# Identity & Access Management (IAM)

Identity and Access Management (IAM) in Azure

Azure Identity and Access Management (IAM) is responsible for managing **who has access** to Azure resources and **what actions** they can perform. Key IAM concepts include **policies, roles, and permissions**:

## 1. IAM Policies, Roles, and Permissions in Azure

### Policies

- Policies in Azure govern the security and compliance requirements of resources.
- They are defined using **Azure Policy** to enforce standards (e.g., only allowing specific regions for deployment).
- Policies are not directly used to assign access but control what users and resources can or cannot do.

### Roles

- Roles define **what actions** users or groups can perform on Azure resources.
- Azure provides **built-in roles**, but **custom roles** can be created for specific needs.
- Example roles:
    - **Owner** – Full access, including permissions management.
    - **Contributor** – Can create and modify resources but cannot assign roles.
    - **Reader** – Can view resources but cannot modify them.
    - **User Access Administrator** – Can manage access but cannot modify resources.

### Permissions

- Permissions define **specific actions** (e.g., read, write, delete) users can perform within a role.
- Permissions are grouped into **roles**, which are then assigned to users, groups, or service principals.

## 2. Multi-Factor Authentication (MFA) in Azure

- **MFA** enhances security by requiring users to provide **two or more verification factors** to access Azure resources.
- Authentication methods include:
    - Password + **SMS code**
    - Password + **Authenticator app**
    - Password + **Biometric authentication**
- It helps **mitigate phishing, brute-force attacks, and unauthorised access**.

## 3. Role-Based Access Control (RBAC) in Azure

- **RBAC** is a mechanism to **control access** to Azure resources based on assigned roles.
- Instead of giving broad permissions, **RBAC follows the principle of least privilege**:
    - Assign **only the required access** for a user, group, or application.
- **RBAC components**:
    - **Security principal** – Users, groups, service principals, or managed identities.
    - **Role definition** – A collection of permissions (e.g., Reader, Contributor).
    - **Scope** – Specifies **where** the role is applied (e.g., subscription, resource group, or individual resource).
    - **Role assignment** – Binding of a security principal to a role at a specific scope.

**RBAC Example:**

If a user needs to manage VMs but not change networking settings:

- Assign **Virtual Machine Contributor** role at the resource group level.

### Summary

| Feature | Description |
|---|---|
| **IAM Policies** | Define security and compliance rules. |
| **IAM Roles** | Define what actions users can perform on resources. |
| **Permissions** | Control specific actions within a role. |
| **MFA** | Adds an extra security layer via two-step authentication. |
| **RBAC** | Assigns roles and limits permissions to follow the least privilege principle. |

This document provides a concise overview of IAM, RBAC, and MFA in Azure. For practical implementations, users can explore **Azure Portal, CLI, or PowerShell** for setting up IAM policies, role assignments, and MFA enforcement.

## Step-by-Step Guide to Setting Up IAM Roles and Policies in Azure

### Step 1: Sign in to Azure Portal

1. Go to Azure Portal and log in with your credentials.
2. Navigate to **Azure Active Directory** from the left menu.

### Step 2: Create a Custom IAM Role (Optional)

1. Go to **Azure Active Directory > Roles & administrators**
2. Click **+ Add > New custom role**
3. Provide a **role name** and **description**
4. Click **Permissions > Add permissions**
5. Select a **resource provider** (e.g., `Microsoft.Compute` for Virtual Machines)
6. Choose specific **actions** (e.g., `Microsoft.Compute/virtualMachines/read`)
7. Click **Review + Create** to save the role.

🔷 **Purpose:** Custom roles allow precise control over what a user can do, ensuring security and compliance.

**Step 3: Assign a Built-in Role to a User**

1. Navigate to **Subscriptions** or **Resource Groups**
2. Select the **resource** where you want to assign permissions.
3. Click on **Access control (IAM)**
4. Click **+ Add > Add role assignment**
5. Select a **built-in role** (e.g., `Virtual Machine Contributor`, `Reader`, etc.)
6. Choose **Assign access to:**
   - **User, group, or service principal**
   - Select a user from the list.
7. Click **Review + Assign**

🔷 **Purpose:** Assigning roles based on the least privilege principle prevents unnecessary access.

**Step 4: Configure an IAM Policy for Security**

1. Navigate to **Azure Policy** in the Azure Portal.
2. Click **+ Assign Policy**
3. Under **Scope**, select the Subscription or Resource Group.
4. Choose a **policy definition** (e.g., **Deny Public IP** to restrict public access).
5. Click **Review + Create**

🔷 **Purpose:** Enforcing policies ensures compliance and enhances security by restricting actions.

**Step 5: Enable Multi-Factor Authentication (MFA)**

1. Navigate to **Azure Active Directory > Security > Conditional Access**
2. Click **+ New policy**
3. Set the name (e.g., "Require MFA for Admins")
4. Under **Assignments**, choose **Users and Groups**
5. Select **All users** or specific admin roles
6. Under **Access Controls**, enable **Require Multi-Factor Authentication**
7. Click **Enable Policy > Create**

🔷 **Purpose:** MFA adds an extra layer of security, preventing unauthorised access.