**JWT Based Authorization with RBAC – Using Azure AD**

Monday, June 15, 2020

In this example we will allow user to access the API Actions based on their User-Role.

For Example:

|  |  |  |
| --- | --- | --- |
| API Action | Role Can Access |  |
| Privacy | Writer |  |
| Foo | Loc1\_User |  |

Pre-Requisite:

1: You have already configured your Client Application with Azure AD (JWT or OAuth2)

2: Your application already tested with [Authorize] attribute and it works with above Authentication mechanism

What we will achieve?

1: Your application is already working with Authentication

2: Now, you want to implement Authentication with Role-Base-Access-Control (RBAC)

Code Snippet:

[Authorize(Roles = "Writer")]

public IActionResult Privacy()

{

     return View();

}

[Authorize(Roles = "Loc1\_User")]

public string Foo()

{

        var user = HttpContext.User;

        var userRole = ((ClaimsIdentity)User.Identity).FindAll(ClaimTypes.Role).ToList();

           return $"User {user.Identity.Name} Access the Action with Role {userRole.FirstOrDefault().Value}";

}

Steps Required:

1: You need to Create Application Registration and configure you Web App/API with the Client ID and Tenant ID

2: Assuming you have Azure Multi-Tenant Option is on with ID Token Access for the registered APP

**How to create User, Role, User Role Assignment in Azure**

1: For this go to Azure Portal (With your Admin access subscription)

2: Go to Azure Search Box and Type “Azure Active Directory”

3: Open the Active Dir Interface and Click the Manage > User menu

[Here you will see list of users available in the Azure AD]

4: You may need to create, Invite user using the Screen and complete the user add part for the new users

5: Once users are created, they are listed in the page

**How to Create Role**

1: Go to the Azure Portal Home

2: Search “App Registration” and open it

3: Under it, pick the App Registration with which you have configured your Web App/API

4: Once the UI opened, go to Manage > **Manifest** menu

5: Edit the Manifest (Add new roles[] here)

6: You may see Blank Roles here as Roles[] – then you need to update the Json to create Roles

|  |
| --- |
| "appRoles": [      {        "allowedMemberTypes": [          "User"        ],        "description": "Loc1\_User Have the ability to create tasks.",        "displayName": "Loc1\_User",        "id": "ef0de34d-0583-47d4-a44a-77461adfba18",        "isEnabled": true,        "lang": null,        "origin": "Application",        "value": "Loc1\_User"      },      {        "allowedMemberTypes": [          "User"        ],        "description": "Writers Have the ability to create tasks.",        "displayName": "Writer",        "id": "d1c2ade8-98f8-45fd-aa4a-6d06b947c66f",        "isEnabled": true,        "lang": null,        "origin": "Application",        "value": "Writer"      } |

[Look at the above template where we have 2 Roles (Loc1\_User and Write)] – Here you can add as many as you want with unique guide.

(Refer for Guid Creation: <https://www.guidgenerator.com/online-guid-generator.aspx> )

|  |
| --- |
|  |

7: Save the template and now Roles are created

**Assign Users to the Role**

1: Open Azure Active DIR

2: Select “Enterprise Application” under Manage Menu

3: There your Application that is registered will be listed

4: Select the Application registered

5: On its Open, go to “User & Groups” menu under Manage

6: Click/Edit User to select the Roles [Loc1\_User/Writer] Created earlier

7: Save it

8: Test your Web App

Example:

<https://localhost:44321/Home/Privacy> (only Writer can access)

<https://localhost:44321/Home/Foo> (only Loc1\_User can Access)

**Note:**

1: The concept has taken from URL:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-add-app-roles-in-azure-ad-apps>

2: One can use the technique when you have

* Single MVC Web APP running on Authentication & Authorization using OAuth2 or JWT

Ref:

* MVC Web APP calling its Down Stream Web API with Delegated Security (Graph API)

Ref: <https://github.com/Rimbik/AzureActiveDir/tree/master/webapi_2_webapi_jwt>

Problem:

1: Yet I have not identified a way to Add/Create Roles using GUI as we have seen that we modified the manifest manually - Azure Active Directory application manifest

What is pending:

1: We need to redirect user to Login Page if UnAuthorize User tries to Access the Action, Page. In non azure cases we redirect user to login page, whereas here we have to redirect to azure OPID login page.