UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERÍA

Año 2020 - 1er Cuatrimestre

Taller de Programación II (75.52)

ChoTuve

AuthServer

Manual del Administrador

Fecha de entrega: 30/07/2020

Grupo 8

79979 – Gonzalez, Juan Manuel (juanmg0511@gmail.com)
82449 – Laghi, Guido (guido321@gmail.com)
86429 – Casal, Romina (casal.romina@gmail.com)
96453 – Ripari, Sebastian (sebastiandripari@gmail.com)
97839 – Daneri, Alejandro (alejandrodaneri07@gmail.com)

Contenido

1. Objetivo

El objetivo de este documento es proveer una guía práctica para descargar, configurar y ejecutar una instancia del AuthServer utilizado en la aplicación ChoTuve.

El resultado de completar los pasos aquí detallados permitirá al administrador contar con una copia inicializada y totalmente funcional del AuthServer, configurada a su gusto.

2. Instalación

En esta sección se describen los requisitos previos y las acciones necesarias para generar una copia local del AuthServer. Adicionalmente, se explica como generar un *tarball* con los archivos fuentes, para su distribución.

Para poder comenzar, se necesitará navegar al repositorio de GitHub donde se encuentra disponible el código fuente:

https://github.com/juanmg0511/fiuba-taller-2-auth-server

2.1 Requisitos previos

Los requisitos previos para el **deploy** son los siguientes:

1. Contar con Docker instalado en el equipo:
    a. Docker engine v19.03.08 o superior.
    b. Compose v1.25.5 o superior.
    c. No es necesario estar registrado en Docker.
2. Acceso a un servidor SMTP, si se desea habilitar la funcionalidad de envío de correos.
3. Un set de “Oauth Credentials” para Web Application de Google, si se desea utilizar la funcionalidad de *Login with Google*.
4. Si se desean hacer pruebas, deberá contarse con un cliente REST como Advanced Rest Client (ARC), o alguna otra forma de realizar *requests* sobre el servidor.

Nota: no existe un requerimiento fuerte de hardware o de sistema operativo, estos se ven satisfechos junto a Docker.

Los requisitos para generar los *distributables* mediante **setuptools** son:

1. Python v3.7.7 o superior.
2. Setuptools v47.1.1 o superior.

Nota: no existe un requerimiento fuerte de hardware o de sistema operativo, alcanza con poder ejecutar scripts de Python en el equipo en el que se desee realizar la operación.

2.2 Deploy Local

Para realizar el deploy local del ambiente deberán seguirse estos pasos:

1. Clonar el repositorio de GitHub a un directorio, por ejemplo:

```
~/taller-2-fiuba-auth-server
```

2. Verificar la existencia de los archivos, en el *root*:

```
Dockerfile
docker-compose.yml
Requirements.txt
```

2.3 Uso de Setuptools

En caso de querer contar con un archivo para distribución de los fuentes, se incluye un archivo *setup.py* que puede ser utilizado con tal propósito.

La lista de pasos a seguir es la siguiente:

1. Clonar el repositorio de GitHub a un directorio, por ejemplo:

```
~/taller-2-fiuba-auth-server
```

2. Ejecutar el siguiente comando, en dicho directiorio:

```
python setup.py sdist
```

3. Como resultado, se habrá creado un sub-directorio *dist* donde se encontrará el siguiente archivo con los fuentes de la aplicación:

```
fiuba-taller-2-auth-server-1.0.tar.gz
```

3. Configuración

En esta sección se exponen los pasos necesarios para configurar el *deploy* realizado en la sección anterior.

Cabe destacar que existen configuraciones propias de Compose, y otras del AuthServer: estas últimas se pueden controlar mediante el uso de variables de entorno. Adicionalmente, prácticamente todos estos settings traen valores propuestos pre-completados, a fin de facilitar el proceso.

Como última barrera, el código también provee valores default hardcodeados para los valores críticos, pueden consultarse en los archivos fuente.

3.1 Configuraciones propias de Compose

Estas configuraciones se realizarán sobre el siguiente archivo, localizado en el root del directorio seleccionado en el paso 2.2.1:

`docker-compose.yml`

Los valores editables son:

Clave	Valor default	Descripción
ports	80:8000	Vincula el valor del puerto del container con el frontend (8000) con el equipo local (80).
ports	27017:27017	Vincula el valor del puerto del container con la base de datos (27017) con el equipo local (27017). **Comentado por default, no se expone la DB al equipo local.**

3.2 Variables de entorno

Estas configuraciones se realizarán sobre el siguiente archivo, localizado en el root del directorio seleccionado en el paso 2.2.1:

`docker-compose.yml`

En la tabla expuesta a continuación pueden consultarse todos los valores configurables. Los

resaltados en amarillo no tienen valor asignado por default, por lo que se recomienda completarlos. En caso de que esto no se hiciera, el sistema mostrará los *WARNINGS* correspondientes en los logs y no podrá utilizarse la funcionalidad asociada.

En particular, se trata del envío de notificaciones por correo electrónico y de la integración de Sign In with Google:

- Si se activa el envío de correos utilizando `SENDMAIL_ACTIVE`, pero no son correctos los datos asociados, el envío de correos producirá una excepción que será logueada por el sistema.
- Si el client ID de Google no es correcto o está vacío, el login de usuarios que utilicen el servicio de Sign In with Google siempre devolverá código 401.

Clave	Valor default	Descripción
GUNICORN_LOG_LEVEL	debug	El nivel de log a usar por Gunicorn: "debug", "info", "warning", "error", "critical".
GUNICORN_WORKERS	4	Cantidad de workers a utilizar por Gunicorn para ejecutar las tareas.
APP_PORT	8000	El puerto que utilizará Gunicorn en el container donde ejecuta.
APP_SERVER_API_KEY	ef00a570-7cfc-4638-8cad-d085fd98b6e3	La clave que protege la API.
SESSION_LENGTH_USER_MINUTES	120	El tiempo de duración en minutos de un delta de sesión de usuario.
SESSION_LENGTH_ADMIN_MINUTES	10	El tiempo de duración en minutos de un delta de sesión de administrador.
RECOVERY_LENGTH_MINUTES	7200	El tiempo de validez en minutos de un pedido de recuperación de contraseña.
PRUNE_INTERVAL_SESSIONS_SECONDS	60	El intervalo de tiempo en segundos entre ejecuciones de la tarea programada que limpia sesiones vencidas.
PRUNE_INTERVAL_RECOVERY_SECONDS	120	El intervalo de tiempo en segundos entre ejecuciones de la tarea programada que limpia

		pedidos de recuperación de contraseña vencidas.
SENDMAIL_ACTIVE	0	Utilizar la funcionalidad de envío de correos de recuperación de contraseña.
SENDMAIL_SERVER	in-v3.mailjet.com	Ruta del servidor SMTP.
SENDMAIL_FROM	*	Dirección de envío de los correos de recuperación de contraseña.
SENDMAIL_PORT	465	Puerto utilizado por el servidor SMTP.
SENDMAIL_USERNAME	*	Usuario para el servidor SMTP.
SENDMAIL_PASSWORD	*	Contraseña para el servidor SMTP.
SENDMAIL_USE_TLS	0	Define si utilizar TLS en el servidor SMTP.
SENDMAIL_USE_SSL	1	Define si utilizar SSL en el servidor SMTP.
SENDMAIL_BASE_URL	https://fiuba-taller-2-web-admin-st.herokuapp.com	URL de base en los links del mail de recuperación de contraseña.
GOOGLE_CLIENT_ID	*	Client ID de Google, utilizado en la funcionalidad de *Sign in with Google*.

3.3 Configuración de Gunicorn

A continuación se detallan las configuraciones más importantes de Gunicorn que pueden variarse, sin alterar el funcionamiento del AuthServer:

Estas configuraciones se realizarán sobre el siguiente archivo, localizado en el root del directorio seleccionado en el paso 2.2.1:

`gunicorn_config.py`

Los valores editables son:

Clave	Valor default	Descripción
proc_name	auth_server	Nombre del proceso del AuthServer.

3.4 Condiciones de inicialización

Completos los pasos de instalación y configuración, se obtendrá un un ambiente integrado de front end y base de datos, escuchando conexiones en el puerto 80 del equipo sobre el que sea ejecutado docker-compose.

El mismo tendrá una base de datos vacía, inicializada con las estructuras correspondientes (estos valores son configurados por variables de entorno en `docker-compose.yml`, pero se recomienda no cambiarlos para tareas de desarrollo o pruebas):

- Nombre de la base: “auth-server-db”
- Usuario administrador y password: “sa” / “123456”
- Usuario de aplicación y password: “authserveruser” / ”123456”

Las variables en `docker-compose.yml` que controlan estos valores son:

Clave	Valor default	Descripción
MONGODB_DATABASE	auth-server-db	El nombre de la base de datos a la que se conectará el frontend.
MONGODB_USERNAME	authserveruser	Usuario que utilizará el frontend para conectarse a la base de datos
MONGODB_PASSWORD	123456	La contraseña a utilizar por el frontend para conectarse a la base de datos.
MONGODB_HOSTNAME	auth-server-mongodb	En nombre del container donde se encuentra el servidor de base de datos.
MONGODB_PORT	27017	El puerto a utilizar por el frontend para conectarse a la base de datos.
MONGO_INITDB_ROOT_USERNAME	sa	Nombre de usuario administrador para el servidor de base de datos.

MONGO_INITDB_ROOT_PASSWORD	123456	Contraseña para el usuario administrador para el servidor de base de datos.
MONGO_NON_ROOT_USERNAME	authserveruser	Nombre de usuario de aplicación para el servidor de base de datos.
MONGO_NON_ROOT_PASSWORD	123456	Contraseña de usuario de aplicación para el servidor de base de datos.
MONGODB_DATABASE	auth-server-db	Nombre de base de datos inicial para el servidor de base de datos.

El AuthServer contará además con un solo usuario administrador, generado con los siguientes datos:

```
{
      'username':'chotuvegod',
      'password':'Ais!rTFC23X$%scd3&/',
      'first_name':'Chotuve',
      'last_name':'God',
      'email':'chotuve.god@heaven.org',
      'Account_closed':false,
      'date_created':'2020-05-10T23:33:14.921956',
      'date_updated': null
}
```

Los datos presentes en la base se guardarán en un volumen, el cual persiste entre ejecuciones del ambiente. Para resetear la base de datos, basta con eliminar de docker-compose el volumen del *container* de la base de datos (mongodbdata).

4. Ejecución

Luego de completados los pasos de instalación y configuración, podrá procederse a levantar el ambiente. Para ello, se deberán ejecutar los siguientes dos comandos, desde el directorio definido en el punto 2.2.1:

```
docker-compose build
docker-compose up
```

El primer comando generará el ambiente, por lo que la primera vez puede tardar aproximadamente unos 5 minutos mientras todas las imágenes y dependencias son bajadas de Internet. El segundo levantará el ambiente, dejándolo listo para recibir conexiones. El *shell* será ocupado por el output de ambos containers.

Aquí podrá visualizarse en forma de log los valores configurados, por ejemplo:

```
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [DEBUG] Log system configured for Gunicorn.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [DEBUG] API key is: "ef00a570-7cfc-4638-8cad-d085fd98b6e3".
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Session length for users is: 120 minutes.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Session length for admins is: 10 minutes.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Recovery length is: 7200 minutes.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Prune interval for sessions is: 60 seconds.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Prune interval for recovery is: 120 seconds.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [WARNING] Send mail functionality is DISABLED. Please enable
"SENDMAIL_ACTIVE".
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Mail server: "in-v3.mailjet.com".
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Port: 465.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Use TLS: False.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Use SSL: True.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Recovery base URL:
"https://fiuba-taller-2-web-admin-st.herokuapp.com".
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Google login configured.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [INFO] Client ID: "*".
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [DEBUG] Configuring BackgroundScheduler for Gunicorn.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [DEBUG] Configuring session prune job, interval 60 seconds.
auth-server-flask | [2020-06-05 18:47:32 +0000] [1] [DEBUG] Configuring recovery prune job, interval 120 seconds.
```

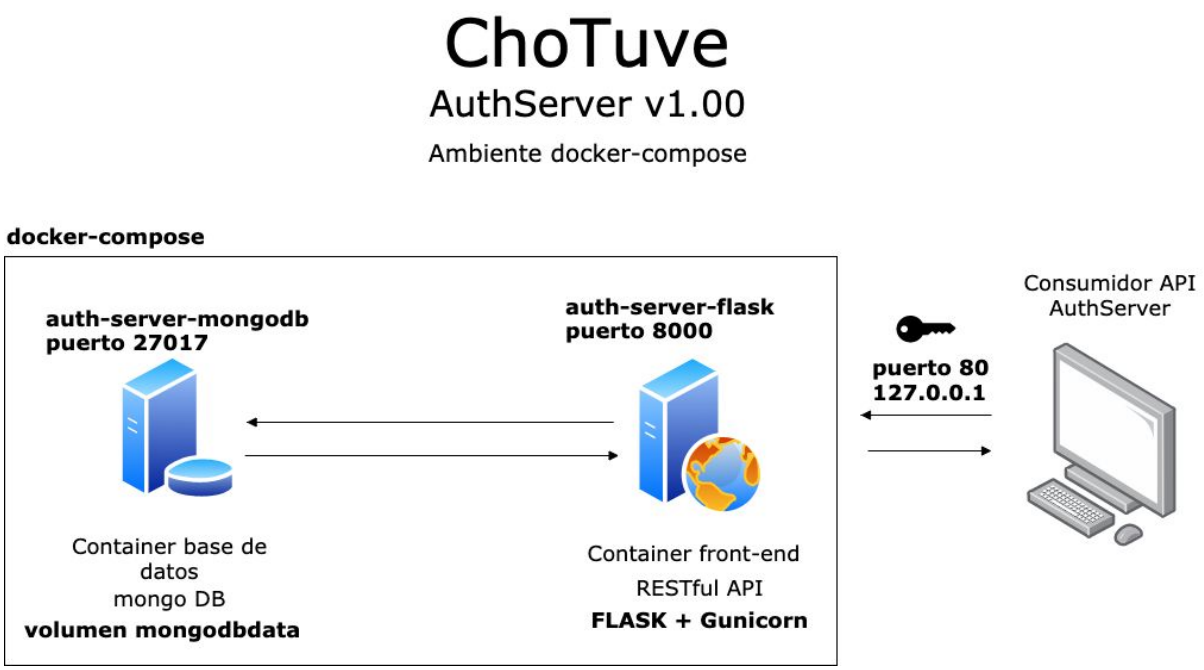
Si se deseara ejecutar el ambiente en forma de *daemon*, el segundo comando debe reemplazarse por el siguiente:

```
docker-compose up -d
```

Para ejecutar las pruebas que vienen incluidas con la aplicación, pueden ejecutarse los siguientes comandos:

```
docker exec -u root -it auth-server-flask bash -c "coverage run --omit
*/virtualenv/* -m unittest tests/*.py -v"
docker exec -u root -it auth-server-flask bash -c "coverage report"
```

Esquemáticamente, a nivel ambiente, el resultado obtenido será:



De esta forma, y con una configuración adecuada de puertos, podrían levantarse los tres servers de la solución en el mismo equipo, para realizar por ejemplo tareas de desarrollo.