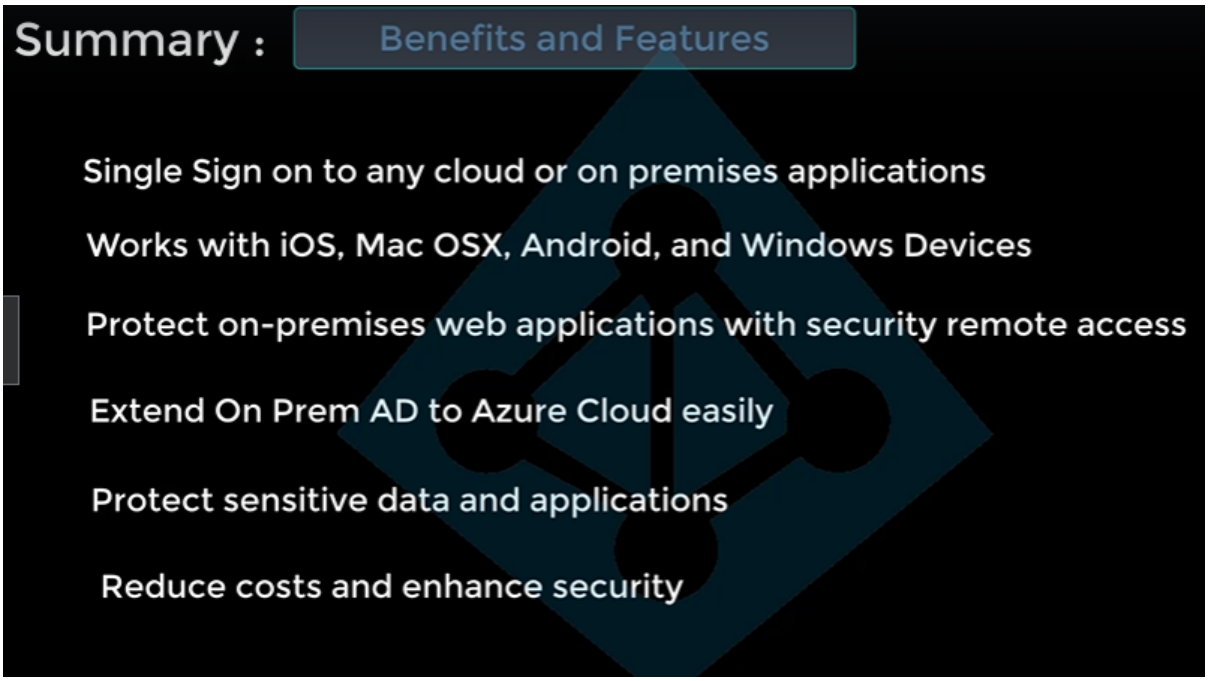
AD

Important keywords

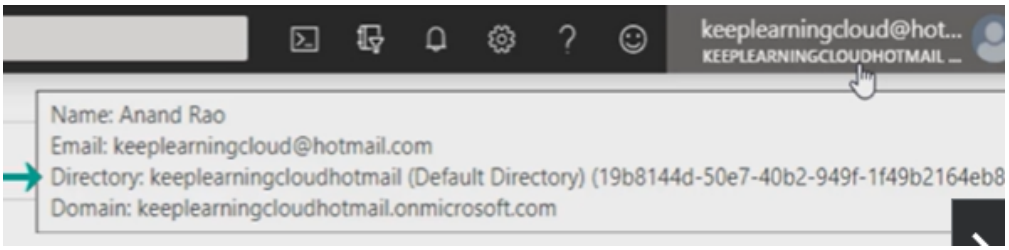
Domain controller	It is a server where you create *users*, *groups*, *organization units*, *group polic* etc.
AD connect	Ad connect will synchronize *on-premises* identities to *Azure AD*.
identity management	is about keeping track of user objects.
access management	is about controlling the way the resources are accessed by the users or identities.
Directory Services	is about storing these objects and resources in a centralized location.
Identity Repository	This is like AD where you would be storing resources like users, computers, service accounts and other user objects.
Identity objects	We mean things that are representing our users and applications.
Delegation	ability to perform an action on behalf of a user

Provisioning	process of creating objects typically done automatically

Benefits and Features



Understanding AAD



- This is a default directory.
- When you create an account an account for yourself in azure, You will get a default directory with standard naming conventions.

Users and groups

creating groups

- In azure active directory you can create two different *types of groups*
  1. Security Groups

2. Office 365 groups

- Entra-Id > Groups > New Group

Membership type

- Direct Assignment - users are directly added to the group.
- Group Assignment - You are adding group to this group. The members of that group will inherit the permissions.
- Rule-Based Assignment - there will be some kind of validation to join this group.

Settings

- General
- Expiration
- Naming Policy

MFA (Multi Factor Authentication)

- Something you know
- Something you are
- Something you have
- Entra-Id > Users > Per user MFA

Authentication Methods

- Call to phone
- Text to phone
- Notification through Mobile App
- Verification code from mobile app

Types of Azure AD Users

Cloud identities

- Identity that is created directly on Azure portal (or) cloud native user accounts.
- These are not synced to on-premises.

Directory Sync identities

- identities that are synced from on-premises to Azure AD are know an Directory Sync identities.

Guests

- When you are working with externals.
- You would like to manage permissions to them to access your VM's.
- The external users can continue to use their Email addresses to access our resources. SO we dont have to create their accounts in azure AD and on-premises

---

Azure AD - Editions

1. free Edition
2. Premium P1
3. Premium P2

Azure AD Domain Join

AD connect

helps to sync the identities in AD(on-premises) to Azure Active directory in the interval of 30 mins.

Azure AD B2B (Business to Business)

- Simplified and streamlined process to connect to Azure AD environment with external environments.

Azure AD B2C (Business to Consumer)

- i want to enable my customer to use some identity to that customer facing app like web app, mobile app.
- This is not about collaboration.
- We cannot give access to the customers to use our azure resources.

Resources : https://youtu.be/U2Temcn-hes

Monitoring azure AD

- Sign-ins
  - risky Sign-ins
  - logs

IAM (Identity and Access Management)

1. Authentication (proving that we are who we say we are)
2. Authorization (the process of granting permissions for the resources or controlling the way of accessing the resources)
3. Protocols (agreed processes, agreed frameworks)

Authentication protocols

1. OAuth 2.0 (Access token)
2. OpenID (ID token)
3. SAML 2.0 (single sign on with A AD)
4. WS-Fed