Microsoft Entra ID
(Prev. Azure Active Directory)

Cloud based Identity & Access management
(IAM)

- ↳ manage identities
- ↳ Enforce Access
- ↳ secures application & data

In cloud
onprem

Runs as service on Windos server as Domain Controller (Active Directory Domain services)

↳ ADDS ~~deos~~ does not have

- ↳ MFA
- ↳ Identity protection
- ↳ Self password reset

Used for

- Identity Managemen
- Configure SSO
- Enabling federation betwen Org.
- Identifying irregular sign-in activity
- MFA
- Extending on-prem AD to Entra ID
- Conditional access
- Configuring Application proxy for cloud & local apps.

Ms Entra ID

Available as

- free tier included in - Office 365 - Intence
- P1
  - MFA
  - Conditional Access
  - Self service group & Password reset
  - Cloud discovery
  - Connect health
- P2
  - P1 +
  - Risk & sign-in policies
  - Additional Security levels for Privileged users
    - Permanent & Temporary admin

Multiple Entra tenants possibe In each subscription.

- Useful for Dev | QA envs.

One Entra tenant can be linked to multiple Azure subscriptions to use same users, groups, applications to manage resources across subsiptions.

ADDS

Entra ID

- "Does not have "Computer class"
  - Does not support Group Policy objects (GPOs)
  - Does not have Org unit (OU)

OUs = Group membership

Objects of Applications Service principa = Applications

Characteristics of AD DS

AD DS

- traditional deployment of Windows Server-based Active Directory on a physical or virtual server.
- includes
  - Active Directory Certificate Services (AD CS),
  - Active Directory Lightweight Directory Services (AD LDS),
  - Active Directory Federation Services (AD FS), and
  - Active Directory Rights Management Services (AD RMS).
- true directory service, with a hierarchical X.500-based structure.
- uses Domain Name System (DNS) for locating resources such as domain controllers.
- You can query and manage AD DS by using Lightweight Directory Access Protocol (LDAP) calls.
- primarily uses the Kerberos protocol for authentication.
- uses OUs and GPOs for management.
- includes computer objects, representing computers that join an Active Directory domain.
- uses trusts between domains for delegated management.

Microsoft Entra ID is

- primarily an identity solution, and it's designed for internet-based applications by using HTTP (port 80) and HTTPS (port 443) communications.
- multi-tenant directory service.
- Microsoft Entra users and groups are created in a flat structure, and there are no OUs or GPOs.
- You can't query Microsoft Entra ID by using LDAP; instead, Microsoft Entra ID uses the REST API over HTTP and HTTPS.
- Microsoft Entra ID doesn't use Kerberos authentication; instead, it uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication, and uses OAuth for authorization.
- Microsoft Entra ID includes federation services, and many third-party services such as Facebook are federated with and trust Microsoft Entra ID.

Ms Entra Domain Services

- Alternative to linking | replicating ADDS to cloud instance
- Runs as part of Entra ID P1 / P2 service
  - ↳ Group policy management
    Domain joining
    Kerberos auth

Use Ms Entra Connect to link Entra ID and ADDS.

Microsoft Entra Domain Services-

- freely migrate applications that use LDAP, NTLM, or the Kerberos protocols from your on-premises infrastructure to the cloud
- Microsoft SQL Server or Microsoft SharePoint Server on VMs or deploy them in the Azure IaaS, without needing domain controllers in the cloud or a VPN to local infrastructure.

current limitations-

- Only the base computer Active Directory object is supported.
- It’s not possible to extend the schema for the Microsoft Entra Domain Services domain.
- The organizational unit (OU) structure is flat and nested OUs aren't currently supported.
- There’s a built-in Group Policy Object (GPO), and it exists for computer and user accounts.
- It’s not possible to target OUs with built-in GPOs. Additionally, you can't use Windows Management Instrumentation filters or security-group filtering.