
🔐 RBAC (Role-Based Access Control)

RBAC is a system that helps control access to resources by assigning **roles** to **users**, **groups**, or **service principals** at different **scopes** (like subscriptions, resource groups, or individual resources).

👤 Users

- **Definition**: Individual identities (often tied to Azure Active Directory or your identity provider).
- **Can be assigned roles** directly or via groups.
- Best practice is to **assign roles to groups**, not individual users, to simplify management.

🧭 Management Groups (Azure-specific concept)

- **Definition**: A container for managing access, policy, and compliance across multiple subscriptions.
- **Hierarchy**: Management groups can be nested. Subscriptions inherit settings and permissions from their parent management group.
- You can apply **RBAC roles at the management group level** to control access across all underlying subscriptions and resources.

✅ How RBAC Works with Users and Management Groups

Element	Description
User	Assigned to roles either directly or via Azure AD groups.
Group	AAD groups can contain users, and be assigned roles.
Role	Defines allowed actions (e.g., Reader, Contributor, Owner). Custom roles also possible.
Scope	Where access applies: Management Group > Subscription > Resource Group > Resource.
Management Group	Allows you to apply RBAC across many subscriptions at once.

🛠️ Example

> Scenario: You want all members of your **IT Admin group** to have **Contributor** access to **all subscriptions** in your organization.

Steps:

1. Create a group in Azure AD: IT-Admins
2. Assign the **Contributor** role to the IT-Admins group **at the Management Group level**.
3. All subscriptions under that management group inherit the role assignment.
4. Any user added to the IT-Admins group automatically gets Contributor access.

LAB

🎬 RBAC + Users + Management Groups – Demo Scenario

🔧 Scenario:

> You're an Azure administrator. You want to give a user named **Alice** the ability to **read all resources** in all subscriptions under your organization's management group.

🗂️ Step 1: Structure Overview

You have:

- ✅ A **Management Group**: ContosoRoot
- ✅ Under it, two **Subscriptions**:
  - Contoso-Prod
  - Contoso-Dev

- ✅ A user: alice@contoso.com

👣 Step 2: Assign Role to User at Management Group Level

Objective: Give Alice **Reader** access at the **Management Group** level.

Azure Portal Steps:

1. Go to **Azure Portal** → Search for **Management Groups**.
2. Select your **Management Group**: ContosoRoot.
3. Click **Access Control (IAM)**.
4. Click **+ Add > Add role assignment**.
5. In the **Role** field, select **Reader**.
6. In **Assign access to**, select **User, group, or service principal**.
7. Search for **alice@contoso.com**, select her.
8. Click **Next** → **Review + assign**.

✅ **Result**: Alice now has **read-only access** to **all subscriptions and resources** under ContosoRoot.

📌 Step 3: (Optional) Use Groups Instead of Individual Users

Best Practice: Use Azure AD Groups

1. Create an AAD Group: Global-Readers
2. Add Alice to the group.
3. Assign the **Reader** role to Global-Readers at the **ContosoRoot Management Group** level.

Now, any user added to Global-Readers will automatically get read access to everything under that management group.

🔍 Verification

To test Alice's access:

1. Sign in as Alice to the Azure Portal.
2. Try browsing to different subscriptions/resources.
3. She can **view** but **not modify** resources.

📉 Visual Summary

```
ContosoRoot (Management Group)
│
├── Contoso-Prod (Subscription)
│
└── Contoso-Dev (Subscription)
```

[RBAC: Reader Role]

↑

Assigned to:

- alice@contoso.com OR

- Azure AD Group: Global-Readers

Let me know if you'd like:

- A **diagram** of this setup.
- A **PowerShell**, **Azure CLI**, or **Bicep** version of the demo.
- To change the scenario (e.g., Contributor role, nested management groups, etc.).