
🧩 Microsoft Entra Identity & Access Management

1. ✅ Overview

- Create and manage **users, groups, and roles**
- Implement **Multi-Factor Authentication (MFA)**
- Configure **Conditional Access Policies**
- Manage **Azure AD roles** and **RBAC**
- Implement **identity protection features**
- Set up **hybrid identity** with on-prem Active Directory

---

2. 🧠 Key Concepts

- **Users and Groups**: Manage access at scale by assigning roles to groups instead of individuals.
- **Azure AD Roles**: Provide control over identity management (e.g., Global Administrator, User Administrator).
- **RBAC (Role-Based Access Control)**: Grant access to Azure resources based on roles (e.g., Contributor, Reader).
- **MFA (Multi-Factor Authentication)**: Adds a second layer of authentication.
- **Conditional Access**: Enforce policies like "Require MFA if accessing from an untrusted location."
- **Hybrid Identity**: Sync on-prem Active Directory users with Azure AD using **Azure AD Connect**.

---

3. 💡 Real-World Scenarios

🔹 Scenario 1: User Management and Role Assignment

Your organization hires 10 developers. You need to give them access to deploy resources in a specific resource group without giving them access to other parts of the subscription.

Solution:

- Create a group “Dev-Team”
- Add the 10 users
- Assign the **Contributor** role to the group on the specific resource group

Command:

az role assignment create --assignee "<group-object-id>" --role "Contributor" --scope "/subscriptions/<sub-id>/resourceGroups/<rg-name>"

🔹 Scenario 2: Secure Admin Access with MFA

You notice failed login attempts on admin accounts from unusual locations. You want to protect global admins with MFA.

Solution:

- Enable MFA for admin roles
- Create a Conditional Access Policy that targets users in the "Global Administrator" role and requires MFA

🔹 Scenario 3: Sync On-Prem Users to Azure

A company uses an on-prem Active Directory. They want to allow existing users to log in to Azure with the same credentials.

Solution:

- Install **Azure AD Connect**
- Enable **Password Hash Sync** or **Pass-through Authentication**

---

4. 🔧 Common Commands & Portal Steps

Create User:

```
az ad user create --display-name "John Doe" --user-principal-name "john@contoso.com" --password "StrongP@ssword!"
```

-

Create Group:

```
az ad group create --display-name "Dev-Team" --mail-nickname "devteam"
```

-

Assign Role via RBAC:

```
az role assignment create --assignee "<user-or-group-id>" --role "Reader" --scope "/subscriptions/<sub-id>"
```

-
- **Enable MFA via Conditional Access (Portal)**:
    - Go to **Microsoft Entra admin center**
    - Conditional Access > New policy
    - Assign users/roles > Assign cloud apps > Conditions (e.g., location) > Grant: Require MFA

---

5. 📝 Exam Tips

- Know the difference between **Azure AD roles** (for identity) and **Azure RBAC roles** (for resource access).

- Practice **Conditional Access scenarios** and what happens when users meet or don't meet the conditions.
- Expect drag-and-drop questions about assigning access using groups, roles, and scopes.
- Be familiar with **Azure AD Connect** setup and syncing methods.
- Understand the **break-glass account** concept (MFA-exempt emergency account).
