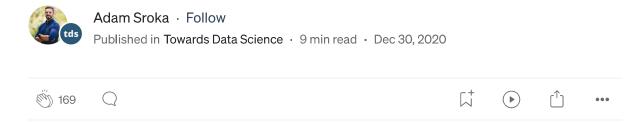


Docker for data scientists-Part 2

A complete guide to develop a machine learning model, write an API, package it in Docker, run it anywhere, and share it with ease.





Docker for data scientists — an end-to-end guide (photo by Rémi Boudousquié on Unsplash).

Overview

In <u>Docker for data scientists</u> — <u>Part 1</u> we covered some of the basics around using Docker and got a simple Hello World! example up and running. If you missed that post and want to run through the code, you can find it here:

Docker for data scientists — Part 1

The basics. A quick guide for data scientists and machine learning engineers to get started with Docker and...

towardsdatascience.com

Our aim in this post is to move on to an example of how a data scientist or machine learning engineer might want to use Docker to share, scale, and productionise their projects.

We'll work our way through the following topics:

- Model serving develop and deploy an API for a simple model
- Serialising models storing and sharing models in Python
- APIs with Flask a very simple example of a prediction API
- Images packaging everything up and running in a container
- Repositories share your work
- Machine learning at scale Introducing <u>Docker Swarm</u> and <u>Kubernetes</u>
- Next steps <u>DataOps</u>, <u>MLOps</u>, and machine learning engineering

Model serving — develop a model, an API, and serve using docker

Example: a random forest classifier for the Iris dataset

To keep things simple, we'll build a simple model for the well-known <u>Iris</u> <u>dataset</u>. We'll write a straightforward API allowing users to call that model to predict on an array. Then, I'll walk through the process of packaging and sharing the whole thing with Docker.

Get data

First, let's get the data. As it's a super-common demo dataset, we can import it directly from <u>scikit-learn</u> within our script using:

Or, if you want the .csv you can get it from GitHub using the terminal with:

It should look something like this:

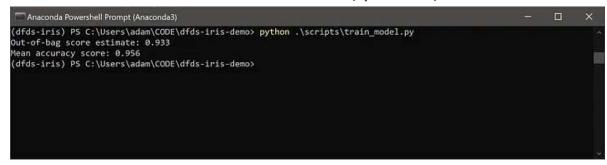
Downloading the Iris dataset as a .csv from GitHub (image by author).

Note: If your terminal is Powershell or the Anaconda PowerShell Prompt on Windows this may not work. By default, PowerShell has the Invoke-WebRequest

command aliased to curl and it may behave differently. Either install <u>cURL</u> using <u>Chocolatey</u> using choco install curl or use whatever method you normally do for getting datasets.

Creating the model

We are going to quickly spin up a <u>Random Forest</u> model. Create a new folder called scripts and in it, a new file called train_model.py in which we'll write some simple code for building the model, as follows:



The output from our simple model creation script giving out-of-bag score and mean accuracy (image by author).

We could go further by looking at the confusion matrix, the ROC curve, and tweaking the features and hyperparameters. I won't just here to keep the example simple — but please take the time to tweak this for your application.

Serialising models

Once we have a model we're happy with, we want to store it. There are a few methods for achieving this. Here we're just going to use <u>Pickle</u> to keep things simple. Pickle allows us to convert between Python in-memory objects and streams of bytes — for transfer over networks or storage on a local filesystem.

Pickle syntax is quite straightforward:

For a good introduction to Pickle check out Manu Kalia's post here:

Don't Fear the Pickle: Using Pickle.dump and Pickle.load

Improve your data science workflow with pickled Python objects shared amongst multiple Jupyter notebooks

medium.com

Now, to pickle our model, either make the changes to the file we have already train_model.py or you can create a new file with a name like build_model.py and put your modified code to build and serialise the model in there.

If you're modifying train_model.py add the import at the top and replace the print statement:

And you should now see the pickled model on your filesystem. To test this out, let's make a new file called <code>load_model.py</code> in which we'll load the model from the serialised object and run a prediction. The code will look something like this:

This should return the value [1] like this:

```
Anaconda Powershell Prompt (Anaconda3)

(dfds-iris) PS C:\Users\adam\CODE\dfds-iris-demo> python .\scripts\load_model.py

[1]
(dfds-iris) PS C:\Users\adam\CODE\dfds-iris-demo>
```

The output from our script testing the prediction from the pickled model (image by author).

There are a lot of advantages to this approach and you should consider using it in your workflows if you aren't already. You're now able to score with our

model without loading the supporting packages, and you can store and share versions of your model.

APIs with Flask

Now that we have our model let's put a quick <u>Flask</u> API around it. We're just going to add a simple score method around it that'll allow users to send an array and get a prediction in return.

We won't delve into error handling or anything here — you can do a lot with Flask and I'd highly recommend taking some time to learn it as adding APIs to your projects is both big and clever! A good place to start is this post by Bharat Choudhary which shows how to build a UI and everything for the Iris dataset:

Deployment of Machine learning project using Flask

machine-learning project in production.

medium.com

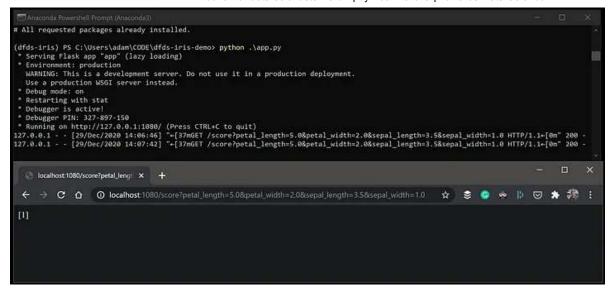
Create a new file called app.py and let's build a simple API that allows us to adjust the input parameters. In this case, we just need to adjust the values after each of the = signs. Our code will look like this:

```
# define imports
    from flask import Flask, request
    import pickle
    from numpy import array2string
5
    # define the path to the pickled model
    model_path = "rf-model.pkl"
7
8
    # unpickle the random forest model
    with open(model_path, "rb") as file:
10
11
         unpickled_rf = pickle.load(file)
12
    # define the app
13
     app = Flask(__name__)
14
15
16
17
     # use decorator to define the /score input method and define the predict function
18
     @app.route("/score", methods=["POST", "GET"])
19
     def predict_species():
20
         # create list and append inputs
21
         flower = []
22
         flower.append(request.args.get("petal_length"))
23
         flower.append(request.args.get("petal_width"))
24
         flower.append(request.args.get("sepal_length"))
25
         flower.append(request.args.get("sepal_width"))
26
27
         # return the prediction
28
         return array2string(unpickled_rf.predict([flower]))
29
30
    # run the app
31
32
     if __name__ == "__main__":
         app.run(host="0.0.0.0", debug=True, port="5001")
33
app.py hosted with 9 by GitHub
                                                                                               view raw
```

Now, if we run app.py we can test that this returns the same prediction as earlier by entering the following URL into our browser:

```
http://localhost:1080/score?
petal_length=5.0&petal_width=2.0&sepal_length=3.5&sepal_width=1.0
```

Your terminal and browser should now look something like this:



The Flask prediction wrapper for the Iris random forest model up and running, giving the same result for the test set as seen earlier (image by author).

Images — package, and run

conda list --export > requirements.txt

Now the model and app are built and working, we're ready to package them up using Docker. Firstly, we'll need to create a requirements.txt to capture all of the packages Python will need to run. This is easily achieved using:

Open in app 7

Open in app 7

Write Q T

Flask==1.1.2 numpy==1.19.4 scikit-learn==0.23.2

To keep things simple, if you've been working through all of the examples, create a new folder called production. In here, create the Dockerfile — remember this is a text file with the name Dockerfile and no extension. Then put a final copy of app.py, requirements.txt and rf-model.pkl. The folder should look like this:

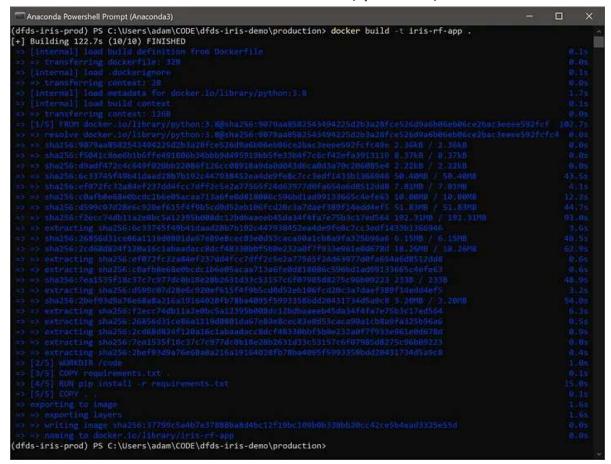
The contents of the Dockerfile are fairly straightforward as we can utilise existing Python images from <u>Dockerhub</u>. The Dockerfile will look like this:

```
# set base image (host OS)
    FROM python:3.8
 4 # set the working directory in the container
 5 WORKDIR /code
 6
 7 # copy the dependencies file to the working directory
    COPY requirements.txt .
10 # install dependencies
11
    RUN pip install -r requirements.txt
12
13
    # copy the content of the directory to the working directory
    COPY . .
14
15
     # command to run on container start
    CMD [ "python", "./app.py" ]
Dockerfile hosted with ♥ by GitHub
                                                                                            view raw
```

With this all in place we can build our image using:

```
docker build -t iris-rf-app .
```

If you haven't already downloaded the python:3.8 image, Docker will do so automatically. Overall this took just two minutes on my machine. Your terminal should look something like this:

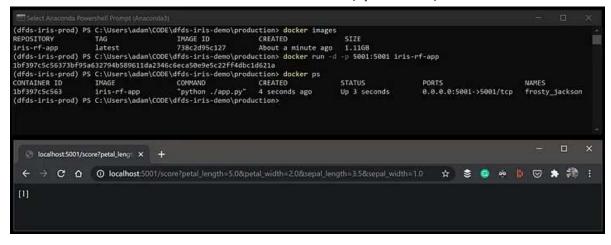


Docker downloading the base image and sequentially building our Iris Flask app on top of it. All in taking about two minutes (image by author).

We can now check the image exists with docker images and run it with:

```
docker run -d -p 5001:5001 iris-rf-app
```

Testing it with our test URL from before we get the same results. The output from the terminal and browser can be observed below:



Running the docker image and checking the output with our test URL as before (image by author).

We now have a working version of our model, with a simple API, that can be run anywhere we can run a Docker container. If we really wanted to we could ramp up our API and start using this approach to build end-to-end machine learning and data science pipelines.

Repositories — sharing your work

Sharing Docker images is also really straightforward. Once you've signed up for an account at <u>hub.docker.com</u> it's really easy to upload your images to the public repo from the command line.

First, you need to log in so your instance of Docker knows your credentials:

```
docker login -u <your_docker_id> --password <your_docker_password>
```

Once logged in you can now upload images to your repo. The only change we need to make is to add tags. This is done in the build stage and follows the format:

```
docker build -t <your_docker_id>/<image_name>:<image_version>
```

If you leave <image_version> blank Docker appends the latest tag to the image. Rebuilding my image gives the following:

```
Administrator: Anaconda Powershell Prompt (Anaconda3)
(dfds-iris-prod) PS C:\Users\adam\CODE\dfds-iris-demo\production> docker build -t asroka/iris-rf-app:1.0 .
[+] Building 2.8s (10/10) FINISHED
(dfds-iris-prod) PS C:\Users\adam\CODE\dfds-iris-demo\production> docker images
                                 IMAGE ID
738c2d95c127
738c2d95c127
REPOSITORY
                                                                    CREATED
                                                                                           SIZE
asroka/iris-rf-app
                      1.0
                                                                    27 minutes ago
                                                                                           1.11GB
                                                                    27 minutes ago
iris-rf-app
                      latest
                                                                                           1.11GB
(dfds-iris-prod) PS C:\Users\adam\CODE\dfds-iris-demo\production> _
```

Rebuilt Iris Flask app with my Docker ID, name, and tag (image by author).

Then you just need to push the image to the repo using:

docker push <your_docker_id>/<image_name>

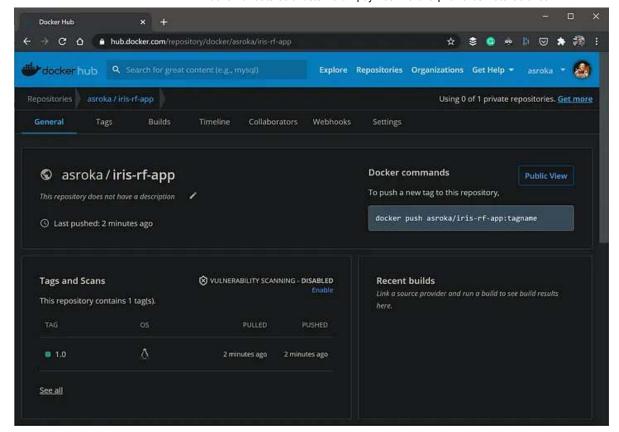
```
Administrator Anaconda Powershell Prompt (Anaconda3)

(dfds-iris-prod) PS C:\Users\adam\CODE\dfds-iris-demo\production> docker push asroka/iris-rf-app
The push refers to repository [docker.io/asroka/iris-rf-app]
c0c50f7d0ca8: Pushed
662d5a239f3e: Pushed
223e54ec996d: Pushed
864093696da4: Pushed
864093696da4: Pushed
8640e3f404a1: Mounted from library/python
e7f6ccee1295: Mounted from library/python
98864f0e5b9f: Mounted from library/python
598406625c92: Mounted from library/python
da87e334550a: Mounted from library/python
c5f4367d4a59: Mounted from library/python
193bc1d68b80: Mounted from library/python
f0e10b20de19: Mounted from library/python
```

Example output of the Docker push command (image by author).

As shown below, our image is now publically viewable by navigating to:

hub.docker.com/repository/docker/<your_docker_id>/<image_name>



Our Iris Flask app publically available on Docker hub (image by author).

If you want to give it a try, you can navigate to my repo shown above and pull and run that image using:

```
docker pull asroka/iris-rf-app:1.0
docker run -d -p 5001:5001 asroka/iris-rf-app:1.0
```

There are also plenty of ways of hosting private Docker repositories — perfect for sharing within your organisation or team. I won't touch on them in detail here but do check out the documentation as a starter <u>here</u>.

Machine learning at scale

So far we've looked at a very simple case but still, the approach here has many uses, allowing data scientists and machine learning engineers to package up, share, and run projects anywhere Docker will run.

There's a lot more to Docker — we haven't touched on multi-container applications. It's possible to define and spin up your entire applications stack — including databases, servers, load balancers, etc. — with Docker and Docker Compose. Once you're in the hang of these approaches, you can start templating and creating complex building blocks for your data pipelines.

If you're interested in a deeper dive into <u>Docker: Up & Running</u> is great.

Managing many Docker containers at once can get complex and cumbersome. What if your app is in huge demand, how do you go from a handful of users to thousands? Luckily, there are tools available for just that.

Kubernetes

Developed by Google, <u>Kubernetes</u> is an open-source container orchestration platform that automates the management, deployment, scaling, and networking of containers.

I'll be covering Kubernetes for data scientists and machine learning engineers in a future post — so watch this space.

Docker Swarm

Another option is Docker Swarm. I won't be covering Docker Swarm as Kubernetes does the job for me but if you're interested I'd highly recommend checking out this post by Gabriel Tanner to get started:

The Definitive Guide to Docker Swarm

Everything you need to know about Docker Swarm and how to use it to scale and securely maintain your Docker projects

medium.com

Conclusion

This post has enough to get you up and running with Docker and deploying a machine learning model into production. With practice, you'll begin to see

the applications in your workflow. There's a lot you can do. Some thoughts for the next steps follow.

Sharing entire project workspaces

Coming from a consultancy background we found Docker was a great way to share a finalised project with a customer without the hassle of environment and dependency management. To get a start on this, check out <u>Cookiecutter Docker Science</u> — a great tool to add to your toolbox.

JupyterLab

Setting up a JupyterLab can sometimes be cumbersome — ensuring credentials and configurations are all in the right place. It's possible to wrap these all up in Docker containers, making it easy to spin up new JupyterLab environments on a range of machines.

MLOps, DataOps, and machine learning engineering

Machine learning engineering is a relatively new field, and the tools and practices are still forming. It looks like containers are here to stay, acting as a fundamental building block of many workflows. The fields of MLOps and DataOps are fascinating and well worth further exploration.

This discussion of MLOps by Cristiano Breuel really works as a first touchpoint:

ML Ops: Machine Learning as an Engineering Discipline

As ML matures from research to applied business solutions, so do we need to improve the maturity of its operation...

towardsdatascience.com

And for an introduction to DataOps, see this great post by DataKitchen on DataOps:

One common misconception about DataOps is that it is just DevOps applied to data analytics. While a little semantically...

medium.com

I hope this was useful, please let me know if you have any feedback reach out at:

- Twitter at www.twitter.com/adzsroka
- LinkedIn at www.linkedin.com/in/aesroka
- Or at www.adamsroka.co.uk

If there are any other topics you're interested in me writing about please let me know!

Please note, this post does contain an affiliate link.

Docker

Data Science

Machine Learning

ΑI

Software Development



Written by Adam Sroka

https://towardsdatascience.com/docker-for-data-scientists-part-2-7655c02fe975

809 Followers · Writer for Towards Data Science



Dr Adam Sroka, Head of Machine Learning Engineering at Origami Energy, is an experienced data and Al leader helping organisations unlock value from data.

More from Adam Sroka and Towards Data Science





Adam Sroka in The Startup

Why So Many Data Scientists Quit **Good Jobs at Great Companies**

A look at why the 'sexiest job of the 21st century' has lost its appeal

· 10 min read · Mar 2, 2021

€⁽¹⁹1) 2.5K

Jimmy Weaver in Towards Data Science

Exposing the Power of the Kalman Filter

As a data scientist we are occasionally faced with situations where we need to model a...

17 min read Nov 7

£16 (FF)





Benjamin Lee in Towards Data Science



Adam Sroka in Towards Data Science

Why You Shouldn't Hire More Data

The New Best Python Package for **Visualising Network Graphs**

A guide on who should use it, when to use it, how to use it, and why I was wrong before...

+ 10 min read 6 days ago

(M) 659

· 8 min read · Apr 26, 2021

Scientists

See all from Adam Sroka

See all from Towards Data Science

Recommended from Medium







What I learned after one year of building a Data Platform from...

My key learnings on building a Data platform, from the tech side to the business side

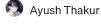
9 min read · Nov 14











Wait! What are Pipelines in Python?

If you are a Python developer, you might have heard of the term pipeline. But what exactly i...

5 min read · Nov 6







Lists



Predictive Modeling w/ **Python**

20 stories · 648 saves



The New Chatbots: ChatGPT, Bard, and Beyond

12 stories · 222 saves



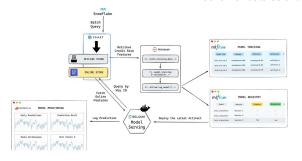
Practical Guides to Machine Learning

10 stories · 729 saves



Coding & Development

11 stories · 291 saves









Building an End-to-End MLOps Pipeline with Open-Source Tools

MLOps Open Source: TL;DR

11 min read · Oct 18

448 Q 4

The ChatGPT Hype Is Over—Now Watch How Google Will Kill...

It never happens instantly. The business game is longer than you know.

+ 6 min read Sep 1

9 19.7K \Q 603

Sumit Pandey in Towards Al

in Towards AI Paul Rose

YOLOv8: The Simple Choice for Better Segmentation on custom...

YOLOv8 is an amazing segmentation model, its easy to train test and deploy. In this tutori...

its easy to train test and deploy. In this tut

→ · 6 min read · Nov 6

) 63 Q

·••

I Found A Very Profitable Al Side Hustle

And it's perfect for beginners

6 min read · Oct 18

11.6K Q 207

~†

See more recommendations