edX

Audit Access Expires May 4, 2020
You lose all access to this course, including your progress, on May 4, 2020.
Upgrade by Apr 20, 2020 to get unlimited access to the course as long as it exists on the site. **Upgrade now**

Exercise 9

In this exercise, you will add a sign-up/sign-in component to your application by using Amazon Cognito. After setting up Amazon Cognito, the photos will get stored to/retrieved from the user created in Amazon Cognito.

Note: Make sure to sign in to your AWS account with the AWS IAM user **edXProjectUser** credentials.

To begin, follow the steps below.

1. Start the RDS database instance.

- In the AWS Console, click **Services**, then click **Relational Database Service** to open the **Amazon RDS dashboard**.

- In the left navigation pane, click **Instances**. From the list of instances, select **edx-photos-db**.

- At the top, click **Instance actions**, and then click **Start**.

2. Locate the Cloud9 Preview URL.

In the previous exercises you have been using the *Preview Running Application* feature of AWS Cloud9. Before creating the Cognito user pool you will retrieve the preview URL used by Cloud9. You will use this to configure the Cognito callback and signout URLs.

- In your AWS Cloud9 environment, on the top menu bar, click **Run -> Run Configurations -> Python3RunConfiguration**.

- Click **Preview -> Preview Running Application** on the top menu bar of the Cloud9 environment.

- Pop out the application in a new window by clicking the **Pop Out** button.

- Note the URL used by the preview, it will look like this:

  ```
  https://0123456789abcdef0123456789abcdef.vfs.cloud9.us-west-2.amazonaws.com/
  ```

  You will use this URL in the next section when configuring your Cognito user pool. Paste this URL into a text editor for future reference.

3. Set up an Amazon Cognito user pool.

- In the AWS Console, go to the **Amazon Cognito**

- Make sure you are still in the **Oregon (us-west-2)** region.

- Click **Manage your User Pools**.

- At the top right corner, click **Create a user pool**.

- For **Pool name**, type **photos-pool**.

- Click **Step through settings**.

- For **How do you want your end users to sign in?**, select **Email address or phone number**.

- For **Which standard attributes do you want to require?**, select **Nickname**.

- Click **Next step**.

- Leave the default settings on the Policy page and click **Next step**.

- Skip the MFA and verifications pages and click **Next step**.

- On the **Message customization** page, select **Verification Type** as **Link**. Feel free to customize the email body.

- Click **Next Step**.

- Skip the Tag section and click **Next Step**.

- Leave the default setting on the Devices page and click **Next step**.

- On the App Clients page, click **Add an app client**.

- For **App client name,** type a client name, for example, **WebsiteClient**.

- Leave the other default settings and click **Create app client**.

- Click **Next Step**.

- Skip the **Triggers** page and click **Next Step**

- On the **Review** page, click **Create Pool**.

- After the pool is created, write down the Pool ID for later use.

- In the left navigation menu, under **App integration**, click **App client settings**.

- For **Enabled Identity Providers**, check **Cognito User Pool**.

- For **Callback URL(s)**, enter the Cloud9 preview URL you noted in the previous step, then add **callback** to the end of the URL.

  As an example the **Callback URL(s)** will look like this **https://0123456789abcdef0123456789abcdef.vfs.cloud9.us-west-2.amazonaws.com/callback**

- For **Sign out URL(s)**, enter the Cloud9 preview URL.

  Note the **Sign out URL(s)** needs to end in the trailing slash, e.g. **https://0123456789abcdef0123456789abcdef.vfs.cloud9.us-west-2.amazonaws.com/**

- Under **OAuth 2.0**, for **Allowed OAuth Flows**, select **Authorization code grant** and for **Allowed OAuth Scopes**, select **openid**.

- Click **Save changes** at the bottom.

- In the left navigation menu, under **App integration**, click **Domain name**.

- Type a domain name, check its availability, and click **Save changes**. Write down the domain name for later use.

- In the left navigation menu, under **General settings**, click **App clients**.

- Click **Show details**.

- Make a note of the App client ID and App client secret for later use.

- Click **Return to pool details** at the bottom to return to the Pool details page.

4. Download and explore the exercise code.

- Type the command below in your AWS Cloud9 terminal to make sure you are in the ~/environment directory of your AWS Cloud9 instance.

```
cd ~/environment
```

- In your AWS Cloud9 environment, download the exercise code by typing the command below in the terminal.

```
wget https://us-west-2-tcdev.s3.amazonaws.com/courses/AWS-100-ADG/v1.1.0/exercises/ex-cognito.zip
```

- Unzip the exercise code .zip file by typing the command below in your AWS Cloud9 terminal.

```
unzip ex-cognito.zip
```

- Open the **exercise-cognito/FlaskApp/application.py** file. Scroll through the contents and find the routes for /login, /logout, and /callback. Notice that the Amazon Cognito settings are being pulled from the config file, **config.py**. You may explore the code by referring to the commented documentation links in each of the routes.

5. Configure the Amazon Cognito environment variables and run the exercise code.

- In your AWS Cloud9 environment, open the **exercise-cognito/FlaskApp/config.py** file.

- You should now see the environment variables COGNITO_POOL_ID, COGNITO_CLIENT_ID, COGNITO_CLIENT_SECRET, COGNITO_DOMAIN, and BASE_URL in the list of environment variables.

- In your AWS Cloud9 environment, on the **Python3RunConfiguration** pane at the bottom, click **ENV** on the right side. You should see a small list showing the previously configured environment variables.

- To configure the Amazon Cognito environment variables, type the environment variable **Name** and **Value** as shown in the table below:

COGNITO_POOL_ID	Copy and paste the pool ID you noted earlier.
COGNITO_CLIENT_ID	Copy and paste the App Client ID you noted earlier.
COGNITO_CLIENT_SECRET	Copy and paste the App Client Secret you noted earlier.
COGNITO_DOMAIN	Copy and paste the domain name you created earlier. It should look similar to the example below. Do not copy the entire URL starting with https://. YOUR_DOMAIN_NAME.auth.us-west-2.amazoncognito.com

BASE_URL	Copy and paste the Cloud9 preview URL you noted earlier. **Do not include a trailing /** for the BASE_URL. For example **https://0123456789abcdef0123456789abcdef.vfs.cloud9.us-west-2.amazonaws.com**

Note: Make sure to delete any white space that was inserted while copy/pasting.

- To run the exercise code, you will need to point the Run Configuration to the correct exercise folder. On the **Python3RunConfiguration** pane at the bottom, type the text shown below in the **Command** text box and click **Run**.

```
exercise-cognito/FlaskApp/application.py
```

You should see a message like the one below:

```
Running on http://0.0.0.0:8080/
```

6. Test the application.

- To test the application, click **Preview -> Preview Running Application** on the top menu bar of the Cloud9 environment.

- Pop out the application in a new window by clicking the **Pop Out** button.

- You should see your application with a message that reads, **Click log in/sign up to access this site**.

- Click **Log in/sign up** at the top right corner of the application and sign up for the application. This will take you through the email verification process and create an entry in the Amazon Cognito user pool directory.

- Upload a few photos and notice that there is a description text box that you can use to add a description to your photos.

- Click **My photos** at the top-right corner of the application. You should see your uploaded photos.

- Click **Home**. You should see a message that reads, **Click my photos to access your photos**. These means your photos are being saved and retrieved against your login.

- Sign out of the application and click **Home**.

- You should see a message that reads, **Click log in/sign up to access this site**. This means that you are now being authenticated to access your photos saved in the database via Amazon Cognito.

Optional Advanced Challenge 1

This one is an *advanced* challenge: can you add Log in with Amazon as a feature to your application?

- First you'll need to create an application with Log in with Amazon. For more information, see Getting Started for Web.

- In Cognito User Pools, you will need to add **Log in with Amazon** as an identity provider. For more information, see Adding Social Identity Providers to a User Pool.

- Enable **Log in with Amazon** as an identity provider with your Amazon Cognito app client

- The application wants a nickname. This will need to be mapped from a Log in With Amazon attribute to a User Pool attribute.

Optional Advanced Challenge 2

A second *advanced* challenge: the code is currently signing out users after the Amazon Cognito access_token expires. See below. *[Math Processing Error]*

```
   expires = datetime.utcfromtimestamp(session['expires'])
   expires_seconds = (expires -
datetime.utcnow()).total_seconds()
   if expires_seconds < 0:
      return None
```

The `refresh_token` from the Cognito response is being stored in a session variable. Instead of signing users out when the `access_token` expires, you can exchange the `refresh_token` for `id_token` and `access_token`. For more information, see <u>TOKEN Endpoint</u>. Replace the `return  None` code above with code to exchange the `refresh_token`. If successful, the user session can be repopulated and logged in with `flask_login.login_user`.

7. Stop the Amazon RDS database instance

In order to keep your AWS account bill at a minimum, consider stopping the Amazon RDS instance and then starting it again when needed. Follow the steps below to stop the Amazon RDS database instance.

- In the AWS Console, click **Services**, then click **Relational Database Service** to open the **Amazon RDS dashboard**.

- In the left navigation pane, click **Instances**. In the list of instances, select **edx-photos-db**.

- At the top, click **Instance actions**, and then **Stop**. You will see a prompt. Click **Yes, stop now**.