**Managing resources in Azure project solution**

**Instructions**: List the steps you will perform to complete each activity in the system. Ensure to provide screenshots for each step. As a sample, we have filled in the information for *Activity 1, Step 1*. You can add more rows as required.

**Task:** You need to Implement Azure Authentication and RBAC for a web application to create a project, and it will involve setting up authentication for your application using Azure Active Directory (Azure AD) and implementing RBAC to control access based on user roles.

|  |  |
| --- | --- |
| **Activity #** | **Steps** |
| **Activity 1:**  Create Azure AD App Registration and implement Azure Authentication for a web application | * **Step 1:** Log in to Azure Portal. * **Step 2:** Navigate to **Azure Active Directory (AAD)** > **App Registrations** > **New Registration**.      * **Step 3:** Provide the following details:   + Name: [Enter your app name]   + Supported Account Types: [Choose Single/Multi-tenant based on your requirements]   + Redirect URI: [Specify the URI of your application]      * **Step 4:** Click "Register". * **Step 5:** After registration:   + Note the **Application (Client) ID** and **Directory (Tenant) ID**.   + Generate and save a **Client Secret** under "Certificates & Secrets".      * **Step 6:** Configure authentication in the web application by integrating AAD credentials using SDKs (e.g., Microsoft Identity Library). |
|  |  |
| **Activity 2:**  Implement RBAC for a web application | * **Step 1:** In the Azure Portal, go to the **App Service** hosting your web application. * **Step 2:** Under **Access Control (IAM)**, click **Add Role Assignment**. * **Step 3:** Assign appropriate roles, such as:   + Reader   + Contributor   + Owner * **Step 4:** Assign these roles to users or groups. |
|  |  |
| **Activity 3:**  Set up authentication for your application using AAD and assign roles to user | * **Step 1:** Update the web application to authenticate users using AAD. * **Step 2:** Implement role claims in your application:   + Use the **Microsoft Graph API** to fetch role assignments for authenticated users.   + Add roles to the user's JWT token as claims. * **Step 3:** Assign roles to users or groups in AAD by creating custom roles under **Enterprise Applications > [Your App] > Users and Groups**. |
|  |  |
| **Activity 4:**  Implement RBAC to control access based on user roles by deploying Azure App Service | * **Step 1:** Modify the web application to check user roles during runtime. * **Step 2:** Restrict access to application features or pages based on roles. Example:   + **Admin Role**: Full access to all features.   + **User Role**: Access to limited features. * **Step 3:** Deploy the application to Azure App Service. * **Step 4:** Test role-based access restrictions using multiple user accounts. |
|  |  |
| **Activity 5:**  Test whether the roles are assigned to the users or not | * **Step 1:** Log in to the web application using different user accounts. * **Step 2:** Verify that:   + Each user has access only to the features permitted by their assigned role.   + Unauthorized users cannot access restricted areas. * **Step 3:** Monitor access logs and role assignments in the Azure Portal to confirm correct behavior. |
|  |  |