

Azure Active Directory



Offerings Of This Session

01

What Is Azure AD?

02

Azure AD Vs Windows AD

03

Service Audience

04

Azure AD Editions

05

Azure AD Tenants



Domain Services Overview

Azure AD
(AAD)

Active Directory
Domain Services
(ADDS)

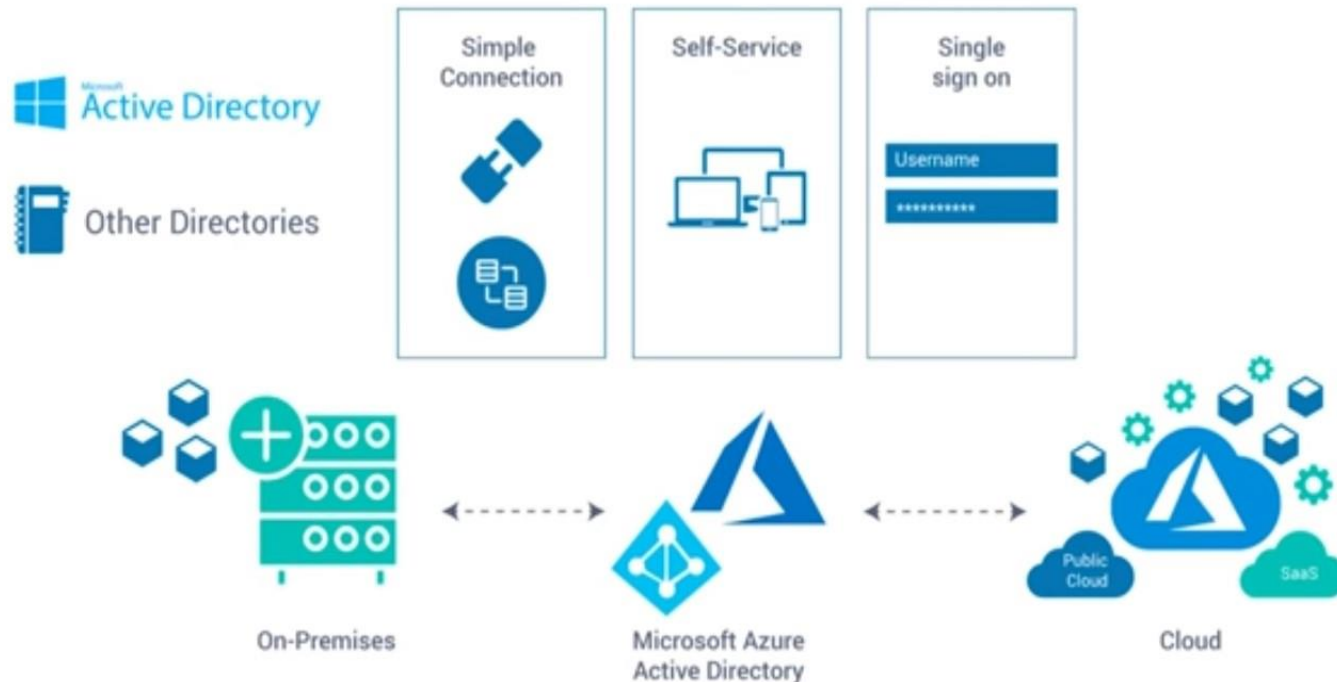
Azure Active
Directory
Domain Services
(AADDs)

WHAT IS AZURE AD?

- Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:
- External resources, such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications.
- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

What Is Azure Active Directory?

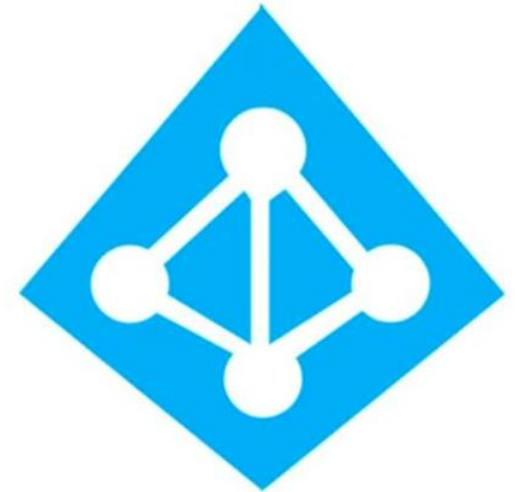
Azure Active Directory (Azure AD) is Microsoft's multi-tenant, cloud-based directory, and identity management service that combines core directory services, application access management, and identity protection into a single solution.



Azure Active Directory

AAD

- Modern AD service built directly for the cloud
- Often the same as O365 directory service
- Can sync with On-premises directory service



Active Directory Domain Services

ADDS

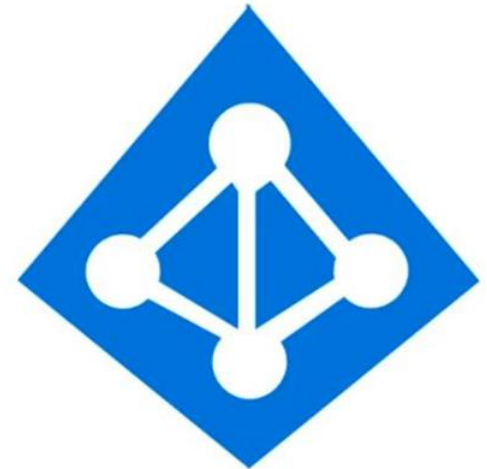
- Legacy Active Directory since Windows 2000
- Traditional Kerberos and LDAP functionality
- Deployed on Windows OS usually on VMs



Azure Active Directory Domain Services

AADDS

- Provides managed domain services
- Allows you to consume domain services without the need to patch and maintain domain controllers on IaaS
- Domain Join, Group Policy, LDAP, Kerberos, NTLM; all supported



	Azure AD Join	Azure AD Domain Services
Authentication	OAuth/OpenID Connect	Kerberos, NTLM
Management	Mobile Device Management (MDM) software like Intune	Group Policy
Networking considerations	Works over the internet	<ul style="list-style-type: none">• Requires machines to be on the same virtual network as the managed domain.• Can use virtual network peering or site-to-site VPNs to extend connectivity.
Great for ...	Windows 10 devices	Server virtual machines deployed in Azure



Windows AD vs Azure AD

Windows AD Vs Azure AD



Active Directory

ADDS

ADLS

ADFS

ADCS

ADRMS



Azure Active Directory

WAAD

Windows Azure Access Control Service



On - Premises AD

- Identity Solution using LDAP and Kerberos
- Not Suitable for internet based application
- Physical server hardware is required

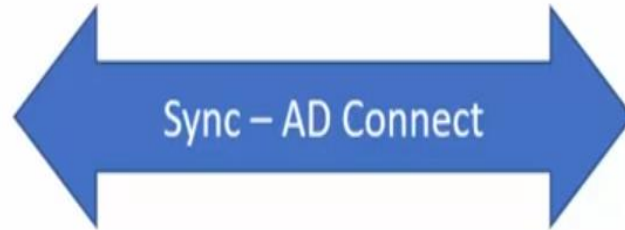


Azure AD

- Identity Solution using HTTP / HTTPS
- For internet based application
- Low cost



On - Premises AD




Azure AD

- | | |
|--|--|
| <ul style="list-style-type: none">• Identity Solution using LDAP and Kerberos• Not Suitable for internet based application• Physical server hardware is required | <ul style="list-style-type: none">• Identity Solution using HTTP / HTTPS• For internet based application• Low cost |
|--|--|

Azure Active Directory Editions



Azure Active
Directory Basic



Azure Active
Directory Premium
1



Azure Active
Directory Premium
2

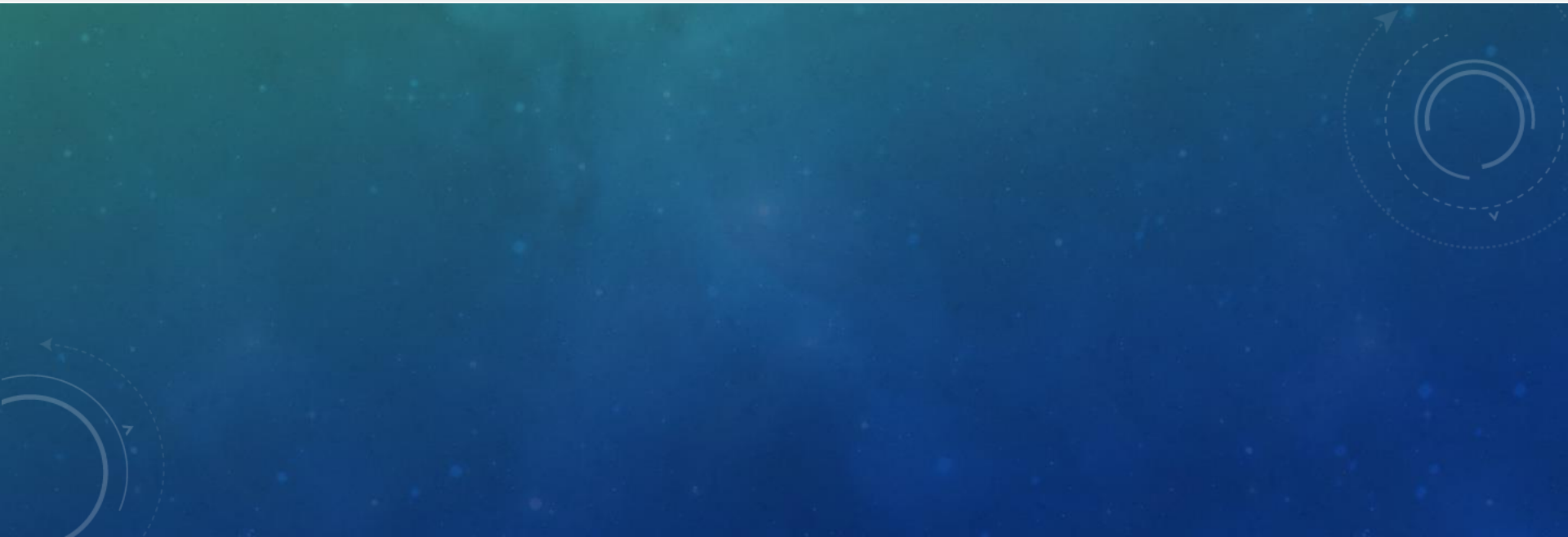
AZURE AD PREMIUMS

- **Azure Active Directory Free**. Provides user and group management, on-premises directory synchronization, basic reports, self-service password change for cloud users, and single sign-on across Azure, Office 365, and many popular SaaS apps.
- **Azure Active Directory Premium P1**. In addition to the Free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
- **Azure Active Directory Premium P2**. In addition to the Free and P1 features, P2 also offers Azure Active Directory Identity Protection to help provide risk-based Conditional Access to your apps and critical company data and Privileged Identity Management to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.
- **"Pay as you go" feature licenses**. You can also get additional feature licenses, such as Azure Active Directory Business-to-Customer (B2C). B2C can help you provide identity and access management solutions for your customer-facing apps. For more information, see Azure Active Directory B2C documentation.

	FREE	OFFICE 365 APPS	PREMIUM P1	PREMIUM P2
Core Identity and Access Management				
Directory Objects ¹	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
Single Sign-On (SSO) (unlimited) ²	✓	✓	✓	✓
User provisioning	✓	✓	✓	✓
Federated Authentication (ADFS or 3rd party IDP)	✓	✓	✓	✓
User and group management (add/update/delete)	✓	✓	✓	✓
Device registration	✓	✓	✓	✓
Cloud Authentication (Pass-Through Auth, Password Hash sync, Seamless SSO)	✓	✓	✓	✓



Azure AD Connect sync (extend on-premises directories to Azure AD)	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓
Azure AD Join: desktop SSO & administrator bitlocker recovery	✓	✓	✓	✓
Password Protection (global banned password)	✓	✓	✓	✓
Multi-Factor Authentication ³	✓	✓	✓	✓
Basic security and usage reports	✓	✓	✓	✓



Premium Features		
Password Protection (custom banned password)	✓	✓
Password Protection for Windows Server Active Directory (global & custom banned password)	✓	✓
Self-service password reset/change/unlock with on-premises write-back	✓	✓
Group access management	✓	✓
Microsoft Cloud App Discovery ⁴	✓	✓
Azure AD Join: MDM auto enrollment & local admin policy customization	✓	✓
Azure AD Join: self-service bitlocker recovery, enterprise state roaming	✓	✓
Advanced security and usage reports	✓	✓

Conditional Access

Conditional Access based on group, location, and device status	✓	✓
Azure Information Protection integration	✓	✓
SharePoint limited access	✓	✓
Terms of Use (set up terms of use for specific access)	✓	✓
Multi-Factor Authentication with Conditional Access	✓	✓
Microsoft Cloud App Security integration	✓	✓
3rd party identity governance partners integration	✓	✓



Identity Governance

Privileged Identity Management (PIM)



Access Reviews



Entitlement Management



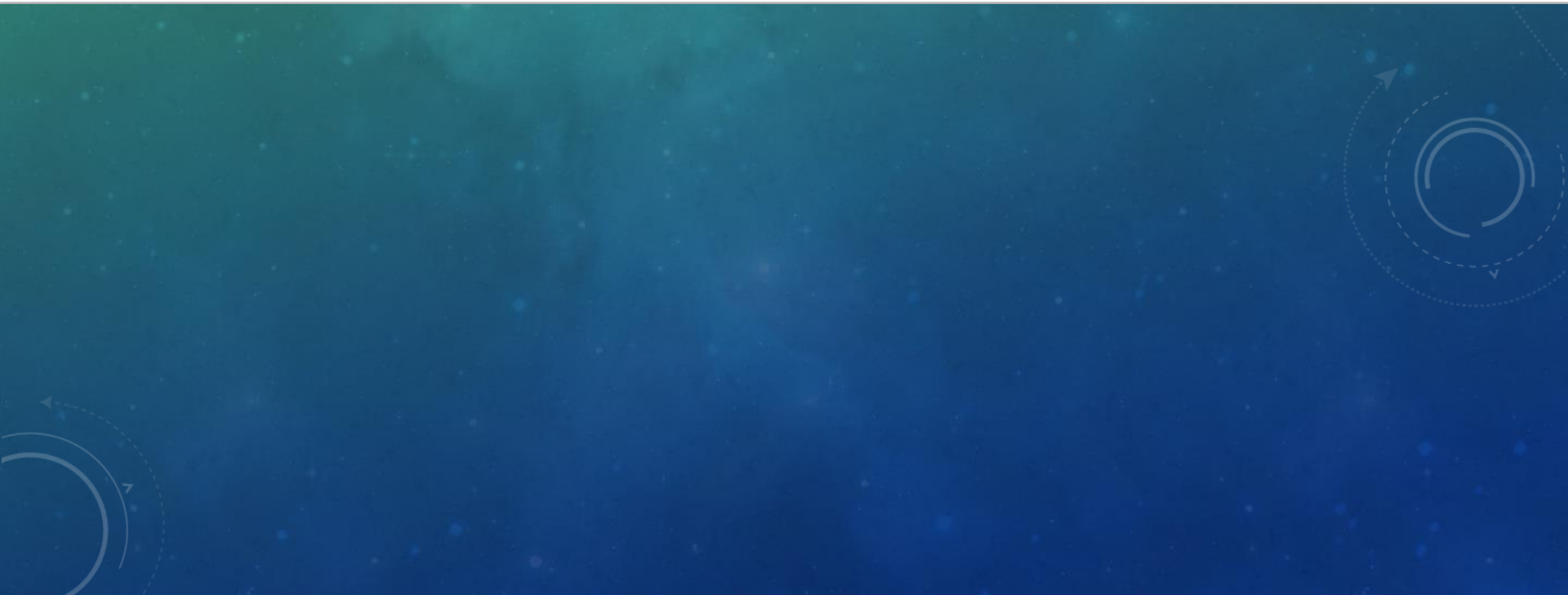
Price

Free

O365 E1, E3, E5, F3

\$6 user/month

\$9 user/month



Data Lake Concepts



Azure Active
Directory Tenants

Tenant means an organisation

It is a dedicated instance of Azure AD service

Microsoft ensures each of these Tenants is
isolated and separate