What is Azure RBAC?

Azure RBAC is a system that helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. It's a key part of Azure's security model.

How Azure RBAC Works

- **Roles:** Azure has built-in roles (like Owner, Contributor, Reader) and you can create custom roles.
- **Scope:** Roles are assigned at a scope: subscription, resource group, or individual resource level.
- **Assignments:** You assign roles to users, groups, service principals, or managed identities.

When a user tries to perform an action, Azure checks their role assignments at the relevant scope and allows or denies based on permissions granted.

Key Components

Component	Description
Role Definition	Collection of permissions (e.g., read, write)
Role Assignment	Linking a role to a user/group at a scope
Scope	Where the role applies (subscription, resource group, resource)

Built-in Roles Examples

- **Owner:** Full access to all resources including the right to delegate access.

- **Contributor:** Can create and manage all types of Azure resources but can’t grant access to others.

- **Reader:** Can view existing Azure resources but cannot make any changes.

How to Assign Roles in Azure

1. Go to the Azure Portal.

2. Navigate to the resource or resource group.

3. Click on **Access control (IAM)**.

4. Click **Add role assignment**.

5. Select the role.

6. Assign the user, group, or service principal.

Benefits of Azure RBAC

- **Fine-grained access control:** Assign permissions at various levels (subscription, resource group, resource).

- **Least privilege principle:** Assign only the permissions needed.

- **Auditing:** Azure logs role assignments for compliance and monitoring.

- **Scalable management:** Use Azure AD groups and service principals to manage many users or applications.

Example Scenario

- A developer is assigned the **Contributor** role on a resource group to manage VMs.

- A security analyst is assigned the **Reader** role on the subscription to monitor resource status.

- An administrator has the **Owner** role on the subscription to manage all access.