**Azure AD Session**

**Session I**

1. Active Directory
2. Azure Active Directory
3. Hybrid Model
4. Azure B2B & B2C
5. Lab 1: Sign in Sign Out with azure b2c
6. Lab 2: User flows with azure b2c

**Session II**

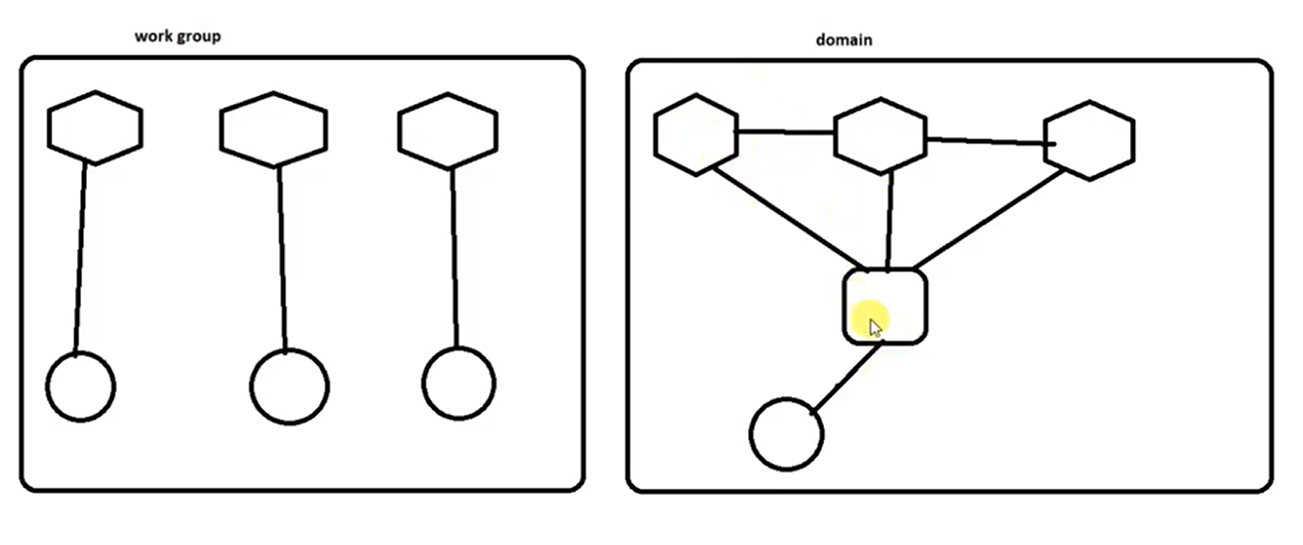
1. OpenID, OAuth, SAML , JWT
2. User roles & MFA
3. MSAL
4. Security
5. SSO Angular App with Distributed API’s

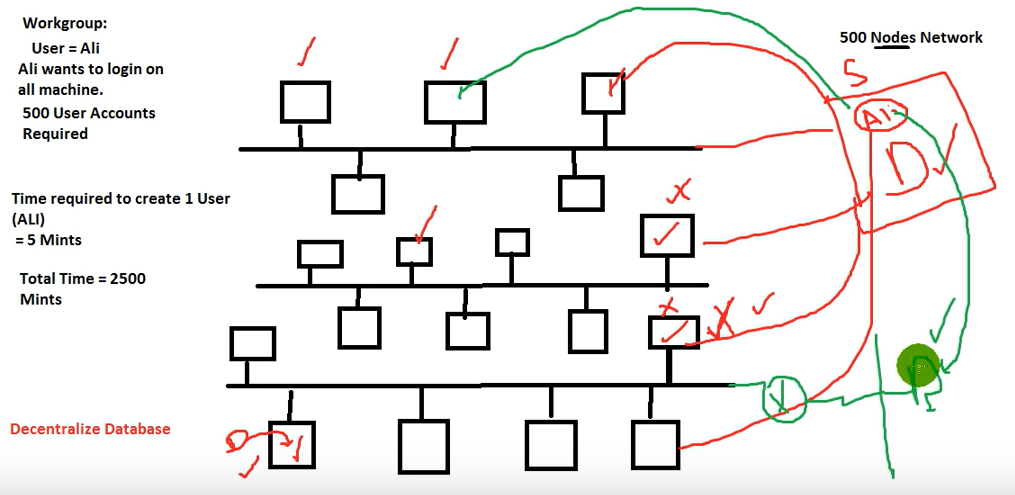
**What Is Active Directory?**

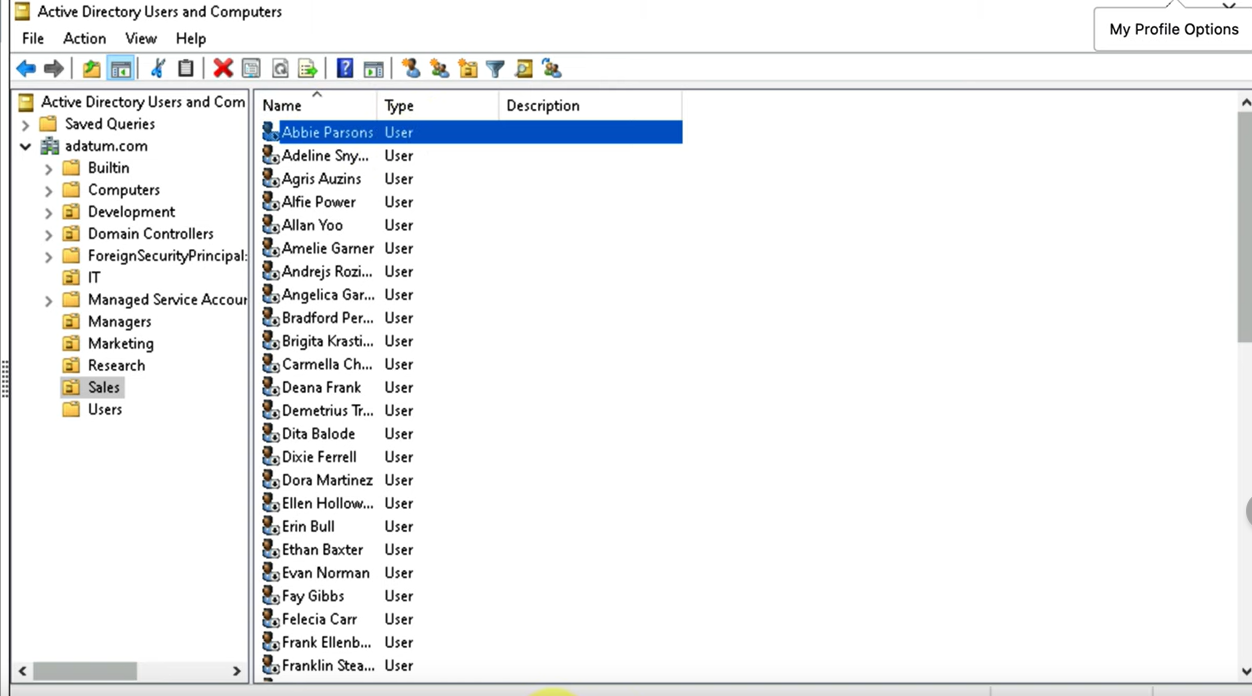
AD stands for Active Directory.  In order to understand what Active Directory is, you’ll need to understand the basics of a Domain Controller.

A Domain Controller is a server on the network that centrally manages access for users, PCs and servers on the network. It does this using AD.

Active Directory is a database that organizes your company’s users and computers. It provides authentication and authorization to applications, file services, printers, and other resources on the network. It uses protocols such as **Kerberos** and **NTLM** for authentication and LDAP to query and modify items in the Active Directory databases.







**What Is Azure AD?**

Microsoft Windows Azure Active Directory (Windows Azure AD or Azure AD) is a [cloud service](https://www.techtarget.com/searchitchannel/definition/cloud-services) that provides administrators with the ability to **manage end-user identities and access privileges**. Its services include core directory, access management and identity protection. As the name implies, Azure AD is part of the [Microsoft Azure](https://www.techtarget.com/searchcloudcomputing/definition/Windows-Azure) public cloud computing platform.

The service gives administrators the freedom to choose which information will stay in the cloud, who can manage or use the information, which services or applications can access the information, and which [end users can have access](https://www.techtarget.com/searchwindowsserver/tip/Using-Azure-AD-conditional-access-for-tighter-security). Azure AD can help to provide single sign-on ([**SSO**](https://www.techtarget.com/searchsecurity/definition/single-sign-on)), so end users don't have to enter passwords multiple times to access cloud applications.

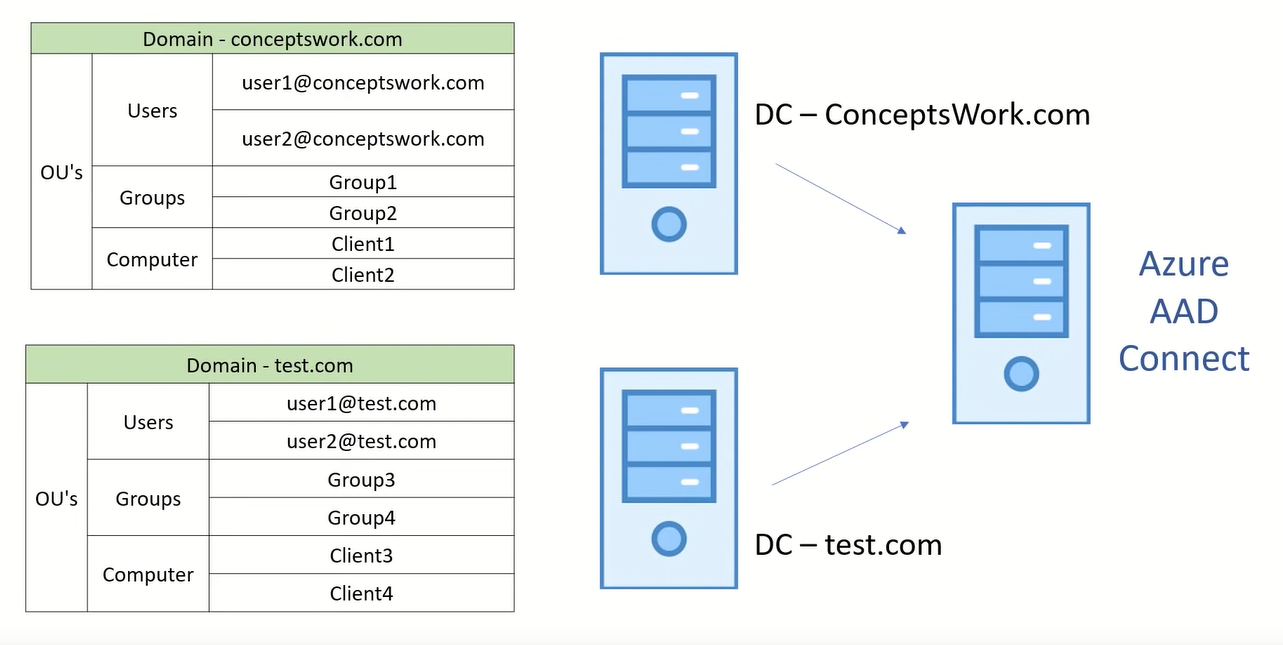
Azure AD is used by IT admins, app developers and Microsoft cloud service subscribers. **IT admins use Azure AD to manage role permissions and control access to specific applications** and resources for individual users. **App developers may use Azure AD to add single sign-on to apps** that work with preexisting user credentials. Azure AD also provides app developers with application program interfaces ([APIs](https://www.techtarget.com/searchapparchitecture/definition/application-program-interface-API)) that use existing data within the organization. Subscribers to Microsoft cloud services, such as Office 365, [Dynamics CRM Online](https://www.techtarget.com/searchcustomerexperience/definition/Microsoft-Dynamics-365) or Azure, are, by default, [tenants](https://www.techtarget.com/searcherp/feature/How-to-make-the-single-tenant-vs-multi-tenant-cloud-ERP-choice) of Azure AD.

**Window AD vs Azure AD?**

* Unlike Windows AD, Azure AD is designed for web-based services. Azure AD supports services that use [**REST**](https://www.techtarget.com/searchapparchitecture/definition/REST-REpresentational-State-Transfer) (Representational State Transfer) APIs for online cloud-based apps such as Office 365.
* Azure AD uses different protocols from Windows AD. Azure AD uses protocols such as **SAML, Open ID and OAuth**.2.0. It does not support NTLM, [Kerberos](https://www.techtarget.com/searchsecurity/definition/Kerberos) or [LDAP](https://www.techtarget.com/searchmobilecomputing/definition/LDAP) (Lightweight Directory Access Protocol).
* Azure AD uses **Azure Policy**, as opposed to [**Group Policy**](https://www.techtarget.com/searchwindowsserver/definition/Group-Policy) in Windows AD.
* Azure AD does not use [OUs](https://www.techtarget.com/searchwindowsserver/definition/organizational-unit-OU) (organizational units) or [forests](https://www.techtarget.com/searchwindowsserver/definition/Active-Directory-forest-AD-forest). It has a flat directory structure.

## What is hybrid identity in the cloud?

As organizations modernize across their on-premises and cloud resources, they must maintain convenient access for their users. A hybrid identity approach synchronizes directories so users can access apps hosted on any cloud or apps that still live on-premises, with full visibility and security controls for IT.



Table

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## Application Proxy?

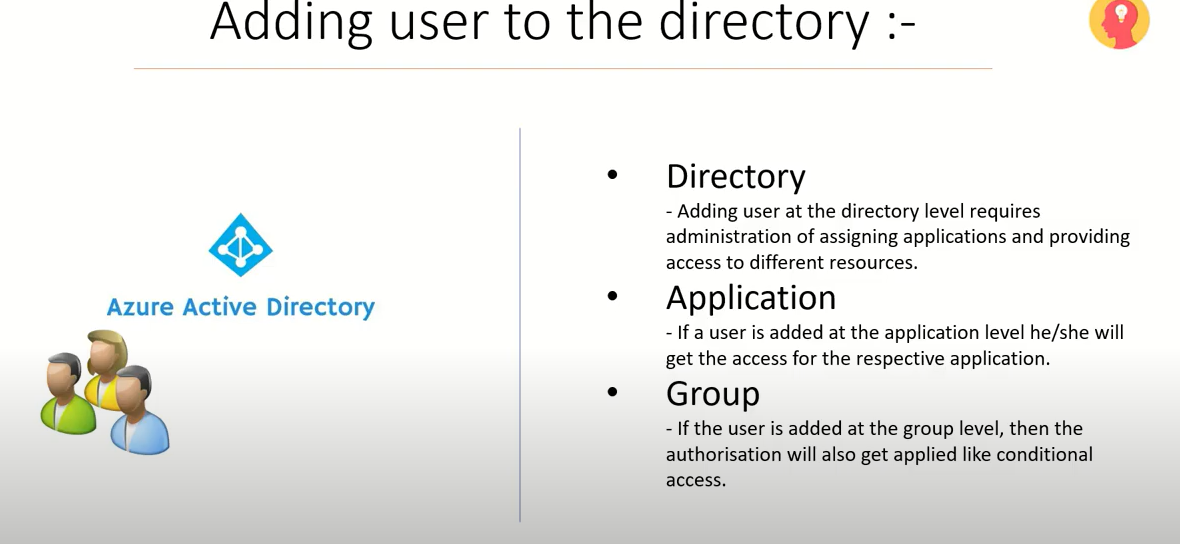
## 

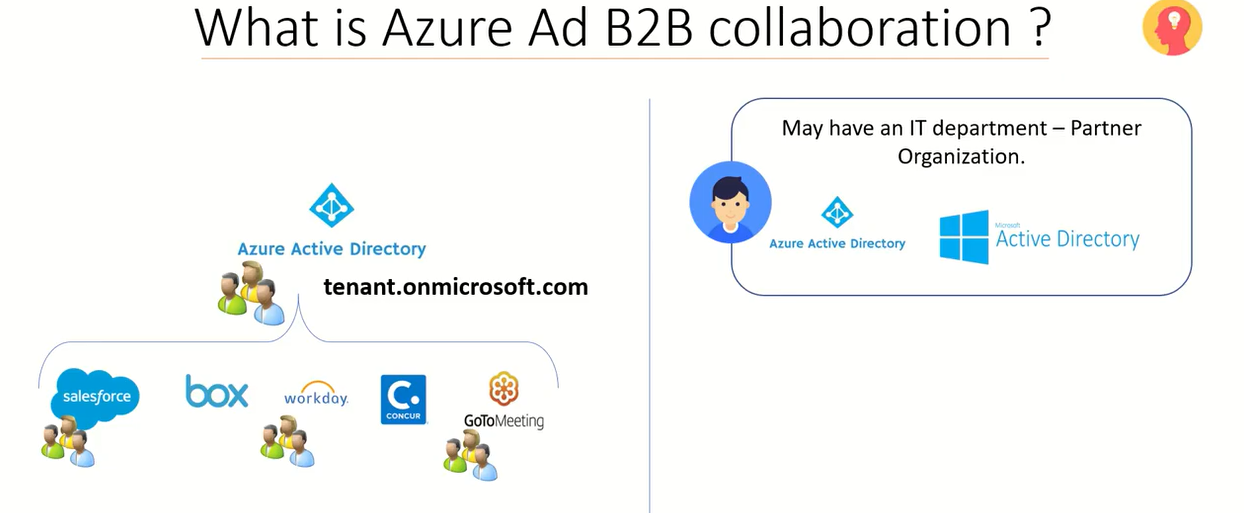
## 

## 

## Users

## 





Graphical user interface, text, application

Description automatically generated

