**Setting up Enterprise Federation b/w Azure Active Directory and Amazon Cognito using OAUTH/OIDC**

Diagram

Description automatically generated

**Create Azure AD App Registration**

* Go to Azure portal -> Azure Active Directory -> App Registrations -> Register New Application.
* On the creation page, fill out the form with desired values.
* Set the Redirect URI to (where xxx is the cognito domain)
* Web – https:// 3v275dnt1hcbo7ermpp3nvgke8.auth.us-east-1.amazoncognito.com/oauth2/idpresponse
* Create the App Registration and note Application (Client) ID, Tenant ID
* Go to App Registration -> Your App -> Certificates and secrets -> Create new client secret and copy Secret value.
* Go to Authentication Details ->select ID tokens for the OAuth authorization endpoint and save the changes.

**Integrating Azure AD with Cognito**

* Go to Cognito user pool -> Your user pool -> Federation -> identity providers -> OpenID Connect.
* Set the Provider name to a string that you want to be displayed on Frontend for this identity provider.
* Paste the Client ID and secret obtained from Azure Active Directory App.
* Set attributes request method to GET and Authorize score to: profile email openid
* Set issuer to https://login.microsoftonline.com/<tenant\_id>/v2.0, replace tenant\_id with the tenant id of the Active directory which will issue the Oauth tokens i.e active directory containing users.
* Click Run Discovery and save the identity provider.

Graphical user interface, text, application

Description automatically generated

* Now go to Federation -> Attribute mapping and set the following mappings:
* name -> Name
* preferred\_username -> Preferred User Name
* unique\_name -> Given Name
* email -> Email
* sub -> Username

A screenshot of a computer

Description automatically generated

**Cognito PostConfirmation Lamda function & trigger:**

Set up below lamda function & trigger to move users to specific groups required for authorization. Code is checked in to github (./fhir-works-on-aws-deployment/scripts/post-confirmation-trigger.js)

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated