What is Microsoft Entra?

Microsoft Entra is Microsoft's family of identity and access management (IAM) solutions. It includes Azure Active Directory (Azure AD), Entra Permissions Management, Entra Verified ID, and more.

Entra RBAC Overview

Within **Microsoft Entra**, **RBAC** primarily manages access to identity and access management features and resources across Microsoft cloud services. It controls **who can perform what actions on Entra resources**, such as managing users, groups, applications, or permissions.

Key Concepts in Microsoft Entra RBAC

- **Roles:** Predefined or custom roles that contain a set of permissions.
- **Assignments:** Roles are assigned to users, groups, or service principals.
- **Scope:** Roles apply at different levels—tenant-wide, specific application, or resource-specific.

Built-in Entra Roles Examples

- **Global Administrator:** Has access to all administrative features in Entra (Azure AD).
- **User Administrator:** Can manage users and groups but limited in other admin tasks.
- **Application Administrator:** Manages application registrations and enterprise apps.
- **Security Administrator:** Manages security policies and reports.
- **Privileged Role Administrator:** Manages role assignments in Entra.

Privileged Identity Management (PIM)

Microsoft Entra integrates with **Azure AD Privileged Identity Management (PIM)** for RBAC, which adds:

- **Just-in-time role activation:** Users activate roles only when needed.
- **Time-bound access:** Temporary role assignments with expiration.
- **Approval workflows:** Role activation can require approval.
- **Access reviews and audits:** Regular review of role assignments for security compliance.

How Entra RBAC Works

1. **Define roles** with specific permissions related to identity and access management.
2. **Assign roles** to users, groups, or service principals in your tenant.
3. Users gain those permissions within the scope (tenant or specific apps/resources).
4. Entra enforces these permissions when users attempt actions.

Why Use Entra RBAC?

- **Centralized identity management:** Control who manages identities and access.
- **Security:** Limit administrative privileges to reduce risk.
- **Compliance:** Track and audit admin actions.
- **Granular control:** Assign narrowly scoped permissions.

Example

Role	Permissions	Typical Use Case
Global Administrator	Full access to all Entra and Azure AD features	Tenant-wide admin
Application Administrator	Manage app registrations and enterprise apps	DevOps or app owners
User Administrator	Create and manage users and groups	HR or support teams

---