

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**.

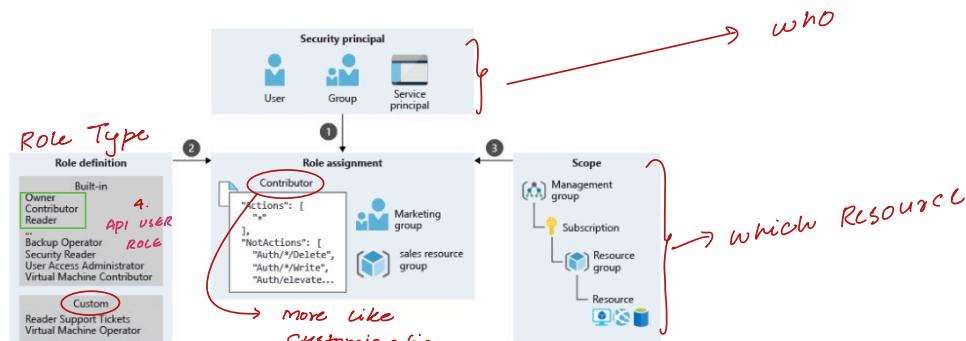
only
Difference

Q: 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

Home > [REDACTED] | Access control (IAM) → Identity Access Management

Access control (IAM)

Action required: 2 users have elevated access in your tenant. You should take immediate action and remove all role assignments with elevated access. View role assignments

Check access Role assignments Roles Deny assignments Classic administrators

My access View my level of access to this resource.

View my access → check your Access

Check access Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Check access → check Access of others

Grant access to this resource Grant access to resources by assigning a role. Learn more

Add role assignment

View access to this resource View the role assignments that grant access to this and other resources. Learn more

View

View deny assignments View the role assignments that have been denied access to specific actions at this scope. Learn more

View

Create a custom role Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization. Learn more

Add

Steps to Role management

1. Create user

Azure portal → **Users**

Home >

Users

All users Audit logs Sign-in logs Diagnose and solve problems Deleted 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 * thetesting.club Domain not listed? Learn more

Mail nickname * Derive from user principal name

Display name *

Password * Auto-generate password

11. 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.

OpenAI Keyword

Name: Cognitive Services OpenAI Contributor Description: Full access including the ability to fine-tune, deploy and generate text Category: All

Selected role Cognitive Services OpenAI Contributor

Assign access to:

- User, group, or service principal
- Managed identity

+ Select members Add member