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**.

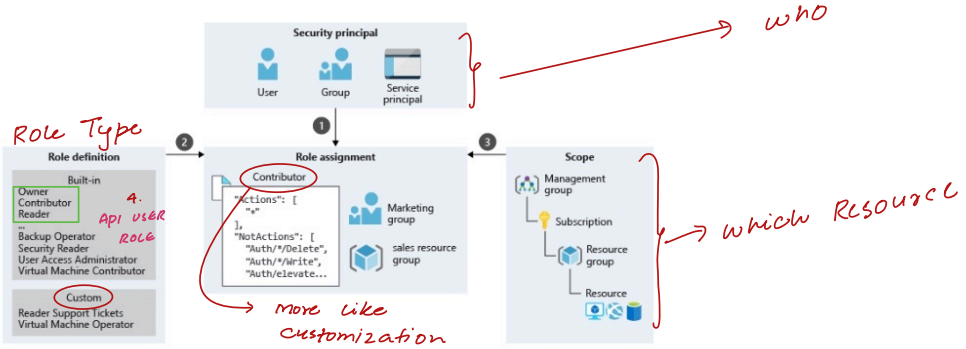
only Difference

Q.. Is RBAC similar to RLS ?

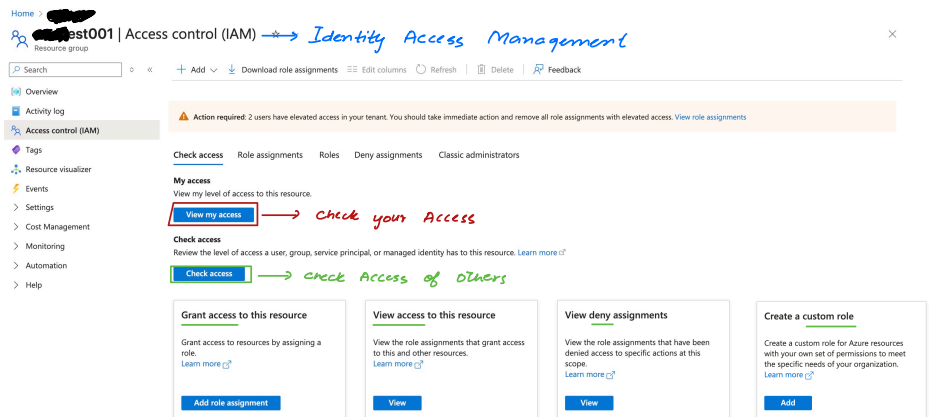
🔹 Difference in one line:

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

Azure RBAC MODEL



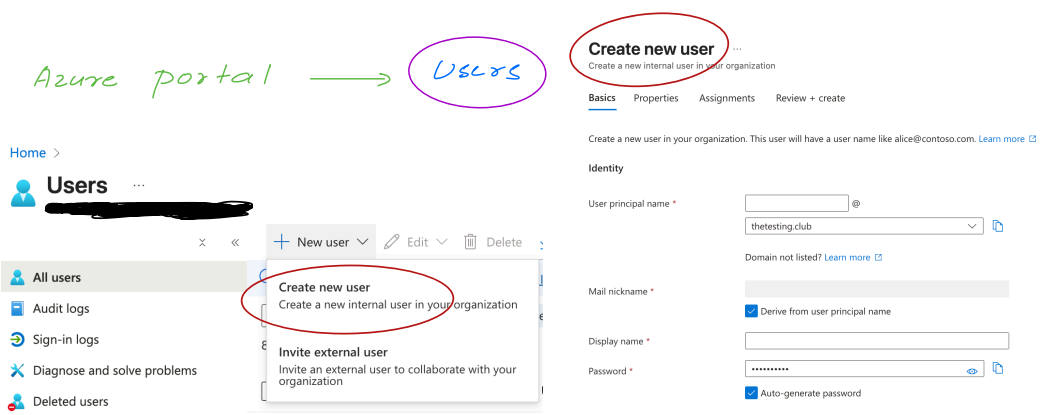
Access Management



Steps to Role Management

1. Create User

Azure portal → Users



11. Role Assignment (IAM)

IAM