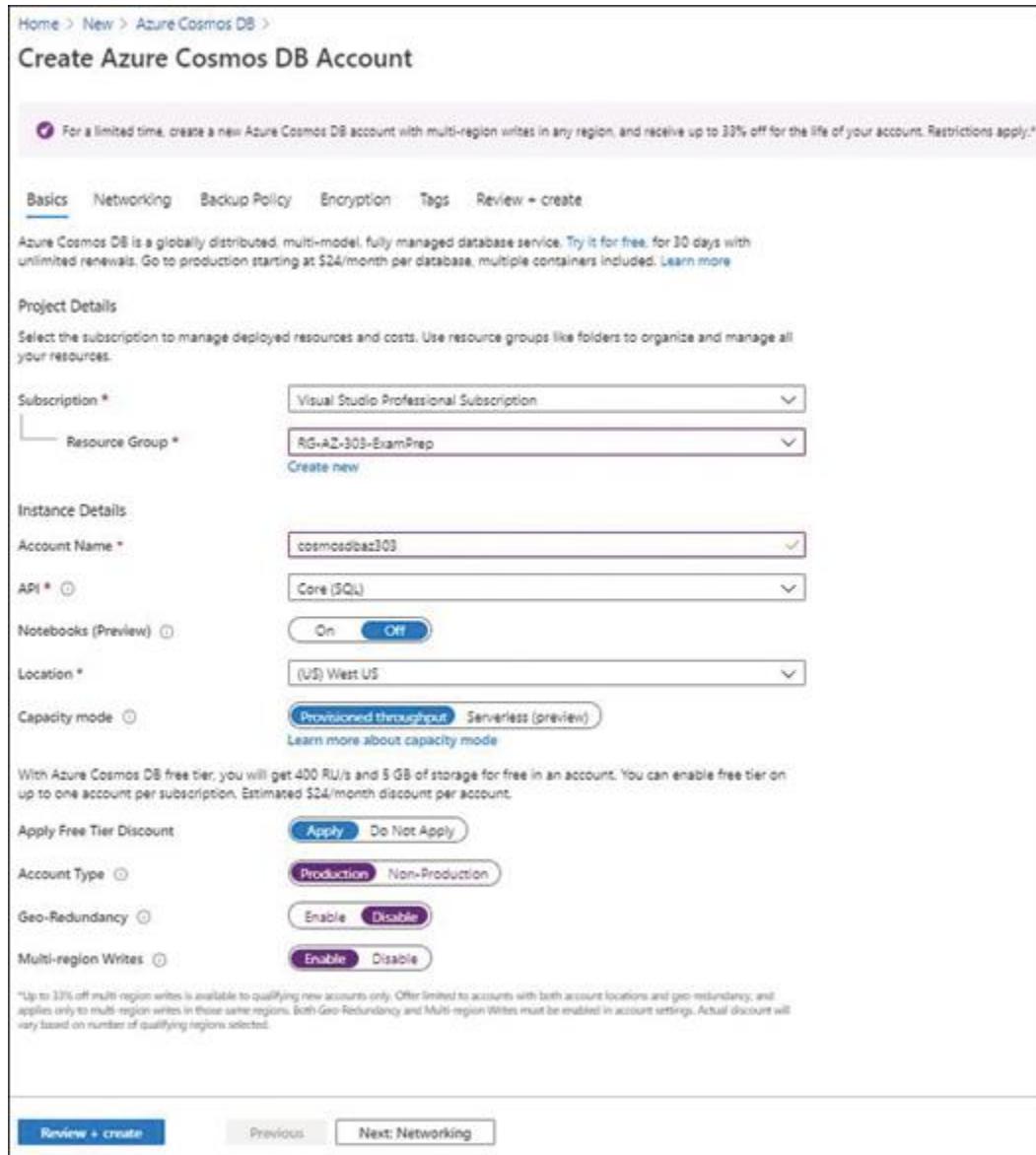


FIGURA 4-9 Asistente para crear una cuenta de Azure Cosmos

Establecer el nivel de coherencia adecuado para las operaciones

En las bases de datos distribuidas geográficamente, es probable que esté leyendo los datos que no son la última versión, lo que se denomina "lectura sucia". La coherencia, la latencia y el rendimiento de los datos no parecen mostrar mucha diferencia dentro de un centro de datos, ya que la replicación de datos es mucho más rápida y solo toma unos pocos

milisegundos. Sin embargo, en el escenario de distribución geográfica, cuando la replicación de datos tarda varios cientos de milisegundos, la historia es diferente, lo que aumenta las posibilidades de lecturas sucias. Cosmos DB proporciona las siguientes opciones de coherencia de datos para elegir con compensaciones entre latencia, disponibilidad y rendimiento.

- ■ **Fuerte.** Un alto nivel de coherencia garantiza que no haya lecturas sucias, y el cliente siempre lee la última versión de los datos comprometidos en las múltiples réplicas de lectura en una omultirregiones. La compensación con una opción de fuerte consistencia es el rendimiento. Cuando escribe en una base de datos, todos esperan a que Cosmos DB proporcione las últimas escrituras después de que se hayan guardado en todas las réplicas de lectura.
- ■ **Caducidad limitada.** La opción de obsolescencia limitada le permite decidir cuántos datos obsoletos puede tolerar una aplicación. Puede especificar las lecturas desactualizadas que desea permitir, ya sea por la versión (X) de las actualizaciones de un elemento o por el intervalo de tiempo (T), las lecturas podrían retrasarse en las escrituras.
- ■ **Sesión.** La sesión asegura que no haya lecturas sucias en las regiones de escritura. Una sesión tiene como alcance una sesión de cliente, y el cliente puede leer lo que escribió en lugar de tener que esperar a que los datos se confirmen globalmente.
- ■ **Prefijo consistente.** El prefijo consistente garantiza que las lecturas nunca estén fuera de orden de las escrituras. Por ejemplo, si un elemento de la base de datos se actualiza tres veces con las versiones V1, V2 y V3, el cliente siempre verá V1, V1V2 o V1V2V3. El cliente nunca los verá fuera de servicio, como V2, V1V3 o V2V1V3.
- ■ **Eventual.** Probablemente utilice la coherencia final cuando menos le preocupe la actualidad de los datos en las réplicas de lectura y el orden de las escrituras a lo largo del tiempo. Lo único que le importa es el nivel más alto de disponibilidad y baja latencia.

Para configurar la consistencia deseada en Cosmos DB, realice los siguientes pasos:

1. Inicie sesión en Azure Portal y navegue hasta su cuenta de Cosmos en **Grupo de recursos**.
2. En el panel **Consistencia predeterminada** (consulte la [Figura 4-10](#)), seleccione la consistencia deseada entre los cinco niveles de consistencia disponibles.
3. Para la **obsolescencia limitada**, defina el retraso en el tiempo o las operaciones que una aplicación puede tolerar.
4. Haga clic en **Guardar**.

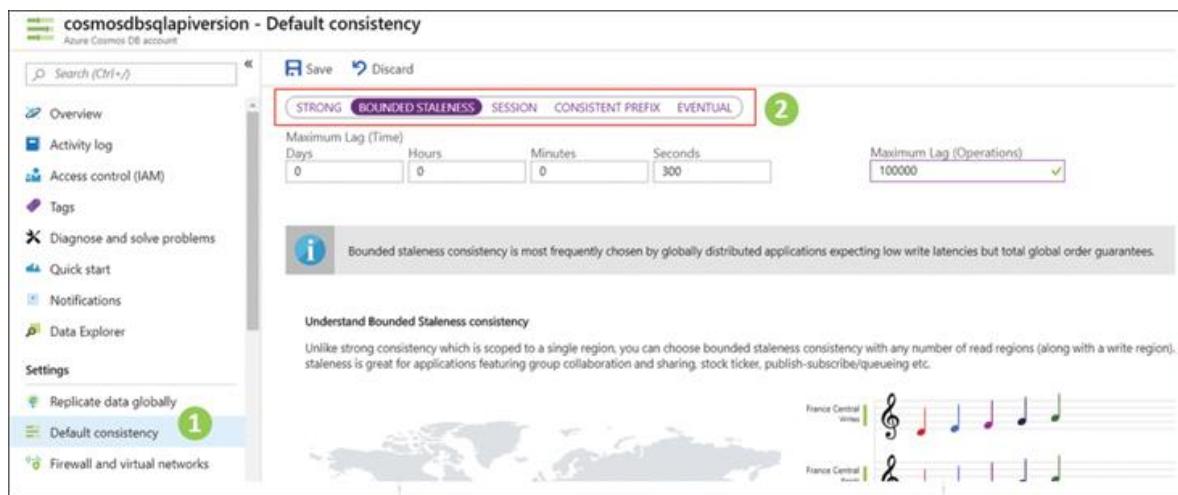


FIGURA 4-10 Configuración de la coherencia de Cosmos DB

Tenga en cuenta la continuidad del negocio y la recuperación ante desastres

Para una alta disponibilidad, se recomienda que configure Cosmos DB con escrituras multirregionales (al menos dos regiones). En caso de una interrupción regional, la conmutación por error es instantánea y la aplicación no tiene que sufrir ningún cambio; sucede de manera transparente detrás de la escena. Si está utilizando un nivel de coherencia predeterminado de Strong, no habrá pérdida de datos antes y después de la conmutación por error. Para la obsolescencia limitada, es posible que encuentre una posible pérdida de datos hasta el retraso (tiempo u operaciones) que haya configurado. Para las opciones Sesión, Prefijo consistente y Consistencia eventual, la pérdida de datos podría ser de hasta un máximo de cinco segundos.

Seleccione las API de Cosmos DB adecuadas

Actualmente, Azure Cosmos DB proporciona las siguientes API en disponibilidad general (GA). Vea la [Figura 4-11](#).

- API Core (SQL) y API MongoDB para datos de documentos JSON.
- Cassandra para un almacén de datos columnar o de familia de columnas.
- API de Azure Table para el almacén de datos de clave-valor.
- API de Gremlin (gráfico) para datos de gráficos.



Sugerencia para el examen

Puede crear solo una API de Cosmos DB por cuenta de Cosmos. Por ejemplo, si necesita crear una base de datos de Cosmos que utilice la API de SQL y una base de datos de Cosmos que utilice la API de MongoDB, deberá crear dos cuentas de Cosmos.

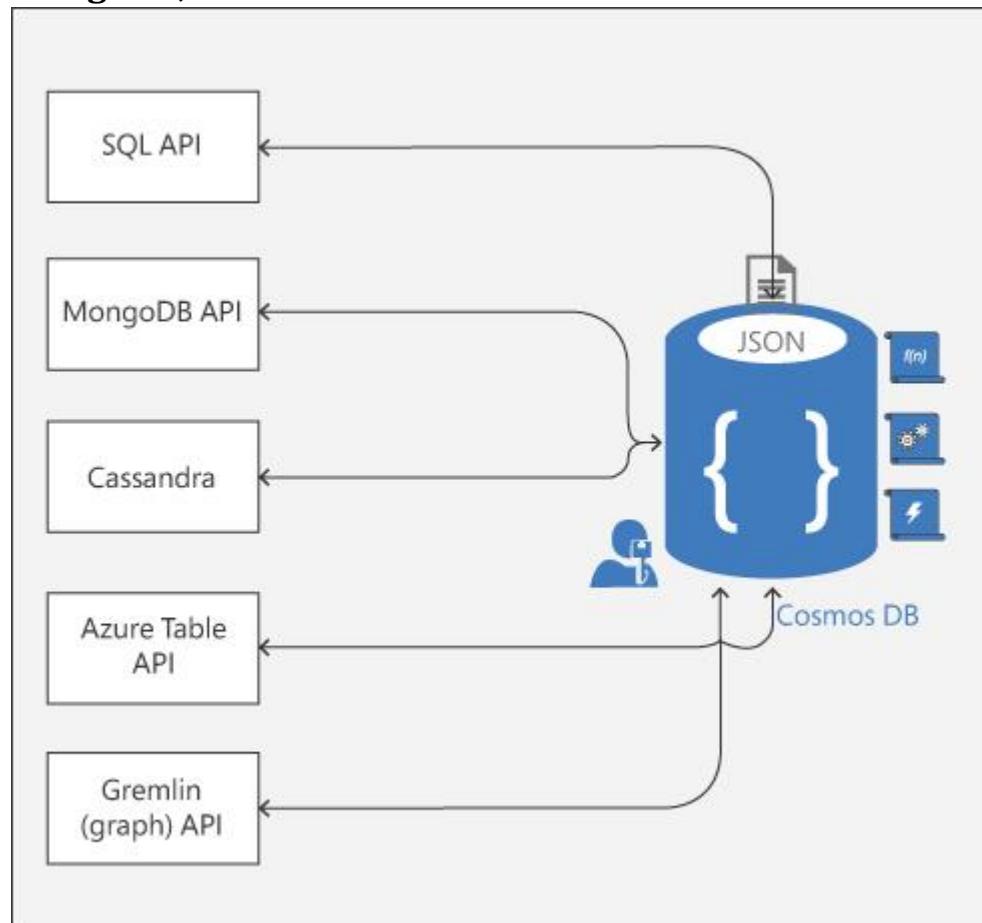


FIGURA 4-11 API de Cosmos DB

La elección de seleccionar API depende en última instancia de su caso de uso. Probablemente sea mejor que seleccione la API de SQL si su equipo ya tiene un conjunto de habilidades de T-SQL y está pasando de una base de datos relacional a una no relacional. Si está migrando una aplicación existente que usa MongoDB y no desea realizar ningún cambio en la aplicación actual, debe seleccionar una API de MongoDB; lo mismo ocurre con la API de Cassandra. De manera similar, para aprovechar un mejor rendimiento y escala global, use Table API si está usando Azure Table Storage. La API de Gremlin se utiliza para el modelado de gráficos entre entidades.

API de SQL

El lenguaje de consulta estructurado (SQL) es la API más popular adoptada por la industria para acceder e interactuar con los datos de Cosmos DB con las habilidades de SQL existentes. Al usar SQL API o Gremlin API, Cosmos DB también le brinda la capacidad de escribir código del lado del servidor mediante procedimientos almacenados, funciones definidas por el usuario (UDF) y desencadenadores, como se muestra en la [Figura 4-12](#). Estas son funciones de JavaScript escritas dentro de la base de datos de Cosmos DB y dentro del ámbito del contenedor.

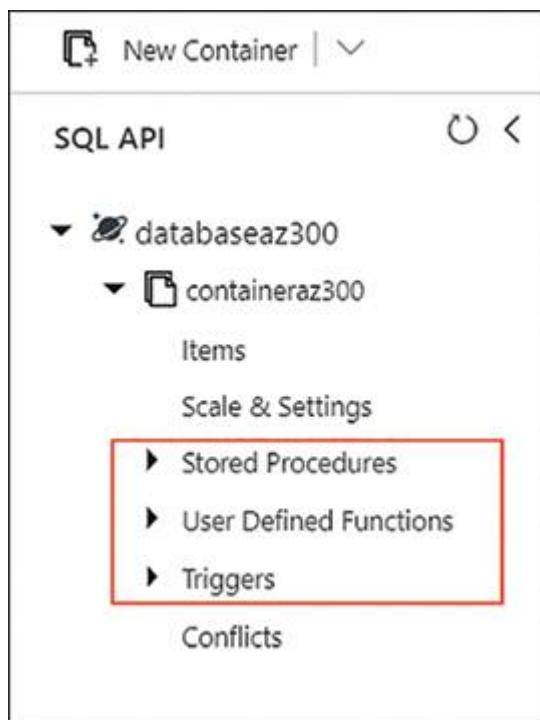


FIGURA 4-12 API SQL

Las siguientes son las consideraciones clave cuando elige escribir código del lado del servidor con Cosmos DB:

- ■ Los desencadenadores y procedimientos almacenados tienen un alcance en la clave de partición y deben proporcionarse con un parámetro de entrada para la clave de partición, mientras que las UDF tienen un alcance en el nivel de la base de datos.
- ■ Los procedimientos almacenados y los disparadores garantizan la atomicidad ACID (Atomicidad, Consistencia, Aislamiento y Durabilidad) como en cualquier base de datos relacional. Cosmos DB revierte automáticamente las transacciones en caso de alguna excepción; de lo contrario, están comprometidos con la base de datos como una sola unidad de trabajo.
- ■ Las consultas que utilizan desencadenadores y procedimientos almacenados siempre se ejecutan en la réplica principal, ya que están destinadas a operaciones de escritura para garantizar una coherencia sólida para una réplica secundaria. Por el contrario, las UDF se pueden escribir en la réplica principal o secundaria, ya que las UDF son solo para operaciones de lectura.
- ■ El código del lado del servidor debe completarse dentro del límite del umbral de tiempo de espera especificado, o debe implementar un modelo de continuación por lotes para el código de larga ejecución. Si el código no se completa dentro del tiempo, Cosmos DB revierte toda la transacción automáticamente.
- ■ Hay dos tipos de activadores que puede configurar:
 - ■ **Pre-disparadores.** Como lo define el nombre, puede invocar cierta lógica en los contenedores de la base de datos antes de que se creen, actualicen o eliminen los elementos.
 - ■ **Post-desencadenantes.** Los disparadores posteriores se ejecutan después de que los datos se escriben o actualizan.

¿Necesita más revisión? Guía de referencia de consultas SQL para Cosmos DB

Para obtener más información sobre los operadores y ejemplos de consultas SQL, visite el documento de Microsoft "Introducción a las consultas SQL" en <https://docs.microsoft.com/en-us/azure/cosmos-db/sql-query-getting-started#GettingStarted>.

API de MongoDB

Puede cambiar de MongoDB a Cosmos DB y aprovechar las excelentes características de servicio, escalabilidad, distribución global llave en mano, varios niveles de consistencia, copias de seguridad automáticas e indexación sin tener que cambiar el código de su aplicación. Todo lo que necesita hacer es crear un Cosmos DB para la API de MongoDB (consulte la figura 4-13). En el momento de redactar este libro, la API MongoDB de Cosmos DB es compatible con la última versión 3.6 del servidor MongoDB, y puede utilizar herramientas, bibliotecas y controladores MongoDB de cliente de código abierto existentes para interactuar con Cosmos DB.

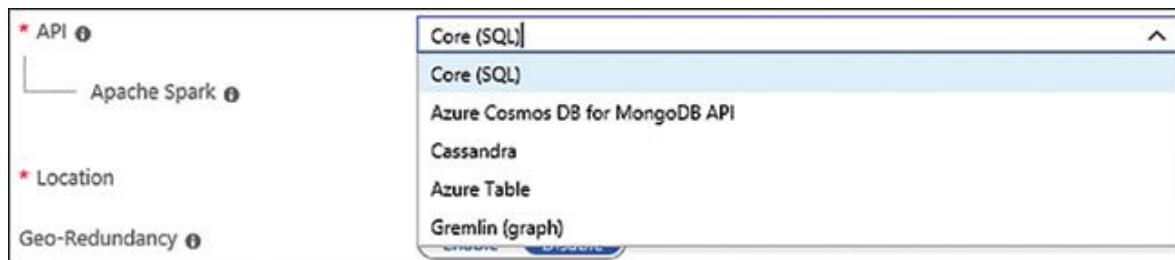


FIGURA 4-13 API compatibles con Cosmos DB

API de tabla

Al igual que la API de MongoDB, las aplicaciones que se escribieron originalmente para el almacenamiento de Azure Table se pueden migrar sin problemas a Cosmos DB sin tener que cambiar el código de la aplicación. En este caso, crearía una tabla de Cosmos DB para Azure a partir de las opciones de la API.

Los SDK de cliente en .Net, Java, Python y Node.js están disponibles para Table API. La migración de Azure Table Storage a Cosmos DB le brinda las

capacidades premium del servicio, como hemos discutido desde el comienzo de este capítulo.

API de Cassandra

Puede cambiar de Apache Cassandra y migrar a Cosmos DB y aprovechar las mejores características de Cosmos DB sin tener que cambiar el código de su aplicación. En el momento de redactar este documento, la API de Cassandra de Cosmos DB es compatible con el lenguaje de consulta Cassandra V4, y puede usar herramientas, bibliotecas y controladores de cliente de código abierto Cassandra existentes para comunicarse con Cosmos DB.

API de Gremlin

La API de Gremlin se utiliza para generar y visualizar un gráfico entre entidades de datos. Cosmos DB es totalmente compatible con un marco de computación de gráficos de código abierto llamado Apache TinkerPOP. Utilice esta API cuando desee presentar relaciones complejas entre entidades en forma gráfica. La mecánica subyacente del almacenamiento de datos es similar a lo que aprendió en las secciones anteriores para otras API, como SQL o Table. Dicho esto, los datos de su gráfico obtienen el mismo nivel de

- ■ Escalabilidad
- ■ Rendimiento y rendimiento
- ■ Indexación automática
- ■ Distribución global con alta disponibilidad garantizada

Los componentes críticos de cualquier base de datos de gráficos son los siguientes:

- ■ **Vértices.** Los vértices denotan un objeto discreto como una persona, un lugar o un evento. Si piensa en la analogía de un sistema de reserva de aerolíneas que discutimos en el ejemplo de la API de SQL, un viajero es un vértice.
- ■ **Bordes.** Los bordes denotan una relación entre vértices. La relación puede ser unidireccional o bidireccional. Por ejemplo, en nuestra analogía, una aerolínea es un vértice. La relación entre el

viajero y la aerolínea que define a qué aerolínea viajó dentro de un año determinado se considera una ventaja.

- ■ **Propiedades.** Las propiedades incluyen la información entre los vértices y los bordes, por ejemplo, las propiedades de un viajero, compuestas por su nombre, fecha de nacimiento, dirección, etc. Las propiedades del borde (aerolínea) podrían ser el nombre de una aerolínea, rutas de viaje, etc.

La API de Gremlin se usa ampliamente para resolver problemas en un modelo de relación comercial complejo como las redes sociales, la recomendación geoespacial o científica en el comercio minorista y otras empresas.

A continuación, se ofrece un vistazo rápido a la analogía de las reservas de aerolíneas y cómo crear vértices y aristas mediante Azure Portal. Puede hacer esto mediante programación utilizando los SDK disponibles en .NET y otros lenguajes.

Creando vértices

Utilice los siguientes pasos para crear un viajero de vértice en la base de datos del gráfico:

1. Inicie sesión en Azure Portal y navegue hasta la cuenta de Cosmos DB que creó para la API de Gremlin.
2. En la hoja **Explorador de datos**, cree una nueva base de datos de gráficos especificando el nombre, la capacidad de almacenamiento, el rendimiento y una clave de partición para la base de datos. Debe proporcionar el valor para la clave de partición que defina. En nuestro ejemplo, la clave de partición es graphdb y su valor es az303 al crear vértices.
3. Una vez creada la base de datos, navegue hasta la ventana **Graph Query**, como se muestra en la [Figura 4-14](#), y ejecute los siguientes comandos para crear vértices, bordes y varias propiedades para viajeros y aerolíneas:

[Haga clic aquí para ver la imagen del código](#)

```
g.addV ('viajero'). property ('id', 'thomas'). property  
('firstName', 'Thomas').
```

```
property ('Apellido', 'Joe'). property ('Dirección',
'Ohio'). property ('Año de viaje',
2018) .property ('graphdb', 'az303')

g.addV ('viajero'). property ('id', 'Gurvinder').
property ('FirstName',
'Gurvinder'). Property ('LastName', 'Singh'). Property
('Address', 'Chicago') .

property ('Año de viaje', 2018) .property ('graphdb',
'az303')

g.addV ('Compañía aérea'). propiedad ('id', 'United
Airlines') .

propiedad ('CompanyName', 'United Airlines'). propiedad
('Ruta 1', 'Chicago') .

propiedad ('Ruta 2', 'Ohio'). propiedad ('graphdb',
'az303')

g.addV ('Compañía aérea'). propiedad ('id', 'American
Airlines') .

property ('CompanyName', 'American Airlines'). property
('Ruta 1', 'California') .

propiedad ('Ruta 2', 'Chicago'). propiedad ('graphdb',
'az303')

g.addV ('Compañía aérea'). propiedad ('id', 'Southwest
Airlines') .

property ('CompanyName', 'Southwest Airlines') .
property ('Ruta 1', 'Chicago') .
```

```

propiedad ('Ruta 2', 'California'). propiedad
('graphdb', 'az303')

g.addV ('Compañía aérea'). property ('id', 'Delta
Airlines'). property ('CompanyName',
'Delta Airlines'). Propiedad ('Ruta 1', 'Chicago').
Propiedad ('Ruta 2', 'Ohio').

propiedad ('graphdb', 'az303')

```

FIGURA 4-14 API de Gremlin

En los comandos de Gremlin anteriores, `g` representa su base de datos gráfica y `g.addV ()` se usa para agregar vértices. `Properties ()` se utiliza para asociar propiedades con vértices.

Creando bordes

Ahora que ha agregado vértices para viajeros y aerolíneas, debe definir la relación de una manera que explique a qué aerolínea ha viajado un viajero en un año determinado y si los viajeros se conocen entre sí.

Cree un borde en el vértice 'viajero' que creó anteriormente. Al igual que los vértices que creó en el paso 3 de la sección anterior, siga el mismo método y ejecute los siguientes comandos en la ventana del gráfico para crear bordes, como se muestra en la [Figura 4-14](#) :

[Haga clic aquí para ver la imagen del código](#)

```

gV ('thomas'). addE ('año de viaje'). to (gV ('Delta
Airlines'))

gV ('thomas'). addE ('año de viaje'). a (gV ('American
Airlines'))

gV ('thomas'). addE ('año de viaje'). a (gV ('United
Airlines'))

gV ('Gurvinder'). addE ('año de viaje'). a (gV ('Delta
Airlines'))

gV ('Gurvinder'). addE ('año de viaje'). a (gV ('United
Airlines'))

gV ('thomas'). addE ('saber'). to (gV ('Gurvinder'))

```

En este ejemplo, `addE ()` define una relación con un viajero de vértice y una aerolínea usando `gV ()`. Después de ejecutar los comandos anteriores, puede ver la conexión entre las entidades en el gráfico mediante Azure Portal, como se muestra en la [Figura 4-15](#).

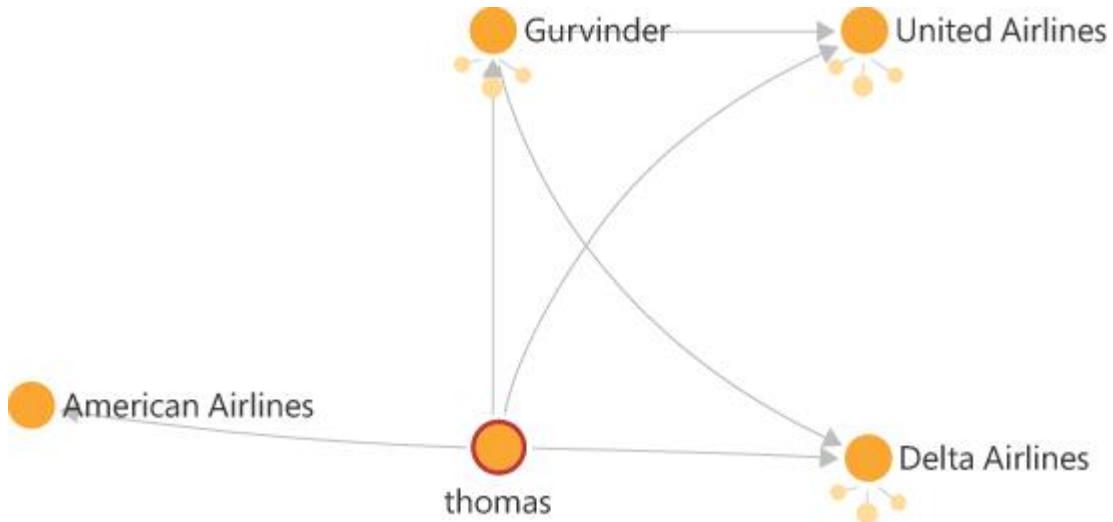


FIGURA 4-15 Gráfico API de Gremlin

Ahora comprende las diferentes API estándar de la industria que están disponibles para elegir, pero la pregunta es, ¿cómo tomar una decisión? [La Tabla 4.1](#) describe los criterios de decisión, que le ayudarán a elegir la API correcta.

TABLA 4-1 Criterios de decisión de API

Criterios	SQL CORE	MongoDB	Cassandra	API de tabla
¿Está iniciando un nuevo proyecto y su equipo tiene el conjunto de habilidades de consultas SQL?	X			
¿Su aplicación actual utiliza MongoDB y desea utilizar las habilidades, el código y la migración sin problemas existentes?		X		
¿Su aplicación necesita impulsar la relación entre entidades y visualizarlas en un gráfico?				
¿Su aplicación actual usa almacenamiento de tabla y tiene grandes volúmenes de datos? ¿Quiere minimizar el tiempo de migración y utilizar el código de aplicación actual al cambiar a Cosmos DB?			X	X

Configurar réplicas en Cosmos DB

Para aplicaciones distribuidas globalmente, es posible que desee distribuir la base de datos de su aplicación en varios centros de datos, para un mejor rendimiento y una baja latencia de lectura / escritura. Además de replicar bases de datos en varios centros de datos, es posible que también desee habilitar patrones activo-activo mediante funciones multimaestro. El multimaestro permite que la aplicación escriba en la base de datos más cercana a la región de la aplicación. Azure Cosmos DB tiene todas estas capacidades y automáticamente se ocupa de la coherencia final en las bases de datos entre regiones para garantizar que se mantenga la coherencia global y la integridad de los datos.

Para configurar la distribución global de sus Cosmos DB y habilitar múltiples réplicas en las regiones, siga los siguientes pasos:

1. En Azure Portal, navegue hasta la cuenta de Cosmos.

2. Haga clic en el menú **Replicar datos globalmente** (consulte la [Figura 4-16](#)). En el panel del lado derecho, puede agregar una región seleccionando el ícono hexagonal para la región deseada en el mapa, o puede elegir en el menú desplegable después de hacer clic en **+ Agregar región**.
3. Para eliminar regiones, borre una o más regiones del mapa seleccionando los hexágonos azules que se muestran con marcas de verificación.



FIGURA 4-16 Configuración de réplicas de varias regiones para Azure Cosmos DB

4. Haga clic en **Habilitar escrituras de múltiples regiones**. Las escrituras multimaestro o multirregión le permiten aprovechar una función complementaria denominada **Zona de disponibilidad** recomendada para cargas de trabajo de producción.
5. Haga clic en **Guardar** para confirmar los cambios.

[La Tabla 4-2](#) proporciona una comprensión justa de las diferentes configuraciones de cuenta de Cosmos entre las que puede elegir según la disponibilidad de la aplicación y los requisitos de rendimiento.

TABLA 4-2 Configuraciones de cuentas de Cosmos DB

Región única	Varias regiones con escrituras de una sola región	Multirregión con escrituras multirregionales
Proporciona SLA del 99,99 por ciento en operaciones de lectura / escritura.	Proporciona SLA del 99,999 por ciento en operaciones de lectura y del 99,99 por ciento en operaciones de escritura.	Proporciona SLA del 99,99999 por ciento en operaciones escritura.
La capacidad de zona de disponibilidad no está disponible en una sola región.	La capacidad de zona de disponibilidad no está disponible con un solo maestro.	El soporte de la zona de disponibilidad proporciona resistencia adicional y disponibilidad dentro de los datos.
La cuenta de una sola región puede experimentar interrupciones durante las interrupciones regionales.	Con lectura multi-región y maestro de escritura única, las cargas de trabajo de producción deben tener la Habilitar conmutación automática por error de ajuste cambia a On para permitir Azure para la conmutación por error automáticamente a su cuenta cuando hay un desastre regional. En esta configuración, la disponibilidad y la pérdida de datos están sujetas al tipo de nivel de coherencia que se utilice.	En escrituras multirregionales, las regiones de lectura se actualizan en la cuenta principal y se convertirán en regiones de escritura y, por lo tanto, la configuración proporciona disponibilidad y la latencia más baja para las lecturas y escrituras de las cargas de trabajo.

Regiones Azure emparejadas con redundancia geográfica *importantes*

Para BCDR, debe elegir regiones basadas en regiones emparejadas de Azure para un mayor grado de aislamiento de fallas y disponibilidad mejorada. Consulte la documentación de Microsoft en <https://docs.microsoft.com/en-us/azure/best-practices-availability-paired-regions>.

HABILIDAD 4.2: IMPLEMENTAR BASES DE DATOS SQL DE AZURE

Las empresas pequeñas, medianas y grandes han estado utilizando bases de datos relacionales durante décadas como una forma preferida de almacenar datos para sus aplicaciones de pequeña o gran escala. En una base de datos relacional, los datos se almacenan como una colección de elementos de datos con una relación predefinida entre ellos. Los datos de cualquier base de datos relacional se almacenan en filas y columnas. Cada fila de la tabla tiene una clave única que representa una colección de valores asociados con una entidad y se puede asociar con filas de otras tablas en la base de datos que define la relación entre entidades. Cada columna de una fila contiene los valores de una entidad u objeto. Además, las bases de datos relacionales vienen con la capacidad incorporada de administrar la integridad de los datos, la coherencia transaccional y el cumplimiento de ACID (atomicidad, coherencia, aislamiento y durabilidad).

Como parte de las ofertas de plataforma como servicio (PaaS), Microsoft proporciona las siguientes bases de datos administradas para elegir según las necesidades de su aplicación:

- ■ **Base de datos SQL de Azure.** Azure SQL Database es un producto principal de Microsoft y la base de datos relacional más popular en la nube.
- ■ **Azure Synapse Analytics.** Anteriormente conocido como Azure SQL Data Warehouse, es una base de datos relacional para análisis de Big Data y almacenamiento de datos empresariales.
- ■ **Base de datos de Azure para MySQL.** Azure Database for MySQL es una base de datos como servicio completamente administrada donde Microsoft ejecuta y administra todos los mecanismos de la base de datos MySQL Community Edition en la nube.
- ■ **Base de datos Azure para PostgreSQL.** Al igual que MySQL, esta es una oferta de base de datos como servicio completamente administrada basada en el motor de base de datos Postgres de código abierto.

- **Base de datos de Azure para MariaDB**. Azure Database for MariaDB también es una base de datos como servicio administrada, de alta disponibilidad y escalable basada en el motor de servidor MariaDB de código abierto.

Independientemente de la base de datos que seleccione para las necesidades de su aplicación, Microsoft administra las siguientes características clave de cualquier oferta de servicios basados en la nube:

- Alta disponibilidad y escala bajo demanda
- Continuidad comercial
- Copias de seguridad automatizadas
- Seguridad y cumplimiento de nivel empresarial

Esta habilidad cubre cómo:

- [Configurar la configuración de la base de datos SQL de Azure](#)
- [Implementar instancias administradas de Azure SQL Database](#)
- [Configurar HA para una base de datos SQL de Azure](#)
- [Publicar una base de datos SQL de Azure](#)

Aprovisionar y configurar bases de datos relacionales

En esta sección, nos sumergimos en los aspectos críticos de cómo configurar una base de datos relacional en la nube y configurar las características nativas de la nube que vienen con las ofertas de servicios nativos.

Base de datos SQL de Azure

Azure SQL Database es el núcleo de Microsoft y la base de datos relacional administrada más popular. El servicio tiene los siguientes tipos de ofertas de bases de datos.

- **Base de datos única.** Con una sola base de datos, asigna procesamiento y almacenamiento preasignados a la base de datos.
- **Piscinas elásticas.** Con los grupos elásticos, crea una base de datos dentro del grupo de bases de datos y comparten los

mismos recursos para satisfacer una demanda de uso impredecible.

- ■ **Instancia administrada.** El tipo de instancia administrada del servicio ofrece una compatibilidad cercana al 100 por ciento con SQL Server Enterprise Edition con características de seguridad adicionales.

Nota Disponibilidad regional de los tipos de servicios de SQL Azure

Aunque el examen AZ-303 no espera que se meta en las malas hierbas de la disponibilidad regional del servicio Azure SQL Database, como arquitecto, debe conocer esta parte. Consulte "Productos disponibles por región"

en <https://azure.microsoft.com/en-us/global-infrastructure/services/?products=sql-database®ions=all> .

Es fundamental comprender los modelos de compra disponibles para elegir el nivel de servicio adecuado que satisfaga las necesidades de su aplicación. Azure SQL Database incluye los siguientes modelos de compra:

- ■ **Modelo de DTU (Unidades de transacción de base de datos).** Las DTU son la combinación de recursos informáticos, de almacenamiento y de E / S que asigna previamente al crear una base de datos en el servidor lógico. Para una sola base de datos, la capacidad se mide en DTU; para las bases de datos elásticas, la capacidad se mide en eDTU. Microsoft ofrece tres niveles de servicio, como se enumeran a continuación en este modelo, que brindan la flexibilidad de elegir el tamaño del proceso con una cantidad fija y preconfigurada de almacenamiento, un período de retención fijo y un precio fijo.
 - ■ **Básico.** Adecuado para carga de trabajo de desarrollo / prueba o genérico, no exige alto rendimiento y baja latencia. Respaldado por un SLA del 99,99 por ciento y una latencia de E / S de 5 ms (lectura) y 10 ms (escritura). La retención máxima de copias de seguridad en un momento determinado para el nivel básico es de 7 días.
 - ■ **Estándar.** Adecuado para carga de trabajo de desarrollo / prueba o genérico, no exige alto rendimiento y baja latencia. Respaldado por un SLA del

99,99 por ciento y una latencia de E / S de 5 ms (lectura) y 10 ms (escritura). La retención de respaldo máxima en un momento dado para el nivel estándar es de 35 días.

- ■ **Premium.** Adecuado para cargas de trabajo de producción que exigen alto rendimiento y baja latencia. Respaldado por un SLA del 99,99 por ciento y una latencia de E / S de 2 ms (lectura / escritura). La retención máxima de copias de seguridad en un momento dado para el nivel premium es de 35 días.
- ■ **Modelo de núcleo virtual (núcleo virtual).** El modelo basado en núcleos virtuales es el modelo de compra recomendado por Microsoft en el que obtiene la flexibilidad de escalar de forma independiente el procesamiento y el almacenamiento para satisfacer las necesidades de su aplicación. Además, tiene la opción de usar su licencia de SQL Server existente para ahorrar hasta el 55 por ciento del costo con la Ventaja híbrida de Azure (AHB) o aprovechar el descuento significativo al reservar recursos informáticos con la instancia reservada (RI) de Azure SQL Database. El modelo de compra de núcleos virtuales proporciona dos niveles de servicio, como se indica a continuación:
 - ■ **Propósito general.** Adecuado para cargas de trabajo genéricas de desarrollo / prueba y respaldado por un SLA del 99,99 por ciento con una latencia de E / S de 5 a 10 ms. El procesamiento y el almacenamiento en el nivel de uso general tiene tres opciones:
 - ■ **Aprovisionado.** Computación y almacenamiento preasignados y se factura por hora.
 - ■ **Sin servidor.** Diseñado para una sola base de datos que necesita escalado automático bajo demanda.
 - ■ **Hiperescala.** Adecuado para cargas de trabajo de producción y destinado principalmente a clientes con muchas bases de datos con necesidades de escalado de hasta 100 TB.

- **Crítico para la empresa.** Recomendado para cargas de trabajo de producción y respaldado por un SLA del 99,99 por ciento con una latencia de E / S de 1-2 ms y un mayor grado de tolerancia a fallas. También puede configurar Read Scale-Out para descargar su carga de trabajo de solo lectura automáticamente sin costo adicional.

Puede elegir un modelo de núcleo virtual en lugar de un modelo de DTU por las siguientes razones:

- Puede aprovechar la función de beneficio híbrido y ahorrar hasta un 55 por ciento del costo de la base de datos mediante el uso de sus licencias de servidor SQL local.
- Puede escalar de forma independiente la computación, las IOPS y el almacenamiento.
- Puede elegir la generación de hardware que podría mejorar el rendimiento de su base de datos. La generación de hardware disponible en el modelo vCore incluye Gen4 / Gen5, M-series (memoria optimizada) y FsV2 series (computación optimizada).

Configuración de la configuración de la base de datos SQL de Azure

En esta sección, aprenderá a usar las diferentes características de Azure SQL Database. Comenzamos creando un servidor de base de datos y una única base de datos SQL de Azure. Un servidor de base de datos es una construcción lógica que actúa como un contenedor de base de datos. Puede agregar una o más bases de datos de Azure SQL en el contenedor y configurar opciones como inicios de sesión de la base de datos, reglas de firewall, auditoría, copias de seguridad y políticas de seguridad. La configuración aplicada en el nivel del servidor de la base de datos se aplica automáticamente a todas las bases de datos del servidor. También puede sobrescribirlos para bases de datos individuales. Siga los pasos a continuación para crear una base de datos SQL de Azure.

1. Inicie sesión en Azure Portal.

2. En la hoja de **navegación** del lado izquierdo del portal, haga clic en **Crear un recurso** y busque **Base de datos SQL** ; que abre la página que se muestra en la Figura 4-17 .

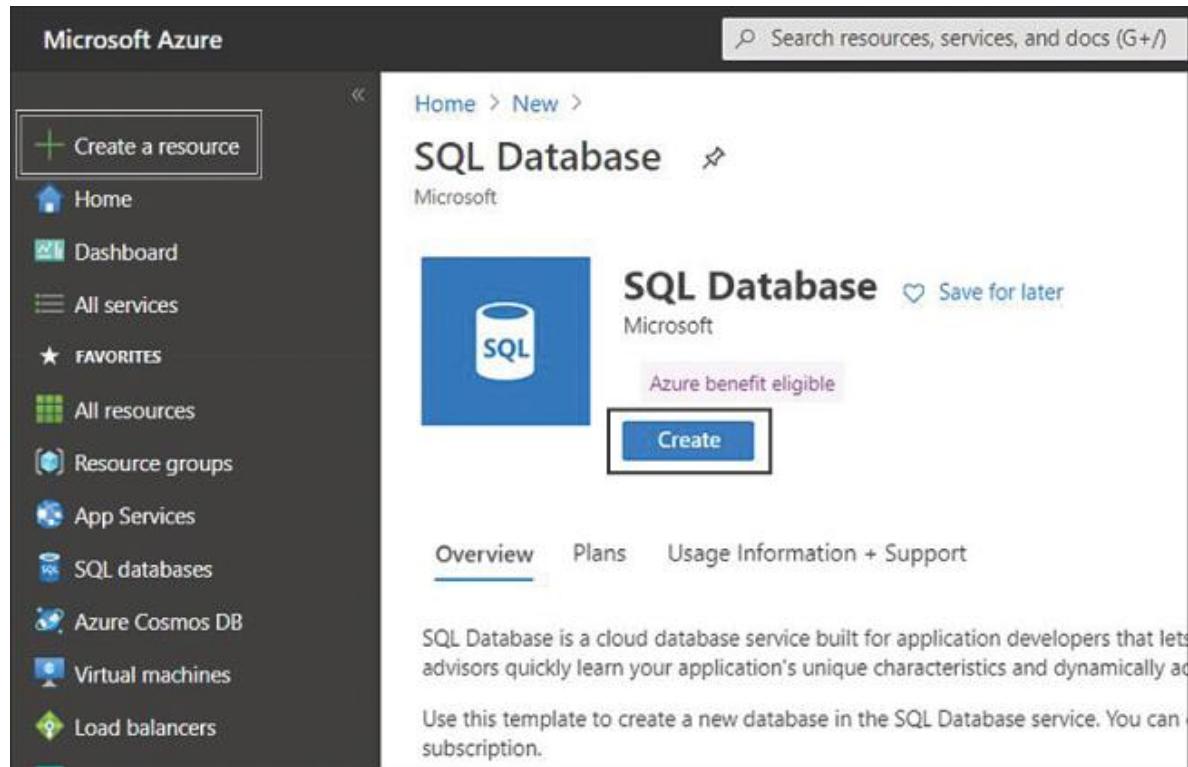


FIGURA 4-17 Crear una base de datos SQL

3. En la pantalla **Crear base de datos SQL** (consulte la Figura 4-18), complete el campo **Nombre de la base de datos** y seleccione **Suscripción , Grupo de recursos y Servidor** . Si SQL Server no existe, puede crear uno haciendo clic en **Crear nuevo** (consulte la Figura 4-19).

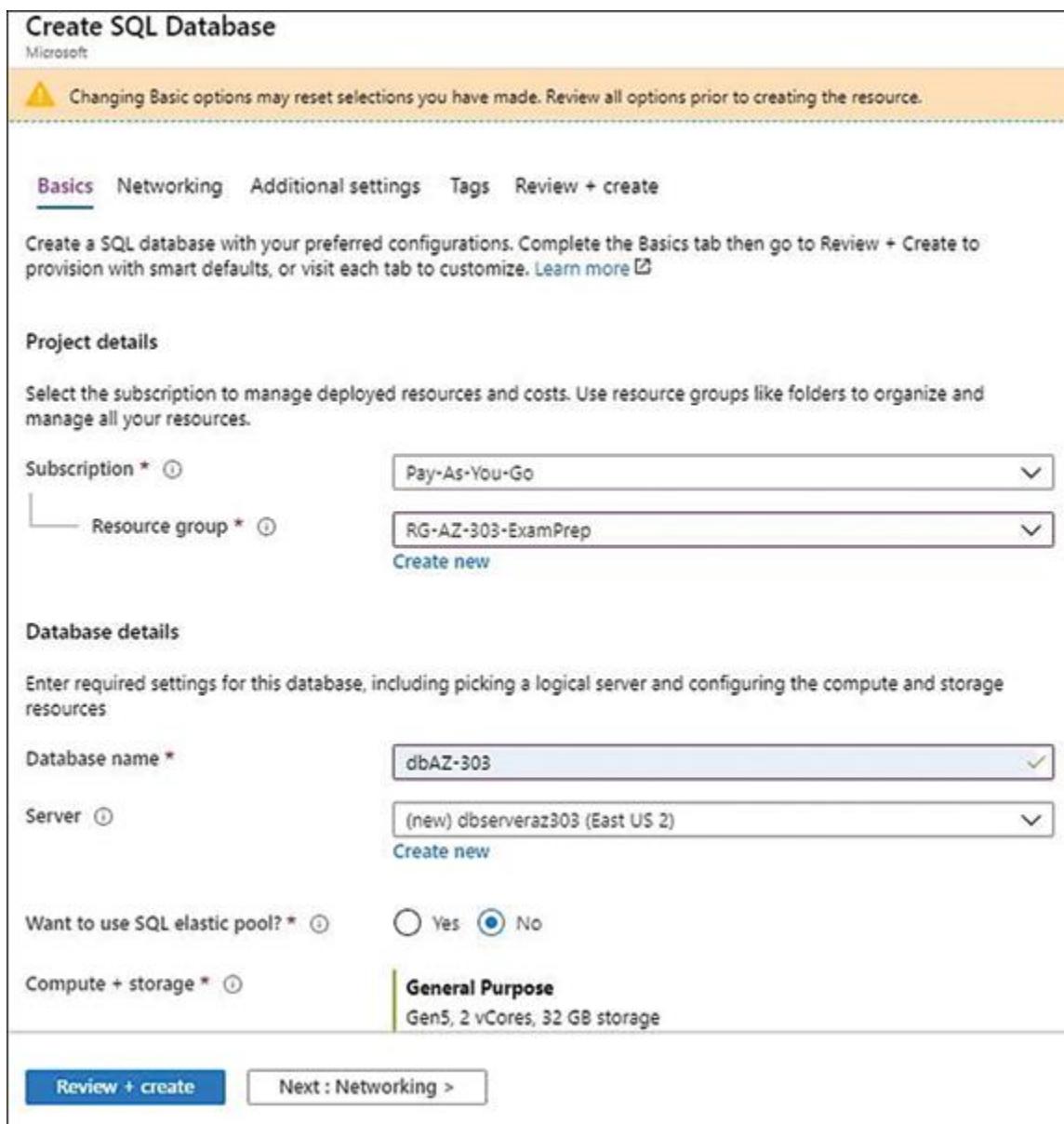


FIGURA 4-18 Crear base de datos SQL



FIGURA 4-19 Cree un servidor SQL

4. Haga clic en **Next Networking** para pasar a la pestaña **Networking**. De forma predeterminada, se puede acceder a la base de datos mediante un punto final público, pero puede restringir el acceso a través de la Internet pública en la pestaña **Redes**. Puede omitir esto, ya que solo estamos creando una base de datos con fines de demostración.
5. También puede ignorar la pestaña **Configuración adicional** que le permite configurar configuraciones opcionales, como la replicación geográfica. Haga clic en **Siguiente etiquetas**.
6. La siguiente pestaña es **Etiquetas**. Las etiquetas se utilizan para etiquetar sus recursos y agruparlos con fines de devolución de cargo, facturación y control. Puede omitir este paso y hacer clic en **Revisar + Crear**.
7. En la pantalla de revisión, puede revisar su configuración y hacer clic en **Crear** para iniciar la implementación de la base de datos, como se muestra en la [Figura 4-20](#).

Create SQL Database

Microsoft

Basics Networking Additional settings Tags **Review + create**

Product details

SQL database by Microsoft Terms of use Privacy policy	Estimated cost per month 380.03 USD View pricing details
---	---

Terms

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. For additional details see [Azure Marketplace Terms](#).

Basics

Subscription	Pay-As-You-Go
Resource group	RG-AZ-303-ExamPrep
Region	East US 2
Database name	adminaz303
Server	(new) dbserveraz303
Compute + storage	General Purpose: Gen5, 2 vCores, 32 GB storage

Networking

Allow Azure services and resources to access this server	No
Private endpoint	None

Create [< Previous](#) [Download a template for automation](#)

FIGURA 4-20 Revisión y creación

Una vez creada la base de datos, puede navegar a la base de datos en Azure Portal buscando la base de datos SQL en el cuadro de búsqueda **Buscar recursos, servicios y documentos** en la parte superior. La hoja Azure SQL Database aparece como se muestra en la [Figura 4-21](#).

The screenshot shows the Azure portal's 'SQL databases' blade. At the top, there are buttons for 'Add', 'Reservations', 'Edit columns', 'Refresh', 'Assign tags', and 'Delete'. Below this, a message encourages users to try the new Azure SQL resource browser. A section for 'Subscriptions' shows a Visual Studio Professional Subscription. The main table lists one item: 'sqldbaaz303examprep' (Status: Online, Replication role: None, Server: sqlserveraz303exam, Pricing tier: Basic, Location: East US). There are also filters for 'Name', 'All resource groups', 'All locations', and 'All tags'.

FIGURA 4-21 Hoja de bases de datos SQL

Ahora tenemos Azure SQL Database en funcionamiento. En la siguiente sección, aprenderá acerca de varias configuraciones de base de datos para Azure SQL Database que puede configurar para sus escenarios comerciales específicos.

- ■ **Administrar copias de seguridad.** La política de respaldo es imperativa para la continuidad del negocio y la recuperación ante desastres de cualquier aplicación de línea de negocio (LOB). La estrategia de copia de seguridad protege su base de datos de errores humanos, como la eliminación accidental de datos o la corrupción de datos o las interrupciones del centro de datos. Las copias de seguridad se cifran automáticamente en reposo mediante cifrado de datos transparente (TDE). Azure SQL Database le ofrece las siguientes opciones para administrar las copias de seguridad de la base de datos.
- ■ **Copias de seguridad automatizadas.** Independientemente del nivel de servicio que elija, las bases de datos SQL de Azure se respaldan automáticamente en almacenamiento de blob con redundancia geográfica de acceso de lectura (RA-GRS) para facilitar la alta disponibilidad de las copias de seguridad incluso en el caso de una interrupción del centro de datos . Las copias de seguridad automáticas se conocen como restauración en un momento determinado (PITR). En PITR, la copia de seguridad completa se realiza semanalmente, una copia de seguridad diferencial cada hora y una copia de seguridad

del registro de transacciones cada 5 a 10 minutos. Las copias de seguridad de PITR se conservan durante 7 días para el nivel básico y hasta 35 días para el nivel premium estándar en el modelo de compra de DTU. Para el modelo de compra de núcleos virtuales, el período de retención es de 7 a 35 días para los niveles de Propósito general y Crítico para la empresa y de 7 días para el nivel Hiperescala.

- **Retención de copias de seguridad a largo plazo.** La opción de **retención de copias de seguridad a largo plazo**, también conocida como **LTR**, mantiene la copia de seguridad completa de la base de datos y se utiliza para conservar las copias de seguridad de la base de datos más allá de los 35 días, hasta 10 años. LTR se puede habilitar para bases de datos únicas o agrupadas. En el momento en que se escribió este libro, las LTR no están disponibles para las bases de datos de instancias administradas.

Siga estos pasos para configurar la retención de copias de seguridad a largo plazo mediante Azure Portal:

1. Inicie sesión en Azure Portal en <https://portal.azure.com> con sus credenciales de suscripción y busque **SQL Server** en el cuadro de búsqueda.
2. En la hoja de **SQL Server**, elija **Administrar copias de seguridad**, como se muestra en la [Figura 4-22](#).

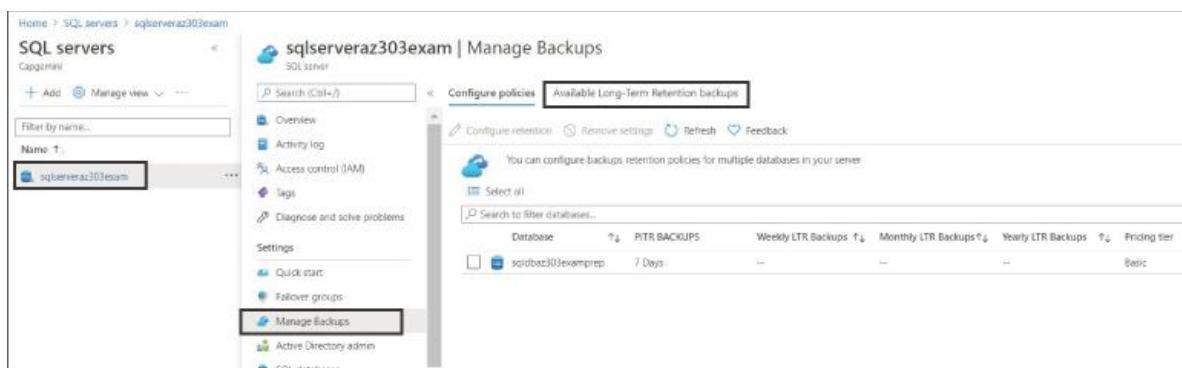


FIGURA 4-22 Configuración de políticas de respaldo

3. Elija la base de datos para la que desea configurar una política de respaldo y haga clic en **Configurar políticas**. Vea la [Figura 4-23](#).

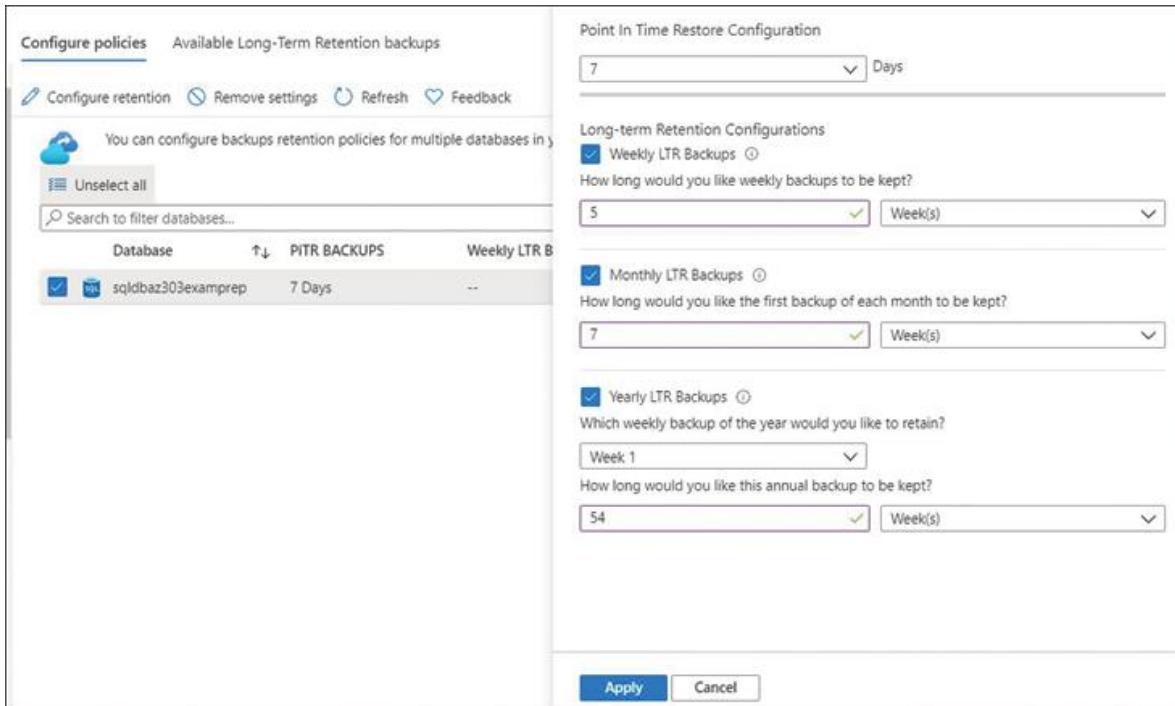


FIGURA 4-23 Configuración de la retención a largo plazo

Como puede ver, las políticas de copia de seguridad de PITR se crean automáticamente y puede modificar el período de retención entre 7 y 35 días. Las políticas de retención a largo plazo se pueden establecer en días, semanas, meses o años. La política de LTR que se muestra en la [Figura 4-23](#) se establece de la siguiente manera:

- **Backups LTR semanales.** Cada copia de seguridad se conserva durante 5 semanas.
 - **Copias de seguridad mensuales de LTR.** La primera copia de seguridad se realiza cada mes y se conserva durante 7 semanas.
 - **Copias de seguridad anuales de LTR.** La primera copia de seguridad se realiza en la semana 1 del año y se conserva durante 54 semanas.
4. Finalmente, haga clic en **Aplicar** en la parte inferior para que se aplique la política. Las copias de seguridad de LTR pueden tardar hasta 7 días en ser visibles y disponibles para su restauración.



Sugerencia para el examen

En el momento en que se escribió este libro, Azure Portal no admitía restaurar LTR en servidores dentro de la misma suscripción que la base de datos principal, y solo admitía restaurar la base de datos en el mismo servidor que la base de datos principal. Por lo tanto, para tales casos, debe usar Azure PowerShell o la CLI de Azure. Se recomienda que consulte la lista de comandos AZ SQL (CLI de Azure) y AZ.sql que se proporcionan en los vínculos siguientes:

- <https://docs.microsoft.com/en-us/cli/azure/sql?view=azure-cli-latest>
- <https://docs.microsoft.com/en-us/powershell/module/az.sql/?view=azps-3.6.1>

Utilice el siguiente script AZ PowerShell para crear y restaurar LTR, utilice los siguientes scripts.

Para crear un LTR, use este comando:

[Haga clic aquí para ver la imagen del código](#)

```
Set-AzSqlDatabaseBackupLongTermRetentionPolicy -ServerName  
{serverName} -DatabaseName  
  
{dbName} -ResourceGroupName {resourceGroup} -WeeklyRetention  
P1W -MonthlyRetention  
  
P4M -Retención anual P10Y -WeekOfYear 11
```

- **-ServerName.** Este es el nombre del servidor SQL en el que desea configurar la política LTR.
- **-DatabaseName.** Este es el nombre de la base de datos SQL de Azure de la que desea realizar una copia de seguridad.
- **-WeeklyRetention.** Este es el período de retención para la copia de seguridad semanal que se realiza cada 7 días durante un máximo de 10 años.
- **-MonthlyRetention.** Este es el período de retención para la copia de seguridad mensual que se realiza cada 30 días durante un máximo de 10 años.
- **-Retención anual .** Este es el período de retención para la copia de seguridad anual que se realiza cada 365 días hasta 10 años.

- **-WeekOfYear.** Esta es la semana definida para la copia de seguridad anual; puede elegir un valor de 1 a 52.

Para restaurar un LTR, use este comando:

[Haga clic aquí para ver la imagen del código](#)

```
Restore-AzSqlDatabase -FromLongTermRetentionBackup -
ResourceId $ ltrBackup.ResourceId

-ServerName $ serverName -ResourceGroupName $ resourceGroup -
TargetDatabaseName $ dbName

-ServiceObjectiveName P1
```

- **FromLongTermRetentionBackup.** Esto indica que la copia de seguridad se restaurará a partir de la retención a largo plazo.
- **ResourceId.** Este es el ID del recurso que se restaurará.
- **ServerName.** Esto especifica el nombre del servidor SQL.
- **ResourceGroupName.** Esto especifica el nombre del grupo de recursos.
- **TargetDatabaseName.** Esto especifica el nombre de la base de datos de destino que se restaurará.
- **ServiceObjectiveName.** Esto especifica el nombre del nivel de servicio.

Nota Cómo configurar la retención a largo plazo para la instancia administrada

No puede configurar LTR para bases de datos en instancias administradas. En su lugar, puede utilizar un trabajo de SQL Agent Server para programar copias de seguridad de bases de datos de solo copia. Para obtener más información, visite la documentación de Microsoft en <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/copy-only-backups-sql-server?view=sql-server-ver15>.

Copias de seguridad manuales

Puede generar una copia de seguridad manual bajo demanda de las bases de datos existentes y almacenarlas en Azure Blob Storage. La copia de seguridad creada manualmente se almacena en Blob Storage en forma de un archivo zip **BACPAC** que contiene tanto los datos como el esquema. Puede utilizar el archivo para restaurar una base de datos cuando sea necesario. Para iniciar una exportación a un archivo BACPAC mediante Azure Portal, vaya a la hoja Azure SQL Database y haga clic en **Exportar** en la parte superior, como se muestra en la [Figura 4-24](#). Una vez iniciada, puede ver el estado de la exportación navegando al servidor SQL que contiene la base de datos. Los archivos BACPAC exportados se pueden usar para restaurar la base de datos mediante SSMS, Azure Portal o PowerShell.

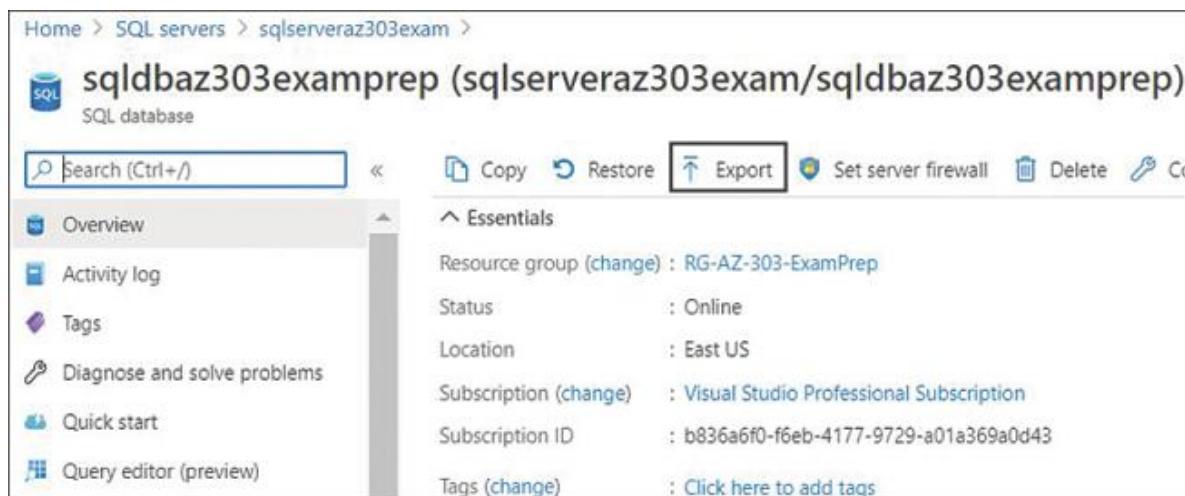


FIGURA 4-24 Exportación de un archivo BACPAC de base de datos a Azure Blob Storage

Escalar una base de datos SQL de Azure

La base de datos SQL Azure se puede escalar hacia arriba o hacia abajo (escalamiento vertical) agregando más procesamiento, almacenamiento o cambiando a niveles de servicio más altos o más bajos. SQL Azure no proporciona escalado horizontal listo para usar.

Siga los pasos que se mencionan a continuación para escalar su base de datos mediante Azure Portal.

1. Inicie sesión en Azure Portal en <https://portal.azure.com> con su suscripción.
2. Navegue hasta la hoja Azure SQL Database y haga clic en **Configurar**, como se muestra en la [Figura 4-25](#).

General Purpose	Hyperscale	Business Critical
Scalable compute and storage options	On-demand scalable storage	High transaction rate and high availability
500 - 20,000 IOPS 2-10 ms latency	500 - 204,800 IOPS 1-10 ms latency	5,000 - 204,800 IOPS 1-2 ms latency

Database utilization:
100%
90%
80%
70%

FIGURA 4-25 Escalado de niveles de servicio de Azure SQL Database

Como se muestra en la [Figura 4-25](#), la hoja horizontal muestra los diferentes niveles de servicio para el modelo DTU y vCore que le permiten cambiar el nivel de servicio para escalar hacia arriba o hacia abajo sin afectar el rendimiento de la base de datos. En este ejemplo, hemos seleccionado el nivel **Business Critical**.

3. Desplácese hacia abajo y elija otros parámetros de escala, como **Generación de hardware**, **núcleos virtuales** y Tamaño de almacenamiento. Opte por los beneficios híbridos si ya posee la licencia del servidor SQL y **haga clic en Aplicar**, como se muestra en la [Figura 4-26](#), para que el escalado surta efecto.

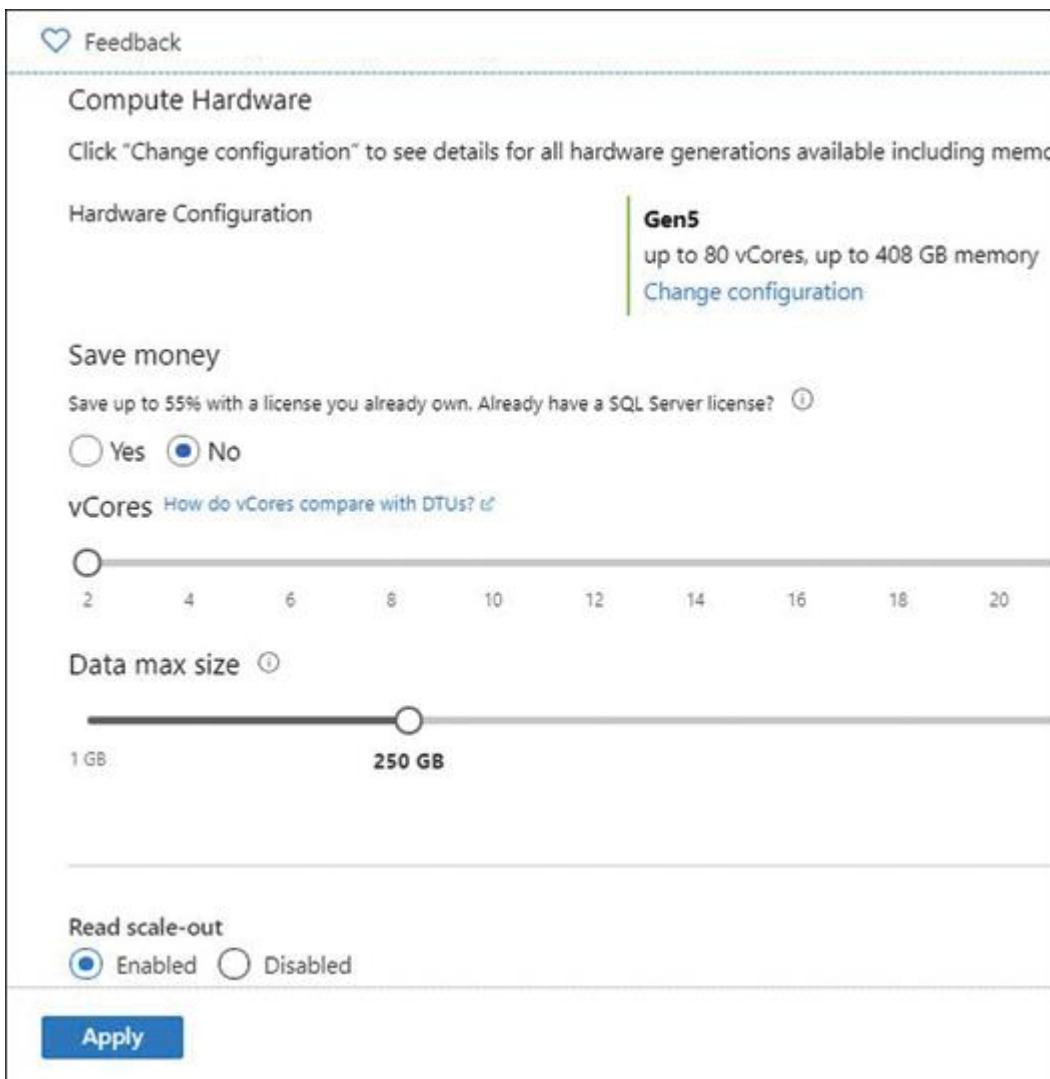


FIGURA 4-26 Configuración del rendimiento y el almacenamiento de Azure SQL Database

Leer escalamiento horizontal

El escalado horizontal de lectura es una característica prometedora para equilibrar la carga de lectura y escritura para mejorar el rendimiento. La función está disponible para los niveles Premium, Hiperescala y Business Critical sin costo adicional. El escalado horizontal de lectura está habilitado de forma predeterminada para los niveles de servicio disponibles cuando crea una nueva base de datos. Después de habilitarlo, obtiene una réplica de solo lectura de su base de datos para descargar la carga de trabajo de lectura, como informes, especificando ApplicationIntent = ReadOnly en la cadena de conexión.

Nota Uso de escalado horizontal de lectura con bases de datos con redundancia geográfica

Si la base de datos SQL de Azure está replicada geográficamente para HADR, asegúrese de que el escalado horizontal de lectura esté habilitado en las bases de datos primaria y secundaria replicadas geográficamente. Esta configuración garantizará que continúe la misma experiencia de equilibrio de carga cuando su aplicación se conecte al nuevo primario después de la conmutación por error.

Seguridad de Azure SQL Database

Para cualquier organización que utilice la nube, la seguridad y la privacidad de los datos de los clientes es siempre la primera y más importante prioridad. Azure SQL Database tiene una estrategia de defensa en profundidad multicapa incorporada para proteger sus datos en varias capas, incluidos los datos físicos, lógicos y en tránsito y en reposo. Dado que Azure SQL Database es un servicio administrado, proteger la base de datos se convierte en una responsabilidad compartida.

Puede utilizar las siguientes capas de defensa en profundidad para configurar una postura de seguridad sólida para su base de datos:

- **Seguridad de la red.** Cuando crea un nuevo servidor de base de datos (único o agrupado), la base de datos obtiene un punto final público de forma predeterminada. Por ejemplo, un servidor de base de datos llamado `mydbAZ303` se llamaría `mydbAZ303.database.windows.net` y sería accesible en el puerto TCP 1433. El firewall de la base de datos es el primer nivel de defensa contra el acceso no autorizado; de forma predeterminada, el cortafuegos de la base de datos bloquea todas las solicitudes entrantes al punto final público del servidor SQL. La configuración de seguridad de la red le permite configurar las reglas del firewall, como se describe en la siguiente viñeta.
- **Reglas de firewall a nivel de servidor.** Las reglas de firewall a nivel de servidor permiten a los clientes acceder a todas las bases de datos en el servidor si la dirección IP del cliente de origen está presente en la regla de permiso. Las reglas

a nivel de servidor se pueden configurar a nivel de red virtual o para una dirección IP o rango de IP específicos.

- ■ **Reglas de firewall a nivel de base de datos.** Las reglas del firewall de la base de datos permiten que una dirección IP particular o rangos de IP se conecten a la base de datos individual. Solo puede configurar direcciones IP y no la red virtual en las reglas de nivel de base de datos.

En lo que respecta a las mejores prácticas, debe configurar un firewall a nivel de base de datos a menos que los requisitos de acceso sean los mismos para todas las bases de datos en el servidor. Independientemente de las reglas del firewall, la conexión hacia la base de datos siempre atraviesa la Internet pública. Aunque SQL Azure cifra los datos en tránsito y en reposo, es posible que una conexión a través de la Internet pública no esté alineada con los requisitos de seguridad de su organización. Puede aprovechar una nueva oferta conocida como enlace privado de Azure, que le permite eliminar la exposición a través de la Internet pública y mantener el tráfico hacia la base de datos SQL de Azure desde la red virtual / subred de Azure a través de la red troncal de Microsoft.

Puede usar Azure Portal, PowerShell, TSQL o la CLI de Azure para configurar reglas de firewall de red. En este ejemplo, veremos algunos ejemplos que utilizan Azure Portal. Debe tener al menos el rol Colaborador de base de datos SQL o Colaborador de SQL Server RBAC para administrar las reglas de firewall a nivel de base de datos o de servidor.

Nota Seguridad de red en instancia de base de datos de Azure SQL administrada

A diferencia de Azure SQL Database, la arquitectura de conectividad de Azure SQL Database de instancia administrada funciona de manera diferente. De forma predeterminada, el punto de conexión de la base de datos se expone a través de una dirección IP privada de Azure o redes híbridas. Consulte la arquitectura de conectividad de la base de datos de instancias administradas más adelante en este capítulo.

Siga estos pasos para configurar las reglas de firewall de nivel de servidor mediante Azure Portal.

1. Inicie sesión en Azure Portal.

2. Vaya a la hoja Azure SQL Database y haga clic en **Establecer servidor de seguridad del servidor**, como se muestra en la Figura 4-27.

FIGURA 4-27 Configuración de las reglas de firewall del servidor SQL

La Figura 4-28 muestra una variedad de configuraciones además de las reglas del firewall:

- ■ **Denegar el acceso a la red pública.** El valor predeterminado es **No**, lo que significa que un cliente puede conectarse a la base de datos a través de un extremo público y privado. Cambiarlo a **Sí** permitirá una conexión solo a través de puntos finales privados.
- ■ **Política de conexión.** Azure SQL Database admite las siguientes tres políticas de conexión:
 - ■ **Redirigir.** Esta es la política recomendada para una baja latencia y un mejor rendimiento y rendimiento. Redirect permite que los clientes se conecten directamente al host de la base de datos. Todas las conexiones que se originan en Azure usan la directiva de conexión de redirección de forma predeterminada. Desde fuera de Azure, si aplica una directiva de redireccionamiento, asegúrese de habilitar las conexiones salientes además del puerto TCP predeterminado 1433 desde la red del cliente para las direcciones IP de Azure en la región en el rango de puertos 11000-11999.
 - ■ **Proxy.** En este modo, las conexiones al host de la base de datos pasan por una puerta de enlace de la base de datos. Todas las conexiones fuera de Azure se establecen de forma predeterminada en la política de proxy.

- **Permitir el acceso a los servicios de Azure.** Esto permite la conectividad desde direcciones IP dentro de los servicios de Azure para acceder a la base de datos.

Firewall settings
sqlserveraz303exam (SQL server)

Save Discard + Add client IP

Deny public network access: Yes

To set Deny Public Network Access, click here to create a new private endpoint.

Minimum TLS Version: >1.0 >1.1 >1.2

You are setting the Minimal TLS Version property for all SQL Database and SQL Data Warehouse databases associated with the server. Any login attempts from clients using TLS version less than the Minimal TLS Version shall be rejected.

Connection Policy: Default

Allow Azure services and resources to access this server: No

Client IP address: 117.220.136.46

Rule name	Start IP	End IP	...

No firewall rules configured.

Virtual networks

Rule name	Virtual network	Subnet	Address Range	Endpoint status

No vnet rules for this server.

FIGURA 4-28 Panel del cortafuegos de SQL Server

3. Como se muestra en la [Figura 4-28](#), haga clic en **Agregar IP de cliente** para agregar la dirección IP de su red y luego haga clic en **Guardar**. Puede actualizar las direcciones IP en cualquier momento o puede eliminarlas haciendo clic en los puntos suspensivos de la regla de IP. Si desea habilitar el acceso desde la subred desde una red virtual de Azure, haga clic en **Agregar red virtual existente**.

4. Haga clic en **Guardar**.

Azure SQL Database también le da libertad para configurar el firewall de nivel de base de datos mediante los comandos de TSQL. El fragmento de código de muestra se muestra a continuación:

[Haga clic aquí para ver la imagen del código](#)

```
EJECUTAR sp_set_database_firewall_rule Regla N'Allow,  
'{0.0.0.0}', '{0.0.0.0}'; IR;
```

En el comando anterior, debe especificar `IR` para que se ejecute el comando. Puede ver las reglas del nivel de la base de datos utilizando la opción `view sys.database_firewall_rules` con el siguiente comando TSQL:

[Haga clic aquí para ver la imagen del código](#)

```
SELECCIONAR * DE sys.database_firewall_rules
```

Control de acceso

Las reglas de firewall permiten que el cliente se conecte a Azure SQL Database. La siguiente capa de protección es el control de acceso, que requiere que el cliente pase por el proceso de autenticación y autorización. Veamos primero el proceso de autenticación. Azure SQL Database admite dos tipos de métodos de autenticación:

- **Autenticación de SQL.** En este proceso de autenticación, crea un usuario de base de datos, también llamado usuario contenido, ya sea en la base de datos maestra o en la base de datos individual. Inicie sesión con su cuenta de administrador de SQL Server, la que creó al configurar el servidor SQL, y use el siguiente comando TSQL para crear usuarios de base de datos:

[Haga clic aquí para ver la imagen del código](#)

```
CREAR USUARIO dbUser CON CONTRASEÑA = 'contraseña  
fuerte'; IR
```

- **Autenticación de Azure AD (AAD).** Este es el método recomendado para conectarse a Azure SQL Database mediante las identidades administradas en Azure Active Directory, también conocido como (AAD).

Los usuarios autenticados, de forma predeterminada, no tienen acceso a los datos. El acceso a los datos también está controlado por los grupos de permisos / roles de la base de datos, como db_datawriter y db_datarader. El comando db_datawriter proporciona acceso de lectura / escritura, mientras que el comando db_datarader proporciona acceso de lectura a la base de datos. Utilice el siguiente comando de TSQL para agregar un usuario a los grupos:

[Haga clic aquí para ver la imagen del código](#)

```
ALTER ROLE db_datarader AÑADIR MIEMBRO dbUser;
```

Protección y cifrado de datos

Azure SQL Database protege sus datos en reposo y en tránsito mediante el cifrado de datos transparente (TDE). La seguridad se aplica a cualquier instancia administrada y base de datos de Azure SQL recién creada, lo que significa que TDE está habilitado de forma predeterminada. Si TDE está habilitado, el cifrado y descifrado de datos se realiza en tiempo real y de forma transparente para todas las operaciones de la base de datos dentro de Azure. La clave de cifrado predeterminada es una clave administrada dentro de Azure, pero tiene la opción de traer su clave de cifrado con un concepto popularmente conocido: Traiga su propia clave (BYOK).

Además de TDE, puede proteger aún más su información confidencial, como la información de identificación personal (PII), habilitando el Enmascaramiento dinámico de datos. Puede usar Azure Portal para configurar el enmascaramiento dinámico de datos y el cifrado de datos transparente navegando a la hoja **Azure SQL Database** y seleccionando la configuración de seguridad correspondiente, como se muestra en la [figura 4-29](#).

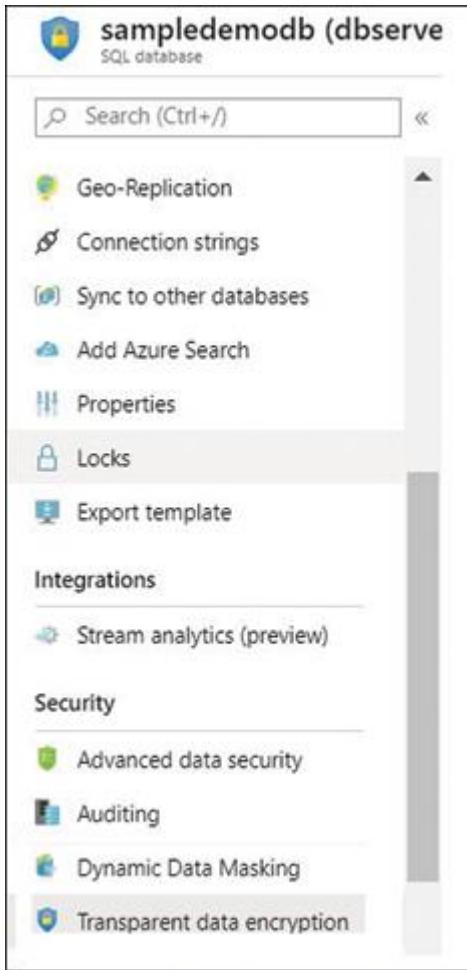


FIGURA 4-29 Configuración de seguridad de la base de datos SQL Azure
Protección avanzada contra amenazas

Azure SQL Database proporciona protección avanzada contra amenazas a través de sus capacidades de seguridad de datos avanzada (ADS), incluido el descubrimiento de datos y la clasificación de datos para datos confidenciales y evaluación de vulnerabilidades. ADS ayuda a descubrir posibles lagunas en la seguridad de la base de datos, como una base de datos sin cifrar, actividades anónimas e inusuales y patrones de acceso a datos sospechosos que podrían conducir a la explotación de datos.

ADS también proporciona alertas inteligentes para posibles vulnerabilidades de la base de datos, inyección de SQL y ataques de fuerza bruta, acciones sospechosas y exfiltración de datos, y proporciona recomendaciones para investigar y mitigar amenazas.

Puede habilitar la característica ADS para bases de datos de instancia única, agrupada o administrada mediante Azure Portal o la CLI de Azure. Siga los pasos a continuación para configurar ADS.

1. Inicie sesión en Azure Portal y navegue hasta la hoja de **base de datos de SQL Server**.
2. Haga clic en **Seguridad de datos avanzada** en el panel **Configuración de seguridad**, como se muestra en la Figura 4-30.
3. Especifique las direcciones de correo electrónico para alertas sobre informes de vulnerabilidad.
4. En la sección **Tipos de protección avanzada contra amenazas**, opte por no participar o no participar en la configuración del análisis de seguridad.
5. Haga clic en **Guardar**.

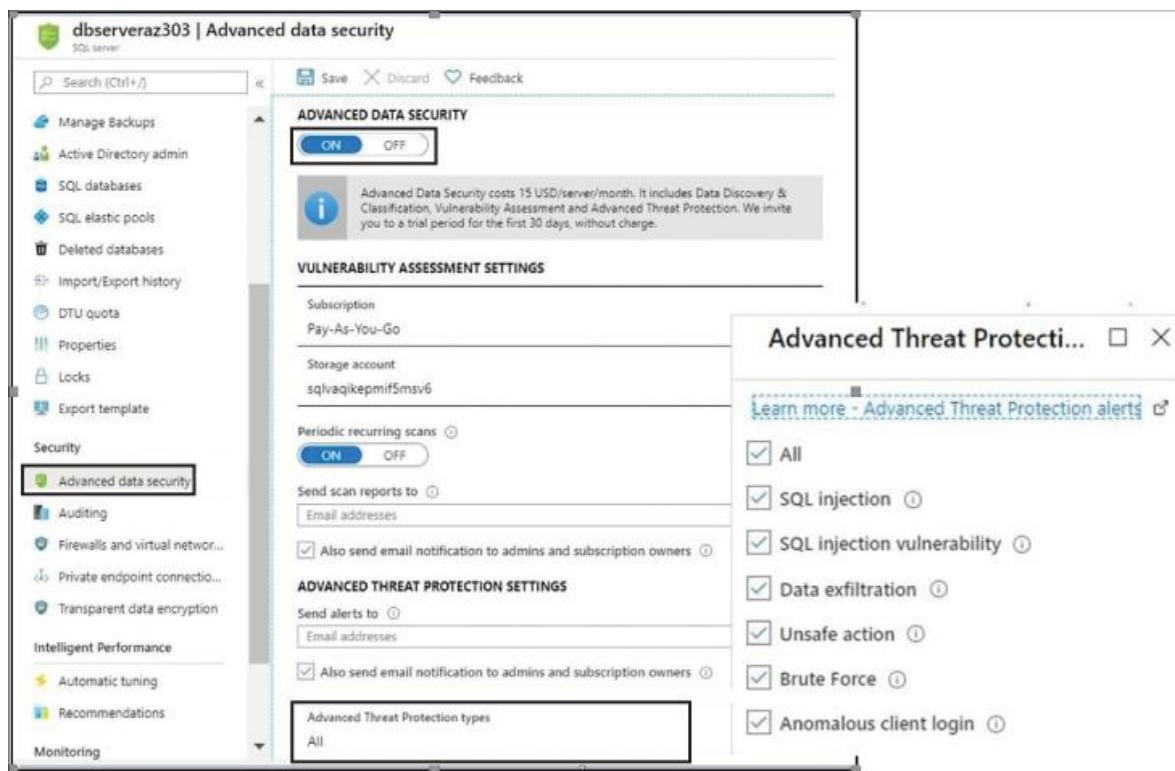


FIGURA 4-30 Configuración de la protección contra amenazas avanzada de la base de datos SQL de Azure

Revisión de cuentas

La auditoría es un aspecto esencial del monitoreo de la base de datos que ayuda a investigar las brechas de seguridad de la base de datos, como actividades sospechosas o acceso no autorizado. Cuando la auditoría está habilitada, puede configurar todas las operaciones de la base de datos para que se registren en el área de trabajo de Azure Storage o Log Analytics, o Event Hubs. Se recomienda que habilite la auditoría en el nivel del servidor de la base de datos que se hereda automáticamente para todas las bases de datos en el servidor, a menos que tenga una necesidad específica de permitir la auditoría a nivel de la base de datos. Siga los pasos a continuación para habilitar la auditoría de nivel de servidor de base de datos:

1. Inicie sesión en Azure Portal y navegue hasta la hoja de **SQL Server**.
2. Bajo el encabezado **Seguridad** en el menú de la izquierda, haga clic en **Auditoría**, como se muestra en la [Figura 4-31](#).
3. En el menú de la derecha, de palanca **Auditoría** de EN y especificar su servicio de almacenamiento preferido.
4. Haga clic en **Guardar**.

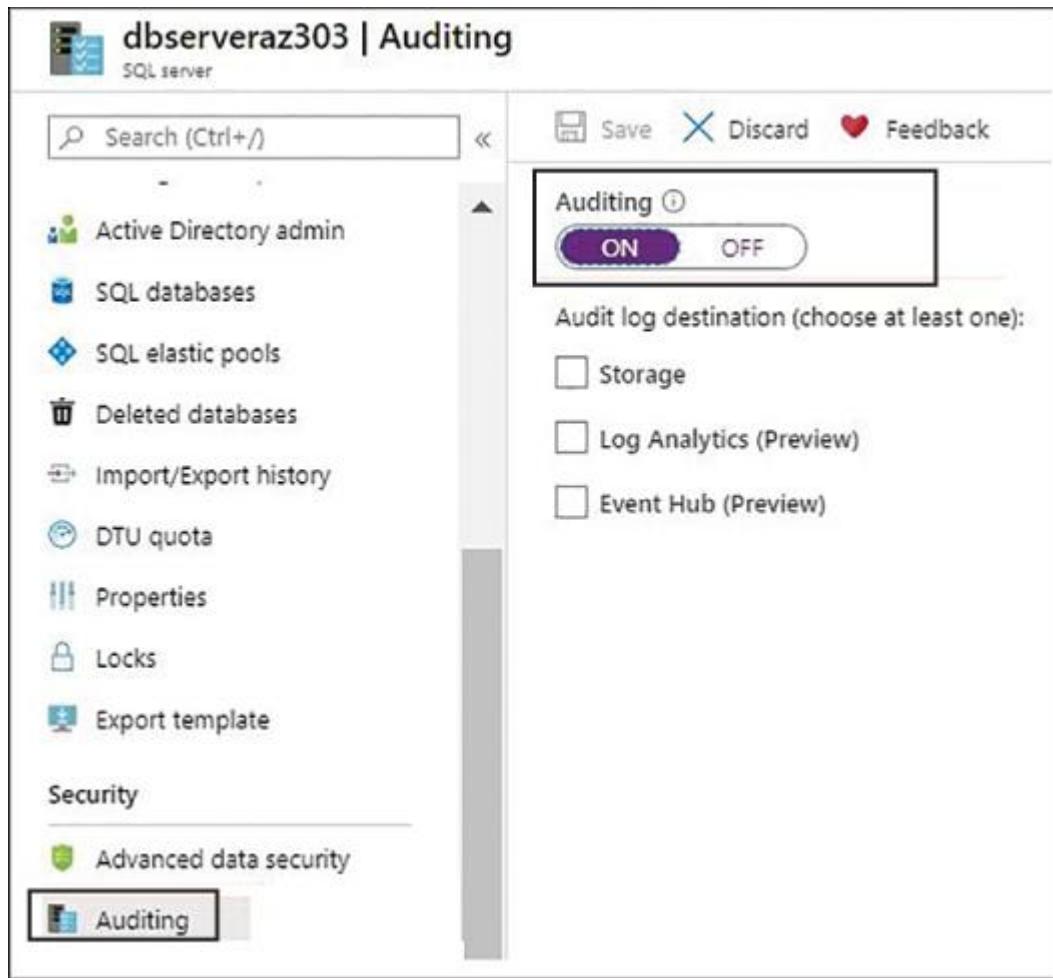


FIGURA 4-31 Configuración de auditoría de base de datos SQL Azure

Implementar una instancia administrada de Azure SQL Database

La instancia administrada de Azure SQL Database es otro tipo de la familia de productos de Azure SQL Database que proporciona casi el 100% de compatibilidad con un motor de base de datos local de SQL Server (Enterprise Edition). Se expone solo a través de una dirección IP privada que permite la conectividad solo desde las redes virtuales emparejadas o la red local mediante Azure VPN Gateway o ExpressRoute.

La instancia administrada se aprovisiona en un solo inquilino con infraestructura dedicada (computación y almacenamiento) bajo el modelo de compra de núcleos virtuales. La figura 4-32 muestra la

arquitectura de conectividad de alto nivel de Azure SQL Managed Instance Database.

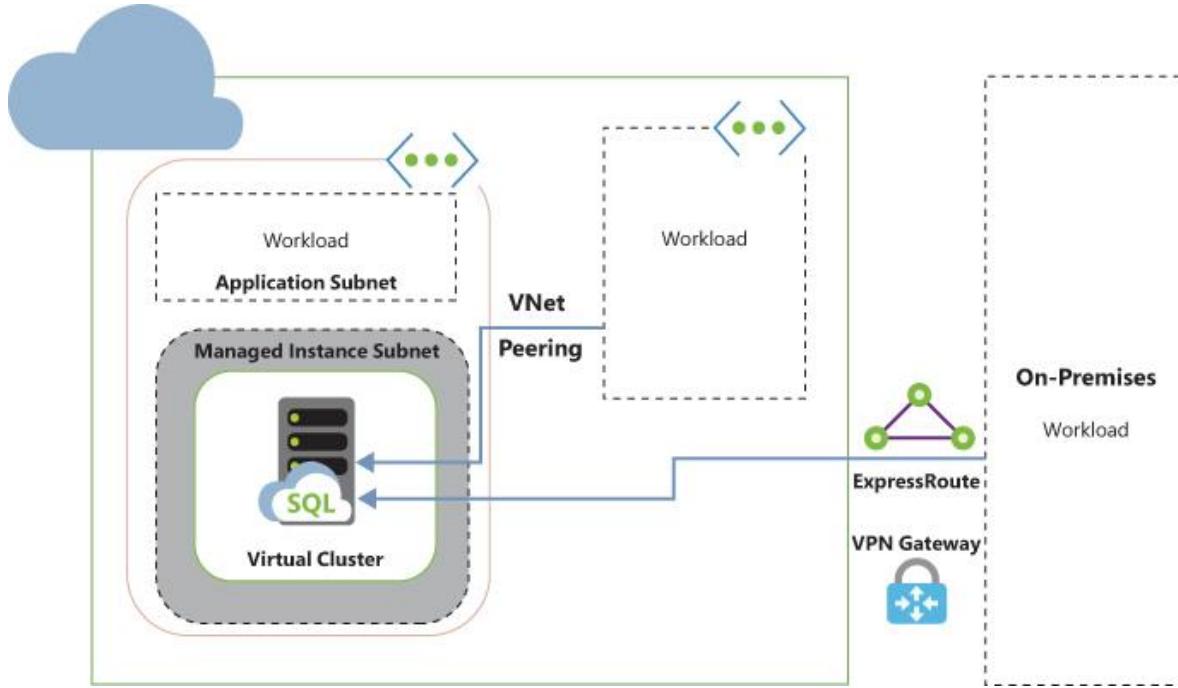


FIGURA 4-32 Arquitectura de conectividad de instancia administrada de base de datos Azure

Como puede ver en la **figura 4-32**, Azure SQL Managed Instance Database está alojado dentro de su subred dedicada. En la subred de red virtual dedicada, Azure crea automáticamente máquinas virtuales aisladas que forman un clúster virtual para alojar una o varias instancias administradas. No puede alojar ningún otro servicio dentro de la subred dedicada de la Instancia administrada. El clúster virtual y las máquinas virtuales son completamente transparentes y están administrados por Azure.

Las aplicaciones cliente pueden conectarse a una instancia administrada a través de una red virtual emparejada, VPN, conexiones ExpressRoute o desde una subred dentro de la misma red virtual que una instancia administrada. Utiliza el nombre de host <datbasename.dns_name.database.windows.net>, que se resuelve automáticamente en la dirección IP privada que pertenece al equilibrador de carga interno de la instancia administrada. Luego, el tráfico se redirige a la puerta de enlace de la instancia administrada, lo

que facilita la conexión a la instancia de base de datos específica dentro de un clúster virtual.

Siga estos para crear una instancia administrada de base de datos SQL de Azure mediante el Portal de Azure.

1. Inicie sesión en Azure con sus credenciales de suscripción de Azure.
2. En el menú de la izquierda, haga clic en **Crear un recurso** y busque **Instancia administrada de Azure SQL**. Verá la pantalla que se muestra en la [Figura 4-33](#).
3. A continuación, haga clic en **Crear**.



FIGURA 4-33 Creación de una instancia administrada de Azure SQL

4. En la pantalla **Crear instancia administrada de base de datos de Azure SQL**, como se muestra en la [Figura 4-34](#), proporcione la información obligatoria, como un **nombre de base de datos único**, **grupo de recursos**, **región**, **SKU** y nombre **de usuario y contraseña del administrador**.
5. Haga clic en **Siguiente: Redes**.
6. En la pestaña **Redes** (consulte la [Figura 4-35](#)), cree una red virtual obligatoria y una subred dedicada para la Instancia administrada; si no lo hace, Azure crea uno automáticamente.

Create Azure SQL Database Managed Instance

Microsoft

Basics Networking Additional settings Review + create

SQL Managed Instance is a fully managed PaaS database service with extensive on-premises SQL Server compatibility and native virtual network security. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ (New) RG-SQL-Managed-Ins

Create new

Managed Instance details

Enter required settings for this instance, including picking a location and configuring the compute and storage resources.

Managed Instance name * azdbsqlmi

Region * (US) East US 2

Not seeing a region?

Compute + storage * ⓘ

General Purpose
Gen5, 8 vCores, 256 GB storage
[Configure Managed Instance](#)

Administrator account

Managed Instance admin login * saadmin

Password *
Confirm password *

[Review + create](#) < Previous Next : Networking >

FIGURA 4-34 Creación de una instancia administrada de Azure SQL

Create Azure SQL Database Managed Instance

Microsoft

Basics Networking Additional settings Review + create

Configure virtual network and public endpoint connectivity for your Managed Instance. Define level of access and connection type. [Learn more](#)

Virtual network

Select or create a virtual network to connect to your Managed Instance securely. Allow us to update subnet configuration for you automatically, or follow our guide to set it up yourself. [Learn more](#)

Virtual network * ⓘ (new) vnet-azdbsqlmi/ManagedInstance

i New virtual network will be created with a single (default) subnet. Network configuration required for Managed Instance will then be applied to this subnet. [Learn more](#)

Connection type

Select a connection type to accelerate application access. This configuration will apply to virtual network and public endpoint. [Learn more](#)

Connection type (private endpoint) ⓘ Proxy (Default)

Public endpoint

Secure public endpoint provides the ability to connect to Managed Instance from the Internet without using VPN and is for data communication (TDS) only. Access is disabled by default unless explicitly allowed. [Learn more](#)

Public endpoint (data) ⓘ **Enable**

Allow access from ⓘ

i Accelerated networking is automatically enabled for this endpoint.

Azure services

Azure services

Internet

No access

Review + create < Previous Next : Additional settings >

FIGURA 4-35 Configuración de la red para una instancia administrada

El siguiente paso es especificar el **tipo de conexión** (consulte la [Figura 4-35](#)).

1.

1. ■ **Proxy (predeterminado).** La conexión proxy permite la conectividad a una instancia administrada a

través de un componente de puerta de enlace (GW). Utiliza el puerto 1433 para una conexión privada y el puerto 3342 para una conexión pública.

2. ■ **Redirigir.** El modo de redireccionamiento proporciona baja latencia y mejor rendimiento porque se conecta directamente a la base de datos. Solo puede utilizar este modo para conexiones privadas. Debe habilitar el firewall y los NSG para permitir conexiones en el puerto 1433 y los puertos 11000-11999.

7. A continuación, tenemos el punto final público. Cambie el botón de alternancia a **Habilitar** si desea permitir puntos finales públicos.

8. A continuación, seleccione **Servicios de Azure , Internet o Sin acceso** para sus requisitos de conectividad. Vea la Figura 4-35 anterior .

9. Puede omitir la configuración opcional, como la zona **horaria de la base de datos, la replicación geográfica y la clasificación** en la pestaña **Configuración adicional** . Si los omite, Azure aplicará automáticamente la configuración predeterminada. A continuación, haga clic en el botón **Revisar + Crear** (consulte la Figura 4-36). Como puede ver en la notificación en la parte superior, a diferencia de la base de datos única / agrupada, la implementación de la base de datos de instancia administrada demora hasta 6 horas en promedio, especialmente cuando está creando una red virtual junto con ella. Cambiar el nivel de servicio en las instancias existentes lleva hasta 2,5 horas y eliminar una base de datos hasta 1,5 horas.

10. Revise la configuración y haga clic en **Crear** (consulte la Figura 4-36).

Create Azure SQL Database Managed Instance

Microsoft

i Deploying Managed Instance is a long running operation taking up to 6 hours to complete.

Basics Networking Additional settings **Review + create**

Product details

SQL Managed Instance by Microsoft Terms of use Privacy policy	Estimated cost per month 1526.76 USD View pricing details
---	--

Terms

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. For additional details see [Azure Marketplace Terms](#).

Basics

Subscription	Pay-As-You-Go
Resource group	RG-SQL-Managed-Ins
Managed Instance name	azdbsqlmi
Region	East US 2
Compute + storage	General Purpose: Gen5, 8 vCores, 256 GB storage
Managed Instance admin login	saadmin

Networking

Virtual network	Create new virtual network
Prepare subnet for Managed Instance	Automatic
Connection type	Proxy
Public endpoint (data)	Enabled

Create < Previous Next: Review + create > Download a template for automation

FIGURA 4-36 Pantalla de revisión de instancia administrada de base de datos SQL

Configurar HA para una base de datos SQL de Azure

Azure SQL Database tiene incorporada una sólida arquitectura de alta disponibilidad que garantiza un SLA del 99,99 por ciento de tiempo de actividad, incluso durante las operaciones de mantenimiento o fallas de red o hardware subyacentes. En esta sección, aprenderá las

características clave que obtiene de inmediato para la alta disponibilidad de Azure SQL Database y recomendaciones para implementar procedimientos de recuperación ante desastres y continuidad del negocio. Antes de profundizar, veamos los conceptos básicos para comprender los términos Alta disponibilidad (HA), Continuidad del negocio y Recuperación ante desastres (BCDR).

- ■ **Alta disponibilidad.** La frase "alta disponibilidad" se refiere a las características clave destinadas a mantener el sistema en funcionamiento según el acuerdo de nivel de servicio definido (SLA) independientemente del hardware subyacente, las fallas de la red o las operaciones de mantenimiento planificadas.
- ■ **Continuidad empresarial.** La frase "continuidad del negocio" se refiere al conjunto de procedimientos y políticas que usted elaboró para mantener sus aplicaciones y negocios operativos en caso de un impacto adverso en el centro de datos que pueda causar una interrupción o pérdida de datos en el centro de datos. Aunque Azure SQL Database proporciona un SLA del 99,99 por ciento, los escenarios disruptivos específicos, como la eliminación de datos por un error humano, las interrupciones regionales del centro de datos, etc., no son manejados automáticamente por Azure SQL Database. Usted tendrá realizar una planificación exclusiva e implementar procedimientos para lograr el estado deseado de continuidad del negocio. Hablaremos de estos procedimientos más adelante en este capítulo.
- ■ **Recuperación ante desastres.** La frase "recuperación ante desastres" se refiere a los procedimientos que implementamos para recuperarnos de una interrupción, pérdida de datos y tiempo de inactividad causado por un desastre, como interrupciones del centro de datos regional o errores humanos.

El diseño de una estrategia de recuperación ante desastres y continuidad del negocio requiere una planificación inmensa, una comprensión de un extremo a otro de la carga de trabajo de las aplicaciones, la infraestructura de las aplicaciones y las dependencias. Hay dos factores clave que debe considerar al diseñar un BCDR:

- ■ **Objetivo de punto de recuperación (RPO).** RPO define la pérdida máxima de datos que una empresa puede permitirse

antes de que la aplicación se restaure a su estado normal. El RPO se mide en unidades de tiempo, no en volumen de datos; por ejemplo, si su aplicación puede permitirse perder hasta una hora de datos transaccionales no comprometidos, su RPO es una hora.

- ■ **Objetivo de tiempo de recuperación (RTO).** RTO es una duración máxima de tiempo de inactividad aceptable que una aplicación puede permitirse antes de la restauración. Por ejemplo, si la base de datos de su aplicación tarda ocho horas en restaurarse, puede definir el tiempo de inactividad aceptable en nueve horas, considerando una hora adicional para la validación y las pruebas rápidas; por lo tanto, su RTO se convierte en nueve horas.

Como se indicó anteriormente, la arquitectura de alta disponibilidad integrada predeterminada de Azure SQL Database le brinda un SLA de tiempo de actividad del 99,99 por ciento, independientemente de los diferentes niveles de servicio que elija. La arquitectura de disponibilidad tiene dos modelos:

- ■ **Modelo de disponibilidad** estándar Los niveles Básico, Estándar y Uso general utilizan el modelo estándar, donde el procesamiento y el almacenamiento se administran por separado. La disponibilidad de procesamiento es administrada por un controlador de Service Fabric que activa la conmutación por error a otro nodo físico en la misma región en caso de falla del nodo actual. La capa de datos que contiene los archivos de datos (.mdf / .ldf) se administra en el almacenamiento Azure Blob altamente redundante. Cuando ocurre la conmutación por error, el almacenamiento persistente de datos y archivos de registro almacenados en el almacenamiento de Azure se adjunta automáticamente al nuevo nodo físico.
- ■ **Modelo de disponibilidad premium** Este modelo funciona según el principio similar de la función SQL Server Always On. El nivel crítico Premium y Business utiliza el modelo de disponibilidad premium para optar por la redundancia de zona que mejora aún más la disponibilidad y la tolerancia a fallas al distribuir las réplicas en la zona de disponibilidad dentro de la región. Los archivos de datos (.mdf / .ldf) en este modo se administran en el mismo almacenamiento SSD adjunto local, lo

que proporciona baja latencia y alto rendimiento. Este modo suele ser para aplicaciones críticas para la empresa.

Además, el modelo premium mantiene las tres réplicas secundarias y el nodo principal en la misma región. Siempre se sincroniza al menos una réplica secundaria antes de confirmar las transacciones. La conmutación por error es administrada por un Service Fabric que inicializa la conmutación por error en la réplica secundaria sincronizada cuando es necesario.

Con las tres réplicas secundarias adicionales, también obtiene una característica llamada Read Scale-Out (sin costo adicional) para separar la carga de trabajo de lectura a una de las réplicas secundarias dentro de una región primaria, lo que parece una característica prometedora para mejorar el rendimiento.

Azure SQL Database ofrece las siguientes opciones que puede aprovechar para diseñar su estrategia de continuidad empresarial, recuperación ante desastres y alta disponibilidad:

- ■ **Copias de seguridad automatizadas.** Como vimos anteriormente en este capítulo, las copias de seguridad automatizadas integradas y la restauración en un momento determinado (PITR) lo ayudan a restaurar la base de datos en caso de falla.
- ■ **Retención de copias de seguridad a largo plazo.** Le permite conservar las copias de seguridad hasta por 10 años.
- ■ **Replicación geográfica activa.** Le permite crear hasta cuatro réplicas de solo lectura de su base de datos dentro de la misma región o en regiones diferentes para que pueda realizar la conmutación por error manualmente a cualquier réplica secundaria en caso de falla de la base de datos principal. La replicación geográfica activa no es compatible con Azure SQL Managed Instance Database. En su lugar, usaría el grupo Auto-failover.
- ■ **Grupo de conmutación por error automática.** Funciona con el principio similar de la replicación geográfica activa que lo ayuda a realizar automáticamente la conmutación por error en caso de un evento catastrófico que pueda causar una interrupción del centro de datos. Con la conmutación por error

automática habilitada, no puede crear réplicas secundarias en la misma región que una base de datos principal.

La estrategia de replicación geográfica no forma una solución BCDR completa y requiere que usted piense en todos los escenarios de fallas potenciales y diseñe un plan sólido. Por ejemplo, en el caso de un error humano, como la eliminación de datos o la corrupción de datos, la replicación sincronizaría los datos con todas las bases de datos secundarias que dan como resultado que las bases de datos secundarias estén en el mismo estado que la base de datos primaria. En este caso, tendría que restaurar los datos de las copias de seguridad disponibles, como la restauración a un momento determinado (PITR) o las copias de seguridad de retención a largo plazo (LTR).

Si está utilizando LTR y replicación geográfica o un grupo de conmutación por error como solución BCDR, debe asegurarse de configurar la LTR en todas las réplicas secundarias para que la copia de seguridad de LTR continúe cuando se produzca la conmutación por error y su réplica secundaria se convierta en primaria.

Configurar un grupo de conmutación por error automática

Como aprendimos anteriormente, el grupo de conmutación por error automática es el método recomendado para un alto grado de tolerancia a fallas y recuperación ante desastres. La característica de grupo de conmutación por error de la familia de productos Azure SQL Database usa la misma tecnología subyacente que la replicación geográfica. Le permite administrar sin problemas la conmutación por error automática de las bases de datos (instancia única, agrupada o administrada) configuradas en el servidor principal y secundario en diferentes regiones de Azure. La conmutación por error se puede configurar para que se active automáticamente, o también puede hacerlo manualmente cuando se produce una interrupción.

La conmutación por error automática solo admite un servidor secundario que debe estar en una región de Azure diferente a la del servidor principal. Si necesita varias réplicas secundarias, considere usar la replicación geográfica activa para crear cuatro réplicas en la misma región que el servidor principal o en las diferentes regiones de Azure desde un servidor principal.

A continuación, se muestran los pasos para configurar el grupo de conmutación por error para las bases de datos SQL de Azure. Veremos una sola base de datos en nuestro ejemplo. (Los pasos son los mismos para las bases de datos del grupo elástico).

1. Inicie sesión en Azure con sus credenciales de suscripción de Azure.
2. Navegue hasta la hoja **Azure SQL Database Server** y, en el menú **Configuración**, elija **Grupos de conmutación por error > Agregar grupo** en la parte superior (consulte la [Figura 4-37](#)).

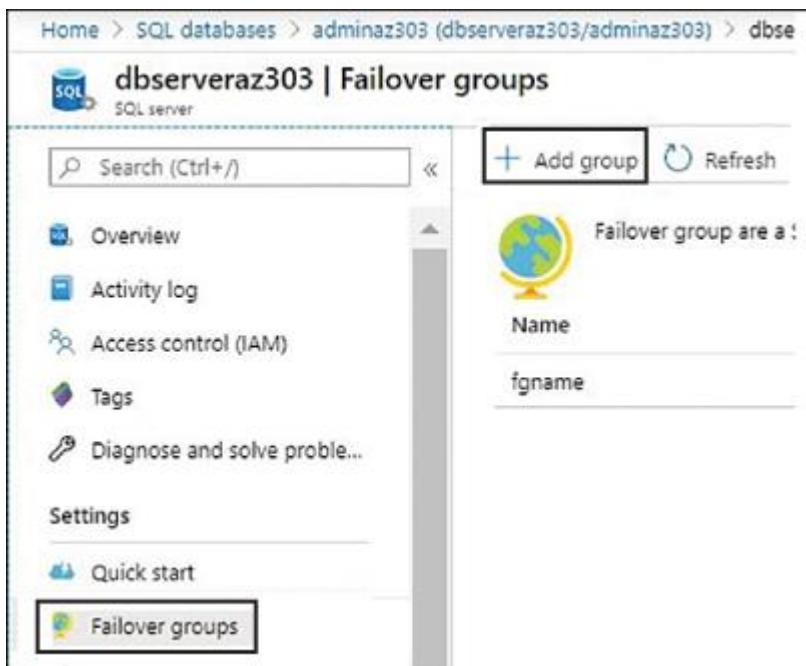


FIGURA 4-37 Configuración de grupos de conmutación por error

El servidor de base de datos dbserveraz303 es nuestro servidor principal en el este de EE. UU., En el que queremos configurar un grupo de conmutación por error.

3. Haga clic en **Agregar grupo** y aparecerá la pantalla que se muestra en la [Figura 4-38](#). Complete la siguiente información requerida:

1. ■ Proporcione el nombre del grupo de conmutación por error.
2. ■ Seleccione o cree el servidor secundario en una **región diferente** a la principal.

3. ■ Especifique la política de conmutación por error que define el período de gracia antes de que se active la conmutación por error tras una interrupción en el servidor principal. El valor predeterminado es 1 hora.
4. ■ Seleccione las bases de datos en el servidor principal para que formen parte del grupo de conmutación por error tal como las ve en la hoja **Bases de datos** en la Figura 4-38.

4. Haga clic en Crear .

Name	Role	Secondary server	Status
adminaz303	Primary	fgserver	Online
database-2	Primary	fgserver	Online

FIGURA 4-38 Creación de un grupo de conmutación por error

Nota SQL Server secundario en el grupo de conmutación por error

El servidor secundario que cree en las diferentes regiones para el grupo de conmutación por error no debe tener una base de datos con el mismo nombre que el servidor principal, a menos que sea una base de datos secundaria existente.

Agregar bases de datos al grupo de conmutación por error activa automáticamente la replicación geográfica para todas las bases de datos del grupo de conmutación por error en la región secundaria seleccionada; vea la Figura 4-39. Como puede ver, cuando se crea un grupo de conmutación por error, Azure forma los dos registros CNAME :

- ■ Escucha de lectura / escritura (servidor primario), que se forma como <fgname.database.windows.net>

- Escucha de solo lectura (servidor secundario), que se forma como <fgname.secondary.database.windows.net>

Para conectarse a una base de datos replicada geográficamente en el servidor secundario, utilice el punto final de escucha secundario para realizar funciones como descargar las consultas de lectura. De forma predeterminada, la comutación por error en el escucha secundario no está habilitada. Debe permitirlo mediante el uso explícito de la propiedad `AllowReadOnlyFailoverToPrimary` para redirigir automáticamente el tráfico de lectura al servidor principal si el servidor secundario está fuera de línea.

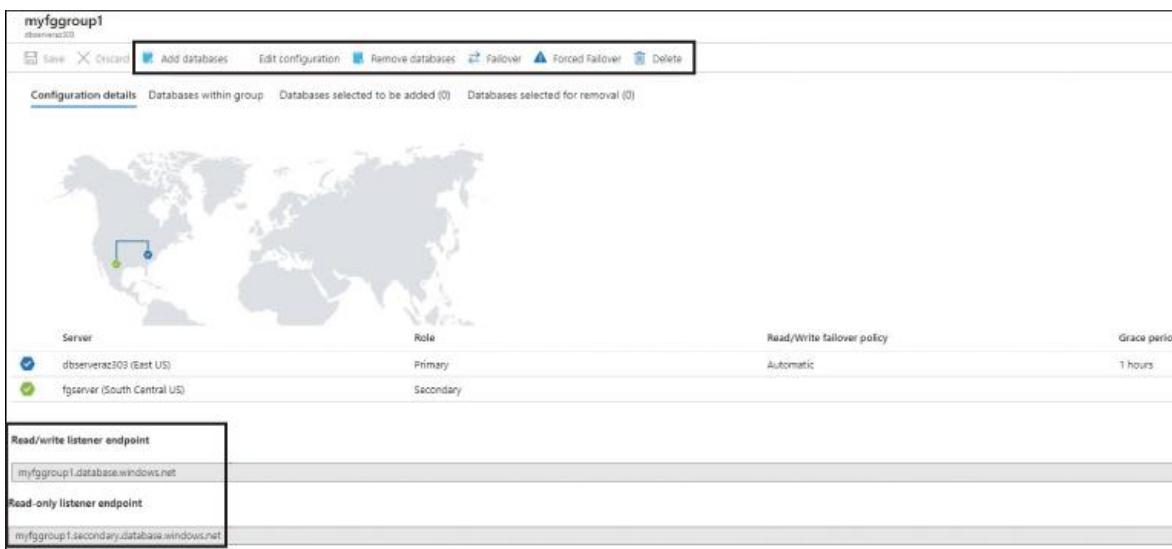


FIGURA 4-39 Bases de datos replicadas geográficamente en un grupo de comutación por error

Nota Leer escalado horizontal versus grupo de comutación por error

El grupo de comutación por error le brinda una base de datos secundaria de solo lectura replicada geográficamente en las diferentes regiones con un costo equivalente al 100 por ciento del costo de la base de datos primaria. El escalado horizontal de lectura, cuando se habilita en la base de datos replicada geográficamente, proporciona otro par de réplicas de solo lectura sin costo adicional.

Importante Eliminación de una base de datos que forma parte del grupo de comutación por error

Debe eliminar la base de datos secundaria del grupo de conmutación por error si desea eliminarla. No se permite eliminar una base de datos secundaria antes de eliminarla del grupo de conmutación por error.

Publicar una base de datos SQL de Azure

La migración de bases de datos de SQL Server locales a Azure SQL Database (instancia única, agrupada o administrada) requiere una inmensa planificación y evaluación para desarrollar la estrategia de migración sólida utilizando los métodos adecuados que se consideran adecuados para un tipo de carga de trabajo determinado. En esta sección, aprenderá a seleccionar la estrategia de migración adecuada para publicar una base de datos SQL local existente en la base de datos SQL de Azure.

El proceso de migración de la base de datos generalmente consta de los siguientes métodos.

- ■ **Descubrimiento.** El modo de descubrimiento comienza con la identificación de la carga de trabajo de la base de datos existente, los escenarios de uso y el nivel de compatibilidad de la versión de la base de datos y explorando la base de datos de destino y el nivel de servicio correctos disponibles en la plataforma de destino.
- ■ **Evaluación.** En la fase de evaluación, descubre cualquier problema de compatibilidad entre la plataforma de origen y la de destino. Por ejemplo, si migra de SQL Server local a Azure SQL Database (único o agrupado), es posible que deba observar las características del servidor SQL, como consultas entre bases de datos, como ejemplo y validar si la base de datos de destino lo admite.
- ■ **Transformar.** En la fase de transformación, realiza cambios en el script SQL existente para resolver cualquier problema de incompatibilidad o adaptarse a las nuevas funciones disponibles en la plataforma de destino.
- ■ **Migrar y supervisar.** En esta fase, migra su base de datos a la base de datos SQL de Azure seleccionada, valida su migración, supervisa la corrección y optimiza el costo.

Microsoft Azure proporciona los siguientes métodos de migración de bases de datos para la base de datos de SQL Server local a la base de datos SQL de Azure.

- ■ **Migración sin conexión mediante el Asistente de migración de bases de datos (DMA).** El asistente de migración de datos de Azure (DMA) es una herramienta gratuita que puede descargar en la máquina local y usar para la evaluación para identificar problemas de compatibilidad antes de intentar migrar. Este método no es compatible con la instancia administrada. Por lo general, se utilizan para bases de datos compatibles cuando una aplicación puede permitirse un tiempo de inactividad más prolongado.
- ■ **Migración en línea mediante Azure Database Migration Service (DMS).** Azure Database Migration Service (DMS) es la forma recomendada de migrar bases de datos a escala con un tiempo de inactividad mínimo. El DMS admite la migración en línea y fuera de línea paraBases de datos de instancia única, agrupada y administrada. En la migración fuera de línea, el tiempo de inactividad de la aplicación comienza cuando inicia la migración. Con la migración en línea, el tiempo de inactividad es mínimo y está limitado al tiempo necesario para realizar la transición real.

¿Más información? Sugerencias para la migración de la base de datos SQL Azure

Cuando migra su base de datos, desea ver un rendimiento comparativamente mejorado en Azure SQL Database. Requiere que evalúe cuidadosamente el escenario de uso del servidor SQL local, la carga de trabajo y la compatibilidad de la base de datos de origen y destino. La publicación del blog en cloudskills.io tiene una guía completa sobre las consideraciones clave que debe tomar antes de migrar. Obtenga más información visitando <https://cloudskills.io/blog/azure-sql-database-performance>.

El proceso de migración general consiste en la migración de los dos elementos, el esquema y los datos. En la fase de evaluación de la migración, comienza por determinar los problemas de compatibilidad entre el servidor SQL de origen y la base de datos SQL de Azure de destino

mediante una herramienta de asistente de migración de base de datos (DMA) y luego corrige los problemas informados, si los hubiera. Una vez que haya solucionado todos los problemas de compatibilidad identificados, debe implementar el script generado por DMA en la base de datos Azure SQL de destino creada previamente. Una vez que se ha migrado el esquema, comienza con el siguiente paso de la migración de datos.

Las siguientes instrucciones paso a paso describen el proceso de un extremo a otro para publicar su base de datos de SQL Server local en Azure SQL Database mediante el servicio de migración de bases de datos de Azure (DMS).

1. Descargue e instale el asistente de migración de Azure Database desde <https://www.microsoft.com/en-us/download/details.aspx?id=53595>.
2. Con la herramienta DMA, cree un proyecto de evaluación haciendo clic en el icono + en la hoja izquierda y proporcionando el nombre del proyecto. Seleccione un servidor SQL como origen, seleccione una base de datos SQL de Azure como destino y haga clic en **Crear**.
3. En este ejemplo, debido a que estamos accediendo a la base de datos de SQL Server local con Azure SQL Database por cualquier incompatibilidad, debe elegir **Comprobar la compatibilidad de la base de datos y Comprobar la paridad de funciones** (consulte la [Figura 4-40](#)). Haga clic en **Siguiente**.
4. Conéctese a la base de datos SQL Server de origen utilizando las credenciales de la base de datos e inicie una evaluación. Tenga en cuenta que la credencial utilizada para conectarse al servidor SQL debe ser miembro de la función del servidor sysadmin.
5. Una vez que los resultados de la evaluación están listos, el siguiente paso es resolver los problemas o cualquier bloqueo de migración que pueda afectar la migración. Repita los pasos de la evaluación hasta que se solucionen todos los problemas.

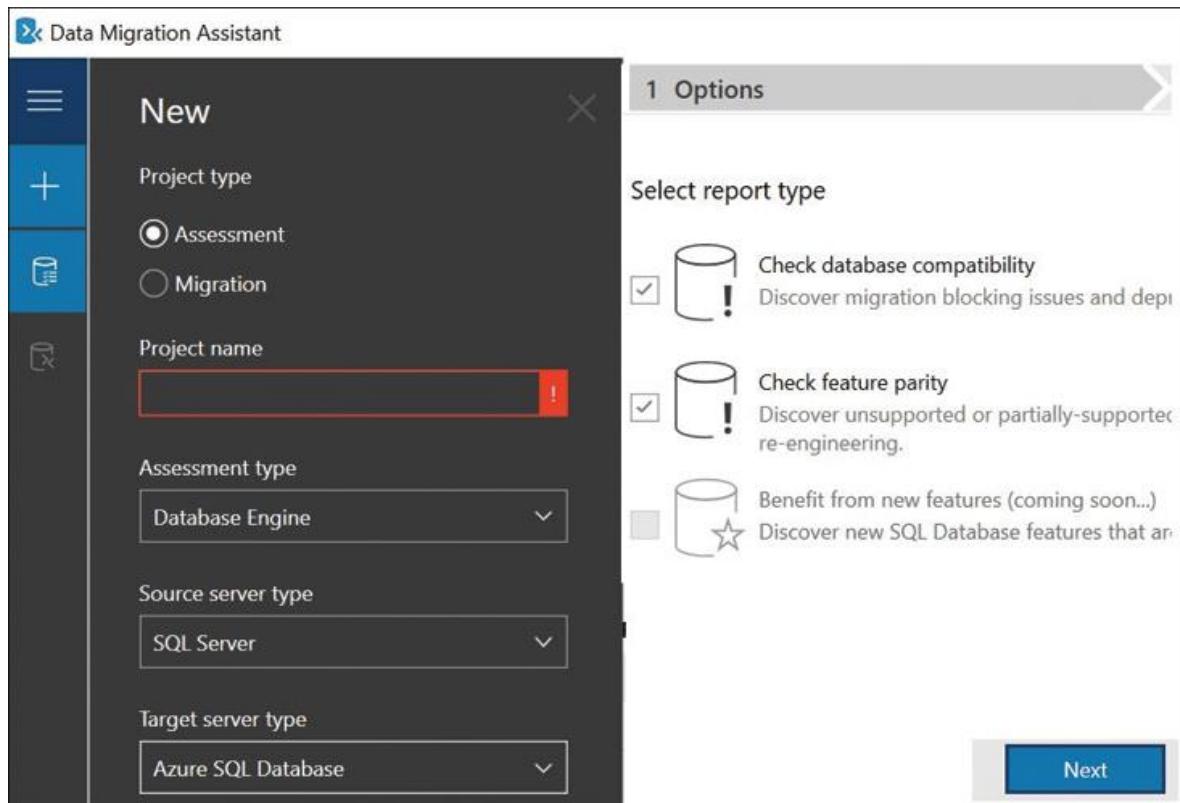


FIGURA 4-40 Asistente de migración de base de datos

Una vez que esté seguro de que se han resuelto todos los problemas y de que la base de datos de SQL Server local se ha convertido en un buen candidato para la migración, continúe con los siguientes pasos para implementar un esquema en Azure SQL Database:

1. Inicie sesión en Azure Portal y cree una base de datos SQL de Azure en blanco.
2. Una vez que la base de datos esté lista, navegue hasta su hoja y cree una regla de permiso de firewall en Azure SQL Database para una dirección IP de salida de la máquina de origen donde está ejecutando su herramienta DMA.
3. A continuación, en la herramienta DMA, cree un nuevo proyecto de migración seleccionando la opción **Migración**, como se muestra en la [Figura 4-40](#). Los asistentes de la herramienta DMA lo guiarán para proporcionar detalles de la base de datos de origen y destino. Debe utilizar una credencial con permiso de servidor de control para conectarse a la base de datos de origen y permiso de la

base de datos de control para conectarse a la base de datos de destino.

4. Con la herramienta DMA, seleccione los objetos del esquema de la base de datos para generar una secuencia de comandos. Una vez que el script esté listo, use la función de implementación de esquema de DMA para implementar el esquema en la base de datos de destino.

Ahora que hemos implementado con éxito el esquema de la base de datos SQL local en la base de datos SQL de Azure, crearemos un servicio de migración de la base de datos de Azure para la migración de datos. Sigue estos pasos:

1. En Azure Portal, busque el recurso **Azure Database Migration Service** y haga clic en **Agregar** (consulte la [Figura 4-41](#)).

The screenshot shows the 'Azure Database Migration Services' blade in the Azure Portal. At the top, there's a breadcrumb navigation: Home > Azure Database Migration Services. Below that is a title bar with 'Azure Database Migration Services' and a 'Default Directory'. There are four buttons: '+ Add' (highlighted with a red box), 'Edit columns', 'Refresh', and 'Assign tags'. A 'Subscriptions' section follows, with a message 'Pay-As-You-Go – Don't see a subscription? Open Directory'. Below this are two input fields: 'Filter by name...' and 'All resource groups...'. Underneath, it says '1 items' and shows a single item with a checkbox labeled 'Name ↑↓' and a 'Status' column. The entire interface has a light blue header and a white body with some shadows.

FIGURA 4-41 Servicios de migración de bases de datos de Azure

2. Tenga en cuenta los siguientes puntos críticos al crear un servicio de migración de base de datos (DMS):
 1. ■ El DMS requiere una red virtual que facilite la conectividad con el servidor de origen. Dicho esto, debe crear una nueva red virtual junto con la configuración de un DMS o elegir entre la existente. Usaría VPN de sitio a sitio o ExpressRoute para la conectividad local. El punto de conexión de servicio, `Microsoft.Sql`, debe agregarse en la red virtual para permitir la conexión saliente a la base de datos SQL de Azure.

2. ■ Asegúrese de que los grupos de seguridad de red de la red virtual de Azure permitan la conectividad entrante para DMS en los puertos TCP 443, 53, 1433, 9354, 445 y 12000.
3. ■ Debe elegir la ubicación del servicio DMS más cercana al centro de datos de su base de datos de origen para lograr una baja latencia y una migración más rápida. Se recomienda que seleccione SKU más altos en la base de datos de destino para acelerar el proceso de migración de datos. Puede reducir la SKU de la base de datos después de que se complete la migración.
3. Ahora que se ha creado el DMS, navegue hasta la hoja de descripción general de DMS y haga clic en **Nuevo proyecto de migración**, como se muestra en la [Figura 4-42](#).

The screenshot shows the Azure portal interface for a Database Migration Service (DMS) named 'dmsaz303'. The top navigation bar includes 'Home', 'Azure Database Migration Services', and the service name 'dmsaz303'. Below the navigation is a search bar and a row of buttons: '+ New Migration Project' (highlighted with a black box), 'Delete service', and 'Refresh'. On the left, a sidebar menu lists 'Overview' (selected), 'Activity log', 'Access control (IAM)', 'Tags', 'Settings', 'Properties', and 'Configuration'. The main content area displays service details: Resource group : RG-AZ-303-Exam, Virtual network & IP Ad... : dmsvnet/subnets/default 10.0.0.4, Subscription : Pay-As-You-Go, SKU : Premium: 4 vCores, and Tags (change) : Click here to add tags. Below this is a table with a single row: Name SQLServerMigration and Source SQL Server.

Name	Source
SQLServerMigration	SQL Server

FIGURA 4-42 Adición de un nuevo proyecto de migración en DMS

4. Complete los campos obligatorios, como se muestra en la [Figura 4-43](#). Establezca el **Tipo de servidor de origen** en **SQL Server** y el **Tipo de servidor de destino** en **Azure SQL Database**. En **Tipo de migración / actividad**, elija **Migración de datos en línea** y haga clic en **Guardar**.

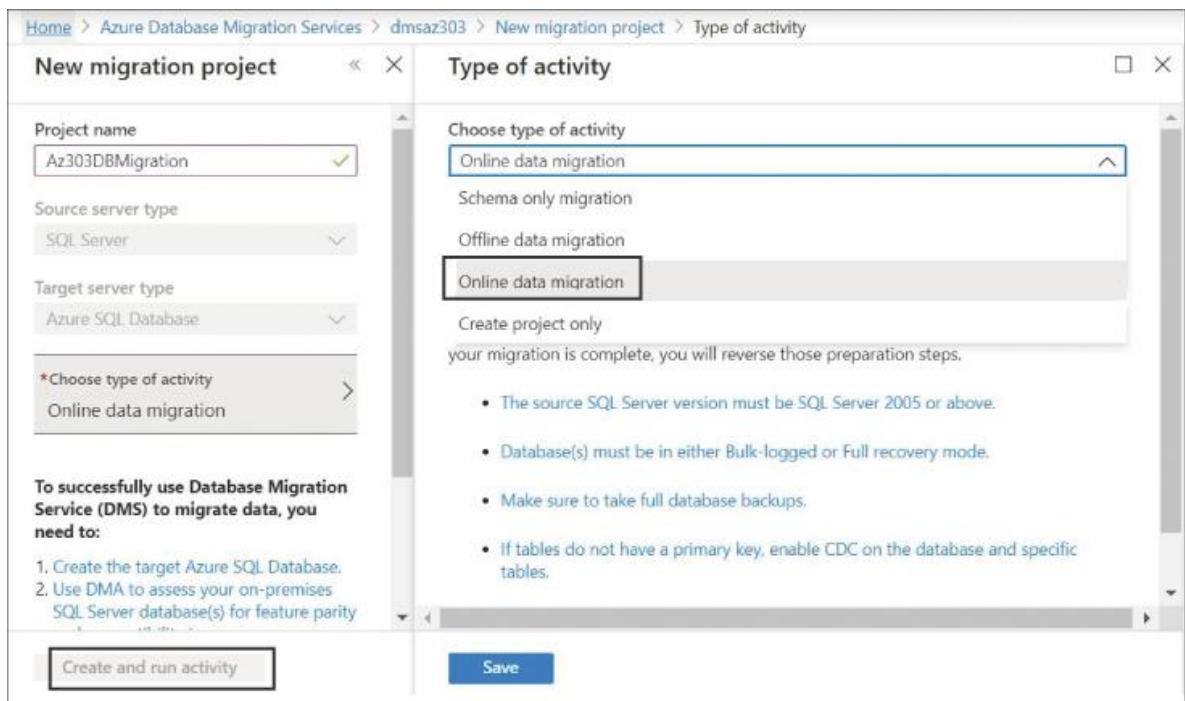


FIGURA 4-43 Configuración de un proyecto de migración de base de datos

Para la migración en línea, se requiere la replicación continua de datos. Por lo tanto, debe realizar las siguientes configuraciones en la base de datos de origen para la replicación.

1. La función de replicación debe instalarse en el servidor SQL de origen. Utilice los siguientes comandos de TSQL para comprobar si el componente de replicación está instalado. Verá un error si no es así:

Haga clic aquí para ver la imagen del código

```
USE maestro; DECLARAR @instalado int; EJECUTAR
@instalado = sys.

sp_MS_rePLICATION_installed;

SELECCIONE @instalado como instalado;
```

2. Utilice el siguiente TSQL para habilitar la replicación:

Haga clic aquí para ver la imagen del código

```
USE maestro
```

```
EXEC sp_replicationdboption @dbname = <databasename>,
@optname = 'publicar', @
valor = 'verdadero' GO
```

3. Una vez habilitada la replicación, configure la función de distribuidor para el SQL Server de origen. Los pasos para publicar la distribución del servidor SQL se dan en la documentación de Microsoft en <https://docs.microsoft.com/en-us/sql/relational-databases/replication/configure-publishing-and-distribution?view=sql-server-ver15>.
4. La base de datos debe estar en modo de recuperación completa. Utilice los siguientes comandos de TSQL para verificar y habilitar el modo de recuperación completo:

Haga clic aquí para ver la imagen del código

```
USE maestro;

SELECCIONE nombre, recovery_model_desc FROM
sys.databases DONDE nombre =
<databasename>

ALTER DATABASE <nombre de la base de datos> SET
RECOVERY FULL;
```

5. Asegúrese de que todas las tablas de la base de datos de origen tengan un índice agrupado (clave principal). Utilice los siguientes comandos de TSQL para buscar tablas sin un índice agrupado y créelos en consecuencia:

Haga clic aquí para ver la imagen del código

```
USE <databasename>; ir

SELECCIONE is_tracked_by_cdc, nombre AS TableName FROM
sys.tables DONDE escriba = 'U' y
is_ms_shipped = 0 Y

OBJECTPROPERTY (OBJECT_ID, 'TableHasPrimaryKey') = 0;
```

6. Asegúrese de realizar la copia de seguridad completa de la base de datos de origen.
7. Asegúrese de configurar una regla de firewall de Windows para permitir que Azure Database Migration Service acceda al SQL Server de origen; de forma predeterminada, este es el puerto TCP 1433.
8. Asegúrese de que el protocolo TCP / IP esté habilitado en el servidor SQL de origen.

Limitaciones importantes de la migración en línea y solución alternativa para una sola base de datos

El servicio DMS tiene algunas limitaciones en la redacción de este libro, y las soluciones para tales limitaciones se detallan en el documento de Microsoft publicado en <https://docs.microsoft.com/en-us/azure/dms/known-issues-azure-sql-online> . Asegúrese de evaluarlos todos antes de adaptarse a la migración en línea.

9. En el asistente de migración que se muestra en la [Figura 4-44](#) , seleccione la base de datos de origen y de destino, como se muestra en los pasos 1 y 2 en el panel del **Asistente de migración** .
10. En el panel de la base de datos de origen, **Detalle del origen de la migración** , proporcione los detalles de conexión para la base de datos de origen. Se recomienda que utilice el certificado de confianza en el servidor de origen para cifrar las credenciales de conexión. En caso de que no lo tenga instalado, puede utilizar un certificado autofirmado creado por DMS seleccionando un certificado de servidor de confianza.
11. Haga clic en **Guardar** .
12. En el panel de la base de datos de destino, en **Detalle del destino de la migración** , especifique los detalles de la conexión para la base de datos SQL de Azure que creó en el paso 6. Se recomienda que cifre la conexión entre las bases de datos de origen y de destino seleccionando **Cifrar conexión** (consulte la [Figura 4-44](#)).
13. Haga clic en **Guardar** .

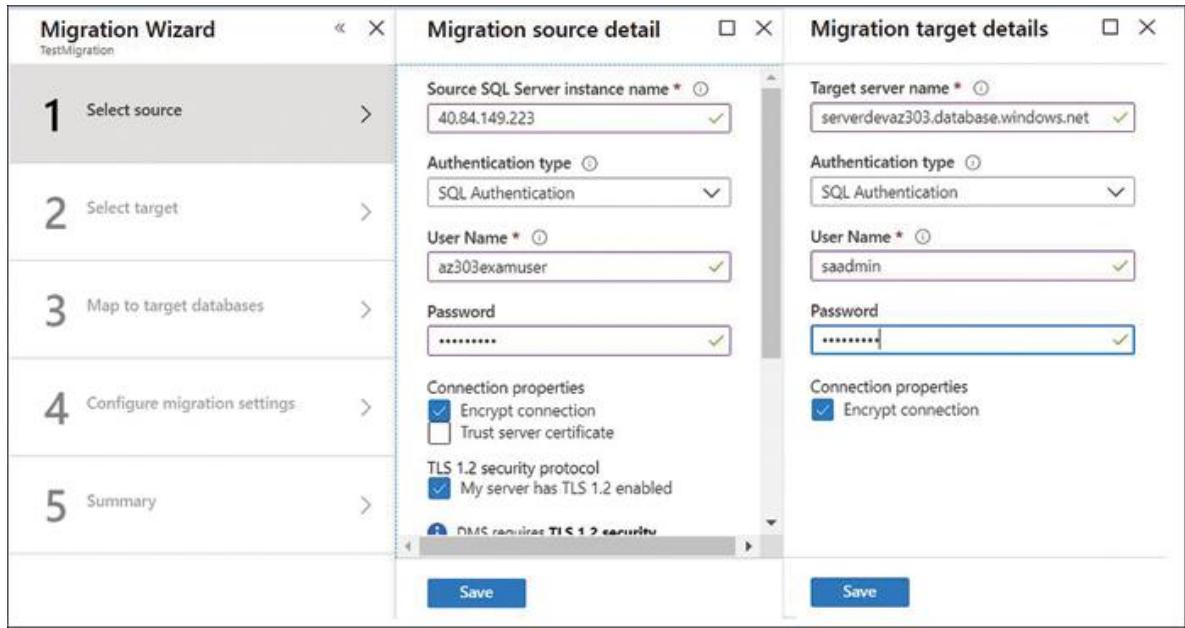


FIGURA 4-44 Configuración de los detalles de conectividad de la base de datos de origen y destino

14. En **Asignar a bases de datos de destino**, asigne las bases de datos de origen y destino a menos que el nombre de la base de datos de destino sea el mismo que el de la base de datos de origen.
15. En **Configurar opciones de migración**, seleccione las tablas de la base de datos de origen que se migrarán.
16. Por último, en la pantalla de resumen, haga clic en **Ejecutar migración**, como se muestra en la [Figura 4-45](#).

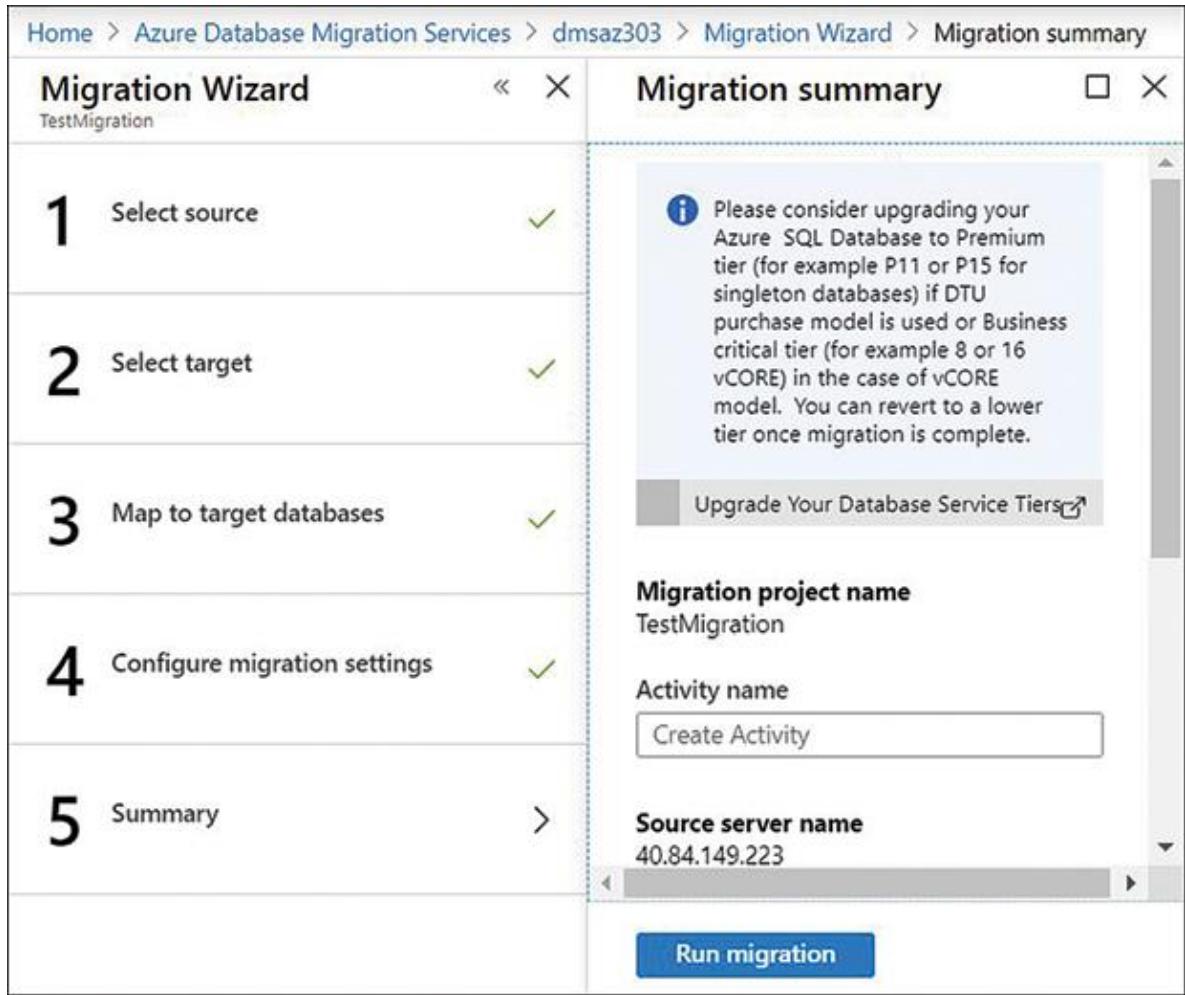


FIGURA 4-45 Asistente de resumen del servicio de migración de la base de datos

17. La figura 4-46 muestra la actividad migratoria. Desde aquí, puede controlar el estado de la migración. Una vez que se haya completado, puede planificar la transición final haciendo clic en el botón **Iniciar transición**. Antes de planificar la transición, asegúrese de detener las transacciones nuevas en la base de datos de origen o espere a que se completen las transacciones pendientes existentes. Una vez realizada la migración, realice la validación de datos en la base de datos SQL de Azure de destino y conecte la aplicación a la nueva base de datos SQL de Azure.

The screenshot shows the Azure Database Migration Services interface. At the top, the navigation path is: Home > Azure Database Migration Services > dmaz303 > SQL Server Migration (dmsaz303/SQLServerMigration) > netrybackupaz3030 > AdventureWorksDW2014. Below the path, the database name is listed as AdventureWorksDW2014.

AdventureWorksDW2014

Key status information:

- Source database name:** AdventureWorksDW2014
- Target database name:** AzureSqlEduS03
- Database status:** Running
- Migration details:** Ready to cutover

Migration progress summary:

Category	Value
Full load completed	2
Full load queued	0
Full load loading	0
Full load failed	0
Incremental updates	0
Incremental inserts	10
Incremental deletes	0

Applied changes: 10. Tables in error state: 0.

Migration details table:

Table name	Status	Completed	Rows	Duration
dbo.DimGeography	Completed	4/12/2020, 8:45:20 PM	656	00:00:03
dbo.DimSalesTerritory	Completed	4/12/2020, 8:45:22 PM	11	00:00:02

Page navigation: — prev Page 1 of 1 next —

FIGURA 4-46 Un asistente de estado de migración de la base de datos

RESUMEN DEL CAPÍTULO

- Las bases de datos NoSQL son bases de datos no relacionales diseñadas para proporcionar un modelo de datos flexible y patrones de acceso para varios conjuntos de datos complejos.
- Los tipos típicos de bases de datos NoSQL incluyen el almacén de datos de valor clave, bases de datos de documentos, bases de datos de gráficos y bases de datos de familias de columnas.
- Azure Table Storage es un almacenamiento de datos de valor clave altamente escalable para datos estructurados.
- Azure Cosmos DB es una base de datos multimaestro distribuida globalmente que le permite escalar de forma independiente el rendimiento y el almacenamiento en todo el mundo con rendimiento y rendimiento garantizados.
- Azure Cosmos DB admite cinco API de programación: SQL API, Mongo API, Cassandra API, Gremlin Graph API y Table API.
- Azure Cosmos DB le permite configurar réplicas de varios maestros en todas las regiones para facilitar la comutación por error y la alta disponibilidad en caso de un evento disruptivo en la región principal.
- Azure SQL Database es una de las bases de datos relacionales administradas más populares. El servicio tiene diferentes niveles

para elegir según las necesidades de rendimiento de su aplicación.

- Las unidades transaccionales de base de datos (DTU) son una medida combinada de recursos informáticos, de almacenamiento y de E / S que se asignan previamente cuando se crea una base de datos en el servidor lógico.
- El modelo basado en núcleos virtuales es el modelo de compra recomendado por Microsoft en el que obtiene la flexibilidad de escalar de forma independiente el procesamiento y el almacenamiento para satisfacer las necesidades de su aplicación.
- Las copias de seguridad de restauración en un momento dado en Azure SQL Database se almacenan hasta 35 días en almacenamiento Blob replicado geográficamente. Si necesita que la copia de seguridad se retenga más allá de los 35 días, puede configurar políticas de retención de copias de seguridad a largo plazo.
- La base de datos de instancias administradas de Azure SQL proporciona una compatibilidad cercana al 100 por ciento con SQL Server local. La base de datos solo se puede crear dentro de una red virtual dedicada y exponerse a través de un punto de conexión privado de forma predeterminada.
- El servicio de migración de bases de datos de Azure admite la migración de bases de datos en línea y sin conexión. El servicio utiliza la herramienta del asistente de migración de bases de datos para la migración de esquemas y la replicación sincrónica entre la base de datos de origen y de destino para la migración de datos.

EXPERIMENTO MENTAL

En este experimento mental, demuestre sus conocimientos y habilidades que ha aprendido a lo largo del capítulo. Las respuestas al experimento mental se dan en la siguiente sección.

Eres arquitecto de una institución de educación en línea. La institución tiene su propio departamento de desarrollo de software y tecnologías de

la información. La institución tiene su base de estudiantes en todo el mundo y ofrece cursos de estudio en línea sobre diversas materias, realiza exámenes y proporciona títulos en línea al completar con éxito el curso. El contenido del curso está disponible en línea durante los días de semana y la capacitación dirigida por un instructor se lleva a cabo durante el fin de semana. El portal web en línea utilizado por la institución tiene un núcleo .NET integrado y el backend es un servidor SQL para almacenar detalles de los cursos disponibles y MongoDB NoSQL para la auditoría personalizada de la aplicación. La solicitud está alojada en los EE. UU. La institución enfrenta varios desafíos y recibe quejas de estudiantes de todo el mundo de que la solicitud de cursos en línea y exámenes de práctica funciona muy lentamente en ocasiones.

1. 1. La institución tiene un presupuesto limitado y no puede permitirse reescribir el código de la aplicación para adoptar la nube. La administración no quiere cambiar el montón de trabajos por lotes escritos en el servidor SQL.
2. 2. La administración de la institución tiene preocupaciones de seguridad al usar las bases de datos en la nube en términos de mantener las bases de datos fuera de la red privada en la nube.

RESPUESTAS DEL EXPERIMENTO MENTAL

Esta sección contiene soluciones al experimento mental.

1. 1. Dado que la aplicación se basa en la pila de tecnología de Microsoft, puede alojarla en Azure App Services y configurar el ajuste de escala automático. Con respecto al backend del servidor SQL, la instancia administrada de Azure SQL Database le proporciona una compatibilidad cercana al 100 por ciento con SQL Server. Por lo tanto, no tendrá que cambiar el código de la aplicación cuando migre de SQL Server a Azure SQL Managed Instance.
2. 2. Para el backend NoSQL, MongoDB, puede usar la API de Cosmos DB MongoDB y migrar sin cambiar ningún código de aplicación.
3. 3. Para abordar los problemas de seguridad, la postura de seguridad de Azure SQL Managed Instance proporciona una integración nativa con la red virtual de Azure donde el tráfico de su

aplicación no pasa por la Internet pública y permanece en la red troncal de Microsoft.

Índice

A

control de acceso, Azure SQL Database, [302](#)
claves de acceso
gestión, [35 - 36](#)
giratorio, [36](#)
políticas de acceso, creación, [177 - 178](#)
niveles de acceso, [32](#)
manchas, [31 - 32](#)
cuentas. *Ver también cuentas de usuario*
Cosmos DB, [277 , 278 - 279](#)
ACI (instancias de contenedor de Azure), [22 , 264](#)
ACR (Registro de contenedores de Azure), [262](#)
creación de recursos para imágenes de contenedor, [262 - 264](#)
ACS (Servicio de contenedor de Azure). *Consulte AKS (Servicio de Azure Kubernetes)*
grupos de acción, creación, [26 - 27](#)
Registro de actividades, [5](#)
ADE (cifrado de disco de Azure), [53 - 56](#)
protección avanzada contra amenazas, Azure SQL Database, [303 - 304](#)
AKS (Servicio de Azure Kubernetes), [22](#)
configurar, [266](#)
crear un clúster con la CLI de Azure, [266 - 267](#)
servicios de pólizas, [231 - 232](#)
alertas
creando, [28 - 29](#)
visualización, [29](#)
API
Cosmos DB, [281 - 282](#)
Cassandra, [283 - 284](#)
Gremlin, [284](#)
MongoDB, [283](#)
SQL, [282 - 283](#)
Mesa, [283](#)
seleccionar, [286](#)

APM (Application Performance Management), la aplicación Insights, [20](#) - [21](#) de pasarelas de aplicación, [188](#) - [189](#) Balanceador de carga de Azure, [195](#) piscinas de fondo, [197](#) configuración, [195](#) - [197](#) sondas de salud, [198](#) reglas, [198](#) - [199](#) configuración de extremo frontal, [190](#) - [191](#) balanceo de carga, [191](#) - [192](#) La ruta basadas URL de enrutamiento, [192](#) - [195](#) Perspectivas de la aplicación, [20](#) - [21](#) disponibilidad, [21](#) fracasos, [21](#) Mapa de aplicación, [20](#) registro de solicitud, [183](#) - [186](#) la creación de un secreto de cliente, [186](#) - [187](#) nivel de archivo, Azure Storage, [32](#) Plantillas ARM (Azure Resource Manager), [63](#) - [64](#) y Azure Blueprint, [235](#) en blanco, [67](#) desplegando desde, [70](#) - [73](#) expresiones, [69](#) - [70](#) modificando, [66](#) - [68](#) parámetros, [67](#) - [68](#) guardar una implementación como, [64](#) - [66](#) VHD (disco virtual), [73](#) - [74](#) ASG (grupos de seguridad de aplicaciones), [211](#) , [214](#) asignación de miembros, [215](#) creando, [214](#) - [215](#) herramientas de evaluación, la migración del servidor, [132](#) - [133](#) asignar miembros de los ASG (grupos de seguridad de aplicaciones), [215](#) pólizas, [229](#) - [230](#) roles, [240](#) - [241](#) auditoría, la base de datos SQL Azure, [304](#) - [305](#) autenticación registro de solicitud, [183](#) - [186](#)

identidad administrada, [181](#) - [183](#)
multifactor, [93](#) - [95](#) , [131](#)
opciones de derivación, [97](#) - [98](#)
configurar métodos de verificación, [100](#) - [101](#)
IP confiables, [98](#) - [99](#)
cuentas de almacenamiento, [42](#) - [46](#)
verificación en dos pasos, [93](#) , [97](#)
grupos de auto-failover, [311](#) - [314](#)
runbook de automatización, creación, [75](#) - [79](#)
ajuste de escala automático, [62](#)
conjuntos de disponibilidad, [56](#) - [59](#)
zonas de disponibilidad, [59](#) - [60](#)
Registro de Azure Active Directory, [5](#)
Azure AD (Active Directory), [86](#) , [176](#)
agregar dominios personalizados, [87](#) - [88](#)
registro de solicitud, [183](#) - [186](#)
la creación de un secreto de cliente, [186](#) - [187](#)
acceso condicional, [108](#) - [111](#)
configurar cuentas de usuario para MFA, [93](#) - [95](#)
Connect Health, [125](#) - [127](#)
alertas de fraude, [96](#) - [97](#)
cuentas de invitado
sumando, [101](#) - [102](#)
gestión, [102](#) - [105](#)
Protección de la identidad, [106](#) - [108](#)
la implementación de autoservicio de restablecimiento de
contraseña, [89](#) - [91](#)
identidad administrada, [181](#) - [183](#)
administrar varios directorios, [88](#) - [89](#)
SSO sin costuras, [123](#) - [125](#)
cuentas de almacenamiento, autenticación, [42](#) - [46](#)
niveles, [86](#) - [87](#)
Azure AD Connect
las opciones de sincronización de identidad, [118](#) - [119](#)
la instalación y configuración, [112](#) - [118](#)
Azure Advisor, recomendaciones, [9](#)- [10](#)
Servicio de aplicaciones de Azure, [249](#)
ACI (Azure Container Instances), creando, [264](#)

ranuras de despliegue, [254](#)
crear, [254 - 255](#)
permitiendo identidad administrada, [182 - 183](#)
Integración de VNet, [253 - 254](#)
aplicaciones web, [250](#)
para recipientes, [251 - 252](#)
creando, [250 - 251](#)
Bastión Azure, [215 - 216](#)
configurar, [216](#)
conectarse a un servidor, [217 - 218](#)
Plano Azure, [232](#)
y plantillas ARM, [235](#)
configurar, [232 - 234](#)
Backend de CosmosDB, [232](#)
CLI de Azure
comandos para la gestión de contenedores, [266](#)
creando un clúster de AKS, [266 - 267](#)
documentación, [273](#)
Azure Cosmos DB, [276 - 277](#)
cuentas, [277](#)
configuraciones, [287 - 288](#)
creando, [278 - 279](#)
API, [281 - 282](#)
Cassandra, [283 - 284](#)
Gremlin, [284](#)
MongoDB, [283](#)
seleccionar, [286](#)
SQL, [282 - 283](#)
Mesa, [283](#)
opciones de coherencia de datos, [279 - 280](#)
configuración de réplicas, [287](#)
Administración de costos de Azure, [15](#)
presupuestos, [16](#)
gasto, [16](#)
informes, [17](#)
Azure rectángulo de los datos, la migración fuera de línea, [146 - 149](#)
Hosts dedicados de Azure, [63](#)
Cortafuegos Azure, [199](#)

configurar en una red virtual, [199 - 200](#)
reglas, [201 - 203](#)
etiquetas de servicio, [202 - 203](#)
inteligencia de amenazas, [203](#)
Puerta de entrada azul, [204](#)
configurar, [204 - 205](#)
Políticas WAF, [206 - 208](#)
Funciones de Azure, [168 , 257](#)
aplicaciones de función, creación, [168 - 170 , 258 - 259](#)
funciones, [257 - 258](#)
creando, [259 - 260](#)
Azure Key Vault, [176](#)
política de acceso, creación, [177 - 178](#)
acceder a un punto final, [181](#)
creando recursos, [176 - 177](#)
operaciones criptográficas, [179](#)
operaciones clave de gestión, [179](#)
operaciones de clave privilegiada, [179 - 180](#)
Eliminación suave, [177](#)
Balanceador de carga de Azure, [195](#)
piscinas de fondo, [197](#)
configuración, [195 - 197](#)
sondas de salud, [198](#)
reglas, [198 - 199](#)
Aplicaciones lógicas de Azure, [255](#)
la creación de una aplicación lógica, [255 - 256](#)
aplicaciones lógicas
creando una acción de correo electrónico, [257](#)
creando un disparador RSS, [256 - 257](#)
Azure Migrate, [132](#)
herramientas de evaluación, [132 - 133](#)
Herramienta de evaluación del servidor, [133 - 138](#)
Evaluación y migración de bases de datos SQL, [141 - 144 , 145 - 146](#)
migración de la infraestructura de escritorio virtual, [146](#)
Monitor de Azure
grupos de acción, creación, [26 - 27](#)
alertas
creando, [28 - 29](#)

visualización, [29](#)
línea de base [8-9](#)
para contenedores, [12 - 22](#)
Insights, [18](#)
Analítica registro de espacio de trabajo, creando, [18 de - 19 de](#)
supervisión de la capacidad de rendimiento, [10 - 11](#)
visualización de datos de diagnóstico, [12 - 13](#)
Registro de Azure Monitor, [10](#)
Vigilante de la red de Azure, [14](#)
topología, el seguimiento, [14 - 15](#)
Política de Azure, [228 - 229](#)
asignar una política, [229 - 230](#)
Portal de Azure
exportar plantillas, [64 - 66](#)
biblioteca de plantillas, [74 - 75](#)
Centro de seguridad de Azure, [3](#)
nivel gratuito, [3](#)
Agente de Log Analytics, [3, 10](#)
nivel estándar, [3](#)
características principales, [3-4](#)
Centinela azur, [4](#)
Autobús de servicio Azure, [174](#)
cola de mensajes, [175](#)
espacio de nombres de bus de servicio, [174](#)
Azure Servicio de Salud, [13 - 14](#)
Recuperación del sitio de Azure, [132 , 153](#)
migrar a Azure, [163](#)
en las instalaciones de componentes, configuración, [155 - 159 , 160](#)
configuración del plan de recuperación, [161 - 162](#)
la replicación de datos de Azure, [160 - 161](#)
recursos, creando, [153 - 154](#)
prueba de conmutación por error, [162](#)
limpieza, [163](#)
Base de datos SQL de Azure, [289 , 318 - 319](#)
copias de seguridad, [294](#)
manual, [297](#)
BCDR (continuidad del negocio y recuperación ante desastres), [310](#)
creando, [291 - 294](#)

sabores, [289](#)
alta disponibilidad, [309 - 310](#) , [311](#)
configurar un grupo de conmutación por error automática, [311 - 314](#)
estrategia de replicación geográfica, [311](#)
modelos, [310](#)
LTR (retención de copia de seguridad a largo plazo) las copias de seguridad, [294 - 296](#)
creando, [296](#)
restaurando, [296 - 297](#)
Instancia administrada, [305 - 306](#)
creando, [306 - 308](#)
especificando tipo de conexión, [307 - 309](#)
publicación, [314 - 321](#)
migración de datos, [315 - 318](#)
DMA (Asistente de migración de base de datos), [314](#) , [315](#)
DMS (Servicio de migración de bases de datos), [314 - 321](#)
métodos, [314](#)
migración en línea, [318 - 319](#)
fases, [314](#)
modelos de compra, [290](#)
leer escalado [horizontal](#) , [299](#)
escala, [297 - 300](#)
seguridad, [299 - 300](#)
control de acceso, [302](#)
protección avanzada contra amenazas, [303 - 304](#)
auditoría, [304 - 305](#)
configurar reglas de firewall a nivel de servidor, [300 - 302](#)
protección de datos y cifrado, [302 - 303](#)
estrategia de defensa en profundidad, [299](#)
Almacenamiento Azure, [30](#)
teclas de acceso, gestión, [35 - 36](#)
comutación por error de cuenta, implementación, [48](#)
Archivos de Azure, configuración, [32 - 34](#)
manchas
niveles de acceso, [31 - 32](#)
almacenamiento, [34 - 35](#)
servicios básicos, [30 - 31](#) , [32](#)
discos, [31](#) , [51](#)

cifrado, [53 - 56](#)
roles, [51 - 52](#)
colas, [31](#)
replicación, [46 - 47](#)
cuentas de almacenamiento
autenticación, [42 - 46](#)
configurar el acceso a la red, [36 - 38](#)
puntos finales privados, [39](#)
SAS (firma de acceso compartido), [39 - 42](#)
tipos, [31](#)
mesas, [31](#)
Azure Table Storage, [270 - 271](#)
la configuración de la tabla de acceso de datos de
almacenamiento, [274 - 276](#)
y API de tabla de Cosmos DB, [276](#)
creación de un servicio de almacenamiento, [273 - 274](#)
modelo de datos, [271 - 272](#)
documentación, [273](#)
llave de partición, [272](#)
clave de fila, [272](#)
SAS (firma el acceso compartido), [274 - 275](#)
política de acceso almacenado, [275 - 276](#)
Propiedad de marca de tiempo, [272](#)
Administrador de tráfico de Azure, [208](#) . Consulte también [NSG](#)
[\(grupos de seguridad de red\)](#)
agregar puntos finales, [209 - 210](#)
configurar, [208 - 209](#)
configurar la monitorización del tráfico, [210 - 211](#)
medidas reales de usuario, [211](#)
vista de tráfico, [211](#)
Administración de actualizaciones de Azure, [149 - 150](#)
configurar, [150 - 151](#)
Máquinas virtuales de Azure
extensión de diagnóstico, [7-8](#)
alta disponibilidad, [56](#)
conjuntos de disponibilidad, [56 - 59](#)
zonas de disponibilidad, [59 - 60](#)
Acceso JIT (justo a tiempo), [4](#)

B

Copia de seguridad y recuperación del sitio, [154 - 155](#)
copias de seguridad
administrar en Azure SQL Database, [294](#)
manual, [297](#)
línea de base [8-9](#)
BEK (clave de cifrado de BitLocker), [55](#)
manchas, [30](#)
niveles de acceso, [31 - 32](#)
almacenamiento, [34 - 35](#)
presupuestos, creación, [16](#)

C

API de Cassandra, [283 - 284](#)
el secreto de cliente, creando, [186 - 187](#)
cmdlets, [33 , 35](#)
Get-AzStorageBlobContent, [43](#)
New-AzWebApp, [252](#)
Set-AzDiagnosticSetting, [7](#)
bases de datos de familias de columnas, [270](#)
acceso condicional, [108 - 111](#)
Configuración como código, [64](#)
configurando
ADE (cifrado de disco de Azure), [53 - 56](#)
AKS (Servicio de Azure Kubernetes), [266](#)
Azure AD Connect, [112 - 118](#)
Bastión azur, [216](#)
Plano Azure, [232 - 234](#)
Archivos de Azure, [33 - 34](#)
Cortafuegos de Azure
reglas, [201 - 203](#)
etiquetas de servicio, [202 - 203](#)
inteligencia de amenazas, [203](#)
Azure Puerta principal, [204 - 205](#)
Políticas WAF, [206 - 208](#)
Carga azul del balanceador, [195 - 197](#)

piscinas de fondo, [197](#)
sondas de salud, [198](#)
reglas, [198 - 199](#)
Azure sitio de recuperación, locales en componentes, [155 - 159](#), [160](#)
Almacenamiento Azure Tabla, acceso a datos de almacenamiento, [274 - 276](#)
Administrador de tráfico de Azure
puntos finales, [209 - 210](#)
medidas reales de usuario, [211](#)
monitoreo de tráfico, [210 - 211](#)
vista de tráfico, [211](#)
Administración de actualizaciones de Azure, [150 - 151](#)
cuentas de invitado, [101 - 105](#)
Log espacio de trabajo Analytics, [18 - 19](#)
Bases de datos NoSQL, tablas de cuentas de almacenamiento, [270](#)
plan de recuperación, [161 - 162](#)
recursos, configuración de diagnóstico, [5-7](#)
juegos de escalas, [60 - 61](#)
ajuste de escala automático, [62](#)
cuentas de almacenamiento
acceso a la red, [36 - 38](#)
SAS (firma de acceso compartido), [39 - 42](#)
Almacenamiento de VM, [50 - 53](#)
VPN
ExpressRoute, [225 - 226](#), [227 - 228](#)
de sitio a sitio, [221 - 222](#)
Connect Health, [125 - 127](#)
Monitor de conexión, [15](#)
opciones de consistencia, Cosmos DB, [279 - 280](#)
contenedor de imágenes
construir un recurso de almacenamiento, [262 - 264](#)
creando, [261 - 262](#)
contenedores, [261](#)
manchas, [34 - 35](#)
comandos de gestión, [266](#)
crear una aplicación web, [251 - 252](#)
métricas, [22](#)
seguimiento, [12 - 22](#)

basada en cookies de afinidad, [191](#) - [192](#)
nivel fresco, Azure Storage, [32](#)
Cosmos DB, [276](#) - [277](#)
cuentas, [277](#)
configuraciones, [287](#) - [288](#)
creando, [278](#) - [279](#)
API, [281](#) - [282](#)
Cassandra, [283](#) - [284](#)
Gremlin, [284](#)
MongoDB, [283](#)
seleccionar, [286](#)
SQL, [282](#) - [283](#)
Mesa, [283](#)
opciones de coherencia de datos, [279](#) - [280](#)
recuperación ante desastres, [281](#)
configuración de réplicas, [287](#)
API de tabla, [276](#)
Gestión de costes, [15](#)
presupuestos, [16](#)
informes, [17](#)
gasto, [16](#)
creando
ACI (instancia de contenedor de Azure), [264](#)
grupos de acción, [26](#) - [27](#)
ASG (grupos de seguridad de aplicaciones), [214](#) - [215](#)
runbook de automatización, [75](#) - [79](#)
Base de datos SQL de Azure, [291](#) - [294](#)
Tabla Azure servicio de almacenamiento, [273](#) - [274](#)
presupuestos, [16](#)
imágenes de contenedores, [261](#) - [262](#)
Cuenta de Cosmos DB, [278](#) - [279](#)
ranuras de despliegue, [254](#) - [255](#)
aplicaciones de función, [168](#) - [170](#) , [258](#) - [259](#)
funciones, [259](#) - [260](#)
Cuenta V2 de uso general, [31](#)
Log espacio de trabajo Analytics, [18](#) - [19](#)
aplicaciones lógicas, [164](#) - [166](#) , [255](#) - [256](#)
acción de correo electrónico, [257](#)

RSS de disparo, [la tecnología](#) [256 - 257](#)
Copias de seguridad LTR (retención de respaldo a largo plazo), [296](#)
proyectos de migración, [132](#)
recursos, [153 - 154](#)
Azure clave Vault, [176 - 177](#)
recurso de almacenamiento para imágenes de contenedores, [262 - 264](#)
aplicaciones web, [250 - 252](#)
dominios personalizados, agregando, [87 - 88](#)

D

bases de datos. *Consulte también Azure SQL Database; Bases de datos NoSQL; Bases de datos SQL*
familia de columnas, [270](#)
Cosmos DB, [276 - 277](#)
lecturas sucias, [279](#)
documento, [270](#)
gráfico, [270](#)
valor-clave, [269 - 270](#)
relacional, [288](#)
seleccionando, [288 - 289](#)
implementación, desde la plantilla ARM, [70 - 73](#)
ranuras de despliegue, [254](#)
crear, [254 - 255](#)
extensión de diagnóstico, máquinas virtuales de Azure, [7-8](#)
lecturas sucias, [279](#)
recuperación ante desastres, Cosmos DB, [281](#)
discos
Azure Storage, [31 , 51 - 52](#)
cifrado, ADE (Azure Disk Encryption), [53 - 56](#)
DMA (Asistente de migración de base de datos), [314 , 315](#)
DMS (Servicio de migración de bases de datos), [314 - 321](#)
Conjunto de herramientas de Docker
ACR (Registro de contenedores de Azure), [262](#)
creación de imágenes de contenedores, [261 - 262](#)
documentación, [262](#)
bases de datos de documentos, [270](#)
documentación

CLI de Azure, [273](#)
Almacenamiento de Azure Table, [273](#)
Conjunto de herramientas Docker, [262](#)
gobernanza, [237](#)
equilibrio de carga, [218](#)
aplicaciones lógicas, [257](#)
DTU (unidades de transacción de datos), [290](#)

M

bordes, creación para base de datos de gráficos, [285 - 286](#)
edición, plantillas ARM, [66 - 68](#)
cifrado
ADE (cifrado de disco de Azure), [53](#)
Base de datos SQL de Azure, [302 - 303](#)
SSE (cifrado del lado del servidor), [53](#)
puntos finales
agregar a Azure Traffic Manager, [209 - 210](#)
Azure Key Vault, accediendo, [181](#)
configurar el acceso a la red, [36 - 38](#)
privado, [39](#)
discos de SO efímeros, [51 - 52](#)
Cuadrícula de eventos, [172](#)
Características, [173 - 174](#)
suscripciones, [173](#)
temas, [172 - 173](#)
eventos, monitoreo, [13 - 14](#)
exportador
recursos, [65 - 66](#)
plantillas, [64 - 66](#)
expresiones, plantillas ARM, [69 - 70](#)
ExpressRoute, [218 - 219 , 225](#)
configurar, [225 - 226 , 227 - 228](#)
configurar una puerta de enlace de red virtual, [227](#)
ajustes de emparejamiento, [226](#)

F

Comutación por falla

automático, [311 - 314](#)
cuenta de almacenamiento, [48](#)
archivos, Azure, configurando, [32 - 34](#)
alertas de fraude, [96 - 97](#)
aplicación de función
creando, [168 - 170](#)
Kudu consola de solución de problemas, [171 - 172](#)
Descripción general cuchilla, [169 de la - 170](#)
Características plataforma blade, [170 - 171](#)
aplicaciones de función, creando, [258 - 259](#)
funciones, [257 - 258](#)
creando, [259 - 260](#)

GRAMO

Cuenta V2 de propósito general, creación, [31](#)
Cmdlet Get-AzStorageBlobContent, [43](#)
GitHub, [66](#)
Emparejamiento de red virtual global, [83 - 84](#)
gobernanza, [228](#). Consulte también la [Política de Azure](#)
documentación, [237](#)
políticas
Acceso, [177 - 178](#)
Política de AKS complemento, [231 - 232](#)
Puerta de entrada azul, [206](#)
acceso condicional, [108 - 111](#)
acceso almacenado, [275 - 276](#)
WAF, [206 - 208](#)
RBAC (control de acceso basado en roles), [237](#)
configurar el acceso a los recursos mediante la asignación de
roles, [240 - 241](#)
configurar el acceso de administración a Azure, [241 - 242](#)
creando un rol personalizado, [237 - 240](#)
resolución de problemas, [243 - 245](#)
bases de datos de gráficos, [270 , 284](#)
creando bordes, [285 - 286](#)
creando vértices, [284 - 285](#)
API de Gremlin, [284](#). Ver también [bases de datos de gráficos](#)

base de datos de gráficos
creando bordes, [285 - 286](#)
creando vértices, [284 - 285](#)
cuentas de invitado, [101 - 105](#)

H

sondas de salud, [189 - 190](#), [198](#)
alta disponibilidad, [56](#)
conjuntos de disponibilidad, [56 - 59](#)
zonas de disponibilidad, [59 - 60](#)
Azure base de datos SQL, [309 - 310](#), [311](#)
configurar un grupo de commutación por error automática, [311 - 314](#)
estrategia de replicación geográfica, [311](#)
modelos, [310](#)
Azure Storage, [46 - 47](#)
nivel activo, Azure Storage, [32](#)
identidades híbridas, [111 - 112](#)

I

IaaS (infraestructura como servicio), [7](#)
IaC (Infraestructura como código), [63 - 64](#), [71](#)
Protección de la identidad, [106 - 108](#)
Insights, [18](#)
Aplicación, [20 - 21](#)
Red, [22](#)
instalación, Azure AD Connect, [112 - 118](#)

JK

Acceso JIT (justo a tiempo), [4](#)
Plantilla de libro de trabajo de métricas clave, [12](#)
Bóvedas de llaves, [180](#). Consulte también [Azure Key Vault](#)
bases de datos de clave-valor, [269 - 270](#)
KQL (lenguaje de consulta Kusto), [10](#), [11 - 12](#)
Kudu consola de solución de problemas, [171 - 172](#)

L

latencia, monitoreo, [15](#)
Máquinas virtuales Linux
tallaje, [49 - 50](#)
almacenamiento, configuración, [50 - 53](#)
Métricas en vivo, [21](#)
balanceo de carga, [187 , 191 - 192](#)
piscinas de fondo, [197](#)
documentación, [218](#)
sondas de salud, [198](#)
leer escalado [horizontal , 299](#)
reglas, [198 - 199](#)
Analítica registro de espacio de trabajo, creando, [18 de - 19 de](#)
Inicio sesión, [8](#)
Carga de trabajo de VM, [24 - 26](#)
aplicaciones lógicas
edificio, [164 - 166 , 255 - la tecnología 256](#)
crear una acción de correo electrónico, [257](#)
creando un disparador RSS, [256 - 257](#)
documentación, [257](#)
LTR (retención de copia de seguridad a largo plazo) las copias de
seguridad, [294 - 295](#)
creando, [296](#)
restaurando, [296 - 297](#)

METRO

identidad administrada, [181 - 183](#)
grupos de gestión, [235 - 236](#)
agregar suscripciones, [236](#)
cambiando, [237](#)
acceso de nivel superior, [236](#)
gerente
teclas de acceso, [35 - 36](#)
contenedores, [266](#)
cuentas de invitado, [101 - 105](#)
identidades híbridas, [111 - 112](#)

conectividad local, [224](#)
copias de seguridad manuales, [297](#)
métrica, [8-9](#), [22](#)
MFA (autenticación multifactor), [131](#)
opciones de derivación, [97 - 98](#)
configurar, [93 - 95](#)
configurar métodos de verificación, [100 - 101](#)
alertas de fraude, [96 - 97](#)
IP confiables, [98 - 99](#)
proyectos de migración. *Consulte también Azure Site Recovery; migración de servidor*
creando [132](#)
Migración fuera de línea de Data Box, [146 - 149](#)
evaluación del entorno del servidor, [133 - 138](#)
Bases de datos SQL
evaluación, [133 , 141 - 144 , 145 , 314](#)
migración, [145 - 146](#)
publicar una base de datos Azure SQL, [314 - 321](#)
gestión de actualizaciones, [150 - 152](#)
evaluación y migración de aplicaciones web, [138 -145](#)
modificar, plantillas ARM, [66 - 68](#)
API de MongoDB, [283](#)
vigilancia, [1](#). *Consulte también Azure Front Door; Administrador de tráfico de Azure; Monitor de conexión*
contenedores, [12 - 22](#)
costos, [15](#)
presupuestos, [16](#)
gasto, [16](#)
redes, [14](#)
latencia, [15](#)
topología, [14 - 15](#)
actuación, [4](#)
de capacidad, [10 - 12](#)
recursos no utilizados, [9- 10](#)
seguridad, [2](#)
servicio de salud, [13 - 14](#)
Movere, [133](#)

Mi portal de Aplicaciones, SSPR (autoservicio de restablecimiento de contraseñas), [90 - 91](#)

NORTE

Perspectivas de la red, [22](#)
redes
latencia, [15](#)
seguimiento, [14](#)
topología, el seguimiento, [14 - 15](#)
Cmdlet New-AzWebApp, [252](#)
Bases de datos NoSQL, [269](#)
y Azure Table Storage, [270 - 271](#)
API de tabla de Cosmos DB, [276](#)
modelos de datos, [269 - 270](#)
tablas de cuentas de almacenamiento, configuración, [270](#)
NPM (Monitor de rendimiento de red), [15](#)
NSG (grupos de seguridad de red), [211 , 214 , 224 , 225](#)
agregar a una VM, [211 - 212](#)
asociarse con recursos, [214](#)
colocación, [212](#)
reglas, [212 - 214](#)

OP

Onedrive, la conexión a, [166 - 167](#)
Modelo de red OSI, [195](#)
PaaS (plataforma como servicio), configuración de diagnósticos en recursos, [5-6](#)
reescritura contraseña, [119 - 122](#)
mirando
ExpressRoute, [226](#)
VNet, [83 - 85](#)
actuación
Línea de base [8-9](#)
métrica, [8-9](#)
vigilancia, [4](#)
de capacidad, [10 - 12](#)
recursos no utilizados, [9- 10](#)

visualización de datos de diagnóstico, [12](#) - [13](#)
Plantilla de libro de trabajo de análisis de rendimiento, [12](#)
registros de la plataforma, [5](#)
políticas
acceso, creación, [177](#) - [178](#)
AKS (Servicio Azure Kubernetes), [231](#) - [232](#)
asignación, [229](#) - [230](#)
Puerta de entrada azul, [206](#)
acceso condicional, [108](#) - [111](#)
acceso almacenado, [275](#) - [276](#)
WAF, [206](#) - [208](#)
PowerShell, [43](#) , [265](#)
cmdlets, [33](#) , [35](#)
Get-AzStorageBlobContent, [43](#)
New-AzWebApp, [252](#)
Set-AzDiagnosticSetting, [7](#)
configurar los ajustes de diagnóstico en los recursos, [7](#)
la configuración de URL de enrutamiento basado en ruta, [193](#) - [195](#)
crear un secreto de cliente, [187](#)
creación de un registro de aplicación, [185](#) - [186](#)
cuentas de almacenamiento, [39](#) - [42](#)
autenticación, [42](#) - [46](#)
en las instalaciones de componentes Azure sitio de recuperación,
configuración, [155](#) - [159](#) , [160](#)
Base de datos SQL local, migración a la base de datos SQL de
Azure, [314](#) - [315](#)
fase de evaluación, [314](#) , [315](#)
puntos finales privados, [39](#)
publicar una base de datos SQL de Azure
migración de datos, [315](#) - [318](#)
DMA (Asistente de migración de base de datos), [314](#) , [315](#)
DMS (Servicio de migración de bases de datos), [314](#) - [321](#)
métodos, [314](#)
migración en línea, [318](#) - [319](#)
fases, [314](#)
modelos de compra, Azure SQL Database, [290](#)

QR

colas, Azure Storage, [31](#)
RBAC (control de acceso basado en roles), [237](#)
configurar el acceso a los recursos mediante la asignación de roles, [240 - 241](#)
configurar el acceso de administración a Azure, [241 - 242](#)
creando un rol personalizado, [237 - 240](#)
resolución de problemas, [243 - 245](#)
leer escalado [horizontal](#) , [299](#)
plan de recuperación, configuración, [161 - 162](#)
bases de datos relacionales, [288](#) . Consulte también [Azure SQL Database](#)
replicación
Azure Storage, [46 - 47](#)
base de datos, [287](#)
permitiendo el sitio de recuperación Azure, [160 - 161](#)
informes, Gestión de costes, [17](#)
registros de recursos, [5](#)
recursos, [1](#), [153](#)
asignación de roles, [240 - 241](#)
asociarse con NSG (Network Security Group), [214](#)
Azure clave Bóveda, creando, [176 - 177](#)
línea de base [8-9](#)
configurar los ajustes de diagnóstico, [5](#)
usando PaaS, [5-6](#)
usando PowerShell, [7](#)
creando en Azure sitio de recuperación, [153 - 154](#)
implementación desde plantilla ARM, [70 - 73](#)
exportador, [65 - 66](#)
sin servidor, [164](#)
Funciones de Azure, [168](#)
aplicación lógica, [164 - 166](#)
salud del servicio, monitoreo, [13 - 14](#)
no usado, [9- 10](#)
Restaurar, LTR (retención de copia de seguridad a largo plazo), las copias de seguridad [296 - 297](#)
giratorio, teclas de acceso, [36](#)

reglas

Azure Firewall, [201](#) - [203](#)

firewall, [300](#) - [302](#)

balanceo de carga, [198](#) - [199](#)

NSG (Grupo de seguridad de red), [212](#) - [214](#)

runbooks, creando, [75](#) - [79](#)

S

SAS (firma de acceso compartido), [39](#) - [42](#), [274](#) - [275](#)

conjuntos de escalas

ajuste de escala automático, [62](#)

configurar, [60](#) - [61](#)

escalamiento, Azure SQL Database, [297](#) - [300](#)

programación, actualizaciones, [151](#) - [152](#)

SDK, [265](#)

SSO sin costuras, [123](#) - [125](#)

seguridad. Consulte también [ASG \(grupos de seguridad de aplicaciones\)](#); [autenticación](#); [Cortafuegos Azure](#); [Centro de seguridad de Azure](#); [NSG \(grupos de seguridad de red\)](#)

Azure Key Vault, [176](#)

creando recursos, [176](#) - [177](#)

Centinela azur, [4](#)

Base de datos SQL de Azure, [299](#) - [300](#)

control de acceso, [302](#)

protección avanzada contra amenazas, [303](#) - [304](#)

auditoría, [304](#) - [305](#)

configurar reglas de firewall a nivel de servidor, [300](#) - [302](#)

protección de datos y cifrado, [302](#) - [303](#)

estrategia de defensa en profundidad, [299](#)

identidad administrada, [181](#) - [183](#)

vigilancia, [2](#)

seleccionar, API, [286](#)

Herramienta de evaluación del servidor, [133](#) - [138](#)

migración de servidor

herramientas de evaluación, [132](#) - [133](#)

Herramienta de evaluación del servidor, [133](#) - [138](#)

recursos sin servidor, [164](#)

Funciones de Azure, [168 - 172](#)
salud del servicio, monitoreo, [13 - 14](#)
Cmdlet Set-AzDiagnosticSetting, [7](#)
VPN de sitio a sitio
configurar, [221 - 222](#)
verificar la conectividad local, [222 - 223](#)
dimensionamiento de máquinas virtuales, [49 - 50](#)
SLA (acuerdo de nivel de servicio), [56](#)
gasto
presupuestos, [16](#)
seguimiento, [16](#)
informes, [17](#)
API de SQL, [282 - 283](#)
Bases de datos SQL. Ver también [bases de datos NoSQL](#)
evaluación, [141 - 144](#), [145](#)
migrando, [133](#), [145 - 146](#)
SSE (cifrado del lado del servidor), [53](#)
SSE (cifrado del servicio de almacenamiento), [30](#)
SSPR (restablecimiento de contraseña de autoservicio)
implementación, [89 - 91](#)
reescritura contraseña, [119 - 122](#)
almacenamiento
manchas, [34 - 35](#)
creación de recursos para imágenes de contenedor, [262 - 264](#)
mesas, [274 - 276](#)
VM, [50 - 53](#)
cuentas de almacenamiento, [160](#)
teclas de acceso, [35 - 36](#)
autenticación, [42 - 46](#)
configurar el acceso a la red, [36 - 38](#)
comutación por error, [48](#)
llaves, [274](#)
puntos finales privados, [39](#)
SAS (firma de acceso compartido), [39 - 42](#)
tipos, [31](#)
políticas de acceso almacenadas, [275 - 276](#)
suscripciones, [173](#)
grupos de gestión, [235 - 236](#)

identidad administrada asignada por el sistema, [181](#)

T

API de tabla, [283](#)
mesas, Azure Storage, [31](#)
biblioteca de plantillas, [74 - 75](#)
inteligencia de amenazas, configuración en Azure Firewall, [203](#)
topología
redes, [14 - 15](#)
Emparejamiento de redes virtuales, [84 - 85](#)
la gestión del tráfico. Ver [Administrador de tráfico de Azure](#)
resolución de problemas, RBAC (control de acceso basado en roles), [243 - 245](#)
IP confiables, [98 - 99](#)
verificación en dos pasos, [93 , 97](#)
opciones de derivación, [97 - 98](#)
configurar métodos de verificación, [100 - 101](#)

U

recursos no utilizados, monitoreo de, [9- 10](#)
actualizaciones, programación, [151 - 152](#)
La ruta basadas URL de enrutamiento, [192 - 195](#)
cuentas de usuario
alertas de fraude, [96 - 97](#)
invitado, [101 - 105](#)
identidades híbridas, [111 - 112](#)
Protección de la identidad, [106 - 108](#)
MFA (autenticación multifactor), [93 - 95](#)
opciones de derivación, [97 - 98](#)
reescritura contraseña, [119 - 122](#)
informes de riesgo, [106 - 108](#)
SSO sin costuras, [123 - 125](#)
identidad administrada asignada por el usuario, [181](#)

V

VDI (infraestructura de escritorio virtual)

Sin conexión de datos de migración Box, [146](#) - [149](#)
migrar a Azure, [146](#)
vértices, creación de base de datos de gráficos, [284](#) - [285](#)
visualización, alertas, [29](#)
visualizaciones
Perspectivas de la aplicación, [20](#)
datos de diagnóstico, [12](#) - [13](#)
VM. Consulte también [máquinas virtuales de Azure](#)
agregar un grupo de seguridad de red, [211](#) - [212](#)
alertas
creando, [28](#) - [29](#)
visualización, [29](#)
Hosts dedicados de Azure, [63](#)
a bordo, [24](#)
alta disponibilidad, [56](#)
conjuntos de disponibilidad, [56](#) - [59](#)
zonas de disponibilidad, [59](#) - [60](#)
supervisión de la capacidad de rendimiento, [10](#) - [11](#)
preparándose para la migración, [155](#) - [160](#)
y endpoints privados, [39](#)
la replicación de datos de Azure, [160](#) - [162](#)
juegos de escalas, [60](#) - [61](#)
ajuste de escala automático, [62](#)
tallaje, [49](#) - [50](#)
almacenamiento, configuración, [50](#) - [53](#)
carga de trabajo, registro, [24](#) - [26](#)
VMSS (conjunto de escalado de máquina virtual), [60](#) - [61](#)
Redes virtuales
Integración de App Service, [253](#) - [254](#)
Azure configuración del cortafuegos, [199](#) - [200](#)
mirando, [83](#) - [85](#)
-a conexiones VNet, [80](#) - [83](#)
VPN, [218](#)
la creación de una pasarela de red virtual, [219](#) - [220](#)
ExpressRoute, [225](#)
configurar una puerta de enlace de red virtual, [227](#)
ajustes de emparejamiento, [226](#)
administrar la conectividad local con Azure, [224](#)

NSG (grupos de seguridad de red), [224](#) , [225](#)

Sitio a Sitio

configurar, [221](#) - [222](#)

verificar la conectividad local, [222](#) - [223](#)

W X Y Z

WAF políticas (aplicación firewall web), [206](#) - [208](#)

evaluación y migración de aplicaciones web, [138](#) - [145](#)

aplicaciones web, [250](#)

para recipientes, [251](#) - [252](#)

creando, [250](#) - [251](#)

VM de Windows

ADE (cifrado de disco de Azure), [53](#) - [56](#)

tallaje, [49](#) - [50](#)

almacenamiento, configuración, [50](#) - [53](#)

plantillas de libros de trabajo

Métricas clave, [12](#)

Análisis de desempeño, [12](#)

gestión de carga de trabajo

herramientas de evaluación, [132](#) - [133](#)

Herramienta de evaluación del servidor de Azure Migrate, [133](#)

evaluación del entorno de servidor, [133](#) - [138](#)

Administración de actualizaciones de Azure

configurar, [150](#) - [151](#)

programación de actualizaciones, [152](#)

la migración de la infraestructura VDI para Azure, [146](#) - [149](#)

Migración de base de datos SQL, [145](#) - [146](#)

evaluación y migración de aplicaciones web, [138](#) - [145](#)

Fragmentos de código

Muchos títulos incluyen código de programación o ejemplos de configuración. Para optimizar la presentación de estos elementos, vea el libro electrónico en modo horizontal de una sola columna y ajuste el tamaño de fuente al valor más pequeño. Además de presentar el código y las configuraciones en el formato de texto ajustable, hemos incluido imágenes del código que imitan la presentación que se encuentra en el libro impreso; por lo tanto, cuando el formato reajustable pueda comprometer la presentación del listado de código, verá un enlace "Haga clic aquí para ver la imagen del código". Haga clic en el enlace para ver la imagen del código de fidelidad de impresión. Para volver a la página anterior vista, haga clic en el botón Atrás en su dispositivo o aplicación.

```
Set-AzDiagnosticSetting -Name sqldb112-diagsettings '  
-ResourceId $dbResource.ResourceId '  
-Category QueryStoreRuntimeStatistics, QueryStoreWaitStatistics, Errors,  
DatabaseWaitStatistics, Deadlocks -Enabled $true '  
-StorageAccountId $storageResource.ResourceId '  
-WorkspaceId $workspaceResource.ResourceId  
  
az aks create --resource-group $resourceGroupName --name myAKSCluster --node-count 1  
--enable-addons monitoring --generate-ssh-keys  
  
az aks enable-addons --addons monitoring --name myAKSCluster --resource-group  
$resourceGroupName  
  
az storage account create --name az303defaultsa --resource-group $resourceGroupName  
az storage account create --name az303blockblob --resource-group $resourceGroupName  
--kind BlockBlobStorage  
  
az storage account create --name az303blobaccesstier --resource-group $resourceGroupName  
-kind StorageV2 --access-tier hot  
  
az storage account create --name az303blobaccesstier --resource-group $resourceGroupName  
--kind StorageV2 --access-tier hot  
  
az storage account update --name az303blobaccesstier --resource-group $resourceGroupName  
--kind StorageV2 --access-tier cool
```

```

$resourceGroupName = "12storage"
.setLocation="northeurope"
$storageAccountName = "az303fsdemosa"
New-AzResourceGroup -Name $resourceGroupName -Location $location ' 
    -Tag @{department="development";env="dev"}
$sacc = New-AzStorageAccount ' 
    -ResourceGroupName $resourceGroupName ' 
        -Name $storageAccountName ' 
            -Location $location ' 
                -Kind StorageV2 ' 
                    -SkuName Standard_LRS ' 
                        -EnableLargeFileShare

$shareName = "az303share"
New-AzRmStorageShare ' 
    -StorageAccount $sacc ' 
        -Name $shareName ' 
            -QuotaGiB 1024

$dirName = "topLevelDir"
New-AzStorageDirectory ' 
    -Context $sacc.Context ' 
        -ShareName $shareName ' 
            -Path $dirName

-Directory: https://az303fsdemosa.file.core.windows.net/az303share

```

Type	Length	Name
Directory	0	topLevelDir

```

"AZ-303 Azure Files share example" | out-file -FilePath "file.txt" -Force
Set-AzStorageFileContent ' 
    -Context $sacc.Context ' 
        -ShareName $shareName ' 
            -Source "file.txt" ' 
                -Path "$($dirName)\file.txt"

$containerName = "images"
New-AzStorageContainer ' 
    -Name $containerName ' 
        -Context $sacc.Context ' 
            -Permission blob

```

```
Set-AzStorageBlobContent -File "D:\az303files\uploadTest.jpg"
-Container $containerName '
-Blob "uploadTest.jpg" '
-Context $sacc.Context

$sacc | Enable-AzStorageDeleteRetentionPolicy -RetentionDays 7

$key1=(Get-AzStorageAccountKey '
-name $storageAccountName '
-ResourceGroupName $resourceGroupName '
).value[0]

$key1

$ctx = New-AzStorageContext '
-StorageAccountName $storageAccountName '
-StorageAccountKey $key1

New-AzStorageAccountKey '
-ResourceGroupName $resourceGroupName '
-Name $storageAccountName '
-KeyName key1

Set-AzStorageBlobContent -File " D:\az303files\uploadTest.jpg" '
-Container $containerName '
-Blob "uploadTest.png" '
-Context $ctx

Set-AzStorageBlobContent : This request is not authorized to perform this
operation. HTTP Status Code: 403 - HTTP Error Message: This request is not
authorized to perform this operation.

$resourceGroupName = "12storage"
$storageAccountName = "az303fsdemosa"
$SASToken = "?sv=2019-10-10&ss=b&srt=co&sp=rx&se=2020-06-19T08:00:00Z&st=2020-06-12T08:0
0:00Z&spr=https&sig=ceDhRXv2uu9370cRaCrtVdrHd1WDy8gLqNboZkqxwxM%3D"
$containerName = "images"

$ctx = New-AzStorageContext '
-StorageAccountName $storageAccountName '
-SasToken $SASToken
```

```

Get-AzStorageBlobContent '
    -Container $containerName '
    -Blob "uploadTest.png" '
    -Destination "d:\az303files\" '
    -Context $ctx
        Container Uri: https://az303fsdemosa.blob.core.windows.net/images

Name          BlobType  Length      ContentType
LastModified   AccessTier SnapshotTime IsDeleted
uploadTest.png BlockBlob  592021     image/png
2020-06-11 23:44:18Z Unknown      False

Set-AzStorageBlobContent -File "D:\az303files\uploadTestSAS.png" '
    -Container $containerName '
    -Blob "uploadTestSAS.png" '
    -Context $ctx
Set-AzStorageBlobContent : This request is not authorized to perform this operation
using this permission. HTTP Status Code: 403 - HTTP Error Message: This request is not
authorized to perform this operation using this permission.
ErrorCode: AuthorizationPermissionMismatch
ErrorMessage: This request is not authorized to perform this operation using this
permission.

$resourceGroupName = "12storage"
$storageAccountName = "az303fsdemosa"
$containerName = "images"

$ctx = New-AzStorageContext '
    -StorageAccountName $storageAccountName '
    -UseConnectedAccount

Get-AzStorageBlobContent '
    -Container $containerName '
    -Blob "storage-az303demo.txt" '
    -Destination "d:\az303files\" '
    -Context $ctx

```

```
using namespace System.Net
# Input bindings are passed in via param block.
param($Request, $TriggerMetadata)
# Write to the Azure Functions log stream.
Write-Host "PowerShell HTTP trigger function processed a request."
$resourceGroupName = "12storage"
$storageAccountName = "az303fsdemosa"
$containerName = "images"
$ctx = New-AzStorageContext ' -StorageAccountName $storageAccountName '
-UseConnectedAccount
$blob = Get-AzStorageBlobContent ' -Container $containerName '
-Blob "storage-az303demo.txt" '
-Context $ctx '
-Force

$body = $blob.ICloudBlob.DownloadText()
# Associate values to output bindings by calling 'Push-OutputBinding'.
Push-OutputBinding -Name Response -Value ([HttpResponseContext]@{
    StatusCode = [HttpStatusCode]::OK
    Body = $body
})
resourceGroupName="12storage"
storageAccountName="az303ragrs"
az storage account create \
--name $storageAccountName \
--resource-group $resourceGroupName \
--kind StorageV2 \
--sku Standard_RAGRS
"secondaryEndpoints": {
    "blob": "https://az303ragrs-secondary.blob.core.windows.net/",
    "dfs": "https://az303ragrs-secondary.dfs.core.windows.net/",
}
az vm list-sizes --location uksouth --output table
Get-AzVMSize -Location uksouth | Where NumberOfCores -EQ '8'
az vm create --name vmLinSizeExample \
--resource-group $resourceGroupName \
--image UbuntuLTS \
--size Standard_B1s \
--generate-ssh-key
```

```
az vm list-vm-resize-options --resource-group $resourceGroupName --name vmLinSizeExample
--output table

az vm resize --resource-group $resourceGroupName --name vmLinSizeExample --size
Standard_DS2_v2

az vm deallocate --resource-group $resourceGroupName --name vmLinSizeExample
az vm convert --resource-group $resourceGroupName --name vmLinSizeExample
az vm start --resource-group $resourceGroupName --name vmLinSizeExample

az vm create \
    --resource-group $resourceGroupName \
    --name vmEphemOSDisk \
    --image UbuntuLTS \
    --ephemeral-os-disk true \
    --os-disk-caching ReadOnly \
    --admin-username azureadmin \
    --generate-ssh-keys

$diskConfig = New-AzDiskConfig -SkuName Premium_LRS -Location uksouth
-CreateOption Empty -DiskSizeGB 128
$disk1 = New-AzDisk -DiskName dataDisk1 -Disk $diskConfig -ResourceGroupName
resourceGroupName
$vm = Get-AzVM -Name vmName -ResourceGroupName resourceGroupName
$vm = Add-AzVMDisk -VM $vm -Name dataDisk1 -CreateOption Attach
-ManagedDiskId $disk1.Id -Lun 1
Update-AzVM -VM $vm -ResourceGroupName resourceGroupName

resourceGroupName="az303chap1_3-rg"
location="uksouth"
vmName="ade-vm"
vaultName="ade-vk"
keyName="ade-kek"

az vm encryption show --resource-group $resourceGroupName --name $vmName
Azure Disk Encryption is not enabled

az vm encryption enable --resource-group $resourceGroupName --name $vmName
--disk-encryption-keyvault $vaultName

az vm encryption enable --resource-group $resourceGroupName --name $vmName
--disk-encryption-keyvault $vaultName --volume-type ALL

az vm encryption show --resource-group $resourceGroupName --name $vmName

az keyvault secret list --vault-name $vaultName

az keyvault key import --name $keyName --vault-name $vaultName --pem-file ./keys/ade-
kek.pem --pem-password $password
az vm encryption enable --resource-group $resourceGroupName --name $vmName --disk-
encryption-keyvault $vaultName --volume-type ALL --key-encryption-key $keyName
```

```
az vm encryption show --resource-group $resourceGroupName --name $vmName
az vm create \
    --resource-group $resourceGroup \
    --name $vmNamei \
    --availability-set az303chap1-ag \
    --size Standard_DS1_v2 \
    --vnet-name $vnetName \
    --subnet $subnetName \
    --image UbuntuLTS \
    --admin-username azureuser \
    --generate-ssh-keys

az vm list-skus -l uksouth --zone --output tsv

New-AzVMConfig -VMName $vmName -VMSize Standard_DS1_v2 -Zone 2
az vmss create \
    --resource-group $resourceGroupName \
    --name myScaleSet \
    --image UbuntuLTS \
    --upgrade-policy-mode automatic \
    --admin-username $adminUser \
    --generate-ssh-keys

az network lb rule create \
    --resource-group $resourceGroupName \
    --name myLoadBalancerRuleWeb \
    --lb-name myScaleSetLB \
    --backend-pool-name myScaleSetLBEPool \
    --backend-port 80 \
    --frontend-ip-name loadBalancerFrontEnd \
    --frontend-port 80 \
    --protocol tcp

az vmss scale --name myScaleSet --new-capacity 3 --resource-group $resourceGroupName
```

```
"outputs": {
    "endPoints": {
        "type": "Object",
        "value": {
            "blob": "https://az303armfrs1x5kksdvcu.blob.core.windows.net/",
            "dfs": "https://az303armfrs1x5kksdvcu.dfs.core.windows.net/",
            "file": "https://az303armfrs1x5kksdvcu.file.core.windows.net/",
            "queue": "https://az303armfrs1x5kksdvcu.queue.core.windows.net/",
            "table": "https://az303armfrs1x5kksdvcu.table.core.windows.net/",
            "web": "https://az303armfrs1x5kksdvcu.z33.web.core.windows.net/"
        }
    }
},
#!/bin/bash

resourceGroupName="az303chap1_4-rg"
deploymentName="simpleWinVM"
templateUri="https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/101-vm-simple-windows/azuredeploy.json"
adminUsername="adminuser"
adminPassword="secretP@ssw0rd"
dnsLabelPrefix="az303depvm"

az deployment group create --resource-group $resourceGroupName \
--name $deploymentName \
--template-uri $templateUri \
--parameters "adminUsername=$adminUsername" \
"adminPassword=$adminPassword" \
"dnsLabelPrefix=$dnsLabelPrefix"
```

```

$conn = "AzureRunAsConnection"
try
{
    # Get the connection "AzureRunAsConnection "
    $sPConnection=Get-AutomationConnection -Name $conn

    Connect-AzAccount '
        -ServicePrincipal '
        -Tenant $sPConnection.TenantId '
        -ApplicationId $sPConnection.ApplicationId '
        -CertificateThumbprint $sPConnection.CertificateThumbprint
}
catch {
    if (!$sPConnection)
    {
        $ErrorMsg = "$conn not found."
        throw $ErrorMsg
    } else{
        Write-Error -Message $_.Exception
        throw $_.Exception
    }
}

# Set the tag for AZ303 Chapter 1 resource removal
$rgTag = "az303chap1"
$toCleanResources = (Get-AzResourceGroup -Tag @{ Usage=$rgTag })

Foreach ($resourceGroup in $toCleanResources) {
    Write-Host "==> $($resourceGroup.ResourceGroupName) is for az303chap1. Deleting
it..."
    Remove-AzResourceGroup -Name $resourceGroup.ResourceGroupName -Force
}

```

