



Despliegue de aplicaciones web

Procedimientos habituales en Azure

CONTENIDO

1.- Introducción.....	2
2.- Cambio de contraseña de máquinas virtuales.....	2
3.- Establecimiento de IP fija en la red interna usando Azure Portal	3
5.- Acceso a la consola serie de las máquinas.....	4
5.1.- La consola serie en máquinas Linux.....	4
5.2.- La consola serie en máquinas Windows Server	4
7.- Dar permisos a otros usuarios a nuestra suscripción	6

1.- Introducción

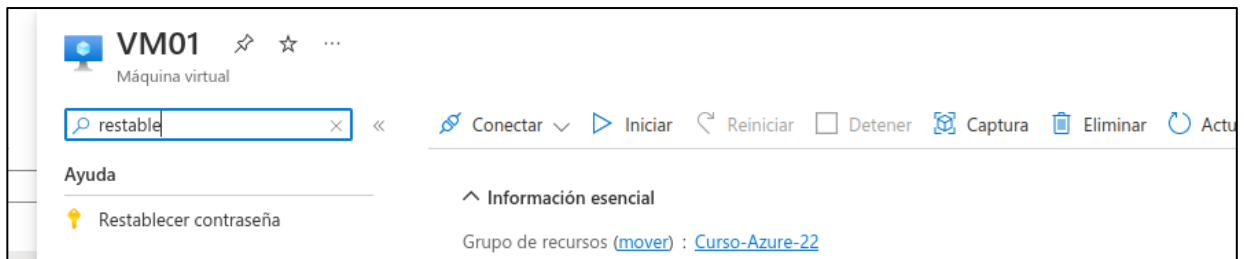
Este documento intenta describir algunos de los procedimientos que se realizan habitualmente con máquinas o redes virtuales en Azure.

2.- Cambio de contraseña de máquinas virtuales


Al crear máquinas virtuales una de las cosas que se suele hacer es establecer un nombre de usuario y una contraseña. Con estos datos, se crea un usuario local en la máquina que estemos creando. Este usuario local será un usuario sudoer en el caso de Linux y un administrador local en el caso de máquinas Windows.

Si olvidamos la contraseña que habíamos asignado al usuario administrador de una máquina, podemos establecerla desde el portal de Azure. Para ello:

- Abrimos el listado de máquinas virtuales, y hacemos clic en el nombre de la máquina virtual para la que necesitamos cambiar contraseña.
- En el menú de la máquina buscaremos y haremos clic en la opción “Restablecer contraseña”



- Aparecerá el formulario para cambiar la contraseña. Si la máquina en cuestión está apagada, Azure informará de que es necesario que la máquina esté arrancada para poder cambiar la contraseña.

 La máquina virtual debe estar ejecutándose para utilizar VMAccess.

Usa la extensión VMAccessForLinux para restablecer las credenciales de un usuario existente o crear un usuario con privilegios sudo y restablecer la configuración de SSH. [Más información](#)

Modo ⓘ

☒ Restablecer la contraseña

☐ Restablecer la clave pública SSH

☐ Restablecer solo la configuración

Nombre de usuario ⓘ

Contraseña

Confirmar contraseña

- Introducir el nombre de usuario y la nueva contraseña por duplicado
- Hacer clic en “Actualizar” para completar el cambio de contraseña

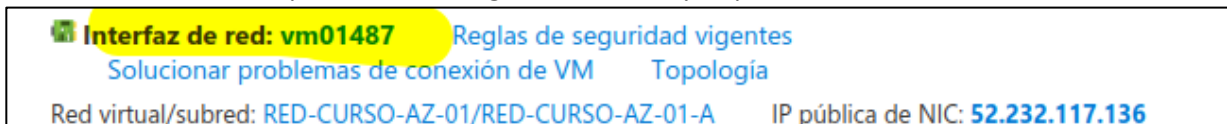
3.- Establecimiento de IP fija en la red interna usando Azure Portal

Normalmente, cuando configuramos un laboratorio para realizar actividades, decidimos asignar a ciertas máquinas una IP específica de nuestro rango de direcciones, porque van a ser servidores con una labor específica. Por ejemplo, un servidor DNS o un servidor FTP.

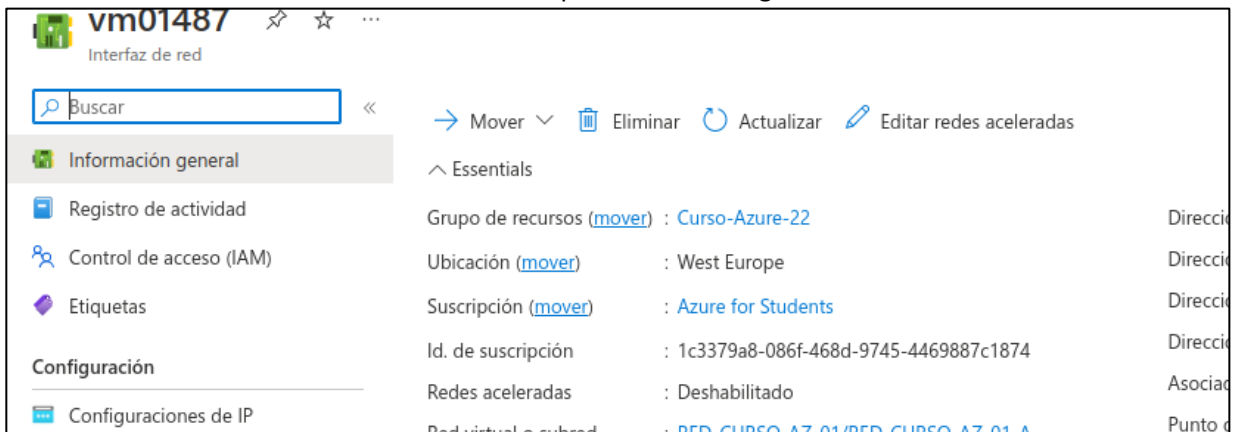
Esto, en el contexto de la virtualización en VirtualBox o VMWare, se hace normalmente en la propia configuración de red de las máquinas, cambiando la configuración de IP dinámica de DHCP a una IP fija.

En Azure, para establecer una IP fija se puede usar una funcionalidad integrada en el propio portal de Azure.

- Acceder a la página inicial de la máquina virtual.
- Hacer clic en “Redes”. Aparecerá la configuración de red y se podrá ver la interfaz de red:



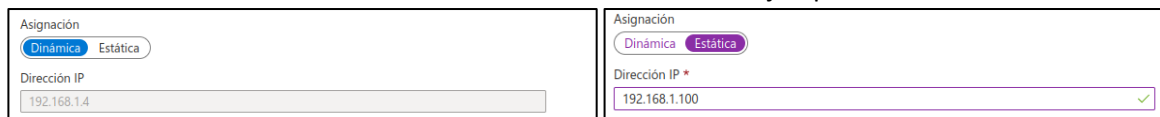
- Hacer clic en el nombre de la interfaz de red. Aparecerá la configuración de la interfaz



- Hacer clic en “Configuraciones de IP”. Aparecerá la configuración IP de la tarjeta. Se puede observar que la IP privada asignada a la tarjeta de red es dinámica. En este caso la 192.168.1.4.



- Hacer clic en la configuración, y aparecerá el formulario para poder cambiar la IP dinámica por una estática. Cambiar a estática e introducir la IP deseada. En nuestro ejemplo la .100



- Clic en guardar. Azure reiniciará la máquina (si está iniciada) para aplicar el cambio de IP.

Si miramos la configuración de la máquina (netplan o networkmanager en Linux o la configuración IP en Windows) veremos que sigue teniendo una IP dinámica. Lo que está pasando en realidad es que Azure está realizando una reserva de IP en el DHCP para esa máquina.

5.- Acceso a la consola serie de las máquinas

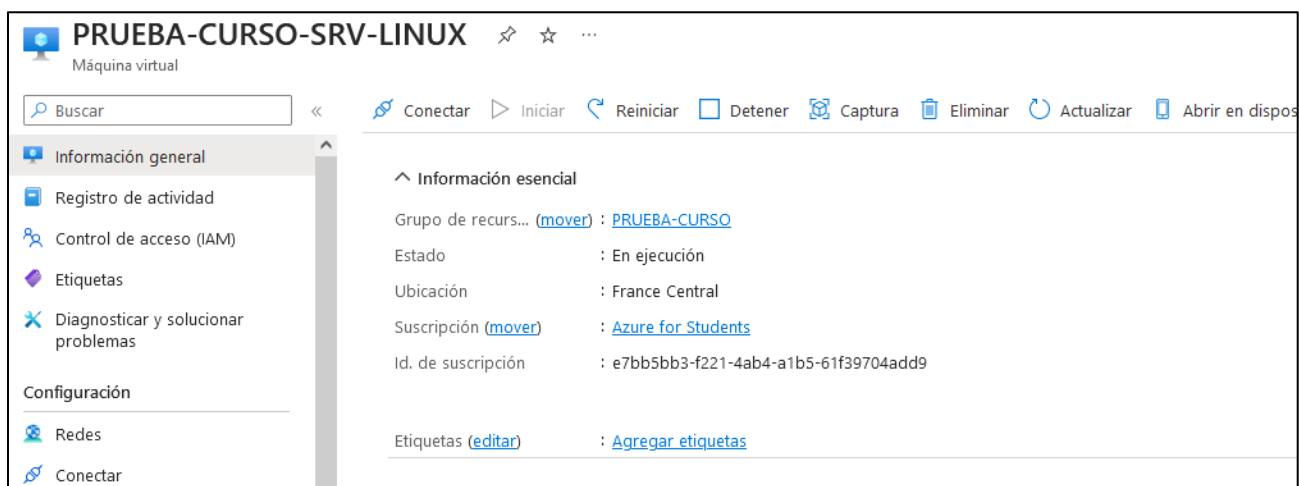
Puede que no tengamos acceso desde el exterior de la red virtual, por SSH o RDP, a una máquina virtual dentro de la red virtual. Bien porque hemos decidido que no necesitan acceso y es más seguro que estén aisladas, bien porque tenemos algún problema en la configuración de la red.

En este caso tenemos tres opciones para acceder a la máquina:

- Acceder a otra máquina en la red virtual, a la que sí podamos acceder, y desde esta “saltar” a la máquina que está fuera de nuestro alcance.
- Montar una VPN para conectar a la red virtual.
- Usar la consola serie de la máquina, que nos permite conectarnos como si estuviéramos conectados físicamente a la máquina.

Vamos a ver como conectar a la consola serie tanto en máquinas virtuales Linux como Windows.

Para abrir la consola serie tenemos que acceder a la página de la máquina virtual:



En el menú lateral, dentro del grupo “Ayuda” encontraremos la opción “Consola serie”. Haciendo clic en esta opción podremos conectar a la máquina. El comportamiento de esta consola serie es algo diferente en máquinas Linux y Windows.

5.1.- La consola serie en máquinas Linux

En máquinas Linux, al hacer clic en la opción “Consola serie” se accede directamente a la consola. En esta podemos logarnos con un usuario y configurar la máquina o reiniciarla si fuera necesario. Al conectar a la consola veremos todos los mensajes de log que el inicio del sistema haya dejado, y si reiniciamos veremos todo el proceso de reinicio, no como en SSH, que al cortar la comunicación se desconecta, como es lógico.

5.2.- La consola serie en máquinas Windows Server

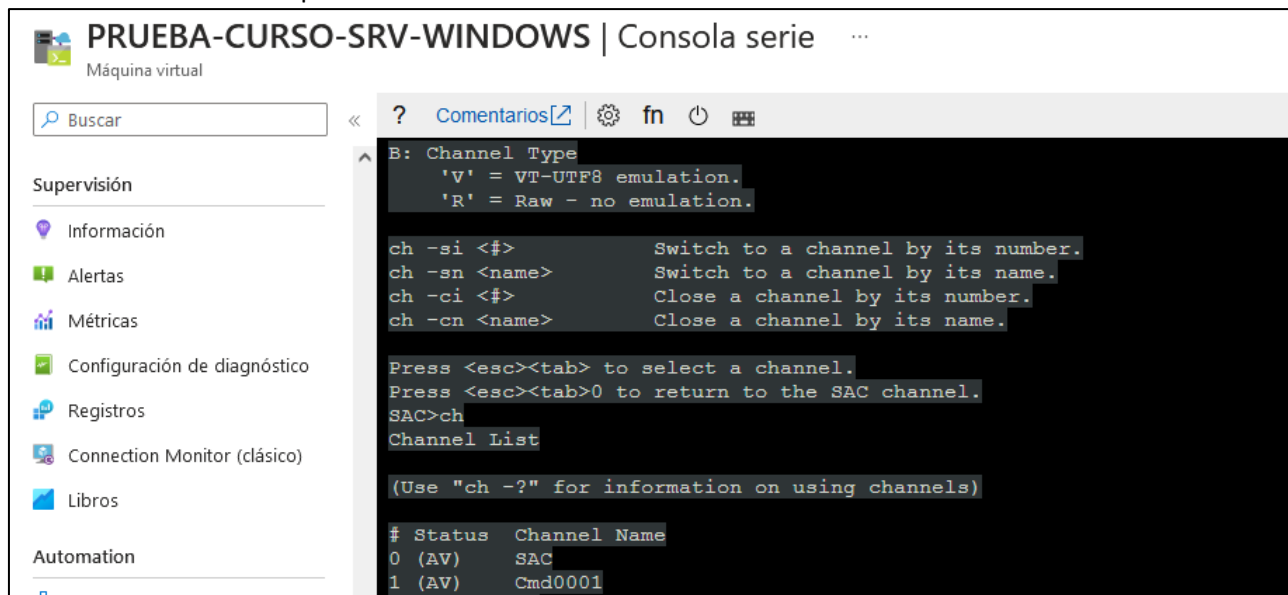
Si el objetivo es abrir una línea de comandos (CMD) en la máquina Windows Server, hay que hacer algunos pasos previos.

Al hacer clic en la consola, aparecerá una consola especial denominada SAC (Special Administration Console). Esta consola especial está disponible en las máquinas Windows creadas desde febrero de 2018.

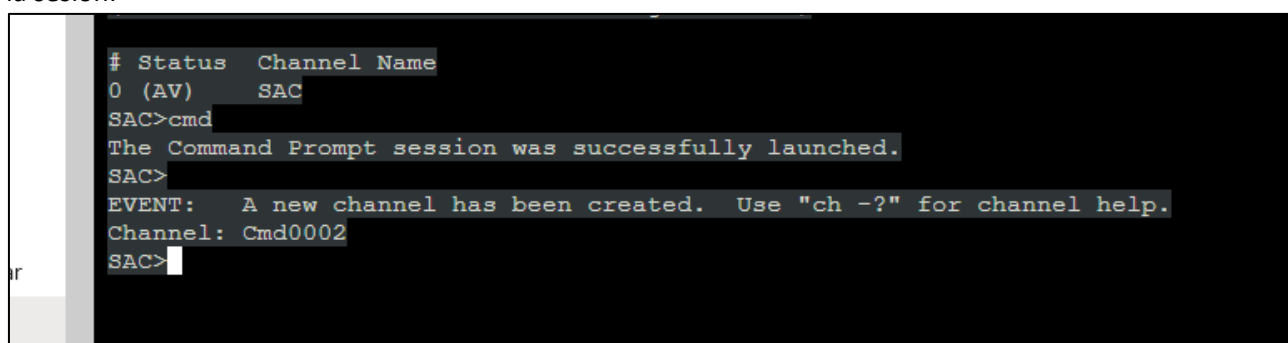
SAC permite abrir múltiples conexiones con la máquina para ejecutar comandos como CMD o PowerShell. Cada instancia de un comando en ejecución se denomina canal o channel.

Para ejecutar un comando CMD y así poder ejecutar otros comandos como si estuviésemos conectados a la máquina, hay que seguir los siguientes pasos:

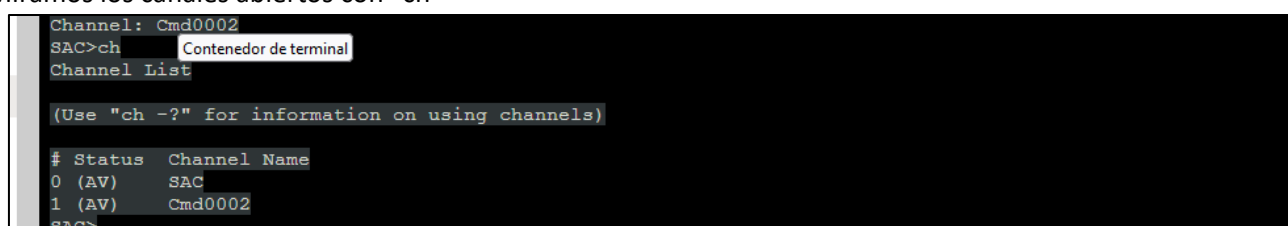
- Clic en “Serial console” aparecerá la ventana de la SAC:



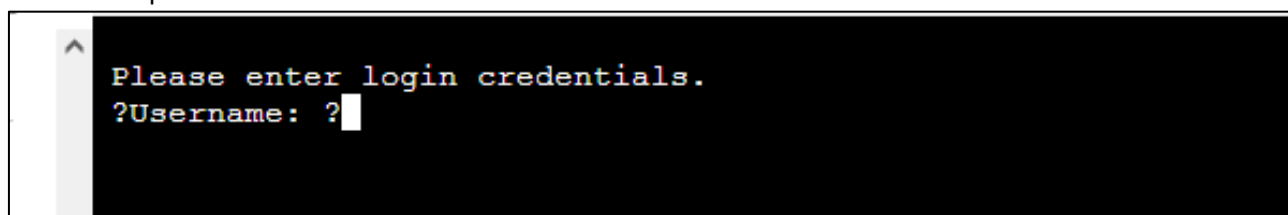
- Ejecutamos el comando CMD, esto abre una nueva sesión del comando y un canal para comunicarse con la sesión:



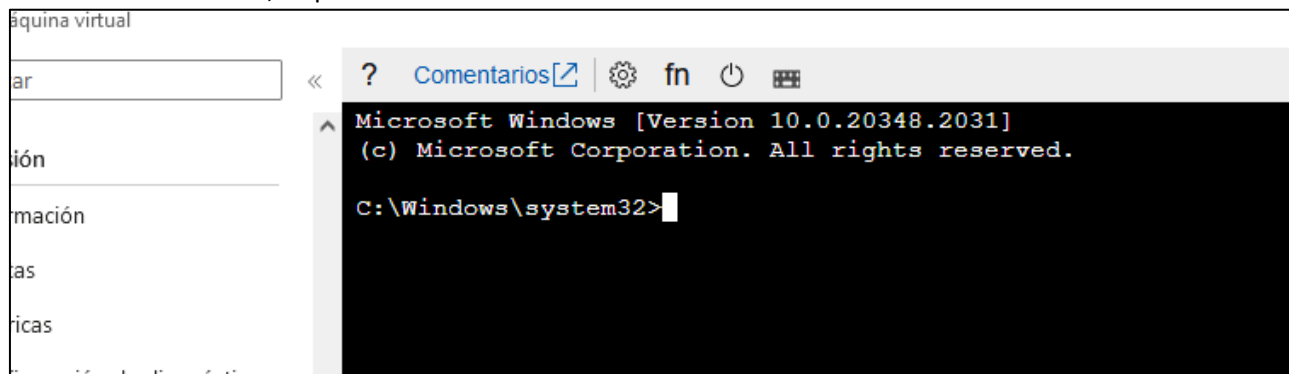
- Miramos los canales abiertos con “ch”



- Y podemos conectar con el canal con “ch -si 1”. 1 es el número del canal asociado a CMD. Una vez abierta la conexión pide credenciales:



- Y cuando se introducen, se podrá utilizar el CMD:



- Para salir del cmd, se podrá hacer un exit igual que en caso de máquinas y sistemas operativos locales.

7.- Dar permisos a otros usuarios a nuestra suscripción

Azure utiliza un sistema de permisos y roles denominado RBAC (Role Based Access Control).

Para una visión general del sistema RBAC consultar <https://learn.microsoft.com/es-es/azure/role-based-access-control/overview>

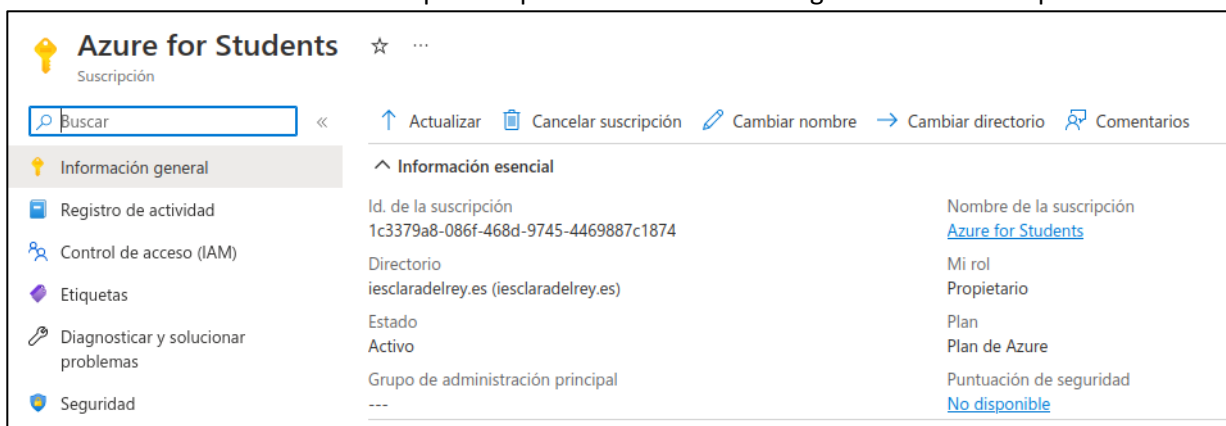
Vamos a ver cómo dar permisos a otro usuario como colaborador en nuestra suscripción de Azure.

El rol de colaborador permite gestionar todos los recursos de la suscripción, salvo la asignación de roles y algunos otros aspectos de seguridad / facturación.

- Acceder, a través del menú principal, del buscador general, o de algún enlace de la página inicial, a la página de suscripciones.



- Hacer clic en el nombre de la suscripción. Aparecerá la información general de la suscripción.



- Hacer clic en el enlace “Control de acceso (IAM)”

- Clic en “Asignación de roles” y de nuevo clic en “Agregar”. Se abrirán tres opciones, y elegimos “Agregar asignación de roles”

- Se abrirá un formulario con tres pestañas: “Rol”, “Miembros” y “Revisión y asignación”. En la pestaña “Roles” podemos elegir entre “Roles de función de trabajo” y “Roles de administrador con privilegios”. Elegimos estos últimos, y buscamos el rol “Colaborador”, hacemos clic en él y hacemos clic en “Siguiente”, con lo que pasamos a la pestaña “Miembros”.

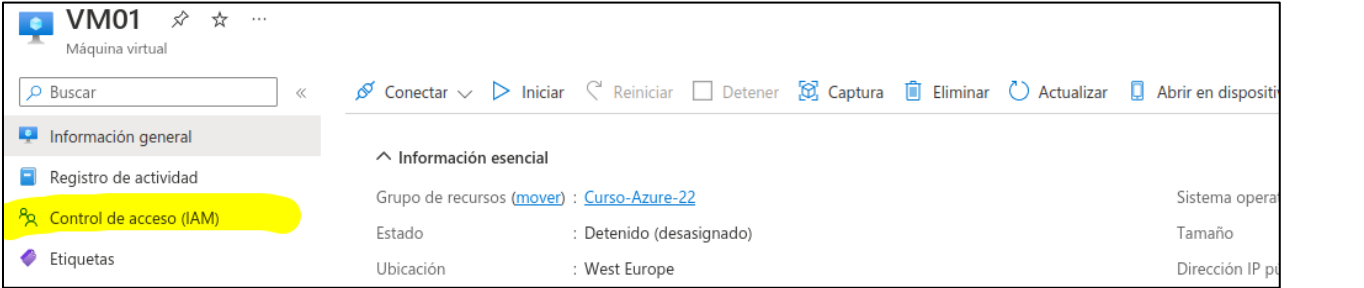
Nombre ↑↓	Descripción ↑↓	Tipo ↑↓	Categoría ↑↓	Detalles
Propietario	Permite conceder acceso total para admi...	BuiltInRole	General	Vista
Colaborador	Concede acceso total para administrar to...	BuiltInRole	General	Vista

- En la pestaña “Miembros”, elegimos la opción “Usuario, grupo o entidad de servicio” en “Asignar acceso a”, y hacemos clic en “Seleccionar miembros”. Se abre un listado de los miembros y roles del AD. Podemos elegir a uno o varios de ellos y pulsar “Seleccionar”.

- Clic en “Siguiente” y por último clic en “Revisar y asignar”.

A partir de ese momento los usuarios a los que se han concedido permisos podrán acceder a la suscripción y gestionarla.

Esta asignación de permisos se puede hacer no sólo al nivel global de suscripción, sino también a nivel de recurso específico. Por ejemplo, en máquinas virtuales:



Y se puede hacer mucho más granular usando los roles de función de trabajo, que conceden permisos a una escala mucho menor.