¿Qué es Azure RBAC?

En lo que respecta a la identidad y al acceso, la mayoría de las organizaciones que están pensando en usar la nube pública se preocupan de dos cosas:

1. Garantizar que cuando los usuarios dejan la organización, pierden el acceso a los recursos en la nube.
2. Conseguir el equilibrio adecuado entre la autonomía y el gobierno central, por ejemplo, para que los equipos de proyecto puedan crear y administrar máquinas virtuales en la nube al mismo tiempo que se controlan de forma centralizada las redes que usan esas máquinas virtuales para comunicarse con otros recursos.

Azure Active Directory (Azure AD) y el control de acceso basado en rol de Azure (Azure RBAC) trabajan juntos para facilitar la consecución de estos objetivos.

Suscripciones de Azure

En primer lugar, recuerde que cada suscripción de Azure está asociada a un único directorio de Azure AD. Los usuarios, grupos y aplicaciones de ese directorio pueden administrar los recursos en la suscripción de Azure. Las suscripciones usan Azure AD para el inicio de sesión único (SSO) y para la administración de acceso. Puede extender su instancia de Active Directory local a la nube con **Azure AD Connect**. Esta característica permite a los empleados administrar sus suscripciones de Azure mediante el uso de sus identidades de trabajo existentes. Cuando se deshabilita una cuenta de Active Directory local, se pierde automáticamente el acceso a todas las suscripciones de Azure conectadas con Azure AD.

¿Qué es Azure RBAC?

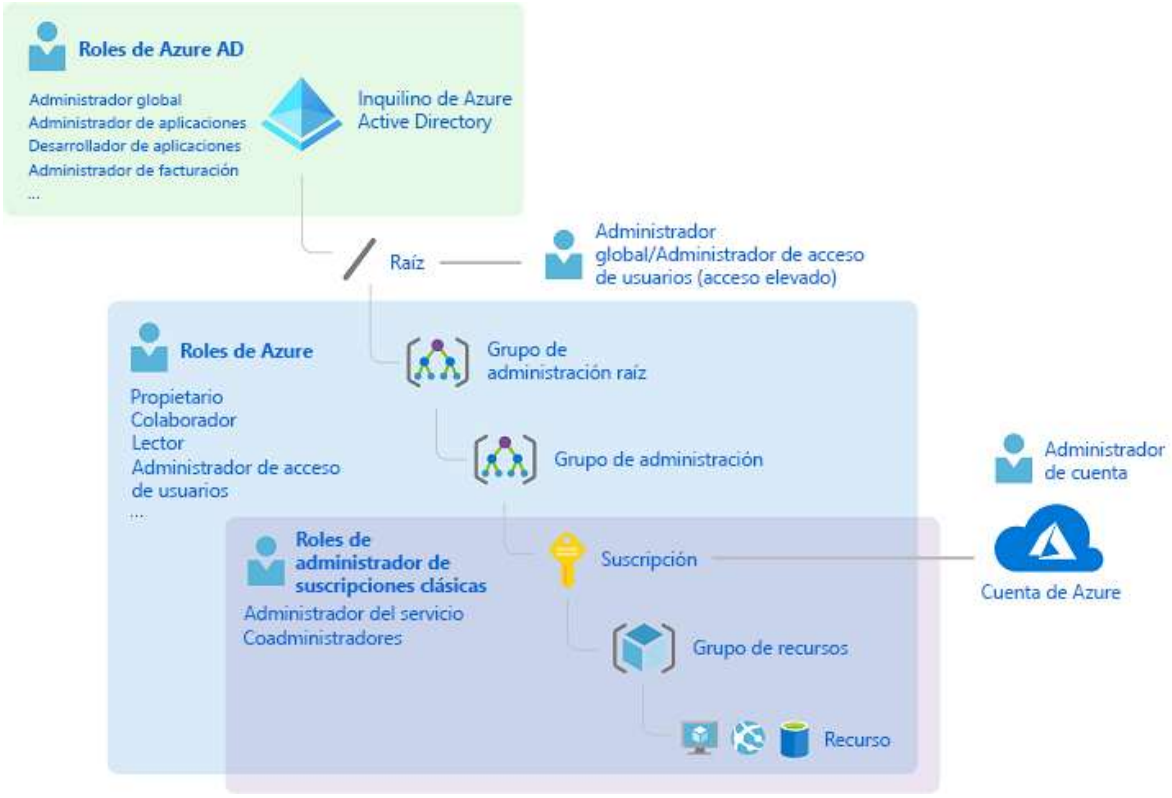
El control de acceso basado en rol de Azure (Azure RBAC) es un sistema de autorización integrado en Azure Resource Manager que proporciona administración de acceso específico a los recursos de Azure. Con Azure RBAC, puede conceder el acceso que los usuarios necesitan para realizar sus trabajos. Por ejemplo, puede usar Azure RBAC para dejar que un empleado administre máquinas virtuales en una suscripción y que otro pueda administrar bases de datos SQL desde la misma suscripción.

¿Qué es el control de acceso basado en rol de Azure?

Puede conceder acceso al asignar el rol de Azure adecuado a usuarios, grupos y aplicaciones de un determinado ámbito. El ámbito de una asignación de roles puede ser un grupo de administración, una suscripción, un grupo de recursos o un único recurso. Un rol asignado en un ámbito principal también concede acceso a los ámbitos secundarios dentro del mismo. Por ejemplo, un usuario con acceso a un grupo de recursos puede administrar todos los recursos que contiene, como sitios web, máquinas virtuales y subredes. El rol de Azure que se asigna determina qué recursos puede administrar el usuario, el grupo o la aplicación dentro de ese ámbito.

En el siguiente diagrama se muestra una visión general de cómo se relacionan los roles de administrador de suscripciones clásicas, los roles de Azure y los roles de Azure AD. Los ámbitos

secundarios, como las instancias de servicio, heredan los roles asignados en un ámbito superior, como una suscripción completa.



En el diagrama anterior, una suscripción está asociada a un solo inquilino de Azure AD. Tenga en cuenta también que un grupo de recursos puede tener varios recursos, pero está asociado a una única suscripción. Aunque no es fácil deducirlo a partir del diagrama, un recurso se puede enlazar a un solo grupo de recursos.

¿Qué puedo hacer con Azure RBAC?

Azure RBAC le permite conceder acceso a los recursos de Azure que controla. Suponga que necesita administrar el acceso a los recursos en Azure para los equipos de desarrollo, ingeniería y marketing. Ha empezado a recibir solicitudes de acceso y necesita saber rápidamente cómo funciona la administración de acceso para los recursos en Azure.

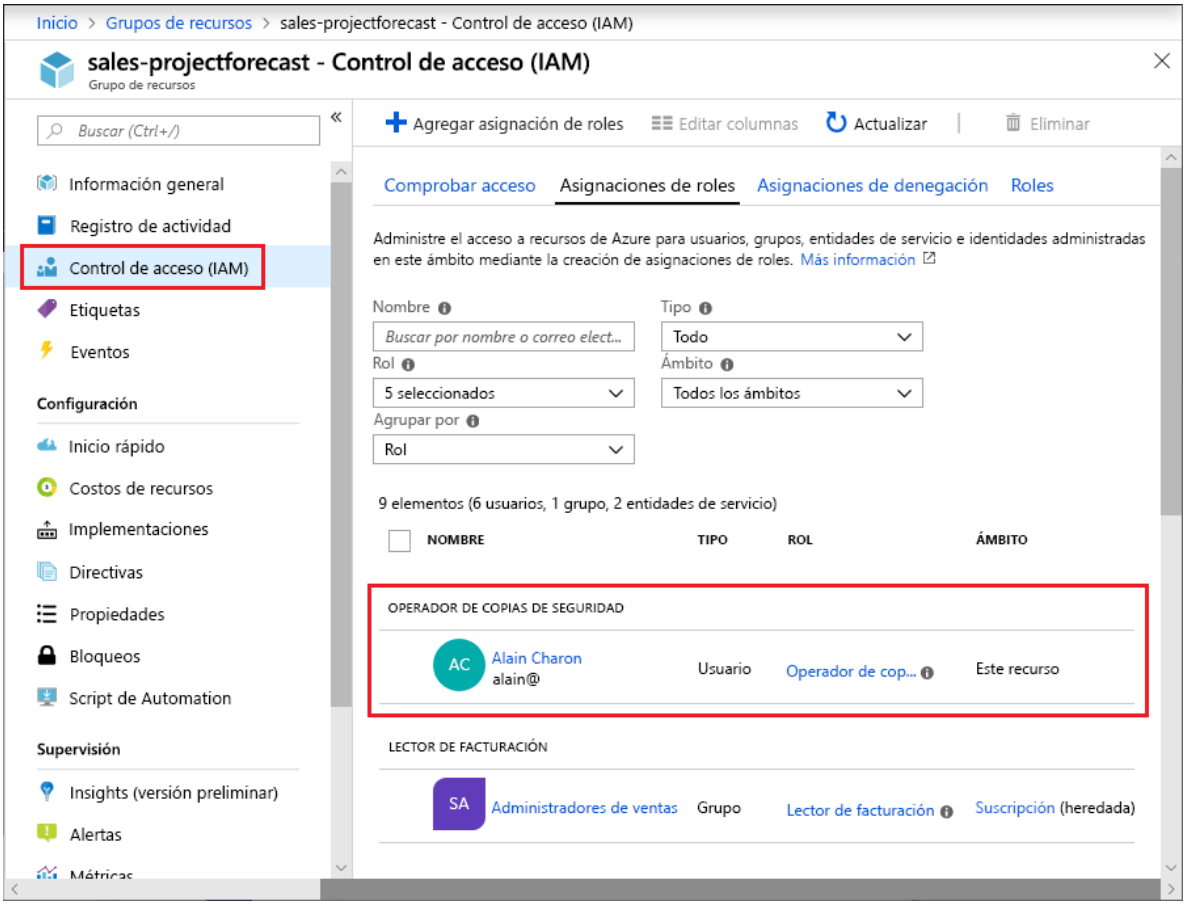
Estos son algunos de los escenarios que puede implementar con Azure RBAC.

- Permitir que un usuario administre las máquinas virtuales de una suscripción y que otro usuario administre las redes virtuales
- Permiso a un grupo de administradores de base de datos para administrar bases de datos SQL en una suscripción
- Permitir que un usuario administre todos los recursos de un grupo de recursos, como las máquinas virtuales, los sitios web y las subredes
- Permitir que una aplicación acceda a todos los recursos de un grupo de recursos

Azure RBAC en Azure Portal

En varias áreas de Azure Portal, verá un panel denominado **Control de acceso (IAM)**, también conocido como *administración de identidad y acceso*. En este panel puede ver quién tiene acceso a dicha área y su rol. Con este mismo panel, puede conceder o quitar el acceso.

A continuación se muestra un ejemplo del panel Control de acceso (IAM) para un grupo de recursos. En este ejemplo, a Alain Charon se le ha asignado el rol de operador de copia de seguridad para este grupo de recursos.



¿Cómo funciona Azure RBAC?

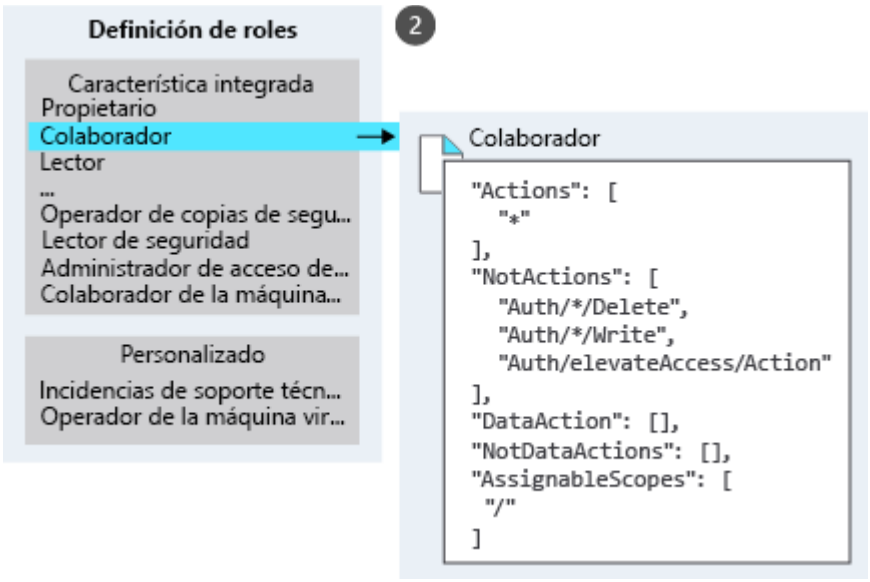
Puede controlar el acceso a los recursos mediante Azure RBAC mediante la creación de asignaciones de roles, que controlan cómo se aplican los permisos. Para crear una asignación de roles, se necesitan tres elementos: una entidad de seguridad, una definición de roles y un ámbito. Puede pensar en estos elementos como "quién", "qué" y "dónde".

1. Entidad de seguridad (quién)

Una *entidad de seguridad* es simplemente un nombre extravagante para un usuario, un grupo o una aplicación a los que quiere conceder acceso.

2. Definición de roles (lo que puede hacer)

Una *definición de roles* es una recopilación de permisos. A veces, se denomina rol simplemente. Una definición de roles enumera los permisos que se pueden realizar, por ejemplo, de lectura, escritura y eliminación. Los roles pueden ser generales, como Propietario, o bien específicos, como Colaborador de máquina virtual.



Azure incluye varios roles integrados que puede usar. Aquí se enumeran cuatros roles integrados fundamentales:

- **Propietario**: tiene acceso total a todos los recursos, incluido el derecho a delegar este acceso a otros.
- **Colaborador**: puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
- **Lector**: puede ver los recursos existentes de Azure.
- **Administrador de acceso de usuario**: permite administrar el acceso de los usuarios a los recursos de Azure.

Si los roles integrados no cumplen las necesidades específicas de su organización, puede crear sus propios roles personalizados.

3. Ámbito (dónde)

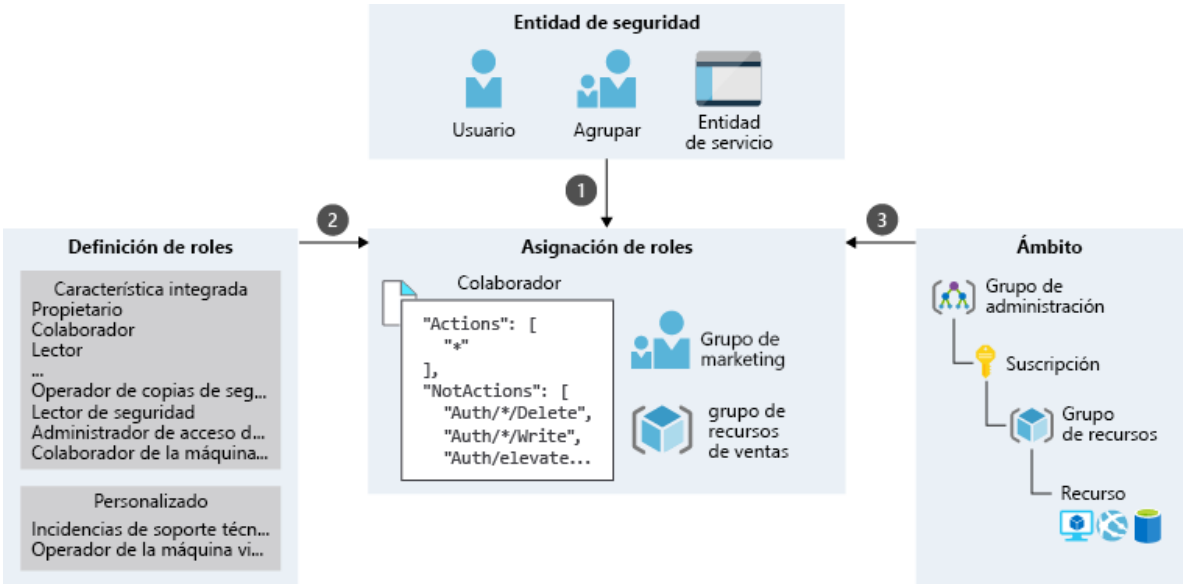
El *ámbito* es donde se aplica el acceso. Esto resulta útil si desea convertir a alguien en colaborador del sitio web, pero solo para un grupo de recursos.

En Azure, puede especificar un ámbito en varios niveles: grupo de administración, suscripción, grupo de recursos o recurso. Los ámbitos se estructuran en una relación de elementos primarios y secundarios. Si otorga acceso a un ámbito primario, esos permisos se heredan en los ámbitos secundarios. Por ejemplo, si asigna el rol Colaborador a un grupo en el ámbito de la suscripción, todos los grupos de recursos y recursos de la suscripción heredarán dicho rol.

Asignación de roles

Cuando haya determinado el quién, qué y dónde, puede combinar estos elementos para conceder acceso. Una *asignación de roles* es el proceso de enlazar un rol a una entidad de servicio en un ámbito determinado con el fin de conceder acceso. Para conceder acceso, creará una asignación de roles. Para revocar el acceso, quitará una asignación de roles,

En el ejemplo siguiente se muestra cómo al grupo de marketing se le asignó el rol Colaborador en el ámbito del grupo de recursos de ventas.



Azure RBAC es un modelo de permiso

Azure RBAC es un modelo de permiso. lo que significa que, cuando se le asigna un rol, Azure RBAC le permite realizar determinadas acciones, como leer, escribir o eliminar. Por tanto, si una asignación de roles concede permisos de lectura a un grupo de recursos y otra asignación de roles concede permisos de escritura al mismo grupo de recursos, tendrá permisos de lectura y escritura en ese grupo de recursos.

Azure RBAC dispone de lo que se conoce como permisos NotActions. Puede usar NotActions para crear un conjunto de permisos no permitidos. El acceso concedido por un rol, los permisos efectivos, se calcula restando las operaciones NotActions de las Actions. Por ejemplo, el rol Colaborador tiene tanto Actions como NotActions. El carácter comodín (*) de Actions indica que puede realizar todas las operaciones en el plano de control. A continuación, reste las siguientes operaciones en NotActions para calcular los permisos efectivos:

- Eliminación de roles y asignaciones de roles
- Creación de roles y asignaciones de roles
- Concesión al autor de llamada de acceso de administrador al acceso de usuarios en el ámbito de inquilinos
- Creación o actualización de los artefactos de plano técnico
- Eliminación de los artefactos de plano técnico

Comprobación de conocimientos

1. ¿Qué es una definición de roles en Azure?

- (●) Una colección de permisos con un nombre que se puede asignar a un usuario, grupo o aplicación
  - ✔ En Azure, una definición de roles es una colección de permisos con un nombre que puede asignar a un usuario, grupo o aplicación.
- ( ) La colección de usuarios, grupos o aplicaciones que tienen permisos para un rol
- ( ) El enlace de un rol a una entidad de seguridad en un ámbito específico para conceder acceso

2. Suponga que un administrador quiere asignar un rol para permitir a un usuario crear y administrar recursos de Azure, pero sin poder conceder acceso a otros usuarios. ¿Cuál de los siguientes roles integrados admitiría esta posibilidad?

- ( ) Propietario
- (●) Colaborador
  - ✔ Un colaborador puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros usuarios.
- ( ) Lector
- ( ) Administrador de acceso de usuario

3. ¿Qué es el orden de herencia para el ámbito en Azure?

- ( ) Grupo de administración, grupo de recursos, suscripción, recurso
- (●) Grupo de administración, suscripción, grupo de recursos, recurso
  - ✔ El orden de herencia para el ámbito es grupo de administración, suscripción, grupo de recursos, recurso. Por ejemplo, si ha asignado el rol Colaborador a un grupo en el nivel del ámbito de la suscripción, todos los recursos y grupos de recursos heredarán dicho rol.
- ( ) Suscripción, grupo de administración, grupo de recursos, recurso
- ( ) Suscripción, grupo de recursos, grupo de administración, recurso

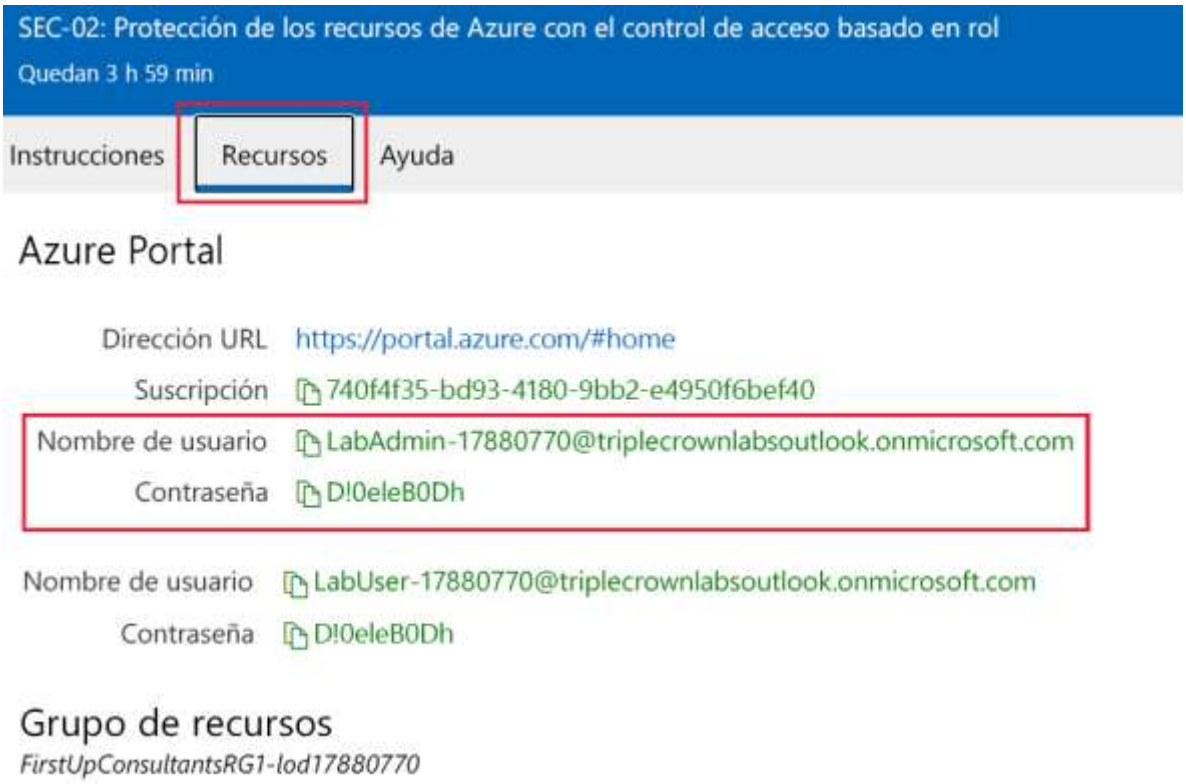
Ejercicio: Muestra del acceso mediante Azure RBAC y Azure Porta

En First Up Consultants, se le ha concedido acceso a un grupo de recursos del equipo de marketing. Quiere familiarizarse con Azure Portal y ver qué roles están asignados actualmente.

Enumeración de las asignaciones de roles para el usuario

Siga estos pasos para ver los roles que tiene asignados actualmente.

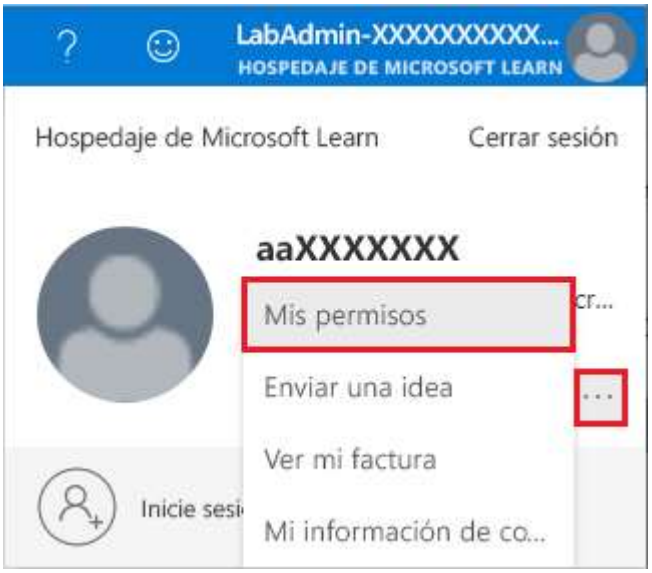
1. Seleccione **Launch lab** (Iniciar laboratorio) y luego **Start lab** (Comenzar laboratorio). En el menú emergente secundario, seleccione **Comenzar**.
2. En el menú de instrucciones del laboratorio, seleccione la pestaña **Recursos**.



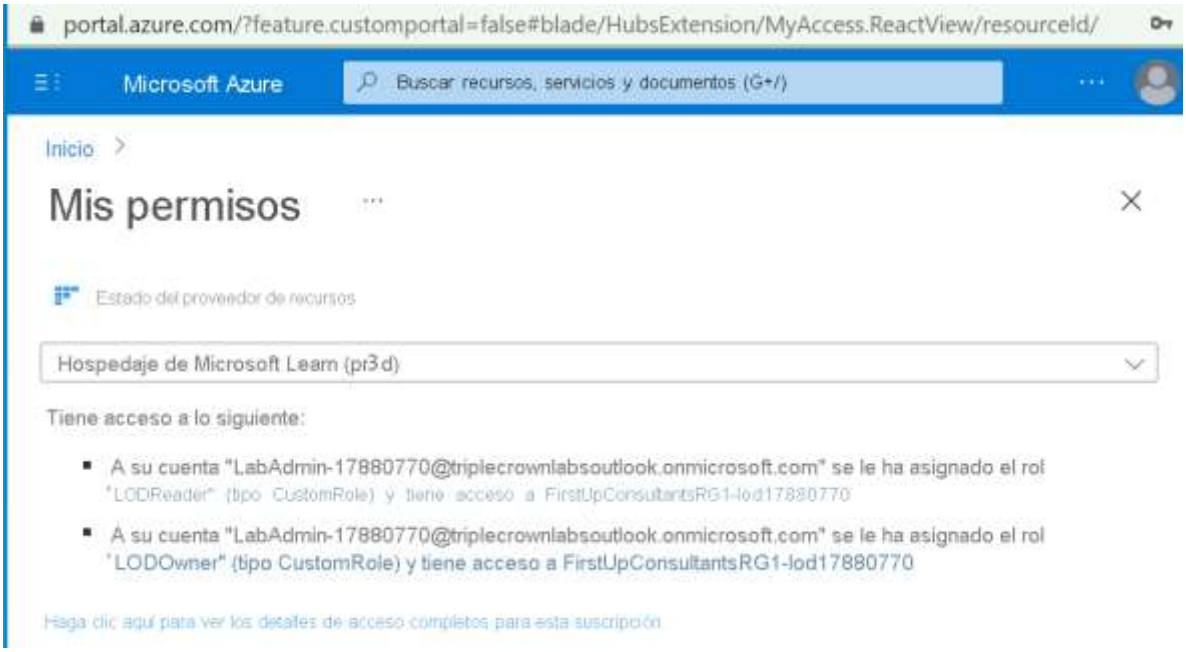
3. Busque un nombre de usuario administrador similar a **LabAdmin-*XXXXXXX*** y la contraseña.
4. Inicie sesión en Azure Portal con el nombre de usuario y la contraseña labAdmin.
5. Cierre el menú emergente de bienvenida y, en la esquina superior derecha de Azure Portal, seleccione la imagen de perfil para abrir el menú de perfil.

6. Asegúrese de que ha iniciado sesión con el usuario **LabAdmin-*XXXXXXX*** que se ha identificado en la pestaña **Recursos** de las instrucciones del laboratorio. Si ha iniciado sesión con otra cuenta, ciérrela y vuelva a iniciarla con estos datos.

7. En el menú **Perfil**, seleccione los puntos suspensivos (**...**) para ver más vínculos.



8. Seleccione **Mis permisos** para abrir el panel **Mis permisos**.

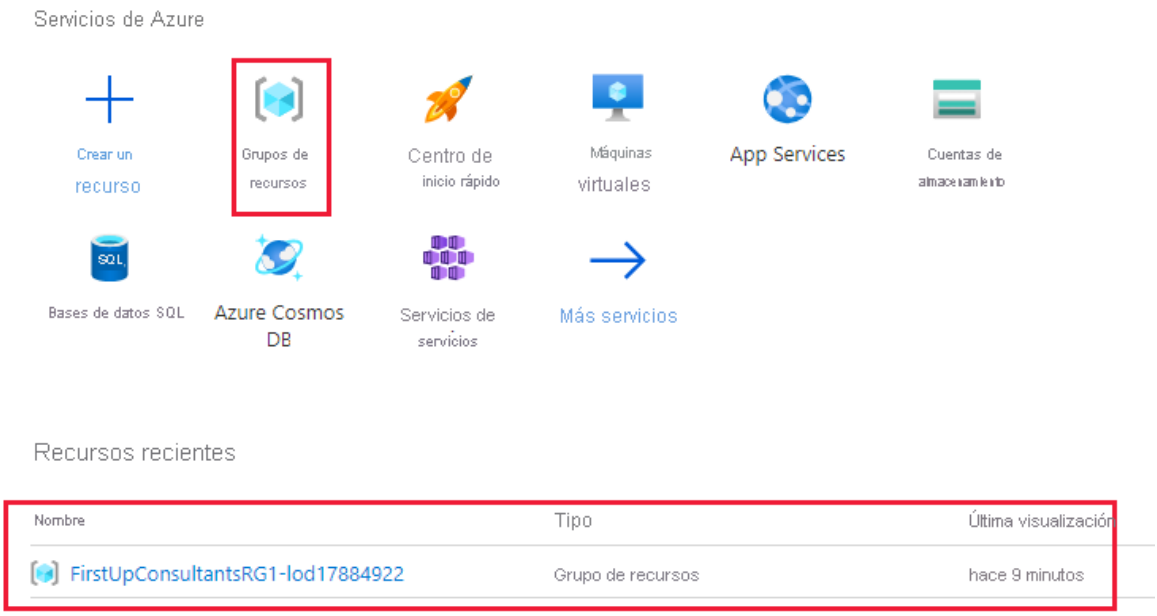


Verá los roles que se le han asignado y el ámbito. En su caso, la lista tendrá otro aspecto.

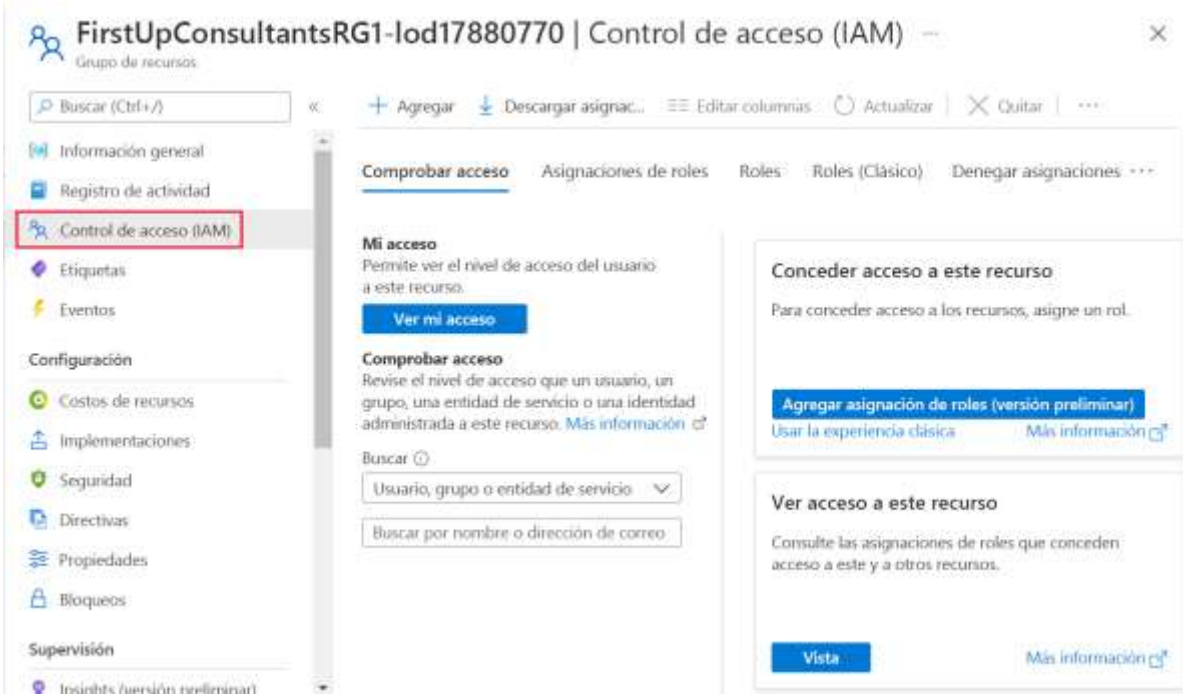
Lista de las asignaciones de roles de un grupo de recursos

Siga estos pasos para ver qué roles se asignan en el ámbito del grupo de recursos.

1. Seleccione **Inicio** y, en **Servicios de Azure**, seleccione **Grupos de recursos**.

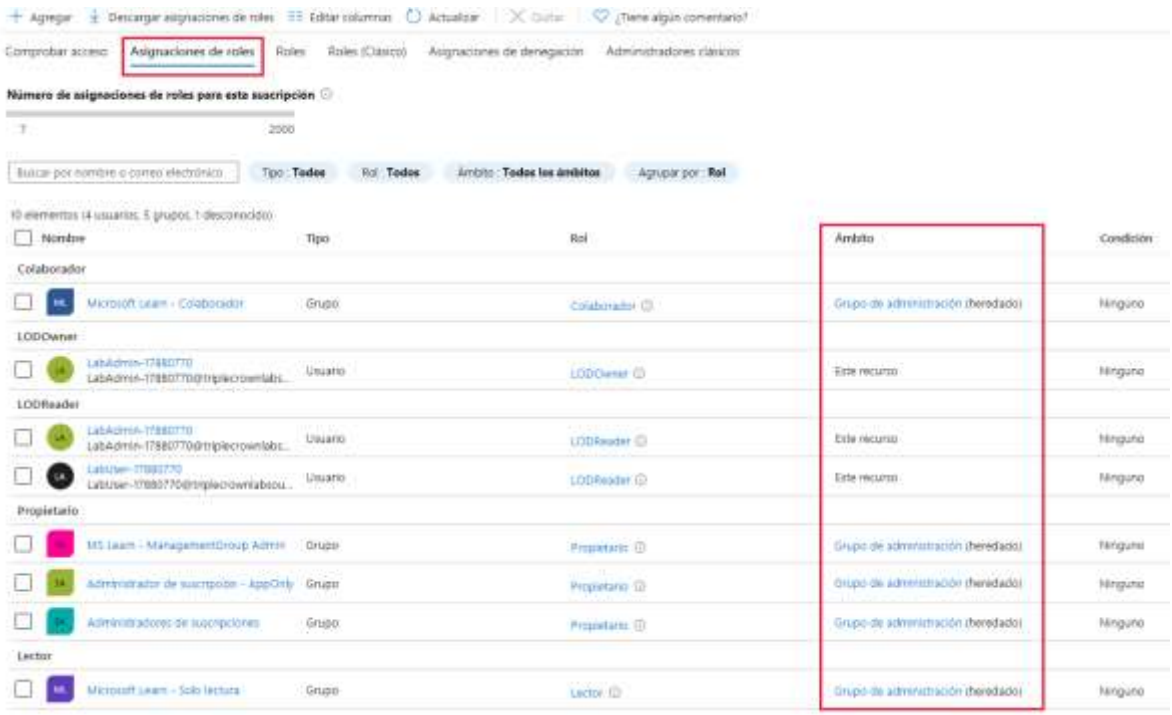


2. Seleccione el grupo de recursos **FirstUpConsultantsRG1-*XXXXXXX*** y, en el panel de menús izquierdo, elija **Control de acceso (IAM)**.



3. Seleccione la pestaña **Asignaciones de roles**.

En esta pestaña se muestra quién tiene acceso al grupo de recursos. Observe que el ámbito de algunos roles es **Este recurso**, mientras que el de otros es **(Heredado)** de un ámbito principal.



Lista de roles

Como ha aprendido en la unidad anterior, un rol es una colección de permisos. Azure tiene más de 70 roles integrados que puede usar en las asignaciones de roles. Siga este paso para enumerar los roles.

- En la barra de menús de la parte superior del panel, seleccione la pestaña **Roles** para enumerar todos los roles integrados y personalizados.

Seleccione un rol en esta pestaña para mostrar el número de usuarios y grupos asignados a ese rol.

Ejercicio: Concesión de acceso mediante Azure RBAC y Azure Portal

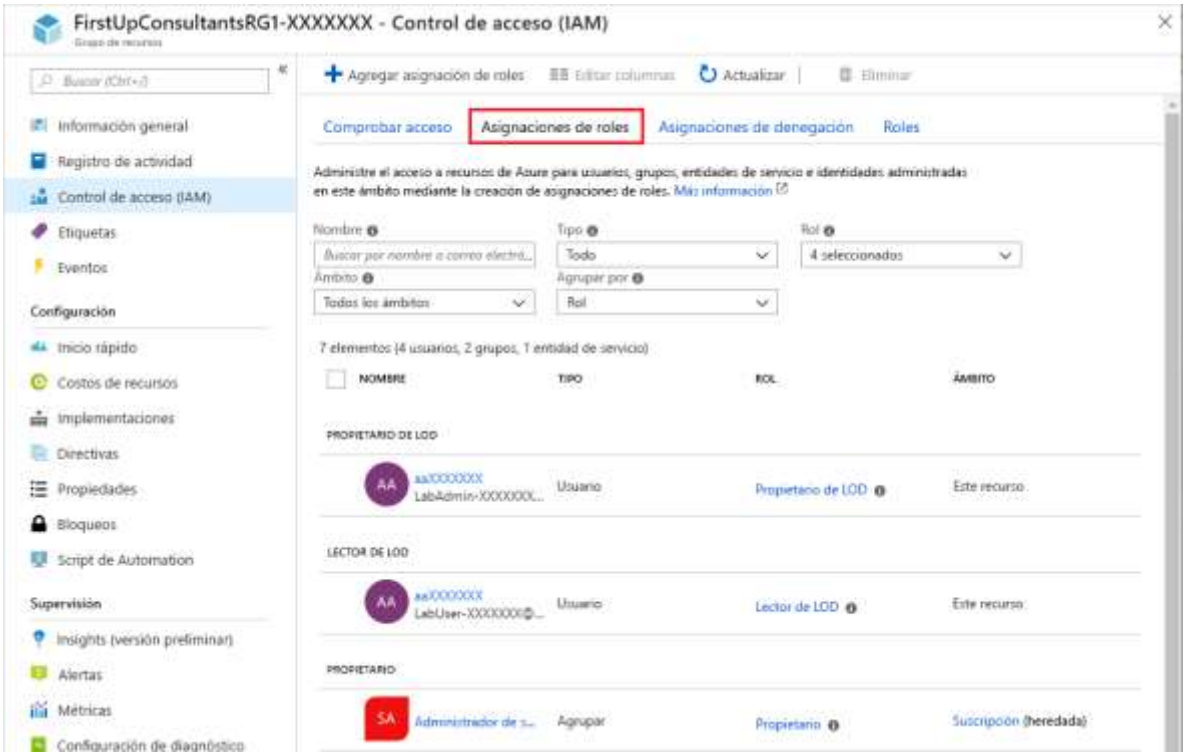
Un compañero de trabajo llamado Alain de First Up Consultants necesita permiso para crear y administrar máquinas virtuales para un proyecto en el que está trabajando. Su jefe le ha pedido que administre esta solicitud. Con el procedimiento recomendado para conceder a los usuarios los privilegios mínimos para realizar el trabajo, decide asignar a Alain el rol de colaborador de máquina virtual en un grupo de recursos.

Concesión de acceso

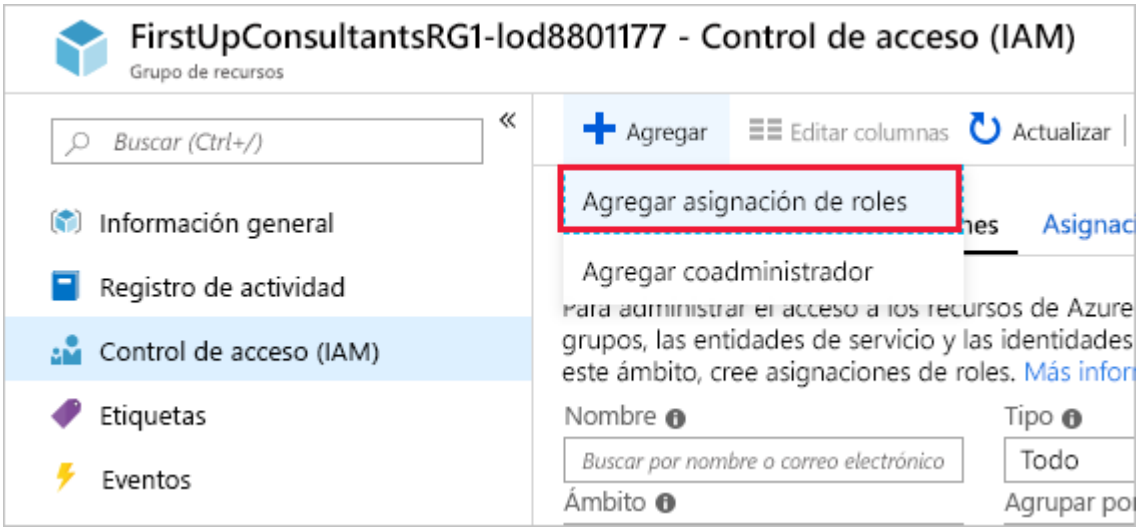
Siga este procedimiento para asignar el rol de colaborador de máquina virtual a un usuario en el ámbito del grupo de recursos.

1. En Azure Portal, en Explorar, seleccione **Grupos de recursos**.
2. Seleccione el grupo de recursos **FirstUpConsultantsRG1-*XXXXXXX***.
3. Seleccione **Access Control (IAM)** .

4. Seleccione la pestaña **Asignaciones de roles** para ver la lista actual de asignaciones de roles.



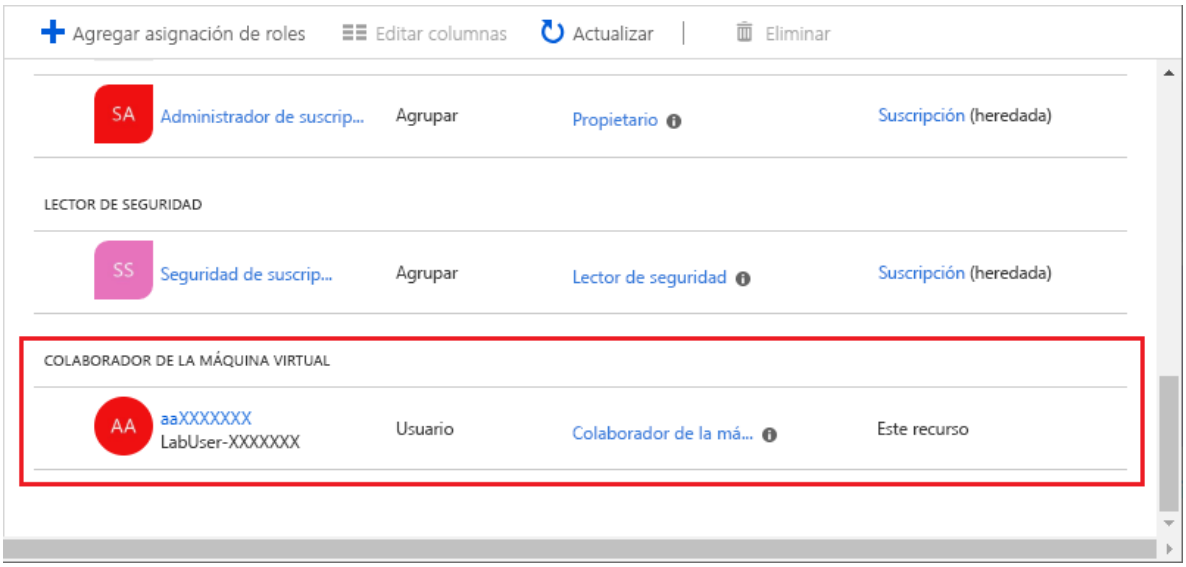
5. En la parte superior, seleccione **Agregar asignación de roles**.



6. En la pestaña **Rol**, busque y seleccione **Colaborador de la máquina virtual**.
7. Seleccione **Next** (Siguiente).
8. En la pestaña **Miembros**, seleccione **+ Seleccionar miembros**.

9. Busque y seleccione el nombre **LabUser-*XXXXXXX*** adecuado. Encontrará el nombre de usuario que se va a usar en la pestaña **Recursos** situada junto a las instrucciones.
10. Seleccione **Next** (Siguiente).
11. Seleccione **Revisar y asignar**.

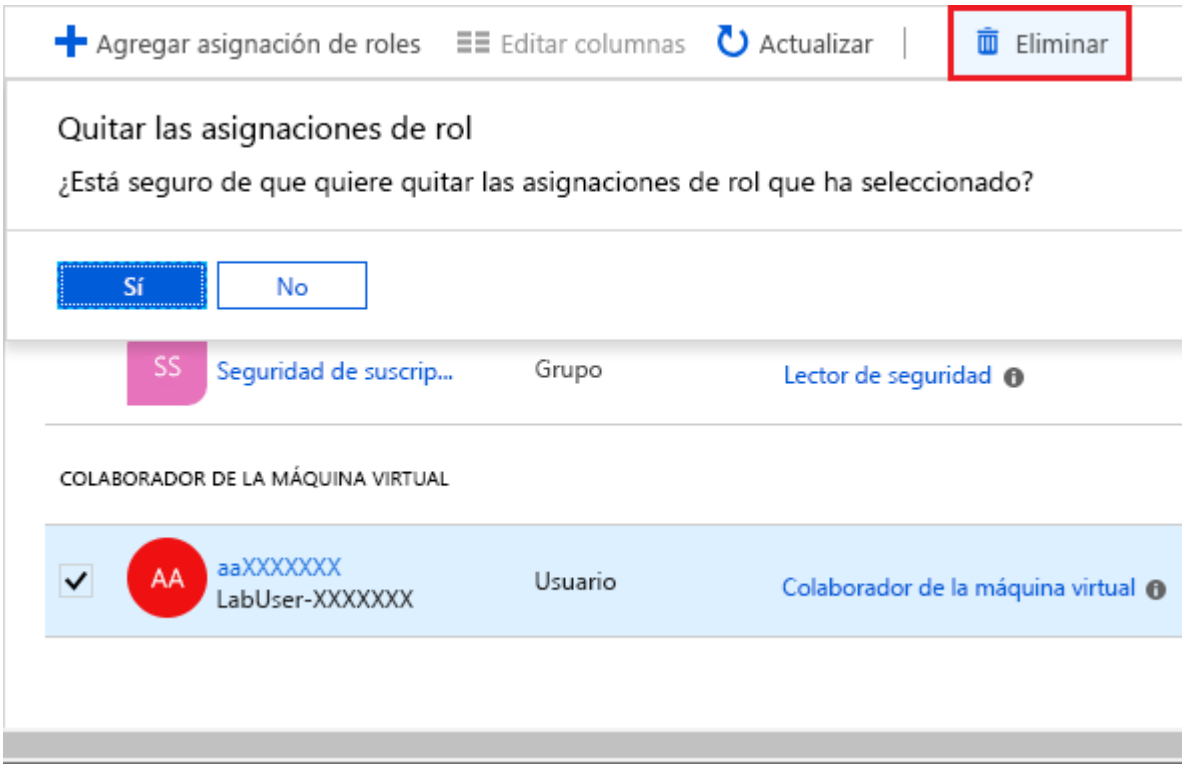
Transcurridos unos instantes, al usuario **LabUser-*XXXXXXXXX*** se le asigna el rol de colaborador de máquina virtual en el ámbito del grupo de recursos **FirstUpConsultantsRG1-*XXXXXXXXX***. El usuario ahora puede crear y administrar máquinas virtuales solo dentro de este grupo de recursos.



Eliminación de acceso

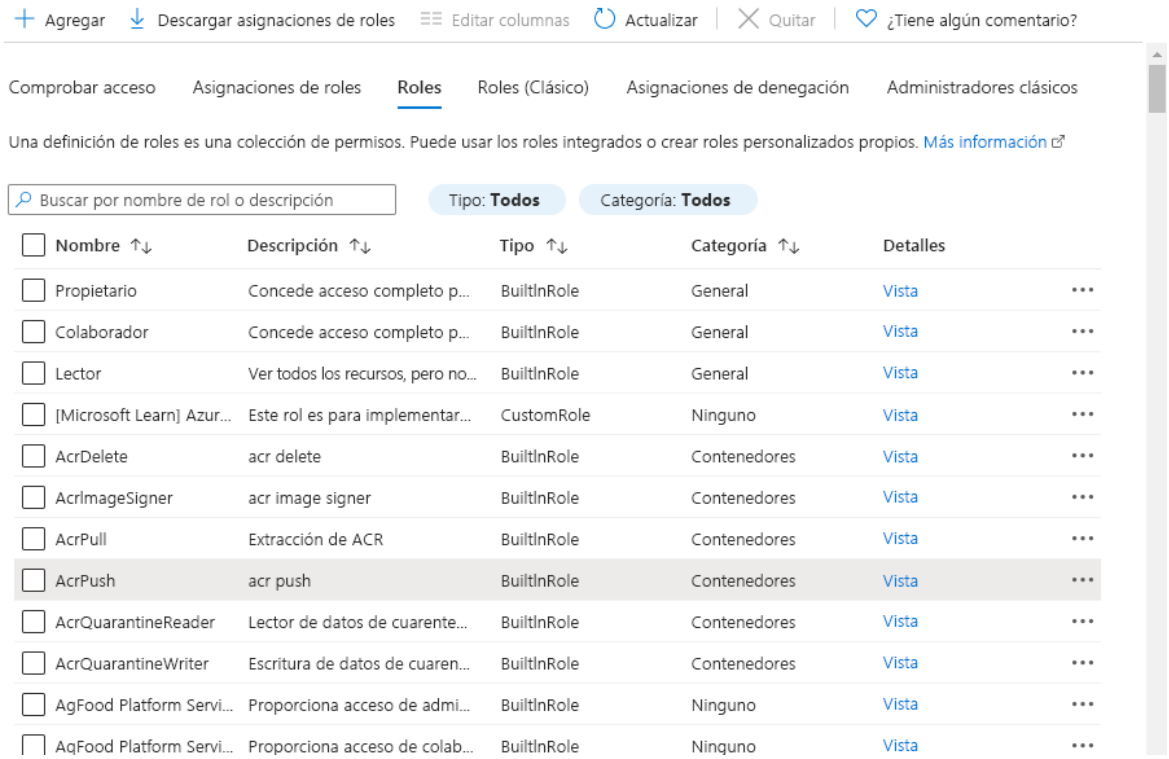
En Azure RBAC, para quitar el acceso hay que quitar una asignación de roles.

1. En la lista de asignaciones de roles, seleccione el usuario **LabUser -*XXXXXXX*** con el rol de colaborador de máquina virtual.
2. Seleccione **Quitar**.



3. En el mensaje **Quitar las asignaciones de rol** que aparece, seleccione **Sí**.

En esta unidad, ha aprendido a conceder acceso a un usuario para crear y administrar máquinas virtuales en un grupo de recursos mediante Azure Portal.



En esta unidad, ha aprendido a mostrar las asignaciones de rol en Azure Portal. También ha aprendido a enumerar las asignaciones de roles de un grupo de recursos.

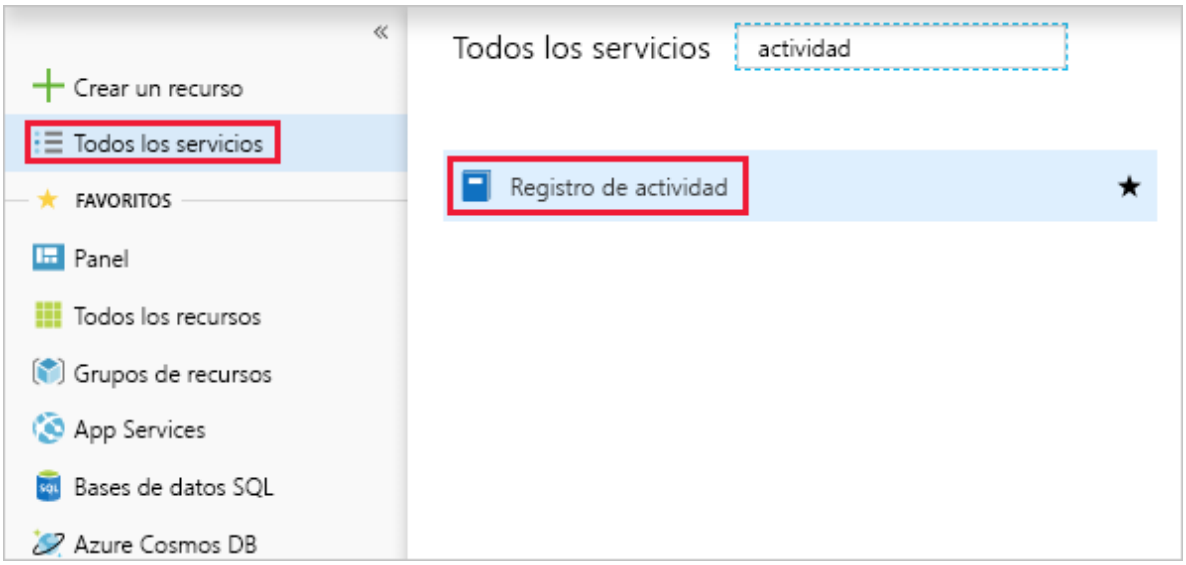
Ejercicio: Visualización de los registros de actividad de cambios de Azure RBAC

First Up Consultants revisa trimestralmente los cambios en el control de acceso basado en rol de Azure (Azure RBAC) con fines de auditoría y solución de problemas. Sabe que los cambios se registran en el registro de actividad de Azure. El administrador le ha preguntado si puede generar un informe de la asignación de roles y los cambios de funciones personalizados del último mes.

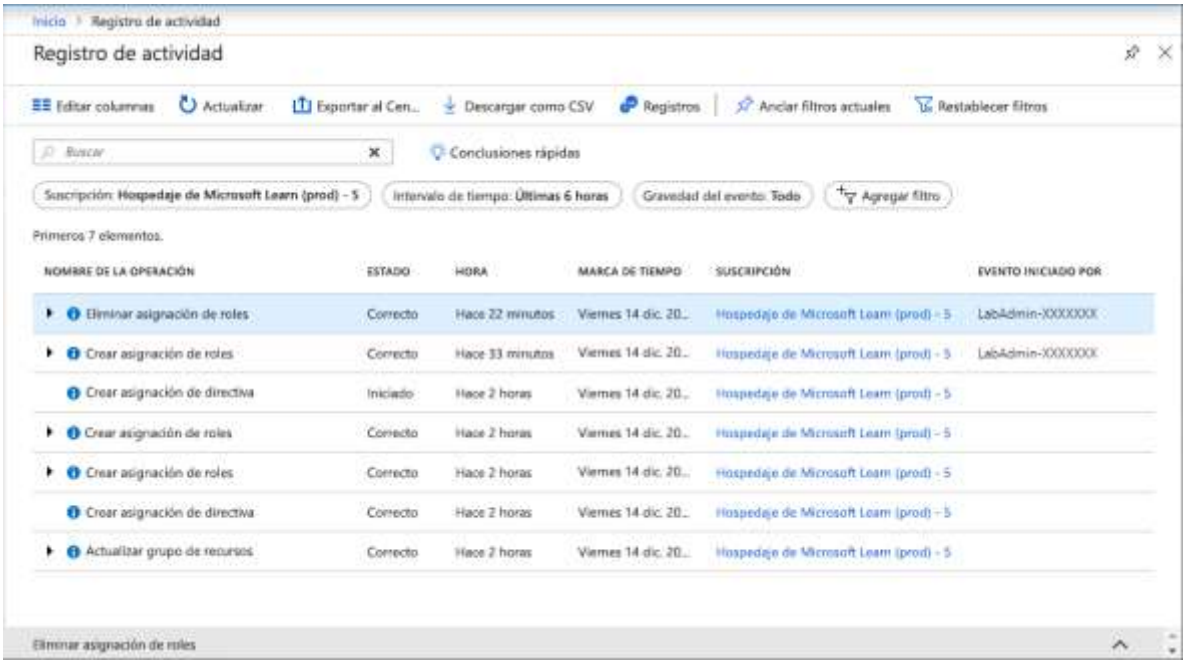
Visualización de registros de actividad

La manera más fácil de empezar a trabajar es ver los registros de actividad con Azure Portal.

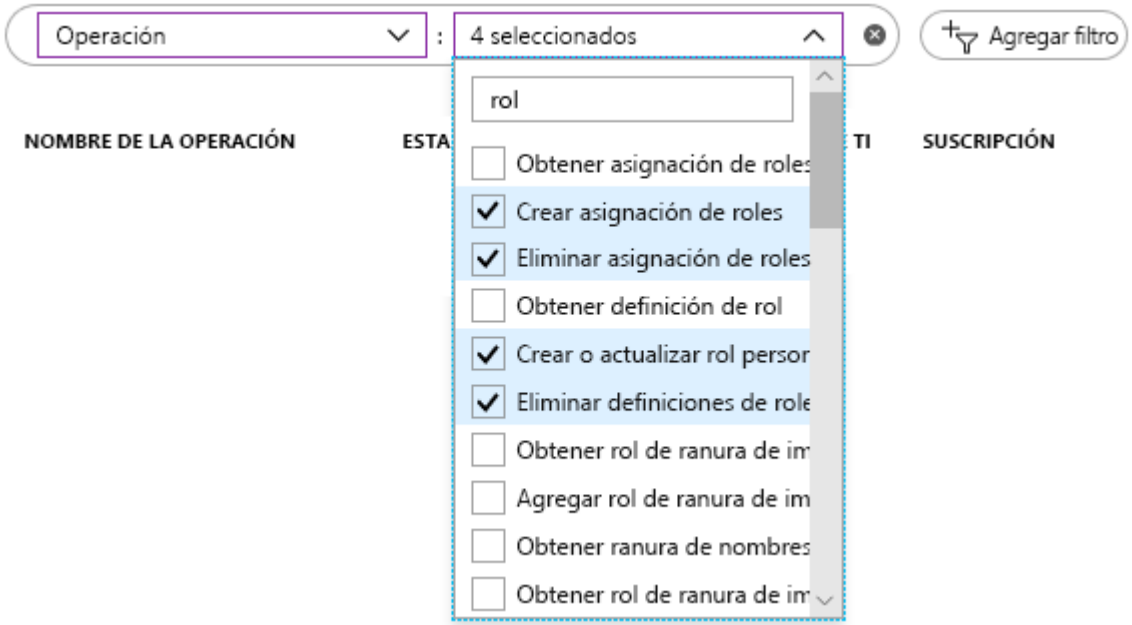
1. Seleccione **Todos los servicios** y luego busque **Registro de actividad**.



2. Seleccione **Registro de actividad** para abrir el registro de actividad.

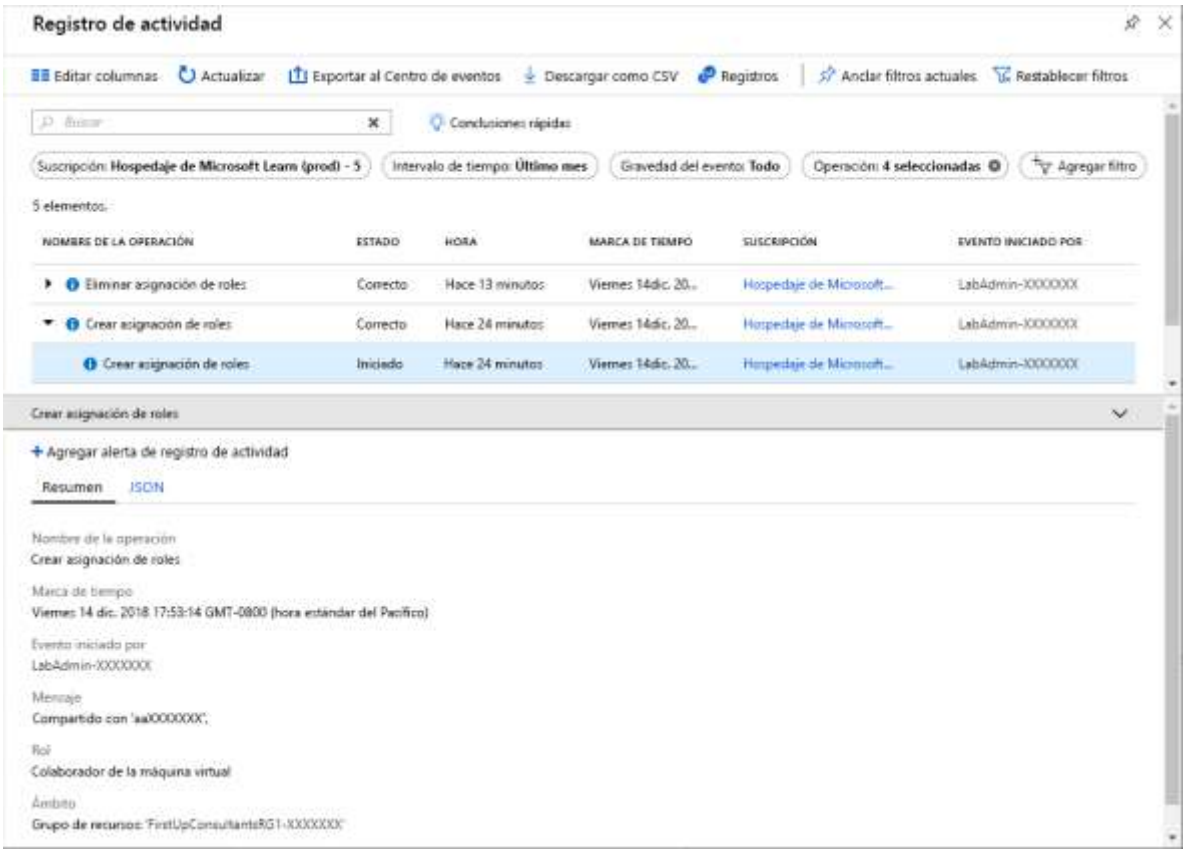


3. Establezca el filtro de **Intervalo de tiempo** en **Mes pasado**.
4. Agregue un filtro **Operación** y escriba **rol** para filtrar la lista.
5. Seleccione las siguientes operaciones de Azure RBAC:
    - Crear asignación de roles (roleAssignments)
    - Eliminar asignación de roles (roleAssignments)
    - Creación o actualización de definiciones de roles personalizadas (roleDefinitions)
    - Eliminación de definiciones de roles personalizadas (roleDefinitions)



Al cabo de unos minutos verá todas las operaciones de asignación y definición de roles del último mes. También incluye un vínculo para descargar los registros de actividad como un archivo CSV.

6. Seleccione una de las operaciones para ver los detalles del registro de actividad.



En esta unidad, ha aprendido a usar el registro de actividad de Azure para enumerar los cambios de Azure RBAC en el portal y generar un informe simple.

1. Supongamos que un miembro del equipo no puede ver los recursos de un grupo de recursos. ¿Adónde debe dirigirse el administrador para comprobar el acceso del miembro del equipo?

- ○ Debe comprobar los permisos del miembro del equipo en su **perfil de Azure > Mis permisos.**
- ◉ Debe ir al grupo de recursos y seleccionar **Control de acceso (IAM)>Comprobar acceso.**
  - ✔ La lista de asignaciones de roles se encuentra en el grupo de recursos.
- ○ Debe ir a uno de los recursos del grupo de recursos y seleccionar **Asignaciones de roles.**

2. Supongamos que un administrador de otro departamento necesita tener acceso a una máquina virtual administrada por el departamento en el que usted trabaja. ¿Cuál es la mejor manera de concederle acceso solo a este recurso?

- ○ En el ámbito del recurso, se crea un rol para esta persona con el acceso adecuado.
- ○ En el ámbito del grupo de recursos, se asigna el rol con el acceso adecuado.
- ◉ En el ámbito del recurso, se asigna el rol con el acceso adecuado.
  - ✔ En este escenario, hay que asignar en el ámbito de la máquina virtual uno de los roles integrados que concede el acceso adecuado para el administrador.

3. Suponga que un desarrollador necesita acceso total a un grupo de recursos. Si está siguiendo los procedimientos recomendados con privilegios mínimos, ¿qué ámbito debe especificar?

- ○ Recurso
- ◉ Grupo de recursos
  - ✔ Siguiendo los procedimientos recomendados con privilegios mínimos, solo tiene que conceder el acceso que el usuario necesita para hacer su trabajo. En este caso, debe establecer el ámbito para el grupo de recursos.
- ○ Suscripción

4. Supongamos que un administrador necesita generar un informe de las asignaciones de roles de la última semana. ¿En qué lugar de Azure Portal generaría el informe?

- ◉ Debe buscar **Registro de actividades** y filtrar por la operación **Crear asignación de roles (roleAssignments).**
  - ✔ En el registro de actividades, debe filtrar por el campo Nombre de la operación para buscar las asignaciones de roles.
- ○ En el ámbito adecuado, debe ir a **Control de acceso (IAM)>Descargar asignaciones de roles.**
- ○ En el ámbito adecuado, debe ir a **Control de acceso (IAM)>Asignaciones de roles.**