

Azure RBAC

Role Based Access Control

It's a way to manage who has access to what in your Azure resources. Instead of giving everyone admin rights (☹️ dangerous), RBAC lets you assign specific roles to users, groups, or applications — so they only get the permissions they actually need.

◆ Key Points About RBAC in Azure

1. **Role-Based** → Access is controlled through roles, not individual permissions each time.
2. **Scope-Based** → You can assign roles at different levels of Azure:
 - Management Group
 - Subscription
 - Resource Group
 - Individual Resource(Permissions flow downward — e.g., a role at subscription level applies to all resource groups inside it).
3. **Principals** → You assign roles to:
 - Users
 - Groups
 - Service Principals (apps)
 - Managed Identities
4. **Deny by Default** → Unless a role is assigned, a user has no access.

◆ Common Built-in Roles

- ✓ **Owner** → Full access, including role assignments.
- ✓ **Contributor** → Create & manage resources, but can't grant access. → *can't assign Roles*
- ✓ **Reader** → View-only access.
- ✓ **API Caller** → *can only call API's*

There are also hundreds of specialized roles (e.g., Virtual Machine Contributor, Storage Blob Reader). You can also create custom roles.

only Difference

Q11. Is RBAC similar to RLS?

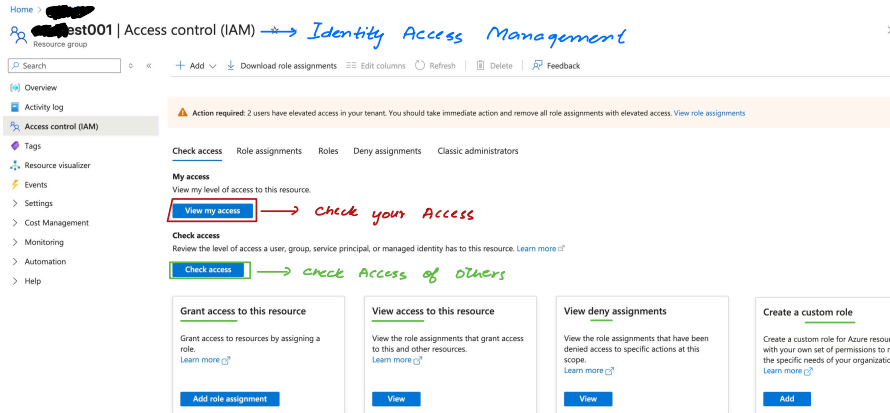
◆ Difference in one line:

- **RBAC** = Access to Azure resources (infra/app level).
- **RLS** = Access to rows in a dataset (data level).

Azure RBAC Model



Access Management



Steps to Role Management

I. Create User

Azure portal

Users

Create new user

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name *

@

Domain not listed? [Learn more](#)

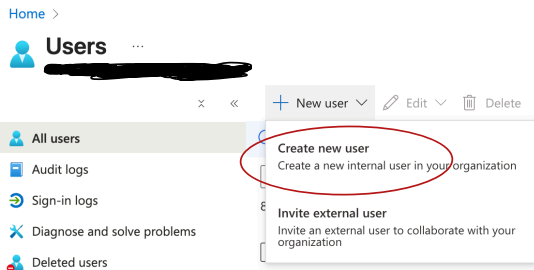
Mail nickname *

☒ Derive from user principal name

Display name *

Password *

☒ Auto-generate password



II. Role Assignment (IAM)

IAM

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

☒ open all ☐ Key word

Name ?

Cognitive Services OpenAI Contributor Full access including the ability to fine-tune, deploy and generate text

Cognitive Services OpenAI User Ability to view files, models, deployments. Readers can't make any changes They can inference and create images

Showing 1 - 2 of 2 results.

Add role assignment

Role Members Conditions Review + assign

Selected role

Cognitive Services OpenAI Contributor

Assign access to

☒ User, group, or service principal

☐ Managed identity

Members

+ Select members

Add member