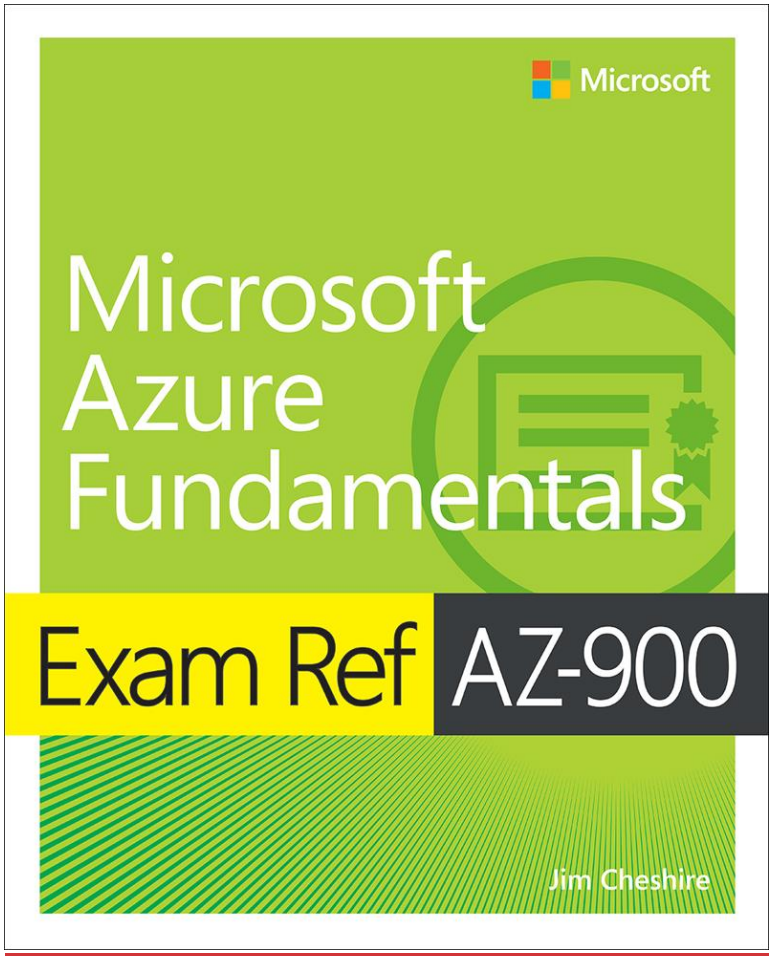

Microsoft
Microsoft Azure Fundamentals
Exam Ref AZ-900
Jim Cheshire

Jim Cheshire

Examen Ref AZ-900 Fundamentos de Microsoft Azure

Publicado con la autorización de Microsoft Corporation por: Pearson Education, Inc.

ISBN-978-0-1357-3218-2

ISBN-0-1357-3218-2

Número de control de la Biblioteca del Congreso: 2019937231

1 19

Marcas registradas

Microsoft y las marcas registradas en *https://www.microsoft.com* en la página web "Marcas registradas" son marcas registradas del grupo de compañías Microsoft. Todas las demás marcas son propiedad de sus respectivos dueños.

Advertencia y descargo de responsabilidad

Editor en jefe
Brett Bartow

Editora ejecutiva
Loretta Yates

Editor Patrocinador
Charvi Arora

Editora de Desarrollo
Troy Mott

Editora Administrativa
Sandra Schroeder

Editora Senior del Proyecto
Tracey Croom

Producción editorial
Backstop Media

Editor de copias
Liv Bainbridge

Sistemas MAP de **indexador**

Corrector de pruebas
Jana Gardner

Editor técnico
Timothy Warner

Diseñador de portada
Twist Creative, Seattle

Contenido de un vistazo

Contenido

Introducción

Tanto las empresas como los individuos están adoptando tecnologías en la nube a un ritmo vertiginoso, y Microsoft Azure a menudo es la opción para aplicaciones y servicios basados en la nube. El propósito del examen AZ-900 es evaluar su comprensión de los fundamentos de Azure. El examen incluye conceptos de alto nivel que se aplican en todo Azure a conceptos importantes que son específicos de un servicio particular de Azure. Al igual que el examen, este libro está orientado a brindarle una amplia comprensión de Azure en sí mismo y de muchos de los servicios y componentes comunes en Azure.

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

Este libro cubre todos los temas 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 regularmente nuevas preguntas al examen, lo que hace imposible cubrir preguntas específicas. Debe considerar 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, utilice el "¿Necesita más revisión?" enlaces que encontrará en el texto para encontrar más información y tomarse el tiempo para investigar y estudiar el tema. Hay gran información disponible en MSDN, TechNet y en blogs y foros.

ORGANIZACIÓN DE ESTE LIBRO.

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

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 diseñay desarrolle, o implemente y soporte, soluciones con productos y tecnologías de Microsoft tanto en las instalaciones como en la nube. La certificación brinda 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* .

¡Vuelve a menudo para ver qué hay de nuevo!

ACCESO RÁPIDO A REFERENCIAS EN LÍNEA.

En todo este libro hay direcciones de páginas web que el autor le ha recomendado que visite para obtener más información. Algunas de estas direcciones (también conocidas como URL) pueden ser difíciles de escribir en un navegador web, por lo que las hemos compilado en una sola lista que los lectores de la edición impresa pueden consultar mientras leen.

Descargue la lista en https://MicrosoftPressStore.com/ExamRefAZ900/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 SOPORTE DE 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 una lista de erratas enviadas y sus correcciones relacionadas, en:

https://MicrosoftPressStore.com/ExamRefAZ900/errata

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

Para obtener asistencia e información adicional sobre libros, visite *https://MicrosoftPressStore.com/Support* .

Tenga en cuenta que el soporte del producto para el 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 *https://support.microsoft.com* .

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 conocimiento del producto. Aunque no hay sustituto para la experiencia en el trabajo, la preparación a través del estudio y la práctica puede ayudarlo a prepararse para el examen. Le recomendamos que aumente su plan de preparación para el examen utilizando una combinación de materiales de estudio y cursos disponibles. Por ejemplo, puede usar la referencia del examen y otra guía de estudio para su preparación "en casa", y tomar un curso de Currículo oficial de Microsoft para la experiencia en el aula. Elige la combinación que creas que funciona mejor para ti.

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.

Capítulo 1. Comprender los conceptos de la nube

La computación en la nube ha sido parte de la tecnología de la información (TI) durante más de 20 años. Durante ese tiempo, se ha convertido en una colección compleja de servicios en la nube y modelos en la nube. Antes de comenzar el proceso de pasar a la nube, es importante que comprenda los conceptos y servicios clave relacionados con la nube.

Importante ¿Has leído la página xix?

Contiene información valiosa sobre las habilidades que necesita para aprobar el examen.

Hay muchas razones para pasar a la nube, pero uno de los principales beneficios es eliminar parte de la carga de TI de su propia empresa. La nube le permite aprovechar la infraestructura y las inversiones de un proveedor de la nube, y le facilita mantener un acceso constante a sus aplicaciones y datos. También obtendrá el beneficio de soluciones llave en mano para realizar copias de seguridad de datos y garantizar que sus aplicaciones puedan sobrevivir a desastres y otros problemas de disponibilidad. Alojar sus datos y aplicaciones en la nube suele ser más rentable que invertir en infraestructura y recursos de TI locales.

Una vez que decida aprovechar la nube, debe comprender las diferentes ofertas disponibles en la nube. Algunos servicios en la nube brindan una experiencia casi sin intervención, mientras que otros requieren que usted mismo administre algunos de los sistemas. Encontrar el equilibrio adecuado para sus necesidades requiere que comprenda completamente cada tipo de servicio.

Este capítulo cubre los beneficios de usar la nube, los diferentes servicios en la nube disponibles y los modelos en la nube que permiten una variedad de configuraciones en la nube.

Habilidades cubiertas en este capítulo:

- Describir los beneficios y las consideraciones del uso de servicios en la nube.
- Describa las diferencias entre Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS) y Software como servicio (SaaS)
- Describir las diferencias entre los modelos de nube pública, privada e híbrida.

HABILIDAD 1.1: DESCRIBA LOS BENEFICIOS Y CONSIDERACIONES DEL USO DE SERVICIOS EN LA NUBE

Las empresas de hoy dependen en gran medida de las soluciones de software y el acceso a los datos. De hecho, en muchos casos, los activos más valiosos de una empresa están directamente vinculados a datos y aplicaciones. Debido a eso, la inversión en TI ha crecido enormemente en las últimas décadas. Confianza enLos departamentos de TI locales trabajaron bien en los primeros días de TI, pero el acceso a los datos y las aplicaciones se ha convertido en una parte tan crítica de las operaciones diarias que los sistemas de TI localizados se han vuelto ineficientes en muchos niveles.

Al tomar decisiones sobre qué mover a la nube y el beneficio asociado con las soluciones en la nube, evalúe estas decisiones frente a los beneficios que la computación en la nube puede proporcionar.

Esta sección cubre:

- Alta disponibilidad
- Escalabilidad y elasticidad.
- Agilidad
- Tolerancia a fallas y recuperación ante desastres
- Principios de economías de escala.
- Diferencias entre gastos de capital y gastos de operaciones
- Modelo basado en el consumo

Alta disponibilidad

La disponibilidad de datos y aplicaciones es un requisito central para cualquier aplicación, ya sea local o en la nube. Si sus datos o aplicaciones no están disponibles para usted, nada más importa. Hay muchas razones por las que puede perder disponibilidad, pero los problemas más comunes son:

- Un corte de red
- Una falla de la aplicación
- Un sistema, como una máquina virtual, corte de energía
- Un apagón
- Un problema con un sistema confiable como una base de datos externa

En un mundo perfecto, experimenta una disponibilidad del 100%, pero si se produce alguno de los problemas anteriores, ese porcentaje comenzará a disminuir. Por lo tanto, es fundamental que su infraestructura minimice el riesgo de problemas que afecten la disponibilidad de su aplicación.

Los proveedores de la nube ofrecen un *acuerdo de nivel de servicio* (SLA) que garantiza un cierto nivel de disponibilidad como porcentaje. Un SLA generalmente garantizará un tiempo de actividad cercano al 100%, pero solo cubre los sistemas controlados por el proveedor de la nube.

Una aplicación alojada en la nube puede ser una desarrollada por su empresa, pero también puede ser una que le haya proporcionado el proveedor de la nube.

Caída de la red

Todas las aplicaciones requieren algún nivel de conectividad de red. Los usuarios de una aplicación requieren conectividad de red a las computadoras que ejecutan la aplicación. La aplicación requiere redconectividad a los sistemas de fondo necesarios, como los servidores de bases de datos. Las aplicaciones también pueden llamar a otras aplicaciones usando una red. Si alguna de estas conexiones de red falla, puede causar falta de disponibilidad.

Más información **Planificación para cortes de red**

Una falla en la red no tiene que significar que su aplicación o sus datos no estén disponibles. Si planifica con cuidado, a menudo puede evitar un problema de aplicación cuando se produce un problema de red. Cubriremos eso con más detalle cuando discutamos la tolerancia a fallas más adelante en este capítulo.

Los proveedores de la nube invierten mucho dinero en infraestructura de red, y al mudarse a la nube obtiene el beneficio de esa infraestructura y la confiabilidad adicional que conlleva. Si algo falla dentro de esa infraestructura, el proveedor de la nube lo diagnostica y lo soluciona, a menudo antes de que te des cuenta de que hay un problema.

Falla de la aplicación

Una falla en la aplicación a menudo es el resultado de un error de software, pero también puede ser causada por el diseño de la aplicación.

Más información **Diseño de aplicaciones y la nube**

No necesita comprender los conceptos de diseño de aplicaciones para el examen AZ-900, pero si está interesado en aprender más sobre el diseño de aplicaciones y la nube, Microsoft tiene una buena referencia en: *https://docs.microsoft.com/ es-es / azure / architecture / patterns /* .

En algunos escenarios de la nube, usted todavía es responsable de las fallas de la aplicación, pero es probable que su proveedor de la nube le brinde herramientas que puede usar para diagnosticar estas fallas más fácilmente. Por ejemplo, Azure ofrece un servicio llamado Application Insights que se integra con su aplicación para brindarle información detallada sobre el rendimiento y la confiabilidad de su aplicación. Los desarrolladores de aplicaciones a menudo pueden usar esta información para acceder directamente al código donde ocurre un problema, reduciendo drásticamente el tiempo necesario para la resolución de problemas.

Los proveedores de la nube ofrecen otras características que pueden reducir los impactos de disponibilidad causados por fallas en la aplicación. A menudo puede probar nuevas versiones de una aplicación en un entorno protegido sin afectar a los usuarios reales. Cuando esté listo para mover usuarios reales a una nueva versión, a menudo puede mover primero un pequeño número de usuarios para asegurarse de que las cosas funcionen correctamente. Si descubre problemas, la nube a menudo hace que sea fácil volver a la versión anterior.

Corte del sistema

Se produce una interrupción del sistema cuando la computadora que ejecuta un sistema en particular no está disponible. En el mundo local, esa computadora podría ser un servidor que ejecuta una base de datos u otra parte de la aplicación. En la nube, estos sistemas se ejecutan dentro de *máquinas* virtuales o máquinas virtuales.

Las máquinas virtuales son computadoras basadas en software que se ejecutan en una computadora física. Una sola computadora puede ejecutar varias máquinas virtuales, y cada máquina virtual tiene su propio sistema operativo y aplicaciones aislados. Todas las máquinas virtuales que se ejecutan en una computadora comparten la CPU, la memoria y el almacenamiento de la computadora host en la que se ejecutan.

Tenga en cuenta que **VMS no es solo para la nube**

Las máquinas virtuales facilitan la adición de computadoras adicionales cuando es necesario, y le permiten administrar mejor los recursos de la computadora, como la CPU, el espacio en disco y la memoria. Por esa razón, las máquinas virtuales son comunes en la mayoría de las empresas.

Dependiendo del servicio en la nube que elija, puede o no ser responsable del mantenimiento de las máquinas virtuales. Sin embargo, ya sea que usted o su proveedor de la nube los mantengan, el proveedor de la nube supervisará constantemente el estado de las máquinas virtuales y contará con sistemas para recuperar una máquina virtual no saludable.

Corte de energía

La electricidad confiable es crítica para la disponibilidad. Incluso un parpadeo rápido de energía puede hacer que las computadoras se reinicien y que los sistemas se reinicien. Cuando eso sucede, su aplicación no está disponible hasta que se restauran todos los sistemas.

Los proveedores de la nube invierten mucho en respaldo de energía operado por batería y otros sistemas redundantes para evitar problemas de disponibilidad causados por cortes de energía. En una situación donde una gran área geográfica se ve afectada por un corte de energía, los proveedores de la nube le ofrecen la posibilidad de ejecutar su aplicación desde otra región que no se ve afectada.

Problemas con un sistema confiable

Su aplicación puede usar sistemas que no están en la nube o que están alojados por un proveedor de nube diferente. Si esos sistemas fallan, puede perder disponibilidad. Al alojar su aplicación en la nube, obtiene el beneficio de las herramientas de solución de problemas, alertas y diagnóstico que ofrece el proveedor de la nube.

Ahora que comprende algunas de las cosas que pueden afectar la disponibilidad, y algunas ventajas generales de la nube para ayudar a aliviar esos problemas, revisemos algunas de las formas específicas en que la nube puede ayudarlo a garantizar una alta disponibilidad.

Escalabilidad, elasticidad y agilidad.

Los recursos informáticos no son gratuitos. Incluso si está utilizando máquinas virtuales, los recursos subyacentes como el espacio en disco, la CPU y la memoria cuestan dinero. La mejor manera de minimizar el costo es utilizar solo los recursos necesarios para sus propósitos. El desafío es que las necesidades de recursos pueden cambiar con frecuencia y rapidez.

Considere una situación en la que aloja una aplicación en la nube que rastrea los datos de ventas de su empresa. Si su personal de ventas ingresa regularmente información sobre las llamadas de ventas diarias al final del día, es posible que necesite recursos informáticos adicionales para manejar esa carga. Esos mismos recursos no son necesarios durante el día cuando el personal de ventas realiza llamadas de ventas y no utiliza la aplicación.

También puede alojar una aplicación web en la nube que utilizan clientes externos. Dependiendo del patrón de uso, es posible que desee agregar recursos informáticos adicionales en ciertos días o durante ciertos momentos. Es posible que también deba adaptarse rápidamente a más usuarios si su empresa recibe publicidad inesperada de los medios u otros medios.

La escala y la *elasticidad le* permiten lidiar fácilmente con este tipo de escenarios. El escalado es el proceso de agregar recursos adicionales o potencia adicional para su aplicación. Hay dos variaciones de escala: la escala de horizonte (a menudo referido como *el horizontal*) y la escala vertical (a menudo referida como *la ampliación*).

Cuando escala, agrega máquinas virtuales adicionales para su aplicación. Cada máquina virtual que agregue es idéntica a otras máquinas virtuales que prestan servicio a su aplicación. El escalado horizontal proporciona recursos adicionales para manejar cargas adicionales.

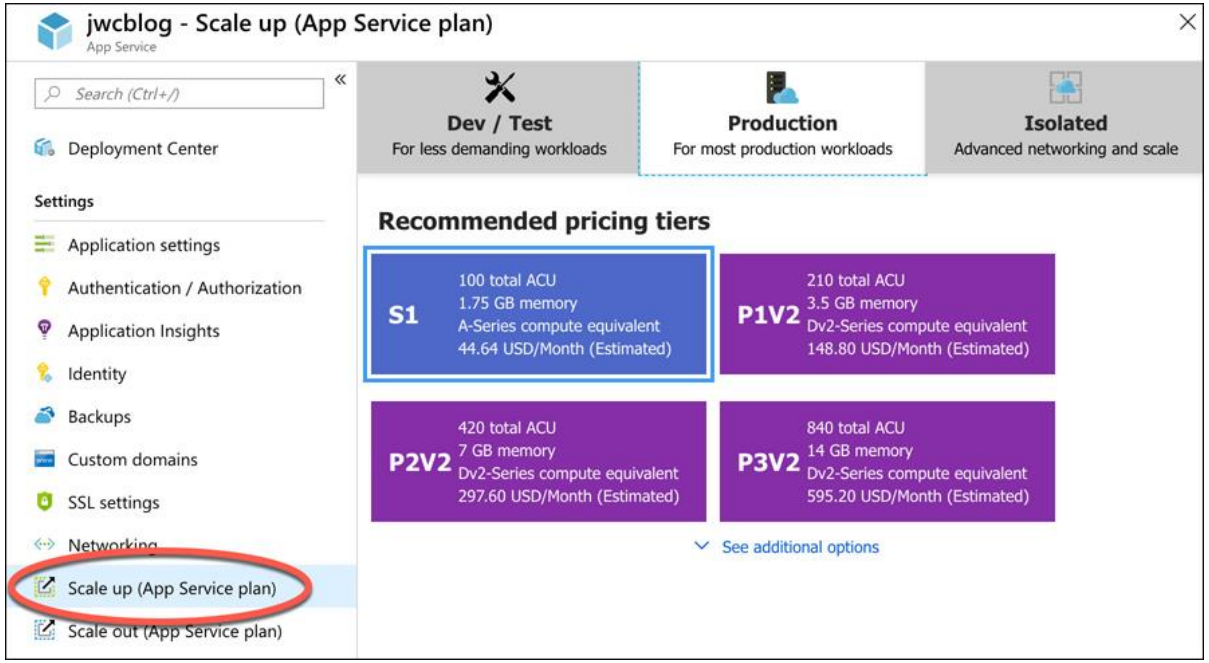
Cuando escala, pasa a una nueva VM con recursos adicionales. Por ejemplo, puede determinar que necesita una CPU más potente y más memoria para su aplicación. En ese caso, la ampliación le permitirá mover su aplicación a una máquina virtual más potente.

***Nota La* ampliación a menudo agrega características**

Cuando escala, a menudo no solo agrega más potencia de CPU y memoria, sino que a menudo obtiene características adicionales debido a la potencia adicional. Por ejemplo, la ampliación podría proporcionarle unidades de disco de estado sólido u otras características que no están disponibles en los niveles inferiores.

La Figura 1-1 muestra un ejemplo de ampliación de una aplicación web alojada en Azure.

Figura 1-1 Ampliación de una aplicación web en Azure



***El* escalamiento del *mundo real* va en ambos sentidos**

Además de ampliar y ampliar, también puede *ampliar* y *reducir* para disminuir el uso de recursos. En una situación del mundo real, querrá aumentar los recursos informáticos cuando sea necesario, reduciéndolos cuando disminuya la demanda.

Los proveedores de la nube facilitan el escalado de su aplicación, y ofrecen la posibilidad de escalar automáticamente según el patrón de uso de su aplicación. Puede escalar automáticamente en función de cosas como el uso de la CPU y el uso de la memoria, y también puede escalar en función de otras métricas que son específicas del tipo de aplicación. El concepto de escala automática se conoce como *elasticidad* .

Consejo de examen

En Azure, puede escalar automáticamente configurando Auto-Scale. Auto-Scale es un servicio de Azure que puede escalar automáticamente las aplicaciones que se ejecutan en muchos servicios de Azure según los patrones de uso, la utilización de recursos, la hora del día y mucho más.

Uno de los principales beneficios de la nube es que le permite escalar rápidamente. Por ejemplo, si está ejecutando una aplicación web en Azure y determina que necesita dos máquinas virtuales más para su aplicación, puede escalar a tres máquinas virtuales en segundos. Azure se encarga de asignar los recursos por usted. Todo lo que tiene que hacer es decirle a Azure cuántas máquinas virtuales desea y está en funcionamiento. Este tipo de velocidad y flexibilidad en la nube a menudo se llama *agilidad en la* nube .

***Más información* Más información sobre las mejores prácticas de escalamiento**

Para obtener más información sobre el escalado en Azure, consulte la documentación en: *https://docs.microsoft.com/azure/architecture/best-practices/auto-scaling* .

Tolerancia a fallas y recuperación ante desastres

En un entorno complejo en la nube, las cosas van a salir mal de vez en cuando. Para mantener un alto nivel de disponibilidad, los proveedores de la nube implementan sistemas que monitorean el estado de los recursos de la nube y toman medidas cuando se determina que un recurso no es saludable, asegurando así que la nube sea *tolerante a fallas* .

Consejo de examen

No confunda la tolerancia a fallas con la escala. El escalado le permite reaccionar a las necesidades adicionales de carga o recursos, pero siempre se supone que todas las máquinas virtuales que está utilizando están en buen estado. La tolerancia a fallas ocurre sin ninguna interacción de su parte, y está diseñada para moverlo automáticamente de un sistema no saludable a un sistema saludable en caso de que las cosas salgan mal.

Además de monitorear el estado de las máquinas virtuales y otros recursos, los proveedores de la nube diseñan su infraestructura de tal manera que garanticen la tolerancia a fallas. Por ejemplo, si tiene una aplicación que se ejecuta en dos máquinas virtuales en Azure, Microsoft se asegura de que esas dos máquinas virtuales estén asignadas dentro de la infraestructura, de modo que es poco probable que se vean afectadas por fallas del sistema.

Más información **Tolerancia a fallas en Azure**

No tiene que comprender los detalles técnicos de cómo Azure implementa la tolerancia a fallas para el examen AZ-900, pero si está interesado en obtener más información, consulte: *https://msdn.microsoft.com/magazine/mt422582. aspx* .

La tolerancia a fallas está diseñada para lidiar con fallas a pequeña escala; moviéndote, por ejemplo, de una VM no saludable a una VM saludable. Sin embargo, hay momentos en que pueden ocurrir fallas mucho mayores. Por ejemplo, los desastres naturales en una región pueden afectar todos los recursos en esa región en particular. Algo así no solo puede afectar la disponibilidad, sino que sin un plan establecido, los desastres también pueden significar la pérdida de datos valiosos.

Recuperación de desastres del *mundo real* y gobiernos

Dependiendo del tipo de datos que almacene, es posible que deba tener un plan de recuperación ante desastres implementado. Los proveedores de la nube generalmente cumplen con los estándares impuestos por leyes como HIPAA, y a menudo proporcionan herramientas de cumplimiento que puede utilizar para garantizar el cumplimiento. Aprenderá más sobre el cumplimiento y Azure en el Capítulo 3 , " Comprender la seguridad, la privacidad, el cumplimiento y la confianza ".

La recuperación ante desastres no solo significa tener copias de seguridad confiables de datos importantes, sino que también significa que la infraestructura de la nube puede replicar los recursos de su aplicación en una región no afectada para que sus datos estén seguros y la disponibilidad de su aplicación no se vea afectada. Los planes de recuperación de desastres se conocen comúnmente como planes de *Continuidad del Negocio y Recuperación de Desastres* (BCDR), y la mayoría de los proveedores de la nube tienen servicios que pueden ayudarlo a desarrollar e implementar un plan que funcione para sus necesidades particulares.

Beneficios económicos de la nube.

Hasta ahora solo hemos hablado sobre el beneficio de disponibilidad de pasar a la nube, pero también hay beneficios económicos. Consideremos tanto el modelo local como el modelo en la nube.

Modelo en las instalaciones

En el modelo local, una empresa compra hardware informático físico para utilizarlo en sus necesidades de TI. Debido a que estas computadoras son activos físicos que están destinados a ser utilizados por más de un año, generalmente se compran como *gastos de capital* .

Hay varios inconvenientes para este modelo. Cuando una empresa compra hardware de computadora, generalmente mantendrá ese hardware en servicio hasta que se obtenga el retorno de esa inversión. En el entorno de rápida evolución de las computadoras, eso puede significar que el hardware está desactualizado mucho antes de que tenga sentido financiero reemplazarlo. Otro inconveniente importante de este método es que esNo es un enfoque ágil. Puede llevar meses solicitar y configurar nuevo hardware, y en la era de la TI moderna, ese enfoque a menudo no tiene sentido.

Más información **Atar dinero**

Las empresas necesitan dinero para las operaciones diarias, y cuando tiene grandes cantidades de dinero inmovilizadas en gastos de capital, puede reducir drásticamente la cantidad de dinero que puede destinar a sus operaciones diarias.

Modelo de nube

Cuando se muda a la nube, ya no confía en su hardware informático local. En cambio, esencialmente alquila hardware del proveedor de la nube. Debido a que no está comprando activos físicos, traslada sus costos de TI de gastos de capital a gastos *operativos* o gastos diarios para su negocio. A diferencia de los gastos de capital, los gastos operativos se rastrean mes a mes, por lo que es mucho más fácil ajustarlos según las necesidades.

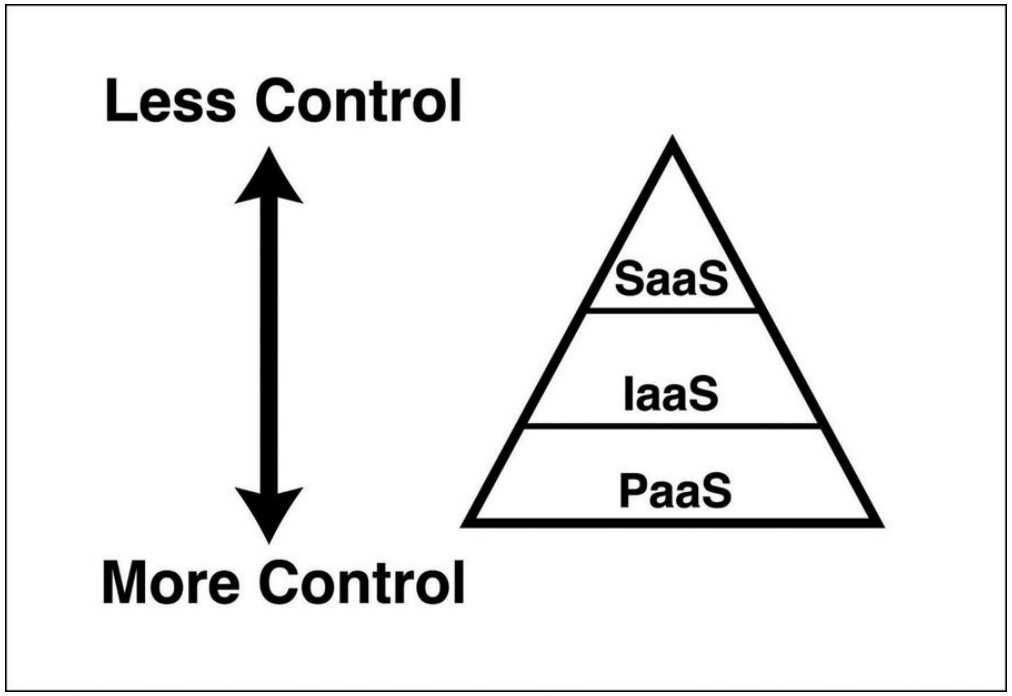
Otro beneficio importante del modelo de nube es la reducción de costos. Cuando utiliza recursos en la nube, está utilizando recursos disponibles de un gran conjunto de recursos propiedad del proveedor de la nube. El proveedor de la nube paga estos recursos por adelantado, pero debido a la gran escala de recursos que compra, el costo para el proveedor de la nube se reduce considerablemente. La reducción en el costo que se realiza al comprar grandes cantidades de un recurso se conoce como el *principio de las economías de escala* , y esos ahorros se transfieren a los consumidores de la nube.

Los proveedores de la nube llevan estos ahorros un paso más allá al ofrecer la capacidad de usar solo los recursos informáticos que necesita en un momento determinado. Esto generalmente se conoce como un *modelo basado en el consumo* , y a menudo se aplica en muchos niveles en la computación en la nube. Como ya hemos discutido, puede escalar su aplicación para usar solo la cantidad de máquinas virtuales que necesita, y puede elegir qué tan poderosas son esas máquinas virtuales. Puede ajustar su número y potencia según sus necesidades. Sin embargo, muchos proveedores de la nube también ofrecen servicios que le permiten pagar solo por el

tiempo que consume los recursos de la computadora. Por ejemplo, puede tener el código de la aplicación alojado en un proveedor de la nube y pagar solo por el tiempo que el código se está ejecutando realmente en una VM. Cuando nadie usa la aplicación, no paga por ningún recurso.

Más información **Computación basada en el consumo**

Para ver un ejemplo de un modelo basado en el consumo, consulte *Computación sin servidor* en el Capítulo 2 , " Comprender los servicios principales de Azure ".



Como puede ver, el modelo de nube ofrece muchos beneficios económicos sobre el modelo local, y esa es solo una de las razones por las cuales las empresas se están moviendo rápidamente a la nube.

HABILIDAD 1.2: DESCRIBA LAS DIFERENCIAS ENTRE INFRAESTRUCTURA COMO SERVICIO (IAAS), PLATAFORMA COMO SERVICIO (PAAS) Y SOFTWARE COMO SERVICIO (SAAS)

Como ha aprendido, uno de los beneficios de pasar a la nube es que descarga parte de la responsabilidad de su infraestructura al proveedor de la nube. Pasar a la nube, sin embargo, no es una cosa de todo o nada. Cuando evalúa su uso de la nube, debe equilibrar su necesidad de controlar los recursos con la conveniencia de permitir que el proveedor de la nube maneje las cosas por usted.

Las ofertas en la nube generalmente se denominan *servicios* , y en esta sección de habilidades, vamos a discutir los tres tipos principales de servicios en la nube: *Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS)* y *Software-as-a-Service (SaaS)* . Cada tipo de servicio tiene ventajas y desventajas, y la forma más fácil de visualizarlos es utilizando la pirámide de la nube como se muestra en la Figura 1-2 . La parte inferior de la pirámide de la nube representa la mayor cantidad de control sobre sus recursos, pero también representa la mayor responsabilidad de su parte. La parte superior de la pirámide representa la menor cantidad de control, pero también la menor cantidad de responsabilidad.
Figura 1-2 La pirámide de nubes

Esta sección cubre:

- Infraestructura como servicio (IaaS)
- Plataforma como servicio (PaaS)
- Software como servicio (SaaS)
- Comparación de tipos de servicio

Infraestructura como servicio (IaaS)

La infraestructura se refiere al hardware que utiliza su aplicación, y IaaS se refiere a la infraestructura virtualizada que ofrece un proveedor de la nube. Cuando crea un recurso IaaS, el proveedor de la nube asigna una VM para su uso. En algunos casos, el proveedor de la nube puede hacer la instalación básica del sistema operativo por usted. En otras situaciones, es posible que deba instalar el sistema operativo usted mismo. En cualquier caso, usted es responsable de instalar otros servicios necesarios y su aplicación.

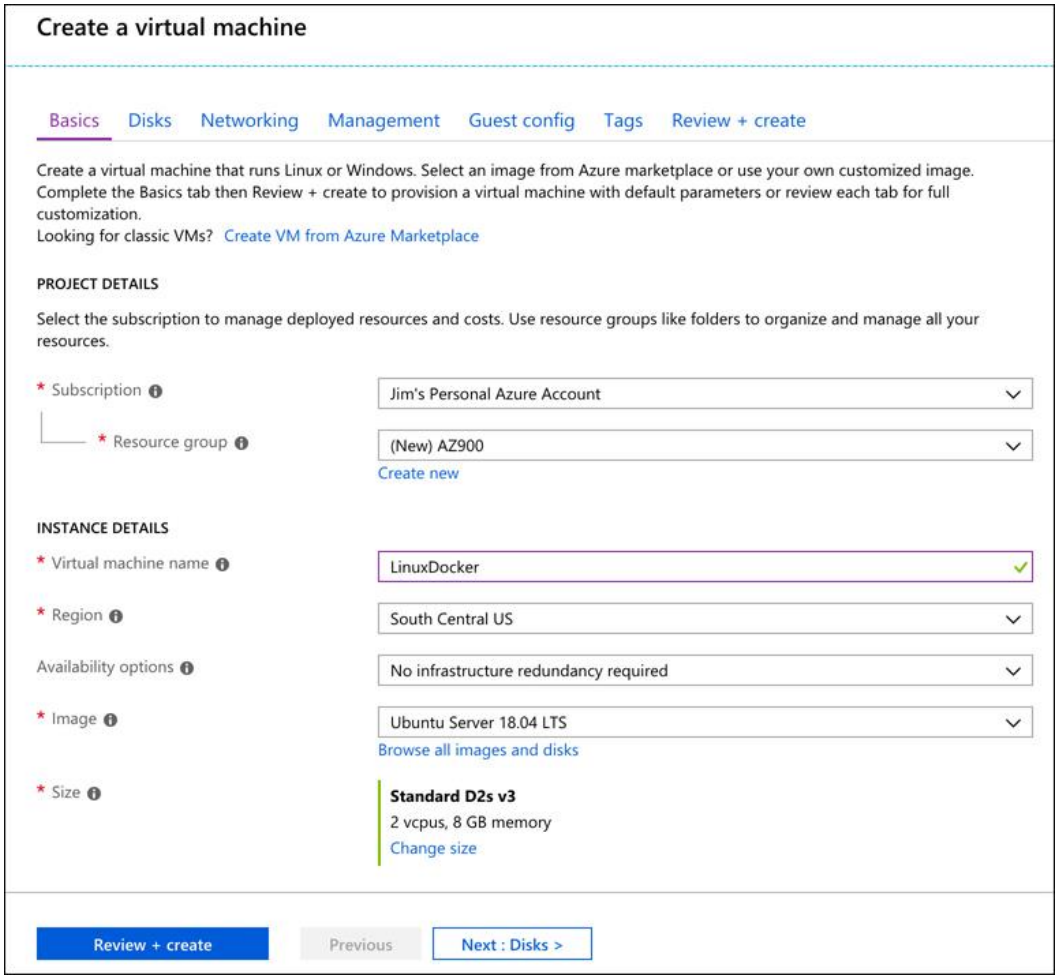
Debido a que controla la instalación del sistema operativo y la instalación de otros servicios, IaaS le brinda un gran control sobre sus recursos en la nube. Sin embargo, también significa que usted es responsable de asegurarse de que su sistema operativo esté parcheado con actualizaciones de seguridad, y si algo sale mal en el sistema operativo, usted es responsable de solucionarlo. El proveedor de la nube solo es responsable de proporcionar la VM. Sin embargo, usted se beneficia de la infraestructura subyacente en el área de tolerancia a fallas y recuperación ante desastres que discutimos anteriormente.

Más información **Acceso remoto a máquinas virtuales IaaS**

Tendrá acceso remoto a sus máquinas virtuales IaaS para que pueda interactuar con ellas como si las estuviera utilizando en su entorno local. Cuando pasa a los servicios de PaaS y SaaS, generalmente pierde esa capacidad porque la infraestructura es administrada por el proveedor de la nube.

En la Figura 1-3 , verá una máquina virtual IaaS en el portal de Azure. El servidor Ubuntu, un sistema operativo Linux, ha sido elegido para la VM. Una vez que la VM esté en funcionamiento, usará Ubuntu Server 18.04. A menos que se instale una actualización, siempre se ejecutará esa versión. Microsoft nunca instalará parches o actualizaciones de versión para mí.

Figura 1-3 Creación de una máquina virtual IaaS en Azure



Una vez que tiene una máquina virtual IaaS ejecutándose en la nube, obtiene acceso a muchos servicios que ofrece el proveedor de la nube. Por ejemplo, Microsoft ofrece Azure Security Center para garantizar la seguridad de sus máquinas virtuales IaaS, Azure Backup

para facilitar la copia de seguridad de los datos, Azure Log Analytics para ayudarlo a resolver cualquier problema que pueda tener, y mucho más.

Más información **Más información sobre IaaS y Azure**

Para obtener más información sobre IaaS y Azure, consulte la documentación en: *https://azure.microsoft.com/overview/what-is-iaas/* .

Los servicios de IaaS le permiten controlar los costos de manera efectiva, ya que solo los paga cuando los está utilizando. Si detiene su máquina virtual IaaS, su facturación se detiene para el recurso. Esto hace que IaaS sea una opción ideal si necesita que los desarrolladores tengan una plataforma para probar una aplicación durante el lanzamiento. Los desarrolladores pueden iniciar una VM de IaaS, probar la aplicación como un equipo y luego detener la VM de IaaS cuando se complete la prueba.

Otro uso popular de IaaS es cuando necesita una o más máquinas virtuales potentes durante un período temporal. Por ejemplo, es posible que deba analizar una gran cantidad de datos para un proyecto. Al utilizar máquinas virtuales IaaS para su proyecto, puede mantener los costos al mínimo, crear recursos rápidamente a medida que los necesite y obtener toda la potencia de procesamiento que necesita.

Los servicios de IaaS se benefician de la escala y la elasticidad que discutimos anteriormente. Si necesita más máquinas virtuales, puede escalar para acomodar eso y luego escalar cuando esos recursos ya no sean necesarios. Si necesita más potencia de CPU, más memoria o más espacio en disco, puede escalar rápidamente para obtener esos beneficios y luego reducir cuando ya no los necesite.

En pocas palabras, los servicios de IaaS son una excelente opción si desea permitir que otra persona administre la infraestructura de hardware (que puede incluir tanto las computadoras como la red) relacionada con su aplicación, pero desea mantener el control de lo que está instalado en el sistema operativo . En un entorno IaaS, el proveedor de la nube no va a instalar algo en el sistema operativo para usted, por lo que siempre conoce el estado actual de lo que está instalado en sus máquinas virtuales. Si esto es importante para sus necesidades particulares, IaaS puede ser la opción correcta para usted. IaaS también es una gran opción si ocasionalmente necesita máquinas virtuales de alta gama para necesidades específicas.

IaaS también es una excelente opción si desea su aplicación y configuración en la nube, pero desea la opción de no pagarla cuando no la esté utilizando. Al detener su VM, puede evitar los costos asociados con ella, y cuando necesite usar su aplicación nuevamente, simplemente puede iniciar su VM y retomarla exactamente donde la dejó.

Plataforma como servicio (PaaS)

En un entorno PaaS, un proveedor de la nube aún proporciona la infraestructura para usted, pero también proporciona el sistema operativo, el software instalado en el sistema operativo para ayudarlo a conectarse a bases de datos y sistemas de red (a menudo denominados *middleware*) y muchas características que le permite construir y administrar aplicaciones complejas en la nube.

PaaS se encuentra justo en el medio de la pirámide de nubes. Los servicios de PaaS le ofrecen la flexibilidad de controlar la aplicación, pero descargan la administración y el control de los sistemas subyacentes al proveedor de la nube. Si está implementando su propia aplicación en la nube y desea minimizar su inversión en administración, un servicio PaaS suele ser la mejor opción.

Suponga que necesita ejecutar una aplicación web que utiliza el marco PHP para conectarse a un sistema de base de datos de fondo. Si tuviera que elegir IaaS para su aplicación, necesitaría asegurarse de instalar y configurar PHP en su VM. Luego deberá instalar y configurar el software necesario para conectarse a su base de datos de fondo. En un escenario de PaaS, simplemente despliega su aplicación web en el proveedor de la nube, y todo lo demás se encarga de usted.

En la Figura 1-4 , tenemos una aplicación web en Azure App Service, una de las ofertas de PaaS en Azure. Ha sido creado en una VM mantenida por Microsoft. Observe la opción de elegir Linux o Windows, pero el sistema operativo aún es administrado por Microsoft. También tenemos la opción de habilitar Application Insights, un servicio en Azure que proporciona una visión profunda del rendimiento de una aplicación, lo que facilita la resolución de problemas si se producen.

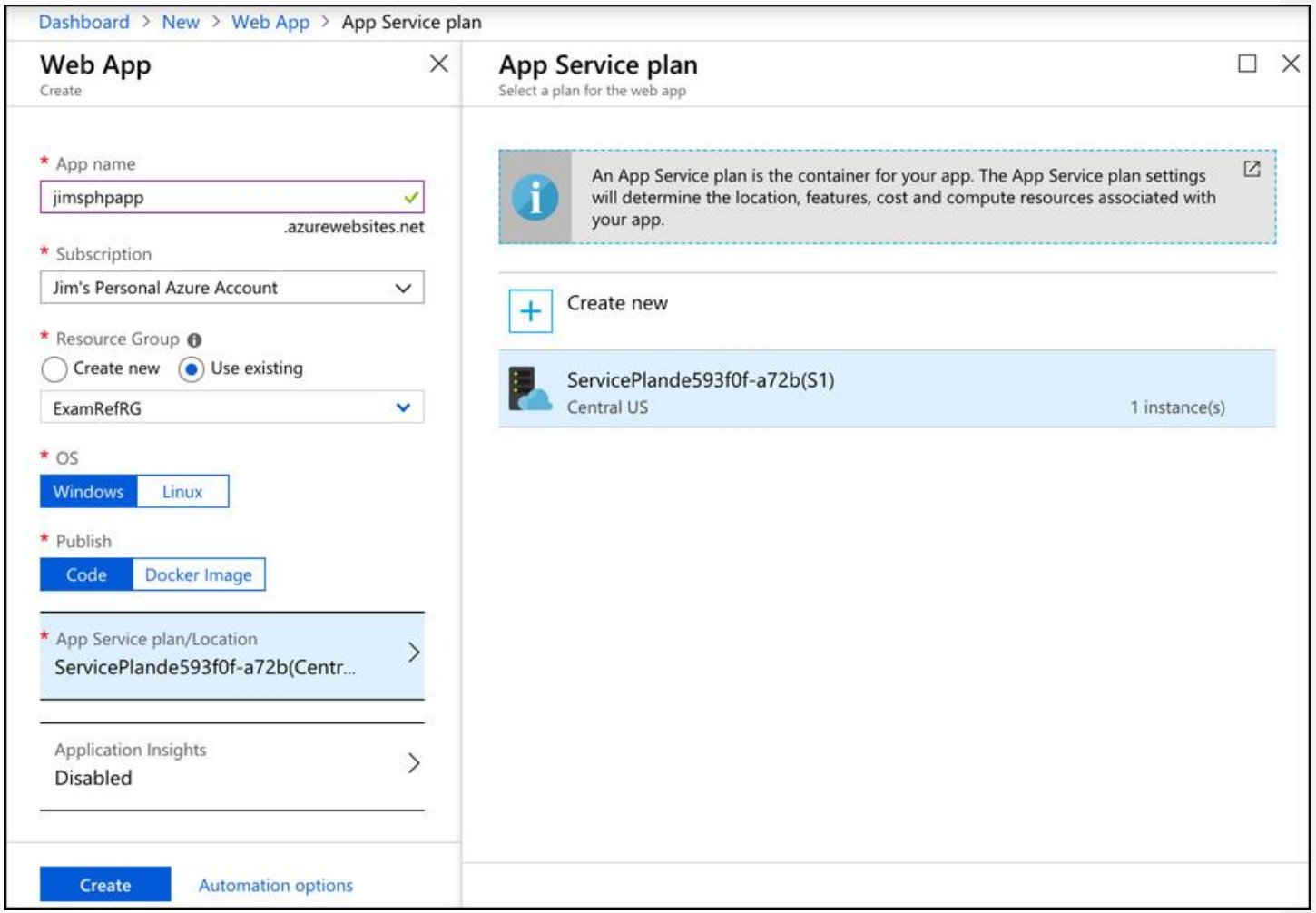


Figura 1-4 Creación de una aplicación web en Azure App Service

Una cosa más interesante en la Figura 1-4 es la opción de publicar su código o una imagen de Docker. Docker es una tecnología que facilita el empaquetado de su aplicación y los componentes que requiere en un *contenedor* que luego puede implementar y ejecutar en

otra computadora en otro entorno, siempre que esa computadora tenga instalado Docker. En Azure App Service, no tengo que preocuparme por la instalación o configuración de Docker. Se incluye automáticamente en todas las máquinas virtuales del Servicio de aplicaciones como parte de la oferta PaaS de Microsoft, y es completamente administrado y mantenido por Microsoft.

En una oferta de PaaS, los proveedores de la nube ofrecen numerosos marcos de aplicaciones como PHP, Node.js, ASP.NET, .NET Core, Java, Python y más. El proveedor de la nube generalmente proporciona múltiples versiones de cada marco para que pueda elegir una versión que sepa que es compatible con su aplicación. El proveedor de la nube también se asegurará de que los componentes comunes necesarios para la conectividad de datos desde su aplicación a otros sistemas estén instalados y configurados. Eso generalmente significa que el código de su aplicación funciona sin que tenga que hacer ningún tipo de configuración compleja. De hecho, este es uno de los principales beneficios de usar un servicio PaaS; a menudo puede mover su aplicación de un entorno local a un entorno en la nube simplemente implementándola en la nube. Este concepto a menudo se conoce como *levantar y cambiar* .

Debido a que el proveedor de la nube controla el sistema operativo y lo que está instalado en la VM, puede proporcionarle capacidades adicionales al agregar sus propias características. Por ejemplo, suponga que desea agregar una función de inicio de sesión a su aplicación web y desea permitir que los usuarios inicien sesión con una cuenta de Microsoft, una cuenta de Facebook o una cuenta de Google. Si desea agregar esta capacidad localmente o en un entorno IaaS, necesita algunos desarrolladores para construirlapara usted, una tarea que no es fácil y que requiere conocimientos especializados. Tendría que tener desarrolladores en su empresa que ya tengan esas habilidades, o tendría que contratarlos. Sin embargo, los proveedores de la nube a menudo ofrecen características como esta en sus servicios de PaaS, y habilitarlos es tan fácil como accionar un interruptor y realizar algunas configuraciones menores específicas para su aplicación.

Un servicio PaaS también se beneficia de todas las otras mejoras que ofrece la nube; obtienes tolerancia a fallas, elasticidad, escalado fácil y rápido, funciones de respaldo y recuperación ante desastres, y más. De hecho, características como la copia de seguridad y la restauración de datos son a menudo más fáciles de usar y ricas en características en un entorno PaaS porque el proveedor de la nube instala software personalizado en las máquinas virtuales PaaS para agregar funcionalidad.

Como puede ver, existen beneficios reales al permitir que el proveedor de la nube controle lo que está instalado en las máquinas virtuales que ejecutan su aplicación, pero también puede haber inconvenientes. Por ejemplo, el proveedor de la nube controla cuándo se aplican parches y actualizaciones tanto al sistema operativo como a otros componentes instalados en las máquinas virtuales. Por lo general, se le avisará con anticipación sobre los cambios importantes para que primero pueda probar su aplicación localmente y evitar cualquier tiempo de inactividad, pero perderá la flexibilidad y el control de decidir cuándo actualizar la VM.

Más información **Más información sobre Paas y Azure**

Para obtener más información sobre las ofertas de PaaS en Azure, consulte: *https://azure.microsoft.com/overview/what-is-paas/* .

Software como servicio (SaaS)

Como ha aprendido, IaaS requiere que controle tanto el sistema operativo como los componentes de middleware junto con su aplicación. Cuando se muda a PaaS, descarga el control del sistema operativo y los componentes de middleware al proveedor de la nube, y usted es responsable solo del código de su aplicación. A medida que avanza hacia la parte superior de la pirámide de la nube y

entra en el reino SaaS, el proveedor de la nube controla todo. En otras palabras, un servicio SaaS es un software proporcionado por un proveedor de la nube que está instalado en una infraestructura completamente controlada por el proveedor de alojamiento.

Los servicios SaaS le ofrecen la flexibilidad de un modelo de pago por uso. Esencialmente, usted alquila su software de un proveedor de servicios. Los usuarios del software generalmente acceden al software desde un navegador web, pero también pueden instalar aplicaciones que solo funcionarán mientras pague por el servicio SaaS. Una gran ventaja del software basado en la web es que funciona desde casi cualquier dispositivo, incluidos los teléfonos inteligentes. Debido a eso, los servicios SaaS permiten la conectividad y la productividad para el personal de campo utilizando dispositivos que ya poseen.

Cuando utiliza un servicio SaaS, no solo se beneficia del uso de software escrito y mantenido por otra persona, sino que también puede beneficiarse al permitir que el proveedor de la nube mantenga y configure la aplicación. Por ejemplo, si su empresa ofrece correo electrónico corporativo, puede optar por usar el servicio SaaS Office 365 de Microsoft. Al usar el servicio Exchange Online en Office 365, puede aprovechar las soluciones de correo electrónico preparadas para la empresa sin tener que contratar personal de TI y crear infraestructura para soportarlo. En cambio, Microsoft mantiene el sistema por usted. No solo se beneficia de la flexibilidad y confiabilidad de la nube, sino que también puede estar tranquilo sabiendo que Microsoft se asegura de que sus servicios de Exchange estén siempre disponibles para sus usuarios.

Los servicios SaaS no son solo para la empresa. De hecho, la mayoría de las personas usan los servicios SaaS todo el tiempo sin siquiera darse cuenta. Si utiliza Hotmail o Gmail u otro servicio de correo electrónico en línea, está utilizando un servicio SaaS. El proveedor de la nube aloja el software de correo electrónico en la nube, y usted inicia sesión y usa ese software usando su navegador web. No tiene que saber nada sobre el software. El proveedor de la nube puede ofrecer nuevas funciones con actualizaciones de software, y esas nuevas funciones están disponibles automáticamente sin ninguna acción de su parte. Si el proveedor de la nube encuentra un problema con el software, puede resolverlo con un parche sin que te des cuenta de que sucedió algo.

Más información **Más información sobre SaaS y Azure**

Para obtener más información sobre los servicios SaaS y Azure, consulte: *https://azure.microsoft.com/overview/what-is-saas/* .

Comparación de tipos de servicio

Ya hemos discutido algunas de las ventajas y desventajas de cada tipo de servicio en la nube, y la pirámide de la nube proporciona una representación visual de cómo los tipos de servicios en la nube difieren en relación con su responsabilidad y lo que puede controlar. Para solidificar estos conceptos, veamos una comparación de cada tipo de servicio.

Como has aprendido, IaaS te brinda la mayor flexibilidad. Puede instalar su propio software y sus propios componentes, y controlar cuándo se actualizan el software y el sistema operativo. Un beneficio adicional es que paga por sus recursos solo cuando se están utilizando, por lo que IaaS tiene la capacidad de reducir sus gastos operativos. Aunque puede ahorrar costos apagando las máquinas virtuales que no está utilizando, los costos más altos asociados con la instalación y el mantenimiento de sus máquinas virtuales pueden compensar ese beneficio.

Los servicios de PaaS le ofrecen la misma flexibilidad que los servicios de IaaS sin la necesidad de administrar la infraestructura. En un servicio PaaS, usted es responsable solo de la aplicación que está instalada en la nube. Puede ser su propia aplicación o una aplicación desarrollada por otra persona (por ejemplo, un sistema WordPress o una solución de comercio electrónico), pero en

cualquier caso, usted es responsable de la aplicación. Los servicios de PaaS son populares para los equipos de desarrolladores que buscan mover aplicaciones locales a la nube de manera fácil y rápida, y generalmente ofrecen muchas opciones de implementación diferentes para que sea lo más fácil posible. Los servicios de PaaS también ofrecen más funciones que los servicios de IaaS, porque el proveedor de la nube instala su propio software y funciones en la plataforma. Sin embargo, cualquier aplicación que se ejecute en un servicio PaaS,

Los servicios de SaaS son bastante diferentes de los servicios de IaaS o PaaS porque el proveedor de la nube los administra y mantiene completamente. No tiene la opción de instalar ninguno de sus propios softwares con un servicio SaaS, por lo que el factor decisivo está completamente relacionado con si el software proporcionado satisface o no sus necesidades. El beneficio de un servicio SaaS es que elimina en gran medida la carga de TI de su empresa y permite que todos en su empresa accedanel software en múltiples dispositivos desde casi cualquier lugar donde esté disponible el acceso a Internet. También se beneficia de la copia de seguridad de datos que el proveedor de la nube incluye en su infraestructura. Sin embargo, si necesita personalizar la aplicación o tiene algún control sobre su configuración, SaaS puede no ser una buena opción para usted.

El mundo real se **ocupa de las complejidades de lo moderno**

Decidir sobre un tipo particular de servicio en la nube puede ser sencillo en algunos casos, pero también puede ser complicado según sus necesidades. Por ejemplo, puede estar en una industria que requiere que parte de su información se almacene solo en las instalaciones. También puede tener algunos sistemas más antiguos que no están listos para moverse a la nube, pero necesita sus aplicaciones en la nube para usar esos sistemas más antiguos. En la siguiente sección de habilidades, aprenderá más sobre cómo lidiar con tales complejidades.

HABILIDAD 1.3: DESCRIBA LAS DIFERENCIAS ENTRE LOS MODELOS DE NUBE PÚBLICA, PRIVADA E HÍBRIDA

En el sentido más simple, la nube representa la infraestructura y las aplicaciones que son accesibles a través de Internet. Los ejemplos cubiertos hasta ahora son la experiencia en la nube más tradicional donde cualquier persona en Internet puede acceder a su aplicación. Si bien es posible que tenga algunos medios para autenticar a las personas que usan su aplicación para que las personas incorrectas no tengan acceso, su aplicación aún se ejecuta en máquinas virtuales que están conectadas a Internet y son accesibles a través de redes públicas.

El modelo de nube tradicional se conoce como la *nube pública* . Además de un modelo de nube pública, las empresas también pueden usar una *nube privada* donde la infraestructura está dedicada a ellas. Finalmente, un modelo de *nube híbrida* representa una mezcla de modelos de nube pública y privada.

Más información **Nubes de la comunidad**

Es posible que vea referencias a un cuarto modelo de nube llamado nube comunitaria. Una nube comunitaria es similar a una nube privada, pero en lugar de que los recursos se dediquen a una sola empresa, se dedican a una comunidad de empresas o individuos que la administran juntos. Por ejemplo, los hospitales pueden usar una nube comunitaria que está explícitamente diseñada para manejar la Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996 (HIPAA) y otras regulaciones de

atención médica. Las instituciones financieras también pueden compartir una nube comunitaria que hace cumplir las regulaciones y políticas relacionadas con los bancos y el comercio financiero.

Las nubes de la comunidad no son parte del examen AZ-900, pero aún es importante comprender qué significa el término en caso de que lo encuentre mientras se prepara para el examen.

Esta sección cubre:

- La nube publica
- La nube privada
- La nube híbrida

La nube publica

El modelo de nube más común es la nube pública. En un modelo de nube pública, utiliza una infraestructura compartida a la que se puede acceder en una red pública. La red, el almacenamiento y las máquinas virtuales que utiliza su aplicación los proporciona un proveedor de la nube y se comparten entre todos los consumidores de la nube pública. Microsoft Azure es un ejemplo de una nube pública.

El modelo de nube pública es beneficioso porque facilita y agiliza el traslado a la nube. Debido a que el proveedor de la nube ya tiene la infraestructura en su lugar y configurada para usted, todo lo que tiene que hacer es decidir el tipo de servicio en la nube que desea y estará listo para funcionar. También se beneficia de la capacidad de escalar de manera rápida y eficiente porque el proveedor de la nube tiene recursos ya aprovisionados y listos para su uso cuando sea necesario.

Como discutimos anteriormente, otra ventaja del modelo de nube pública es que puede controlar los costos de manera más eficiente porque solo paga por los recursos que está utilizando. Si necesita escalar a más máquinas virtuales, el proveedor de la nube las tiene disponibles y esperando por usted. No tiene que mantener un grupo de recursos usted mismo. En su lugar, aprovecha los recursos en los que ha invertido el proveedor de la nube.

Importante **entorno multiempresa**

Debido a que está compartiendo recursos en una nube pública con otras personas que usan esa nube pública, a menudo verá nubes públicas que se conocen como un entorno de múltiples inquilinos.

Si bien la flexibilidad y la conveniencia de la nube pública es atractiva, presenta algunas desventajas. En primer lugar, renuncia al control de la infraestructura cuando utiliza la nube pública. La cantidad de control depende de dónde aterrice en la pirámide de la nube, pero pase lo que pase, el proveedor de la nube controlará una parte de su infraestructura.

También puede haber problemas de seguridad al operar en la nube pública. La red involucrada en la nube pública es Internet pública, y está disponible para cualquier persona con conexión a Internet. Eso significa que deberá contar con medidas de seguridad para evitar el

acceso no autorizado a su aplicación y sus datos. Los proveedores de la nube se dan cuenta de esto, y brindan medidas de seguridad para ayudar a protegerlo, pero es posible que esas medidas no cumplan con sus requisitos de seguridad.

Otra desventaja de la nube pública es que te bloquea en la configuración específica definida por el proveedor de la nube. Por ejemplo, suponga que tiene una aplicación que necesita una gran cantidad de almacenamiento en disco, pero solo necesita un sistema de CPU única para ejecutarla. Para cumplir con los requisitos de espacio en disco, el proveedor de la nube puede requerir que escale a una VM de CPU múltiple de alta potencia, lo que aumenta sus costos innecesariamente.

Más información **Más información sobre nubes públicas**

Para obtener más información sobre nubes públicas y Azure, consulte: *https://azure.microsoft.com/overview/what-is-a-public-cloud/* .

La nube privada

El modelo de nube privada proporciona muchos de los beneficios atractivos de la nube (cosas como escalamiento fácil y elasticidad) en un entorno privado dedicado a una sola empresa. Una nube privada se puede alojar en un entorno local, pero también se puede alojar en un proveedor de alojamiento externo.

Entorno *importante para un* solo inquilino

Debido a que los recursos en una nube privada están dedicados a una sola organización, a menudo verá que la nube privada se conoce como un entorno de un solo inquilino.

Dos de las principales razones por las cuales las empresas eligen una nube privada son: privacidad y preocupaciones regulatorias. A diferencia de la nube pública, las nubes privadas operan en una red privada a la que solo puede acceder una sola organización. Las empresas como los bancos y los proveedores médicos pueden tener regulaciones vigentes que requieren que ciertos datos sean inaccesibles desde Internet, y en esas situaciones, una nube privada podría ser una buena opción. Otro consumidor común de nubes privadas es la industria de cruceros. Los cruceros operan en áreas remotas donde el acceso a Internet no está disponible, pero aún así quieren aprovechar los beneficios de la nube para las operaciones diarias de los sistemas de barcos complejos.

Consejo de examen

A menudo escuchará que una nube privada consiste en una infraestructura que es propiedad de una empresa individual, pero que en realidad no siempre es así. Si una empresa ejecuta una nube privada en las instalaciones, generalmente será propietaria del hardware y la infraestructura utilizados para la nube privada, pero también es posible alojar una nube privada en un centro de datos de terceros. En esa situación, la infraestructura es propiedad del proveedor de alojamiento, pero aún está completamente dedicada a la compañía que paga por la nube privada.

La conclusión es que la diferencia entre una nube pública y una privada es la privacidad de la infraestructura y los datos. Realmente no importa quién posee la infraestructura

Hay algunas desventajas en una nube privada. Si aloja su nube privada en las instalaciones, probablemente gastará tanto en TI como lo haría en un entorno que no sea en la nube. Tendrá que pagar por hardware y sistemas virtualizados para su nube, y necesitará personal de TI que sea capaz de administrar el software y la infraestructura para su nube.

Evitar los costos de TI es una de las razones principales por las que las empresas eligen usar un proveedor de alojamiento externo para nubes privadas, pero esa opción también tiene algunos inconvenientes. Por ejemplo, una vez que descarga la administración de su nube privada a un tercero, pierde el control de consideraciones importantes, como la seguridad de sus datos. A menudo es imposible lograr el plenotransparencia al tratar con proveedores externos, y no siempre puede garantizar que los datos en su red privada en la nube permanecerán protegidos de la manera que usted lo requiera.

Más información **Más información sobre nubes privadas**

Para obtener más información sobre nubes privadas, consulte: *https://azure.microsoft.com/overview/what-is-a-private-cloud/* .

La nube híbrida

Como es de esperar, las nubes híbridas son una mezcla de nubes públicas y privadas. En un entorno de nube híbrida, es posible que tenga una aplicación que se ejecute dentro de la nube pública, pero que acceda a datos almacenados de forma segura en las instalaciones. También puede tener un escenario donde su aplicación y la mayoría de sus recursos se encuentran en una nube privada, pero desea utilizar servicios o infraestructura que se encuentran en una nube pública. De hecho, los diversos escenarios que son adecuados para un modelo híbrido son casi infinitos.

Los modelos de nube híbrida suelen ser la primera incursión de una empresa en la nube. Muchas compañías tienen sistemas locales heredados que son costosos de mover a la nube, sin embargo, es posible que desee aprovechar algunos de los beneficios de la nube. En tal escenario, una empresa podría mover solo una parte de un sistema en particular a la nube, dejando el sistema heredado en las instalaciones hasta un momento posterior.

No todas las empresas que adoptan un modelo de nube híbrida lo hacen debido a los sistemas heredados. En algunas situaciones, una empresa puede querer mantener un control completo sobre parte de su infraestructura o datos. Pueden decidir construir una infraestructura local junto con la construcción de su presencia en la nube pública.

El **híbrido** ***importante*** **no siempre incluye locales**

Recuerde, una nube privada es una nube dedicada a una sola organización. No tiene que estar ubicado en las instalaciones. También se puede alojar en un centro de datos de terceros, por lo que un modelo de nube híbrida podría ser la combinación de un centro de datos de terceros y una nube pública.

Cuando las empresas adoptan un modelo híbrido, a menudo requieren la capacidad de conectar la red privada local con la red de nube pública. Los proveedores de la nube ofrecen muchas tecnologías para hacerlo posible. En Microsoft Azure, las redes virtuales, las conexiones híbridas y el bus de servicio son solo algunos ejemplos de tales tecnologías.

Más información **Más información sobre las ofertas de red de Azure**

Cubriremos algunas de las ofertas de redes de Azure en el Capítulo 2 , Habilidad 2.2.

Si bien puede que no sea inmediatamente obvio, un modelo de nube híbrida presenta varios desafíos. En primer lugar, los equipos de desarrollo de aplicaciones deberán garantizar que los datos compartidos entre la nube pública y privada sean compatibles. Esto puede requerir algunas habilidades de desarrollo especializadas y resolución de problemas complejos. Las complejidades de las redes en un híbridoEl entorno también puede ser bastante desafiante, especialmente porque la infraestructura de red en proveedores externos puede presentar problemas que son difíciles de solucionar. Finalmente, la distribución de los recursos de la aplicación entre una nube pública y una privada puede causar ralentizaciones de la aplicación debido a la distancia geográfica entre los sistemas que ejecutan la aplicación y los datos que la aplicación utiliza. Todas estas situaciones deben evaluarse cuidadosamente al decidir utilizar un modelo de nube híbrida.

Para facilitar la nube híbrida para sus clientes, Microsoft proporciona Azure Stack. Azure Stack se vende como un paquete, que incluye software y hardware validado para ejecutarlo. Azure Stack le permite ejecutar servicios de Azure en las instalaciones, lo que facilita la transferencia de aplicaciones a la nube con una cantidad mínima de trabajo. Debido a que el hardware es parte de Azure Stack y ha sido validado por Microsoft, no tiene la carga de intentar determinar las necesidades de hardware para implementar Azure Stack, pero sí tiene que administrar el hardware local.

EXPERIMENTO MENTAL

Apliquemos lo que has aprendido en este capítulo. Puede encontrar las respuestas en la sección que sigue.

Trabaja para Contoso Medical Group (CMG), y su gerente está frustrado con una de sus aplicaciones de uso común. El departamento de TI de CMG tiene recursos limitados y tienen dificultades para garantizar que la aplicación esté siempre disponible.

El equipo de desarrollo ha estado actualizando la aplicación con frecuencia, pero debido a la falta de conocimiento en los métodos de implementación, solo tienen la opción de copiar directamente los archivos, y esto está causando problemas con el seguimiento de los cambios que se están realizando. Al mismo tiempo, el equipo de desarrollo no tiene datos para mostrar si la aplicación se está ejecutando correctamente.

El problema se volvió crítico hace dos días cuando se acercaba una fecha límite para actualizar los registros médicos. La aplicación experimentó mucho más uso de lo normal, y el sistema se sobrecargó rápidamente y dejó de responder. El equipo de TI determinó que el problema era que el servidor se estaba quedando sin recursos, pero les tomó dos horas construir un segundo servidor para manejar la carga.

Su gerente ha acudido a usted pidiéndole una solución que aborde todos estos problemas. Cualquier solución que ofrezca debe tener en cuenta que los datos médicos en esta aplicación están cubiertos por HIPAA, y su gerente quiere que CMG retenga todo el control de los datos. Su gerente también quiere controlar cuidadosamente los costos.

Decidió que CMG debería mover la aplicación a la nube, pero debe vender la idea a su gerente.

Responde las siguientes preguntas:
1. ¿Qué tipo de servicio en la nube recomendaría?
2. ¿Cómo justificaría su elección en relación con los problemas que encuentra el equipo de TI?
3) ¿Cómo justificaría su elección en relación con los problemas que encuentra el equipo de desarrollo?
4. ¿Qué otros beneficios complacerán a su gerente si se siguen sus consejos?

5. ¿Cómo puede cumplir los requisitos relacionados con los registros médicos y la necesidad de controlarlos?

EXPERIENCIAS DE PENSAMIENTO RESPUESTAS

En esta sección, discutiremos las respuestas de la sección anterior.

1. Un servicio PaaS tiene más sentido en esta situación. Un entorno IaaS requeriría que su departamento de TI administre las máquinas virtuales, y eso no cumpliría con sus requisitos. Un servicio SaaS le proporciona el software y, en este caso, debe ejecutar la aplicación personalizada de su empresa en la nube.
2. El departamento de TI tiene pocos recursos y tiene el desafío de mantener la aplicación disponible. En un servicio PaaS, la gestión de las máquinas virtuales que ejecutan la aplicación se descarga al proveedor de la nube. El proveedor de la nube también ofrece un SLA para que su aplicación esté siempre disponible. El equipo de TI también se beneficiará del escalado fácil que se ofrece en un entorno de nube y, en lugar de dos horas, puede agregar más servidores casi al instante.
3. En un servicio PaaS, el proveedor de la nube ofrece opciones de implementación flexibles que facilitan la implementación de una aplicación utilizando el método que prefiera. También proporcionan registros para que el equipo de desarrollo pueda rastrear los cambios realizados en la aplicación. Las funciones de diagnóstico en un servicio PaaS (como Azure Insights de aplicación) proporcionan datos detallados sobre el rendimiento de una aplicación y pueden alertarlo sobre problemas de código en una aplicación.
4. Su gerente quiere reducir costos, y mudarse a la nube debería satisfacer esa necesidad. Su departamento de TI ya ha creado un segundo servidor, de modo que cuando se requiera una necesidad adicional, podrá satisfacerla. Sin embargo, el mayor uso fue temporal. Aun así, estaba relacionado con una fecha límite para la presentación de registros, y la próxima vez que se cumpla ese plazo, necesitará ese segundo servidor. Al pasar a la nube, se beneficia de una escala y elasticidad fáciles para que pueda escalar cuando necesite el segundo servidor para manejar la carga, y luego pueda volver a escalar fácilmente para reducir sus costos.
5. Al adoptar un modelo de nube híbrida, puede mantener sus datos médicos confidenciales en las instalaciones, mientras se beneficia de la aplicación que se ejecuta en la nube.

RESUMEN DEL CAPÍTULO

En este capítulo, aprendió algunos de los conceptos generales relacionados con la nube. Aprendió sobre las ventajas de pasar a la nube, aprendió sobre los diferentes tipos de servicios en la nube y aprendió sobre los diferentes modelos de nube disponibles para usted. Aquí están los conceptos clave de este capítulo.

- Los proveedores de la nube ofrecen acuerdos de nivel de servicio (SLA) que garantizan un cierto nivel de disponibilidad, pero solo para aquellos sistemas que están controlados por ellos.
- Pasar a la nube puede ayudar a evitar el tiempo de inactividad causado por cortes de red, cortes de sistema y cortes de energía. También puede ayudarlo si necesita diagnosticar problemas con una aplicación o problemas con un sistema externo que utiliza su aplicación.
- Puede escalar (o verticalmente) cuando desee agregar CPU adicionales o más memoria utilizando una VM más potente.
- Puede escalar (u horizontalmente) si desea agregar más máquinas virtuales para manejar cargas adicionales.

- Los proveedores de la nube le brindan formas de escalar automáticamente según los patrones de uso, la utilización de los recursos y los momentos del día. Esto se conoce como *elasticidad* .
- Los proveedores de la nube supervisan el estado de la infraestructura. Cuando una máquina virtual no es saludable, el proveedor de la nube puede moverlo automáticamente a una máquina virtual saludable sin que tenga que hacer nada. Esto se llama *tolerancia a fallas* .
- Los proveedores de la nube también operan en múltiples centros de datos que se encuentran en diferentes regiones del mundo. Si ocurre un desastre natural (o cualquier otro desastre) en una región, puede cambiar a otra región, suponiendo que haya replicado su entorno en varias regiones. Este tipo de planificación se llama planificación de Continuidad del Negocio y Recuperación de Desastres, y los proveedores de la nube a menudo tienen funciones para facilitar la implementación de un plan. Esto a menudo se conoce como recuperación ante desastres.
- Debido a que está utilizando la infraestructura propiedad del proveedor de la nube, mudarse a la nube reduce sus *gastos de capital* , los principales gastos en que se incurre por la infraestructura y otras compras importantes. Los proveedores de la nube aprovechan el *principio de las economías de escala* al comprar grandes cantidades de infraestructura para ser utilizadas por los consumidores de la nube.
- Los gastos diarios (gastos *operativos*) también se pueden reducir en la nube porque solo paga por los recursos que está utilizando en un momento determinado. Este *modelo basado en el consumo* es un beneficio clave de la nube.
- Infraestructura como servicio (IaaS) ofrece infraestructura que se ejecuta en la nube, pero debe mantener el sistema operativo y lo que está instalado en esa infraestructura. Los servicios de IaaS le ofrecen el mayor control en la nube, pero también conllevan la mayor carga administrativa.
- La plataforma como servicio (PaaS) descarga la administración de la infraestructura y también descarga el sistema operativo y los componentes instalados en las máquinas virtuales al proveedor de la nube. Usted es responsable de su solicitud. Los servicios de PaaS también ofrecen muchas características adicionales que facilitan agregar funcionalidad a una aplicación sin tener que escribir código complejo. Los equipos de desarrollo también tienen una amplia variedad de métodos de implementación disponibles, y el proveedor de la nube a menudo automatiza gran parte de ese proceso.
- Software-as-a-Service (SaaS) proporciona una aplicación alojada en la nube a la que se accede más comúnmente mediante un navegador web. En un servicio SaaS, el proveedor de la nube gestiona todo por usted. Básicamente está alquilando el uso del software deproveedor de la nube. Una gran ventaja de SaaS es que hace que las aplicaciones sean fácilmente accesibles para los empleados en el campo en cualquier dispositivo.
- El modelo de nube pública a veces se conoce como un entorno multiinquilino. Varias empresas y usuarios comparten la misma infraestructura. Las máquinas virtuales y otras infraestructuras se asignan a los usuarios cuando las necesitan, y cuando ya no las necesitan, se devuelven al grupo para que otros usuarios las usen. La red está disponible públicamente a través de Internet, pero usted tiene la capacidad de implementar métodos de seguridad para controlar el acceso a sus recursos.

- El modelo de nube privada a veces se conoce como un entorno de un solo inquilino. Toda la infraestructura es privada para un individuo o una empresa, y la red solo está disponible dentro de la nube privada. No está expuesto a Internet. En muchos casos, la infraestructura utilizada en una nube privada es propiedad de la empresa, pero no siempre. Es posible alojar una nube privada en un centro de datos de terceros.
- Un modelo de nube híbrida es una mezcla de los modelos de nube pública y privada. Las nubes híbridas a menudo se usan cuando una empresa necesita usar recursos locales en una aplicación en la nube.

Capítulo 2. Comprender los servicios principales de Azure

En el Capítulo 1 , " Comprender los conceptos de la nube ", aprendió sobre la nube y cómo puede beneficiarse del uso de los servicios en la nube. Se mencionó Microsoft Azure, pero no con mucho detalle.

En este capítulo, nos sumergimos en los muchos servicios y soluciones que ofrece Azure. Obtendrá una comprensión de los conceptos clave en la arquitectura de Azure, que se aplican a todos los servicios de Azure. Cubrimos los centros de datos de Azure y las formas en que Microsoft implementa la tolerancia a fallas y la recuperación ante desastres mediante la difusión de la infraestructura de Azure en todo el mundo. También aprenderá sobre las zonas de disponibilidad, que son la solución de Microsoft para garantizar que sus servicios no se vean afectados cuando un centro de datos de Azure en particular experimenta un problema.

También descubrirá cómo administrar y rastrear sus recursos de Azure, y cómo puede trabajar con los recursos como un grupo usando los grupos de recursos de Azure. Aprenderá cómo usar los grupos de recursos no solo para planificar y administrar los recursos de Azure, sino también cómo los grupos de recursos pueden ayudarlo a clasificar sus gastos operativos en Azure.

Para comprender realmente los grupos de recursos y cómo Azure funciona de manera oculta, es importante comprender Azure Resource Manager (ARM), el sistema subyacente que Azure usa para administrar sus recursos. Aprenderá sobre los beneficios que ofrece ARM y verá cómo ARM abre algunas posibilidades poderosas para implementar soluciones de Azure del mundo real de manera rápida y fácil.

Una vez que tenga la comprensión fundamental de Azure, profundizará en algunos de los productos principales que ofrece Microsoft, como Azure Compute, redes, almacenamiento y ofertas de bases de datos, que están cubiertos desde una perspectiva de Azure. Aprenderá acerca de algunos de los productos disponibles en cada una de estas áreas, y tendrá una idea de cómo funcionan conjuntamente los productos de Azure. En el camino, aprenderá sobre Azure Marketplace y cómo permite la creación e implementación de soluciones complejas con un trabajo mínimo de su parte, y debido al conocimiento "oculto" que tendrá al principio del capítulo, Azure Marketplace no parecerá magia negra.

Incluso aprenderá sobre algunas de las áreas tecnológicas más actuales y lo que Azure tiene para ofrecer en esas áreas. Esto incluye Internet de las cosas (IoT) y cómo usa Azure para conectarse y administrar dispositivos de todo tipo. Azure puede ayudarlo a analizar grandes cantidades de datos utilizando productos de Big Data y análisis, y aprenderá cómo estas ofertas pueden ayudarlo a controlar los costos.

Una de las tecnologías más populares en este momento es la inteligencia artificial o IA. Azure ofrece una plataforma integral de inteligencia artificial que incluye algunos poderosos componentes de aprendizaje automático, yhablaremos sobre lo que ofrece Azure en esta área y cómo puede usar la inteligencia artificial y el aprendizaje automático para crear soluciones poderosas y perspicaces. Concluiremos con la cobertura de la informática sin servidor en Azure y cómo puede crear servicios potentes y flexibles en Azure sin gastar mucho dinero y, a menudo, ¡sin gastar nada en absoluto!

Además, aprenderá sobre las herramientas que ofrece Microsoft para crear y administrar sus servicios de Azure, incluido el portal de Azure, que es una herramienta de administración basada en un navegador web que ofrece excelentes herramientas para profundizar en sus recursos de Azure y administrarlos fácilmente. También cubrimos cómo usar herramientas de línea de comandos con PowerShell y la interfaz de línea de comandos de Azure. Y terminaremos todo con un vistazo a Azure Advisor, el servicio de Microsoft que le brinda consejos sobre las mejores prácticas para sus servicios de Azure.

Si crees que es mucho para cubrir, ¡tienes razón! Es importante que comprenda todos estos temas para aprobar el examen AZ-900. Con el conocimiento fundamental de la nube del Capítulo 1 , descubrirá que comprender los conceptos específicos de Azure será más fácil de lo que cree.

Habilidades cubiertas en este capítulo:

- Comprender los componentes arquitectónicos principales de Azure
- Describa algunos de los productos principales disponibles en Azure
- Describa algunas de las soluciones disponibles en Azure
- Comprender las herramientas de administración de Azure

HABILIDAD 2.1: COMPRENDER LOS COMPONENTES ARQUITECTÓNICOS PRINCIPALES DE AZURE

Si le pidiera a cualquier CEO que enumere los cinco activos más importantes de su compañía, es probable que los datos de la compañía estén cerca de la parte superior de la lista. El mundo en que vivimos gira en torno a los datos. Solo mira empresas como Facebook y Google. Estas empresas nos ofrecen servicios que nos gustan. A todos les gusta ver fotos de amigos y familiares en Facebook (mezcladas con cosas que no nos gustan tanto), y ¿quién no usa Google para buscar cosas en Internet? Facebook y Google no ofrecen esos servicios porque quieren ser amables con nosotros. Ofrecen esos servicios porque es una forma de recopilar una gran cantidad de datos sobre sus clientes, y esos datos son su activo más valioso.

Facebook y Google no están solos. La mayoría de las empresas tienen grandes cantidades de datos que son clave para su negocio, y mantener esos datos seguros es la piedra angular de las decisiones comerciales. Es por eso que muchas empresas dudan en pasar a la nube. Tienen miedo de perder el control de sus datos. No solo temen que alguien más pueda obtener acceso a datos confidenciales, sino que también están preocupados por perder datos que serían difíciles (o incluso imposibles) de recrear.

Microsoft es muy consciente de esos temores, y Azure ha sido diseñado desde cero para infundir confianza en esta área. Veamos algunos componentes arquitectónicos centrales que ayudan a Microsoft a cumplir la promesa de la nube.

Esta sección cubre:

- Regiones azules
- Zonas de disponibilidad
- Administrador de recursos de Azure (ARM)
- Grupos de recursos

Regiones azules

El término "nube" tiene una tendencia a hacer que las personas piensen en Azure como una entidad nebulosa que no se puede ver claramente, pero eso sería un error. Si bien ciertamente hay construcciones lógicas para Azure, también tiene componentes físicos. Después de todo, al final del día, ¡estamos hablando de computadoras!

Para proporcionar servicios de Azure a personas de todo el mundo, Microsoft ha creado límites llamados geografías. Un límite geográfico es a menudo la frontera de un país, y hay buenas razones para ello. A menudo, existen regulaciones para el manejo de datos que se aplican a todo un país, y tener una geografía definida para un país permite a Microsoft asegurarse de que existan regulaciones de manejo de datos. Muchas empresas (especialmente aquellas que se ocupan de datos confidenciales) también se sienten mucho más cómodas si sus datos están contenidos dentro de los límites del país en el que operan.

Hay numerosas geografías en Azure. Por ejemplo, hay una geografía de los Estados Unidos, una geografía de Canadá, una geografía del Reino Unido, etc. Cada geografía se divide en dos o más regiones, cada una de las cuales está típicamente a cientos de millas de distancia. Como ejemplo, dentro de la geografía de los Estados Unidos, hay muchas regiones, incluida la región central de los Estados Unidos en Iowa, la región del este de los Estados Unidos en Virginia, la región del oeste de los Estados Unidos en California y la región del centro sur de los Estados Unidos en Texas. Microsoft también opera regiones aisladas que están completamente dedicadas a los datos del gobierno debido a las regulaciones adicionales que requieren los datos gubernamentales.

 ***Consejo de examen***

Es importante el hecho de que cada geografía contiene al menos dos regiones separadas por una gran distancia física. Así es como Azure mantiene la recuperación ante desastres, y es probable que este concepto se incluya en el examen. Cubriremos más sobre esto más adelante en este capítulo.

En cada región, Microsoft ha creado centros de datos (edificios físicos) que contienen el hardware físico que usa Azure. Estos centros de datos contienen edificios con clima controlado que albergan los racks de servidores que contienen hardware físico para computadoras. También tienen una infraestructura de red compleja y confiable para proporcionar la potencia de la red.

Más información Los **clientes solo ven las regiones**

Cuando un cliente crea recursos de Azure, solo la región es visible. El concepto de geografías es una implementación interna de Azure que los clientes realmente no tienen visibilidad cuando usan Azure.

Cada centro de datos tiene una fuente de alimentación aislada y generadores de energía en caso de corte de energía. Todo el tráfico de red que ingresa y sale del centro de datos pasa por la red de fibra óptica de Microsoft, en fibra propiedad o alquilada por Microsoft. Incluso los datos que fluyen entre regiones a través de los océanos viajan a través de los cables de fibra óptica de Microsoft que atraviesan los océanos.

Más información **Datacenter Power**

A partir de 2018, todos los centros de datos de Microsoft usaban al menos un 50% de energía natural que consistía en energía solar, eólica, etc. Para 2020, el objetivo es el 60% y el objetivo a largo plazo es utilizar energía 100% sostenible.

Con el fin de eliminar la dependencia de proveedores de energía de terceros, Microsoft también está invirtiendo en el desarrollo de celdas de combustible totalmente integradas que funcionen con gas natural. Las celdas de combustible no solo proporcionan energía limpia, sino que también eliminan las fluctuaciones de energía y otras desventajas de depender de la red eléctrica.

Para garantizar que los datos en Azure estén a salvo de desastres y fallas debido a posibles problemas en una región en particular, se alienta a los clientes a replicar datos en múltiples regiones. Si, por ejemplo, la región centro-sur de EE. UU. Se ve afectada por un tornado devastador (no está fuera de discusión en Texas), los datos que también se replican en la región centro-norte de EE. UU. En Illinois aún están seguros y disponibles. Para garantizar que las aplicaciones sigan funcionando tan rápido como sea posible, Microsoft garantiza un rendimiento de red de ida y vuelta de 2 milisegundos o menos entre regiones.

Zonas de disponibilidad

El hecho de que las regiones estén separadas físicamente por cientos de millas protege a los usuarios de Azure de la pérdida de datos y las interrupciones de la aplicación debido a desastres en una región en particular. Sin embargo, también es importante que los datos y las aplicaciones mantengan la disponibilidad cuando se produce un problema en un centro de datos en particular dentro de una región. Por esa razón, Microsoft desarrolló zonas de disponibilidad.

Nota **Disponibilidad Disponibilidad de zona**

Las zonas de disponibilidad no están disponibles en todas las regiones de Azure. Para ver la lista más actualizada de regiones habilitadas para zonas habilitadas, consulte: *https://docs.microsoft.com/azure/availability-zones/az-overview* .

Hay al menos tres zonas de disponibilidad dentro de cada región habilitada, y debido a que cada zona de disponibilidad existe dentro de su propio centro de datos en esa región, cada una tiene un suministro de agua, un sistema de enfriamiento, una red y una fuente de alimentación aislada de otras zonas. Al implementar un servicio de Azure en dos o más zonas de disponibilidad, puede lograr una alta disponibilidad en una situación en la que hay un problema en una zona.

Consejo de examen

Las zonas de disponibilidad proporcionan alta disponibilidad y tolerancia a fallas, pero pueden no ayudarlo con la recuperación ante desastres. Si hay un desastre localizado, como un incendio en un centro de datos que alberga una zona, se beneficiará de las zonas de disponibilidad. Debido a que las zonas de disponibilidad se encuentran en la misma región de Azure, si hay un desastre natural a gran escala, como un tornado, es posible que no esté protegido. En otras palabras, las zonas de disponibilidad son solo una faceta de una recuperación general ante desastres y un diseño tolerante a fallas.

Debido a que las zonas de disponibilidad están diseñadas para ofrecer una mayor disponibilidad de infraestructura, no todos los servicios admiten zonas de disponibilidad. Por ejemplo, Azure tiene un servicio llamado App Service Certificate que le permite comprar y administrar un certificado SSL a través de Azure. No tendría ningún sentido alojar un Certificado de Servicio de Aplicaciones dentro de una zona de disponibilidad porque no es un componente de infraestructura.

En este momento, las zonas de disponibilidad son compatibles con los siguientes servicios de Azure.

- Máquinas virtuales de Windows
- Máquina virtual de Linux
- Conjuntos de báscula de máquina virtual
- Discos gestionados
- Equilibrador de carga
- Dirección IP pública
- Almacenamiento de zona redundante
- Base de datos SQL

- Centros de eventos
- Bus de servicio (solo nivel Premium)
- VPN Gateway
- ExpressRoute
- Application Gateway (actualmente en versión preliminar)
- Entornos de servicio de aplicaciones (actualmente en versión preliminar en regiones limitadas)
-

Nota **Manténgase al día con los cambios en Azure**

Puede mantenerse al día con todas las noticias relacionadas con las actualizaciones de Azure mirando el blog de Azure en *https://azure.com/blog* .

Al implementar su servicio en dos o más zonas de disponibilidad, se asegura la máxima disponibilidad para ese recurso. De hecho, Microsoft garantiza un acuerdo de nivel de servicio (SLA) de 99.99% de tiempo de actividad para las máquinas virtuales de Azure solo si se implementan dos o más máquinas virtuales en dos o más zonas. La Figura 2-1 ilustra el beneficio de correr en múltiples zonas. Como puede ver, aunque la zona de disponibilidad 3 se ha desconectado por algún motivo, las zonas 1 y 2 siguen operativas.

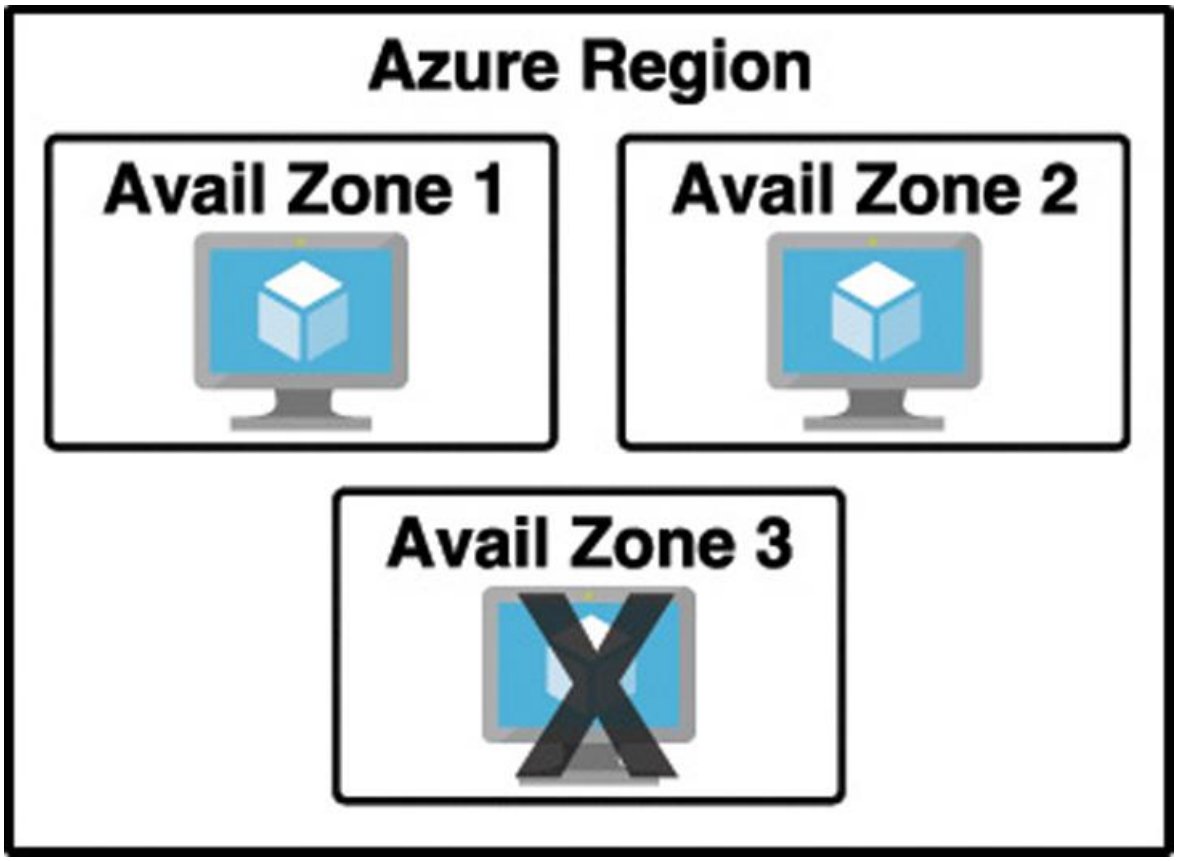


Figura 2-1 Máquina virtual de Azure dentro de tres zonas de disponibilidad

Consejo de examen

No confunda las zonas de disponibilidad con los conjuntos de disponibilidad. Los conjuntos de disponibilidad le permiten crear dos o más máquinas virtuales en diferentes racks de servidores físicos en un centro de datos de Azure. Microsoft garantiza un SLA del 99.95% con un conjunto de disponibilidad.

Una zona de disponibilidad le permite implementar dos o más servicios de Azure en dos centros de datos distintos dentro de una región. Microsoft garantiza un 99.99% de SLA con zonas de disponibilidad.

Hay dos categorías de servicios que admiten zonas de disponibilidad: servicios *zonales* y servicios de *zona redundante* . Los servicios zonales son servicios como máquinas virtuales, discos administrados utilizados en una máquina virtual y direcciones IP públicas utilizadas en máquinas virtuales. Para lograr una alta disponibilidad, debe implementar explícitamente servicios zonales en dos o más zonas.

Tenga en cuenta los **discos administrados y las direcciones IP públicas**

Cuando crea una máquina virtual en Azure y la implementa en una zona de disponibilidad, Azure implementará automáticamente los discos administrados y la dirección IP pública (si está configurada) en la misma zona de disponibilidad automáticamente.

Los servicios de zona redundante son servicios como el almacenamiento de zona redundante y las bases de datos SQL. Para usar las zonas de disponibilidad con estos servicios, especifique la opción para que sean redundantes cuando las cree. (Para el almacenamiento, la característica se llama ZRS o almacenamiento de zona redundante. Para la Base de datos SQL, existe una opción para hacer que la base de datos sea redundante de zona). Azure se encarga del resto por usted replicando datos en múltiples zonas de disponibilidad automáticamente.

Administrador de recursos de Azure (ARM)

Casi todos los sistemas que se trasladan a la nube consisten en más de un servicio de Azure. Por ejemplo, puede tener una máquina virtual de Azure para una parte de su aplicación, sus datos pueden estar en una Base de datos SQL de Azure, puede tener algunos datos confidenciales almacenados en Azure Key Vault y puede tener una parte basada en web de su aplicación alojada en Azure App Service.

Si tiene que administrar todos estos diferentes servicios de Azure por separado, puede ser un gran dolor de cabeza, y si tiene varias aplicaciones en la nube, puede ser aún peor. No solo sería confuso realizar un seguimiento de qué servicios están relacionados con qué aplicaciones, sino que cuando agrega la complejidad de implementar actualizaciones en su aplicación, las cosas realmente pueden desorganizarse.

Para facilitar la implementación y la administración de los servicios de Azure, Microsoft desarrolló Azure Resource Manager o ARM. ARM es un servicio que se ejecuta en Azure y es responsable de toda interacción con los servicios de Azure. Cuando crea un nuevo servicio de Azure, ARM lo autentica para asegurarse de que tiene el acceso correcto para crear ese recurso, y luego habla con un *proveedor de recursos* para el servicio que está creando. Por ejemplo, si está creando una nueva aplicación web en Azure App

Service, ARM pasará su solicitud al proveedor de recursos de Microsoft.Web, porque sabe todo sobre las aplicaciones web y cómo crearlas.

 *Consejo de examen*

Hay proveedores de recursos para cada servicio de Azure, pero es posible que los nombres no siempre tengan sentido. Por ejemplo, el Microsoft. El proveedor de recursos informáticos es responsable de crear recursos de máquinas virtuales.

No es necesario que conozca los detalles sobre los proveedores de recursos para el examen AZ-100, pero debe comprender el concepto general, porque se espera que sepa sobre Azure Resource Manager.

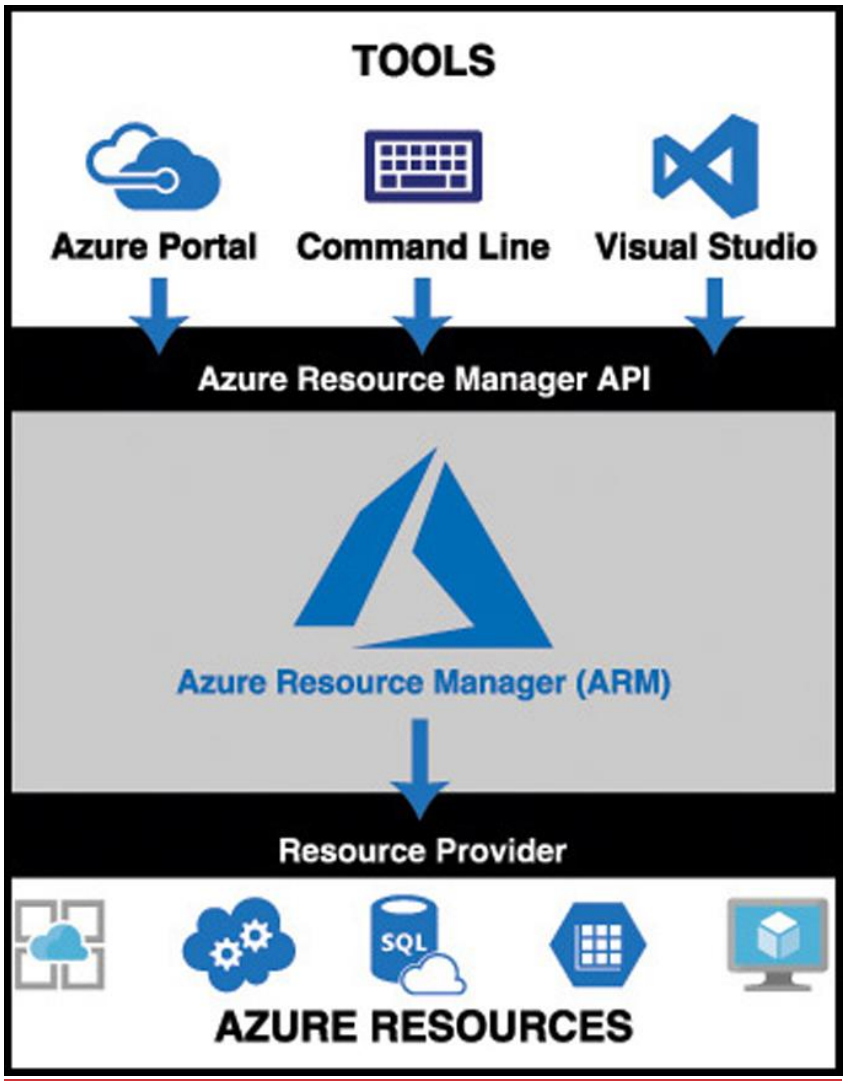
Más adelante en este capítulo, aprenderá a usar Azure Portal para crear y administrar servicios de Azure. También aprenderá cómo puede usar las herramientas de línea de comandos para hacer lo mismo. Tanto el portal como las herramientas de línea de comandos funcionan mediante ARM, e interactúan con ARM mediante la interfaz de programación de aplicaciones ARM o API. La API de ARM es la misma si está utilizando el portal o las herramientas de línea de comandos, y eso significa que obtiene un resultado consistente. Esotambién significa que puede crear un recurso de Azure con el portal y luego realizar cambios en él utilizando herramientas de línea de comandos, lo que le permite la flexibilidad que necesitan los consumidores de la nube.

Más información **Visual Studio y ARM**

Visual Studio, el entorno de desarrollo de Microsoft para escribir aplicaciones, también tiene la capacidad de crear recursos de Azure e implementar código en ellos. Hace esto usando la misma API ARM que usan las herramientas que mencionamos. De hecho, puede pensar en la API de ARM como su interfaz en el mundo de Azure. Realmente no puede crear ni administrar ningún servicio de Azure sin pasar por la API de ARM.

El flujo de una solicitud ARM típica para crear o administrar un recurso es sencillo. Una herramienta como Azure Portal, herramientas de línea de comandos o Visual Studio realiza una solicitud a la API de ARM. La API pasa esa solicitud a ARM donde el usuario está autenticado y autorizado para realizar la acción. ARM luego pasa la solicitud a un proveedor de recursos, y el proveedor de recursos crea el nuevo recurso o modifica un recurso existente. La Figura 2-2 ilustra este flujo y presenta una pequeña muestra de los muchos

Figura 2-2 Administrador de recursos de Azure


TOOLS
Azure Portal
Command Line
Visual Studio
Azure Resource Manager API
Azure Resource Manager (ARM)
Resource Provider
SQL
AZURE RESOURCES

La solicitud que se realiza a ARM no es una solicitud complicada basada en código. En cambio, ARM usa *sintaxis declarativa* . Eso significa que, como consumidor de Azure, le dice a ARM lo que quiere hacer y ARM lo hace por usted. No tiene que decirle a ARM *cómo* hacer lo que quiere. Simplemente tienes que decirle lo que quieres. Para hacer eso, ARM usa archivos que están codificados en JavaScript Object Notation (o JSON) llamados *plantillas ARM* .

Nota **plantillas ARM**

No necesita saber cómo usar las plantillas ARM para el examen AZ-900, pero para comprender cómo funciona ARM, realmente necesita saber al menos un poco sobre ellas.

En el sentido más básico, una plantilla ARM contiene una lista de recursos que desea crear o modificar. Cada recurso está acompañado por propiedades como el nombre del recurso y las propiedades que son específicas de ese recurso. Por ejemplo, si estaba utilizando una plantilla ARM para implementar una aplicación web en App Service, su plantilla ARM especificaría la región en la que desea que se cree su aplicación, el nombre de la aplicación, el plan de precios para su aplicación, cualquier dominio nombres que desea que use su aplicación, etc. No tiene que saber cómo configurar todas esas propiedades. Simplemente le dice a ARM que lo haga (declara su intención a ARM), y ARM se encarga de usted.

Más información **Más sobre plantillas de brazo**

Las plantillas ARM son increíblemente poderosas, pero también son bastante simples. Si desea leer más sobre cómo usar las plantillas ARM, consulte la documentación en: *https://docs.microsoft.com/azure/azure-resource-manager/resource-group-authoring-templates* .

Hay un aspecto más importante para la implementación de plantillas ARM. Cuando implementa múltiples recursos (que, como se señaló, es un escenario típico del mundo real), a menudo tiene dependencias de servicio. En otras palabras, está implementando uno o más servicios que dependen de otros servicios que ya se están creando.

Piense, por ejemplo, en una situación en la que está implementando un certificado para usarlo con una aplicación web. Una de las propiedades que necesita establecer en la aplicación web es el certificado que desea usar, pero si ese certificado aún no se ha implementado, su implementación fallará. ARM le permite especificar dependencias para que pueda evitar problemas como este. Simplemente le dice a ARM que la aplicación web depende del certificado y ARM se asegurará de que la implementación del certificado se complete antes de implementar la aplicación web.

Como puede ver, ARM tiene muchos beneficios, y debe tenerlos en cuenta para su examen:

- ARM le permite implementar fácilmente múltiples recursos de Azure a la vez.
- ARM hace posible reproducir cualquier implementación con resultados consistentes en cualquier momento en el futuro.

- ARM le permite crear plantillas declarativas para la implementación en lugar de requerirle que escriba y mantenga scripts de implementación complejos.
- ARM hace posible configurar dependencias para que sus recursos se implementen en el orden correcto cada vez.

Ahora hablemos de otro aspecto de ARM que lo ayuda a administrar los recursos de Azure, y son los grupos de recursos.

Grupos de recursos

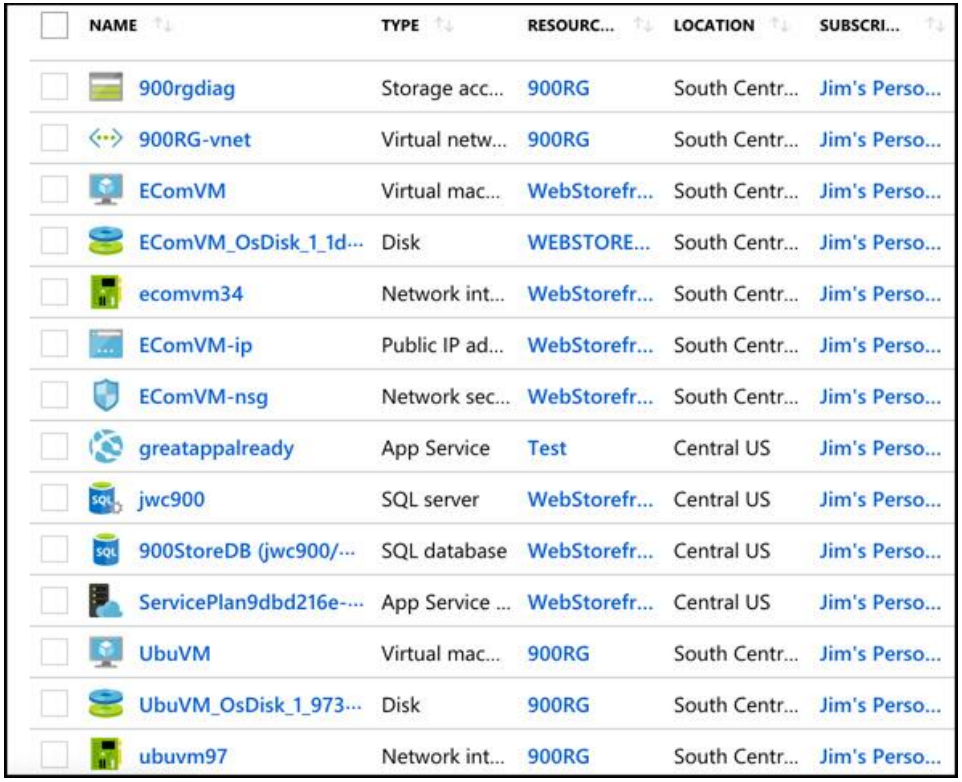
Ahora debería darse cuenta de que mudarse a la nube puede no ser tan simple como parecía al principio. Crear un único recurso en Azure es bastante simple, pero cuando se trata de aplicaciones de nivel empresarial, generalmente se trata de una gama compleja de servicios. No solo eso, sino que puede estar lidiando con múltiples aplicaciones que usan múltiples servicios, y pueden estar distribuidas en múltiples regiones de Azure. Las cosas ciertamente pueden volverse caóticas rápidamente.

Afortunadamente, Azure proporciona una función en ARM que lo ayuda a lidiar con este tipo de problema: el grupo de recursos. Un grupo de recursos es un contenedor lógico para los servicios de Azure. Al crear todos los servicios de Azure asociados con una aplicación en particular en un solo grupo de recursos, puede implementar y administrar todos esos servicios como una sola entidad.

Organizar los recursos de Azure en un grupo de recursos tiene muchas ventajas. En primer lugar, puede configurar fácilmente implementaciones utilizando una plantilla ARM. Las implementaciones de plantillas ARM suelen ser para un solo grupo de recursos. Puede implementar en múltiples grupos de recursos, pero hacerlo requiere que configure una cadena complicada de plantillas ARM.

Otra ventaja de los grupos de recursos es que puede nombrar un grupo de recursos con un nombre fácilmente reconocible para que pueda ver de un vistazo todos los recursos de Azure utilizados en una aplicación en particular. Esto puede no parecer tan importante hasta que realmente comience a implementar recursos de Azure y se dé cuenta de que tiene muchos más recursos de lo que pensaba. Por ejemplo, cuando crea una máquina virtual de Azure, Azure crea no solo una máquina virtual, sino también un recurso de disco, una interfaz de red, un recurso de IP pública y un grupo de seguridad de red. Si está mirando todos sus recursos de Azure, puede ser difícil diferenciar qué recursos van con cada aplicación. Los grupos de recursos resuelven ese problema.

En la Figura 2-3 , puede ver muchos servicios de Azure. Algunos de estos fueron creados automáticamente por Azure para admitir otros servicios, y en muchos casos, Azure le da al recurso un nombre irreconocible.



NAME	TYPE	RESOURC...	LOCATION	SUBSCRI...
900rgdiag	Storage acc...	900RG	South Centr...	Jim's Perso...
900RG-vnet	Virtual netw...	900RG	South Centr...	Jim's Perso...
EComVM	Virtual mac...	WebStorefr...	South Centr...	Jim's Perso...
EComVM_OsDisk_1_1d···	Disk	WEBSTORE...	South Centr...	Jim's Perso...
ecomvm34	Network int...	WebStorefr...	South Centr...	Jim's Perso...
EComVM-ip	Public IP ad...	WebStorefr...	South Centr...	Jim's Perso...
EComVM-nsg	Network sec...	WebStorefr...	South Centr...	Jim's Perso...
greatappalready	App Service	Test	Central US	Jim's Perso...
jwc900	SQL server	WebStorefr...	Central US	Jim's Perso...
900StoreDB (jwc900/···	SQL database	WebStorefr...	Central US	Jim's Perso...
ServicePlan9dbd216e-···	App Service ...	WebStorefr...	Central US	Jim's Perso...
UbuVM	Virtual mac...	900RG	South Centr...	Jim's Perso...
UbuVM_OsDisk_1_973···	Disk	900RG	South Centr...	Jim's Perso...
ubuvm97	Network int...	900RG	South Centr...	Jim's Perso...

Figura 2-3 Todos mis recursos de Azure

En la Figura 2-4 , puede ver los recursos que están en el grupo de recursos de WebStorefront. Estos son los recursos de Azure utilizados en el escaparate de comercio electrónico.

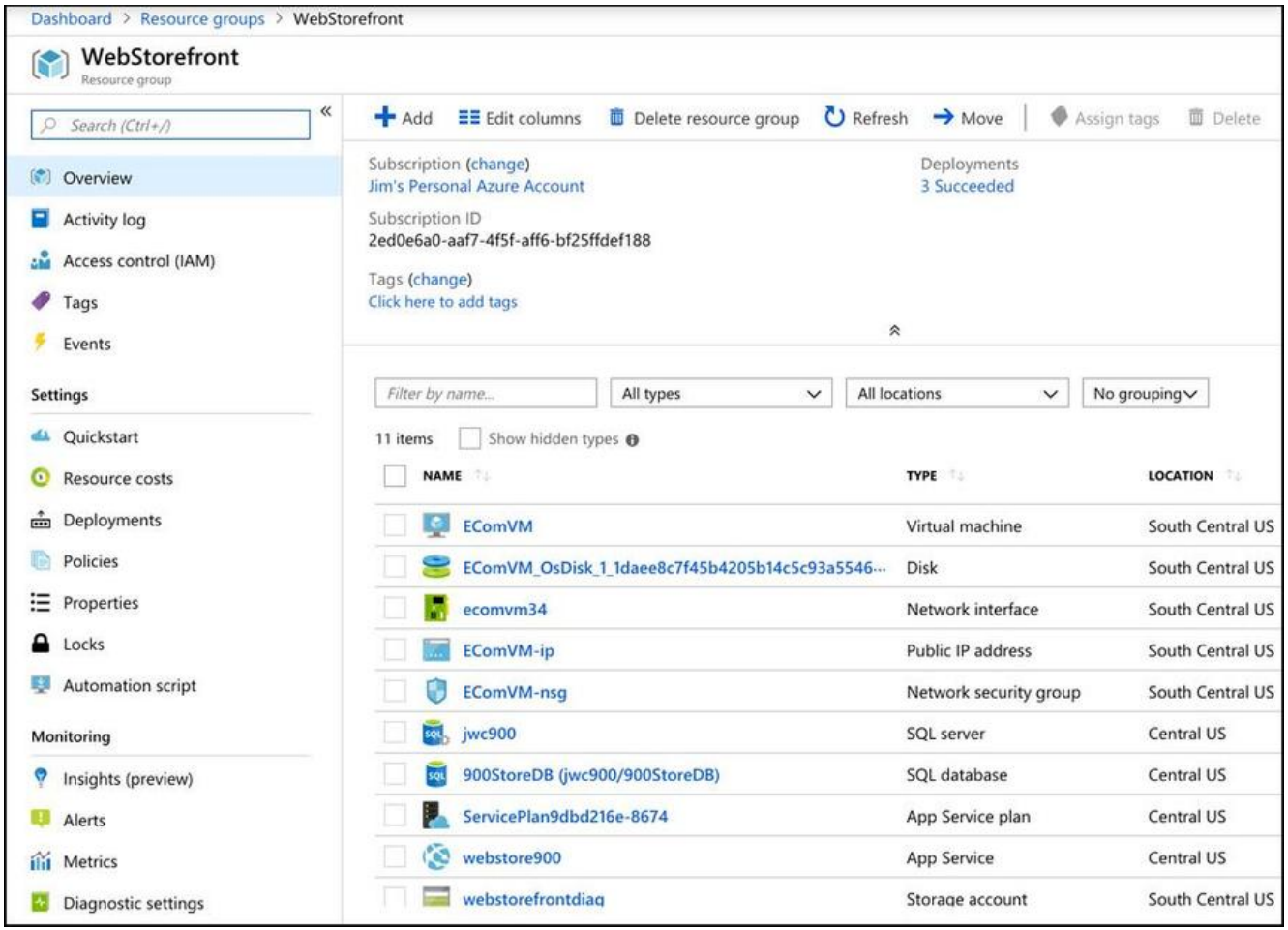


Figura 2-4 Un grupo de recursos de Azure

Es conveniente ver todos los recursos asociados con una aplicación en particular, pero no está bloqueado en ese paradigma. Este es un ejemplo útil, porque es un uso común de los grupos de recursos, pero puede organizar sus grupos de recursos de la forma que elija. Observe en la Figura 2-4 que ve recursos en varias regiones de Azure diferentes (las regiones están en la columna Ubicación). Si tiene acceso a varias suscripciones de Azure, "también puede" tener recursos de varias suscripciones en un solo grupo de recursos.

Si observa el lado izquierdo de la Figura 2-4 , verá un menú de operaciones que puede realizar en su grupo de recursos. No analizaremos todo esto porque está fuera del alcance del examen AZ-900, pero hay algunos que son útiles para comprender los beneficios de los grupos de recursos.

Si hace clic en **Costos de recursos** , puede ver el costo de todos los recursos en este grupo de recursos. Tener esa información a su alcance es especialmente útil en situaciones en las que desea asegurarse de que ciertos departamentos de su empresa cobren correctamente por los recursos utilizados. De hecho, algunas empresas crearán grupos de recursos para cada departamento en lugar de crearlos en un ámbito para las aplicaciones. Tener un grupo de recursos de ventas y marketing o un grupo de recursos de soporte de TI, por ejemplo, puede ayudarlo enormemente a informar y controlar los costos.

Consejo de examen

Un recurso de Azure solo puede existir en un grupo de recursos. En otras palabras, no puede tener una máquina virtual en un grupo de recursos llamado WebStorefront y también en un grupo de recursos llamado SalesMarketing, porque debe estar en un grupo u otro. Puede mover recursos de Azure de un grupo de recursos a otro.

También puede hacer clic en Automation Script y Azure generará una plantilla ARM que puede usar para implementar todos estos recursos de Azure. Esto es útil en una situación en la que desea implementar estos recursos más adelante o cuando desea implementarlos en otra suscripción de Azure.

Si hace clic en Etiquetas, puede aplicar una o más etiquetas que elija a su grupo de recursos. Una etiqueta consta de un nombre y un valor. Por ejemplo, supongamos que una empresa participa en dos eventos comerciales: uno en Texas y otro en Nueva York. También ha creado muchos recursos de Azure para admitir esos eventos. Desea ver todos los recursos de Azure para un evento específico, pero están distribuidos en varios grupos de recursos. Al agregar una etiqueta a cada grupo de recursos que identifica el evento al que está asociado, puede resolver este problema.

En la Figura 2-5 , puede ver las etiquetas asociadas con un grupo de recursos de WebStorefront. A este grupo de recursos se le ha asignado una etiqueta llamada EventName, y el valor de esa etiqueta es ContosoTexas. Al hacer clic en el icono del cubo a la derecha de la etiqueta, puede ver todos los recursos que tienen esa etiqueta.

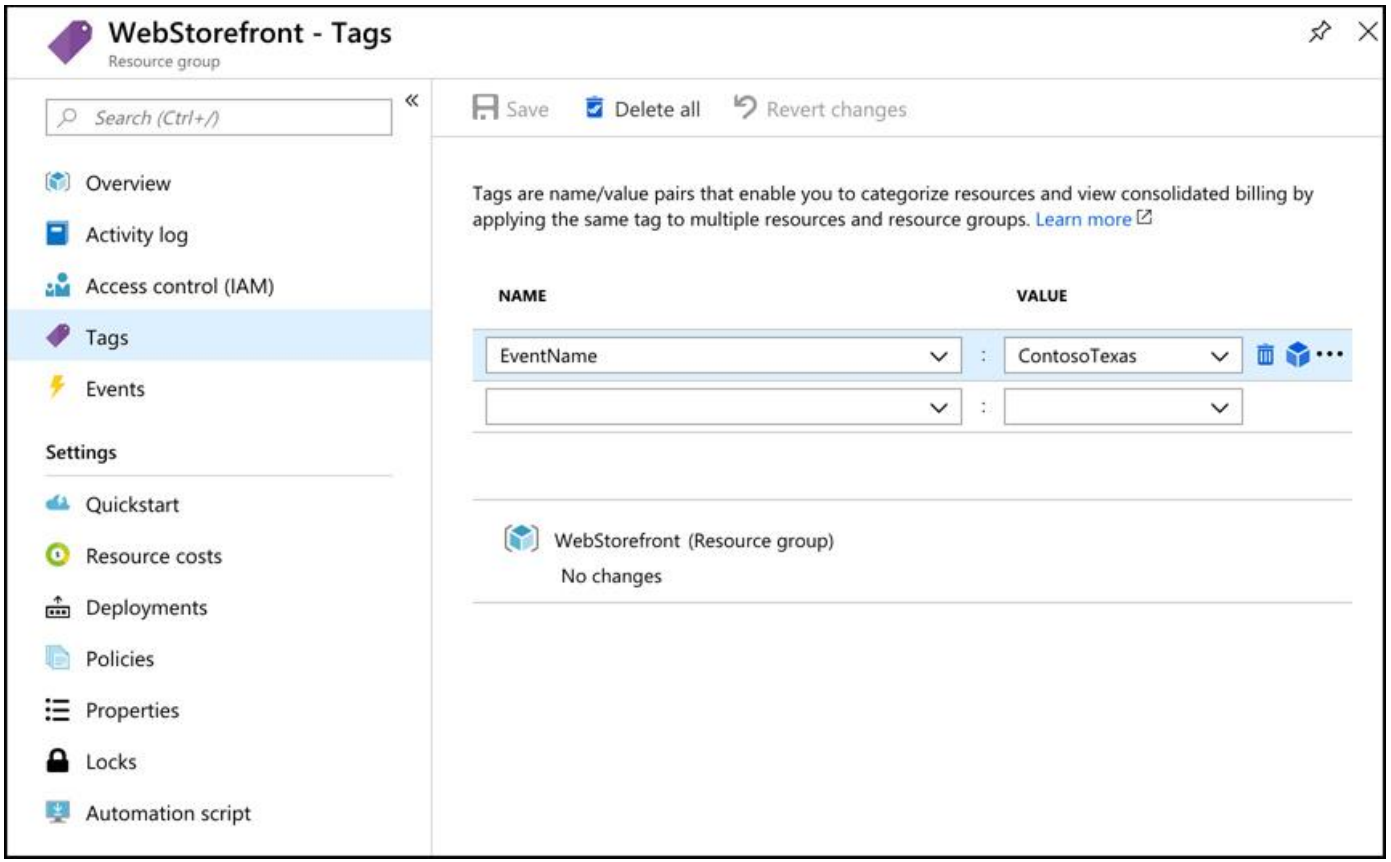


Figura 2-5 Etiquetado de un grupo de recursos

Para ver todas sus etiquetas, elija **Todos los servicios** en el menú principal del portal y luego haga clic en Etiquetas como se muestra en la Figura 2-6 .

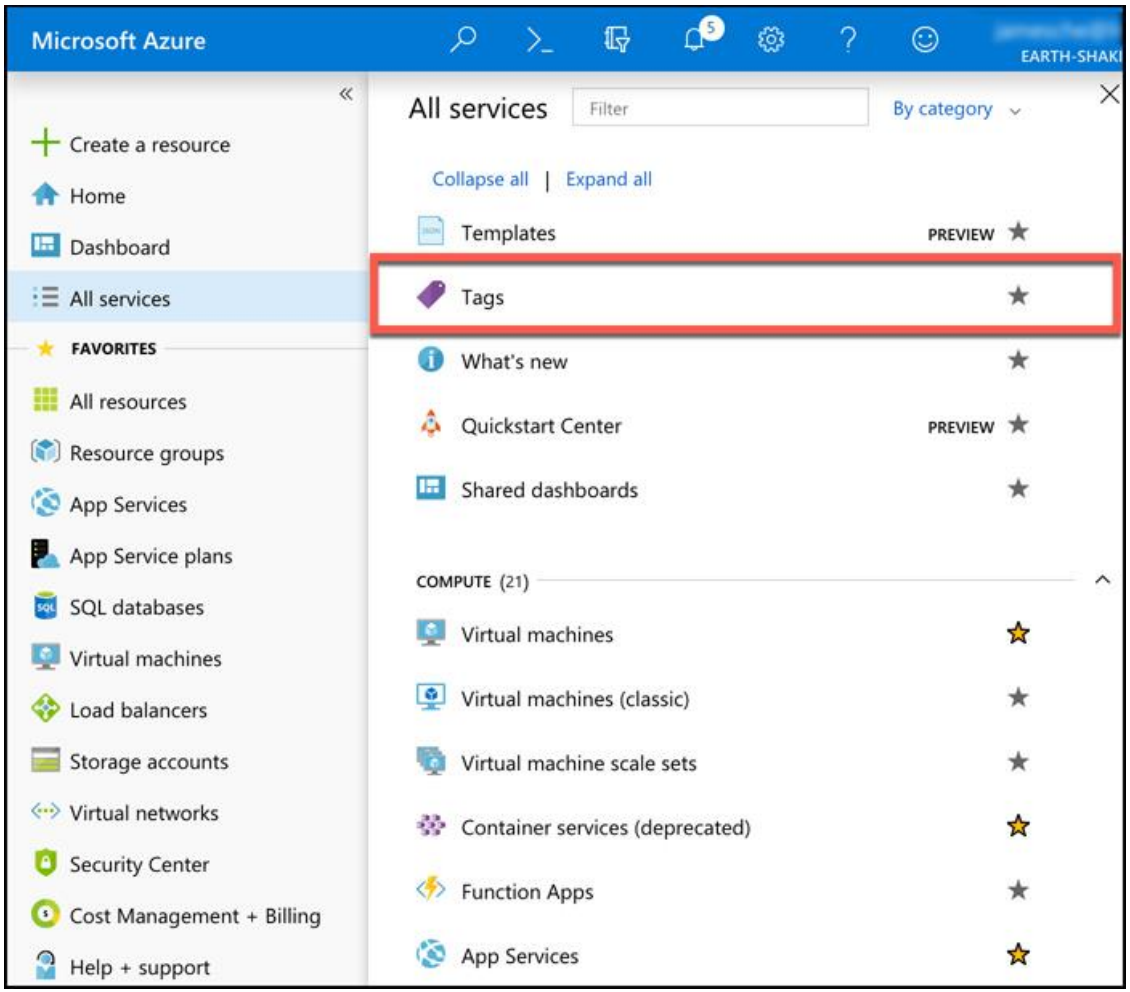


Figura 2-6 Visualización de todas las etiquetas

Puede aplicar una etiqueta a la mayoría de los recursos de Azure, no solo a los grupos de recursos. También es importante comprender que al agregar una etiqueta a un grupo de recursos, no está agregando esa etiqueta a los recursos dentro del grupo de recursos. Si tiene

una aplicación web en el grupo de recursos de WebStorefront, esa aplicación web no hereda la etiqueta que se aplica al grupo de recursos. Debido a eso, las etiquetas agregan una capa adicional de flexibilidad y poder al visualizar sus recursos de Azure.

Consejo de examen

Las etiquetas también pueden ayudarlo a organizar sus gastos de facturación de Azure. Cuando descargue su factura de Azure, las etiquetas de recursos aparecerán en una de las columnas, y dado que las facturas de Azure se pueden descargar como valores separados por comas, puede usar herramientas como Microsoft Excel para filtrar según las etiquetas.

Cuando elimina un grupo de recursos, todos los recursos en ese grupo de recursos se eliminan automáticamente. Esto facilita la eliminación de múltiples recursos de Azure en un solo paso. Supongamos que está probando un escenario y necesita crear un par de máquinas virtuales, una base de datos, una aplicación web y más. Al colocar todos estos recursos en un grupo de recursos, puede eliminar fácilmente ese grupo de recursos después de la prueba y Azure eliminará automáticamente todos los recursos que contenga. Esta es una excelente manera de evitar costos inesperados asociados con recursos que ya no usa.

A lo largo de esta sección de habilidades, ha aprendido algunos de los beneficios de usar Azure. Debido a que las regiones de Azure se extienden por todo el mundo en diferentes geografías, puede estar seguro de que sus datos y aplicaciones están alojados donde los necesita y que se cumplen todas las regulaciones o requisitos de datos. Aprendió que hay varios centros de datos en cada región, y al implementar sus aplicaciones en zonas de disponibilidad, puede evitar el impacto de una falla en un centro de datos en particular.

También aprendió sobre Azure Resource Manager (ARM) y cómo puede ayudarlo a lograr implementaciones consistentes en Azure y administrar sus recursos de Azure fácilmente. Finalmente, aprendió sobre el uso de grupos de recursos para organizar sus recursos de Azure y cómo clasificar la facturación mediante etiquetas. En la siguiente sección de habilidades, aprenderá detalles sobre algunos de los productos específicos que son esenciales para Azure.

HABILIDAD 2.2: DESCRIBA ALGUNOS DE LOS PRODUCTOS PRINCIPALES DISPONIBLES EN AZURE

Al repasar los componentes arquitectónicos principales de Azure, notó algunas referencias a algunos de los productos disponibles en Azure. También hubo algunos detalles sobre el portal de Azure, pero lo trataremos en detalle en Skill 2.4. En esta sección de habilidades, hablaremos sobre algunos de los productos principales de Azure en cuatro categorías diferentes:

- **Cálculo de Azure** Esto se refiere a los recursos que proporcionan potencia informática para ejecutar sus aplicaciones. Azure ofrece productos de cómputo IaaS y PaaS.
- **Redes de Azure** Estos productos proporcionan conectividad entre los recursos de Azure y hacia y desde Internet o sus recursos locales.
- **Almacenamiento de Azure** Estos productos le brindan almacenamiento en la nube seguro y confiable para sus datos.
- **Base de datos de Azure** Estos productos proporcionan soluciones altamente escalables para alojar bases de datos de muchas variedades.

Nota sobre el **uso de Azure**

En esta sección de habilidades, creará un par de recursos de Azure, por lo que necesitará una suscripción de Azure. Si no tiene uno, puede obtener una prueba gratuita visitando: *https://azure.microsoft.com/free/* .

Esta sección cubre:

- Productos informáticos de Azure
- Productos de red de Azure
- Productos de almacenamiento de Azure
- Productos de base de datos de Azure
- Azure Marketplace y sus escenarios de uso

Productos informáticos de Azure

Los productos informáticos de Azure le permiten asignar de manera fácil y dinámica los recursos necesarios para cualquier tarea informática. Puede crear recursos informáticos rápidamente cuando los necesite, y cuando sus necesidades crezcan, puede escalar esos recursos para manejar requisitos adicionales. Al usar los recursos informáticos de Azure para sus necesidades informáticas, puede controlar más fácilmente los costos porque no paga por los recursos a menos que los necesite. También puede asignar infraestructura mucho más rápido de lo que puede en el mundo local, y puede beneficiarse de las economías de escala que ofrece Azure y usar computadoras extremadamente potentes que de otro modo no podría permitirse.

Algunos ejemplos de productos informáticos en Azure son las máquinas virtuales de Azure, el servicio de aplicaciones de Azure, las ofertas de contenedores en Azure y la informática sin servidor. (La informática sin servidor está cubierta en la habilidad 2.3).

Máquinas virtuales de Azure

Una máquina virtual (VM) es una computadora basada en software que se ejecuta en una computadora física. La computadora física se considera el *host* y proporciona los componentes físicos subyacentes, como espacio en disco, memoria, potencia de la CPU, etc. La computadora host ejecuta un software llamado hipervisor que puede crear y administrar una o más máquinas virtuales, y esas máquinas virtuales se conocen comúnmente como *invitados* .

El sistema operativo en un invitado no tiene que ser el mismo sistema operativo que el host está ejecutando. Si su host ejecuta Windows 10, puede ejecutar un invitado que use Windows Server 2016, Linux o muchos otros sistemas operativos. Esta flexibilidad hace que las máquinas virtuales sean extremadamente populares. Sin embargo, debido a que las máquinas virtuales que se ejecutan en un host usan los sistemas físicos en ese host, si necesita una VM poderosa, necesitará una computadora física poderosa para alojarla.

Al usar Azure Virtual Machines, puede aprovechar las potentes computadoras host que Microsoft pone a disposición cuando necesita potencia informática, y cuando ya no la necesita, ya no tiene que pagarla.

Para crear una máquina virtual de Azure, inicie sesión en el portal de Azure con su cuenta de Azure y luego siga estos pasos como se muestra en las Figuras 2-7 a 2-9.

1. Haz clic en **Crear un recurso** .
2. Haz clic en **Calcular** .
3. Haz clic en **Servidor Ubuntu** .

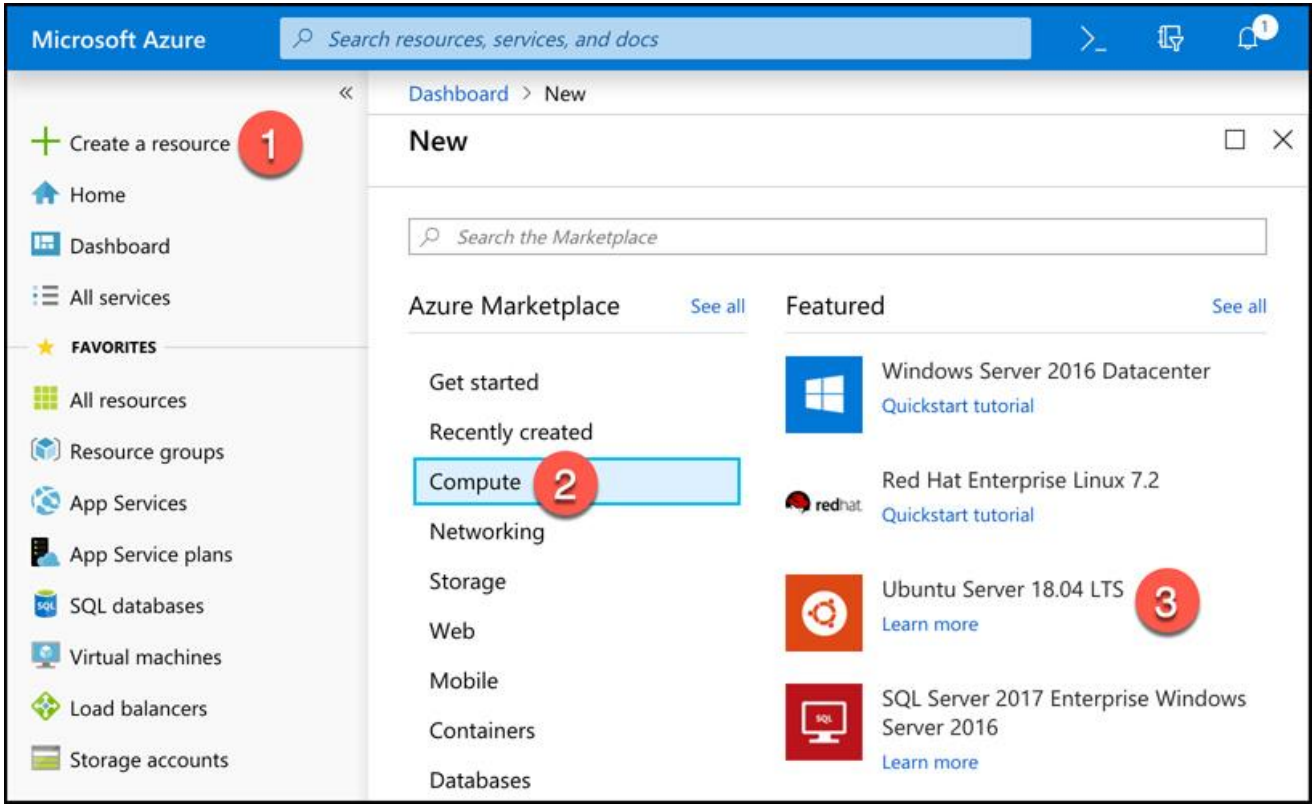


Figura 2-7 Crear una máquina virtual

4. Junto a Grupo de recursos, haga clic en **Crear nuevo** para crear un nuevo grupo de recursos.
5. Ingrese **TestRG** como el nombre del grupo de recursos y haga **clic** en **Aceptar** .

6. Ingrese **TestVM** como su nombre de VM.
7. Desplácese hacia abajo y seleccione **Contraseña** para el tipo de autenticación.
8. Ingrese un nombre de usuario para su cuenta de administrador.
9. Ingrese una contraseña que le gustaría usar para su cuenta de administrador.
10. Confirma la contraseña.
11. Deje todas las demás configuraciones como están y haga clic en **Revisar + Crear** para validar su configuración.

Más información **Configuración y opciones de la máquina virtual**

Hay muchas más opciones que puede elegir para su VM. Podríamos haber hecho clic en Siguiente: Discos , como se muestra en la Figura 2-9 , para pasar a páginas adicionales que contienen muchas más opciones. También puede hacer clic en una de las pestañas (Discos, Redes, Administración, etc., como se muestra en la Figura 2-8) para cambiar configuraciones específicas. Sin embargo, si elige, puede usar la configuración predeterminada como lo hemos hecho haciendo clic en Revisar + Crear tan pronto como haya ingresado la información que Azure requiere para una VM.

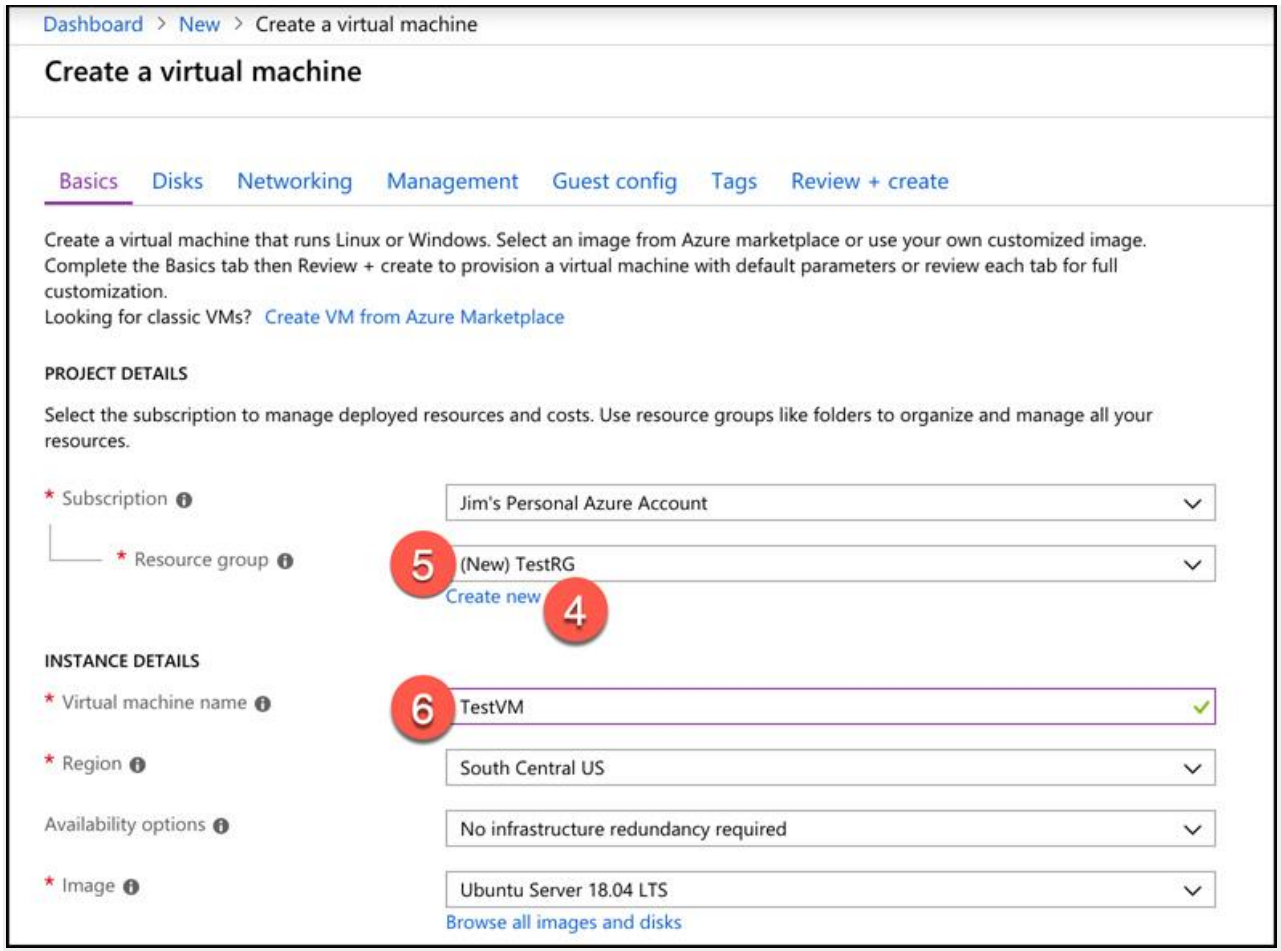

Dashboard > New > Create a virtual machine
Create a virtual machine
Basics
Disks
Networking
Management
Guest config
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.
Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.
Looking for classic VMs? Create VM from Azure Marketplace
PROJECT DETAILS
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
* Subscription
Jim's Personal Azure Account
* Resource group
5
(New) TestRG
Create new
4
INSTANCE DETAILS
* Virtual machine name
6
TestVM
* Region
South Central US
Availability options
No infrastructure redundancy required
* Image
Ubuntu Server 18.04 LTS
Browse all images and disks

Figura 2-8 Configuración de máquina virtual

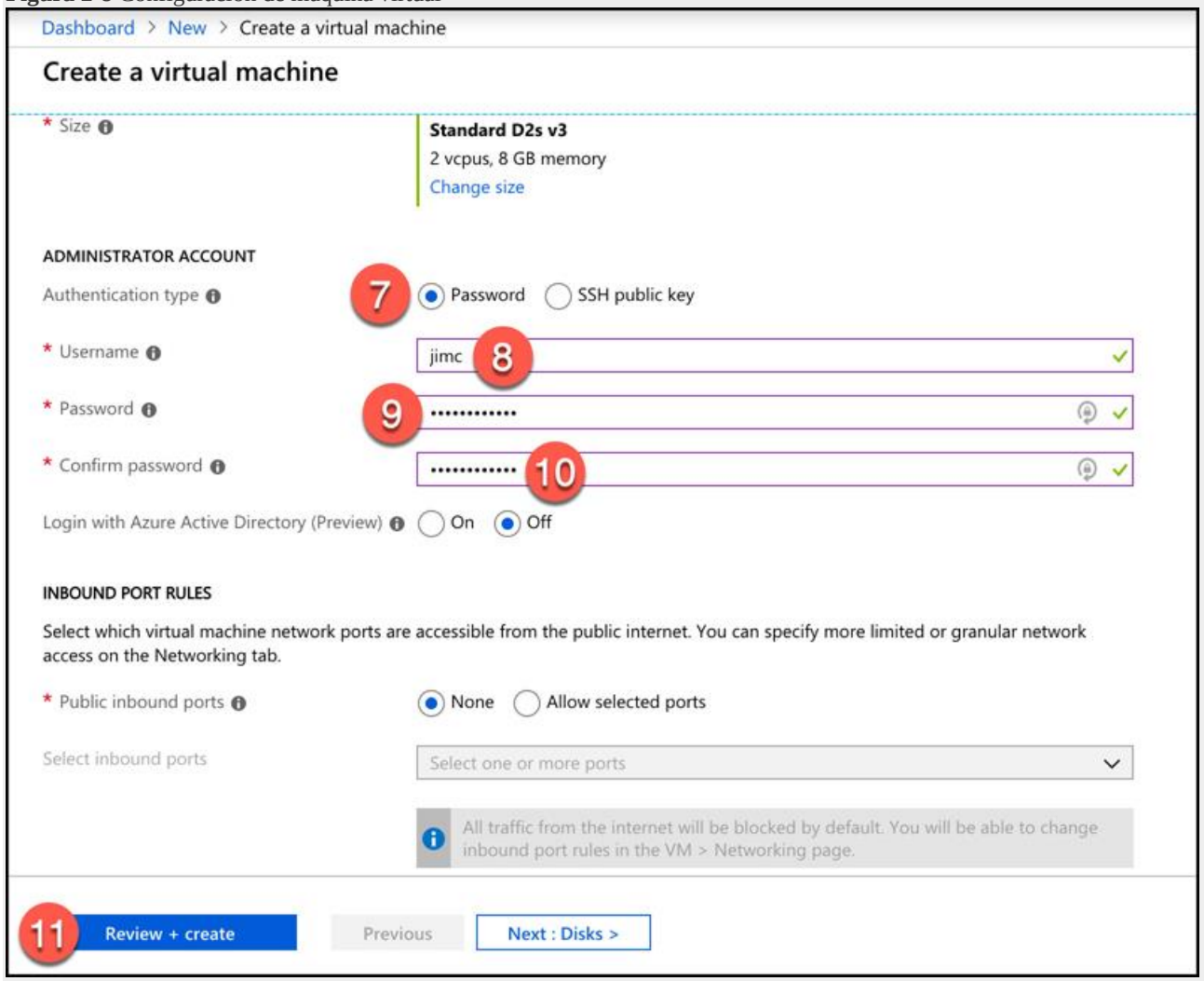


Figura 2-9 Configuración de máquina virtual

Después de hacer clic en **Revisar + Crear** , Azure validará su configuración para asegurarse de que no haya omitido nada. Una vez que haya pasado la validación, verá un botón Crear. Haga clic en el botón **Crear** para comenzar la implementación de su nueva VM.

Más información **Cómo Azure implementa su VM**

Cuando hace clic en Crear para crear su VM, el portal de Azure está usando una plantilla ARM para implementar su VM. Esa plantilla ARM contiene parámetros que se reemplazan con la información que ingresó para su VM. Cada máquina virtual que se crea en Azure se crea con una plantilla ARM. Esto asegura que las implementaciones sean consistentes.

A medida que se implemente su VM, verá el estado que se muestra en Azure Portal como se muestra en la Figura 10-10. Puede ver los recursos de Azure que se crean para admitir su VM. Puede ver el nombre del recurso, el tipo de recurso (que comienza con el proveedor de recursos) y el estado de cada recurso.

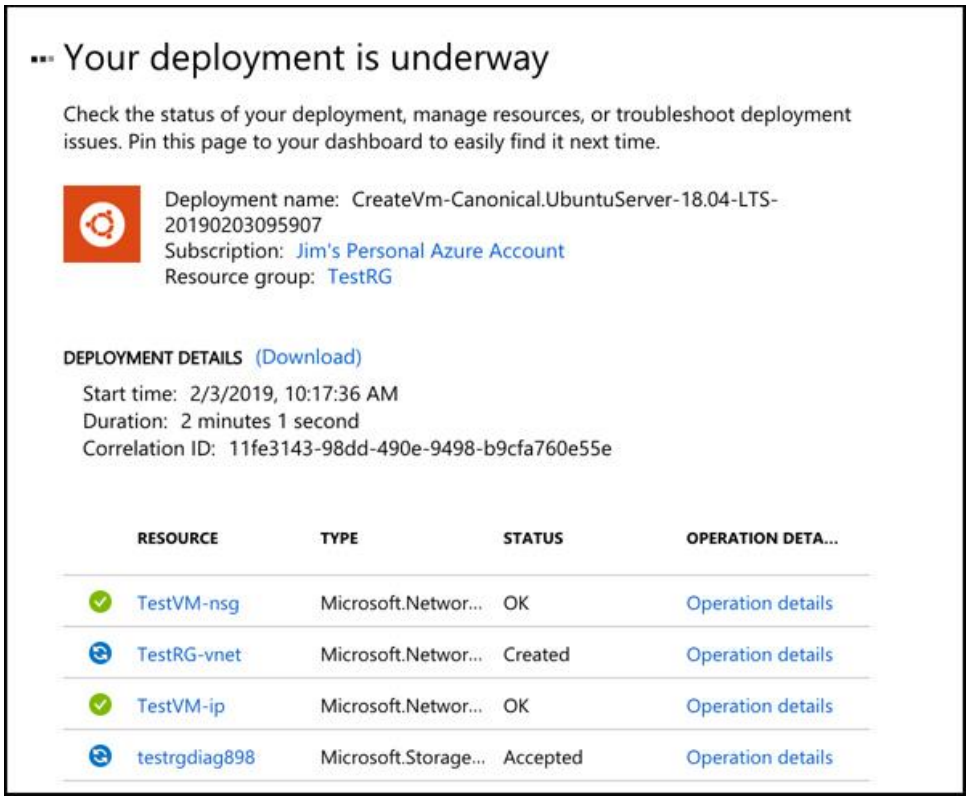


Figura 2-10 Configuración de máquina virtual

Una vez que se hayan creado todos los recursos necesarios para su VM, su VM se considerará completamente implementada. Luego podrá hacer clic en el botón **Ir a recursos** para ver la interfaz de administración de su VM en Azure Portal como se muestra en la Figura 2-11 .

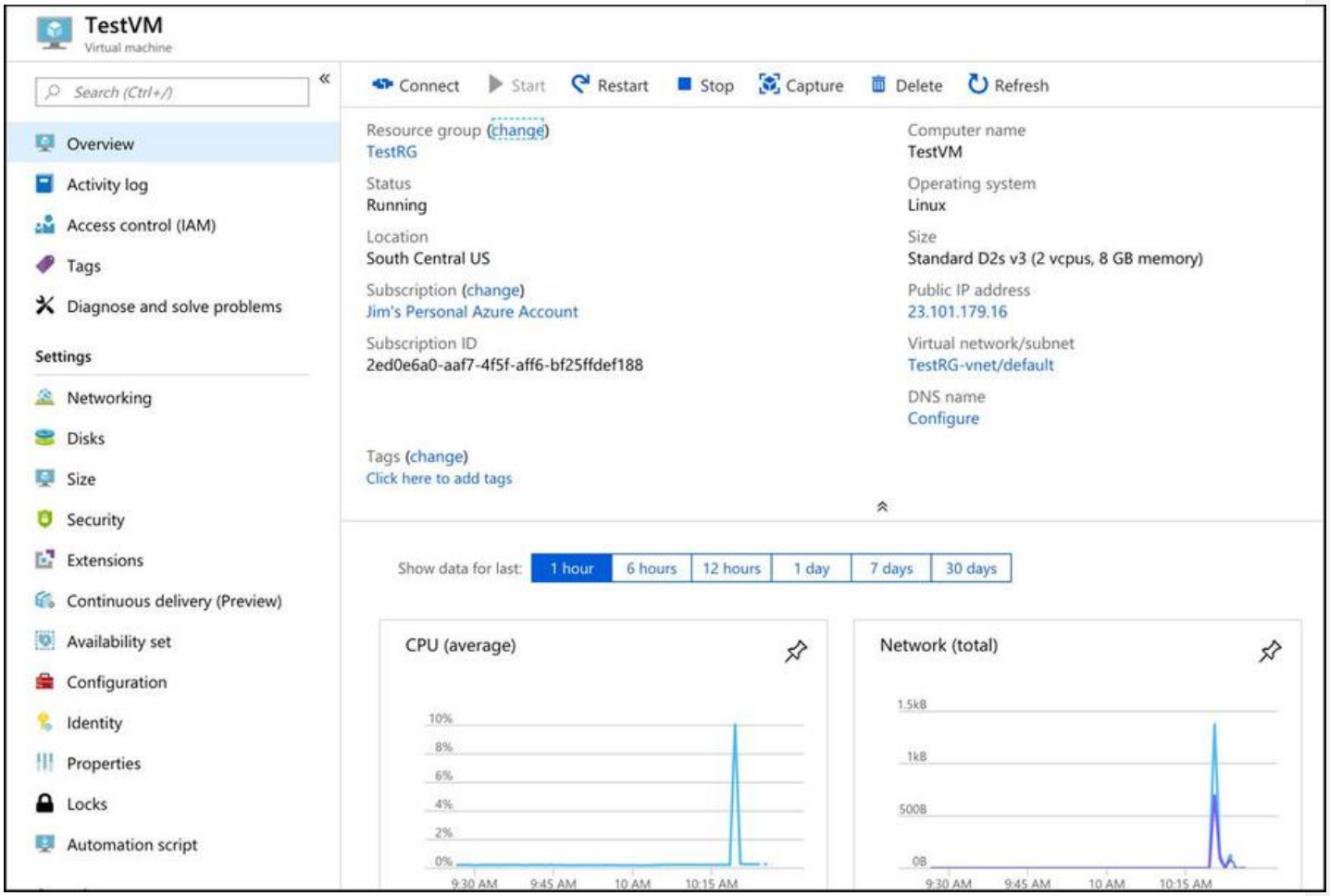


Figura 2-11 Visualización de una máquina virtual

Nuestra nueva máquina virtual es un invitado en una computadora física con un centro de datos de Azure. En ese centro de datos hay un bastidor físico de servidores de computadora, y nuestra VM está alojada en uno de esos servidores. Microsoft administra la computadora host, pero usted administra la VM, porque esta es una oferta de IaaS en Azure.

Tenga en cuenta las **máquinas virtuales y la facturación**

Se le cobrará por las máquinas virtuales de Azure mientras se estén ejecutando. Para detener la facturación de esta VM, haga clic en el botón Detener en la parte superior de la pantalla que se muestra en la Figura 2-11 . Azure guardará el estado actual de la VM y la facturación se detendrá. No podrá usar la VM mientras está en estado detenido, pero también evitará la facturación de esa VM. Tenga en cuenta que, a menos que haya configurado una dirección IP estática para su VM, es probable que su dirección IP cambie la próxima vez que la inicie.

También puede detener una máquina virtual desde el sistema operativo invitado en la máquina virtual, pero cuando lo haga, aún se le cobrarán los recursos que utiliza la máquina virtual porque todavía está asignada a usted. Eso significa que aún incurrirá en cargos por discos administrados y otros recursos.

A partir de ahora, esta máquina virtual es susceptible al tiempo de inactividad debido a tres tipos de eventos: *el mantenimiento planificado* , *mantenimiento no planificado* , y *el tiempo de inactividad inesperado* .

El mantenimiento planificado se refiere a las actualizaciones planificadas que Microsoft realiza en la computadora host. Esto incluye cosas como actualizaciones del sistema operativo, actualizaciones de controladores, etc. En muchos casos, las actualizaciones no afectarán su VM, pero si Microsoft instala una actualización que requiere un reinicio de la computadora host, su VM estará inactiva durante ese reinicio.

Azure tiene sistemas subyacentes que monitorean constantemente el estado de los componentes de la computadora. Si uno de estos sistemas subyacentes detecta que un componente dentro de la computadora host podría fallar pronto, Azure marcará la computadora por mantenimiento no planificado. En un evento de mantenimiento no planificado, Azure intentará mover su VM a una computadora host en buen estado. Cuando hace esto, conserva el estado de la VM, incluido lo que hay en la memoria y los archivos que están abiertos. A Azure solo le lleva poco tiempo mover la VM, tiempo durante el cual está en estado de pausa. En caso de que falle la operación de movimiento, la VM experimentará un tiempo de inactividad inesperado.

Para garantizar la confiabilidad cuando ocurre una falla en un rack dentro del centro de datos de Azure, puede (y debe) aprovechar una característica llamada *conjuntos de disponibilidad* . Los conjuntos de disponibilidad lo protegen de eventos de mantenimiento y tiempos de inactividad causados por fallas de hardware. Para hacer eso, Azure crea algunas entidades subyacentes en un conjunto de disponibilidad llamado *dominios de actualización* y *dominios de falla* . (Para protegerse en caso de eventos de mantenimiento o tiempo de inactividad, debe implementar al menos dos máquinas virtuales en la transposición del conjunto de disponibilidad).

Los dominios de falla son una representación lógica del bastidor físico en el que está instalada una computadora host. De manera predeterminada, Azure asigna dos dominios de falla a un conjunto de disponibilidad. Si se produce un problema en un dominio de falla (un rack de computadora), las VM en ese dominio de falla se verán afectadas, pero las VM en el segundo dominio de falla no lo serán. Esto lo protege de eventos de mantenimiento no planificados y tiempos de inactividad inesperados.

Los dominios de actualización están diseñados para protegerlo de una situación en la que se reinicia la computadora host. Cuando crea un conjunto de disponibilidad, Azure crea cinco dominios de actualización de forma predeterminada. Estos dominios de actualización

se distribuyen entre los dominios de falla en el conjunto de disponibilidad. Si se requiere reiniciar en computadoras en el conjunto de disponibilidad (ya sean computadoras host o máquinas virtuales dentro del conjunto de disponibilidad), Azure solo reiniciará computadoras en un dominio de actualización a la vez y esperará 30 minutos para que las computadoras se recuperen del reinicio antes de pasa al siguiente dominio de actualización. Los dominios de actualización lo protegen de los eventos de mantenimiento planificados.

La Figura 2-12 muestra el diagrama que Microsoft usa para representar un conjunto de disponibilidad. En este diagrama, los dominios de falla FD0, FD1 y FD2 abarcan tres bastidores físicos de computadoras. UD0, UD1 y UD2 son dominios de actualización dentro de los dominios de falla. Verá esta misma representación de un conjunto de disponibilidad dentro de otra capacitación de Azure, pero es un poco engañoso porque los dominios de actualización no están vinculados a un dominio de falla particular.

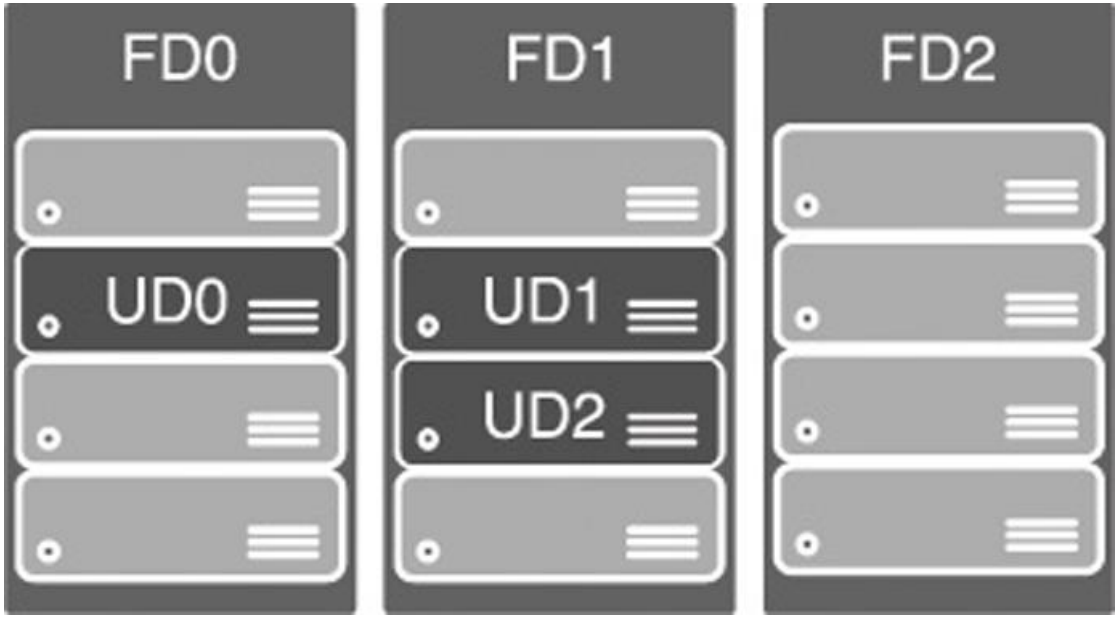


Figura 2-12 Representación de documentación de Microsoft de un conjunto de disponibilidad

La Figura 2-13 muestra una mejor representación de un conjunto de disponibilidad, con cinco máquinas virtuales en el conjunto de disponibilidad. Hay dos dominios de falla y tres dominios de actualización. Cuando se crearon máquinas virtuales en este conjunto de disponibilidad, se asignaron de la siguiente manera:

- A la primera máquina virtual se le asigna Fault Domain 0 y Update Domain 0.
- A la segunda VM se le asigna Fault Domain 1 y Update Domain 1.
- A la tercera VM se le asigna Fault Domain 0 y Update Domain 2.
- A la cuarta VM se le asigna Fault Domain 1 y Update Domain 0.
- A la quinta máquina virtual se le asigna Fault Domain 0 y Update Domain 1.

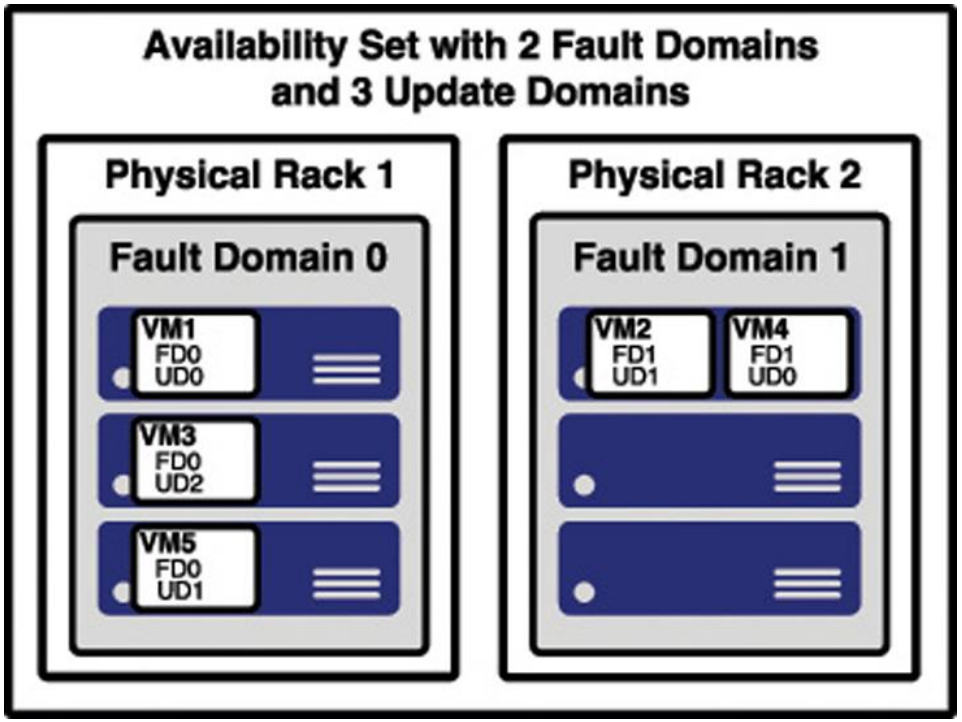


Figura 2-13 Una mejor representación de un conjunto de disponibilidad

Puede verificar la ubicación de los dominios de falla y actualizar los dominios creando cinco máquinas virtuales en un conjunto de disponibilidad con dos dominios de falla y tres dominios de actualización. Si observa el conjunto de disponibilidad creado en Azure Portal como se muestra en la Figura 2-14 , puede ver la misma configuración que se muestra en la Figura 2-13 .

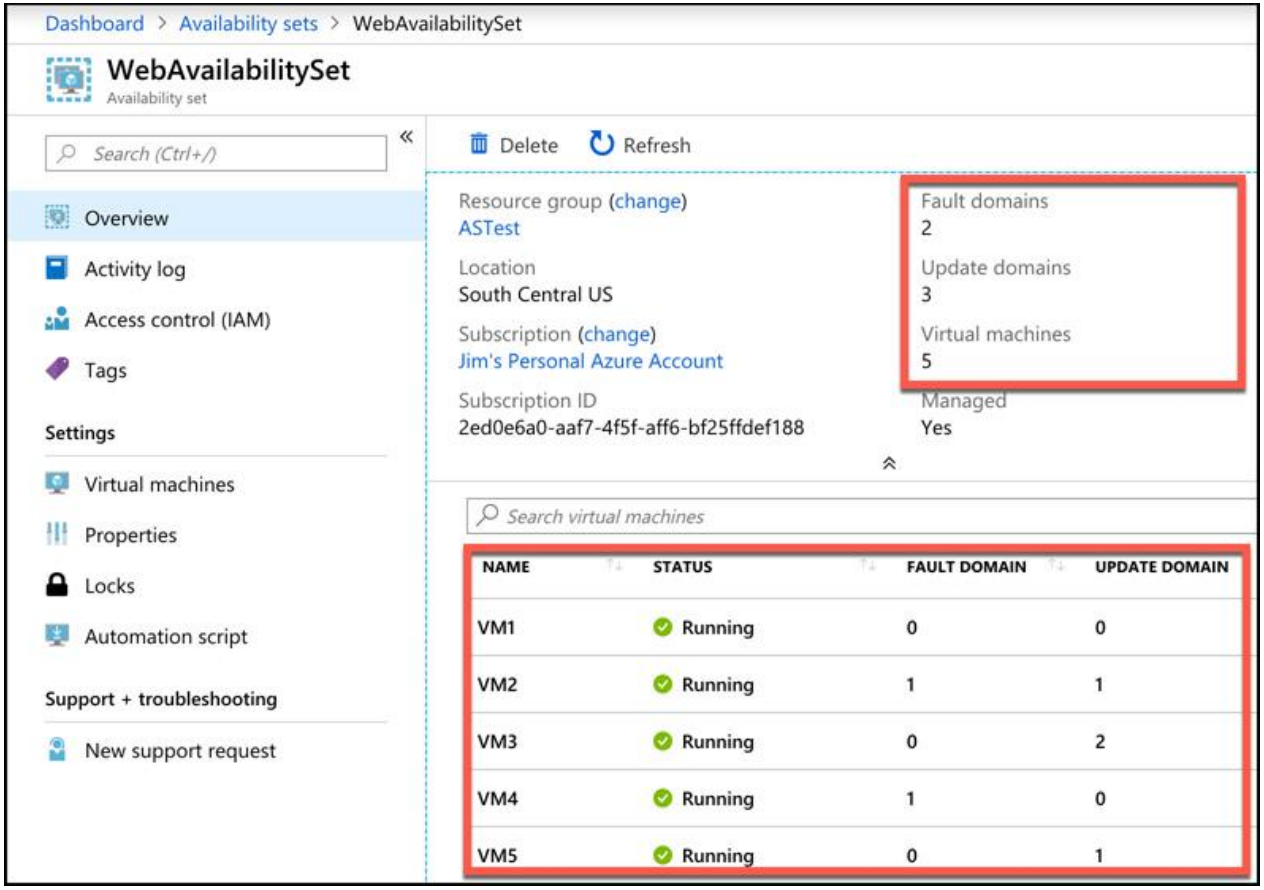


Figura 2-14 Un conjunto de disponibilidad en Azure Portal que muestra dominios de falla y dominios de actualización

Observe en la Figura 2-14 que el conjunto de disponibilidad se denomina WebAvailabilitySet. En este conjunto de disponibilidad, ejecutamos cinco máquinas virtuales que ejecutan un servidor web y alojan el sitio web para una aplicación. Suponga que necesita una base de datos para esta aplicación y desea alojar esa base de datos también en máquinas virtuales. En esa situación, desearía separar las máquinas virtuales de la base de datos en su propio conjunto de disponibilidad. Como práctica recomendada, siempre debe separar sus cargas de trabajo en conjuntos de disponibilidad separados.

Los conjuntos de disponibilidad ciertamente brindan un beneficio en la protección contra el tiempo de inactividad en ciertas situaciones, pero también tienen algunas desventajas. En primer lugar, cada máquina en un conjunto de disponibilidad debe crearse explícitamente. Si bien puede usar una plantilla ARM para implementar múltiples máquinas virtuales en una sola implementación, aún tiene que configurar esas máquinas con el software y la configuración necesarios para admitir su aplicación.

Un conjunto de disponibilidad también requiere que configure algo delante de sus máquinas virtuales que manejará la distribución del tráfico a esas máquinas virtuales. Por ejemplo, si su conjunto de disponibilidad está prestando servicio a un sitio web alojado en las máquinas virtuales, deberá configurar un equilibrador de carga que se encargará de enrutar a los usuarios de su sitio web a las máquinas virtuales que lo ejecutan.

Otra desventaja de los conjuntos de disponibilidad se relaciona con el costo. En una situación en la que sus necesidades de VM cambian a menudo en función de cosas como la carga en la aplicación, es posible que pague por muchas más VM de las que necesita.

Azure ofrece otra característica para las máquinas virtuales llamada *conjuntos de escalas* que resuelve estos problemas muy bien. Cuando crea un conjunto de escalas, le dice a Azure qué sistema operativo desea ejecutar y luego le dice a Azure cuántas máquinas virtuales desea en su conjunto de escalas. Tiene muchas otras opciones, como crear un equilibrador de carga o puerta de enlace, etc. Azure creará tantas máquinas virtuales como haya especificado (hasta 1,000) en un simple paso.

Más información **usando una imagen personalizada**

El conjunto predeterminado de plantillas para máquinas virtuales es básico e incluye solo el sistema operativo. Sin embargo, puede crear una VM, instalar todos los componentes necesarios que necesita (incluidas sus propias aplicaciones) y luego crear una imagen que se pueda usar al crear conjuntos de escalas.

Para obtener más información sobre el uso de imágenes personalizadas, consulte: *https://docs.microsoft.com/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-deploy-app#build-a-custom-vm- imagen* .

Los conjuntos de escalas se implementan en conjuntos de disponibilidad automáticamente, por lo que se beneficia automáticamente de múltiples dominios de falla y dominios de actualización. Sin embargo, a diferencia de las máquinas virtuales en un conjunto de disponibilidad, las máquinas virtuales en un conjunto de escala también son compatibles con las zonas de disponibilidad, por lo que está protegido contra problemas en un centro de datos de Azure.

Como puede imaginar, también puede escalar un conjunto de escalas en una situación en la que necesita más o menos máquinas virtuales. Puede comenzar con solo una máquina virtual en un conjunto de escalado, pero a medida que aumenta la carga en esa máquina virtual, es posible que desee agregar máquinas virtuales adicionales automáticamente. Los conjuntos de escalas proporcionan esa funcionalidad mediante el uso de la función de escala automática de Azure. Defina reglas de escala que utilicen métricas como CPU, uso de disco, uso de red, etc. Puede configurar cuándo Azure debe agregar instancias adicionales y cuándo debe reducir y desasignar instancias. Esta es una excelente manera de garantizar la disponibilidad y, al mismo tiempo, reducir los costos aprovechando la elasticidad que proporciona la escala automática.

Más información **Escala y conjuntos de disponibilidad**

Antes de la introducción de conjuntos de escalas, tenía la capacidad de configurar reglas de escala automática para un conjunto de disponibilidad. Probablemente todavía verá documentación y capacitación de terceros que habla sobre los conjuntos de disponibilidad de escalado, pero esa funcionalidad ha sido reemplazada por conjuntos de escalado.

Microsoft garantiza un SLA del 99.95% cuando utiliza un escenario de implementación de varias máquinas virtuales, y para la mayoría de los escenarios de producción, se prefiere una implementación de varias máquinas virtuales. Sin embargo, si usa una VM de instancia única y usa almacenamiento premium, Microsoft garantiza un SLA del 99.9%. El almacenamiento premium utiliza unidades de estado sólido (SSD) que se encuentran en el mismo servidor físico que aloja la VM para mejorar el rendimiento y el tiempo de actividad.

Contenedores en Azure

Se está volviendo bastante común que las empresas muevan aplicaciones entre "entornos", y este tipo de cosas es aún más frecuente cuando se trata de la nube. De hecho, uno de los aspectos más complejos de mudarse a la nube es lidiar con las complejidades de mudarse a un nuevo entorno. Para ayudar con este problema y facilitar el cambio de aplicaciones a nuevos entornos, se inventó el concepto de *contenedores* .

Un contenedor se crea usando una versión comprimida de una aplicación llamada *imagen* , e incluye todo lo que la aplicación necesita para ejecutarse. Eso podría incluir un motor de base de datos, un servidor web, etc. La imagen se puede implementar en cualquier entorno que admita el uso de contenedores. Una vez allí, la imagen se usa para iniciar un contenedor en el que se ejecuta la aplicación.

Para ejecutar una aplicación en un contenedor, una computadora necesita tener un tiempo de ejecución de contenedor instalado. El tiempo de ejecución de contenedores más popular es Docker, un tiempo de ejecución desarrollado y mantenido por una compañía llamada Docker Inc. Docker no solo sabe cómo ejecutar aplicaciones en contenedores, sino que también impone ciertas condiciones para garantizar un entorno seguro.

Más información **Docker Images**

No estás limitado a tus propias imágenes. De hecho, Docker ejecuta un repositorio de imágenes que puede usar libremente en sus propias aplicaciones. Puede encontrarlo en: *https://hub.docker.com* .

Cada contenedor opera dentro de un entorno aislado. Tiene su propia red, su propio almacenamiento, etc. Otros contenedores que se ejecutan en la misma máquina no pueden acceder a los datos y sistemas utilizados por otro contenedor. Esto hace que las aplicaciones en contenedores sean una solución ideal cuando la seguridad es una preocupación.

Azure ofrece numerosas tecnologías para hospedar contenedores. Azure Container Instances (ACI) es un servicio de PaaS que facilita el inicio de un contenedor con una configuración mínima. Simplemente le dice a ACI dónde encontrar la imagen (usando una etiqueta Docker o una URL para la imagen) y alguna configuración básica para la VM en la que desea que se ejecute el contenedor.

Azure crea recursos del servidor según sea necesario para ejecutar su contenedor, pero no está pagando por una VM subyacente. En cambio, paga por la memoria y la CPU que utiliza su contenedor. Eso se traduce en costos extremadamente bajos en la mayoría de los casos. Por ejemplo, si su aplicación ACI se ejecuta en una máquina con 1 CPU y 1 GB de memoria y usa la aplicación durante 5 minutos al día, al final del mes, ¡su costo sería inferior a 5 centavos!

***Los* contenedores de *notas* usan su propio sistema operativo**

El sistema operativo para un contenedor es en realidad parte de la imagen. La VM que está configurando cuando crea una aplicación ACI es la VM que ejecuta el tiempo de ejecución del contenedor. Aun así, es importante que elija un sistema operativo que sea compatible con su contenedor. Una imagen de Docker que se creó para Linux no se ejecutará en un host de Windows y viceversa.

ACI está diseñado para trabajar con aplicaciones simples. Puede definir un grupo de contenedores y ejecutar varios contenedores dentro de una instancia de ACI, pero si tiene una aplicación que los usuarios utilizan muchomuchas personas y que tal vez necesiten aprovechar la escala, ACI no es una buena opción para usted. En cambio, el Servicio Kubernetes de Azure (AKS) sería una mejor opción.

Kubernetes es un servicio de orquestación de contenedores. Esto significa que es responsable de monitorear los contenedores y garantizar que siempre estén funcionando. También puede escalar para agregar contenedores adicionales cuando las necesidades lo requieran, y luego puede volver a escalar cuando las necesidades se reduzcan.

Kubernetes crea contenedores en una *vaina* . Un pod es un grupo de contenedores relacionados, y los contenedores dentro de un pod pueden compartir recursos. Esta es una de las ventajas de usar Kubernetes, ya que lo libera de la restricción de uso compartido de recursos que generalmente se impone en un entorno de contenedores múltiples. Sin embargo, un contenedor en un pod no puede compartir recursos con un contenedor en otro pod.

La computadora en la que se ejecutan los pods de Kubernetes se llama *nodo* o *trabajador* . Esta computadora debe tener un tiempo de ejecución de contenedor como Docker ejecutándose en ella. Además de los pods, el nodo también ejecuta varios servicios necesarios para que Kubernetes administre los pods, y así sucesivamente. Habitualmente habrá múltiples nodos dentro de una instancia de Kubernetes, y todos están controlados por un nodo maestro llamado *maestro de* Kubernetes . Todo el entorno del maestro y todos sus nodos se denomina *clúster de* Kubernetes .

Un maestro de Kubernetes contiene toda la configuración y los servicios necesarios para administrar la orquestación de pods y otras entidades de Kubernetes. Configurar un maestro puede ser complejo, y es, con mucho, la tarea más laboriosa de usar Kubernetes. Por esa razón, servicios como Azure Kubernetes Service (AKS) se están volviendo más populares.

AKS descarga la carga de tratar con el maestro Kubernetes a Microsoft. Cuando crea un clúster de Kubernetes en AKS, Azure crea el maestro y los nodos por usted. Todo lo que tiene que hacer es implementar sus contenedores, y estará en funcionamiento con un clúster de Kubernetes administrado.

AKS simplifica la creación de un clúster de Kubernetes, pero también hace que sea extremadamente fácil administrar un clúster (consulte la Figura 2-15). Las operaciones, como actualizar un clúster o escalar un clúster, son simples usando las opciones del menú de Azure Portal. También puede obtener información detallada sobre su clúster, incluido cada nodo que se ejecuta en el clúster.

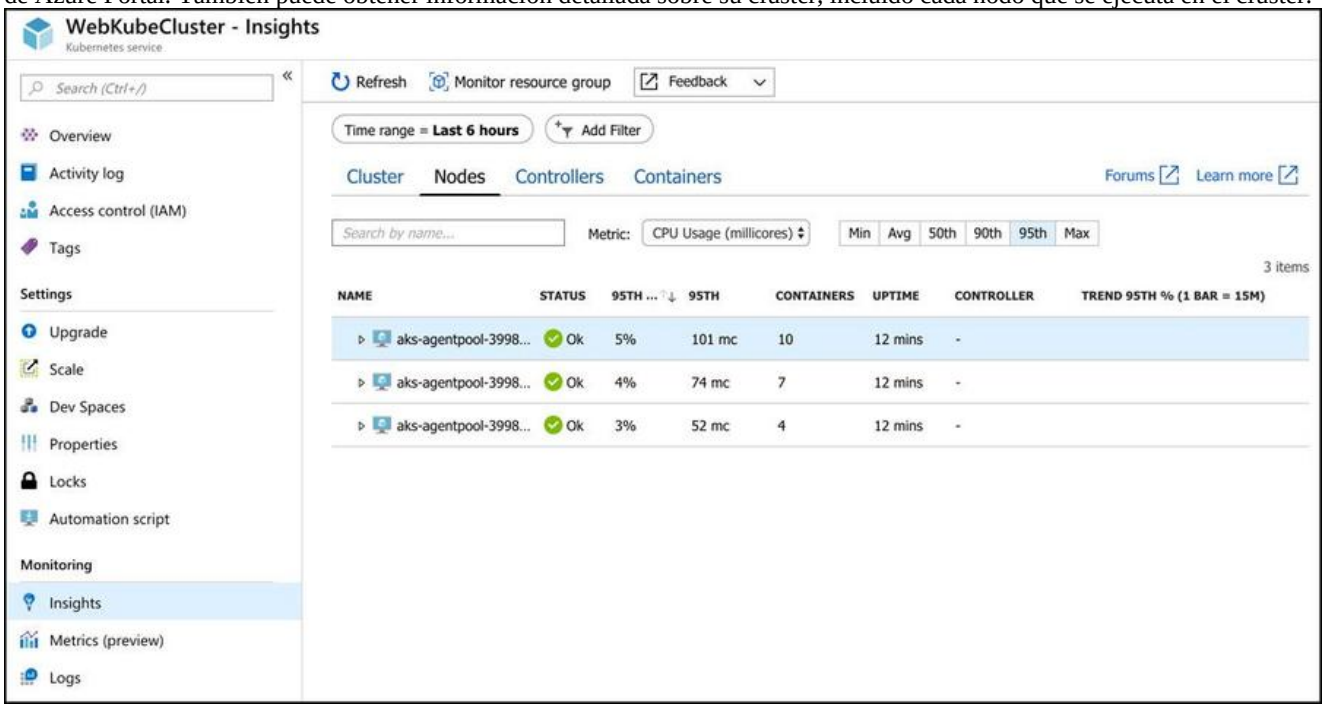


Figura 2-15 Un clúster AKS en Azure Portal

Si bien AKS facilita la adopción y administración de Kubernetes, no ofusca completamente a Kubernetes. Para implementar sus aplicaciones, aún necesita entender cómo usar Kubernetes, y en algunos casos necesitará usar la línea de comando de Kubernetes. Sin embargo, Azure lo hace mucho más fácil que hacer todo el trabajo de campo y el mantenimiento usted mismo. Aún mejor, AKS en Azure es gratis. Solo paga por la computadora Azure por los recursos que usa dentro de su clúster.

Para una verdadera experiencia de PaaS en alojamiento de contenedores, Microsoft ofrece Web App for Containers, una característica del Servicio de aplicaciones de Azure. Cuando crea una aplicación de aplicación web para contenedores, especifica el sistema operativo que desea (Windows o Linux) y especifica la ubicación de la imagen de Docker (consulte la Figura 2-16). La imagen puede estar en Docker Hub, un registro privado o en Azure Container Services.

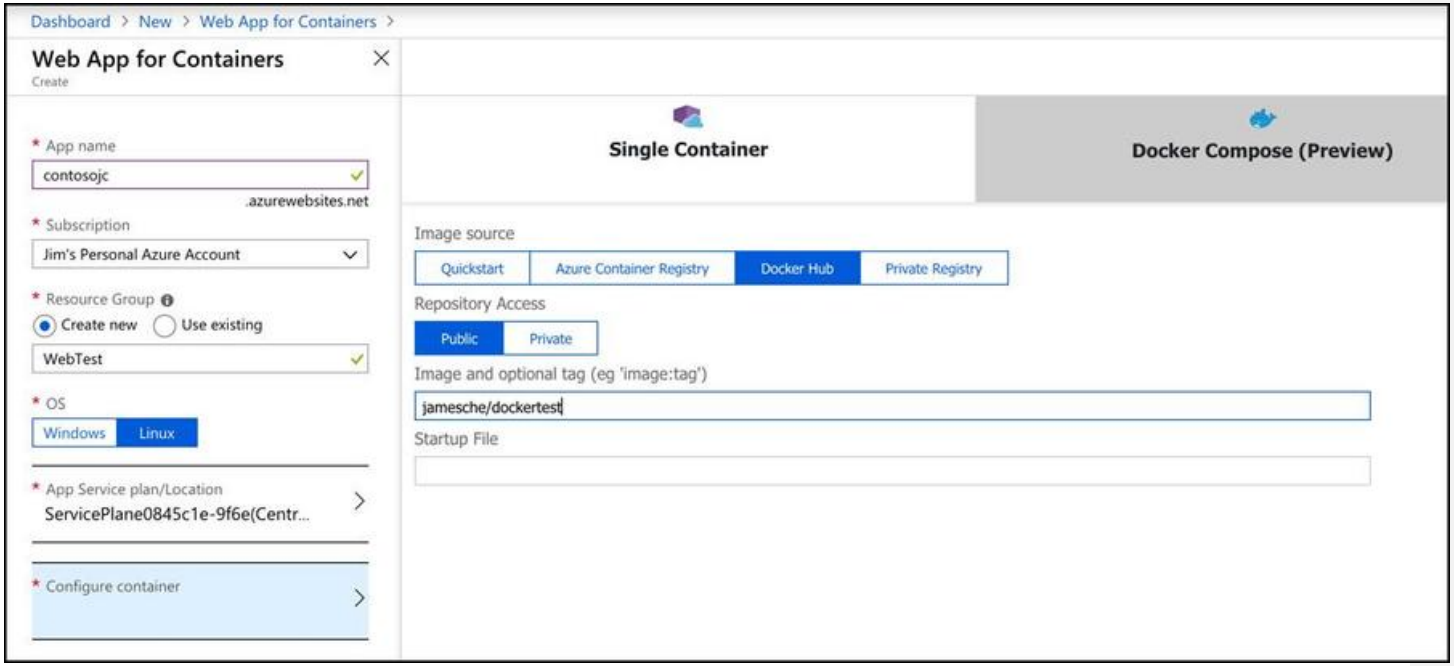


Figura 2-16 Creación de una aplicación web para la aplicación Contenedores

Los contenedores que se ejecutan en la aplicación web para contenedores disfrutan de los beneficios de todas las características de PaaS de Azure App Service. Microsoft administra la infraestructura que está involucrada, por lo que solo debe preocuparse por la aplicación contenida en la imagen.

A diferencia de ACI, paga por el Servicio de aplicaciones de Azure, ya sea que esté utilizando la aplicación o no, porque su aplicación se ejecuta en una VM dedicada en el Servicio de aplicaciones. Esa VM está asociada con un plan de App Service, y cada plan de App Service está asociado con un nivel de precios específico. Puede cambiar el nivel de precios de su Plan de servicio de aplicaciones en cualquier momento. Por ejemplo, si decide que su aplicación necesita más memoria de la que pensaba, puede escalar a un nivel superior y obtener más memoria. App Service se encarga de mover su aplicación a la nueva VM.

App Service también facilita el escalado mediante el uso de la escala automática de Azure. Al igual que escalar un conjunto de escalado de VM, puede especificar métricas que se utilizan para determinar cuándo escalar su aplicación. Sin embargo, tenga en cuenta que paga por cada VM que usa, por lo que si escala a una gran cantidad de VM, verá una factura igualmente grande al final del mes.

Otro beneficio de usar la aplicación web para contenedores es que, debido a que es un verdadero servicio PaaS, ofrece muchas características llave en mano que puede usar en su aplicación sin tener que lidiar con problemas complicados de desarrollo o configuración. Por ejemplo, si desea aplicar la autenticación en su aplicación y desea que los usuarios puedan usar su cuenta de Microsoft,Las credenciales de inicio de sesión de Facebook, Twitter o Google, puede configurarlo fácilmente con la autenticación del Servicio de aplicaciones como se muestra en la Figura 2-17 .

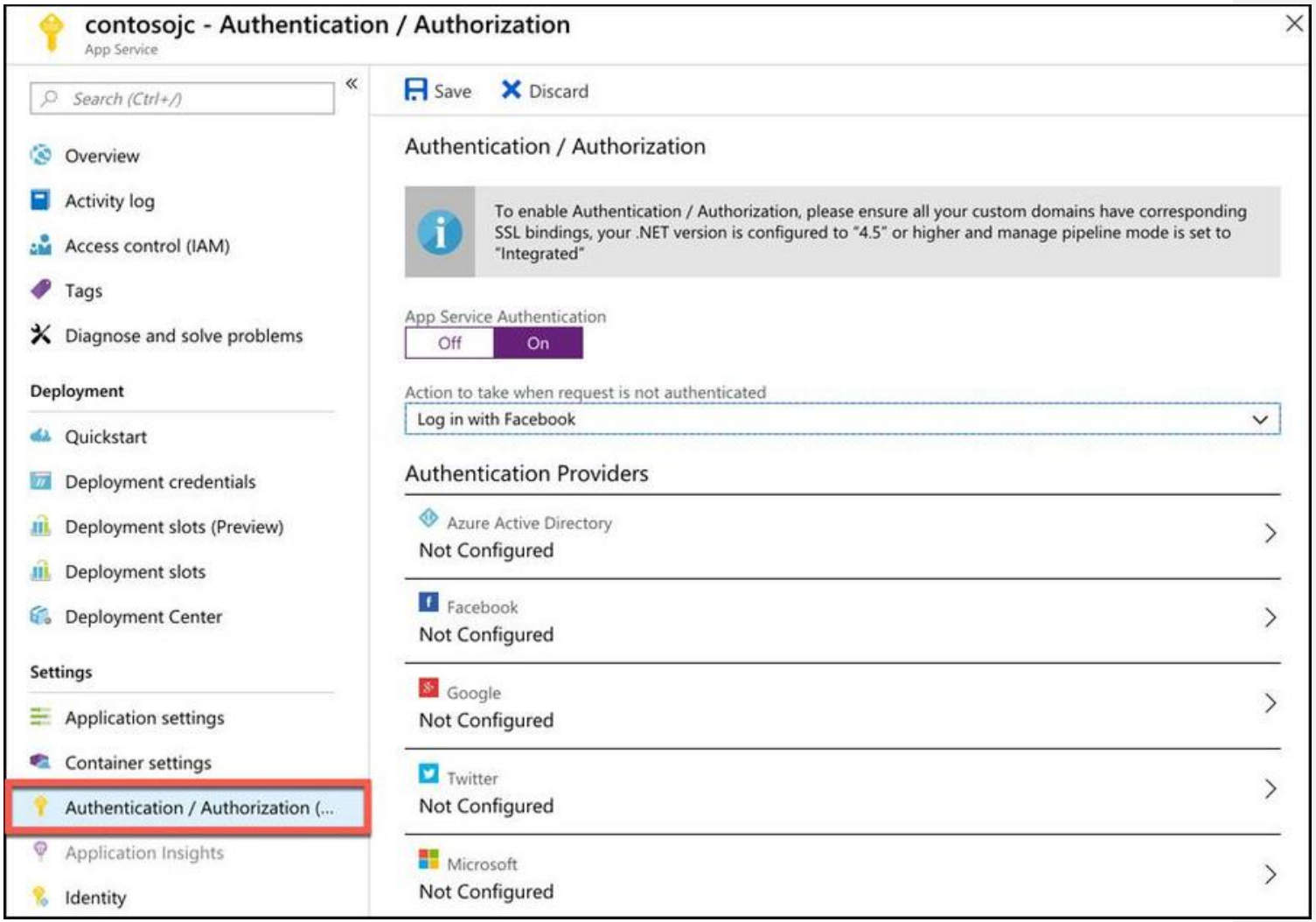


Figura 2-17 Configuración de autenticación para la aplicación web para contenedores

Productos de red de Azure

Las aplicaciones en Azure casi siempre están compuestas por múltiples servicios de Azure que trabajan juntos. A pesar de que estos servicios múltiples dependen unos de otros para que la aplicación funcione, no deben integrarse estrechamente. En cambio, las aplicaciones deberían diseñarse utilizando una *arquitectura débilmente acoplada* .

En una arquitectura débilmente acoplada, cada componente de una aplicación se puede reemplazar o actualizar sin interrumpir la aplicación. Para diseñar aplicaciones de esta manera, debe separar los distintos componentes y ellos deben operar en su propio nivel de la aplicación. Es esta separación de componentes lo que le permite ser más flexible en los detalles de implementación de su aplicación, y es un componente crítico para una aplicación diseñada para la nube. Las aplicaciones diseñadas de esta manera se denominan aplicaciones de *N niveles* .

 ***Consejo de examen***

El examen AZ-900 no es un examen para desarrolladores, por lo que no entraremos en ningún nivel de detalle sobre el diseño de la aplicación. Sin embargo, es importante que comprenda el concepto de aplicaciones de varios niveles para que comprenda por qué las funciones de red de Azure funcionan de la manera en que lo hacen.

Suponga que tiene una aplicación que registra los datos de ventas de su empresa. Los usuarios ingresan sus registros de ventas, y la aplicación realiza un análisis de ellos, y luego almacena la información en una base de datos. La aplicación utiliza tres niveles: un nivel web, un nivel medio y un nivel de datos.

El nivel web es un sitio web que se ejecuta en Azure App Service. Está ahí solo para darle al usuario una forma de interactuar con la aplicación. No maneja ninguna lógica. Simplemente toma lo que el usuario ingresa y lo pasa al nivel medio donde el trabajo realmente sucede.

El nivel medio (o nivel de aplicación) es donde existe toda la lógica de la aplicación. Aquí es donde la aplicación analiza los datos de ventas en busca de tendencias y le aplica las reglas de negocio mientras se ejecuta en una máquina virtual de Azure. El nivel de datos es donde almacena los datos de ventas, pero el nivel medio también puede recuperar datos de ventas cuando necesita mostrar informes. El nivel de datos consta de una base de datos SQL Azure. La Figura 2-18 muestra un diagrama de la aplicación.

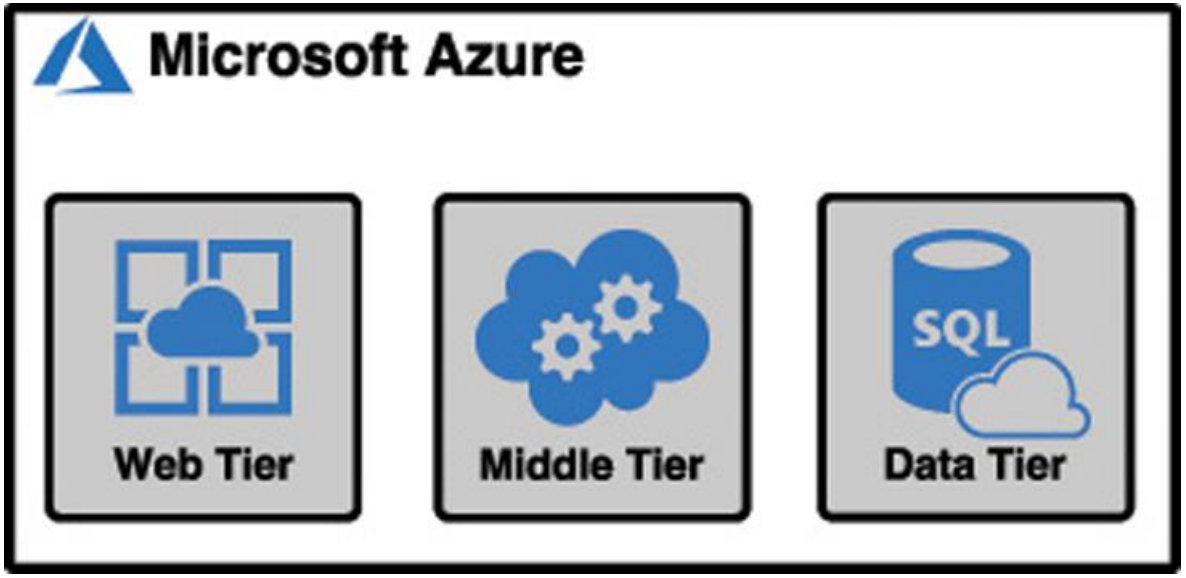


Figura 2-18 Un ejemplo de una aplicación de n niveles.

Aquí hay algunos requisitos para esta aplicación.

- Solo el nivel web puede hablar desde y hacia Internet.
- El nivel web puede hablar con el nivel medio, pero no puede hablar con el nivel de datos.
- El nivel medio puede hablar desde y hacia el nivel web y el nivel de datos.
- El nivel de datos puede hablar desde y hacia el nivel medio, pero no puede hablar con el nivel web.

Estos requisitos son típicos para un diseño de N niveles y ayudan a mantener los datos seguros y a prevenir problemas de seguridad con la aplicación. Dado que cada uno de estos niveles se ejecuta en un servicio de Azure separado, no pueden comunicarse entre sí de manera predeterminada. Para comunicarse entre los niveles de su aplicación, necesita una red informática, y ahí es donde entran en juego los productos de red de Azure.

Red virtual de Azure

Una red virtual de Azure (a menudo llamada VNET) permite que los servicios de Azure se comuniquen entre sí y con Internet. Incluso puede usar una red virtual para comunicarse entre sus recursos locales y sus recursos de Azure. Cuando creó la máquina virtual

anteriormente en este capítulo, Azure creó una red virtual para usted. Sin esa red virtual, no podría controlaren la VM, o use la VM para cualquiera de sus aplicaciones. También puede crear su propio VNET y configurarlo de la forma que elija.

Una Azure VNET es como cualquier otra red informática. Se compone de una tarjeta de interfaz de red (una NIC), direcciones IP, etc. Puede dividir su VNET en varias subredes y configurar una parte del espacio de direcciones IP de su red para esas subredes. Luego puede configurar reglas que controlen la conectividad entre esas subredes.

La Figura 2-19 ilustra un Azure VNET que podríamos usar para la aplicación de ventas. La red virtual utiliza direcciones IP en el rango de direcciones 10.0.0.0 y cada subred tiene su propio rango de direcciones. Los rangos de direcciones IP en las redes virtuales se especifican utilizando la notación de enrutamiento entre dominios sin clase (CIDR), y una discusión al respecto está muy fuera del alcance de este examen. Sin embargo, con la configuración que se muestra en la Figura 2-19, tenemos 65.536 direcciones IP disponibles en nuestra red virtual y cada subred tiene 256 direcciones IP asignadas. (Las primeras cuatro direcciones IP y la última dirección IP en el rango están reservadas para el uso de Azure, por lo que realmente solo tiene 251 direcciones para usar en cada subred). Este es un diseño típico porque todavía tiene una gran cantidad de direcciones disponibles en su red para su posterior expansión en subredes adicionales.

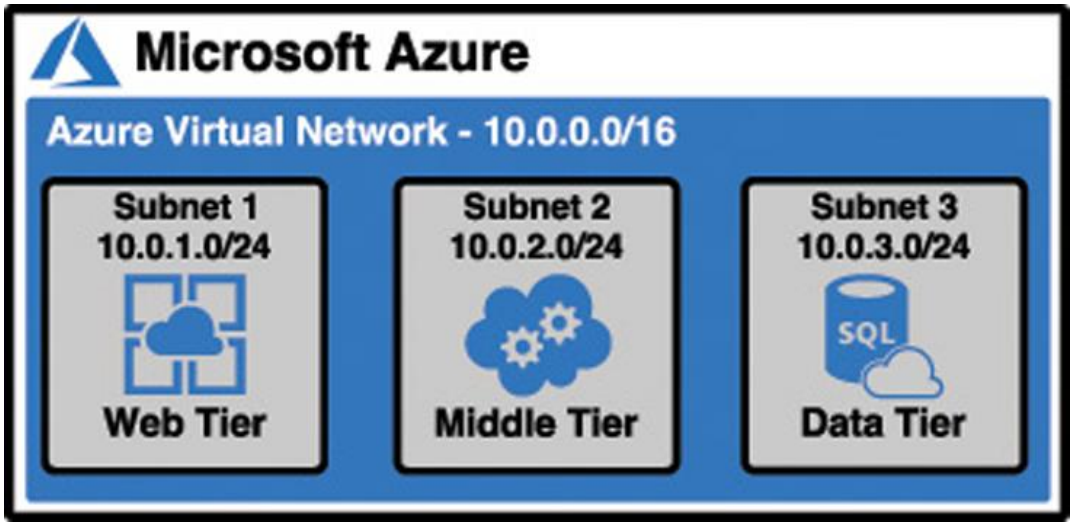


Figura 2-19 Su aplicación en una red virtual de Azure

En la mayoría de los casos, crea redes virtuales antes de crear los recursos que las utilizan. Si regresa y mira la Figura 2-10 , verá que Azure ha creado automáticamente un VNET para la VM. Lo hace porque no puede usar una VM a menos que haya una red asociada a

ella. Si bien puede conectar una red virtual a una máquina virtual existente, no puede mover una máquina virtual a otra red. Por esa razón, crea su VNET antes de crear su VM.

Nuestro nivel web, por otro lado, se ejecuta en Azure App Service, una oferta de PaaS. Esto se ejecuta en una VM que administra Microsoft, por lo que Microsoft ha creado y administra la VM y su red. Para usar ese nivel con el VNET, el Servicio de aplicaciones ofrece una característica llamada Integración de VNET que le permite integrar una aplicación web en el Servicio de aplicaciones con un VNET existente.

Las direcciones IP dentro de la red virtual en este punto son todas direcciones IP privadas. Permiten que los recursos dentro de la red virtual se comuniquen entre sí, pero no puede usar una dirección IP privada en Internet. Necesita una dirección IP pública para dar acceso a Internet a su nivel web.

Más información **Conectividad de Internet saliente**

No es necesario asignar una dirección IP pública a un recurso para que ese recurso se conecte saliente a Internet. Azure mantiene un grupo de direcciones IP públicas que pueden asignarse dinámicamente a un recurso si necesita conectarse al saliente. Esa dirección IP no se asigna exclusivamente al recurso, por lo que no se puede usar para la comunicación entrante de Internet al recurso de Azure.

Dado que el nivel web se ejecuta en Azure App Service (un servicio PaaS), Microsoft administra la red pública por nosotros. Obtiene acceso a Internet en ese nivel sin tener que hacer nada. Si desea ejecutar el nivel web en una máquina virtual IaaS, configure la dirección IP pública para el nivel web. En esas situaciones, Azure le permite crear un recurso de Dirección IP pública y asignarlo a una red virtual.

Más información **Grupos de seguridad de red**

Azure ofrece una característica llamada Grupos de seguridad de red que le permite aplicar reglas sobre qué tipo de tráfico está permitido en la red virtual. Cubriremos los Grupos de seguridad de red en el Capítulo 3 , " Comprender la seguridad, la privacidad, el cumplimiento y la confianza ".

Balanceador de carga azul

Es fácil escalar el nivel web en nuestra aplicación de ventas cuando es necesario. App Service se encarga de garantizar que la carga se distribuya en todas las máquinas virtuales que estamos utilizando. App Service utiliza un equilibrador de carga para hacer esto, y una de las ventajas de elegir una oferta de PaaS para el nivel web es que no tiene que preocuparse por administrarlo. Si usa una máquina virtual IaaS que ejecuta un servidor web para el nivel web, es posible que desee tener más de una máquina virtual para manejar la carga adicional si es necesario. La Figura 2-20 representa el aspecto que podría tener el nivel web utilizando un modelo IaaS.

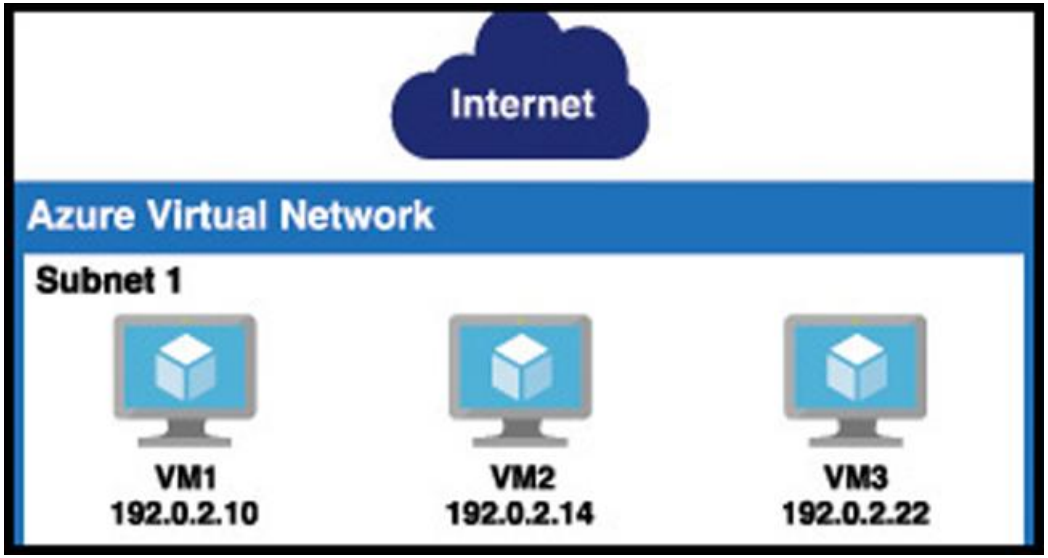


Figura 2-20 El nivel web que usa un modelo IaaS con máquinas virtuales de Azure

Este tipo de configuración es típica para mantener una alta disponibilidad en su aplicación, pero agrega una capa adicional de complejidad. Como cada una de estas máquinas virtuales tiene su propia dirección IP pública, un usuario usará solo una máquina virtual. Idealmente, tiene un sistema que garantiza que si una de estas máquinas virtuales experimenta un problema, el tráfico se envía a las otras máquinas virtuales. Además de eso, cuando hay una gran carga, desea distribuir la carga en estas tres máquinas virtuales. La solución a este problema es usar Azure LoadBalancer.

Azure Load Balancer está dentro de la red virtual, pero se encuentra entre el usuario y la subred. Cuando un usuario se conecta al nivel web, se conecta a la dirección IP del equilibrador de carga, no a la dirección IP de una de mis máquinas virtuales. El equilibrador de carga dirige las solicitudes al nivel web a las máquinas virtuales, y puede usar reglas para garantizar que el tráfico se distribuya equitativamente entre ellas. Si una de las máquinas virtuales se cae y no responde, el equilibrador de carga puede enviar ese tráfico a otra máquina virtual sin que el usuario se dé cuenta de que hay un problema.

La Figura 2-21 muestra el nivel web de la Figura 2-20 con Azure Load Balancer agregado a la mezcla. Observe que la IP pública ahora está en el equilibrador de carga y que las máquinas virtuales están utilizando las direcciones IP privadas de la subred.

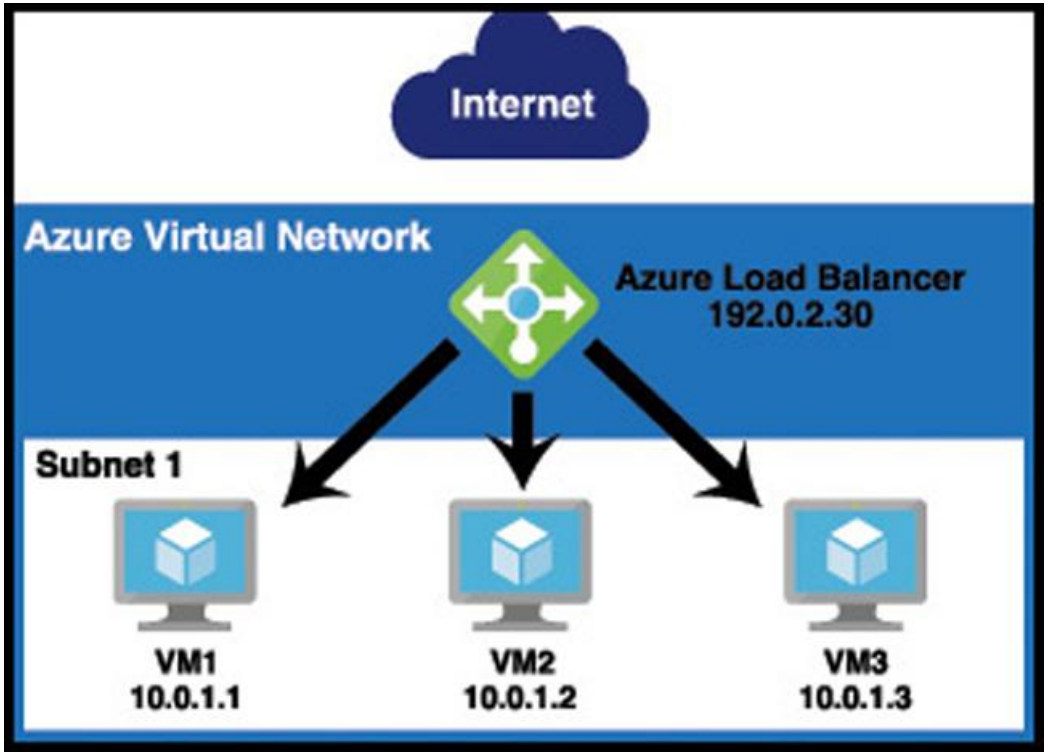


Figura 2-21 El nivel web con Azure Load Balancer

Azure Load Balancer no es solo para distribuir el tráfico de Internet. Para que nuestra aplicación mantenga una alta disponibilidad, debemos garantizar la misma escalabilidad de otros niveles, y Azure Load Balancer también puede ubicarse dentro de otros niveles para garantizar que la carga se distribuya y para garantizar que la aplicación mantenga la alta disponibilidad necesaria para el negocio

Azure Application Gateway

Usar Azure Load Balancer para el nivel web es una solución perfectamente adecuada, pero dado que el nivel web solo usa tráfico HTTP para el sitio web, podemos obtener características adicionales específicas para el tráfico HTTP mediante Azure Application Gateway.

Azure Application Gateway es un equilibrador de carga que está específicamente diseñado para manejar el tráfico HTTP. Dado que Application Gateway comprende el tráfico HTTP, puede tomar decisiones basadas en ese tráfico HTTP. Por ejemplo, Application Gateway puede:

- Enrute el tráfico a una máquina virtual específica o grupo de máquinas virtuales en función de la URL.
- Use una cookie para asegurarse de que un usuario siempre se enruta a la misma VM en una situación en la que esa VM contiene información de estado sobre ese usuario que debe mantenerse.
- Muestre una página de error personalizada, completa con la marca de su empresa, cuando no se encuentra una página o cuando se produce un error.
- Controle el tráfico SSL de su sitio para que los niveles de su aplicación no tengan la carga de tratar de descifrar el tráfico.

También puede agregar Firewall de aplicaciones web (WAF) a Application Gateway. WAF está diseñado para evitar que las vulnerabilidades conocidas entren en su VNET, lo que le permite operar en un entorno más seguro. Si una solicitud intenta ingresar a su red y se determina que es una amenaza, se rechaza en la puerta de enlace y nunca llega a su aplicación.

VPN Gateway

En algunos casos, es posible que necesite su aplicación alojada en Azure para comunicarse con un recurso local. Hablamos sobre este tipo de escenarios en el Capítulo 1 cuando cubrimos escenarios de nube híbrida. Para implementar dicho sistema, puede usar la puerta de enlace VPN de Azure.

VPN Gateway conecta sus recursos locales a su Azure VNET mediante una red privada virtual o VPN. El tráfico que fluye sobre esta VPN está encriptado. Existen múltiples configuraciones para las conexiones de VPN Gateway como se muestra en la Tabla 2-1 .

Tabla 2-1 Tipo de conexiones de puerta de enlace VPN

Tipo de conección	Descripción
VPN de sitio a sitio (S2S)	Conecta tu VNET a una única ubicación local. Requiere una VPN con dirección IP pública local. Una variante multisitio le permite conectarse a múltiples ubicaciones locales.
VPN de punto a sitio (P2S)	Conecta una PC cliente local específica a su VNET. Se pueden conectar varios clientes, pero cada uno se conecta a través de su propio cliente VPN.
VNET a VNET	Conecta dos Azure VNET entre sí. Útil en situaciones en las que tiene dos redes virtuales en diferentes regiones de Azure y desea conectarlas de forma segura.

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

Más información **VNET PEERING**

Como alternativa al uso de conexiones VNET a VNET, puede usar el emparejamiento de VNET para establecer la comunicación entre dos VNET de Azure en la misma región, y puede usar el emparejamiento de VNET global para conectar VNET en diferentes regiones de Azure. El emparejamiento se usa generalmente en un escenario en el que no necesita una puerta de enlace para la conectividad a los recursos locales.

Para obtener más información sobre el emparejamiento VNET, consulte *https://docs.microsoft.com/azure/virtual-network/virtual-network-peering-overview* .

Red de entrega de contenido de Azure

Azure Content Delivery Network (CDN) es una forma efectiva de entregar archivos grandes o transmitir contenido a través de Internet. Hace que la descarga de archivos grandes sea mucho más rápida al almacenar en caché los archivos en múltiples ubicaciones geográficas para que los usuarios puedan obtener los archivos de un servidor lo más cerca posible de ellos. Las CDN generalmente se usan con imágenes, videos y otros archivos de gran tamaño similar.

Un CDN funciona almacenando una versión en caché de archivos en un servidor de *punto de presencia* (POP) que se encuentra en el borde exterior de una red. Estos servidores (llamados *borde* servidores) son capaces de servir el contenido sin tener que ir a través de toda la red, un proceso que añade tiempo a una solicitud.

Microsoft tiene servidores periféricos CDN ubicados en todo el mundo, por lo que cuando un usuario solicita archivos grandes desde cualquier ubicación geográfica, puede servir una copia en caché lo más cerca posible de la ubicación del usuario. El contenido de un servidor perimetral tiene asociada una propiedad de *tiempo de vida* (TTL) que le indica al servidor perimetral cuánto tiempo debe conservar la copia en caché. Si no se especifica un TTL, el tiempo TTL predeterminado es de siete días. Una vez que se elimina una copia en caché, la próxima vez que se solicite ese recurso, el servidor perimetral realizará una solicitud al servidor donde se encuentra la copia original del recurso. Luego lo almacenará en caché nuevamente para futuros usuarios hasta que caduque el TTL.

Administrador de tráfico de Azure

Azure Traffic Manager es un sistema basado en el sistema de nombres de dominio (DNS) diseñado para mejorar la velocidad y la confiabilidad de su aplicación. Para usar Traffic Manager, configura *puntos finales* dentro de Traffic Manager. Un punto final es simplemente un recurso al que desea que los usuarios se conecten. Traffic Manager admite direcciones IP públicas conectadas a máquinas virtuales de Azure, aplicaciones web que se ejecutan en App Service y servicios en la nube alojados en Azure. Un punto final también puede ser un recurso ubicado localmente o incluso en otro proveedor de alojamiento.

Una vez que haya configurado sus puntos finales, especifique las reglas de enrutamiento que desea que Traffic Manager les aplique. Hay muchas reglas de enrutamiento disponibles en Traffic Manager.

- **Prioridad** Todo el tráfico se envía a un punto final primario, pero los puntos finales de respaldo están disponibles en caso de que el punto final primario experimente una interrupción.

- **El** tráfico **ponderado** se distribuye entre los puntos finales. De manera predeterminada, todo el tráfico se distribuye de manera uniforme, pero puede especificar un peso para cada punto final y el tráfico se distribuirá según lo especifique.
- **Performance** Traffic Manager determina el punto final con la latencia de red más baja desde la ubicación del usuario y usa ese punto final.
- **El** tráfico **geográfico** se enruta en función de la ubicación geográfica del servidor DNS que consulta Traffic Manager.
- **Multivalor** Devuelve todos los puntos finales válidos que usan la versión de protocolo de Internet especificada, ya sea IPv4 o IPv6.
- **El** tráfico de **subred** se enruta según el rango de direcciones IP del usuario final.

Una cosa importante para recordar es que Traffic Manager está basado en DNS. Eso significa que un usuario nunca habla directamente con Traffic Manager. Traffic Manager solo se usa para la búsqueda de DNS. Una vez que se conoce una dirección IP para el punto final deseado, todas las solicitudes posteriores omiten completamente Traffic Manager. Además, debido a que Traffic Manager se basa en DNS, el tráfico real entre el usuario y el recurso nunca se envía a través de Traffic Manager.

Productos de almacenamiento de Azure

Azure ofrece muchas opciones para almacenar datos. Si necesita almacenar datos temporalmente en un disco montado en una máquina virtual, o si necesita poder almacenar datos a largo plazo, Azure tiene una opción para satisfacer sus necesidades.

Azure Blob Storage

Azure Blob Storage está diseñado para almacenar datos no estructurados, que no tienen una estructura definida. Eso incluye archivos de texto, imágenes, videos, documentos y mucho más. Una entidad almacenada en Blob Storage se denomina *blob* . Hay tres tipos de blobs en Azure Storage.

- **Bloquear blobs** Se utiliza para almacenar archivos utilizados por una aplicación.
- **Agregar blobs** Son como blobs de bloque, pero los blobs de agregar están especializados para operaciones de agregar. Por esa razón, a menudo se utilizan para almacenar datos actualizados constantemente, como registros de diagnóstico.
- **Blobs de página** Se usan para almacenar archivos de disco duro virtual (.vhd) que se usan en máquinas virtuales de Azure. Los cubriremos en Azure Disk Storage más adelante en este capítulo.

Las gotas se almacenan en contenedores de almacenamiento. Un contenedor se usa como un medio para organizar blobs, por lo que puede tener un contenedor para archivos de video, otro contenedor para archivos de imagen, etc. La elección, sin embargo, es totalmente suya.

Microsoft ofrece numerosos niveles de almacenamiento que tienen un precio de acuerdo con la frecuencia con la que se accede a los datos, cuánto tiempo tiene la intención de almacenarlos, etc. El nivel de almacenamiento en caliente es para los datos a los que necesita acceder con frecuencia. Tiene el mayor costo de almacenamiento, pero el costo para acceder a los datos es bajo. El nivel de

almacenamiento Cool es para datos que tiene la intención de almacenar durante un período más largo y no accede con tanta frecuencia. Tiene un costo de almacenamiento más bajo que el nivel Hot, pero los costos de acceso son más altos. También debe mantener los datos almacenados durante al menos 30 días.

Microsoft también ofrece un nivel de almacenamiento de archivos para el almacenamiento de datos a largo plazo. Los datos almacenados en el nivel Archivo tienen los costos de almacenamiento más bajos disponibles, pero los costos de acceso son los más altos. Debe mantener los datos almacenados durante un mínimo de 180 días en el nivel Archivo. Porque los datos en elEl nivel de archivo no está diseñado para un acceso rápido y frecuente, puede tomar mucho tiempo recuperarlo. De hecho, mientras que los niveles de acceso en caliente y en frío garantizan el acceso al primer byte de datos en milisegundos, el nivel de archivo solo garantiza el acceso al primer byte en 15 horas.

Si planea mover datos de las instalaciones a Azure Storage, hay muchas opciones disponibles para usted. Puede usar Azure Storage Explorer, una herramienta gratuita disponible de Microsoft, para cargar datos. También puede usar las herramientas de línea de comandos que Microsoft proporciona para cargar en Azure Storage.

Si desea mover una gran cantidad de datos, Microsoft ofrece un servicio llamado Data Box. Data Box tiene un servicio en línea llamado Data Box Edge que hace que copiar datos a Azure Storage sea tan fácil como copiarlos en un disco duro de su sistema. Para cantidades aún mayores de datos, Microsoft ofrece un servicio fuera de línea de Data Box donde le enviarán discos duros. Simplemente copie sus datos en los discos duros, cifre los discos con BitLocker y luego los envíe de vuelta a Microsoft. ¡Incluso ofrecen Data Box Heavy, un servicio donde le enviarán un dispositivo resistente sobre ruedas que puede contener hasta 1 petabyte de datos!

Azure Queue Storage

Una cola de mensajes es un componente en una aplicación que puede almacenar mensajes que una aplicación usa para saber qué tareas tomar. Por ejemplo, puede tener una aplicación que realice la manipulación de imágenes en imágenes, y algunas de esas manipulaciones pueden llevar mucho más tiempo que otras. Si tiene miles de personas utilizando la aplicación, una cola de mensajes puede ayudar a garantizar una aplicación receptiva y confiable al permitir que un componente ponga mensajes en la cola y su componente de manipulación de imágenes pueda recuperar esos mensajes, realizar la manipulación y colocar un mensaje de nuevo en la cola.

Azure Queue Storage proporciona una cola de mensajes basada en la nube a la que se puede acceder de forma segura desde los componentes de la aplicación ubicados en cualquier lugar. Se pueden ubicar en la nube o en las instalaciones. Queue Storage puede procesar de forma asíncrona millones de mensajes de hasta 64 KB de tamaño. El remitente del mensaje espera que el receptor tome medidas solo cuando esté listo. Puedes pensar en esto de la misma manera que funciona el correo electrónico. Envía un correo electrónico a un receptor y el receptor se ocupa de él cuando tiene tiempo. No esperas una respuesta inmediata.

Más información **Autorización para el almacenamiento en cola**

El acceso al almacenamiento en cola está protegido y autorizado mediante Azure Active Directory o una clave compartida.

Para acceder a Queue Storage, su aplicación utiliza las API disponibles para el idioma en que se escribió la aplicación. Microsoft proporciona API para usar con .NET, Java, Node.js, C ++, PHP, Python y Ruby.

Azure Disk Storage

El almacenamiento en disco en Azure se refiere a los discos que se usan en máquinas virtuales. Azure crea un disco para usted cuando crea una máquina virtual, que se designa automáticamente para el almacenamiento temporal. Estasignifica que los datos en ese disco se perderán si hay un evento de mantenimiento en la VM. Si necesita almacenar datos durante un período de tiempo más largo que persistirá entre las implementaciones de VM y los eventos de mantenimiento, puede crear un disco con una imagen almacenada en Azure Storage.

Los discos de Azure están disponibles como discos duros tradicionales (HDD) y unidades de estado sólido (SSD). Azure Standard HDD Disk es más económico y está diseñado para datos no críticos. Los discos SSD están disponibles en un nivel Estándar para uso ligero y como Azure Premium Disk para uso intensivo.

Los discos de Azure están disponibles como discos administrados o discos no administrados. Todos los discos de Azure están respaldados por blobs de página en Azure Storage. Cuando usa discos no administrados, usan una cuenta de Azure Storage en su suscripción de Azure, y debe administrar esa cuenta. Esto es particularmente problemático porque hay limitaciones en Azure Storage, y si usa mucho el disco, puede terminar experimentando un tiempo de inactividad debido a la aceleración.

Cuando pasa a Discos administrados, Microsoft maneja la cuenta de almacenamiento y se eliminan todas las limitaciones de almacenamiento. Todo lo que tiene que preocuparse es su disco. Puede dejar la cuenta de Almacenamiento en manos de Microsoft.

Más información **Discos gestionados**

Microsoft recomienda discos administrados para todas las máquinas virtuales nuevas. También recomiendan que todas las máquinas virtuales que actualmente usan discos no administrados se trasladen a discos administrados.

Quizás una razón aún más importante para usar Managed Disks es que al hacerlo, evita un posible punto único de falla en su VM. Cuando usa discos no administrados, existe la posibilidad de que las cuentas de Azure Storage que respaldan sus discos puedan existir dentro de la misma unidad de escala de almacenamiento. Si ocurre una falla en esa unidad de escala, perderá todos sus discos. Al asegurarse de que cada disco administrado esté en una unidad de escala separada, evita la situación de un solo punto de falla.

Azure Files

Los discos de Azure son una buena opción para agregar un disco a una máquina virtual, pero si solo necesita espacio en disco en la nube, no tiene sentido asumir la carga de administrar una máquina virtual y su sistema operativo. En esas situaciones, Azure Files es la solución perfecta.

Tenga en cuenta los **archivos de Azure y el almacenamiento de Azure**

Los recursos compartidos de Azure Files están respaldados por Azure Storage, por lo que necesitará una cuenta de almacenamiento para crear un recurso compartido de Azure Files.

Azure Files es un recurso compartido de archivos completamente administrado que puede montar como cualquier recurso compartido de archivos SMB. Eso significa aplicaciones existentes que usan dispositivos de almacenamiento conectado a la red (NAS) oLos archivos compartidos SMB pueden usar Azure Files sin ninguna herramienta especial, y si tiene varias aplicaciones que necesitan acceder al mismo recurso compartido, eso también funcionará con Azure Files.

 ***Consejo de examen***

Puede montar recursos compartidos de Azure Files en máquinas virtuales de Azure y locales en Windows, Linux y MacOS. Sin embargo, no puede usar Windows 7 o Windows Server 2008 para montar un recurso compartido de archivos de Azure localmente porque esos sistemas operativos solo son compatibles con SMB 2.1.

Además, debido a que los archivos compartidos de Azure Files usan SMB, deberá asegurarse de que el puerto TCP 445 esté abierto en su red. En Windows, puede usar el cmdlet Test-NetConnection PowerShell para probar la conectividad a través del puerto 445. Para obtener más información, consulte: *https://docs.microsoft.com/azure/storage/files/storage-how-to-use-files - ventanas* .

Un posible problema con el uso de Azure Files es la ubicación remota de los archivos. Si sus usuarios o aplicaciones están utilizando un recurso compartido de archivos asignado a Azure Files, pueden experimentar tiempos de transferencia de archivos más largos de lo habitual porque los archivos están en Azure. Para resolver ese problema, Microsoft presentó Azure File Sync.

Instale Azure File Sync en uno o más servidores en su red local y mantendrá sus archivos en Azure Files sincronizados con su servidor local. Cuando los usuarios o las aplicaciones necesitan acceder a esos archivos, pueden acceder a la copia local rápidamente. Cualquier cambio que realice en el recurso compartido centralizado de Azure Files se sincronizará con cualquier servidor que ejecute Azure File Sync.

Productos de base de datos de Azure

La mayoría de las aplicaciones usan algún tipo de base de datos para almacenar datos que pueden recuperarse a través de consultas y usarse en la aplicación. Azure proporciona numerosas soluciones de bases de datos, y si va a pasar a la nube, es importante que comprenda las diferencias entre ellas.

Azure SQL Database

Azure SQL Database es una oferta de PaaS para el alojamiento de bases de datos de SQL Server. Microsoft administra la plataforma, por lo que solo tiene que preocuparse por su base de datos y los datos que contiene.

Las bases de datos de SQL Server son bases de datos *relacionales* formadas por tablas de datos, y cada tabla tiene un esquema que define cómo deberían verse los datos. Por ejemplo, el esquema puede definir que sus datos contienen un número de identificación, un nombre, un apellido y una fecha. Cualquier dato que agregue a la tabla debe seguir el esquema, por lo que debe tener todos los campos definidos en el esquema.

Una base de datos contendrá muchas tablas de datos que están relacionadas entre sí, y al usar consultas especializadas, los desarrolladores pueden devolver datos que son el resultado de unir datos relacionados de múltiples tablas. Por ejemplo, puede tener una tabla de Clientes y una tabla de Órdenes, cada una con un campo "CustomerID" que identifica a un cliente. Al consultar y unir los datos de ambas tablas, puede proporcionar al usuario una factura que muestre todos sus pedidos. Esta relación entre las tablas es cómo las bases de datos relacionales obtuvieron su nombre, como se muestra en la Figura 2-22 .

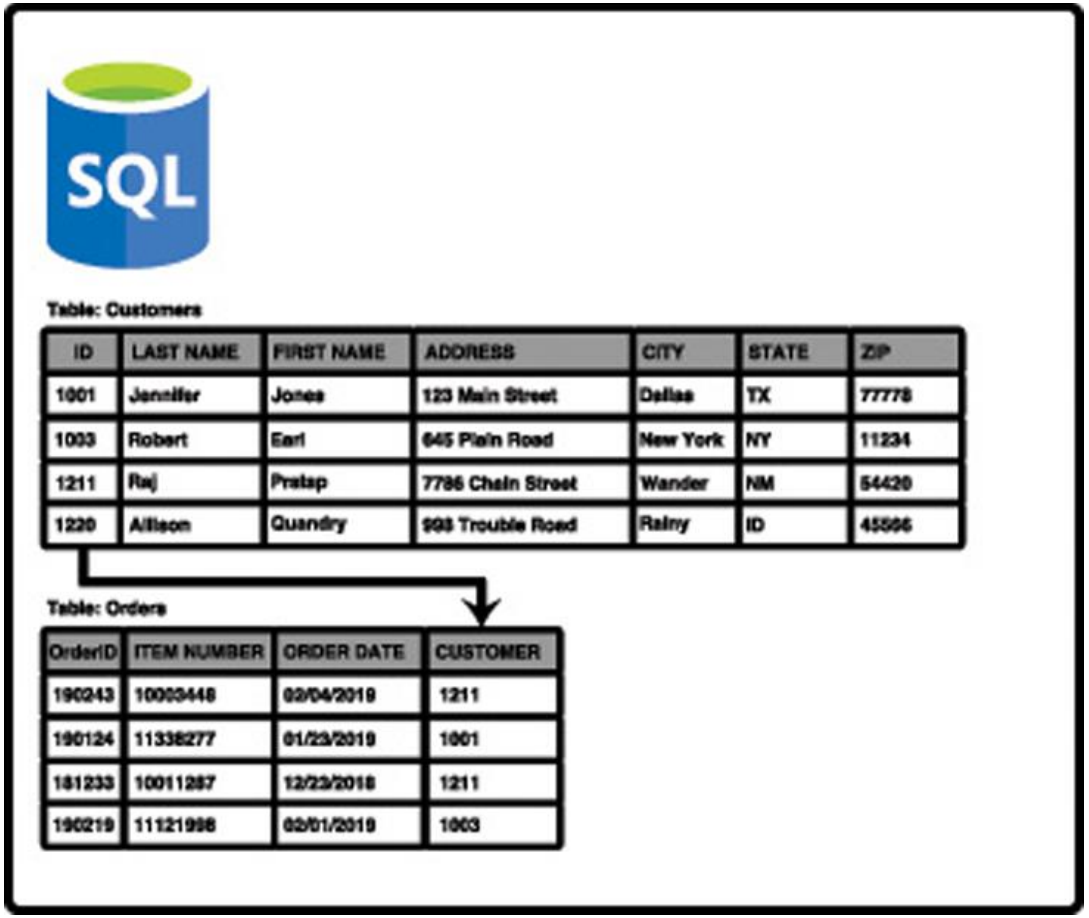


Figura 2-22 Dos tablas en una base de datos relacional

Nota **Bases de datos relacionales**

SQL Server no es el único sistema de base de datos relacional. Existen muchos sistemas de bases de datos relacionales, incluidos Oracle, PostgreSQL y MySQL.

Azure ofrece tres opciones de implementación diferentes para Azure SQL Database: base de datos única, grupo elástico e instancia administrada.

Una sola base de datos es simplemente una base de datos que se ejecuta en una instancia de SQL Server alojada que se ejecuta en Azure. Microsoft administra el servidor de la base de datos, por lo que solo tiene que preocuparse por la base de datos en sí. Microsoft proporciona dos modelos de compra diferentes para bases de datos individuales. La Tabla 2-2 muestra estos modelos y sus diferencias.

Tabla 2-2 Modelos de compra de base de datos única

Modelo de unidad de transacción de base de datos (DTU)	Modelo VCore
Buena opción para usuarios que no necesitan un alto grado de flexibilidad con la configuración y que desean un precio fijo.	Buena opción si necesita un alto nivel de visibilidad y control de recursos individuales (como memoria, almacenamiento y potencia de CPU) que utiliza su base de datos.
Límites preconfigurados para transacciones en la base de datos y configuraciones de almacenamiento, CPU y memoria preconfiguradas.	Flexibilidad en la potencia de CPU, memoria y almacenamiento con almacenamiento cargado en función del uso.
Ofertas básicas y estándar, junto con un nivel Premium para bases de datos de producción con una gran cantidad de transacciones.	Propósito general y ofertas de negocio crítico para proporcionar costos más bajos cuando se desee y alto rendimiento y disponibilidad cuando sea necesario.
Capacidad para escalar a un nivel superior cuando sea necesario.	Capacidad y flexibilidad para escalar CPU, memoria y almacenamiento según sea necesario.
Almacenamiento de respaldo y retención a largo plazo de datos proporcionados por un cargo adicional.	Almacenamiento de respaldo y retención a largo plazo de datos proporcionados por un cargo adicional.

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

Un grupo elástico consta de más de una base de datos (y, a menudo, muchas bases de datos), todas administradas por el mismo servidor de Base de datos SQL. Esta solución está orientada a las ofertas de SaaS donde es posible que desee tener múltiples usuarios (o tal vez incluso cada usuario) para que se les asigne su propia base de datos. Puede mover fácilmente bases de datos dentro y fuera de un grupo elástico, lo que lo hace ideal para SaaS.

En algunos casos, es suficiente poder escalar una sola base de datos para agregar potencia adicional. Si su aplicación tiene grandes variaciones en el uso y le resulta difícil predecir el uso (como con un servicio SaaS), sin embargo, es mucho más deseable poder agregar más bases de datos a un grupo. En un grupo elástico, se le cobra por el uso de recursos del grupo frente a las bases de datos individuales, y tiene control total sobre cómo las bases de datos individuales usan esos recursos. Esto hace posible no solo controlar los costos, sino también garantizar que cada base de datos tenga los recursos que necesita sin dejar de ser previsible en los gastos. Además, puede pasar fácilmente una sola base de datos a un grupo elástico simplemente moviendo la base de datos a un grupo.

Nota **Modelos de precios de piscinas elásticas**

La información del modelo de precios en la Tabla 2-2 también se aplica a las piscinas elásticas. Sus recursos no se aplican a una base de datos individual, sin embargo, se aplican al grupo.

Consejo de examen

Si bien puede escalar hacia arriba y hacia abajo fácilmente con Azure SQL Database al pasar a un nivel superior o agregar recursos informáticos, de memoria y de almacenamiento, las bases de datos relacionales no se escalan horizontalmente. Hay algunas opciones disponibles para escalar una copia de solo lectura de su base de datos, pero en general, las bases de datos relacionales no ofrecen la capacidad de escalar para proporcionar copias adicionales de sus datos en múltiples regiones.

Una instancia administrada está diseñada explícitamente para clientes que desean una ruta de migración fácil desde las instalaciones u otro entorno que no sea de Azure a Azure. Las instancias administradas son totalmente compatibles con SQL Server local, y debido a que su servidor de base de datos está integrado con un VNET aislado y tiene una dirección IP privada, su servidor de base de datos puede ubicarse dentro de su VNET Azure privado. Las características están diseñadas para usuarios que desean levantar y cambiar una base de datos local a Azure sin muchos cambios de configuración o problemas. Están disponibles los niveles de servicio de propósito general y de negocio crítico.

Microsoft desarrolló el Servicio de migración de base de datos de Azure (DMS) para facilitar a los clientes mover fácilmente las bases de datos locales o las bases de datos alojadas en otra parte de la nube a una instancia administrada. El DMS funciona al guiarlo a través de una experiencia de asistente para indicarle a Azure qué base de datos y tablas desea migrar de su base de datos de origen a la Base de datos SQL de Azure. Luego usará Azure VNET que viene con la instancia administrada para migrar los datos. Una vez que se han migrado los datos, DMS configura la sincronización entre la base de datos de origen y la Base de datos SQL de Azure. Esto significa que mientras la base de datos de origen permanezca en línea, cualquier cambio realizado en ella se sincronizará con la instancia administrada en Azure SQL Database.

Más información **Dms y bases de datos locales**

Para migrar una base de datos local, debe tener conectividad entre Azure y su red local a través de VPN o mediante un servicio como ExpressRoute.

Para obtener más información sobre ExpressRoute, consulte: *https://docs.microsoft.com/azure/expressroute/expressroute-introduction* .

Azure Cosmos DB

Como ha visto en nuestra discusión sobre las bases de datos de SQL Server, las bases de datos relacionales lo encierran en una estructura específica para sus datos. Si bien ciertamente hay un lugar para las bases de datos relacionales, a medida que las empresas comenzaron a recopilar cada vez más datos, comenzaron a buscar una forma más flexible de almacenar esos datos. Esto eventualmente condujo a lo que se llama sistemas de base de datos NoSQL.

En un sistema de base de datos NoSQL, no está bloqueado en un esquema para sus datos. Si está almacenando información como la que se muestra en la tabla Clientes en la Figura 2-22 , y desea comenzar a almacenar también los cumpleaños de los clientes, simplemente agregue el cumpleaños a sus datos y agréguelo a la base de datos. A la base de datos no le importa qué tipo de datos hay y qué campos hay.

Existen cuatro tipos de sistemas de bases de datos NoSQL: clave-valor, columna, documento y gráfico. La Tabla 2-3 enumera cada uno de estos tipos y alguna información sobre ellos.

Tabla 2-3 Sistemas de bases de datos NoSQL

Sistema	Descripción	Uso común
Valor clave	Almacena datos vinculados a una clave única. Pase la clave y la base de datos devolverá los datos.	Dado que el valor puede ser casi cualquier cosa, las bases de datos de valores clave tienen muchos usos.
Columna	Las bases de datos NoSQL se denominan *espacios de claves* , y un espacio de claves contiene familias de columnas. Una columna contiene filas y columnas como una tabla relacional, pero cada fila puede tener su propio conjunto de columnas. No estás encerrado en un esquema.	Almacenar datos de perfil de usuario para un sitio web. Además, debido a que las bases de datos de columnas se escalan bien y son extremadamente rápidas, son muy adecuadas para almacenar grandes cantidades de datos.
Documento	Los datos se almacenan como una cadena de texto estructurada llamada documento. Esto puede ser HTML,	Igual que el valor-clave, pero las bases de datos de documentos tienen ventajas. Se escalan bien

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

Sistema	Descripción	Uso común
	JSON, etc. Esto es similar a una base de datos de valores clave, excepto que el documento es un valor estructurado.	horizontalmente y le permiten consultar el valor y devolver partes del valor. Una consulta de base de datos de valores clave devuelve el valor completo asociado con la clave.
Grafico	Almacena datos y las relaciones entre cada pieza de datos. Los datos se almacenan en nodos, y las relaciones se dibujan entre nodos.	Muchos sistemas usan bases de datos de gráficos porque son extremadamente rápidos. Una red social podría usar una base de datos gráfica porque sería fácil almacenar las relaciones entre las personas y también las cosas que les gustan, y así sucesivamente.

Con formato: Fuente: 12 pto

Con formato: Fuente: 12 pto

Hay muchos sistemas de bases de datos NoSQL diferentes, y la mayoría de ellos están orientados a un modelo de base de datos particular. Microsoft ofrece un sistema de base de datos NoSQL alojado en Azure llamadoCosmos DB y Cosmos DB son compatibles con todos los tipos de bases de datos NoSQL. Microsoft ha creado un código personalizado alrededor de Cosmos DB para que los desarrolladores puedan usar sus habilidades existentes con otros sistemas de bases de datos con una base de datos Cosmos DB. Esto facilita que las aplicaciones existentes comiencen a aprovechar Cosmos DB sin que los ingenieros tengan que escribir un nuevo código.

Cuando crea una base de datos Cosmos DB, elige la API que desea usar, y esto determina el tipo de base de datos para su base de datos. Los tipos de API de la base de datos son:

- **Core (SQL)** Crea una base de datos de documentos que puede consultar utilizando la sintaxis SQL con la que podría estar familiarizado al usar bases de datos relacionales.
- **Azure Cosmos DB para MongoDB API** Se usa para migrar una base de datos MongoDB a Cosmos DB. Las bases de datos MongoDB son bases de datos de documentos.
- **Cassandra** Se utiliza para migrar una base de datos Cassandra a Cosmos DB. Las bases de datos de Cassandra son bases de datos de columnas.
- **Azure Table** Se usa para migrar datos almacenados en Azure Table Storage a Cosmos DB. Esto crea una base de datos clave-valor.
- **Gremlin** Se utiliza para migrar las bases de datos de Gremlin a Cosmos DB. Las bases de datos de Gremlin son bases de datos de gráficos.

La razón por la que Microsoft llama a estas API es porque son solo eso. Son interfaces de programación de aplicaciones que permiten a los desarrolladores que ya están utilizando una tecnología de base de datos NoSQL existente migrar a Cosmos DB sin tener que cambiar su código.

Otra gran ventaja de Cosmos DB es una característica que Microsoft llama distribución global llave en mano. Esta característica aprovecha la escalabilidad horizontal de las bases de datos NoSQL y le permite replicar sus datos globalmente con unos pocos clics. En Azure Portal, simplemente puede hacer clic en las regiones donde desea replicar los datos, como se muestra en la Figura 2-23 . Una vez que haga clic en Guardar, Cosmos DB comenzará a replicar datos, que estarán disponibles en las regiones seleccionadas. Esto facilita asegurar que los usuarios tengan la experiencia más rápida posible con una aplicación.

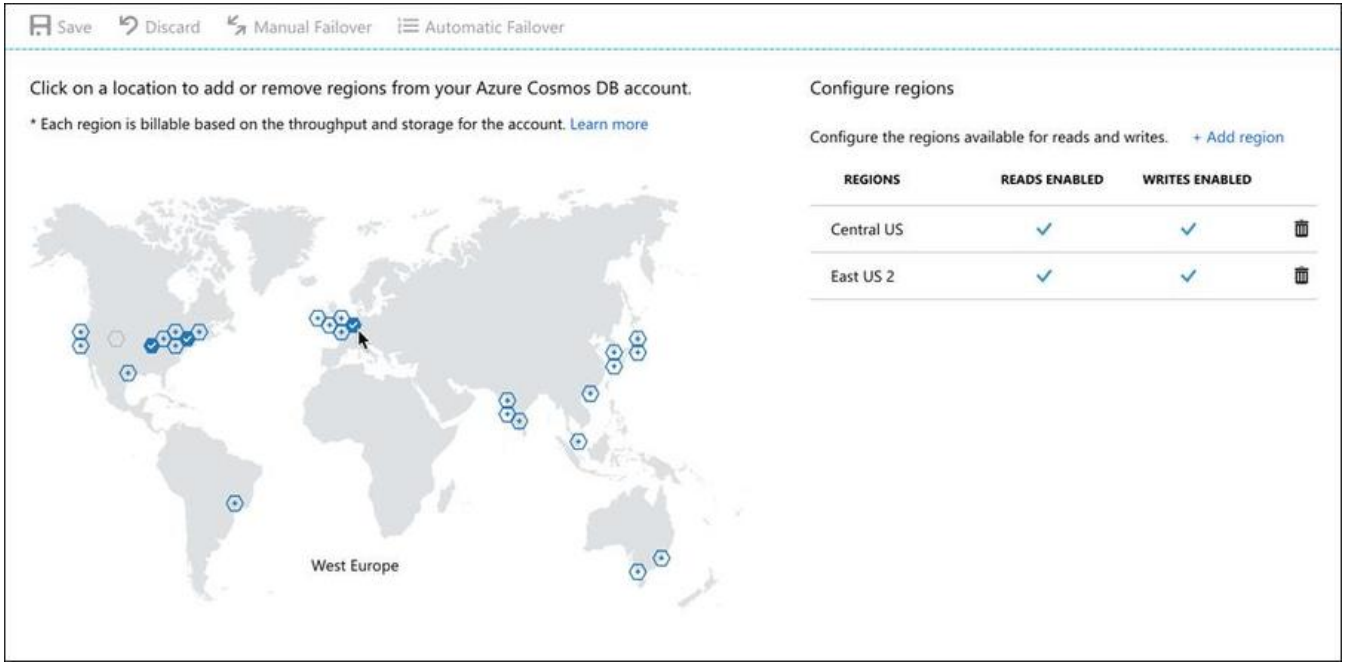


Figura 2-23 Fácil replicación en todo el mundo con Cosmos DB

Azure Marketplace y sus escenarios de uso

Has aprendido sobre muchos de los productos y servicios disponibles en Azure, pero hay muchos productos disponibles fuera de lo que hemos discutido. Microsoft no solo ofrece muchos servicios adicionales, sino que los proveedores externos también proporcionan una amplia gama de recursos que puede usar en Azure. Todos estos recursos están disponibles en un único repositorio llamado Azure Marketplace.

Para acceder a Azure Marketplace, haga clic en **Crear un recurso** en Azure Portal como se muestra en la Figura 2-24 . Esto mostrará una lista de categorías entre las que puede elegir. También mostrará una lista de ofertas populares de todas las categorías. Puede hacer clic en una categoría para ver todas las plantillas en esa categoría, y puede hacer clic en una plantilla en la lista de plantillas populares, ingresar un término de búsqueda o incluso hacer clic en **Ver todo** para ver todas las plantillas que están disponibles.

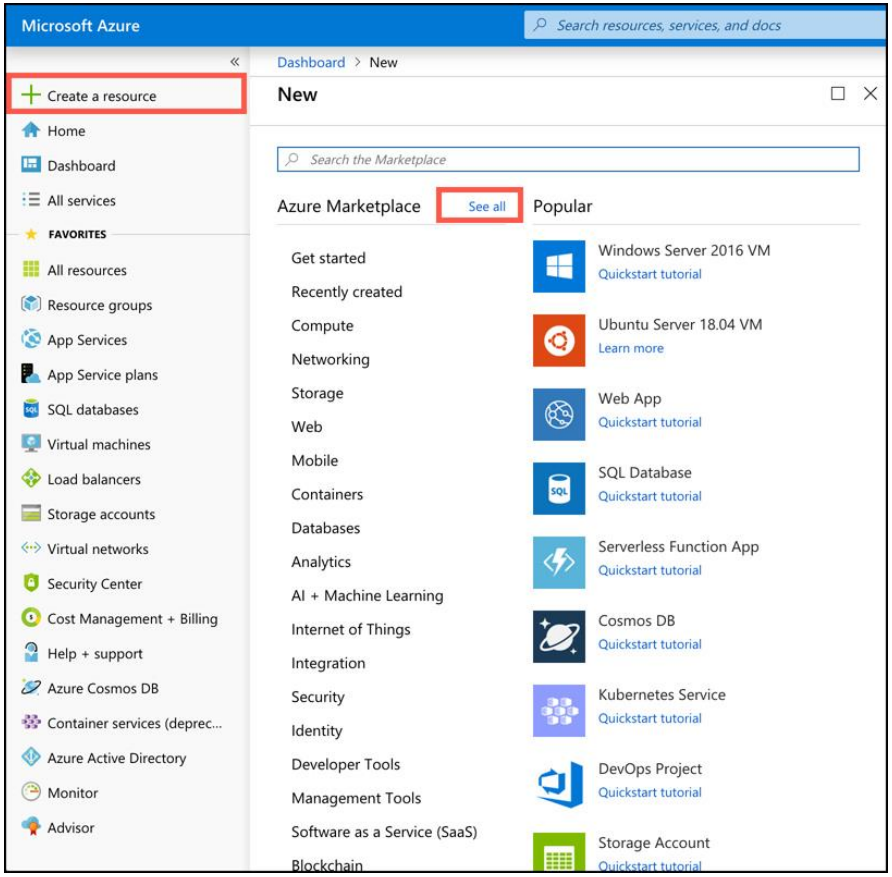


Figura 2-24 El mercado de Azure

Si hace clic en **Ver todo** , accederá a la experiencia completa de Marketplace, donde puede filtrar según los precios, los sistemas operativos y el editor, como se muestra en la Figura 2-25 .

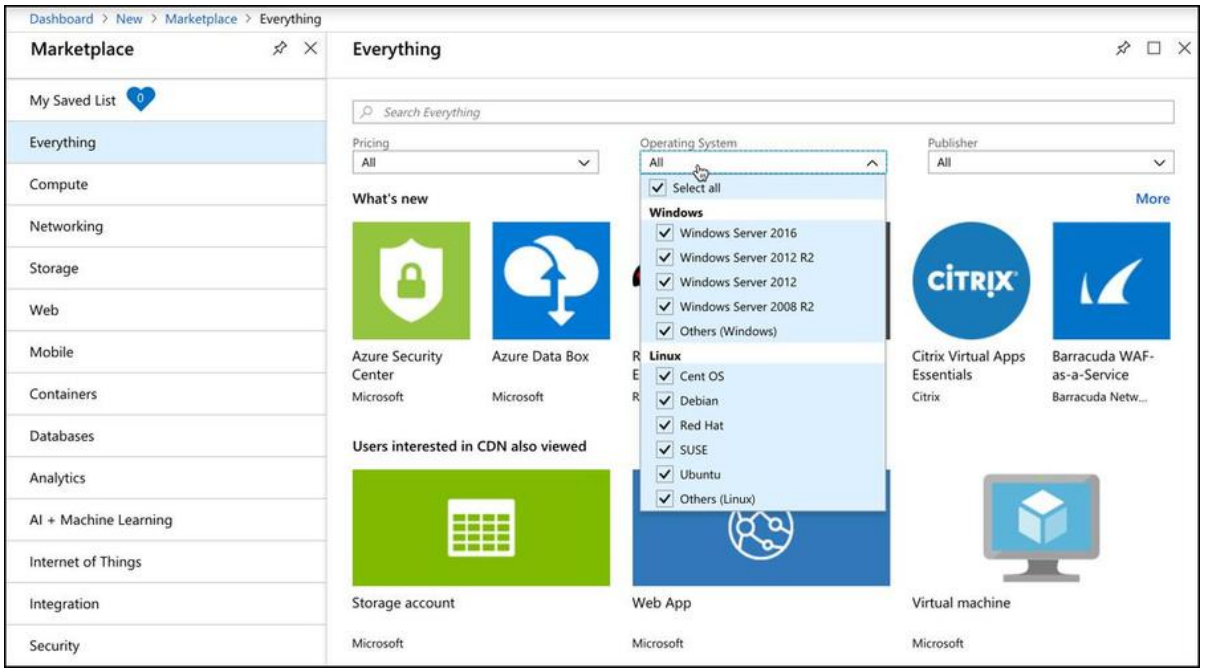


Figura 2-25 Filtrado de Azure Marketplace

Consejo de examen

Todas las plantillas en Azure Marketplace son plantillas ARM que implementan uno o más servicios de Azure. Recuerde de nuestra discusión anterior de Azure Resource Manager que todas las implementaciones de ARM se implementan utilizando plantillas de ARM. El mercado no es diferente.

Algunas de las plantillas en Marketplace implementan un solo recurso. Por ejemplo, si hace clic en la plantilla de aplicación web, creará una aplicación web que se ejecuta en el Servicio de aplicaciones de Azure. Otras plantillas crean muchos recursos que se combinan para hacer una solución completa. Por ejemplo, puede crear un clúster de base de datos DataStax Enterprise y la plantilla creará entre 1 y 40 nodos DataStax Enterprise.

Se le factura por cada oferta de Marketplace en su factura de Azure, por lo que si crea un clúster DataStax Enterprise con 40 nodos, no verá la facturación por separado para 40 VM, VNET, etc. En cambio, verá una factura por un clúster de DataStax Enterprise. Esto hace que la facturación sea mucho más fácil de entender.

Como se muestra en la Figura 2-26 , muchas plantillas de Marketplace proporcionan enlaces a documentación y otra información para ayudarlo a aprovechar al máximo la plantilla. Si decide que no desea crear los recursos inmediatamente, puede hacer clic en **Guardar para más tarde** y la plantilla se agregará a su lista guardada a la que puede acceder haciendo clic en **Mi lista guardada** como se muestra en la esquina superior izquierda de la Figura 2-25 .

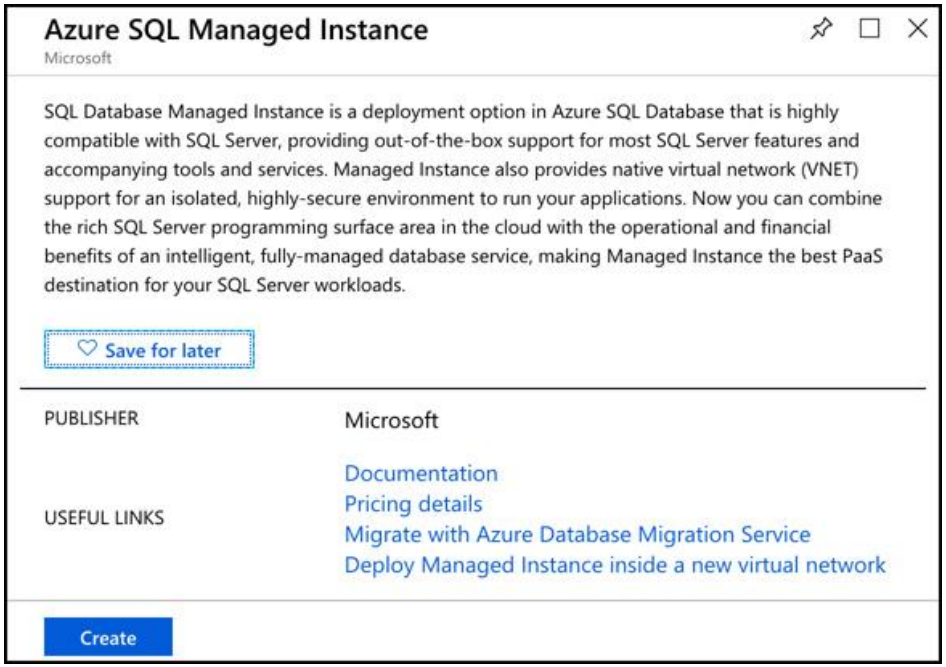


Figura 2-26 Enlaces de Marketplace y Lista guardada

HABILIDAD 2.3: DESCRIBA ALGUNAS DE LAS SOLUCIONES DISPONIBLES EN AZURE

En la sección Skill 2.2, aprendió sobre algunos de los productos principales de Azure. En esta sección, aprenderá sobre algunas de las tecnologías más avanzadas que están disponibles en Azure actualmente. Esto incluye Internet de las cosas (IoT), Big Data y análisis, inteligencia artificial (AI) y computación sin servidor en Azure.

Esta sección cubre:

- Internet de las cosas (IoT)
- Big Data y analítica
- Inteligencia artificial
- Computación sin servidor

Internet de las cosas (IoT)

Muchos de nosotros no vivimos en hogares inteligentes de alta tecnología, por lo que es posible que no nos demos cuenta de cuán grande se está convirtiendo IoT. Para ponerlo en contexto, el popular portal de estadísticas Statista informa que actualmente hay más de 25 mil millones de dispositivos conectados a IoT, y se espera que ese número crezca a la asombrosa cifra de 75 mil millones para el año 2025. Hay aproximadamente 3,2 mil millones de personas en Internet hoy. , y la población mundial es de alrededor de 8 mil millones. Estos dispositivos de IoT eclipsan a la raza humana en número, y la cantidad de información que recopilan y comparten es alucinante.

Para ayudar a las empresas a administrar los dispositivos y manejar los datos que recopilan, Azure tiene varios servicios destinados a IoT, incluidos IoT Hub e IoT Central.

Azure IoT Hub

Para tener más sentido de los servicios de IoT de Azure, consideremos una compañía teórica llamada ContosoPharm, que en este ejemplo es una compañía farmacéutica con un gran edificio de varios pisos donde almacenan medicamentos en desarrollo, junto con componentes sensibles utilizados en la investigación. . Estos artículos deben estar bajo estricto control climático. Si la temperatura o la humedad se mueven fuera de un rango muy estrecho, se pierden materiales invaluables.

Para proteger su inversión, ContosoPharm utiliza sistemas de control de clima conectados a IoT, junto con generadores y sistemas de iluminación conectados a IoT. Estos sistemas monitorean constantemente el entorno y envían alertas si algo sale mal. Hay aproximadamente 5,000 dispositivos IoT en el edificio, y ContosoPharm debe cumplir con los siguientes requisitos para todos esos dispositivos.

- Deben actualizar el firmware en los dispositivos IoT fácilmente y de forma escalonada, de modo que no se actualicen todos al mismo tiempo.
- Deben alterar la configuración de los dispositivos, como cambiar los niveles de alerta, pero estas configuraciones son específicas de la ubicación física de los dispositivos en el edificio.

- Deben asegurarse de que cualquier conectividad a los dispositivos sea completamente segura.

IoT Hub puede resolver fácilmente todos estos problemas. Los dispositivos IoT se agregan a IoT Hub, y luego puede administrarlos, monitorearlos y enviarles mensajes, ya sea individualmente o a grupos que cree. Puede agregar hasta 1,000,000 de dispositivos IoT a un solo IoT Hub.

La Figura 2-27 muestra un dispositivo IoT agregado al IoT Hub para ContosoPharm.

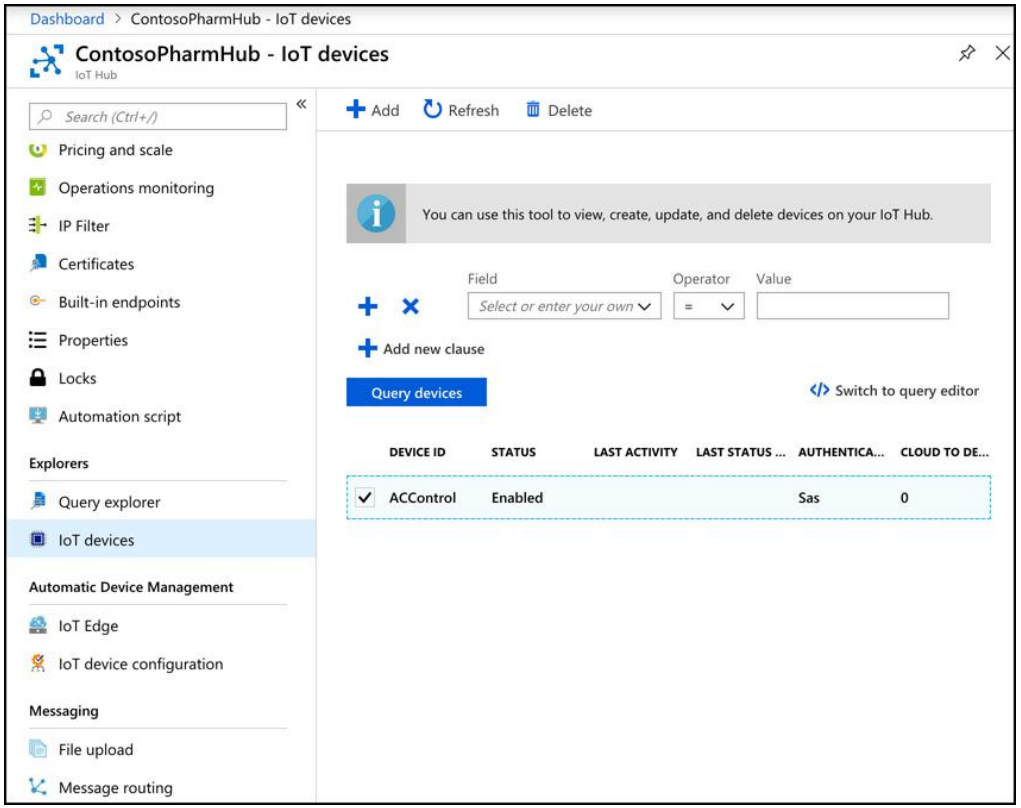


Figura 2-27 Un dispositivo IoT en IoT Hub

Desde IoT Hub, puede enviar mensajes a dispositivos (llamados mensajes de nube a dispositivo o C2D) o desde su dispositivo a IoT Hub (llamados mensajes de dispositivo a nube o D2C). También puede enrutar mensajes de manera inteligente a Event Hub, Azure Storage y Service Bus en función del contenido del mensaje.

Cuando agrega un nuevo dispositivo IoT, IoT Hub crea una cadena de conexión que utiliza una clave de acceso compartida para la autenticación. Esta clave evita el acceso no autorizado a su IoT Hub. Una vez conectado, los mensajes entre su dispositivo y IoT Hub se cifran para mayor seguridad.

Además de los mensajes, también puede usar IoT Hub para enviar archivos a sus dispositivos. Esto le permite actualizar fácilmente el firmware de sus dispositivos de forma segura. Para actualizar el firmware en un dispositivo IoT, simplemente copie el firmware en el dispositivo. El dispositivo detectará el firmware y se reiniciará y actualizará el nuevo firmware al dispositivo.

Un concepto importante en IoT Hub es el concepto de lo que se llama un *dispositivo gemelo* . Cada dispositivo IoT en IoT Hub tiene un equivalente lógico que se almacena en IoT Hub en formato JSON. Esta representación JSON del dispositivo se llama dispositivo gemelo y proporciona capacidades importantes.

Cada dispositivo gemelo puede contener metadatos que agregan categorización adicional para el dispositivo. Estos metadatos se almacenan como etiquetas en el JSON para el dispositivo gemelo, y el dispositivo real no lo conoce. Solo IoT Hub puede ver estos metadatos. Uno de los requisitos de ContosoPharm era actualizar el firmware por etapas en lugar de actualizar todos los dispositivos al mismo tiempo. Pueden lograrlo agregando etiquetas para los dispositivos gemelos desde sus dispositivos que podrían tener el siguiente aspecto:

Haga clic aquí para ver la imagen del código

```
"etiquetas": {

     "deployation": {

            "departamento": "researchInjectibles",

            "piso": "14"

      }

}
```

Luego pueden elegir enviar archivos de firmware solo a dispositivos en el piso 14, por ejemplo, o decirles a dispositivos en el departamento de ResearchInjectibles. La Figura 2-28 muestra la configuración gemela del dispositivo en IoT Hub con etiquetas establecidas para la ubicación del dispositivo. Observe la etiqueta de "construcción" con un valor nulo. Esta es una etiqueta que se configuró previamente en el dispositivo gemelo, y al establecerla como nula, la etiqueta se eliminará.

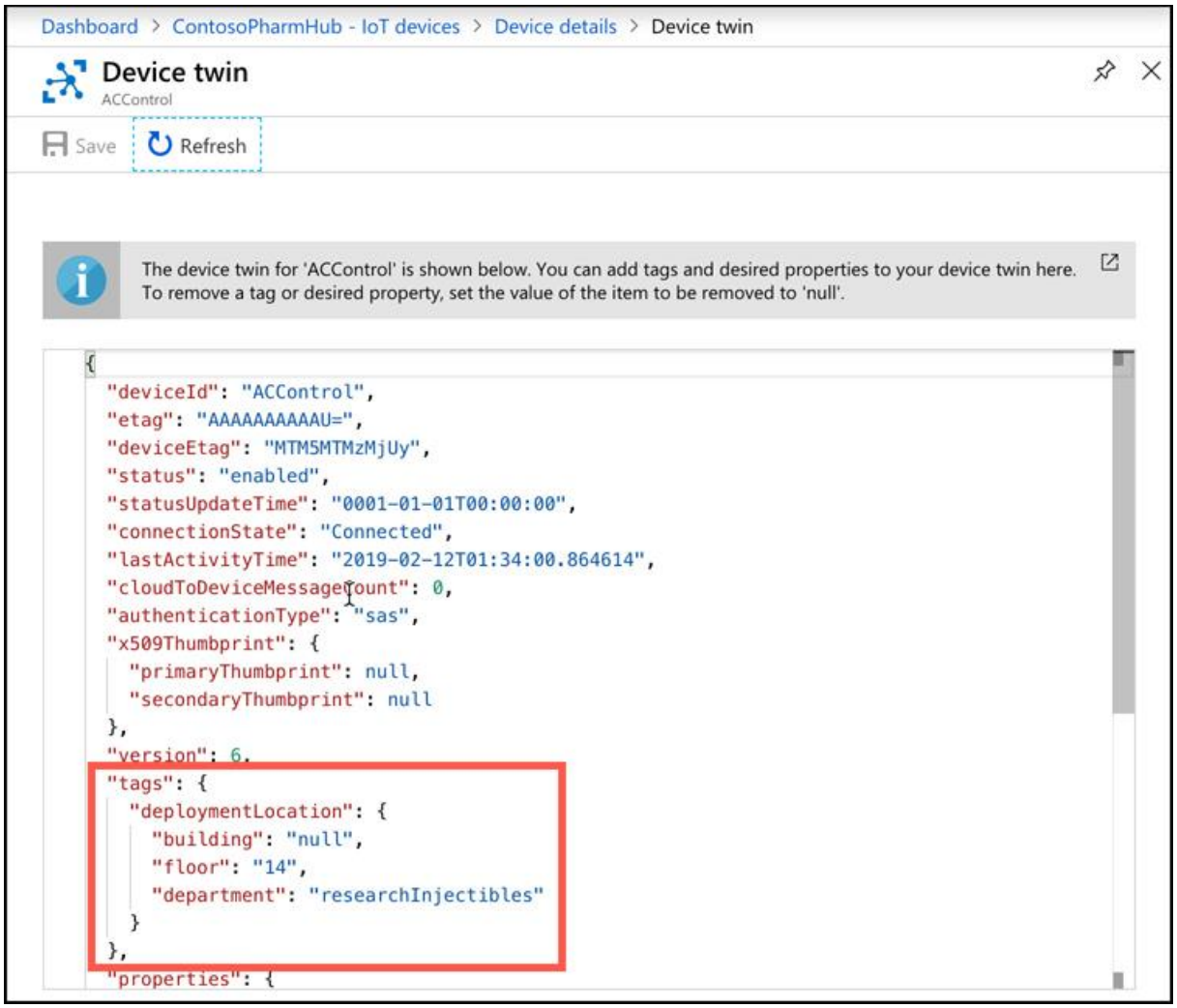


Figura 2-28 Dispositivo gemelo que muestra etiquetas establecidas en el JSON

El dispositivo gemelo también contiene las propiedades para el dispositivo IoT. Hay dos copias de cada propiedad. Una es la propiedad "informada" y la otra es la propiedad "deseada". Puede cambiar la propiedad de un dispositivo en IoT Hub cambiando la propiedad "deseada" a un nuevo valor. La próxima vez que el dispositivo se conecte a IoT Hub, esa propiedad se establecerá en el dispositivo. Hasta que eso suceda, la propiedad "informada" contendrá el último valor que el dispositivo informó a IoT Hub. Una vez que se actualiza la propiedad, la propiedad "informada" y "deseada" será igual.

La razón por la que IoT Hub usa este método para configurar propiedades es que no siempre puede tener una conexión con cada dispositivo. Por ejemplo, si un dispositivo se pone en suspensión para ahorrar energía, IoT Hub no puede escribir cambios de propiedad en ese dispositivo. Al mantener una versión "deseada" e "informada" de cada propiedad, IoT Hub siempre sabe si una propiedad debe escribirse en un dispositivo la próxima vez que el dispositivo se conecte a IoT Hub.

Para ayudar a los usuarios que desean agregar una gran cantidad de dispositivos IoT a IoT Hub, Microsoft ofrece el Servicio de aprovisionamiento de dispositivos IoT Hub, o DPS. El DPS usa grupos de inscripción para agregar dispositivos a su IoT Hub. El concepto es que una vez que el dispositivo se despierta (a menudo por primera vez si es un dispositivo nuevo), debe saber que debe conectarse a su IoT Hub. Para hacer eso, el DPS necesita identificar de manera única el dispositivo, y lo hace con un certificado o mediante un chip de módulo de plataforma confiable.

Una vez que DPS confirma la identidad del dispositivo, puede usar los detalles del grupo de inscripción para determinar a qué IoT Hub se debe agregar. Luego proporcionará al dispositivo la información de conexión para conectarse a ese IoT Hub. Además de eso, el grupo de inscripción también puede proporcionar la configuración inicial para el dispositivo gemelo. Esto le permite especificar propiedades como una versión de firmware que el dispositivo necesita tener cuando se inicia.

A medida que sus dispositivos envían mensajes a IoT Hub, puede enrutar esos mensajes a Azure Storage, Event Hub y otros puntos finales. Puede elegir el tipo de mensajes que desea enrutar, y también puede escribir una consulta para filtrar qué mensajes se enrutan. En la Figura 2-29 , hemos configurado una ruta que envía mensajes a Azure Blob Storage. Puede ver en la consulta que solo vamos a enrutar los mensajes que provienen de un dispositivo con un dispositivo gemelo que contiene la etiqueta para nuestro departamento de investigación de inyectables.

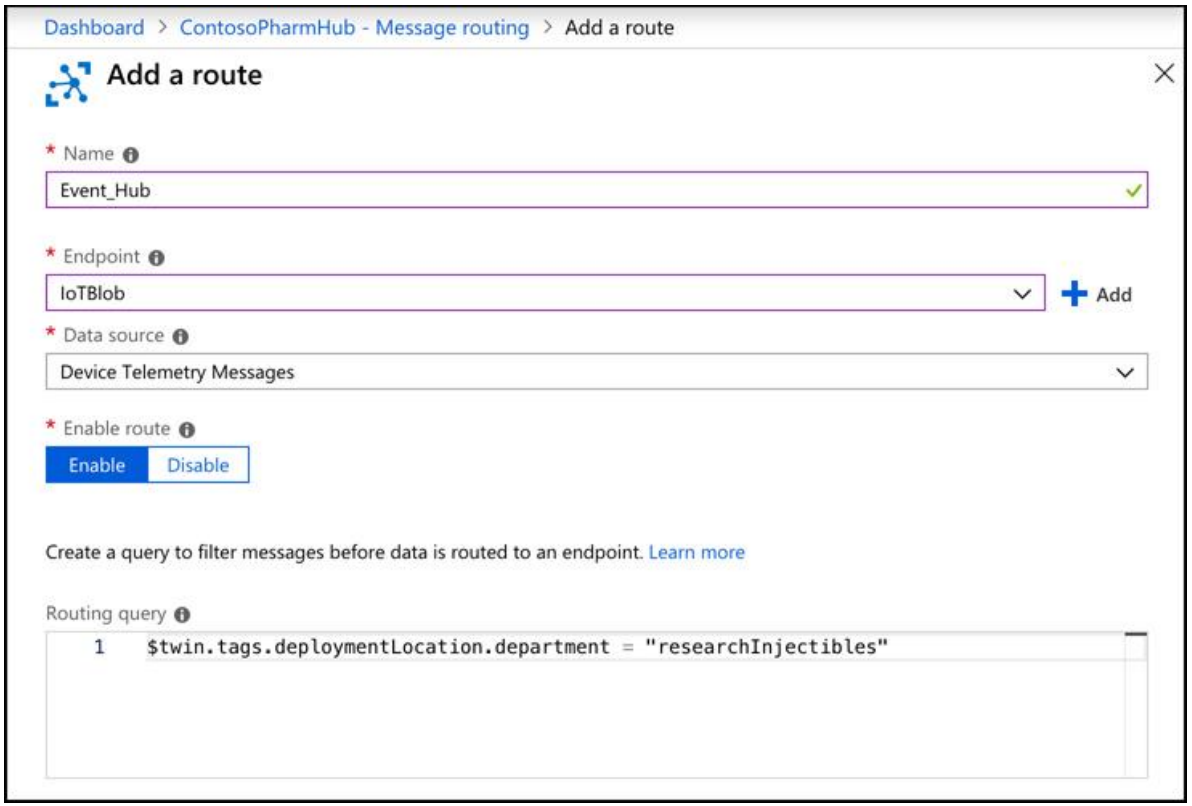


Figura 2-29 Agregar una ruta de mensajes en IoT Hub

Hay dos niveles de precios para IoT Hub: Básico y Estándar. Cada nivel ofrece múltiples ediciones que ofrecen precios basados en la cantidad de mensajes por día para cada unidad IoT Hub. Cuando ustedescalar un IoT Hub, agrega unidades adicionales. Esto agrega la capacidad de manejar más mensajes a un precio mayor. La Tabla 2-4 muestra las ediciones y los precios para el nivel Básico. La Tabla 2-5 muestra las ediciones y los precios para el nivel Estándar.

Tabla 2-4 Precios de nivel básico de IoT Hub

Edición	Precio mensual por unidad IoT Hub	Mensajes por día por unidad IoT Hub
B1	$ 10	400,000
B2	$ 50	6,000,000
B3	$ 500	300,000,000

Tabla 2-5 Precios de nivel estándar de IoT Hub

Edición	Precio mensual por unidad IoT Hub	Mensajes por día por unidad IoT Hub
Gratis	Gratis	8,000
S1	$ 25	400,000
S2	$ 250	6,000,000
S3	$ 2,500	300,000,000

Consejo de examen

El precio de la escala en IoT Hub es bastante claro. La mayoría de las empresas elegirán el nivel Estándar debido a la funcionalidad adicional disponible en ese nivel. Luego elegirán una edición que satisfaga sus necesidades mínimas de mensajes. Cuando necesiten mensajes adicionales durante los picos, se escalarán a más unidades IoT Hub.

Por ejemplo, suponga que las necesidades de mensajes de ContosoPharm son de aproximadamente 5,000,000 por día. Elegirían el nivel de precios S2 y pagarían $ 250 por mes si están ejecutando 1 unidad IoT Hub. Si el número de mensajes aumenta a 8,000,000 (ya sea debido a cambios en la configuración o la adición de dispositivos IoT adicionales), probablemente elegirían escalar a 2 unidades IoT Hub. Hacerlo les daría 12,000,000 de mensajes por día a un costo de $ 500 por mes.

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

Nota **Cambiar el nivel de precios**

No puede cambiar a un nivel de precios más bajo después de crear su IoT Hub. Si crea su IoT Hub en el nivel Estándar, no puede cambiarlo al nivel Básico. Si crea un IoT Hub en el nivel Estándar utilizando la edición S1, S2 o S3, no puede cambiarlo a la edición Gratis.

También es importante tener en cuenta que las siguientes características solo están disponibles en el nivel Estándar.

- Device Streams para transmitir mensajes en tiempo casi real
- Mensajería de nube a dispositivo
- Gestión de dispositivos, dispositivo doble y módulo doble
- IoT Edge para manejar dispositivos IoT en el borde de la red donde residen

Si usa el Servicio de aprovisionamiento de dispositivos, hay un cargo de $ 0.10 por cada 1,000 operaciones.

Azure IoT Central

IoT Hub es una excelente manera de administrar y aprovisionar dispositivos, y proporciona un medio robusto para tratar mensajes. Incluso puede usar Azure Stream Analytics para enrutar mensajes a Power BI para un tablero casi en tiempo real de mensajes del dispositivo, pero hacerlo requiere un poco de configuración compleja. Si está buscando una experiencia de primera clase en el monitoreo de dispositivos IoT sin tener que hacer una configuración compleja, IoT Central es una buena opción.

IoT Central es una oferta SaaS para dispositivos IoT. A diferencia de IoT Hub, no tiene que crear ningún recurso de Azure para usar IoT Central. En su lugar, navega hasta *https://apps.azureiotcentral.com* y crea su aplicación dentro de la interfaz del navegador web como se muestra en la Figura 2-30 .

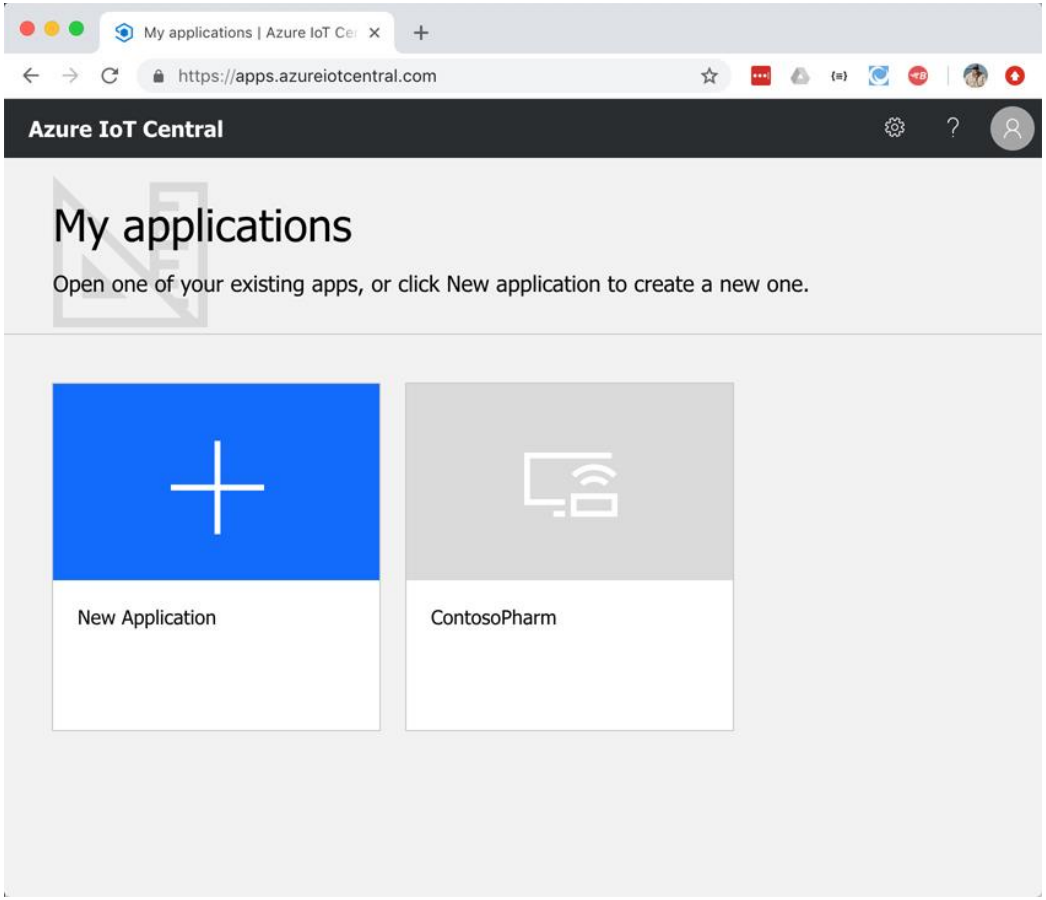


Figura 2-30 La página de inicio de Azure IoT Central

Para crear una aplicación IoT, haga clic en **Nueva aplicación** . Esto abre la pantalla Crear aplicación que se muestra en la Figura 2-31 , donde puede elegir el Plan de prueba (que no requiere unSuscripción de Azure) o Pay-As-You-Go con una suscripción de Azure. Si elige un plan de prueba, tiene 7 días para probar IoT Central con cualquier cantidad de dispositivos sin cargo, y puede actualizar la aplicación a Pay-As-You-Go en cualquier momento dentro de esos 7 días. Si elige Pago por uso, paga según la cantidad de dispositivos que tenga, pero los primeros cinco dispositivos siempre son gratuitos.

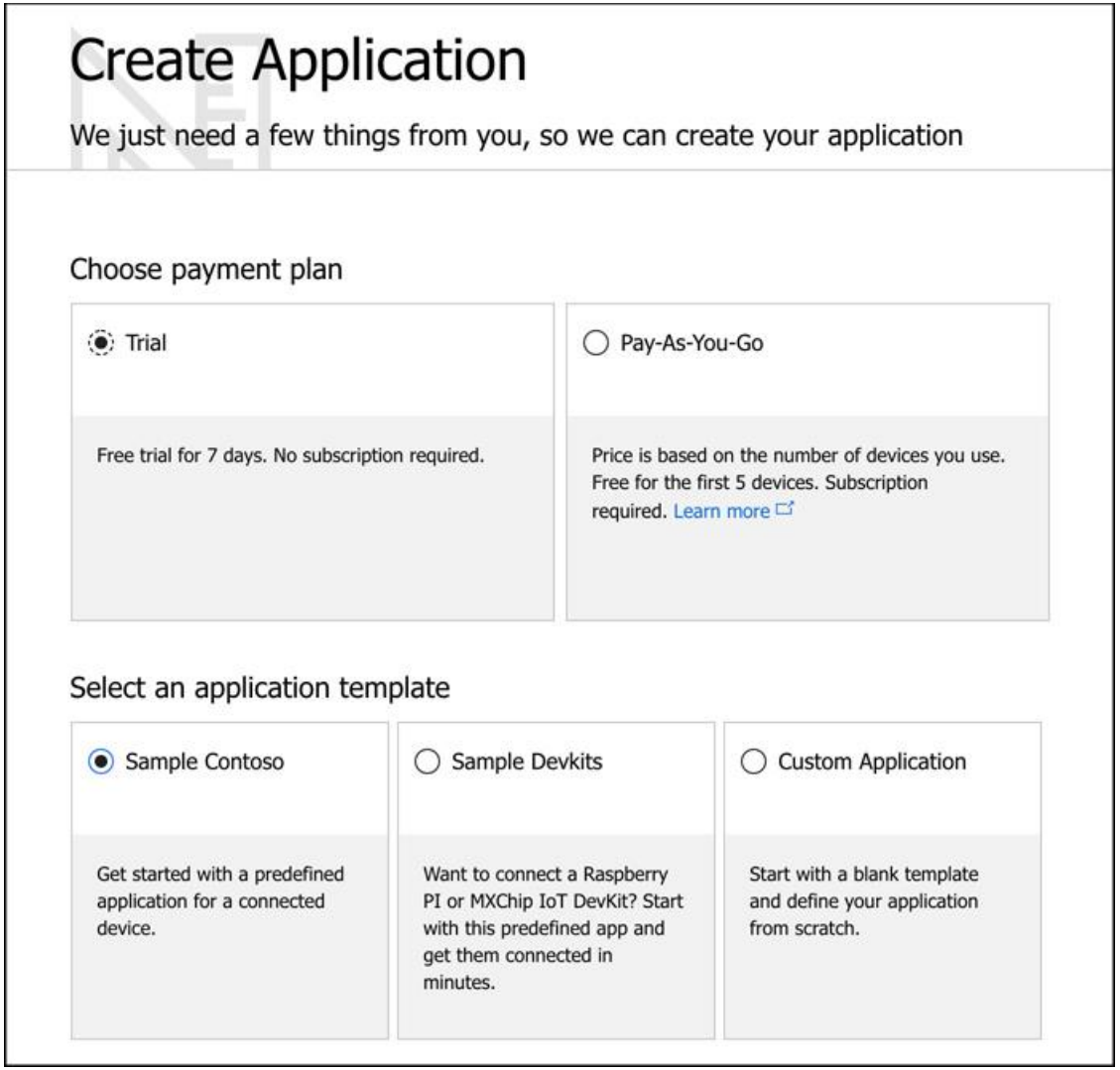


Figura 2-31 Creación de una nueva aplicación IoT Central

También tiene la opción de elegir una plantilla o crear una plantilla en blanco. La plantilla Sample Contoso crea una aplicación de muestra con un dispositivo de máquina expendedora refrigerada simulada. Si tiene un Raspberry PI o un MXChip IoT DevKit del Kit de inicio de Azure IoT, puede usar la plantilla de ejemplo Devkits. Tiene plantillas de dispositivo para que pueda agregar estos dispositivos a su aplicación IoT Central. Finalmente, la plantilla de Aplicación personalizada le permite comenzar desde cero y agregar cualquier dispositivo IoT que pueda tener.

Después de seleccionar su plantilla, desplácese hacia abajo para especificar el nombre de su aplicación y la URL. Puede usar los nombres predeterminados o especificar los suyos, pero se recomienda usar los suyos para poder identificar fácilmente su aplicación. Además, una vez que se ha creado su aplicación, puede acceder a ella directamente utilizando la URL que especifique, por lo que es posible que también desee que sea descriptiva.

Si usa Pay-As-You-Go, deberá especificar un Azure Active Directory asociado con su suscripción, su suscripción de Azure y la región donde desea crear su aplicación. (Si es posible, es mejor elegir una región que esté geográficamente cerca de sus dispositivos IoT). Haga clic en **Crear** para finalizar la creación de su aplicación como se muestra en la Figura 2-32 .

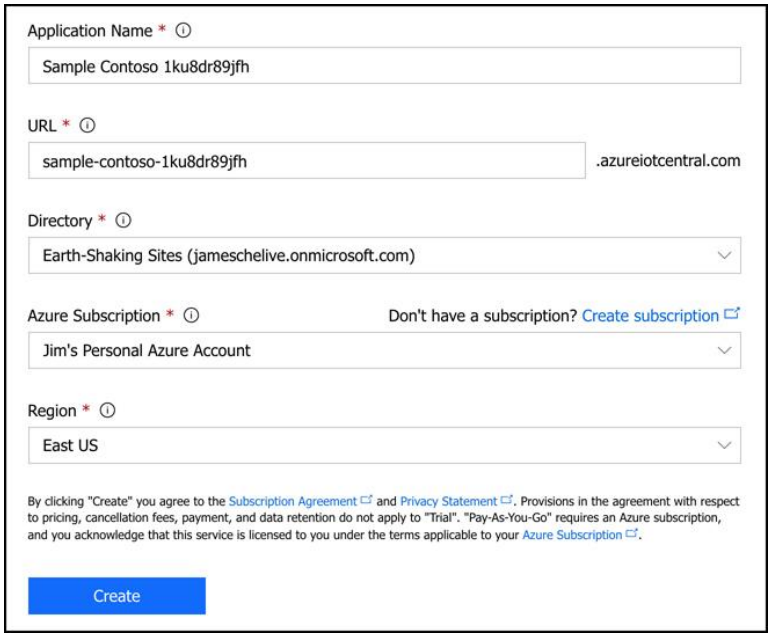


Figura 2-32 Especificación de un nombre de aplicación, URL e información de suscripción de Azure

En la Figura 2-30 , puede ver que ya hemos creado una aplicación llamada ContosoPharm. Cuando hace clic en esa aplicación, ve un menú en el lado izquierdo de la página, y si hace clic en Explorador de dispositivos, puede ver cualquier dispositivo agregado como se muestra en la Figura 2-33 .

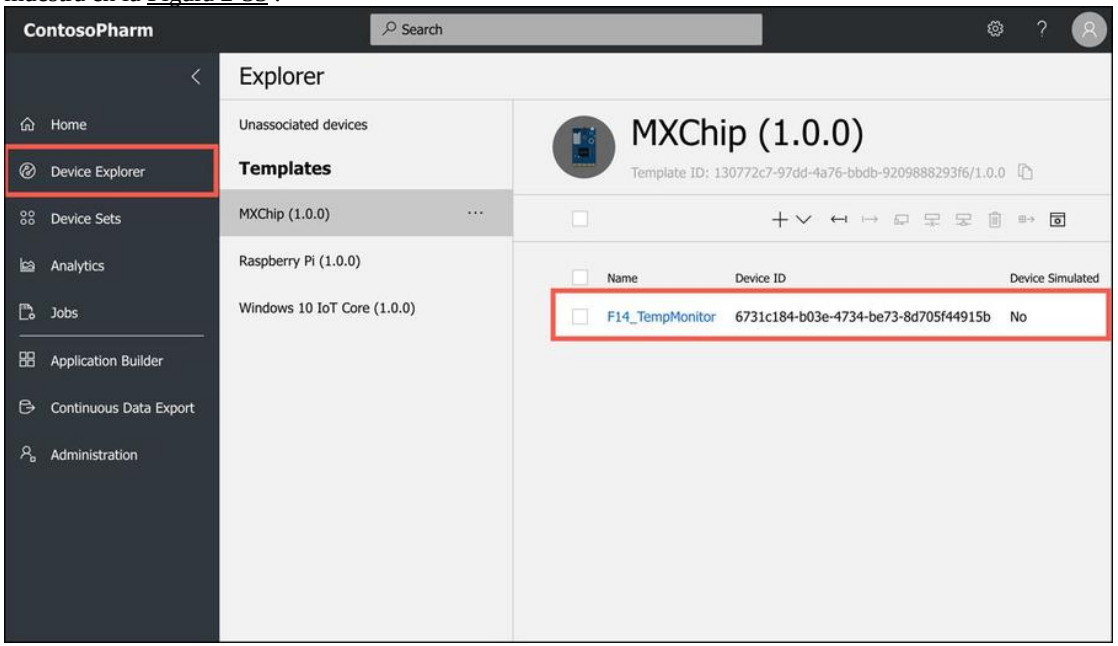


Figura 2-33 El dispositivo IoT en IoT Central

Agregue un nuevo dispositivo haciendo clic en el signo más como se muestra en la Figura 2-34 . Tiene la opción de agregar un dispositivo real si tiene uno, pero también puede agregar un dispositivo simulado. Agregar dispositivos simulados es una buena manera de configurar todo de la manera que desee en IoT Central y luego puede agregar dispositivos reales más adelante.

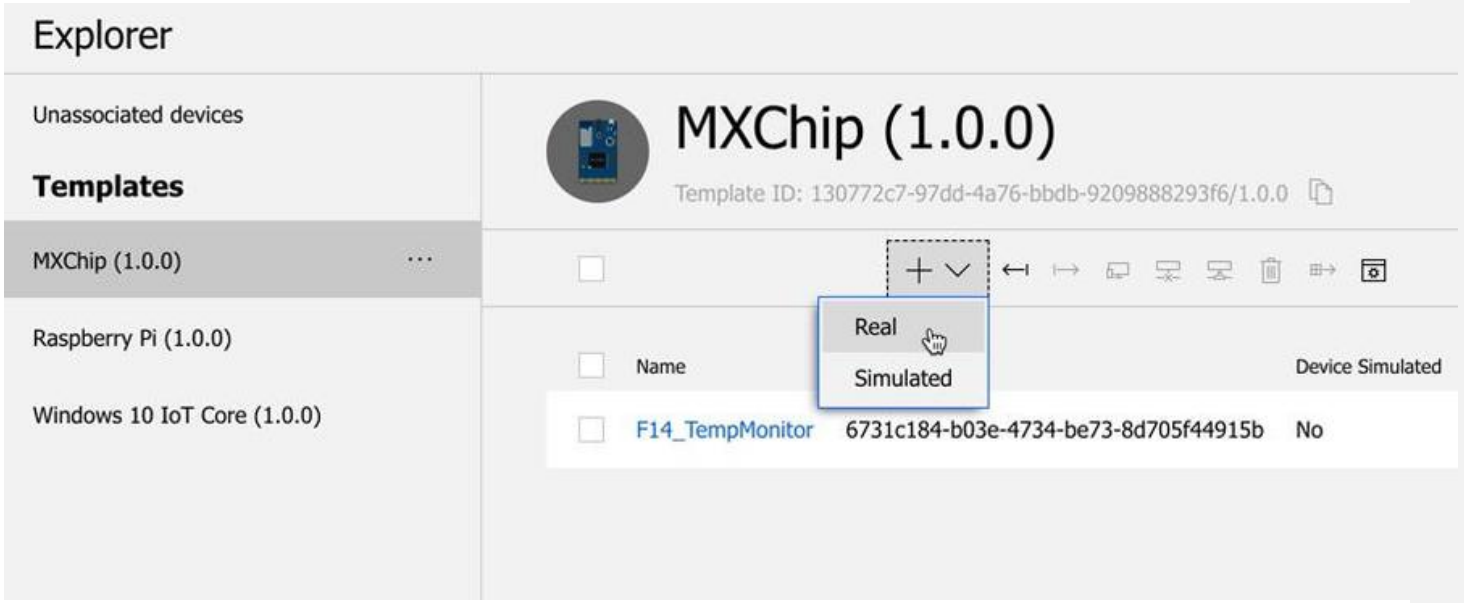


Figura 2-34 Agregar un dispositivo en IoT Central

Nota **dispositivos simulados son una característica exclusiva de IoT Central**

La capacidad de crear un dispositivo simulado es específica de IoT Central. IoT Hub no ofrece esta capacidad.

Cada página dentro de su aplicación se puede editar directamente en el navegador. La Figura 2-35 muestra la página de inicio de la aplicación IoT Central. Si hace clic en el botón Editar, puede eliminar mosaicos, agregar mosaicos y editar información en mosaicos en un punto y hacer clic en la interfaz directamente dentro de mi navegador.

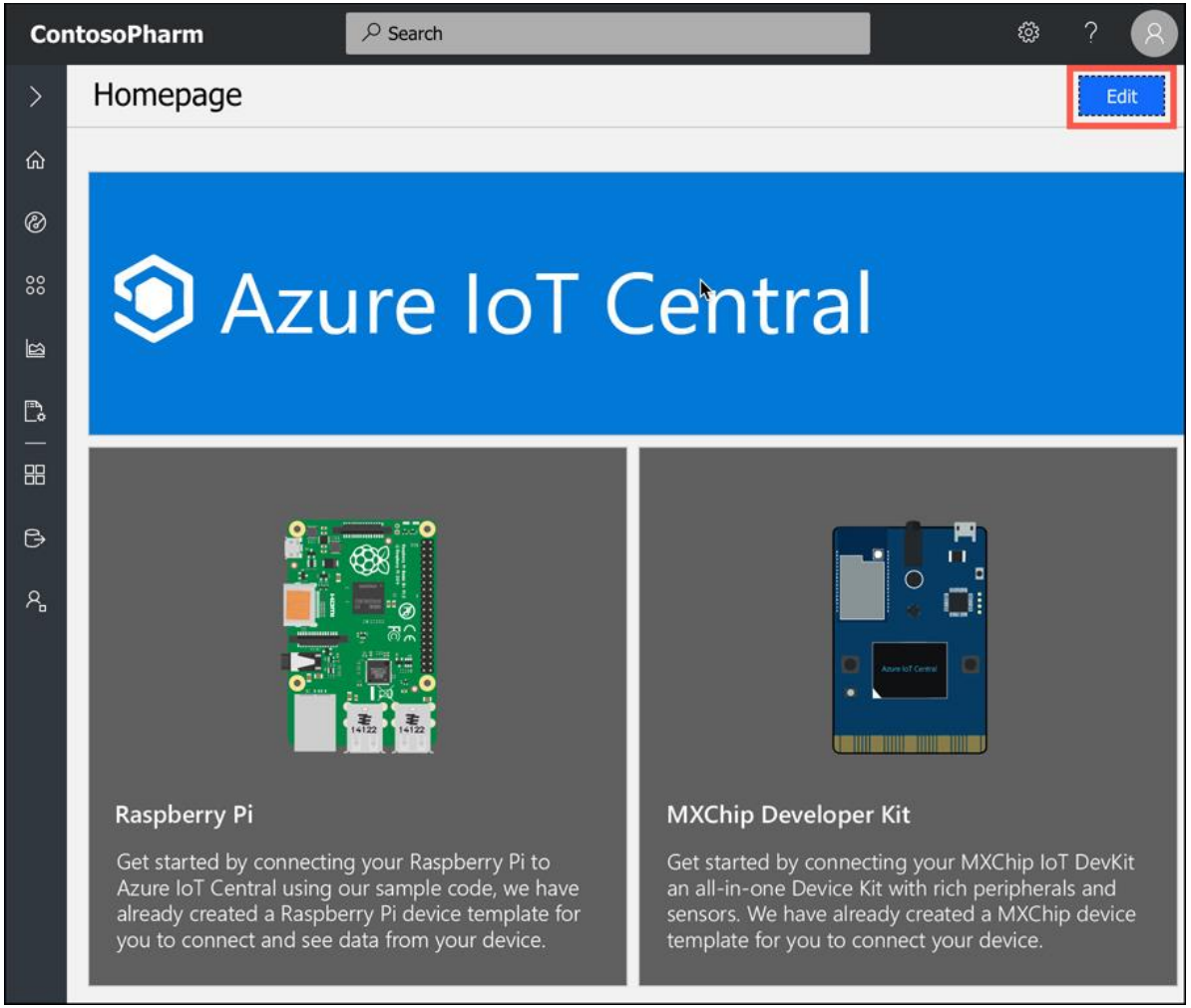


Figura 2-35 Edición de una página en IoT Central

La razón por la que vemos un botón Editar es porque este usuario está configurado como administrador de esta aplicación. IoT Central le brinda control sobre quién puede hacer qué mediante los roles. Hay tres roles integrados a los que puede asignar un usuario.

- **Los** usuarios **administradores de aplicaciones** en este rol tienen acceso completo a la aplicación y pueden editar la página y agregar nuevos usuarios.
- **Los** usuarios de **Application Builder** en este rol pueden editar páginas, pero no pueden realizar ninguna tarea administrativa, como agregar usuarios, cambiar roles de usuario, cambiar la configuración de la aplicación, etc.
- **Operador de la aplicación Los** usuarios en este rol pueden usar la aplicación, pero no pueden editar ninguna página y no pueden realizar tareas administrativas.

En algunas situaciones, estos roles integrados pueden no ofrecer la flexibilidad que necesita, por lo que Microsoft está trabajando para permitirle definir sus propios roles con permisos personalizados.

Para administrar su aplicación, haga clic en **Administración** en el menú de la izquierda como se muestra en la Figura 2-36 . Luego puede agregar y eliminar usuarios, ajustar las funciones de los usuarios, cambiar el nombre o la URL de la aplicación, agregar una imagen personalizada para su aplicación, etc. También puede copiar o eliminar su aplicación desde esta pantalla.

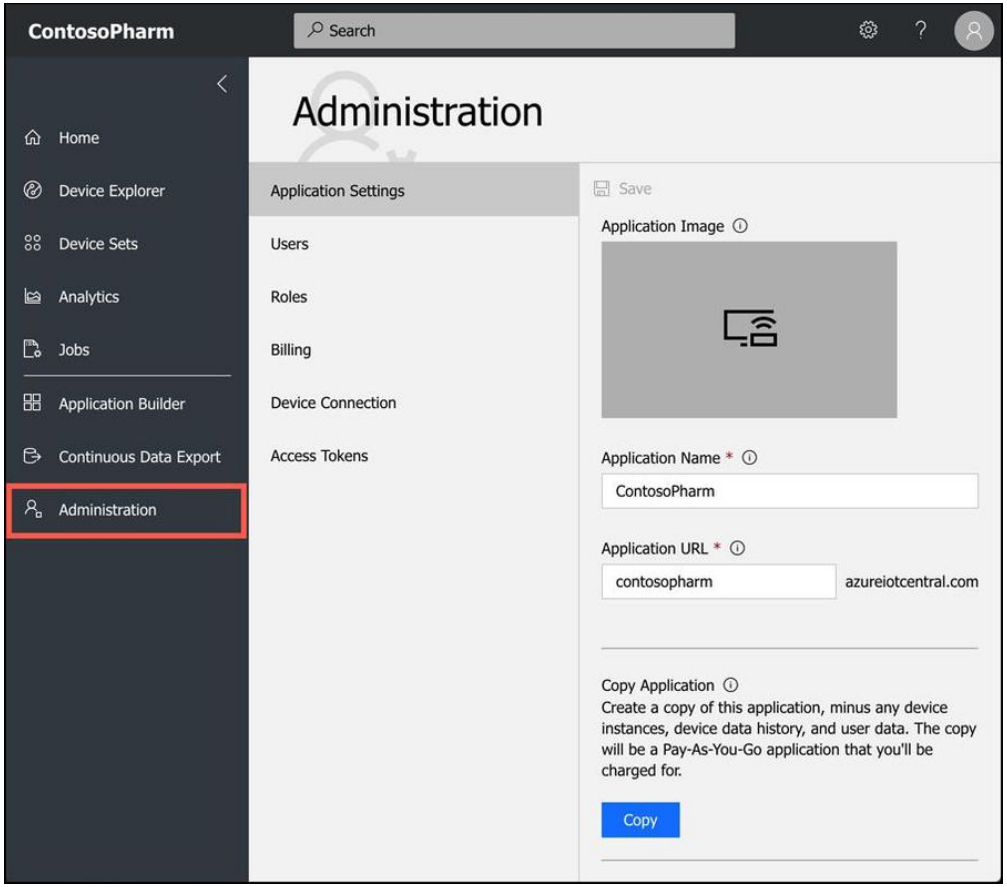


Figura 2-36 Administración de una aplicación en IoT Central

Si hace clic en un dispositivo, puede ver la información proveniente de los sensores del dispositivo. En la Figura 2-37 , puede ver los sensores de humedad y temperatura en un dispositivo F14_TempMonitor. La humedad es la línea superior y la temperatura es la línea inferior. Como puede ver, estamos experimentando un pequeño aumento de la temperatura y un aumento bastante fuerte de la humedad.

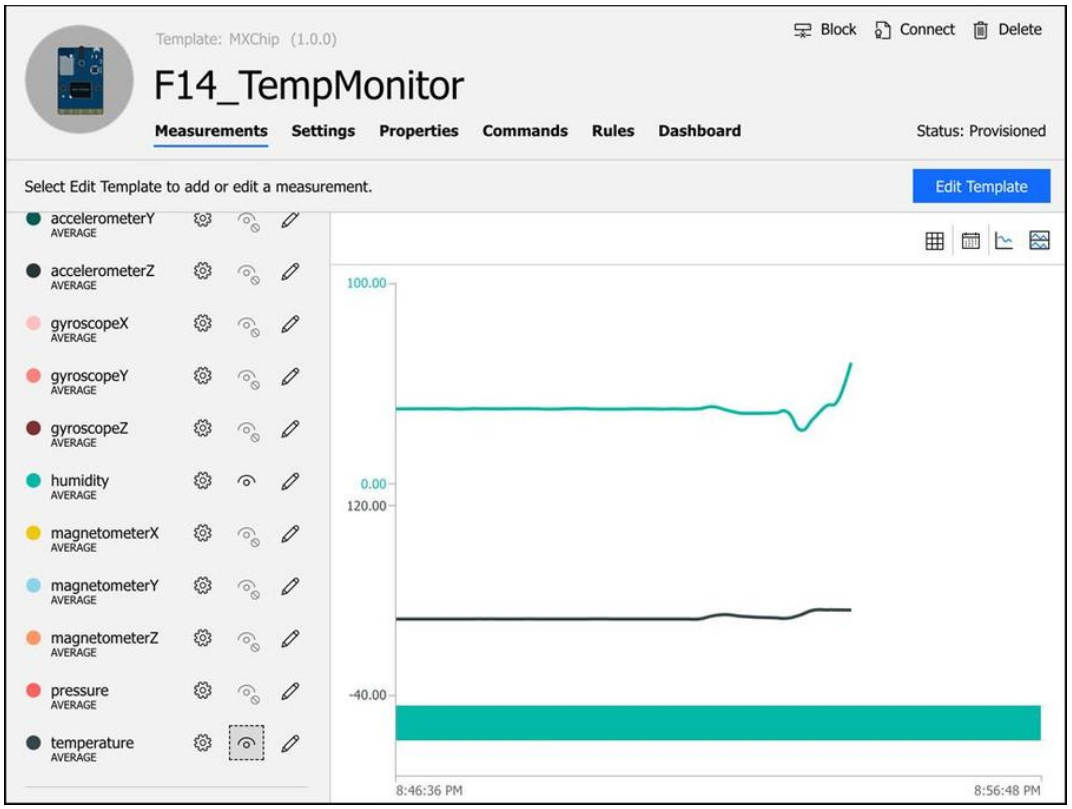


Figura 2-37 Administración de una aplicación en IoT Central

Si desea una mejor vista de los datos de su dispositivo, puede hacer clic en Panel como se muestra en la parte superior de la pantalla en la Figura 2-37 . El tablero de instrumentos, como otras páginas de su aplicación, es personalizable para que pueda ver exactamente los datos que desea. La Figura 2-38 muestra un tablero creado para un dispositivo.

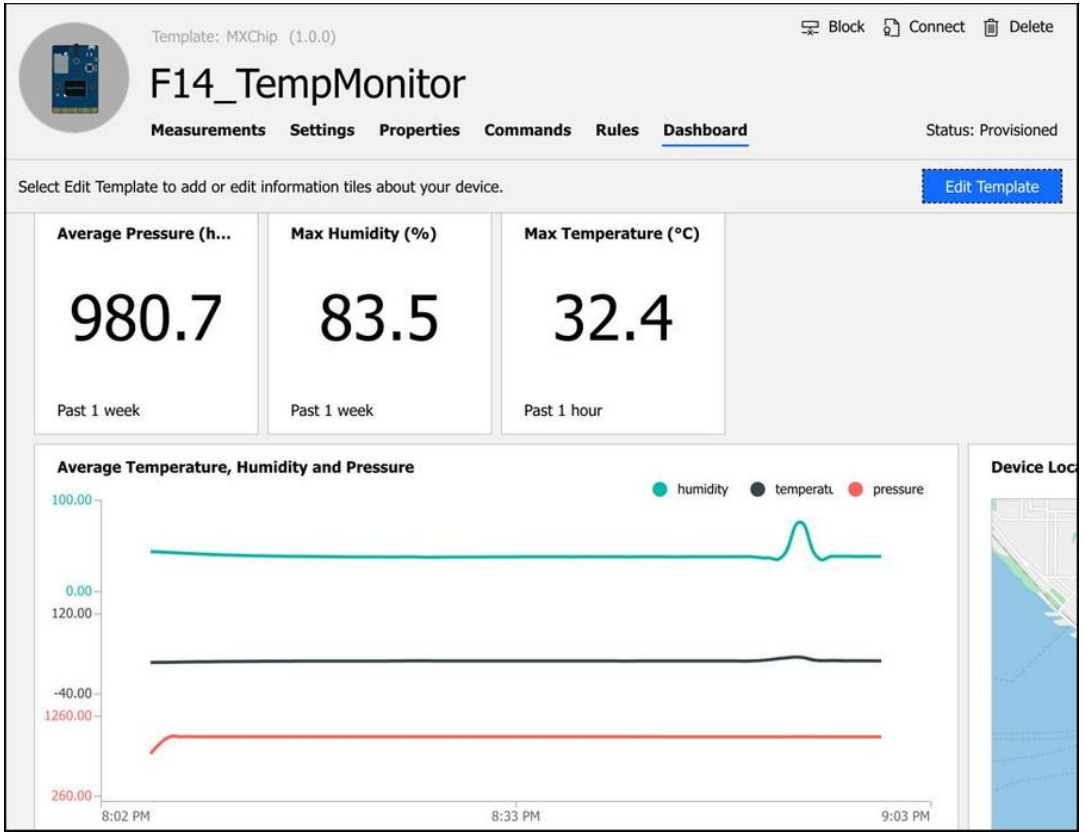


Figura 2-38 Crear un panel de control para su dispositivo

***Nota*Tableros de**

Los paneles son para un solo dispositivo. Si desea ver información personalizada para más de un dispositivo, puede agregar mosaicos para los dispositivos a su página de inicio ubicada en *https: // <your_app_name> .azureiotcentral.com.*

IoT Central también le permite configurar fácilmente reglas que supervisarán sus dispositivos y realizar una acción que elija cuando se active su regla. En la Figura 2-39 , estamos configurando una regla que se activará cuando la humedad alcance 60 o más. Tenga en

cuenta que también tenemos una vista histórica en vivo de la métrica en un gráfico a la derecha para que pueda tomar decisiones más inteligentes sobre los umbrales.

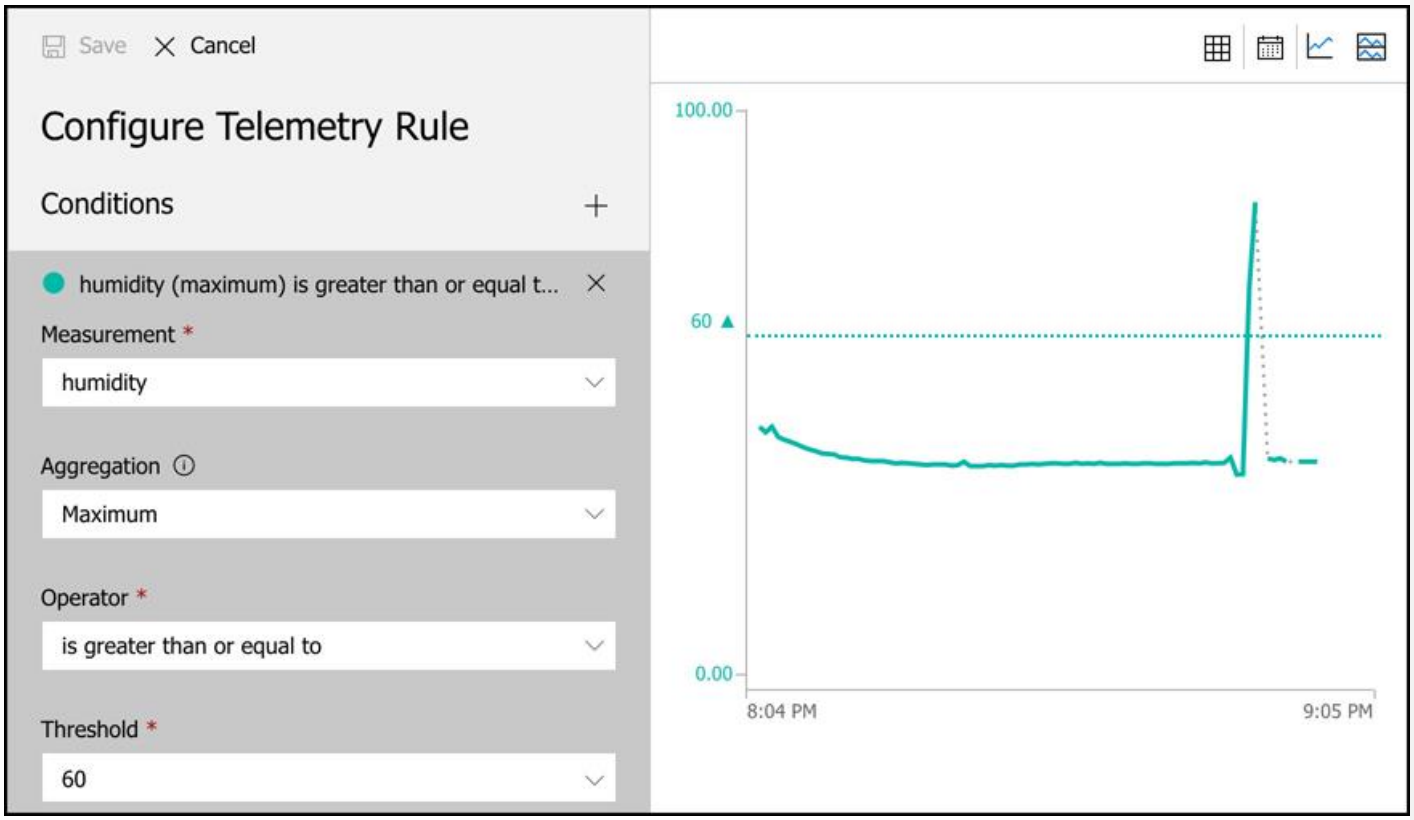


Figura 2-39 Crear una regla

Cuando se activa una regla, IoT Central puede enviar un correo electrónico a alguien con detalles de lo que sucedió. También puede elegir activar un webhook, realizar una llamada a una función de Azure, ejecutar un flujo de trabajo en una aplicación Azure Logic o ejecutar un flujo de trabajo en Microsoft Flow. Estas opciones proporcionan la flexibilidad para realizar casi cualquier tarea cuando se activa una regla.

Cuando tiene una gran cantidad de dispositivos, es conveniente agrupar los dispositivos en un conjunto de dispositivos para que pueda tomar medidas en muchos dispositivos a la vez. Para crear un conjunto de dispositivos, especifique una condición que se debe cumplir para que un dispositivo se agregue al conjunto. En la Figura 2-40 , estamos creando un conjunto de dispositivos para todos los dispositivos que tienen F14 en el nombre. Si el nombre contiene "F14", el dispositivo se agrega automáticamente al conjunto de dispositivos. Incluso cuando agregue un nuevo dispositivo más adelante, será parte de este conjunto de dispositivos si el nombre contiene "F14".

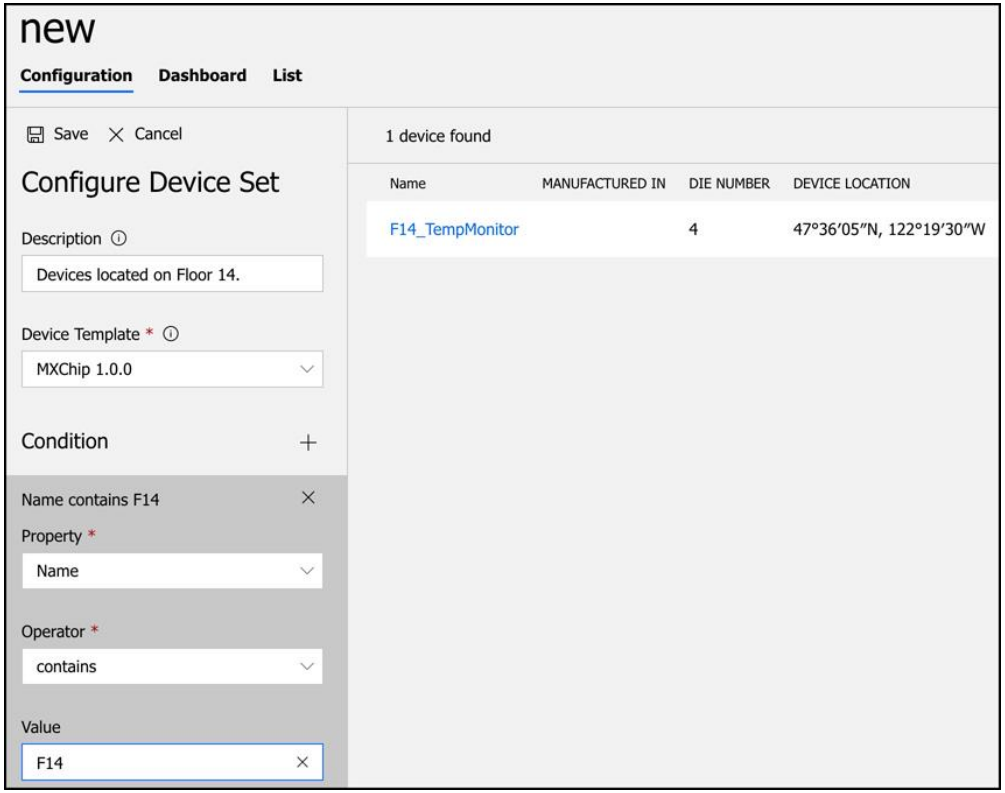


Figura 2-40 Creación de un conjunto de dispositivos

Una vez que haya creado un conjunto de dispositivos, puede tomar medidas sobre los dispositivos que contiene creando un trabajo. Haga clic en **Trabajos** en el menú principal de su aplicación para configurar su trabajo. Un trabajo puede modificar propiedades, cambiar configuraciones o enviar comandos a dispositivos. En la Figura 2-41 , creamos un trabajo que activará el sensor IR para todos los dispositivos en nuestro conjunto de dispositivos.

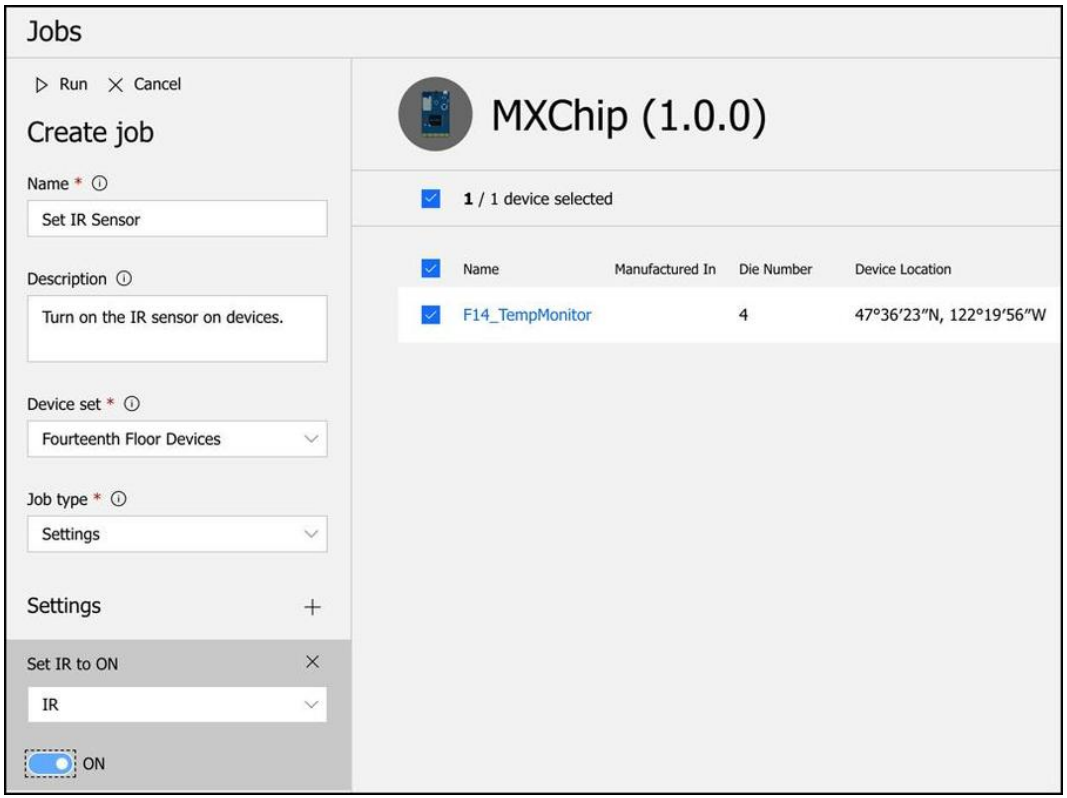


Figura 2-41 Crear un trabajo

IoT Central también le permite realizar análisis de métricas de dispositivos en un conjunto de dispositivos. Por ejemplo, puede ver todos los dispositivos que registraron temperaturas superiores a cierto nivel. Para un análisis de datos aún más rico, puede configurar IoT Central para exportar continuamente datos desde sus dispositivos a Azure Blob Storage, Azure Event Hubs o Azure Service Bus.

Big Data y analítica

Las empresas recopilan enormes cantidades de datos de muchas fuentes diferentes. Como ya ha aprendido, Microsoft ofrece un SLA en los servicios de Azure que están en el área de 99.9% + para disponibilidad. Microsoft no pone ese número allí y luego cruza los dedos para que nada salga mal. Mantienen enormes cantidades de datos sobre cómo funciona la infraestructura de Azure, y usan esos datos para predecir problemas y reaccionar ante ellos antes de que afecten a los clientes.

Debido a la enorme magnitud de la infraestructura de Azure, puede imaginar cuántos datos se están generando para cada sistema en esa infraestructura, y para cumplir con los SLA, deben poder analizar esos datos de manera confiable en tiempo real. ¿Cómo hacen exactamente eso? Realmente no puede arrojar esa cantidad de datos a una VM o un grupo de VM sin sobrecargar el sistema hasta el punto de falla.

El problema de hacer algo con la gran cantidad de datos que recopilamos es común en todas las empresas, y esto es lo que queremos decir con *big data* . Big data significa más datos de los que puede analizar a través de medios convencionales dentro del marco de tiempo deseado.

Al colocar big data en un almacén de datos, puede usar cantidades masivas de potencia informática para analizar múltiples datos en paralelo, y puede realizar análisis de los datos mucho más rápido de lo que podría hacerlo de otra manera.

Entraremos en el análisis de big data más adelante en este capítulo. Primero, hablemos sobre dónde almacenar big data. Microsoft tiene dos ofertas de Azure para almacenar grandes datos para su análisis: Azure SQL Data Warehouse y Azure Data Lake Storage. Son similares en propósito pero bastante diferentes en diseño.

Consejo de examen

Azure Blob Storage también se puede usar como un almacén de datos para Big Data. Sin embargo, SQL Data Warehouse y Data Lake Storage están diseñados explícitamente para este propósito. Microsoft también lanzó recientemente Data Lake Storage Gen2, que combina las características de Blob Storage con Data Lake Storage, por lo que el uso de Blob Storage para el almacenamiento de datos se está volviendo innecesario.

Azure SQL Data Warehouse

Azure SQL Data Warehouse está diseñado para almacenar grandes datos en forma de datos relacionales. Los datos almacenados en el Almacén de datos SQL tienen una forma bastante similar a las tablas en los datos de un servidor SQLbase, y de hecho, cuando analiza datos en el Almacenamiento de datos SQL, ejecuta consultas SQL complejas contra los datos.

SQL Data Warehouse proporciona autenticación segura utilizando la autenticación de SQL Server en la cadena de conexión, que es autenticación de nombre de usuario y contraseña, y Azure Active Directory. Una vez que un usuario se autentica, solo puede realizar acciones para las que haya sido autorizado, y esa autorización se controla a través de los permisos de la base de datos.

Mientras sus datos se encuentran en el Almacenamiento de datos SQL, se encriptan utilizando el cifrado AES-256 de cifrado de datos transparentes (TDE). Los datos se cifran utilizando una clave de cifrado de la base de datos, y esta clave está protegida por un certificado de servidor que es único para cada servidor de Base de datos SQL. Microsoft rota estos certificados al menos cada 90 días, por lo que puede estar seguro de que sus datos están seguros.

Almacenamiento de datos SQL utiliza varios métodos para controlar los costos. De hecho, en un estudio reciente de GigaOm, se descubrió que SQL Data Warehouse es un 94% menos costoso que Google BigQuery y hasta un 31% menos costoso que Amazon AWS Redshift. (SQL Data Warehouse también fue mucho más rápido en puntos de referencia que cualquiera de estas ofertas). Una forma en que SQL Data Warehouse reduce los costos es desacoplando el almacenamiento de datos de los recursos informáticos. Esto le permite escalar fácilmente a más recursos de cómputo cuando los necesita, y luego volver a escalar para ahorrar dinero cuando ya no necesite la energía.

Hay dos niveles de rendimiento disponibles en el Almacén de datos SQL, y ambos admiten la ampliación o la reducción y la pausa de recursos para que no pague por ellos. El nivel de rendimiento Gen1 mide los recursos de cómputo en unidades de depósito de datos o DWU. Cuando escala los almacenes de datos Gen1 para obtener más potencia, agrega DWU. El nivel Gen2 usa unidades de almacenamiento de datos de cómputo, o cDWU. La diferencia es que Gen2 utiliza una memoria caché local basada en disco para mejorar el rendimiento. Mientras no escale o pause el almacén de datos, la memoria caché mejorará sustancialmente el rendimiento. Si escala o pausa, cuando se reinicia el almacén de datos, la memoria caché tendrá que actualizarse, y no experimentará la misma mejora de rendimiento hasta que se complete la actualización.

Para usar el Almacén de datos SQL, crea una instancia de él en Azure y luego carga los datos en él mediante consultas en la base de datos o mediante herramientas como ADF Copy, SQL Server Integration Services o la línea de comandos. Luego puede ejecutar consultas complejas contra sus datos. Debido a la potencia de SQL Data Warehouse, las consultas que de otro modo tardarían varios minutos en ejecutarse pueden ejecutarse en segundos, y una consulta que puede tardar días en completarse puede finalizar en horas. Finalmente, puede usar Power BI de Microsoft para obtener información importante sobre sus datos en un entorno basado en un navegador web fácil de usar.

Más información **Migración de datos a Sql Data Warehouse**

Para obtener más información sobre la migración de datos a SQL Data Warehouse, consulte: *https://docs.microsoft.com/azure/sql-data-warehouse/sql-data-warehouse-migrate-data* .

Almacenamiento de Azure Data Lake

Al igual que SQL Data Warehouse, Azure Data Lake Storage está diseñado para almacenar grandes cantidades de datos que le gustaría analizar, pero Data Lake Storage está diseñado para una amplia gama de datos en lugar de datos relacionales. En un lago de datos, los datos se almacenan en *contenedores* . Cada contenedor generalmente contiene datos relacionados.

Nota **no solo Azure**

Los términos lago de datos y almacén de datos no son específicos de Azure. Son términos genéricos. Un lago de datos se refiere a un repositorio de datos no ordenados, y un almacén de datos se refiere a un repositorio de datos ordenados.

Los dos modos comunes de acceso a los datos están basados en objetos (como Azure Blob Storage) y en archivos. En un modo basado en objetos, no existe una jerarquía de objetos. Simplemente almacena el objeto en un modelo plano. Los lagos de datos tradicionales usan el modo de acceso basado en objetos, pero el uso de este modo no siempre es eficiente porque requiere que interactúes individualmente con cada objeto.

Con la introducción de Data Lake Storage Gen2, Microsoft introdujo el concepto de un espacio de nombres jerárquico para el almacenamiento. Esto organiza los objetos en un sistema de directorios muy similar a la estructura de los archivos en su computadora, y permite el uso de modelos basados en objetos y en archivos en el mismo lago de datos. Microsoft llama a esta capacidad *de almacenamiento multimodal* , y Data Lake Storage Gen2 es la primera solución basada en la nube que ofrece esta capacidad.

Data Lake Storage es ideal para realizar análisis contra grandes cantidades de datos que no se almacenan de forma relacional. Por ejemplo, la gran cantidad de información que Google o Facebook podrían haber almacenado en los usuarios se puede guardar en un lago de datos para su análisis. Sin embargo, los datos de un lago de datos a menudo no son ideales para la presentación a los usuarios de una manera fácil de entender. Las personas trabajan mejor con datos que son relacionales, y por esa razón, es bastante común que los datos sean analizados en un lago de datos y luego estructurados y trasladados a un almacén de datos para su posterior análisis y presentación.

Al igual que Azure Blob Storage, Data Lake Storage está disponible en niveles Hot, Cool y Archive. El nivel dinámico tiene los costos de almacenamiento más altos, pero los costos de acceso más bajos. El nivel de archivo tiene los costos de almacenamiento más bajos, pero tiene los costos de acceso más altos.

Si usa el almacenamiento basado en archivos en Data Lake Storage Gen2, hay algunos costos adicionales para los metadatos necesarios para implementar la jerarquía basada en archivos. También hay algunos costos adicionales asociados con las operaciones que requieren llamadas recursivas contra la jerarquía. Data Lake Storage admite varias plataformas de análisis de datos de código abierto, incluidas HDInsight, Hadoop, Cloudera, Azure Databricks y Hortonworks.

Una vez que tenga datos disponibles en SQL Data Warehouse o Data Lake Storage, puede usar uno de los servicios analíticos de Azure para analizar los datos, incluidos Azure HDInsight y Azure Databricks.

Más información **Azure Databricks**

Debido a que Azure Databricks es un servicio de big data que se usa con mayor frecuencia con el aprendizaje automático, lo discutiremos más adelante en este capítulo cuando cubramos la inteligencia artificial.

Azure HDInsight

HDInsight hace posible crear y administrar fácilmente grupos de computadoras en un marco común diseñado para realizar el procesamiento distribuido de grandes datos. HDInsight es esencialmente el servicio administrado de Microsoft que proporciona una implementación basada en la nube de una popular plataforma de análisis de datos llamada Hadoop, pero también es compatible con muchos otros tipos de clúster como se muestra en la Tabla 2-6 .

Tabla 2-6 Tipos de clúster compatibles con HDInsight

Tipo de clúster	Descripción
Hadoop	Procesamiento de datos a gran escala que puede incorporar componentes adicionales de Hadoop como Hive (para consultas similares a SQL), Pig (para usar lenguajes de script) y Oozie (un sistema de programación de flujo de trabajo).
HBase	Base de datos NoSQL extremadamente rápida y escalable.
Tormenta	Procesamiento rápido y confiable de flujos de datos ilimitados en tiempo real.
Chispa - chispear	Análisis extremadamente rápido utilizando caché en memoria a través de múltiples operaciones en paralelo.
Consulta interactiva	Análisis en memoria utilizando Hive y LLAP (procesos que ejecutan fragmentos de consultas de Hive).
Servidor R	Análisis de nivel empresarial con R, un lenguaje especializado para análisis de big data.
Kafka	Procesamiento extremadamente rápido de grandes cantidades de flujos de datos síncronos, a menudo desde dispositivos IoT.

Construir su propio clúster lleva mucho tiempo y, a menudo, es difícil a menos que tenga experiencia previa. Con HDInsight, Microsoft hace todo el trabajo pesado en su propia infraestructura. Usted se beneficia de un entorno seguro y uno fácilmente escalable para manejar grandes tareas de procesamiento de datos.

Un clúster de HDInsight realiza análisis mediante la división de grandes bloques de datos en segmentos que luego se entregan a los nodos dentro del clúster. Los nodos realizan análisis en los datos y los reducen a un conjunto de resultados. Todo este trabajo ocurre en paralelo para que las operaciones se completen dramáticamente más rápido de lo que serían de otra manera. Al agregar nodos adicionales a un clúster, puede aumentar la potencia de sus análisis y procesar más datos aún más rápido.

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

Cuando crea un clúster de HDInsight, especifica el tipo de clúster que desea crear y le da un nombre al clúster como se muestra en la Figura 2-42 . También especificará un nombre de usuario y contraseña para acceder al clúster y un usuario SSH para un acceso remoto seguro.

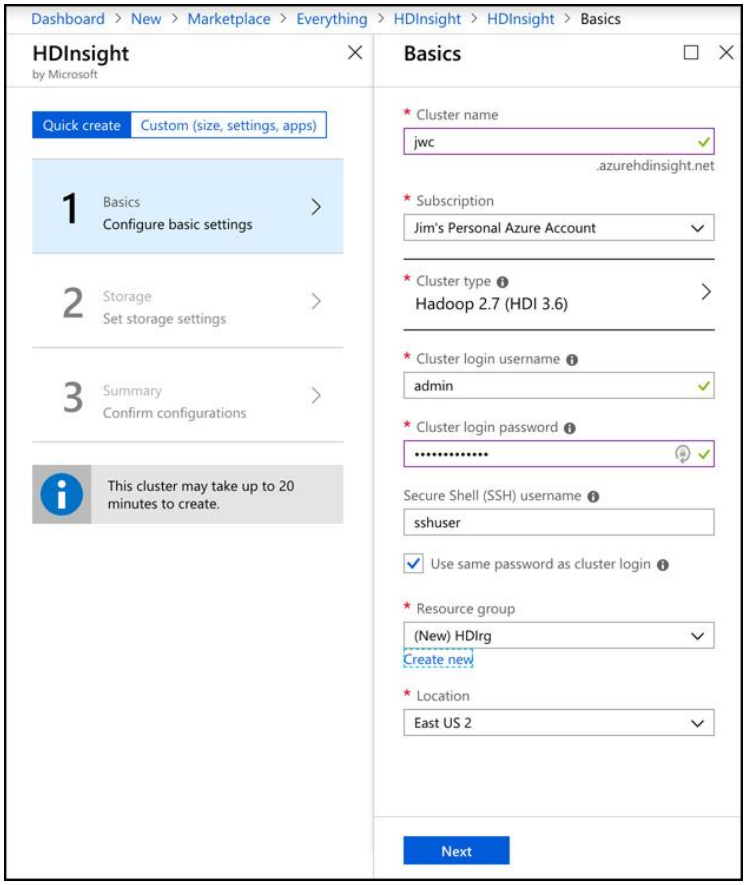


Figura 2-42 Creación de un clúster de HDInsight Hadoop

Después de hacer clic en el botón Siguiente, configura la cuenta de almacenamiento y el acceso a Data Lake Storage si lo desea. Observe en la Figura 2-43 que solo ve Data Lake Storage Gen1. Para usar Data Lake Storage Gen2, primero debe crear la cuenta de almacenamiento y completar alguna configuración adicional como se describe en: *https://azure.microsoft.com/blog/azure-hdinsight-integration-with-data-lake-storage-gen -2-preview-acl-and-security-update /* .

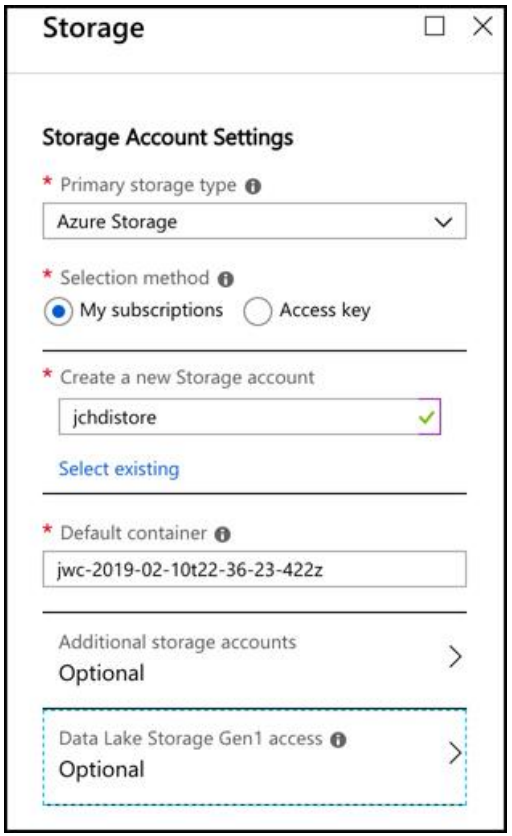


Figura 2-43 Configuración de una cuenta de almacenamiento del clúster de HDInsight

Nota de **creación rápida y personalizada**

El proceso de creación rápida en las Figuras 2-42 y 2-43 crea seis nodos Hadoop con 40 núcleos. Si desea una configuración diferente, puede hacer clic en Personalizar (como se muestra en la Figura 2-42) para especificar su propia configuración.

Una vez que comience la creación de su clúster Hadoop, puede tardar hasta 20 minutos en completarse, según su configuración. Una vez que su clúster esté listo, puede comenzar el análisis de datos escribiendo consultas sobre él. Incluso si sus consultas analizan millones de filas, HD Insight puede manejarlo, y si necesita más potencia de procesamiento, puede agregar nodos adicionales según sea necesario.

Los clústeres de HD Insight se facturan por hora, y usted paga más por hora en función de la potencia de las máquinas en su clúster. Para obtener detalles completos sobre precios, consulte: *https://azure.microsoft.com/pricing/details/hdinsight/* .

Inteligencia artificial

Volvamos a lo que hemos aprendido hasta este punto. Sabemos que la cantidad de dispositivos IoT supera con creces la cantidad de humanos, y esos dispositivos IoT están generando enormes cantidades de datos. Está bastante claro que se está recopilando una cantidad alucinante de datos.

Aprendimos sobre tecnologías que nos permiten almacenar esta enorme cantidad de datos y cómo podemos mantenerlos seguros y acceder a ellos rápidamente. De lo que no hemos hablado es de lo que hacemos con todos esos datos. Ahí es donde entra en juego la inteligencia artificial (IA).

Antes de ir demasiado lejos en la IA, primero lleguemos a un acuerdo sobre lo que entendemos por IA. Cuando muchas personas piensan en la IA de la computadora, la imagen que les viene a la mente es un androide que mata humanos o alguna otra tecnología hostil obsesionada con librar al mundo de los humanos. Se sentirá aliviado al saber que en realidad no es lo que significa AI en este contexto.

La IA de hoy se llama Inteligencia Artificial Estrecha (o a veces IA débil), y se refiere a una IA que es capaz de realizar una tarea específica de manera mucho más eficiente de lo que un humano puede realizar esa misma tarea. Toda la IA que hemos desarrollado hasta ahora es una IA débil. En el otro extremo del espectro de IA se encuentra la Inteligencia General Artificial, o IA fuerte. Este es el tipo de IA que ves representado en películas y libros de ciencia ficción, y actualmente no tenemos este tipo de capacidad.

En muchos sentidos, es un poco engañoso llamar débil a la tecnología de IA existente. Si lo coloca en el contexto de la IA fuerte imaginaria, ciertamente tiene capacidades limitadas, pero la IA débil puede hacer cosas extraordinarias, y casi seguramente se beneficiará de sus capacidades todos los días. Por ejemplo, si habla con su teléfono o su altavoz inteligente y entiende lo que ha dicho, se ha beneficiado de la inteligencia artificial.

En la edición de 1973 de Perfiles del futuro, el famoso escritor de ciencia ficción Arthur C. Clarke dijo: "Cualquier tecnología suficientemente avanzada es indistinguible de la magia". Si bien la IA aún no era una cosa cuando Clarke hizo esta afirmación, las capacidades que la IA hace posible son ciertamente aplicables, pero la IA no es mágica. La IA es en realidad matemática, y como cualquier persona familiarizada con las computadoras le dirá, las computadoras son muy buenas en matemáticas.

Para desarrollar capacidades de IA, los ingenieros informáticos se propusieron dar a las computadoras la capacidad de "aprender" de la misma manera que el cerebro humano aprende. Nuestro cerebro está formado por neuronas y sinapsis. Cada neurona se comunica con todas las otras neuronas en el cerebro, y juntas forman lo que se conoce como una red neuronal. Si bien cada neurona por sí sola no puede hacer mucho, toda la red es capaz de cosas extraordinarias.

La IA funciona creando una red neuronal digital. Cada parte de esa red neuronal puede comunicarse y compartir información con cualquier otra parte de la red. Al igual que nuestros cerebros, una red neuronal de computadora toma entrada, la procesa y proporciona salida. AI puede usar muchos métodos para procesar la entrada, y cada método es un subconjunto de AI. Los dos más comunes son la comprensión del lenguaje natural y el aprendizaje automático.

La comprensión del lenguaje natural es IA diseñada para comprender el habla humana. Si intentáramos programar una computadora para entender la palabra hablada por medios informáticos tradicionales, llevaría décadas a un ejército de programadores acercarse al reconocimiento utilizable. No solo tendrían que tener en cuenta los acentos y las diferencias de vocabulario que ocurren en diferentes regiones geográficas, sino que tendrían que tener en cuenta el hecho de que las personasa menudo pronuncian palabras de manera diferente incluso en las mismas regiones. Las personas también tienen cadencias de discurso diferentes, y eso hace que algunas palabras se unan. La computadora tiene que saber distinguir palabras individuales cuando eso no sea fácil de hacer. Además de toda esta complejidad, la computadora tiene que tener en cuenta el hecho de que el lenguaje es algo que cambia constantemente.

Dada esta complejidad, ¿cómo desarrolló Amazon alguna vez el Echo? ¿Cómo entiende Siri lo que dices? ¿Cómo sabe Cortana hacer un chiste inteligente cuando le preguntamos sobre Siri? La respuesta en todos estos casos es la IA. Tenemos millones de horas de grabaciones de audio, y tenemos millones de horas más en videos que incluyen audio. Hay tantos datos disponibles que ningún ser humano podría procesarlos, pero una computadora procesa los datos mucho más rápido. No solo tiene más vías analíticas que los humanos, sino que también procesa la información mucho más rápido.

Más información Las **computadoras son rápidas**

Cuando digo que las computadoras pueden procesar información más rápidamente que los humanos, ¡lo digo en serio! La información en un cerebro humano viaja entre las neuronas a una velocidad que está justo por debajo de la velocidad del sonido. Si bien eso es bastante rápido para nuestras necesidades, no es nada en comparación con las computadoras. La información en una red neuronal de IA viaja a la velocidad de la luz, y eso es lo que permite a las computadoras procesar enormes cantidades de datos. De hecho, el sistema de inteligencia artificial de una computadora puede procesar 20,000 años de aprendizaje a nivel humano en solo una semana.

Si introducimos todas esas grabaciones en un motor de comprensión del lenguaje natural, tiene muchos ejemplos para determinar qué palabras estamos hablando cuando decimos algo a un altavoz o teléfono inteligente, y determinar el significado de estas palabras es simplemente reconocimiento de patrones. Como Apple, Amazon y Microsoft estaban trabajando en esta tecnología, la ajustaron al recibir sus comentarios. A veces, en realidad, podrían preguntarte si lo hicieron bien, y otras veces, podrían suponer que algo está mal si acabas de abandonar la conversación antes. Con el tiempo, el sistema mejora y mejora a medida que obtiene más datos.

El aprendizaje automático (ML) es similar en el sentido de que utiliza una red neuronal para realizar una tarea, pero la tarea es diferente a la comprensión del habla. De hecho, el aprendizaje automático se puede utilizar en muchas aplicaciones. Uno de los usos comunes del aprendizaje automático es el reconocimiento de imágenes. Como resultado, las redes neuronales de IA son particularmente buenas para reconocer patrones en imágenes, y al igual que el audio, tenemos una enorme cantidad de datos para trabajar.

 *Consejo de examen*

En ML, el proceso de toma de decisiones en varios puntos a lo largo de la red neuronal AI se conoce como la tubería ML. Es una serie de decisiones tomadas por el modelo ML que eventualmente resulta en un resultado particular.

Muchos ejemplos de ML se relacionan con el procesamiento de imágenes porque ML es muy adecuado para hacer ese tipo de trabajo. Sin embargo, una gran cantidad de ML se enfoca en usar los datos existentes para hacer una predicción sobre lo que sucederá en el futuro y hacerlo con un alto grado de confiabilidad.

Es probable que todos sepamos que los satélites han estado fotografiando la superficie de la tierra durante bastante tiempo. Tenemos imágenes detalladas de casi cada pulgada cuadrada de nuestro planeta, y esas imágenes son valiosas en muchos sentidos. Por ejemplo, los científicos que están trabajando en los esfuerzos de conservación se benefician al saber cómo nuestro planeta está cambiando con el tiempo. Los ingenieros forestales necesitan saber sobre la salud de nuestros bosques. Los conservacionistas de la vida silvestre necesitan saber dónde enfocar los esfuerzos en dónde los animales están en mayor riesgo. Al aplicar un modelo ML a todas estas imágenes, Microsoft puede satisfacer todas estas necesidades.

Más información **Microsoft AI para la Tierra**

Para obtener más información sobre todas las formas en que Microsoft usa la IA para la conservación y las ciencias de la tierra, consulte: *http://aka.ms/aiforearth* .

El análisis de imágenes AI no se limita a la escala planetaria. También es útil cuando queremos buscar en nuestras propias imágenes. Quizás desee encontrar todas las fotografías que haya tomado de una persona en particular, o tal vez esté interesado en encontrar todas sus fotografías de flores. Es probable que su teléfono pueda hacer este tipo de cosas, y lo hace usando AI y ML. De hecho, Google Photos incluso puede identificar personas específicas en las fotos cuando el tiempo entre dos fotos está separado por décadas. Todo esto usa ML.

ML utiliza un algoritmo de aprendizaje que es la base de la IA. Una vez que se desarrolla el algoritmo, se le suministran datos de prueba y se examina el resultado. Según ese resultado, puede determinar que necesita ajustar el algoritmo. Una vez que el algoritmo es adecuado para su tarea, generalmente lo implementa en un entorno donde tiene una gran variedad de recursos informáticos que puede

asignarle. Luego puede alimentar grandes cantidades de datos para su procesamiento. A medida que el algoritmo trata con más datos, puede mejorarse al reconocer patrones.

Cuando prueba un modelo de ML, generalmente configura un escenario en el que solo una parte de su conjunto de datos completo se envía a su modelo para capacitación. Una vez que su modelo está entrenado, envía el resto de sus datos a través de su modelo para calificar los resultados. Como se trata de un conjunto de datos histórico, ya sabe lo que su modelo está tratando de resolver, por lo que puede determinar con precisión la precisión de su modelo. Una vez que haya alcanzado la precisión deseada de su modelo, puede implementarlo y comenzar a usarlo contra los datos de producción.

Incluso con un modelado y puntuación cuidadosos, los algoritmos de ML pueden cometer errores. En un artículo sobre ML publicado en 2016, Marco Ribeiro, Sameer Singh y Carlos Guestrin escribieron sobre un experimento de ML diseñado para mirar imágenes y diferenciar entre perros y lobos. Como resultado, el algoritmo estaba cometiendo muchos errores, pero los humanos no podían entender por qué.

Cuando regresaron y probaron el algoritmo ML para determinar cómo estaba tomando estas decisiones incorrectas, descubrieron que el algoritmo había llegado a la conclusión de que las imágenes con lobos en ellas tenían un fondo nevado y las imágenes con perros tenían hierba en el fondo. Por lo tanto, cada imagen con una criatura parecida a un perro que se tomó en un fondo nevado se clasificó de inmediato (a veces incorrectamente) como un lobo.

Más información **AI y confianza**

La analogía del lobo ilustra una de las principales preocupaciones de la IA, y es cómo determinar cuándo confiar en un modelo de IA. Si desea profundizar en este concepto, consulte este documento al que se hace referencia en: *https://arxiv.org/pdf/1602.04938.pdf* .

Cuando se trata de desarrollar y usar AI con la enorme cantidad de datos disponibles hoy en día, la nube ofrece algunas ventajas distintas. Puede aprovechar los enormes recursos informáticos que los proveedores de la nube ponen a su disposición, y puede usar esos recursos en segmentos de tiempo solo cuando necesite trabajar. Esto hace posible utilizar recursos más potentes de los que tendría disponibles en las instalaciones, y también permite controlar sus costos al escalar su uso.

Microsoft ofrece muchas tecnologías en Azure para ayudarlo con sus necesidades de IA y ML. Incluso puede comenzar sin hacer su propio trabajo de IA y ML utilizando algunos de los servicios proporcionados que Microsoft mismo utiliza. Estos servicios forman parte de Azure Cognitive Services e incluyen:

- **Visión por computadora** Analice imágenes y reconozca caras, texto y escritura a mano.
- **Microsoft Speech** Reconoce, transcribe y traduce el discurso.
- **Servicio inteligente de comprensión del lenguaje (LUIS)** Servicio de lenguaje natural que utiliza ML para comprender el habla y tomar medidas al respecto.

- **Búsqueda de Azure y Búsqueda de Bing Busque** datos específicos para crear conjuntos de datos complejos.

Estas ofertas le permiten acelerar sus capacidades de ML aprovechando el trabajo que Microsoft ha realizado para respaldar sus propios servicios como Bing, Office 365 y más. Microsoft también proporciona recursos que puede usar para crear sus propias ofertas utilizando muchas de las herramientas con las que los ingenieros ya están familiarizados. Incluso proporcionan un entorno de desarrollo rico en funciones llamado Visual Studio Code que ejecuta multiplataforma y permite el desarrollo rápido de modelos ML.

Microsoft también admite numerosos marcos de ML que los desarrolladores de soluciones de inteligencia artificial utilizan habitualmente. Estos incluyen ONNX (Open Neural Network Exchange), Pytorch, TensorFlow y Sci-Kit Learn. Esto permite a los programadores de IA (conocidos como *científicos de datos*) comenzar en Azure sin tener que aprender nuevos marcos y técnicas.

Los servicios de Azure dirigidos a científicos de datos ejecutan los marcos mencionados anteriormente. Estos servicios incluyen Azure Databricks, Azure Machine Learning Service y Azure Machine Learning Studio. Los servicios de infraestructura son componentes de infraestructura especialmente adecuados para AI y ML.

Azure Databricks

Hemos analizado algunos de los servicios de Azure para almacenar grandes datos como SQL Data Warehouse y Azure Data Lake Storage. Los datos que se almacenan en estos servicios suelen ser datos sin procesar que a menudo no están estructurados y son difíciles de consumir para construir un modelo de ML. También podemos necesitardatos para nuestro modelo de ML que provienen de múltiples fuentes, algunas de las cuales incluso pueden estar fuera de Azure. Azure Databricks es una solución ideal para acumular datos y para formar los datos (denominado *modelado de datos*) para que sea óptimo para los modelos ML.

La Figura 2-44 muestra una nueva instancia de un recurso Azure Databricks. Toda su interactividad con Databricks se realiza a través del espacio de trabajo de Databricks, un portal basado en la web para interactuar con sus datos, y para acceder al espacio de trabajo, haga clic en el botón **Iniciar espacio de trabajo que** se muestra en la Figura 2-44 .

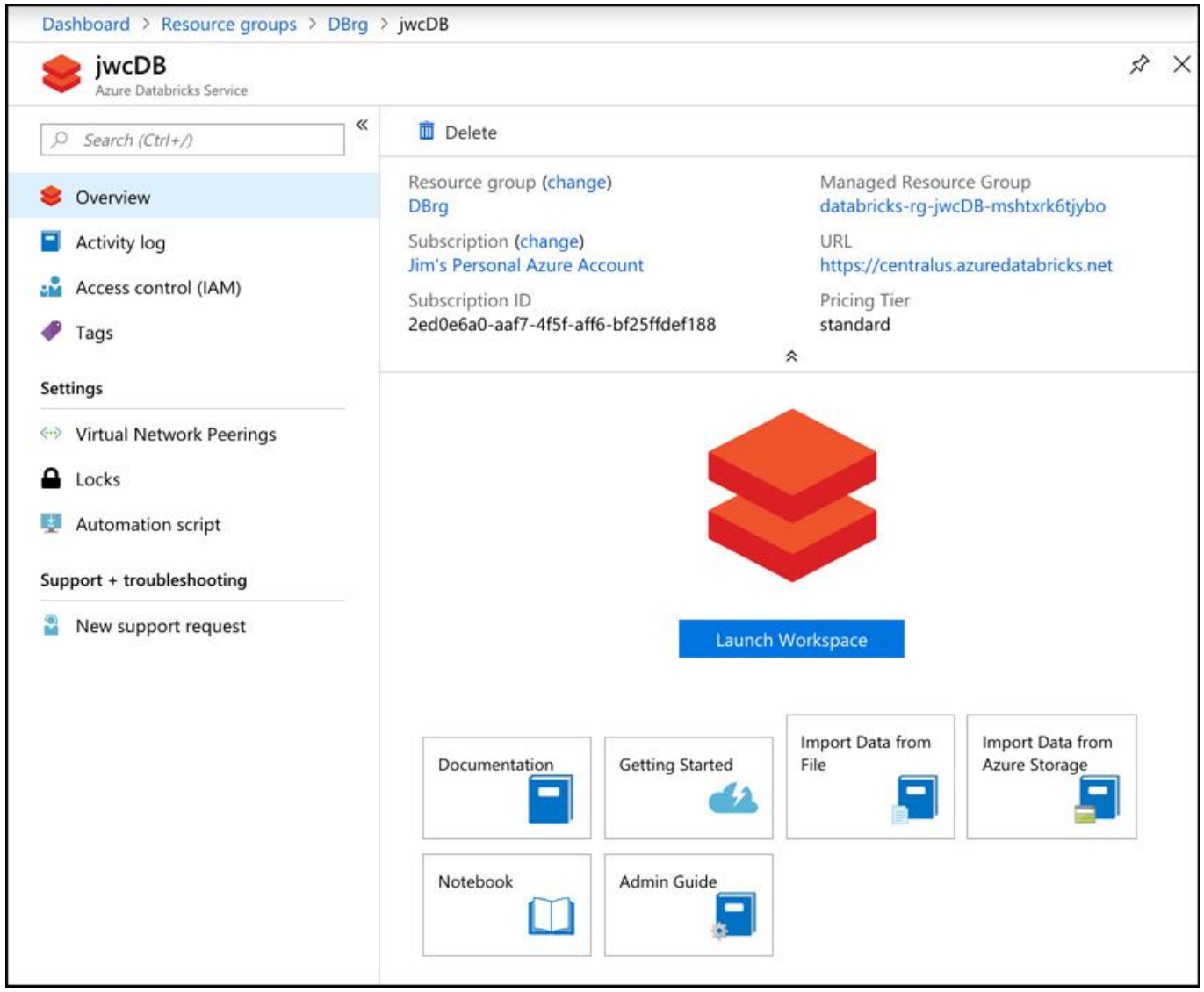

Dashboard > Resource groups > DBrg > jwcDB
jwcDB
Azure Databricks Service
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Settings
Virtual Network Peerings
Locks
Automation script
Support + troubleshooting
New support request
Delete
Resource group (change)
DBrg
Subscription (change)
Jim's Personal Azure Account
Subscription ID
2ed0e6a0-aaf7-4f5f-aff6-bf25ffdef188
Managed Resource Group
databricks-rg-jwcDB-mshtxrk6tjybo
URL
https://centralus.azuredatabricks.net
Pricing Tier
standard
Launch Workspace
Documentation
Getting Started
Import Data from File
Import Data from Azure Storage
Notebook
Admin Guide

Figura 2-44 Una instancia de Azure Databricks en Azure Portal

Al hacer clic en **Iniciar espacio de trabajo** , se lo dirige al espacio de trabajo de Databricks. Azure iniciará sesión automáticamente cuando lo haga con su cuenta de Azure. Mi instancia de Databricks está completamente vacía en este momento. En el lado izquierdo de la página (como se muestra en la Figura 2-45) hay enlaces para acceder a todas las entidades de Databricks, como espacios de trabajo, tablas y trabajos. También hay una sección de Tareas comunes, que le permite acceder a estas entidades, así como crear nuevos cuadernos, que se detallarán pronto.

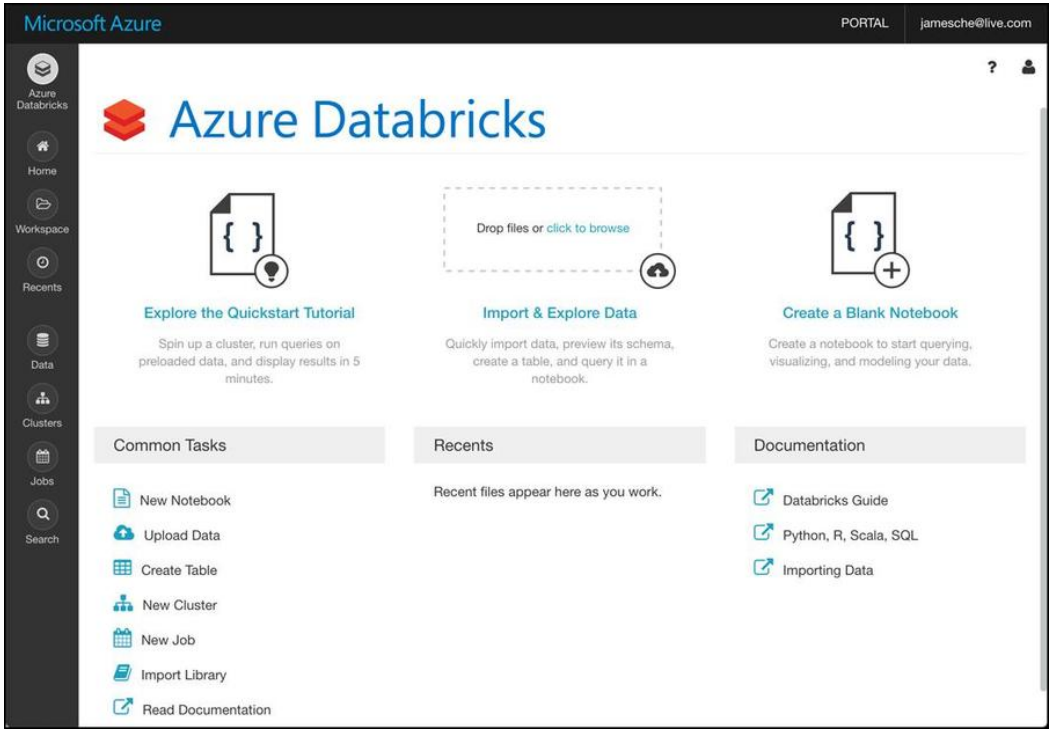


Figura 2-45 El portal de Azure Databricks

Ahora creemos un clúster. Databricks realiza todo su trabajo utilizando clústeres, que son los recursos informáticos. Para crear un clúster, puede hacer clic en **Nuevo clúster** en **Tareas comunes** . Ahora verá la pantalla Crear clúster que se muestra en la Figura 2-46 , donde el nuevo clúster se denominó "jcCluster", y todas las demás opciones son las predeterminadas.

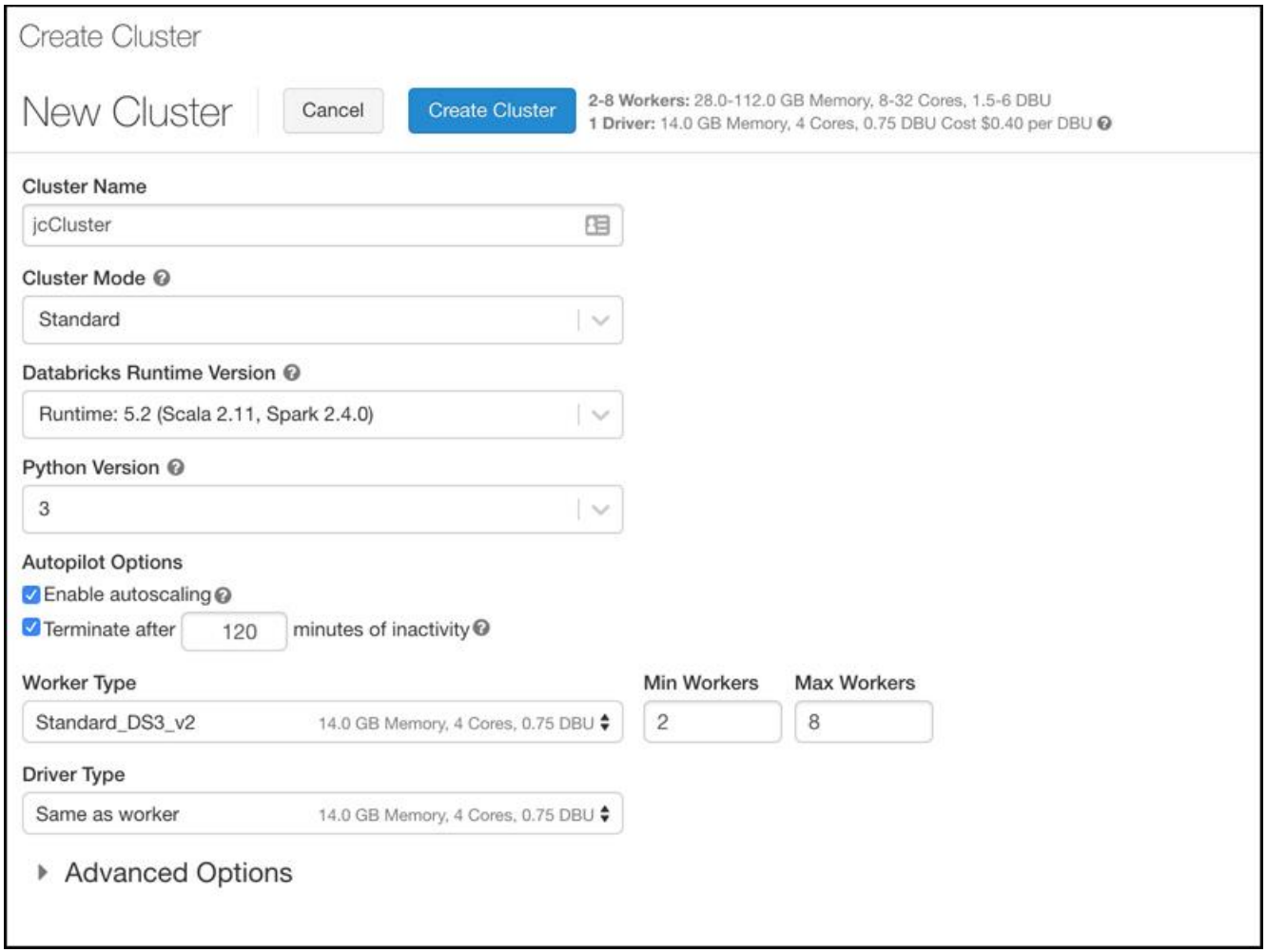


Figura 2-46 Creación de un clúster de Databricks

A continuación, crearemos un cuaderno. Los cuadernos son una forma poderosa de presentar e interactuar con datos relacionados. Cada cuaderno contiene no solo datos, sino también visualizaciones y documentación de esos datos para ayudarnos a

comprender los datos. Una vez que sus datos estén en su computadora portátil, puede ejecutar comandos contra marcos ML para construir su modelo ML directamente dentro de su computadora portátil.

Al hacer clic en el botón Azure Databricks en el menú de la izquierda (que se muestra en la Figura 2-45), puede hacer clic en **Nuevo cuaderno** para crear un cuaderno. En la Figura 2-47 , creamos un nuevo cuaderno que usa SQL como el idioma principal. Databricks asumirá que el código escrito en este cuaderno será código SQL a menos que se especifique. También puede elegir especificar Python, Scala o R como el idioma.

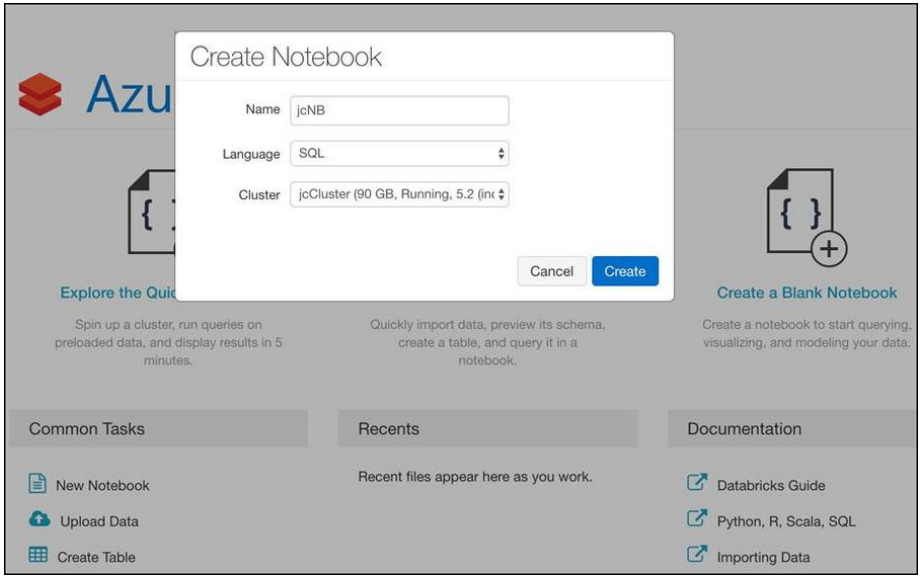


Figura 2-47 Crear un cuaderno

Después de crear un cuaderno nuevo, verá un cuaderno vacío con una celda. Dentro de esa celda, puede ingresar cualquier dato que desee. Por ejemplo, es posible que desee tener alguna documentación que defina lo que contiene este cuaderno. La documentación en los cuadernos se ingresa utilizando *Markdown* , un lenguaje que es muy adecuado para escribir documentación. La Figura 2-48 muestra el nuevo cuaderno con algunas rebajas que documentan lo que está en el cuaderno. Observe que el descuento comienza con "% md". Esto le dice a Databricks cómo el contenido que sigue está en Markdown y no en el lenguaje primario de SQL.

Figura 2-48 Documentando un cuaderno usando Markdown

Si hace clic fuera de esta celda, el código de reducción se representará en formato HTML. Para agregar algunos datos a este cuaderno, debe crear una nueva celda presionando "B" en su teclado o pasando el cursor sobre la celda existente y haciendo clic en el botón "+" para agregar una nueva celda.

Nota **Atajos de teclado**

Los atajos de teclado son, con mucho, la forma más rápida de trabajar en Databricks. Puede encontrar la lista completa de métodos abreviados de teclado haciendo clic en el enlace "Métodos abreviados" que se muestra en la Figura 2-48 .

Después de presionar "B" en su teclado, se inserta una nueva celda al final de su computadora portátil. Puede ingresar algún código SQL en esta celda para completar una tabla con algunos datos como se muestra en la Figura 2-49 . (Este código fue tomado del tutorial de inicio rápido de Databricks en *https://docs.azuredatabricks.net/getting-started/index.html* .) Después de ingresar su código, puede ejecutarlo haciendo clic en el botón **Ejecutar** .

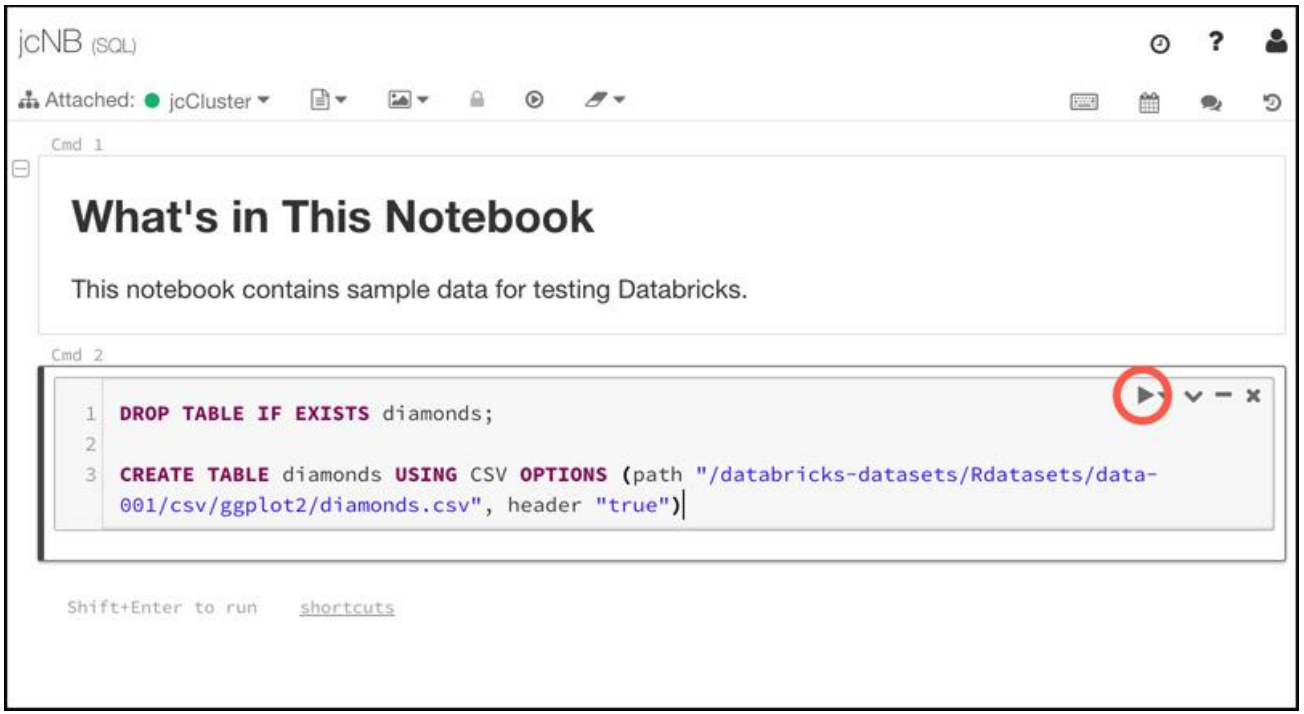


Figura 2-49 Agregar código y ejecutar un comando

***Más información de* dónde provienen los datos**

Observe que la ruta ingresada para los datos comienza con / databricks-datasets. Al crear un clúster, obtiene acceso a una colección de conjuntos de datos llamados Conjuntos de datos de Azure Databricks. En estos conjuntos de datos se incluyen algunos datos de muestra en un formato de valores separados por comas, y la ruta especificada apunta a esos datos. Cuando se ejecuta este comando, extrae esos datos en su computadora portátil.

Puede ejecutar una consulta con los datos que se agregaron usando el comando que se muestra en la Figura 2-49 escribiendo una consulta SQL en una nueva celda. La Figura 2-50 muestra los resultados de una consulta contra los datos.

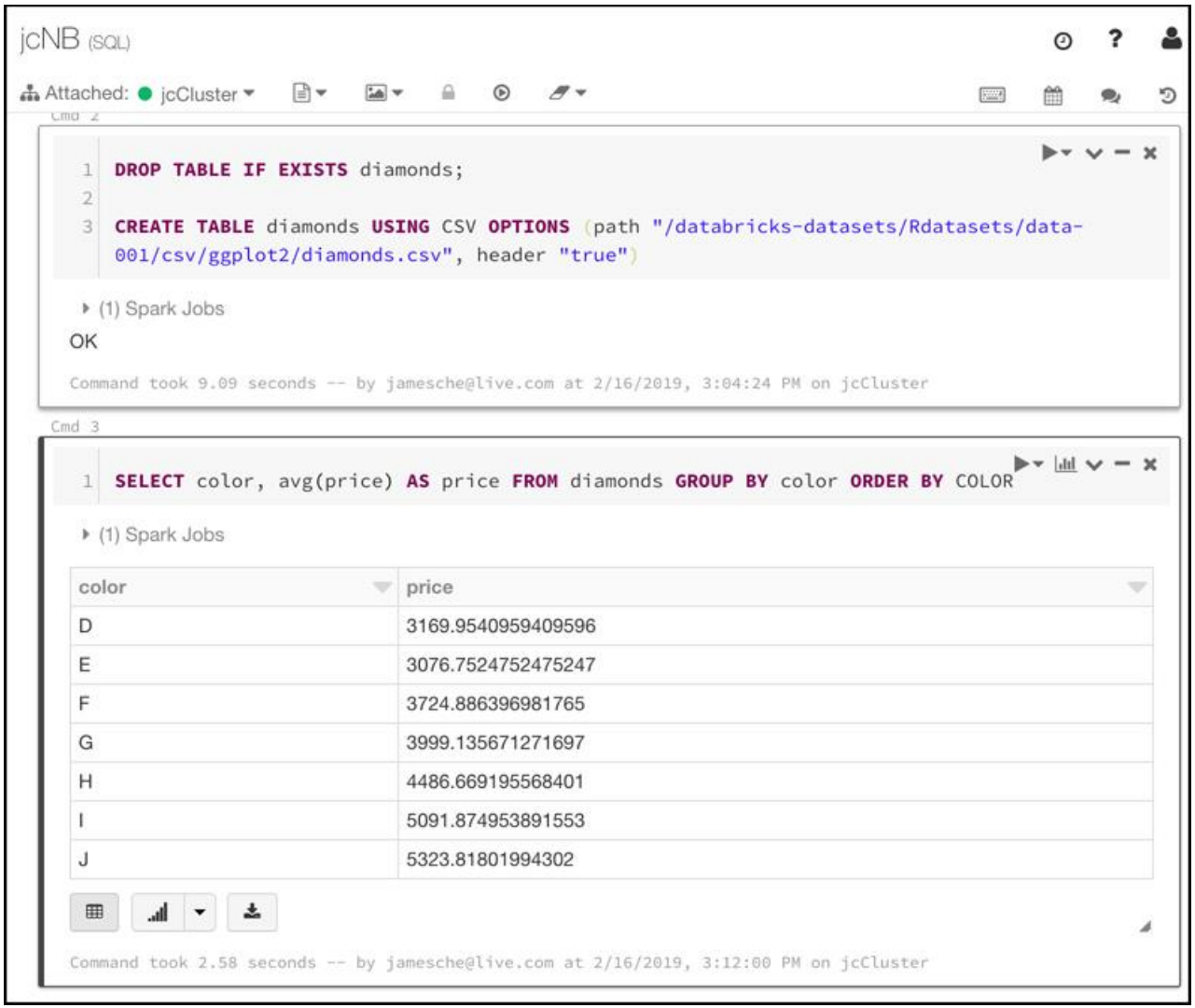


Figura 2-50 Consultando mis datos

Cuando ejecuta comandos en una celda, Databricks crea un trabajo que se ejecuta en los recursos informáticos que asignó a su clúster. Databricks utiliza un modelo de computación sin servidor. Eso significa que cuando no está ejecutando ningún trabajo, no tiene ninguna máquina virtual o recursos informáticos asignados. Cuando ejecuta un trabajo, Azure asignará máquinas virtuales a su clúster temporalmente para procesar ese trabajo. Una vez que se completa el trabajo, libera esos recursos.

Este ejemplo es bastante simple, pero ¿cómo se relaciona todo esto con ML? Azure Databricks incluye Databricks Runtime for Machine Learning (Databricks Runtime ML) para que pueda usar datos en Databricks para entrenar algoritmos de ML. Databricks Runtime ML incluye varias bibliotecas populares para ML, que incluyen: Keras, PyTorch, TensorFlow y XGBoost. También permite utilizar Horovod para algoritmos de aprendizaje profundo distribuidos. Puede usar estos componentes sin usar Databricks Runtime ML. Son de código abierto y están disponibles gratuitamente, peroDatabricks Runtime ML le ahorra la molestia de aprender cómo instalarlos y configurarlos.

Consejo de examen

Una discusión sobre cómo programar los modelos ML está muy fuera del alcance del examen AZ-900 y no lo discutiremos aquí. El punto importante a recordar es que Databricks funciona con marcos de ML de terceros para permitirle construir modelos de ML.

Para utilizar Databricks Runtime ML, deberá especificarlo cuando cree su clúster o editar su clúster existente para usarlo. Para ello, elija uno de los tiempos de ejecución de ML como se muestra en la Figura 2-51 .

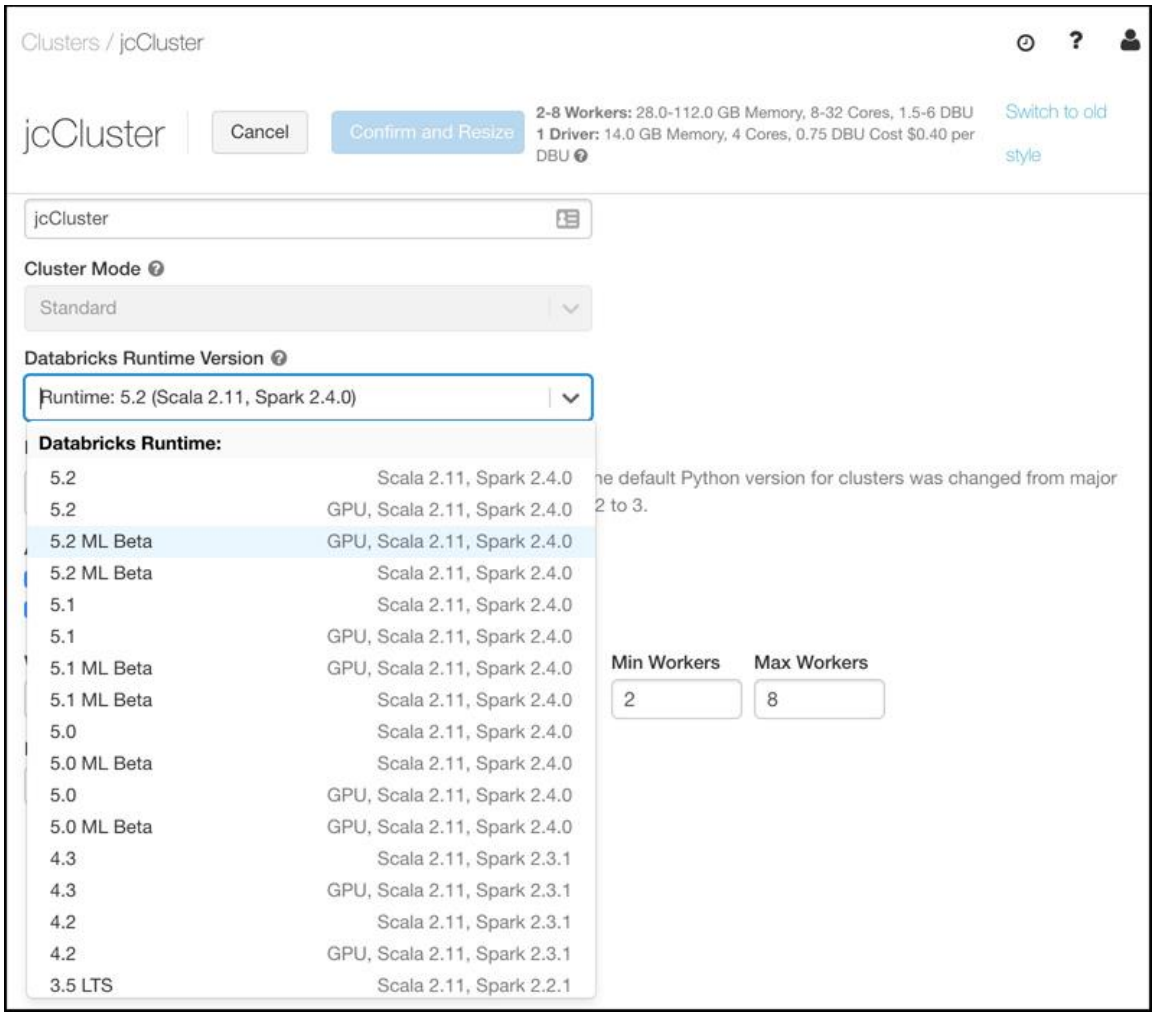


Figura 2-51 Databricks Runtime ML en la configuración del clúster

No está limitado a las bibliotecas incluidas con Databricks Runtime ML. Puede configurar la mayoría de las herramientas de ML de terceros en Azure Databricks, y Microsoft proporciona algunos consejos sobre cómo hacerlo en su documentación ubicada en: *https://docs.azuredatabricks.net/spark/latest/mllib/index.html#third- fiestas-bibliotecas* .

 ***Consejo de examen***

Es posible que haya notado varias referencias a Spark en Databricks. Esto se debe a que Databricks se basa en Apache Spark, un sistema de código abierto para realizar trabajos informáticos en un entorno agrupado.

Una vez que haya construido su modelo ML en Databricks, puede exportarlo para usarlo en un sistema ML externo. Este proceso se conoce como *producción de* la tubería ML, y Databricks le permite realizar la producción usando dos métodos diferentes: MLeap y Databricks ML Model Export.

MLeap es un sistema que puede ejecutar un modelo de ML y hacer predicciones basadas en ese modelo. Databricks le permite exportar su modelo a lo que se llama un paquete MLeap. Luego puede usar ese paquete en MLeap para ejecutar su modelo contra nuevos datos.

Databricks ML Model Export está diseñado para exportar sus modelos y tuberías de ML para que puedan usarse en otras plataformas de ML. Está específicamente diseñado para exportar modelos y tuberías ML basados en Apache Spark.

Servicio Azure Machine Learning

El servicio Azure Machine Learning proporciona una solución basada en la nube para crear modelos de ML. El Servicio de aprendizaje automático utiliza un lenguaje de programación llamado Python, por lo que deberá estar familiarizado con Python para usar el servicio.

El objetivo principal del Servicio de aprendizaje automático de Azure es utilizar recursos basados en la nube para ejecutar los complejos cálculos necesarios para construir modelos de ML. A diferencia de Databricks, donde todo está en la nube, con Machine Learning Service, puede construir sus conjuntos de datos en las instalaciones y luego cargar sus datos en la nube para realizar el modelado ML.

Al igual que Databricks, el Servicio de aprendizaje automático utiliza portátiles. Puede usar Jupyter Notebooks localmente, pero también puede usar Azure Notebooks, una oferta de Jupyter Notebook basada en la nube de Microsoft. Ya sea que use un bloc de notas local o un bloc de notas de Azure, normalmente comenzará por entrenar su modelo localmente para ahorrar en costos de cómputo. Una vez que esté listo para entrenar su modelo en Machine Learning Services, puede mover los datos a la nube, crear un script basado en la nube para su modelo y comenzar a entrenar su modelo, todo dentro de su computadora portátil.

La Figura 2-52 muestra el resultado de la capacitación de un modelo ML probado en una máquina local. Este modelo analiza imágenes de números escritos a mano e intenta identificar correctamente los números que se escribieron. Nos llevó tres minutos entrenar en una máquina local, lo que nos proporciona un nivel de precisión del 92%.

```
In [8]: %%time
        from sklearn.linear_model import LogisticRegression

        clf = LogisticRegression()
        clf.fit(X_train, y_train)

        CPU times: user 2min 42s, sys: 4.45 s, total: 2min 46s
        Wall time: 2min 46s

In [9]: y_hat = clf.predict(X_test)
        print(np.average(y_hat == y_test))

        0.9201
```

Figura 2-52 Entrenamiento de un modelo de ML simple y predicción ejecutada localmente con Azure Notebook

Cuando envíe su modelo a su clúster del Servicio de Aprendizaje Automático para capacitación, preparará el modelo y luego lo pondrá en cola para la capacitación en el clúster. Al igual que Databricks, el Servicio de aprendizaje automático es un servicio sin servidor, lo que significa que solo utiliza recursos informáticos cuandousando el clúster. Cuando envía un trabajo, se pone en cola hasta que los recursos de cómputo estén disponibles, por lo general, solo demora unos segundos. Una vez que se completa su trabajo, se liberan esos recursos.

En la Figura 2-53 , hemos enviado el modelo a un clúster en Machine Learning Services ejecutando un experimento en él para probar su precisión. Si hace clic en el enlace al portal de Azure, puede ver información adicional sobre la ejecución.

```
In [14]: run = exp.submit(config=est)
         run
```

Out[14]:

Experiment	Id	Type	Status	Details Page	Docs Page
sklearn-mnist	sklearn-mnist_1550362047_20a6c675	azureml.scriptrun	Starting	Link to Azure Portal	Link to Documentation

Figura 2-53 Ejecución de un script para entrenar un modelo en la nube

En la Figura 2-54 , puede ver el nodo en el clúster donde se ejecuta este script. En esta prueba, solo tenemos un nodo en el clúster, pero puede agregar recursos informáticos adicionales si es necesario. Si estaba entrenando un modelo complejo, es posible que desee agregar recursos de cómputo para entrenar más rápidamente ese modelo.

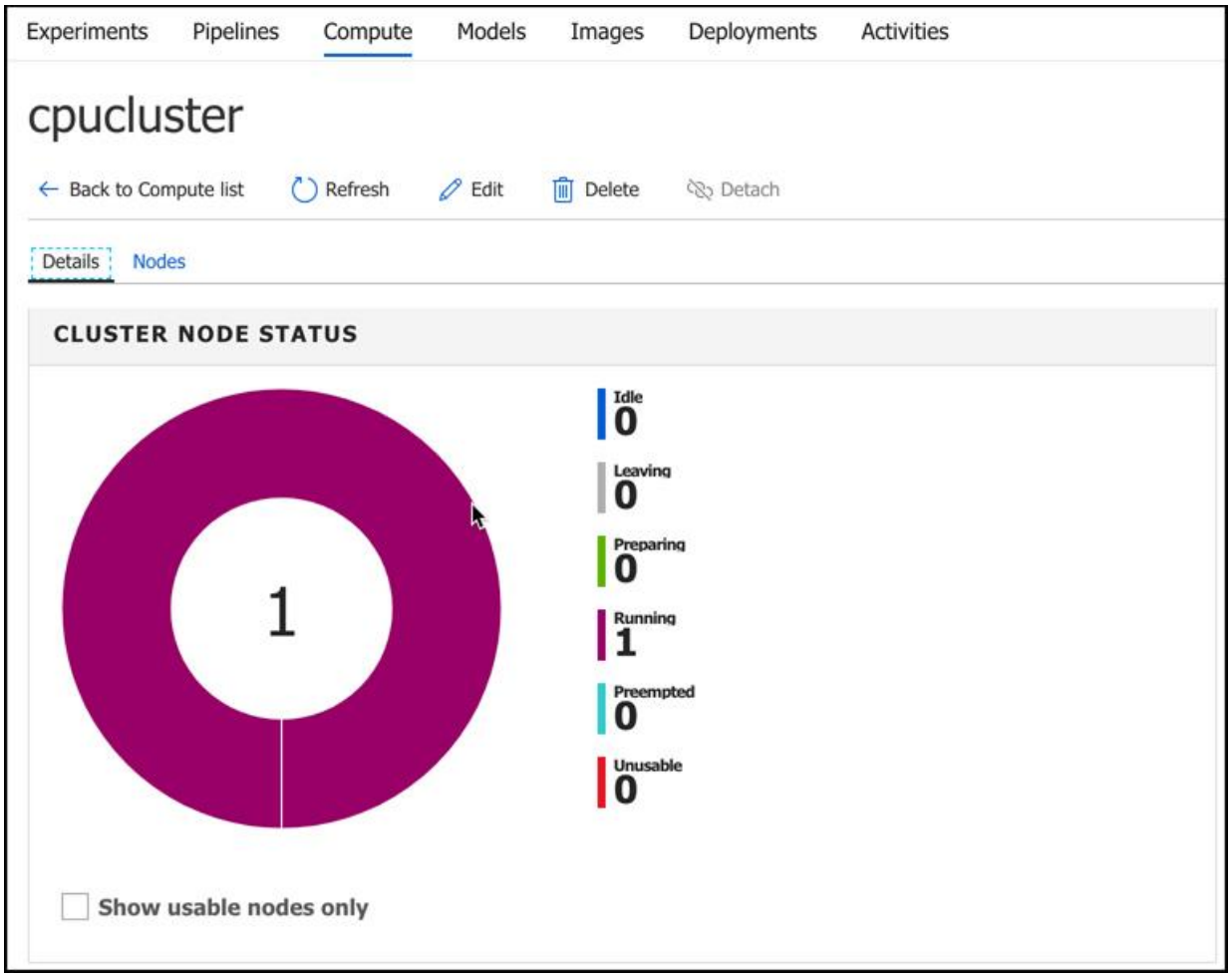


Figura 2-54 Nodo de Machine Learning Services que ejecuta un experimento

Cuando entrena modelos en Machine Learning Services, se crea un contenedor Docker y su modelo realmente se ejecuta dentro de ese contenedor. Un contenedor Docker es una copia comprimida de todo lo necesario para ejecutar su modelo. Esa copia comprimida se

llama imagen de Docker, y se puede ejecutar en cualquier computadora que esté ejecutando el tiempo de ejecución de Docker, incluida la VM que forma el clúster de Machine Learning Services.

Cuando desee exportar su modelo para poder usarlo en una carga de trabajo de producción, puede exportarlo como una imagen de Docker. Mediante el uso de imágenes de Docker, Machine Learning Services puedehaga que su modelo sea portátil para que pueda ejecutarse en casi cualquier lugar. Además de eso, puede usar potentes servicios de agrupación de contenedores como el Servicio Azure Kubernetes para ejecutar sus modelos a gran escala.

Más información **Contenedores Docker**

Una discusión sobre los contenedores Docker está fuera del alcance de esta guía, pero si está interesado en aprender más sobre Docker, consulte: *https://www.docker.com* .

Machine Learning Services también puede exportar su modelo como una imagen FPGA. FPGA significa matriz de compuerta programable en campo, y es similar a un microprocesador, excepto que puede ser programado por un usuario después de la fabricación. Los FPGA son extremadamente rápidos porque se pueden programar explícitamente para la tarea en cuestión. Lo único más rápido para el procesamiento de IA es el circuito integrado específico de la aplicación, o ASIC, pero un ASIC debe fabricarse para su propósito final. No se puede reprogramar más tarde.

Microsoft ha invertido mucho en una infraestructura FPGA para IA, y los FPGA están disponibles hoy en todos los centros de datos de Azure. De hecho, Microsoft potencia sus propios servicios cognitivos para la búsqueda de Bing y más mediante FPGA.

Estudio de aprendizaje automático de Azure

El examen AZ-900 no es un examen técnico, y es bastante difícil abordar el concepto de ML e IA sin ser técnico. Hasta este punto, hemos tratado de mantener las cosas en un nivel alto y no ser demasiado técnicos, y debido a eso, algunos de los conceptos pueden ser un poco difíciles de entender. Afortunadamente, hay una manera de lidiar con los conceptos de ML de una manera visual. Azure Machine Learning Studio permite a las personas que no son científicos de datos profundizar en ML y obtener una mejor comprensión de los conceptos que hemos discutido hasta este momento.

Machine Learning Studio es SaaS para ML. Proporciona una interfaz de arrastrar y soltar fácil de usar para crear, probar e implementar modelos ML. En lugar de tener que escribir sus propios modelos, Machine Learning Studio incluye una gran colección de modelos escritos previamente que puede aplicar a los datos. La mejor manera de manejar Machine Learning Studio es un enfoque práctico, así que usemos Machine Learning Studio para construir un modelo de ML y probarlo.

Para iniciar Machine Learning Studio, abra un navegador web y vaya a *https://studio.azureml.net* . Haga clic en **Iniciar sesión** en la esquina superior derecha e inicie sesión con su nombre de usuario y contraseña de suscripción de Azure.

Una vez que se abre Machine Learning Studio, se lo llevará a su espacio de trabajo predeterminado. Un espacio de trabajo es un contenedor lógico para sus experimentos, conjuntos de datos, modelos, etc. Machine Learning Studio asigna a su espacio de trabajo un

nombre predeterminado, pero puede cambiarlo haciendo clic en **Configuración** en la esquina inferior izquierda como se muestra en la Figura 2-55 .

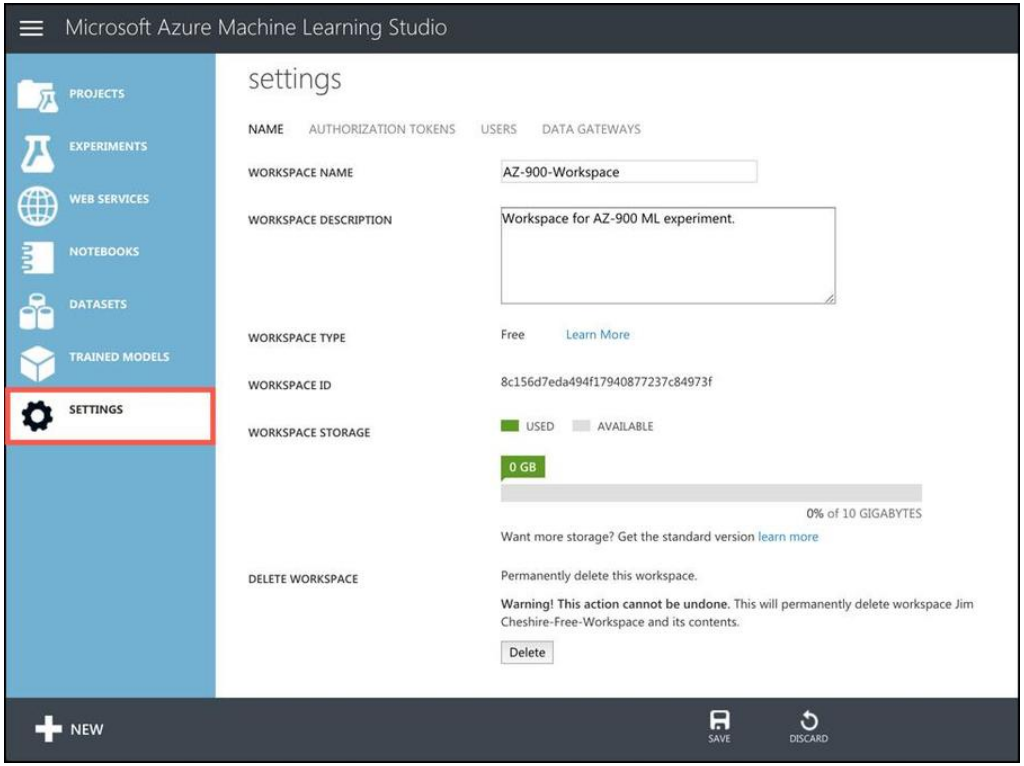


Figura 2-55 Cambio de configuración de nuestro espacio de trabajo de Machine Learning Studio

Observe en la Figura 2-55 que el tipo de espacio de trabajo es Libre. Hay dos niveles en Machine Learning Studio: gratuito y estándar. El nivel gratuito es para experimentación, mientras que el nivel estándar es lo que querría usar si está utilizando su modelo ML en un escenario de producción. Hay capacidades adicionales en el nivel Estándar, y debe pagar los espacios de trabajo que usan el nivel Estándar.

Más información **Precios de niveles de Studio de Machine Learning**

Para obtener más información sobre las características y los precios de los niveles de Machine Learning Studio, haga clic en el enlace Más información junto a Tipo de espacio de trabajo como se muestra en la Figura 2-55 . Esto lo llevará a la página de precios de Machine Learning Studio.

Cuando crea un espacio de trabajo navegando directamente a Machine Learning Studio, siempre estará en el nivel Gratis. Si desea crear un espacio de trabajo en el nivel Estándar, deberá usar Azure Portal para crear un Espacio de trabajo de Machine Learning Studio. Luego puede elegir su nivel.

El nivel gratuito está bien para nuestros propósitos porque solo estamos ejecutando algunas pruebas. Cambie el nombre del espacio de trabajo a "AZ-900-Workspace" y agregue una descripción útil. Luego puede hacer **clic** en **Guardar** en la parte inferior de la pantalla para guardar su nuevo nombre y descripción.

Ahora estamos listos para crear nuestro modelo ML, pero antes de hacerlo, repasemos exactamente lo que vamos a hacer. Lo haremos:

- Cree un experimento para que podamos probar y entrenar el modelo ML.
- Agregue datos que usaremos para entrenar el modelo ML.
- Agregue un algoritmo ML preexistente de Machine Learning Studio.
- Configure Machine Learning Studio para entrenar el modelo basado en el conjunto de datos.
- Ejecute un experimento para ver qué tan confiable es el algoritmo ML.

Para este experimento, vamos a utilizar los datos que se incluyen con Machine Learning Studio. Los datos muestran los datos de llegada y salida a tiempo de varias aerolíneas durante un período de un año. Utilizaremos estos datos para construir un modelo que prediga la probabilidad de que un vuelo en particular llegue a tiempo a su destino.

Paso 1: crea un experimento

El primer paso para construir un modelo ML para nuestra predicción de vuelo es crear un nuevo experimento. Aquí es donde crearemos y probaremos el modelo ML, y se llama experimento por una razón. Después de probar el modelo, cambiaremos algunas cosas para intentar aumentar la confiabilidad del modelo.

Para crear un experimento en Machine Learning Studio, haga clic en **Experimentos** en el menú de la izquierda y luego haga clic en el botón **Nuevo** en la parte inferior de la pantalla, como se muestra en la Figura 2-56 .

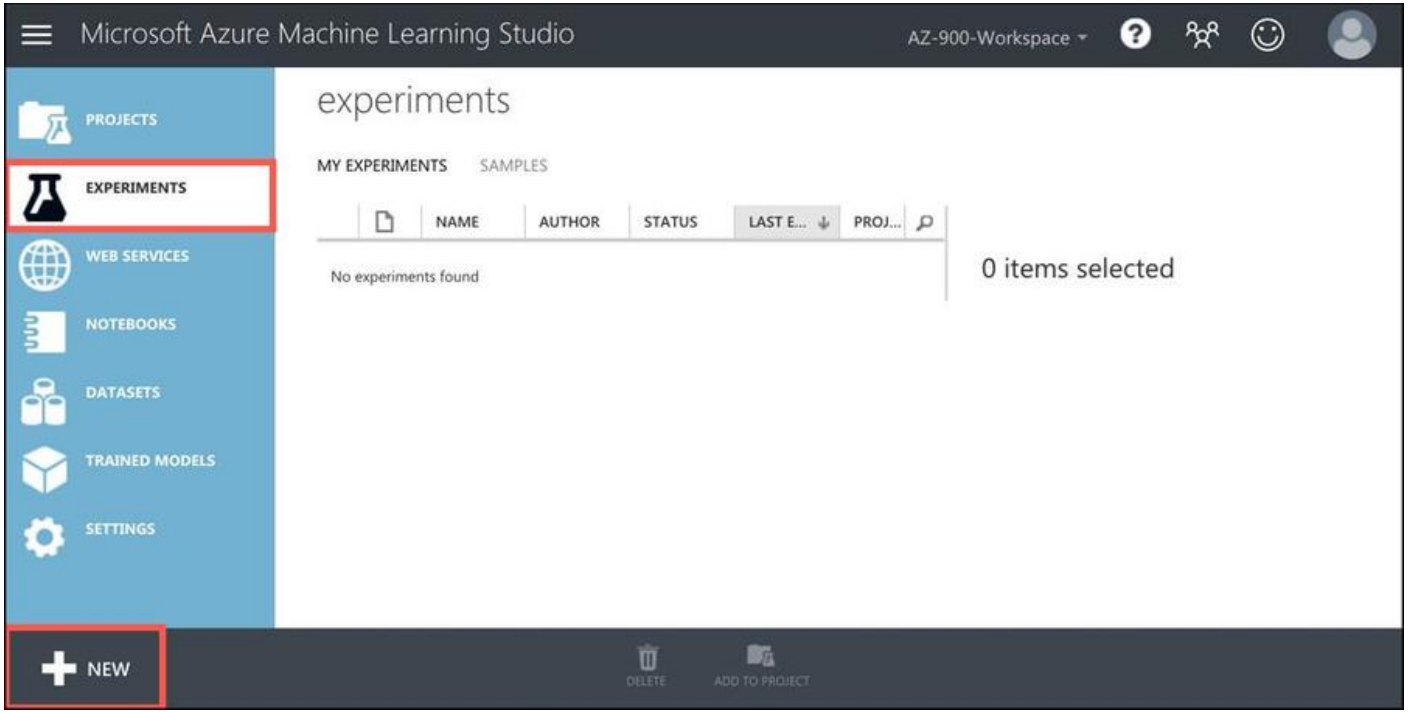


Figura 2-56 Creación de un nuevo experimento en Machine Learning Studio

Cuando haga esto, verá una colección de plantillas que Microsoft proporciona para experimentos. Todos estos son experimentos ML preconstruidos, y puedes aprender mucho eligiendo uno de ellos para ver cómo funcionan, pero para nuestros propósitos, comenzaremos con un experimento en blanco. Luego haga clic en **Experimento** en **blanco** como se muestra en la Figura 2-57 .

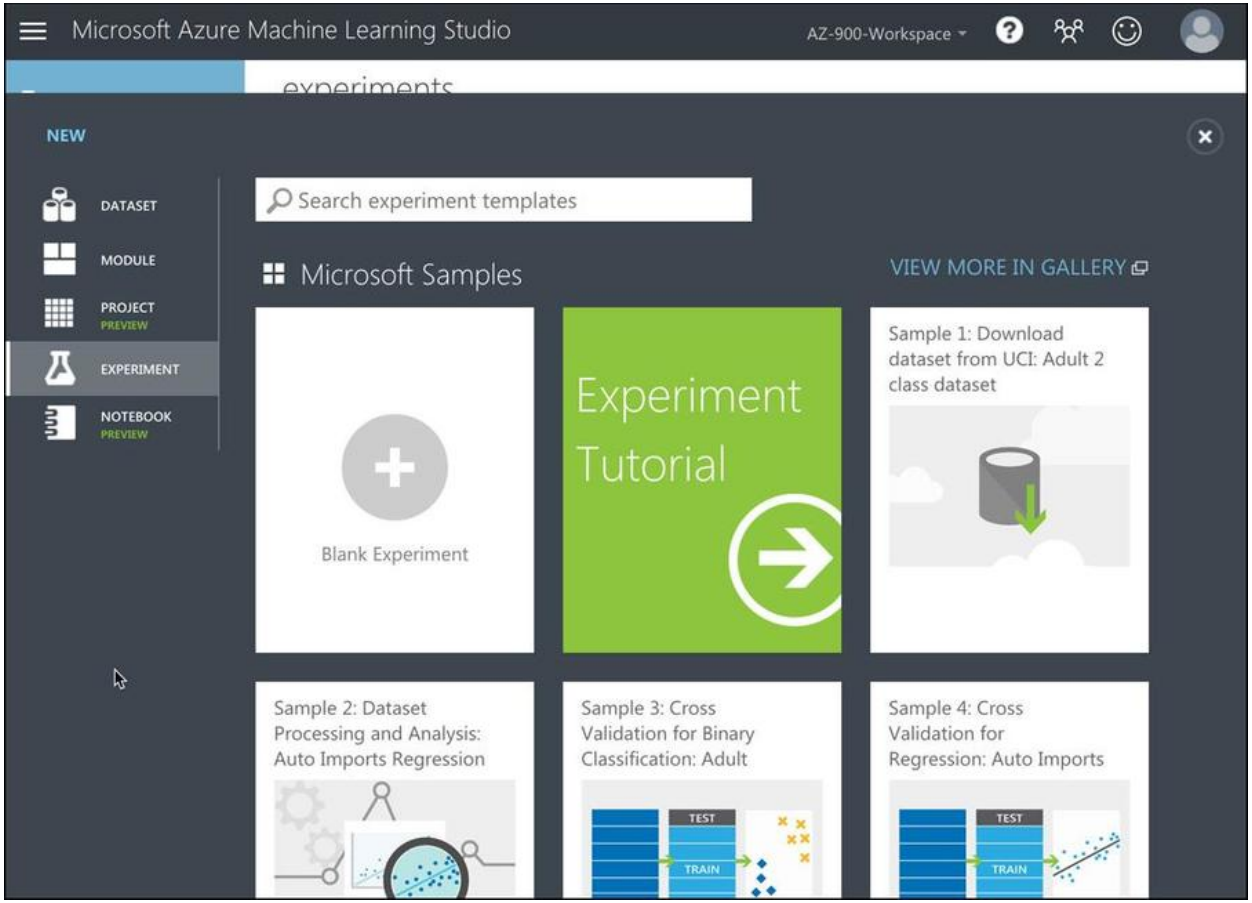


Figura 2-57 Crear un experimento en blanco

Una vez que haya creado su experimento, verá la pantalla que se muestra en la Figura 2-58 . En el lado izquierdo, verá una lista de todos los elementos que puede agregar a su experimento. Verá una lista de datos de muestra, pero si se desplaza hacia abajo, verá todo tipo de elementos que puede usar para construir un modelo.

La parte principal de la pantalla es donde construirá su modelo, y lo hará arrastrando elementos de la lista de la izquierda y soltándolos en la pantalla principal. Luego conectarás elementos para construir tu modelo.

Antes de hacer eso, cambiemos el nombre de este experimento para que podamos identificarlo fácilmente. El nombre de su experimento aparece en la parte superior de la pantalla. Haga clic en eso e ingrese un nuevo nombre para su experimento como se muestra en la Figura 2-58 .

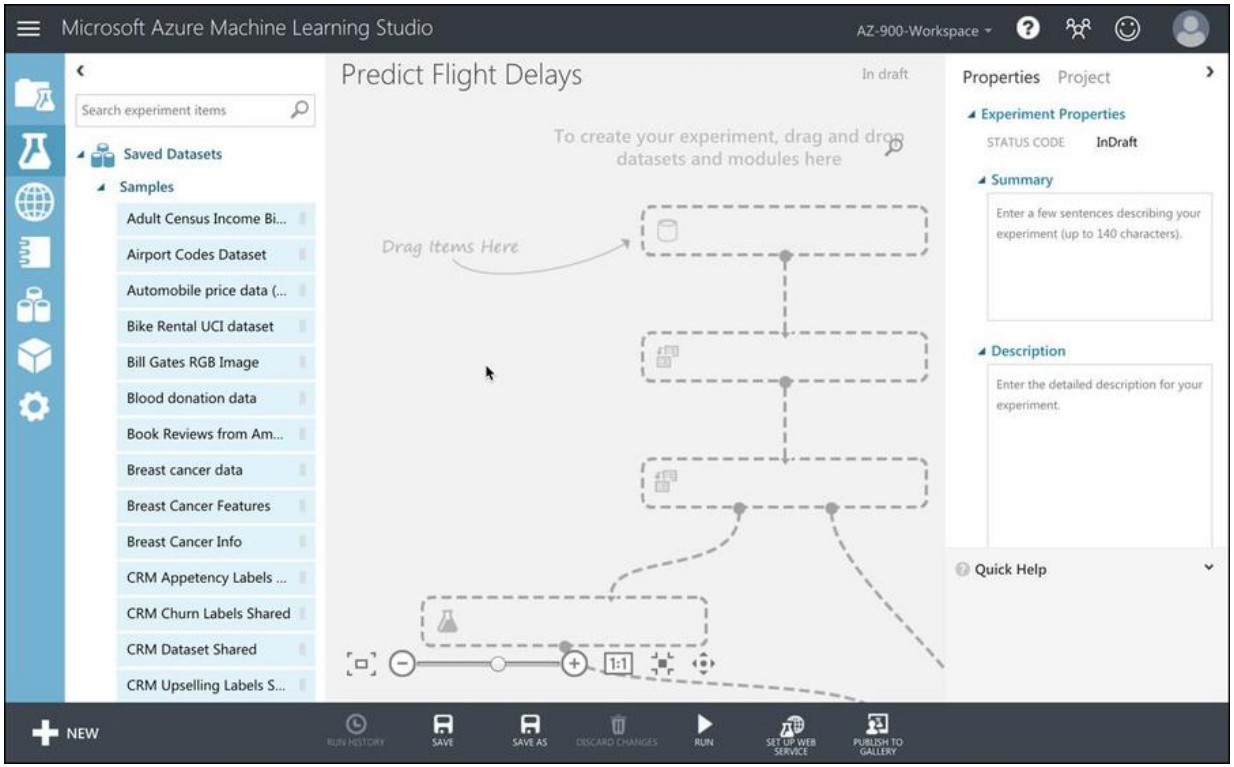


Figura 2-58 Un experimento en blanco en Machine Learning Studio

Paso 2: Agregar datos

Para entrenar un algoritmo de ML, debe ingresar datos en él. ML utiliza datos históricos para aprender a predecir un resultado particular en el futuro, y cuantos más datos use para entrenar su modelo, más confiable será su modelo.

Machine Learning Studio facilita la importación de datos de Azure Blob Storage, Azure SQL Database, consultas de Hive, Azure Cosmos DB y más. Sin embargo, para nuestro modelo ML, vamos a utilizar algunos datos de muestra que se incluyen con Machine Learning Studio.

Para encontrar los datos que queremos usar, ingrese "vuelo" en el cuadro de búsqueda a la izquierda. Cuando lo haga, verá "Datos de retrasos de vuelo". Estos son los datos que queremos usar, así que haga clic en ellos y arrástrelos a la pantalla principal a la derecha como se muestra en la Figura 2-59 .

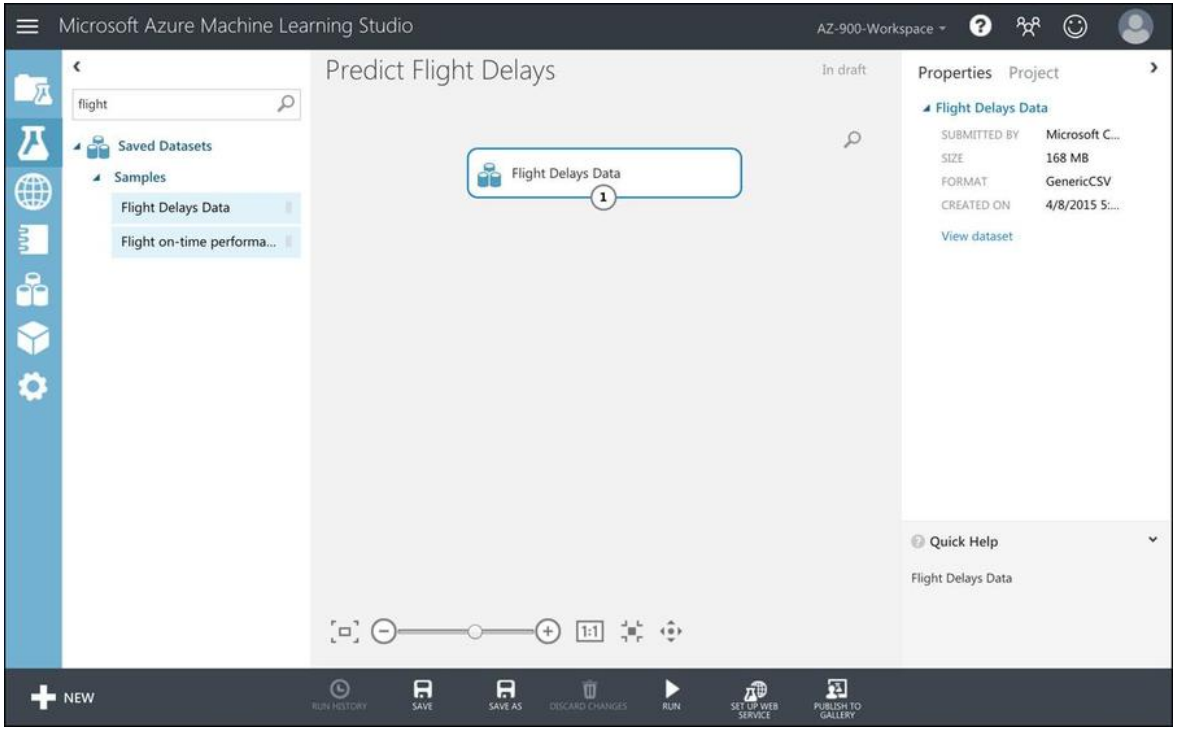


Figura 2-59 Agregar datos a nuestro experimento

Antes de trabajar en la construcción de un modelo ML, debe tener una buena comprensión de los datos que utilizará para entrenar ese modelo. Solo al tener una buena comprensión de sus datos podrá construir un modelo confiable, y Machine Learning Studio facilita el aprendizaje de sus datos. Si hace clic con el botón derecho en el elemento **Datos de retrasos de vuelo** que acaba de arrastrar a su

experimento, puede hacer clic en **Conjunto** de **datos** y luego **Visualizar** , como se muestra en la Figura 2-60 , para ver los datos contenidos en el conjunto de datos.

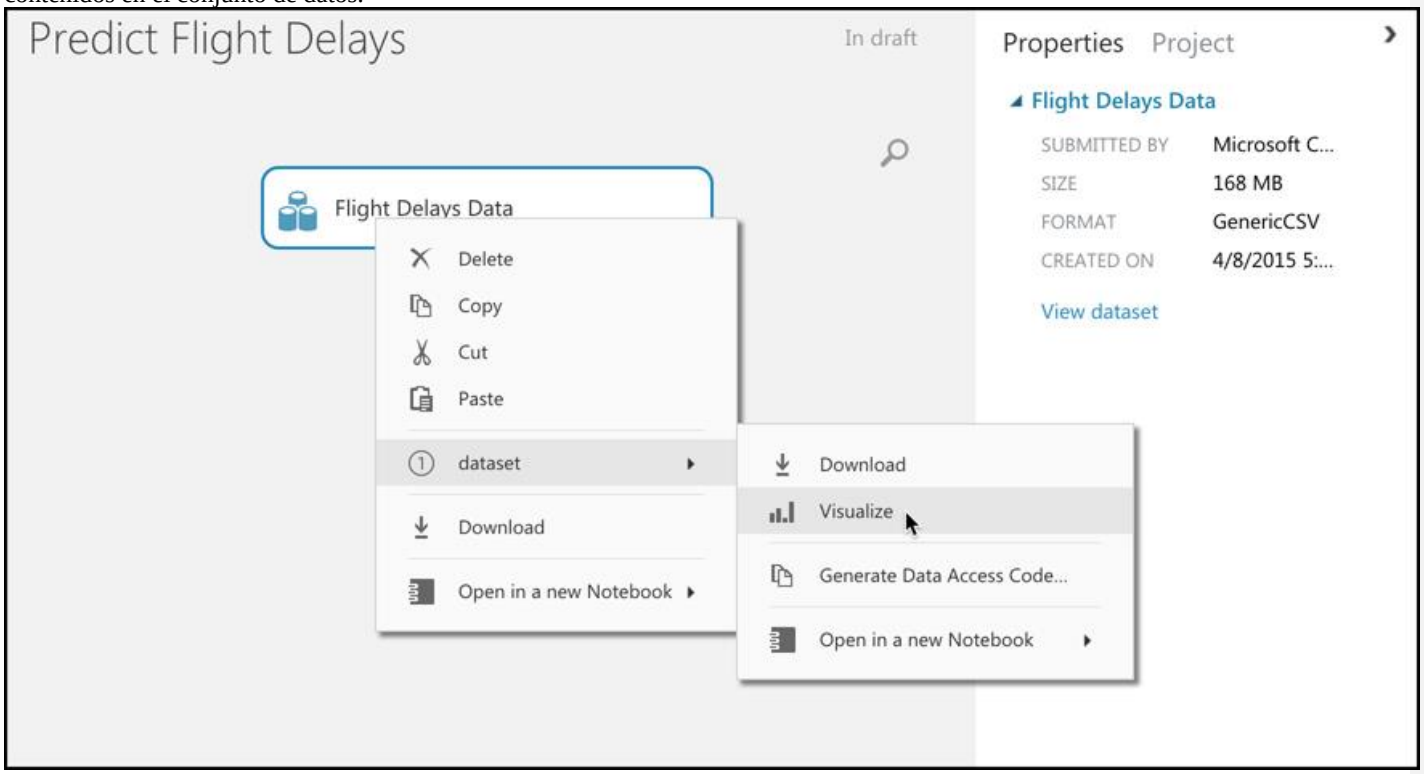


Figura 2-60 Uso de Machine Learning Studio para visualizar datos

Una vez que su conjunto de datos se abra en Machine Learning Studio, verá que tenemos un poco más de 2.7 millones de filas de datos para trabajar. Si hace clic en el encabezado de la columna Mes, verá que tenemos 7 valores únicos para el mes, como se muestra en la Figura 2-61 . Eso significa que tenemos datos aquí durante 7 meses al año, y aunque no es perfecto, eso será suficiente para lo que estamos haciendo. Si fuera a utilizar nuestro modelo en un escenario real, es probable que desee más datos para meses adicionales.

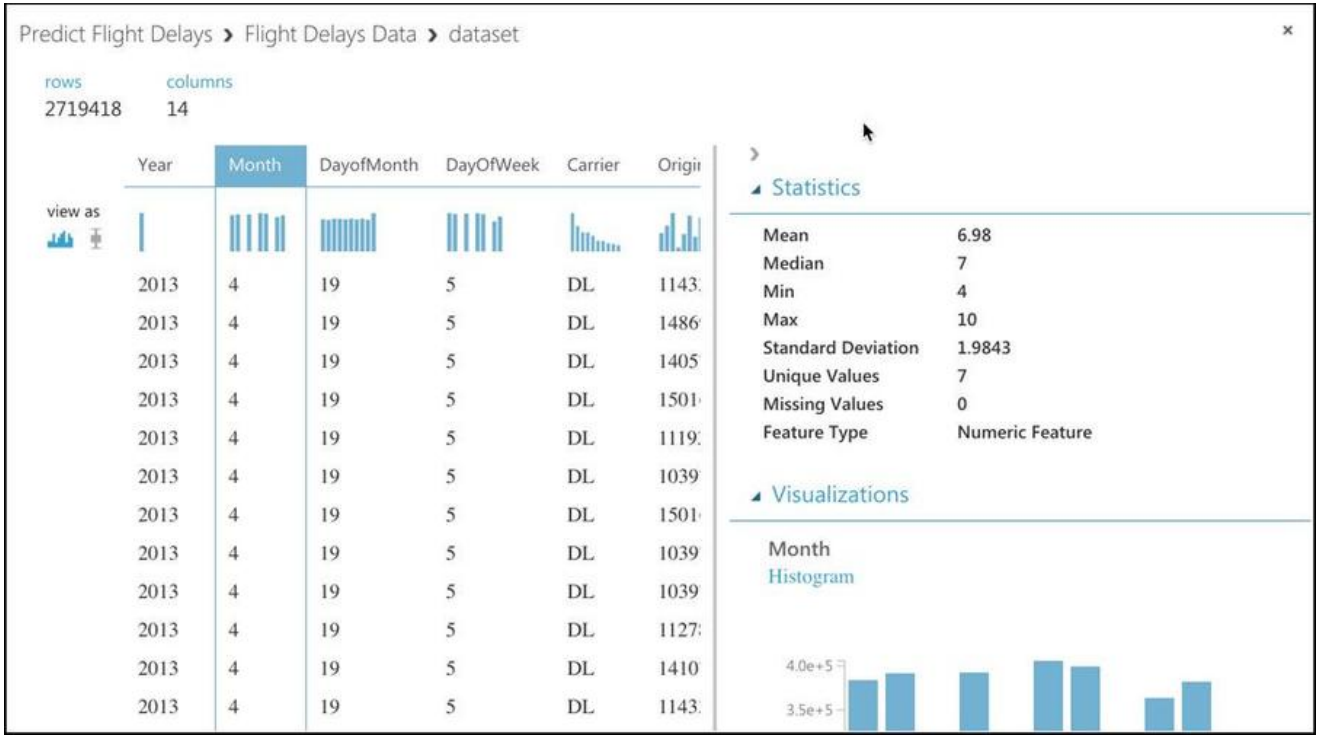


Figura 2-61 Visualización de un conjunto de datos en Machine Learning Studio

Algo importante a tener en cuenta con los datos de modelado de ML es el campo Valores perdidos que se muestra en la Figura 2-61 . Un valor faltante significa que faltan datos por completo o que tiene un 0 en un campo numérico. Si le faltan datos, su modelo tendrá fallas, por lo que querrá probar y asegurarse de que no le faltan datos importantes.

En este conjunto de datos en particular, tenemos algunas columnas que tienen valores faltantes. Machine Learning Studio incluye elementos que puede agregar a su modelo para tener en cuenta los valores faltantes. Haga clic en la X en la esquina superior derecha de su conjunto de datos para cerrarlo. Ingrese "faltante" en el cuadro de búsqueda y verá un elemento en Transformación de datos llamado Limpiar datos faltantes. Arrastre eso a su modelo como se muestra en la Figura 2-62 .

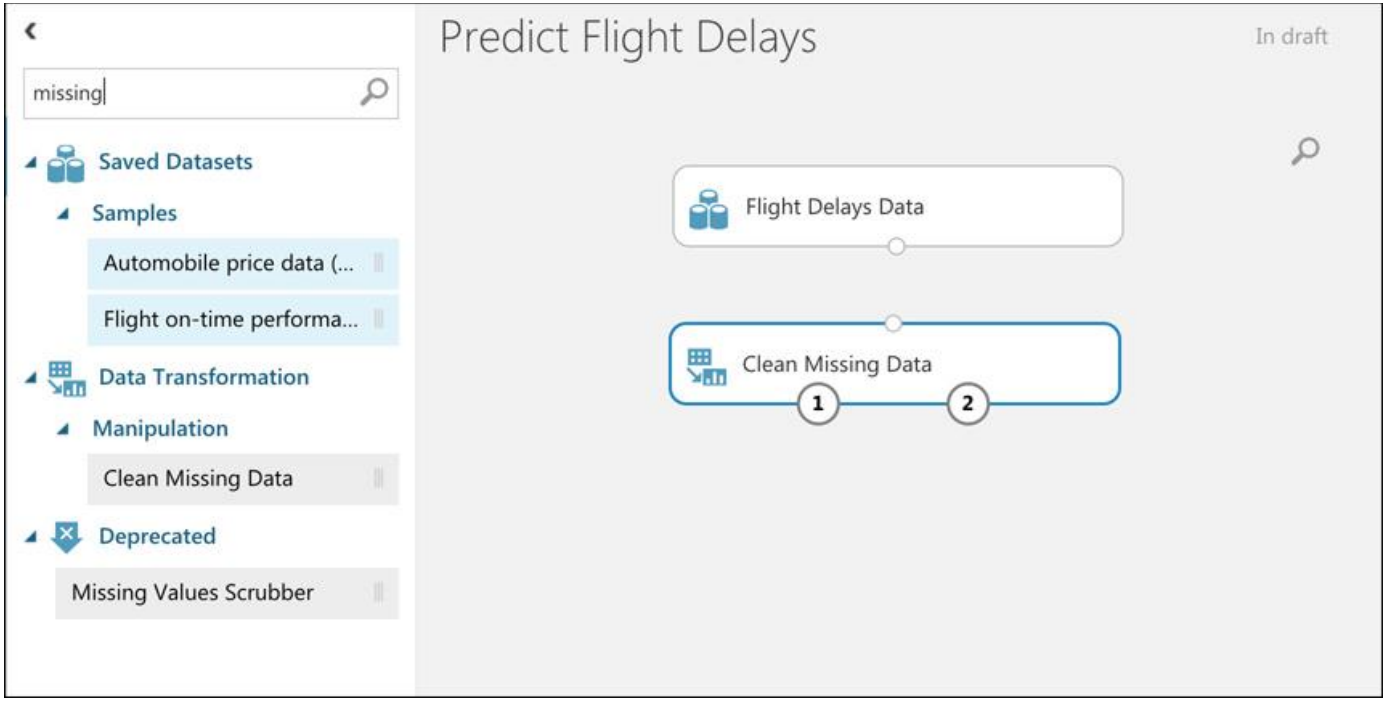


Figura 2-62 El elemento Limpiar datos faltantes ayuda a tener en cuenta los valores faltantes

Para que Clean Missing Data haga algo al conjunto de datos, necesitamos alimentarlo con el conjunto de datos. Para hacerlo, haga clic en **Datos de retrasos de vuelo** y verá un círculo con un "1". Ese círculo representa la salida del conjunto de datos, y debemos conectarlo a la entrada de la transformación Limpiar datos faltantes. Haga clic y mantenga presionado el "1" y arrástrelo hacia abajo al círculo pequeño en la parte superior de Clean Missing Data. Verá que el círculo pequeño en la parte superior de Clean Missing Data se vuelve verde como se muestra en la Figura 2-63 . Una vez que los dos nodos estén conectados, suelte el botón del mouse.

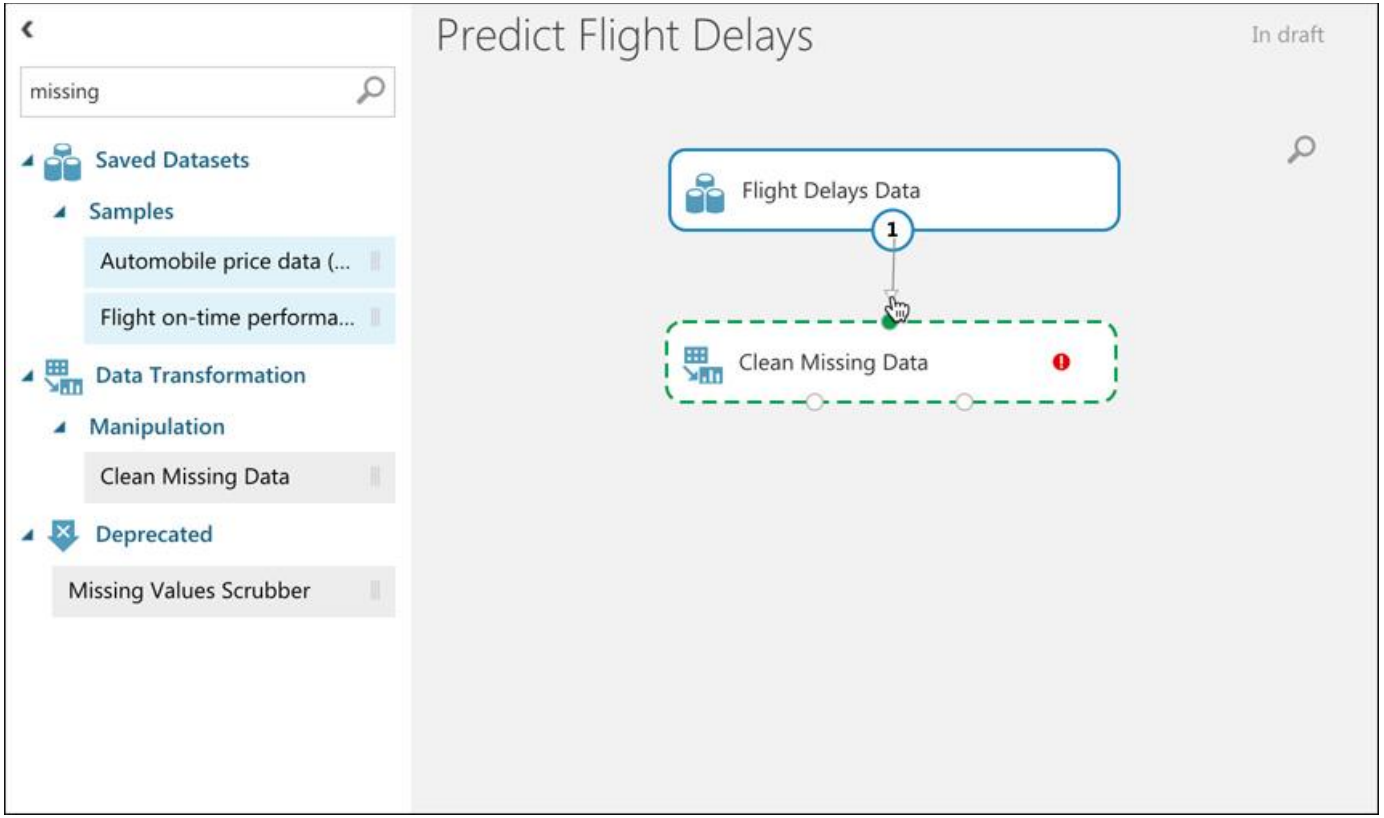


Figura 2-63 Conexión de nodos en Machine Learning Studio

Ahora tenemos que decirle a Machine Learning Studio qué queremos hacer con los valores perdidos. Haga clic en Limpiar datos faltantes y verá algunas propiedades que puede establecer en el panel de la derecha. Lo primero que debemos hacer es seleccionar las columnas que tienen valores faltantes.

Podemos descubrir esas columnas visualizando el conjunto de datos como se muestra en la Figura 2-61 . En base a eso, sabemos que las columnas DepDelay, DepDel15 y ArrDelay tienen valores faltantes. Sin embargo, en el modelo, no nos interesan las columnas DepDelay o ArrDelay. Estas columnas contienen la cantidad de minutos que un vuelo se retrasó en la salida o llegada, pero las columnas que queremos usar son DepDel15 y ArrDel15. Esas columnas contendrán un 0 si un vuelo partió o llegó dentro de los 15 minutos del horario y un 1 si no lo hizo. Por lo tanto, solo necesitamos limpiar la columna DepDel15 de valores faltantes.

- Con Limpiar datos faltantes seleccionado, haga clic en Iniciar selector de columnas en el panel Propiedades como se muestra en la Figura 2-64 .

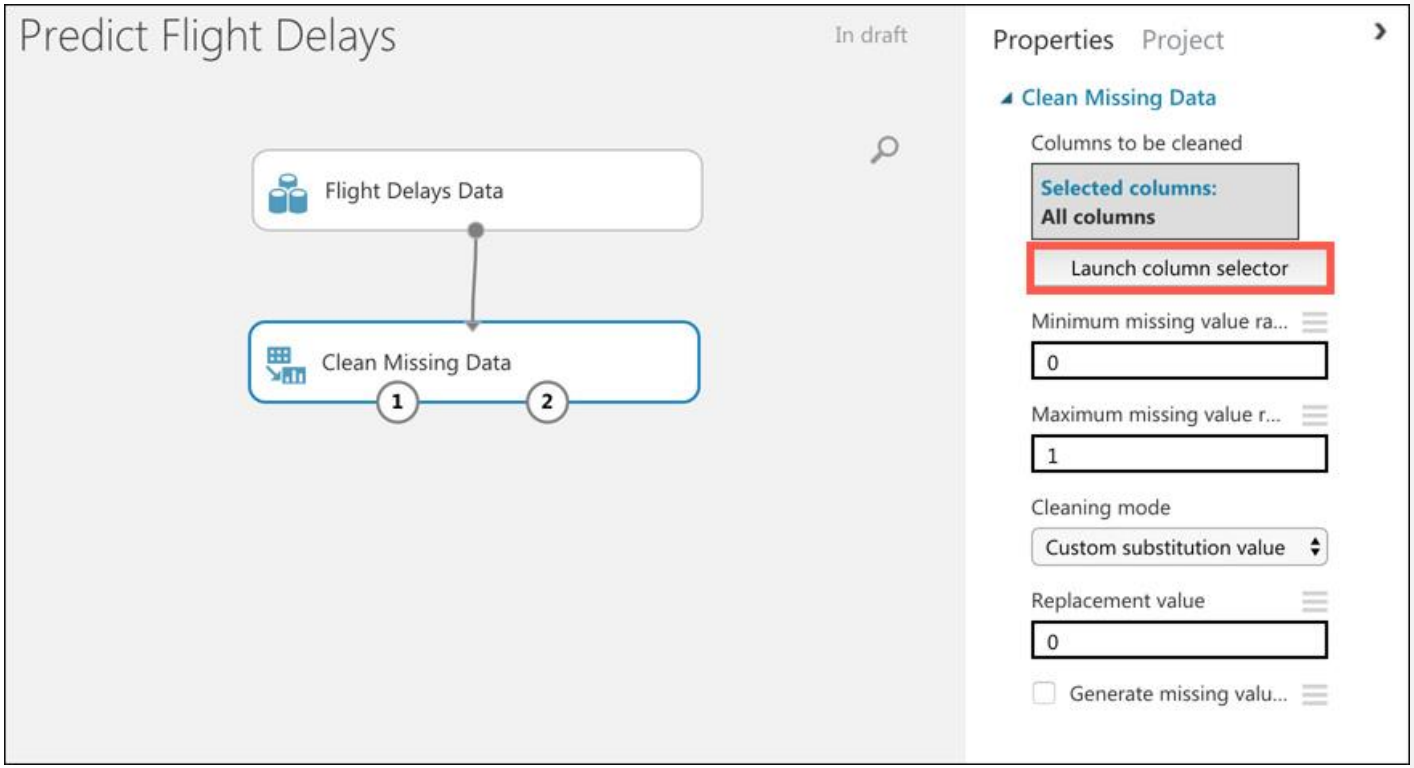


Figura 2-64 Propiedades de datos faltantes limpios

- En la pantalla Seleccionar columnas, haga clic en **Sin columnas** en Comenzar con.
- Cambie los **índices** de **columna a nombres de columna** e ingrese DepDel15 en el cuadro de entrada. Cuando lo haga, aparecerá una lista de columnas.
- Haga clic en DepDel15 para seleccionar esa columna. La pantalla Seleccionar columnas ahora debería verse como la que se muestra en la Figura 2-65 .

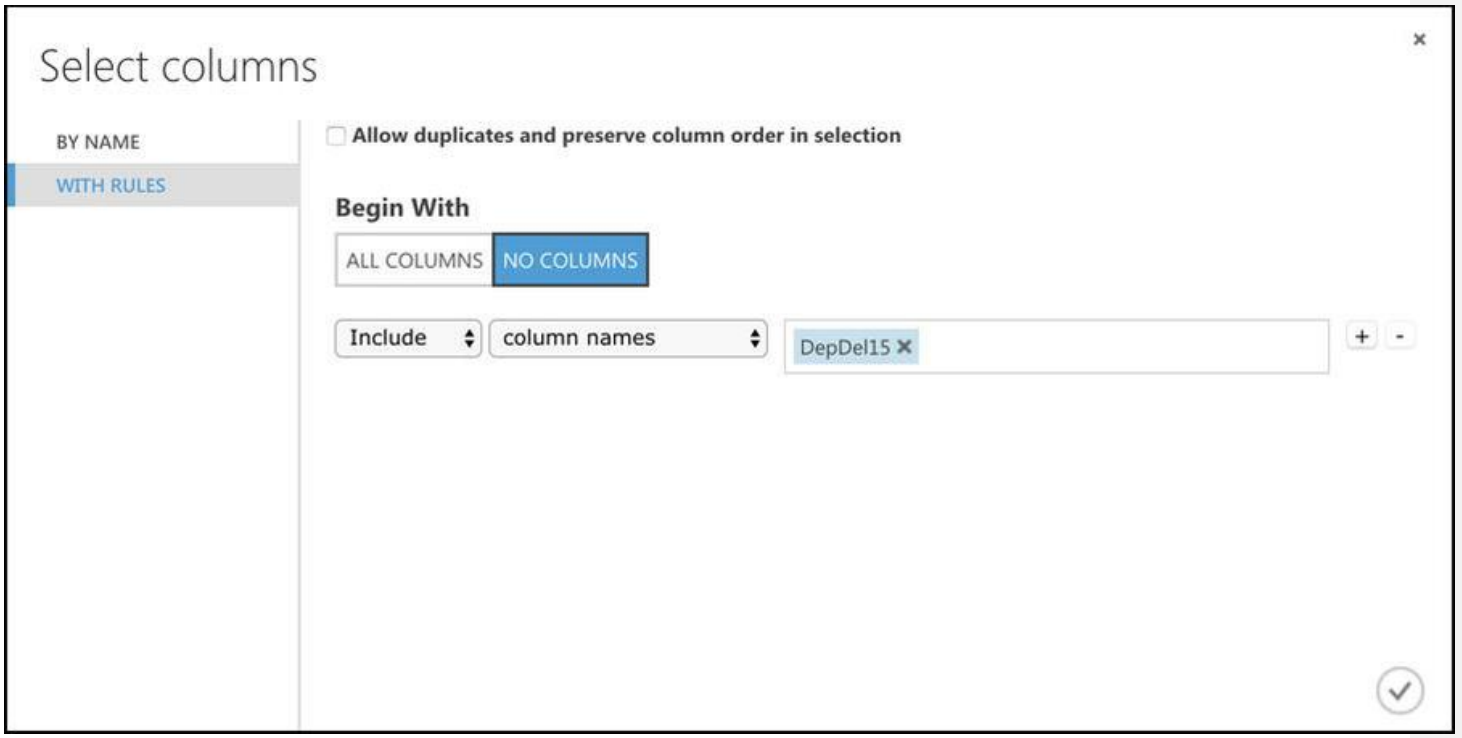


Figura 2-65 Seleccionar columnas para limpiar

- Una vez que haya ingresado a la columna DepDel15, haga clic en el botón de marca de verificación en la esquina inferior derecha para guardar esa configuración.

Vamos a eliminar completamente cualquier fila que tenga valores faltantes en la columna DepDel15.

- Haga clic en el menú desplegable **Modo de limpieza** (que se muestra en la Figura 2-64) y seleccione **Eliminar toda la fila** . Ahora podemos realizar nuestra transformación de datos y verificar los resultados.
- Haga clic en el botón **Ejecutar** en la parte inferior de Machine Learning Studio. Esto pondrá en cola nuestro trabajo de transformación y verá que aparece un pequeño reloj en el nodo Limpiar datos faltantes.

Cuando comience el proceso de transformación, verá un círculo verde giratorio. La transformación va a limpiar casi 3 millones de filas, por lo que tomará aproximadamente un minuto. Cuando esté completo, aparecerá un cheque verde.

Ahora podemos ver nuestro conjunto de datos limpios para verificar los resultados de nuestra limpieza de datos.

- Haga clic derecho en **Limpiar datos faltantes** .
- Apunte al **conjunto de datos limpiado** .
- Haga clic en **Visualizar** , como se muestra en la Figura 2-66 .

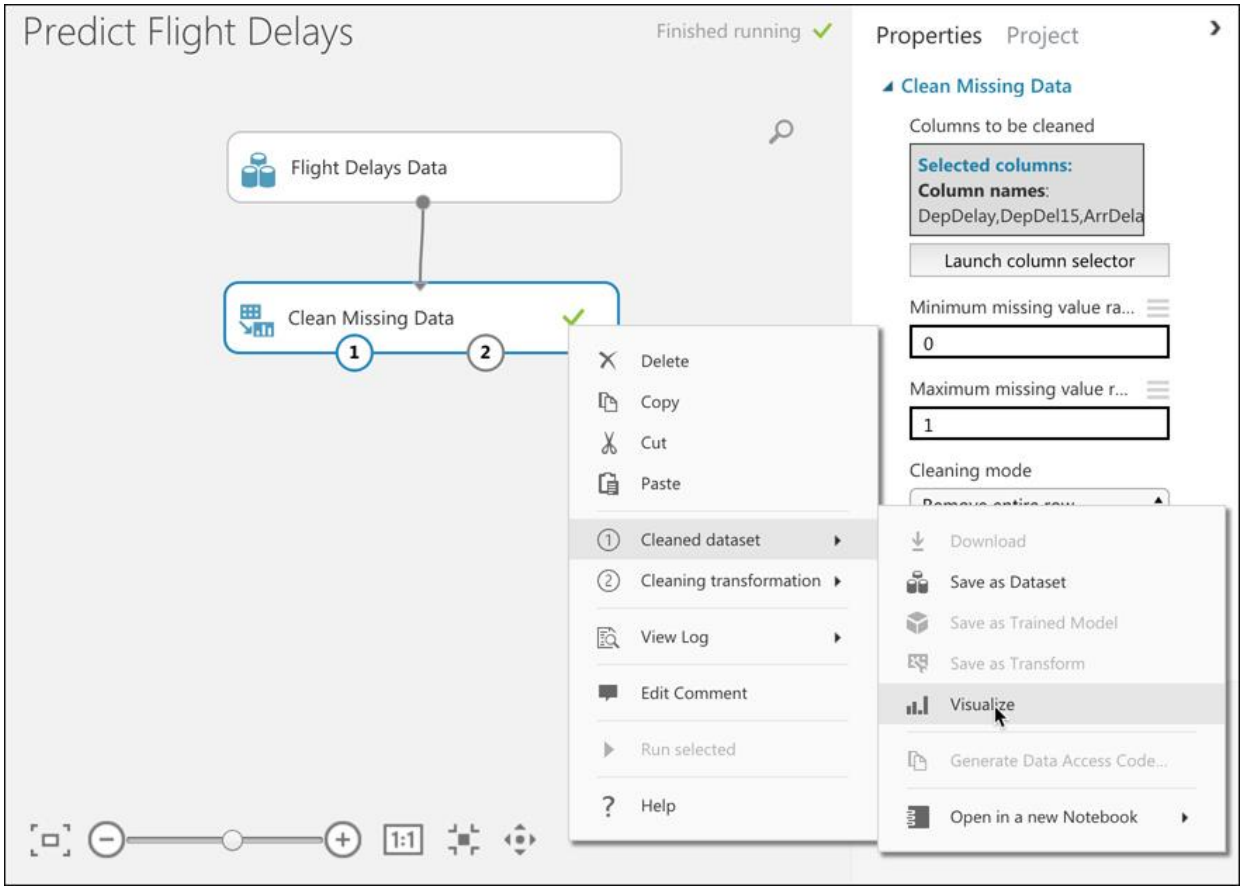


Figura 2-66 Visualización de un conjunto de datos limpio

Use la misma técnica que utilizó anteriormente al visualizar el conjunto de datos. Notarás que tenemos menos registros que antes porque nuestra transformación de datos eliminó filas dondefaltaban datos Si hace clic en la columna DepDel15, verá que ahora no le faltan valores.

Ahora que tenemos datos limpios, necesitamos decirle a nuestro modelo qué columnas de estos datos son de interés para nuestro modelo. Queremos crear un modelo que prediga la probabilidad de que un vuelo en particular llegue tarde, por lo que solo queremos columnas en el conjunto de datos que sean importantes para nosotros para predecir eso. Cualquier otra cosa es solo ruido que el modelo no necesita tener en cuenta.

Para decirle al modelo qué columnas mirar, usaremos el elemento Seleccionar columnas en el conjunto de datos.

- Haga clic en el cuadro de búsqueda e ingrese **Seleccionar** .
- Localice las columnas Seleccionar columnas en la transformación del conjunto de datos. Arrástrelo desde la lista y suéltelo directamente en Limpiar datos faltantes.
- Para conectar el conjunto de datos limpio a Seleccionar columnas en el conjunto de datos, haga clic en **Limpiar datos faltantes** y arrastre el nodo "1" al nodo superior de Seleccionar columnas en el conjunto de datos como se muestra en la Figura 2-67 .

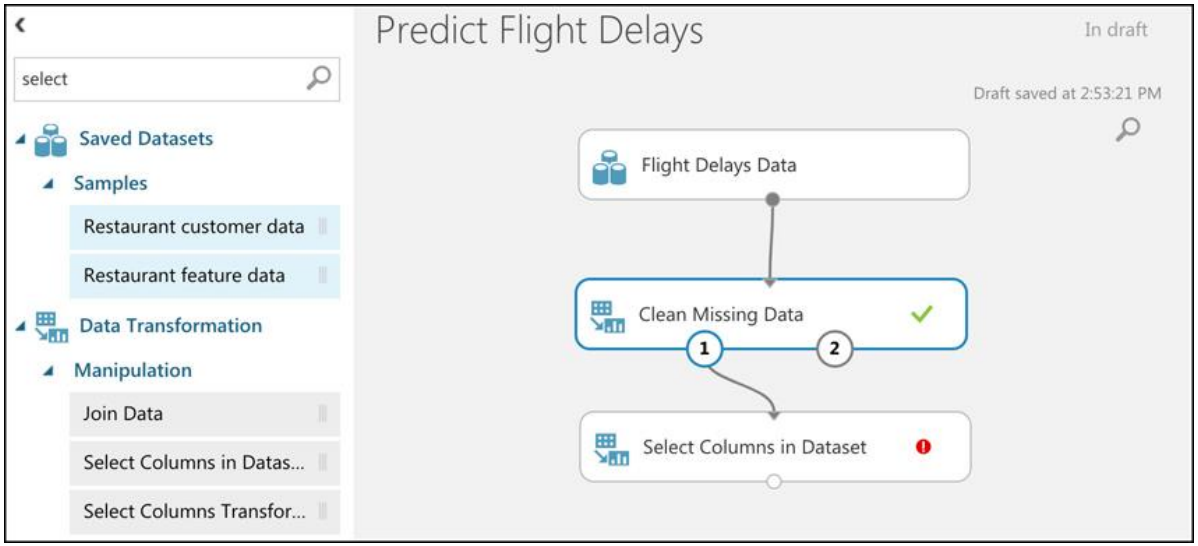


Figura 2-67 Conexión de un conjunto de datos limpio para seleccionar columnas en el conjunto de datos

Observe que Seleccionar columnas en el conjunto de datos muestra un círculo rojo con un signo de exclamación. Eso nos dice que necesitamos configurar algo para que funcione. En este caso, necesitamos decirle qué columnas queremos seleccionar.

- Haga clic en **Seleccionar columnas en el conjunto de datos** y haga clic en **Iniciar selector de columnas** en el panel Propiedades.
- Seleccione **Año** de la lista de la izquierda y haga clic en el botón de flecha derecha para moverlo a la lista de columnas seleccionadas.
- Haga lo mismo para todas las columnas, excepto DepDelay, ArrDelay y Canceled. Debería ver una pantalla como la que se muestra en la Figura 2-68 .

Figura 2-68 Selección de columnas relevantes para el modelo

Las columnas que seleccionamos son todas las columnas que contienen información que podría afectar la hora de llegada de cualquier vuelo en particular. Ahora estamos listos para comenzar a entrenar el modelo ML con el nuevo conjunto de datos.

Nota **Pase tiempo con sus datos**

Pasamos mucho tiempo mirando los datos y trabajando para limpiarlos. Este paso es extremadamente importante cuando se trata de ML. No solo necesita comprender completamente sus datos, sino que también debe asegurarse de que sus datos estén tan limpios como sea posible y que solo envíe datos relevantes a su modelo.

Una de las mejores cosas de Machine Learning Studio es que siempre puedes regresar y rehacer las cosas fácilmente si cometes errores.

Paso 3: entrena al modelo

Cuando entrena un modelo de lenguaje de máquina, no proporciona todos sus datos. En su lugar, divide sus datos y envía un porcentaje de los datos al modelo para capacitación. Una vez que el modelo está entrenado, utiliza los datos restantes para probar su modelo. El proceso de probar un modelo se llama *calificar* el modelo. Al usar datos con valores conocidos para calificar el modelo, puede ver cuántas veces su modelo entrenado obtuvo la predicción justo antes de arrojar datos reales con resultados desconocidos.

Machine Learning Studio facilita la división de sus datos para el entrenamiento.

- Ingrese **split** en el cuadro de búsqueda y ubique el elemento Split Data.
- Arrástrelo debajo del nodo Seleccionar columnas del conjunto de datos.
- Conecte el nodo de salida Seleccionar columnas en el conjunto de datos (el círculo en la parte inferior) al nodo superior de Datos divididos como se muestra en la Figura 2-69 .

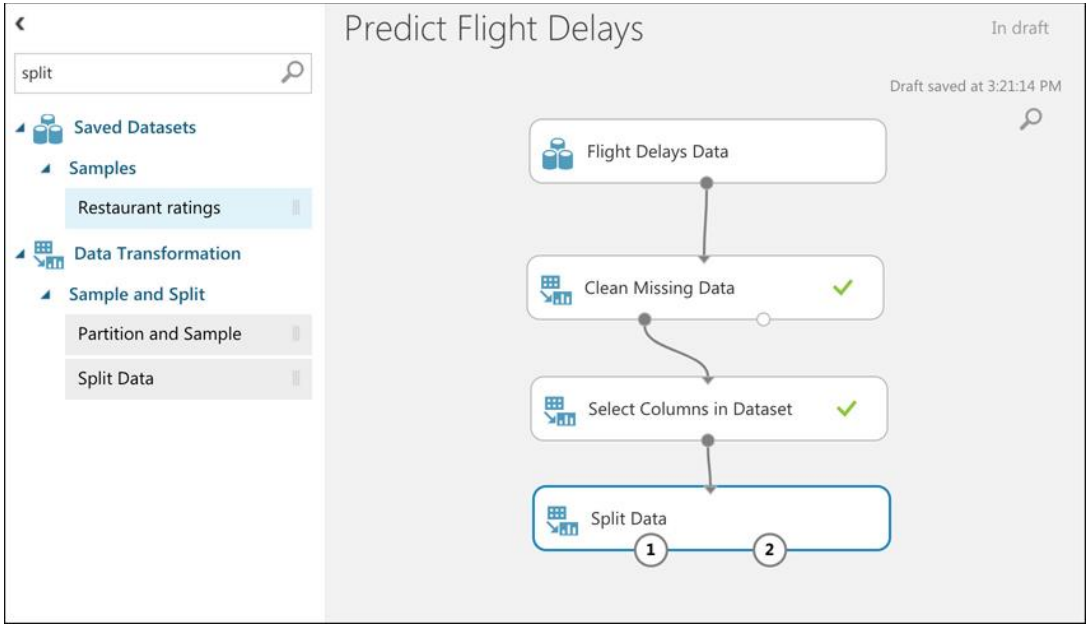


Figura 2-69 Datos divididos para entrenar su modelo ML

Como regla general, es una buena idea enviar aproximadamente el 80% de sus datos a su modelo para capacitación y el 20% de sus datos para calificar el modelo entrenado. Para hacer eso, haga clic en **Dividir datos** y configure la fracción de filas para incluir en el primer conjunto de datos de salida en .8 como se muestra en la Figura 2-70 .

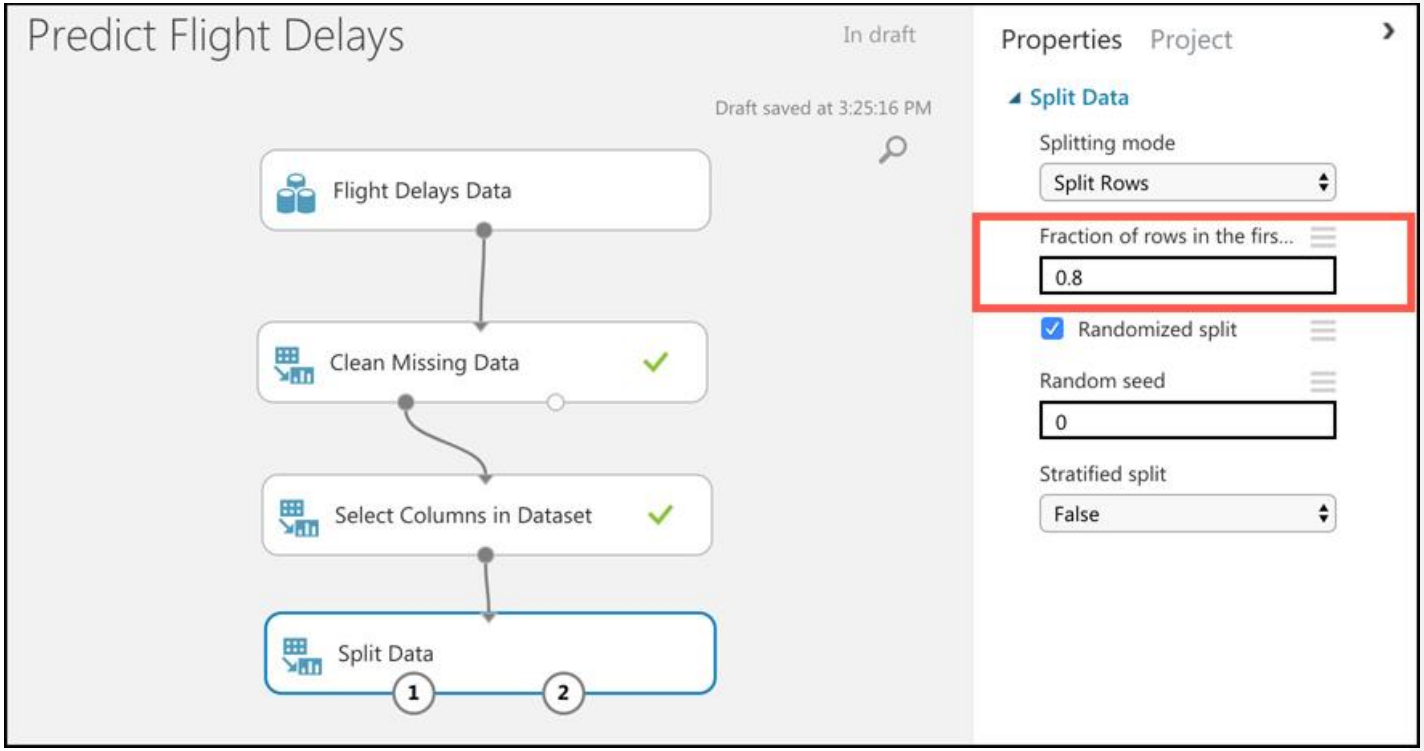


Figura 2-70 Configuración de una fracción para nuestro primer conjunto de datos

Para entrenar un modelo en Machine Learning Studio, use el elemento Train Model.

- Haga clic en el cuadro de búsqueda e ingrese el **modelo de tren** .
- Arrastre Modelo de tren a su pantalla en Datos divididos.
- Para hacer espacio para nuestros artículos adicionales, haga clic en el botón dentro de un círculo Figura 2-71 para habilitar el modo panorámico y mover sus artículos hacia arriba.
- Una vez que los haya movido a donde lo desee, haga clic nuevamente en el botón de modo panorámico para desactivarlo.
- Conecte el nodo izquierdo de Datos divididos al nodo superior derecho del elemento Modelo de tren como se muestra en la Figura 2-71 . Esto envía el 80% de nuestro conjunto de datos al elemento Modelo de tren.

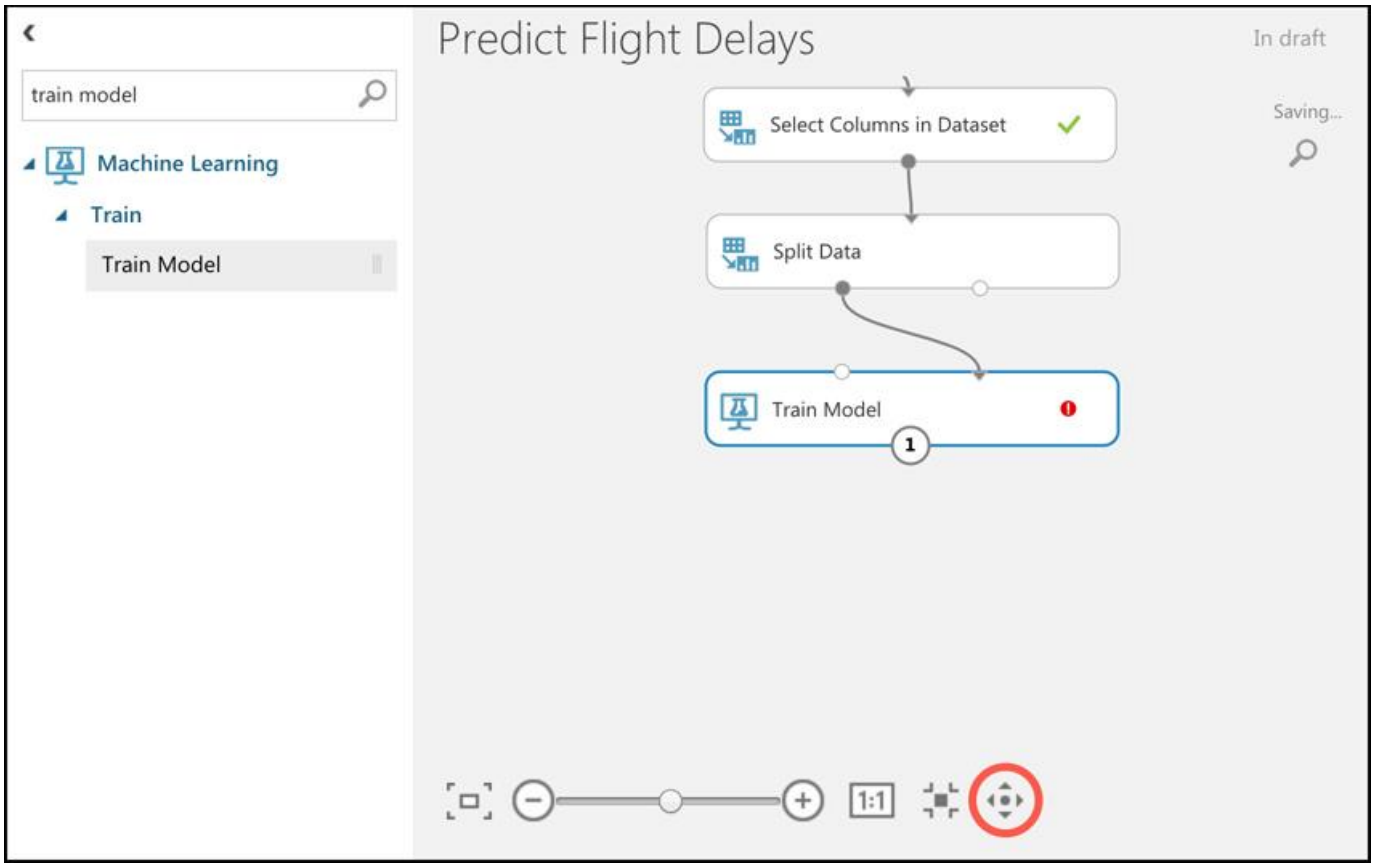


Figura 2-71 Conexión del primer conjunto de datos de datos divididos al modelo de tren

Hay un par de cosas que debemos decirle a Train Model antes de comenzar a entrenar. En primer lugar, debemos decirle qué queremos que prediga nuestro modelo. Queremos que este modelo prediga si un vuelo en particular llegará a su destino a tiempo, por lo que queremos que prediga el valor de la columna ArrDel15. (Recuerde, este valor será 0 si el vuelo estuvo dentro de los 15 minutos de la hora de llegada programada y 1 si no lo está).

- Haga clic en **Modelo de tren** y haga clic en **Iniciar selector de columnas** en el panel Propiedades.
- Haga clic en la columna ArrDel15 para seleccionarlo y luego haga clic en el botón de verificación.

A continuación, debemos decirle a Train Model qué tipo de modelo ML queremos que use. Si estuviera escribiendo este modelo de ML usted mismo, tendría que escribirlo utilizando un lenguaje de programación como Python o R, pero Machine Learning Studio contiene una gran cantidad de modelos de ML que puede usar sin ninguna programación.

Más información **Modelos Ml**

Hay algoritmos de ML específicos que se adaptan bien a situaciones particulares. Una excelente manera de determinar el mejor algoritmo en Machine Learning Studio es usar la Cheat Sheet de Machine Learning. Puede encontrarlo en: *https://aka.ms/mlcheatsheet* .

El modelo va a predecir un valor booleano basado en datos de entrada, y para este tipo de modelo, el algoritmo de árbol de decisión potenciado de dos clases es ideal.

- Haga clic en el cuadro de búsqueda y escriba **dos clases impulsadas** .
- Arrastre el elemento Árbol de decisión potenciado de dos clases a su pantalla y suéltelo a la izquierda de Modelo de tren.
- Conecte el nodo en el Árbol de decisión potenciado de dos clases al nodo izquierdo del Modelo de tren como se muestra en la Figura 2-72 .

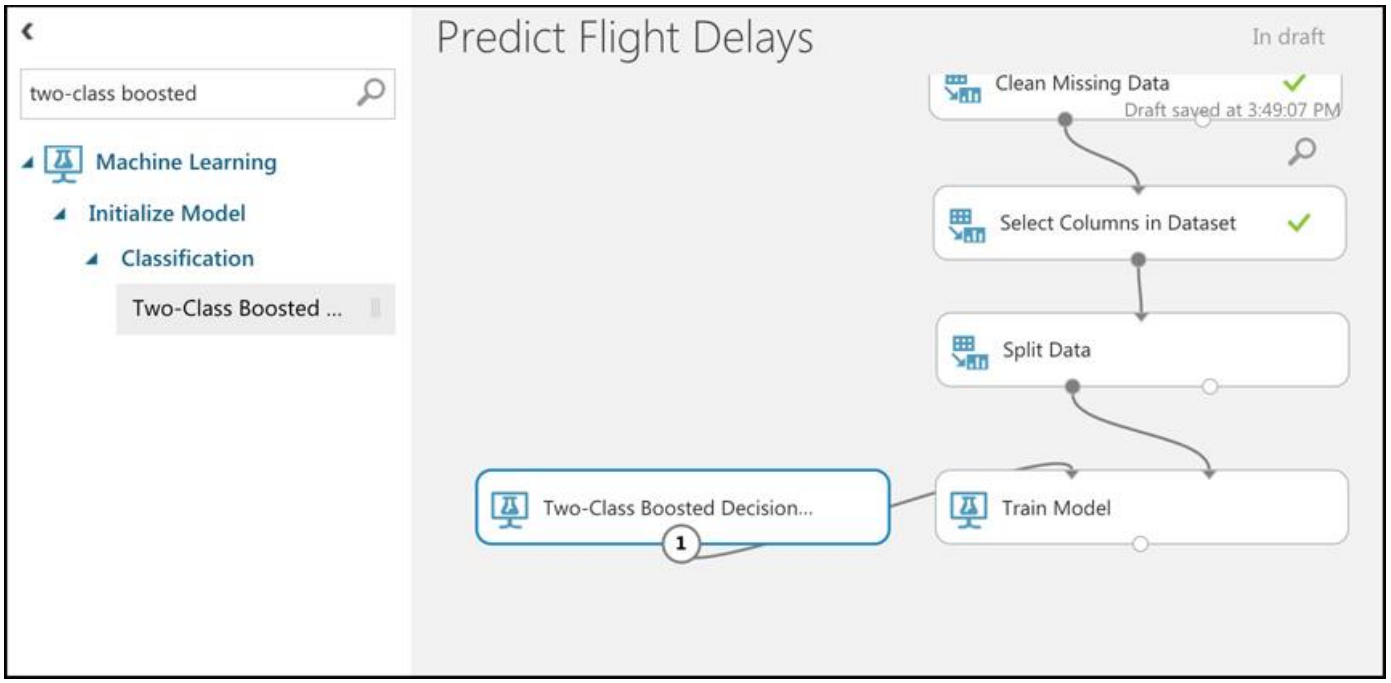


Figura 2-72 Agregar un algoritmo para entrenar nuestro modelo

Ahora tenemos todo en su lugar para entrenar realmente el modelo ML, pero también queremos calificar el modelo para ver qué tan preciso es. Antes de entrenarlo, configuremos el espacio de trabajo para que podamos ver qué tan bien funcionó el modelo después del entrenamiento.

Paso 4: puntuar el modelo

Para saber qué tan exitoso es este modelo, necesitamos poder calificarlo con el 20% restante de los datos. Usaremos el elemento Modelo de puntuación en Machine Learning Studio para hacerlo.

- Haga clic en el cuadro de búsqueda y escriba el **modelo de puntuación** .
- Arrastre el elemento Modelo de puntuación a su espacio de trabajo y suéltelo en Modelo de tren.
- Conecte el nodo de salida del Modelo de tren al nodo superior izquierdo del Modelo de puntuación. Esto envía el modelo entrenado al Modelo de puntuación.

- Para enviar el 20% restante de los datos al Modelo de puntuación para la puntuación, conecte el nodo de salida derecho de **Datos divididos** al nodo superior derecho del Modelo de puntuación como se muestra en la Figura 2-73 .

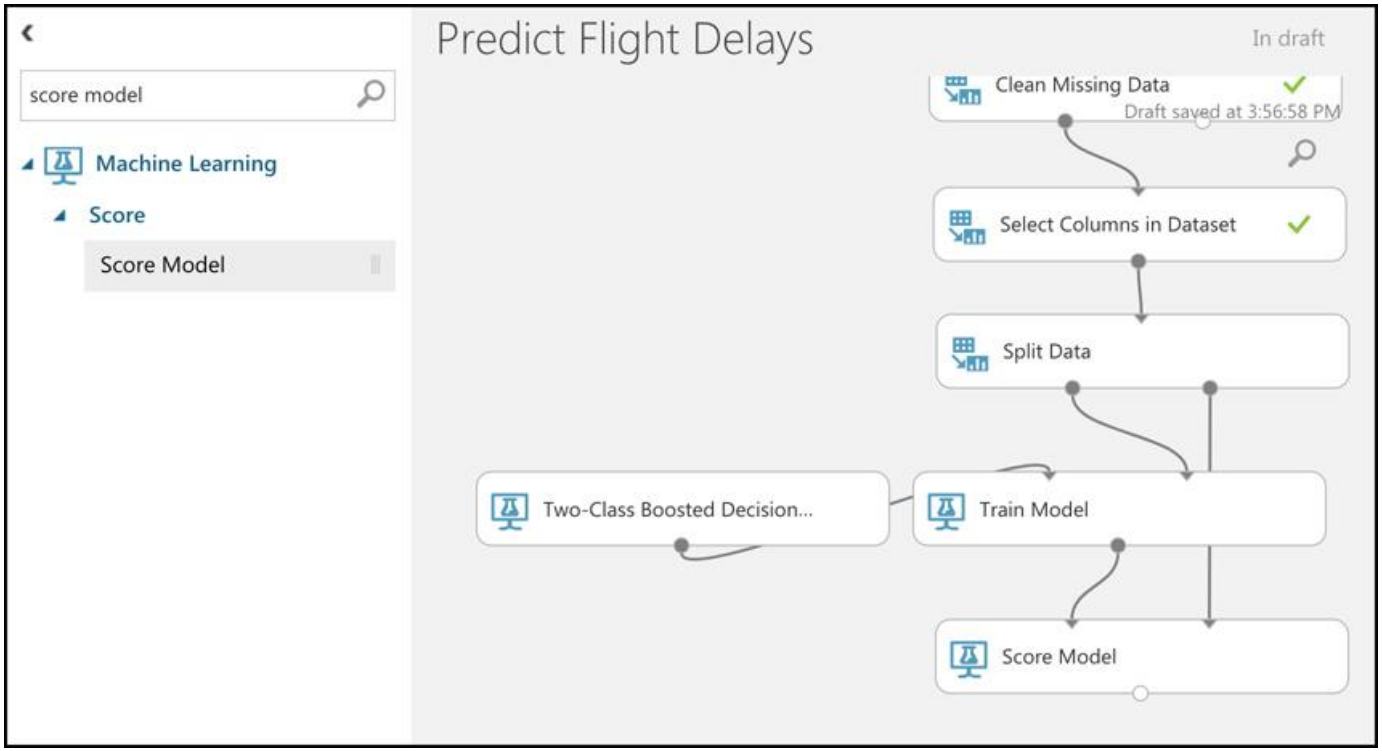


Figura 2-73 Puntuación de nuestro modelo con el Modelo de puntuación

Acaba de completar todos los pasos necesarios para crear un modelo ML, enviarle millones de filas de datos para capacitación y luego probar su modelo entrenado para ver qué tan bien tiene éxito. Lo único que queda es ejecutar el entrenamiento y la puntuación y ver el resultado. Todavía necesitamos agregar una forma de evaluar ese resultado.

- Haga clic en el cuadro de búsqueda y escriba **evaluar** .
- Arrastre el elemento **Evaluar modelo** para que esté debajo del **Modelo de puntuación** .
- Conecte el nodo inferior del **Modelo** de **puntuación** al nodo superior izquierdo del **Modelo** de **evaluación** como se muestra en la Figura 2-74 .

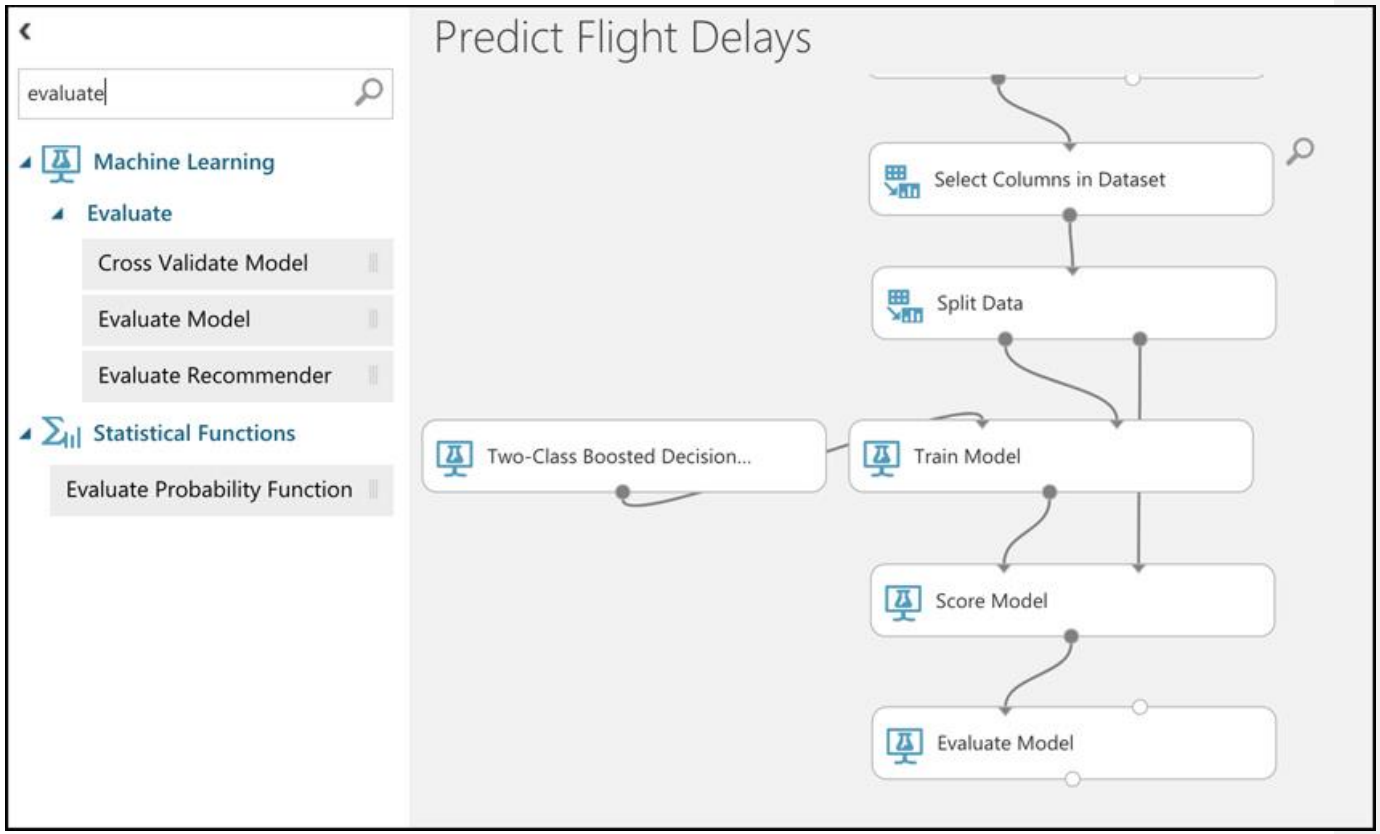


Figura 2-74 Evaluar un modelo con Evaluar modelo

El elemento Evaluar modelo le permitirá ver un informe fácil de leer que nos muestra la precisión del modelo.

Paso 5: entrenar y puntuar el modelo

Para entrenar el modelo y luego calificarlo con el 20% restante de los datos, haga clic en el botón **Ejecutar** en la parte inferior del espacio de trabajo. Tomará un tiempo correr, así que sea paciente.

Cuando el modelo haya sido entrenado y calificado, verá una marca verde en cada elemento de su espacio de trabajo. Para ver los resultados del experimento, haga clic con el botón derecho en **Evaluar modelo** , apunte a **Resultados de evaluación** y haga clic en **Visualizar** , como se muestra en la Figura 2-75 .

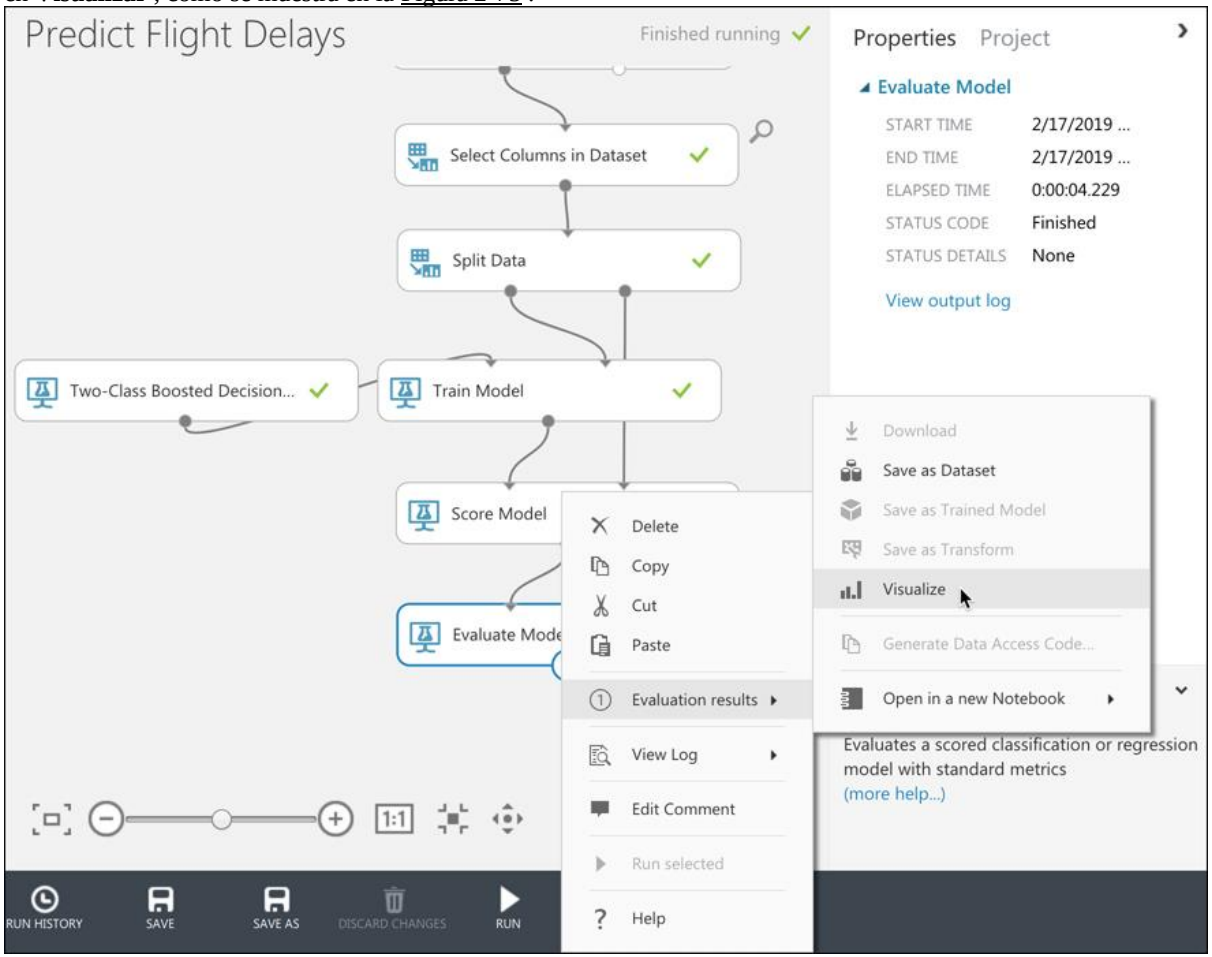


Figura 2-75 Visualización de resultados de evaluación

Después de hacer clic en Visualizar, Machine Learning Studio le mostrará una curva ROC como se muestra en la Figura 2-76 . ROC significa la característica de funcionamiento del receptor, y es un gráfico típico para determinar la efectividad de un modelo ML. Cuanto más lejos esté la línea a la izquierda del gráfico, mejor será el modelo ML. En este caso, vemos que el modelo funcionó bien. Desplácese hacia abajo para ver detalles sobre qué tan bien lo hicimos.

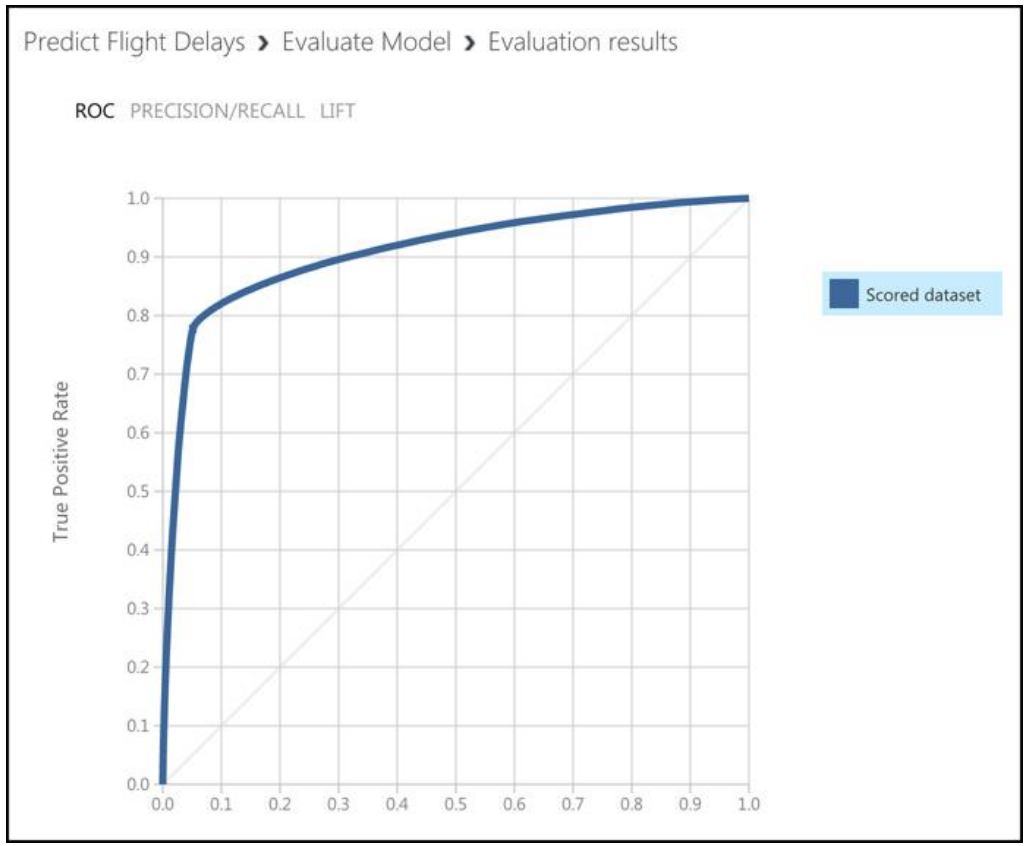
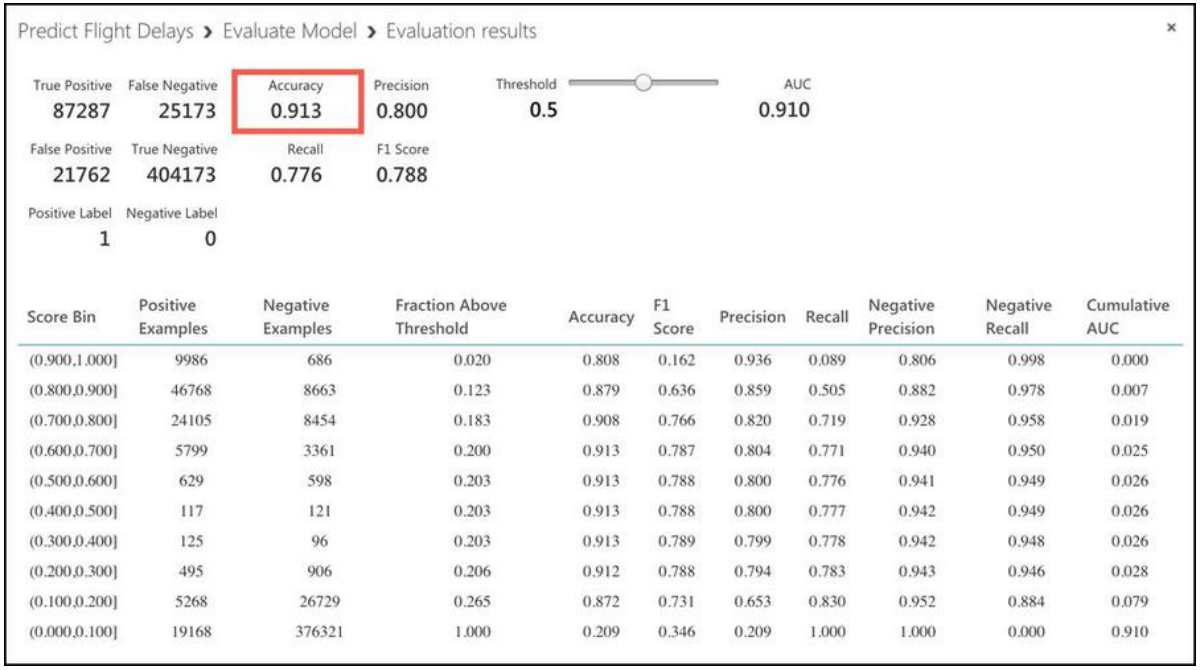


Figura 2-76 Una curva ROC que muestra los resultados de la puntuación

En la Figura 2-77 , puede ver los resultados completos del experimento. Puede ver que obtuvimos una tasa de precisión del 91.3%. Podemos mejorar esta tasa alimentando más datos al modelo, o posiblemente usando un algoritmo diferente. Siéntase libre de

experimentar por su cuenta, y si desea profundizar en una versión mucho más complicada de este experimento, consulte la plantilla de experimento Clasificación binaria: predicción de retraso de vuelo en Machine Learning Studio.



Score Bin	Positive Examples	Negative Examples	Fraction Above Threshold	Accuracy	F1 Score	Precision	Recall	Negative Precision	Negative Recall	Cumulative AUC
(0.900,1.000]	9986	686	0.020	0.808	0.162	0.936	0.089	0.806	0.998	0.000
(0.800,0.900]	46768	8663	0.123	0.879	0.636	0.859	0.505	0.882	0.978	0.007
(0.700,0.800]	24105	8454	0.183	0.908	0.766	0.820	0.719	0.928	0.958	0.019
(0.600,0.700]	5799	3361	0.200	0.913	0.787	0.804	0.771	0.940	0.950	0.025
(0.500,0.600]	629	598	0.203	0.913	0.788	0.800	0.776	0.941	0.949	0.026
(0.400,0.500]	117	121	0.203	0.913	0.788	0.800	0.777	0.942	0.949	0.026
(0.300,0.400]	125	96	0.203	0.913	0.789	0.799	0.778	0.942	0.948	0.026
(0.200,0.300]	495	906	0.206	0.912	0.788	0.794	0.783	0.943	0.946	0.028
(0.100,0.200]	5268	26729	0.265	0.872	0.731	0.653	0.830	0.952	0.884	0.079
(0.000,0.100]	19168	376321	1.000	0.209	0.346	0.209	1.000	1.000	0.000	0.910

Figura 2-77 Precisión del modelo ML

Una vez que esté satisfecho con el resultado del modelo ML, puede publicarlo en Internet para que los usuarios puedan llamarlo. Machine Learning Studio utiliza un servicio web (que es un sitio web) para hacer esto, y puede implementar fácilmente su modelo ML en un servicio web haciendo clic en **Configurar servicio web** en la parte inferior. Cuando lo haga, Machine Learning Studio agregará algunos nodos a una nueva pestaña llamada Experimento predictivo en su espacio de trabajo, por lo que deberá hacer clic en el botón Ejecutar para probar la nueva configuración antes de poder usar el servicio web.

Después de hacer clic en Ejecutar y completar su nuevo experimento predictivo con éxito, haga clic en el botón **Implementar en servicio web** para terminar de crear su servicio web. Machine Learning Studio mostrará su servicio web como se muestra en la Figura 2-78 , e incluso puede hacer clic en **Probar** para probar su nuevo servicio web.

Figura 2-78 Un nuevo servicio web para el modelo ML

Computación sin servidor

Como ya ha aprendido, una de las grandes ventajas de pasar a la nube es que puede aprovechar las grandes cantidades de infraestructura en las que han invertido los proveedores de la nube. Puede crear máquinas virtuales en la nube y pagarlas solo cuando Estás corriendo. A veces solo necesita "tomar prestada" una computadora para ejecutar un cálculo o realizar una tarea rápida. En esas situaciones, un entorno sin servidor es ideal. En una situación sin servidor, paga solo cuando su código se ejecuta en una VM. Cuando su código no se está ejecutando, no paga nada.

El concepto de computación sin servidor surgió porque los proveedores de la nube tenían máquinas virtuales no utilizadas en sus centros de datos y querían monetizarlas. Todos los proveedores de la nube necesitan capacidad excedente para poder satisfacer las necesidades de los clientes, pero cuando las máquinas virtuales están sentadas esperando a un cliente que quiera usarlo, el proveedor de la nube pierde ingresos. Para resolver ese problema, los proveedores de la nube crearon planes basados en el consumo que le permiten ejecutar su código en estas máquinas virtuales excedentes y usted paga solo por su uso mientras su código se está ejecutando.

Consejo de examen

Es importante comprender que "sin servidor" no significa que no haya máquinas virtuales involucradas. Simplemente significa que la VM que ejecuta su código no está explícitamente asignada a usted. Su código se mueve a la VM, se ejecuta y luego se retira.

Debido a que su código sin servidor se ejecuta con capacidad excedente, los proveedores de la nube generalmente ofrecen grandes descuentos en planes basados en el consumo. De hecho, para pequeñas cargas de trabajo, es posible que no pague nada.

Azure tiene muchos servicios sin servidor. Ya hemos comentado que Azure Databricks y Azure Machine Learning Service no tienen servidor. Sin embargo, hay otros servicios sin servidor que no encajan en las categorías que ya hemos discutido. Son Azure Functions para cómputo sin servidor, Azure Logic Apps para flujos de trabajo sin servidor y Azure Event Grid para enrutamiento de eventos sin servidor.

Funciones Azure

Azure Functions es el componente informático de las ofertas sin servidor de Azure. Eso significa que puede usar funciones para escribir código sin tener que preocuparse por implementar ese código o crear máquinas virtuales para ejecutar su código. Las aplicaciones que usan Azure Functions a menudo se denominan aplicaciones de función.

Más información **Función Aplicaciones Uso Servicio de aplicaciones**

Las aplicaciones de función no tienen servidor, pero bajo el capó se ejecutan en Azure App Service. De hecho, puede optar por crear su aplicación de función en un plan de App Service, en cuyo caso no se beneficia del modelo de consumo de pagar solo cuando se ejecuta su código. Cubriremos eso con más detalle más adelante en este capítulo.

Las funciones se pueden crear de muchas maneras diferentes. Puede crear una aplicación de función usando:

- Microsoft Visual Studio
- Código de Microsoft Visual Studio
- Aplicaciones de funciones de Maven para Java
- Línea de comando de Python para aplicaciones de funciones de Python
- Interfaz de línea de comandos (CLI) de Azure en Windows o Linux
- El portal de Azure

Suponiendo que no está creando su aplicación de función utilizando un método específico para un idioma en particular, puede elegir entre .NET (para aplicaciones de función C # y F #), Java y JavaScript (para aplicaciones de función de nodo). En la Figura 2-79 , estamos creando una aplicación de función en el portal de Azure,y seleccionó .NET como el tiempo de ejecución de la aplicación de función para que pueda usar el lenguaje C # para escribir funciones.

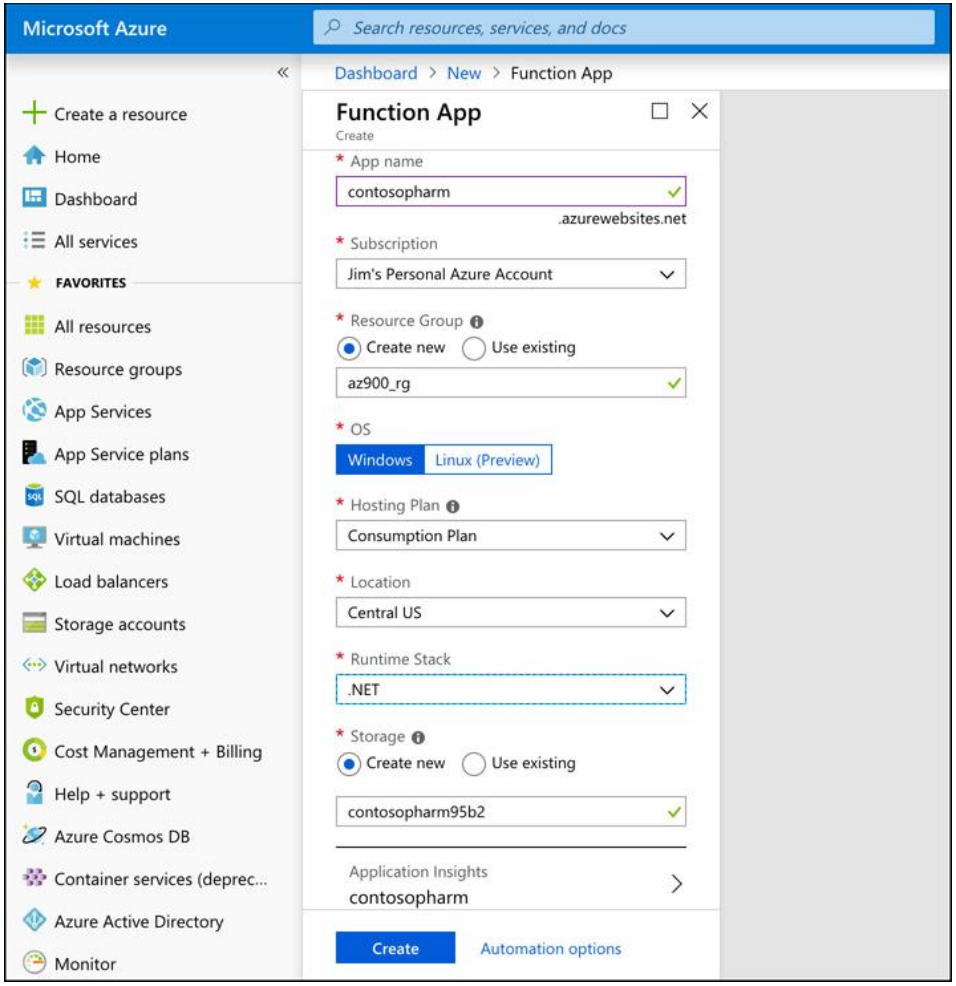


Figura 2-79 Creación de una nueva aplicación de función en Azure Portal

Una vez que su aplicación de función esté lista, puede abrirla en el portal para comenzar a crear funciones. La Figura 2-80 muestra la nueva aplicación de función en el portal de Azure.

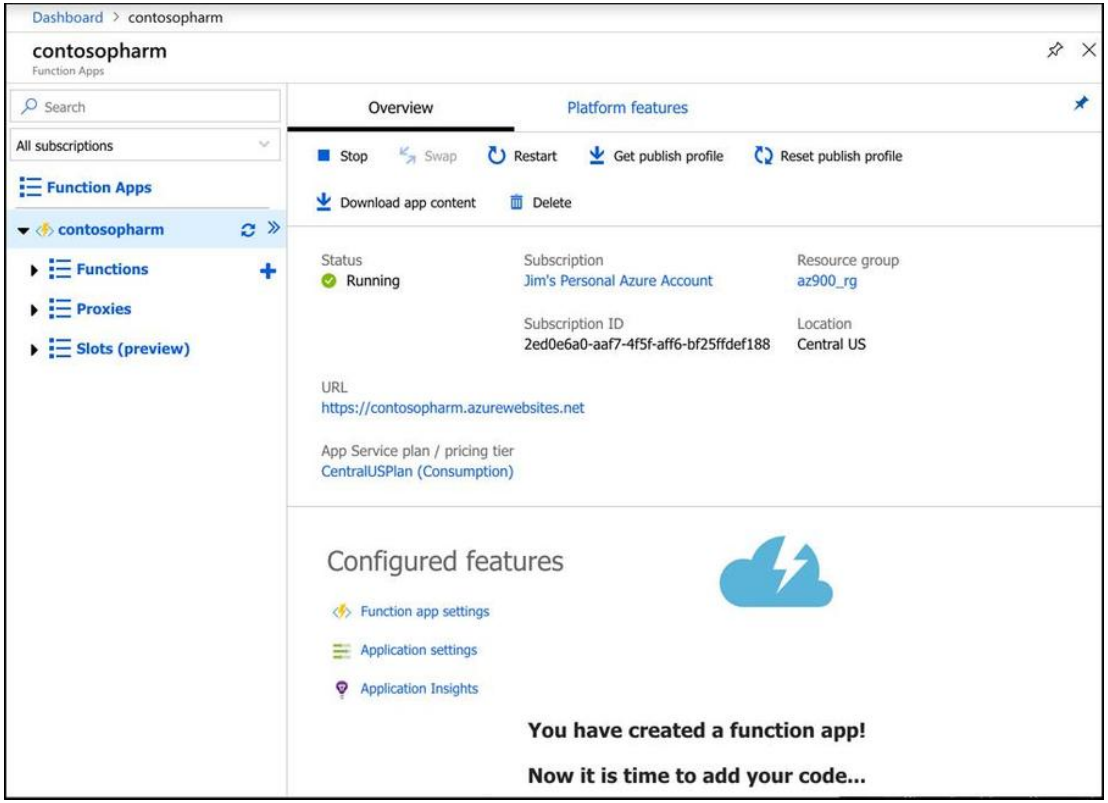


Figura 2-80 Una nueva aplicación de función en Azure Portal

Desde aquí, puede crear una nueva función, un nuevo proxy o una nueva ranura. Una función es un código que se ejecuta cuando algo lo activa. (Pronto veremos los desencadenantes). Un proxy le permite configurar múltiples puntos finales para su aplicación de función, pero los expone a todos a través de una única URL. Las ranuras le permiten crear una copia de su aplicación de función que no es pública. Puede escribir código y probar esta copia, y cuando esté satisfecho de que está listo para la producción, puede cambiarlo a producción con solo hacer clic en un botón. Esta característica en App Service se llama ranuras de implementación.

Si hace clic en **Configuración de la aplicación de función** en **Funciones** configuradas (que se muestra en la Figura 2-80), podemos cambiar algunas configuraciones para la Aplicación de función, como se muestra en la Figura 2-81 .

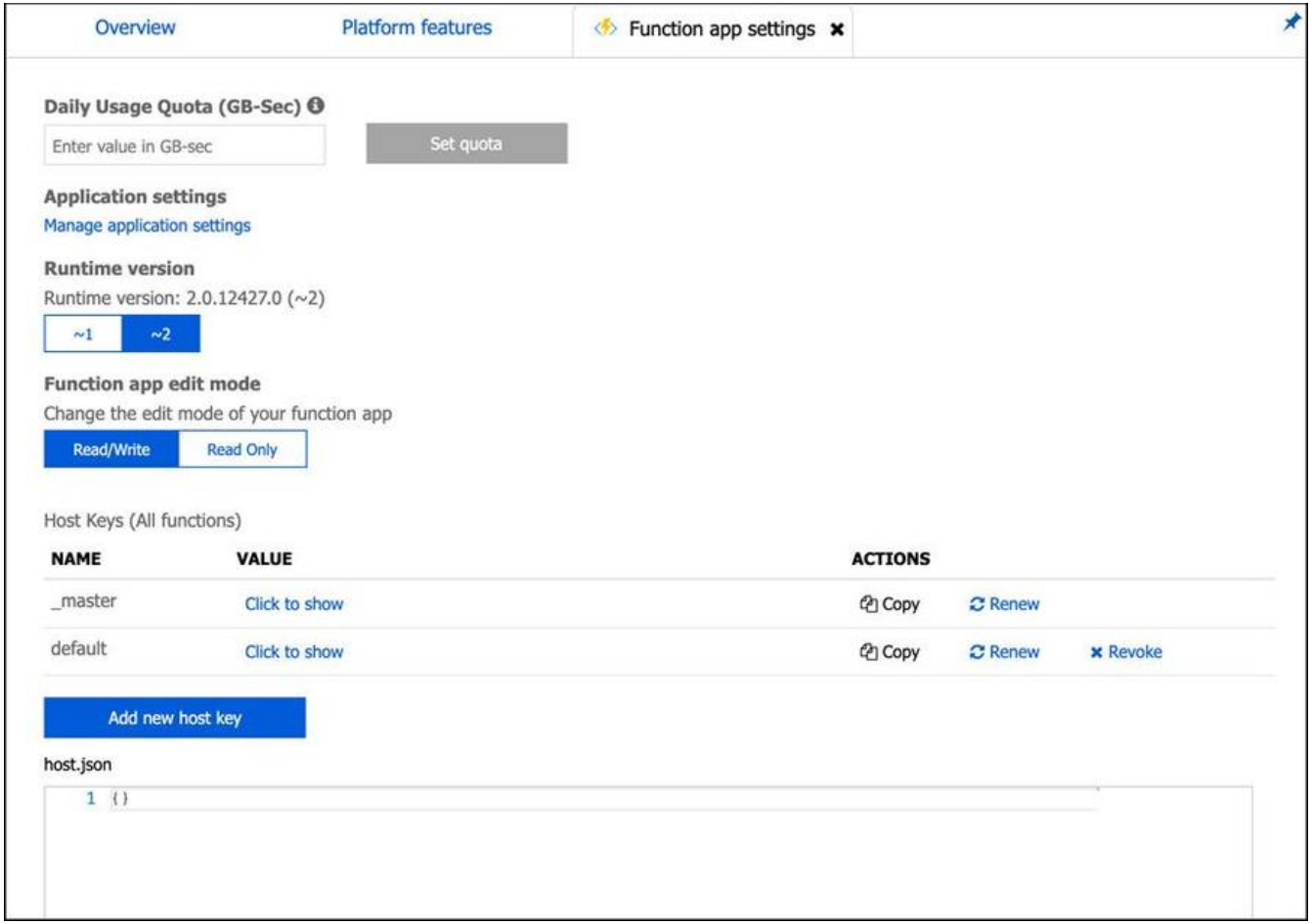


Figura 2-81 Configuración de la aplicación de funciones

Desde esta pantalla, puede configurar una cuota diaria para su aplicación de función. Una vez que alcance la cuota, Azure detendrá la aplicación de función hasta el día siguiente. También puede cambiar la versión de tiempo de ejecución de la aplicación de función. Esta es la versión en tiempo de ejecución de Azure Functions, y aunque generalmente se recomienda usar la última versión, si sus funciones se escribieron en una versión anterior, no podrá actualizarlas simplemente cambiando la versión aquí. Cambiar las

versiones principales puede hacer que su aplicación se rompa, por lo que Microsoft evitará que cambie la versión si tiene funciones existentes en su aplicación de funciones.

También puede cambiar su aplicación de función al modo de solo lectura para evitar cualquier cambio en ella. Esto es útil si tienes múltiples desarrolladores escribiendo código para tu aplicación y no quieres que alguien cambie algo sin tu conocimiento. Finalmente, puede ver, renovar, revocar y agregar nuevas claves de host. Una clave de host se utiliza para controlar el acceso a sus funciones. Cuando crea una función, puede especificar si alguien puede usarla o si se necesita una clave.

 *Consejo de examen*

Aunque una clave puede ayudar a proteger sus funciones, no están diseñadas para ofrecer seguridad completa de las aplicaciones de funciones. Si desea proteger su aplicación de función del uso no autorizado, debe utilizar las funciones de autenticación disponibles en el Servicio de aplicaciones para solicitar la autenticación. También puede usar Microsoft API Management para agregar requisitos de seguridad a su aplicación de función.

Si hace clic en Configuración de la aplicación (que se muestra en la Figura 2-80), puede configurar los ajustes para la aplicación de función. Estas son configuraciones específicas para App Service. La Figura 2-82 muestra algunas de estas configuraciones, incluso si la aplicación se ejecuta en 32 bits o 64 bits, la versión HTTP, cómo puede acceder a sus archivos mediante FTP y más. También puede configurar cadenas de conexión de base de datos desde esta página.

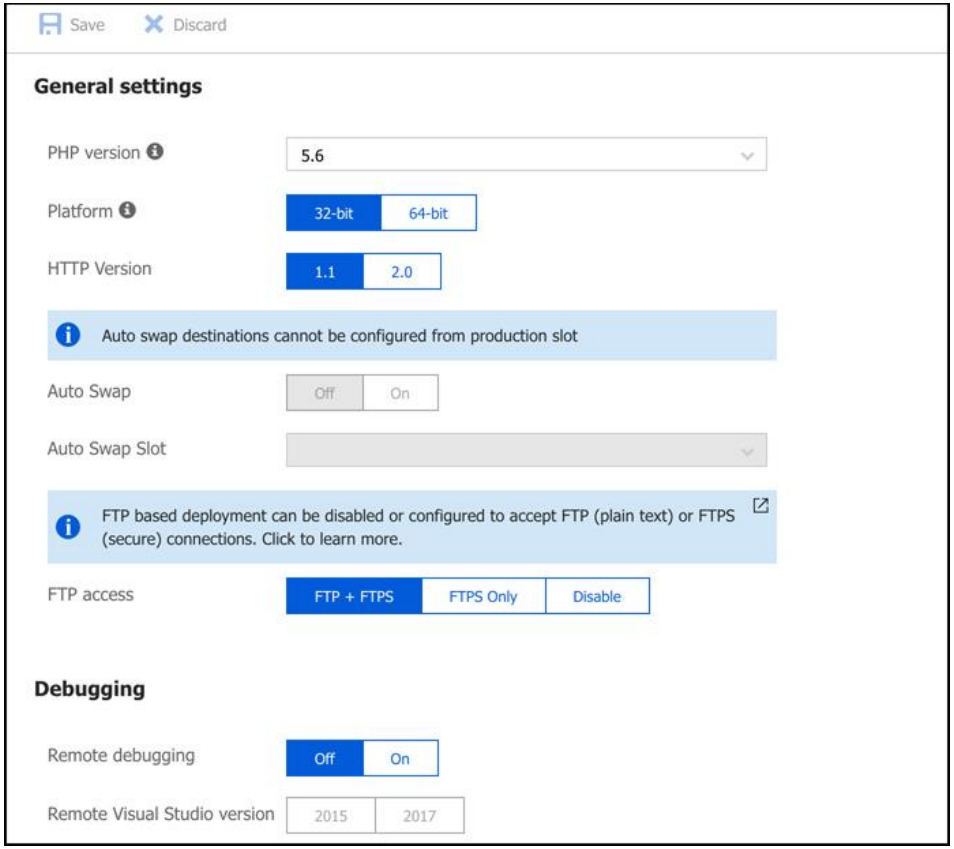


Figura 2-82 Algunas de las configuraciones de la aplicación de funciones

Finalmente, si hace clic en la pestaña Características de la plataforma, puede ver todas las características disponibles en la plataforma del Servicio de aplicaciones, como se muestra en la Figura 2-83 . Desde aquí, puede configurar cosas como certificados SSL, nombres de dominio personalizados para su aplicación de función, autenticación llave en mano y más.

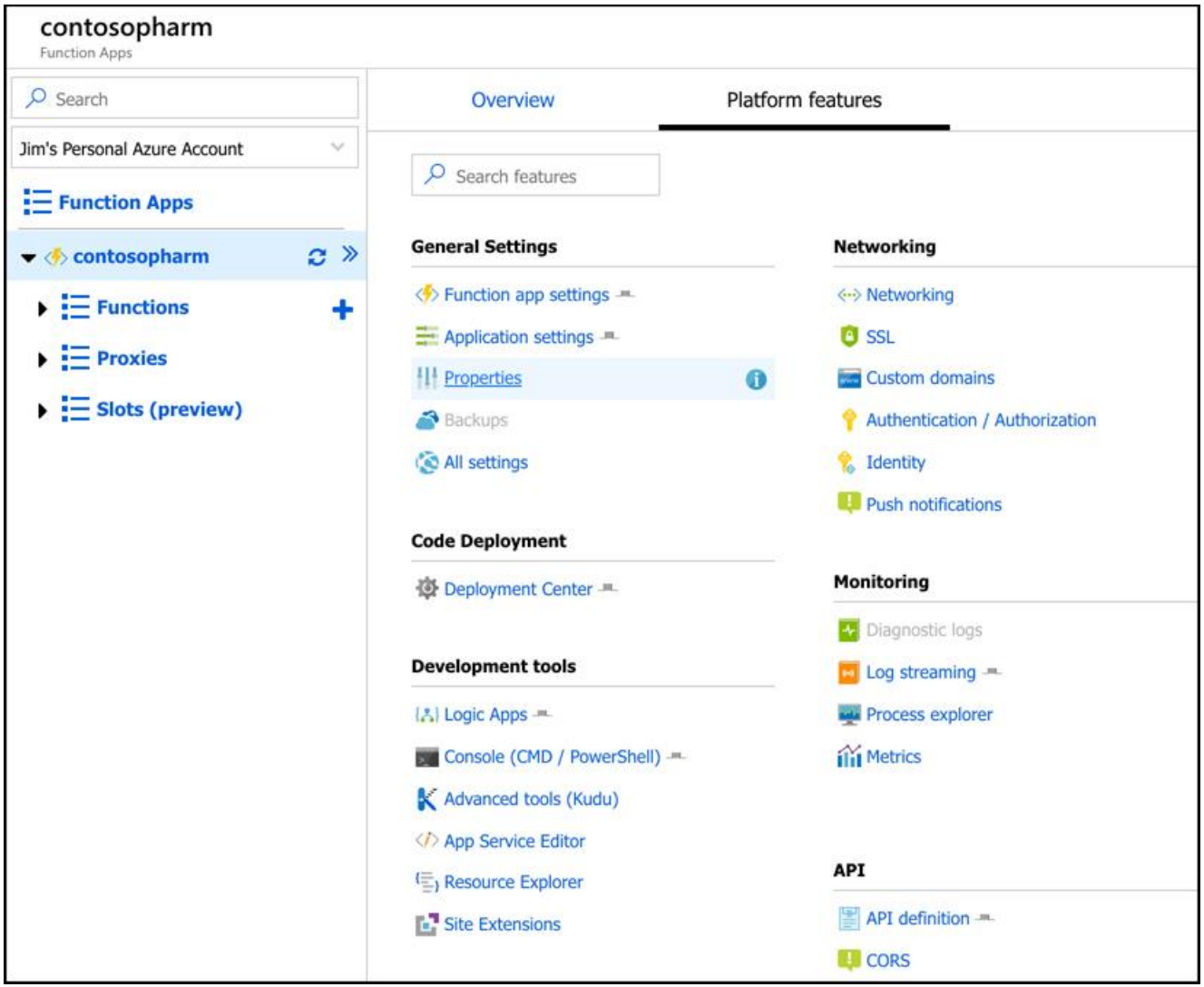


Figura 2-83 Características de la plataforma del servicio de aplicaciones disponibles para su aplicación de funciones

Más información **Azure App Service**

Una discusión completa de Azure App Service está fuera del alcance de este libro, pero si desea obtener más información, consulte: *https://azure.microsoft.com/services/app-service* .

Para crear una nueva función, haga clic en el signo + como se muestra en la Figura 2-84 . Luego puede elegir su entorno de desarrollo. Puede elegir Visual Studio, Visual Studio Code, un entorno de desarrollo dentro del portal de Azure, o puede usar un editor de código de su elección junto con las Herramientas principales de Azure Functions.

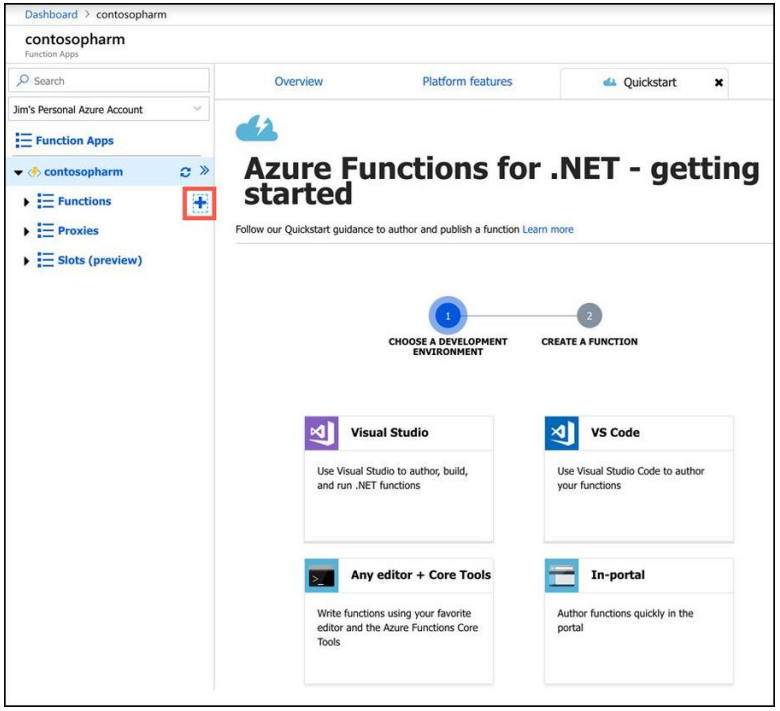


Figura 2-84 Crear una función

Si elige cualquier opción que no sea In-Portal, deberá especificar cómo desea implementar su función en App Service. Sus opciones dependen del entorno de desarrollo que elija, pero generalmente implicará el uso de funciones de su entorno para enviar la función

directamente al Servicio de aplicaciones, o deberá usar el Centro de implementación del Servicio de aplicaciones. De cualquier manera, la implementación es rápida y fácil.

Según el entorno de desarrollo que elija, es probable que deba completar algunos pasos previos para desarrollar su función. Verás una pantalla que te dice exactamente qué hacer para que todo funcione correctamente. En la Figura 2-85 , puede ver lo que se requiere para usar VS Code para desarrollar funciones. En la mayoría de los casos, requerirá que instale las herramientas principales de Azure Functions.

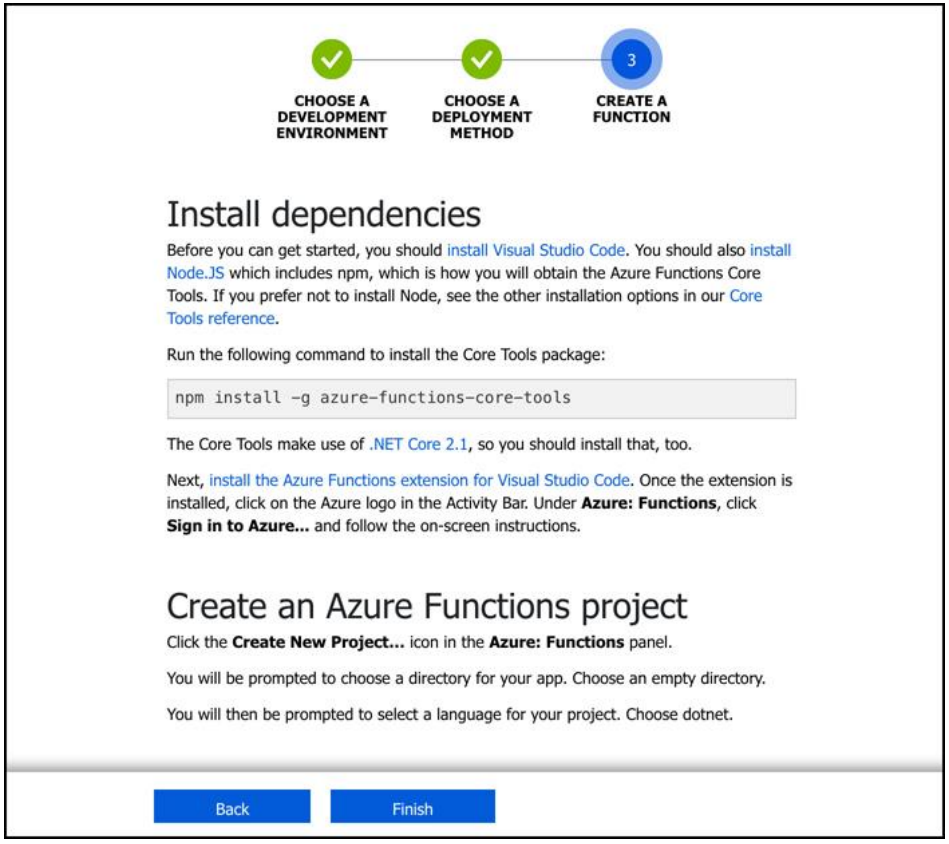


Figura 2-85 Creación de una función con Visual Studio Code y Azure Functions Core Tools

Las funciones funcionan utilizando un sistema basado en disparadores. Cuando crea su función, elige un disparador que iniciará su función. Cuando se activa, se ejecutará su código de función. Por lo general, querrá que su código de función haga algo simple. Si necesita una función más compleja que realice muchas cosas, puede usar Proxies de función para crear varias funciones que funcionen juntas para completar una tarea. Este tipo de desarrollo se conoce como *microservicios* , y le permite cambiar rápidamente la funcionalidad simplemente cambiando una sola función.

Una vez que se activa su función y se ejecuta el código, puede elegir qué sucede utilizando lo que se denomina *enlace de salida* . El tipo de enlaces que puede usar depende del tipo de función que cree. La Figura 2-86 muestra algunos de los diferentes enlaces de salida disponibles cuando se utiliza un HttpTrigger para una función. Esta función se ejecutará tan pronto como se solicite una URL particular.

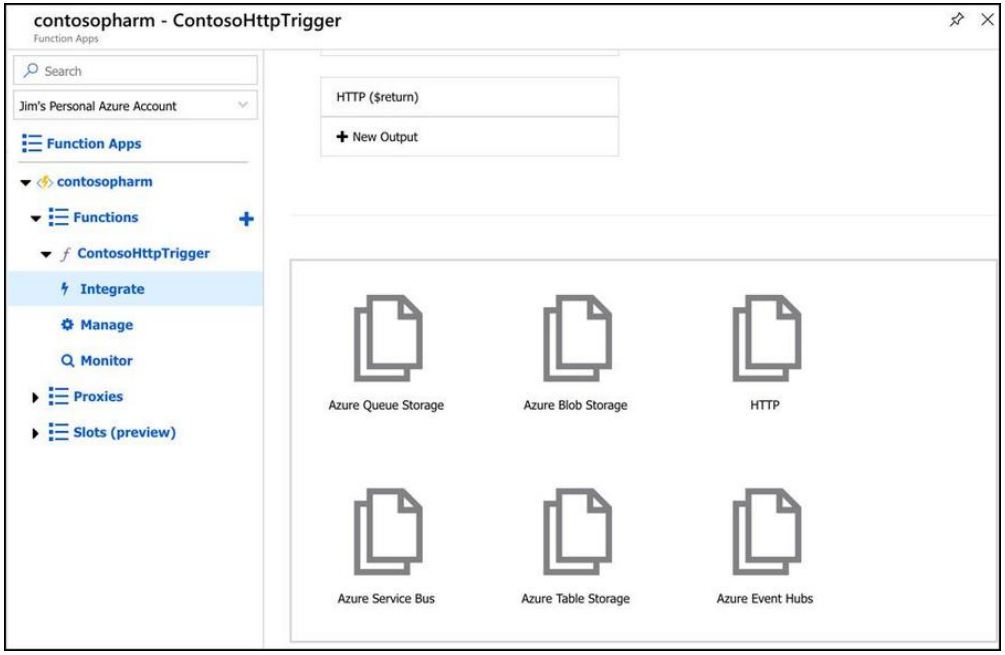


Figura 2-86 Enlaces de salida en Azure Functions

Más información **Funciones Httptrigger**

Las funciones HttpTrigger son increíblemente poderosas porque pueden llamarse como un webhook. Muchos servicios en línea admiten webhooks. En un escenario de webhook, puede configurar un servicio para realizar una solicitud a una URL particular en respuesta a eventos. Si configura ese webhook para llamar a la URL de su función de Azure, puede agregar fácilmente una funcionalidad potente a su flujo de trabajo.

También puede configurar múltiples salidas para su función. Sin embargo, para flujos de trabajo más complejos, Logic Apps suele ser una mejor opción, y puede integrar Logic Apps directamente con Azure Functions.

Aplicaciones de Azure Logic

Las aplicaciones lógicas son similares a las aplicaciones de función en el sentido de que son activadas por un disparador, pero lo que sucede después de eso es completamente diferente. A diferencia de las aplicaciones de funciones, no tiene que escribir código para crear algunos flujos de trabajo potentes con las aplicaciones lógicas.

Un flujo de trabajo simplemente significa que una aplicación lógica reacciona a algo que sucede y responde realizando una serie de tareas, como enviar un correo electrónico, transferir datos a una base de datos, etc. Puede hacer estas cosas en orden, pero también puede hacer dos cosas a la vez. Como ejemplo, es posible que tenga un sitio de comercio electrónico y cuando un cliente ordena un producto que desee:

- Actualice su recuento de inventario del producto
- Generar una factura para el artículo.
- Enviar la factura por correo electrónico al cliente
- Suscríbase al cliente para recibir su boletín informativo
- Generar una etiqueta de envío para el artículo.

Logic Apps le permite crear fácilmente este tipo de flujos de trabajo complejos, y debido a que Logic Apps se integra con más de un centenar de otros servicios (servicios de Azure y servicios de terceros), puede hacer casi cualquier cosa en un flujo de trabajo de Logic Apps.

Hay tres componentes en Logic Apps que hacen posible los flujos de trabajo: conectores, disparadores y acciones. Un conector es un componente que conecta su aplicación lógica a algo. Ese podría ser otro servicio de Azure, pero también podría ser un servicio de terceros, un servidor FTP, etc. Cada conector tendrá uno o más desencadenantes y acciones específicas para ese conector. Un desencadenante es una acción específica que hará que se ejecute el flujo de trabajo de su aplicación lógica, y una acción es lo que hará su aplicación lógica como salida. Puede combinar varias acciones para un conector, y también puede combinar varios conectores para crear flujos de trabajo complejos y potentes.

Crea aplicaciones lógicas en el portal de Azure. Una vez que lo crea, el diseñador de Logic Apps se muestra de forma predeterminada. Desde el diseñador, puede elegir el disparador para su aplicación lógica como se muestra en la Figura 2-87 . La lista que se muestra es una breve lista de desencadenantes comunes, pero hay muchos más para elegir. De hecho, también hay un activador para Azure Functions, por lo que puede activar un flujo de trabajo de Logic Apps cuando se ejecuta su función.

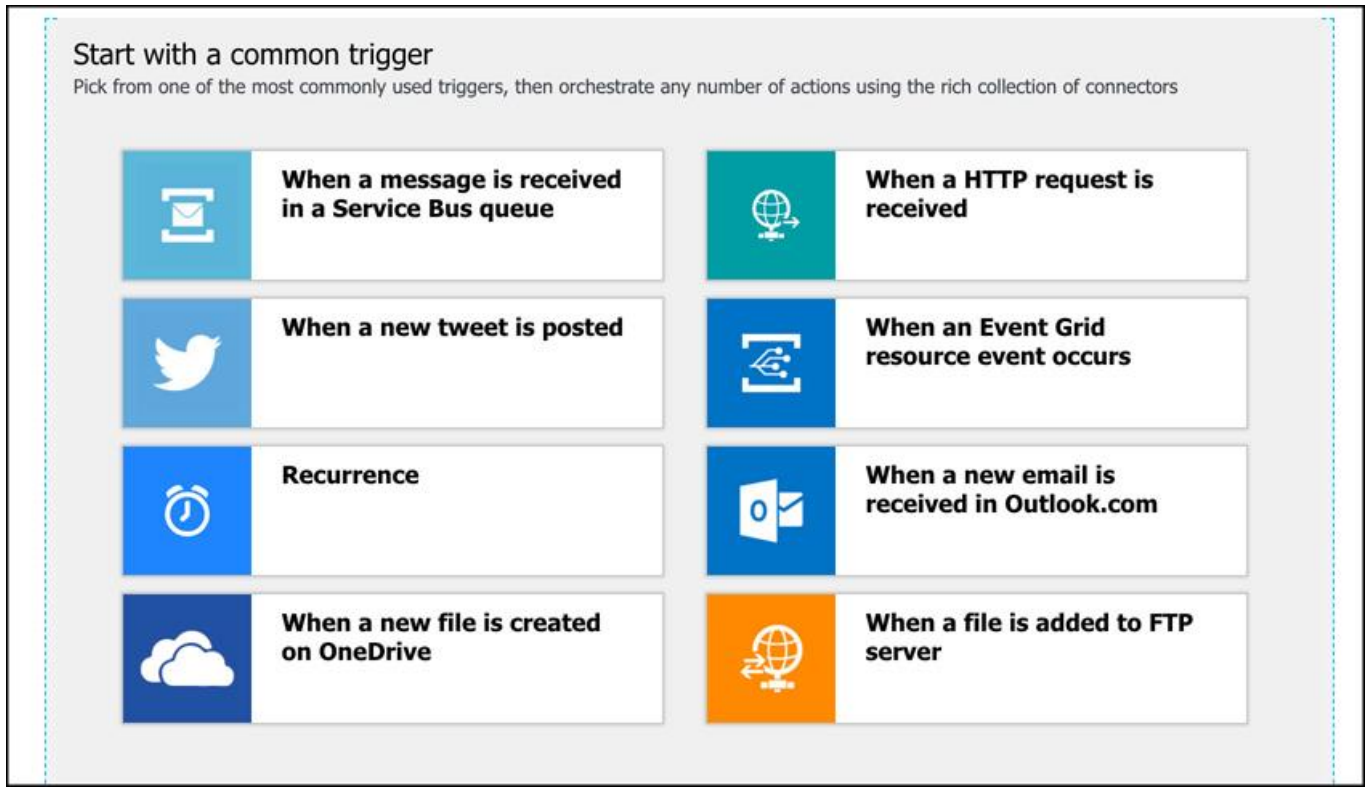


Figura 2-87 Disparadores de la aplicación lógica común

Consejo de examen

Es importante comprender la diferencia entre conectores y disparadores. Todos los elementos que se muestran en la Figura 2-87 son desencadenantes asociados con conectores específicos. Por ejemplo, cuando se crea un nuevo archivo en OneDrive es un disparador para el conector de OneDrive. También hay otros desencadenantes de OneDrive disponibles, que incluyen cuándo se modifica un archivo y cuándo se elimina un archivo.

Si se desplaza hacia abajo, verá una gran cantidad de plantillas que puede usar para crear una aplicación lógica, como se muestra en la Figura 2-88 . Estas plantillas configurarán automáticamente una aplicación lógica que contiene un flujo de trabajo completo que puede modificar para sus propios fines. Esta es la forma más rápida de comenzar, pero las plantillas incluidas pueden no ser exactamente lo que desea, por lo que también puede crear una aplicación lógica en blanco y comenzar desde cero.

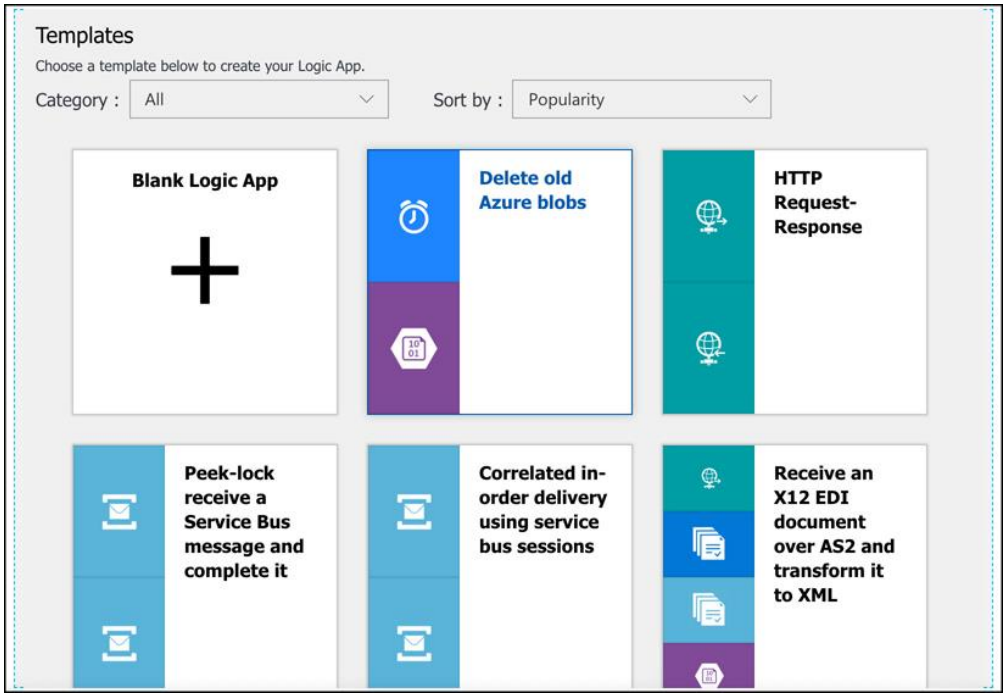


Figura 2-88 Plantillas de aplicación lógica

Después de crear su aplicación lógica en blanco, puede elegir entre varias formas de comenzar a construir su flujo de trabajo. Puede seleccionar un activador de la lista, buscar un activador o conector, o simplemente puede seleccionar un conector de la lista y ver qué activadores están disponibles. Como se muestra en la Figura 2-89 , hay muchas opciones disponibles para comenzar.

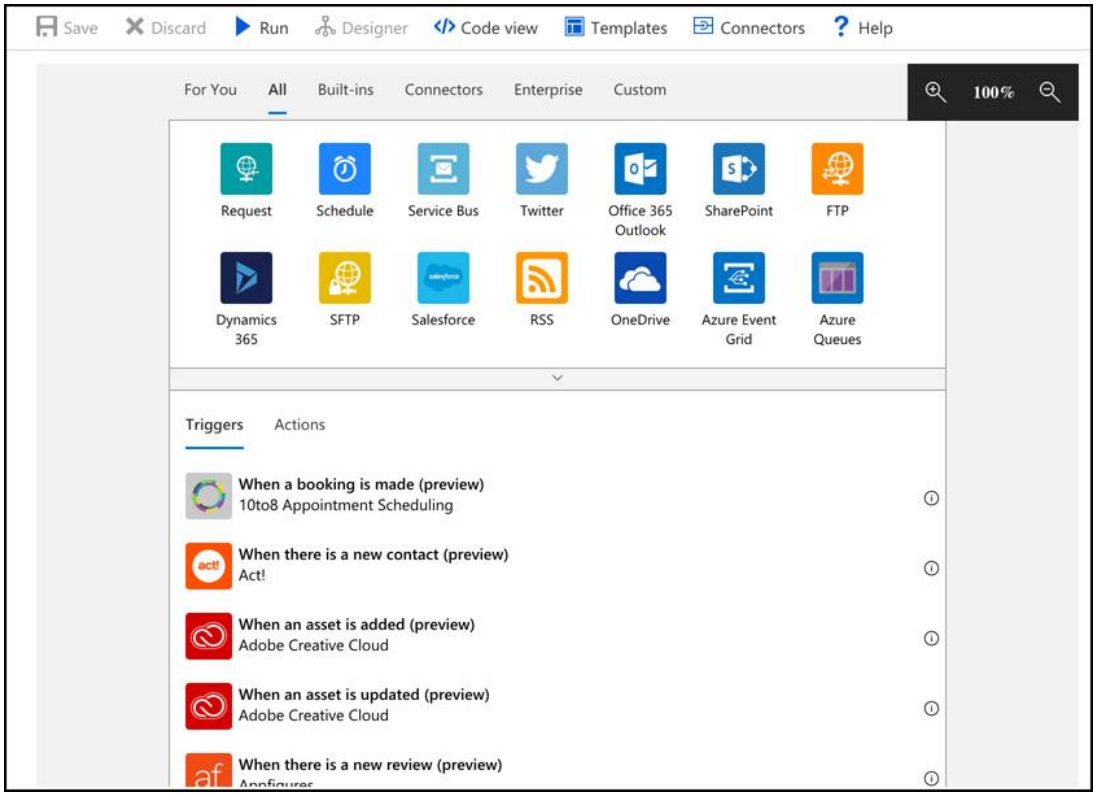


Figura 2-89 Agregar disparadores a su aplicación lógica

En la Figura 2-90 , hemos configurado el conector OneDrive para monitorear una carpeta en OneDrive. Cuando se modifica un archivo en esa carpeta, se iniciará el flujo de trabajo de la aplicación lógica. Para hacer algo cuando se modifica un archivo, haga clic en **Nuevo paso** para agregar una acción.

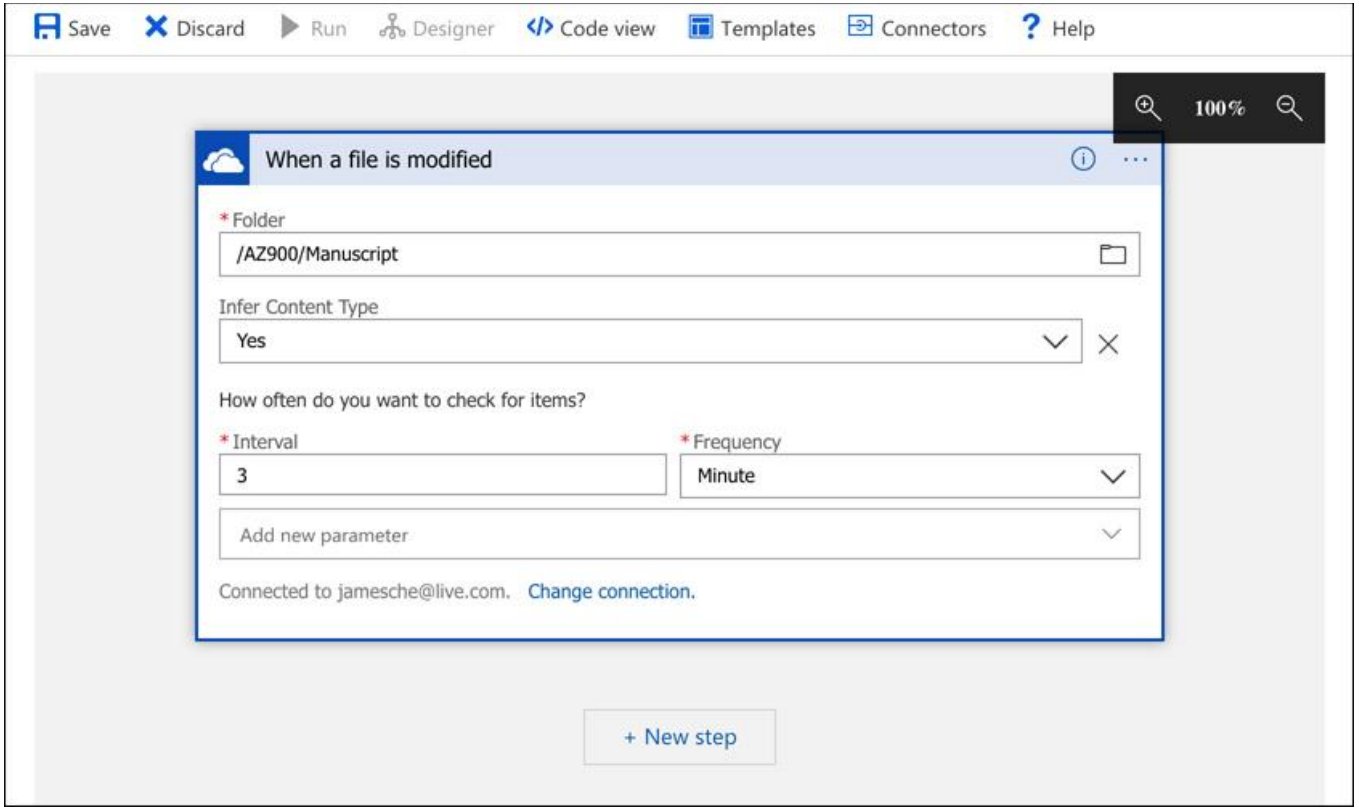


Figura 2-90 Uso del conector OneDrive

Al hacer clic en **Nuevo paso** , verá el mismo tipo de pantalla que se muestra cuando se inicia la aplicación lógica. Dado que agregamos un paso a un flujo de trabajo que ya tiene un desencadenante, Logic Apps muestra las acciones que puede tomar cuando se activa la aplicación. Hay muchas acciones para elegir, como se muestra en la Figura 2-91 .

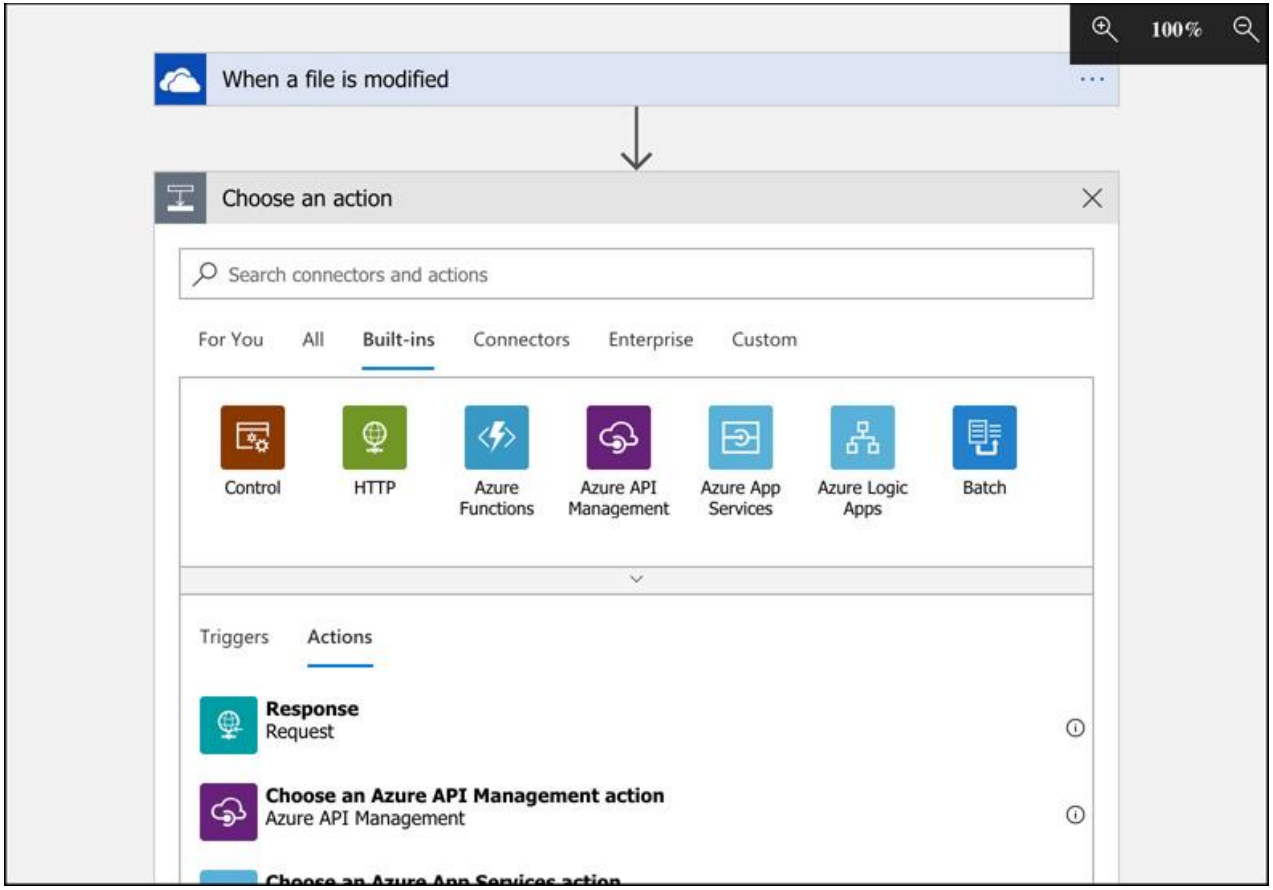


Figura 2-91 Agregar una acción a la aplicación lógica

En la Figura 2-92 , configuramos la aplicación lógica para llamar a la aplicación de función cuando se modifica un archivo en la carpeta OneDrive. Puede pasar el nombre de archivo que se modificó a la aplicación de función para que sepa qué ha cambiado, lo que puede hacer con contenido dinámico. Simplemente haga clic en **Nombre de archivo** de la lista. Por supuesto, solo puede pasar un elemento de contenido dinámico en su acción.

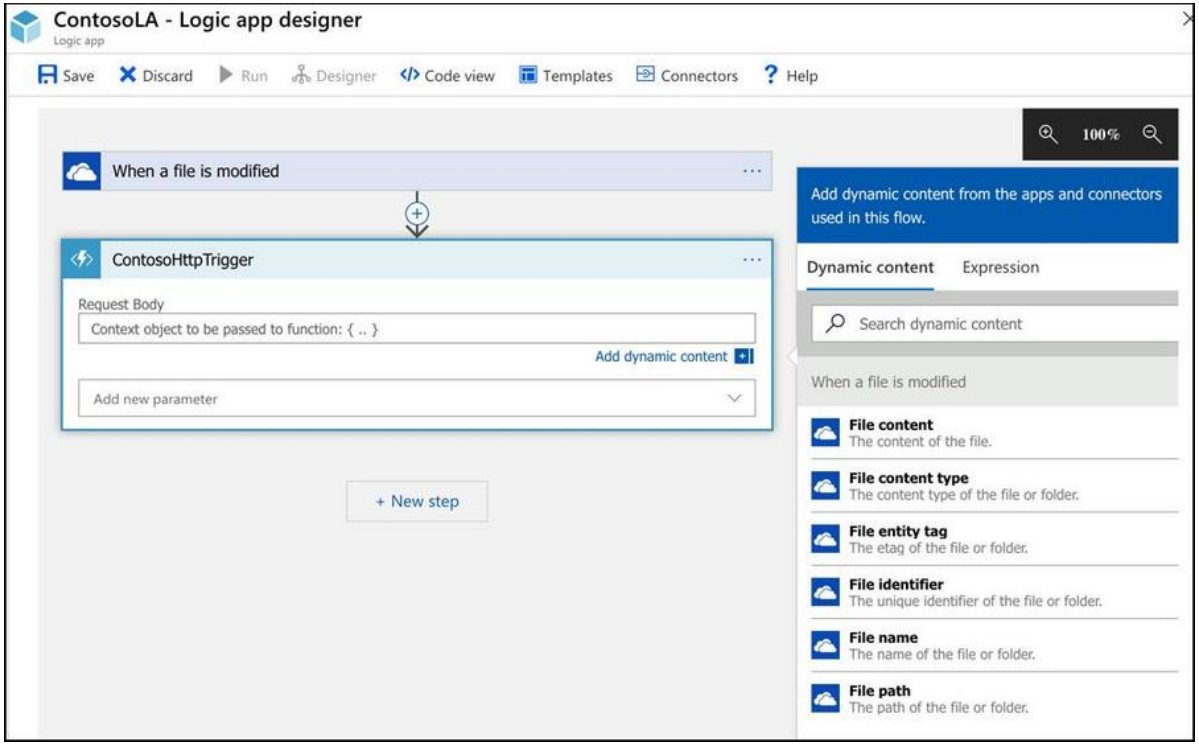


Figura 2-92 Configuración de una acción de aplicación de función

Más información **Pasando parámetros a funciones de aplicaciones**

Cuando use una aplicación lógica para llamar a una aplicación funcional, asegúrese de que la aplicación funcional esté diseñada para aceptar los datos que la aplicación lógica le está transmitiendo. De lo contrario, la aplicación de función encontrará un error cuando sea activada por la aplicación lógica.

Consejo de examen

Mientras configura los desencadenantes y las acciones en el diseñador de Logic Apps, Logic Apps está escribiendo código para usted bajo el capó que implementará su flujo de trabajo. Los flujos de trabajo de la aplicación lógica se definen usando archivos JSON, y el diseñador genera este código JSON mientras configura su aplicación.

Ahora tiene una aplicación lógica en funcionamiento. Puede probar el flujo de trabajo haciendo **clic** en **Guardar** en la parte superior del diseñador. El conector OneDrive se configuró para buscar un archivo modificado cada tres minutos (consulte la Figura 2-90), por lo que es posible que deba esperar unos minutos antes de que se active el flujo de trabajo. También puede hacer clic en **Ejecutar disparador** en la parte superior del diseñador para ejecutar manualmente el disparador.

Puede monitorear sus aplicaciones lógicas mediante el portal de Azure. Abra la aplicación y haga clic en **Descripción general** para ver cuándo se activó su activador y si ejecutó o no su flujo de trabajo como se muestra en la Figura 2-93 .

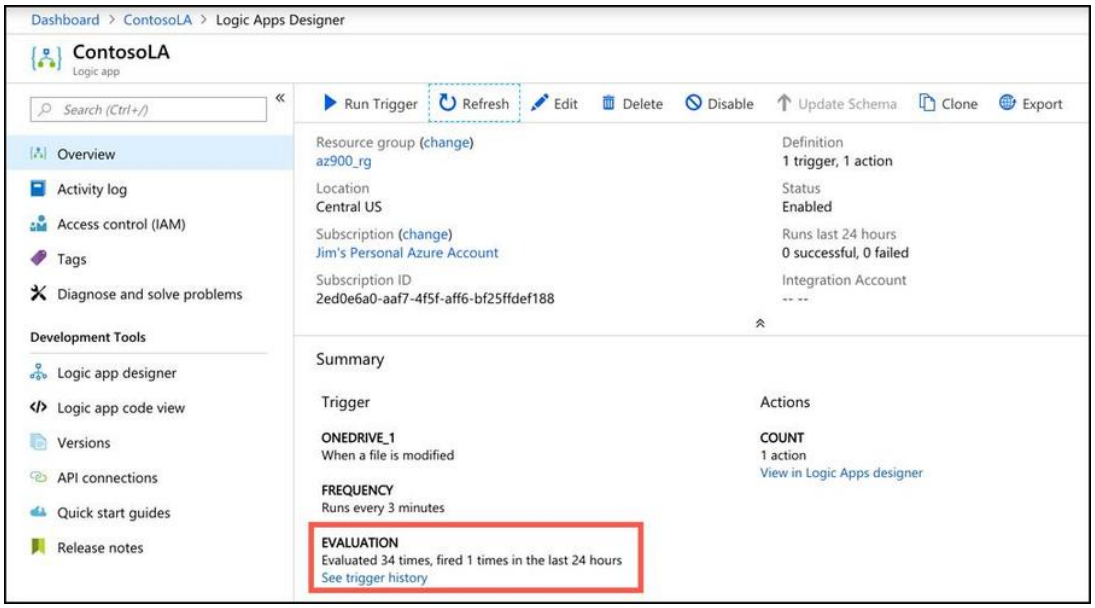


Figura 2-93 El portal de Azure que se muestra cuando se ejecutó el flujo de mi aplicación lógica

Si hace clic en **Ver historial de activadores** , puede ver un historial completo de cuándo se evaluó su activador y cuándo activó el flujo de trabajo para su aplicación lógica.

En este caso, hemos usado una aplicación lógica para llamar a una función de Azure, pero podría haber escrito un archivo de registro en Azure Storage o almacenado alguna información en una base de datos Azure SQL. Si desea que su aplicación lógica se integre específicamente con otros servicios de Azure como este, puede integrar su aplicación lógica con Azure Event Grid para una experiencia más óptima.

Cuadrícula de eventos de Azure

El concepto de diferentes servicios de Azure que interactúan entre sí ya debería serle bastante familiar. Hay muchas formas de integrar servicios como este y, en algunos casos, necesita un recurso de Azure para saber acerca de un cambio en otro recurso de Azure. Puede usar un método de sondeo para esto, similar a la aplicación lógica que comprueba una vez contra OneDrive cada tres minutos buscando un cambio. Sin embargo, es más eficiente habilitar un servicio de Azure para desencadenar un evento cuando sucede algo específico, y configurar otro servicio de Azure para escuchar ese evento para que pueda reaccionar ante él. Event Grid proporciona esa funcionalidad.

Note la **cuadrícula de eventos y la computación sin servidor**

Event Grid tiene muchas capacidades que no están relacionadas con la informática sin servidor, pero en el alcance de este capítulo, solo cubrimos las capacidades sin servidor y Event Grid.

Tanto Azure Functions como Azure Logic Apps están integradas con Event Grid. Puede configurar una función para que se ejecute cuando ocurra un evento Event Grid. En la Figura 2-94 , puede ver la lista de recursos de Azure que puede activar eventos de Event Grid. No todos los servicios de Azure están representados en Event Grid, pero con el tiempo se agregan más servicios.

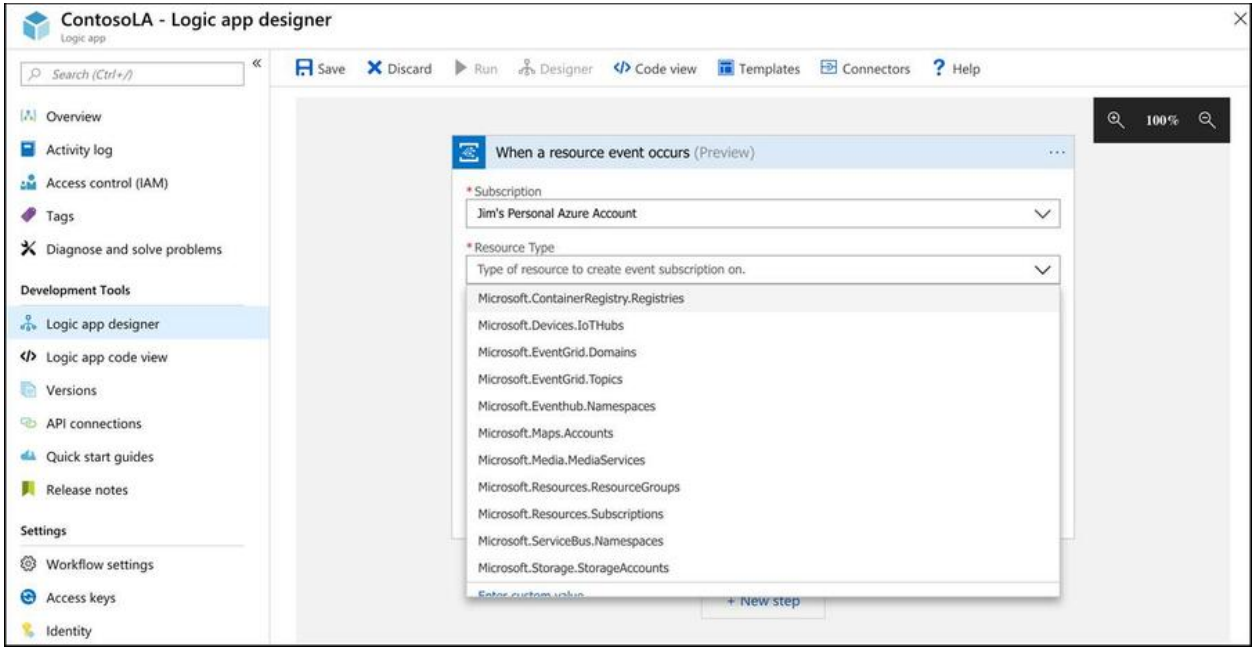


Figura 2-94 Recursos disponibles en Event Grid

Una vez que haya seleccionado el tipo de recurso, configure el evento que desea escuchar. Los eventos disponibles pueden variar según el recurso que haya seleccionado. En la Figura 2-95 , estamos creando un evento para una suscripción de Azure.

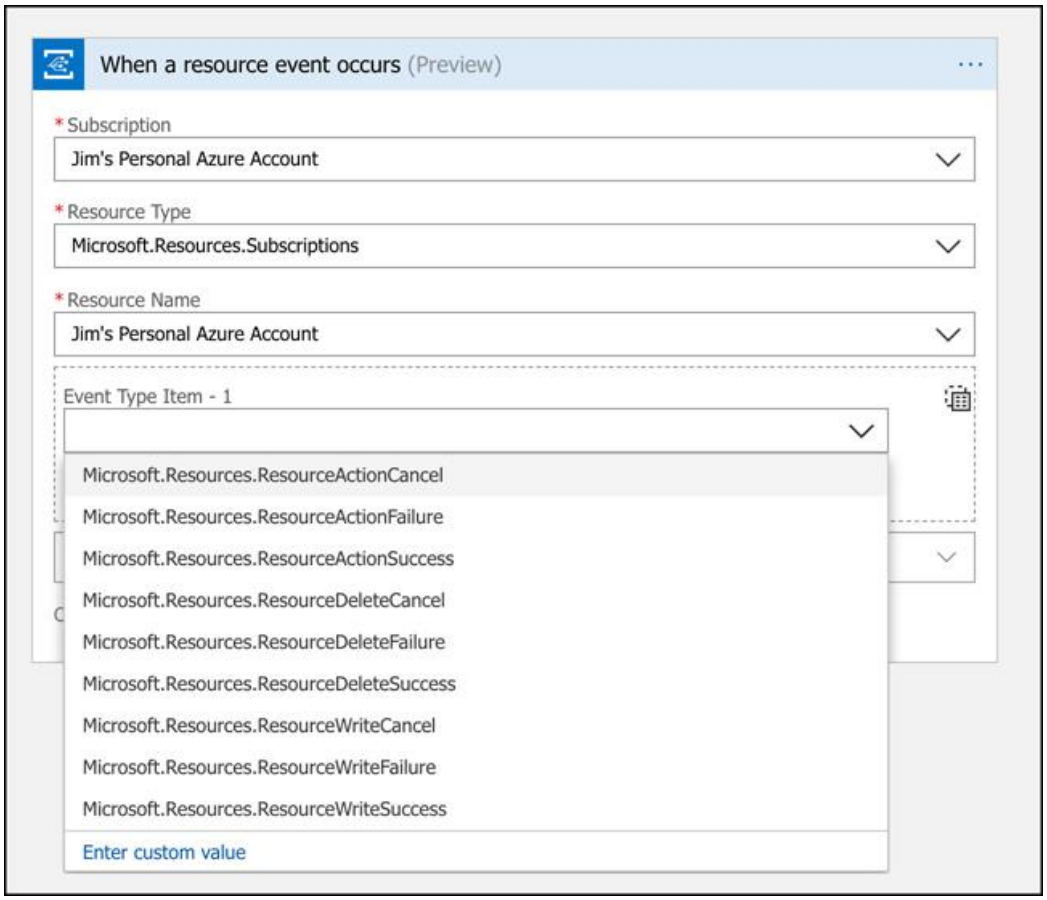


Figura 2-95 Eventos para una suscripción de Azure

Más información **Eventos**

Para obtener detalles completos sobre todos los eventos y su significado, consulte: *https://docs.microsoft.com/azure/event-grid/event-schema* .

Cuando se produce un evento, puede realizar una acción contra un recurso de Azure mediante el conector del Administrador de recursos de Azure en una aplicación lógica. También puede ejecutar un script que interactúa con el recurso de Azure para hacer algo como etiquetar un recurso o configurarlo de una manera específica para su organización.

El principal beneficio de utilizar Event Grid de esta manera es el rápido desarrollo de soluciones. También se beneficia de Event Grid que activa sus eventos de manera confiable. Si un evento Event Grid no se activa por algún motivo, Event Grid continuará intentando volver a activar el evento por hasta 24 horas. Event Grid también es extremadamente rentable. Las primeras 100,000 operaciones por mes son gratuitas, y después de ese punto, paga 60 centavos por cada millón de operaciones.

HABILIDAD 2.4: COMPRENDER LAS HERRAMIENTAS DE ADMINISTRACIÓN DE AZURE

Ahora tiene experiencia en el uso de Azure Portal y Azure Resource Manager (ARM). Si bien el uso del portal de Azure es una forma común de interactuar con los servicios de Azure, a veces no es la forma más eficiente, especialmente si está haciendo muchas cosas al mismo tiempo. Para esas situaciones más complejas, Microsoft ofrece cmdlets de PowerShell que puede usar para interactuar con los recursos de Azure, y también ofrece la Interfaz de línea de comandos (CLI) para usuarios multiplataforma.

Más información **Rest API y aplicación de Azure**

Microsoft también ofrece una API REST para interactuar con Azure, pero no cubriremos eso en este libro porque no está cubierto en el examen AZ-900.

Esta sección cubre:

- El portal de Azure
- Azure y PowerShell
- CLI de Azure
- Asesor de Azure

El portal de Azure

El portal de Azure que está en uso hoy es la tercera iteración del portal de Azure, y surgió cuando Microsoft se mudó a ARM. Todo lo que haces en Azure Portal llama a ARM en el back-end.

Consejo de examen

Para el examen AZ-900, probablemente no necesite saber que Azure Portal solo está haciendo llamadas a ARM en el back-end, pero no está de más saberlo. Para el resto de esta sección, sin embargo, cubriremos solo las diferentes partes del portal y cómo navegar y personalizarlo. Esa información está en el examen AZ-900.

La primera vez que abra el portal de Azure, se le pedirá que realice un recorrido por el portal. Si no está completamente familiarizado con el portal, realizar un recorrido lo ayudará a tener una idea de cómo funciona. Si elige no hacerlo y cambia de opinión más adelante, puede hacer clic en el signo de interrogación en la barra de herramientas superior para acceder a la visita guiada en cualquier momento.

La vista predeterminada en el portal es Inicio, como se muestra en la Figura 2-96 . Desde aquí, puede ver iconos para varios servicios de Azure, y si hace clic en uno de esos iconos, le mostrará los recursos de ese tipo que haya creado. El menú del lado izquierdo incluye estos mismos íconos y más.

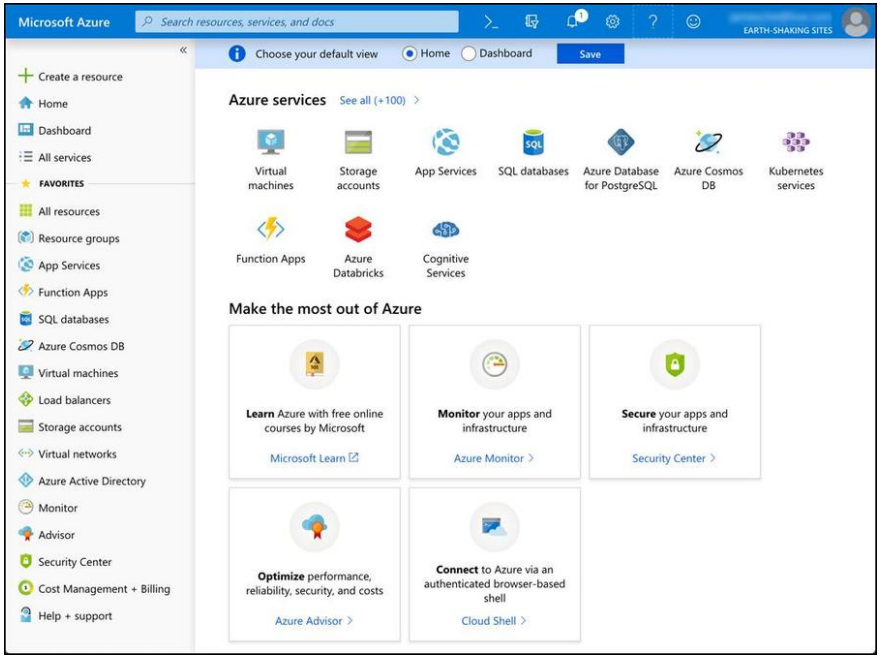


Figura 2-96 La pantalla de inicio en Azure Portal

La parte inferior de la pantalla incluye grandes mosaicos diseñados para ayudarlo a aprender más sobre Azure. Si hace clic en uno de los enlaces provistos en estos mosaicos, se abrirá una nueva pestaña en su navegador para que no pierda su lugar en el portal.

En la parte superior de la pantalla, puede elegir su vista predeterminada para el portal. Puede seleccionar entre Inicio y Panel de control. El Panel de control es una pantalla totalmente personalizable que veremos más adelante. Una vez que haya elegido, haga clic en **Guardar** y el portal siempre se abrirá en la pantalla que elija. Sin embargo, siempre puede acceder a la pantalla de Inicio o al Panel haciendo clic en los enlaces relevantes en el menú en el lado izquierdo del portal de Azure.

A lo largo de la barra de color superior, encontrará una barra de búsqueda donde puede buscar servicios de Azure, documentos o sus recursos de Azure. A la derecha del cuadro de búsqueda hay un botón que iniciará Azure Cloud Shell. Cloud Shell es un shell de comandos basado en la web donde puede interactuar con Azure desde la línea de comandos. Puede crear recursos de Azure y más. Mientras lee la documentación de Azure, es posible que vea un botón Probar y esos botones usan Cloud Shell para ayudarlo a probar diferentes servicios y características.

A la derecha del botón Cloud Shell hay un botón de filtro que le permite configurar el portal para que solo muestre recursos en una determinada suscripción de Azure o Azure Active Directory. A la derecha de eso está el botón de Notificación. Aquí es donde verá las notificaciones de Azure relacionadas con sus servicios y suscripción. En la Figura 2-96 , puede ver el número 1 en el botón. Eso indica que tiene una notificación no leída.

A la derecha del botón de notificaciones está el botón Configuración. Al hacer clic en eso, aparece un panel donde puede modificar la configuración del portal como se muestra en la Figura 9-97.

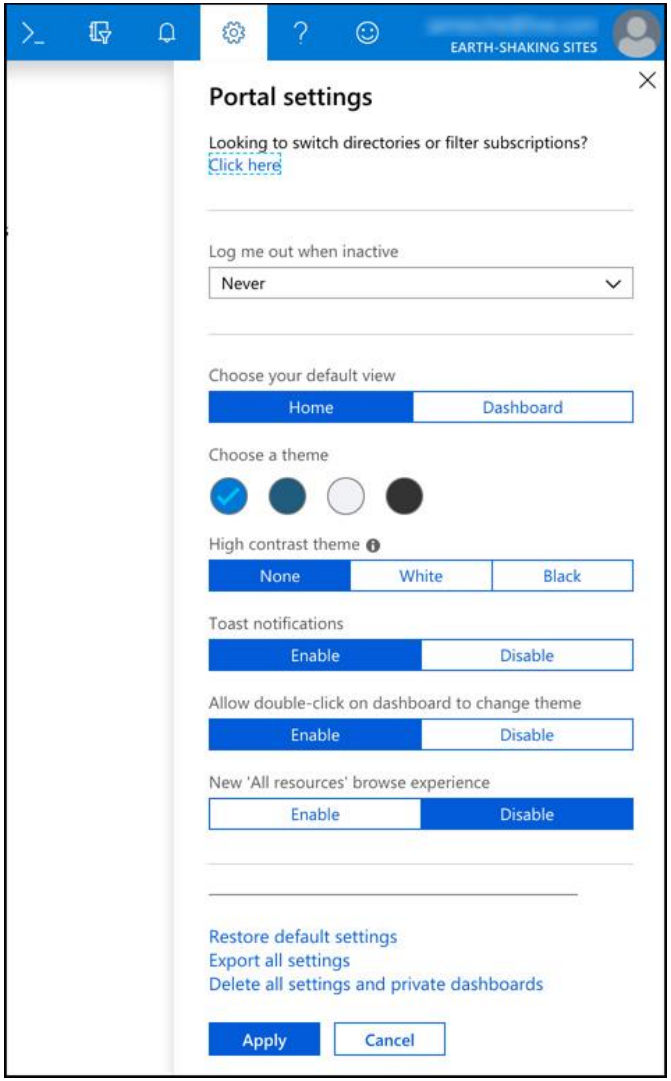


Figura 2-97 Configuración del portal

Desde Configuración, puede cambiar su vista predeterminada, puede alterar la combinación de colores del portal, puede deshabilitar las notificaciones de tostadas o notificaciones emergentes que Microsoft puede mostrar de vez en cuando. Otras configuraciones que aparecen aquí pueden cambiar a medida que Microsoft agrega nuevas funciones. Por ejemplo, en la Figura 2-97 , puede ver cómo, si lo desea, puede cambiar el portal a la nueva experiencia de exploración para sus recursos.

Si hace clic en su nombre en la esquina superior derecha (que se muestra en la Figura 2-96), puede cerrar sesión o cambiar a otras cuentas de Azure. También puede cambiar Azure Active Directory para acceder a recursos en otro directorio. Esto es útil si su empresa tiene un directorio corporativo y usted también tiene un directorio personal.

El menú en el lado izquierdo del portal contiene una lista predeterminada de recursos de Azure. Al hacer clic en uno de ellos, se mostrarán todos los recursos de ese tipo. Si no encuentra un servicio en esa lista que le gustaría agregar a la lista, haga clic en **Todos los servicios** , busque el servicio que desea agregar a la lista y haga clic en la estrella a la derecha del servicio para marcar como favorito, como se muestra en la Figura 2-98 .

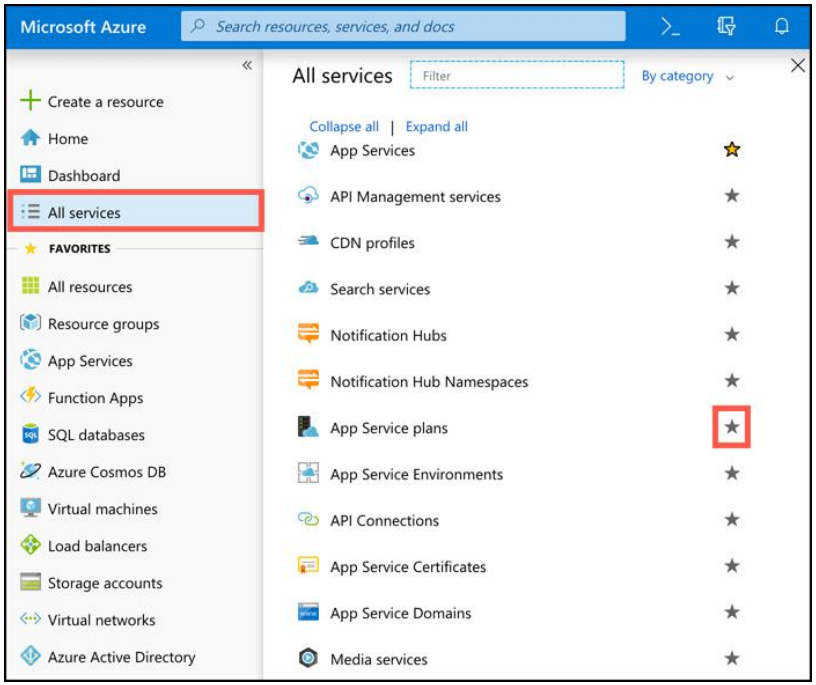


Figura 2-98 Marcado de un servicio favorito

Nota **Mover elementos del menú**

Puede reordenar elementos en el menú. Haga clic y mantenga presionado un elemento y arrástrelo a una nueva ubicación en el menú.

En la Figura 2-99 , hicimos clic en **Planes del Servicio de aplicaciones** en el menú para ver todos los planes del Servicio de aplicaciones. Desde esta lista, puede hacer clic en un recurso para ver ese recurso. También puede hacer clic en el encabezado de una columna para ordenar por esa columna, suponiendo que tenga más de un recurso de ese tipo. Haga clic en **Editar columnas** para editar las columnas que se muestran aquí. Para crear un nuevo recurso de este tipo, haga clic en **Agregar** . Finalmente, puede hacer clic en los tres puntos en el extremo derecho del recurso para eliminar el recurso.

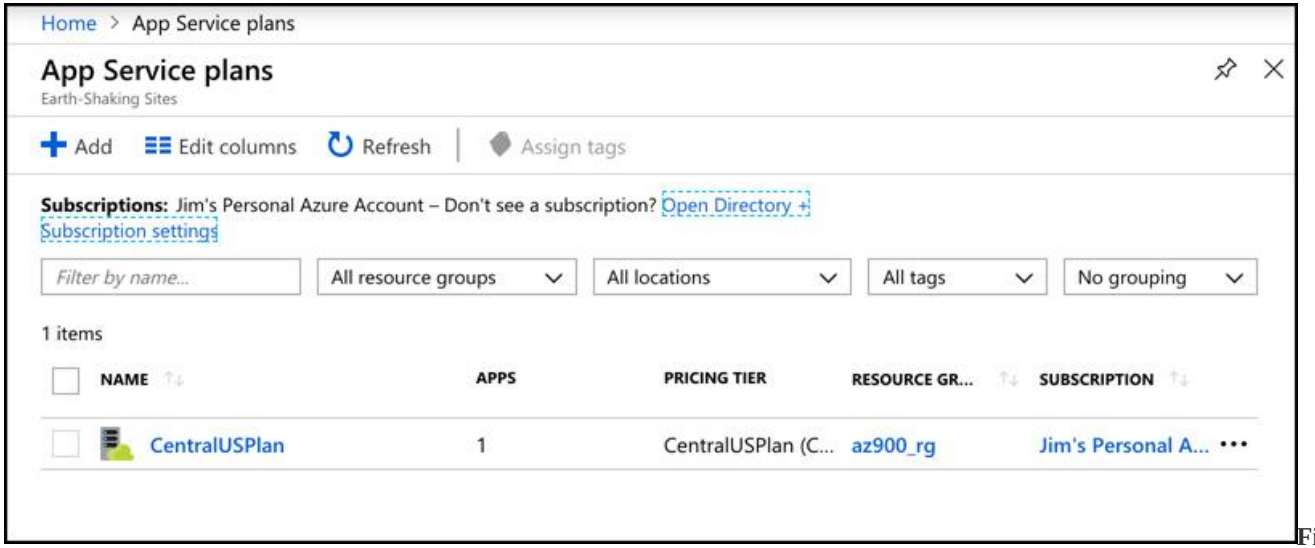


Figura 2-99 Ver una lista de recursos

Cuando hace clic en un recurso en particular, se abrirá ese recurso en el portal. En el lado izquierdo habrá un menú específico para el tipo de recurso que abrió. En la ventana principal, verá diferentes elementos según el tipo de recurso que está viendo. Estas áreas de ventana en el portal a menudo se denominan cuchillas.

En la Figura 2-100 , verá una aplicación web del Servicio de aplicaciones en el portal. La hoja Descripción general es una hoja común a la mayoría de los recursos de Azure, pero la información que aparece allí diferirá según el recurso. En una aplicación web, puede ver

el grupo de recursos en el que se encuentra, el estado, la región y más. También tenemos varios mosaicos relacionados con aplicaciones web, como el mosaico Http 5xx y el mosaico de entrada de datos. En la esquina superior derecha de estos mosaicos hay un botón de pin. Si hace clic en ese marcador, agregará ese mosaico al panel del portal.

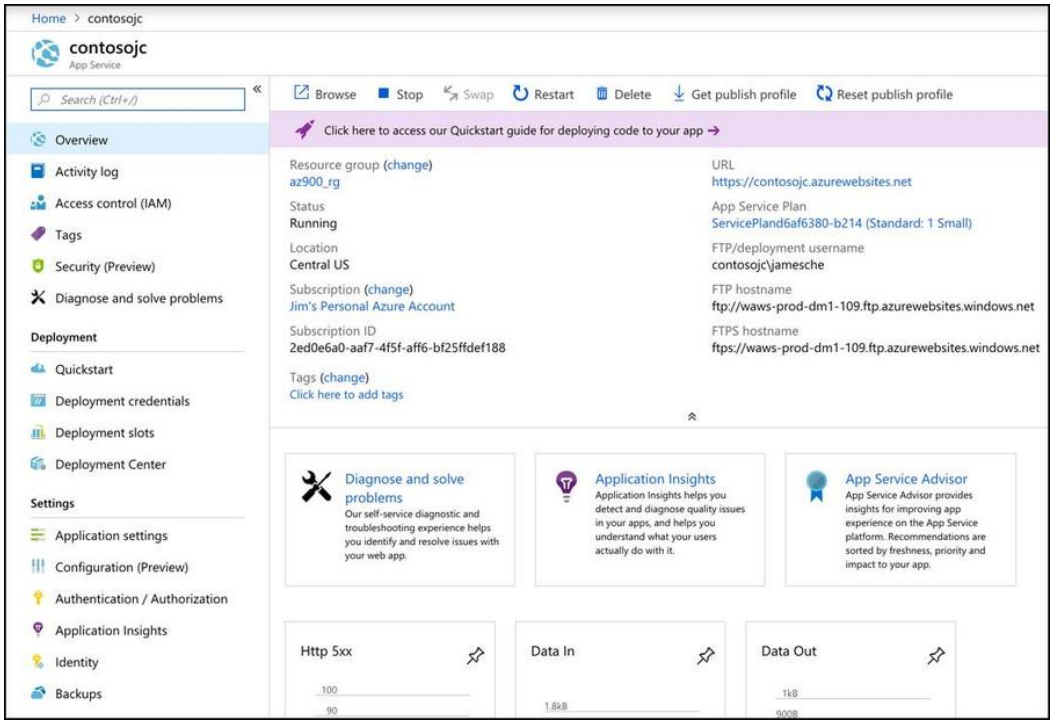


Figura 2-100 Visualización de una aplicación web en el portal

En la parte superior de la hoja para la aplicación web hay varios botones para interactuar con el recurso. Para una aplicación web, tiene un botón Examinar que abrirá la aplicación en un navegador, un botón Detener para detener la aplicación web, un botón Cambiar para intercambiar ranuras de implementación, etc. Cada tipo de recurso tendrá diferentes botones disponibles para que pueda interactuar fácilmente con el recurso desde la hoja Descripción general.

Si hace clic en un elemento en el menú de la izquierda, el contenido de la hoja Descripción general se reemplaza con el nuevo elemento seleccionado. En la Figura 2-101 , hemos hecho clic en **Diagnosticar y resolver problemas** , que reemplaza la hoja Descripción general con nuevo contenido de la hoja Diagnóstico y solución de problemas.

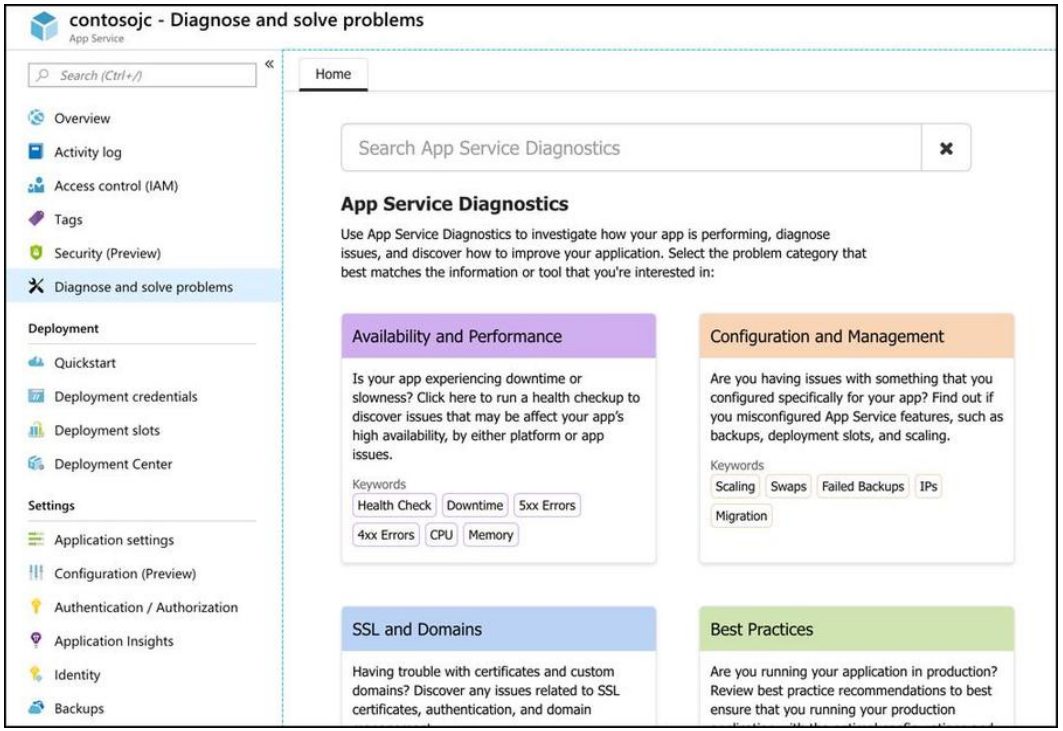


Figura 2-101 Una nueva cuchilla

A medida que use el portal, encontrará que hay inconsistencia entre los diferentes servicios. Cada equipo en Microsoft tiene su propio sub-equipo de desarrollo de portal, y tienden a diseñar interfaces de portal que tengan sentido para su propio equipo. Por esa razón, es posible que vea botones en la parte superior en algunas hojas y botones en la parte inferior en otras hojas.

Puede personalizar su experiencia de portal utilizando el panel de control. Si hace clic en Panel desde la pantalla de inicio del portal, verá su panel predeterminado. Mientras administra sus recursos, haga clic en los pines (como se muestra en la Figura 2-100) para fijar

los mosaicos en su tablero. Luego puede mover estos mosaicos y personalizarlos de otras maneras para crear una vista que sea única para sus necesidades.

Para personalizar su tablero, haga clic en **Tablero** en el menú para mostrar el tablero y luego haga clic en **Editar** como se muestra en la Figura 2-102 .

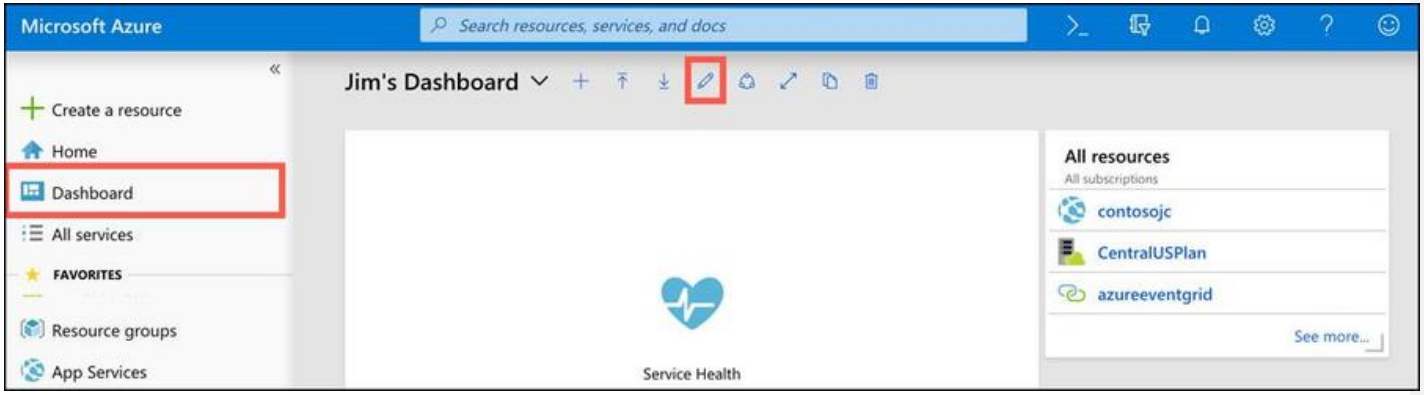


Figura 2-102 Edición de un tablero de instrumentos

Desde la pantalla de personalización que se muestra en la Figura 2-103 , puede cambiar el nombre de su tablero haciendo clic dentro del nombre actual y cambiándolo a un nuevo nombre. Puede agregar mosaicos al tablero eligiendo uno de los cientos de mosaicos disponibles en la Galería de mosaicos en el lado izquierdo del portal, y puede buscar y filtrar la lista si es necesario. Si pasa el cursor sobre un mosaico existente, verá un botón Eliminar y un botón de menú representado por tres puntos. Haga clic en el botón **Eliminar** para eliminar el mosaico del tablero. Haga clic en el botón de menú para acceder a un menú contextual donde puede cambiar el tamaño del mosaico.

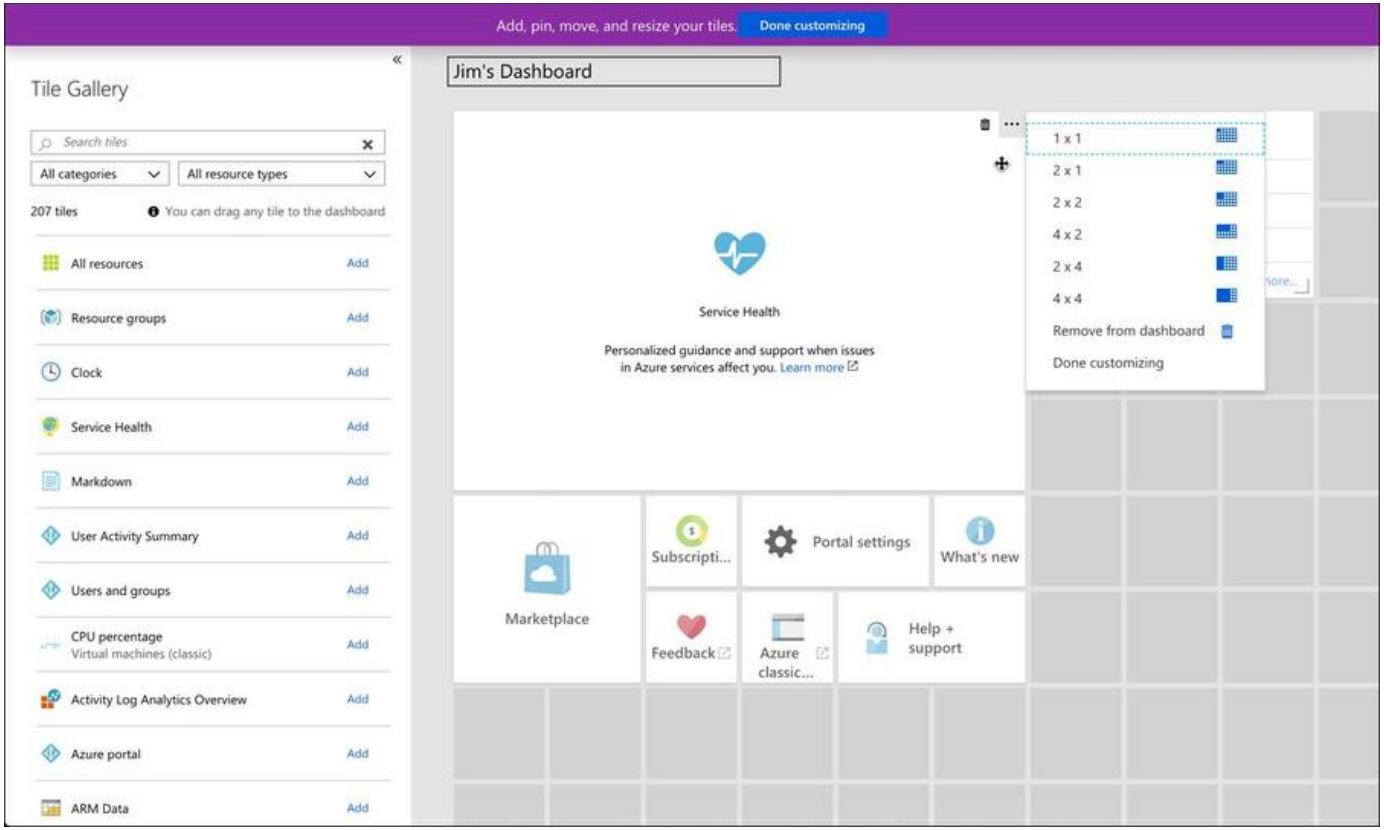


Figura 2-103 Personalizando un tablero

Cuando esté satisfecho con su panel de control, haga clic en **Finalizar personalización** para cerrar la pantalla de personalización.

Puede crear nuevos paneles para fines específicos haciendo clic en el signo más (que se muestra en la Figura 2-102) al lado del nombre del panel. Esto lo lleva a una pantalla de personalización para su nuevo tablero, como el que se muestra en la Figura 2-103 .

En la Figura 2-104 , hemos creado un tablero específico para aplicaciones web. Puede cambiar fácilmente entre este tablero y el tablero predeterminado haciendo clic en la flecha hacia abajo junto al nombre del tablero.

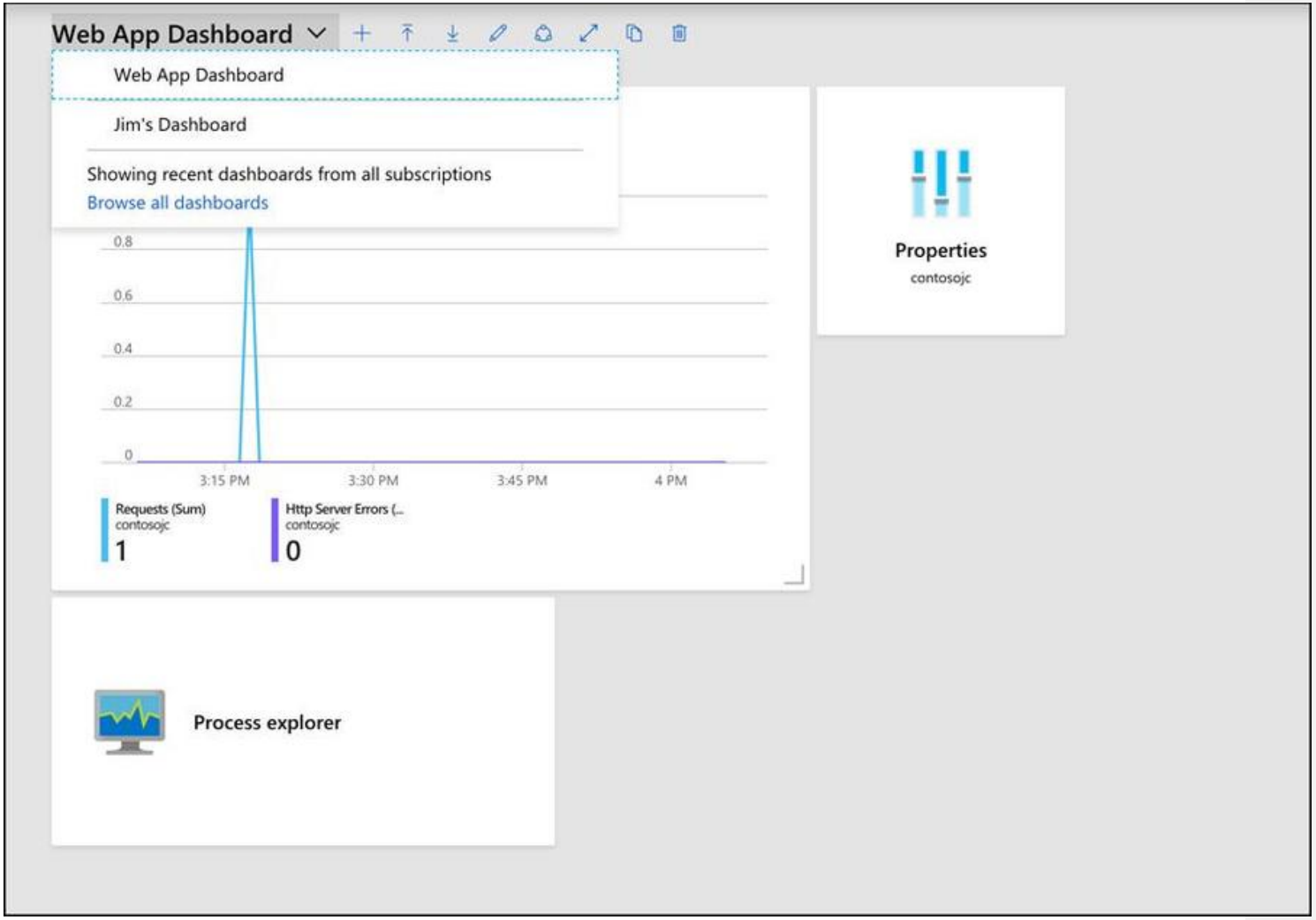


Figura 2-104 Cambio entre paneles

Azure y PowerShell

Si es un usuario de PowerShell, puede aprovechar ese conocimiento para administrar sus recursos de Azure con el módulo Azure PowerShell Az. Este módulo ofrece soporte multiplataforma, por lo que si usa Windows, Linux o macOS, puede usar el módulo PowerShell Az.

Más información **Azurerm And Az**

El módulo PowerShell Az es relativamente nuevo. Antes de eso, todos los comandos de PowerShell usaban el módulo AzureRm. Los comandos que usa con ambos son idénticos. La única diferencia es el nombre del módulo.

Más información **INSTALE POWERSHELL EN LINUX O MACOS**

Si está ejecutando Linux, puede encontrar detalles sobre la instalación de PowerShell en *https://docs.microsoft.com/powershell/scripting/install/installing-powershell-core-on-linux?view=powershell-6* . Los usuarios de MacOS pueden encontrar los pasos en *https://docs.microsoft.com/powershell/scripting/install/installing-powershell-core-on-macos?view=powershell-6* .

 ***Consejo de examen***

El módulo PowerShell Az utiliza la biblioteca .NET Standard para la funcionalidad, lo que significa que se ejecutará con PowerShell versión 5.xo 6.x. PowerShell 6.x es multiplataforma y puede ejecutarse en Windows, Linux o macOS.

Si está ejecutando Windows 7 o posterior y tiene PowerShell 5.x, también necesitará instalar .NET Framework 4.7.2.

Antes de poder usar el módulo PowerShell Az, deberá instalarlo. Para hacer eso, primero debe ejecutar PowerShell elevado. En Windows, eso significa ejecutarlo como administrador. En Linux y macOS, deberá ejecutarlo con privilegios de superusuario con sudo.

Para instalar el módulo, ejecute el siguiente comando.

Haga clic aquí para ver la imagen del código

```
Install-Module -Name Az -AllowClobber
```

Cuando instala un nuevo módulo de PowerShell, PowerShell comprueba todos los módulos existentes para ver si tienen algún nombre de comando que sea igual al nombre de comando en el módulo que está instalando. Si lo hacen, la instalación del nuevo módulo falla. Al especificar -AllowClobber, le está diciendo a PowerShell que está bien que el módulo Az tenga prioridad sobre cualquier comando que también exista en otro módulo.

Si no puede ejecutar PowerShell con privilegios elevados, puede instalar el módulo para su ID de usuario solo con el siguiente comando.

Haga clic aquí para ver la imagen del código

```
Install-Module -Name Az -AllowClobber -Scope CurrentUser
```

Una vez que haya instalado el módulo, debe iniciar sesión con su cuenta de Azure. Para hacer eso, ejecuta el siguiente comando.

```
Connect-AzAccount
```

Este comando mostrará un token en la ventana de PowerShell. Deberá navegar hasta ***https://microsoft.com/devicelogin*** e ingresar el código para autenticar su sesión de PowerShell. Si cierra PowerShell, deberá ejecutar el comando nuevamente en su próxima sesión.

Más información **Credenciales persistentes**

Es posible configurar PowerShell para conservar sus credenciales. Para obtener más información sobre cómo hacerlo, consulte: *https://docs.microsoft.com/powershell/azure/context-persistence* .

Si tiene más de una suscripción de Azure, querrá configurar la suscripción activa para que los comandos que ingrese afecten la suscripción deseada. Puede hacerlo utilizando el siguiente comando.

Haga clic aquí para ver la imagen del código

```
Set-AzContext -Subscription "suscripción"
```

Reemplace la **suscripción** con el nombre o ID de suscripción de su suscripción de Azure que desea usar con el módulo Az.

Todos los comandos del módulo Az tendrán una sintaxis común que comienza con un verbo y un objeto. Los verbos son cosas como **Nuevo** , **Obtener** , **Mover** o **Eliminar** . El objeto es lo que desea que impacte el verbo. Por ejemplo, el siguiente comando creará un grupo de recursos llamado MyRG en la región centro sur de los EE. UU.

Haga clic aquí para ver la imagen del código

```
New-AzResourceGroup -Name MyRG -Location "South Central US"
```

Si esto tiene éxito, verás un mensaje que te lo hará saber. Si falla, verá un error. Para eliminar el grupo de recursos, ejecute el siguiente comando.

Haga clic aquí para ver la imagen del código

```
Remove-AzResourceGroup -Name MyRG
```

Cuando ingrese este comando, se le pedirá que confirme si desea eliminar el grupo de recursos. Escriba a **y** el grupo de recursos se eliminará como se muestra en la Figura 2-105 .

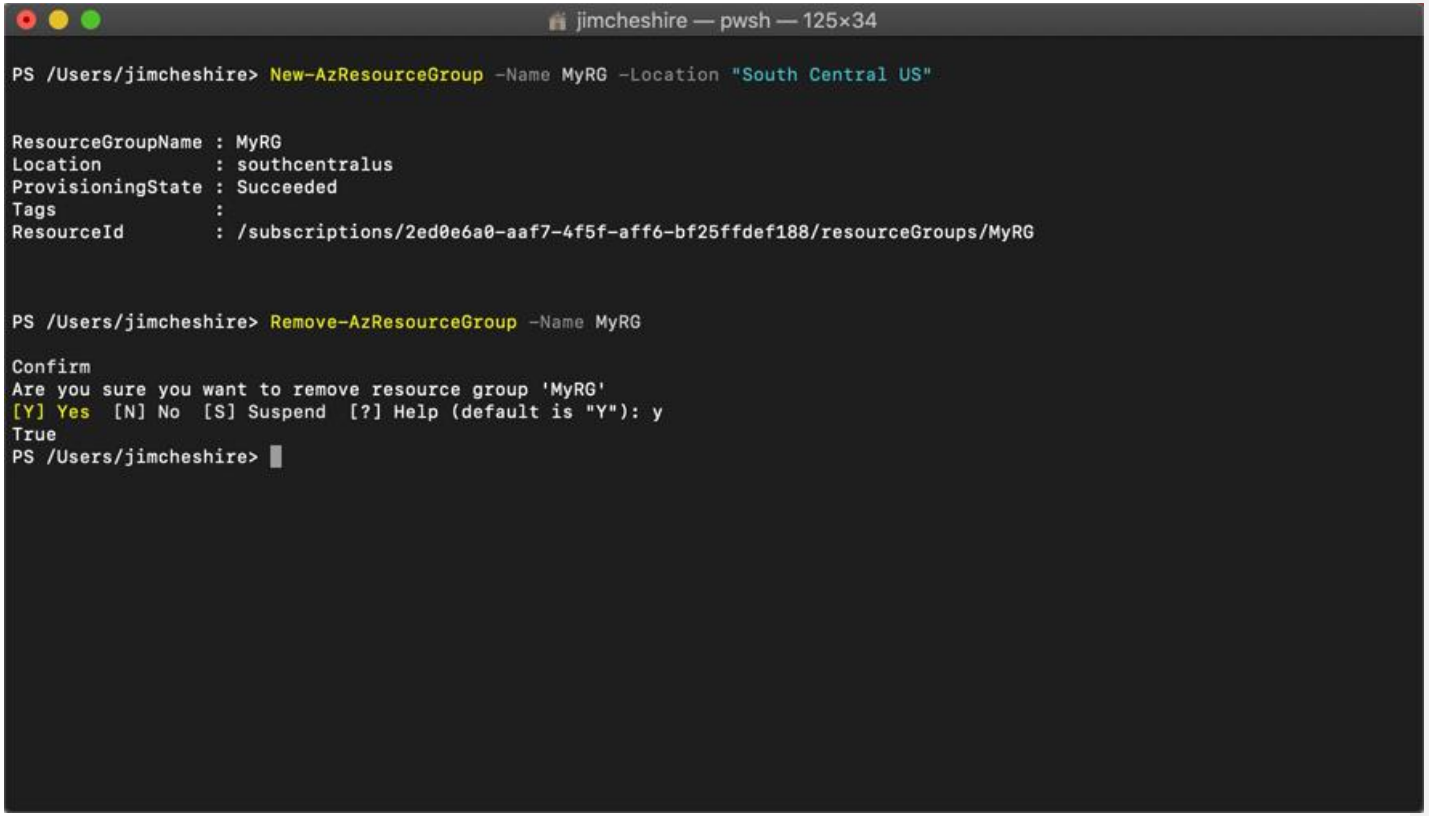


Figura 2-105 Crear y eliminar un grupo de recursos con PowerShell Az

En muchas situaciones, incluirá comandos de PowerShell en un script para que pueda realizar varias operaciones a la vez. En ese caso, no podrá confirmar un comando escribiendo **y** , por lo que puede usar el parámetro **-Force** para omitir la solicitud. Por ejemplo, puede eliminar el grupo de recursos con el siguiente comando y no se le solicitará.

Haga clic aquí para ver la imagen del código

```
Remove-AzResourceGroup -Name MyRG -Force
```

Puede encontrar todos los comandos disponibles con el módulo PowerShell Az navegando a: *https://docs.microsoft.com/powershell/module/?view=azps-1.3.0* .

CLI de Azure

Como señalé anteriormente, uno de los principales beneficios de PowerShell es la capacidad de guiar las interacciones con los recursos de Azure. Sin embargo, si desea realizar un script con PowerShell, necesitará a alguien que conozca el desarrollo de PowerShell. Si no tiene a nadie que pueda hacer eso, la interfaz de línea de comandos de Azure (CLI de Azure) es una excelente opción. La CLI de Azure se puede programar mediante scripts de shell en varios idiomas, como Python, Ruby, etc.

Al igual que el módulo PowerShell Az, la CLI de Azure es multiplataforma y funciona en Windows, Linux y macOS siempre que use la versión 2.0. Los pasos de instalación son diferentes según su plataforma. Puede encontrar los pasos para todos los sistemas operativos en: *https://docs.microsoft.com/cli/azure/install-azure-cli?view=azure-cli-latest* .

Una vez que instale la CLI de Azure, deberá iniciar sesión en su cuenta de Azure. Para hacer eso, ejecuta el siguiente comando.

```
inicio de sesión az
```

Cuando ejecuta este comando, la CLI abrirá un navegador automáticamente para que pueda iniciar sesión. Una vez que inicie sesión, si tiene varias suscripciones de Azure, puede establecer la predeterminada ingresando el siguiente comando.

Haga clic aquí para ver la imagen del código

```
conjunto de cuentas az - suscripción "suscripción"
```

Reemplace la **suscripción** con el nombre o ID de suscripción que desea usar.

Para encontrar una lista de comandos que puede ejecutar con la CLI, escriba **az** y presione Entrar. Verá una lista de todos los comandos que puede ejecutar. Puede encontrar ayuda detallada sobre cualquier comando ingresando el comando y agregando un parámetro **--help** . La Figura 2-106 muestra la ayuda para un **recurso az** .

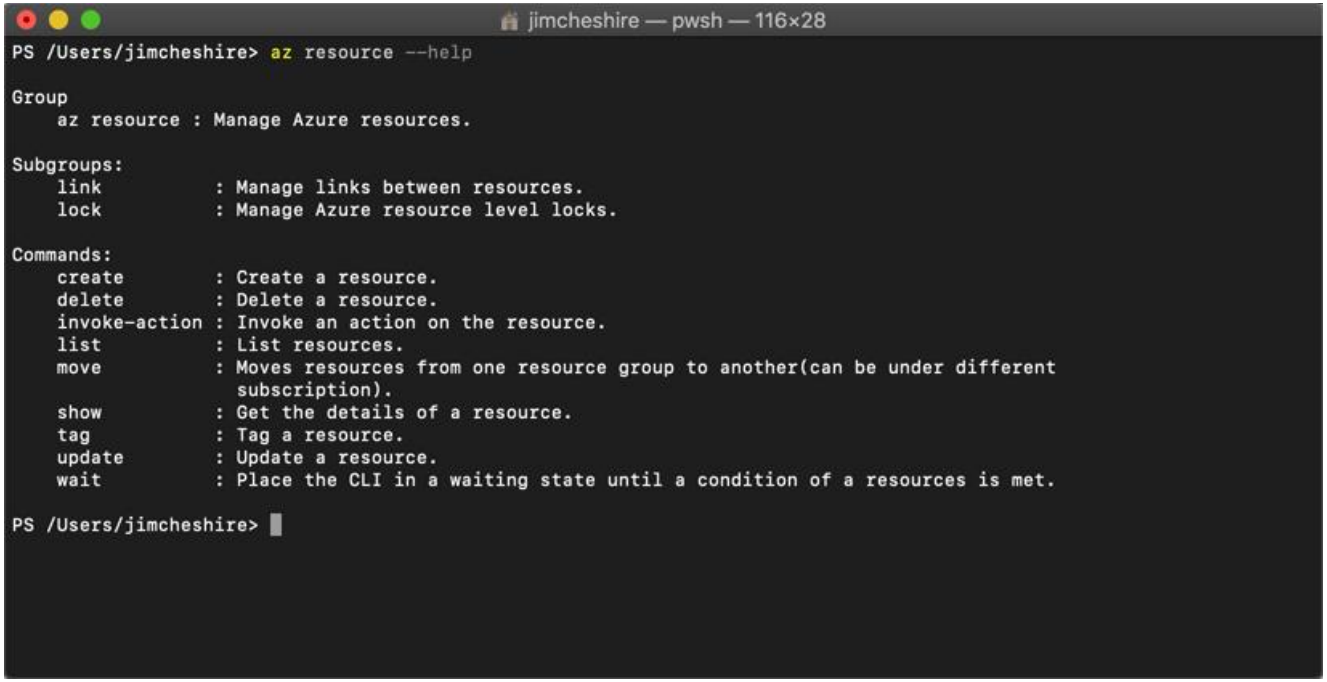


Figura 2-106 Ayuda de la CLI de Azure

Puede llevar esto un paso más allá si no está seguro de lo que hacen los comandos. Puede, por ejemplo, ejecutar el siguiente comando para obtener ayuda sobre la sintaxis de **az resource create** .

```
az resource create --help
```

Esto le proporciona ayuda y comandos de ejemplo para comprender la sintaxis.

Consejo de examen

Al igual que PowerShell, la mayoría de los comandos en la CLI de Azure tienen un parámetro --force que puede incluir para que no se muestren mensajes. Al crear scripts de PowerShell o la CLI, debe incluir este parámetro o su script no funcionará. Tenga cuidado con los ejemplos en el examen AZ-900 que evalúan este tipo de conocimiento.

Una forma aún más fácil de aprender la CLI es cambiar al modo interactivo. Esto le proporciona autocompletar, el alcance de los comandos y más. Para cambiar al modo interactivo, ingrese **az interactive** en el símbolo del sistema. La CLI instalará una extensión para agregar esta funcionalidad. La Figura 2-107 muestra la CLI de Azure con el modo interactivo activo. Usted ha escrito **que** en el símbolo del sistema, y es que muestra el resto de la orden en el texto atenuado. Puede presionar la tecla de flecha hacia la derecha para ingresar el texto atenuado de una sola vez.

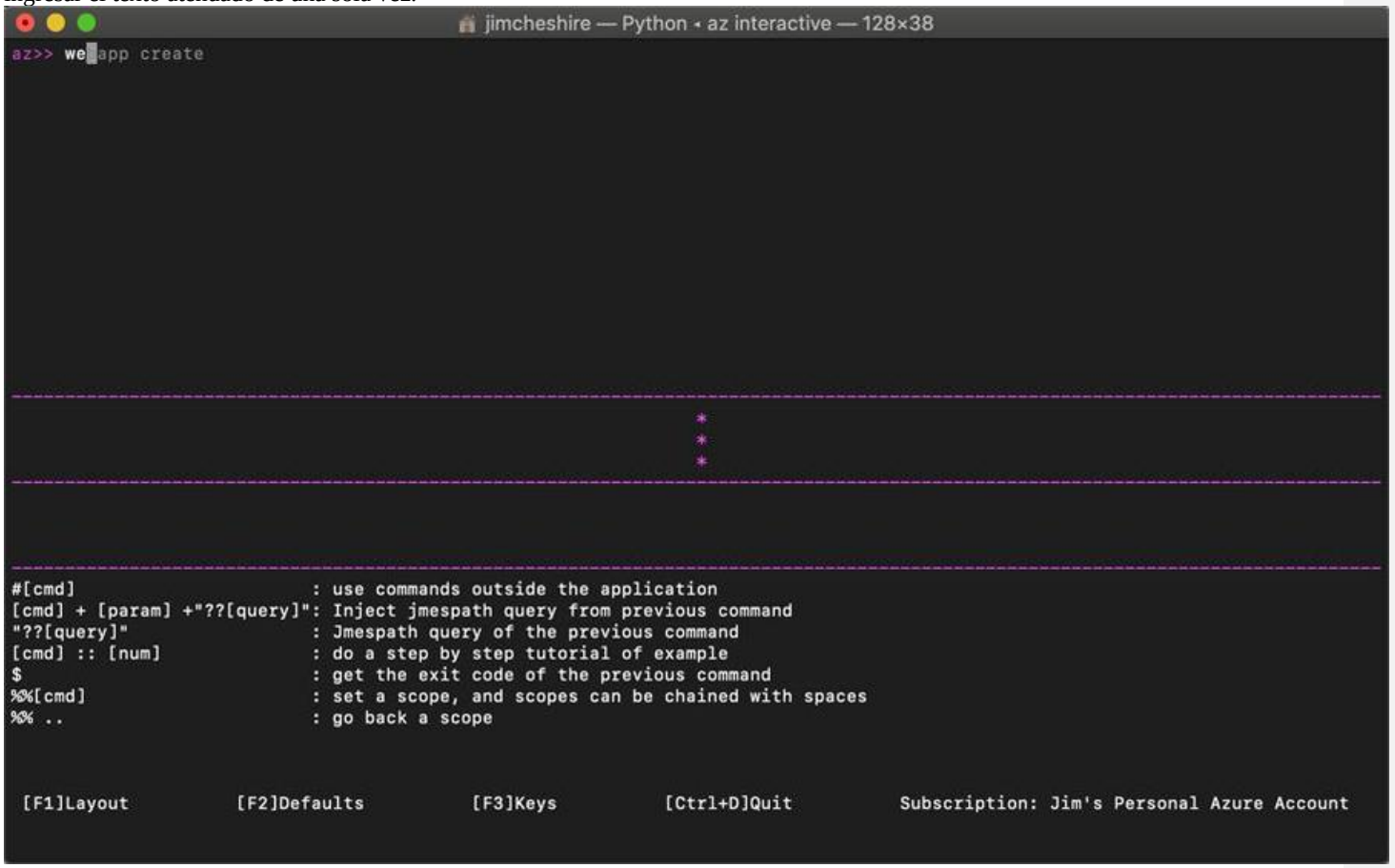


Figura 2-107 Modo interactivo de CLI

Puede instalar extensiones adicionales para una funcionalidad adicional. Debido a que la CLI usa una arquitectura de extensión, los equipos de Azure pueden brindar soporte para nuevas funcionalidades sin tener que esperar una nueva versión de la CLI. Puede encontrar una lista de todas las extensiones disponibles que Microsoft proporciona ejecutando el siguiente comando.

Haga clic aquí para ver la imagen del código

```
lista de extensiones az disponible - tabla de salida
```

Esto no solo le mostrará las extensiones disponibles, sino que le mostrará si ya tiene la extensión instalada y si hay una actualización que debe instalar. Para instalar una extensión, ejecute el siguiente comando.

Haga clic aquí para ver la imagen del código

```
extensión az agregar --nombre nombre_extensión
```

Reemplace **extension_name** con el nombre de la extensión que desea instalar.

Asesor de Azure

Administrar sus recursos de Azure no solo incluye crear y eliminar recursos. También significa asegurarse de que sus recursos estén configurados correctamente para una alta disponibilidad y eficiencia. Descubrir exactamente cómo hacerlo puede ser una tarea desalentadora. Se han escrito libros completos sobre las mejores prácticas para implementaciones en la nube. Afortunadamente, Azure puede notificarle sobre problemas en su configuración para que pueda evitarlos. Lo hace a través del Asesor de Azure.

Azure Advisor puede ofrecer asesoramiento en el área de alta disponibilidad, seguridad, rendimiento y costo. Si bien la documentación indica que Azure Advisor está disponible solo para máquinas virtuales de Azure, conjuntos de disponibilidad, puertas de enlace de aplicaciones, aplicaciones de servicio de aplicaciones, SQL Server y Azure Redis Cache, muchos servicios adicionales se incorporan a Azure Advisor y obtendrá recomendaciones para casi todos sus servicios de Azure.

Para acceder a Azure Advisor, inicie sesión en Azure Portal y haga clic en Advisor en el menú de la izquierda. La Figura 2-108 muestra Azure Advisor con 1 recomendación de bajo impacto para alta disponibilidad y 2 recomendaciones de alto impacto para seguridad.

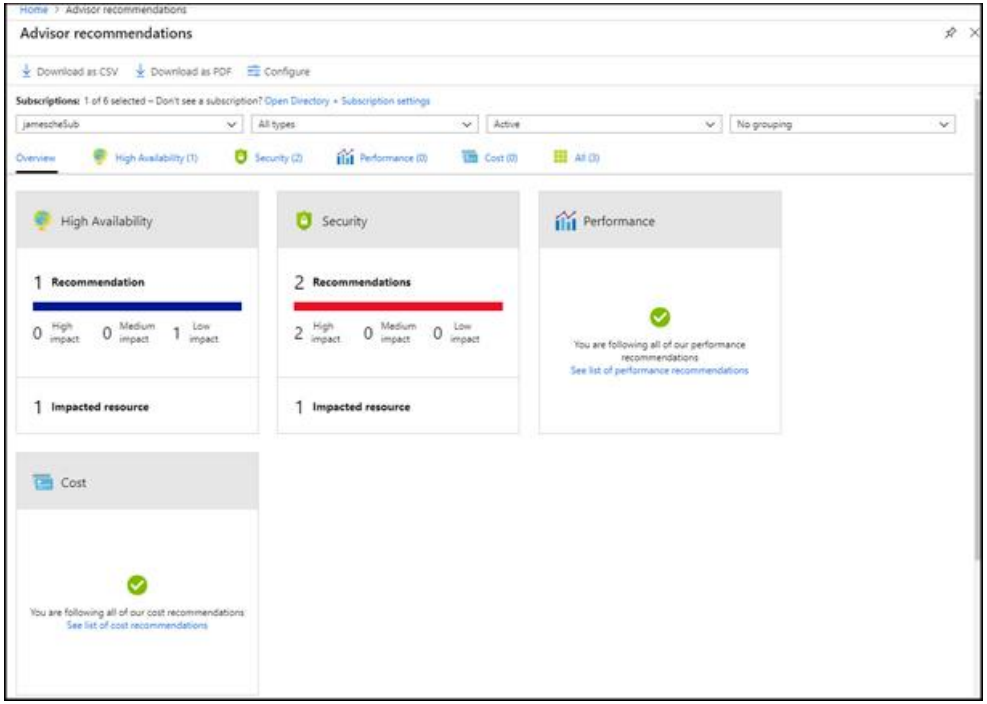


Figura 2-108 Asesor de Azure

Para revisar los detalles de una recomendación, haga clic en el mosaico. En la Figura 2-109 , hemos hecho clic en el mosaico de alta disponibilidad y puede ver una recomendación para crear una alerta de mantenimiento del servicio de Azure.

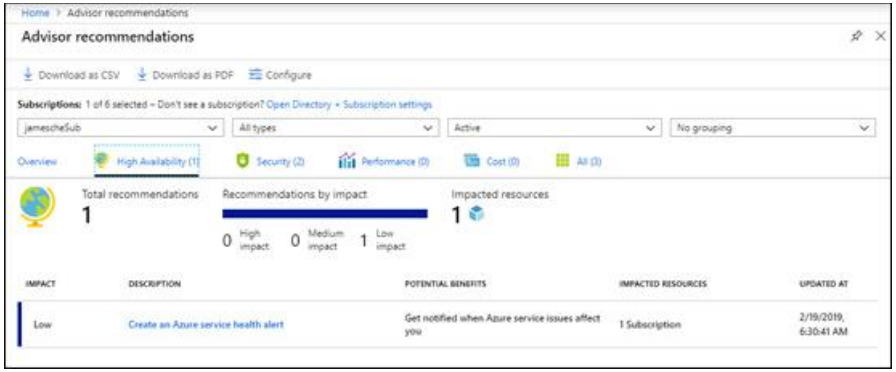


Figura 2-109 Recomendaciones del asesor

No tiene que hacer lo que recomienda Azure Advisor. Si hace clic en la descripción, puede decidir posponer o descartar la alerta como se muestra en la Figura 2-110 . Si elige posponer la alerta, tiene la opción de recibir un recordatorio en 1 día, 1 semana, 1 mes o 3 meses.

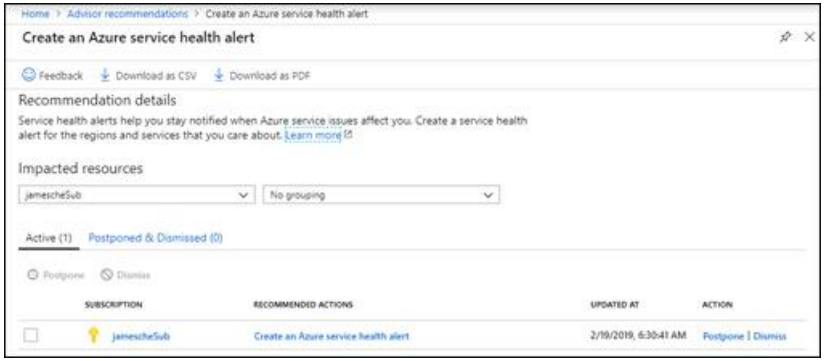


Figura 2-110 Actuando sobre una recomendación

Si tiene una gran cantidad de recomendaciones, o si no es la persona adecuada para tomar medidas sobre las recomendaciones, puede descargar las recomendaciones de Azure Advisor como un archivo de valores separados por comas o como PDF. Haga clic en **Descargar como CSV** o **Descargar como PDF** , como se muestra en la Figura 2-108 . También puede descargar un archivo con recomendaciones específicas haciendo clic en el botón de descarga apropiado mientras revisa los detalles como se muestra en la Figura 2-109 y la Figura 2-110 .

EXPERIMENTO MENTAL

Ahora que ha aprendido sobre los servicios principales de Azure, apliquemos ese conocimiento. Puede encontrar las respuestas a este experimento mental en la siguiente sección.

ContosoPharm se ha puesto en contacto con usted para obtener ayuda en la configuración de algunas máquinas virtuales de Azure para alojar sus servicios de Azure. Quieren asegurarse de que sus servicios experimenten una alta disponibilidad y estén protegidos contra los desastres que puedan ocurrir en un centro de datos en un determinadoRegión azul. Además de eso, quieren asegurarse de que un corte de energía en un centro de datos en particular no afecte su servicio en esa región. También quieren asegurarse de que su aplicación no se caiga en caso de que una VM deba reiniciarse por algún motivo.

Las máquinas virtuales de ContosoPharm también usarán configuraciones específicas para redes virtuales, y quieren asegurarse de que puedan implementar fácilmente estos recursos en nuevas regiones de Azure, si es necesario, en un momento posterior. Para ellos es fundamental que las implementaciones posteriores tengan exactamente la misma configuración que todas las demás implementaciones porque cualquier diferencia puede causar incompatibilidades de aplicación.

Algunas de las máquinas virtuales que están implementando están bajo el centro de costos para investigación y desarrollo. Otras máquinas virtuales se utilizarán para marketing para rastrear pedidos farmacéuticos. Para los informes de costos, es importante que puedan informar sobre los gastos de Azure para cada centro de costos por separado.

Durante algunos períodos de tiempo, ContosoPharm ha notado que sus aplicaciones pueden causar picos extremos de CPU. Quieren un sistema que tenga en cuenta eso y posiblemente agregue máquinas virtuales adicionales durante estos momentos pico, pero quieren controlar los costos y no quieren pagar estas máquinas virtuales adicionales cuando no están experimentando un aumento en el uso. Cualquier consejo que pueda ofrecer para eso sería un bono.

La aplicación de marketing utiliza un sitio web para los pedidos, y mantener un inventario preciso en tiempo real es fundamental. ContosoPharm tiene personal de ventas en todo el mundo, y desean implementar un sistema en el que un usuario que accede al sitio en una región geográfica particular se dirija a un sitio web que se ejecuta en un centro de datos de Azure cercano.

Además de eso, quieren asegurarse de mantener una copia de cada factura de pedido. Estas facturas se cargan en el sitio web en formato PDF y desean mantenerlas en la nube. No necesitan poder ejecutar ningún tipo de informe sobre estas facturas, pero las necesitan en caso de que los reguladores las soliciten en algún momento en el futuro.

Todos los productos químicos y farmacéuticos de ContosoPharm se mantienen en una gran instalación de investigación. Les gustaría integrar una base de datos en esa instalación con sus servicios de Azure, y necesitan que esa conexión sea encriptada y segura. También necesitan poder rastrear cuidadosamente la temperatura de esa instalación donde se almacena la base de datos local. Han agregado dispositivos de termostato habilitados para Internet en el edificio, pero actualmente no tienen forma de asegurarse de que puedan ser notificados si algo está fuera de lo normal con la temperatura.

Debido a la sensibilidad del inventario local, les gustaría almacenar toda la telemetría de todos los dispositivos que controlan la temperatura. Actualmente tienen más de 500,000 sensores que registran la temperatura cada dos segundos. El CTO de la compañía le ha dicho que cree que deberían poder tomar todas esas lecturas históricas y establecer algún tipo de sistema que pueda predecir cuándo

está ocurriendo una anomalía antes de que se convierta en un problema y ponga sus activos en riesgo. Le gustaría una recomendación sobre cómo podemos implementar eso.

El último requisito que tienen es la capacidad de saber fácilmente si tienen alguna oportunidad de reducir los costos en función del uso de recursos de Azure a lo largo del tiempo. Han invertido una gran cantidad de dinero en la planificación de este sistema, y quieren asegurarse de que se controlen los gastos adicionales siempre que sea posible.

Proporcione una recomendación a ContosoPharm que cumpla con todos sus requisitos. No necesita darles detalles técnicos específicos sobre cómo implementar todo, pero debe señalarlos en la dirección correcta si no tiene detalles.

EXPERIENCIAS DE PENSAMIENTO RESPUESTAS

En esta sección, repasaremos las respuestas al experimento mental.

Para asegurarse de que sus máquinas virtuales estén protegidas contra desastres en un centro de datos dentro de una región particular de Azure, debe recomendar que ContosoPharm use zonas de disponibilidad. Al implementar máquinas virtuales en zonas de disponibilidad, pueden garantizar que las máquinas virtuales se distribuyan en diferentes edificios físicos dentro de la misma región de Azure. Cada edificio tendrá energía, agua, sistema de enfriamiento y red separados.

Para proteger su aplicación cuando se debe reiniciar una VM, deben usar un conjunto de disponibilidad. Un conjunto de disponibilidad les proporcionaría múltiples dominios de fallas y dominios de actualización, de modo que si se debe reiniciar una VM, todavía tendrían una VM operativa en otro dominio de actualización.

Para garantizar implementaciones consistentes ahora y en el futuro, ContosoPharm puede crear una plantilla ARM para su implementación. Al usar una plantilla ARM, pueden asegurarse de que cada implementación de sus recursos será idéntica.

Para separar el seguimiento de facturas para el departamento de I + D y el departamento de marketing, Contoso Pharm puede usar etiquetas de recursos para cada uno de sus recursos. Su factura de Azure se puede filtrar en estas etiquetas para que puedan rastrear los gastos.

Para asegurarse de que siempre tengan suficientes máquinas virtuales para manejar la carga cuando los picos de CPU, deben usar conjuntos de escalado. Luego pueden configurar reglas de escala automática para escalar cuando la carga lo requiera y volver a escalar para controlar los costos.

Para garantizar que el personal de ventas que utiliza el sitio web de marketing se dirija a un centro de datos que esté geográficamente cerca de ellos, ContosoPharm debe usar Azure Traffic Manager con reglas geográficas. Esto asegurará que el tráfico vaya a un centro de datos más cercano al servidor DNS que realizó la solicitud.

Para almacenar sus facturas en la nube, ContosoPharm puede usar Azure Blob Storage. Podrían almacenarlos en una base de datos como blobs binarios, pero como no necesitan ejecutar ningún tipo de informes o consultas en su contra, Azure Blob Storage será más barato.

Para conectar su base de datos local a los recursos de Azure, pueden usar una VPN con VPN Gateway. Esto les permite configurar un túnel cifrado entre sus recursos locales y su red virtual de Azure.

Para monitorear sus dispositivos de termostato locales, ContosoPharm puede usar IoT Hub. Pueden configurar alertas para notificar a alguien cuando las temperaturas están fuera del rango normal. Incluso pueden usar el dispositivo gemelo para configurar etiquetas para que puedan configurar diferentes reglas para diferentes grupos de dispositivos IoT. Debido a que necesitarán agregar más de 500,000 dispositivos, pueden usar el Servicio de aprovisionamiento de dispositivos de IoT Hub para aprovisionar todos esos dispositivos.

Puede aconsejar al CTO que enrute los datos de IoT de IoT Hub a Azure Data Lake Storage. Luego puede usar Azure Databricks para limpiar esos datos y alimentarlos al Servicio de aprendizaje automático de Azure.Si sus desarrolladores pueden desarrollar un modelo de ML que pueda ser entrenado para descubrir anomalías, pueden calificar ese modelo para determinar si pueden predecir de manera confiable un problema antes de que ocurra. Si no tienen a nadie con la experiencia para desarrollar un modelo, es probable que puedan hacer ese trabajo sin programar con Machine Learning Studio. El modelo puede exponerse como un servicio web al que puede llamar otra aplicación.

Finalmente, para asegurarse de que están tomando medidas para reducir los costos tanto como sea posible, puede aconsejarles que utilicen Azure Advisor para tomar medidas sobre cualquier recomendación de costos.

RESUMEN DEL CAPÍTULO

¡Este capítulo cubrió mucho terreno! No solo aprendió algunos de los conceptos básicos de Azure relacionados con las regiones y los grupos de recursos, sino que también aprendió sobre muchos de los servicios principales que Azure proporciona. También aprendió sobre algunos de los temas más candentes de la tecnología actual: IoT, aprendizaje automático y computación sin servidor. Lo resumimos con información sobre cómo puede usar algunas de las herramientas de administración que proporciona Azure.

Aquí hay un resumen de lo que cubre este capítulo.

- Una región de Azure es un área dentro de un límite geográfico específico, y cada región está típicamente a cientos de millas de distancia.
- Una geografía suele ser un país, y cada geografía contiene al menos dos regiones.
- Un centro de datos es un edificio físico dentro de una región, y cada centro de datos tiene su propia energía, suministro de refrigeración, soporte de agua, generadores y red.
- La latencia de ida y vuelta entre dos regiones no debe ser mayor de 2 ms, y esta es la razón por la cual las regiones a veces se definen como un "límite de latencia".
- Los clientes deben implementar recursos de Azure en varias regiones para garantizar la disponibilidad.
- Las zonas de disponibilidad aseguran que sus recursos se implementen en centros de datos separados en una región. Hay al menos tres zonas de disponibilidad en cada región.
- Azure Resource Manager (ARM) es cómo las herramientas de administración de Azure crean y administran los recursos de Azure.
- ARM utiliza proveedores de recursos para crear y administrar recursos.

- Una plantilla ARM le permite garantizar la coherencia de las grandes implementaciones de Azure.
- Los grupos de recursos le permiten separar los recursos de Azure de una manera lógica, y puede etiquetar recursos para una administración más fácil.
- Las máquinas virtuales de Azure son una oferta de IaaS en la que administra el sistema operativo y la configuración.
- Los conjuntos de disponibilidad protegen sus máquinas virtuales con dominios de falla y dominios de actualización. Los dominios de falla protegen su VM de una falla de hardware en un rack de hardware. Está protegido contra reinicios de máquinas virtuales mediante dominios de actualización.
- Los conjuntos de escala le permiten configurar reglas de escala automática para escalar horizontalmente cuando sea necesario.
- Los contenedores le permiten crear una imagen de una aplicación y todo lo necesario para ejecutarla. Luego puede implementar esta imagen en las instancias de Azure Container, Azure Kubernetes Service o Web App for Containers.
- Una red virtual de Azure (VNET) permite que los servicios de Azure se comuniquen entre sí y con Internet.
- Puede agregar una dirección IP pública a una red virtual para la conectividad de Internet entrante. Esto es útil si un sitio web se está ejecutando en su VNET y desea permitir que las personas accedan a él.
- Azure Load Balancer puede distribuir el tráfico de Internet a través de varias máquinas virtuales en su red virtual.
- Azure Application Gateway es un equilibrador de carga adecuado para el tráfico HTTP y es una buena opción para sitios web.
- VPN Gateway le permite configurar túneles VPN seguros en su VNET. Esto se puede usar para conectarse a través de regiones de Azure o incluso a máquinas locales.
- Azure Content Delivery Network almacena recursos en caché para que los usuarios puedan obtener una experiencia más rápida en todo el mundo.
- Azure Traffic Manager es una solución basada en DNS que puede ayudar a equilibrar la carga de las solicitudes web, enviar tráfico a una nueva región en una interrupción o enviar usuarios a una región en particular más cercana a ellos.
- Azure Blob Storage es una buena opción de almacenamiento para datos no estructurados, como archivos binarios.
- Si necesita mover una gran cantidad de datos a Blob Storage, Azure Data Box es una buena opción. Puede recibir discos duros de numerosos tamaños. Agregue sus datos a ellos y envíelos de regreso a Microsoft, donde se agregarán a su cuenta de almacenamiento.
- Azure Queue Storage almacena mensajes de aplicaciones en una cola para que puedan procesarse de forma segura.
- Azure Disk Storage es almacenamiento de disco virtual para máquinas virtuales de Azure. Los discos administrados le permiten eliminar la carga administrativa de los discos.

- Azure Files le permite tener espacio en disco en la nube que puede asignar a una unidad local.
- Azure SQL Database es un sistema de base de datos relacional en la nube que está completamente administrado por Microsoft.
- Azure Cosmos DB es una base de datos NoSQL en la nube para datos no estructurados.
- Azure Marketplace es una fuente de plantillas para crear recursos de Azure. Algunos son proporcionados por Microsoft y otros son proporcionados por terceros.
- Internet de las cosas (IoT) se refiere a dispositivos con sensores que se comunican entre sí y con Internet.
- Azure IoT Hub le permite administrar dispositivos IoT y enrutar mensajes hacia y desde esos dispositivos.
- El servicio de aprovisionamiento de Azure IoT Hub facilita el aprovisionamiento de una gran cantidad de dispositivos en IoT Hub.
- Azure IoT Central es una oferta de SaaS para monitorear dispositivos IoT.
- Big data se refiere a más datos que puede analizar a través de medios convencionales dentro de un marco de tiempo deseado.
- Big data se almacena en un almacén de datos. En Azure, puede ser Azure SQL Data Warehouse o Azure Data Lake Storage. SQL Data Warehouse es bueno para datos relacionales. Data Lake Storage es bueno para cualquier tipo de datos.
- HDInsight es la solución de Microsoft para el procesamiento en clúster de Hadoop de big data.
- El proceso de toma de decisiones de IA en varios puntos a lo largo de la red neuronal se conoce como la tubería ML.
- Azure Databricks es una buena solución para modelar datos desde un almacén de datos para que pueda usarse de manera efectiva en el modelado ML.
- Los clústeres de databricks están formados por cuadernos que pueden almacenar todo tipo de información.
- El Servicio Azure Machine Learning utiliza recursos basados en la nube para entrenar modelos ML mucho más rápido.
- Azure Machine Learning Studio le permite crear, entrenar y puntuar modelos ML en una interfaz de arrastrar y soltar.
- La informática sin servidor se refiere al uso de máquinas virtuales excedentes en Azure para ejecutar su código a pedido. Solo paga cuando se ejecuta su código.
- Azure Functions es el componente de cómputo de serverless en Azure.
- Azure Logic Apps es una solución sin servidor de flujo de trabajo que usa conectores, disparadores y acciones.
- Azure Event Grid permite generar y controlar eventos a medida que interactúa con sus recursos de Azure.
- El portal de Azure es una interfaz basada en la web para interactuar con sus servicios de Azure. Utiliza llamadas API de ARM bajo el capó para hablar con Azure Resource Manager.

Capítulo 3. Comprender la seguridad, la privacidad, el cumplimiento y la confianza

A medida que las empresas se trasladan a la nube, una de las preocupaciones más importantes es la seguridad de las aplicaciones y los datos en la nube. El término seguridad, sin embargo, es un término amplio con muchos significados. Las empresas quieren asegurarse de que alguien con intenciones maliciosas no pueda afectar la disponibilidad de una aplicación o acceder a los datos de la aplicación, pero también quieren asegurarse de que el acceso de sus propios empleados a los recursos de la nube esté controlado. Además, las empresas también tienen muchas normas y políticas legales que deben cumplir, y se debe confiar en que un proveedor de la nube cumpla con esas normas.

Azure tiene servicios y características que se centran en todas estas preocupaciones. Las aplicaciones que están expuestas a Internet público están protegidas por características de red como Azure Firewall, Grupos de seguridad de red y Protección DDoS. Su cuenta de Azure está protegida con ofertas de identidad como Azure Active Directory y autenticación multifactor. Los datos y otros activos, como documentos y correos electrónicos, están protegidos por características como Azure Key Vault y Azure Information Protection.

Incluso con estas protecciones implementadas, Azure puede monitorear constantemente sus recursos en la nube en busca de signos de ataque con Azure Advanced Threat Protection. El Centro de seguridad de Azure proporciona recomendaciones basadas en sus recursos y en cómo están configurados, para que pueda prevenir proactivamente las amenazas en primer lugar.

Las características como las Políticas de Azure y el Control de acceso basado en roles aseguran que los usuarios con acceso legítimo a su suscripción puedan acceder solo a los recursos que desee, e incluso puede bloquear recursos para que no puedan reconfigurarse o eliminarse por error. Azure Monitor y Azure Service Health aseguran que siempre sepas lo que sucede con tus recursos de Azure.

Finalmente, Azure tiene muchos servicios y características que se centran en los estándares de cumplimiento y protección de datos. Microsoft Trust Center es un sitio web que le enseña cómo Azure protege y protege sus datos en la nube, y Service Trust Portal es un sitio web que ofrece herramientas como Azure Compliance Manager que le ayuda a garantizar que cumple con los estándares que son importantes para usted.

Con eso como marco, aquí están las habilidades que cubriremos en este capítulo.

Habilidades cubiertas en este capítulo:

- Comprender la seguridad de la conectividad de red en Azure
- Describir los servicios principales de Azure Identity.
- Describir las herramientas y características de seguridad de Azure.
- Describir las metodologías de gobierno de Azure.

- Comprender las opciones de supervisión e informes en Azure
- Comprender los estándares de privacidad, cumplimiento y protección de datos en Azure

HABILIDAD 3.1: COMPRENDER LA SEGURIDAD DE LA CONECTIVIDAD DE RED EN AZURE

El principal vector de ataque para aplicaciones y datos en la nube es la red, y si su aplicación está expuesta a Internet pública, la amenaza es mucho mayor. Las aplicaciones web a menudo son el objetivo de ataques que tienen como objetivo desactivar una aplicación u obtener acceso no autorizado a los datos. Sin embargo, las amenazas externas no son la única fuente de vulnerabilidades. Para mantener su aplicación y sus datos seguros, también es importante que controle el tráfico dentro de su red virtual en Azure. En esta sección de habilidades, aprenderá sobre varios servicios y características de Azure diseñados para abordar estos problemas de seguridad.

Esta sección cubre:

- Firewall azul
- Protección DDoS
- Grupos de seguridad de red
-
- Elegir una solución de seguridad de Azure adecuada

Firewall azul

En lenguaje informático, un firewall es un dispositivo a través del cual viaja el tráfico de red dentro y fuera de una red particular. El propósito de un firewall es permitir solo el tráfico deseado en la red y rechazar cualquier tráfico que pueda ser malicioso o que provenga de un origen desconocido. Un cortafuegos impone control sobre la red mediante reglas que especifican un rango de direcciones IP de origen y destino y una combinación de puertos.

En una configuración típica de firewall, todo el tráfico se deniega de manera predeterminada. Para que el firewall permita que el tráfico pase a través de él, una regla debe coincidir con ese tráfico. Por ejemplo, si desea permitir que alguien en Internet público acceda a una aplicación web que está ejecutando en un servidor en particular, cree una regla de firewall que permita la comunicación a los puertos 80 y 443 (los puertos para el tráfico HTTP y HTTPS). configure la regla para enviar ese tráfico a su servidor web.

Hay varios firewalls disponibles de terceros en Azure Marketplace, pero Microsoft también ofrece su propio firewall llamado Azure Firewall. Azure Firewall es una oferta de PaaS en Azure, y se administra fácilmente y ofrece un SLA del 99.95%. Azure Firewall escala según sus necesidades de red, por lo que no tiene que preocuparse por los picos de tráfico que causan latencia o tiempo de inactividad para sus aplicaciones.

Nota **Azure Firewall es un firewall con estado**

Azure Firewall es un firewall con *estado* . Eso significa que almacena datos en su memoria sobre el estado de las conexiones de red que fluyen a través de ella. Cuando nuevos paquetes de red para una conexión existente llegan al firewall, puede determinar si el estado de esa conexión representa una amenaza de seguridad.

Por ejemplo, si alguien falsifica su dirección IP e intenta obtener acceso a su red virtual en Azure, el firewall reconocerá que la dirección de hardware de la computadora utilizada ha cambiado y rechazará la conexión.

Una configuración típica para Azure Firewall consiste en lo siguiente:

- Una red centralizada que contiene Azure Firewall y una VM que funciona como un *jumpbox* . El firewall expone una dirección IP pública, pero la máquina virtual jumpbox no.
- Una o más redes adicionales (llamadas redes *radiales*) que no exponen una dirección IP pública. Estas redes contienen sus diversos recursos de Azure.

Jumpbox es una máquina virtual a la que puede acceder de forma remota para administrar otras máquinas virtuales en sus redes. Todas las demás máquinas virtuales están configuradas para permitir solo el acceso remoto desde la dirección IP de la máquina virtual Jumpbox. Si desea acceder a una máquina virtual en una red de radios, primero debe acceder de forma remota a la máquina virtual de jumpbox, y luego acceder de manera remota a la máquina virtual de la red de radios desde jumpbox. Esta configuración se conoce como configuración de *concentrador y radio* , y proporciona seguridad adicional para sus recursos de red.

Tenga en cuenta que **otras configuraciones de red son posibles**

Una configuración de concentrador y radio no es la única configuración donde se puede usar Azure Firewall. Por ejemplo, es posible que tenga una sola red virtual y Azure Firewall en esa red para filtrar el tráfico de Internet. Una configuración de red de concentrador y radio es la más común en las aplicaciones empresariales del mundo real.

La Figura 3-1 es una ilustración de una configuración típica de concentrador y radio que también incluye Azure Firewall. El tráfico que proviene de Internet a través del puerto 443 (tráfico HTTPS) es dirigido por el firewall a un servidor web que se ejecuta en Spoke VNet 1. El tráfico que ingresa a través del puerto de escritorio remoto se dirige a la máquina virtual jumpbox, y los usuarios pueden RDP desde Jumpbox VM a VM en Spoke VNet 2.

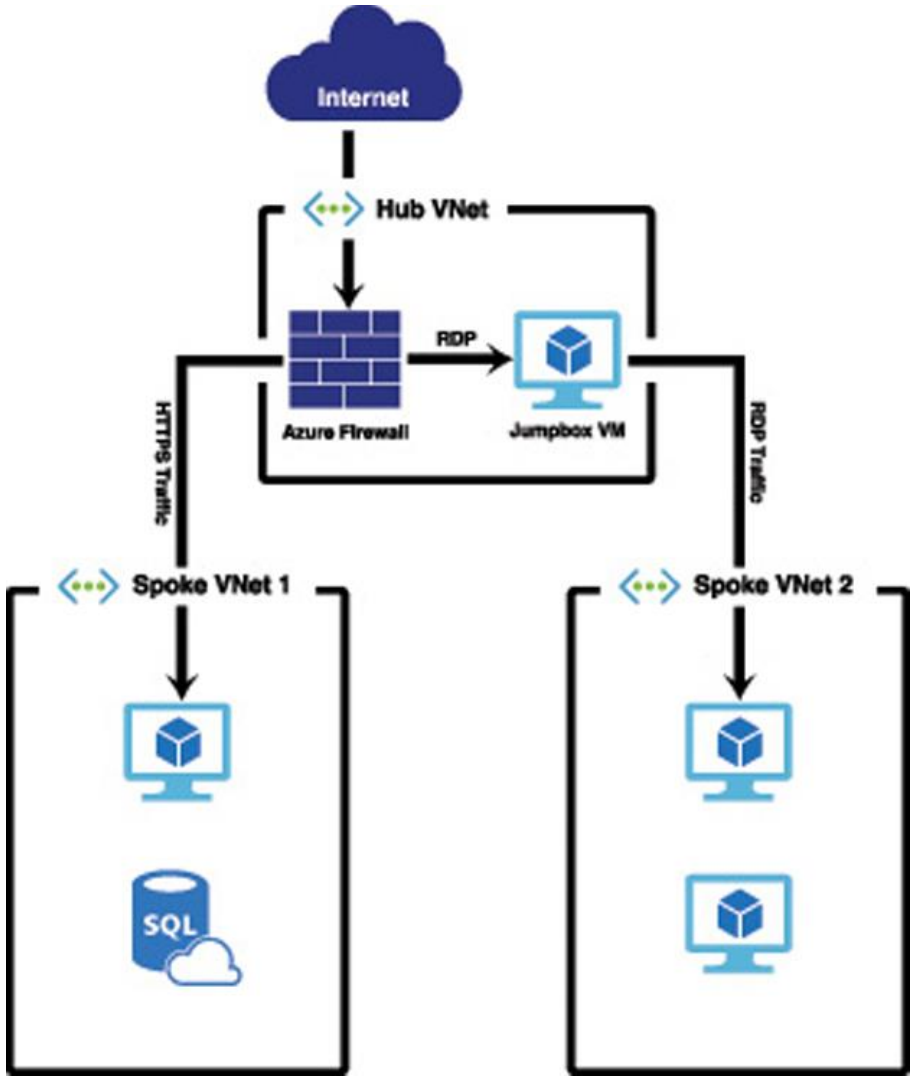


Figura 3-1 Un ejemplo de una configuración de red de concentrador y radio con Azure Firewall

Antes de que pueda configurar un firewall para manejar el tráfico de red, deberá crear una instancia de Azure Firewall. Puede elegir incluir Azure Firewall cuando creesu red virtual en Azure, o puede crear un firewall y agregarlo a una red virtual existente. La Figura 3-2 muestra que se está creando Azure Firewall durante la creación de una nueva red virtual.

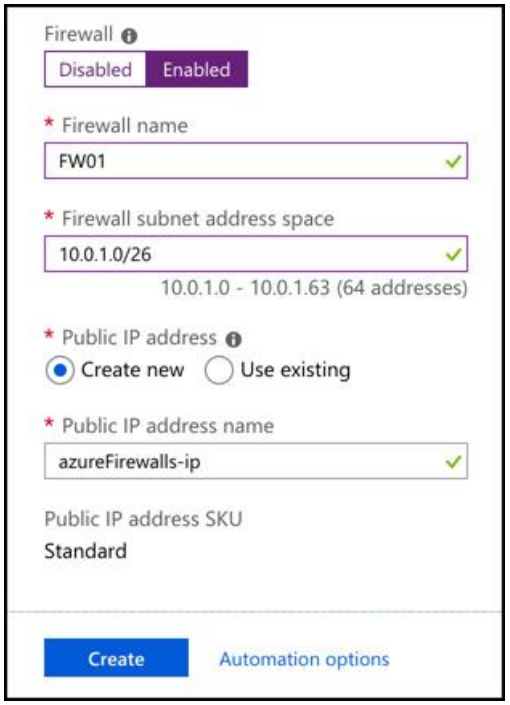


Figura 3-2 Creación de Azure Firewall

Cuando crea un firewall durante la creación de una red virtual, Azure crea una subred en la red virtual llamada AzureFirewallSubnet, y utiliza el espacio de direcciones que especifique para esa subred. También se crea una dirección IP pública para el firewall para que se pueda acceder desde Internet.

Si bien la naturaleza PaaS de Azure Firewall elimina gran parte de la complejidad, usar un firewall no es tan simple como habilitarlo en su red virtual. También deberá indicarle a Azure que envíe tráfico al firewall, y luego deberá configurar las reglas en el firewall para que sepa qué hacer con ese tráfico.

Para enviar tráfico a su firewall, debe crear una tabla de ruta. Una tabla de ruta es un recurso de Azure que está asociado con una subred y contiene reglas (llamadas *rutas*) que definen cómo se maneja el tráfico de red en la subred.

Se crea una tabla de ruta con el elemento Tabla de ruta en Azure Marketplace. Una vez que cree una nueva tabla de ruta, debe asociarla con una o más subredes. Para hacer eso, haga clic en **Subred** y luego haga clic en **Asociar** como se muestra en la Figura 3-3 .

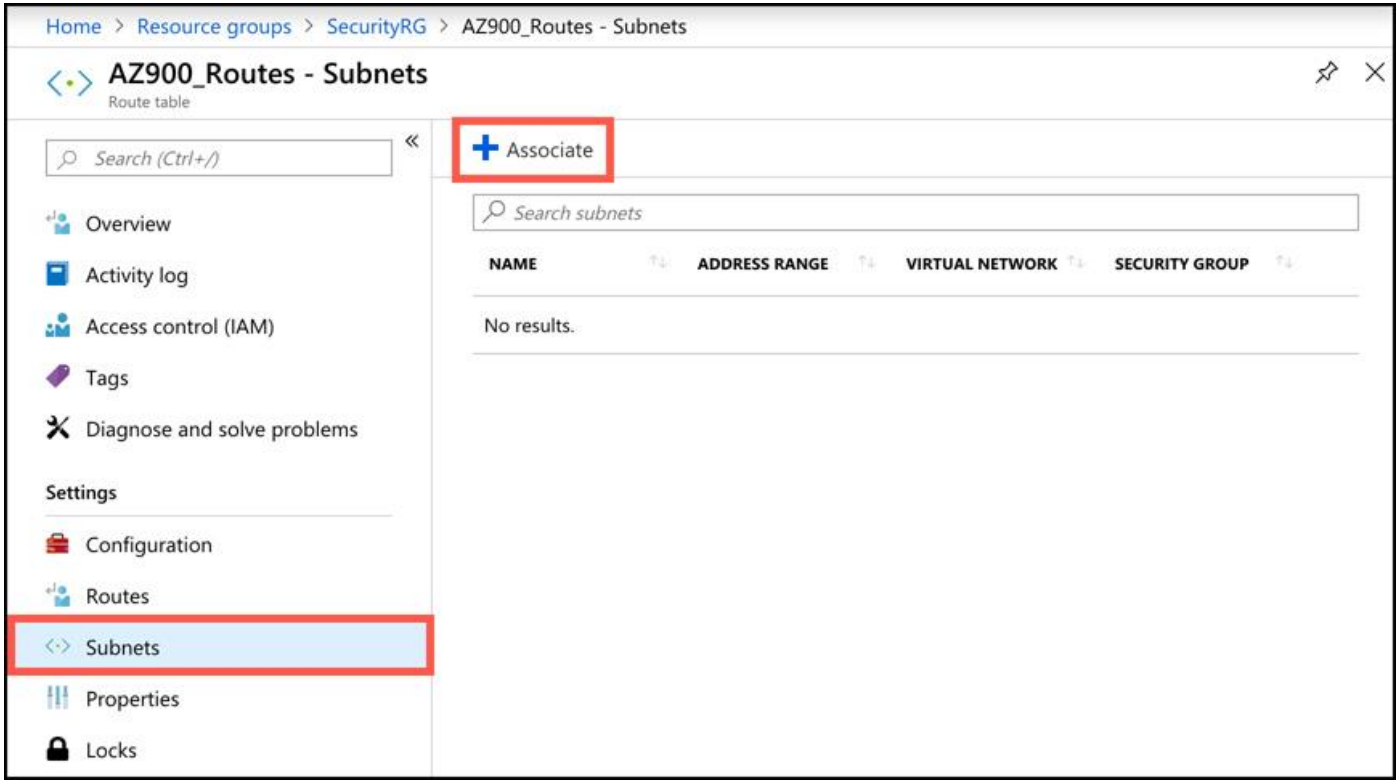


Figura 3-3 Asociación de una tabla de ruta con una subred

Después de hacer clic en Asociar, seleccione la red virtual y la subred como se muestra en la Figura 3-4 .

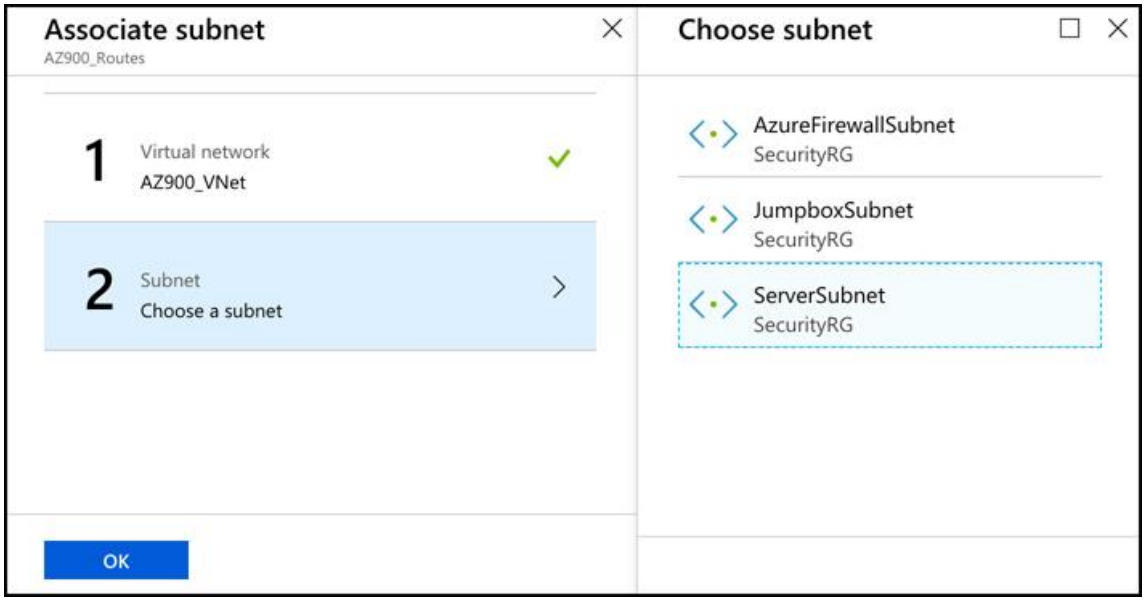


Figura 3-4 Elección de una subred para asociar

En nuestra configuración particular, queremos asociar tanto JumpboxSubnet como ServerSubnet con la tabla de rutas. Esto asegurará que el cortafuegos gestionará todo el tráfico de red a la máquina virtual jumpbox y todo el tráfico fuera de ServerSubnet.

Consejo de examen

Es importante comprender que un firewall puede (y debe) usarse para filtrar el tráfico que fluye dentro y fuera de una red. Por ejemplo, desea que el firewall maneje el tráfico en su jumpbox, pero también quiere asegurarse de que el tráfico que fluye desde la subred donde se encuentran otros servidores sea seguro y no envíe datos de manera inapropiada fuera de su red.

Una vez que hemos asociado la tabla de rutas con las subredes, creamos una ruta definida por el usuario para que el tráfico se dirija a través de Azure Firewall. Para hacer eso, haga clic en **Rutas** y luego haga clic en **Agregar** como se muestra en la Figura 3-5 .

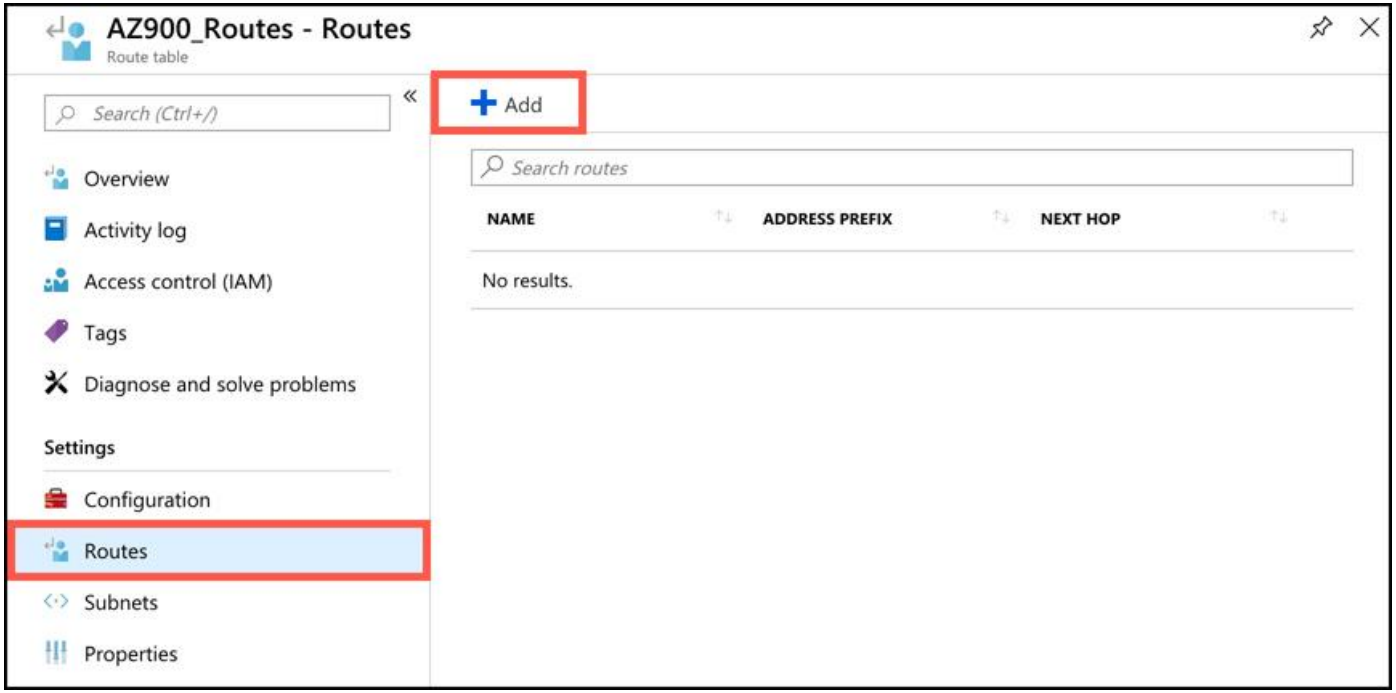


Figura 3-5 Agregar una nueva ruta definida por el usuario a la tabla de rutas

La Figura 3-6 muestra la configuración de una nueva ruta definida por el usuario llamada ToFirewall. Esta ruta está configurada para 0.0.0.0/0, la notación para todo el tráfico. Luego envía ese tráfico a un dispositivo virtual (Azure Firewall en este caso) ubicado en la dirección IP 10.1.1.4, que es la dirección IP interna de este firewall. Una vez configurada esta ruta, se aplicará inmediatamente a todos los dispositivos en las subredes asociadas con la tabla de rutas.

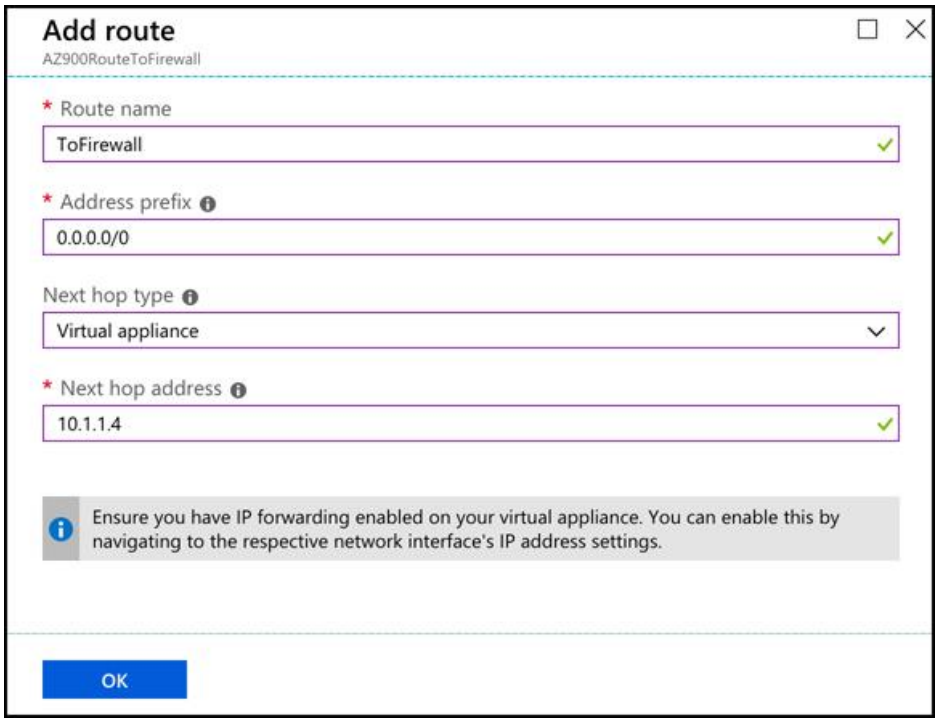


Figura 3-6 Agregar una ruta definida por el usuario

Recuerde que Azure Firewall bloquea todo el tráfico de forma predeterminada, por lo que en este momento, no hay forma de llegar a la máquina virtual Jumpbox que está en JumpboxSubnet. Para acceder a esa VM, debe configurar una regla de firewall en Azure Firewall que reenviará el tráfico apropiado a la VM de jumpbox.

Para agregar una regla de firewall, abra Azure Firewall en Azure Portal y haga clic en **Reglas** , seleccione el tipo de regla y haga clic en el botón **Agregar** para agregar una nueva colección de reglas como se muestra en la Figura 3-7 .

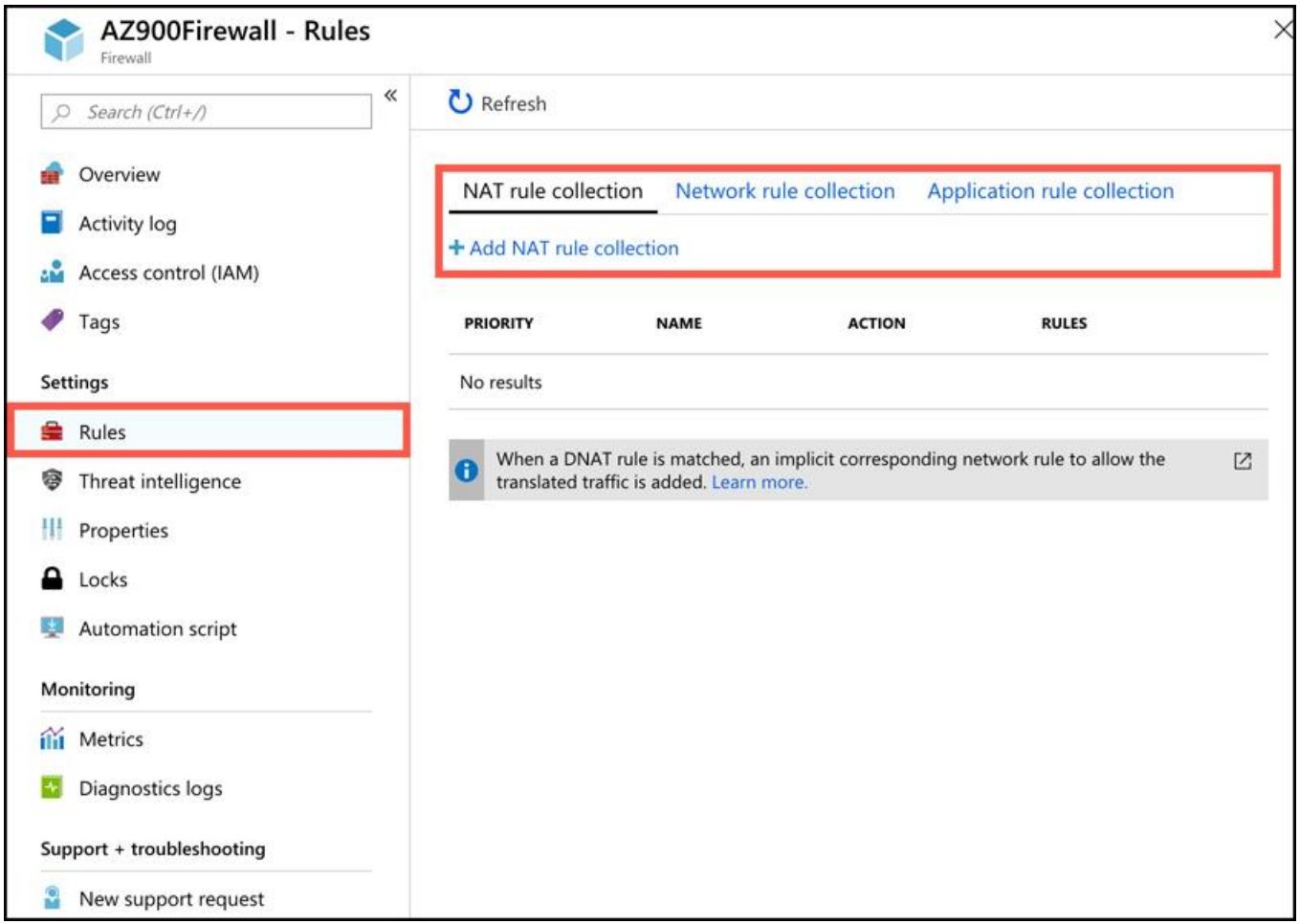


Figura 3-7 Colecciones de reglas de Azure Firewall en Azure Portal

Hay tres tipos de colecciones de reglas disponibles en Azure Firewall.

- **Reglas de traducción de direcciones de red (NAT)** Estas reglas se utilizan para reenviar el tráfico desde el firewall a otro dispositivo en la red.
- **Reglas de red** Estas son reglas que permiten el tráfico en rangos específicos de direcciones IP y puertos que especifique.
- **Reglas de** aplicación **Las reglas de** aplicación se utilizan para permitir que aplicaciones como Windows Update se comuniquen a través de su red. También se pueden usar para permitir nombres de dominio particulares como azure.com y microsoft.com.

Azure Firewall combina todas las reglas de un tipo específico y prioridad en una colección de reglas. La prioridad es un número entre 100 y 65,000. Los números más bajos representan una prioridad de regla más alta y se procesan primero. En otras palabras, si desea asegurarse de que una regla siempre se aplique antes que todas las demás reglas, incluya esa regla en una colección de reglas con una prioridad de 100.

Cuando el tráfico de red ingresa al firewall, las reglas NAT se aplican primero. Si el tráfico coincide con una regla NAT, Azure Firewall aplica una regla de red implícita para que el tráfico se pueda enrutar adecuadamente y se detiene todo el procesamiento de la regla adicional.

Si no hay una regla NAT que coincida con el tráfico, se aplican las reglas de red. Si una regla de red coincide con el tráfico, se detiene todo el procesamiento adicional de reglas. Si no hay una regla de red que se aplique al tráfico, se aplican las reglas de la aplicación. Si ninguna de las reglas de la aplicación coincide con el tráfico, el firewall rechaza el tráfico.

Para permitir el acceso remoto a la máquina virtual jumpbox, puede configurar una regla NAT que reenvíe cualquier tráfico en el puerto 55000 al puerto 3389 (el puerto para escritorio remoto) en la IP interna de la máquina virtual jumpbox como se muestra en la Figura 3-8 . Debido a que el puerto 55000 es un puerto general que normalmente no se usaría para el escritorio remoto, es probable que alguien con intenciones maliciosas nunca descubra que se está utilizando para ese propósito.

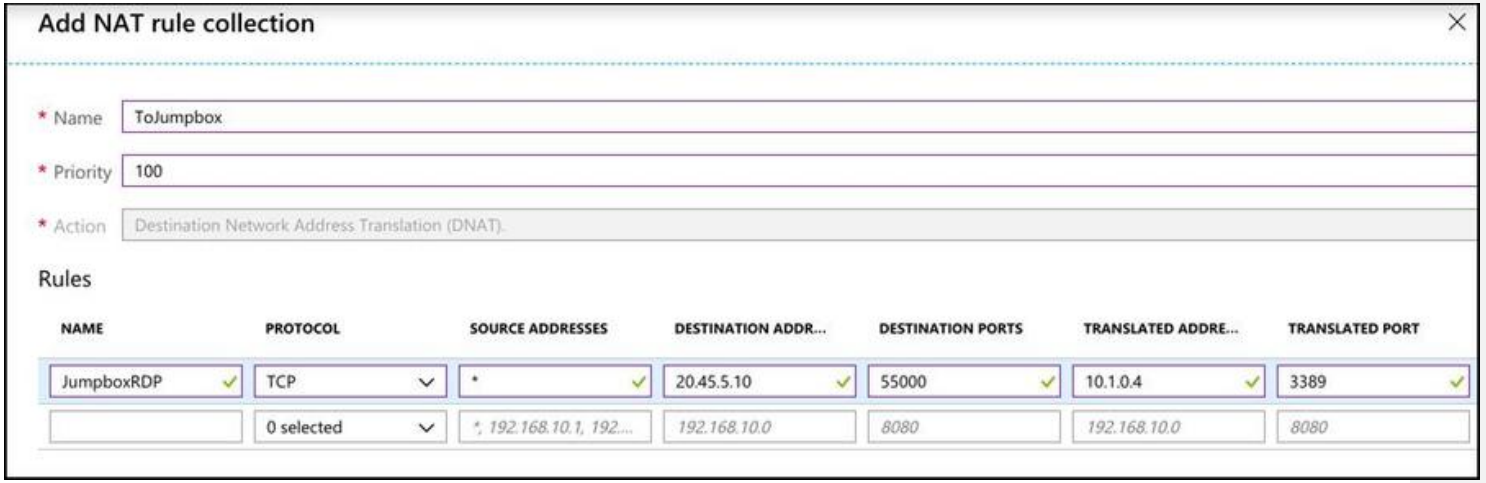


Figura 3-8 Agregar una regla NAT

Además de las reglas que configura, la función de inteligencia de amenazas (actualmente en versión preliminar) en Azure Firewall puede protegerlo de direcciones IP y nombres de dominio maliciosos conocidos. Microsoft actualiza constantemente su lista de actores malos conocidos, y los datos recopilados se proporcionan en el feed de Inteligencia de amenazas de Microsoft.

Cuando habilita la inteligencia de amenazas, puede elegir que Azure le avise si el tráfico de una dirección IP maliciosa o nombre de dominio conocido intenta ingresar a su red. También puede elegir que el firewall denegue el tráfico automáticamente como se muestra en la Figura 3-9 .

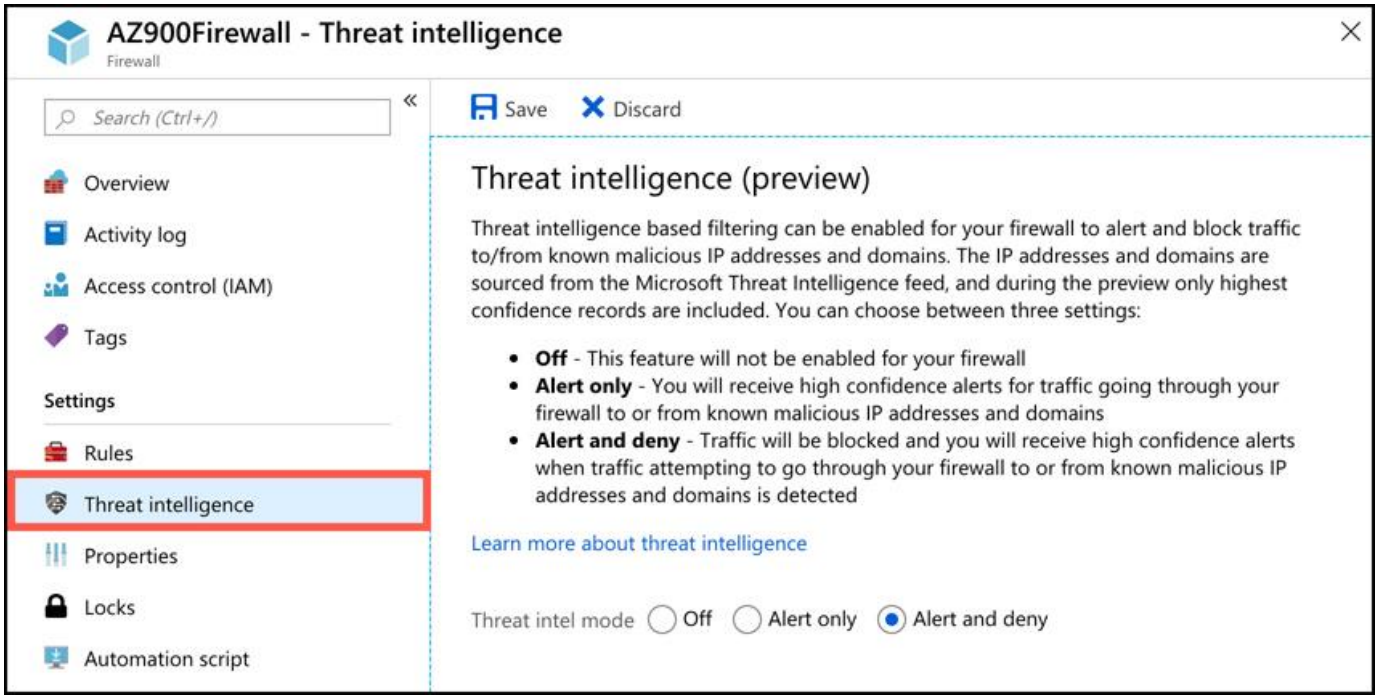


Figura 3-9 La inteligencia de amenazas puede ayudar a proteger su red virtual de Azure

Por cada hora que tenga implementado un Firewall de Azure, Microsoft le facturará $ 1.25. También se le factura $ 0.03 por cada gigabyte de datos procesados por el firewall.

Protección DDoS

Las aplicaciones en la nube a las que se puede acceder desde Internet a través de una dirección IP pública son susceptibles a *ataques de denegación de servicio* (DDoS) distribuidos. Los ataques DDoS pueden abrumar los recursos de una aplicación y a menudo pueden hacer que la aplicación no esté completamente disponible hasta que se mitigue el ataque. Los ataques DDoS también se pueden utilizar para explotar fallas de seguridad en una aplicación y atacar sistemas a los que se conecta una aplicación.

Azure puede ayudar a proteger contra ataques DDoS con la protección DDoS. La protección DDoS es una característica de las redes virtuales de Azure. Hay dos niveles de protección DDoS; Básico y estándar. Basic lo protege de ataques DDoS basados en volumen al distribuir grandes cantidades de volumen en toda la infraestructura de red de Azure. La protección básica DDoS se aplica a las direcciones IP públicas IPv4 e IPv6. Con el nivel básico, no tiene registro ni informe de ninguna mitigación de DDoS, y no hay forma de configurar alertas, de modo que se le notifique si se detecta un problema. Sin embargo, el nivel básico es gratuito y proporciona protección básica.

El nivel DDoS Standard ofrece protección no solo contra ataques DDoS basados en volumen, sino que cuando se usa en combinación con Azure Application Gateway, también protege contra ataques diseñados para atacar la seguridad de sus aplicaciones. Ofrece registro y alertas de eventos y mitigaciones DDoS, y si necesita ayuda durante un ataque DDoS, Microsoft proporciona acceso a expertos que pueden ayudarlo. El nivel estándar de DDoS se aplica solo a las direcciones IP públicas de IPv6.

El nivel estándar está dirigido a clientes empresariales y se factura a $ 2,994.00 por mes, más una pequeña tarifa por gigabyte para los datos que se procesan. El precio mensual fijo cubre hasta 100 recursos. Si necesita cubrir recursos adicionales, paga $ 30.00 adicionales por recurso por mes.

Para habilitar el nivel DDoS Standard, haga clic en **Protección DDoS** en su red virtual en Azure Portal y seleccione **Standard** como se muestra en la Figura 3-10 .

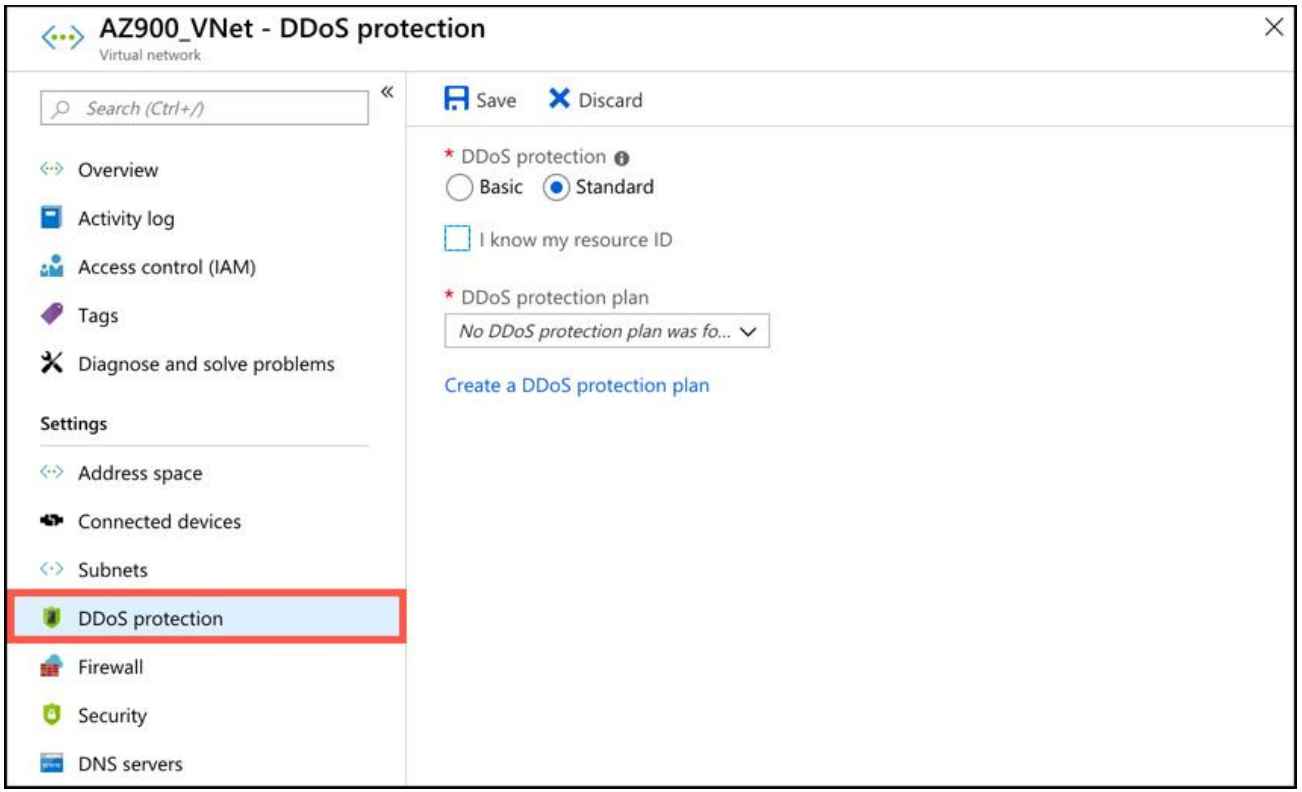


Figura 3-10 Protección DDoS en Azure Portal

Para habilitar el nivel Estándar, necesitará un plan de protección DDoS. Si actualmente no tiene uno, haga clic en **Crear un plan de protección DDoS** para crear uno en Azure Portal. Luego puede aplicar ese plan de protección DDoS a su red virtual y a otras redes virtuales a las que tiene acceso en Azure. No se requiere que las redes virtuales que usan el plan de protección DDoS estén en la misma suscripción, por lo que en la mayoría de los casos, una organización solo necesitará un único plan de protección DDoS para proteger todas sus redes virtuales.

Consejo de examen

El hecho de que pueda agregar redes virtuales desde múltiples suscripciones de Azure al mismo plan de protección DDoS es un concepto importante. Se le factura un gran cargo mensual por el plan de protección DDoS, y si crea dos planes de protección DDoS, acaba de duplicar sus costos.

El nivel estándar de protección DDoS monitorea el tráfico de su red las 24 horas del día, los 7 días de la semana, y utiliza el aprendizaje automático para perfilar su tráfico a lo largo del tiempo y ajustarse para adaptarse al perfil de tráfico de su red. Durante un evento DDoS, el nivel estándar le permite transmitir registros a un sistema de *información de seguridad y gestión de eventos* (SIEM). Los sistemas SIEM están diseñados para permitir la agregación de datos de una gran cantidad de fuentes para fines de análisis y para cumplir con las políticas y estándares de retención de datos.

Una vez que haya configurado cualquier alerta y monitoreo para la protección DDoS, puede simular un evento DDoS utilizando una cuenta de BreakingPoint Cloud disponible en: *https://www.ixiacom.com/products/breakingpoint-cloud* . Esto le permite asegurarse de que su protección DDoS lo protege de los ataques DDoS.

Grupos de seguridad de red

Un grupo de seguridad de red (NSG) le permite filtrar el tráfico en su red y aplicar reglas sobre ese tráfico. Un NSG contiene varias reglas integradas proporcionadas por Azure que están diseñadas para permitir que sus recursos en la red virtual se comuniquen entre sí. Luego puede agregar sus propias reglas al NSG para controlar el tráfico dentro y fuera de la red, y también entre los recursos de la red.

La Figura 3-11 muestra la aplicación de varios niveles que se muestra por primera vez en el Capítulo 2 , Descripción de los servicios principales de Azure.

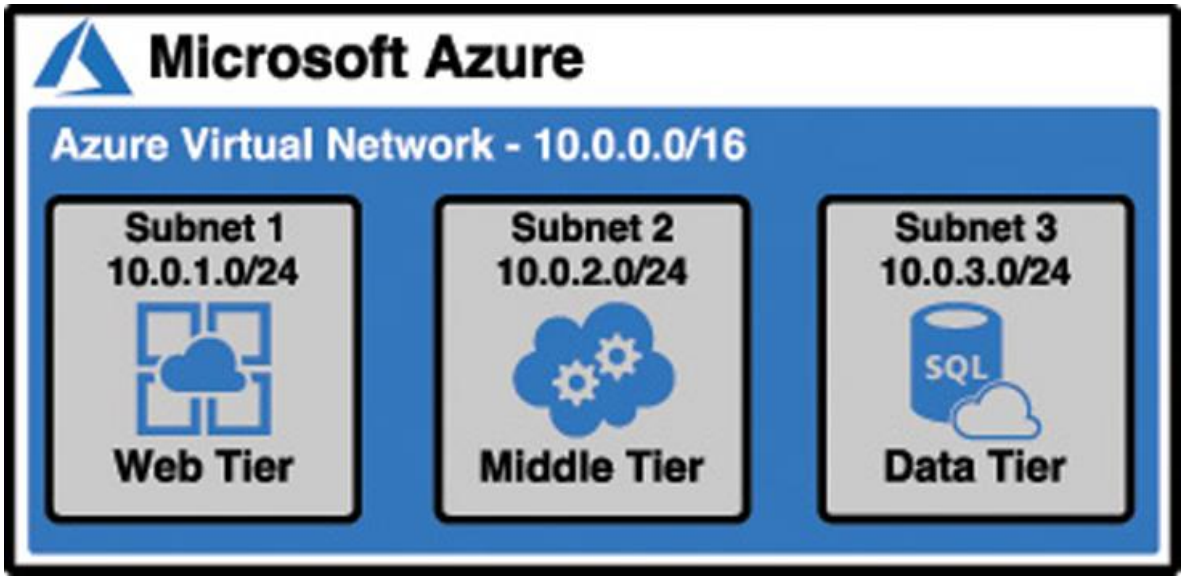


Figura 3-11 Una aplicación de varios niveles

Aquí está el flujo de tráfico de esta aplicación.

- La subred 1 recibe datos de otra red virtual que ejecuta Azure Firewall.
- La subred 1 se comunica con la subred 2 para procesar las solicitudes.
- La subred 2 se comunica con un servidor de base de datos en la subred 3 para acceder a los datos.

Si desea garantizar un entorno seguro, la Subred 1 no debería poder comunicarse directamente con los recursos de la Subred 3. Del mismo modo, la Subred 3 no debería poder comunicarse directamente con los recursos de la Subred 1. Finalmente, solo la Subred 1 debería poder comunicarse con la otra red virtual que ejecuta Azure Firewall. Puede usar NSG para implementar reglas que hagan cumplir estas políticas.

Los NSG se pueden asociar con una subred o con una interfaz de red conectada a una VM. Cada interfaz de red o subred solo puede tener un NSG asociado, pero puede crear hasta 1,000 reglas en un solo NSG, por lo que debería poder aplicar fácilmente toda la lógica de reglas necesaria para cualquier tarea. Si asocia un NSG a una subred y a una o más interfaces de red dentro de esa subred, primero se aplican las reglas para el NSG asociado con las interfaces de red, y luego se aplican las reglas del NSG de la subred.

 *Consejo de examen*

Un NSG asociado con una subred afecta a todas las máquinas virtuales dentro de esa subred, así como al tráfico hacia y desde la subred. Por ejemplo, si configura un NSG para evitar todo el tráfico, excepto el tráfico de Internet, y luego asocia ese NSG con una subred que contiene dos máquinas virtuales, esas dos máquinas virtuales ya no podrán comunicarse entre sí porque solo el tráfico de Internet está permitido por el NSG.

Para evitar que las reglas interfieran entre sí, cada regla que cree en un NSG tiene una prioridad entre 100 y 4.096. Las reglas con una prioridad más baja tienen prioridad sobre las reglas con una prioridad más alta. El tráfico de red se aplica contra la regla con el número de prioridad más bajo primero. Si el tráfico coincide con esa regla, se aplica la regla y se detiene el procesamiento de la regla. Si el tráfico no coincide con la regla, se evalúa contra la siguiente regla de menor prioridad. Esto continúa hasta que el tráfico haya coincidido con una regla o no haya reglas adicionales.

Más información **Prioridad de las reglas predeterminadas**

Las reglas predeterminadas que Azure aplica a todos los NSG tienen una prioridad en el rango de 65,000. Esto evita que las reglas predeterminadas anulen alguna vez una regla explícita que cree, y le facilita anular las reglas predeterminadas si es necesario.

Para crear un NSG, busque el Grupo de seguridad de red en Azure Marketplace. Cuando cree un NSG, asígnele un nombre, elija o cree un grupo de recursos y especifique la ubicación del NSG, como se muestra en la Figura 3-12 .

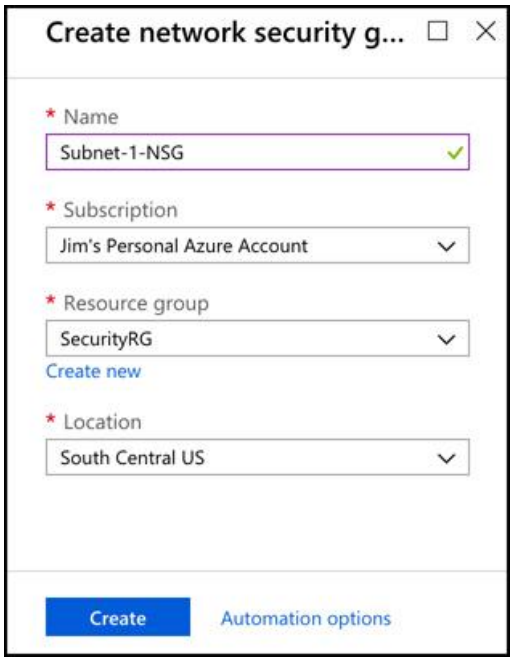


Figura 3-12 Crear un NSG

Después de crear un NSG, puede agregar reglas entrantes y salientes para el NSG. Una vez que abra el NSG en Azure Portal, haga clic en **Reglas de seguridad de entrada** para agregar nuevas reglas de entrada y en **Reglas de seguridad de salida** para agregar reglas de salida.

En la Figura 3-13 , hacemos clic en Reglas de seguridad de entrada para agregar una nueva regla que permita el tráfico de la red virtual que ejecuta Azure Firewall. Después de eso, el NSG se asociará con la Subred-1. Tenga en cuenta que puede asociar el NSG con una subred o interfaz de red antes de agregar reglas.

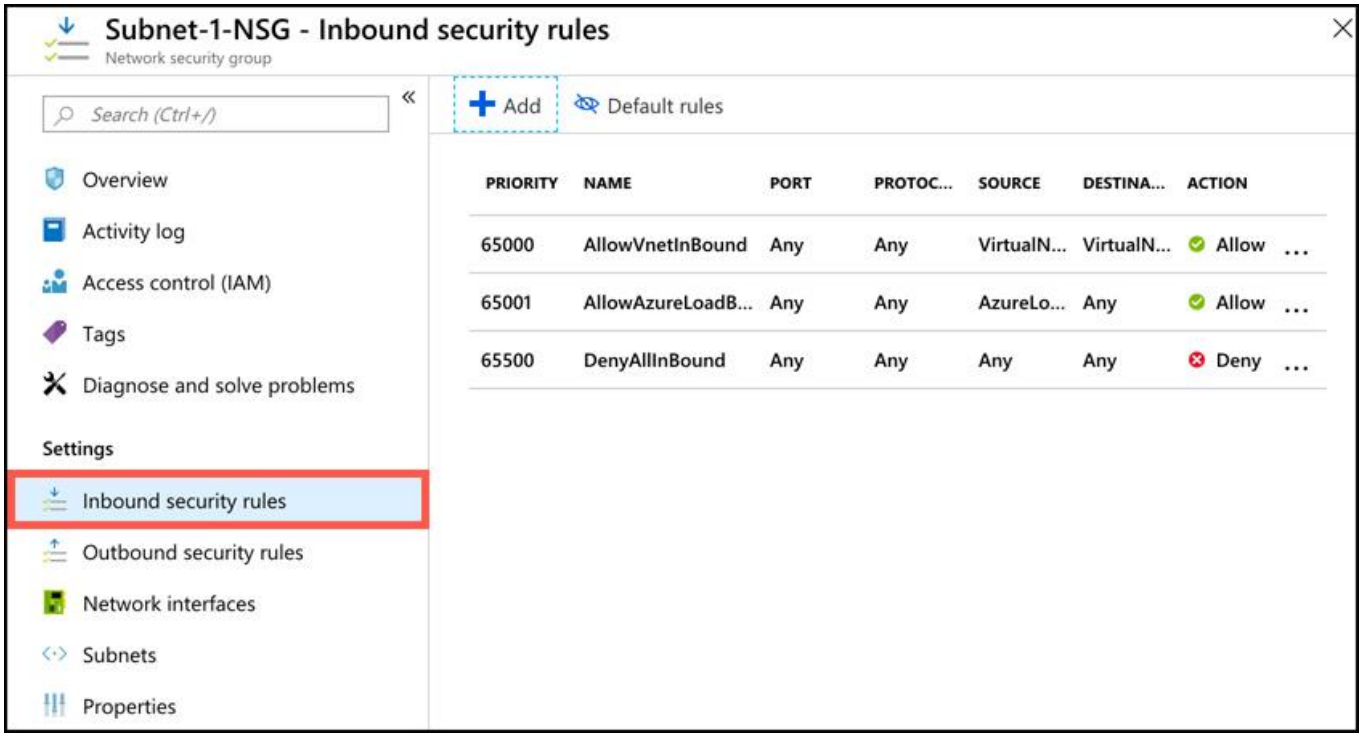


Figura 3-13 Reglas de seguridad de entrada para un NSG

Haga clic en Agregar para agregar una nueva regla NSG. La Figura 3-14 muestra una nueva regla que se agrega que permite el tráfico en esta subred desde el espacio de direcciones de otra red virtual que ejecuta Azure Firewall.

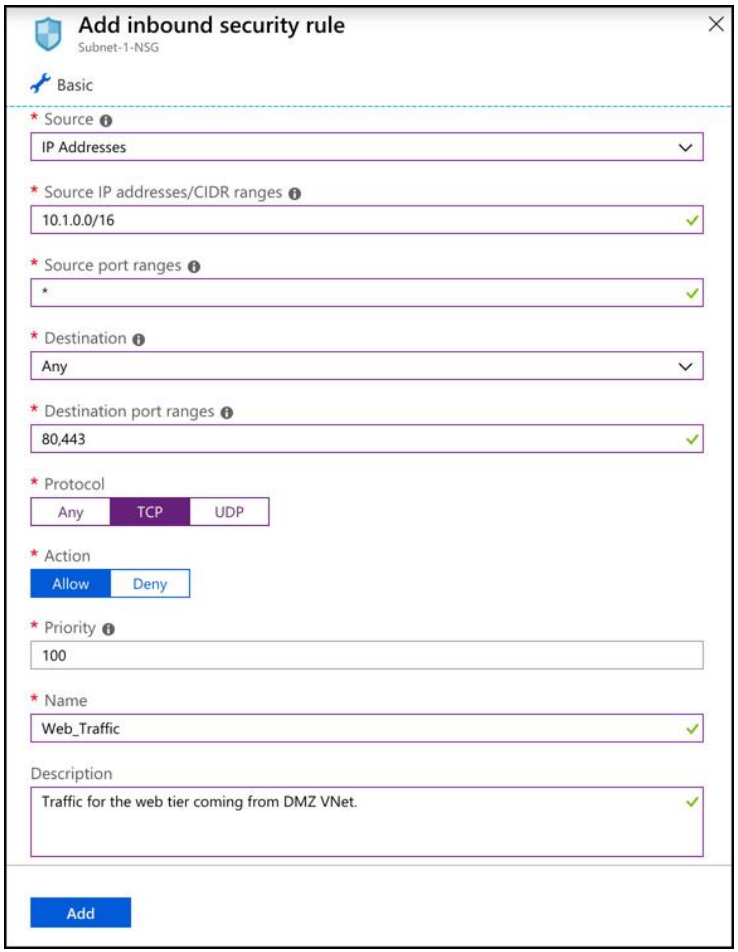


Figura 3-14 Creación de una regla de entrada NSG

La regla que se configura en la Figura 3-14 usa la notación CIDR para las direcciones IP de origen, pero también puede ingresar una dirección IP específica o cambiar el menú desplegable Fuente a **Cualquiera** si desea que la regla se aplique a todas las direcciones IP.

Haga clic en **Subredes** para asociar un NSG con una subred, o **Interfaces de red** para asociarlo con una interfaz de red utilizada por una VM. Luego haga clic en **Asociar** , como se muestra en la Figura 3-15 .

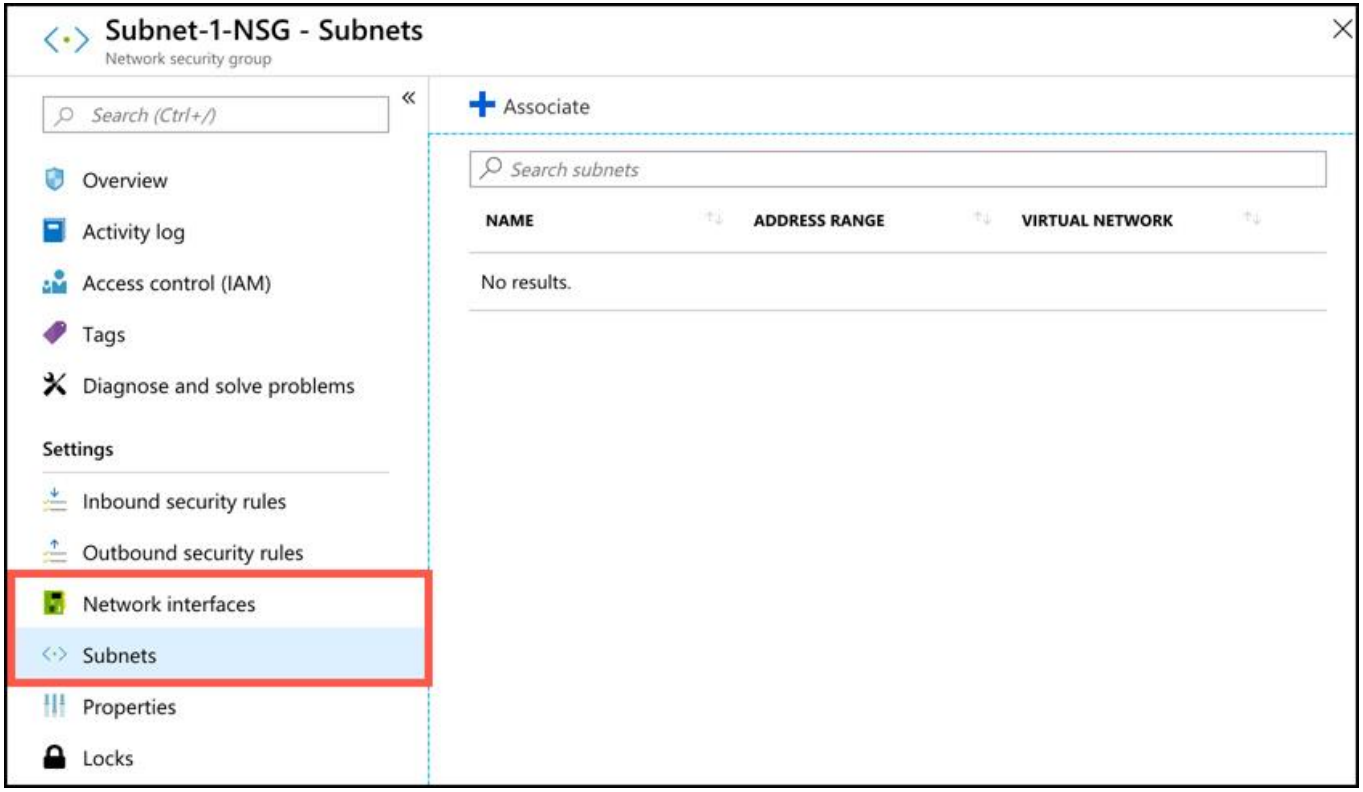


Figura 3-15 Asociando un GSN

La Figura 3-16 muestra la hoja donde un NSG está asociado con una subred.

Figura 3-16 Asociando un NSG con una subred

Las reglas de seguridad de salida se crean de la misma manera que las reglas de entrada. Sin embargo, no es necesario que cree una regla de salida correspondiente para cada regla de entrada. Los NSG mantienen lo que se llama un *registro de flujo* que almacena el estado de una conexión, y el NSG permitirá el tráfico que corresponde a ese registro de flujo sin una regla explícita.

Si una regla de seguridad permite el tráfico entrante al puerto 80 desde direcciones IP en el rango de 10.1.0.0/16, como la regla configurada en la Figura 3-14 , el NSG también permitirá el tráfico saliente en el puerto 80 a direcciones en ese mismo rango utilizando el registro de flujo. Solo una vez que el tráfico deja de fluir durante unos minutos, el registro de flujo ya no estará vigente.

Hay algunos casos en los que no conocerá el rango específico de direcciones IP. Por ejemplo, si desea configurar una regla NSG en una red virtual que permita todo el tráfico de Internet,no especificarías un rango de direcciones exacto. Para lidiar con eso, los NSG le permiten usar *etiquetas de servicio* al configurar reglas.

Una etiqueta de servicio es un identificador especial creado por Microsoft que se aplica a Internet o a un tipo de servicio específico dentro de Azure. Por ejemplo, si tiene algunas aplicaciones web ejecutándose en Azure App Service y desea permitir que se comuniquen con su subred, puede usar la etiqueta del servicio AppService en su regla de entrada para permitir eso. Los servicios de Azure también tienen etiquetas de servicio específicas de la región para que pueda permitir o denegar el tráfico solo de regiones específicas.

Para usar una etiqueta de servicio, establezca la Fuente de su regla en Etiqueta de servicio. Luego puede seleccionar una etiqueta de servicio en el menú desplegable Etiqueta de servicio de origen. En la Figura 3-17 , la etiqueta del servicio AppService.CentralUS se está utilizando para permitir el tráfico de los recursos del Servicio de aplicaciones de Azure en la región central de los EE. UU.

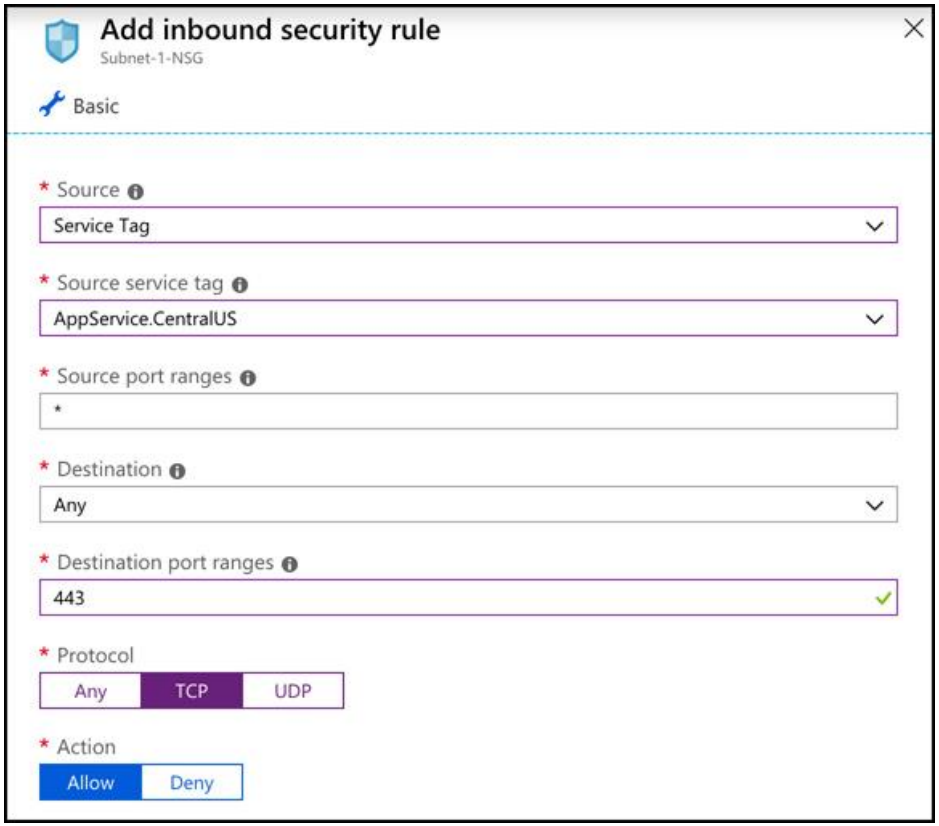


Figura 3-17 Uso de una etiqueta de servicio en una regla NSG

Elegir una solución de seguridad de Azure adecuada

Dependiendo de su aplicación y su configuración, es posible que necesite o no todas las soluciones de seguridad que hemos discutido. Los GSN deben considerarse en casi todos los escenarios para garantizar que solo el tráfico de red deseado fluya entre sus

recursos. Si su aplicación está expuesta a Internet, los NSG pueden garantizar que el tráfico de Internet solo se permita a subredes o máquinas virtuales específicas. Incluso si no está utilizando una dirección IP pública, los NSG pueden ayudarlo a imponer una comunicación segura entre las capas de una aplicación.

Azure Firewall es una forma poderosa de garantizar que el tráfico en sus redes virtuales esté estrictamente controlado. A diferencia de un NSG, Azure Firewall es una solución con estado que comprende la composición de una conexión de red y puede identificar si se está intentando un ataque en su red. Sin embargo, Azure Firewall no es necesario si su aplicación no expone una dirección IP pública.

La protección DDoS es un medio eficaz para proteger su red de ataques diseñados para impactar sus aplicaciones con un gran volumen de tráfico aparentemente legítimo. Puede agregar otra capa de protección mediante el uso de Application Gateway junto con el nivel estándar de protección DDoS para protegerse contra las amenazas de seguridad a la aplicación.

HABILIDAD 3.2: DESCRIBIR LOS SERVICIOS PRINCIPALES DE AZURE IDENTITY

La seguridad no se trata solo de controlar el tráfico de red. Para proporcionar un entorno seguro, debe tener algunos medios para identificar quién accede a su aplicación. Una vez que conoce la identidad de un usuario, debe asegurarse de que no se les permita el acceso a datos u otros recursos a los que no deberían acceder.

La autenticación es el proceso por el cual se confirma la identidad de un usuario. Una vez que un usuario se autentica y comienza a interactuar con una aplicación, se pueden realizar verificaciones adicionales para confirmar qué acciones está y no puede realizar el usuario. Ese proceso se llama autorización, y las verificaciones de autorización se realizan contra un usuario que ya está autenticado.

Azure ofrece un servicio llamado Azure Active Directory que proporciona capacidades de autenticación y autorización para recursos y aplicaciones, tanto en la nube como en las instalaciones.

Esta sección cubre:

- Azure Active Directory
- Autenticación multifactor

Azure Active Directory

Si tiene alguna experiencia con Windows Active Directory local, es posible que entender el Azure Active Directory (Azure AD) sea un desafío. Esto se debe a que Azure AD no es el equivalente en la nube de Windows Active Directory. Es completamente diferente.

Azure AD es un servicio de identidad basado en la nube en Azure que puede ayudarlo a autenticar y autorizar a los usuarios. Puede usar Azure AD para dar acceso a los usuarios a los recursos de Azure. También puede dar a los usuarios acceso a recursos de terceros utilizados por su empresa y recursos locales, todos con el mismo nombre de usuario y contraseña.

***Más información que* otorga acceso a los recursos de Azure**

Aprenderá cómo puede dar acceso a otros usuarios a sus recursos de Azure cuando cubramos el control de acceso basado en roles en la Habilidad 3.4, "Describa las metodologías de gobierno de Azure".

El núcleo de Azure AD es un directorio de usuarios. Cada usuario tiene una *identidad* que se compone de una ID de usuario, una contraseña y otras propiedades. Los usuarios también tienen uno o más *roles de directorio* asignados a ellos. El ID de usuario y la contraseña se usan para autenticar al usuario, y los roles se usan para la autorización para realizar ciertas actividades en Azure AD.

Cuando se suscribe a una suscripción de Azure, se crea automáticamente un recurso de Azure AD para usted y se usa para controlar el acceso a los recursos de Azure que crea bajo su suscripción. La Figura 3-18 muestra Azure AD en el portal de Azure.

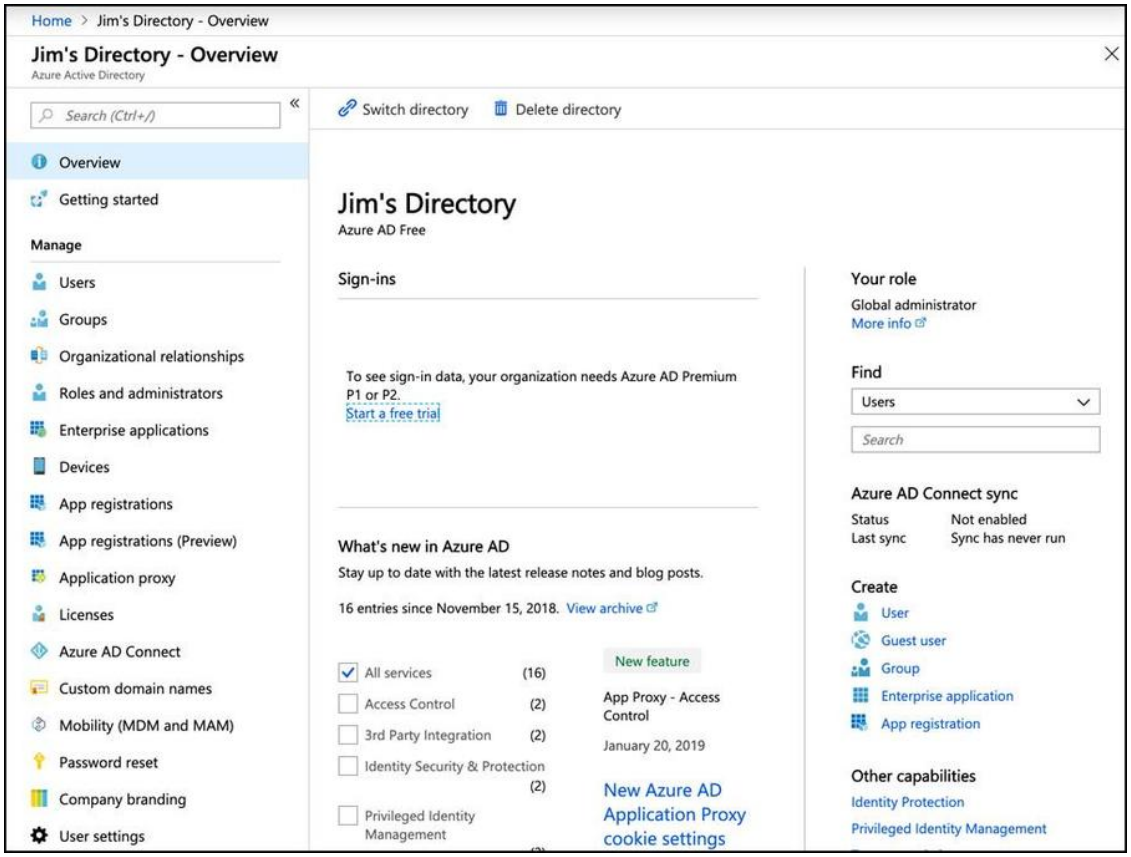


Figura 3-18 Azure AD en el portal de Azure

Para ver o administrar usuarios en Azure AD, haga clic en **Usuarios** en el menú en el lado izquierdo de la página. Esto abre la hoja Todos los usuarios que se muestra en la Figura 3-19 .

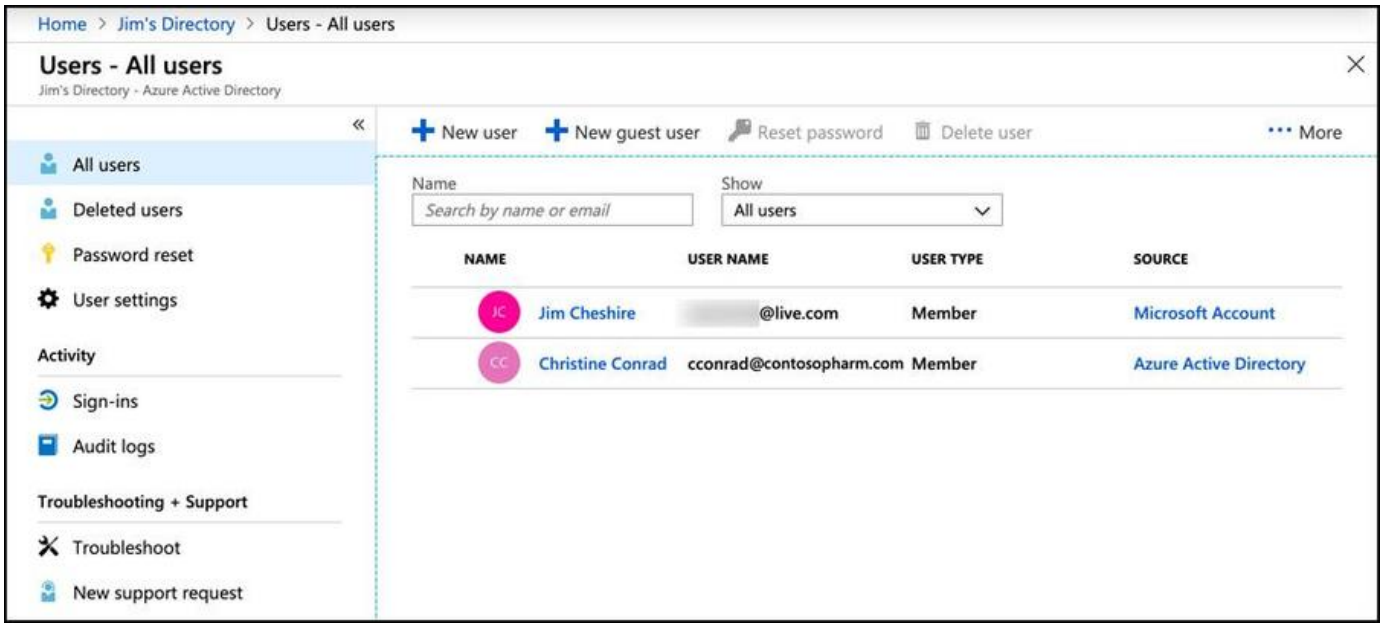


Figura 3-19 La hoja Todos los usuarios en Azure Portal

El Azure AD que se muestra en la Figura 3-19 contiene dos usuarios. La fuente del primer usuario es la cuenta de Microsoft, lo que significa que este usuario está vinculado a una dirección de correo electrónico de la cuenta de Microsoft. El otro usuario es un usuario de Azure Active Directory que se agregó manualmente.

Para agregar un nuevo usuario de su empresa a su Azure AD, haga clic en **Nuevo usuario** para mostrar la hoja que se muestra en la Figura 3-20 .

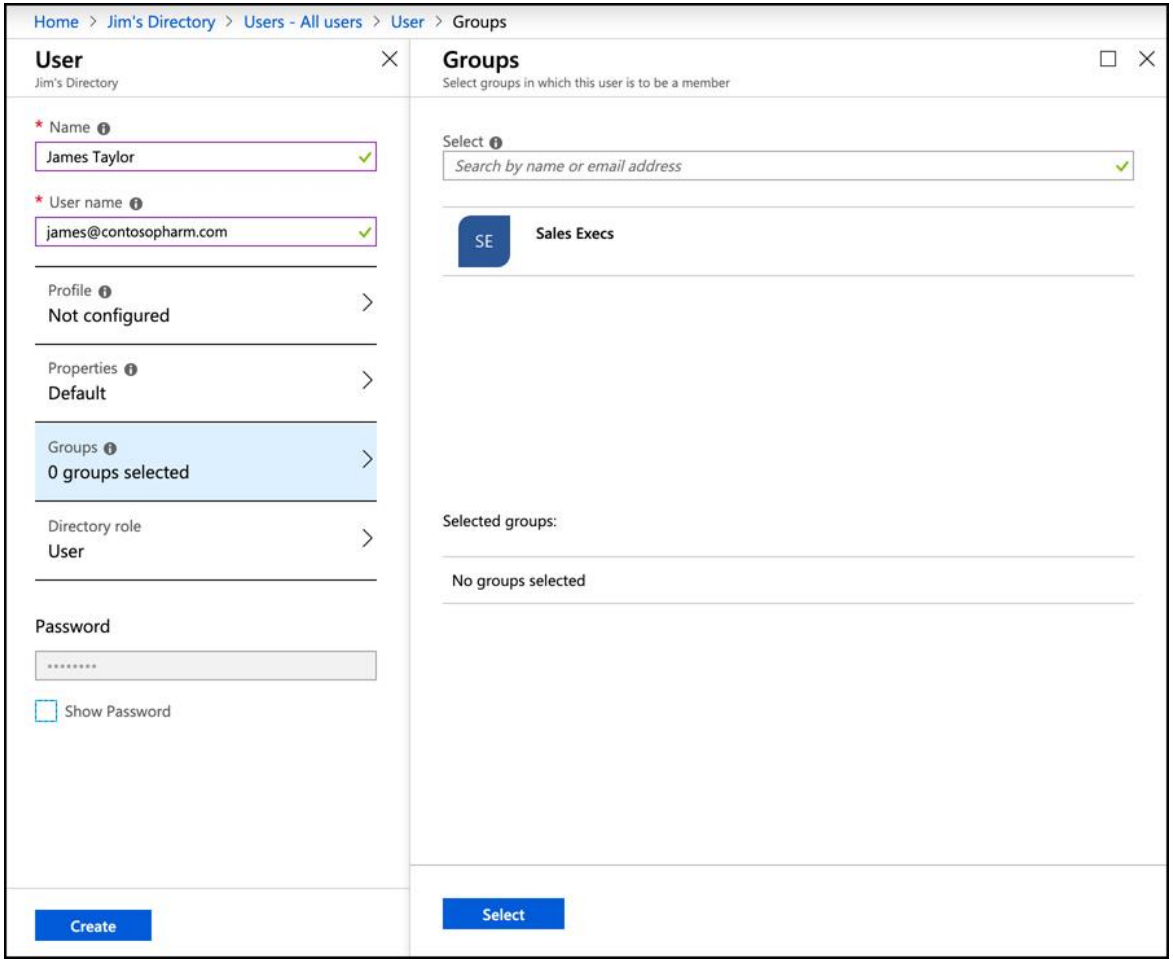


Figura 3-20 Agregar un nuevo usuario de Azure AD

El nombre de usuario especificado se usa para iniciar sesión en Azure AD. El nombre de dominio que use debe ser uno de su propiedad y que esté asociado con su Azure AD. También puede hacer clic en **Grupos** para elegir un grupo para este usuario. Grupos facilita la administración de grupos más grandes de usuarios similares.

Azure AD ofrece una función llamada colaboración de Azure AD B2B (empresa a empresa) que le permite agregar usuarios que no pertenecen a su empresa. Por lo tanto, puede invitar a otros usuarios externos a su empresa a ser miembros de su Azure AD. A esos usuarios se les puede dar acceso a sus recursos. Los usuarios que no forman parte de su empresa se denominan *usuarios invitados* . Para agregar un usuario invitado, haga clic en Nuevo usuario invitado que se muestra en la Figura 3-19 . Esto abrirá la hoja Nuevo usuario invitado que se muestra en la Figura 3-21 .

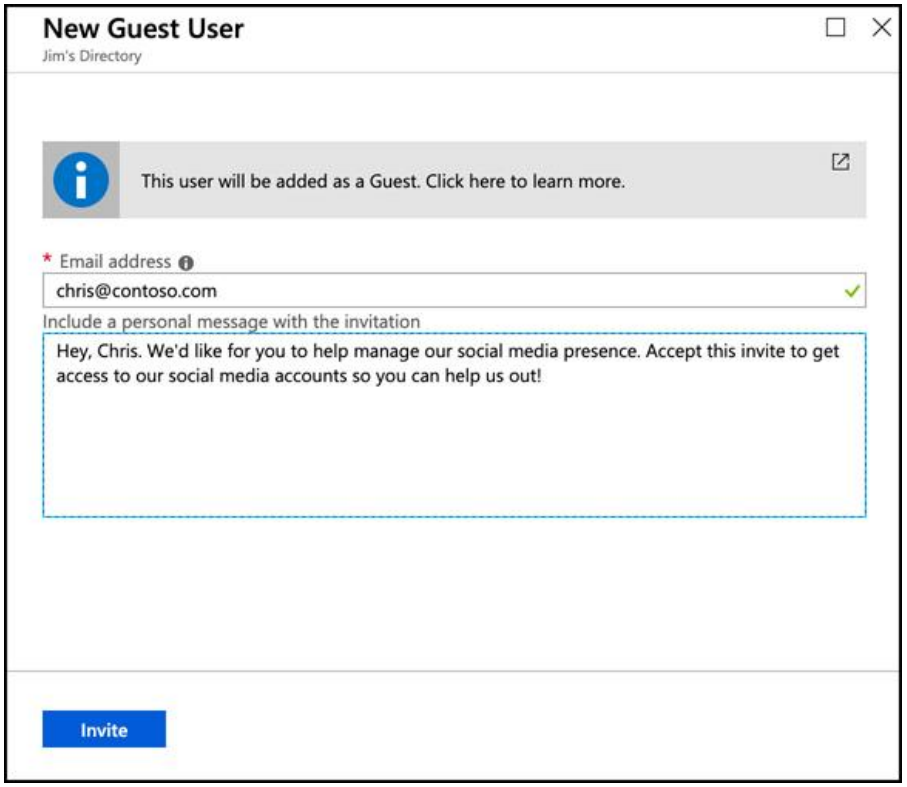


Figura 3-21 Agregar un nuevo usuario invitado

Cuando invita a un usuario invitado, se envía una invitación para unirse a su Azure AD a la dirección de correo electrónico que especifique. Para aceptar la invitación, la dirección de correo electrónico del usuario debe estar asociada a una cuenta de Microsoft. Si el usuario no tiene una cuenta de Microsoft, se le dará la opción de crear una para que pueda unirse a su Azure AD.

Al usuario en la Figura 3-21 se le puede dar acceso a las cuentas de redes sociales corporativas agregando esas aplicaciones a Azure AD. Las aplicaciones para agregar incluyen, no solo aplicaciones de redes sociales como Facebook y Twitter, sino también miles de otras. Para agregar una aplicación, abra Azure AD en Azure Portal, haga clic en **Aplicaciones empresariales** y haga clic en **Nueva aplicación** , como se muestra en la Figura 3-22 .

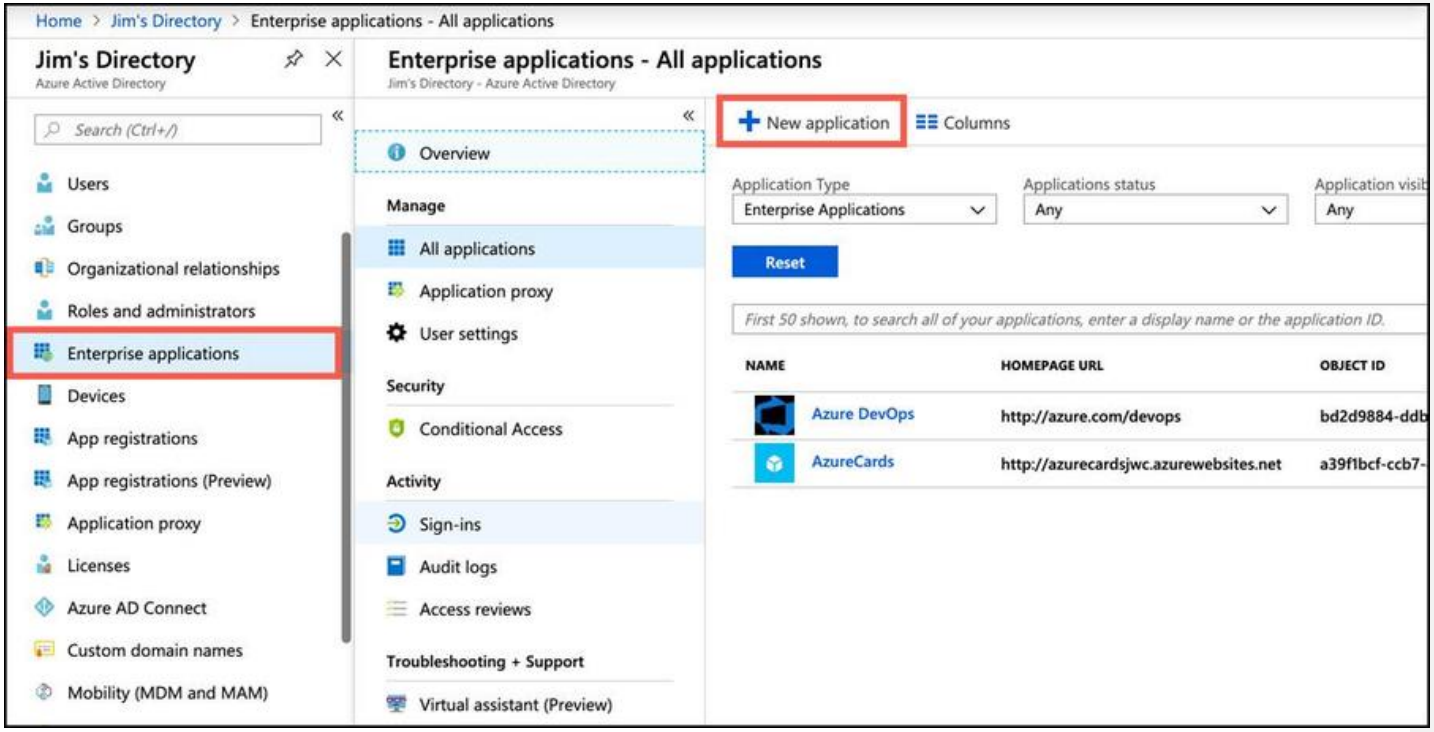


Figura 3-22 Aplicaciones empresariales en Azure AD

Después de hacer clic en Nueva aplicación, puede elegir de una lista de aplicaciones incluidas, como se muestra en la Figura 3-23 . También puede agregar su propia aplicación, agregar una aplicación que exista en su entorno local o integrar cualquier otra aplicación. La aplicación que agregue debe exponer una página de inicio de sesión a la que pueda apuntar Azure AD para integrarla.

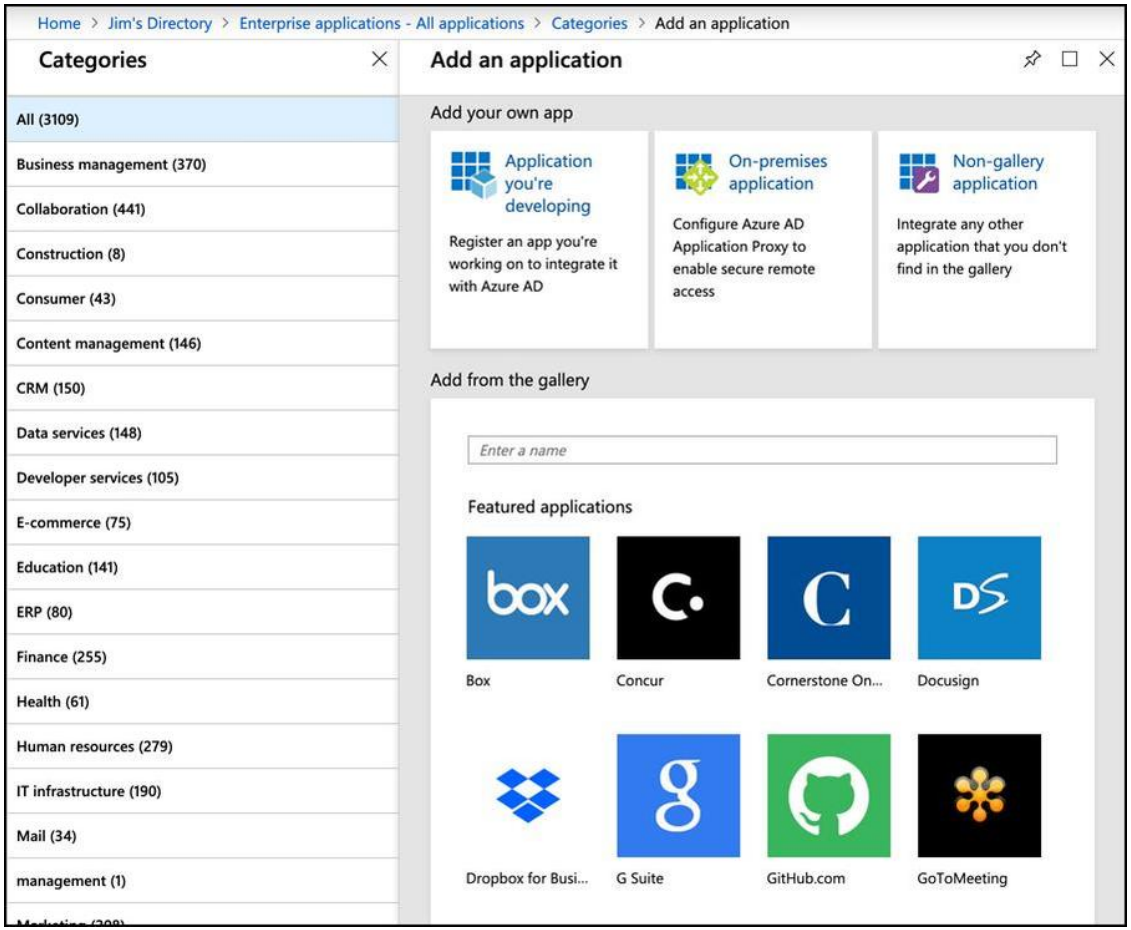


Figura 3-23 Galería de aplicaciones empresariales

Después de agregar una aplicación, puede configurar Azure AD para que los usuarios con acceso a esa aplicación puedan autenticarse con las mismas credenciales que usan para iniciar sesión en Azure AD. Este tipo de autenticación se conoce como *inicio de sesión único* (o SSO), y es uno de los beneficios clave de usar Azure AD.

 ***Consejo de examen***

Azure AD B2B le permite invitar a usuarios invitados a su Azure AD desde otras empresas. Otra característica de AD llamada Azure AD B2C le permite dar a los usuarios acceso a las aplicaciones de Azure AD iniciando sesión con cuentas existentes como una cuenta de Facebook o Google.

Otro beneficio importante de usar Azure AD para administrar el acceso de los usuarios a otras aplicaciones es que puede revocar fácilmente ese acceso desde una única interfaz. Por ejemplo, si le da a un usuario el nombre de usuario y la contraseña de su cuenta de redes sociales para que puedan publicar en su cuenta, cuando ya no quiera que ese usuario tenga acceso, tendría que cambiar el nombre de usuario y la contraseña en sus redes sociales cuenta. Sin embargo, si les otorga acceso mediante Azure AD con SSO configurado, puede eliminar ese acceso fácilmente dentro del portal de Azure. El usuario nunca tiene que saber el nombre de usuario y la contraseña que usa para la cuenta de redes sociales.

Autenticación multifactor

Todas las características de Azure AD que hemos cubierto hasta ahora están incluidas en la versión gratuita de Azure AD que obtienen todos los que tienen una suscripción de Azure. Azure AD tiene otros tres niveles de precios que no son gratuitos: Básico, Premium P1 y Premium P2. Si actualiza a uno de los planes Premium, puede habilitar la autenticación multifactor para sus usuarios.

 ***Consejo de examen***

Si usa el plan gratuito de Azure AD, tiene un subconjunto de características de MFA solo para administradores globales. Estas características le permiten habilitar MFA para administradores globales al acceder al portal de Azure y al centro de administración de Microsoft 365.

Más información **Precios de Azure Active Directory**

Para obtener más información sobre los planes de precios de Azure AD y lo que se incluye en cada uno de ellos, consulte: *https://aka.ms/aadpricing* .

De manera predeterminada, los usuarios pueden iniciar sesión en su Azure AD usando solo un nombre de usuario y contraseña. Incluso si requiere que sus usuarios usen contraseñas seguras, es arriesgado permitir el acceso a sus recursos con solo un nombre de usuario y contraseña. Si un pirata informático obtiene la contraseña mediante el uso de un software que adivina las contraseñas, o al robar si se trata de phishing u otros medios, sus recursos ya no son seguros.

La autenticación multifactor resuelve este problema. El concepto detrás de la autenticación multifactor es que debe autenticarse utilizando una combinación de:

- Algo que sabes, como un nombre de usuario y contraseña.
- Algo que tenga, como un teléfono o dispositivo móvil.
- Algo que eres, como el reconocimiento facial o una huella digital.

Si la autenticación de múltiples factores requiere estos tres, se conoce como autenticación de tres factores o, a veces, 3FA. Si solo se requieren los dos primeros, se denomina autenticación de dos factores o, a veces, 2FA. (Microsoft en realidad lo llama *verificación en dos pasos*). La autenticación de múltiples factores de Azure es autenticación de dos factores.

Nota **biométrica en dispositivos móviles**

Aunque la autenticación de múltiples factores de Azure es de dos factores, si está utilizando un dispositivo móvil que incluye características biométricas, es posible que se esté autenticando mediante la autenticación de tres factores. Sin embargo, el tercer factor es impuesto por su dispositivo móvil y no por Azure. La autenticación multifactor de Azure no requiere autenticación de tres factores.

Para habilitar la autenticación multifactor para uno o más usuarios de su Azure AD, abra la hoja Todos los usuarios y haga clic en **Autenticación multifactor** como se muestra en la Figura 3-24 .

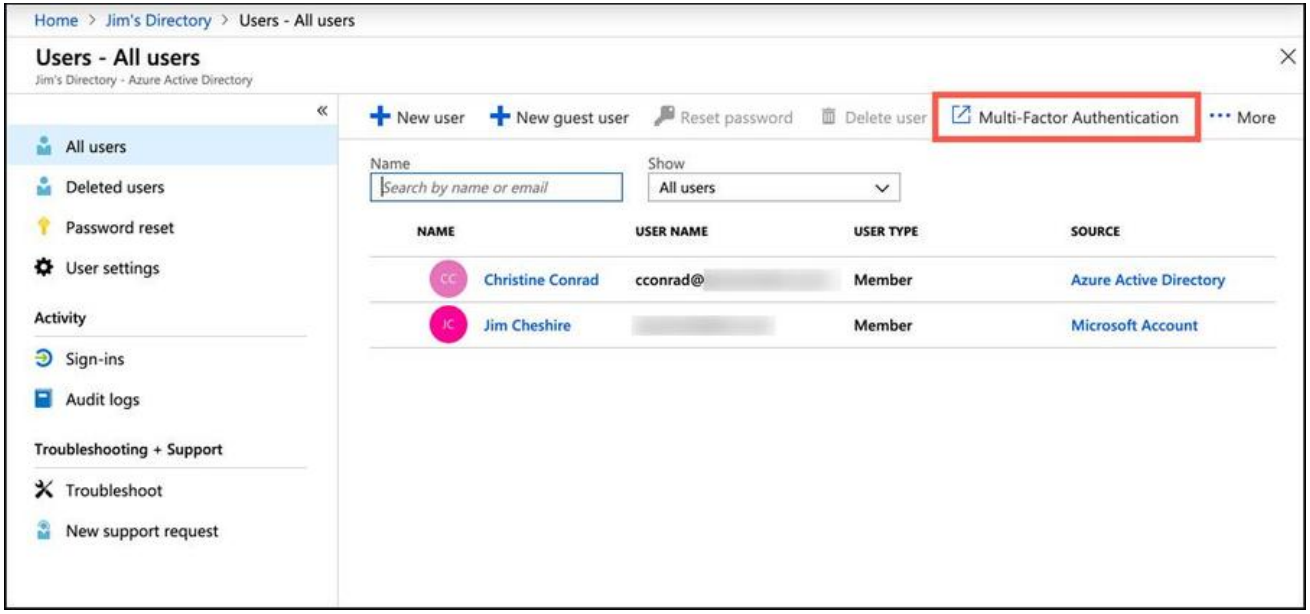


Figura 3-24 Habilitación de la autenticación multifactor

Cuando hace clic en Autenticación multifactor, se abre una nueva ventana del navegador que muestra el sitio de administración de usuarios de Azure AD. Seleccione uno o más usuarios para los que desea habilitar la autenticación multifactor y haga clic en **Habilitar** como se muestra en la Figura 3-25 .

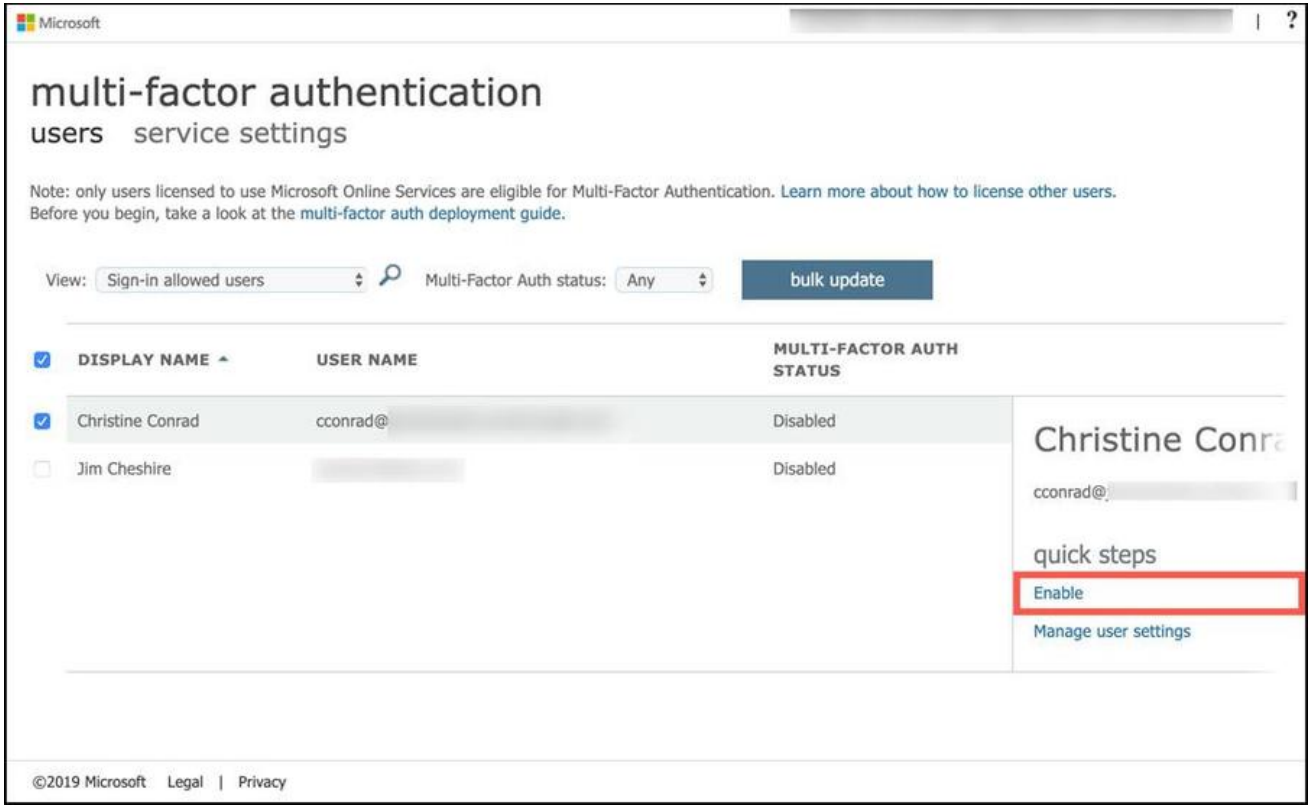


Figura 3-25 Habilitación de la autenticación multifactor

No puede habilitar la autenticación multifactor para usuarios invitados que usan este método. Si desea aplicar la autenticación multifactor para los usuarios invitados, deberá configurar el acceso condicional a su Azure AD. Para hacerlo, abra su Azure AD en el portal de Azure y haga clic en **Acceso condicional** como se muestra en la Figura 3-26 .

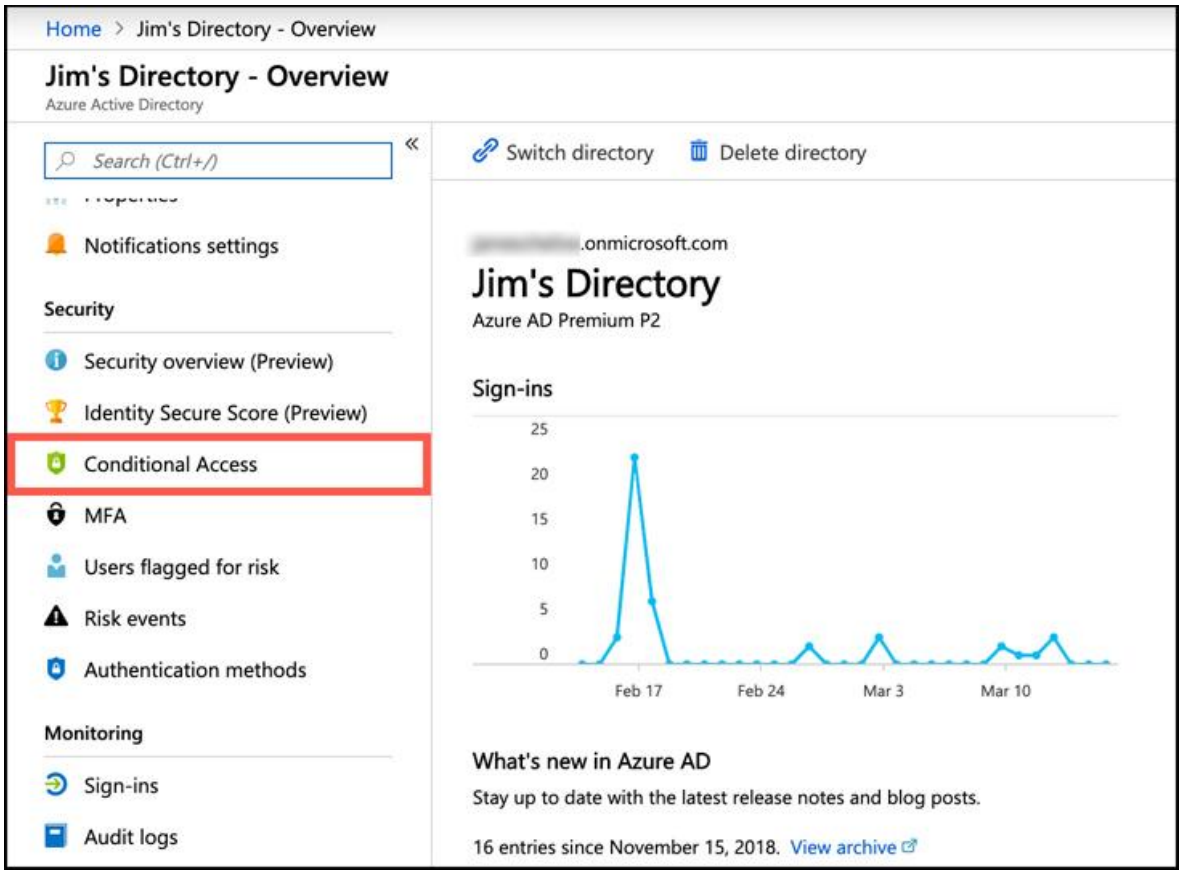


Figura 3-26 Configuración de acceso condicional

En la hoja Acceso condicional, haga clic en **Nueva política** como se muestra en la Figura 3-27 .

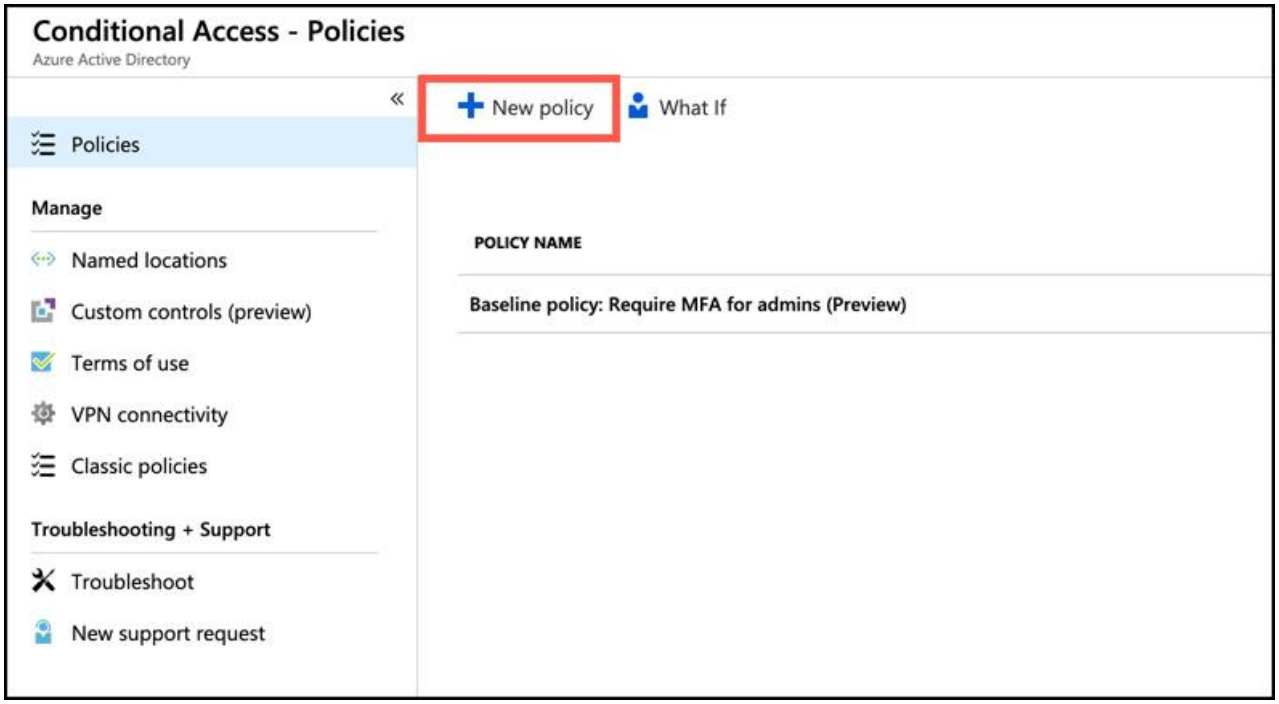


Figura 3-27 Agregar una política de acceso condicional

Ingrese un nombre para la nueva política y haga clic en **Usuarios y grupos** en Asignaciones. Haga clic en el botón de **selección Seleccionar usuarios y grupos** y marque la casilla de verificación **Todos los usuarios invitados** . Luego haga clic en **Listo** como se muestra en la Figura 3-28 .

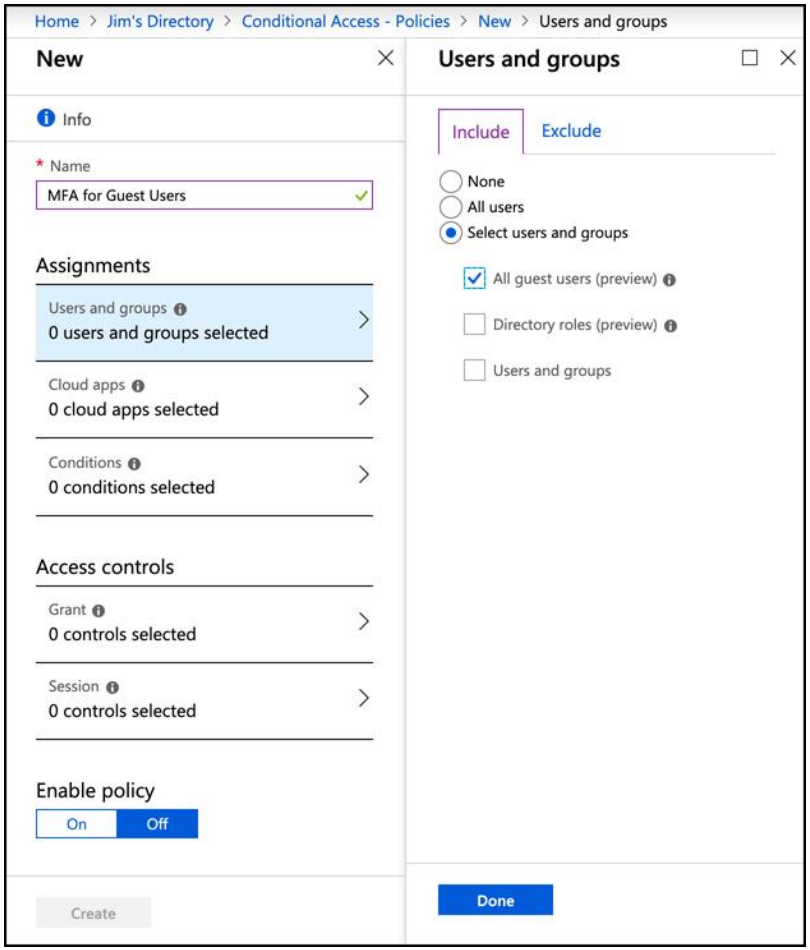


Figura 3-28 Configuración de una política para usuarios invitados

Ahora debe configurar a qué aplicación se aplica esta política. Para hacerlo, siga estos pasos como se muestra en la Figura 3-29 .

1. Haz clic en **Aplicaciones en la nube** .
2. Haga clic en el botón de **opción Seleccionar aplicaciones** .
3. Haz clic en **Seleccionar** .
4. Seleccione la **aplicación Microsoft Azure Management** .
5. Haz clic en **Seleccionar** .

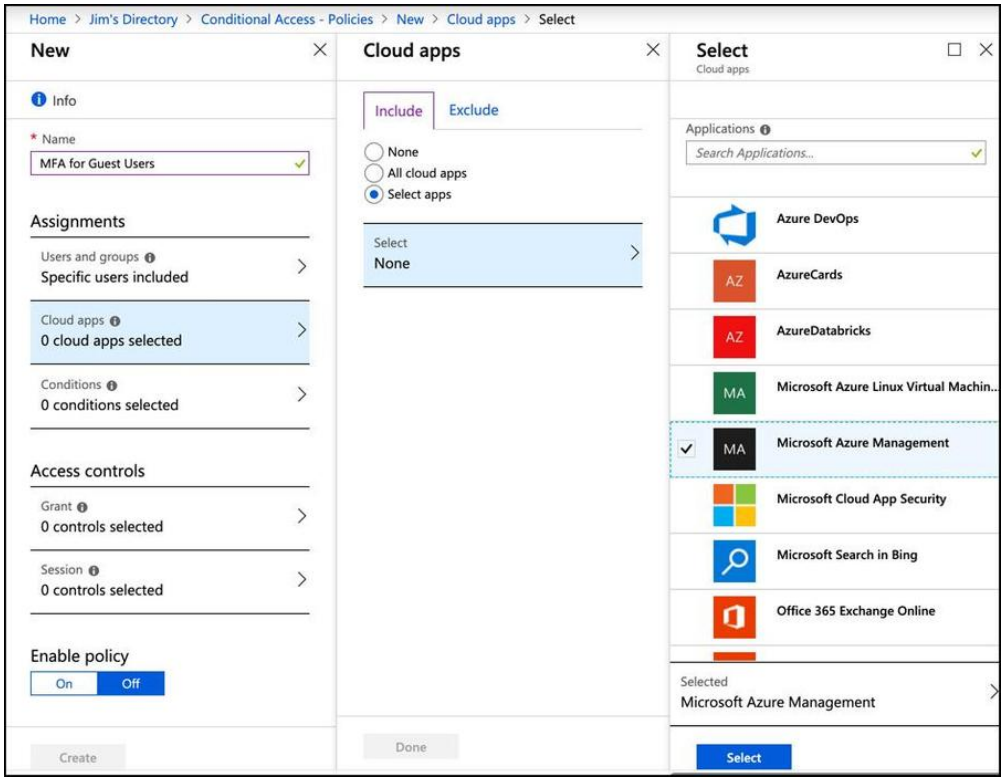


Figura 3-29 Agregar la aplicación Microsoft Azure Management a la política

Consejo de examen

El acceso condicional requiere un plan Premium para Azure AD.

Para agregar un requisito de autenticación multifactor a la política, haga clic en **Conceder** en Controles de acceso como se muestra en la Figura 3-30 . Haga clic en **Conceder acceso** y marque la casilla de verificación **Requerir autenticación** multifactor. Luego deberá hacer clic en **Seleccionar** para agregar el control de acceso. Finalmente, habilite la política y haga clic en **Crear** para finalizar el proceso.

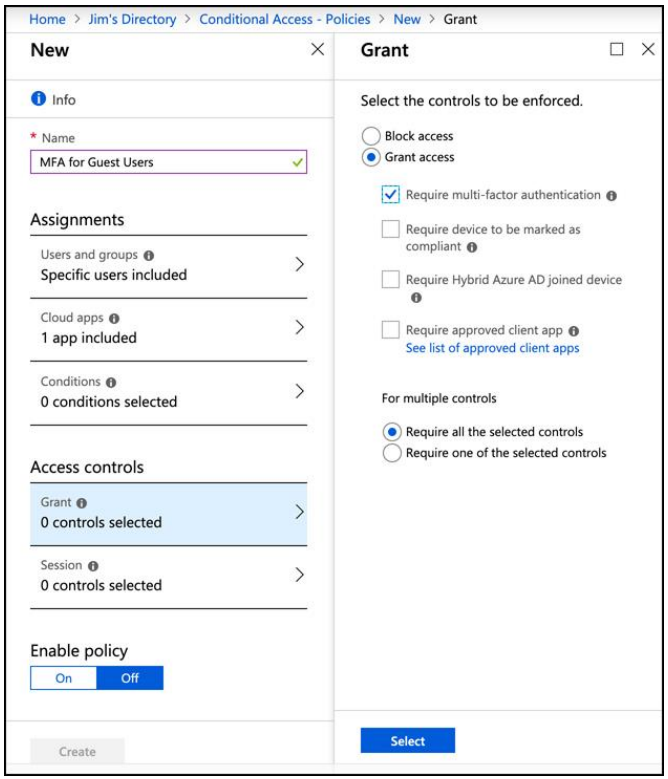


Figura 3-30 Configuración de una política para requerir autenticación de múltiples factores

HABILIDAD 3.3: DESCRIBIR LAS HERRAMIENTAS Y CARACTERÍSTICAS DE SEGURIDAD DE AZURE

Las amenazas a sus datos y recursos pueden originarse desde cualquier lugar. Algunas amenazas son externas, como los piratas informáticos que intentan acceder de forma remota a sus máquinas virtuales adivinando las contraseñas de administrador. Otras amenazas, como que los empleados no cumplan con las mejores prácticas de seguridad, pueden venir desde adentro. Garantizar la seguridad de sus recursos en la nube puede ser un desafío, y a medida que la cantidad de recursos de Azure que ha implementado aumenta con el tiempo, ese desafío puede crecer exponencialmente.

Esta sección cubre:

- Centro de seguridad de Azure
- Azure Key Vault
- Protección de la información de Azure
- Protección contra amenazas avanzada de Azure

Centro de seguridad de Azure

Azure Security Center es un servicio en Azure que le ofrece un portal único para monitorear y administrar la seguridad de sus recursos de Azure. También puede agregar recursos locales a Security Center instalando un agente de Security Center en sus recursos locales.

El Centro de seguridad ofrece dos niveles de servicio. El nivel gratuito proporciona evaluación general y recomendaciones para proteger sus recursos de Azure y cubre solo máquinas virtuales de Azure y el Servicio de aplicaciones de Azure. El nivel estándar agrega cobertura de sus bases de datos SQL Azure, bases de datos MySQL, PostgreSQL y almacenamiento de blobs de Azure, así como características adicionales como detección avanzada de amenazas, análisis de Microsoft Threat Intelligence y la capacidad de administrar el cumplimiento normativo de sus recursos de Azure . El nivel estándar se factura por hora, y los detalles completos sobre los precios se pueden encontrar en *https://azure.microsoft.com/en-us/pricing/details/security-center* .

Para comenzar con Security Center, haga clic en **Security Center** en el menú en Azure Portal. Esto lo llevará a la hoja Descripción general, donde puede ver una descripción general de todos sus recursos protegidos por Security Center como se muestra en la Figura 3-31 .

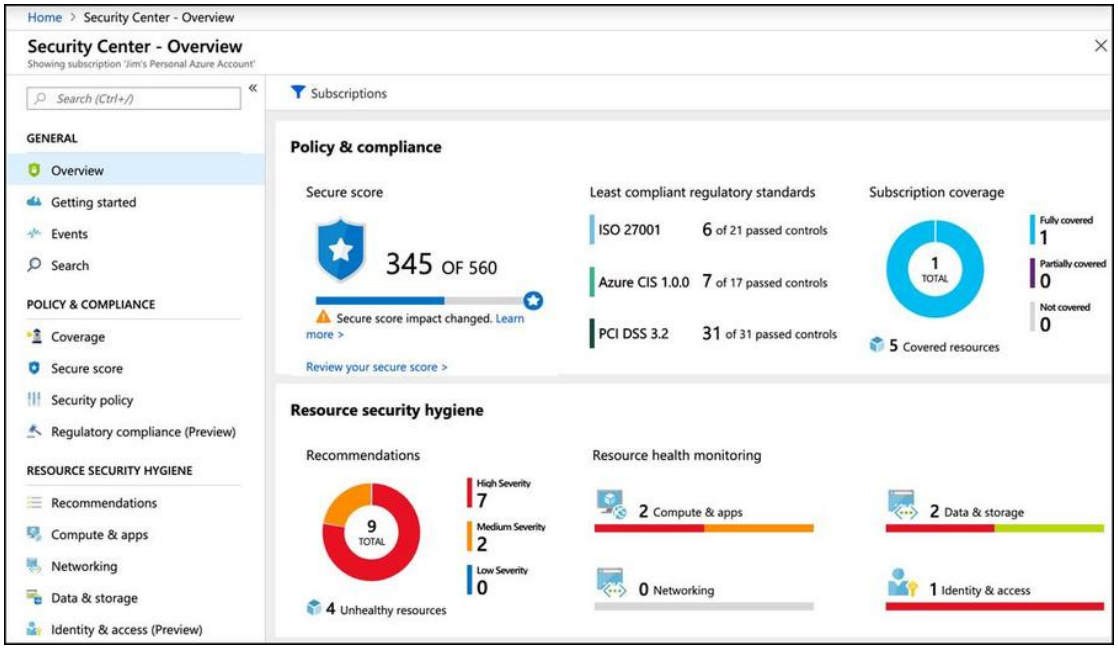


Figura 3-31 Centro de seguridad de Azure

Hay tres áreas principales de cobertura en Security Center.

- **Política y cumplimiento** Proporciona una puntuación segura y general de la seguridad de sus recursos. Esta área también cubre su cumplimiento con los estándares regulatorios.
- **Higiene de seguridad de recursos** Proporciona una visión general de alto nivel de la salud de sus recursos desde una perspectiva de seguridad. Los problemas de seguridad se clasifican en severidad alta, media o baja.
- **Protección contra amenazas** Le muestra cualquier ataque o amenaza activa o pasada en sus recursos.

La información para las dos primeras áreas es proporcionada por el servicio protegido. Esta información a menudo está relacionada con las mejores prácticas. La protección contra amenazas, por otro lado, está específicamente dirigida a analizar tanto el tráfico de red como el comportamiento de los usuarios de sus recursos. Si algo parece sospechoso, lo informa Security Center.

Microsoft Threat Intelligence se usa para identificar amenazas de seguridad. Threat Intelligence utiliza los datos históricos de Microsoft y el aprendizaje automático para identificar posibles amenazas. Estas amenazas podrían ser un hacker que intenta obtener acceso a un recurso, o podrían estar relacionadas con actividades sospechosas realizadas por un usuario. Por ejemplo, si un usuario eleva sus privilegios en una VM y ejecuta un proceso desconocido, eso probablemente se marcaría como un incidente que debería investigarse.

Más información **Protección avanzada contra amenazas**

La información de protección contra amenazas se obtiene mediante Azure Advanced Threat Protection. Aprenderá más sobre Protección contra amenazas avanzada más adelante en esta habilidad.

Al hacer clic en un elemento en la hoja Descripción general, puede profundizar en más detalles. En la Figura 3-32 , hemos hecho clic en **Compute & Apps** en la hoja Descripción general. Puede ver todas las recomendaciones para las máquinas virtuales, el servicio de aplicaciones, los servicios en la nube y los recursos del contenedor. También puede ver cuánto mejorará su puntaje seguro si aborda cada recomendación.

Figura 3-32 Descripción general de todas las recomendaciones de Azure Compute en Security Center

Al hacer clic en una de las recomendaciones, se proporcionará información adicional. En la mayoría de los casos, verá un enlace a instrucciones sobre cómo puede abordar la recomendación, pero Security Center tiene la capacidad de encargarse automáticamente de las recomendaciones. Por ejemplo, al hacer clic en la recomendación de Instalar Endpoint Protection en mis máquinas virtuales, se accede a la pantalla que se muestra en la Figura 3-33 .

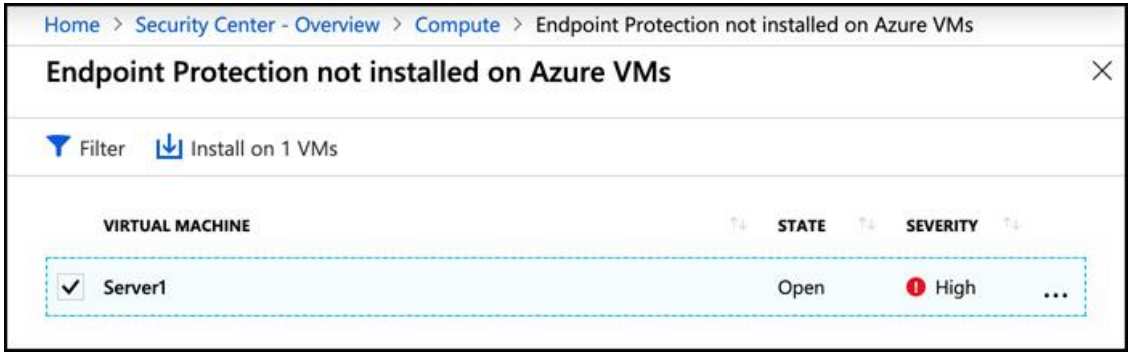


Figura 3-33 Detalles sobre una recomendación del Centro de seguridad

Desde aquí, puede hacer clic en Instalar en máquinas virtuales 1 para instalar automáticamente la protección de punto final directamente desde el Centro de seguridad. En este escenario, solo tenemos una VM, pero puede imaginar lo útil que sería esta capacidad si tuviera cientos de VM ejecutándose en Azure. Con solo hacer clic en un botón, puede instalar protección de punto final en todos ellos.

Una de las mayores amenazas de seguridad para sus recursos en la nube son los puertos de red abiertos en sus máquinas virtuales. El acceso a sus máquinas virtuales mediante el escritorio remoto para máquinas virtuales de Windows, o SSH para máquinas virtuales Linux, es una parte necesaria de la administración de esos recursos, pero los piratas informáticos suelen utilizar los puertos de red utilizados para la administración remota para entrar en las máquinas virtuales. Security Center proporciona una característica llamada acceso justo a tiempo (JIT) que ayuda a proteger sus máquinas virtuales de ataques en puertos de administración.

Cuando el acceso JIT está habilitado, los usuarios deben solicitar acceso a una VM para poder acceder a ella de forma remota. Hasta que alguien tenga acceso a JIT, los puertos de administración en la VM están cerrados para que no se pueda acceder a ellos. Una vez que se le da acceso a JIT a un usuario, los puertos están abiertos durante un período de tiempo específico según lo solicitado por el usuario. Una vez transcurrido ese período de tiempo, los puertos de administración se vuelven a cerrar.

Para habilitar el acceso JIT en una VM, haga clic en **Just In Time VM Access** en Security Center, como se muestra en la Figura 3-34 . Haga clic en la pestaña Recomendado para ver las máquinas virtuales que actualmente no están configuradas para el acceso JIT. Seleccione una o más máquinas virtuales y haga clic en **Habilitar JIT** para activar la función.

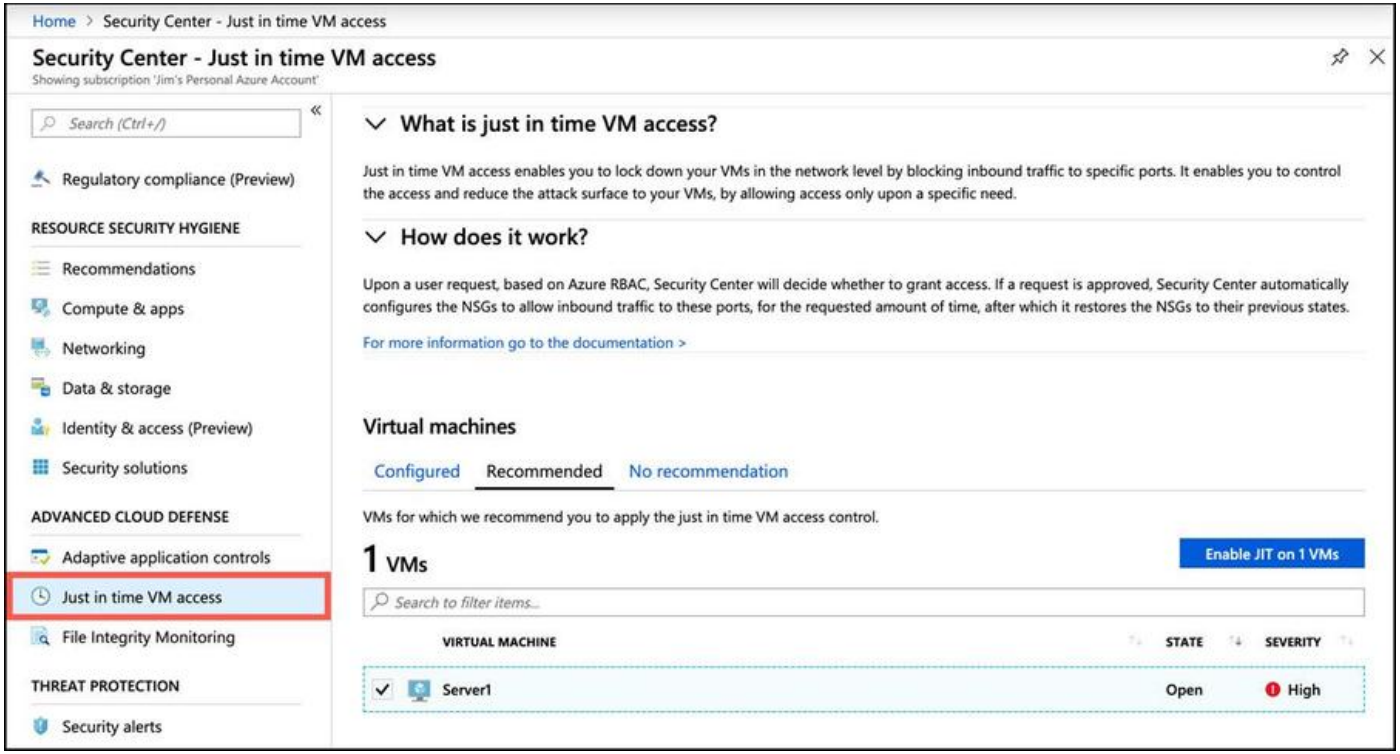


Figura 3-34 Habilitación del acceso JIT en una VM

Al habilitar el acceso JIT, puede elegir qué puertos desea proteger como se muestra en la Figura 3-35 . Se enumeran los puertos recomendados para la administración, pero puede agregar sus propios puertos. Por ejemplo, si ha cambiado la configuración de su VM para que la administración se realice en un puerto no típico, puede agregar ese puerto para el acceso JIT.

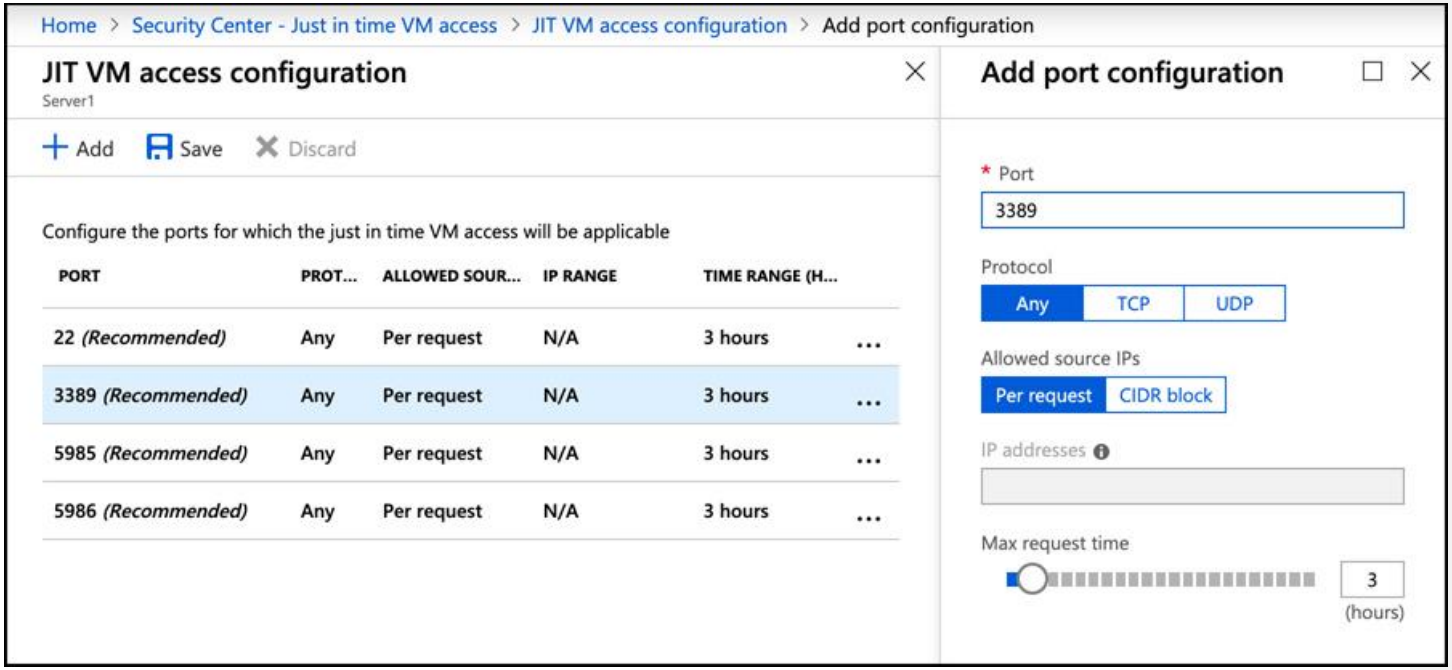


Figura 3-35 Configuración de acceso JIT

Además de especificar el puerto, también puede controlar qué protocolos están permitidos en el puerto y qué direcciones IP están permitidas. Si las IP permitidas se establecen en **Por solicitud** , el usuario que solicita acceso tendrá la opción de especificar una dirección IP o un bloque CIDR. De lo contrario, puede especificar un bloque CIDR usted mismo para permitir el acceso solo desde un rango específico de direcciones IP.

Cuando un usuario solicita acceso, se puede especificar la cantidad de horas que se le da acceso hasta la cantidad máxima de horas que especifique en la configuración del puerto. El tiempo máximo de solicitud se puede configurar en cualquier lugar de 1 a 24 horas.

Una vez que una VM está configurada para el acceso JIT, los usuarios solicitan acceso desde el interior del Centro de seguridad. Después de hacer clic en **Just in Time VM Access** , seleccione la VM y haga clic en **Solicitar acceso** como se muestra en la Figura 3-36 .

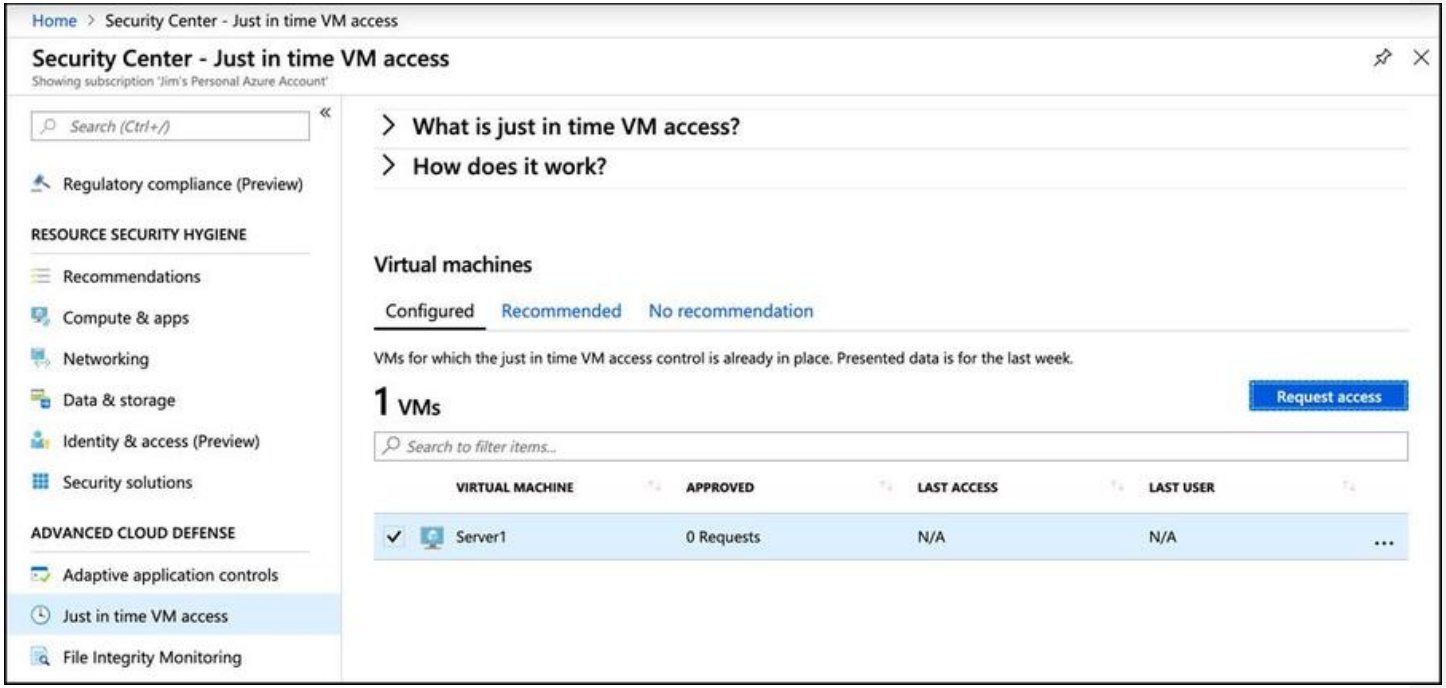


Figura 3-36 Solicitud de acceso JIT

Como se muestra en la Figura 3-37 , los usuarios que solicitan acceso deben especificar qué puertos abrir, las direcciones IP que están permitidas (suponiendo que no se especificaron cuando se habilitó el acceso JIT para la VM) y cuánto tiempo se necesita acceso, hasta El tiempo máximo configurado. Una vez que se hace clic en **Abrir puertos** , los puertos solicitados permanecerán abiertos durante el período especificado.

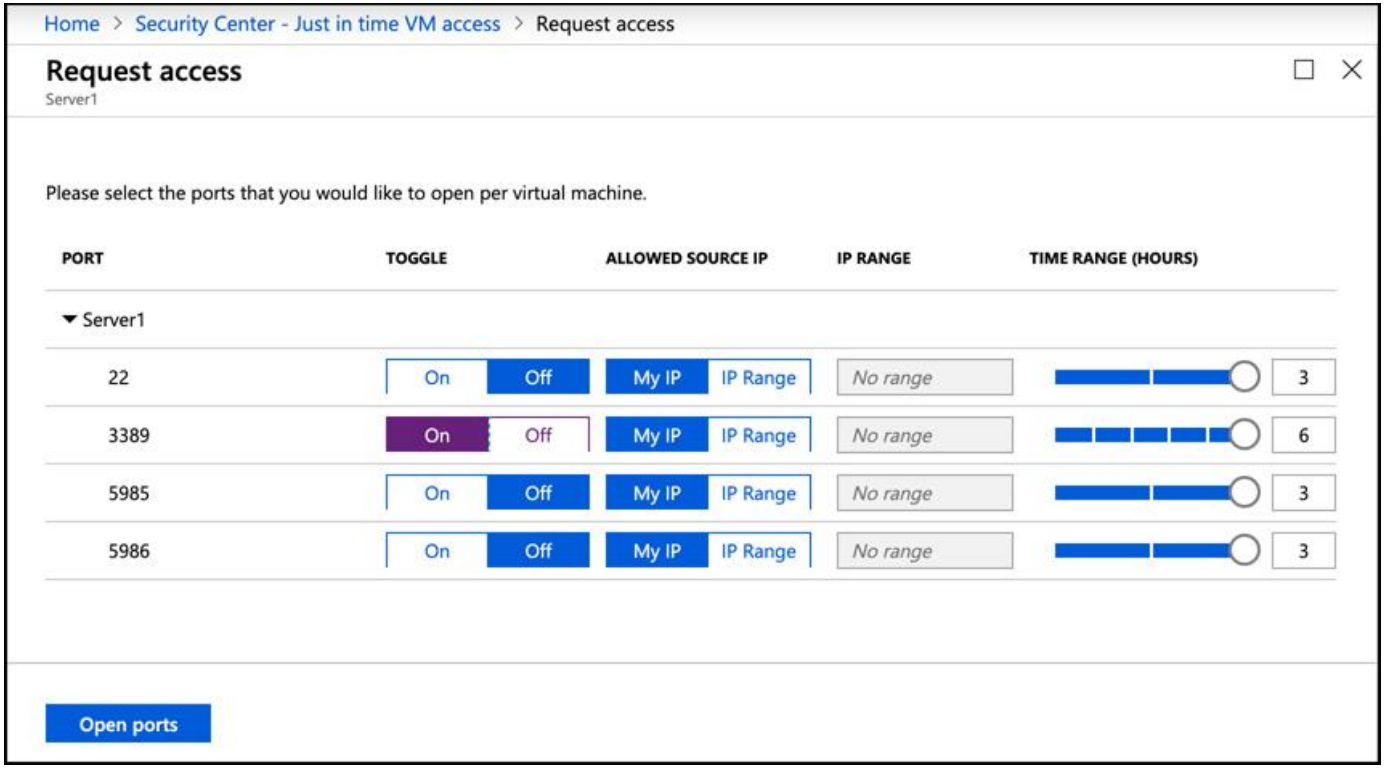


Figura 3-37 Detalles de una solicitud de acceso JIT

Azure Key Vault

La mayoría de las aplicaciones utilizan información confidencial o secreta. Por ejemplo, una aplicación que usa una base de datos necesita saber cómo conectarse a esa base de datos, y esa información de conexión se almacena en una cadena de conexión. La cadena de conexión puede contener un nombre de usuario y una contraseña que protegen la base de datos, y almacenar ese nombre de usuario y contraseña en un archivo de texto claro sería un riesgo de seguridad obvio.

Azure Key Vault proporciona una forma segura de almacenar secretos, claves y certificados. Una vez que un elemento se almacena en Key Vault, puede aplicar políticas de seguridad que definen qué usuarios y aplicaciones pueden acceder a él. Key Vault se cifra utilizando claves de cifrado, pero Microsoft no tiene visibilidad de las claves de cifrado ni de los datos cifrados.

Las Bóvedas clave se crean en Azure Portal como se muestra en la Figura 3-38 .

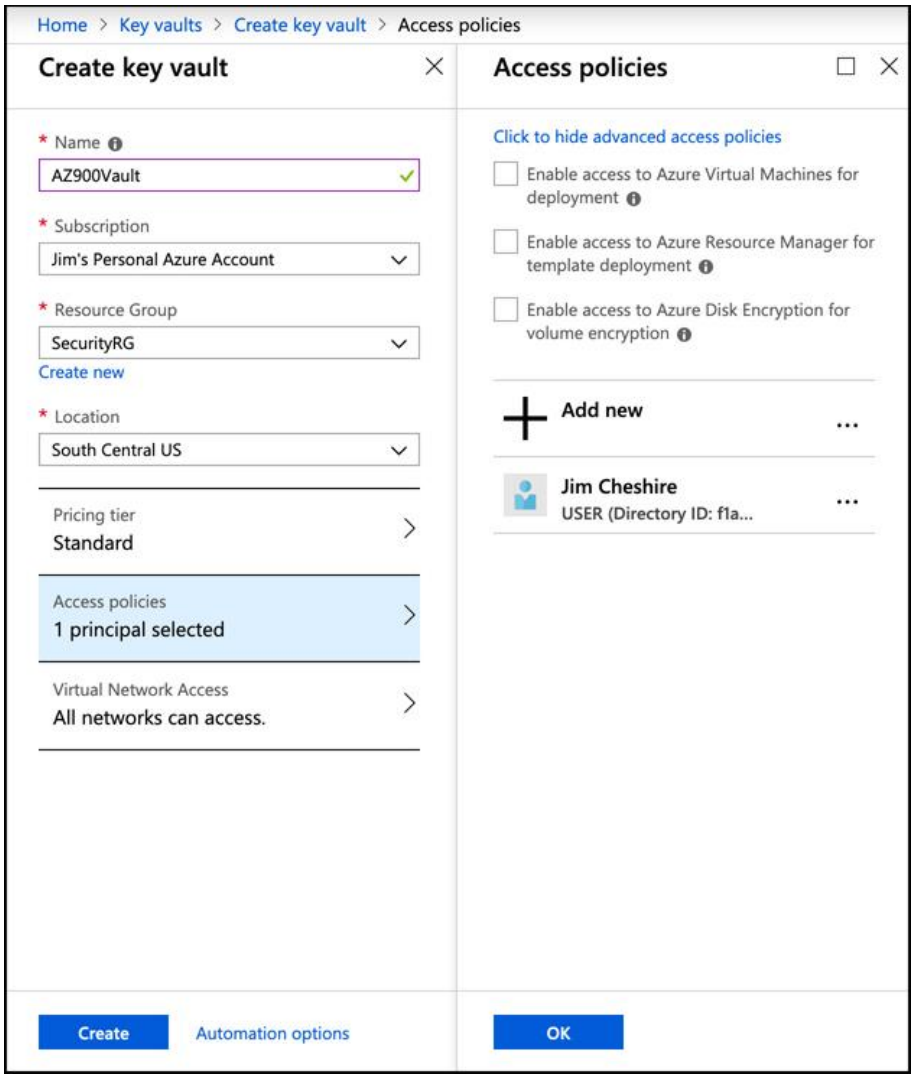


Figura 3-38 Creación de un almacén de claves

Hay dos niveles de precios disponibles en Key Vault: Standard y Premium. La única diferencia entre los dos es que las claves se almacenan en módulos de seguridad de hardware (HSM) en el nivel Premium. Un HSM es una pieza de hardware separada que está diseñada para almacenar de forma segura contenido cifrado, y también está especializada para procesar datos criptográficos.

Consejo de examen

Se requiere mantener las claves de cifrado en un límite HSM para el Estándar Federal de Procesamiento de Información (FIPS) 140-2, por lo que las empresas que necesitan cumplir con FIPS 140-2 pueden hacerlo utilizando el nivel Premium de Key Vault.

Puede importar una clave, secreto o certificado en Key Vault, pero Key Vault también puede generar claves de seguridad y certificados para usted. Por ejemplo, es posible que desee generar una clave de seguridad que su empresa pueda usar para firmar certificados. Si desea generar una clave de seguridad de 4.096 bits para este propósito y almacenarla en Key Vault, haga clic en **Claves** y luego en **Generar / Importar** como se muestra en la Figura 3-39 .

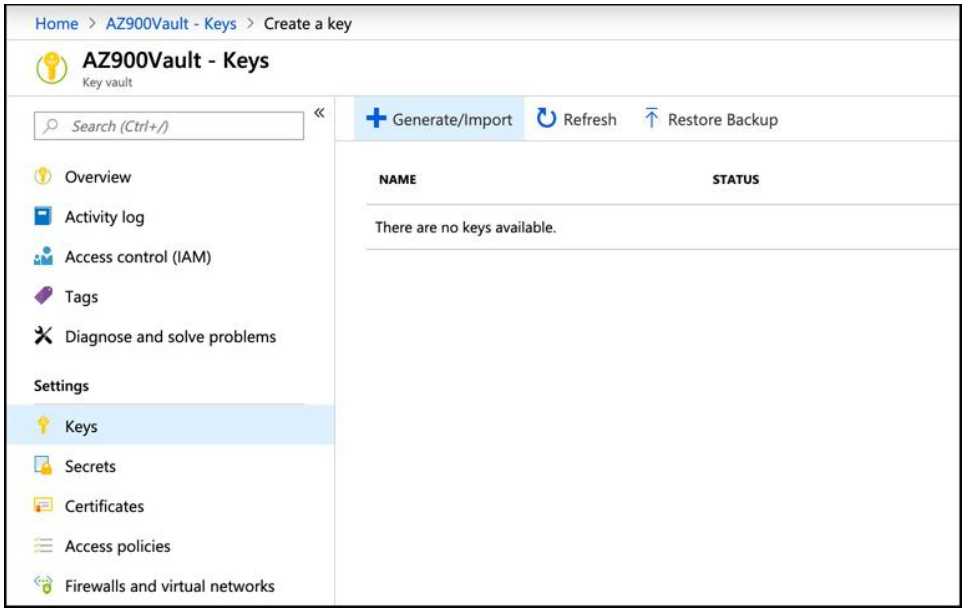


Figura 3-39 Agregar una clave a Key Vault

En la Figura 3-40 , se genera y almacena una clave RSA de 4.096 bits en Key Vault.

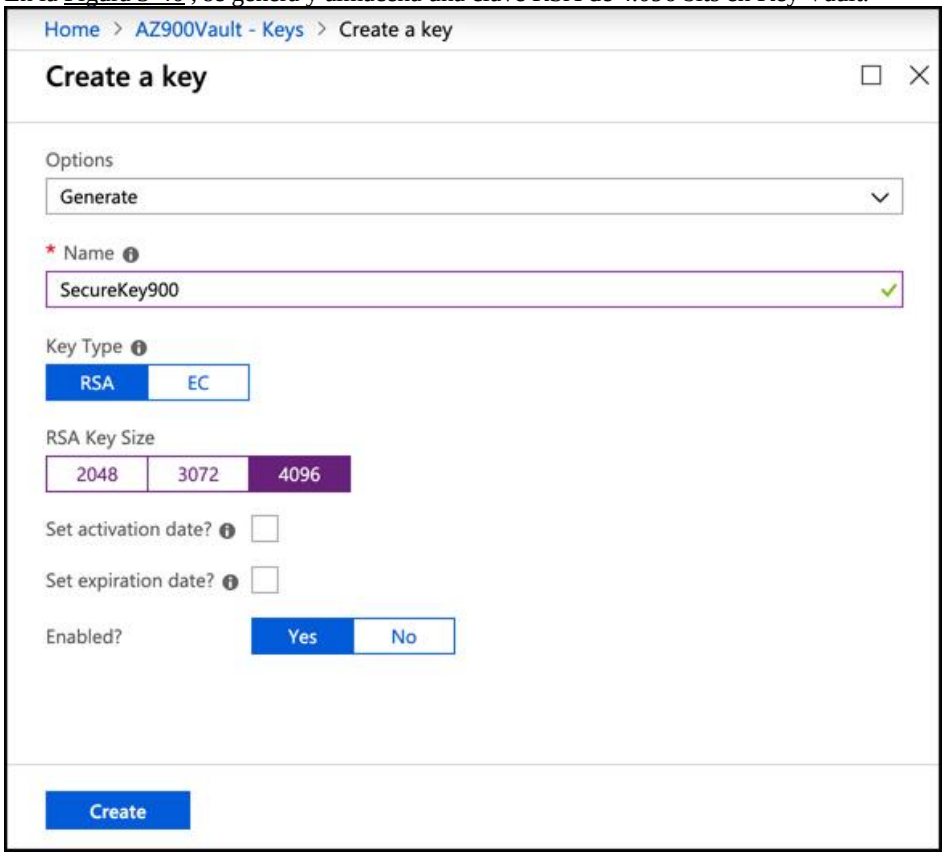


Figura 3-40 Generando una clave RSA

Como se muestra en la Figura 3-41 , una vez que la clave ha sido almacenada, puede ver la entrada para obtener el identificador de la clave, una URL que los usuarios o las aplicaciones autorizadas pueden utilizar para recuperar la clave. Sin embargo, no puede ver la clave porque está encriptada y no está disponible, excepto a través del identificador de clave.

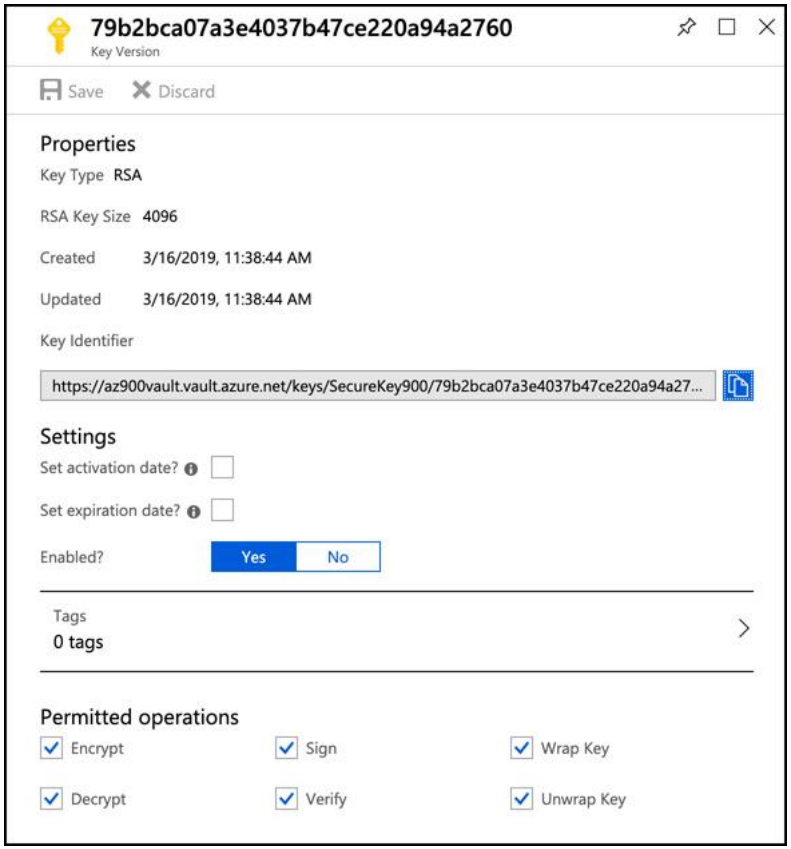


Figura 3-41 Detalles sobre una clave

Consejo de examen

Por lo general, una aplicación accede a una clave almacenada en Azure Key Vault mediante programación. Para proteger la clave, los desarrolladores de aplicaciones pueden recuperar la clave cada vez que la necesiten en lugar de recuperarla una vez y almacenarla en la memoria. Esto asegura que la clave permanezca segura.

Otro escenario de uso común para Key Vault es almacenar claves de cifrado para máquinas virtuales de Azure. Una de las recomendaciones de seguridad ofrecidas por Security Center es cifrar discos VM. Un disco VM se almacena como un archivo VHD, y cuando se cifra, el sistema operativo host que ejecuta la VM debe poder acceder a la clave de seguridad para descifrar el VHD y ejecutar la VM. Key Vault ofrece capacidades que están específicamente dirigidas a este tipo de escenario.

Para utilizar Key Vault para claves de cifrado de disco, las políticas de acceso deben configurarse para permitir la bóveda para el cifrado de disco. Si esto no se hizo cuando se creó la bóveda, puede cambiarla haciendo clic en **Políticas de acceso** y marcando la opción para habilitar el acceso a Azure Disk Encryption como se muestra en la Figura 3-42 .

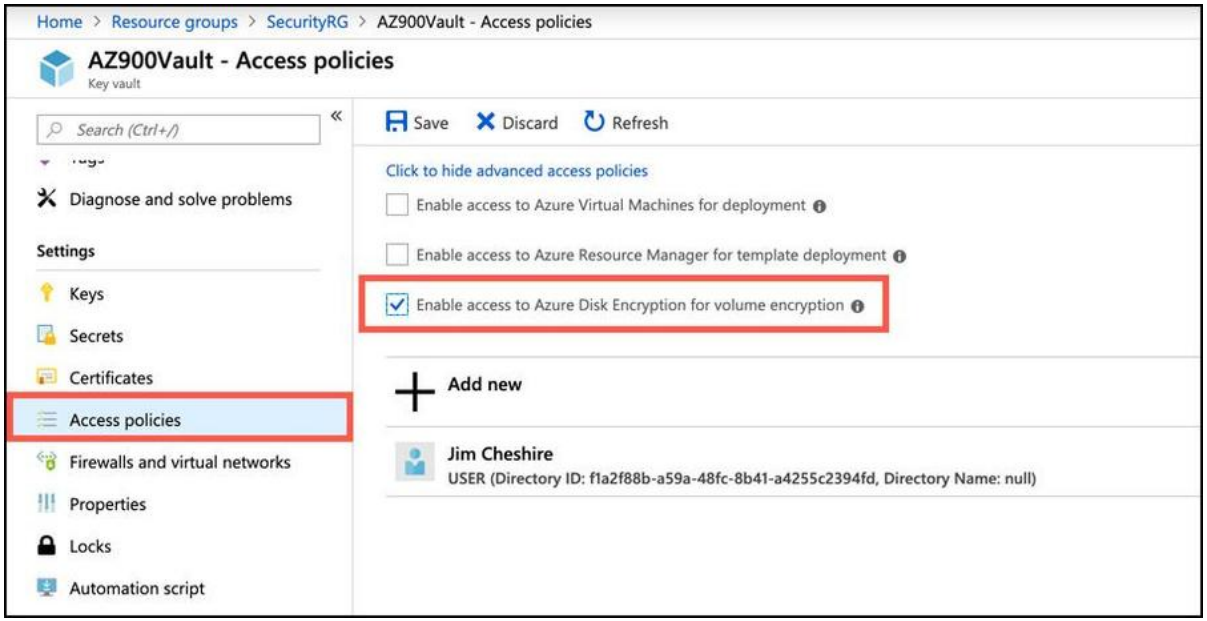


Figura 3-42 Configuración de políticas de acceso para permitir el acceso a Azure Disk Encryption

Azure Disk Encryption está habilitado en sus máquinas virtuales mediante Azure PowerShell o la interfaz de línea de comandos (CLI) de Azure.

Más información **HABILITAR LA ENCRIPTACIÓN**

Para habilitar el cifrado y almacenar las claves en Key Vault, sus máquinas virtuales y Key Vault deben estar en la misma suscripción de Azure, y deben estar en la misma región de Azure. Para obtener más detalles sobre los requisitos de cifrado de disco y los pasos para habilitarlo, consulte: *https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites* .

Protección de la información de Azure

Soluciones como Azure Key Vault son efectivas para garantizar que la información que nunca abandona su control sea segura. A menudo hay situaciones en las que se comparte información confidencial o confidencial fuera de su empresa. Para esas situaciones, Azure Information Protection (o AIP) puede ayudarlo a mantener la información bajo su control.

AIP protege los correos electrónicos y documentos de Microsoft Office de llegar a manos equivocadas. Al configurar diferentes clasificaciones para correos electrónicos y otros documentos, y luego especificar restricciones que se aplican a cada clasificación, una empresa puede garantizar que la información no se comparta en exceso o que la información confidencial no salga de la empresa.

En la Figura 3-43 , se envía un correo electrónico que contiene un número de tarjeta de crédito. Para evitar que alguien use indebidamente mi tarjeta de crédito, puede usar AIP para clasificar el correo electrónico de modo que solo el destinatario que especificó pueda leerlo.

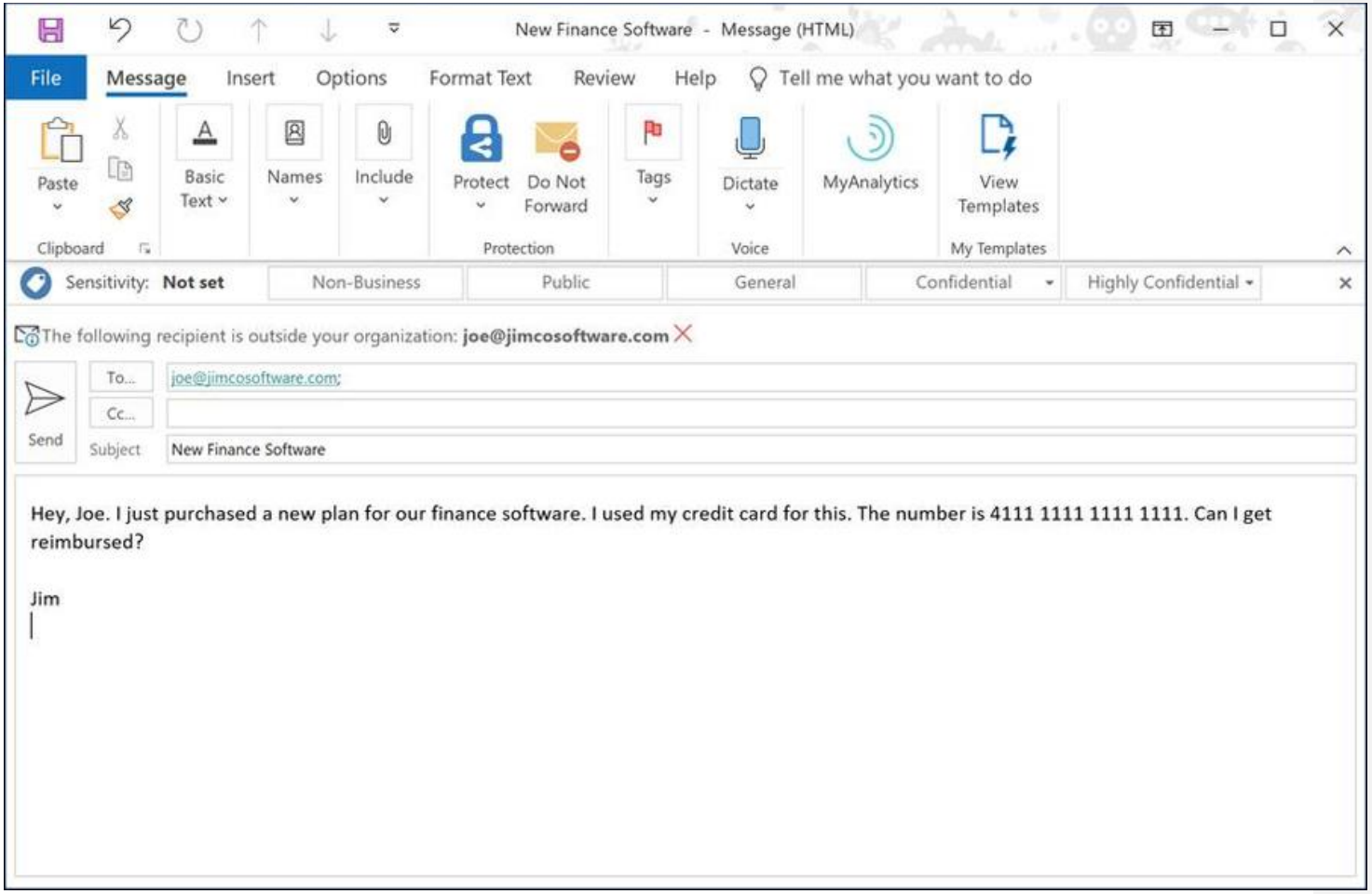


Figura 3-43 Un correo electrónico confidencial que contiene información confidencial

El botón Proteger en Microsoft Outlook le permite clasificar y proteger fácilmente su correo electrónico. Al hacer clic en el botón **Proteger** , como se muestra en la Figura 3-44 , puede marcar este correo electrónico para que solo el destinatario pueda leerlo.

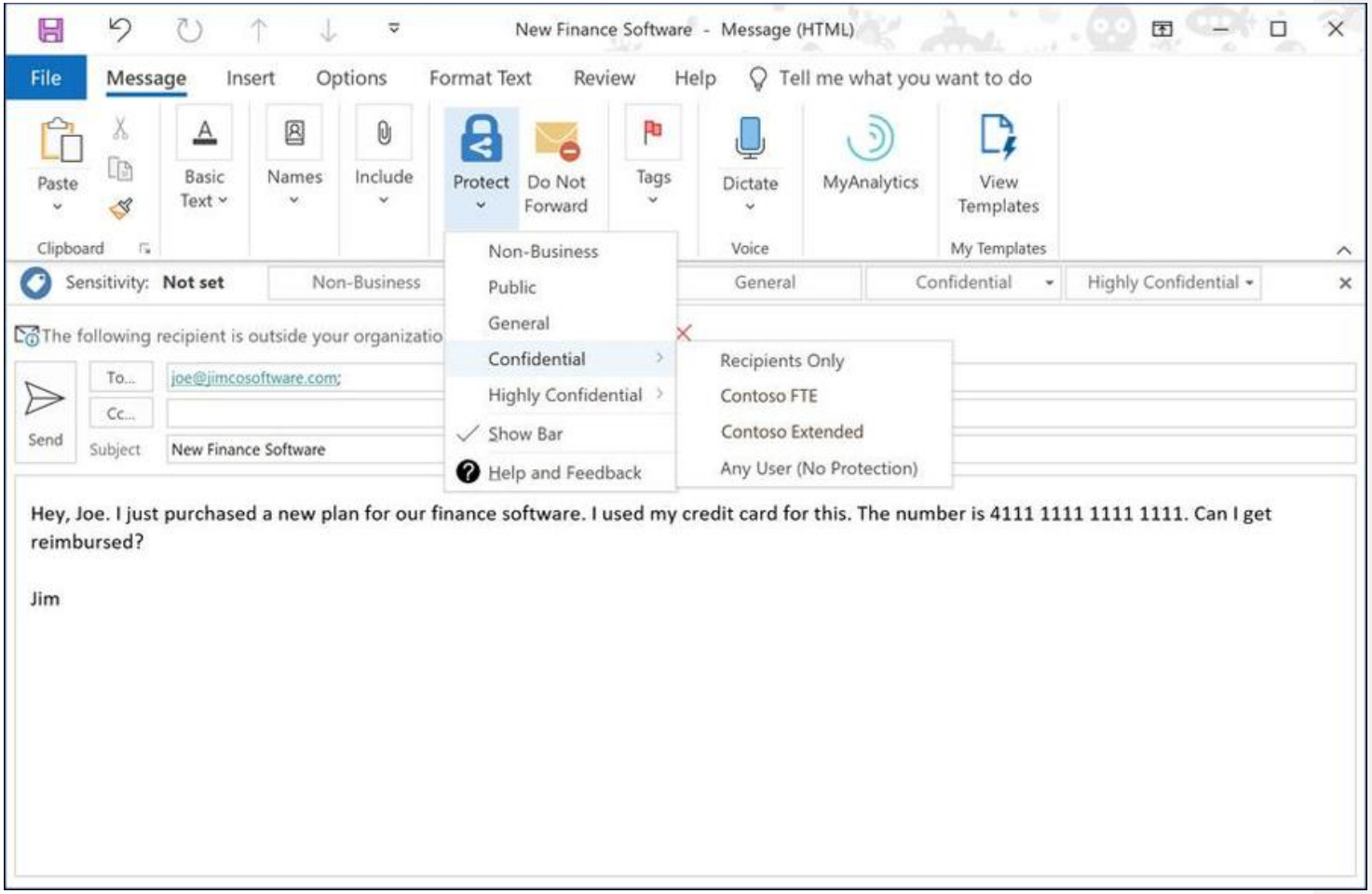


Figura 3-44 Un correo electrónico confidencial que contiene información confidencial

Este mensaje puede ser leído por un destinatario que usa Microsoft Outlook. Si el destinatario no está utilizando Microsoft Outlook, estará disponible un enlace para leer el mensaje, como se muestra en la Figura 3-45 . Al hacer clic en ese enlace, se enviará al usuario un código de acceso de un solo uso que puede ingresar para leer el mensaje de correo electrónico en Office 365 en un navegador web. Este código de acceso funcionará incluso si el usuario no es suscriptor de Office 365.

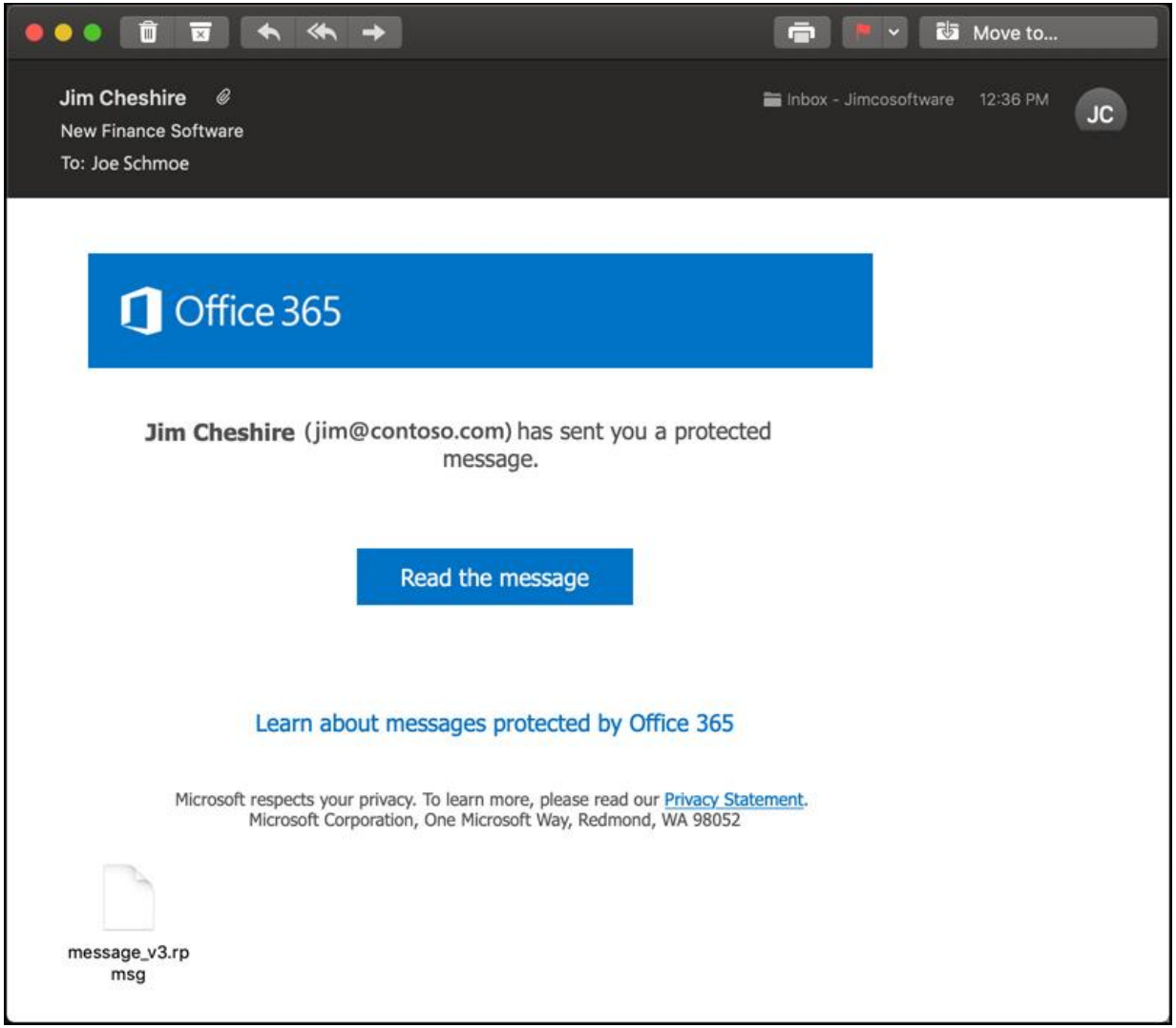


Figura 3-45 Abrir un mensaje protegido

Consejo de examen

Como se mencionó anteriormente, AIP también se puede utilizar para proteger documentos de Office de la misma manera. Incluso puede controlar si los usuarios pueden editar el documento o simplemente leer su contenido. Si un usuario no tiene la aplicación de Office utilizada para crear el documento, se abrirá en Office Online en un navegador web.

Protección contra amenazas avanzada de Azure

Aprendió sobre algunos de los servicios de Azure diseñados para proteger sus recursos de Azure de ataques a la red, y aquellos diseñados para proteger contra ataques en sus máquinas virtuales y aplicaciones que se ejecutan en la nube. Sin embargo, uno de los vectores de ataque más comunes (y uno que a menudo es más difícil de detectar) es un ataque a la identidad de un usuario dentro de su entorno local o mediante otros dispositivos que los empleados usan para conectarse a su red. Los ataques a sus recursos en la nube a menudo se inician en las instalaciones o en dispositivos móviles donde el objetivo puede no ser tan duro.

Estos tipos de ataques son difíciles de detectar porque a menudo parecen tráfico legítimo. Los piratas informáticos ingresarán a su entorno en una máquina utilizando credenciales robadas, y se moverán lateralmente a través de su infraestructura para intentar acceder a sistemas adicionales y datos confidenciales. Los dispositivos móviles también son un vector de ataque común porque pueden conectarse a redes inseguras.

Azure Advanced Threat Protection (o ATP) está disponible como parte de la suite Enterprise Mobility + Security 5 de Microsoft. También puede comprarlo con una licencia independiente. ATP está diseñado para identificar y mitigar las amenazas de identidad en su entorno local y en dispositivos que se conectan a su entorno.

Implementar ATP en su entorno es un proceso de varios pasos.

Paso 1: determinar la capacidad

ATP recopila información en su red, servidores y entorno utilizando el software que instala llamado *sensor ATP* . Para planificar su capacidad ATP, debe determinar cuántos sensores necesita y de qué tamaño deben ser esos sensores. (El tamaño del sensor se basa en el volumen del tráfico de red en su entorno).

Microsoft tiene una guía sobre cómo planificar su capacidad ATP en: *https://docs.microsoft.com/azure-advanced-threat-protection/atp-capacity-planning* .

Paso 2: crear una instancia de Azure ATP

Los sensores ATP que instale localmente se conectarán a una instancia ATP de Azure en la nube. Ahí es donde almacenarán todos los datos que se recopilan para realizar análisis y detección de amenazas.

Su instancia de Azure ATP se crea navegando al portal de Azure ATP en *https://portal.atp.azure.com* . Necesitará una licencia ATP de Azure para acceder a este sitio.

Paso 3: conecte ATP a Active Directory local

Azure ATP se conecta a su Active Directory local para obtener información sobre su entorno y sus usuarios. También puede conectarse a un Active Directory de varios bosques.

Los detalles completos sobre cómo conectar ATP a su Active Directory están disponibles en: *https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step2* .

Paso 4: descargue, instale y configure los sensores ATP

Los sensores ATP están disponibles en un paquete de Microsoft. Una vez que descargue e instale el sensor ATP, deberá configurarlo antes de comenzar a ver los datos.

Puede encontrar detalles sobre la instalación y configuración del sensor ATP en: *https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step3* .

Una vez instalado y configurado, ATP puede usar sus análisis y aprendizaje automático para identificar qué es normal y qué no, y lo hace en tiempo real. Si ocurre un ataque, ATP puede proporcionar herramientas a su departamento de TI para investigar la naturaleza del ataque y tomar las medidas apropiadas.

Consejo de examen

ATP representa un ecosistema completo en Microsoft a través de varias ofertas. Office 365 ATP está diseñado para ofrecer a los usuarios de Office 365 protección contra amenazas relacionadas con el correo electrónico y los documentos de Office. Windows Defender ATP ayuda a proteger las computadoras con Windows de amenazas y ataques. Azure ATP protege sus identidades y servidores locales. También protege los dispositivos móviles que se utilizan para conectarse a su entorno local.

HABILIDAD 3.4: DESCRIBIR LAS METODOLOGÍAS DE GOBIERNO DE AZURE

A medida que aumenta su presencia en la nube, es probable que termine con una gran cantidad de recursos de Azure que abarcan muchos servicios de Azure diferentes. A menos que tenga cierto control sobre cómo se crean y administran esos recursos, los costos pueden descontrolarse. Además del control de costos, es posible que también tenga otras restricciones que desee, como en qué regiones se deben crear ciertos recursos o cómo se etiquetan ciertos recursos, y así sucesivamente.

La forma tradicional de manejar tales problemas de gobernanza sería enviar un memorando a todos explicando cuáles eran los requisitos y luego cruzando los dedos para que las personas se adhieran a ellos. Afortunadamente, Azure Policy puede garantizar que se cumplan sus requisitos y políticas.

Esta sección cubre:

- Política de Azure
- Control de acceso basado en roles
- Cerraduras
- Asesor de Azure

Política de Azure

La Política de Azure le permite definir reglas que se aplican cuando se crean y administran los recursos de Azure. Por ejemplo, puede crear una política que especifique que solo se puede crear una máquina virtual de cierto tamaño y que las máquinas virtuales se deben crear en la región centro-sur de EE. UU. Azure se encargará de hacer cumplir esta política para que usted cumpla con sus políticas corporativas.

Para acceder a la Política de Azure, escriba la **política** en el cuadro de búsqueda en el Portal de Azure y haga clic en **Política** . Alternativamente, puede hacer clic en **Todos los servicios** y buscar "política" en la lista. Esto mostrará la hoja Política como se muestra en la Figura 3-46 .

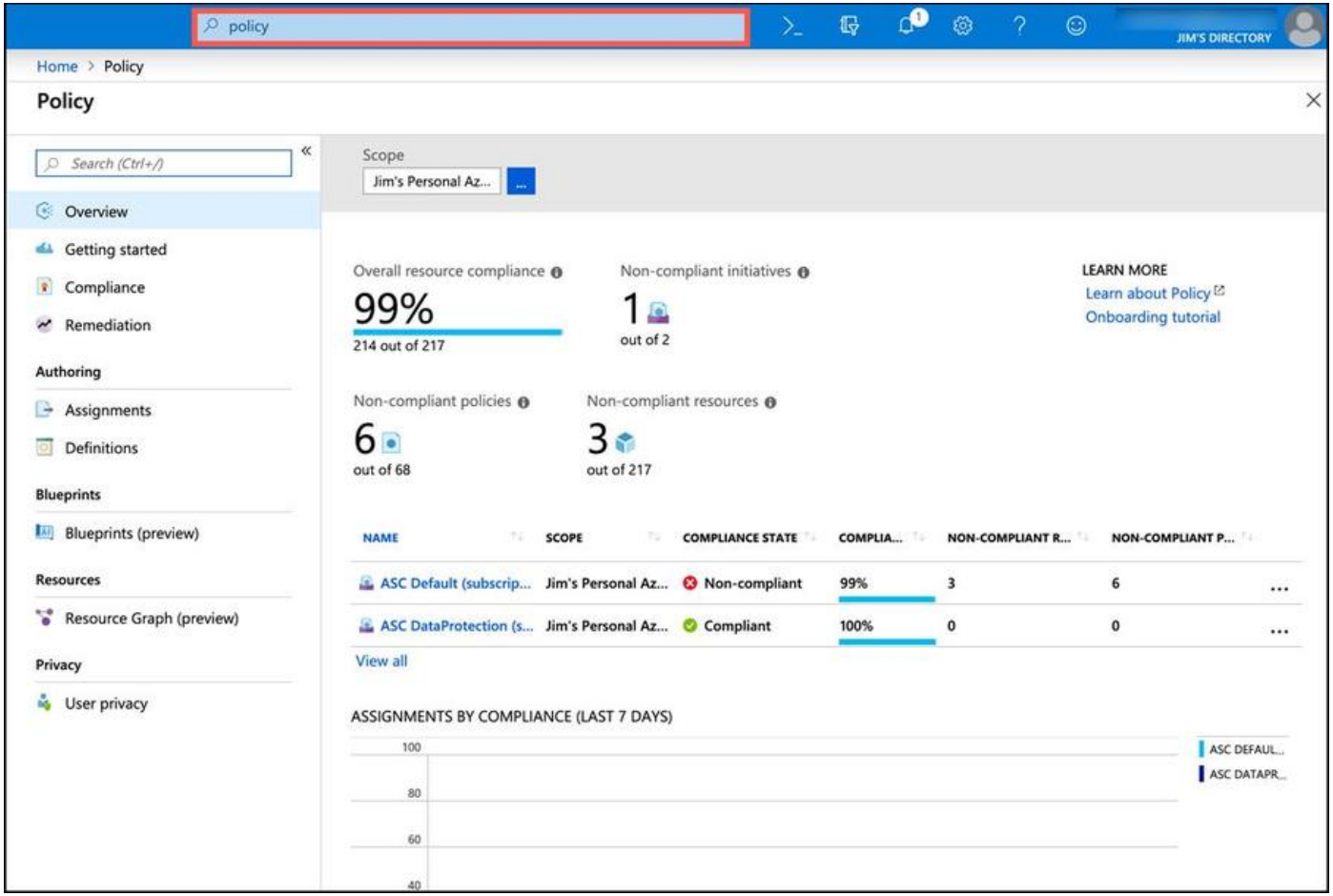


Figura 3-46 Política de Azure en el portal de Azure

De manera predeterminada, la Política de Azure muestra su cumplimiento con las políticas definidas en una suscripción de Azure. Si lo desea, puede ampliar esta vista a una suscripción diferente o a un grupo de recursos haciendo clic en el botón **...** junto al alcance y seleccionando el nuevo alcance como se muestra en la Figura 3-47 .

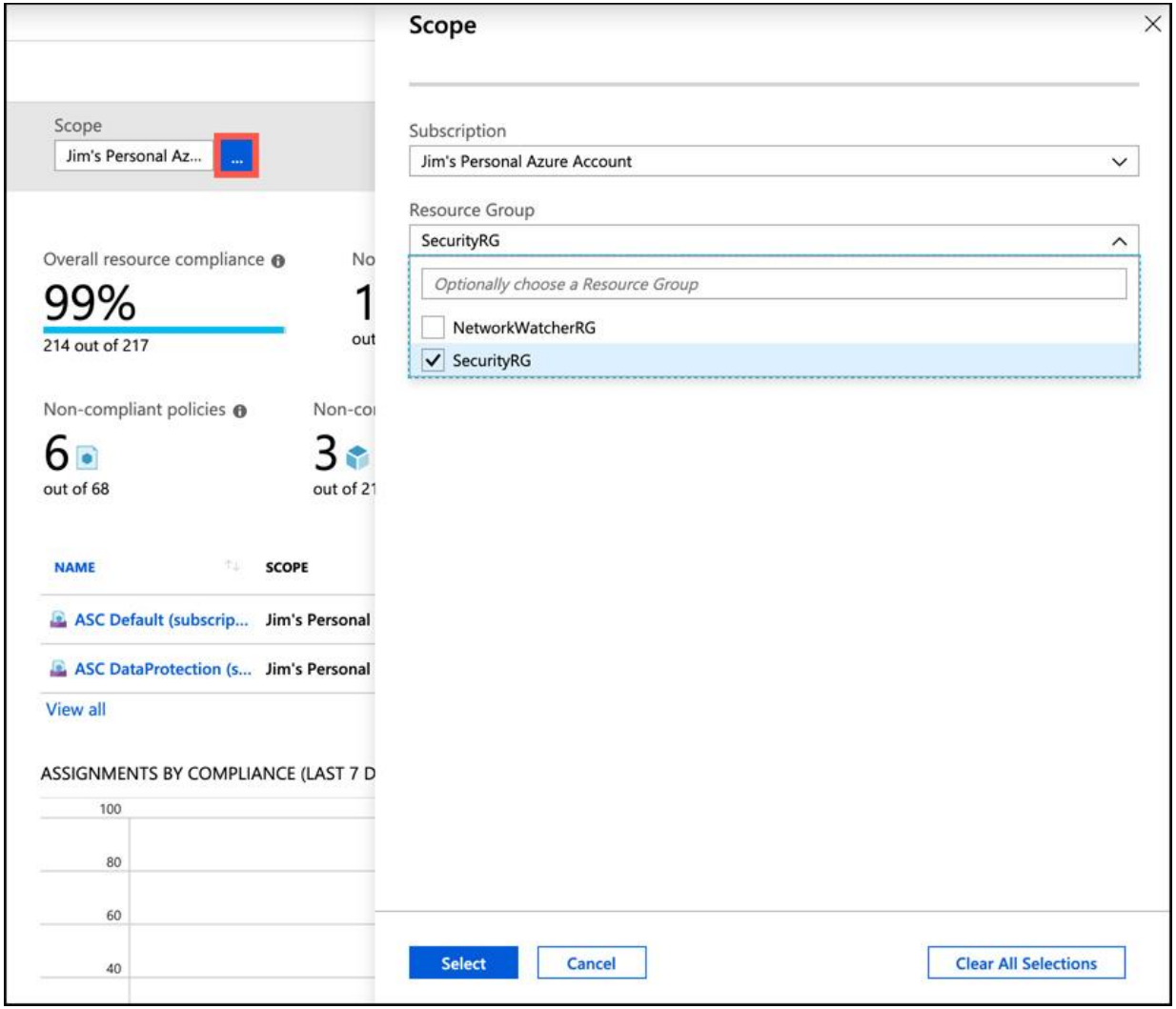


Figura 3-47 Cambio del alcance de la hoja Política en el portal

El incumplimiento que se muestra en la Figura 3-46 se basa en políticas implementadas por Azure Security Center. Al hacer clic en el elemento no compatible, puede ver los detalles completos de lo que está y no está dentro de la política, como se muestra en la Figura 3-48 .

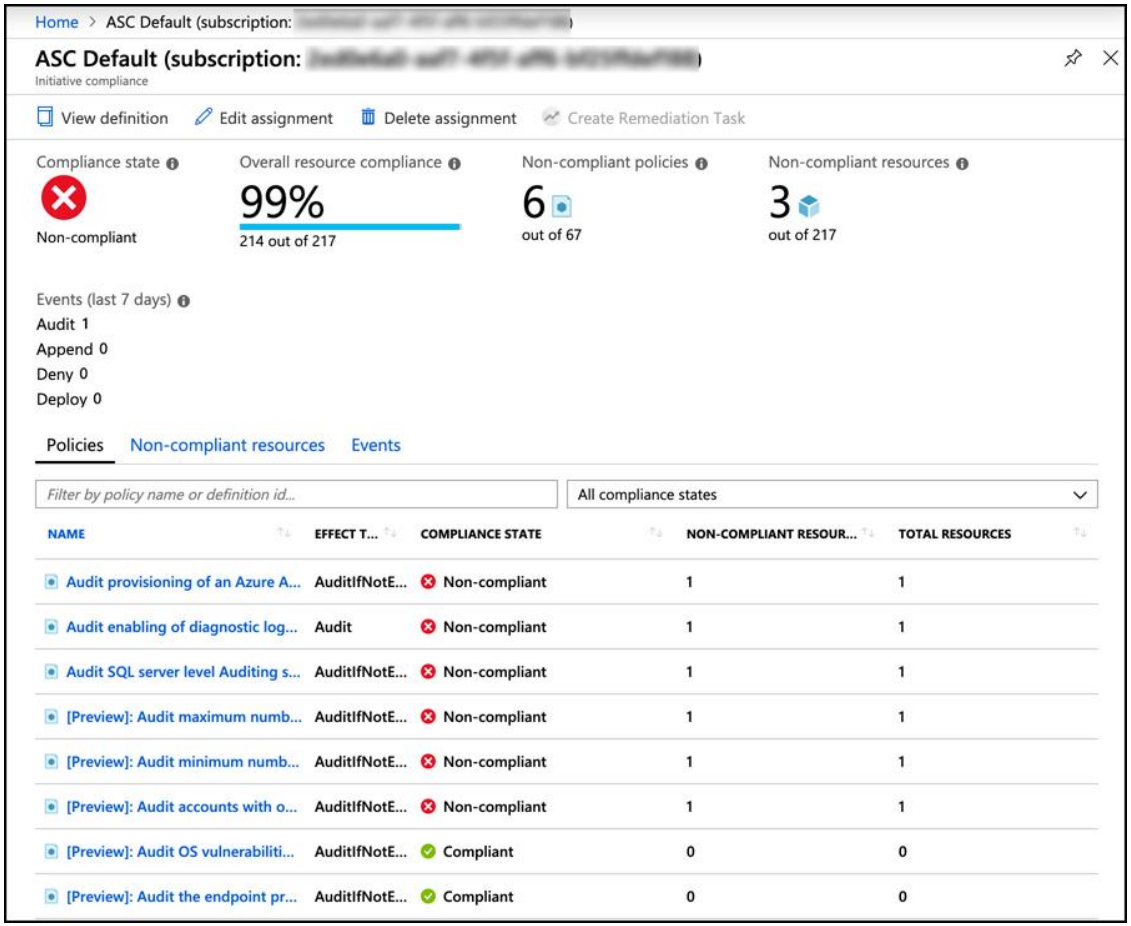


Figura 3-48 Detalles sobre cumplimiento

Tenga en cuenta que el título de este elemento es ASC Default seguido de un ID de suscripción. ASC Default es en realidad una colección de múltiples políticas definidas por Azure Security Center. Azure Policy facilita la imposición de un conjunto completo de políticas al combinarlas en un grupo llamado *iniciativa* . Al definir una iniciativa, puede definir fácilmente reglas complejas que garanticen el gobierno de las políticas de su empresa.

Puede asignar una nueva política seleccionando una política de una lista de políticas incluidas o creando su propia política. Para asignar una política de la lista de políticas incluidas, haga clic en **Asignaciones** y luego haga clic en **Asignar política** , como se muestra en la Figura 3-49 .

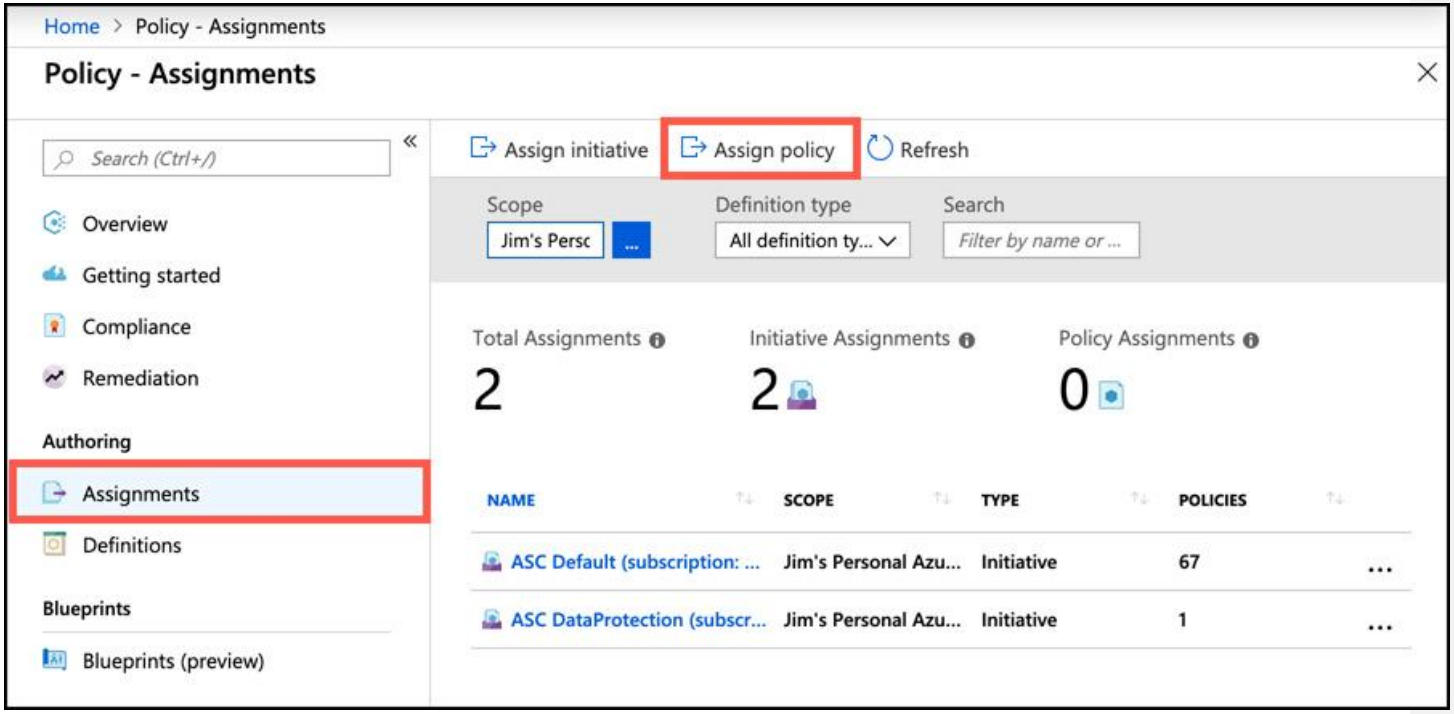


Figura 3-49 Asignación de una política

Haga clic en los puntos suspensivos junto a Definición de política como se muestra en la Figura 3-50 para seleccionar una política.

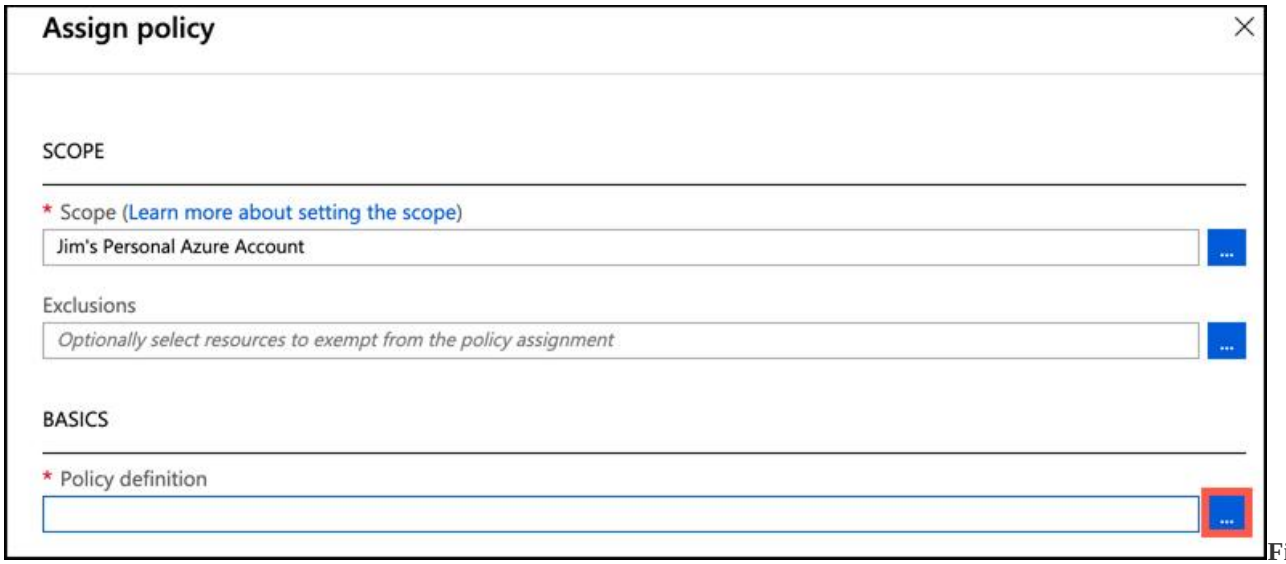


Figura 3-50 Selección de una definición de política

En este caso, aplica una política que garantizará que cualquier aplicación de App Service que se cree tenga habilitado el registro de diagnóstico. Puede hacerlo ingresando el **servicio de aplicaciones** en el cuadro de búsqueda y seleccionando la política integrada que se aplica a esa política, como se muestra en la Figura 3-51 .

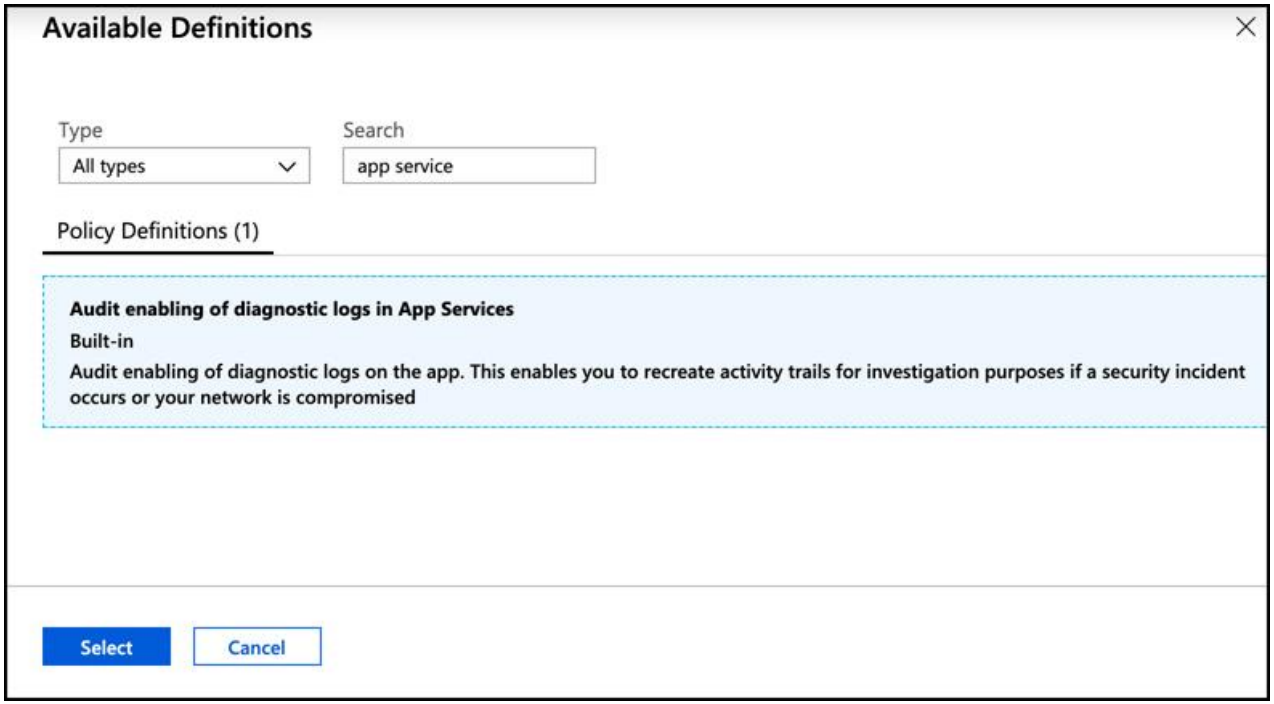


Figura 3-51 Agregar una definición de política incorporada

Como se muestra en la Figura 3-52 , el efecto de esta política particular es Auditoría, lo que significa que si la política no cumple, aparecerá una advertencia en el portal, pero aún permitirá que se cree el recurso.

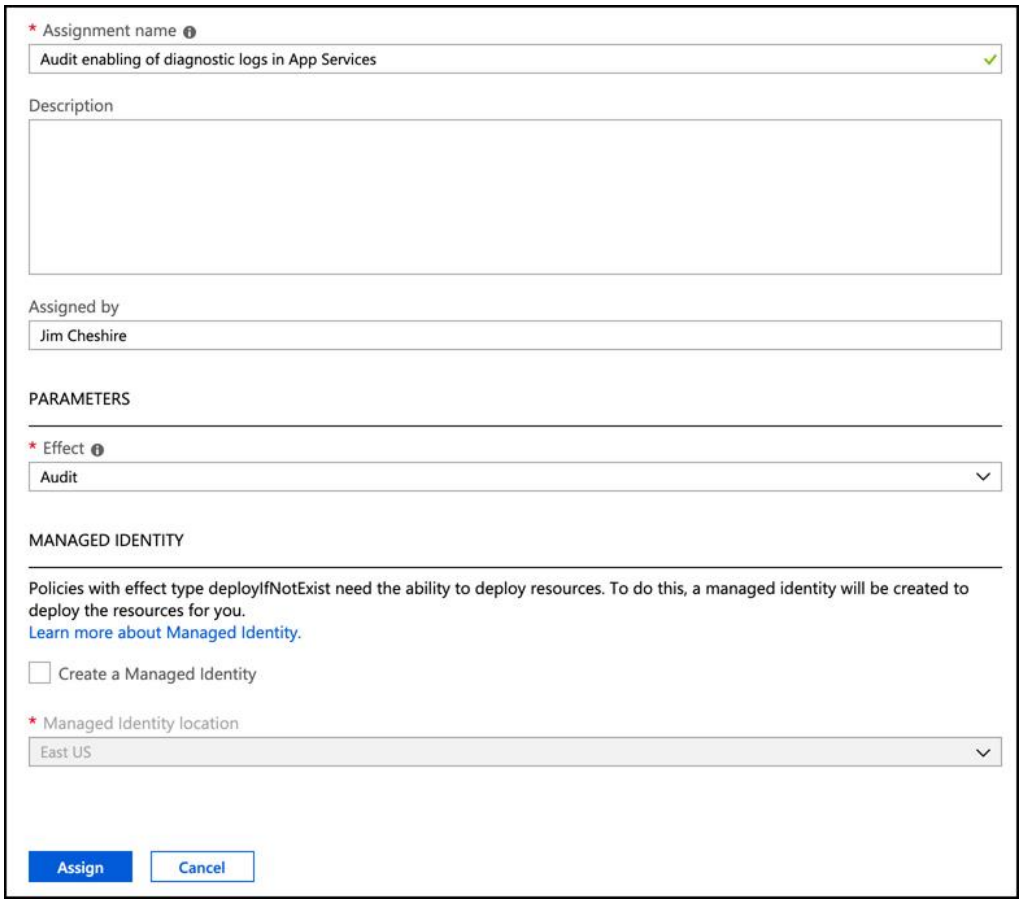


Figura 3-52 Completando la tarea

Hay seis efectos diferentes admitidos en la política de Azure. Sin embargo, no todos los efectos están disponibles para las políticas integradas. Los efectos son:

- **Agregar** Agrega propiedades adicionales a un recurso. Se puede usar para agregar una etiqueta con un valor específico a los recursos.
- **Auditoría** Registra una advertencia si no se cumple con la política.
- **AuditIfNotExists** Le permite especificar un tipo de recurso adicional que debe existir junto con el recurso que se está creando o actualizando. Si ese tipo de recurso no existe, se registra una advertencia.
- **Denegar Niega** la operación de creación o actualización.
- **DeployIfNotExists** Le permite especificar un tipo de recurso adicional que desea implementar, junto con el recurso que se está creando o actualizando. Si ese tipo de recurso no está incluido, se implementa automáticamente.
- **Deshabilitado** La política no está vigente.
-

Más información Más información **sobre los efectos de la política**

Para obtener más información sobre los efectos de la política, incluidos ejemplos de cada uno, consulte: *https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects* .

Además de utilizar las políticas integradas, también puede definir sus propias políticas creando una definición de política personalizada. Las definiciones de políticas personalizadas son plantillas ARM que definen la política. Para obtener más información sobre cómo crear una definición de política personalizada, consulte: *https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition* .

Control de acceso basado en roles

El control de acceso basado en roles (RBAC) es un término genérico que se refiere al concepto de autorizar a los usuarios a un sistema basado en roles definidos a los que pertenece el usuario. Azure implementa RBAC en todos los recursos de Azure para que pueda controlar cómo los usuarios y las aplicaciones pueden interactuar con sus recursos de Azure.

Es posible que desee permitir que los usuarios que administran sus bases de datos tengan acceso a las bases de datos en un grupo de recursos en particular, pero no desea permitir que esas personas creen nuevas bases de datos o eliminen las existentes. Es posible que también desee que algunos desarrolladores web puedan implementar un nuevo código en sus aplicaciones web, pero no desea que puedan escalar la aplicación a un plan de mayor precio. Estos son solo dos ejemplos de lo que puede hacer con RBAC en Azure.

Hay cuatro elementos para RBAC.

- **Principal de** seguridad El **principal de** seguridad representa una identidad. Puede ser un usuario, un grupo, una aplicación (que se denomina entidad de servicio) o una entidad AAD especial llamada *identidad administrada* . Una identidad administrada es cómo autoriza a otro servicio de Azure a acceder a su recurso de Azure.
- **Rol** Un rol (a veces denominado definición de rol) es lo que define cómo la entidad de seguridad puede interactuar con un recurso de Azure. Por ejemplo, un rol podría definir que unEl principal de seguridad puede leer las propiedades de un recurso pero no puede crear nuevos recursos o eliminar recursos existentes.
- **Alcance** El alcance define el nivel en el que se aplica el rol y controla cuánto control tiene el principal de seguridad. Por ejemplo, si el alcance es para un grupo de recursos, el rol define actividades que se pueden realizar en todos los recursos coincidentes en el grupo de recursos.
- **Asignaciones de** roles Los roles se asignan a un principal de seguridad en un ámbito particular, y eso es lo que finalmente define el nivel de acceso para el principal de seguridad.

RBAC incluye muchos roles incorporados. Tres de estos roles integrados se aplican a todos los recursos de Azure.

- Los miembros **propietarios** de este rol tienen acceso total a los recursos.
- **Los** miembros **contribuyentes** de este rol pueden crear recursos y administrar recursos, pero no pueden delegar ese derecho a nadie más.
- Los miembros **lectores** de este rol pueden ver los recursos de Azure, pero no pueden crear, eliminar ni administrar esos recursos.
-

Todos los demás roles integrados son específicos de ciertos tipos de recursos de Azure.

Para otorgar a alguien acceso a un recurso mediante RBAC, abra el recurso al que desea otorgar acceso en Azure Portal. Haga clic en **Control de acceso (IAM)** en el portal para configurar RBAC. En la Figura 3-53 , RBAC se está configurando para una aplicación web alojada en Azure App Service. Al hacer clic en **Agregar** en el cuadro Agregar una asignación de roles, puede agregar un rol.

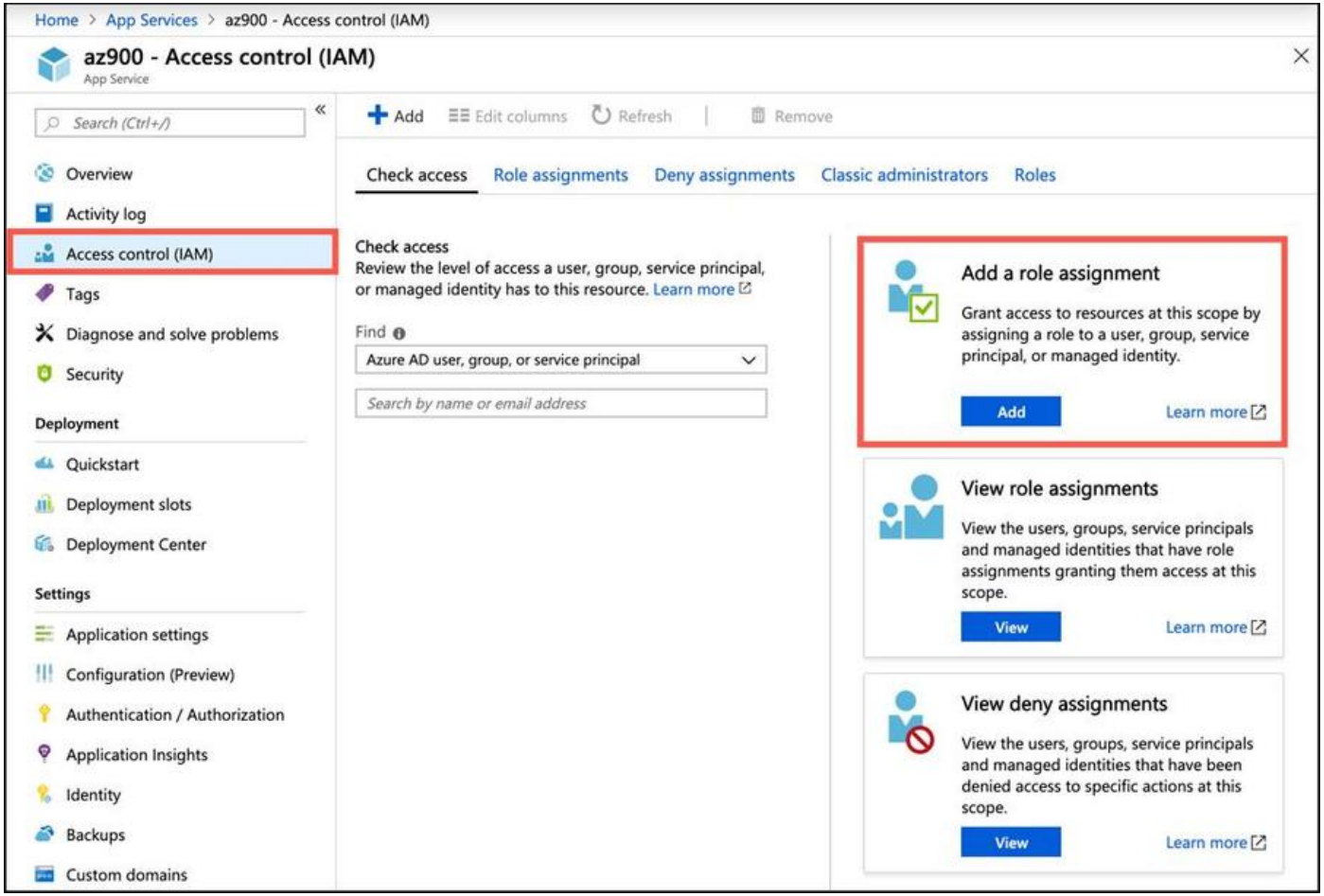


Figura 3-53 Configuración de RBAC para una aplicación web

Consejo de examen

El alcance de RBAC se define por el lugar donde se asigna el rol RBAC. Por ejemplo, si abre un grupo de recursos en el portal y asigna un rol RBAC a un usuario, el alcance está en el nivel del grupo de recursos. Por otro lado, si abre una aplicación web dentro de ese grupo de recursos y asigna el rol, el alcance es solo para esa aplicación web. Ese usuario no tendrá acceso a otras aplicaciones en el grupo de recursos a menos que aplique otras asignaciones de roles al usuario.

Los roles de RBAC se pueden abarcar al grupo de administración, suscripción, grupo de recursos o nivel de recursos.

Después de hacer clic en **Agregar** , elija el rol que desea asignar. La lista de roles diferirá según el tipo de recurso que sea. Elija a quién o a qué desea asignar el rol y luego haga clic en **Guardar** , como se muestra en la Figura 3-54 .

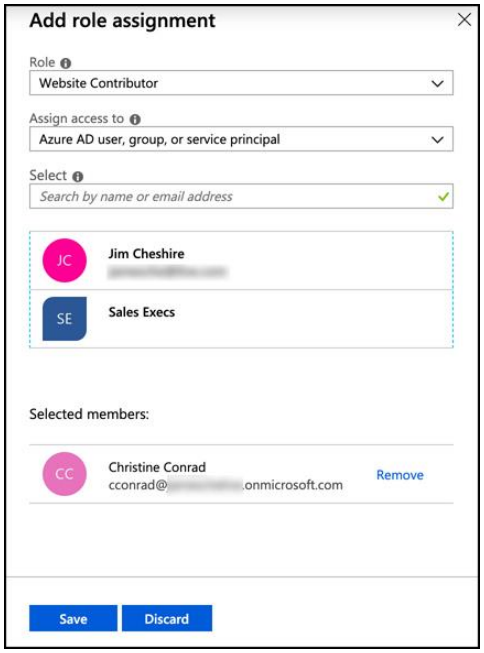


Figura 3-54 Agregar una asignación de roles

La Figura 3-54 muestra una lista de usuarios en AAD, porque el menú desplegable Asignar acceso a está configurado en objetos AAD. Puede ver una lista de otros tipos de objetos seleccionando un tipo diferente. Por ejemplo, en la Figura 3-55 , estamos seleccionando un tipo de identidad administrado integrado que agregará máquinas virtuales de Azure a la función Colaborador del sitio web para esta aplicación web.

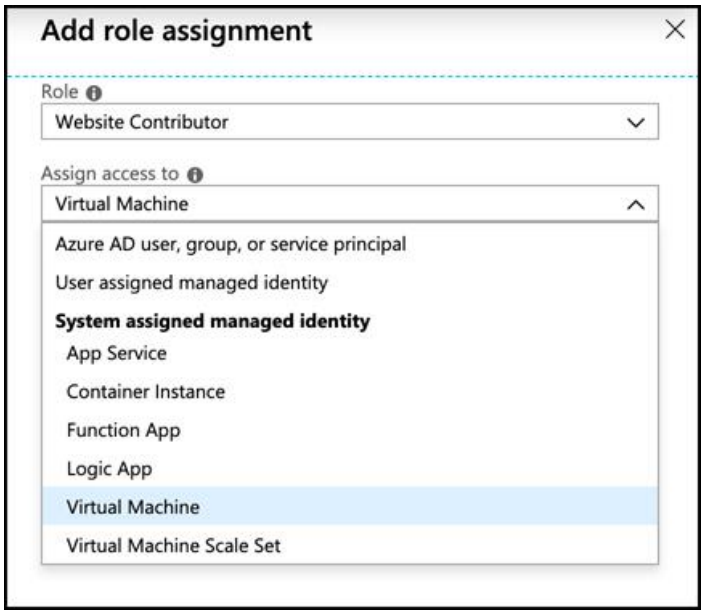


Figura 3-55 Asignación de una identidad administrada a un rol

Consejo de examen

Es importante comprender que las asignaciones de roles son aditivas. Sus habilidades RBAC en cualquier ámbito particular son el resultado de todas las asignaciones de roles hasta ese nivel. En otras palabras, si tengo el rol de Propietario en un grupo de recursos y usted me asigna el rol de Colaborador del sitio web en una aplicación web dentro de ese grupo de recursos, la asignación del Colaborador del sitio web no tendrá efecto porque ya tengo el rol de Propietario en todo el recurso grupo.

RBAC se aplica mediante Azure Resource Manager (ARM). Cuando intenta interactuar con un recurso de Azure, ya sea en el portal de Azure o mediante una herramienta de línea de comandos, ARM se autentica y se genera un token para usted. Ese token es una representación de su identidad y todas sus asignaciones de roles, y se incluye con todas las operaciones que realiza en el recurso. ARM puede determinar si la acción que está realizando está permitida por los roles a los que está asignado. Si es así, la llamada tiene éxito. Si no, se le niega el acceso.

Puede asegurarse de que alguien tenga los derechos que desea comprobando el acceso en el portal de Azure. Abra el recurso y haga clic en **Control de acceso (IAM)** . Haga clic en la pestaña **Comprobar acceso** y busque el usuario o recurso al que le ha otorgado acceso, como se muestra en la Figura 3-56 .

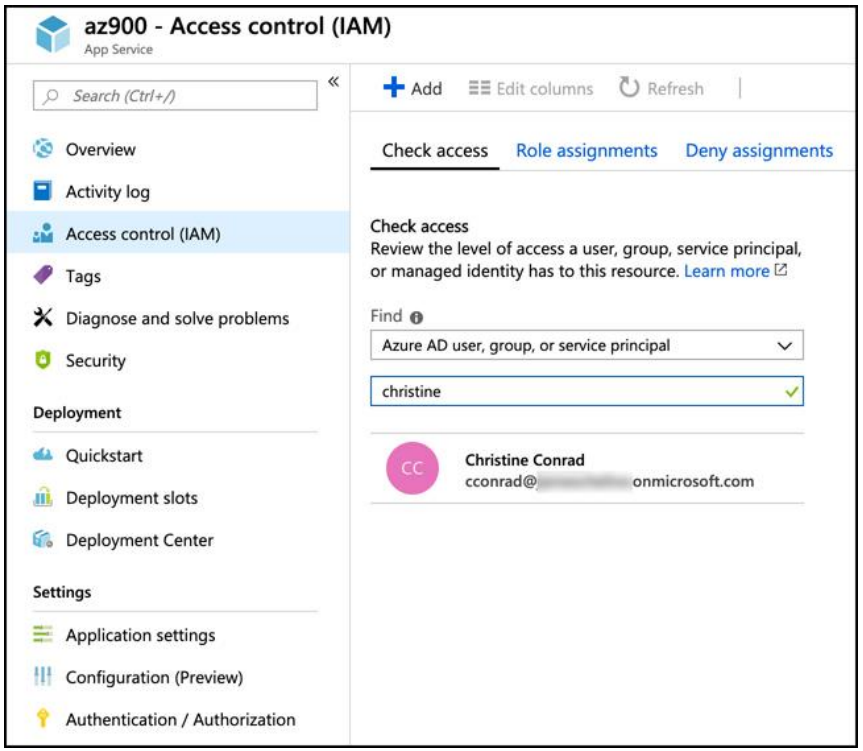


Figura 3-56 Comprobando el acceso

Haga clic en el usuario u otro objeto y el acceso al recurso se mostrará como se muestra en la Figura 3-57 .

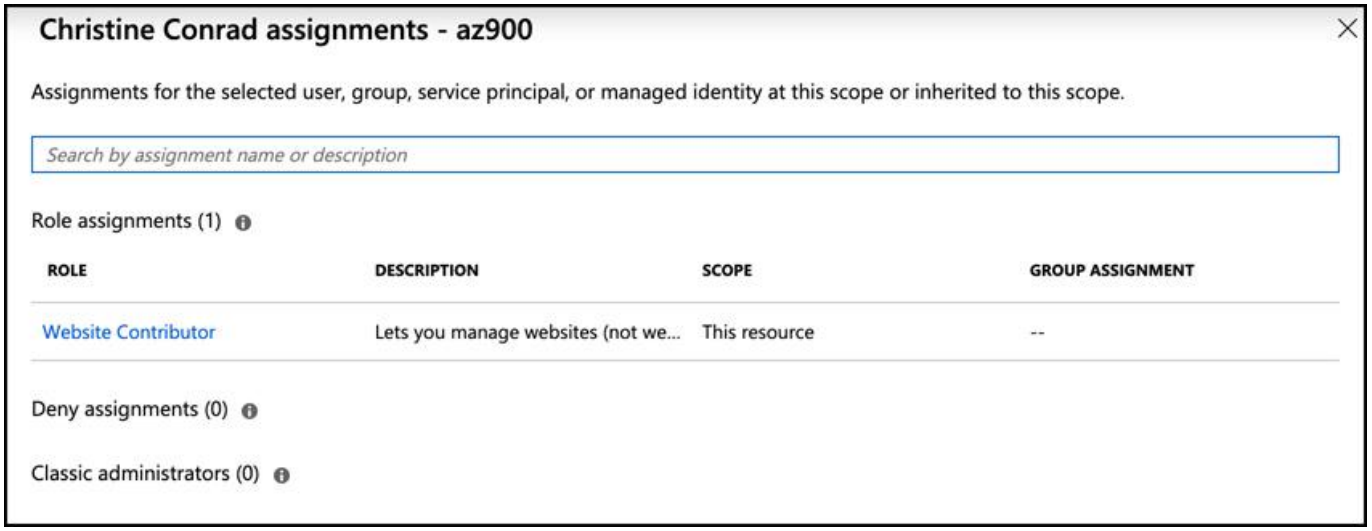


Figura 3-57 Visualización de asignaciones de roles para un usuario

Para obtener un mayor nivel de detalle sobre qué operaciones exactas están permitidas y cuáles no, haga clic en el rol que se muestra. Esto le permitirá ver una lista detallada de operaciones y la combinación de lectura, escritura, eliminación y otras acciones que un principal de seguridad puede realizar como se muestra en la Figura 3-58 .

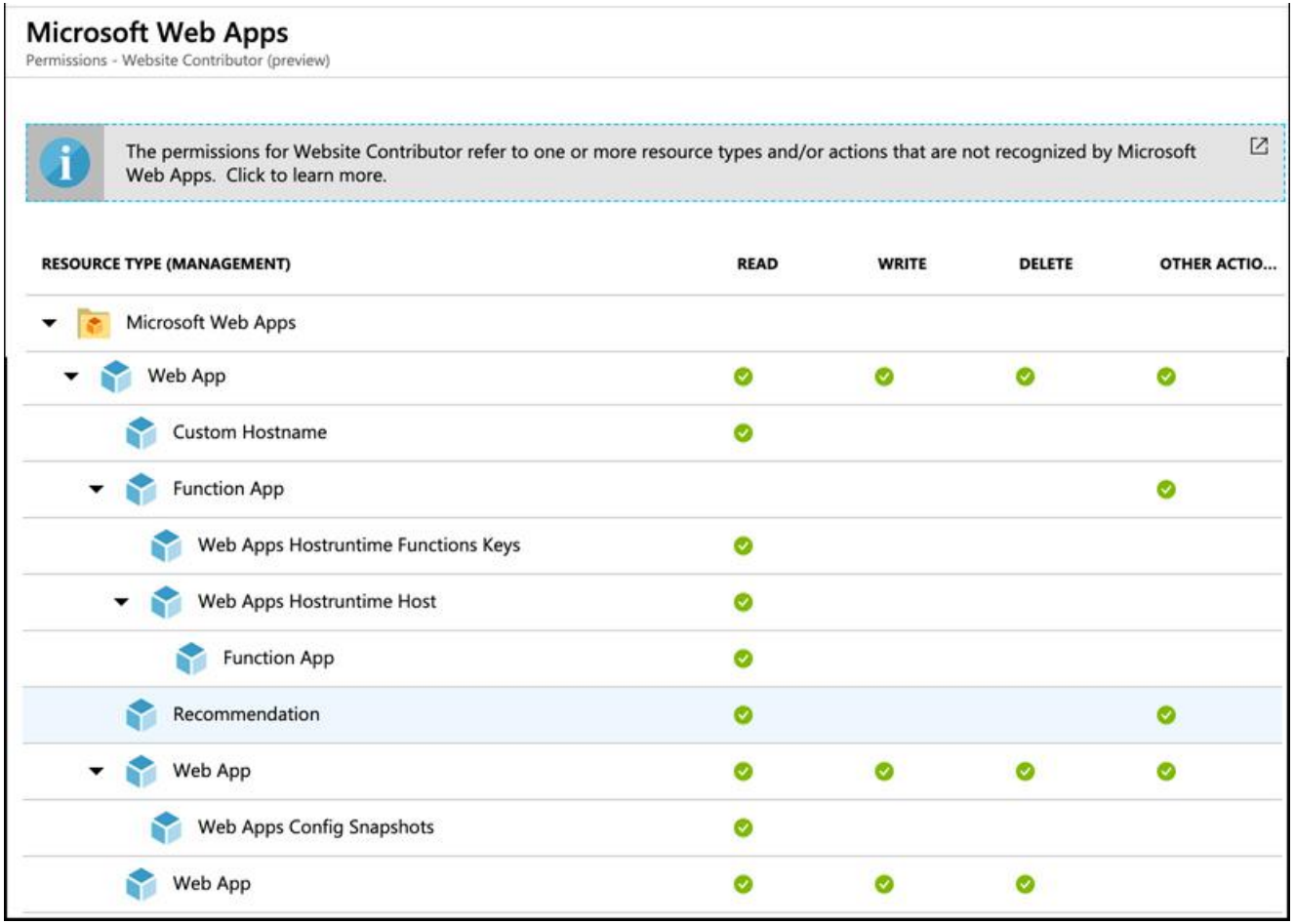


Figura 3-58 Permisos detallados aplicados a un usuario para una aplicación web

Cerraduras

RBAC es una excelente manera de controlar el acceso a un recurso de Azure, pero en los casos en que solo desea evitar cambios en un recurso, o evitar que ese recurso se elimine, los bloqueos son una solución más simple. A diferencia de RBAC, los bloqueos se aplican a todos los que tienen acceso al recurso.

Consejo de examen

Para crear un bloqueo, debe estar en el rol Propietario o Administrador de acceso de usuario en RBAC. Alternativamente, un administrador puede crear un rol personalizado que le otorgue el derecho de crear un bloqueo.

Los bloqueos se pueden aplicar a nivel de recurso, a nivel de grupo de recursos o a nivel de suscripción. Para aplicar un bloqueo a un recurso, abra el recurso en Azure Portal y haga clic en **Bloqueos** en la sección Configuración del menú de la izquierda, como se muestra en la Figura 3-59 .

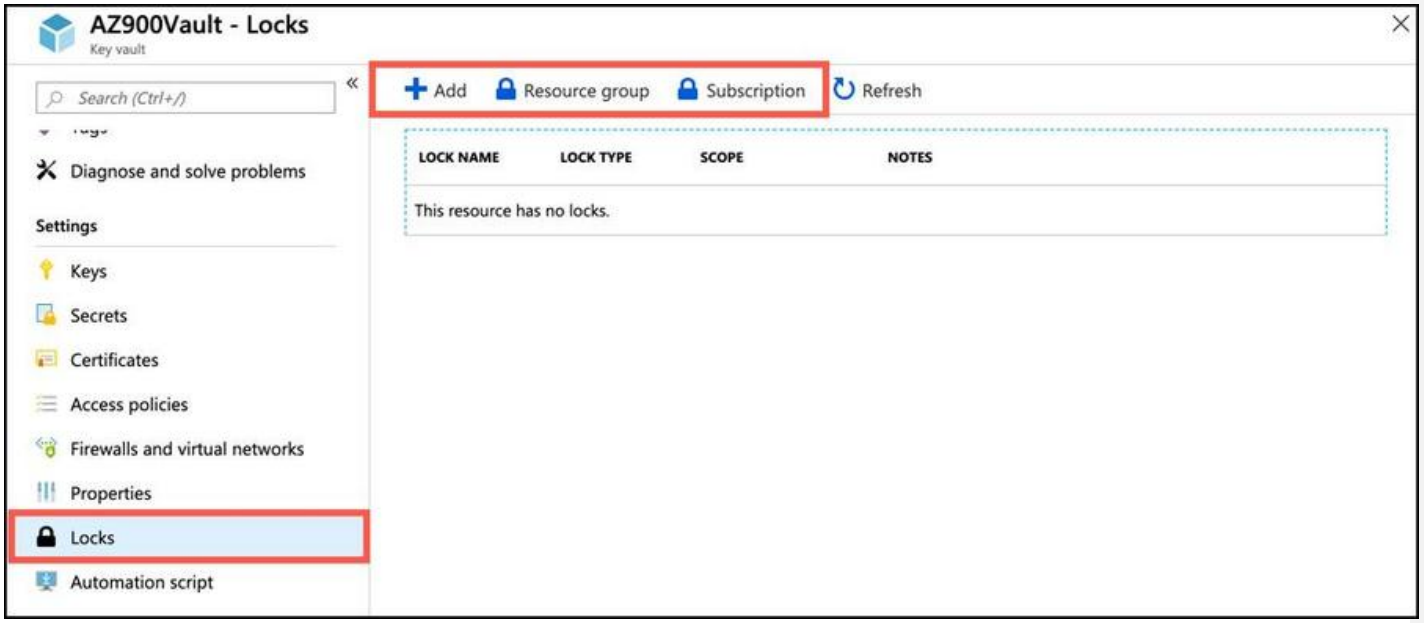


Figura 3-59 Bloqueo de un recurso

Para agregar un bloqueo al recurso, haga clic en **Agregar** . (También puede revisar y agregar bloqueos al grupo de recursos haciendo clic en **Grupo de recursos** , o a la suscripción haciendo clic en **Suscripción**). Proporcione un nombre para el bloqueo, establezca el tipo de bloqueo y agregue una nota opcional como se muestra en la Figura 3 -60 .

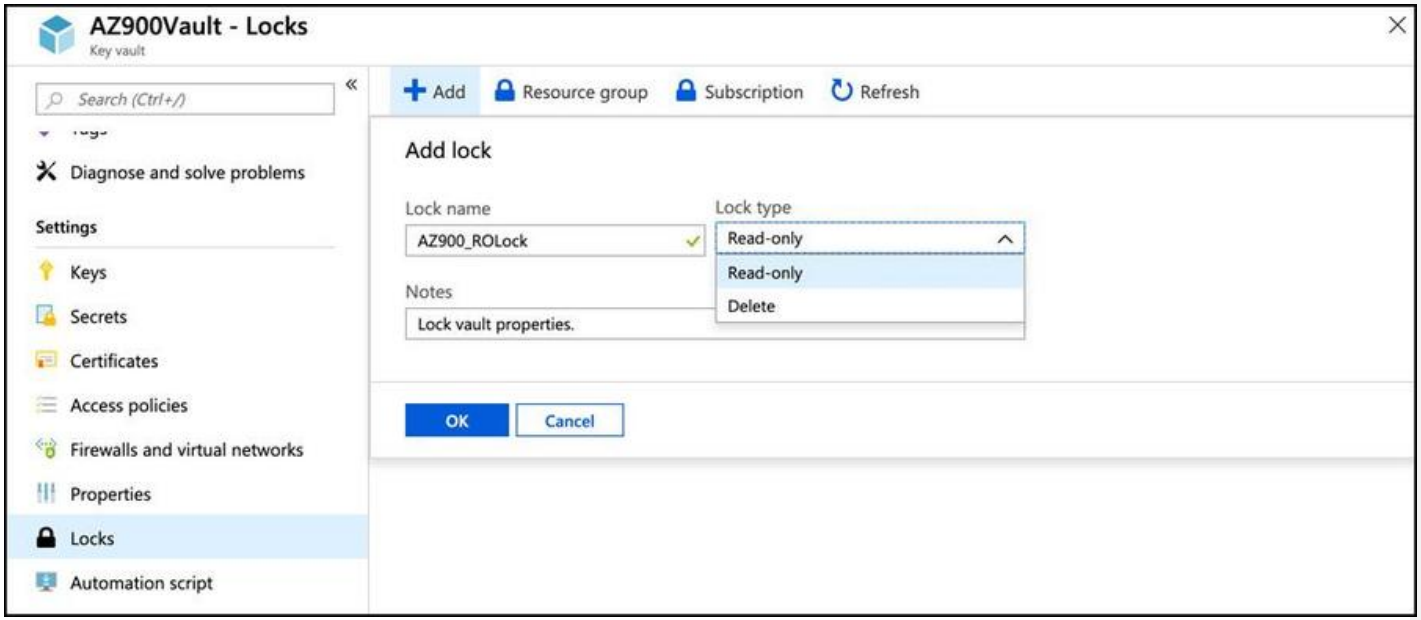


Figura 3-60 Agregar un bloqueo de solo lectura

Un bloqueo de solo lectura es el bloqueo más restrictivo. Impide cambiar las propiedades del recurso o eliminar el recurso. Un bloqueo de eliminación evita que el recurso se elimine, pero las propiedades aún se pueden cambiar. El resultado de un bloqueo de solo lectura a menudo es impredecible, debido a la forma en que Azure maneja los bloqueos.

Los bloqueos solo se aplican a operaciones manejadas por ARM, y algunas operaciones específicas de un recurso son manejadas internamente por el recurso en lugar de ser manejadas por ARM. Por ejemplo, el bloqueo de solo lectura aplicado a Azure Key Vault en la Figura 3-60 evitará que un usuario cambie las políticas de acceso en la bóveda, pero los usuarios aún pueden agregar y eliminar claves, secretos y certificados porque esas operaciones se manejan internamente por Key Vault.

Hay otras situaciones en las que un bloqueo de solo lectura puede evitar operaciones que se producen inesperadamente. Por ejemplo, si coloca un bloqueo de solo lectura en una cuenta de almacenamiento, evitará que todos los usuarios enumeren las claves de acceso para

la cuenta de almacenamiento, porque la operación para enumerar las claves hace que las claves estén disponibles para acceso de escritura.

Si se aplica un bloqueo a un grupo de recursos, todos los recursos en ese grupo de recursos heredan el bloqueo. Del mismo modo, si se aplica un bloqueo en el nivel de suscripción, todos los recursos de la suscripción heredan el bloqueo. Es posible anidar cerraduras, y en tales situaciones, la cerradura más restrictiva es la cerradura efectiva. Por ejemplo, si tiene un bloqueo de solo lectura en un grupo de recursos y un bloqueo de eliminación en un recurso en ese grupo de recursos, el recurso tendrá un bloqueo de solo lectura aplicado. El bloqueo de eliminación explícito no es efectivo.

Consejo de examen

Las cerraduras también son heredadas por los recursos recién creados. Si aplica un bloqueo de eliminación a un grupo de recursos y agrega un nuevo recurso al grupo de recursos más adelante, el nuevo recurso heredará automáticamente el bloqueo de eliminación.

Cuando se intenta una operación en el portal y se deniega debido a un bloqueo, se mostrará un error como se muestra en la Figura 3-61 . Tenga en cuenta que no hay ninguna información sobre por qué falló la operación, por lo que, a menos que sepa que se aplica un bloqueo en un recurso, puede encontrar esta falla confusa.

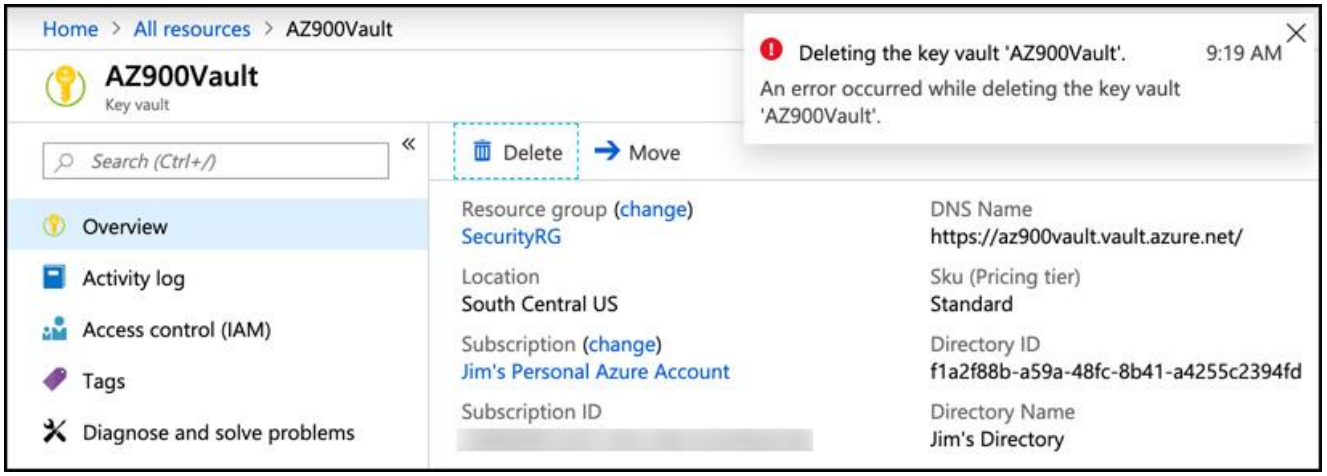


Figura 3-61 Denegada por un candado

Sin embargo, intentar eliminar Key Vault de la interfaz de línea de comandos (CLI) de Azure muestra claramente que la eliminación falló debido a un bloqueo, como se muestra en la Figura 3-62 .

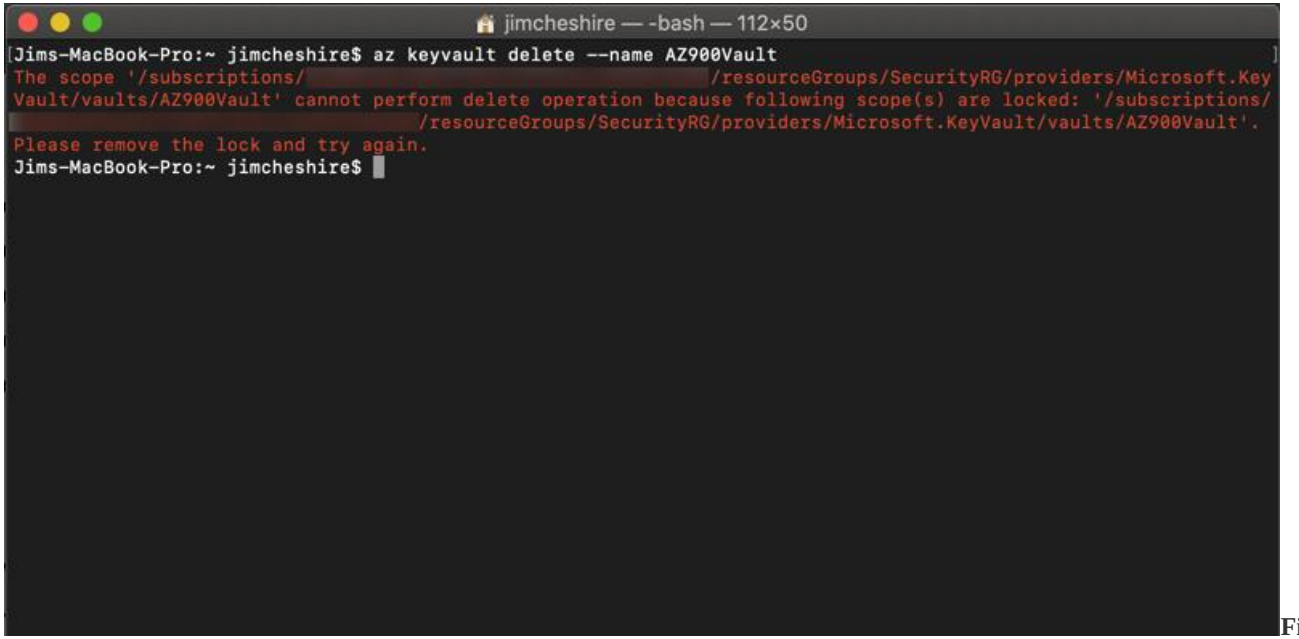


Figura 3-62 Error en la CLI de Azure debido a un bloqueo

Algunos tipos de recursos son mejores para mostrar errores detallados en el portal, pero si usa bloqueos en los recursos y experimenta un error inesperado al trabajar con un recurso, siempre es una buena idea intentar la operación en PowerShell o la CLI de Azure para ver si un bloqueo podría estar impactando en ti.

Asesor de Azure

Azure Advisor es un analizador de mejores prácticas para los recursos de Azure. El objetivo de Azure Advisor es ayudarlo a garantizar la alta disponibilidad y el rendimiento, controlar los costos y asegurar sus recursos de Azure. La asistencia de seguridad en Azure Advisor se suministra directamente desde el Centro de seguridad de Azure, pero Azure Advisor proporciona una vista única de todas las recomendaciones, incluida la capacidad de tomar medidas directamente sobre la recomendación en la hoja de Azure Advisor.

Para acceder a Azure Advisor, haga clic en **Advisor** en el menú en Azure Portal, como se muestra en la Figura 3-63 .

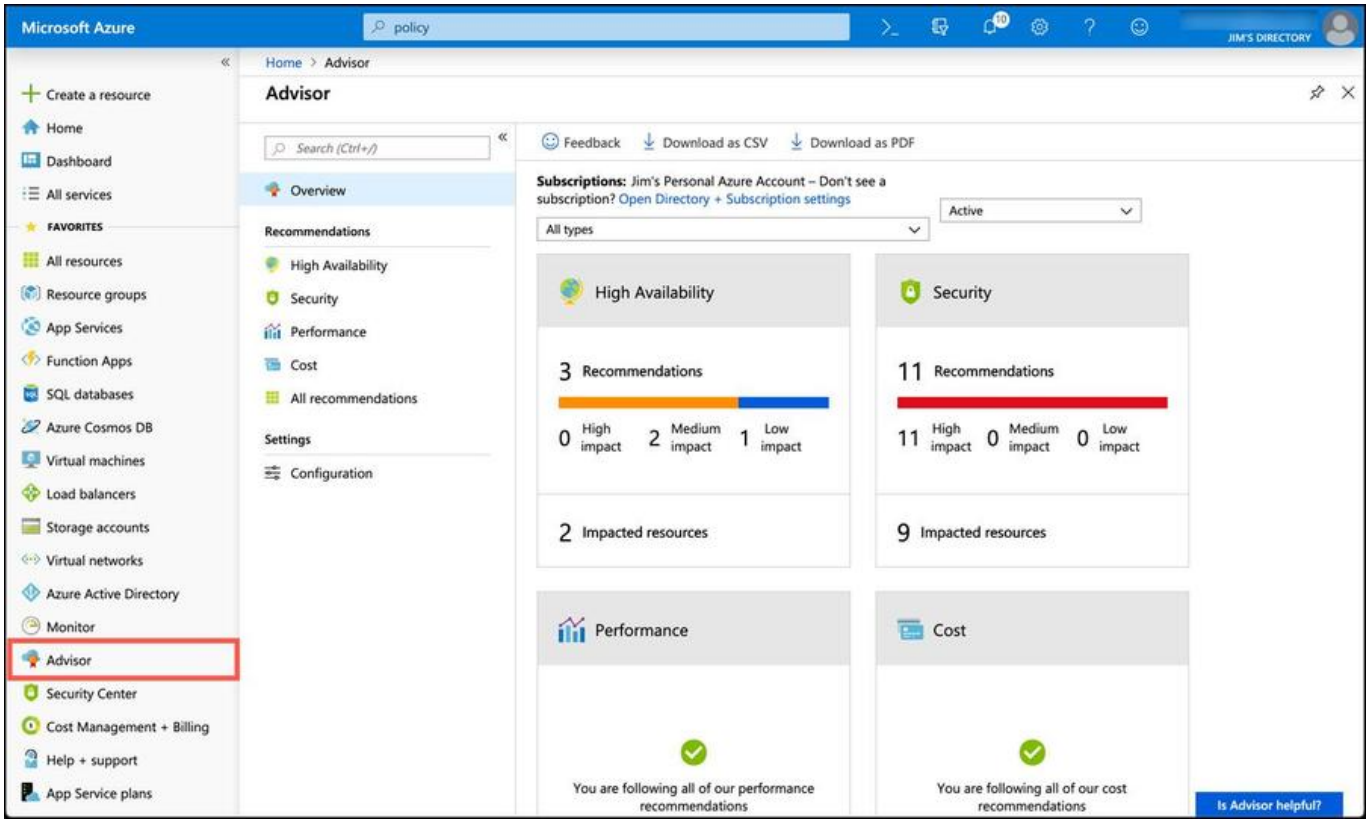


Figura 3-63 Asesor de Azure

Al hacer clic en el mosaico de Seguridad, podrá ver todas las recomendaciones de seguridad como se muestra en la Figura 3-64 .

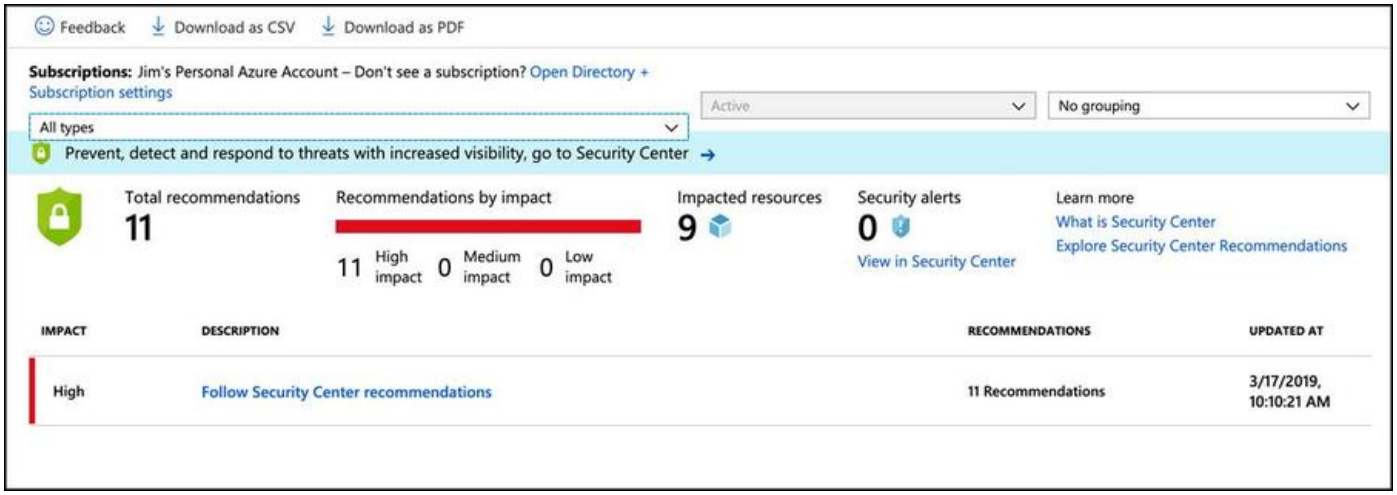


Figura 3-64 Recomendaciones de seguridad de Azure Advisor

Desde esta hoja, puedo abrir el Centro de seguridad para ver detalles sobre estas recomendaciones, pero también puedo hacer clic en **Seguir las recomendaciones del Centro de seguridad** para ver y tomar medidas directamente desde Azure Advisor.

Cuando se hace clic en este, se lo lleva a una lista completa, como se muestra en la Figura 3-65 . Haga clic en cualquiera de estas recomendaciones para obtener más detalles y tomar medidas sobre la recomendación.

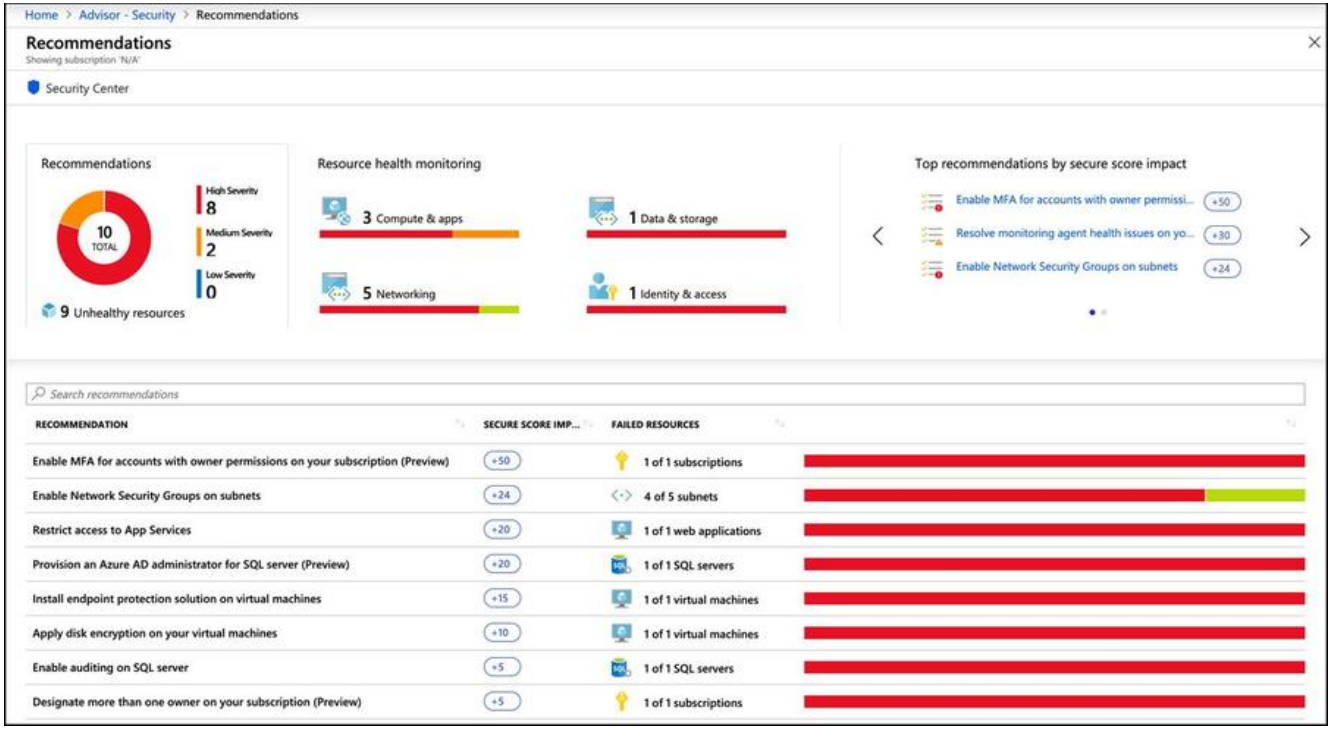


Figura 3-65 Visualización de recomendaciones de seguridad

En la Figura 3-66 , se muestra una recomendación individual. También puede ver los pasos a seguir para abordar la recomendación y una lista de los recursos de Azure afectados por la recomendación.

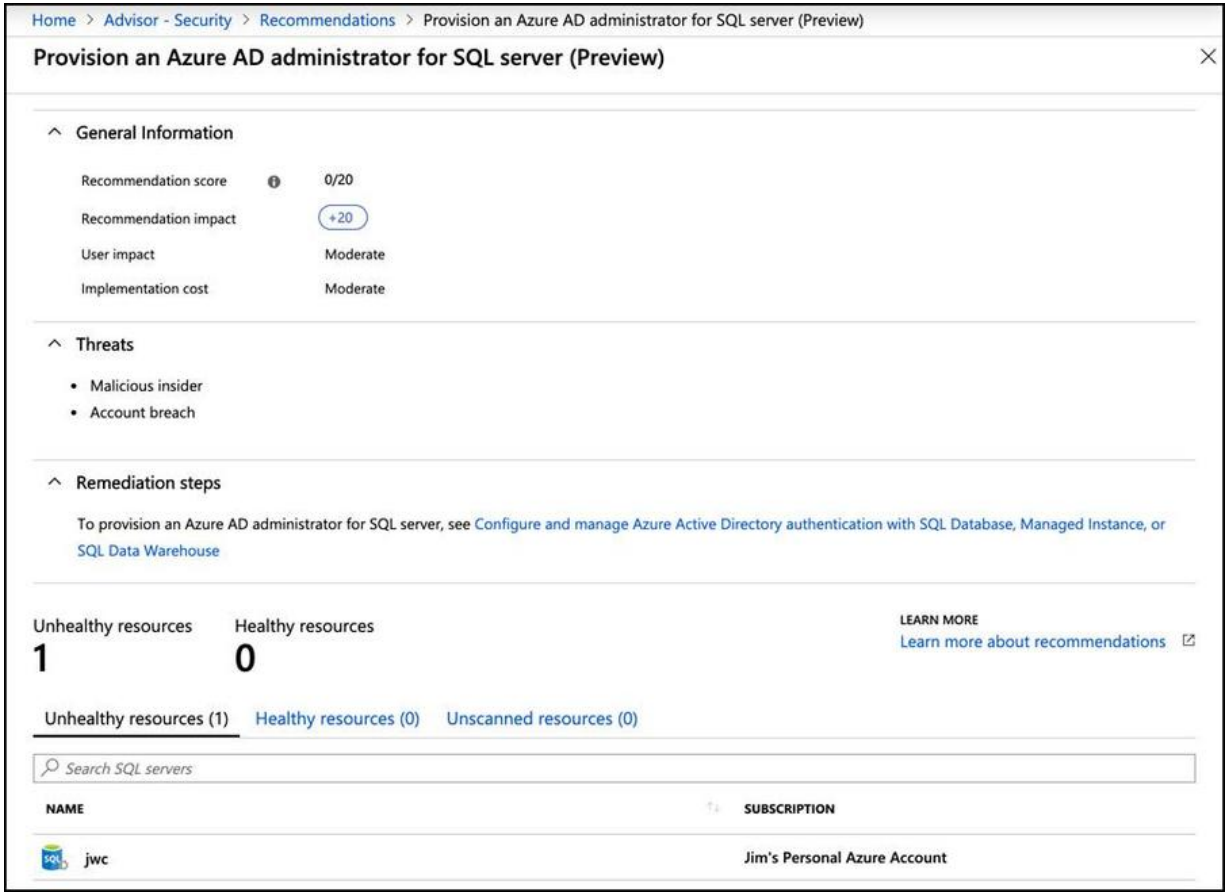


Figura 3-66 Ver una recomendación específica

HABILIDAD 3.5: COMPRENDER LAS OPCIONES DE SUPERVISIÓN E INFORMES EN AZURE

Ya sea que tenga miles de recursos de Azure o solo unos pocos, es importante poder monitorear el uso de recursos en Azure. También es importante comprender el estado de sus recursos de Azure y si un problema en su configuración o un problema en el propio Azure está afectando el estado de sus aplicaciones en la nube. Azure Monitor y Azure Service Health son dos servicios de Azure que proporcionan estas características.

Esta sección cubre:

- Monitor azul
- Estado del servicio de Azure

Monitor azul

Azure Monitor agrega métricas para los servicios de Azure y las expone en una única interfaz. También puede crear alertas que le notifiquen a usted, o a otra persona, cuando haya inquietudes que desee abordar.

Para acceder a Azure Monitor, haga clic en **Monitor** en Azure Portal para mostrar la hoja Azure Monitor, como se muestra en la Figura 3-67 . Azure Monitor es personalizable, por lo que puede ver exactamente lo que más le interesa. Por esa razón, no muestra ninguna métrica hasta que las configura. Para ver las métricas, haga clic en **Métricas** y luego **seleccione un recurso** .

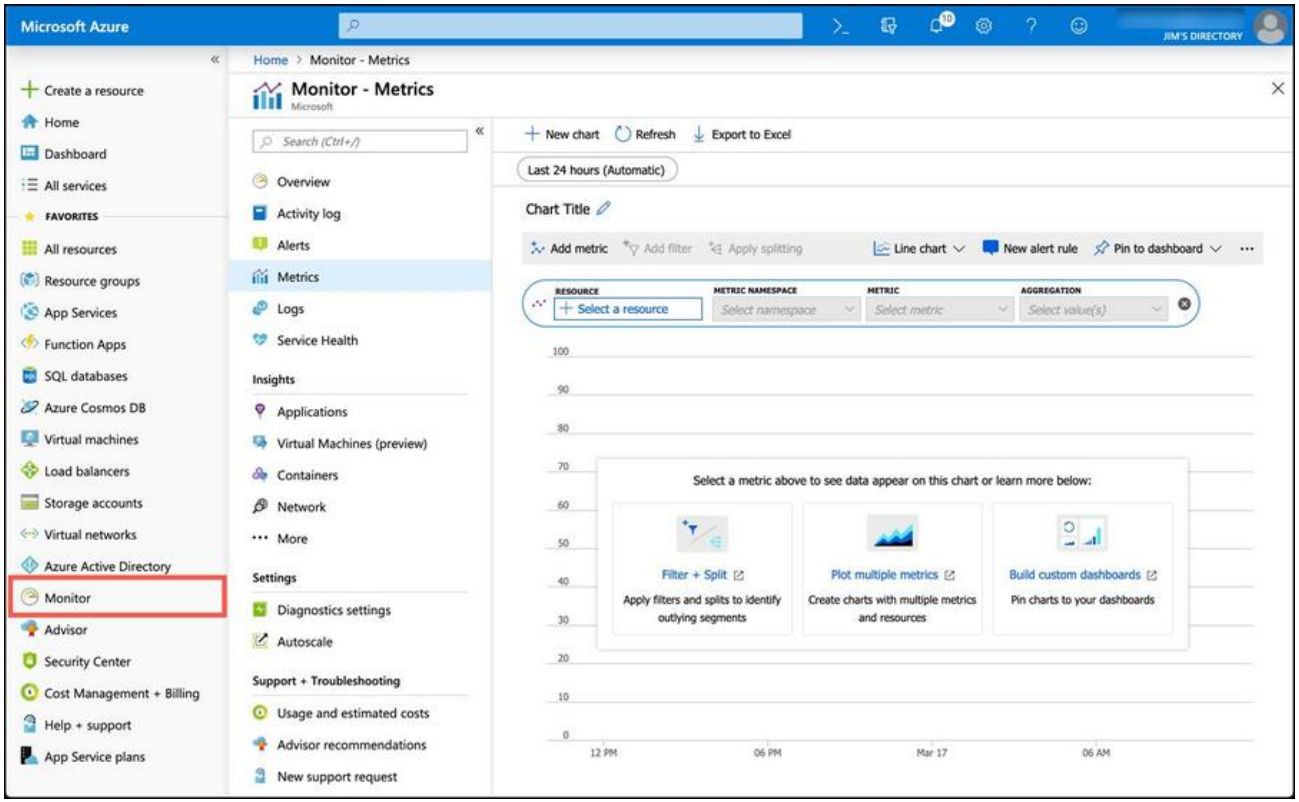


Figura 3-67 Monitor de Azure

En la Figura 3-68 , hemos seleccionado una VM en el grupo de recursos SecurityRG para que pueda ver las métricas de esta VM en Monitor.

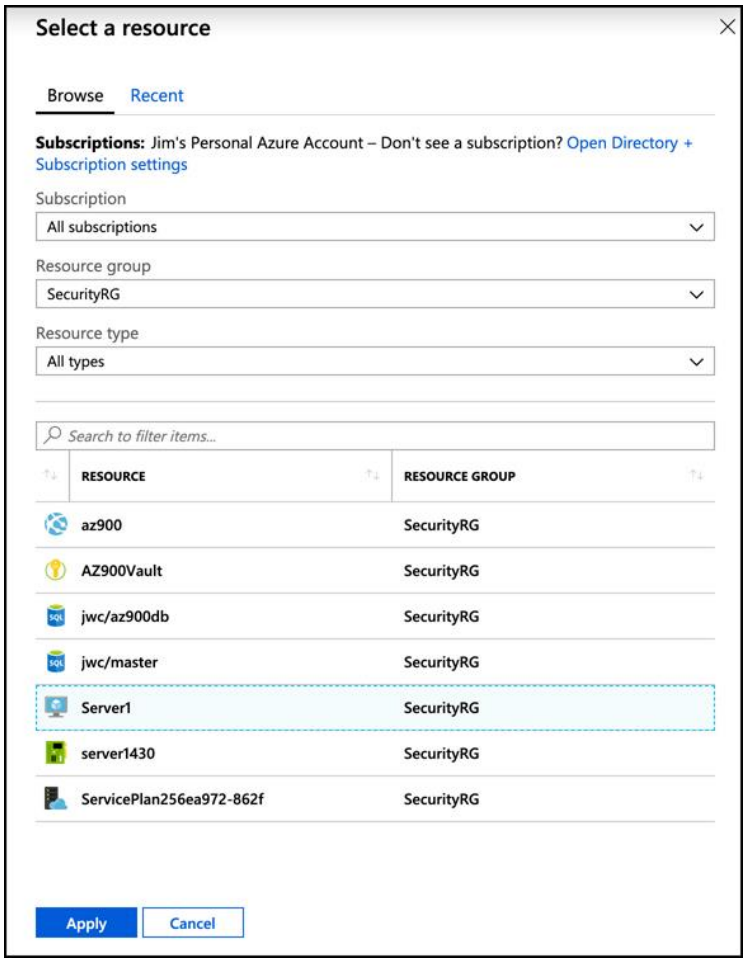


Figura 3-68 Selección de un recurso para monitorear

Una vez que selecciona un recurso, se le presenta una lista de métricas relacionadas con ese recurso. Los recursos para las máquinas virtuales se muestran en la Figura 3-69 .

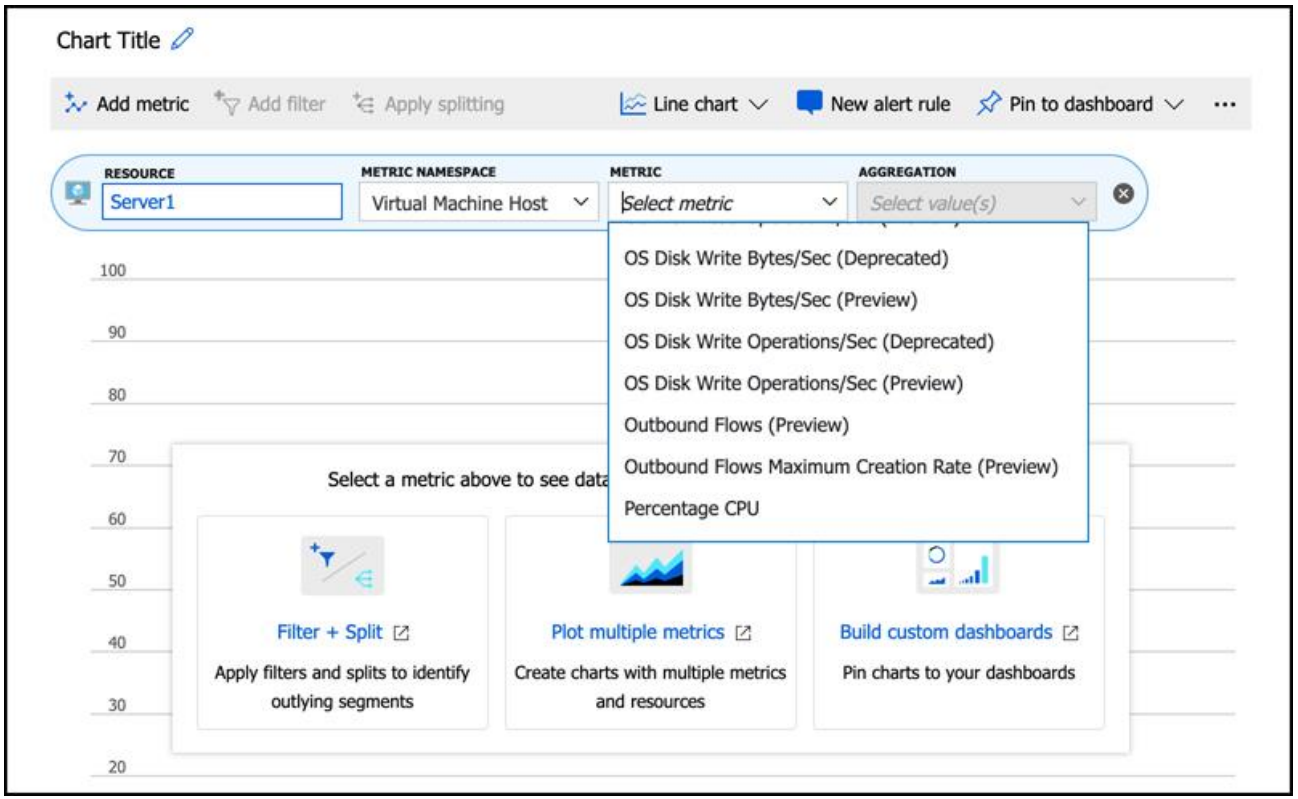


Figura 3-69 Métricas para máquinas virtuales

Tan pronto como seleccione una métrica, el gráfico se actualiza para mostrar un gráfico de esa métrica. Puede agregar métricas adicionales a su gráfico haciendo clic en **Agregar métrica** , como se muestra en la Figura 3-70 .

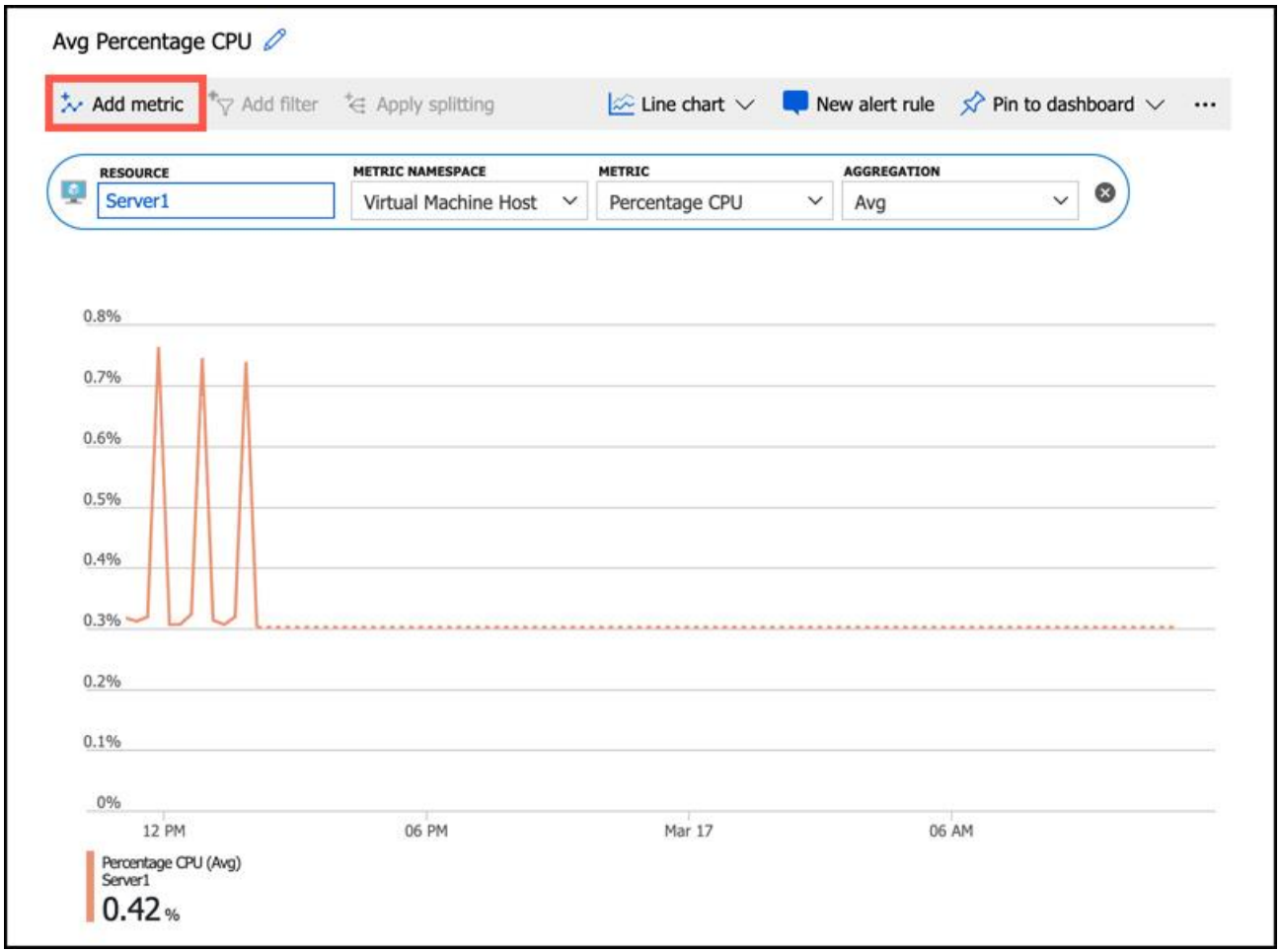


Figura 3-70 Supervisión del uso de CPU de VM

Al agregar varias métricas, querrá incluir solo las métricas que comparten una métrica común. Por ejemplo, si tuviera que agregar la métrica Bytes de lectura de disco al gráfico que se muestra en la Figura 3-70 , no tendría mucho sentido porque los Bytes de lectura de disco se miden en bytes y el porcentaje de CPU se mide como un porcentaje.

En la Figura 3-71 , hemos agregado Bytes de lectura de disco y Bytes de escritura de disco a un gráfico. Azure Monitor codifica en color cada métrica automáticamente para distinguir entre ellas. También hemos seleccionado el **Gráfico de área** como el tipo de gráfico para ver más claramente los patrones.

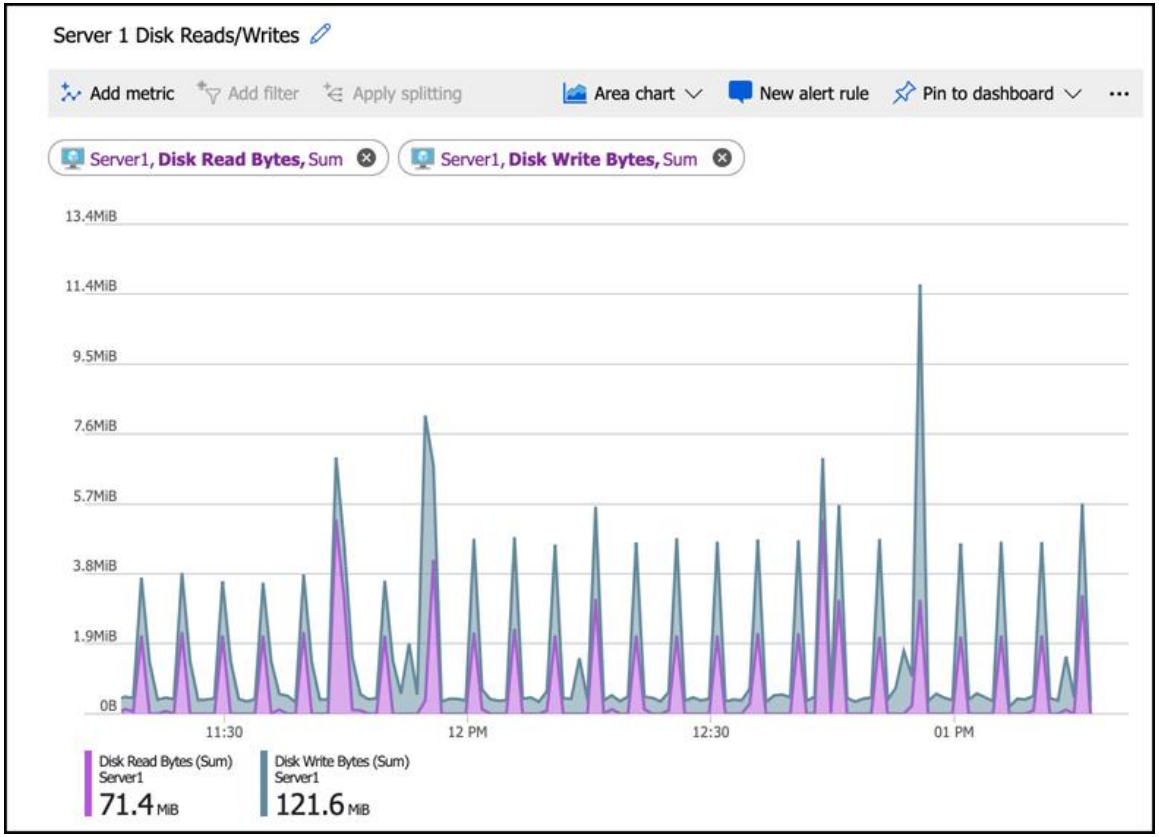


Figura 3-71 Gráfico que muestra el uso del disco

Por defecto, los gráficos se muestran para el último período de 24 horas, y el valor en tiempo real se muestra en el borde derecho del gráfico. Sin embargo, puede personalizar el período de tiempo que se muestra haciendo clic en el período de tiempo y ajustándolo a lo que desea ver, como se muestra en la Figura 3-72 .

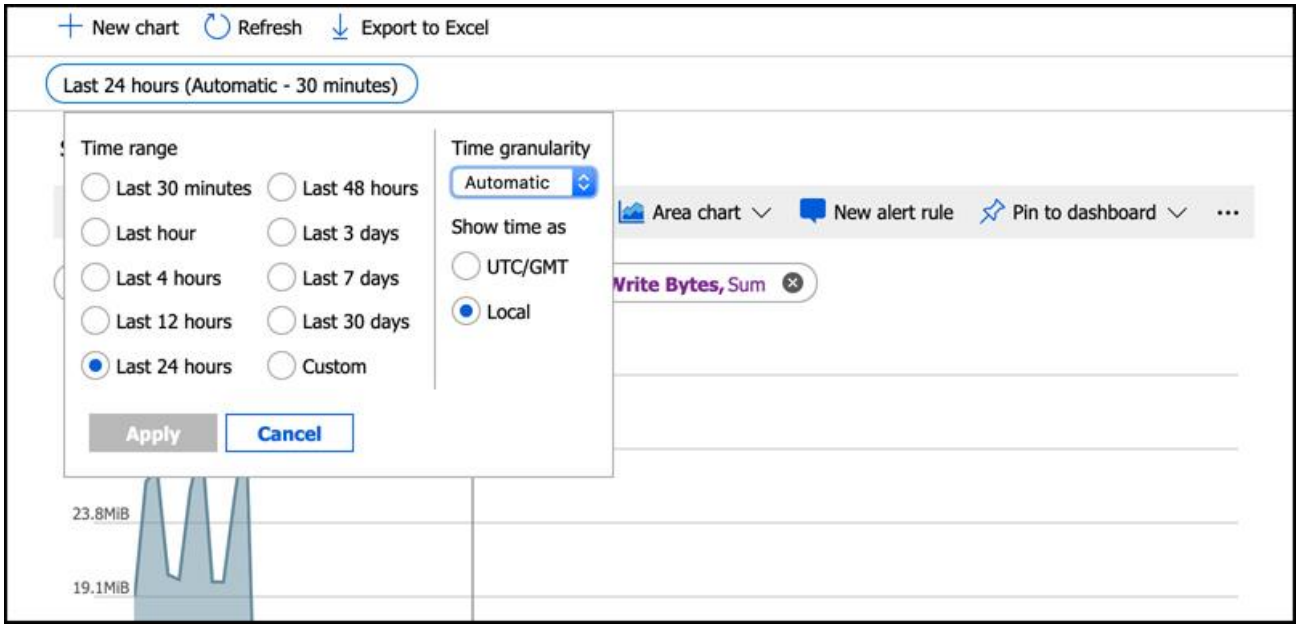


Figura 3-72 Cambio del marco de tiempo del gráfico

Una vez que tenga un gráfico que le resulte útil, puede anclar ese gráfico al tablero del portal haciendo clic en **Anclar al tablero** . Como se muestra en la Figura 3-73 , puede anclarlo al tablero actual, o puede anclarlo a un tablero específico para crear un tablero de monitoreo en el portal personalizado para un uso específico.

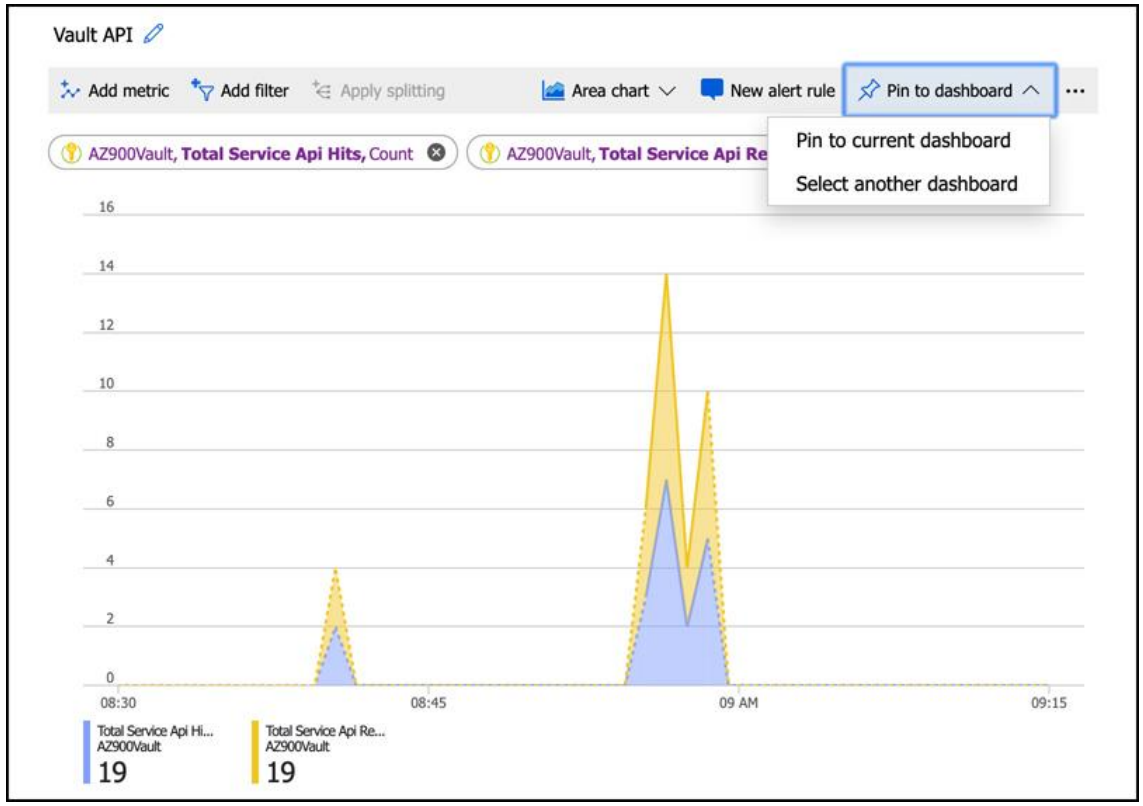


Figura 3-73 Anclar un gráfico

Las alertas de Azure Monitor pueden notificarle a usted u otras personas con un correo electrónico o mensaje de texto SMS, ejecutar un flujo de aplicación lógica, llamar a una aplicación de función, realizar una solicitud a un webhook y más, cuando se cumple una determinada condición. Las alertas se basan en reglas que usted define, y cuando se cumple la condición de una regla, una alerta realiza la acción que especifique.

Puede crear una regla de alerta que se configure automáticamente para las métricas que ha seleccionado en su gráfico haciendo clic en **Nueva regla de alerta** en la parte superior de su gráfico. También puede comenzar desde cero haciendo clic en **Alertas** en el menú de Azure Monitor, como se muestra en la Figura 3-74 , y luego haciendo clic en **Nueva regla de alerta** .

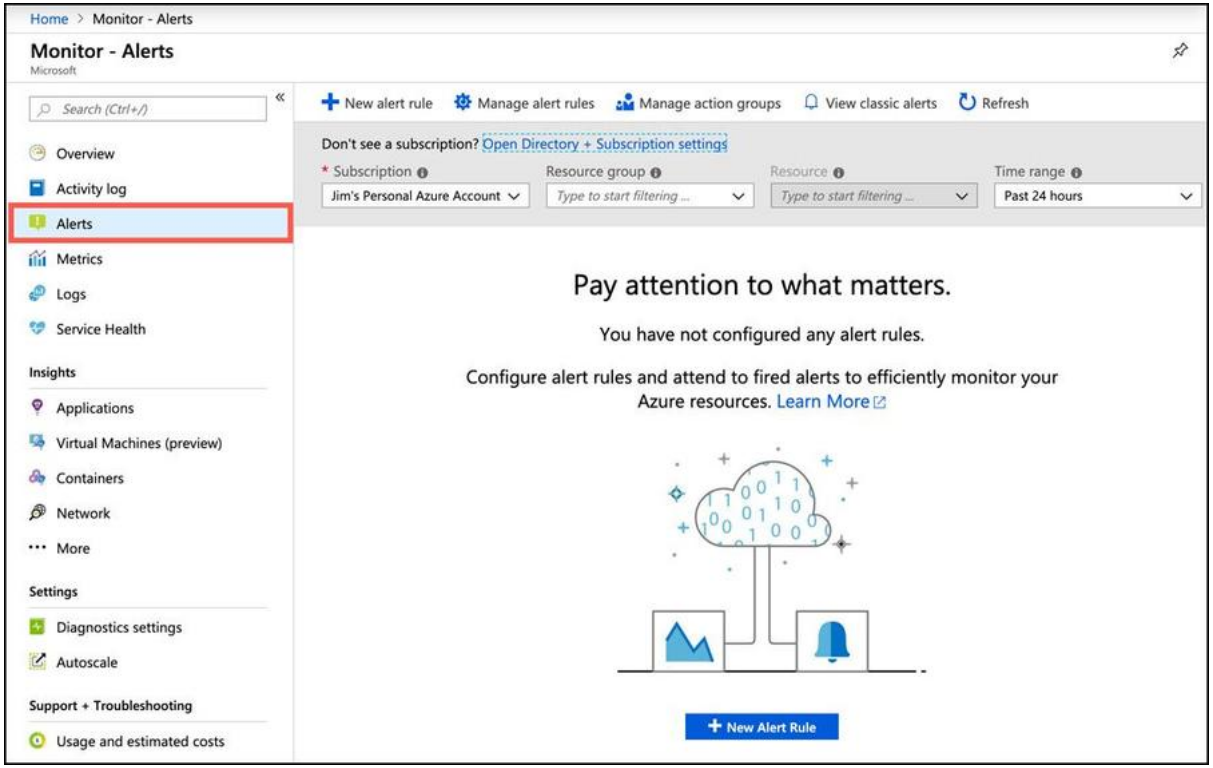


Figura 3-74 Crear una regla de alerta

Para comenzar su regla, haga clic en **Seleccionar** y seleccione el recurso para el que desea configurar una alerta. En la Figura 3-75 , hemos seleccionado mi VM para una nueva regla de alerta.

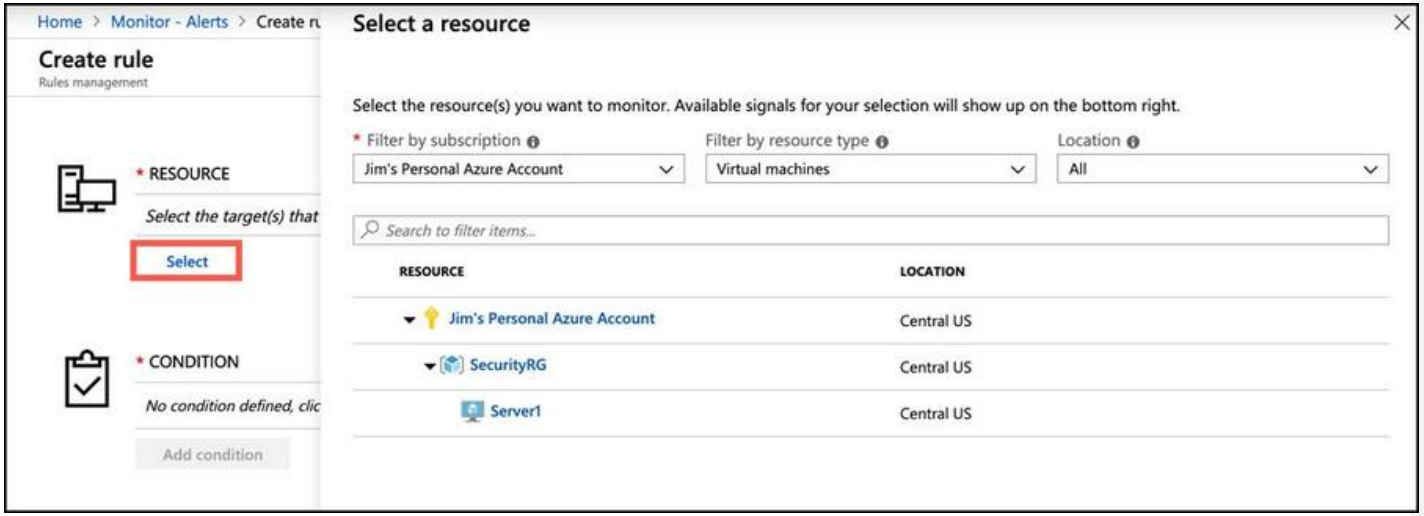


Figura 3-75 Selección de un recurso para una alerta

A continuación, deberá especificar la condición de su alerta. Haga clic en **Agregar condición** y luego seleccione la señal que desea monitorear para su alerta. En la figura 3-76 , configuramos una alerta basada en la señal de porcentaje de CPU de la VM.

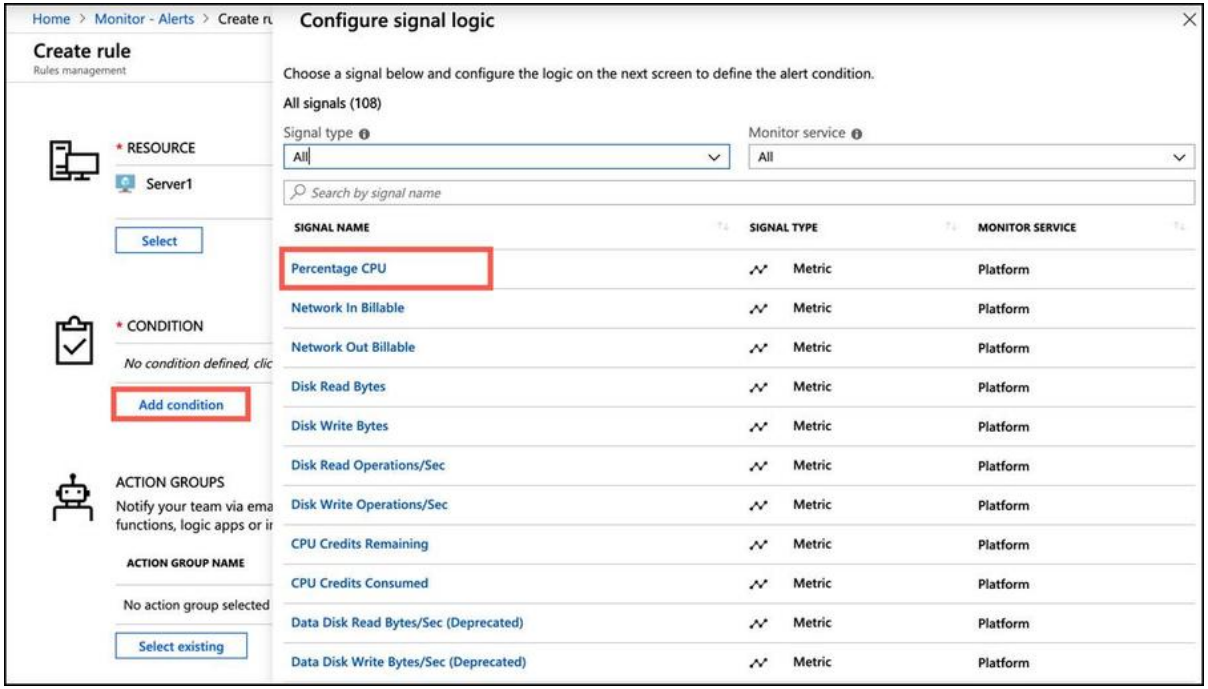


Figura 3-76 Configuración de una condición

Una vez que selecciona una señal, se configura la lógica de la señal. Como se muestra en la Figura 3-77 , Monitor muestra un gráfico interactivo de la señal que ha elegido, para que pueda tener una idea de cómo ha estado funcionando su recurso históricamente. Esto muestra las últimas cuatro horas de forma predeterminada, aunque puede ajustar el período del gráfico. Puede especificar un operador, tipo de agregación, umbral y hacer clic en **Listo** para crear la lógica de la alerta.

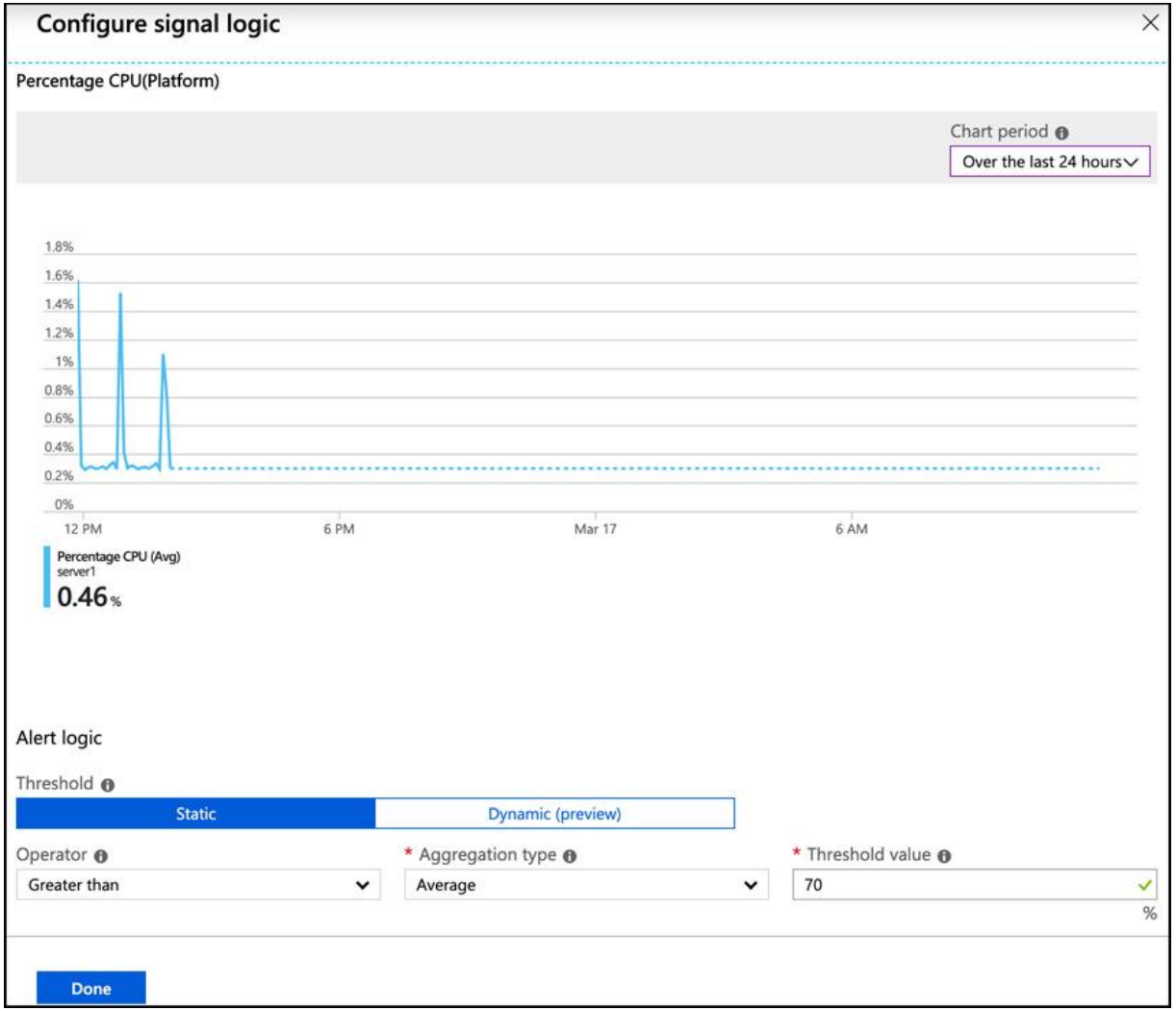


Figura 3-77 Lógica de regla de alerta

Nota **múltiples condiciones**

Una regla de alerta puede constar de múltiples condiciones. Por ejemplo, puede tener una regla que solo se active si el promedio de CPU es superior al 70% y el uso del disco también es alto. La decisión es tuya.

Cuando se activa una alerta, realiza una acción que usted especifica utilizando un *grupo de acciones* . Un grupo de acciones contiene una lista de acciones para realizar cuando se activa una alerta. Para crear un nuevo grupo de acción, haga clic en **Crear nuevo** , como se muestra en la Figura 3-78 .

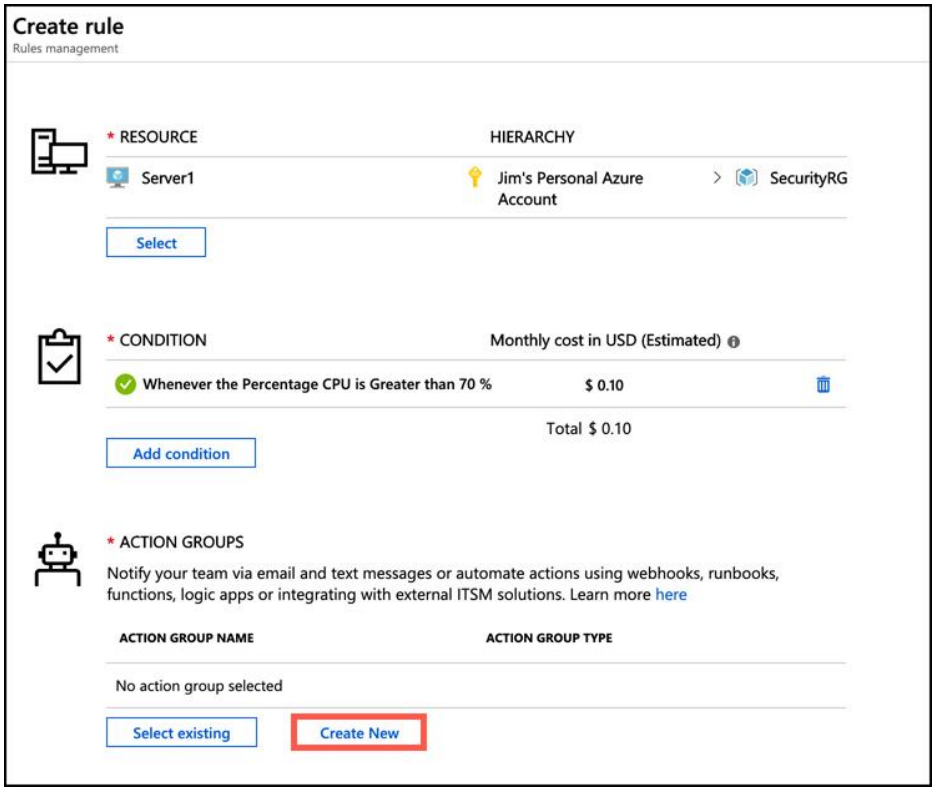


Figura 3-78 Crear un grupo de acción

En la Figura 3-79 , estamos creando una acción para notificar al director de TI. En este caso, la acción enviará un mensaje de texto al director de TI, y también enviará una notificación push mediante la aplicación Azure Mobile.

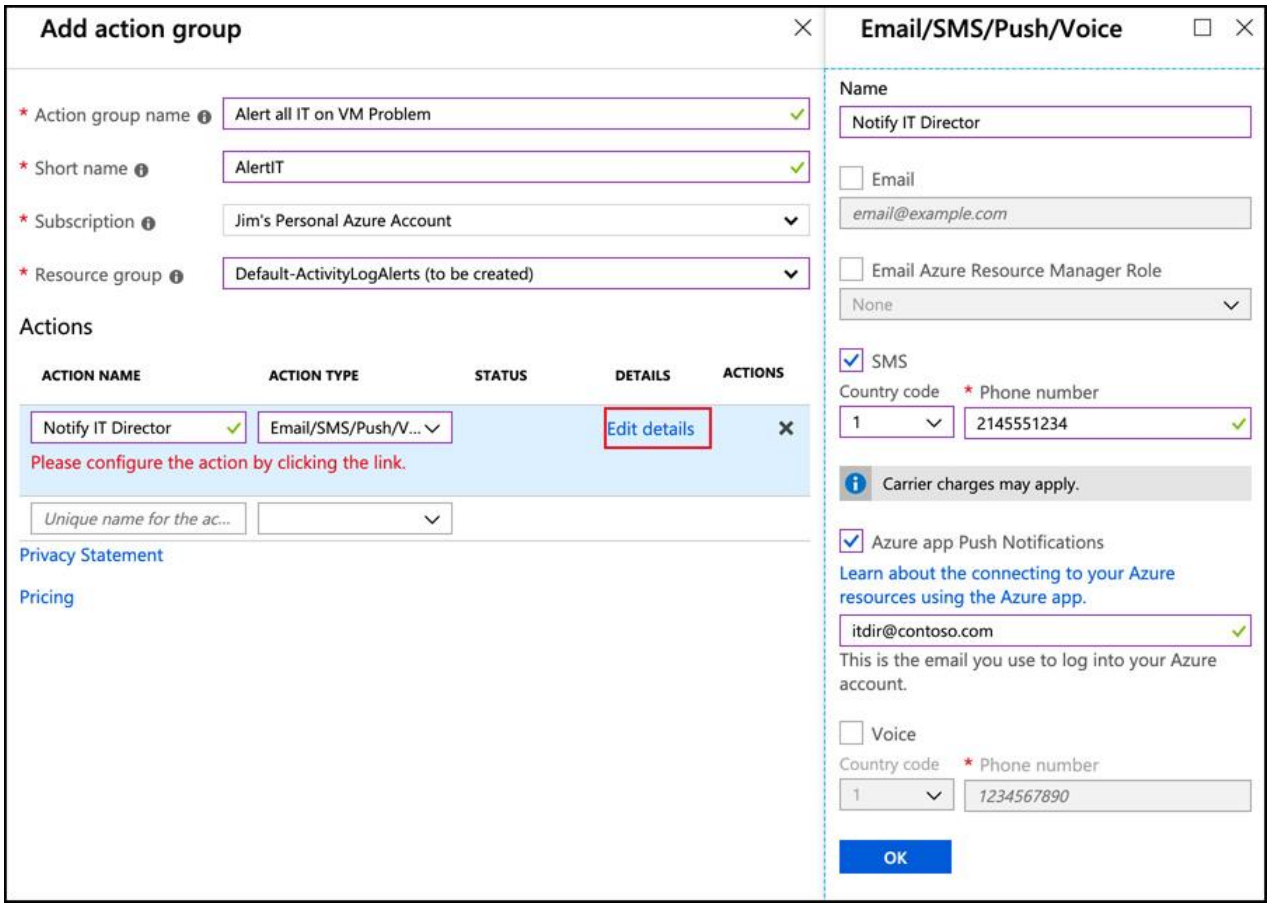


Figura 3-79 Crear una acción

Los grupos de acciones están diseñados para contener varias acciones que se ejecutan cuando se activa una alerta. En la Figura 3-80 , hemos editado una acción adicional para el grupo de acciones. Esta acción llama a una aplicación de función que ejecuta un código para reiniciar la máquina virtual.

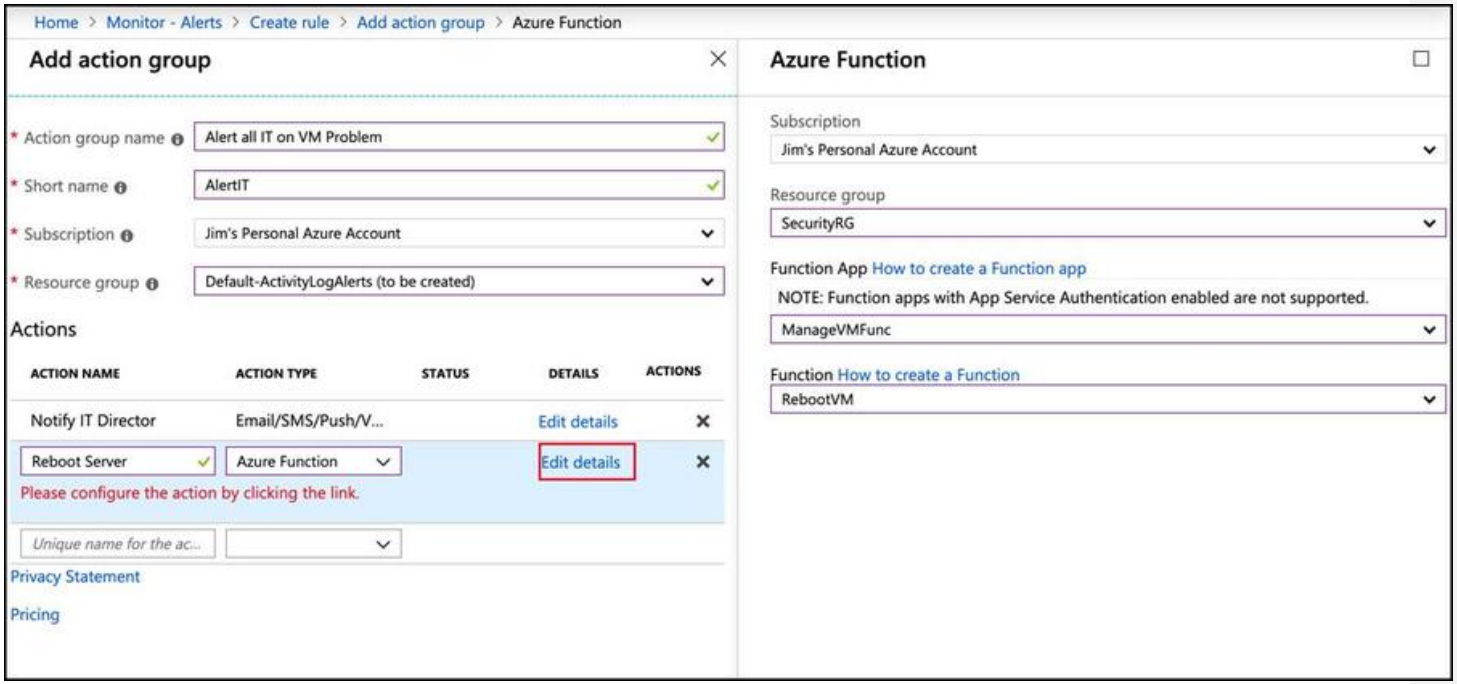


Figura 3-80 Agregar otra acción

Estado del servicio de Azure

Microsoft opera una página web de Estado de Azure donde puede ver el estado actual de los servicios de Azure en todas las regiones donde opera Azure. Si bien es una vista útil del estado general de Azure, el enorme alcance de la página web no lo convierte en la forma más efectiva de obtener una visión general del estado de sus servicios específicos. Azure Service Health puede proporcionarle una vista específica de sus recursos.

Para acceder a Service Health, haga clic en **Todos los servicios** y luego haga clic en **Service Health** como se muestra en la Figura 3-81 .

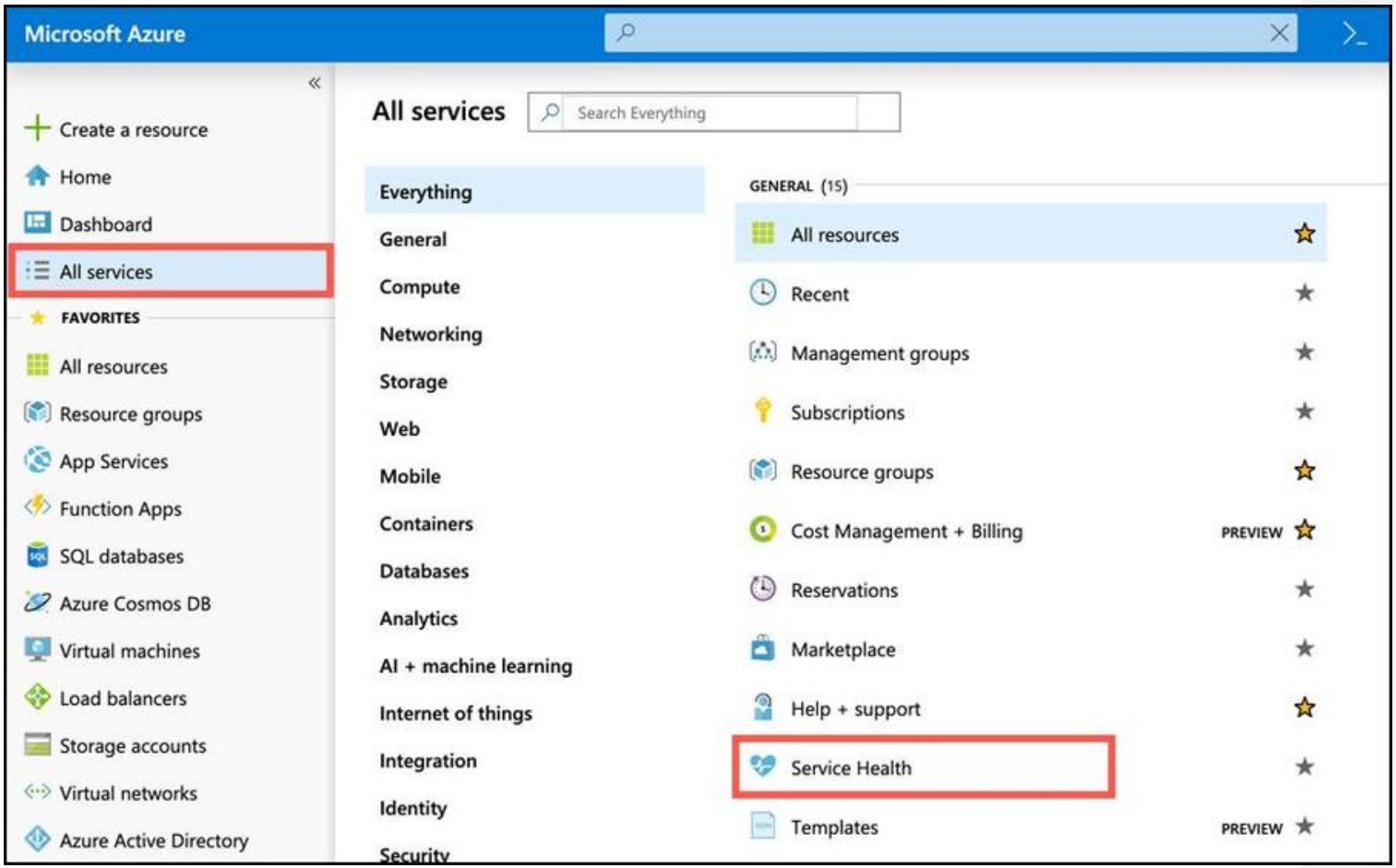


Figura 3-81 Estado del servicio de Azure

La Figura 3-82 muestra la hoja Estado del servicio que muestra el estado y el estado de mis recursos. El mapa que se muestra tiene dos puntos verdes que representan el estado de las dos regiones de Azure donde se implementan los recursos. Este mapa es específico, y al hacer clic en **Pin World Map Filtered to Dashboard** , puede tener una referencia rápida de la salud de Azure solo para las regiones donde tiene recursos.

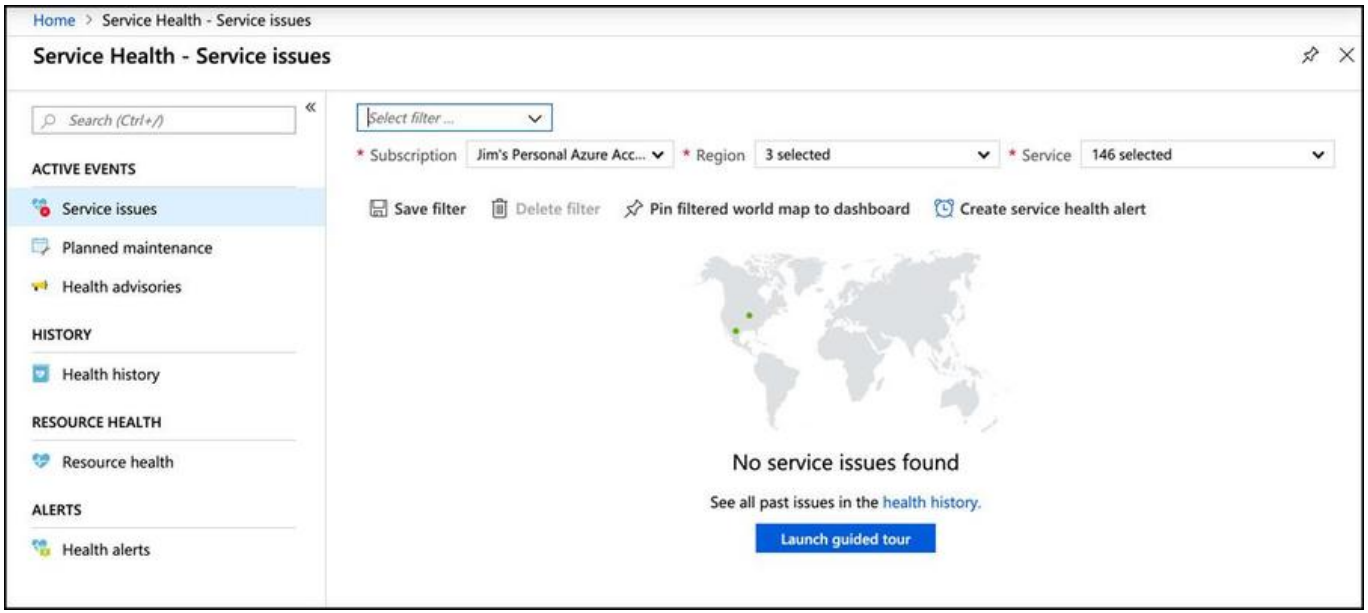


Figura 3-82 Problemas de servicio en el estado del servicio

También puede ver cualquier próximo mantenimiento planificado que pueda afectarlo haciendo clic en Mantenimiento planificado. Al hacer clic en Avisos de salud, puede ver información de salud que puede estar relacionada con su propia configuración y no es un problema en algún lugar de Azure.

Cuando un problema del servicio lo está afectando, verá detalles sobre el problema como se muestra en la Figura 3-83 . Además de los detalles completos del incidente, también tiene un enlace que hace referencia a los detalles del incidente. También puede descargar un PDF que contiene un aviso oficial de Microsoft del incidente.

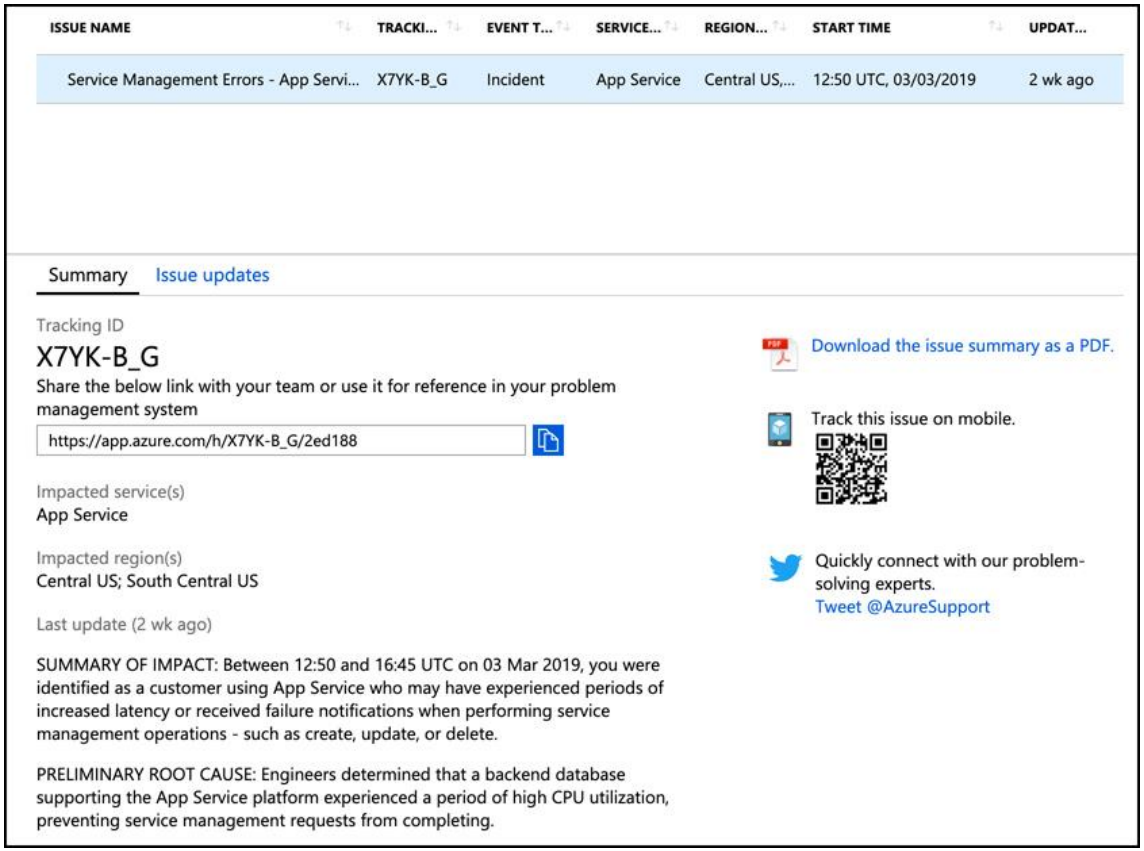


Figura 3-83 Incidente de Azure Service Health

Tanto Azure Monitor como Azure Service Health son fundamentales para la vista general de sus recursos de Azure. Azure Monitor está orientado a monitorear el costo y el rendimiento de sus recursos y alertarlo a usted y a otros cuando las condiciones lo justifiquen. Azure Service Health, por otro lado, es el punto de verdad único para obtener información sobre el estado de Azure y cómo los incidentes de Azure están afectando sus recursos. La combinación de estos dos servicios le proporciona todas las herramientas que necesita para mantenerse al día con sus recursos de Azure y qué tan bien están funcionando.

HABILIDAD 3.6: COMPRENDER LOS ESTÁNDARES DE PRIVACIDAD, CUMPLIMIENTO Y PROTECCIÓN DE DATOS EN AZURE

A medida que avanza a la nube, descarga parte de la responsabilidad de sus servicios y datos a su proveedor de la nube. Esto incluye parte de la responsabilidad del cumplimiento de las normas de protección de datos. Aunque el proveedor de la nube se haga cargo de parte de esa carga por usted, es vital que tenga confianza en el proveedor de la nube y que confíe en ellos para mantener el cumplimiento.

Hay muchas normas que las empresas deben cumplir. Por ejemplo, en 2016, la Unión Europea aprobó el Reglamento General de Protección de Datos, o GDPR. El RGPD regula la forma en que se manejan los datos personales de las personas con la UE, pero también controla los datos personales que se exportan fuera de la UE. Las empresas que hacen negocios en países de la UE están legalmente obligadas a cumplir con el GDPR.

Una forma en que las organizaciones pueden asegurarse de cumplir con el GDPR y otras regulaciones que regulan los datos es mantener el cumplimiento de los estándares de toda la industria centrados en ayudar a las organizaciones a mantener segura la información. Una de esas normas es la norma 27001 de la Organización Internacional de Normas (ISO). Las empresas que cumplen con el estándar ISO 27001 pueden confiar en que mantienen las mejores prácticas necesarias para mantener segura la información. De hecho, muchas compañías no harán negocios con un proveedor de la nube a menos que puedan probar el cumplimiento de la norma ISO 27001.

Los sistemas que manejan datos gubernamentales deben mantener el cumplimiento de los estándares que mantiene el Instituto Nacional de Estándares y Tecnología, o NIST. El NIST SP 800-53 es una publicación de NIST que describe todos los requisitos para los sistemas de información que tratan con datos gubernamentales. Para que cualquier agencia gubernamental use un servicio, primero debe probar el cumplimiento de NIST SP 800-53.

Microsoft aborda estos requisitos de cumplimiento en toda su infraestructura de muchas maneras diferentes.

Esta sección cubre:

- Declaración de privacidad de Microsoft
- Centro de confianza
- Portal de confianza de servicio
- Gerente de Cumplimiento
- Gobierno azur
- Alemania azur

Declaración de privacidad de Microsoft

La declaración de privacidad de Microsoft es una declaración exhaustiva de Microsoft que describe lo siguiente en relación con el manejo de datos y su información personal.

- Datos personales que Microsoft recopila
- Cómo usa Microsoft los datos personales
- Motivos por los que Microsoft comparte datos personales
- Cómo acceder y controlar sus datos personales recopilados por Microsoft
- Cómo usa Microsoft las cookies y tecnologías similares
- Qué organizaciones que le proporcionan software de Microsoft pueden hacer con sus datos
- Qué datos se comparten cuando usa una cuenta de Microsoft con un tercero
- Detalles específicos sobre cómo Microsoft protege los datos, dónde se procesan y las políticas de retención

Microsoft enlaza con la declaración de privacidad en todas las comunicaciones oficiales, y puede acceder a la declaración de privacidad en línea en: ***https://aka.ms/privacystatement*** .

Centro de confianza

El Centro de confianza es un portal web donde puede aprender todo sobre el enfoque de Microsoft en materia de seguridad, privacidad y cumplimiento. Puede acceder al Centro de confianza navegando a: *https://www.microsoft.com/en-us/trustcenter/default.aspx* .

Explore el Centro de confianza utilizando los menús desplegables en la parte superior de la página como se muestra en la Figura 3-84 . A medida que evolucionan los estándares y el cumplimiento, siempre puede encontrar la información más reciente en el sitio web del Centro de confianza.

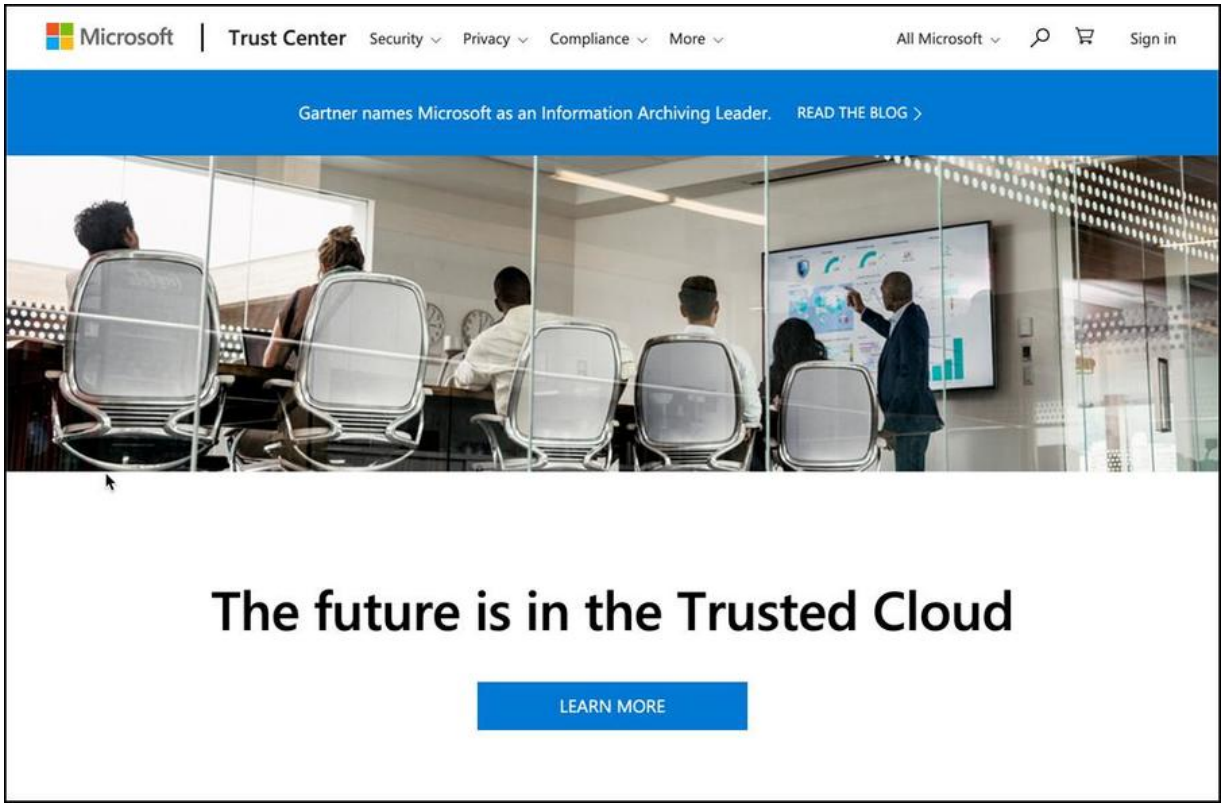


Figura 3-84 Centro de confianza de Microsoft

Portal de confianza de servicio

El Service Trust Portal (STP) es un portal que proporciona acceso a varias herramientas de cumplimiento que Microsoft proporciona para que pueda realizar un seguimiento del cumplimiento en sus aplicaciones que se ejecutan en las diversas plataformas de Microsoft. Puede acceder al STP navegando a: ***https://aka.ms/STP*** . La Figura 3-85 muestra la página de inicio de STP.

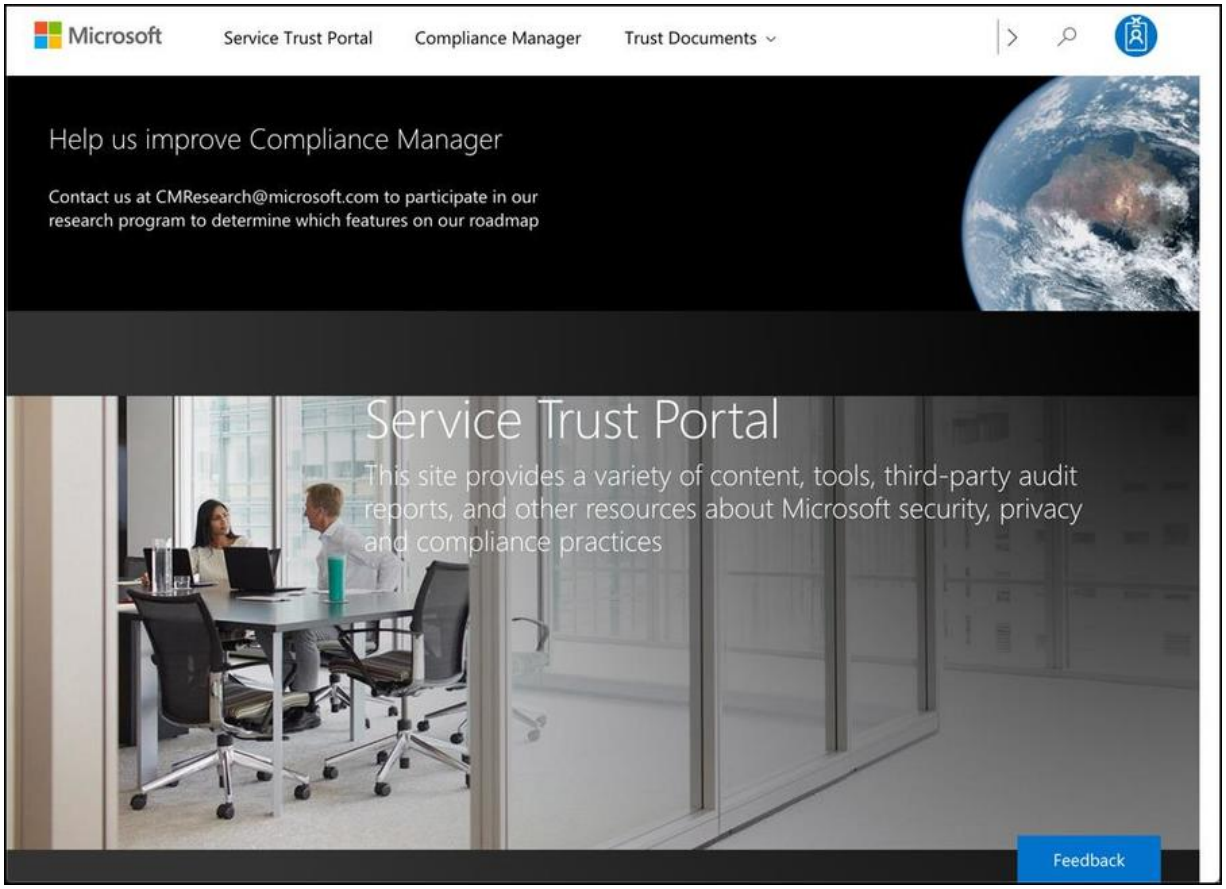


Figura 3-85 Portal de Azure Service Trust

El STP es un punto de partida para los siguientes recursos.

- **Administrador de cumplimiento** Una herramienta para administrar su cumplimiento normativo en la nube.
- **Informes de auditoría Informes** completos y recursos que le permiten ver detalles sobre cómo Microsoft mantiene el cumplimiento.
- **Información de protección de datos** Detalles completos sobre cómo Microsoft diseña sus ofertas en la nube para garantizar que los datos de los clientes estén protegidos.
- Información de **privacidad** relacionada con la forma en que Microsoft lo ayuda a mantener el cumplimiento de GDPR.

Gerente de Cumplimiento

Compliance Manager es una herramienta dentro del STP que facilita la visualización de su cumplimiento con los estándares de la industria. El Administrador de cumplimiento también proporciona detalles sobre cómo puede mejorar el cumplimiento, y para aquellas áreas donde el cumplimiento es responsabilidad de Microsoft, proporciona detalles completos sobre cómo Microsoft mantiene el cumplimiento.

Para acceder a Compliance Manager, haga clic en Compliance Manager en la parte superior de la página STP. El Administrador de cumplimiento le permite realizar un seguimiento de su cumplimiento con las aplicaciones relacionadas al agruparlas en grupos a los que puede asignar el nombre que desee. Cada grupo que cree está representado por un mosaico en el Administrador de cumplimiento, y puede ver de un vistazo cuánto ha avanzado en el cumplimiento en cada grupo, como se muestra en la Figura 3-86 .

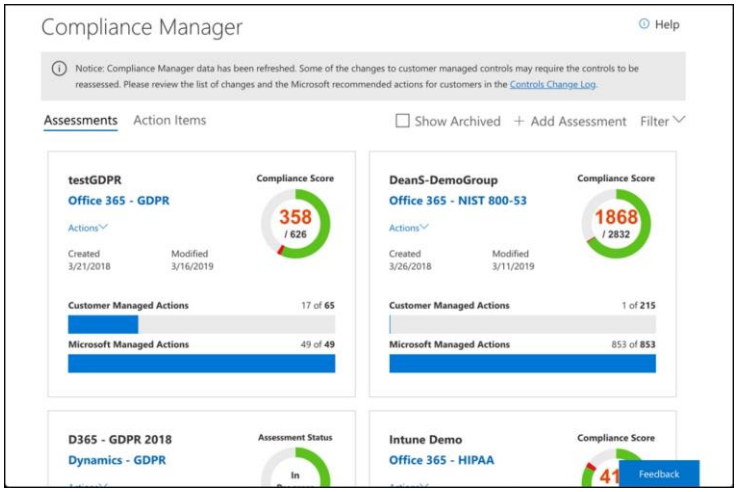


Figura 3-86 Administrador de cumplimiento

Puede agregar una nueva evaluación haciendo clic en **Agregar evaluación** . Puede agregar una evaluación a un grupo existente o puede crear un nuevo grupo como se muestra en la Figura 3-87 .

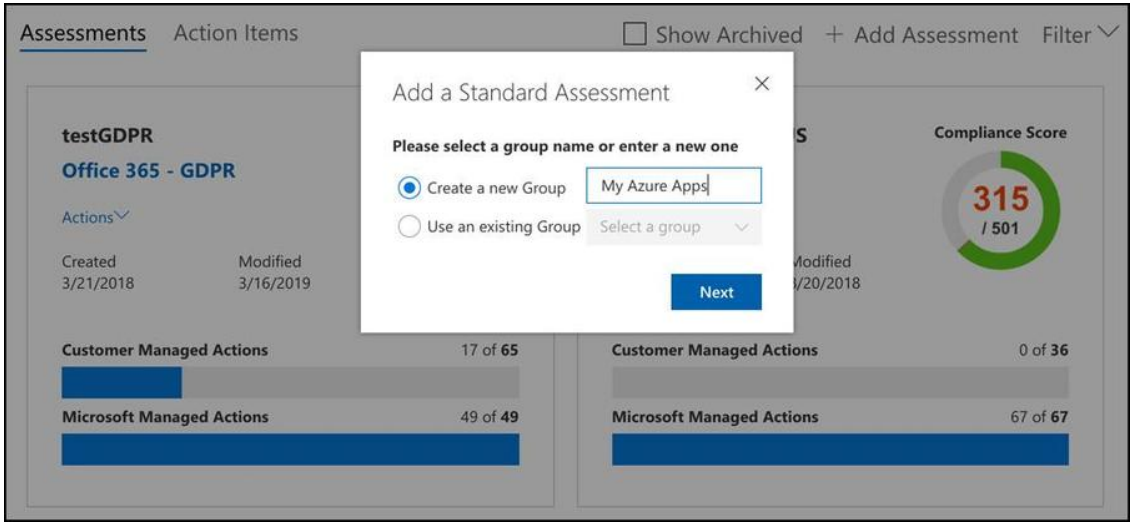


Figura 3-87 Agregar una nueva evaluación

Puede elegir evaluar Azure, Office 365, Microsoft Dynamics y más. También puede elegir el estándar con el que desea evaluar. En la Figura 3-88 , hemos elegido evaluar los recursos de Azure frente a GDPR.

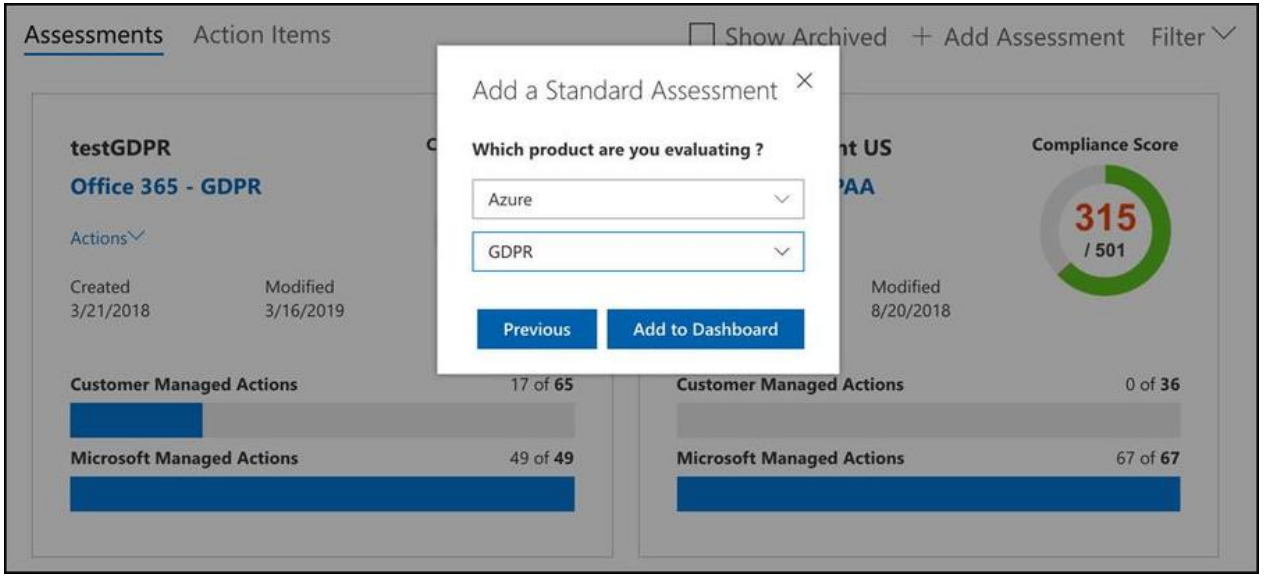


Figura 3-88 Evaluación del cumplimiento de GDPR

En función de los productos que estamos evaluando, Compliance Manager sabe qué partes del cumplimiento son responsabilidad de Microsoft y cuáles son responsabilidad del cliente. En la Figura 3-89 , se muestra una evaluación recién creada en Compliance Manager. Las responsabilidades de Microsoft se muestran en la parte superior de la lista y ya están completas. Mis responsabilidades también aparecen en la lista, y describen todos los requisitos que debemos cumplir para cumplir con el RGPD.

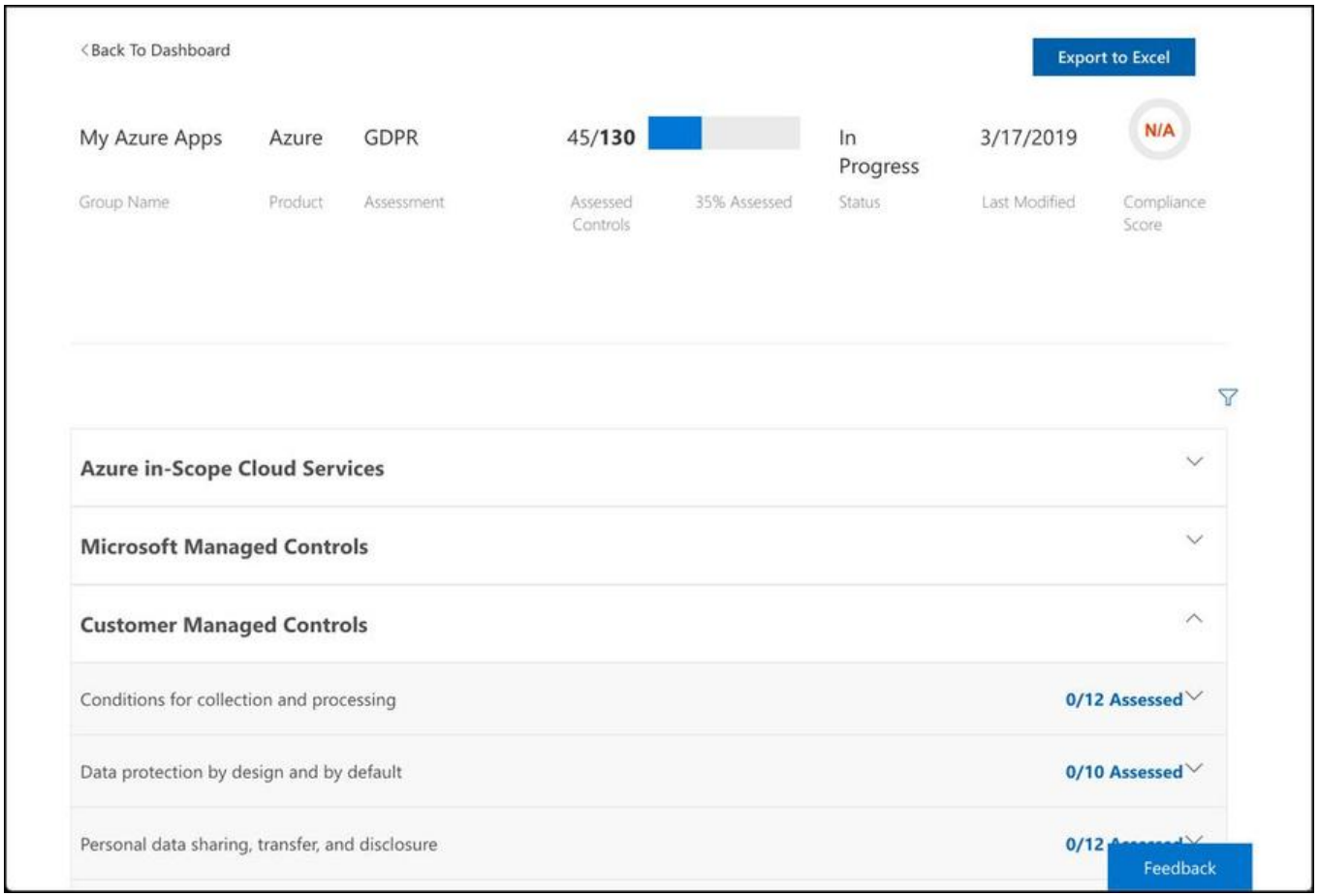


Figura 3-89 Una evaluación de **GDPR** en el Administrador de cumplimiento

Si hace clic en uno de los controles de Microsoft, verá detalles sobre lo que ha hecho Microsoft para garantizar el cumplimiento. En el control que se muestra en la Figura 3-90 , puede ver cómo Microsoft cumplió con los artículos específicos de GDPR, cuándo se probó y cómo se probó.

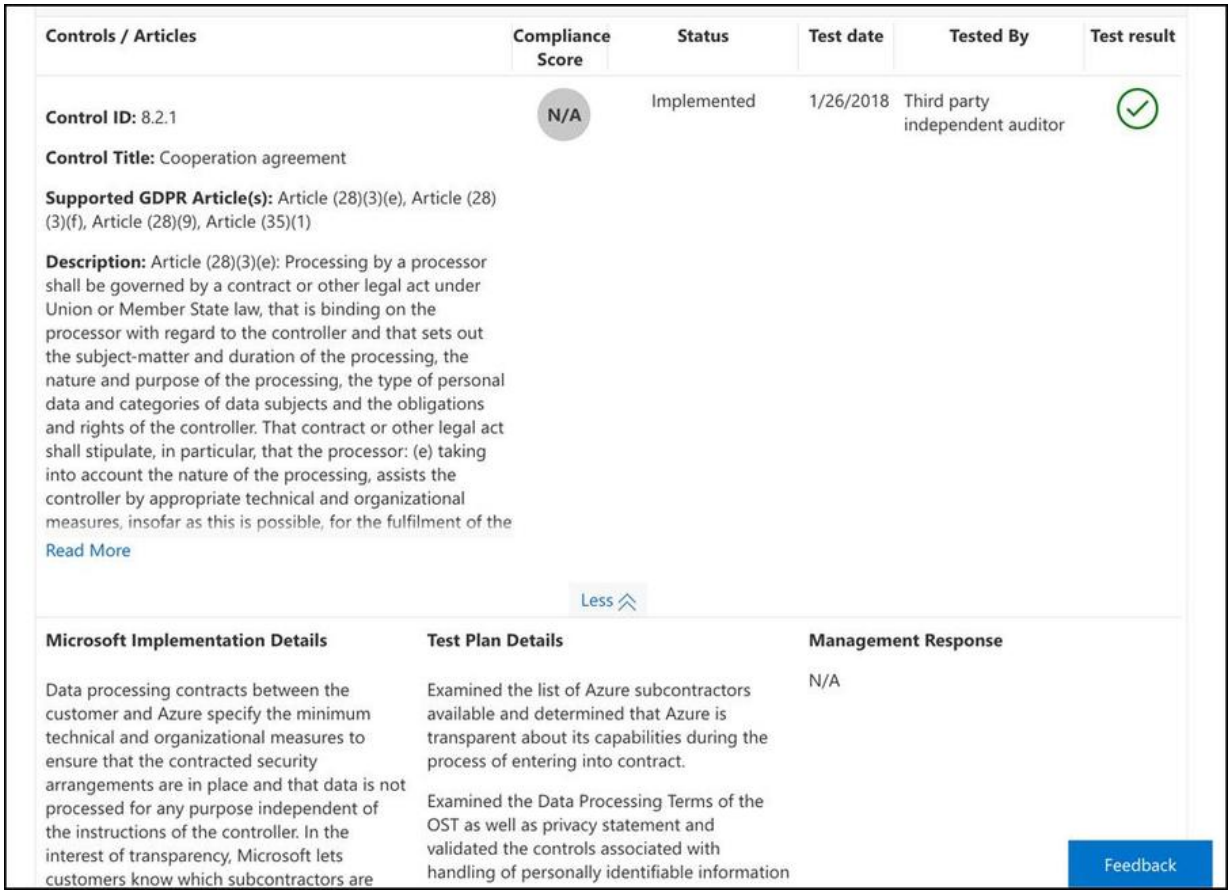


Figura 3-90 Cumplimiento de Microsoft con artículos GDPR

Si hace clic en un control administrado por el cliente, puede ver detalles sobre lo que debe hacer para cumplir. En la Figura 3-91 , se muestran detalles sobre lo que debe hacer para cumplir con el Artículo GDPR (5) (1) (b). Tiene la opción de asignar esta tarea a un usuario específico si lo desea, y puede hacer clic en Administrar documentos para cargar documentos de respaldo en el Administrador de cumplimiento.

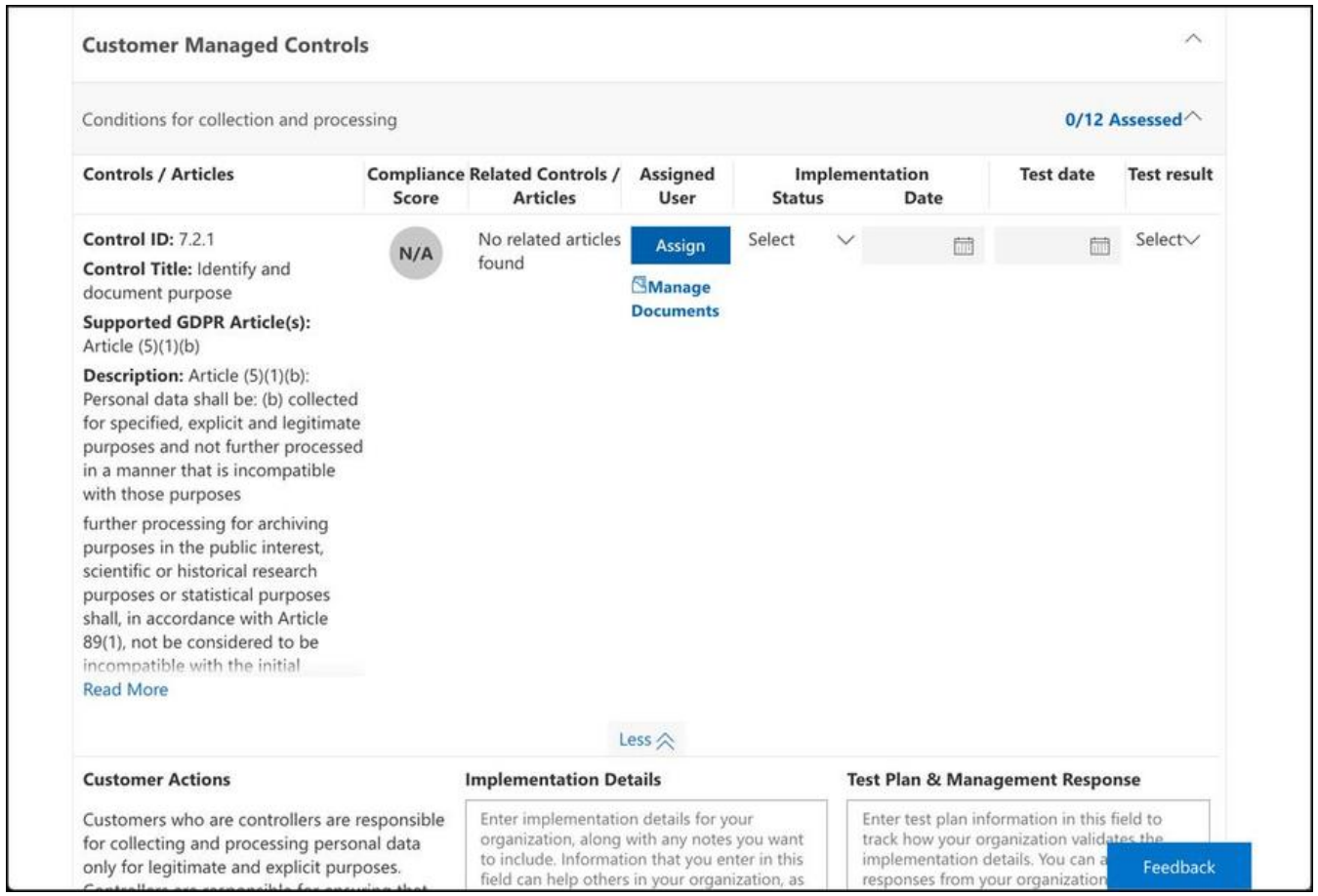


Figura 3-91 Mis requisitos de cumplimiento

Con este método de evaluación, siempre puede determinar si sus aplicaciones son compatibles. La carga de comprender ciertos estándares y regulaciones se elimina porque el Administrador de Cumplimiento lo gestiona por usted.

Gobierno azur

El cumplimiento de GDPR y las otras normas mencionadas se relaciona con la privacidad de los datos de un individuo. Algunos escenarios de cumplimiento del gobierno de los Estados Unidos requieren que los datos permanezcan dentro de los Estados Unidos de América y que solo los ciudadanos de los Estados Unidos tengan acceso a los sistemas utilizados para almacenar esos datos. El cumplimiento de estos requisitos es imposible con la nube pública, por lo que Microsoft ha desarrollado centros de datos de Azure completamente aislados que forman la nube de Azure Government.

Los centros de datos de Azure Government están separados de los centros de datos públicos. Todos los empleados que trabajan en Azure Government son examinados y son ciudadanos de los EE. UU. Incluso los empleados de Microsoft que brindan soporte técnico a los clientes de Azure Government deben ser ciudadanos estadounidenses.

Debido a que Microsoft también quería permitir una comunicación compatible entre la nube de Azure Government y los sistemas gubernamentales locales, también desarrollaron ubicaciones dedicadas de Microsoft ExpressRoute que están completamente aisladas de otras redes de Azure y que usan sus propios componentes de fibra óptica dedicados.

Azure Government no es solo para agencias del gobierno federal. Las ciudades y los municipios también se aprovechan de Azure Government para el cumplimiento. Cuando un cliente se inscribe en Azure Government, Microsoft examina a ese usuario para asegurarse de que sea representante de una agencia gubernamental. Solo entonces se les otorga una suscripción a Azure Government.

La nube de Azure Government tiene las mismas características y servicios que la nube pública, pero existen pequeñas diferencias. Por ejemplo, el portal de Azure Government se encuentra en *https://portal.azure.us en* lugar de *https://portal.azure.com* . Las URL para los servicios de Azure también usan el dominio de nivel superior .us, por lo que si crea una aplicación web del Servicio de aplicaciones en Azure Government, su nombre de dominio predeterminado es *https://webapp.azurewebsites.us* . Sin embargo, fuera de esa diferencia, todo lo demás es igual, por lo que los desarrolladores que tengan un conjunto de habilidades en el desarrollo de la nube en Azure descubrirán que sus habilidades se transfieren directamente al Gobierno de Azure.

El Departamento de Defensa de los Estados Unidos tiene requisitos de cumplimiento adicionales llamados Autorización Provisional de Nivel de Impacto 5 del DoD. El cumplimiento de esto se relaciona con la información no clasificada controlada que requiere niveles adicionales de protección. Estos requisitos adicionales de DoD se cumplen mediante un subconjunto de centros de datos dentro de Azure Government que están aprobados para el uso de DoD.

Alemania azur

Al igual que Azure Government, Azure Germany es un sistema en la nube distinto que está diseñado para satisfacer necesidades específicas de cumplimiento. En el caso de Azure Alemania, esas necesidades se relacionan con los estrictos requisitos impuestos por la UE. Azure Alemania está disponible para clientes que hacen negocios en la UE, la Asociación Europea de Libre Comercio y el Reino Unido.

Los centros de datos de Azure Alemania están ubicados físicamente en Alemania y son operados bajo estrictas medidas de seguridad por una compañía local llamada T-Systems International (una subsidiaria de Deutsche Telekom) que opera como administrador de datos. El administrador de datos tiene control total sobre todos los datos almacenados en Azure Alemania y toda la infraestructura utilizada para almacenar esos datos. Microsoft participa en la administración de solo aquellos sistemas que no tienen acceso alguno a los datos del cliente.

EXPERIMENTO MENTAL

Apliquemos los conceptos relacionados con la seguridad, la privacidad, el cumplimiento y la confianza que ha aprendido en este capítulo a un experimento mental. Puede encontrar la respuesta a este experimento mental en la sección que sigue.

ContosoPharm ha asegurado un contrato para realizar un desarrollo farmacéutico para el Departamento de Defensa de los Estados Unidos. Debido a que este trabajo será de naturaleza extremadamente sensible, hay varios requisitos que deben cumplir antes de que el Departamento de Defensa apruebe el proyecto.

El acceso a la aplicación por parte del personal del Departamento de Defensa será a través de una interfaz web a través de dispositivos que están conectados a Internet en el campo. El DoS requiere controles de seguridad estrictos para cualquier acceso a la aplicación, y es importante que la aplicación esté protegida contra ataques maliciosos que puedan parecer tráfico legítimo. Este requisito se aplica tanto a las máquinas virtuales en la nube como a las locales.

También se requiere que la configuración de la aplicación proteja contra situaciones en las que se robe la contraseña de alguien. Si alguien fuera del Departamento de Defensa intenta iniciar sesión en la aplicación con una contraseña robada, se debe denegar ese inicio de sesión.

La aplicación usa mucho la Base de datos SQL de Azure, y los usuarios de la aplicación deberían poder crear sus propias tablas de base de datos. Sin embargo, no deberían poder dar acceso a nadie a la base de datos que el administrador no le otorga permiso explícito. Además de eso, los usuarios de la parte de la base de datos de la aplicación tienen un horario de rotación, por lo que debe ser muy fácil revocar el acceso sin tener que cambiar ninguna contraseña de la base de datos.

Algunos de los sistemas se ejecutarán en las instalaciones debido al acceso a información confidencial. El administrador del sistema desearía una interfaz única donde se pueda monitorear el estado de seguridad de todos los recursos en la nube y los recursos locales. A medida que los nuevos sistemas se ponen en línea, el administrador debe poder garantizar que se cumplan los requisitos de DoD para el software antivirus.

Una VM en la aplicación necesitará ser administrada remotamente, pero un requisito del DoD es que los puertos de administración remota en la máquina no pueden dejarse abiertos. Por lo tanto, necesitan que sugiera una forma en que puedan administrar de forma remota y segura la VM.

El componente de almacenamiento en caché en la aplicación contiene datos confidenciales que están protegidos por una clave RSA cifrada. El DoD requiere que la clave necesaria para acceder a los datos en caché no se almacene en ningún lugar dentro de la aplicación. Se requiere que se otorgue acceso a la clave a la aplicación cuando sea necesario, pero solo cuando sea necesario.

Durante el desarrollo de la aplicación, la información se compartirá en documentos de Office y en correos electrónicos. Algunas de las personas que recibirán esta información no son empleados del Departamento de Defensa, por lo que parte de esta información se enviará fuera del Departamento de Defensa. Aun así, es un requisito que nadie más que el destinatario de los datos pueda leerlos, y no deberían poder compartirlos con otros.

El departamento de TI del DoD tiene parámetros operativos que todas las máquinas virtuales deben cumplir para su disponibilidad. Estas métricas giran en torno al uso del disco, la utilización de la CPU y el uso de la memoria. Cuando las métricas caen fuera del funcionamiento normal, es fundamental que se tomen medidas de inmediato, por lo que el departamento de TI ha desarrollado algunas secuencias de comandos que pueden ejecutar rápidamente para abordarlo. Si es posible, les gustaría automatizar este proceso para que el sistema se cuide solo si no hay nadie disponible para resolver un problema de inmediato.

Finalmente, la aplicación debe cumplir con los estándares DoD Impact Level 5, y también se debe mantener la privacidad de los datos de cada individuo.

EXPERIENCIAS DE PENSAMIENTO RESPUESTAS

Esta sección cubre las respuestas al experimento mental.

Para proteger las máquinas virtuales en la nube del tráfico malicioso, se puede implementar Azure Firewall en la red. Esto puede ayudar a proteger del tráfico que de otro modo parece legítimo debido a la capacidad de Azure Firewall de recordar el estado de una conexión. Para aplicar el mismo nivel de protección a las máquinas locales, el Departamento de Defensa puede usar Protección contra amenazas avanzada. Al instalar sensores ATP en las instalaciones, el DoD puede garantizar que estos recursos locales estén protegidos.

Para evitar que alguien inicie sesión en el sistema con una contraseña robada, el DoD debe implementar la autenticación multifactor. MFA requerirá que los usuarios no solo tengan una contraseña, sino que también tengan acceso a un dispositivo aprobado asociado con ellos.

Para dar a los usuarios la capacidad de crear tablas de bases de datos, pero no dar acceso a nadie más, DoD debe crear usuarios en su Azure Active Directory y asignar roles RBAC a las bases de datos SQL. Debido a que los usuarios con acceso RBAC no están usando una contraseña asociada con la base de datos para leer datos, el acceso puede ser revocado rápidamente cuando sea necesario sin tener que cambiar una contraseña en la base de datos.

Azure Security Center puede proporcionar información sobre el estado de seguridad de los recursos en una sola interfaz. Security Center también mostrará el incumplimiento de las máquinas virtuales donde la protección de punto final no está instalada, y el DoD podrá instalar fácilmente el antivirus en una o más máquinas virtuales con solo hacer clic en un botón.

Para la única VM que debe administrarse de forma remota, DoD puede habilitar el acceso JIT en Security Center. Esto les permite dejar los puertos de administración cerrados hasta que un usuario solicite acceso, e incluso puede especificar su dirección IP específica para el acceso, lo que protegerá aún más la VM. Una vez transcurrido el tiempo de acceso, se cierran los puertos de administración.

Para proteger la clave RSA utilizada con su componente de almacenamiento en caché, el DoD puede usar Azure Key Vault. También pueden usar Key Vault para generar la clave si lo desean. Cuando la aplicación necesita la clave, puede acceder a ella a través de una URL segura.

Para proteger la información en correos electrónicos y documentos, incluidos los enviados fuera del DoD, se puede usar Azure Information Protection. Al clasificar los correos electrónicos como Confidenciales y solo para destinatarios, se protegerá el acceso a la información por correo. Estas mismas protecciones se pueden aplicar a sus documentos de Office.

Azure Monitor se puede usar para monitorear máquinas virtuales y garantizar que operen dentro de los parámetros operativos. Se puede crear un grupo de alertas que se activará cuando lo desee, y debido a que una alerta puede llamar a un webhook, una aplicación de función o iniciar un flujo de aplicación lógica, hay muchas opciones para automatizar los scripts que usan para resolver problemas, incluso si nadie alrededor para ver el problema de inmediato.

Para cumplir con los estándares DoD Impact Level 5, la aplicación deberá estar alojada en un centro de datos aprobado por DoD dentro de Azure Government. El DoD también puede usar el Administrador de cumplimiento para garantizar que se cumplan los estándares de privacidad de datos para la aplicación.

RESUMEN DEL CAPÍTULO

La seguridad, el cumplimiento, la privacidad y la confianza son las piedras angulares de Microsoft Azure, y Microsoft ha demostrado su compromiso con estos principios al proporcionar herramientas y servicios líderes en la industria para ayudarlo. En este capítulo, ha aprendido sobre muchas de estas herramientas y servicios.

Aquí hay un resumen de lo que se cubrió en este capítulo:

- El vector de ataque principal para las aplicaciones en la nube es la red, y Azure Firewall es un firewall con estado que puede proteger su red de ataques.
- Todo el tráfico al firewall está bloqueado de manera predeterminada y las reglas están configuradas para permitir que pase cierto tráfico.
- Se utiliza una tabla de ruta para dirigir el tráfico a la subred de su firewall.
- La protección DDoS Basic en Azure Firewall protege contra ataques de red comunes.

- La protección estándar DDoS está disponible por un cargo adicional y protegerá contra ataques adicionales mediante la Protección avanzada contra amenazas.
- Los grupos de seguridad de red (NSG) pueden usarse para controlar qué subredes y recursos pueden comunicarse entre sí en una red virtual.
- Las etiquetas de servicio se pueden usar para permitir los servicios de Azure o Internet mediante un NSG.
- Azure Active Directory es un servicio de identificación basado en la nube en Azure que autentica y autoriza a los usuarios.
- Las aplicaciones empresariales en Azure AD le permiten integrar a terceros con Azure AD para que los usuarios puedan experimentar una experiencia de inicio de sesión único.
- La autenticación multifactor en Azure AD requiere que los usuarios tengan una contraseña y un dispositivo propio para iniciar sesión.
- Azure Security Center proporciona un portal único para monitorear y administrar la seguridad de los recursos de Azure y los recursos locales.
- Justo a tiempo, el acceso a VM en Security Center hace que sea fácil controlar cuándo y durante cuánto tiempo están abiertos los puertos de administración en las VM.
- Azure Key Vault proporciona una forma segura de almacenar secretos, claves y certificados.
- Azure Information Protection lo ayuda a clasificar los correos electrónicos y documentos y protegerlos del acceso de personas no autorizadas.
- La Protección contra amenazas avanzada permite proteger los controladores y servidores de dominio locales de los ataques.
- Azure Policy le permite definir reglas que se aplican con los recursos de Azure que se crean y administran.
- El control de acceso basado en roles permite dar acceso a los usuarios y las aplicaciones a sus recursos de Azure y controlar lo que pueden y no pueden hacer.
- Los bloqueos le permiten bloquear propiedades que pasan por ARM para que no se modifiquen en un recurso o para evitar que se elimine un recurso.
- Azure Advisor proporciona un portal para analizar e informar sobre las mejores prácticas relacionadas con sus recursos de Azure.
- Azure Monitor puede mostrar gráficos con métricas de datos para sus recursos de Azure.
- Las alertas de Azure Monitor pueden notificarlo según las condiciones. También pueden llamar a un webhook, ejecutar una aplicación de función, iniciar un flujo de aplicación lógica y más.

- Azure Service Health proporciona una descripción general del estado de Azure y de sus recursos de Azure que se limita a aquellas regiones donde tiene recursos.
- La Declaración de privacidad de Microsoft es la promesa de Micrsosoft a los clientes relacionada con la forma en que protegerá los datos personales.
- Trust Center es un portal donde puede obtener información sobre el enfoque de Microsoft en materia de seguridad, privacidad y cumplimiento.
- Service Trust Portal proporciona acceso a herramientas de cumplimiento e información sobre cumplimiento.
- Compliance Manager es parte de Service Trust Portal y facilita la gestión del cumplimiento de las normas estándar de la industria mediante evaluaciones.
- Azure Government es una nube privada para gobiernos que funciona con centros de datos distintos dentro de los Estados Unidos. Todos los empleados son evaluados y son ciudadanos estadounidenses.
- Azure Government tiene como objetivo garantizar el cumplimiento de las normas gubernamentales.
- Los centros de datos de DoD dentro de Azure Government proporcionan un control más estricto para cumplir con los estándares de DoD.
- Azure Germany es una nube privada operada fuera de Alemania que está diseñada para cumplir con las estrictas directrices de la UE.
- Los datos individuales en Azure Alemania son controlados y accesibles solo por un administrador de datos. Microsoft no tiene acceso a ningún sistema que toque los datos del cliente.

Capítulo 4. Comprenda los precios y el soporte de Azure

Aunque hemos cubierto muchos temas en este libro, no hemos examinado las principales preocupaciones al pasar a la nube: precios y soporte.

El precio no solo implica conocer el precio de los recursos de Azure. Las empresas a menudo quieren saber cuánto costarán los recursos en la nube antes de que las aplicaciones se implementen en la nube, y una vez que se implementa la aplicación, quieren minimizar los costos tanto como sea posible y tener visibilidad de los costos de los recursos de Azure.

El soporte también es crítico en un entorno de nube. Como hemos aprendido, cuando se muda a la nube, al menos una parte de la gestión de la infraestructura pasa al proveedor de la nube. Cuando algo sale mal, es fundamental que obtenga el soporte que necesita para mantener la disponibilidad de sus aplicaciones. También es importante comprender qué nivel de soporte se ofrece para servicios específicos, especialmente servicios que pueden estar en versión preliminar y no lanzados oficialmente.

En este capítulo, examinaremos todos estos aspectos relacionados con Azure. Cubriremos su suscripción de Azure, cómo planificar y administrar los costos, las opciones de soporte disponibles para usted, los acuerdos de nivel de servicio de Azure y el ciclo de lanzamiento de los servicios de Azure.

Habilidades cubiertas en este capítulo:

- Comprender las suscripciones de Azure
- Comprender la planificación y gestión de costes.
- Comprenda las opciones de soporte disponibles en Azure
- Describir los acuerdos de nivel de servicio de Azure.
- Comprender el ciclo de vida del servicio en Azure
-

HABILIDAD 4.1: COMPRENDER LAS SUSCRIPCIONES DE AZURE

Obtiene una suscripción de Azure automáticamente cuando se registra en Azure y todos los recursos que crea se crean dentro de esa suscripción. Sin embargo, puede crear suscripciones adicionales vinculadas a su cuenta de Azure. Las suscripciones adicionales son útiles en los casos en que desea tener algunas agrupaciones lógicas para los recursos de Azure, o si desea poder informar sobre los recursos utilizados por grupos específicos de personas.

Esta sección cubre:

- Suscripción de Azure
- Usos y opciones con suscripciones de Azure

Suscripción de Azure

Al igual que cualquier otro recurso de Azure, puede administrar su suscripción en el portal de Azure. Puede ver y administrar costos, puede dar acceso a otras personas mediante RBAC, puede aplicar bloqueos, etc.

Cada suscripción de Azure tiene límites (a veces llamados cuotas) asignados. Por ejemplo, puede tener hasta 200 cuentas de Azure Storage por región en una suscripción, hasta 25,000 máquinas virtuales por región y hasta 980 grupos de recursos por suscripción en todas las regiones.

Más información **Límites de suscripción**

Puede encontrar detalles sobre todos los límites de suscripciones en: *https://docs.microsoft.com/azure/azure-subscription-service-limits* .

Consejo de examen

El soporte de Microsoft tiene la capacidad de aumentar los límites en algunos escenarios. Por ejemplo, si tiene una buena justificación comercial, Microsoft puede aumentar el límite de cuentas de almacenamiento a 250 por suscripción, por región. Sin embargo, algunos límites no se pueden aumentar.

La Figura 4-1 muestra una suscripción de Azure en el portal de Azure.

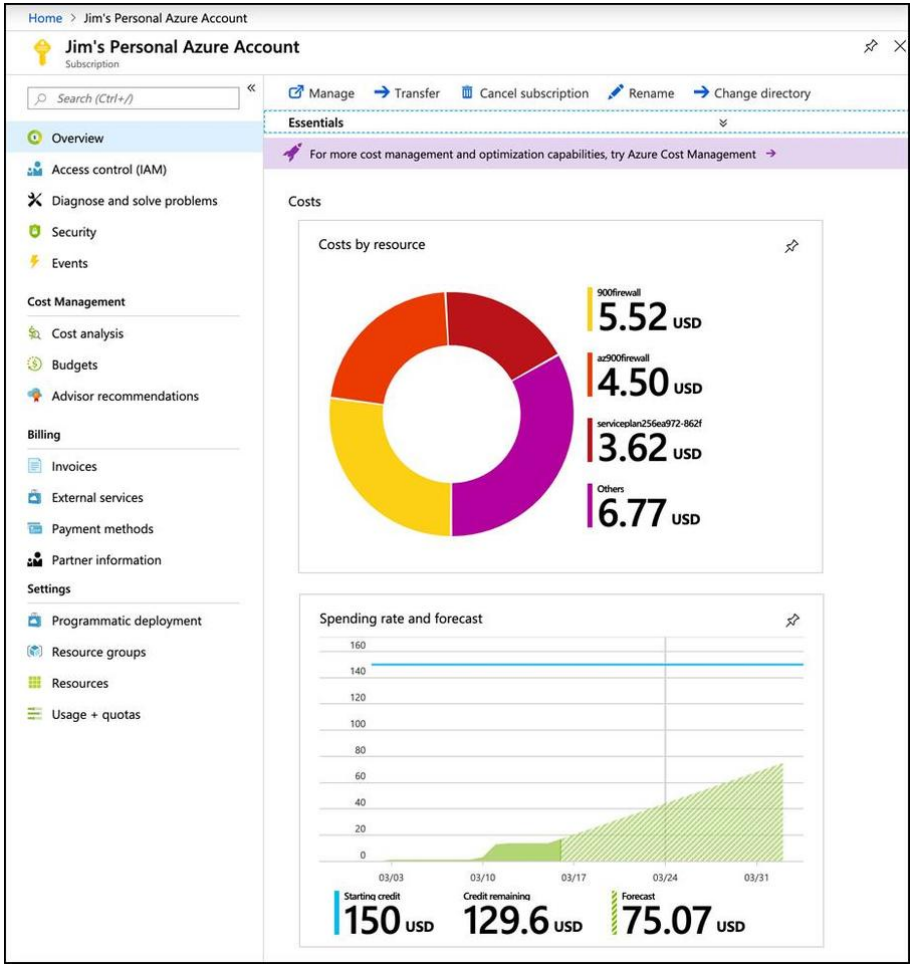


Figura 4-1 suscripción de Azure en el portal de Azure

En la hoja Descripción general, puede ver un desglose de costos para cada uno de los recursos. También puede ver la tasa de gasto para la suscripción, junto con un costo pronosticado para finales del mes actual. Si hace clic en el mosaico Costos por recurso, puede ver un desglose adicional de los gastos de Azure, como se muestra en la Figura 4-2 . En esta vista, verá los costos por Nombre del servicio, Ubicación (región de Azure) y Grupo de recursos, junto con un gráfico de los costos del mes.

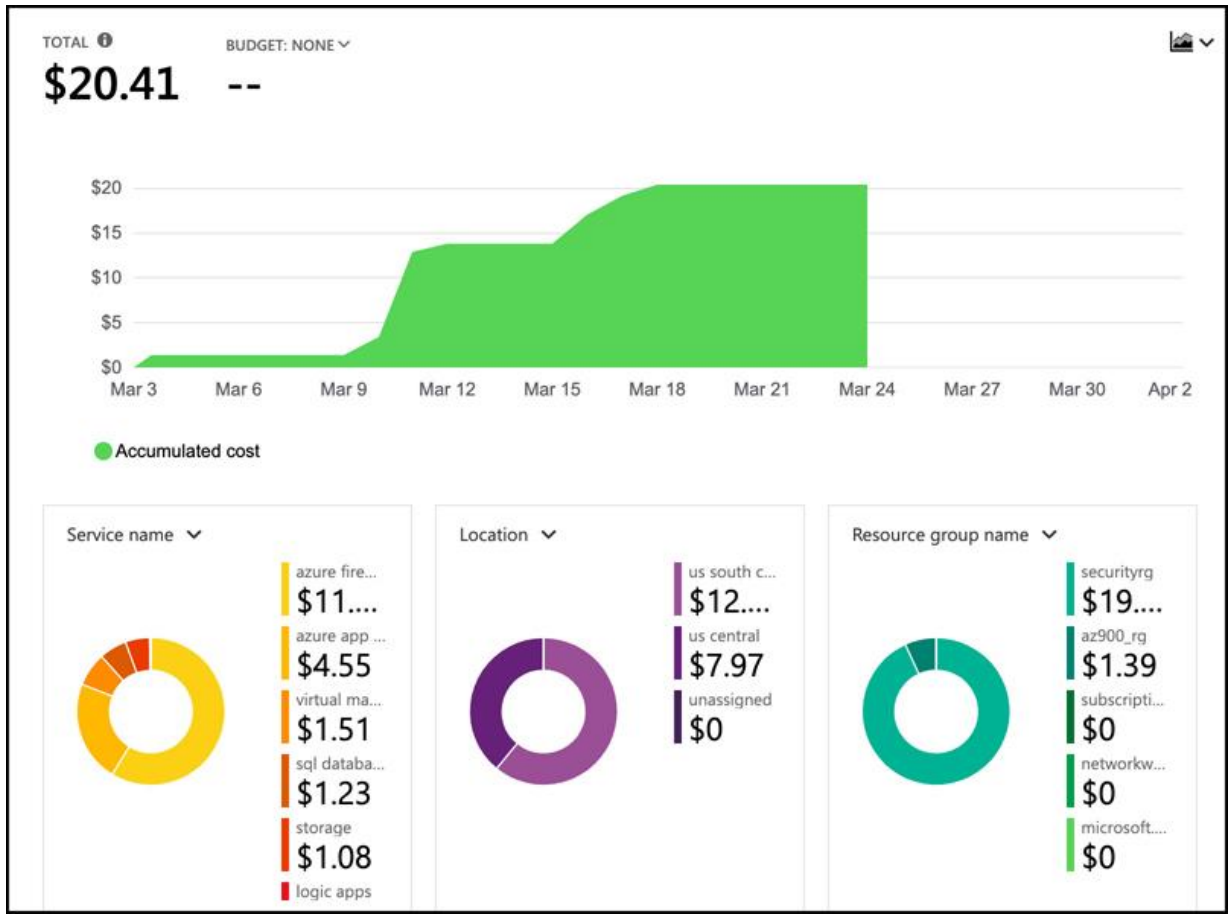


Figura 4-2 Análisis de costos de suscripción de Azure

Más información **Crear presupuestos**

Puede administrar sus costos en Azure creando presupuestos. Aprenderá más sobre eso en la sección de administración de costos de Azure de la Habilidad 4.2: "Comprender la planificación y administración de costos".

Las facturas de Azure también están disponibles para la suscripción desde el portal de Azure. Puede ver todas las facturas anteriores haciendo clic en Facturas en el menú para la suscripción, como se muestra en la Figura 4-3 .

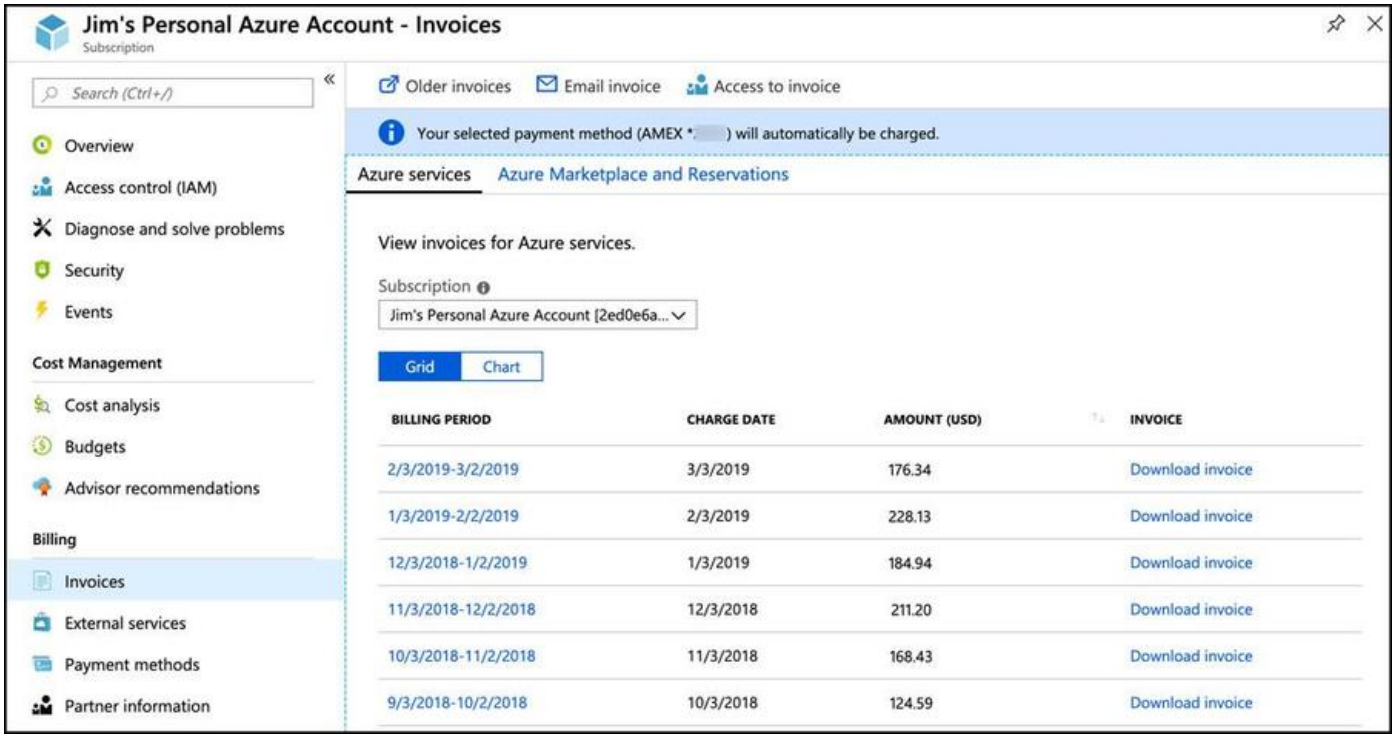


Figura 4-3 Facturas de Azure

Usos y opciones con suscripciones de Azure

Puede crear suscripciones de Azure adicionales en su cuenta de Azure. Esto es útil en los casos en que desea separar los costos o si se acerca a un límite de suscripción en un recurso. Para crear una nueva suscripción de Azure, ingrese la **suscripción** en el cuadro de búsqueda y haga clic en **Suscripciones** como se muestra en la Figura 4-4 .

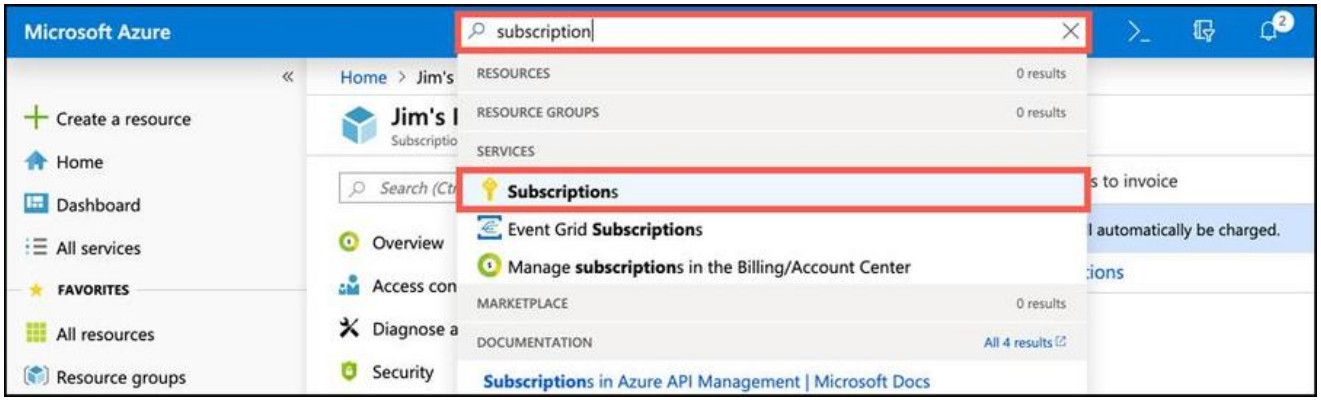


Figura 4-4 suscripciones de Azure

Para crear una nueva suscripción, haga clic en **Agregar** en la hoja Suscripciones como se muestra en la Figura 4-5 .

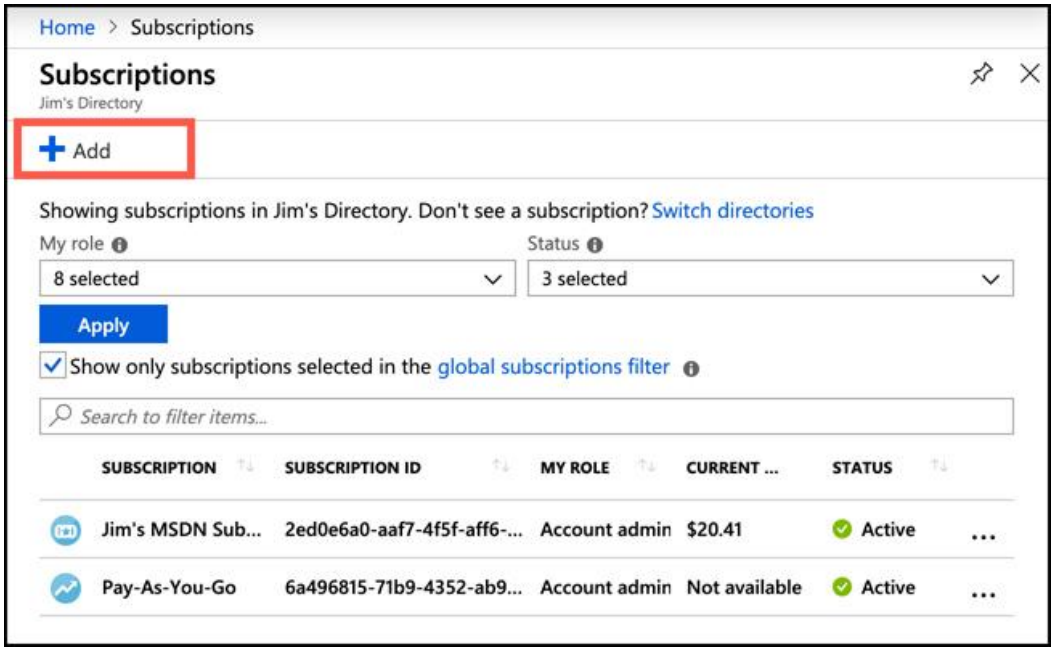


Figura 4-5 Crear una nueva suscripción

Después de hacer clic en **Agregar** , debe elegir qué tipo de suscripción desea crear. Existen varios tipos de suscripciones de Azure.

- **Prueba** gratuita Proporciona acceso gratuito a los recursos de Azure por un tiempo limitado. Solo hay una suscripción de prueba gratuita disponible por cuenta, y no puede crear una nueva prueba gratuita si una anterior ha expirado.
- **Pay-As-You-Go** Usted paga solo por los recursos que usa en Azure. No hay un costo inicial y puede cancelar la suscripción en cualquier momento.
- **Pay / As-You-Go Dev / Test** Una suscripción especial para suscriptores de Visual Studio que se puede usar para desarrollo y prueba. Esta suscripción ofrece tarifas con descuento en máquinas virtuales, pero no puede usarla para aplicaciones de producción.

-

Tenga en cuenta los **tipos de suscripción de Azure**

Es posible que tenga opciones de suscripción adicionales, según el tipo de cuenta de Azure que tenga.

 *Consejo de examen*

Cada suscripción está asociada con un identificador único llamado *ID de suscripción* . Puede asignar a cada suscripción un nombre descriptivo para ayudarlo a identificarlo, pero Azure siempre usará el ID de suscripción para identificar su suscripción. Cuando habla con Microsoft acerca de su cuenta de Azure, a menudo también le piden su ID de suscripción.

HABILIDAD 4.2: COMPRENDER LA PLANIFICACIÓN Y GESTIÓN DE COSTOS

A medida que comience a pensar en mudarse a la nube, lo primero que probablemente querrá hacer es determinar cuáles serán sus costos en función de sus necesidades de recursos. Una vez que haya comenzado a implementar y usar los recursos de Azure, administrar sus costos se vuelve importante para mantenerse dentro de sus presupuestos. Azure tiene herramientas que lo ayudan con la planificación y la administración de sus costos en Azure.

Esta sección cubre:

- Opciones para comprar productos y servicios de Azure
- Opciones alrededor de la cuenta gratuita de Azure
- Factores que afectan los costos
- Zonas
- La calculadora de precios
- La calculadora del costo total de propiedad (TCO)
- Mejores prácticas para minimizar los costos de Azure
- Azure Cost Management

Opciones para comprar productos y servicios de Azure

Hay un par de formas de comprar productos y servicios de Azure. Puede comprar productos y servicios directamente de Microsoft, o puede comprar a través de un Microsoft Cloud Solution Partner (CSP).

Cuando compra directamente de Microsoft, decide qué servicios de Azure desea comprar y administra todas sus implementaciones y el uso de esos servicios. Cada mes, Microsoft le facturará por su uso de Azure, y usted tendrá acceso a esas facturas en el portal de

Azure. Si necesita soporte para sus recursos de Azure, puede obtener soporte directamente de Microsoft utilizando uno de los planes de soporte disponibles para Azure.

Más información **Planes de soporte de Azure**

Aprenderá más sobre los planes de soporte en Azure en la habilidad 4.3: "Comprenda las opciones de soporte disponibles en Azure".

Cuando compra en un CSP, no está comprando recursos de Azure individuales. En cambio, está comprando una solución de nube completa desarrollada por el CSP. Cuando necesita implementar su aplicación, trabaja con el CSP para administrar la implementación. El CSP también le proporciona información sobre los costos de uso de sus recursos, y si necesita soporte, lo obtiene del CSP, no de Microsoft.

Cuando compra en Microsoft, tiene la opción de comprar directamente desde el portal o de que sus servicios se agreguen a un Acuerdo Enterprise existente con Microsoft. Los acuerdos empresariales están diseñados para grandes empresas que tienen una gran cantidad de uso en Azure. Cuando se suscribe a un Enterprise Agreement, trabaja con Microsoft para llegar a un compromiso financiero anual para el uso de Azure. Se le cobra anualmente el precio comprometido, y si usa más del uso acordado, se le cobrará por el uso adicional a la tarifa que usted y Microsoft acuerden.

Comprar directamente de Microsoft ofrece la mayor flexibilidad y control porque usted decide qué recursos individuales está comprando. También es importante tener en cuenta que su equipo de desarrollo puede tener experiencia en el desarrollo contra tipos específicos de recursos de Azure, y al controlar los tipos de recursos que usa, puede reducir la cantidad de posibles problemas en sus aplicaciones.

Por otro lado, si necesita implementar una solución de nube compleja y no tiene experiencia local en algunas áreas, un CSP puede ser la mejor opción para usted. Debido a que el CSP está certificado para tener experiencia en los servicios que ofrece, es posible que pueda brindarle una solución más eficiente que pueda ayudarlo a reducir los costos y las necesidades de soporte.

Opciones alrededor de la cuenta gratuita de Azure

Si nunca ha tenido una prueba gratuita de Azure y nunca ha sido un cliente pagado de Azure, es elegible para una cuenta gratuita de Azure. Una cuenta gratuita le brinda 12 meses de acceso gratuito a los servicios de Azure más populares, y muchos otros servicios de Azure ofrecen uso gratuito incluso después de que hayan transcurrido esos 12 meses. También obtiene un crédito de $ 200 que puede usar para los servicios de Azure por un período de 30 días después de registrarse para obtener una cuenta gratuita.

Consejo de examen

El crédito de $ 200 no se puede usar para pagar las ofertas de Azure Marketplace. Sin embargo, muchas ofertas de Azure Marketplace ofrecen sus propias pruebas gratuitas.

Microsoft establece un límite de gasto de $ 200 en cuentas gratuitas para que no exceda accidentalmente el crédito gratuito de $ 200. Si alcanza ese límite de gasto, deberá actualizar su suscripción a una suscripción de pago por uso para crear recursos adicionales.

Al final del período de 30 días, los recursos que no son gratuitos durante 12 meses o más se eliminan automáticamente, por lo que querrá asegurarse de actualizar su suscripción de Azure antes de que hayan transcurrido los 30 días si desea continuar usando su recursos

Consejo de examen

Microsoft no requiere que los recursos utilizados con una cuenta gratuita se utilicen solo para desarrollo o pruebas. Usted es libre de usar estos recursos para uso de producción.

Más información **Lista completa de cuenta gratuita Disponibilidad de productos**

Para obtener una lista completa de los productos incluidos en la cuenta gratuita y cuánto tiempo están disponibles de forma gratuita, consulte: *https://azure.microsoft.com/free/free-account-faq* .

Factores que afectan los costos

Mientras planifica sus implementaciones de Azure, debe tener en cuenta los factores que pueden afectar sus costos. Los factores principales que afectan los costos son el tipo de recurso, cómo compra el recurso, las regiones de Azure que está utilizando y la zona de facturación en la que se encuentran sus recursos.

Los servicios de Azure se facturan según los *medidores* asociados con un recurso. Estos medidores registran cuánto ha utilizado una métrica específica por el recurso. Por ejemplo, no se cobra específicamente por una red virtual de Azure, y no se le cobra ningún tráfico de red dentro de una red virtual, pero se le cobra por gigabyte por el tráfico que entra y sale de la red virtual desde redes virtuales pares.

Consejo de examen

Cada servicio de Azure tiene una página de precios que describe las estimaciones de precios para ese recurso en función del uso típico.

A medida que determine qué recursos necesita usar en su implementación de Azure, considere cómo esos recursos van a usar las métricas por las que cobran los recursos. Por ejemplo, si puede planificar sus redes virtuales para tener menos redes pares, puede ahorrar sustancialmente a largo plazo.

También puede encontrar que comprar recursos de Azure de manera diferente puede ofrecer ahorros de costos. Si acepta pagar por adelantado utilizando un Acuerdo de empresa, Microsoft le ofrecerá un descuentoVelocidad. Los acuerdos a más largo plazo ofrecen incluso más descuentos en los precios. Los CSP también pueden proporcionarle soluciones completas que son más rentables que comprar todos los recursos usted mismo.

Los costos de Microsoft para operar los servicios de Azure difieren según la región, incluso cuando esas regiones están dentro del mismo límite geográfico. Por lo tanto, su precio diferirá según la región de Azure que use. Por ejemplo, una VM implementada en la región central de EE. UU. Costará más que la misma VM implementada en la región este de EE. UU. Microsoft no proporciona un desglose de sus costos, pero puede suponer que la electricidad y otros recursos necesarios para un centro de datos de Azure son más caros en la región central de EE. UU. Que en la región oriental de EE. UU.

Consejo de examen

Por lo general, elegir la región menos costosa para cada uno de sus recursos de Azure no es una buena manera de controlar los costos. Puede terminar pagando el tráfico de red en todas las regiones, y eso puede aumentar sus costos por encima del monto que está ahorrando. Muchos recursos de Azure no cobran por el tráfico de red dentro de la misma región, pero cobrarán por el tráfico en todas las regiones.

También es importante tener en cuenta que no se le cobra por el tráfico de red en un centro de datos de Azure, pero se le cobra por el tráfico de red fuera de un centro de datos. Sin embargo, sus primeros 5 GB de datos salientes son gratuitos. Después de ese punto, se le cobrará una cantidad establecida en un modelo escalonado. El monto que se le cobra depende de la zona de facturación.

Más información sobre **precios de ancho de banda de red**

Para obtener más información sobre el precio del ancho de banda de red en Azure, consulte: *https://azure.microsoft.com/pricing/details/bandwidth* .

Zonas

Las geografías de Azure se dividen en cuatro grupos separados para fines de facturación. Estos grupos se denominan *zonas de facturación* , o más comúnmente, simplemente zonas. Los costos de Microsoft para el tráfico de red fuera de cada zona difieren, por lo que sus costos también serán diferentes.

La Tabla 4-1 enumera las zonas en Azure y sus geografías correspondientes.

Tabla 4-1 Zonas y geografías

Nombre de zona	Geografías incluidas
Zona 1	Estados Unidos, Europa, Canadá, Reino Unido, Francia
Zona 2	Asia Pacífico, Japón, Australia, India, Corea
Zona 3	Brasil
DE Zona 1	Alemania

Los costos de red de salida más baratos se encuentran en la Zona 1. La Zona 1 DE es la segunda más barata, seguida de la Zona 2 y la Zona 3.

Como puede ver, hay muchos factores que pueden afectar sus costos en Azure, y puede ser difícil estimar los costos en función de todos estos factores. Afortunadamente, Microsoft ofrece una calculadora de precios que puede ayudarlo a controlar sus costos a medida que se traslada a la nube.

La calculadora de precios

La calculadora de precios de Azure puede ayudarlo a obtener una estimación de los gastos en función de los productos que piensa usar, así como dónde se implementarán esos productos, etc. Puede acceder a la calculadora de precios navegando a: *https://azure.microsoft.com/en-us/pricing/calculator* .

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

El primer paso para calcular una estimación de sus gastos de Azure es seleccionar qué productos desea usar. Como se muestra en la Figura 4-6 , algunos de los productos de Azure más comunes se muestran de manera predeterminada, y puede agregar cualquiera de esos productos haciendo clic en su mosaico.

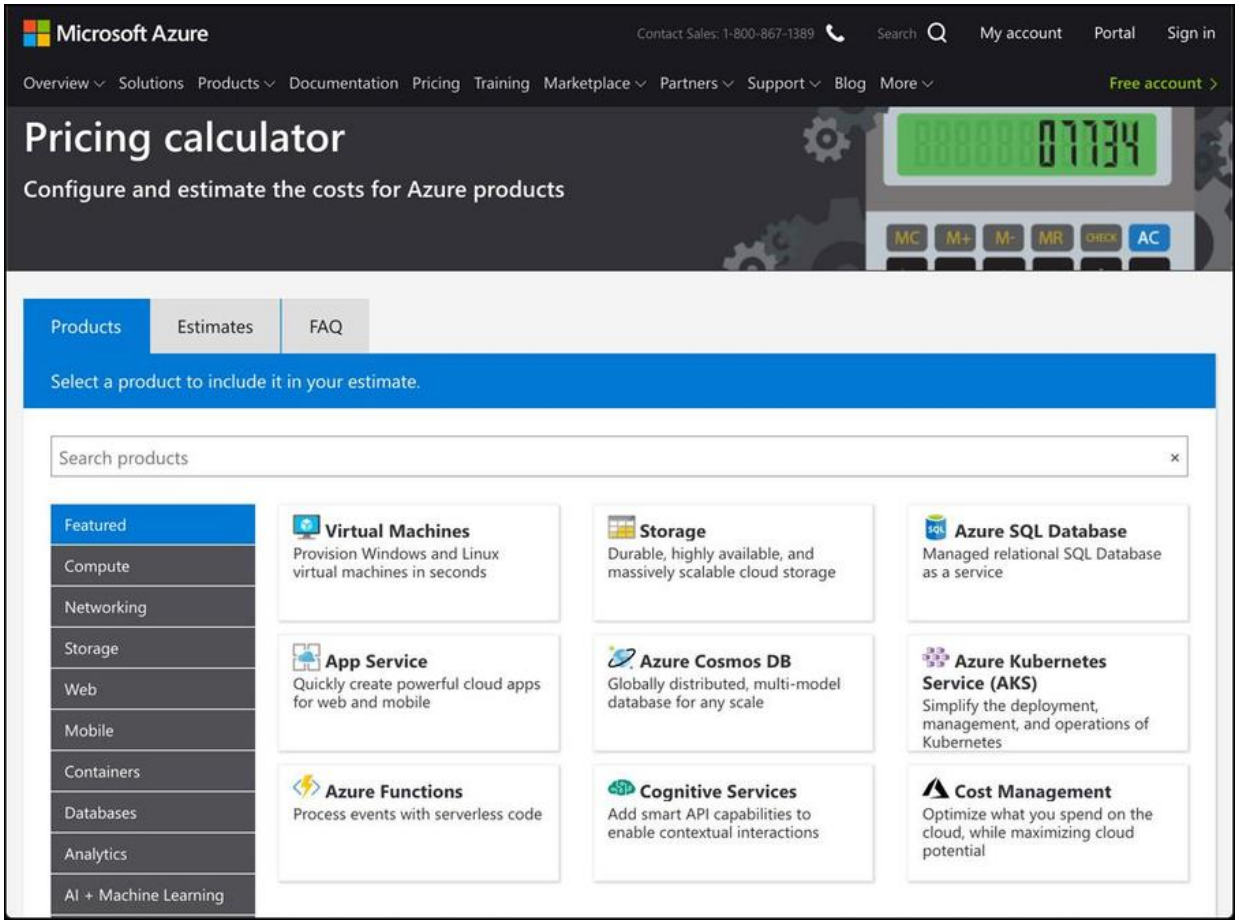


Figura 4-6 La calculadora de precios

Si el producto que desea no está en la lista, puede hacer clic en una categoría de productos en la lista de la izquierda o puede buscar su producto ingresando su nombre en el cuadro de búsqueda.

Después de agregar los productos que desea usar, desplácese hacia abajo para configurar los detalles específicos de cada servicio. Estos detalles varían según la forma en que Microsoft cobra por el producto. La Figura 4-7 muestra las opciones para Azure SQL Database.

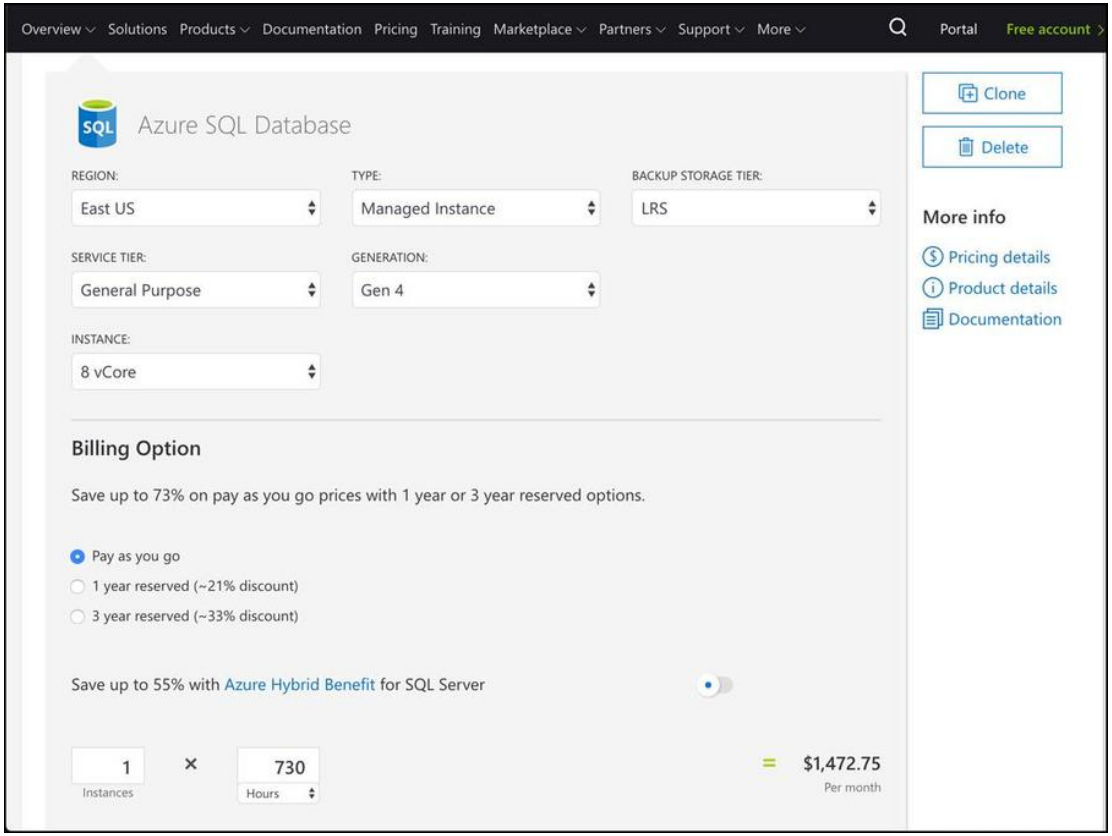


Figura 4-7 Opciones de precios para Azure SQL Database

Al hacer clic en Detalles de precios, se abrirá la página de precios para el producto en una nueva pestaña. También puede hacer clic en Detalles del producto o Documentación para leer más sobre el servicio y ayudarlo a tomar mejores decisiones sobre las opciones que seleccione.

Una vez que haya configurado un producto según sus necesidades, puede hacer clic en el botón Clonar para agregar otra instancia de ese producto a su estimación. Por ejemplo, suponga que necesita dos bases de datos SQL Azure para su aplicación, y cada una de ellas utilizará el mismo nivel de servicio, tamaño de instancia, etc. La forma más fácil de agregar estos es agregar un producto de Azure SQL Database a su estimación, configurarlo con las opciones de precios deseadas y luego hacer clic en Clonar para agregar la segunda instancia.

Para revisar su estimación de precios, desplácese hasta la parte inferior de la página. Como se muestra en la Figura 4-8 , puede elegir un plan de soporte para agregar a su estimación. Si tiene un Acuerdo de empresa o un Acuerdo de cliente de Microsoft, puede elegirlos para que ese precio se aplique a su estimación. Luego puede hacer clic en **Exportar** para guardar su estimación como un archivo de Excel, luego seleccionar **Guardar** para guardar su estimación en la calculadora de precios para realizar cambios más adelante, o seleccionar **Compartir** para crear un enlace para compartir su estimación para que otros puedan verla.

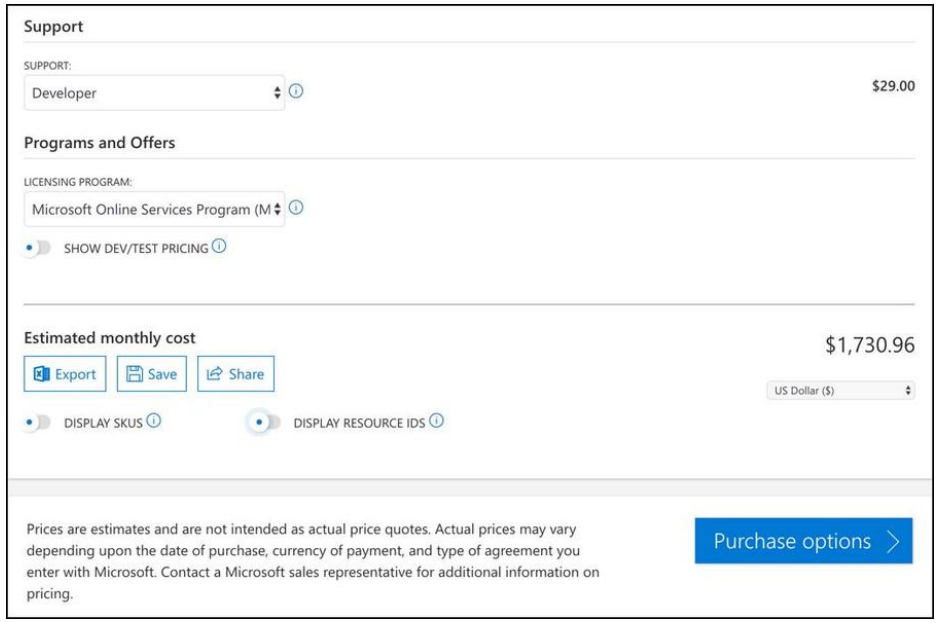


Figura 4-8 Cómo completar una estimación en la calculadora de precios

***Tenga en cuenta las* estimaciones guardadas**

Si guarda una estimación en la calculadora de precios, puede acceder a ella más tarde haciendo clic en la pestaña Estimaciones en la parte superior de la página.

Más* opciones de soporte de *información

Cubriremos las opciones de soporte en la Habilidad 4.3: "Comprenda las opciones de soporte disponibles en Azure".

La calculadora del costo total de propiedad (TCO)

La calculadora de precios es útil para estimar sus gastos para nuevas aplicaciones en Azure, pero si tiene aplicaciones locales que desea migrar a Azure y desea una estimación de cuánto puede ahorrar en Azure, la calculadora de TCO es una mejor opción . Puede acceder a la calculadora de TCO navegando a: *https://azure.microsoft.com/en-us/pricing/tco/calculator* .

El primer paso al usar la calculadora de TCO es agregar detalles sobre sus servidores locales, bases de datos, almacenamiento y uso de la red. En la Figura 4-9 , se ha configurado un servidor local para una aplicación web. Puede configurar todos los detalles sobre el servidor, incluido el sistema operativo, ya sea una máquina virtual o un servidor físico, y más.

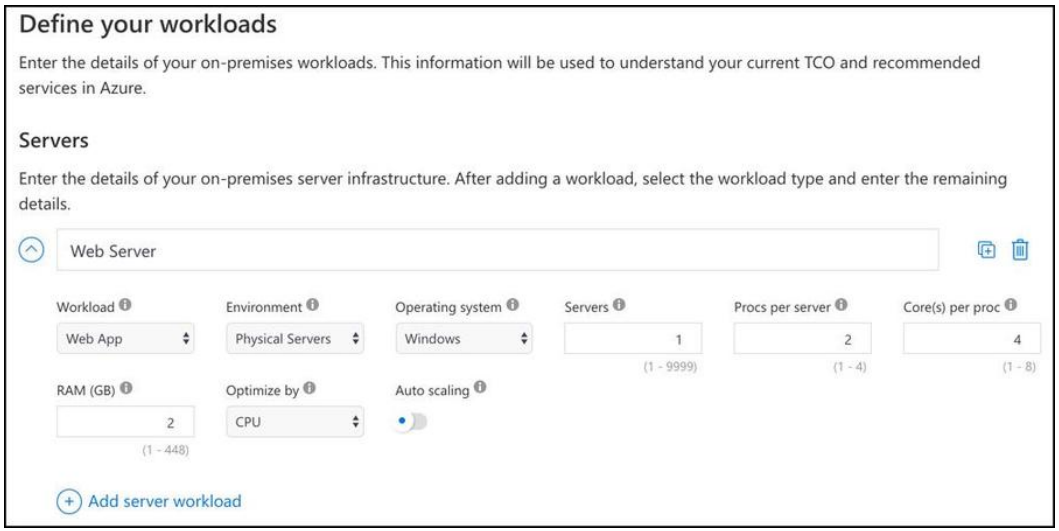


Figura 4-9 Configuración de un servidor local en la calculadora de TCO

También se deben agregar bases de datos y sistemas de almacenamiento locales, además de cualquier uso de red para su aplicación. En la Figura 4-10 , se agregó un sistema de almacenamiento y se especificó el uso de la red para la aplicación.

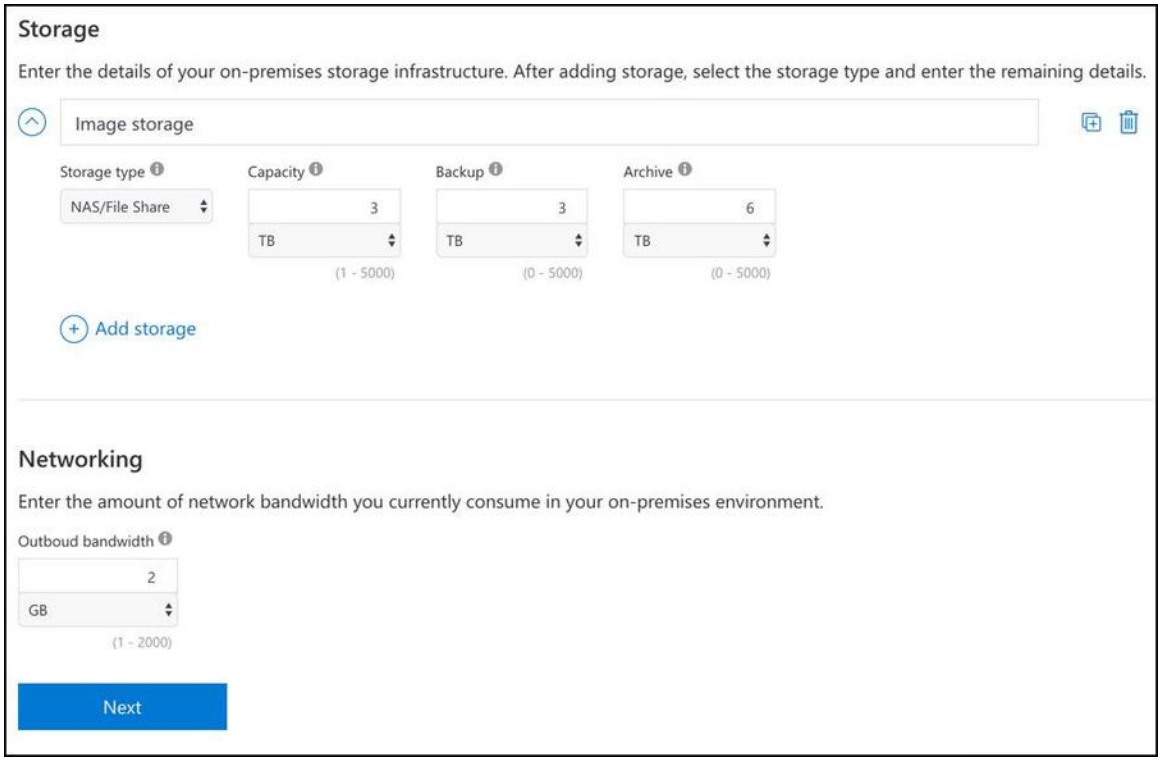


Figura 4-10 Configuración de almacenamiento y redes

Después de ingresar todas sus cargas de trabajo locales, puede ver los supuestos que usa la calculadora de TCO haciendo clic en **Siguiente** . La calculadora de TCO utiliza una lista completa de localessupuestos de gastos que Microsoft ha reunido en base a años de experiencia, y estos supuestos se utilizan para proporcionarle la mejor estimación posible de sus ahorros de costos. Como se muestra en la Figura 4-11 , los supuestos incluyen elementos tales como si ha comprado un plan de Software Assurance para sus servidores locales, detalles sobre sus gastos actuales locales, sus costos de mano de obra de TI y mucho más. Para una estimación precisa de TCO, es mejor registrar cuidadosamente sus gastos antes de generar un informe de TCO.

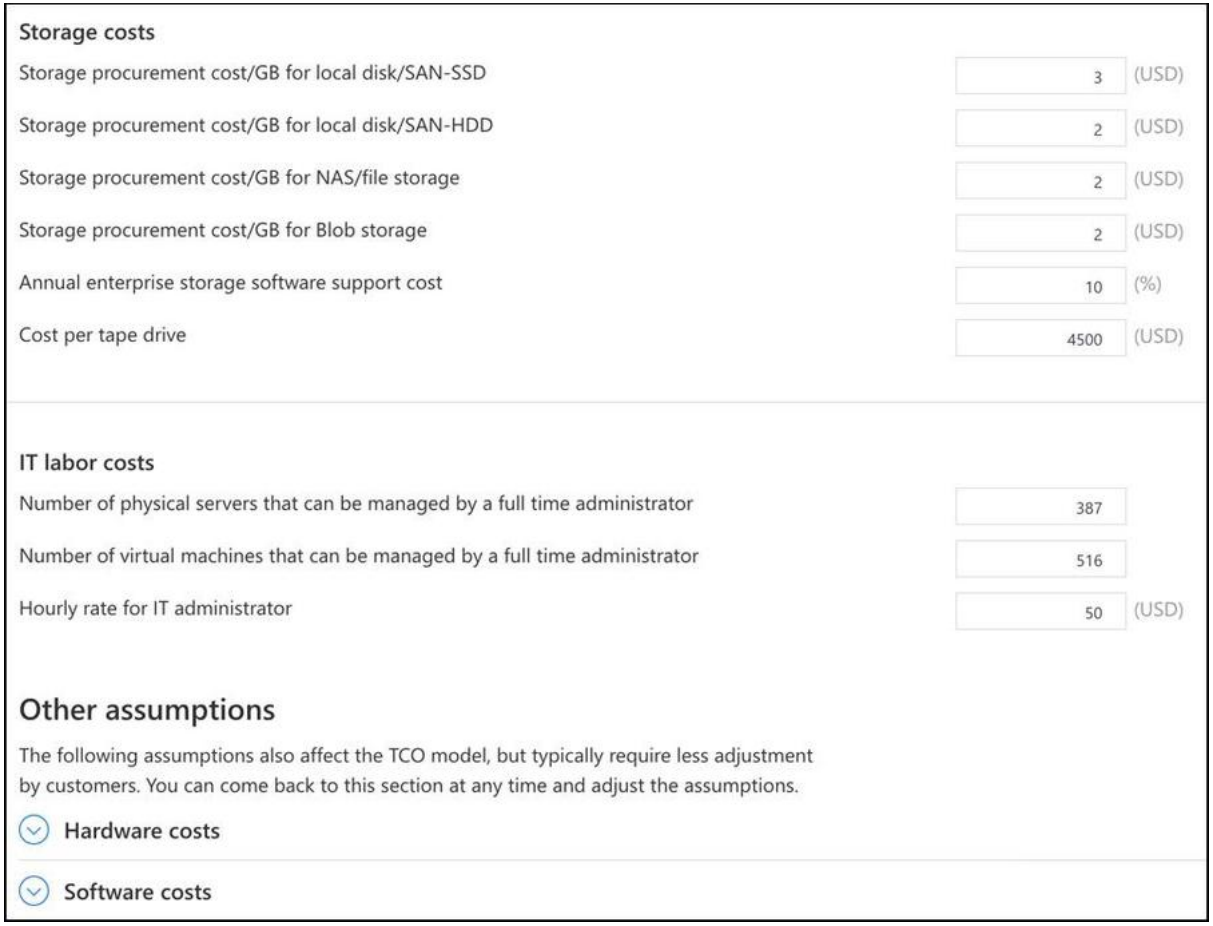


Figura 4-11 Supuestos de ajuste hechos por la calculadora de TCO

Después de ajustar sus suposiciones, desplácese hasta la parte inferior de la pantalla y haga clic en **Siguiente** para ver su informe de TCO. Su informe de TCO le muestra cuánto puede ahorrar en los próximos 5 años al mover su aplicación a Azure como se muestra en la Figura 4-12 .

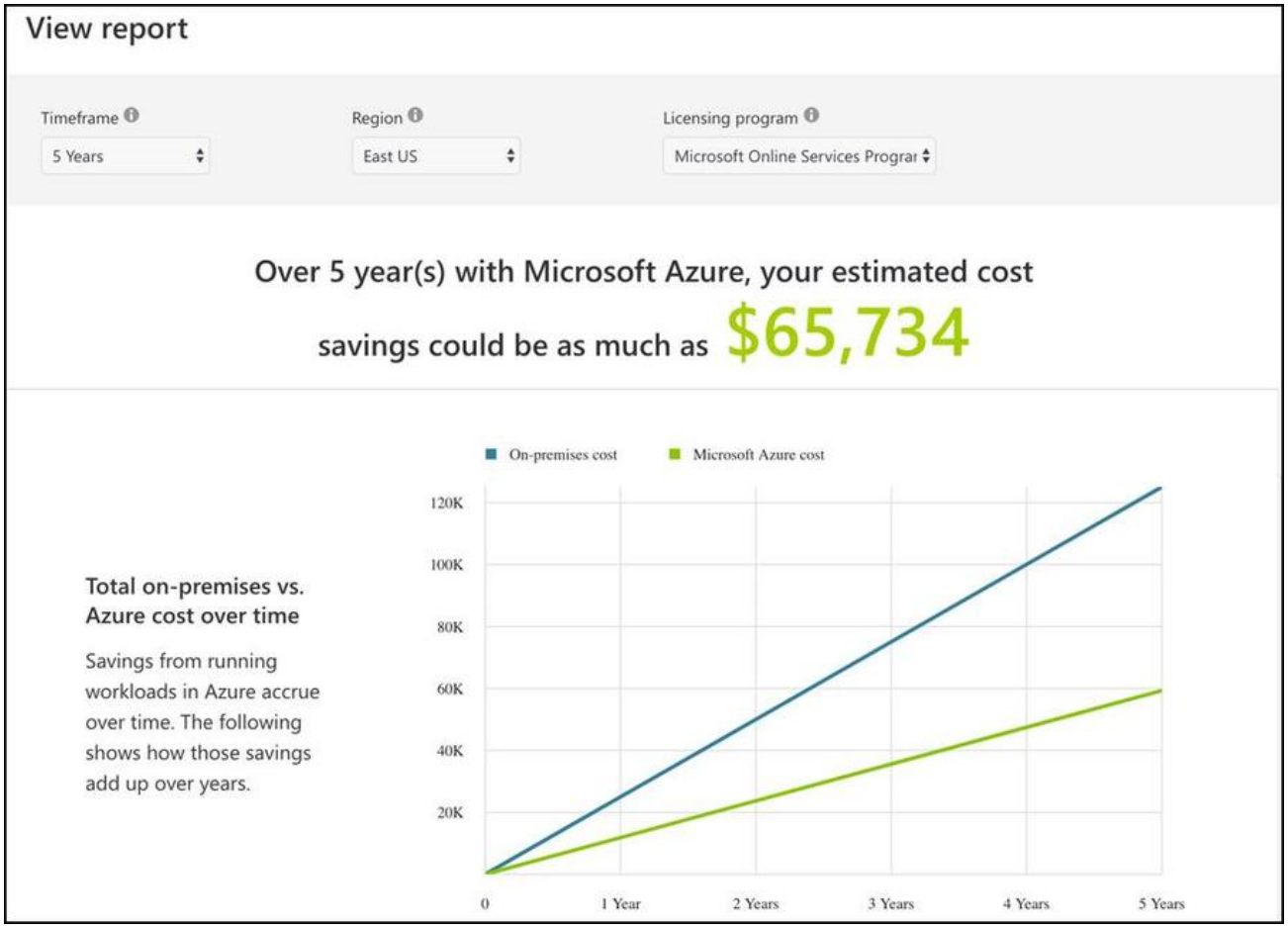


Figura 4-12 Informe de ahorro de TCO

Un informe de TCO incluye cuadros detallados de ahorro de gastos, y en la parte inferior del informe, encontrará un desglose de los costos locales y los costos de Azure para que pueda determinar fácilmente dónde ahorrará dinero. Al igual que con la calculadora de precios, los informes generados por la calculadora de TCO se pueden descargar, guardar y copiar haciendo clic en el botón apropiado como se muestra en la Figura 4-13 .

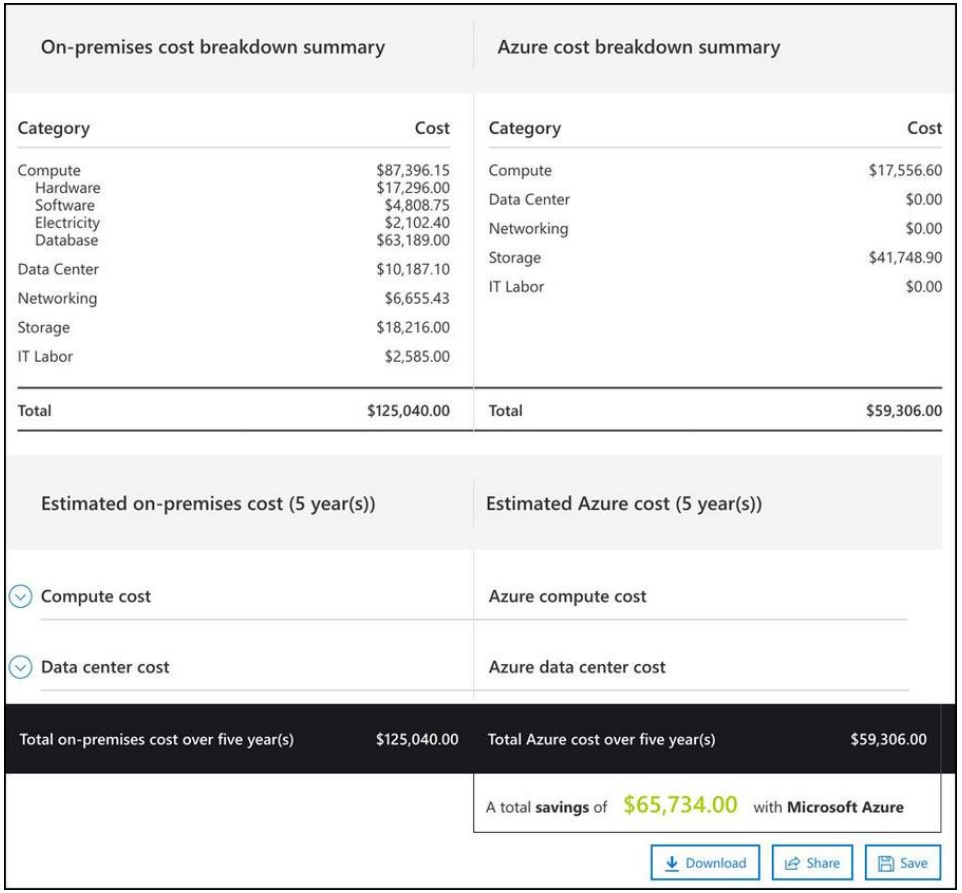


Figura 4-13 Resumen de costos locales y en Azure

Mejores prácticas para minimizar los costos de Azure

Minimizar sus costos en Azure comienza con una planificación cuidadosa antes de incluso crear un solo recurso de Azure. La planificación debe involucrar a los actores clave de su organización, como su departamento de finanzas, los gerentes responsables de la planificación e implementación del presupuesto y los diseñadores de aplicaciones que están en la mejor posición para decidir qué tipos de recursos probablemente se necesitan.

Las herramientas, como la calculadora de precios y la calculadora de costo total de propiedad, son valiosas en la planificación, pero solo son tan precisas como los datos que usted les proporciona. Asegúrese de que, al analizar sucargas de trabajo locales, se asegura de que todos los recursos que utiliza su aplicación sean realmente requeridos por la aplicación. Si está utilizando un servidor que es mucho más poderoso de lo que las necesidades dictan, ese es un punto importante a considerar en su planificación.

Consejo de examen

Una parte importante de minimizar los costos en Azure es asegurarse de que utiliza por completo todos sus recursos en la nube. Debido a que la mayor parte del uso de la nube se factura por el consumo de un recurso, no usar porciones de un recurso representa gastos innecesarios. La planificación adecuada puede ayudar a evitar recursos en la nube no utilizados.

Mientras analiza su uso local y planifica su mudanza a Azure, debe aprovechar la oportunidad para organizar sus recursos en función de la responsabilidad de los gastos. Luego, puede usar esa estructura organizativa en Azure para aplicar etiquetas a los recursos de modo que cada organización dentro de su empresa tenga una visibilidad adecuada de sus gastos. Esto ayudará a garantizar que si un recurso se está subutilizando, las personas adecuadas tendrán rápidamente visibilidad para poder hacer ajustes.

Una vez que se complete la planificación, deberá determinar qué plan de suscripción de Azure es el más adecuado para sus necesidades. Si planea usar Azure para alojar una aplicación de producción a largo plazo, puede ahorrar dinero comprando un Acuerdo de empresa y aceptando un compromiso a más largo plazo. Sin embargo, si solo planea realizar una prueba por un corto período de tiempo, una suscripción gratuita o de pago por uso es una mejor opción.

En esta etapa de su planificación, la calculadora de precios y la calculadora de TCO pueden ser útiles para estimar sus gastos en la nube. El uso de la opción de compartir una copia de sus estimaciones e informes puede ayudar a garantizar que todos en su organización estén en la misma página, y puede ayudarlo a ajustar sus cálculos según sea necesario.

Consejo de examen

Mientras planifica sus implementaciones en la nube, asegúrese de tener en cuenta el hecho de que Azure puede escalar sus recursos en función de las necesidades de la aplicación. No use los servidores más potentes y otros recursos que cree que necesitará. En su lugar, elija SKU de productos que satisfagan sus necesidades mínimas y configure reglas de escala que puedan acomodar necesidades de recursos adicionales a medida que aumentan los patrones de uso de la aplicación.

Una vez que haya implementado recursos en Azure, es importante monitorear el uso de recursos con cuidado. Si bien puede usar las herramientas disponibles en el portal de Azure para revisar el uso de recursos individuales, es más efectivo obtener una visión general del uso de recursos usando herramientas como Azure Advisor.

Más información **Azure Advisor**

Si necesita actualizar su memoria al usar Azure Advisor, consulte " Azure Advisor " en la Habilidad 2.4: "Comprender las herramientas de administración de Azure".

Su factura de Azure también tendrá detalles sobre el uso de los recursos, y siempre que organice sus recursos de manera efectiva y etiquete los recursos en función de la alineación de la organización, puede proporcionar fácilmente a diferentes organizaciones dentro de su empresa detalles sobre su uso específico.

Más información **Azure Cost Management**

Para obtener más información sobre Azure Cost Management, consulte *https://docs.microsoft.com/azure/cost-management* .

Si tiene trabajos por lotes más pequeños que desea ejecutar en Azure, puede ahorrar sustancialmente mediante el uso de máquinas virtuales que Microsoft ha asignado en los centros de datos, pero que los clientes no están utilizando. Esta oferta se llama Azure Batch y utiliza máquinas virtuales no utilizadas para ejecutar cargas de trabajo que no son urgentes y que no necesitan ejecutarse durante largos períodos. Puede leer más sobre Azure Batch en: *https://docs.microsoft.com/en-us/azure/batch/batch-low-pri-vms* .

Más información **Mejores prácticas para minimizar costos**

Para obtener más información sobre las mejores prácticas para minimizar los costos, consulte: *https://docs.microsoft.com/azure/cost-management/cost-mgt-best-practices* .

Azure Cost Management

Azure Cost Management es una herramienta en Azure que facilita el análisis de sus costos a nivel granular. La administración de costos le permite crear un presupuesto para sus gastos de Azure, establecer alertas configurables para saber si se está acercando a un límite presupuestado y analizar sus costos en detalle.

Para comenzar con Cost Management, abra Azure Portal y busque **Cost Management** , y haga clic en **Cost Management + Billing** .

Consejo de examen

También verá Administración de costos en Azure Marketplace. Esa es una oferta diferente que se basa en Cloudyn, una compañía de administración de gastos en la nube que compró Microsoft.

Una vez que se cargue Cost Management + Billing en el portal, haga clic en **Cost Management** como se muestra en la Figura 4-14 para acceder a Cost Management.

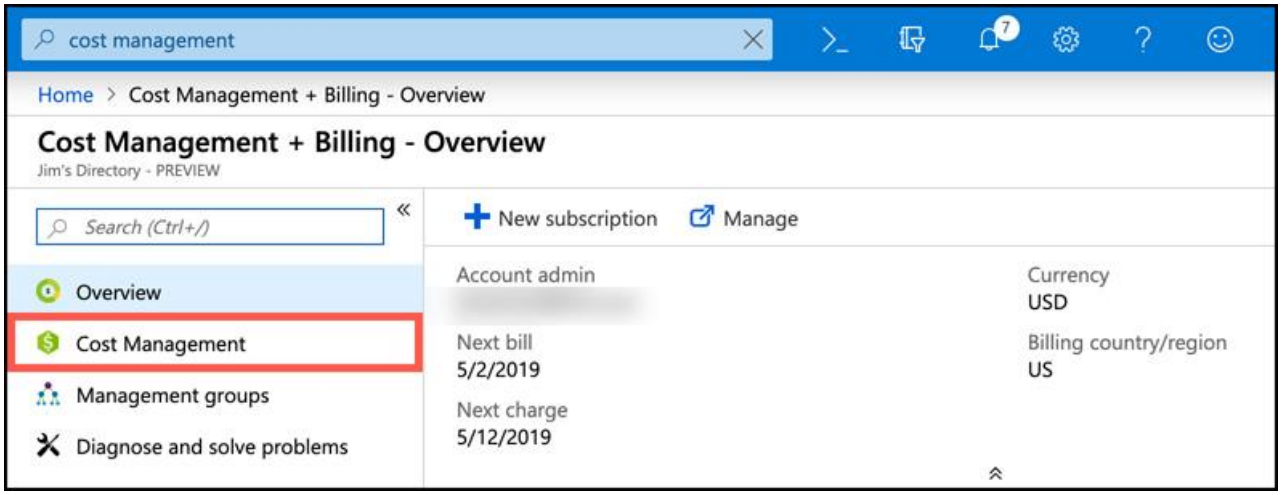


Figura 4-14 Gestión de costes + facturación y gestión de costes

Para monitorear efectivamente sus costos, debe crear un presupuesto en la Administración de costos. No es necesario crear un presupuesto, pero le permitirá visualizar sus gastos en comparación con sus gastos planificados.

1. Haga clic en **Presupuestos** , y luego haga clic en **Agregar** , como se muestra en la Figura 4-15 .

1.2.

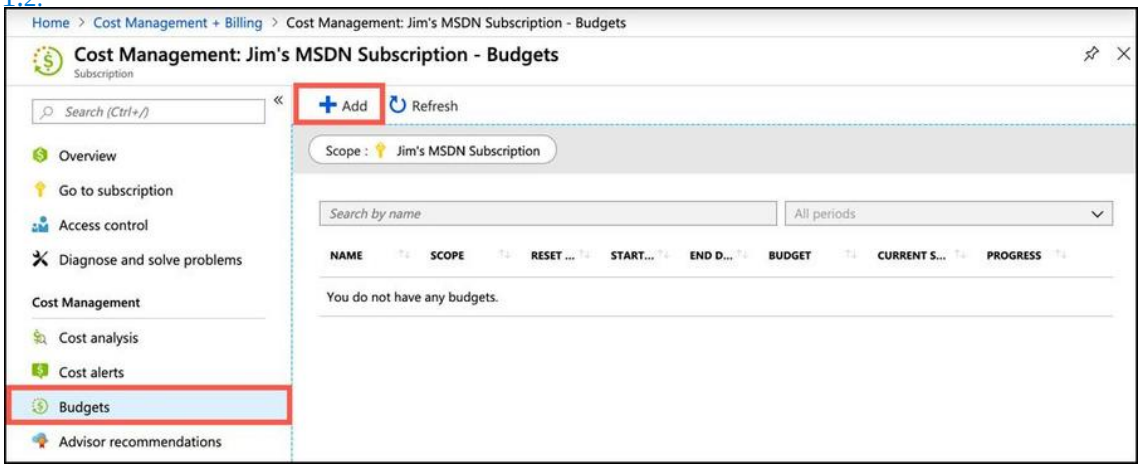


Figura 4-15 Agregar un nuevo presupuesto

2.3. Ingrese un nombre para su presupuesto.

3.4. Ingrese un monto de gasto y el período en el que se reinicia su gasto.

4.5. Ingrese una fecha de inicio para su presupuesto.

5.6. Ingrese una fecha de vencimiento.

6.7. Configure cualquier alerta para su presupuesto.

7.8. Ingrese las direcciones de correo electrónico de las personas a las que se debe enviar cualquier información de alerta activada.

9. Haga clic en **Crear** para completar su presupuesto.

8.10.

En la Figura 4-16 , se está creando un presupuesto de $ 10,000 para un año fiscal. Se agrega una alerta cuando se alcanza el 80% de ese presupuesto, y Azure enviará un correo electrónico a jim@contosopharm.com si los costos han alcanzado los $ 8,000.

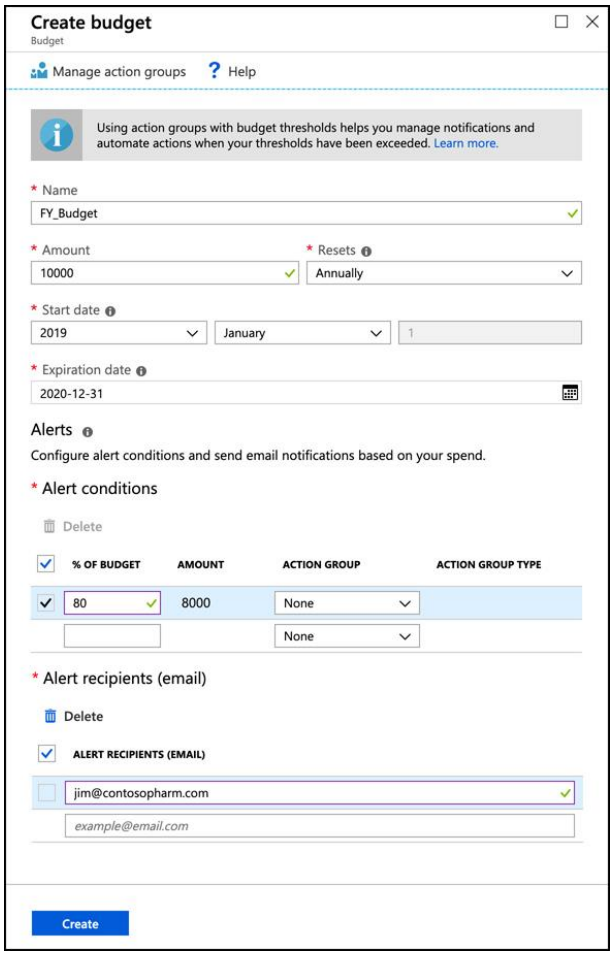


Figura 4-16 Crear un presupuesto

Después de crear un presupuesto, haga clic en **Análisis de costos** para ver cómo se compara su gasto con su presupuesto. En la Figura 4-17 , puede ver cómo hemos gastado un poco más del gasto anual presupuestado, según el mes actual de mayo. Como puede ver, estamos gastando más del doble de lo que hemos presupuestado.

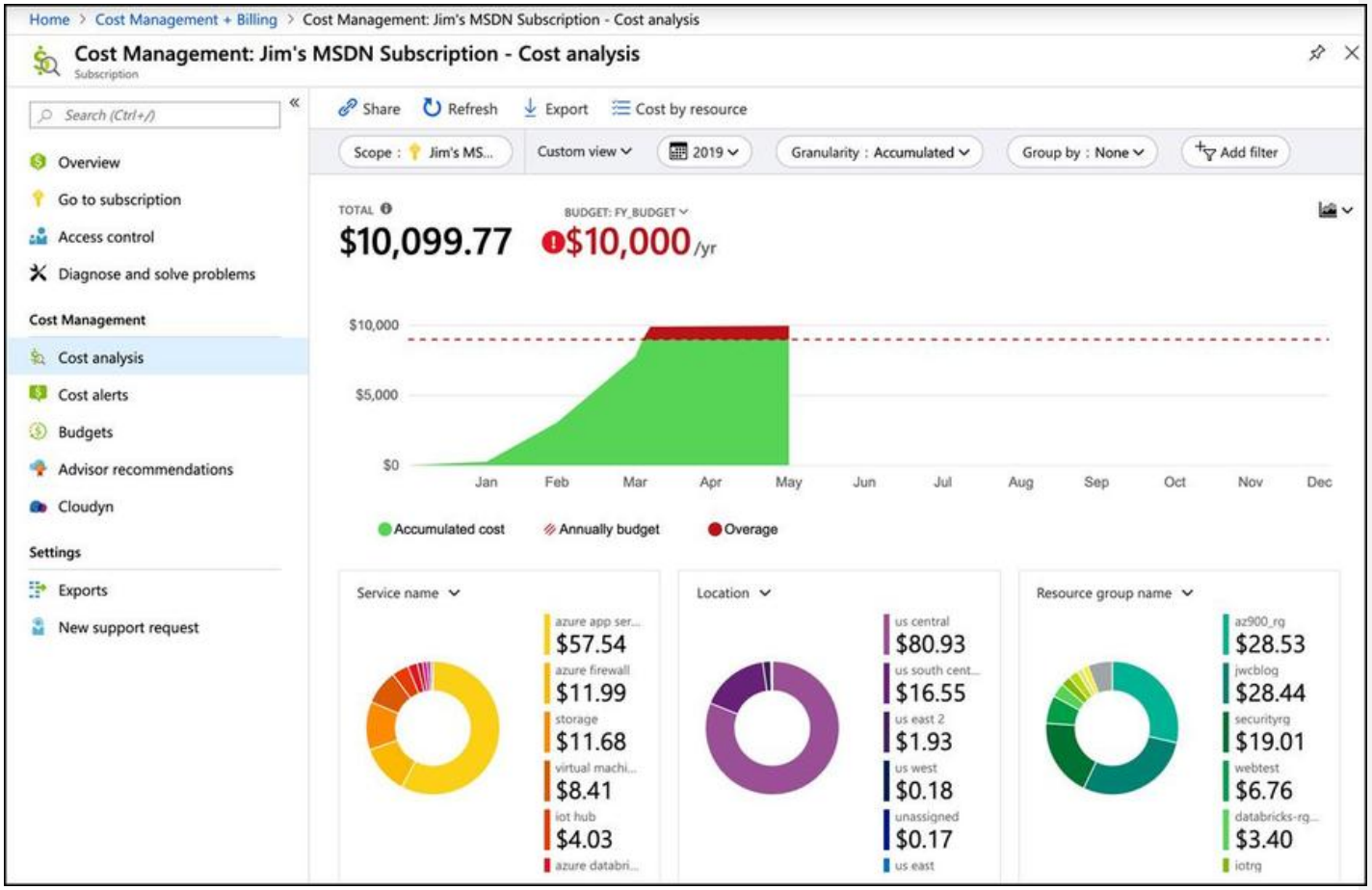


Figura 4-17 Visualización del análisis de costos

En la Figura 4-17 , puede ver los gastos de todo un año porque el presupuesto se creó para un año fiscal. Haga clic en **Vista personalizada** para elegir ver solo los costos acumulados, que mostrarían la misma vista que la Figura 4-17 . Sin embargo, cuando haga eso, no verá su presupuesto incluido en el gráfico. También puede elegir ver los costos diarios, los costos por servicio o los costos por recurso. Para cada vista, puede elegir un rango de fechas, una granularidad (como diaria, mensual, etc.) y cómo desea que la pantalla se agrupe por gastos (por período de facturación, nombre del grupo de recursos, etc.).

Para profundizar en los gastos, puede aplicar un filtro personalizado haciendo clic en **Agregar filtro** . En la Figura 4-18 , se agrega un filtro para mostrar solo los gastos de una aplicación llamada databricks.

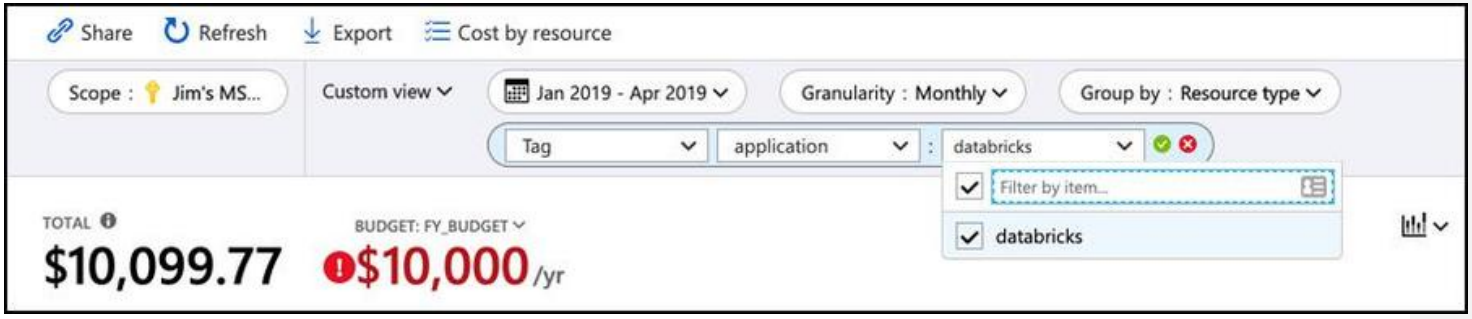


Figura 4-18 Aplicación de un filtro

HABILIDAD 4.3: COMPRENDER LAS OPCIONES DE SOPORTE DISPONIBLES EN AZURE

Azure proporciona muchas herramientas de diagnóstico que puede usar para solucionar problemas de su aplicación cuando las cosas salen mal, pero es probable que en algún momento necesite ayuda del soporte de Azure. Si necesita ayuda adicional para solucionar problemas de su aplicación o si necesita soporte para la plataforma Azure en sí, Microsoft ofrece numerosas opciones de soporte para interactuar con su organización de soporte de clase mundial.

Esta sección cubre:

- Planes de apoyo
- Cómo abrir un caso de soporte
- Canales de soporte disponibles fuera de los planes de soporte
- Centro de Conocimiento

Planes de apoyo

Microsoft ofrece numerosos planes de soporte para clientes de Azure. Antes de entrar en los detalles de cada plan, hay algunos términos con los que debería estar familiarizado en relación con el soporte de Azure.

- **Horario comercial** Microsoft define *el horario comercial* para la mayoría de los países como días laborables de 9:00 a.m. a 5:00 p.m., hora local. Sin embargo, en Norteamérica, el horario comercial es de lunes a viernes de 6:00 a.m. a 6:00 p.m., hora del Pacífico, y en Japón, el horario comercial es de lunes a viernes de 9:00 a.m. a 5:30 p.m. En todas las regiones, el horario comercial no incluye feriados.
- **Caso de Severidad A** Microsoft usa la *Severidad A* para referirse a una aplicación de producción que está completamente inactiva, o cuando un componente crítico de una aplicación de producción no está disponible.
- **Caso de gravedad B** Microsoft usa la *gravedad B* para referirse a una aplicación de producción que se ve afectada de manera moderada. Este nivel de gravedad es subjetivo y está de acuerdo con el soporte de Microsoft y el cliente.
- **Caso de gravedad C** Microsoft usa la *gravedad C* para referirse a una situación que está causando un impacto mínimo. Estos son casos que se refieren a problemas que ya no ocurren o casos que no están afectando una aplicación de producción.

Microsoft ofrece los siguientes planes de soporte para Azure.

- **Soporte básico** limitado que es gratuito para todas las suscripciones de Azure.
- Soporte de Azure para **desarrolladores** para prueba gratuita y aplicaciones que no son de producción.
- Soporte **estándar de** Azure para aplicaciones de producción.
- Soporte **profesional directo de** Azure para aplicaciones críticas para el negocio.
- Soporte **Premier** Contratado para todos los productos de Microsoft, incluido Azure.

Todos los planes de soporte ofrecen soporte 24x7 para cualquier problema de facturación o problemas de suscripción, acceso a las recomendaciones de Azure Advisor, Service Health Dashboard y Health API. Todos los planes de soporte de pago ofrecen acceso a los ingenieros de soporte de Microsoft.

Más información **Otras opciones de soporte**

Microsoft ofrece numerosas opciones de soporte fuera de los planes de soporte descritos aquí. Se tratarán más adelante en este capítulo en la sección "Canales de soporte disponibles fuera de los planes de soporte".

La Tabla 4-2 describe los diferenciadores entre los planes de soporte pagado.

Tabla 4-2 Zonas y geografías

	Desarrollador	**Estándar**	**Pro Direct**	**Primer ministro**
Precio	$ 29 por mes	$ 100 por mes	$ 1,000 por mes	El precio del contrato varía
Apoyo técnico	Acceso a ingenieros de soporte por correo electrónico solo durante el horario comercial.	Acceso a ingenieros de soporte 24x7 por correo electrónico o teléfono.	Acceso a ingenieros de soporte 24x7 por correo electrónico o teléfono.	Acceso a ingenieros de soporte 24x7 por correo electrónico o teléfono.
Gravedad disponible	Gravedad C solamente.	Todos los niveles de gravedad.	Todos los niveles de gravedad.	Todos los niveles de gravedad.
Tiempo de respuesta	Menos de 8 horas hábiles.	Sev C: Menos de 8 horas hábiles. Sev B: Menos de 4 horas hábiles. Sev A: Menos de 1 hora comercial.	Sev C: Menos de 4 horas hábiles. Sev B: Menos de 2 horas hábiles. Sev A: Menos de 1 hora comercial.	Sev C: Menos de 4 horas hábiles. Sev B: Menos de 2 horas hábiles. Sev A: Menos de 1 hora comercial o menos de 15 minutos con la compra de Azure Rapid Response o Azure Event Management.
Orientación de arquitectura	Solo general	Solo general	Orientación basada en las mejores prácticas.	Orientación personalizada que incluye revisiones de diseño, ajuste de rendimiento, asistencia de configuración, etc.
Soporte de Operaciones			Asistencia con la incorporación, revisiones de servicios y consultas de Azure Advisor.	Revisiones de servicio e informes dirigidos por un gerente de cuenta técnica (TAM) asignado a su cuenta.

Con formato: Fuente: 12 pto

Con formato: Fuente: 12 pto

Con formato: Fuente: 12 pto

Con formato: Fuente: 12 pto

Con formato: Fuente: 12 pto

Con formato: Fuente: 12 pto

	Desarrollador	Estándar	Pro Direct	Primer ministro
Formación			Seminarios web realizados por equipos de ingeniería de Azure.	Seminarios web realizados por equipos de ingeniería de Azure. Capacitación bajo demanda coordinada a través de TAM.
Orientación proactiva			Proporcionado por entrega gestionar para Pro Direct.	Proporcionado por TAM.
Lanzamiento de soporte				Disponible a través de Azure Event Management por un costo adicional.

Consejo de examen

Puede cambiar su plan de soporte o cancelar su plan de soporte a través del portal de Azure. Si cancela un plan de soporte a mitad de mes, no se le reembolsará el monto prorrateado.

Cómo abrir un caso de soporte

Los casos de soporte de Azure se abren usando el portal de Azure. Los casos de soporte se pueden crear desde la página de inicio del portal haciendo clic en **Ayuda + Soporte** en el menú del lado izquierdo de la página. También puede crear un caso de soporte desde un recurso particular de Azure abriendo el recurso y haciendo clic en **Nueva solicitud** de soporte en la sección Soporte + Solución de problemas del menú de la izquierda.

Nota **Abrir casos de soporte**

Cuando abre un caso de soporte desde un recurso de Azure, el tipo de recurso y el nombre del recurso se rellenan automáticamente. Si abre un caso de soporte desde la página de inicio del portal, deberá seleccionar el recurso antes de poder abrir un caso de soporte.

En esta sección, mostraremos la experiencia de crear un caso de soporte desde la página de inicio del portal.

Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto
Con formato: Fuente: 12 pto

Después de hacer clic en **Ayuda + Soporte** en Azure Portal, se le presentan algunas opciones de autoayuda, como se muestra en la Figura 4-19 .

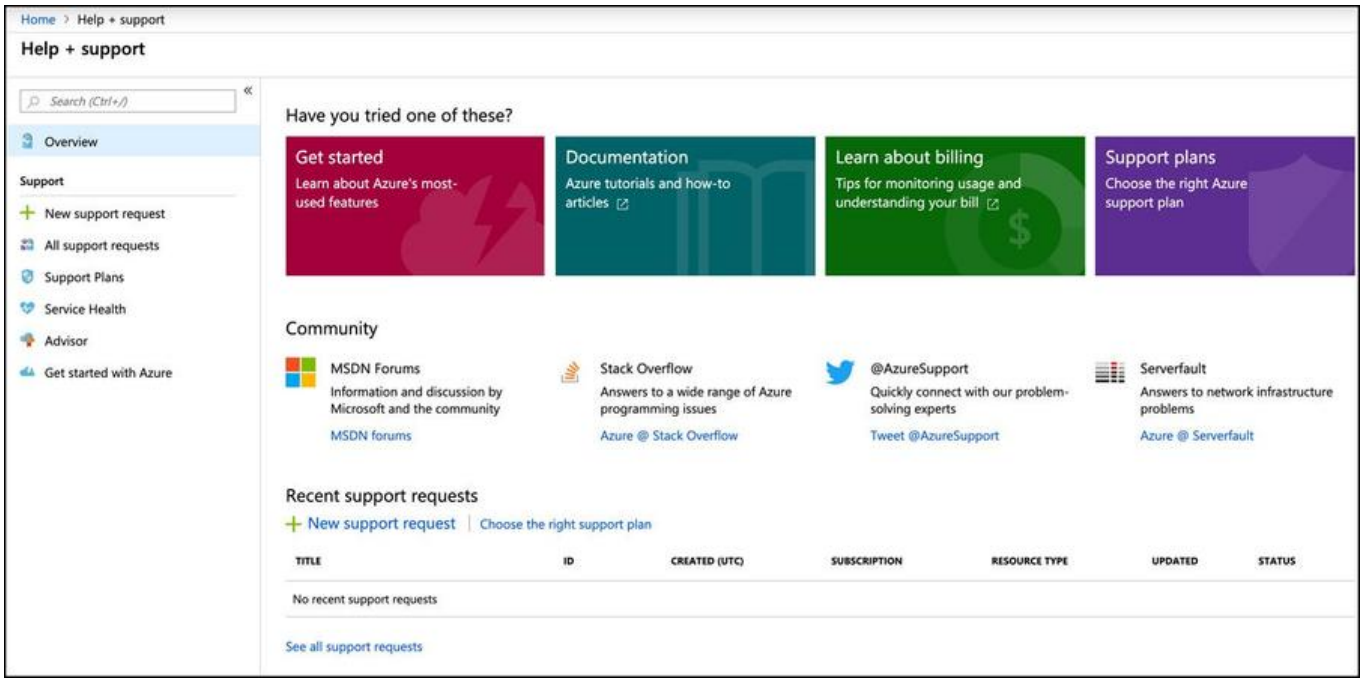


Figura 4-19 Opciones de ayuda y soporte en Azure Portal

Las opciones de autoayuda incluidas aquí son de naturaleza general e incluyen enlaces a documentación y enlaces a foros donde puede solicitar ayuda de otros usuarios de Azure. También puede twittear a @AzureSupport para obtener asistencia rápida para problemas simples.

Para crear un caso de soporte para un ingeniero de soporte de Microsoft, haga clic en **Nueva solicitud de soporte** . Crear un caso de soporte es un proceso de cuatro pasos, el primero de los cuales es proporcionar información básica como se muestra en la Figura 4-20 .

1. Seleccione **Sí** para indicar que tiene un problema relacionado con una suscripción de Azure. (La opción No es para problemas relacionados con Azure Active Directory).
2. Seleccione el tipo de problema. El tipo de problema puede ser un problema de facturación, un problema de suscripción, un problema de cuota o un problema técnico. En este ejemplo, estamos utilizando el tipo de problema técnico.
3. Seleccione el servicio de Azure.
4. Seleccione el recurso con el que necesita ayuda. (Su elección estará restringida al tipo de servicio de Azure que seleccionó).
5. Selecciona tu tipo de problema. Las opciones de tipo de problema variarán según el tipo de servicio.
6. Seleccione el subtipo del problema. Las opciones de subtipo de problema variarán según el tipo de servicio.
7. Ingrese un tema breve para su caso de soporte.
8. Haga clic en **Siguiente: Soluciones** para pasar al siguiente paso.

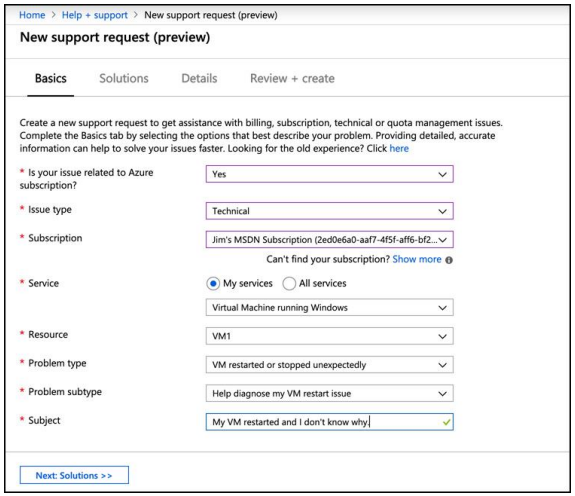


Figura 4-20 Opciones de ayuda y soporte en Azure Portal

Microsoft analiza constantemente los problemas históricos de los clientes para que puedan ofrecerle posibles soluciones basadas en la información que proporciona al abrir un caso. Usan el tipo de problema, el subtipo del problema y el texto que ingresa en el asunto para determinar cuál podría ser el problema.

En la Figura 4-21 , puede ver que Microsoft sugiere que el reinicio podría deberse a un reinicio de la VM iniciado por el usuario. Si decide que esto no causó el problema, haga clic en **Siguiente: Detalles** para pasar al siguiente paso.

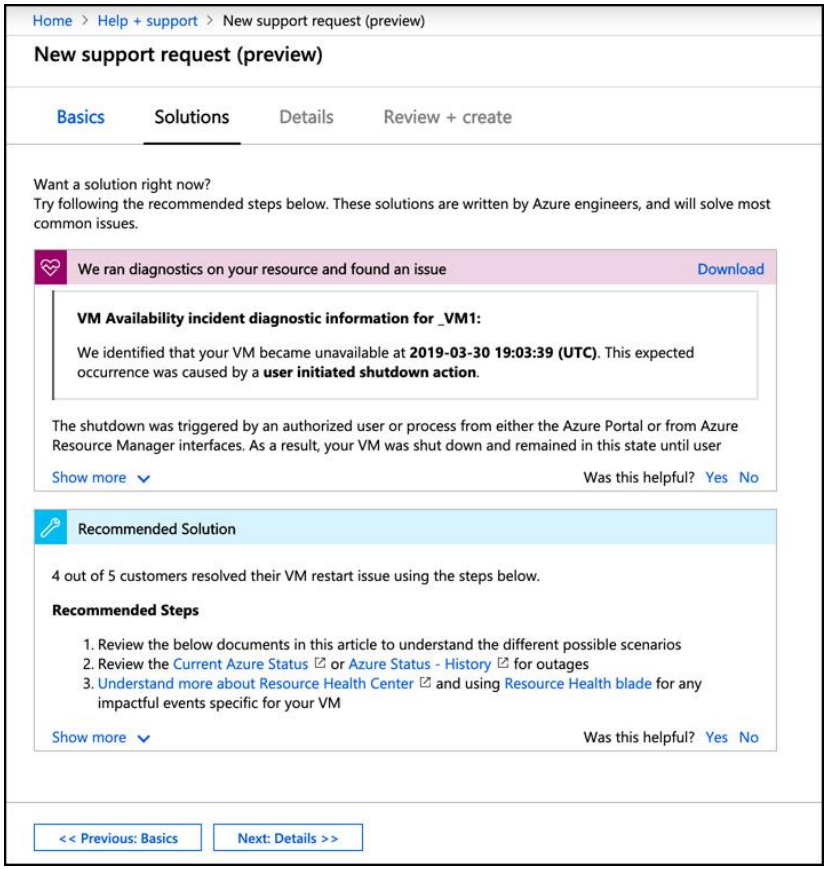


Figura 4-21 Posibles causas del problema

El último paso para crear un caso es ingresar los detalles de su problema como se muestra en la Figura 4-22 . Algunas de estas opciones diferirán según el tipo de recurso. En este ejemplo, las opciones son para una máquina virtual de Azure.

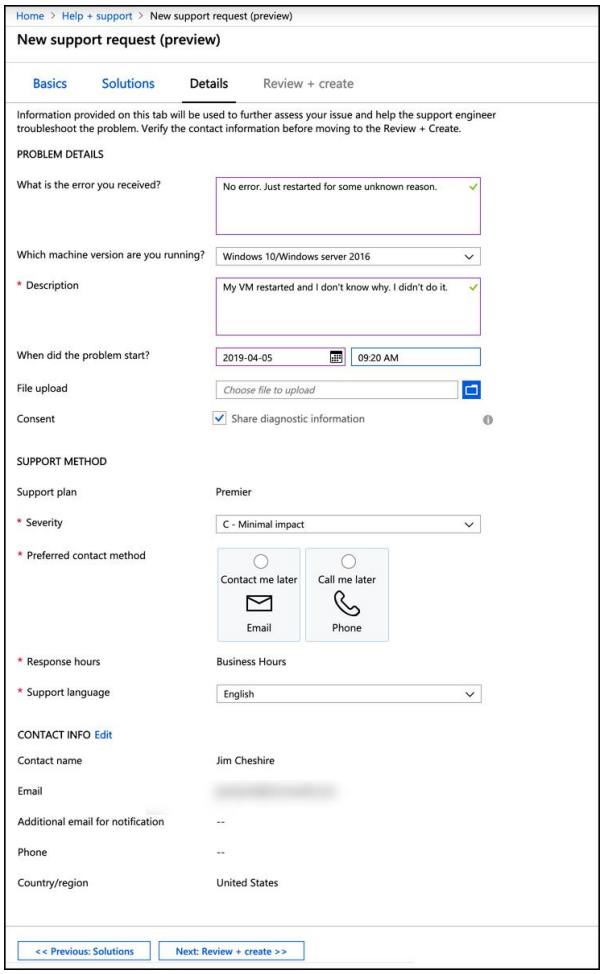


Figura 4-22 Introducción de detalles del caso de soporte

1. Ingrese cualquier error que haya recibido.
2. Seleccione el sistema operativo del menú desplegable.
3. Ingrese una descripción de su problema.
4. Ingrese una fecha y hora para cuando comenzó su problema. Si el problema fue un evento único, ingrese la fecha y hora en que ocurrió el problema.
5. Cargue todos los archivos relevantes, como capturas de pantalla o registros de errores.
6. Si desea compartir información de diagnóstico con Microsoft, marque la casilla de verificación **Consentimiento** .
7. Elige tu nivel de gravedad. Si tiene un plan de soporte para Desarrolladores, solo podrá seleccionar Severity C.
8. Elige tu método de contacto. Microsoft se comunicará con usted dentro de un período de tiempo determinado por su nivel de gravedad y su plan de soporte.
9. Elige tu idioma de soporte.
10. Edite su información de contacto si es necesario.
11. Haga clic en **Siguiente: Revisar + Crear** para continuar. Se le mostrará la información que ingresó para su confirmación y tendrá un botón Crear para completar el caso de soporte.

Canales de soporte disponibles fuera de los planes de soporte

Si no tiene un plan de soporte de Azure, aún puede obtener ayuda con problemas técnicos de Azure en foros o Twitter, pero no tendrá ningún SLA de soporte y no podrá hablar directamente con un soporte de Microsoft ingeniero.

Hay dos canales de foro disponibles para problemas de Azure.

- **Foros de MSDN** Accesible en: *https://aka.ms/MSDNForums* . Busque su producto para encontrar el foro relevante.
- **Foros de Stack Overflow** Accesible en: *https://stackoverflow.com* . Haga clic en **Etiquetas** y busque su servicio de Azure.

Los foros de MSDN y Stack Overflow son foros de usuario a usuario donde los clientes de Azure pueden ayudarse entre sí. Microsoft también monitorea los foros y puede brindar asistencia con problemas simples. Sin embargo, en algunos casos, le pedirán que abra un caso de soporte.

También puede tuitear a @AzureSupport para obtener ayuda con problemas simples. Esta es la cuenta oficial de Microsoft Twitter para ayudarlo a encontrar respuestas a preguntas comunes y soporte para problemas básicos.

Centro de Conocimiento

Para ayudarlo a encontrar documentación y publicaciones de blog sobre problemas comunes, Microsoft desarrolló el Centro de conocimiento. Puede acceder al Centro de conocimiento navegando a: *https://azure.microsoft.com/en-ca/resources/knowledge-center* .

Como se muestra en la Figura 4-23 , puede filtrar en el producto Azure que le interesa. Cada producto tiene una serie de etiquetas que puede usar para filtrar aún más los enlaces que ve en el Centro de conocimiento. También puede ingresar un término de búsqueda para encontrar algo más específico para su problema.

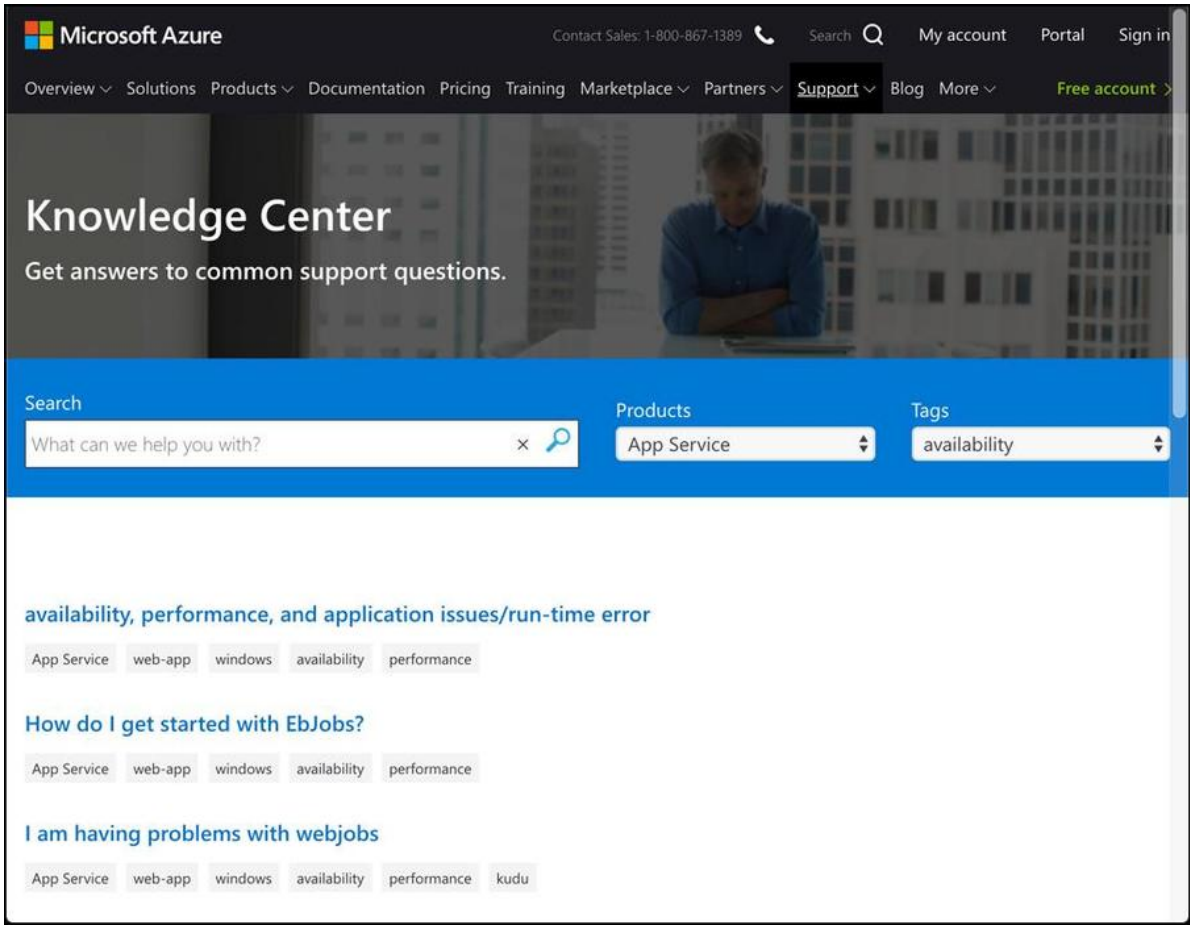


Figura 4-23 Centro de conocimiento

HABILIDAD 4.4: DESCRIBIR LOS ACUERDOS DE NIVEL DE SERVICIO DE AZURE

Muchos de los servicios que utiliza hoy en día incluyen un *acuerdo de nivel de servicio* (SLA) que sirve como un contrato entre usted y el proveedor de servicios para un cierto nivel de servicio.

Esta sección cubre:

- Acuerdo de nivel de servicio (SLA)
- Determinar el SLA para un producto o servicio particular de Azure

Acuerdo de nivel de servicio (SLA)

Los SLA establecen objetivos específicos de disponibilidad, y también definen lo que hará el proveedor de servicios cuando no se cumplan esos objetivos. Los SLA se expresan como un porcentaje y casi siempre son del 99% o más. El nivel más alto de disponibilidad expresado en un SLA es 99.999%, comúnmente conocido como *5 nueves* . Para brindarle un poco de contexto mientras discutimos los SLA, un servicio con un SLA de 5 nueves garantiza que el tiempo de inactividad durante todo un año no excederá los 5.56 minutos. Un SLA más razonable de 99.9% garantiza que el tiempo de inactividad durante el período de un mes no excederá los 43.2 minutos.

Más información **Slas y cantidades de tiempo de inactividad**

Para obtener detalles sobre los niveles de SLA y el tiempo de inactividad máximo permitido dentro del SLA, consulte: *https://docs.microsoft.com/azure/architecture/resiliency/#slas* .

Un concepto importante en los SLA de servicios en la nube es que el proveedor de la nube considera que una aplicación está fuera del SLA solo cuando no se cumple el porcentaje de disponibilidad debido a un problema que el proveedor de la nube puede controlar. En otras palabras, si implementa un nuevo código en su aplicación y hace que su aplicación se bloquee, el proveedor de la nube no considerará que se trata de una violación del SLA. Si instala un componente en su máquina virtual y hace que la máquina se caiga, eso no está bajo el control del proveedor de la nube y no se clasifica como que no cumple con el SLA.

Debido a que los SLA solo se refieren a problemas dentro del control del proveedor de la nube, cuando una aplicación adolece de falta de disponibilidad, es importante determinar si el problema es un problema de plataforma o un problema con su código o configuración. Responder esa pregunta puede ser más difícil de lo que piensas.

Azure es un entorno altamente complejo que involucra una gran cantidad de servicios que operan juntos. Por ejemplo, Azure App Service (uno de los servicios más populares de Azure) utiliza servicios en la nube de Azure, sistemas DNS de Azure, Azure Storage, Azure SQL Database y otros servicios de Azure. La degradación del rendimiento de cualquiera de esos servicios puede afectar eldisponibilidad de una aplicación que se ejecuta en App Service. Si informa que su aplicación App Service no está disponible, Microsoft debe determinar si eso es un problema de su parte o un problema con su aplicación.

Microsoft mantiene una enorme cantidad de datos de diagnóstico en todas las operaciones de Azure en todos los servicios de Azure. Cuando abre un caso de soporte con Microsoft para informar que su aplicación no está disponible, Microsoft puede realizar análisis de datos contra estos datos para determinar si hubo un problema con la plataforma Azure.

Si cree que la disponibilidad de su aplicación ha caído por debajo del SLA, es su responsabilidad presentar un reclamo a Microsoft. Puede hacerlo abriendo un caso de soporte. Si Microsoft determina que no se ha cumplido el SLA, puede recibir un crédito en su factura de Azure. El monto del crédito depende de la duración en que no se cumplió el SLA y la política específica de SLA del servicio de Azure.

 ***Consejo de examen***

Para ser elegible para un crédito debido a un incumplimiento de SLA, debe enviar un reclamo a Microsoft dentro de los dos meses posteriores al final del ciclo de facturación durante el cual se produjo el tiempo de inactividad.

La mayoría de los servicios de Azure ofrecen un SLA de al menos 99.9%, y el cliente puede lograr SLA más altos con una configuración adicional. Por ejemplo, una única VM que usa almacenamiento Premium para todos los discos tiene un SLA de 99.9%. Si implementa dos o más máquinas virtuales en el mismo conjunto de disponibilidad, ese SLA aumenta al 99.95%. Implemente esas dos o más instancias en dos o más zonas de disponibilidad dentro de la misma región de Azure y el SLA se mueve al 99.99%.

 ***Consejo de examen***

Microsoft ocasionalmente cambia los SLA. Si los términos de un SLA cambian, los nuevos términos entrarán en vigencia solo cuando renueve su suscripción de Azure. Hasta ese momento, estará bajo el SLA que estaba en vigencia cuando su suscripción se renovó por última vez o cuando se suscribió a una suscripción de Azure.

Determinar el SLA para un producto o servicio particular de Azure

Como el SLA varía entre los servicios de Azure y las configuraciones específicas pueden afectar el SLA de un único servicio de Azure, es importante poder determinar el SLA específico para los servicios de Azure que está utilizando. Microsoft proporciona una página web que tiene detalles sobre el SLA para cada servicio de Azure. Puede encontrarlo en: *https://azure.microsoft.com/en-us/support/legal/sla* .

Como se muestra en la Figura 4-24 , una vez en la página web de SLA, puede seleccionar una categoría para ver todos los servicios de Azure en esa categoría. También puede ingresar el nombre de su servicio en el cuadro de búsqueda para encontrar el SLA de ese servicio. Una vez que encuentre el servicio que le interesa, haga clic en él para leer los detalles sobre el SLA.

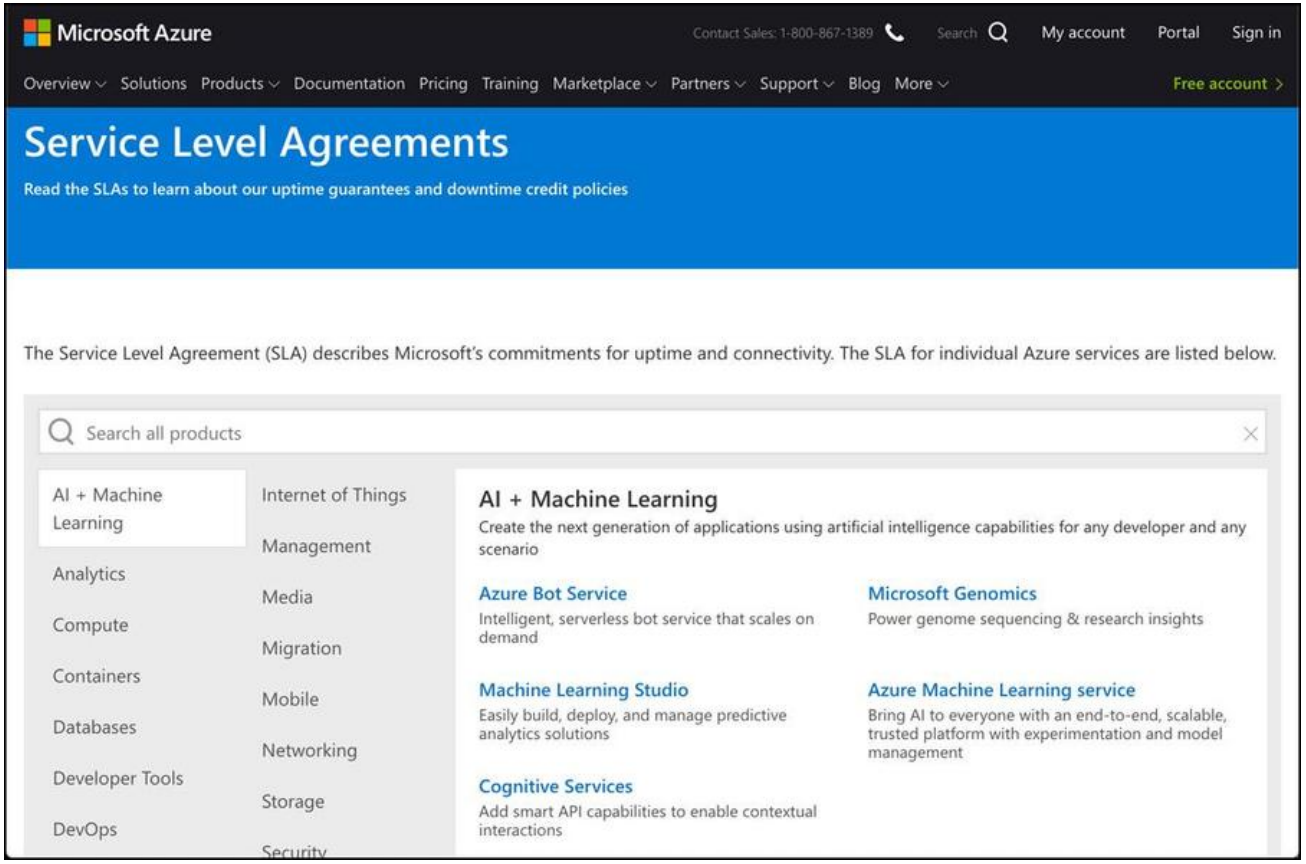


Figura 4-24 Página web de Azure SLA

Cuando hace clic en un servicio, verá detalles sobre el SLA proporcionado por ese servicio. La Figura 4-25 muestra la página SLA para máquinas virtuales de Azure. Los tres puntos en la parte superior de la página describen el SLA para las máquinas virtuales de Azure.

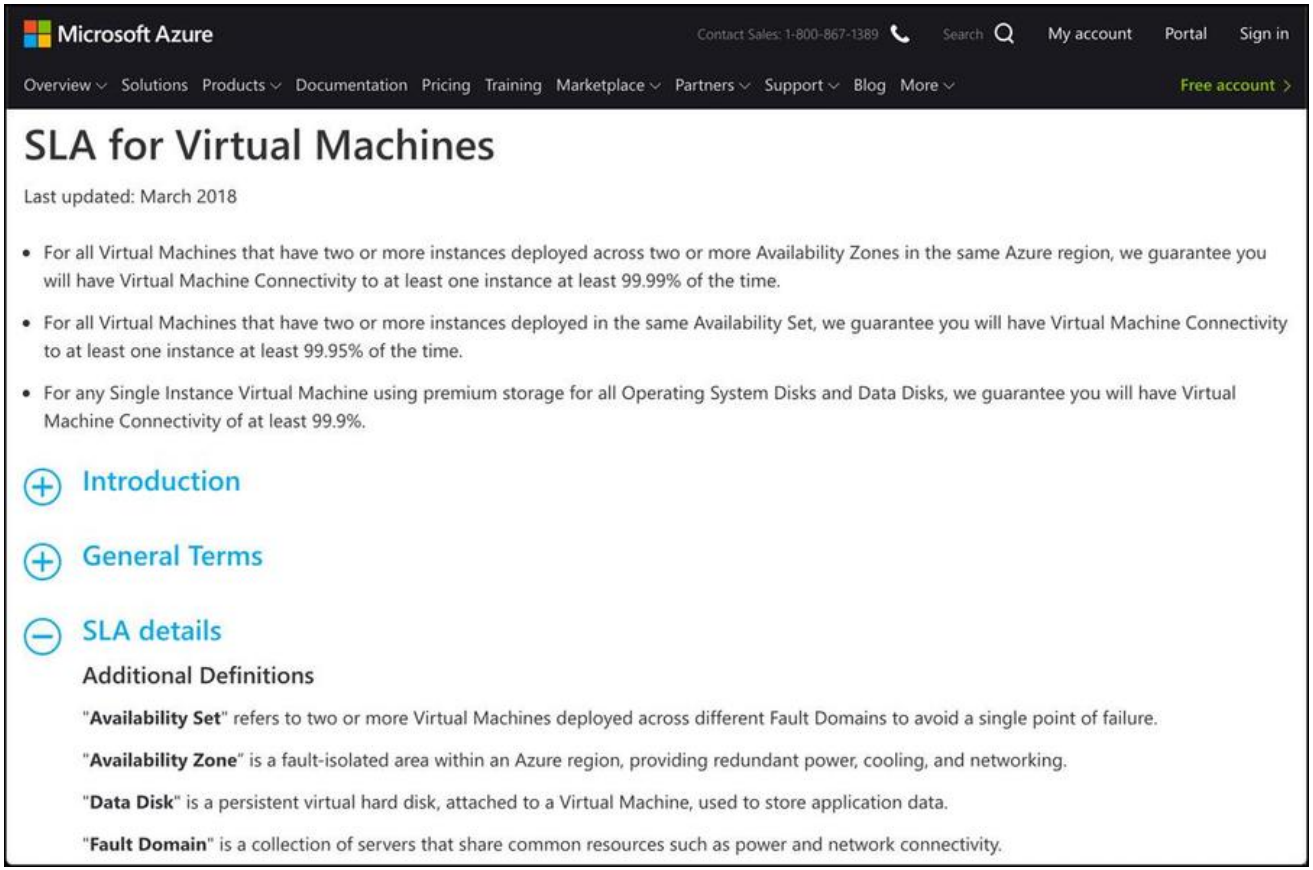


Figura 4-25 SLA de máquinas virtuales de Azure

La sección Introducción describe los SLA de Azure en general. La sección Términos generales describe los términos de SLA, como Portal de administración, Nivel de servicio y Tiempo de inactividad que se refieren a todos los servicios de Azure. También explica cómo puede realizar un reclamo y limitaciones para los SLA de Azure.

La sección Detalles de SLA se aplica al servicio de Azure específico que está viendo. Por ejemplo, esta sección en la página VM SLA define términos específicos de VM que se relacionan con el SLA para VM. Si se desplaza hacia abajo, verá detalles adicionales que se muestran en la Figura 4-26 , incluido cómo calcular la disponibilidad y la cantidad de crédito que puede recibir si no se cumple un SLA.

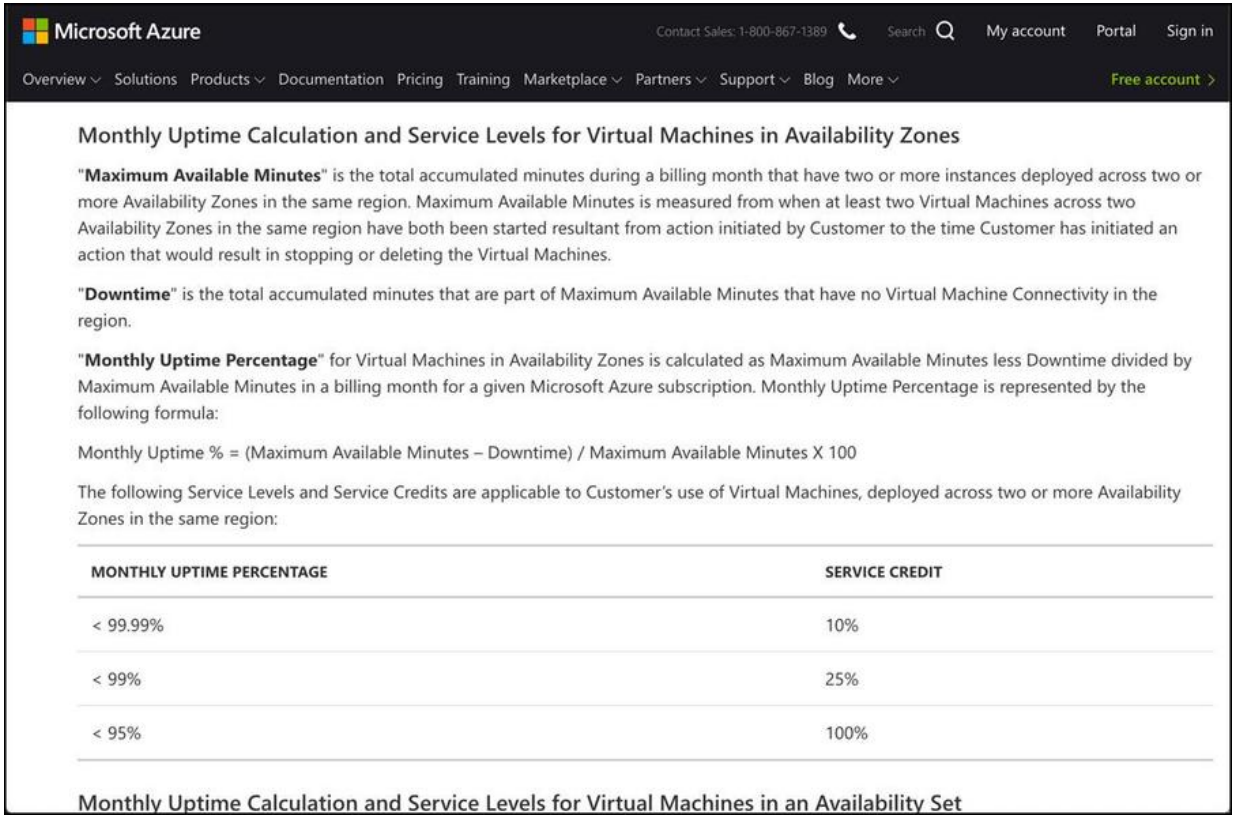


Figura 4-26 Detalles sobre Azure VM SLA

Si su aplicación usa múltiples servicios de Azure, se le aplicarán múltiples SLA. Si experimenta un tiempo de inactividad, debe enviar un reclamo por todos los servicios de Azure que cayeron por debajo del SLA si desea ser considerado para un crédito. Sin embargo, el crédito monetario no es su única preocupación relacionada con la disponibilidad de su aplicación. El tiempo de inactividad en su aplicación afecta negativamente a su negocio, por lo que siempre debe asegurarse de tener el SLA más alto posible, y cuando se trata de múltiples servicios de Azure con diferentes SLA, es importante comprender cómo eso afecta su SLA general.

Al calcular el SLA para una aplicación que usa varios servicios de Azure, debe calcular un SLA compuesto basado en los servicios que está usando. Por ejemplo, si tiene una aplicación web de App Service que también usa una única máquina virtual de Azure que usa almacenamiento Premium, debe combinar el SLA para ambos servicios para determinar el SLA general de su aplicación.

Nota **compuesto Slas**

Es importante comprender que los SLA de servicios individuales aún se aplican a usted cuando usa varios servicios de Azure. Sin embargo, comprender los SLA compuestos es importante porque le permite determinar cuándo una configuración específica aumenta la probabilidad de que experimente un tiempo de inactividad.

El SLA para App Service es del 99.95%, y el SLA para una sola VM que ejecuta almacenamiento Premium es del 99.9%. Por lo tanto, su SLA general para su aplicación es 99.95% x 99.9%, o 99.85%. Al implementar dos máquinas virtuales en dos zonas de disponibilidad en la misma región, puede obtener un SLA del 99.99% para sus máquinas virtuales, y eso aumenta su SLA general al 99.94%.

Más información **Informática Composite Slas**

Para obtener más información sobre cómo calcular SLA compuestos, consulte: *https://docs.microsoft.com/azure/architecture/resiliency/#composite-slas* .

HABILIDAD 4.5: COMPRENDER EL CICLO DE VIDA DEL SERVICIO EN AZURE

Azure es un entorno siempre cambiante y siempre se introducen nuevos servicios. Los servicios existentes también evolucionan con el tiempo e introducen nuevas características. Es importante comprender el ciclo de vida del servicio en Azure, cómo puede mantenerse al día con los cambios y cómo el ciclo de vida de un servicio podría afectar su soporte y su SLA.

Esta sección cubre:

- Funciones de vista previa públicas y privadas
- Cómo acceder a las funciones de vista previa
- Disponibilidad general (GA)
- Monitoreo de actualizaciones de funciones

Funciones de vista previa públicas y privadas

A medida que los equipos de productos de Azure desarrollan nuevos servicios y características, es importante que reciban comentarios de los clientes que usan esos servicios y características en un entorno del mundo real. Por esa razón, Microsoft a menudo ofrecerá nuevos servicios y características a los clientes como *ofertas preliminares* . Si bien el término oficial de Microsoft es una *vista previa* , a menudo verá que las personas se refieren a estos servicios y características como una oferta *beta* .

Consejo de examen

Los servicios y características que se encuentran en la vista previa no ofrecen un SLA y no están destinados a ser utilizados en aplicaciones de producción. Las características de vista previa tampoco suelen ofrecerse en todas las regiones de Azure. Microsoft proporcionará documentación sobre qué regiones están disponibles para una vista previa específica.

Los servicios y características de vista previa a veces se ofrecen primero como vista previa privada. En la vista previa privada, el servicio o la función se ponen a disposición de un pequeño conjunto de clientes para realizar pruebas. El acceso a una vista previa privada a veces es por invitación del equipo de ingeniería que desarrolla el servicio o la función. En otros casos, Microsoft puede proporcionar una forma para que cualquier cliente se registre para acceder a la vista previa privada. Si el registro está abierto para todos, Microsoft cerrará el registro después de que se haya registrado un número objetivo de clientes.

Servicios de *notas* versus características

Muchas vistas previas son para características de un servicio existente. Por ejemplo, el Servicio de aplicaciones puede agregar una nueva función para el servicio existente, y antes de que se lance completamente, pasará por un período en la fase de vista previa.

Los servicios y características de vista previa privada comúnmente exponen solo un subconjunto de la funcionalidad que eventualmente lo incluirá en el servicio o característica. Microsoft a menudo les pedirá a los clientes que utilicen una vista previa privada para probar escenarios específicos y proporcionar comentarios. Esto ayuda a los equipos de ingeniería a descubrir errores y problemas de usabilidad en los complejos entornos del mundo real que utilizan los clientes.

 *Consejo de examen*

No todos los servicios o características ofrecen una vista previa privada. Si no se ofrece una vista previa privada, el servicio o la función se ponen a disposición primero como una vista previa pública. Todos los servicios y características pasan por un período de vista previa pública.

Se pueden ofrecer vistas previas privadas a los clientes sin costo, pero es más común que se ofrezcan con un descuento sustancial

Una vez que un servicio o característica cumple con una barra específica establecida por el equipo de ingeniería, pasará a la vista previa pública. Esto generalmente ocurre una vez que el servicio o característica es completamente funcional o muy cercano a él. Sin embargo, si hay errores en una parte específica de la funcionalidad que el equipo de ingeniería considera crítica, pueden retrasar la vista previa pública hasta que se corrijan esos errores.

Las características y servicios que se encuentran en versión preliminar pública se proporcionan a una tarifa con descuento, pero al igual que las características y servicios de vista previa privada, generalmente no ofrecen un SLA y se proporcionan tal cual.

Cómo acceder a las funciones de vista previa

Los clientes que participan en una vista previa privada a veces reciben un enlace secreto al portal de Azure que habilita el servicio o la función. Cuando el cliente usa ese enlace, Microsoft puede usar su ID de suscripción de Azure para determinar si se ha registrado y está aprobado para la vista previa privada. Si no lo están, la función o el servicio no estarán disponibles, incluso si usan el enlace secreto.

En otras situaciones, la experiencia de Azure Portal no se ha desarrollado para una función o servicio de vista previa privada. En esos casos, los clientes reciben instrucciones de la línea de comandos para usar el servicio o la función. Es más común que la interfaz de usuario del portal se desarrolle durante la fase de vista previa privada, por lo que los primeros usuarios generalmente solo tienen acceso a la línea de comandos.

Una vez que un servicio o función alcanza la vista previa pública, se pone a disposición de todos los clientes en las regiones donde está disponible, y no es necesario registrarse para usar el servicio o la función. Se mostrará una insignia de vista previa en Azure Portal para que los usuarios sepan que el servicio o la función es una oferta de vista previa. La Figura 4-27 muestra las características del contenedor Docker en una aplicación web del Servicio de aplicaciones que se ejecuta en Windows, y cada configuración del contenedor lleva una insignia de vista previa.

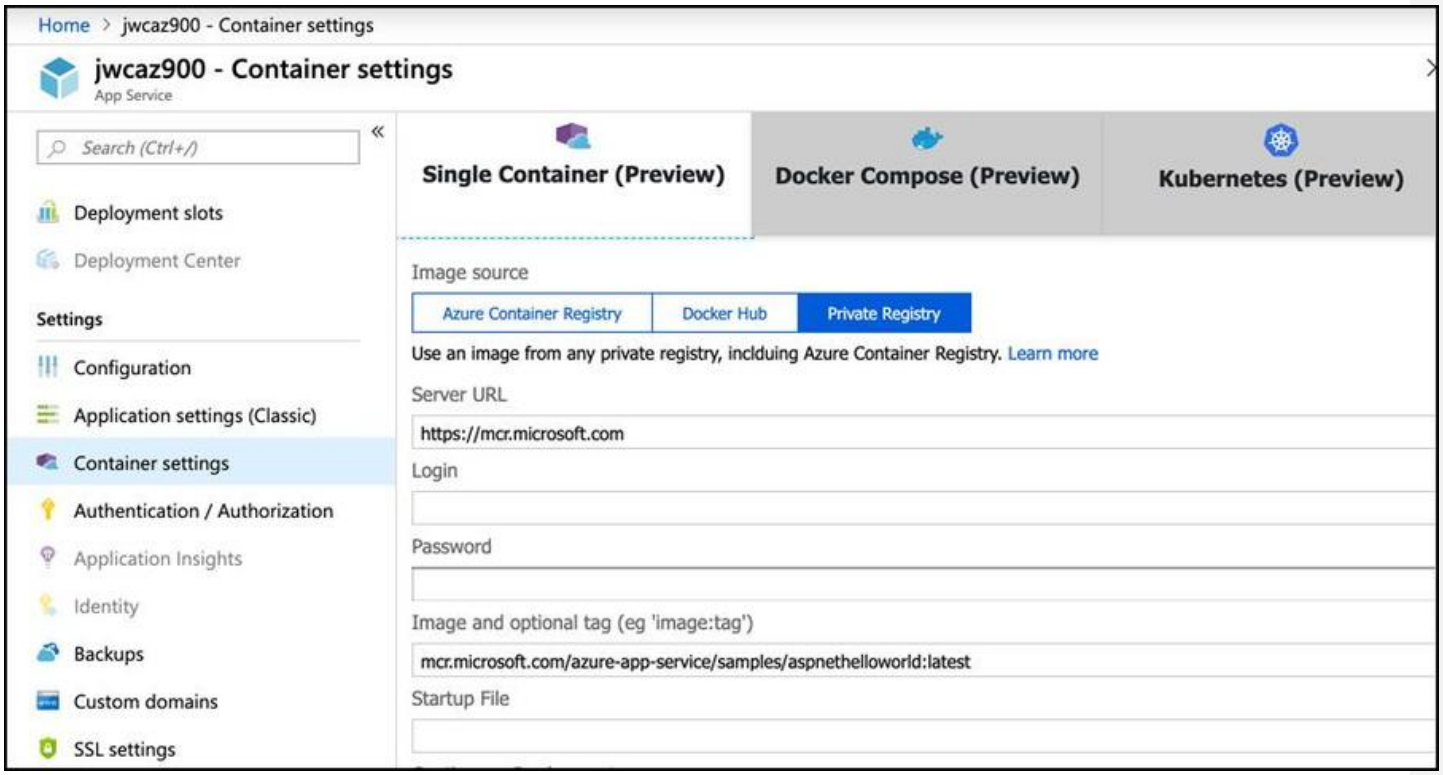


Figura 4-27 Funciones de vista previa en App Service

Los servicios y características que se encuentran en la vista previa pública generalmente son compatibles con Microsoft como si se hubieran lanzado por completo. Sin embargo, los SLA no se aplican a las vistas previas, y hay algunas situaciones en las que un servicio o característica no será compatible con los ingenieros de soporte de Microsoft durante la vista previa. En esos casos, puede ser derivado a foros para recibir asistencia.

Disponibilidad general

Una vez que un servicio o función de vista previa alcanza una barra de calidad y disponibilidad adecuada para el equipo de ingeniería, declararán *disponibilidad general* o GA. En este punto, el servicio o característica es totalmente compatible.

Una vez que un servicio o función llega a GA, cae bajo el SLA que proporciona Microsoft. Si se trata de un nuevo servicio, se publicará un nuevo SLA en la página web del SLA. Para las nuevas funciones de los servicios existentes, una vez que se alcanza el GA, la función heredará el SLA del servicio del que es una característica.

Si estaba utilizando una función o servicio durante la vista previa pública, por lo general no tendrá que hacer nada para recibir el respaldo oficial de GA. Sin embargo, en algunas situaciones, Microsoft le pedirá que elimine los recursos creados durante la vista previa y los vuelva a crear. Esto generalmente ocurre cuando los restos que quedan del código de vista previa pueden causar un problema con un servicio o función que se ejecuta en GA.

Cuando un servicio o características llega a GA, puede que no sea GA en todas las geografías de Azure. En esos casos, otras geografías generalmente serán GA más adelante en el ciclo de vida del servicio o característica. El precio de vista previa también puede permanecer vigente durante un período de tiempo posterior a GA. Detalles como este se publican en el anuncio oficial de GA en el sitio web de Azure.

Monitoreo de actualizaciones de funciones

Microsoft generalmente publicará anuncios de nuevas características y servicios en el blog de Azure en: *https://azure.microsoft.com/en-us/blog/topics/announcements* . Sin embargo, una fuente de información más confiable sobre actualizaciones de características y servicios es la página web de Actualizaciones de Azure disponible en: *https://azure.microsoft.com/en-us/updates* .

La Figura 4-28 muestra la página web Actualizaciones de Azure. De manera predeterminada, se muestran todas las actualizaciones, pero puede filtrar tipos específicos de actualización mediante el menú desplegable Tipo de actualización.

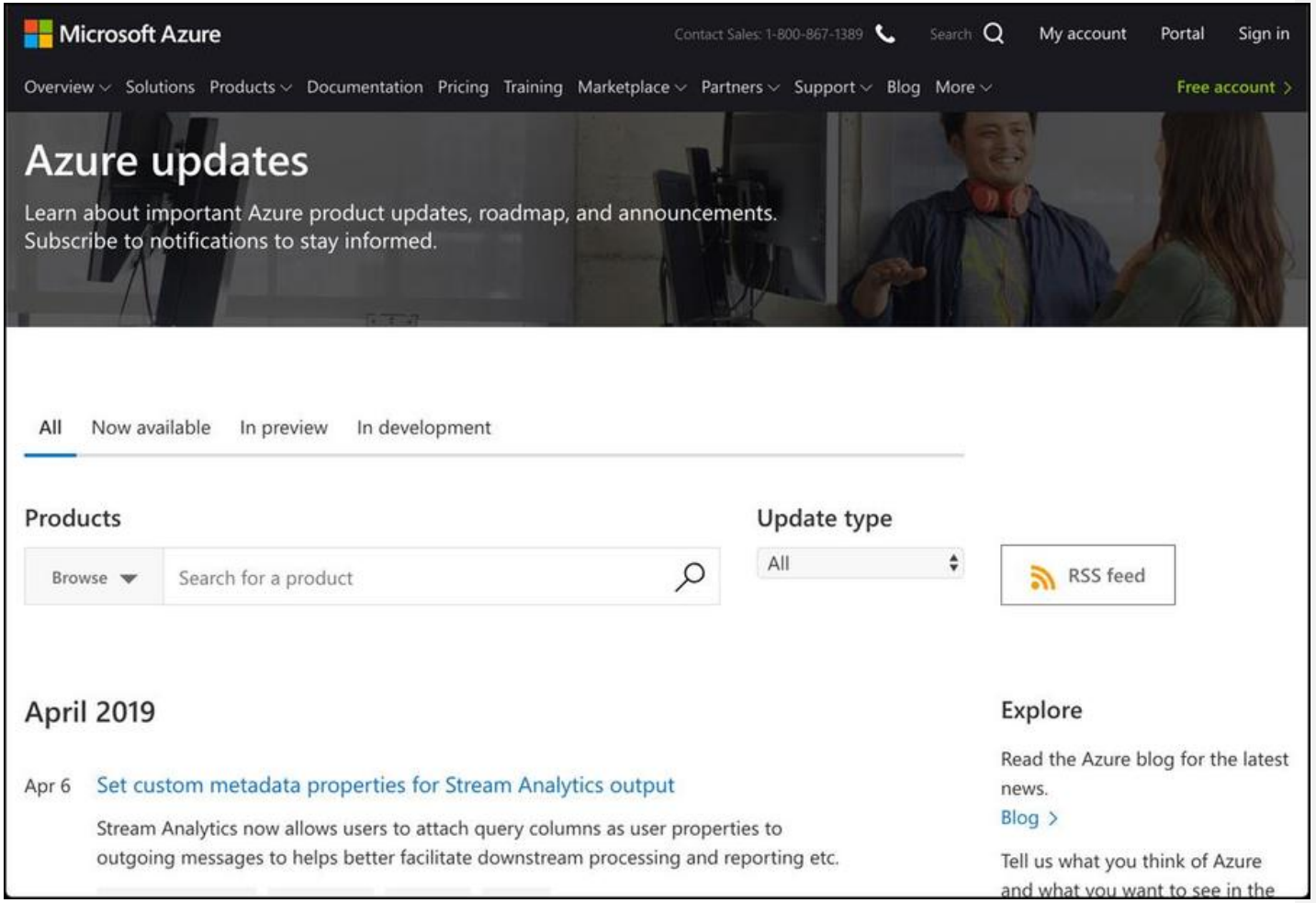


Figura 4-28 Página web de actualizaciones de Azure

Para mostrar solo las actualizaciones en una etapa particular del ciclo de vida del producto, use las pestañas en la parte superior de la lista. La pestaña Ahora disponible muestra todas las actualizaciones sobre los servicios y características de GA. La pestaña En vista previa mostrará todos los servicios y características en vista previa pública o privada. La pestaña En desarrollo mostrará información relacionada con características o servicios que están actualmente en desarrollo pero que aún no están disponibles para los clientes.

Tenga en cuenta **Vista previa privada y actualizaciones de desarrollo**

Las vistas previas privadas a veces no se anuncian al público en general, por lo que es posible que no siempre aparezcan en la página web de Actualizaciones de Azure. Del mismo modo, no se anunciarán todas las características o servicios en desarrollo.

Para mostrar actualizaciones solo para los productos que le interesan, puede buscar un producto ingresándolo en el cuadro de búsqueda. También puede hacer clic en **Examinar** y seleccionar uno o más productos de la lista como se muestra en la Figura 4-29 .

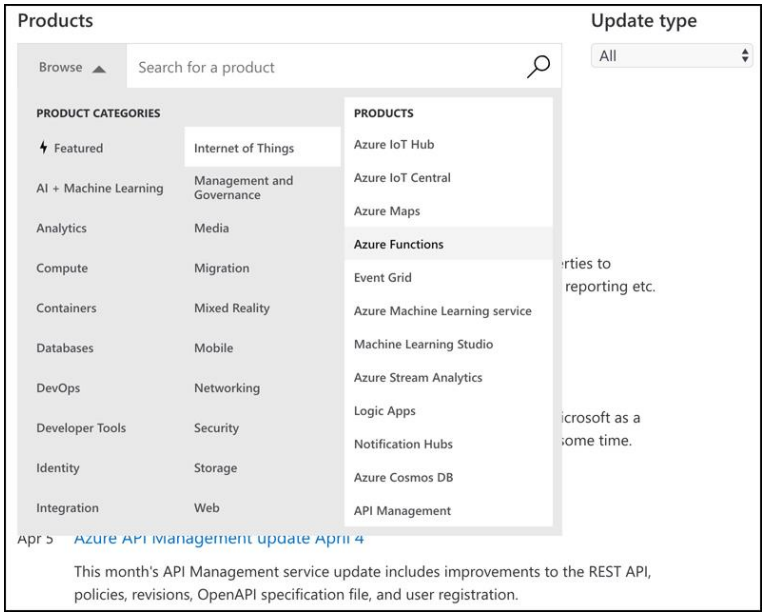


Figura 4-29 Filtrado de actualizaciones en productos específicos

EXPERIMENTO MENTAL

Pongamos en práctica los conceptos que has aprendido en este capítulo usando un experimento mental. Las respuestas a este experimento mental se pueden encontrar en la siguiente sección.

ContosoPharm tiene una aplicación local que utiliza un servidor web instalado en un servidor físico que ejecuta Windows Server 2016. Utiliza otro servidor físico que ejecuta SQL Server para el almacenamiento de datos de back-end. También almacenan documentos escaneados en un dispositivo de almacenamiento conectado a la red (NAS).

La base de datos contiene información de ventas para farmacias que almacenan productos ContosoPharm. El personal de ventas accede a la base de datos utilizando una sección del sitio web asignada a las ventas. La división reguladora de ContosoPharm utiliza una sección separada del sitio web para cargar documentos escaneados en el dispositivo NAS.

El director de TI de ContosoPharm ha recomendado que la aplicación se traslade a la nube. Sin embargo, el director financiero de la compañía requiere que se envíe un informe detallado que pruebe que ContosoPharm puede ahorrar dinero usando la nube.

El CIO, John, está preocupado por la separación de departamentos. En la configuración actual, el personal de ventas no puede acceder a ninguno de los recursos utilizados por la división reguladora, y desean asegurarse de que esta política se mantenga vigente. John también quiere asegurarse de que la naturaleza crítica de la aplicación se realice después de que se mueva a la nube. Si hay un problema con la disponibilidad de la aplicación, John quiere asegurarse de que puedan involucrar a alguien en Microsoft sobre el problema dentro de una hora.

El CEO, Jill, también está preocupado por mudarse a la nube. A Jill le preocupa el gasto excesivo en recursos en la nube y, dado que los gastos en ContosoPharm no son los mismos mes a mes, le preocupa vigilar los gastos a largo plazo.

Se le encarga asesorar al director de TI sobre el cumplimiento de los requisitos de los diversos ejecutivos de nivel C en ContosoPharm para convencerlos de que se muden a Azure.

EXPERIENCIAS DE PENSAMIENTO RESPUESTAS

Esta sección proporciona las respuestas al experimento mental.

Primero decide abordar los problemas de costos del CFO. Con la calculadora de costo total de propiedad, compila un informe detallado que muestra cuánto puede ahorrar en los próximos cinco años si se muda a Azure. La calculadora de TCO tiene en cuenta todos los ahorros, incluidos los ahorros en hardware de computadoras, costos de electricidad y costos de infraestructura de TI. Con este método, puede mostrar claramente un ahorro de decenas de miles de dólares en un período de cinco años. También puede descargar una copia del informe para que otros ejecutivos de nivel C puedan consultarlo para reforzar su caso.

También elabora una estimación de sus gastos totales de Azure con la calculadora de precios. Al exportar este informe a una hoja de cálculo de Excel, el CFO puede incorporarlo fácilmente en los presupuestos existentes para ver cómo los gastos de Azure se ajustan a la planificación financiera.

Para abordar las inquietudes del CIO sobre la separación de departamentos, recomienda que se usen dos suscripciones de Azure. Los recursos para ventas se pueden crear bajo una suscripción y los recursos para la división reguladora se pueden crear bajo la otra suscripción. Luego puede usar RBAC para imponer restricciones de acceso a las suscripciones, de modo que solo las personas a las que desea tener acceso puedan acceder a los recursos de cada suscripción.

Para abordar las inquietudes del CIO relacionadas con el soporte, usted recomienda que ContosoPharm compre un plan de soporte Pro Direct. Si bien este plan de soporte le costará a ContosoPharm $ 1,000 por mes, les dará acceso a los ingenieros de soporte de Microsoft 24x7, y si surge un problema crítico que afecte la disponibilidad de la aplicación, ConotosoPharm puede abrir un caso de soporte de Sev A con Microsoft y recibir una respuesta dentro de una hora .

Para abordar las inquietudes del CEO, prepara una presentación que describe la gestión de costos. Su presentación incluye información sobre la creación de presupuestos que puede aplicar a los gastos. Muestra cómo puede crear alertas que notificarán a las personas apropiadas cuando los gastos lleguen a un punto determinado. Debido a que los gastos varían mes a mes, usted demuestra cómo se pueden aplicar los presupuestos a plazos específicos y cómo se pueden crear presupuestos múltiples para cubrir todos los escenarios de gastos.

También presenta información sobre el análisis de costos en Administración de costos y cómo puede ver fácilmente los gastos desglosados por servicios, grupos de recursos, ubicaciones, etc. Estos informes también se pueden abarcar a suscripciones específicas para que los ejecutivos de nivel C puedan revisar los gastos solo para el personal de ventas, solo para la división reguladora o para todos combinados.

Finalmente, presenta información sobre las recomendaciones del asesor en la gestión de costos y cómo esta característica puede ayudar a resaltar las áreas donde se pueden lograr ahorros de costos. También recomienda que si Jill está realmente interesada en usar los recursos de Azure a largo plazo, ContosoPharm probablemente pueda ahorrar dinero comprando un Acuerdo de empresa y aceptando un compromiso a largo plazo para el uso de los recursos de Azure.

RESUMEN DEL CAPÍTULO

Los costos y el soporte se encuentran entre las principales preocupaciones de las empresas que se mudan a la nube, y es importante comprender cómo minimizar los costos y garantizar que sus opciones de soporte satisfagan sus necesidades. En este capítulo, aprendió sobre los siguientes conceptos relacionados con los precios y el soporte.

- Los recursos de Azure se crean dentro de una suscripción de Azure.
- Las suscripciones tienen límites asociados, y puede crear suscripciones adicionales si necesita más de lo que permiten estos límites.
- Azure ofrece una suscripción de prueba gratuita y suscripciones de pago por uso.
- Puede comprar productos y servicios de Azure directamente de Microsoft o a través de un Microsoft Cloud Solution Partner (CSP).

- Los CSP venden soluciones completas en la nube y no administra recursos individuales de Azure.
- Puede comprar productos y servicios de Azure de Microsoft en el portal de Azure o puede comprometerse a un uso a largo plazo de los recursos de Azure y ahorrar dinero con un Acuerdo de empresa.
- Una suscripción de prueba gratuita le brinda acceso gratuito a los servicios de Azure más populares durante un año. También proporciona $ 200 en crédito para productos y servicios de Azure.
- Los servicios de Azure se facturan según los medidores asociados con un recurso.
- Los costos de los servicios de Azure pueden variar en diferentes regiones. Los costos también varían según las zonas de facturación que incluyen geografías específicas.
- La calculadora de precios facilita la estimación de sus costos de Azure al seleccionar los productos que pretende usar, y las estimaciones se pueden compartir, guardar para referencia posterior o exportar a Excel.
- La calculadora de TCO le permite determinar sus ahorros de costos en Azure sobre los gastos locales durante un período de cinco años.
- Puede controlar sus gastos en Azure asegurándose de utilizar todos los recursos de Azure por los que está pagando.
- Puede ahorrar dinero cuando necesite recursos en la nube para trabajos más pequeños que no son urgentes mediante el uso de Azure Batch para ejecutar sus cargas de trabajo en máquinas virtuales no utilizadas.
- La creación de presupuestos en Azure Cost Management puede hacer que sea fácil ver cuándo los gastos se acercan a límites predefinidos, y las alertas se pueden usar para notificar a las personas adecuadas cuando los gastos alcanzan un umbral definido.
- El análisis de costos puede ayudarlo a ver qué recursos contribuyen a sus gastos de Azure.
- Microsoft ofrece soporte gratuito para problemas de suscripción y facturación. Los problemas técnicos requieren la compra de un plan de soporte de Azure o una cuenta Premier.
- Los niveles del plan de soporte determinan cuándo puede hablar con el personal de soporte de Microsoft y el tiempo de respuesta que Microsoft promete cuando abre un caso de soporte.
- Puede abrir un caso de soporte desde el portal mediante la página de inicio o la opción de menú Nueva solicitud de soporte mientras se encuentra dentro de un recurso de Azure específico.
- Microsoft proporciona foros de MSDN y foros de desbordamiento de pila para soporte fuera de los planes de soporte. También puede usar la cuenta de Twitter @AzureSupport para problemas simples.
- El Centro de conocimiento puede ayudarlo a encontrar artículos de soporte para productos Azure específicos.
- Los servicios de Azure ofrecen un acuerdo de nivel de servicio (SLA) que garantiza un cierto nivel de disponibilidad. Los servicios que no cumplan con el SLA pueden hacerlo elegible para un crédito en su factura de Azure.

- Puede usar la página web de SLA en el sitio web de Microsoft para encontrar detalles de SLA para todos los servicios de Azure.
- El ciclo de vida del servicio de Azure puede incluir una vista previa privada y siempre incluye una vista previa pública y disponibilidad general (GA).
- Los servicios y características de la vista previa no ofrecen un SLA y generalmente están disponibles con un descuento.
- Las vistas previas privadas generalmente están disponibles mediante herramientas de línea de comandos. Las vistas previas públicas están disponibles para todos en Azure Portal.
- Una vez que una característica o servicio cumple con el nivel de calidad para soporte completo y SLA, está generalmente disponible (GA).
- La página Actualizaciones de Azure proporciona detalles sobre actualizaciones de características y servicios y ciclos de vida.