

# 1- AD(Active Directory)

- [RBAC](#)
- [Multi Factor Authentication](#)
- [Azure AD Identification Protection](#)
- [Conditional Access](#)

---


Azure **Active Directory** (Azure AD) is Microsoft's cloud-based identity and access management service that allows organizations to manage and secure user identities and access to applications and resources in the Azure ecosystem.

An **Azure tenant** is a dedicated and isolated instance of the Azure Active Directory (Azure AD) service, which represents an organization's identity and access management environment within the Azure cloud. It is a distinct organizational boundary that contains users, groups, applications, and policies specific to that organization's Azure resources and services.

- So Basically Azure AD is serving more than one customer.
- and each customer is know to be a tenant.
- Every tenant is isolated to each other.
- one tenant cannot see the data of another tenant.

- 
- main function of Active Directory is **Authorization**.
  - When Active Directory is installed in a server. That server can be called as **DC (Domain Controller)**.
  - DC creates a Logical boundary.

---

 [https://www.youtube.com/watch?v=mVV\\_40\\_QPI0&list=PLUGuCqrhcwZzht4r2sbByidApmrvEjL9m&index=3&pp=iAQB](https://www.youtube.com/watch?v=mVV_40_QPI0&list=PLUGuCqrhcwZzht4r2sbByidApmrvEjL9m&index=3&pp=iAQB)

---

Account creation

↓

Directory will be created (Default Directory or **Tenant**)

↓

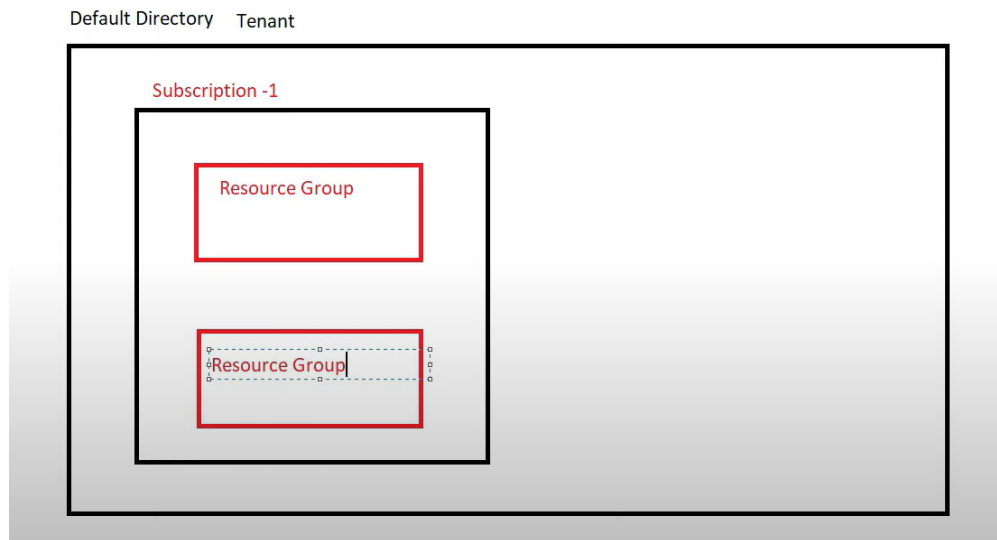
Subscription



Resource Group




Resource



---

## RBAC

RBAC -  <https://www.youtube.com/watch?v=Lpm0v8jojRw&list=PLUGuCqrhcwZzht4r2sbByidApmrvEjL9m&index=5&pp=iAQB>

---

## Multi Factor Authentication

MFA -  <https://www.youtube.com/watch?v=rCD3YXGdgqM&list=PLUGuCqrhcwZzht4r2sbByidApmrvEjL9m&index=6&pp=iAQB>

- enables multi layer of authentication.
- provides an extra layer of security.

---

## Azure AD Identification Protection

- Identification means user account

- Protecting the user account from external attack.
  - Protection, detection, remediation's are automatically done.
  - We can create 3 kinds of policies using identity protection.
1. User risk policy (protection for compromised passwords).
    1. **mitigations**  
making a user to change password forcefully.
  2. Sign-in policy (related to sign-in's).
    1. **mitigations**  
will block anonymous users.
  3. MFA registration policy (makes a particular or group to register to MFA).
- 

## Conditional Access

- allows to access only when certain conditions are matched.
-