# **Introducción**

Completado

100 XP

* 3 minutos

Ha sido contratado por una empresa global dedicada a las carreras de automóviles para que modernice totalmente su plataforma web y de supervisión. Han decidido reemplazar los servidores Linux existentes por una infraestructura en la nube que aprovecha las últimas tendencias en arquitectura. Parte del sistema se ejecutará en la plataforma sin servidor de Azure con Azure Functions para procesar los datos de las carreras en tiempo real y se insertarán las estadísticas, los datos de las carreras y otros fragmentos relevantes de información analizada en clústeres de bases de datos. Quieren conservar el sitio web que tienen, ya que se remozó hace solo un año, pero hay que conectarlo a este flujo de datos moderno.

El sitio web se ejecuta en Apache con Linux y, como ya está en funcionamiento, usted decide trasladarlo directamente a Azure usando una máquina virtual de Azure. De esta forma puede acceder a los datos con una cantidad mínima de trabajo por su parte.

## **Objetivos de aprendizaje**

En este módulo, aprenderá a:

* Entender las opciones disponibles para las máquinas virtuales en Azure
* Crear una máquina virtual Linux mediante Azure Portal
* Conectarse a una máquina virtual Linux en ejecución mediante SSH
* Instalar el software y cambiar la configuración de red en una máquina virtual mediante Azure Portal

# **Creación de una máquina virtual Linux en Azure**

Completado

100 XP

* 10 minutos

Tenemos un sitio web que se ejecuta en un servidor Ubuntu Linux local. Nuestro objetivo es crear una máquina virtual (VM) de Azure con la imagen de Ubuntu más reciente y luego migrar el sitio a la nube. En esta unidad, obtendrá información sobre las opciones que hay que evaluar al crear una máquina virtual en Azure.

## **Introducción a Azure Virtual Machines**

Azure Virtual Machines es un recurso de informática en la nube escalable y a petición. Incluye procesadores, memoria, almacenamiento y recursos de red. Las máquinas virtuales se pueden iniciar y detener a voluntad y se administran desde Azure Portal o con la CLI de Azure. También se puede usar Secure Shell (SSH) remoto para conectarse directamente a la máquina virtual en ejecución y ejecutar los comandos como si estuviese en un equipo local.

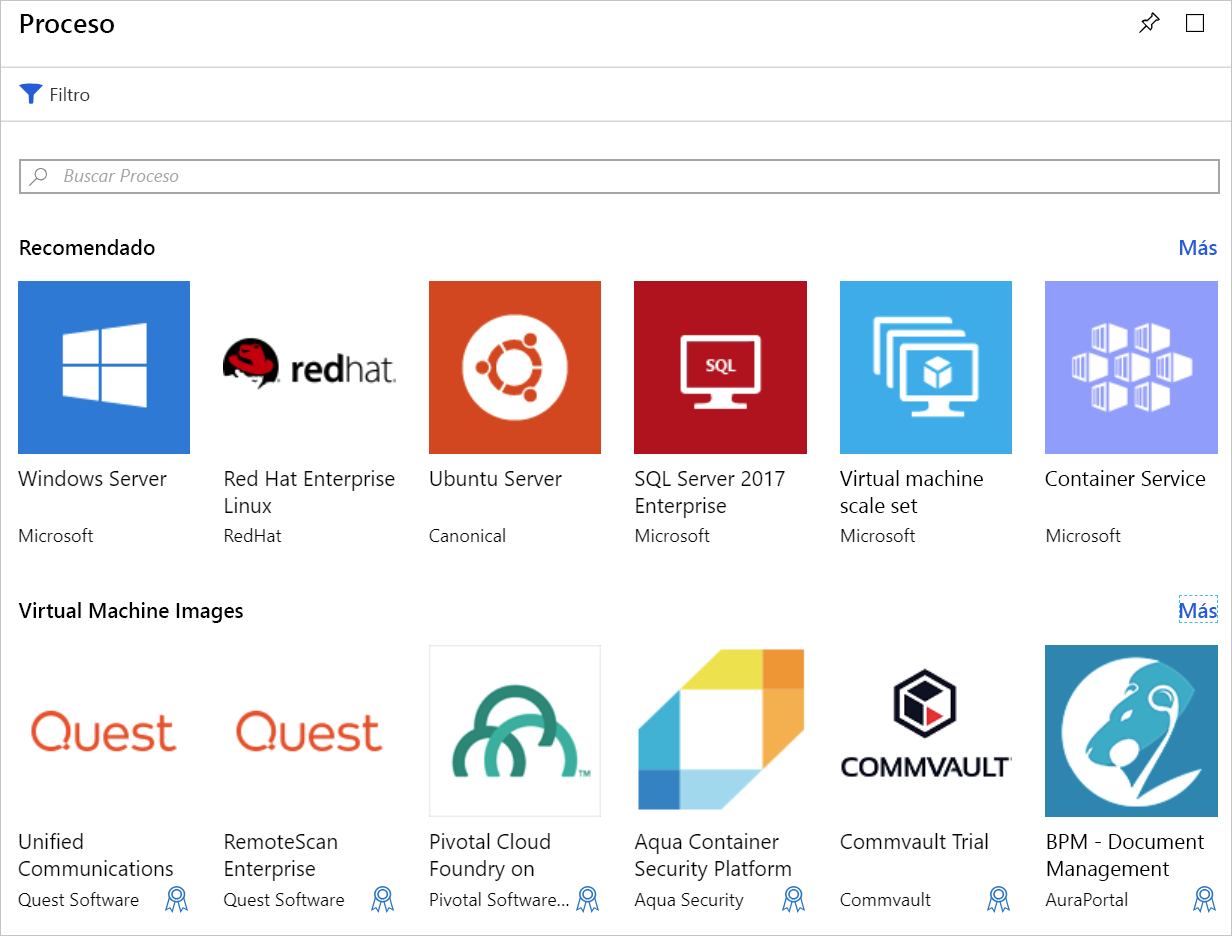
### **Ejecución de Linux en Azure**

Es muy fácil crear máquinas virtuales Linux en Azure. Microsoft colabora con los principales proveedores de Linux para garantizar que sus distribuciones estén optimizadas para la plataforma Azure. Puede crear máquinas virtuales a partir de imágenes precompiladas de diferentes distribuciones de Linux conocidas, como SUSE, Red Hat y Ubuntu, o bien compilar una distribución de Linux propia para ejecutarla en la nube.

## **Creación de una máquina virtual de Azure**

Las máquinas virtuales se pueden definir e implementar en Azure de varias formas: Azure Portal, un script (mediante la CLI de Azure o Azure PowerShell) o una plantilla de Azure Resource Manager. En todos los casos, será necesario proporcionar cierta información que se indicará en breve.

En Azure Marketplace también se ofrecen imágenes preconfiguradas que incluyen tanto un sistema operativo como herramientas populares de software instaladas para escenarios específicos.



## **Recursos que se usan en una máquina virtual Linux**

Al crear una máquina virtual Linux en Azure, también se crean los recursos necesarios para hospedarla. Estos recursos funcionan de forma conjunta para virtualizar un equipo y ejecutar el sistema operativo Linux. Deben existir ya (y seleccionarse durante la creación de la máquina virtual); de lo contrario, se crean con la máquina virtual:

* Una máquina virtual que proporcione recursos de CPU y memoria
* Una cuenta de Azure Storage que hospede los discos duros virtuales
* Discos virtuales que hospeden el sistema operativo, las aplicaciones y los datos
* Una red virtual para conectar la máquina virtual a otros servicios de Azure o al hardware local
* Una interfaz de red para comunicarse con la red virtual
* Una dirección IP pública opcional para acceder a la máquina virtual

Al igual que con otros servicios de Azure, necesitará un grupo de recursos que contenga la máquina virtual (y, opcionalmente, agrupar estos recursos para su administración). Al crear una máquina virtual, puede usar un grupo de recursos existente o crear uno nuevo.

## **Elección de la imagen de máquina virtual**

La selección de una imagen es una de las primeras y más importantes decisiones que deberá tomar al crear una máquina virtual. Una imagen es una plantilla que se usa para crear una máquina virtual. Estas plantillas incluyen un sistema operativo y, a menudo, otro software, como herramientas de desarrollo o entornos de hospedaje web.

Todo lo que se pueda instalar en un equipo se puede incluir en una imagen. Se puede crear una máquina virtual a partir de una imagen preconfigurada para realizar exactamente las tareas que se necesitan como, por ejemplo, hospedar una aplicación web en un servidor HTTP de Apache.

Sugerencia

También se pueden crear y cargar imágenes de disco personalizadas.

## **Tamaño de la máquina virtual**

Al igual que una máquina física tiene cierta cantidad de memoria y potencia de CPU, ocurre lo mismo con una máquina virtual. Azure ofrece una variedad de máquinas virtuales de distintos tamaños con diferentes precios. El tamaño que elija determinará factores como la capacidad de procesamiento, la memoria y la capacidad de almacenamiento máxima de la máquina virtual.

Advertencia

Existen límites de cuota en cada suscripción, lo que puede afectar a la creación de máquinas virtuales. Si experimenta estos límites de cuota, puede [abrir una solicitud de soporte técnico al cliente en línea](https://docs.microsoft.com/es-es/azure/azure-supportability/resource-manager-core-quotas-request) para aumentar los límites.

Los tamaños de máquina virtual se agrupan en categorías, desde la serie B para las pruebas básicas hasta la serie H para tareas de computación masivas. Debe seleccionar el tamaño de máquina virtual según la carga de trabajo que desee realizar. El tamaño de la máquina virtual se puede cambiar después de haberla creado, pero antes hay que detenerla. Por lo tanto, es mejor ajustar su tamaño correctamente desde el principio, si es posible.

#### **Estas son algunas instrucciones en función del escenario de destino**

| **¿Qué hace?** | **Considere estos tamaños** |
| --- | --- |
| Web o informática de uso general: para desarrollo y pruebas, bases de datos pequeñas o medianas, y servidores web de tráfico bajo o medio. | B, Dsv3, Dv3, DSv2, Dv2 |
| Tareas de cálculo intensivo: para servidores web de tráfico medio, aplicaciones de red, procesos por lotes y servidores de aplicaciones. | Fsv2, Fs, F |
| Gran uso de memoria: para servidores de bases de datos relacionales, memorias caché de capacidad media o grande y análisis en memoria. | Esv3, Ev3, M, GS, G, DSv2, Dv2 |
| Almacenamiento y procesamiento de datos: bases de datos de macrodatos, SQL y NoSQL que necesitan alto rendimiento de disco y de E/S. | Ls |
| Representación de gráficos intensiva o edición de vídeo, así como para el aprendizaje y la inferencia de modelos (ND) con aprendizaje profundo. | NV, NC, NCv2, NCv3, ND |
| Informática de alto rendimiento (HPC): sus cargas de trabajo necesitan las máquinas virtuales de CPU más rápidas y eficaces con interfaces de red de alto rendimiento opcionales. | H |

## **Elección de opciones de almacenamiento**

El siguiente conjunto de decisiones gira en torno al almacenamiento. En primer lugar, puede elegir la tecnología de disco. Las opciones incluyen una unidad de disco duro (HDD) tradicional con platos o una moderna unidad de estado sólido (SSD). Al igual que el hardware que se adquiere, el almacenamiento SSD cuesta más, pero ofrece mejor rendimiento.

Sugerencia

Hay dos niveles de almacenamiento SSD: Estándar y Premium. Elija discos SSD Estándar si tiene cargas de trabajo normales, pero desea mejorar el rendimiento. Elija discos SSD Premium si tiene cargas de trabajo que realizan un uso intensivo de la E/S o sistemas críticos que necesitan procesar datos muy rápidamente.

### **Asignación de almacenamiento a discos**

Azure usa los discos duros virtuales (VHD) para representar discos físicos para la máquina virtual. Los discos duros virtuales replican el formato lógico y los datos de una unidad de disco, pero se almacenan como blobs en páginas en una cuenta de Azure Storage. En cada uno de los discos puede elegir el tipo de almacenamiento que debe usar (SSD o HDD). Esto permite controlar su rendimiento, probablemente en función de la E/S que planea realizar en él.

De forma predeterminada, se crean dos discos duros virtuales (VHD) para la máquina virtual Linux:

1. El disco del sistema operativo: esta es la unidad principal y tiene una capacidad máxima de 2048 GB. De forma predeterminada se etiquetará como /dev/sda.
2. Un disco temporal: este proporciona almacenamiento temporal para el sistema operativo o las aplicaciones. En las máquinas virtuales Linux, el disco es /dev/sdb y el agente de Linux de Azure lo formatea y monta en /mnt. Su tamaño se ajusta en función del tamaño de la máquina virtual y se usa para almacenar el archivo de intercambio.

Advertencia

El disco temporal no es persistente. En este disco solo se deben escribir datos que no sean críticos para el sistema.

#### **¿Qué sucede con los datos?**

Los datos se pueden almacenar en la unidad principal junto con el sistema operativo, pero es mejor crear *discos de datos* dedicados. Puede crear y conectar discos adicionales a la máquina virtual. Cada disco puede contener un máximo de 32 767 gibibytes (GiB) de datos y la cantidad máxima de almacenamiento la determina el tamaño de máquina virtual que seleccione.

Nota

Los tamaños de los discos virtuales de Azure se miden en Gibibytes (GiB), que no son lo mismo que Gigabytes (GB); un GiB es aproximadamente 1,074 GB. Por lo tanto, para obtener un equivalente aproximado del tamaño del disco virtual en GB, multiplique el tamaño en GiB por 1,074 y eso devolverá un tamaño en GB relativamente cercano. Por ejemplo, 32,767 GiB serían aproximadamente 35,183 GB.

Una funcionalidad interesante es crear una imagen de disco duro virtual a partir de un disco real. Esto permite migrar fácilmente la información *existente* desde un equipo local a la nube.

### **Diferencias entre discos administrados y no administrados**

Finalmente, debe decidir entre usar discos no administrados o administrados.

Con los discos no administrados, usted es el responsable de las cuentas de almacenamiento que contienen los discos duros virtuales correspondientes a sus discos de máquina virtual. Las tarifas de la cuenta de almacenamiento que se pagan dependen de la cantidad de espacio que se use. Una cuenta de almacenamiento tiene un límite fijo de 20 000 operaciones de E/S por segundo, lo que significa admite 40 discos duros virtuales estándar a máxima potencia. Si desea realizar un escalado horizontal, necesitará más de una cuenta de almacenamiento, lo que puede complicar las cosas.

Los discos administrados son el modelo de almacenamiento en disco más reciente y el recomendado. Solucionan de forma elegante esa complejidad al pasar a Azure la carga de administrar las cuentas de almacenamiento. Especifique el tipo (Premium o Estándar) y tamaño del disco, y Azure creará y administrará tanto el disco *como* el almacenamiento que use. No tiene que preocuparse por los límites de la cuenta de almacenamiento, lo que facilita el escalado horizontal. También ofrecen otras ventajas:

* Mayor confiabilidad: Azure garantiza que los discos duros virtuales asociados con máquinas virtuales de alta confiabilidad se colocarán en distintas partes de Azure Storage para proporcionar niveles similares de resistencia.
* Mayor seguridad: los discos administrados son recursos reales administrados en el grupo de recursos, lo que significa que pueden usar el control de acceso basado en rol para restringir quién puede trabajar con los datos del disco duro virtual.
* Compatibilidad con instantáneas: se pueden usar instantáneas para crear una copia de solo lectura de un disco duro virtual. Se recomienda apagar la máquina virtual para borrar cualquier proceso que esté en curso. La creación de la instantánea solo tarda unos segundos. Una vez hecho esto, puede encender la máquina virtual y usar la instantánea para crear un duplicado de la máquina virtual a fin de solucionar un problema de producción o revertirla al punto en el tiempo en que se ha tomado la instantánea.
* Compatibilidad con copias de seguridad: con Azure Backup se pueden realizar copias de seguridad automáticas de los discos administrados en regiones diferentes para la recuperación ante desastres sin que esto afecte a los servicios de la máquina virtual.

## **Comunicación de red**

Las máquinas virtuales se comunican con los recursos externos mediante una red virtual (VNet). La red virtual representa una red privada de una sola región en la que se comunican los recursos. Una red virtual es igual que las redes que usted administra de forma local. Las redes virtuales se pueden dividir en subredes para aislar recursos, conectarlas a otras redes (incluidas las redes locales) y aplicar reglas de tráfico para controlar las conexiones entrantes y salientes.

### **Planeamiento de la red**

Cuando cree una máquina virtual, tendrá la opción de crear una nueva red virtual o usar una existente en su región.

Es fácil hacer que Azure cree la red junto con la máquina virtual, pero es probable que no sea la mejor opción para la mayoría de los escenarios. Es mejor planear los requisitos de red *por adelantado* para todos los componentes de la arquitectura y crear la estructura de la red virtual por separado. Luego, cree las máquinas virtuales y colóquelas en las redes virtuales ya creadas. Más adelante en este módulo examinaremos las redes virtuales más detalladamente.

Antes de crear una máquina virtual, es preciso que decidamos cómo queremos administrarla. Veamos las opciones.

# **Ejercicio: Decisión de un método de autenticación de SSH**

Completado

100 XP

* 10 minutos

Espacio aislado activado. Tiempo restante: 1 h 55 min

Usó 1 de 10 espacios aislados por hoy. Mañana habrá disponibles más espacios aislados.

Para poder crear una máquina virtual Linux en Azure, es preciso pensar en el acceso remoto. Queremos poder iniciar sesión en nuestro servidor web de Linux para configurar el software y realizar el mantenimiento. El enfoque predeterminado para administrar máquinas virtuales Linux hospedadas en Azure es SSH.

## **¿Qué es SSH?**

Secure Shell (SSH) es un protocolo de conexión cifrada que permite inicios de sesión seguros a través de conexiones no seguras. SSH permite conectarse a un shell de terminal desde una ubicación remota mediante una conexión de red.

Se pueden usar dos métodos para autenticar una conexión SSH: nombre de usuario y contraseña o un par de claves SSH.

Aunque SSH proporciona una conexión cifrada, el uso de contraseñas con conexiones SSH deja a la máquina virtual vulnerable ante ataques por fuerza bruta de contraseñas. Un método más seguro y preferible para conectarse a una máquina virtual Linux con SSH es un par de claves pública- privada, lo que se conoce también como claves SSH.

Con un par de claves SSH, puede iniciar sesión en máquinas virtuales de Azure basadas en Linux sin contraseña. Este método es más seguro si solo se planea iniciar sesión en la máquina virtual desde varios equipos. Si necesita poder acceder a la máquina virtual Linux desde varias ubicaciones, es posible que una combinación de nombre de usuario y contraseña sea un enfoque mejor. Un par de claves SSH consta de dos partes: una clave pública y una clave privada.

* La clave pública se coloca en la máquina virtual Linux o en cualquier otro servicio que se quiera usar con una criptografía de clave pública. Se puede compartir con cualquiera.
* La clave privada es la que se presenta para verificar la identidad en la máquina virtual Linux al crear una conexión SSH. Considere que es información confidencial y protéjala como si fuera una contraseña o cualquier otro dato privado.

Puede usar el mismo par único de claves pública y privada para acceder a varios servicios y máquinas virtuales de Azure.

## **Creación del par de claves SSH**

En Windows 10, Linux y macOS, puede usar el comando ssh-keygen integrado para generar los archivos de clave pública y privada SSH.

Windows 10 incluye un cliente SSH con Fall Creators Update. Las versiones anteriores de Windows requieren software adicional para el uso de SSH; [consulte la documentación para obtener los detalles completos](https://docs.microsoft.com/es-es/azure/virtual-machines/linux/ssh-from-windows). Como alternativa, puede instalar el subsistema de Linux para Windows y obtener la misma función.

Usaremos Azure Cloud Shell, que almacena las claves generadas en Azure en la cuenta de almacenamiento privado. Si lo prefiere, también puede escribir estos comandos directamente en el shell local. Si adopta este método, deberá ajustar las instrucciones que aparecen a lo largo de este módulo para reflejar una sesión local.

Aquí está el comando mínimo necesario a fin de generar el par de claves para una máquina virtual de Azure. Esto crea un par de claves pública y privada de RSA con el protocolo SSH 2 (SSH 2). La longitud mínima es de 2048 bits, pero para este módulo de aprendizaje usaremos 4096.

1. En Cloud Shell, ejecute el comando siguiente.
2. Bash
3. Copiar

ssh-keygen -m PEM -t rsa -b 4096

1. Presione Entrar para aceptar la ubicación predeterminada. El comando crea dos archivos: id\_rsa e id\_rsa.pub, en el directorio ~/.ssh. Si los archivos existen, se sobrescriben.
2. Escriba una frase de contraseña que pueda recordar. Necesitará esta frase de contraseña cuando use la clave SSH para acceder a la máquina virtual.

Se pueden usar varias opciones para especificar el nombre de archivo o una frase de contraseña a fin de evitar las solicitudes.

### **Frase de contraseña de clave privada**

También se puede especificar una frase de contraseña al generar la clave privada. Es una contraseña que debe escribir al usar la clave. Esta frase de contraseña se usa para acceder al archivo de claves SSH privado y no es la contraseña de la cuenta de usuario.

Cuando agrega una frase de contraseña a la clave SSH, cifra la clave privada mediante AES de 128 bits para que la clave privada no se pueda usar sin la frase de contraseña para descifrarla.

Se recomienda encarecidamente agregar una frase de contraseña. Si un atacante robara su clave privada y esta no tuviera una frase de contraseña, podría usarla para iniciar sesión en los servidores que tuvieran la clave pública correspondiente. Si una frase de contraseña protege una clave privada, ese atacante no la puede usar. Esto proporciona una capa adicional de seguridad para la infraestructura en Azure.

## **Usar el par de claves SSH con una máquina virtual Linux de Azure**

Cuando se haya generado el par de claves, podrá usarlo con una máquina virtual Linux en Azure. La clave pública se puede especificar durante la creación de máquinas virtuales o se puede agregar después de que se haya creado la máquina virtual.

Puede ver el contenido del archivo en Cloud Shell si ejecuta el comando siguiente.

Bash

Copiar

cat ~/.ssh/id\_rsa.pub

Tendrá un aspecto similar a la salida siguiente:

Resultado

Copiar

ssh-rsa XXXXXXXXXXc2EAAAADAXABAAABAXC5Am7+fGZ+5zXBGgXS6GUvmsXCLGc7tX7/rViXk3+eShZzaXnt75gUmT1I2f75zFn2hlAIDGKWf4g12KWcZxy81TniUOTjUsVlwPymXUXxESL/UfJKfbdstBhTOdy5EG9rYWA0K43SJmwPhH28BpoLfXXXXXGX/ilsXXXXXKgRLiJ2W19MzXHp8z3Lxw7r9wx3HaVlP4XiFv9U4hGcp8RMI1MP1nNesFlOBpG4pV2bJRBTXNXeY4l6F8WZ3C4kuf8XxOo08mXaTpvZ3T1841altmNTZCcPkXuMrBjYSJbA8npoXAXNwiivyoe3X2KMXXXXXdXXXXXXXXXXCXXXXX/ azureuser@myserver

Copie este valor para poder usarlo en el ejercicio siguiente.

### **Uso de la clave SSH al crear una máquina virtual Linux**

Para aplicar la clave SSH al crear una nueva máquina virtual Linux, será preciso copiar el contenido de la clave pública y especificarlo en Azure Portal, *o* especificar el archivo de clave pública para el comando de CLI de Azure o de Azure PowerShell. Usaremos este método al crear nuestra máquina virtual Linux.

### **Adición de la clave SSH a una máquina virtual Linux existente**

Si ya ha creado una máquina virtual, puede instalar la clave pública en la máquina virtual Linux con el comando ssh-copy-id. Cuando se haya autorizado la clave SSH, se concederá acceso al servidor sin contraseña, aunque se le seguirá pidiendo la frase de contraseña en la clave si la tiene establecida.

Por ejemplo, si tuviéramos una máquina virtual Linux denominada *myserver* con un usuario *azureuser*, podríamos ejecutar el comando siguiente para instalar el archivo de clave pública y autorizar al usuario con la clave.

Bash

Copiar

ssh-copy-id -i ~/.ssh/id\_rsa.pub azureuser@myserver

Ahora que tenemos la clave pública, vamos a cambiar a Azure Portal y crear una máquina virtual Linux.

# **Ejercicio: Creación de una máquina virtual Linux con Azure Portal**

Completado

100 XP

* 20 minutos

Espacio aislado activado. Tiempo restante: 1 h 51 min

Usó 1 de 10 espacios aislados por hoy. Mañana habrá disponibles más espacios aislados.

Recordemos que el objetivo es mover un servidor Linux existente que ejecuta Apache a Azure. Comenzaremos por crear un servidor de Ubuntu Linux.

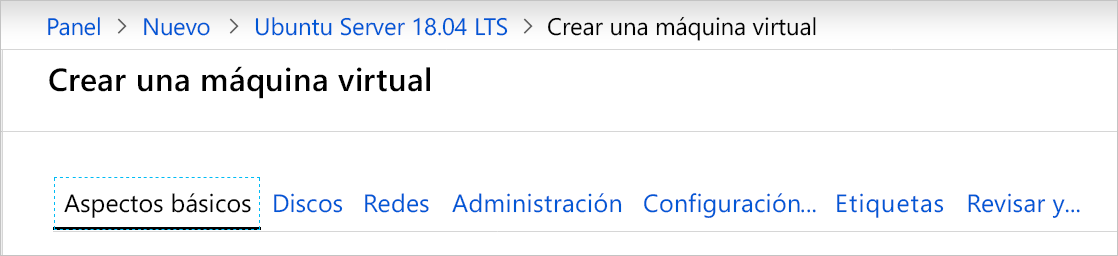
## **Creación de una máquina virtual Linux**

Se pueden crear máquinas virtuales Linux con Azure Portal, la CLI de Azure o Azure PowerShell. El enfoque más sencillo cuando se empieza con Azure es usar el portal, porque lo guiará a través de la información necesaria, y proporciona sugerencias y mensajes útiles durante la creación:

1. Inicie sesión en [Azure Portal](https://portal.azure.com/learn.docs.microsoft.com) con la misma cuenta con la que ha activado el espacio aislado.
2. En el menú de Azure Portal o la página Inicio de Servicios de Azure, seleccione Máquinas virtuales. También puede escribir *Máquinas virtuales* el cuadro de búsqueda superior y presionar Entrar. Se mostrará el panel Máquinas virtuales.
3. En la barra de menús superior, seleccione Agregar > Máquina virtual. Aparece el panel Crear una máquina virtual.

## **Configuración de la máquina virtual, adición de discos de datos para la máquina virtual y configuración de la red**

La experiencia de creación de la máquina virtual en el portal se presenta en un formato de asistente que le guía a través de todas las áreas de configuración de la máquina virtual. Si selecciona Siguiente, se le dirigirá a la siguiente sección configurable. Pero se puede mover entre las secciones a voluntad con las pestañas de la parte superior, que identifican cada parte.



Una vez que haya completado todas las opciones necesarias (identificadas con asteriscos de color rojo), puede omitir el resto de la experiencia del asistente y empezar a crear la máquina virtual. Para ello, seleccione Revisar y crear en la parte inferior del asistente.

Empezaremos por la pestaña Datos básicos. Recuerde que estas instrucciones usan el espacio aislado. Si usa otra cuenta de Azure Portal, es posible que tenga que adaptar algunos detalles según corresponda.

1. En la pestaña Aspectos básicos, escriba los valores siguientes para cada opción.

| **Configuración** | **Value** |
| --- | --- |
| Detalles del proyecto |  |
| Suscripción | Suscripción de Concierge (la suscripción del espacio aislado debe estar seleccionada de forma predeterminada). |
| Resource group | Seleccione learn-83b1475d-ea79-4b5a-959b-22c0a9f050d5. |
| Detalles de instancia |  |
| Nombre de la máquina virtual | Escriba un nombre para la máquina virtual de servidor web, como test-web-eus-vm1. Esto indica el entorno (test), el rol (web), la ubicación (East US), el servicio (vm) y el número de instancia (1). Se considera un procedimiento recomendado estandarizar los nombres de recurso para poder identificar rápidamente su propósito. Los nombres de máquinas virtuales Linux deben tener entre 1 y 64 caracteres, y estar formados por números, letras y guiones. |
| Region | Selección de una ubicación cercana a usted. Vea la información que aparece justo después de esta tabla para consultar las regiones disponibles. |
| Opciones de disponibilidad | Seleccione No se requiere redundancia de la infraestructura. Esta opción se puede usar para garantizar la alta disponibilidad de la máquina virtual al agrupar varias máquinas virtuales en un conjunto para hacer frente a eventos o interrupciones de mantenimiento planeados o no planeados. Para este ejercicio no se necesitará este servicio. |
| Imagen | En la lista desplegable, seleccione Ubuntu Server 18.04 LTS - Gen1 |
| Size | D2s v3. Esta opción le ofrece dos vCPU con 8 GB de RAM. |
| Cuenta de administrador |  |
| Tipo de autenticación | Clave pública SSH. |
| Nombre de usuario | Escriba un nombre que se usará para iniciar sesión con SSH. Anótela. |
| Origen de la clave pública SSH | Use la clave pública existente. |
| Nombre del par de claves | Pegue la clave SSH del archivo de clave pública que se creó en la unidad anterior. Debe ser similar al ejemplo mostrado en la unidad 3, sin espacios en blanco ni avances de línea. |

1. El espacio aislado gratuito permite crear recursos en un subconjunto de las regiones globales de Azure. Seleccione una región de la lista siguiente al crear los recursos:
   * Oeste de EE. UU. 2
   * Centro-sur de EE. UU.
   * Centro de EE. UU.
   * Este de EE. UU.
   * Oeste de Europa
   * Sudeste de Asia
   * Japón Oriental
   * Sur de Brasil
   * Sudeste de Australia
   * Centro de la India
2. Seleccione Siguiente: Discos > para ir a la sección Discos.
3. En la pestaña Discos, escriba los valores siguientes para cada opción.

| **Configuración** | **Value** |
| --- | --- |
| Opciones de disco |  |
| Tipo de disco del sistema operativo | SSD Premium |
| Tipo de cifrado | (Predeterminado) Cifrado en reposo con una clave administrada por la plataforma. |
| Discos de datos | *Recuerde que vamos a obtener un disco del sistema operativo (/dev/sda) y un disco temporal (/dev/sdb). Aquí también agregaremos un disco de datos.* |
| Crear y adjuntar un nuevo disco | Seleccione el vínculo. Aparecerá el panel Crear un disco. Acepte todos los valores de configuración predeterminados. Tenga en cuenta que el tipo de origen es donde puede usar una instantánea o Azure Blob Storage para crear un disco duro virtual. |

1. Seleccione Aceptar para crear el disco. Se volverá a mostrar la sección Discos en el panel Crear una máquina virtual.  
   Aparece un nuevo disco en la primera fila.  
   
2. Seleccione Siguiente: Redes > para ir a la sección Redes.
3. En la pestaña Redes, acepte todos los valores predeterminados para cada configuración.  
   En un entorno de producción en el que ya hay otros componentes, le interesaría usar una red virtual *existente*. De esta forma, la máquina virtual se puede comunicar con el resto de servicios en la nube de la solución. Si todavía no hay ninguna definida en esta ubicación, la puede crear aquí y configurar lo siguiente:
   * Subred: primera subred que subdivide el espacio de direcciones. Debe caber en el espacio de direcciones definido. Una vez que se ha creado la red virtual, se pueden agregar subredes adicionales.
   * Dirección IP pública: espacio total de IPv4 disponible para esta red.
4. De forma predeterminada, Azure crea una red virtual, una interfaz de red y una IP pública para la máquina virtual. No es sencillo cambiar las opciones de red después de haber creado la máquina virtual, así que compruebe siempre las asignaciones de red en los servicios que se crean en Azure. Para este ejercicio, los valores predeterminados deben funcionar bien.  
   El resto de las opciones del asistente tienen valores predeterminados razonables y no es necesario cambiar ninguno. Si quiere, puede explorar las otras pestañas. Las opciones individuales tienen un icono (i) junto a ellas que muestra una sugerencia de ayuda para explicar la opción. Esta es una excelente manera de aprender acerca de las diversas opciones que puede utilizar para configurar la máquina virtual.
5. Para acabar de configurar la máquina virtual y crear la imagen, seleccione Revisar y crear.
6. Una vez que el sistema haya validado las opciones y le proporcione los detalles de la máquina virtual que se está creando, seleccione Crear para crearla e implementarla. El panel de Azure mostrará la máquina virtual que se va a implementar. Este proceso podría tardar varios minutos.

Mientras se implementa, veamos lo que se puede hacer con esta máquina virtual.

# **Opciones SSH y direcciones IP de las máquinas virtuales de Azure**

Completado

100 XP

* 5 minutos

Ha creado una máquina virtual Linux en Azure. Lo siguiente que tiene hacer es configurarla para las tareas que quiera mover a Azure.

A menos que haya configurado una VPN de sitio a sitio en Azure, las máquinas virtuales de Azure no serán accesibles desde la red local. Si está empezando a usar Azure, es poco probable que tenga una VPN de sitio a sitio que funcione. Por tanto, ¿cómo se conecta a la máquina virtual?

## **Direcciones IP de las máquinas virtuales de Azure**

Tal como vimos hace un momento, las máquinas virtuales de Azure se comunican mediante una red virtual. Asimismo, también pueden tener una dirección IP pública opcional asignada. Gracias a una dirección IP pública, puede interactuar con la máquina virtual a través de Internet. Como alternativa, podemos configurar una red privada virtual (VPN) que conecte la red local a Azure, lo que nos permitirá conectarnos de forma segura a la máquina virtual sin tener que exponer una dirección IP pública. Si le interesa explorar esa opción, este enfoque se analiza en otro módulo y está completamente documentado.

De forma predeterminada, en Azure las direcciones IP públicas se asignan dinámicamente. Eso significa que la dirección IP puede cambiar con el tiempo; para las máquinas virtuales, la asignación de direcciones IP se produce cuando se reinicia la máquina virtual. Si quiere conectarse directamente a una dirección IP y necesita asegurarse de que no cambie, puede pagar más para asignar direcciones estáticas.

Asumiendo estas restricciones y las alternativas que se han descrito anteriormente, en este módulo se usará la dirección IP pública de la máquina virtual.

## **Conexión a la máquina virtual con SSH**

Para conectarse a la máquina virtual a través de SSH, necesita los siguientes elementos:

* Dirección IP pública de la máquina virtual
* Nombre de usuario de la cuenta local en la máquina virtual
* Clave pública configurada en esa cuenta
* Acceso a la clave privada correspondiente
* Puerto 22 abierto en la máquina virtual

Anteriormente, ha generado un par de claves SSH, ha agregado la clave pública a la configuración de la máquina virtual y se ha asegurado de que el puerto 22 estaba abierto.

En la siguiente unidad, usará esta información para abrir un terminal seguro en la máquina virtual mediante SSH.

Una vez que el terminal esté abierto, tendrá acceso a todas las herramientas de línea de comandos estándar de Linux.

A continuación, se conectará a la máquina virtual mediante SSH.

# **Ejercicio: Conexión a una máquina virtual Linux mediante SSH**

Completado

100 XP

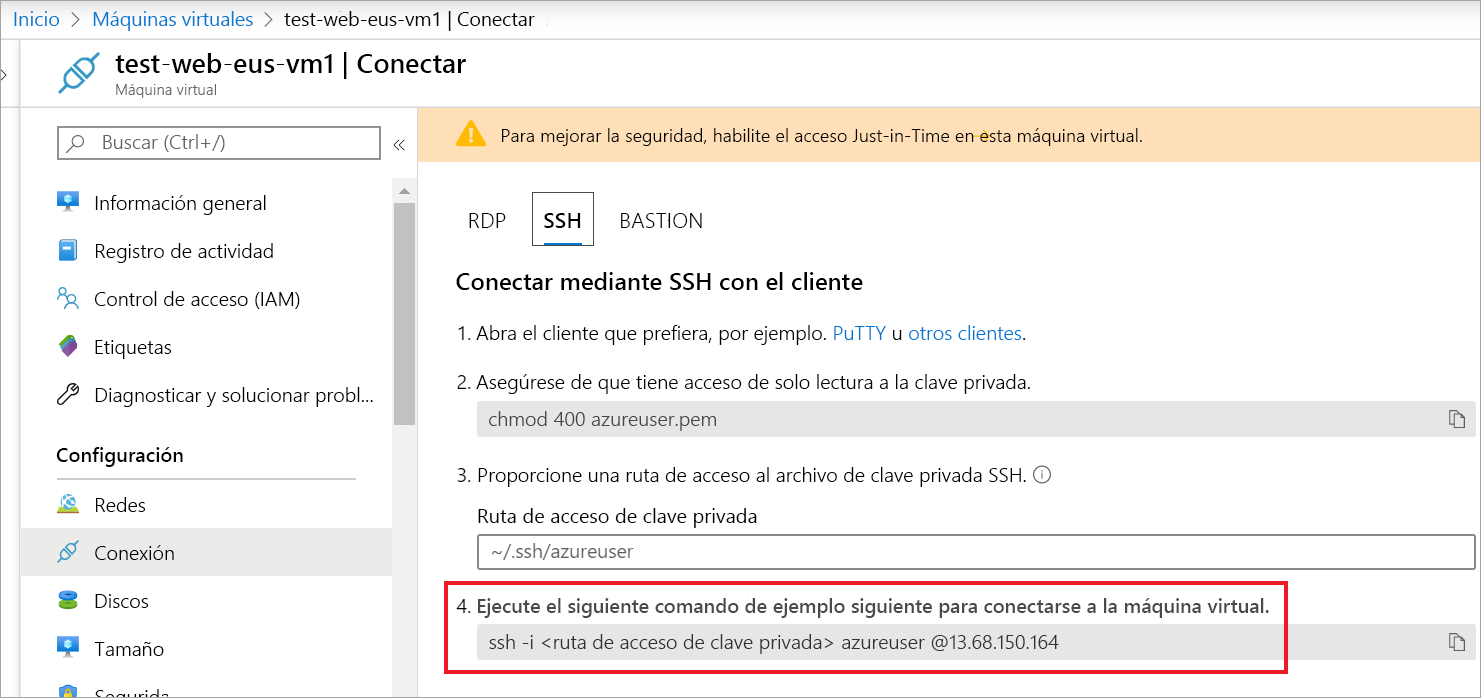
* 15 minutos

Espacio aislado activado. Tiempo restante: 1 h 43 min

Usó 1 de 10 espacios aislados por hoy. Mañana habrá disponibles más espacios aislados.

Nos conectaremos a ella con SSH y configuraremos Apache para tener un servidor web en ejecución.

### **Obtención de la dirección IP pública de la VM**

1. En la cuenta de [Azure Portal](https://portal.azure.com/learn.docs.microsoft.com) del ejercicio anterior, seleccione Ir al recurso. Se mostrará el panel Información general de la máquina virtual que acaba de crear. También puede encontrar la máquina virtual en Todos los recursos si tiene que abrirla. El panel Información general le permite hacer lo siguiente:
   * Ver si la máquina virtual se está ejecutando
   * Detener o reiniciar la máquina virtual
   * Obtención de la dirección IP pública de la VM
   * Ver la actividad de la CPU, el disco y la red
2. Seleccione Conectar > SSH en la parte superior del panel.
3. En el paso 4, copie el comando en el Portapapeles.  
   
4. Hemos usado la ruta de acceso del archivo de clave privada SSH predeterminada cuando hemos creado el par de claves SSH. No es necesario especificar la ruta de acceso de la clave privada en el comando mediante el uso de la marca -i con la ruta de acceso de clave privada. Si ha escrito una ruta de acceso diferente al crear el par de claves SSH, debe agregar esa ruta de acceso al comando.

## **Conexión con SSH**

1. Pegue el comando desde el Portapapeles a Azure Cloud Shell. Elimine la marca -i y el marcador de posición de la ruta de clave privada. Después, ejecute el comando. Debe ser similar al ejemplo siguiente, con una dirección IP y un nombre de usuario diferentes.
2. Bash
3. Copiar

ssh azureuser@13.68.150.164

1. La primera vez que nos conectemos, SSH nos preguntará sobre la autenticación en un host desconocido. SSH le informa de que nunca se ha conectado a este servidor. Si eso es cierto, es perfectamente normal, y puede responder con Sí para guardar la huella digital del servidor en el archivo de host conocido.
2. Resultado
3. Copiar

The authenticity of host '137.117.101.249 (137.117.101.249)' can't be established.

ECDSA key fingerprint is SHA256:w1h08h4ie1iMq7ibIVSQM/PhcXFV7O7EEhjEqhPYMWY.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '137.117.101.249' (ECDSA) to the list of known hosts.

1. Escriba la frase de contraseña que ha usado al crear el par de claves SSH.
2. En el símbolo del sistema del shell de Linux, intente ejecutar algunos comandos de Linux:
   * ls -la /: para mostrar la raíz del disco.
   * ps -l: para mostrar todos los procesos en ejecución.
   * dmesg: para enumerar todos los mensajes de kernel.
   * lsblk para enumerar todos los dispositivos de bloque, donde verá las unidades de disco.
3. El aspecto más interesante a observar en la lista de unidades es lo que *falta*. Observe que la unidad Datos (sdc) está presente, pero no está montada en el sistema de archivos. Azure agregó un disco duro virtual, pero no lo inicializó.

## **Inicialización de discos de datos**

Tendrá que inicializar y dar formato a las unidades adicionales que cree desde cero. El proceso para la inicialización es idéntico al de un disco físico.

1. En primer lugar, identifique el disco que acaba de crear. También se puede usar dmesg | grep SCSI, que mostrará una lista de todos los mensajes del kernel para los dispositivos SCSI.
2. Una vez que sepa la unidad (sdc) que tiene que inicializar, puede usar fdisk para hacerlo. Deberá ejecutar el comando con sudo y especificar el disco que quiera particionar. Puede usar el siguiente comando para crear una partición principal.
3. Bash
4. Copiar

(echo n; echo p; echo 1; echo ; echo ; echo w) | sudo fdisk /dev/sdc

1. Después, hay que escribir un sistema de archivos en la partición con el comando mkfs.
2. Bash
3. Copiar

sudo mkfs -t ext4 /dev/sdc1

1. Por último, es necesario montar la unidad en el sistema de archivos. Supongamos que vamos a tener la carpeta data. Vamos a crear la carpeta de punto de montaje y montar la unidad.
2. Bash
3. Copiar

sudo mkdir /data && sudo mount /dev/sdc1 /data

Inicializamos el disco y lo montamos. Si quiere saber más sobre este proceso, vea el módulo Incorporación de discos en Azure Virtual Machines y selección de tamaño. Esta tarea se trata ahí con más detalle.

## **Instalación de software en la máquina virtual**

Como puede ver, SSH permite trabajar con la máquina virtual Linux como si fuera un equipo local. Puede administrarla igual que cualquier otro equipo Linux: instalar software, configurar roles, ajustar características y otras tareas cotidianas. Vamos a centrarnos en la instalación de software.

También puede instalar software desde Internet cuando se conecta a la máquina virtual a través de SSH. De forma predeterminada, las máquinas de Azure están conectadas a Internet. Puede usar comandos estándar para instalar paquetes de software conocidos directamente desde los repositorios estándar. Vamos a usar este enfoque para instalar Apache.

### **Instalación del servidor web Apache**

Apache está disponible en los repositorios de software predeterminados de Ubuntu, por lo que se instalará mediante herramientas de administración de paquetes convencionales:

1. Empiece por actualizar el índice de paquetes local para reflejar los cambios ascendentes más recientes.
2. Bash
3. Copiar

sudo apt-get update

1. Después, instale Apache.
2. Bash
3. Copiar

sudo apt-get install apache2 -y

1. Se debería iniciar de forma automática; el estado se puede comprobar mediante systemctl.
2. Bash
3. Copiar

sudo systemctl status apache2 --no-pager

1. El comando systemctl devuelve algo parecido a la salida siguiente.
2. Resultado
3. Copiar

apache2.service - The Apache HTTP Server

Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)

Drop-In: /lib/systemd/system/apache2.service.d

└─apache2-systemd.conf

Active: active (running) since Mon 2018-09-03 21:00:03 UTC; 1min 34s ago

Main PID: 11156 (apache2)

Tasks: 55 (limit: 4915)

CGroup: /system.slice/apache2.service

├─11156 /usr/sbin/apache2 -k start

├─11158 /usr/sbin/apache2 -k start

└─11159 /usr/sbin/apache2 -k start

test-web-eus-vm1 systemd[1]: Starting The Apache HTTP Server...

test-web-eus-vm1 apachectl[11129]: AH00558: apache2: Could not reliably determine the server's fully qua

test-web-eus-vm1 systemd[1]: Started The Apache HTTP Server.

1. Por último, podemos intentar recuperar la página predeterminada a través de la IP pública. Pero, aunque el servidor web se ejecute en la máquina virtual, no obtendrá ninguna conexión o respuesta válidas. ¿Sabe por qué?

Es necesario realizar un paso más para poder interactuar con el servidor web. La red virtual está bloqueando la solicitud entrante. Esto se puede cambiar mediante la configuración. A continuación veremos cómo permitir la solicitud de entrada.

# **Configuración de red y seguridad**

Completado

100 XP

* 10 minutos

Los ajustes en la configuración del servidor se realizan normalmente con equipos en el entorno local. En este sentido, puede considerar las máquinas virtuales de Azure como una extensión de ese entorno. Puede modificar la configuración, administrar redes, abrir o bloquear el tráfico y mucho más mediante Azure Portal, la CLI de Azure o las herramientas de Azure PowerShell.

El servidor está en ejecución, y Apache está instalado y sirviendo páginas. Nuestro equipo de seguridad exige que se bloqueen todos los servidores y todavía no hemos hecho nada a esta máquina virtual. No hemos hecho nada y eso permitió que Apache escuchara en el puerto 80. Vamos a examinar la configuración de red de Azure para ver cómo usar la compatibilidad de seguridad integrada para fortalecer el servidor.

## **Apertura de puertos en máquinas virtuales de Azure**

De forma predeterminada, las nuevas máquinas virtuales están bloqueadas.

Las aplicaciones pueden realizar solicitudes salientes, pero el único tráfico entrante permitido es desde la red virtual (por ejemplo, otros recursos en la misma red local) y desde Azure Load Balancer (comprobaciones de sondeo).

Hay dos pasos para ajustar la configuración para que admita otros protocolos en la red. Al crear una nueva VM, tiene la oportunidad de abrir algunos puertos comunes (RDP, HTTP, HTTPS y SSH). Sin embargo, si necesita otros cambios en el firewall, tendrá que hacerlos manualmente.

El proceso implica dos pasos:

* Crear un grupo de seguridad de red.
* Crear una regla de entrada que permita el tráfico con los puertos que se necesitan.

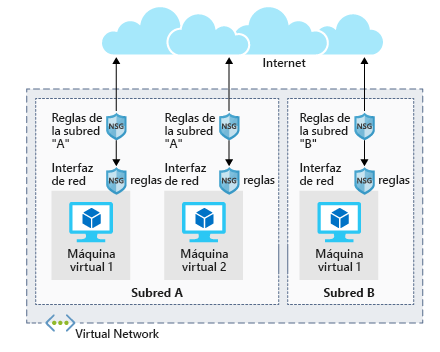
### **¿Qué es un grupo de seguridad de red?**

Las redes virtuales (VNet) constituyen la base del modelo de red de Azure y proporcionan aislamiento y protección. Los grupos de seguridad de red (NSG) son la principal herramienta para aplicar y controlar las reglas de tráfico de red en el nivel de red. Los grupos de seguridad de red son una capa de seguridad opcional que proporciona un firewall de software gracias al filtrado del tráfico entrante y saliente de la red virtual.

Se pueden asociar a una interfaz de red (para reglas por host), una subred de la red virtual (para aplicar a varios recursos) o a ambos niveles.

#### **Reglas del grupo de seguridad**

Los NSG usan *reglas* para permitir o denegar el movimiento del tráfico a través de la red. Cada regla identifica las direcciones de origen y destino (o rangos), el protocolo, el puerto (o rango), la dirección (entrante o saliente), una prioridad numérica y si desea permitir o denegar el tráfico que coincide con la regla.



Cada grupo de seguridad tiene un conjunto de reglas de seguridad predeterminadas para aplicar las reglas de red predeterminadas descritas anteriormente. Estas reglas predeterminadas no se pueden modificar, pero se *pueden* reemplazar.

#### **Uso de las reglas de red por parte de Azure**

Para el tráfico entrante, Azure procesa el grupo de seguridad asociado a la subred y, a continuación, el grupo de seguridad que se aplica a la interfaz de red. El tráfico saliente se controla en orden inverso (la interfaz de red en primer lugar, seguida de la subred).

Advertencia

Tenga en cuenta que los grupos de seguridad son opcionales en ambos niveles. Si no hay ningún grupo de seguridad aplicado, Azure permite todo el tráfico. Si la máquina virtual tiene una dirección IP pública, esto podría plantear un riesgo grave, especialmente si el sistema operativo no proporciona un firewall integrado.

Las reglas se evalúan en *orden de prioridad*, comenzando por la regla de prioridad más baja. Las reglas de denegación siempre detienen la evaluación. Por ejemplo, si una regla de la interfaz de red bloquea una solicitud saliente, no se comprobarán las reglas aplicadas a la subred. Para permitir el tráfico a través del grupo de seguridad, debe pasar por *todos* los grupos aplicados.

La última regla es siempre una regla de Denegar todo. Se trata de una regla predeterminada que se agrega a todos los grupos de seguridad para el tráfico entrante y saliente con una prioridad de 65500. Esto significa que, para que el tráfico pase por el grupo de seguridad, *debe tener una regla de permiso* o la regla final predeterminada lo bloqueará.

Nota

SMTP (puerto 25) es un caso especial. Según el nivel de suscripción y la fecha de creación de la cuenta, es posible que bloquee el tráfico SMTP saliente. Puede solicitar quitar esta restricción por justificación comercial.

## **Creación de grupos de seguridad de red**

Los grupos de seguridad son recursos administrados, como casi todo en Azure. Puede crearlos en Azure Portal o mediante las herramientas de scripting de línea de comandos. El desafío consiste en definir las reglas. Veamos la definición de una nueva regla para permitir el acceso HTTP y bloquear todo lo demás.

# **Ejercicio: Configuración de la red**

Completado

100 XP

* 10 minutos

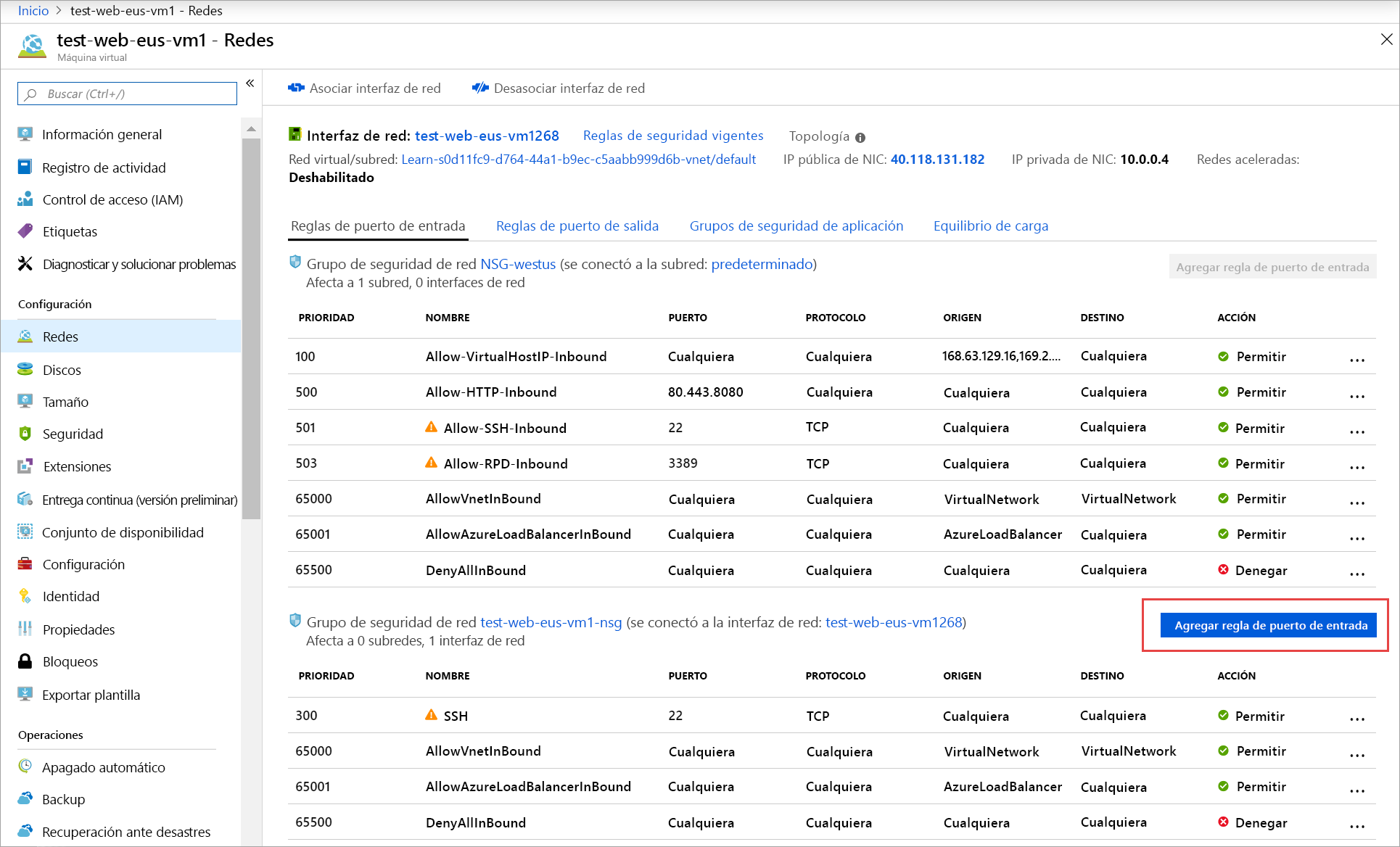
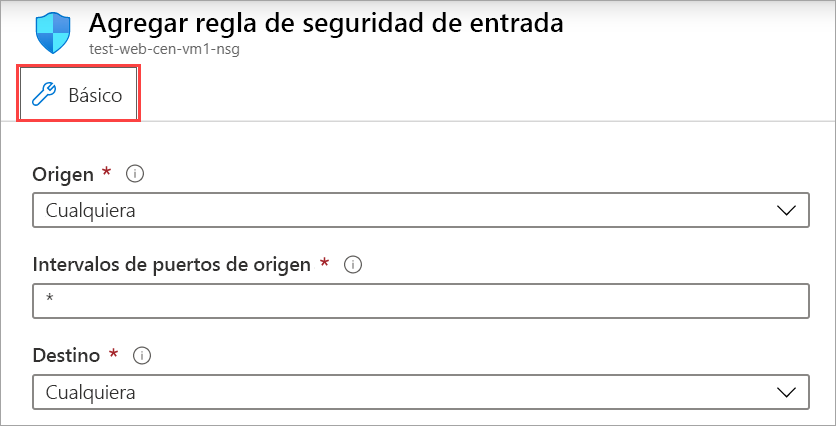
Espacio aislado activado. Tiempo restante: 1 h 37 min

Usó 1 de 10 espacios aislados por hoy. Mañana habrá disponibles más espacios aislados.

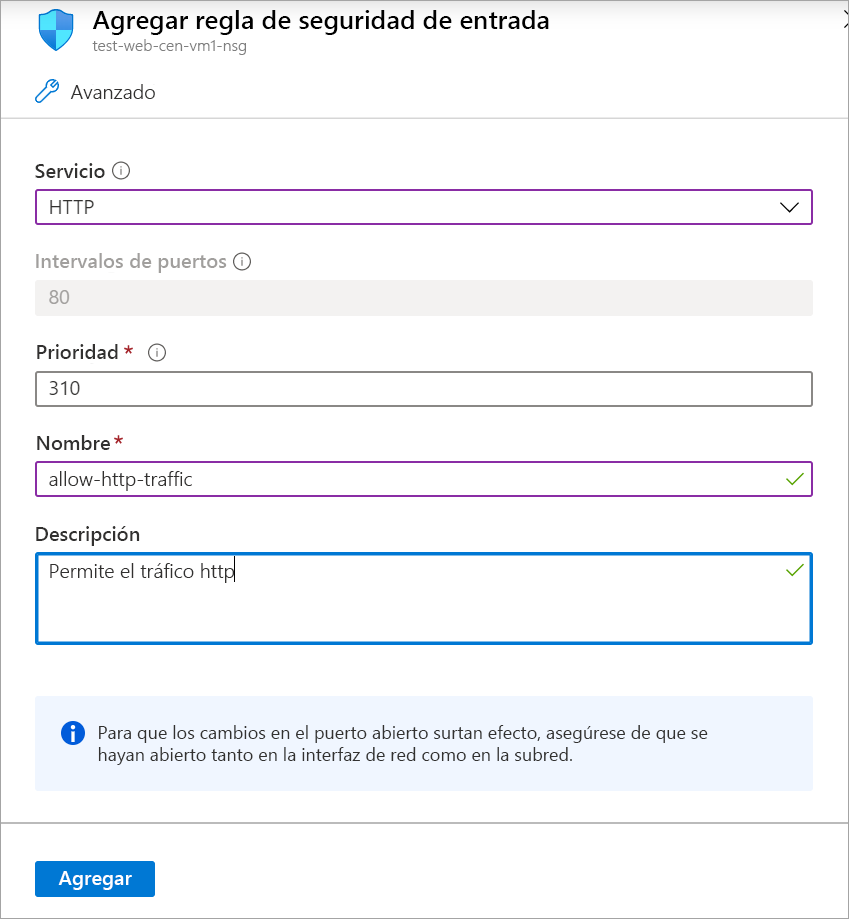
Cuando creamos la máquina virtual, seleccionamos el puerto de entrada *SSH* para poder conectarnos a la máquina virtual. Esto ha creado un grupo de seguridad de red que está adjuntado a la interfaz de red de la máquina virtual. Ese grupo de seguridad de red está bloqueando el tráfico HTTP. Vamos a actualizar este grupo de seguridad de red para permitir el tráfico HTTP entrante en el puerto 80.

## **Actualización del grupo de seguridad de red en la interfaz de red**

El puerto 80 está abierto en el grupo de seguridad de red que se aplica a la subred. Sin embargo, el puerto 80 está bloqueado por el grupo de seguridad de red que se aplica a la interfaz de red. Vamos a solucionarlo para que podamos conectarnos al sitio web.

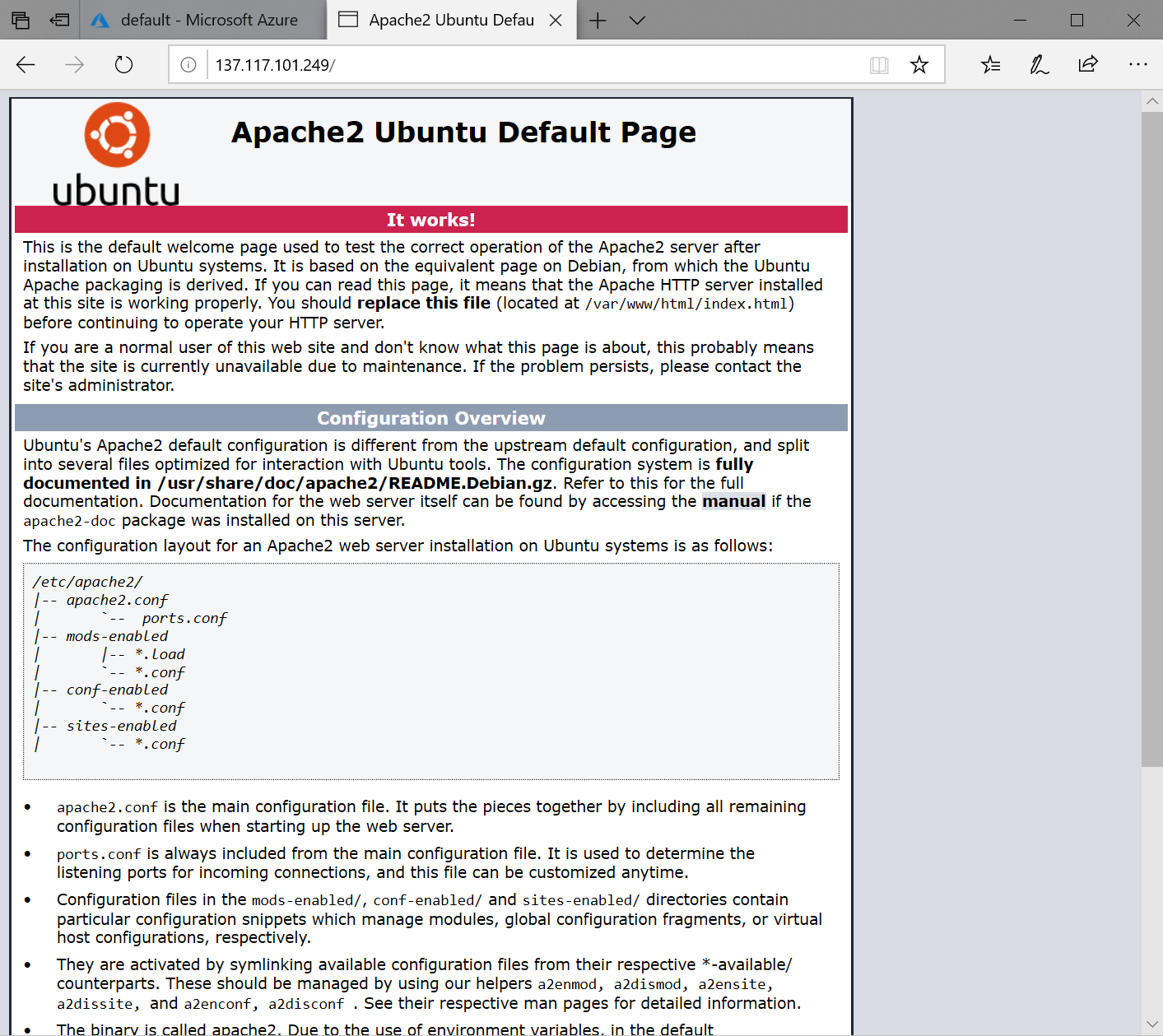
1. Vuelva al panel Información general de la máquina virtual. Puede encontrar la máquina virtual en Todos los recursos.
2. En el panel del menú de la izquierda, en Configuración, seleccione Redes.
3. Verá las reglas de grupo de seguridad de red de la subred en la sección superior y las reglas del grupo de seguridad de red de la interfaz de red en la sección inferior de la misma pestaña. En la sección inferior, en las reglas del grupo de seguridad de red de la interfaz de red, seleccione Agregar regla de puerto de entrada.  
     
   Aparece el panel Agregar regla de seguridad de entrada.  
   
4. Escriba los valores siguientes para la regla HTTP.

| **Configuración** | **Valor** |
| --- | --- |
| Servicio | HTTP |
| Prioridad | 310 |
| Nombre | allow-http-traffic |
| Descripción | Permite el tráfico http |

1. 
2. Para crear la regla, seleccione Agregar. Volverá a mostrarse el panel Redes de la máquina virtual.

## **Apertura de la página web predeterminada**

Para realizar una solicitud HTTP, copie y pegue la dirección IP pública de NIC del servidor en un navegador y presione Entrar. Ahora debería funcionar.



## **Una última consideración**

Asegúrese siempre de bloquear los puertos usados para el acceso administrativo. Un enfoque aún mejor consiste en crear una VPN para vincular la red virtual a la red privada y permitir solo las solicitudes RDP o SSH desde ese rango de direcciones. También puede cambiar el puerto usado por SSH a otro valor distinto del predeterminado. Tenga en cuenta que cambiar los puertos no es suficiente para detener los ataques. Simplemente dificulta un poco la detección.