Azure Data Lake Role Based Access Control

Quiero explicar el Control de acceso basado en roles (Role based access control [RBAC]). Ahora, sabemos que Azure Active Directory es nuestro Identity provider, así que aquí, podemos crear usuarios y el usuario puede realmente iniciar sesión en nuestra cuenta de Azure. Ahora, digamos que definimos un usuario en Azure Active Directory. Ahora, este usuario puede iniciar sesión en nuestra cuenta Azure, básicamente tener acceso a nuestra suscripción Azure. Pero inicialmente, no tendrá ningún permiso para acceder a los recursos que se definen como parte de la suscripción. Tendremos que darle acceso explícitamente a través de algo conocido como "Role based access control (RBAC)". Así que si tenemos una cuenta de almacenamiento, si tenemos una Azure Data Lake Gen2 storage account, si queremos que tengan acceso a esa cuenta de almacenamiento, lo primero que tenemos que hacer es dar acceso a través de "Role based access control".

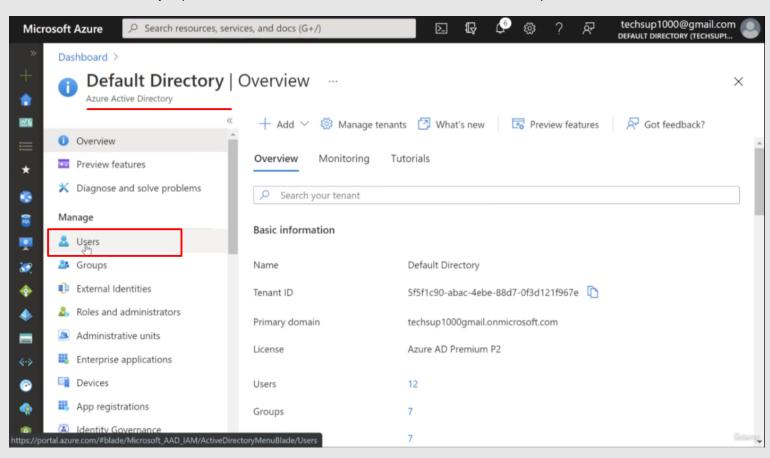
https://learn.microsoft.com/es-es/azure/role-based-access-control/built-in-roles

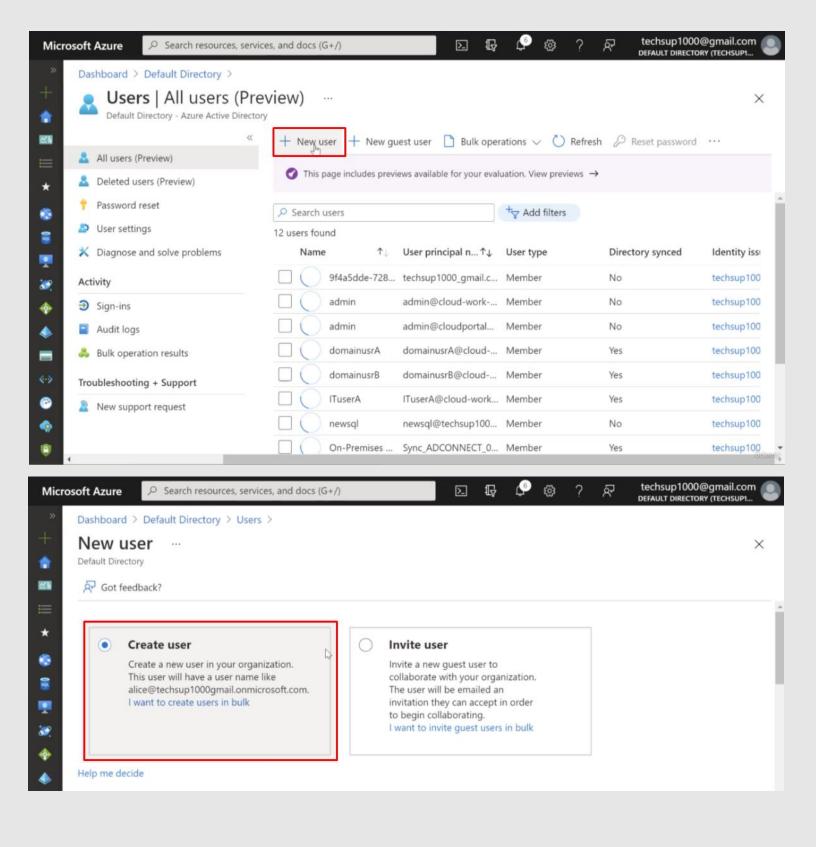
El control de acceso basado en rol de Azure (Azure RBAC) tiene varios roles integrados de Azure que se pueden asignar a usuarios, grupos, entidades de servicio e identidades administradas. Las asignaciones de roles sirven para controlar el acceso a los recursos de Azure. Si los roles integrados no satisfacen las necesidades específicas de la organización, puede crear roles personalizados de Azure propios.

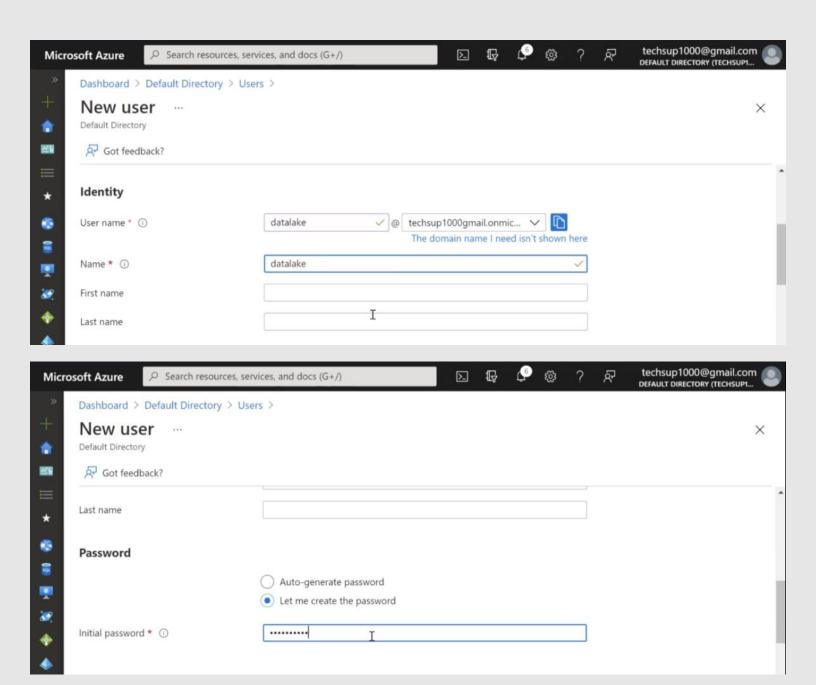
En la tabla siguiente se proporciona una breve descripción de cada rol integrado. Haga clic en el nombre del rol para ver la lista de Actions, NotActions, DataActions y NotDataActions para cada rol.

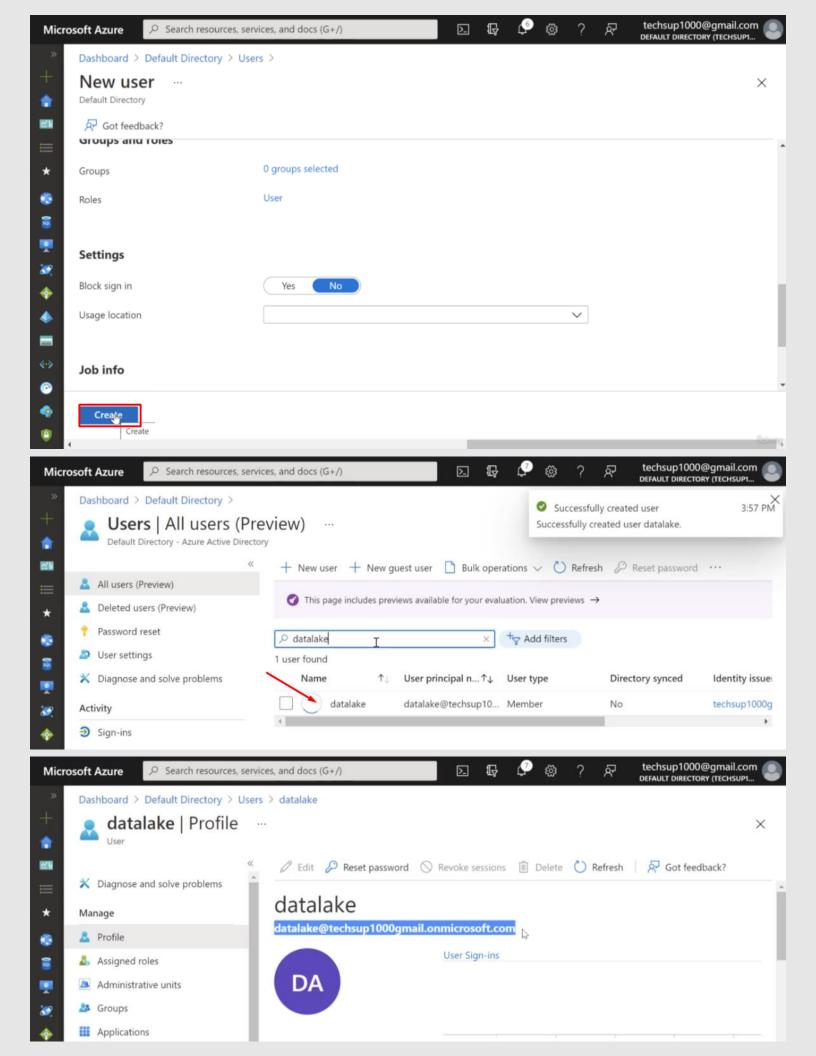
Rol integrado	Descripción	id
General		
Colaborador Contributor	Concede acceso completo para administrar todos los recursos, pero no le permite asignar roles en Azure RBAC, administrar asignaciones en Azure Blueprints ni compartir galerías de imágenes.	b24988ac-6180-42a0-ab88- 20f7382dd24c
Propietario Owner	Permite conceder acceso total para administrar todos los recursos, incluida la posibilidad de asignar roles en Azure RBAC.	8e3af657-a8ff-443c-a75c- 2fe8c4bcb635
Lector Reader	Permite ver todos los recursos, pero no realizar ningún cambio.	acdd72a7-3385-48ef-bd42- f606fba81ae7
Administrador de acceso de usuario	Permite administrar el acceso de usuario a los recursos de Azure.	18d7d88d-d35e-4fb5-a5c3- 7773c20a72d9
User Access Administrator		

Vamos a ejemplificarlo creando un nuevo usuario en Azure Active Directory

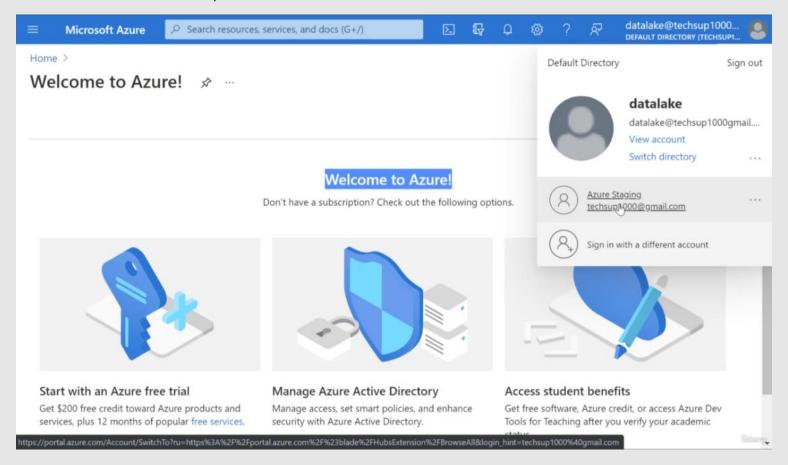




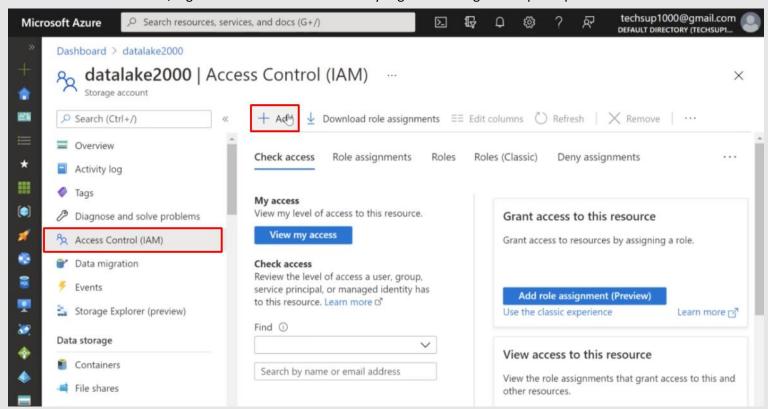


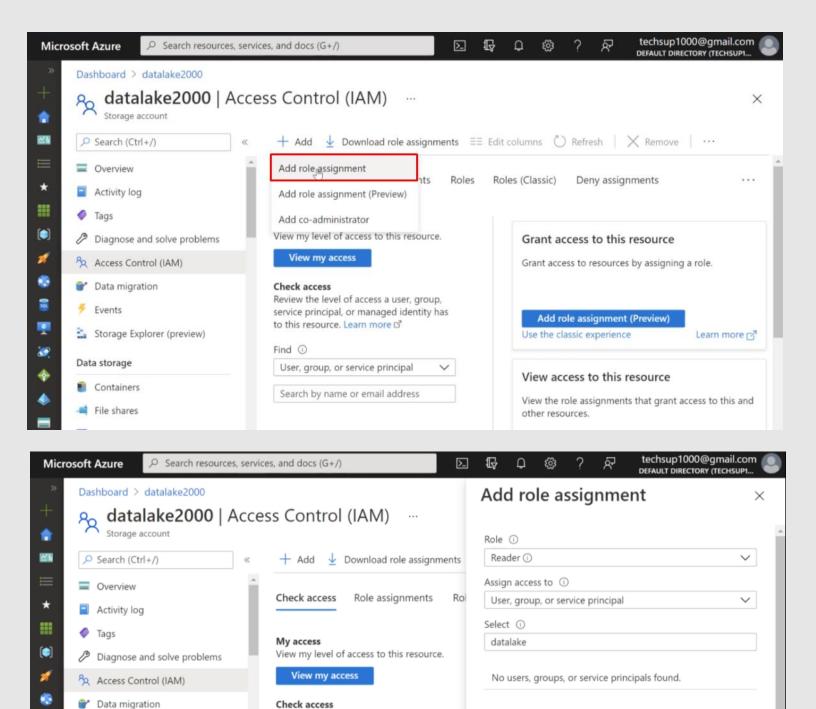


Si ingresamos a Azure con la cuenta del nuevo usuario, veremos que no podemos visualizar ningún recurso de la suscripción.



Nuevamente, ingresamos con la cuenta admin y seguimos los siguientes pasos para crear un RBAC





Review the level of access a user, group,

User, group, or service principal

Search by name or email address

Find ①

service principal, or managed identity has to this resource. Learn more \Box

Selected members:

datalake

Discard

datalake@techsup1000gmail.onmicro... Remove

Events

Data storage

Containers

File shares

Queues

Tables

Storage Explorer (preview)

Ahora si volvemos a logearnos con el nuevo usuario podremos ver nuestra Azure Data Lake Storage account. Esto es posible porque hemos dado el control de acceso basado en roles (Role based access control) a esta cuenta de almacenamiento.

