Practical Exercise: Defining Users and Roles

Training Objective

In this section, you will learn how to set up custom roles and users. Roles contain permissions for users to manage the server. You can create different roles with various combinations of permissions and assign them to a user or a group of users. User roles can be reused throughout the system and prevent the overhead of granting multiple permissions to each and every user individually.

Business Scenario

PizzaShack has an employee who will be creating the menu, order and delivery APIs, and another employee who will be publishing this to the website. API consumers can log in to the site and access these APIs. Separate user roles and users should be created for API creators and publishers.

High-Level Steps

- Define roles
- Map the custom roles to internal roles.
- Define users via the admin console

Detailed Instructions
Define Roles

1. Open a Command Line Interface.
2. Start the WSO2 API Manager by navigating to the <API-M_HOME>/bin directory and running wso2server.bat (on Windows) or sh wso2server.sh (on Linux)
3. Log in to the API-M admin console, which is available by default at: https://localhost:9443/carbon. You can log in to the console using the default admin/admin credentials.
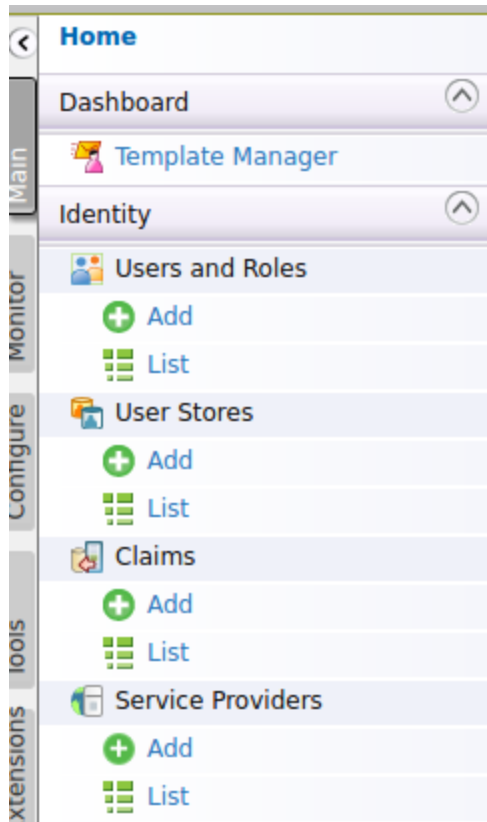
4. Click **Main** > **Users and Roles**> **Add > Add New Role**.
5. Provide **apicreator** as the role name.
6. Click **Next** - You will be presented with a list of permissions. For the creator role, you need to select the following permissions:
   - **Configure** > **Governance** and all underlying permission
   - **Login**
   - **Manage** > API > **Create**
   - **Manage** > **Resources** > **Govern** and all underlying permissions.
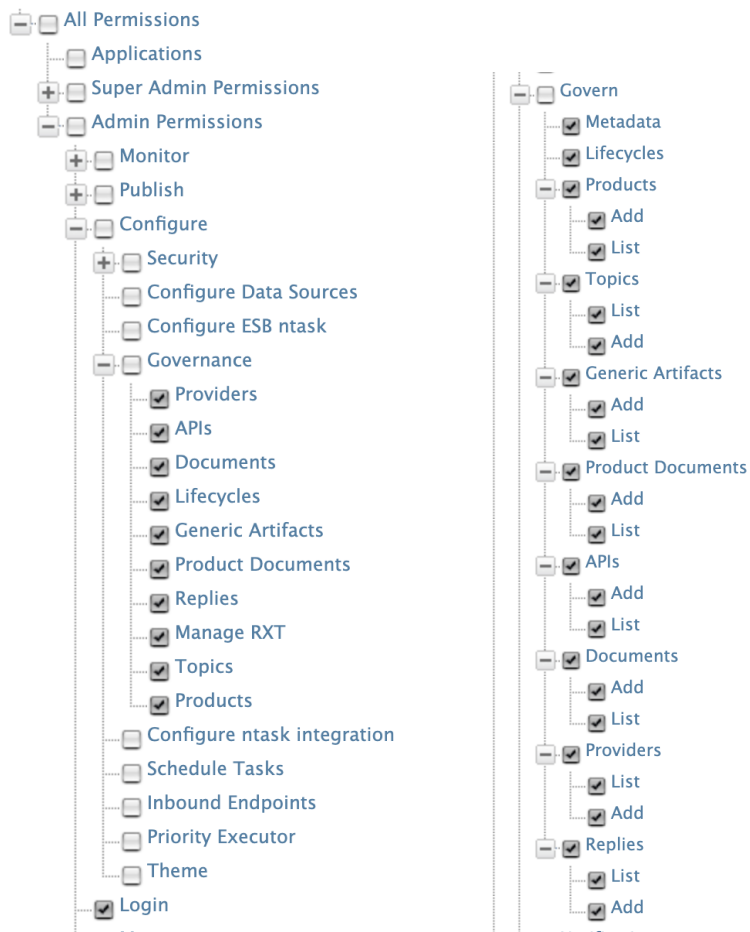
7. Click **Finish** (at the bottom of the page).

Repeat the steps to create the **apipublisher** role, with the **following permissions**:
- **Login**
- **Manage** > **API** > **Publish**
  Finish

Add Role Mapping

In APIM 3.2.0, the publisher and dev portal uses REST APIs and access control is done based on OAUth2 scopes. Each action in the portal requires a specific scope. These scopes are mapped with the **APIM Internal/*** roles.
`apim:api-create` scope is bound with Internal/creator.

In order to enable our custom creator role to be functional as the Internal/creator role, we have to add a role mapping.

1. Log in to the API Manager Admin portal (https://localhost:9443/admin) and go to **Settings -> Role Permissions**.
2. In the **Role Permissions** table, click on **Add role permission**
3. Provide the role name as **apicreator** and add the **Internal/creator** role as the mapping role.

Add new role permissions

- ✓ Provide role name

- ② Select permissions
  - ⦿ Role alias

    Mapping role
    Internal/creator ▾

    Role **apicreator** will be mapped to the selected role

  - ○ Custom permissions

    ⊟ Permissions (49)
      ⊞ admin (18)
      ⊞ store (7)
      ⊞ publisher (24)

4. Click the Save button to add the role mapping.

Repeat the above steps for **apipublisher** role as follows.
Role name: apipublisher, Mapping role: Internal/publisher

Define Users via the Admin Console

You can now create a user for each of those roles. To do so:

1. Click **Main** > **Users and Roles**> **Add** > **Add New User**
2. Provide user name (creator) and password (password)
3. Click **Next**.
4. Select the **apicreator** role.
5. Click **Finish**.

Note : You can also choose the **Internal/creator** role available by default in the management console, in Step 4

Create a user named 'publisher'' and assign him the 'apipublisher' role that we created:

1. Click **Main** > **Users and Roles** > **Add**.
2. Click **Add New User**.
3. Provide user name (publisher) and password (password)
4. Click **Next**.
5. Select the **'apipublisher'** role.
6. Click **Finish**.

Create a user named 'subscriber' and assign him the 'Internal/Subscriber' role:

7. Click **Main** > **Users and Roles** > **Add**.
8. Click **Add New User**.
9. Provide user name (subscriber) and password (password)
10. Click **Next**.
11. Select the **'Internal/subscriber'** role.
12. Click **Finish**.

Create a user named mike and do not assign him any roles::

13. Click **Main** > **Users and Roles** > **Add**.
14. Click **Add New User**.
15. Provide user name (mike) and password (password)
16. Click **Finish**.

Expected Outcome

A creator role with permissions for creating APIs and a publisher role with permissions for publishing APIs have been created. Users named 'creator' and 'publisher' have been created and given the appropriate roles. Users named 'subscriber' and 'mike' have been created to test out the PizzaShack application.