Role-Based Access Control (RBAC) in Microsoft Entra ID (Azure Active Directory) allows you to manage user access to Azure resources effectively. Here's how you can configure RBAC:

**Step 1: Sign in to the Azure Portal**

1. **Go to the Azure portal**: [Azure Portal](https://portal.azure.com/)
2. **Sign in** with your Azure account credentials.

**Step 2: Navigate to the Resource**

1. **Select the Resource**:
   * Navigate to the resource you want to manage (e.g., a subscription, resource group, or specific resource).
   * Click on the resource to open its management pane.

**Step 3: Access the Access Control (IAM) Pane**

1. **Open the IAM Pane**:
   * In the resource's management pane, find and select **Access control (IAM)** in the left-hand menu.

**Step 4: Add a Role Assignment**

1. **Add a Role Assignment**:
   * In the Access control (IAM) pane, click **+ Add** and then select **Add role assignment**.
2. **Select a Role**:
   * In the Role pane, select a role to assign (e.g., Owner, Contributor, Reader, or any custom role you have created).
3. **Assign Access**:
   * **Assign access to**: Select the type of security principal you want to assign access to (User, Group, Service principal, Managed identity).
   * **Select**: Search for and select the user, group, or service principal you want to assign the role to.
4. **Review and Assign**:
   * Review your selections and click **Save** to assign the role.

**Step 5: Verify the Role Assignment**

1. **Check the Assignments**:
   * After assigning the role, you can verify the role assignments in the **Role assignments** tab within the Access control (IAM) pane.
   * Ensure the user, group, or service principal is listed with the correct role.

**Creating Custom Roles (Optional)**

If built-in roles do not meet your needs, you can create custom roles.

1. **Navigate to Azure Active Directory**:
   * In the left-hand navigation pane, select **Azure Active Directory**.
2. **Roles and Administrators**:
   * In the Azure Active Directory pane, select **Roles and administrators**.
3. **+ New custom role**:
   * Click **+ New custom role** and fill in the required details:
     + **Basics**: Provide a name and description for the custom role.
     + **Permissions**: Add the necessary permissions by selecting from the list of available permissions.
     + **Review + create**: Review your selections and click **Create**.
4. **Assign the Custom Role**:
   * Follow the same steps as above to assign the custom role to users, groups, or service principals.

**Example: Assigning a Built-in Role to a User**

Here's a detailed example of assigning the "Contributor" role to a user at the subscription level:

1. **Navigate to Subscriptions**:
   * In the Azure portal, select **Subscriptions** from the left-hand navigation pane.
2. **Select a Subscription**:
   * Click on the subscription you want to manage.
3. **Access Control (IAM)**:
   * In the subscription pane, click **Access control (IAM)**.
4. **Add a Role Assignment**:
   * Click **+ Add** and select **Add role assignment**.
5. **Select the Role**:
   * In the Role pane, select **Contributor**.
6. **Assign Access to User**:
   * In the Assign access pane, select **User, group, or service principal**.
   * Search for and select the user you want to assign the role to.
7. **Review and Assign**:
   * Click **Save** to assign the role.