🧩 Microsoft Entra ID – Overview (AZ-104)

✅ 1. What is Microsoft Entra ID?

Microsoft Entra ID is Microsoft's **cloud-based identity and access management (IAM)** service. It is the **backbone of authentication and authorization** in Azure, Microsoft 365, and other cloud services.

It allows administrators to:

- Authenticate users and devices
- Manage access to apps and resources
- Enforce security controls like MFA
- Support hybrid identity (on-prem + cloud)

> 📌 Formerly known as **Azure Active Directory (Azure AD)**. Now it's rebranded as **Microsoft Entra ID** as part of the Entra product family.

🧠 2. Key Features Relevant to AZ-104

Feature	Description
Users & Groups	Create/manage identities and group them for access control
Azure RBAC Integration	Assign roles like Reader, Contributor, etc. to users/groups
MFA (Multi-Factor Authentication)	Add extra security using phone/email/apps
Conditional Access	Create policies to enforce MFA, block risky logins, etc.

Device Management	Control which devices can access resources
Hybrid Identity	Sync on-prem Active Directory with Azure using Azure AD Connect
Service Principals & Managed Identities	Allow apps/scripts to authenticate securely

---

💡 3. Real-World Scenarios (AZ-104)

🔹 Scenario 1: Give Developers Access to a Resource Group

A team of developers needs Contributor access to a specific resource group but **not** to the entire subscription.

Solution:

- Create a group in **Microsoft Entra ID**
- Add developers to the group
- Assign the **Contributor** role at the **resource group level** using RBAC

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

🔹 Scenario 2: Enforce MFA for Admins

Security team wants to ensure that all Global Administrators are protected with MFA.

Solution:

- Create a **Conditional Access policy**
- Target users in the **Global Administrator** role
- Require MFA when accessing cloud apps

🔹 **Scenario 3: Hybrid Identity**

Your organization uses on-prem Active Directory and wants users to use the same credentials in Azure.

Solution:

- Deploy **Azure AD Connect**
- Sync on-prem users to **Microsoft Entra ID**
- Enable **Password Hash Sync** or **Pass-through Authentication**

🧰 4. Key Portal Areas & Tools

Portal Area	Purpose
Microsoft Entra Admin Center	Manage Entra ID users, groups, roles, MFA, and devices
Azure Portal → Access control (IAM)	Assign RBAC roles using Entra ID identities
Azure AD Connect (on-prem)	Set up hybrid identity with sync options
PowerShell / CLI	Automate user and role management

🧪 5. Sample AZ-104 Question

> **Q:** You need to allow a group of support engineers to reset passwords for other users in the organization. What should you do?

A. Assign them the Owner role on the subscription
B. Assign them the Password Administrator role in Microsoft Entra ID
C. Add them to the Global Administrator role
D. Create a Conditional Access policy

✅ **Correct Answer: B** — the **Password Administrator** role allows users to reset passwords without full admin access.

📝 6. Exam Tips

- Know the **difference** between:
  - **Azure roles (RBAC)** – for managing access to Azure resources
  - **Entra ID roles** – for managing identities (e.g., Global Admin, User Admin)
- Practice **Conditional Access** setup and MFA enforcement
- Understand **RBAC scopes**: Subscription, Resource Group, Resource
- Expect questions around **syncing users** from on-prem to cloud
- Know how to manage **service principals** and **managed identities**

🔁 Summary Table

Capability	Where It Happens
User creation	Microsoft Entra Admin Center / CLI
Group-based access	Microsoft Entra ID + Azure RBAC
MFA	Enforced via Conditional Access
Hybrid identity	Azure AD Connect
App identity (automation)	Managed Identities / Service Principals

---