**AZURE Active Directory**

PoC (Proof Of Concept)

---------------------

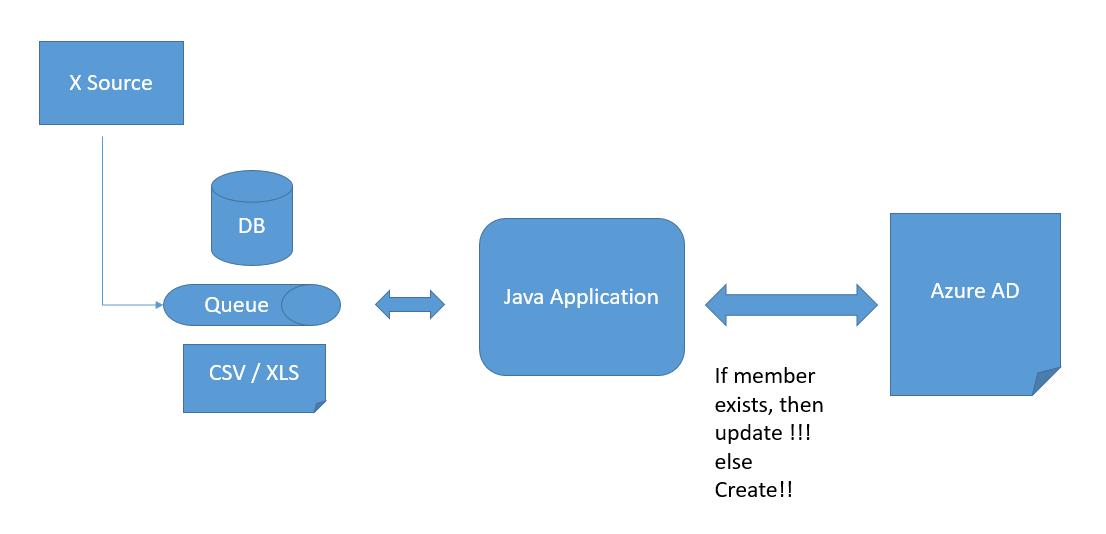
Steps:

1. Create Azure id - Free account - done

close the services as soon as you are over with it – log out

2. Azure Active Directory/AD

* What is this? - done
* How to integrate with Java? - done
* Authentication with AAD using java – done
* Using Java - Authentication checked with 2 AADs – Org1, Org2 – in progress
* How to add members? - done
* How to Remove members? – done
* How to update members? – done



----------Azure AD----------------

Azure Active Directory is Microsoft’s multi-tenant, cloud-based directory and identity management service.

multi-tenant service that provides enterprise level identity and access mngmnt for the cloud.

For an organization, Azure AD helps employees sign up to multiple services and access them anywhere over the cloud

with a single set of login credentials.

In Azure Active Directory (Azure AD), authentication involves more than just the verification of a username and password. To improve security and reduce the need for help desk assistance, Azure AD authentication includes the following components:

- Self-service password reset

- Azure AD Multi-Factor Authentication

- Hybrid integration to write password changes back to on-premises environment

- Hybrid integration to enforce password protection policies for an on-premises environment

- Passwordless authentication

Properties file – (application.yml)

azure:

activedirectory:

tenant-id: 525acd43-e1d1-4070-8ebb-2801d916e63d

client-id: 369af494-b854-4218-913d-d43c9a63275f

client-secret: oEA7Q~AZ99AXcDzOBMvKDkLOyd6BNcZRC45xv

user-group:

allowed-groups: group1

client-

id, secret, scope, consent, token

Azure key vault - to store the passwords

Default directory – test user – pass - User@12345

Org1 – test user –

Id - test@domainex1.onmicrosoft.com

pass - %+@GL&@333dW!Uq

creating user

Id – test2@domainex1.onmicrosoft.com

pass - %+@TS&@333dW!Uq

azure:

activedirectory:

# Specifies your Active Directory ID:

tenant-id: 8d6e41cc-6198-4a72-9015-171b7220d27e

# Specifies your App Registration's Application ID:

client-id: 61a85a32-99ff-4b7a-b522-b940430d9402

# Specifies your App Registration's secret key:

client-secret: DzW7Q~UOP6vjXLdh.txVYkAIqT-KQgp2dA2YR

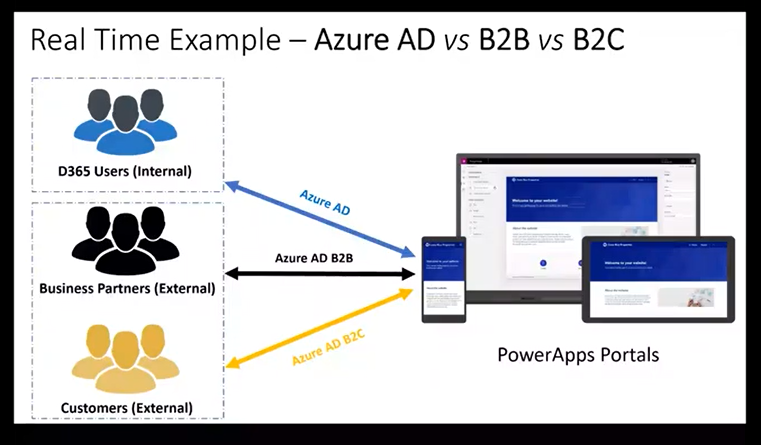
QHZ8Q~wwYHvlEVi70~-YOKWOGCOSEAwv5Zk3edt0

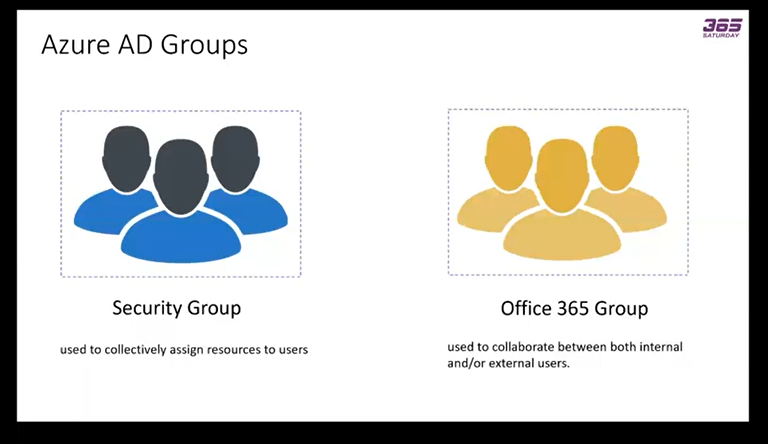
# Specifies the post-log-out-redirect-uri, where to return your app after logout.

post-logout-redirect-uri: http://localhost:8085

Azure AD B2B (for Business partners(external) )

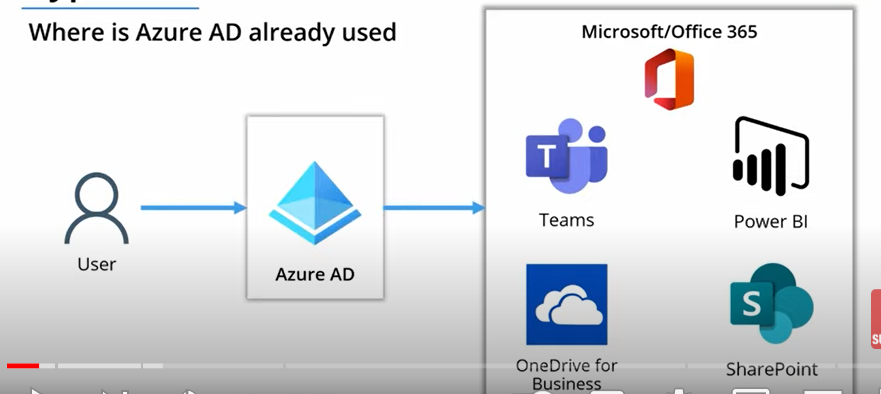
No need to register – invited as a guest – can redeem the invitation and they can start accessing the portal.



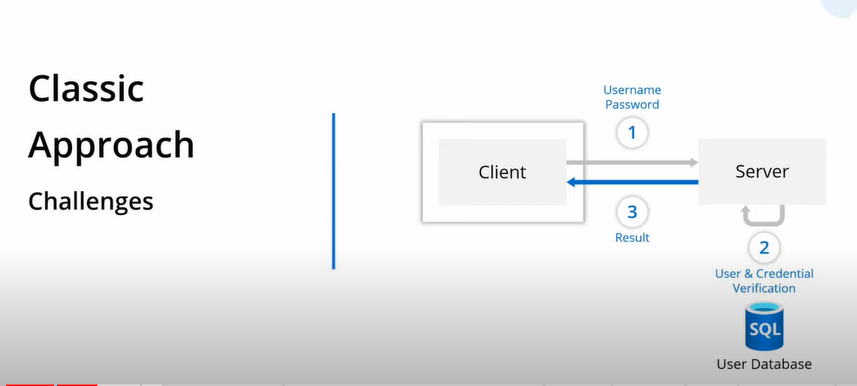


Azure AD usage -

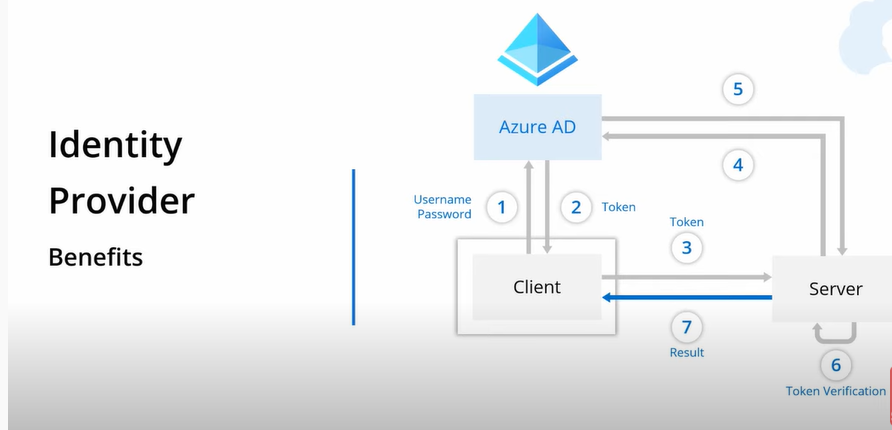
outlook, skype, onedrive, teams, sharepoint - using AAD



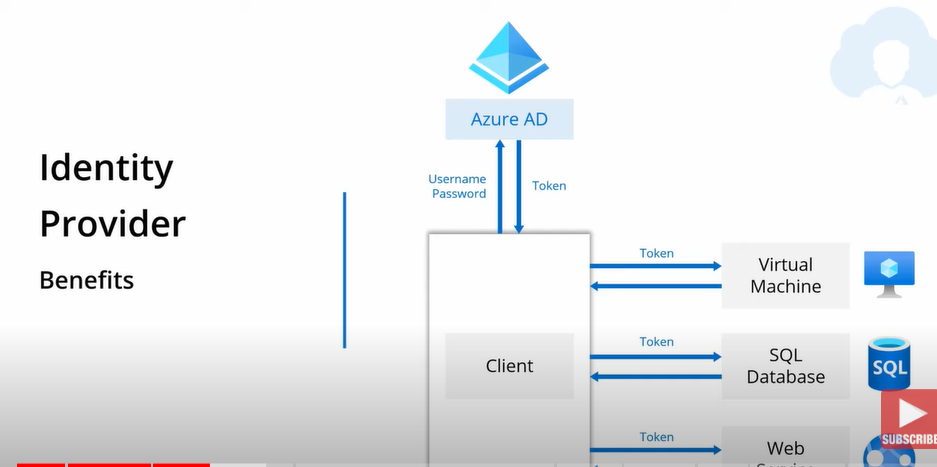
Already getting used for login



Traditional approach – used before - (security breach risks)



With Azure AD, its gets more trusted and secure

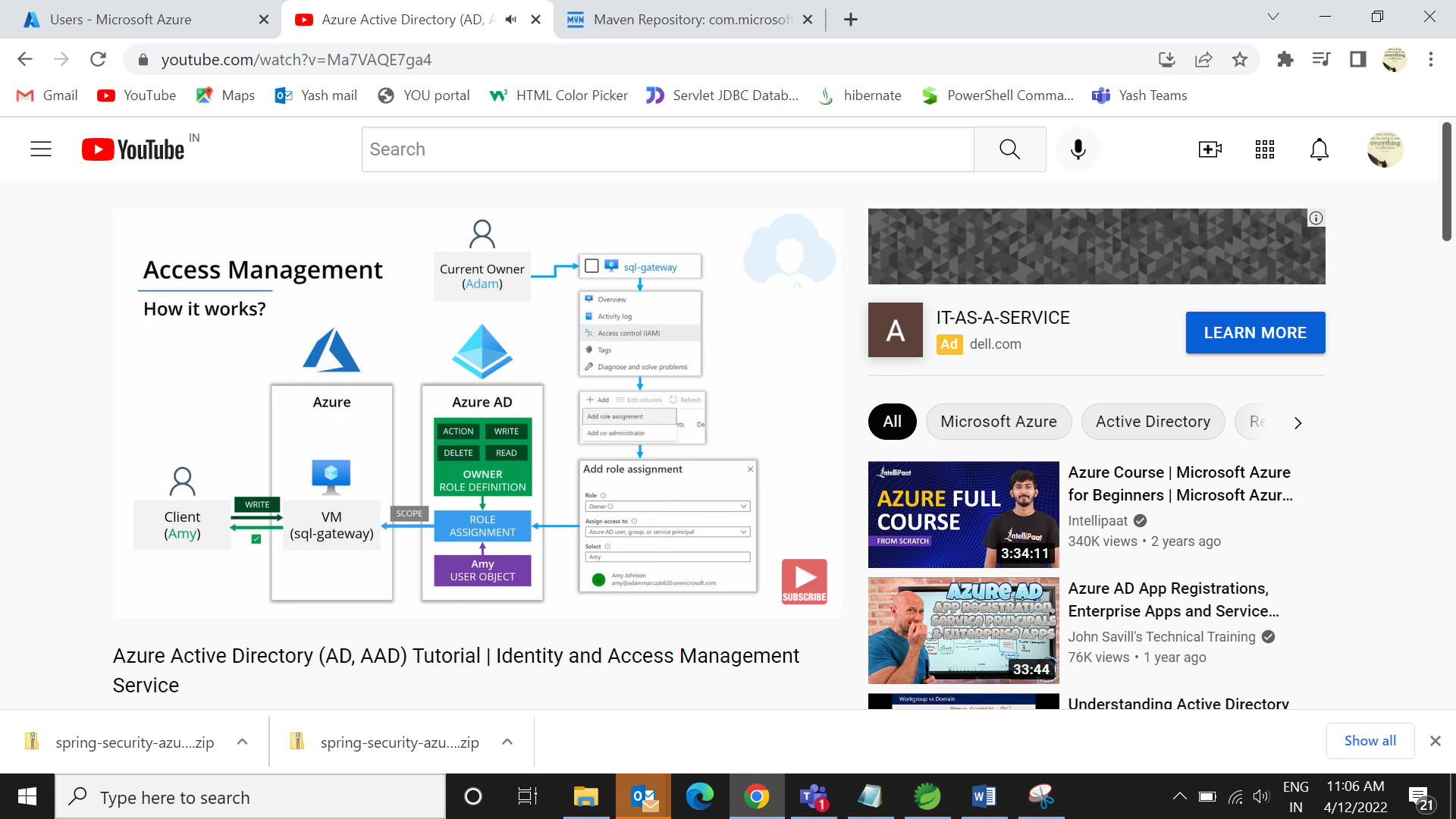


First azure directory of org1

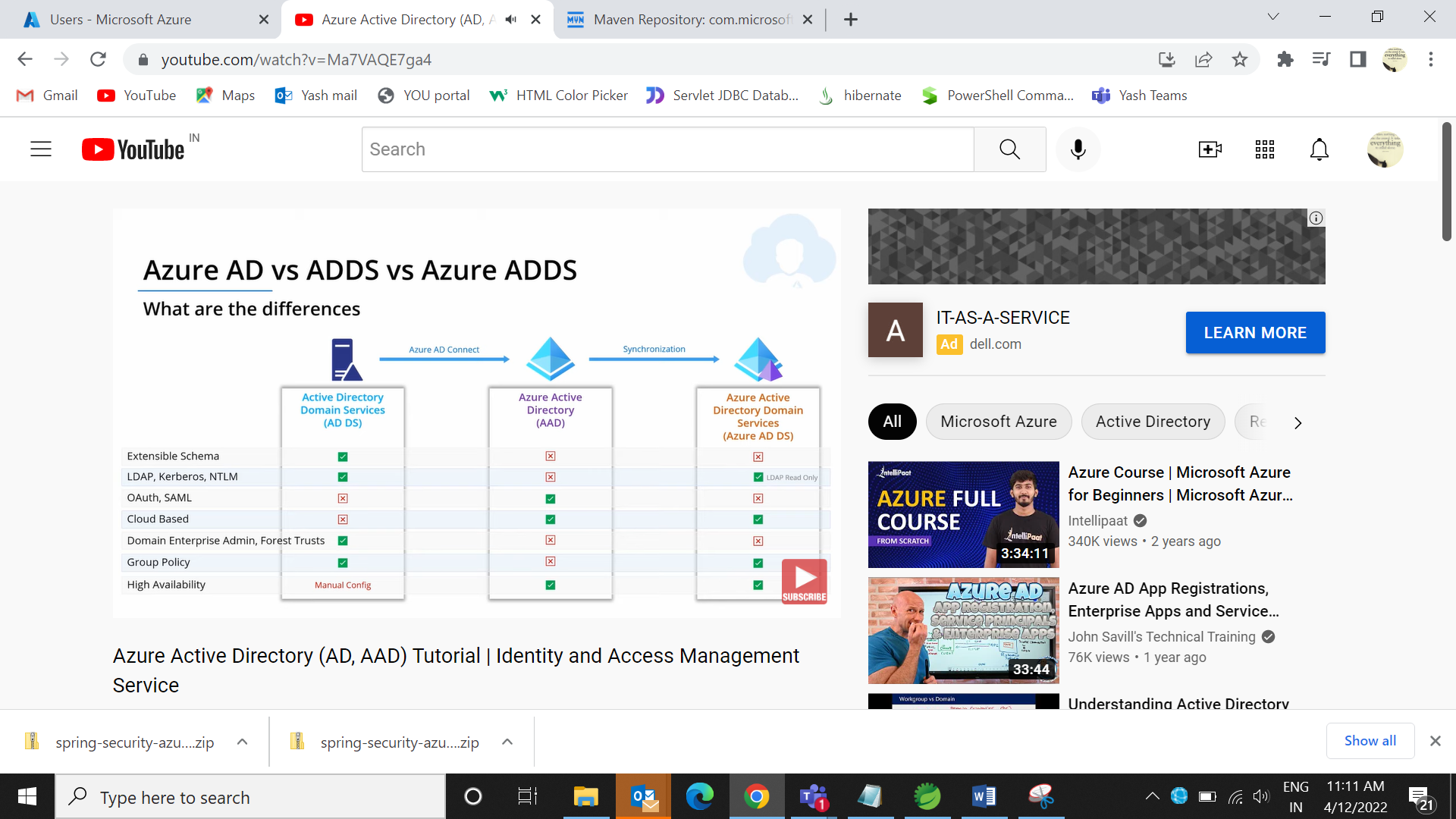


Second azure directory of org2





Role based access management (RBAC – Role based access control)



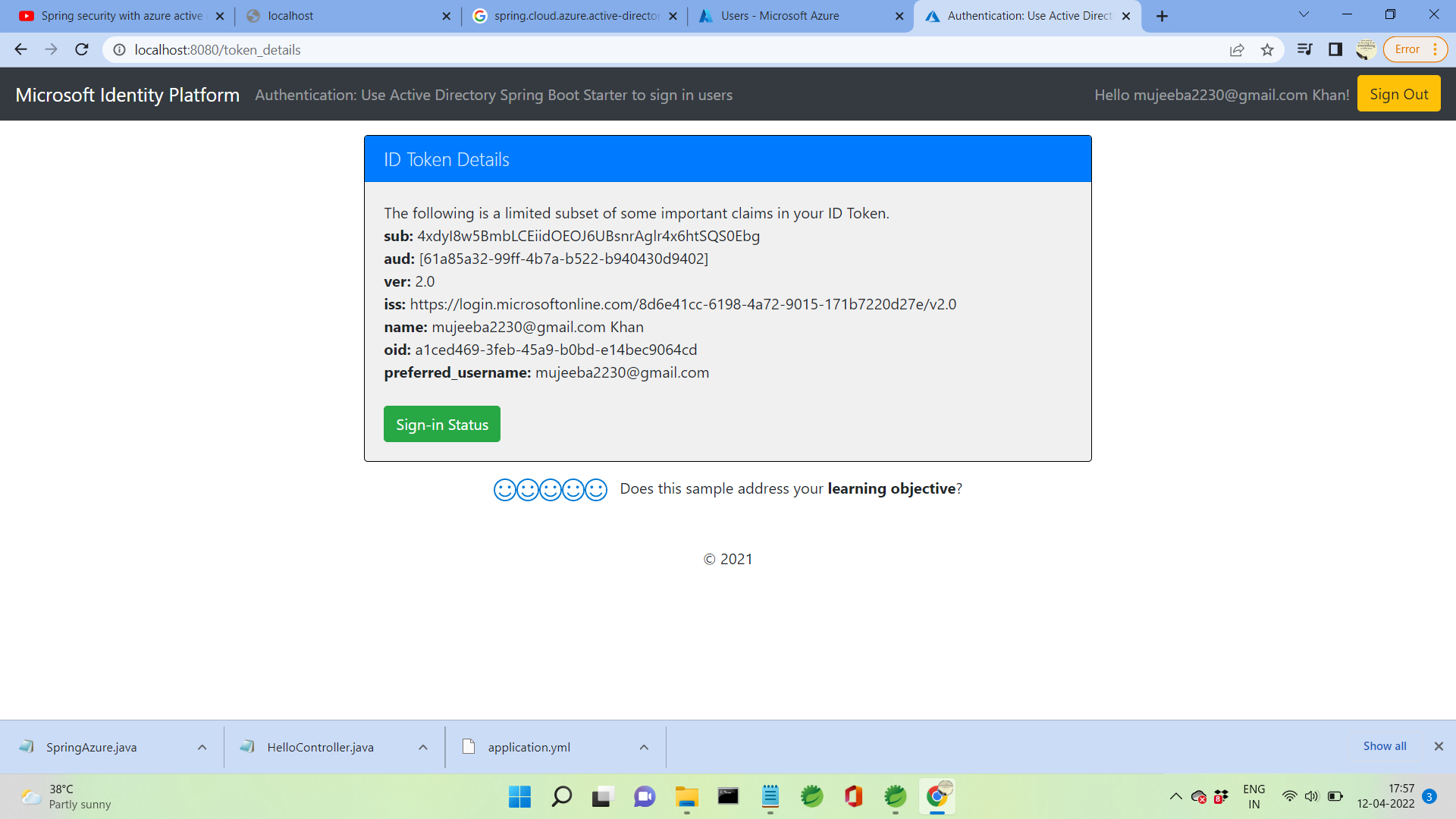
Directory domain services (on-premises directory) can be connected to Azure AD via Azure AD Connect

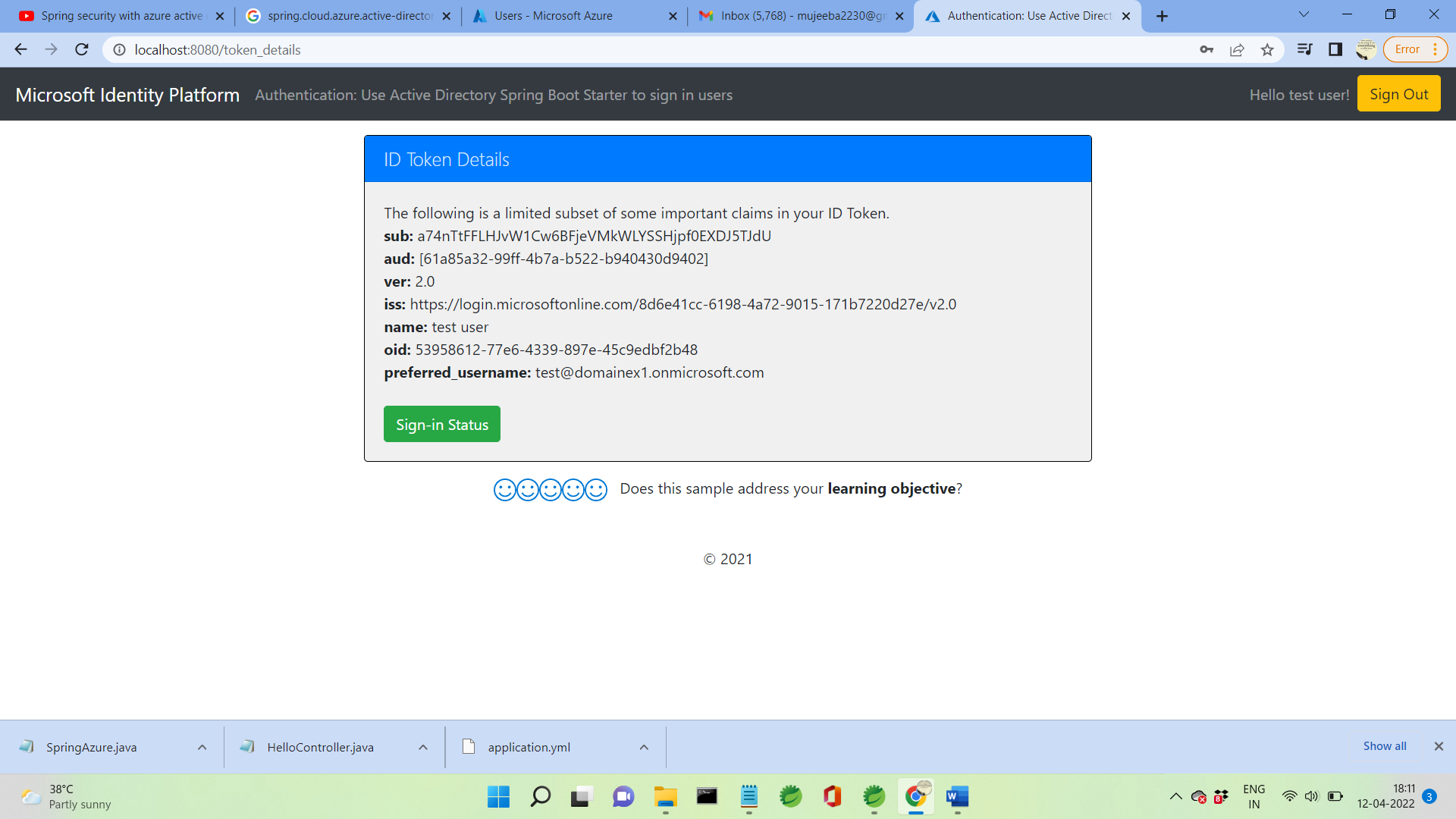
Azure AD Connect – will synch all users from on premise directory to azure AD

Requires Windows server OS

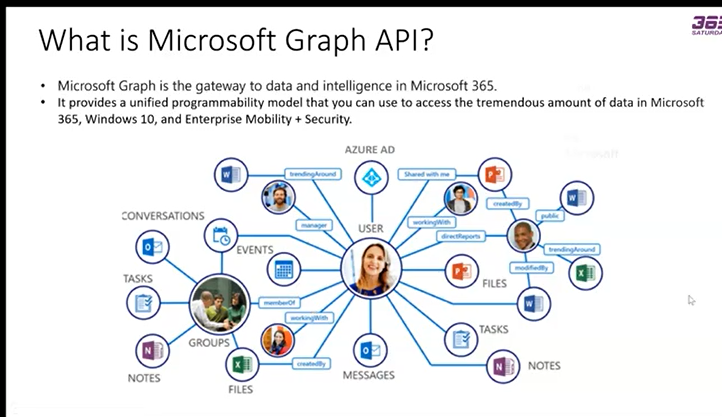
It will run every 30 mins

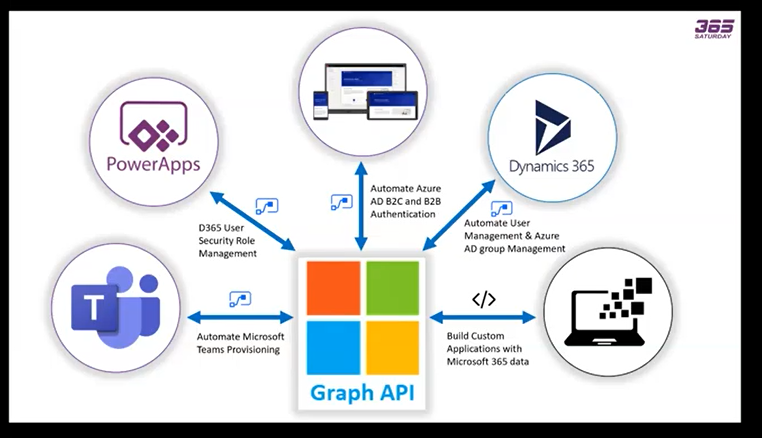
Authentication done using java – displaying token details





Microsoft Graph API





Code for CRUD operations for user in Azure AD

jars add ki hai

new class - AzureADAuthentication

changes made in -

DataIntegrityAction

SaveFileDataDAO

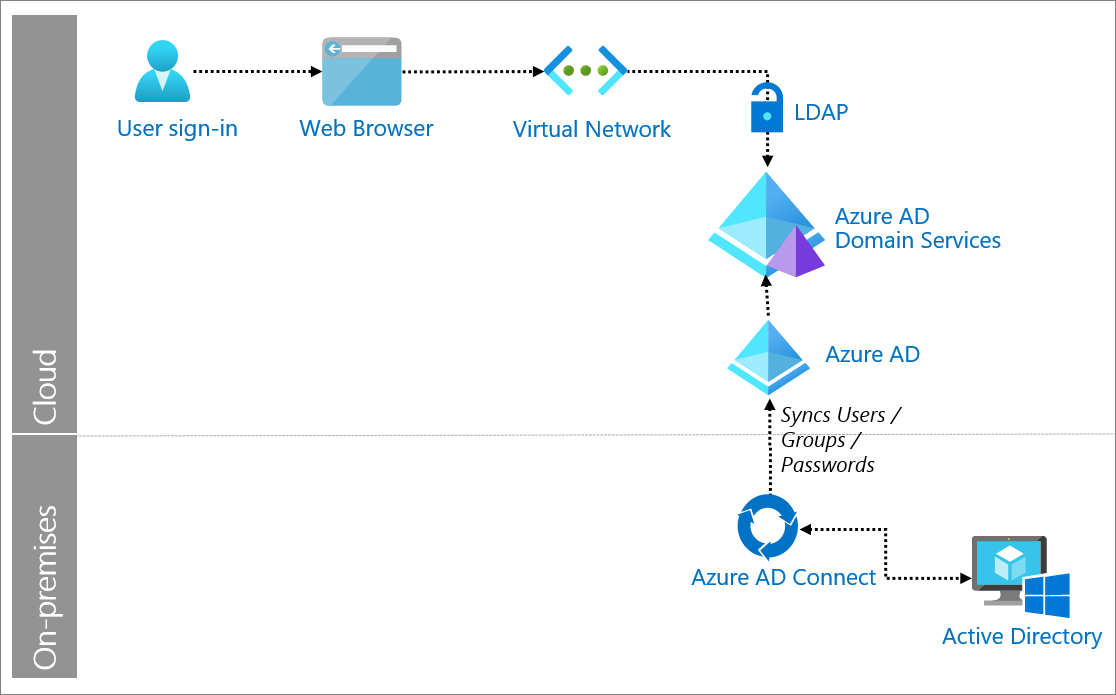
DataComparisonDAO

**LDAP authentication with Azure Active Directory**

Lightweight Directory Access Protocol (LDAP) is an application protocol for working with various directory services. Directory services, such as Active Directory, [store user and account information](https://www.dnsstuff.com/active-directory-service-accounts), and security information like passwords.

Azure Active Directory (Azure AD) supports this pattern via Azure AD Domain Services (AD DS). It allows organizations that are adopting a cloud-first strategy to modernize their environment by moving off their on-premises LDAP resources to the cloud.

There is a need to for an application or service to use LDAP authentication.



* **Azure AD**: Synchronizes identity information from organization’s on-premises directory via Azure AD Connect.
* **Azure AD Domain Services (AD DS)**: Performs a one-way synchronization from Azure AD to provide access to a central set of users, groups, and credentials. The AD DS instance is assigned to a virtual network. Applications, services, and VMs in Azure that connect to the virtual network assigned to AD DS can use common AD DS features such as LDAP, domain join, group policy, Kerberos, and NTLM authentication.
* **Azure AD Connect**: A tool for synchronizing on premises identity information to Microsoft Azure AD. The deployment wizard and guided experiences help you configure prerequisites and components required for the connection, including sync and sign on from Active Directory to Azure AD.
* **Active Directory**: Directory service that stores [on-premises identity information such as user and account information](https://www.dnsstuff.com/active-directory-service-accounts), and security information like passwords.

Users and groups are the basic building blocks for Azure AD. You can further organize users into groups that will all behave similarly. For example, you may put your Product Management team in one Azure AD group and grant permissions at the group level, so when users leave the organization, you only need to deactivate one account, and the rest of the group stays the same.

What this means is that you can bring people outside of your organization inside your tenant and grant them specific permissions just like they are part of your organization. When done correctly, this provides an additional level of security to the organization’s data.

Organisational Unit -> Administrative Units

