Azure AD Integration with Polycloud VCC

This document provides a comprehensive guide on integrating Azure Active Directory (Azure AD) with the Polycloud VCC server application and a client application. It includes steps for app registration, token generation, and role management using Azure AD.

# 1. Creation of "Polycloud VCC" Server App in Azure AD with Scope

The 'Polycloud VCC' server application is a crucial component in Azure AD for managing access and authentication. The following steps guide you through creating and configuring the 'Polycloud VCC' server app in Azure AD.

1. Log in to the Azure Portal and navigate to Azure Active Directory.  
2. Select 'App registrations' and then click 'New registration'.  
3. Enter the name 'Polycloud VCC' for the application.  
4. Specify the supported account types (e.g., Single tenant, Multitenant).  
5. Set a redirect URI if applicable (this is typically required for web applications).  
6. Once registered, go to the 'Expose an API' section and set the Application ID URI.  
7. Add scopes required by the application, defining the access level and permissions.

[Screenshot Placeholder: Azure Portal - Polycloud VCC Registration]

# 2. Client App Creation on Azure AD

1. In the Azure Portal, go to Azure Active Directory and select 'App registrations'.  
2. Click on 'New registration' and provide a name for the client application.  
3. Choose the appropriate account types and set the redirect URI(s).  
4. After registration, go to 'API permissions' and click 'Add a permission'.  
5. Select 'My APIs' and then choose 'Polycloud VCC' to request permissions.  
6. Add the required permissions (delegated or application permissions) to access 'Polycloud VCC'.

[Include Screenshot: Azure Portal - Client App Registration]

# 3. Token Generation Using Postman

1. Open Postman and create a new OAuth 2.0 request.  
2. In the 'Authorization' tab, select 'OAuth 2.0' as the type. Click on 'Get New Access Token'.  
3. Fill in the token name, grant type (e.g., 'Authorization Code'), callback URL (use Postman's default callback URL), auth URL, and access token URL.  
4. Specify the client ID and client secret from the Azure AD application registration.  
5. Set the scope to the Polycloud VCC's scope and request both the access token and ID token.  
6. Click 'Request Token'. Postman will handle the authentication and retrieve the tokens.

[Include Screenshot: Postman Setup for Token Generation]

# 4. Role Addition and Assignment using appRoles in "Polycloud VCC"

2. For role addition, go to the 'App roles' section in the Azure AD application settings of 'Polycloud VCC'.  
3. Click 'Add role' to create a new role.  
4. Provide details for the new role, including 'Display name', 'Allowed member types', 'Value', and 'Description'.  
5. After filling in the details, save the role configuration.

[Include Screenshot: Azure Portal - Adding appRoles]