Teclado

Deploying with uWSGI and nginx

This is a tutorial on setting up a server on DigitalOcean, a cloud computing platform. We will go through the whole process, from creating an account to setting up a server and connecting to it.

> Are you looking for a guide on setting up your DigitalOcean server? Check out this guide instead!

Connecting to our server

In order to connect to our server, we need to use a tool called `SSH` (Secure Shell). We can SSH our server using the command:

```
ssh root@<your server ip>
```

You will be asked for the root password (or the SSH key if you have set it up previously). Beware that `SSH` command only works on `UNIX`, not on `Windows`. However, there are plenty of software that you can use to SSH from Windows, PuTTy is a popular choice.

After connecting to our server and logging in as the `root` user, it is recommended to run the below command first to get all the available updates:

```
apt-get update
```

We can use the following command to install packages:

```
apt-get install <package1> <package2>
```

Note that this is a just an example to install different packages using one command, we will see real use cases in the following sections.

Creating another user

Since the `root` user is the most powerful, essentially a root user can do everything on the server, so we may want to limit access to it to improve security. So in this section, we will create a new user and configure it to "act like" a `root` user but with certain limitations, and we will login as this user from then on. It is highly recommended to do so.

Hello, John Doe

In this section, we will create a user named `johndoe`. You may choose any name you want, just remember to swap `johndoe` with your username for each command and configuration. We can create a new user `johndoe` with the following command:

```
adduser johndoe
```

You will be asked to enter and confirm the password for this user, and then provide some info about this user. Notice that you can leave the info sections blank if you want to. And if you entered unmatching passwords, just complete the info section and we can change the password later by using the command:

```
passwd johndoe
```

Providing user with additional privilege

Since we will be logging in as `johndoe` for most of the time in the future, we will want it to have some “extra power”, that is, temporarily acting as a super user. To do this, we need to run the command:

```
visudo
```

First, and we will see a text file popping up. Then we navigate to the lines containing:

```
# User privilege specification
root ALL=(ALL:ALL) ALL
```

You can do this with the arrow keys. We need to add a new line for our user in this section:

```
# User privilege specification
root ALL=(ALL:ALL) ALL
johndoe ALL=(ALL:ALL) ALL
```

Remember that the `ALL` has to be **all uppercase**, otherwise it will raise syntax error.

After adding this line, use `ctrl + o` to save and press `ENTER` to overwrite, then press `ctrl + x` to quit.

Enabling SSH for our new user

Next, we want to allow us to login as `johndoe` using SSH, and we may also want to disable login as `root` from SSH to make our server more secure. To do this, use the command:

```
vi /etc/ssh/sshd_config
```

And we will be prompted with another text file. Navigate to the section which contains:

```
# Authentication
PermitRootLogin yes
```

Press `i` on your keyboard to enter insert mode and change the `yes` to `no` to disallow login as root.

Next, look for a configuration called `PasswordAuthentication`:

```
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication yes
```

Important: make sure to set it as `yes` so that you can use your password to login in the future. It should be set to `yes` already, however, there are some platforms that enforces SSH key authentication and set it to `no` instead.

Then go to the bottom of the file and add the following lines:

```
AllowUsers johndoe
```

For this section, if you already have other users on the server, make sure to include them as well. On AWS, for instance, a user named `ubuntu` is initialized and used to login for the first time. If you choose to create a new user, say `johndoe`, then you will need to add them together into `AllowUsers`:

```
AllowUsers johndoe ubuntu
```

Otherwise, you will no longer be able to login as `ubuntu` in the future.

Next, press `Esc` to quit insert mode, press `:` (colon) to enable the command function and enter `wq` to write and quit (after hitting `ENTER` to confirm).

Some other useful vi commands are: `:q` to quit without modification and `:q!` to force quit and discard changes.

Finally, we use the command:

```
service sshd reload
```

to enable our modifications.

Now we've created a new user `johndoe` and enabled both its super user privilege and SSH access. Next, we'll be learning to link this user to our PostgreSQL database.

Configuring Postgres

Postgres allows from the start a user to access a database with its own name. Thus we must create a `johndoe` user inside PostgreSQL, and create a `johndoe` database in PostgreSQL.

Because we have a `johndoe` user in our server, it will automatically have permission to access the `johndoe` user in Postgres, and will be able to access the `johndoe` database.

Installing PostgreSQL

```
apt-get install postgresql postgresql-contrib
```

Creating a Postgres user

We use the following command to switch to a super user in Postgres named `postgres` and use it to create a Postgres user:

```
sudo -i -u postgres
createuser johndoe -P
```

After inputting and confirming the password, we now have created a Postgres user. Remember that we use the same username `johndoe` to create the Postgres user, since by default, Postgres only allows the UNIX user with the same name as its Postgres user to interact with it.

Creating a PostgreSQL database for our user

After having created the Postgres user, we use the command

```
createdb johndoe
```

to create a database also name `johndoe`. Now, our UNIX user `johndoe` can directly interact with the PostgreSQL database named `johndoe` using the command:

```
psql
```

Some useful Postgres commands

To see the current connection info, use:

```
\conninfo
```

To quit Postgres:

```
\q
```

Improving security on our PostgreSQL database

However, notice that we've created a password for the Postgres user but never have to use it just because we used the same username in UNIX and Postgres. It is safer to require a password when connecting to the database. Use the below command to configure Postgres security options.

```
sudo vi /etc/postgresql/9.5/main/pg_hba.conf
```

Navigate to the bottom of the file, and we may see something like this:

```
# Database administrative login by Unix domain socket
local   all             postgres                                peer

# TYPE  DATABASE        USER            ADDRESS                 METHOD

# “local” is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             all             127.0.0.1/32            md5
# IPv6 local connections:
host    all             all             ::1/128                 md5
```

Change the line

```
local   all             all                                     peer
```

to

```
local   all             all                                     md5
```

to enable password authentication.

Important: SQLAlchemy will not work unless we do this modification.

Getting code from GitHub

In this section, we will pull our code from `GitHub`, which integrates a popular VCS (Version Control System) called `Git`. `Git` is a very good tool to manage and access your code both locally and remotely.

Setting up our app folder

First, we create a folder called `items-rest` for our app, since our sample project is a REST API which manages items of stores. We create this folder using the following command:

```
sudo mkdir /var/www/html/items-rest
```

The folder is owned by the `root` user since we used `sudo` to create it. We need to transfer ownership to our current user:

```
sudo chown johndoe:johndoe /var/www/html/items-rest
```

Remember that `johndoe` is the username in our tutorial, make sure you change it to yours accordingly. The same goes for `items-rest`.

Next, we get our app from `Git`:

```
cd /var/www/html/items-rest/
git clone https://github.com/schoolofcode-me/stores-rest-api.git .
```

Note that there's a trailing space and period (`.`) at the end, which tells `Git` the destination is the current folder. If you're not in this folder `/var/www/html/items-rest/`, remember to switch to it or explicitly specify it in the `Git` command. And for the following commands in this section, we all assume that we are inside the folder `/var/www/html/items-rest/` unless specified otherwise.

In order to store logs, we need to create a log folder, (under `/var/www/html/items-rest/`):

```
mkdir log
```

Then we will install a bunch of tools we need to set up our app:

```
sudo apt-get install python-pip python3-dev libpq-dev
```

Next, we will install `virtualenv`, which is a python library used to create virtual environment. Since we may want to deploy several services on one server in the future, using virtual environment allows us to create independent environment for each project so that their dependencies won't affect each other. We may install `virtualenv` using the following command:

```
pip install virtualenv
```

After it is installed, we can create a `virtualenv`:

```
virtualenv venv --python==python3.5
```

Note that `Ubuntu` usually comes with `Python3.5` and it is what we used in the sample code, if you choose to use different versions of `Python`, feel free to change it accordingly and it will be the Python version inside your `virtualenv`.

To activate `virtualenv`:

```
source venv/bin/activate
```

You should see `(venv)` appears at the start of your command line now. We assume that we are in `virtualenv` for all the following commands in this section unless specified otherwise.

Next, use the command below to install the specified dependencies:

```
pip install -r requirements.txt
```

`requirement.txt` is a text file that includes all the dependencies that we created in our `Git` folder. It's highly recommended to have a `requirements.txt` file with all libraries your project requires.

Note that when installing these requirements, we are inside the virtual environment `venv`, so all the libraries are installed into `venv`, and once we quit `venv`, these libraries won't take effect.

Hint: to quit a virtual environment, use the command `deactivate`.

uWSGI

In this section, we will be using `uWSGI` to run the app for us, in this way, we can run our app in multiple threads within multiple processes. It also allow us to log more easily. More details on `uWSGI` can be found here.

First, we define a `uWSGI` service in the system by:

```
sudo vi /etc/systemd/system/uwsgi_items_rest.service
```

And the content we are going to input is shown below:

```
[Unit]
Description=uWSGI items rest

[Service]
Environment=DATABASE_URL=postgres://johndoe:<johndoe_postgres_
password>localhost:5432/johndoe

ExecStart=/var/www/html/items-rest/venv/bin/uwsgi --master --emperor /var/www/html/
items-rest/uwsgi.ini --die-on-term --uid johndoe --gid johndoe --logto /var/www/
html/items-rest/log/emperor.log

Restart=always
KillSignal=SIGQUIT
Type=notify
NotifyAccess=all

[Install]
WantedBy=multi-user.target
```

We will explain the basic idea of these configs. Each pair of square brackets `[]` defines a `section` which can contain some properties.

The `Unit` section simply provides some basic description and can be helpful when looking at the logs.

The `Service` section contains several properties related to our app. The `Environment` properties defines all the environment variables we need in our code. In our sample code, we want to retrieve the `DATABASE_URL` from system environment. And this is the place where you should keep all your secrets, such as secret keys and credentials. Beware that the `DATABASE_URL` should follow the format:

```
<database_type>://<db_username>:<db_user_password>@localhost:<db_port>/<db_name>
```

If we want to add multiple environment variables, we just need to add multiple lines of the `Environment` entry following the syntax:

```
Environment=key=value
Environment=key=value
```

```
Environment=key=value
...
```

The `ExecStart` property informs `uWSGI` on how to run our app as well as log it.

At last, the `WantedBy` property in `Install` section allows the service to run as soon as the server boots up.

Important: remember to change the username, password, database name and service name/folder accordingly in your own code.

Hint: after editing the above file, press `ESC` to quit insert mode and use `:wq` to write and quit.

Configuring uWSGI

Our next step is to configure `uWSGI` to run our app. To do so, we need to create a file named `uwsgi.ini` with the following content:

```
[uwsgi]
base = /var/www/html/items-rest
app = run
module = %(app)

home = %(base)/venv
pythonpath = %(base)

socket = %(base)/socket.sock

chmod-socket = 777

processes = 8

threads = 8

harakiri = 15

callable = app

logto = /var/www/html/items-rest/log/%n.log
```

Note that you should change the `base` folder accordingly in your own app. For the second entry, `run` is referred to the `run.py` in our sample app, which serves as the entry point of our app, so you may need to change it accordingly in your own project as well. We defined the `socket.sock` file here which will be required by the `nginx` later. The socket file will serve as the connection point between `nginx` and our `uWSGI` service.

We asked for 8 processes with 8 threads each for no particular reason, you may adjust them according to your server capacity and data volume. The `harakiri` is a Japanese word for suicide, so in here it means for how long (in seconds) will the `emperor` kill the thread if it has failed. This is also an advantage we have with `uWSGI`, it allows our service to be resilient to minor failures. And it also specifies the log location.

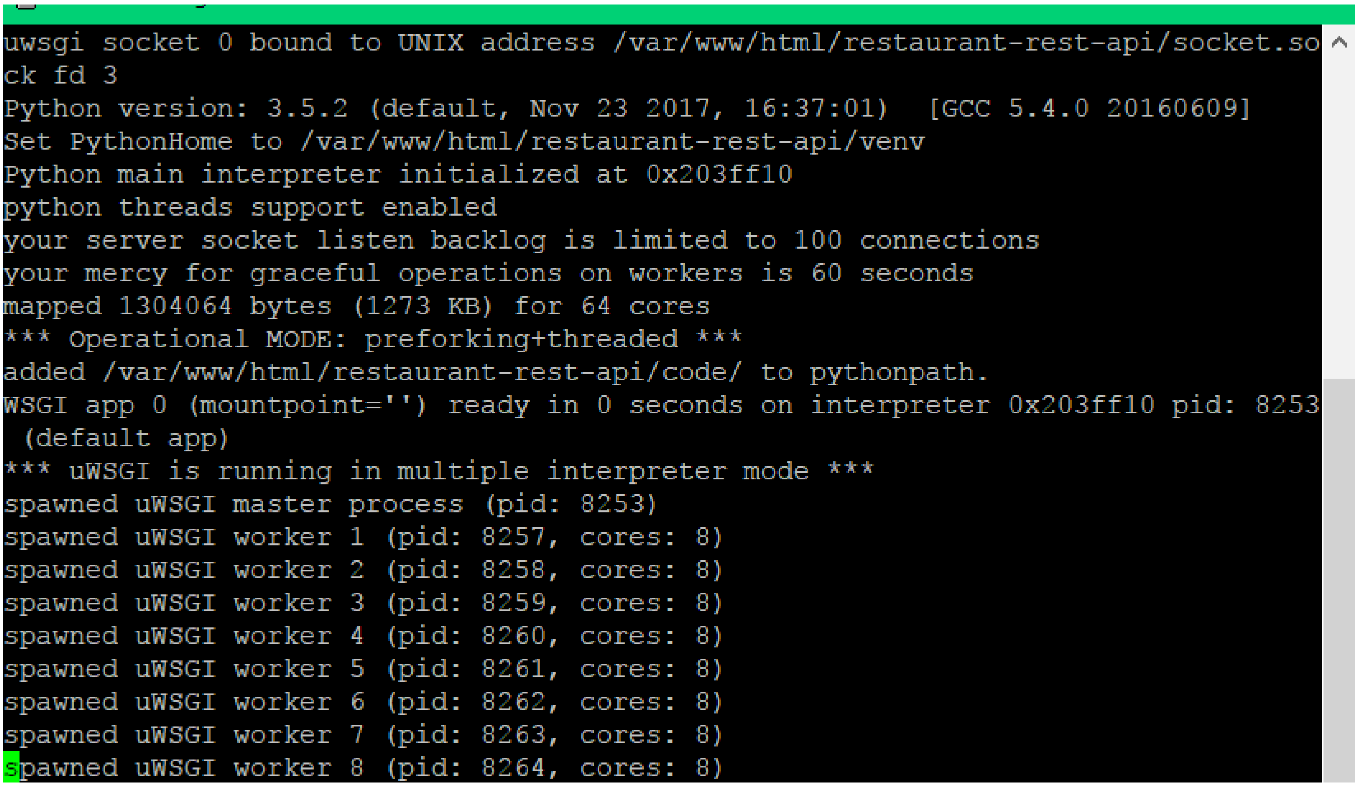
And at last, after saving the above file, we use the command below to run the `uWSGI` service we defined earlier:

```
sudo systemctl start uwsgi_items_rest
```

And we should be able to check the `uWSGI` logs immediately to make sure it's running by using the command:

```
vi log/uwsgi.log
```

If anything is running normally, we should be seeing something like this:



```
uwsgi socket 0 bound to UNIX address /var/www/html/restaurant-rest-api/socket.so
ck fd 3
Python version: 3.5.2 (default, Nov 23 2017, 16:37:01)  [GCC 5.4.0 20160609]
Set PythonHome to /var/www/html/restaurant-rest-api/venv
Python main interpreter initialized at 0x203ff10
python threads support enabled
your server socket listen backlog is limited to 100 connections
your mercy for graceful operations on workers is 60 seconds
mapped 1304064 bytes (1273 KB) for 64 cores
*** Operational MODE: preforking+threaded ***
added /var/www/html/restaurant-rest-api/code/ to pythonpath.
WSGI app 0 (mountpoint='') ready in 0 seconds on interpreter 0x203ff10 pid: 8253
 (default app)
*** uWSGI is running in multiple interpreter mode ***
spawned uWSGI master process (pid: 8253)
spawned uWSGI worker 1 (pid: 8257, cores: 8)
spawned uWSGI worker 2 (pid: 8258, cores: 8)
spawned uWSGI worker 3 (pid: 8259, cores: 8)
spawned uWSGI worker 4 (pid: 8260, cores: 8)
spawned uWSGI worker 5 (pid: 8261, cores: 8)
spawned uWSGI worker 6 (pid: 8262, cores: 8)
spawned uWSGI worker 7 (pid: 8263, cores: 8)
spawned uWSGI worker 8 (pid: 8264, cores: 8)
```

But if there is any error in our code, it will also be reflected in the log.

Nginx

`nginx` (engine x) is an HTTP and reverse proxy server, a mail proxy server, and a generic TCP/UDP proxy server. In this tutorial, we use `nginx` to direct traffic to our application. `nginx` can be really helpful in scenarios like running our app on multiple threads, and it performs very well so we don't need to worry about it slowing down our app. More details about `nginx` can be found here.

Installing nginx

```
sudo apt-get install nginx
```

Configuring the firewall to grant access to nginx

First, check if the firewall is active:

```
sudo ufw status
```

If not, we will enable it later. Before that, let's add some new rules:

```
sudo ufw allow 'Nginx HTTP'
sudo ufw allow ssh
```

Important: the second line, adding SSH rules, is not related to `nginx` configuration, but since we're activating the firewall, we don't want to get blocked out of the server!

If the UFW (Ubuntu Firewall) is inactive, use the command below to activate it:

```
sudo ufw enable
```

To check if `nginx` is running, use the command:

```
systemctl status nginx
```

Some other helpful command options for system controller are:

```
systemctl start <service_name>
systemctl restart <service_name>
systemctl reload <service_name>
systemctl stop <service_name>
```

Configuring nginx for our app

Before deploying our app onto the server, we need to configure `nginx` for our app. Use the below command to create a config file for our app:

```
sudo vi /etc/nginx/sites-available/items-rest.conf
```

Note that `items-rest` is what we named our service, you may change it accordingly, but remember to remain consistent throughout the configurations.

Next, we input the below text into `items-rest.conf` file. **Remember to change your service name accordingly in this file as well**.

```
server {
  listen 80;
  real_ip_header X-Forwarded-For;
  set_real_ip_from 127.0.0.1;
  server_name localhost;

  location / {
    include uwsgi_params;
    uwsgi_pass unix:/var/www/html/items-rest/socket.sock;
    uwsgi_modifier1 30;
  }

  error_page 404 /404.html;
  location = /404.html {
    root /usr/share/nginx/html;
  }

  error_page 500 502 503 504 /50x.html;
  location = /50x.html {
    root /usr/share/nginx/html;
  }
}
```

The above config allows `nginx` to send the request coming from our user’s browser to our app. It also sets up some error pages for our service using `nginx` predefined pages.

And at last, in order to enable our configuration, we need to do something like this:

```
sudo rm /etc/nginx/site-enabled/default
sudo ln -s /etc/nginx/sites-available/items-rest.conf /etc/nginx/sites-enabled/
```

We need to remove the default file since `nginx` will look at this file by default. We want `nginx` to look at our config file instead, thus we added a soft link between our config file and the `site-enabled` folder.

Running our app

Finally, we can launch our app! We can do so by starting the `nginx` and `uWSGI` services we defined (we already started the `uWSGI` service in the previous section).

```
sudo systemctl start nginx
```

If any of these services is already running, you may use the below commands (taking `nginx` for example) to reload and restart it so that it has the latest changes.

```
sudo systemctl reload nginx
sudo systemctl restart nginx
```

Deployment wrap-up

As the tutorial is very detailed, you may find it a bit hard to put the pieces together. Here's a quick wrap-up that may help you sort things out.

- We created a `UNIX` user and granted him some privilege.
- We set up `PostgreSQL` database and configured our user to interact with it.
- We used `uWSGI` to run our app multi-processly and multi-threadly.
- We used `nginx` to direct requests to our `uWSGI` service.

Thanks for reading!