Azure Active Directory (Azure AD)

What is Azure AD?

- Azure Active Directory is the cloud identity and access management service from Microsoft.

- It enables organizations to manage users, groups, and permissions for secure access to applications and resources.

Key Features:

✅ Single Sign-On (SSO) – Users can log in once and access multiple applications.
✅ Conditional Access – Enforce security policies based on location, device, and risk levels.
✅ Seamless Integration – Works with Microsoft 365, SaaS apps, and on-prem AD.

Practical Example: Add a User to Azure AD

Step 1: Create a New User

```
az ad user create \
    --display-name "XYZ" \
    --user-principal-name  XYZ@yourdomain.com \
    --password "MySecurePassword123"
```

Step 2: List All Users in Azure AD

```
 az ad user list --output table
```

Step 3: Add a User to a Group

```
az ad group create
--display-name "Developers"
--mail-nickname "DevelopersGroup"

az ad group member add
--group "Developers"
--member-id XYZ@yourdomain.com
```

✅ Use case: Secure Management of User Access to Applications.

2. Role-Based Access Control (RBAC)

What is RBAC?

Role-Based Access Control (RBAC) enables providing specific permissions to users, groups, or applications based on roles.

Key RBAC Roles in Azure:

Owner - has full rights to use the resources assigned.

Contributor -can create and manage resources but cannot assign roles.

Reader -can view the resources.

How it works: Assigning an RBAC role

Step 1: Assignment of Contributor Role to a User

```
az role assignment create
--assignee XYZ@yourdomain.com \
--role Contributor \
--scope /subscriptions/<subscription-
id>/resourceGroups/MyResourceGroup
```

Step 2: Verify User's Assigned Roles

```
 az role assignment list
--assignee XYZ@yourdomain.com
--output table
```

✅ Use Case: Verify that users have the appropriate level of access to resources.

3. Multi-Factor Authentication (MFA)

What is MFA?

MFA adds a layer of security in that the system requires an additional verification method beyond a password.

This might include an SMS code or the Authenticator app.

How to turn on MFA in Azure AD

Step 1: Enable MFA for a User

```
      az ad user update \
    --id XYZ@yourdomain.com \
    --force-change-password-next-sign-in true
```

Step 2: Configure MFA Settings in Azure Portal

-> Azure Portal → Azure AD → Security → MFA
-> Enable MFA per user and enforce authentication methods.

✅Use Case: Adding an extra step for authenticating sensitive resources.

Comparison: Azure AD, RBAC, MFA

Feature	Azure AD	RBAC	MFA
Purpose	User identity management	Access control for resources	Extra security for user login
Use Case	Managing users and groups	Assigning permissions	Preventing unauthorized access
Implementation	Cloud-based directory	Role assignments per resource	Requires authentication setup