Configuring and Running OAuth2.0 Demo Application

The demo application provides a quick way to test the installation, configuration, and deployment of OAuth 2.0 and OpenID connect feature.

The application is a test ground where a classic use case of OAuth 2.0 involving a RESTful API service and a client application is demonstrated. Also, the application provides a way to test the various endpoints of OpenID connect including metadata, userinfo, and tokeninfo endpoints.

Configuring the demo OAuth application includes the following steps:

1. Prerequisites

Ensure that you meet the following prerequisites before running the demo application:

- Install a Linux operating system such OpenSuSE or SuSE Linux Enterprise System or a Windows operating system.
- Set up Java SE Runtime Environment 7 8. You can download it here: http://www.oracle.com/technetwork/java/javase/downloads/index.html
- Install a web browser. The recommended browser is Google Chrome.
- Install Access Manager 4.1 or later and configure basic settings. See *NetIQ Access Manager Appliance 4.3 Installation and Upgrade Guide* and "Section 3.0, Setting Up a Basic Access Manager Appliance Configuration" of the *Administration Guide*.
- Ensure that you have performed the activities listed in Access Manager Configuration Checklist.
- Download the OAuth 2.0 Demo Application.
- Edit host entries for Access Manager and the demo application. See Editing Host Entries.

1.1 Editing Host entries

Host Entries are needed if your client and server machines are not in the DNS system.

1.1.1 Adding Access Manager Host entries

If the NetIQ Access Manager system is not on a DNS, then you need to add a host entry to your desktop system. Identify the base URL of Identity Server by looking at the **Identity Server** > ***<Cluster name>*** > **Base URL**. Add that entry to your host files.

On Windows: *%WINDOWS%\System32\etc\drivers\hosts*

On Linux: */etc/hosts*

Edit the file and add the host entries. For example:

10.0.0.0 namtest.mycompany.com

1.1.2 Adding Demo Application host entries

When accessing the demo application through browser, it is better to access through a DNS name and register that as “redirect uri” in Identity Server. Localhost cannot be registered at Identity Server for security reasons.

127.0.0.1 mydemoclient.mycompany.com

1.2 Access Manager Configuration Checklist

Ensure that you have performed the following actions before running the demo application:

- Install Access Manager Administration Console. See Installing Access Manager in the NetIQ Access Manager Installation and Upgrade Guide.
- Install the Access Manager Identity Server and import it into Administration Console. See Installing Access Manager in the NetIQ Access Manager Installation and Upgrade Guide.
- Create an Identity Server cluster configuration and add the imported Identity Server to that cluster. See Section 3.4, Identity Servers Cluster in the Administration Guide.
- Enable OAuth & OpenID Connect in **Administration Console** > **Devices** > **Identity Server** > **cluster** > **General**.
- Extend the user store to host a new attribute on User Object named **nidsOAuthGrant**. Scopes use this attribute to store the authorization grants provided by a user. If you use the embedded user store of Administration Console for authenticating users at Identity Server, then perform the following steps mentioned in Extending a User Store for OAuth 2.0 Authorization Grant Information.

  NOTE**:* User Store under Identity **Server** > ***cluster name > **Local** must have the IP address of Administration Console.

- Create a new certificate with key size 2048 and SHA algorithm set to SHA256.
  In Administration Console, go to **Security** > **Certificates** > **New** and specify the name as *oauth2048*. You will need this certificate while accessing OpenID Connect endpoints.
  In Access Manager, OpenID Connect uses certificate configured in **Identity Server** > **cluster** > **OAuth2 & OpenID Connect** > **Global Settings**. OpenID Connect uses the reverse proxy certificate in Access Manager Appliance.
- Perform the following actions under **Identity Server** > ***cluster*** > **OAuth2 & OpenID Connect** > **Global Settings**:
  - Set Authorization Grant LDAP Attribute to **nidsOAuthGrant** or the name you specified when you extended the user store.
  - Select all Grant Types and Token Types.
  - Click Support Signing and choose the certificate you have created for this demo configuration.
  - Specify the certificate's algorithm.

2. Registering the Demo RESTful Service at Administration Console

The demo application contains a simple RESTful web service. This RESTful web service exposes a REST API to add, modify, and delete tasks. A client application can post a request to create, modify, or delete a task by using a REST API. OAuth 2.0 protects this communication. Therefore, each request must contain an OAuth 2.0 Access token with necessary scope list_todo, create_todo, delete_todo to list tasks, add tasks, and delete tasks respectively. Define these scopes in Administration Console. Later, the client application can request any of these scopes.

To create the scopes, perform the following steps:

1. Click **Devices** > **Identity Server** > **Edit** > **OAuth & OpenID Connect** > **Resource Server** > **New**.
2. Specify Todo Service and click **OK**.
3. Click newly created services (Todo Service) > **Scopes**.
4. Click **New** and specify the following details:
    - **Name**: create_todo
    - **Description**: Create Task Items
    - **Require user permission**: Select this option
5. Repeat step 4 and add the following scopes:
    - **Name**: list_todo, Description: Access your task list
    - **Name**: delete_todo, Description: Delete your task list

    In this step, you can select Allow modification in consent.
6. Click **OK** > **OK** > **Update All**.

3. Registering the Demo Client at Identity Server

The client application needs to communicate with Identity Server through the OAuth 2.0 protocol. As per this protocol's specification, Identity Server must uniquely identify each client application. You must register client application in the Identity Manager.

To register a client application in Identity Server, the user must have the NAM_OAUTH2_DEVELOPER role defined in the OAuth policy. Hence, an administrator needs to create the role in Administration Console and assign it to the user.

3.1 Creating an OAuth 2.0 Developer Role for Registering a Client Application in Identity Server

Perform the following steps:

1. Click **Devices** > **Identity Servers** > **cluster** > **General** > **Roles**.
2. Click **Manage Policies** > **New**. Specify the following details:
    - **Name**: oauth_developers

- **Type**: Identity Server: Roles

3. Click **OK**.
4. Specify the following details under Condition Group:
   - **New**: LDAP Attribute: LDAP Attribute: cn
   - **Comparison**: **String**: Equals
   - **Value**: Data Entry Field: admin or provide your own condition here.
5. Specify the following detail under Actions:
   - **Activate Role**: NAM_OAUTH2_DEVELOPER
6. Click **OK** > **OK** > **Apply Changes**.
7. Select the oauth_developers and click **Close**.
8. Select the oauth_developers policy again and click **Enable** > **OK** > **Update All**.

3.2 Registering a Client Application in Identity Server

Perform the following steps:

1. Determine Identity Server's base URL.
   Go to **Administration Console** > **Identity Server** > **cluster** > **General** > **Base URL**.
2. Launch this base URL (https://<base_url>/nidp/) in a web browser.
3. Log into as an administrator.
4. Go to **Applications** > **My Applications** > **Register New Clients** > **Client Configuration**.
5. Specify the following details:
   - **Client Name**: NetIQ Demo Application
   - **Client Type**: Web
   - **Redirect Uri**: Specify the following URLs with the host name you specified in Editing Host Entries (mydemoclient.mycompany.com) and the last one with host name of Access Manager installation (namtest.mycompany.com).

     Add each URL in a separate text box.

     https://mydemoclient.mycompany.com:9443/_oauth-callback

     https://mydemoclient.mycompany.com:9443/_oauth-callback2

     https://mydemoclient.mycompany.com:9443/ag/callback

     https://mydemoclient.mycompany.com:9443/callback

     https://mydemoclient.mycompany.com:9443/oidc/_oauth-callback

     https://mydemoclient.mycompany.com:9443/oidc/_oauth-callback2

     https://namtest.mycompany.com/nidp/netiq/nam/oauth/nam-oauth-callback.html
6. Select all grants required and token types options.

7. Click **Register Client**.
8. Click **NetIQ Demo Application** (newly registered client application) and note the values of **Client ID** and **Client Secret**.
9. Log out of Identity Server.

4. Running the REST services

Now, the demo application is ready to run.

1. Launch the resource server (Task Service).
2. Open a command editor. (Windows: cmd, Linux: any terminal)
3. Verify that the JAVA class path is set correctly:

   Windows: set PATH=c:\Program Files\Jdk\bin;%PATH%

   Linux: export PATH=/usr/lib64/jvm/jdk1.8/bin:$PATH

   Replace the path of JDK wherever it is installed.
4. Locate the downloaded demo application file.
5. Extract *todo-service-0.1-SNAPSHOT.zip*.

   NOTE: On Windows, ensure that the environment variable **IDP_BASE_URL** is set to Identity Sever Base URL. Use command set *IDP_BASE_URL=https://namtest.mycompany.com/nidp* to set the variable.
6. Go to todo-service-0.1-SNAPSHOT.
7. Open Identity Server Base URL *(https://namtest.mycompany.com/nidp/bin/todo-service -Dhttp.port=9001).*
8. Replace the host name with Identity Server URL. This will run the todo REST service in the port 9001.

5. Running the Client Application

Perform the following steps:

1. Launch a command editor. (Windows: cmd, Linux: any terminal)
2. Ensure that the Java path is correct. Verify this by running java. If not, set the path to JAVA_HOME's bin:

   Windows: set PATH=c:\Program Files\Jdk\bin;%PATH%

   Linux: export PATH=/usr/lib64/jvm/jdk1.8/bin:$PATH

   Replace with the path of JDK wherever it is installed.
3. Locate the downloaded demo application file.
4. Extract *todo-webapp-0.1-SNAPSHOT.zip*.
5. Go to todo-webapp-0.1-SNAPSHOT.

6. Open this Administration Console URL= *https://namtest.mycompany.com:8443/nps IDP_BASE_URL=https://namtest.mycompany.com/nidp OAUTH2_CLIENT_ID=uJaQKe5QIC2RZLx5d53lA6sc1-PMOXI_psOrUABLzVQSktHBGoVLF9bXOJElCJ3yft17CbwJmgMHuaz604i55Q OAUTH2_CLIENT_SECRET=ZcX_SxxwmcTezB9nloCxQzHRFo4Yci-2wmbDmyZNMN0CSkhm6UtraPFPFNzB88iEyA5MqluiDq8vomqGUq8RNQ TODO_SERVICE_PORT=9001 TODO_SERVICE_HOST=localhost ./bin/todo-webapp -Dhttp.port=9000 -Dhttps.port=9443*

This will run the client web application in the port 9443.

6. Accessing the Client Application through Browser

You can access the application in a browser by using this URL:
https://mydemoclient.mycompany.com:9443/

You can run the various demos by following the screen icons.

Note: If you have not configured “Encryption Options” in “Advanced OpenID Connect” Configuration in the Client Registration page, go to **OpenID Connect Sample** > **Options**, deselect the **Encrypt ID Token** option, and click **Submit**.