5- Entra ID, ADDS, Windows AD

Questions

- [ ] what are domain controllers?
- [ ] Why do we need domain controllers if we have Azure AD (Entra ID).

Previous Name	New Name
Azure AD	Microsoft Entra ID
Azure AD Domain Services	Microsoft Entra Domain Services
Azure AD Connect Sync	Microsoft Entra Connect Sync
Azure AD Verifiable Credentials	Microsoft Entra Verified ID
Azure AD Activity Logs	Microsoft Entra Activity Logs
Azure AD B2B	Microsoft Entra B2B
Azure AD Conditional Access	Microsoft Entra Conditional Access
Azure AD MFA	Microsoft Entra MFA

- `#Entra_ID` supports modern authentication protocols like `#OAuth_2`, `#Open_ID_Connect`, and `#SMAL`.
- ! There are 3 Domain services

1. Windows Active Directory Domain Services (Windows AD)
2. Azure Active Directory (Azure AD)
3. Azure Active Directory Domain Services (Azure ADDS)

These different services provide different authentication services.

Windows AD

- installed Active directory domain services installed on a `#domain_controller` running on a windows server OS.

Features of Windows AD

- Objects are stored as hierarchical directory.
- Stores users, groups, and security principles
- can use Group policies for users and device management
- Highly available, multi-master which means there is no one master domain controller.
- Supports Network based Authentication protocols like `#Kerberos`, `#LDAP`, `#NTLM`.

- Based on the standards like `#LDAP` and `#DNS`.
- requires dedicated server as a domain controller.

Azure AD

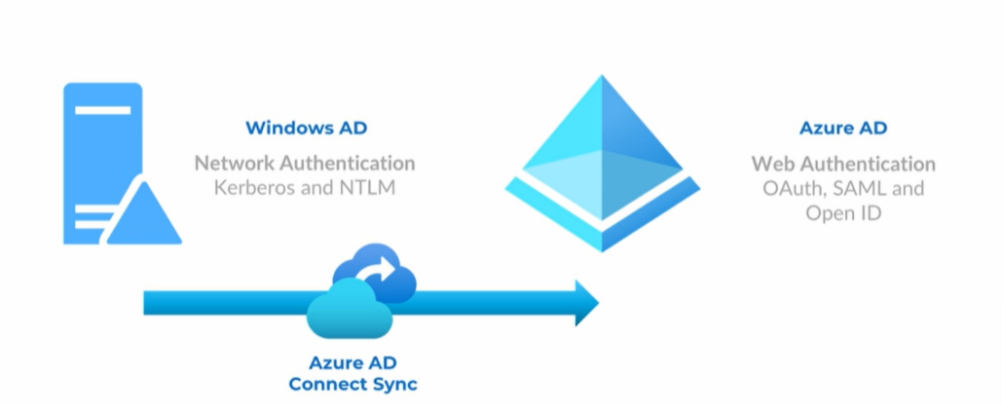
used to manage identity and access management in azure.

Features of Entra ID

- Cloud based identity solution
- contains users, groups and security principles …
- Uses web based Authentication protocols like `#OAuth`, `#SAML`, and `#Open_ID`.
- It is multi-tenant meaning the services are shared securely with other organizations.
- Flat architecture.
- Not extendable means attributes cannot be added
- No group policies
- 3 licence options
  - Free
  - P1
  - P2
- Tenant based

Azure AD connect Sync

to not manage identities in two locations, we use `#AD_Connect_Sync` to sync identities of Windows AD to Azure AD



ADDS

- PaaS service
- There are two forests present in Azure ADDS
  - `#user_forest`
  - `#resource_forest`

User

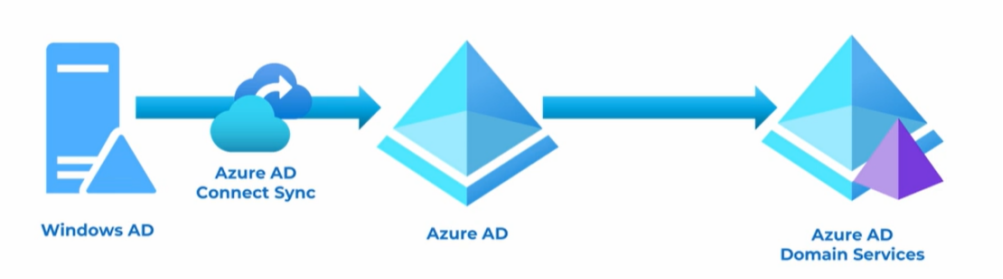
- Synchronize objects from Azure AD
- Works with password has synchronization

Resource

- Does not Synchronize users from Azure AD
- One-way trust for authentication

Features of ADDS

- Cloud based PaaS
- LDAP, Kerberos, NTLM
- Compatible with Windows AD
- Integrates with Azure AD
- No domain or enterprise account
- Not extendable
- Limited forest trust
- LDAP read-only
- Azure AD is the source for Azure ADDS objects with the user forest type.
- Objects in Azure AD replicated in ADDS
- ADDS is an extension of Azure AD.



Creating a windows AD

```
Domain con name : DC1
Network : 10.10.0.0/16
Admin account : isdomadmin
Win AD domain name : isdomcode.local
```