KUBERMATIC

Container Days 2021 - Hamburg

Dockerfile Best Practices

How to create secure and efficient images

Koray Oksay
Site Reliability Engineer

koray@kubermatic.com
@korayoksay
kubermatic/kubermatic

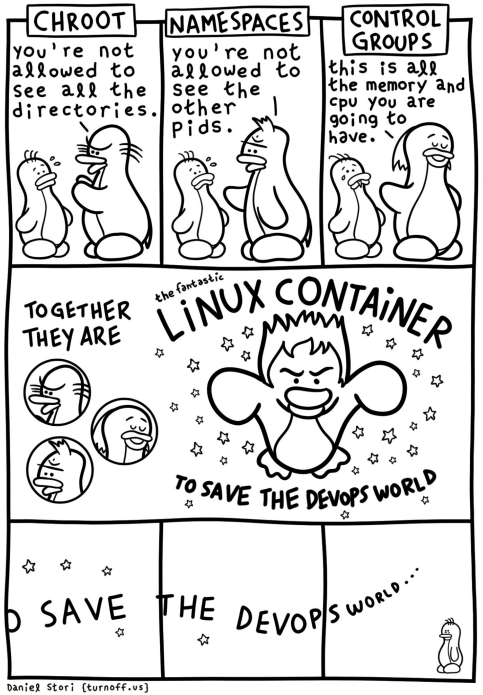
What Else?

- Consultant / Site Reliability Engineer
- Working remotely from Istanbul
- Interested in Linux, Kubernetes, and cloud technologies
- CKA | CKAD | RHCE

What is a container?

* Original post:
https://www.commitstrip.com/en/2016/06/24/how-to-host-a-coder-dinner-party

Conta ses
bo
anch es
con s



* Original post:
http://turnoff.us/geek/linux-containers/

Dockerfile-v1

```
FROM ubuntu

RUN apt-get -y update; apt-get clean
RUN apt-get -y install python3-pip python3; apt-get clean

COPY ./requirements.txt /app/requirements.txt

WORKDIR /app

RUN pip3 install --upgrade pip

RUN pip3 install -r /app/requirements.txt
COPY . /app

ENTRYPOINT [ "python" ]

EXPOSE 80

CMD [ "app.py" ]
```

```
$ tree
.
├── Dockerfile-v1
├── Dockerfile-v2
├── Dockerfile-v3
├── Dockerfile-v4
├── Dockerfile-v5
├── README.md
├── ansible
│   ├── deploy_app.yml
│   ├── files
│   └── hosts
│       ├── bastion_aws_ec2.yml
│       ├── nonwl.gcp.yml
│       └── wl_aws_ec2.yml
├── app.py
├── bitbucket-pipelines.yml
├── environment.jpeg
├── requirements.txt
└── tf
    ├── dns.tf
    ├── instances.tf
    ├── network.tf
    ├── provider.tf
    └── variables.tf

4 directories, 19 files
```

Build Dockerfile-v1

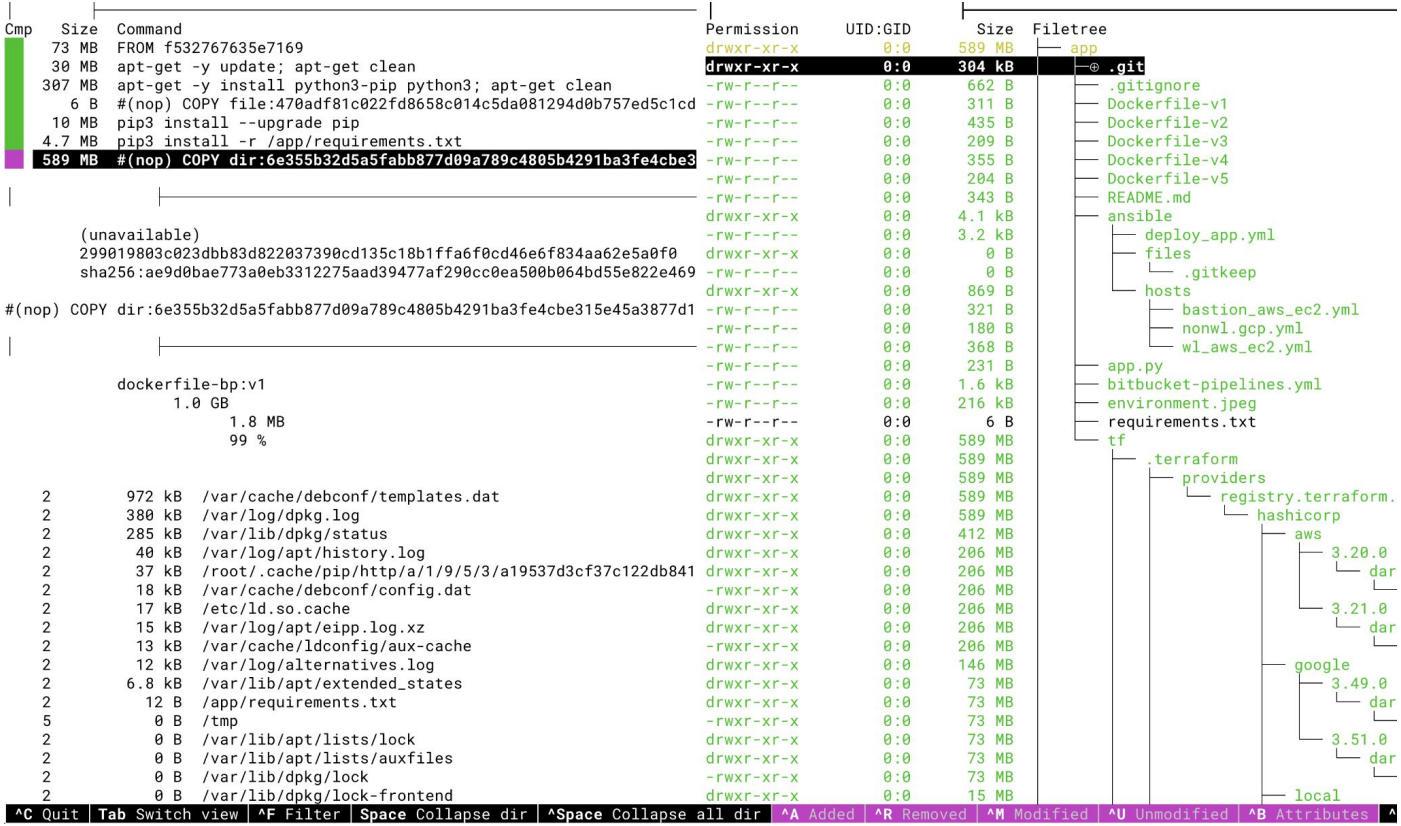
```
$ time docker build -t dockerfile-bp:v1 -f Dockerfile-v1 --no-cache .
Sending build context to Docker daemon  589.6MB
Step 1/11 : FROM ubuntu
latest: Pulling from library/ubuntu
35807b77a593: Already exists
Digest: sha256:9d6a8699fb5c9c39cf08a0871bd6219f0400981c570894cd8cbea30d3424a31f
Status: Downloaded newer image for ubuntu:latest
 ---> fb52e22af1b0
Step 2/11 : RUN apt-get -y update; apt-get clean
 ---> Running in 61bc9c65d930
Get:1 http://archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]


Step 10/11 : EXPOSE 80
 ---> Running in 51f17edc38df
Removing intermediate container 51f17edc38df
 ---> cde194050387
Step 11/11 : CMD [ "app.py" ]
 ---> Running in 9882ad8c3b6c
Removing intermediate container 9882ad8c3b6c
 ---> 50caddc65bcf
Successfully built 50caddc65bcf
Successfully tagged dockerfile-bp:v1

real    1m3.846s
user    0m4.655s
sys     0m3.016s
```

```
$ du -ksh *
4.0K    Dockerfile-v1
4.0K    Dockerfile-v2
4.0K    Dockerfile-v3
4.0K    Dockerfile-v4
4.0K    Dockerfile-v5
4.0K    README.md
 16K    ansible
4.0K    app.py
4.0K    bitbucket-pipelines.yml
212K    environment.jpeg
4.0K    requirements.txt
561M    tf
```

```
├── nonwl.gcp.yml
└── wl_aws_ec2.yml
├── app.py
├── bitbucket-pipelines.yml
├── environment.jpeg
├── requirements.txt
└── tf
    ├── dns.tf
    ├── instances.tf
    ├── network.tf
    ├── provider.tf
    └── variables.tf

4 directories, 19 files
```

KUBERMATIC

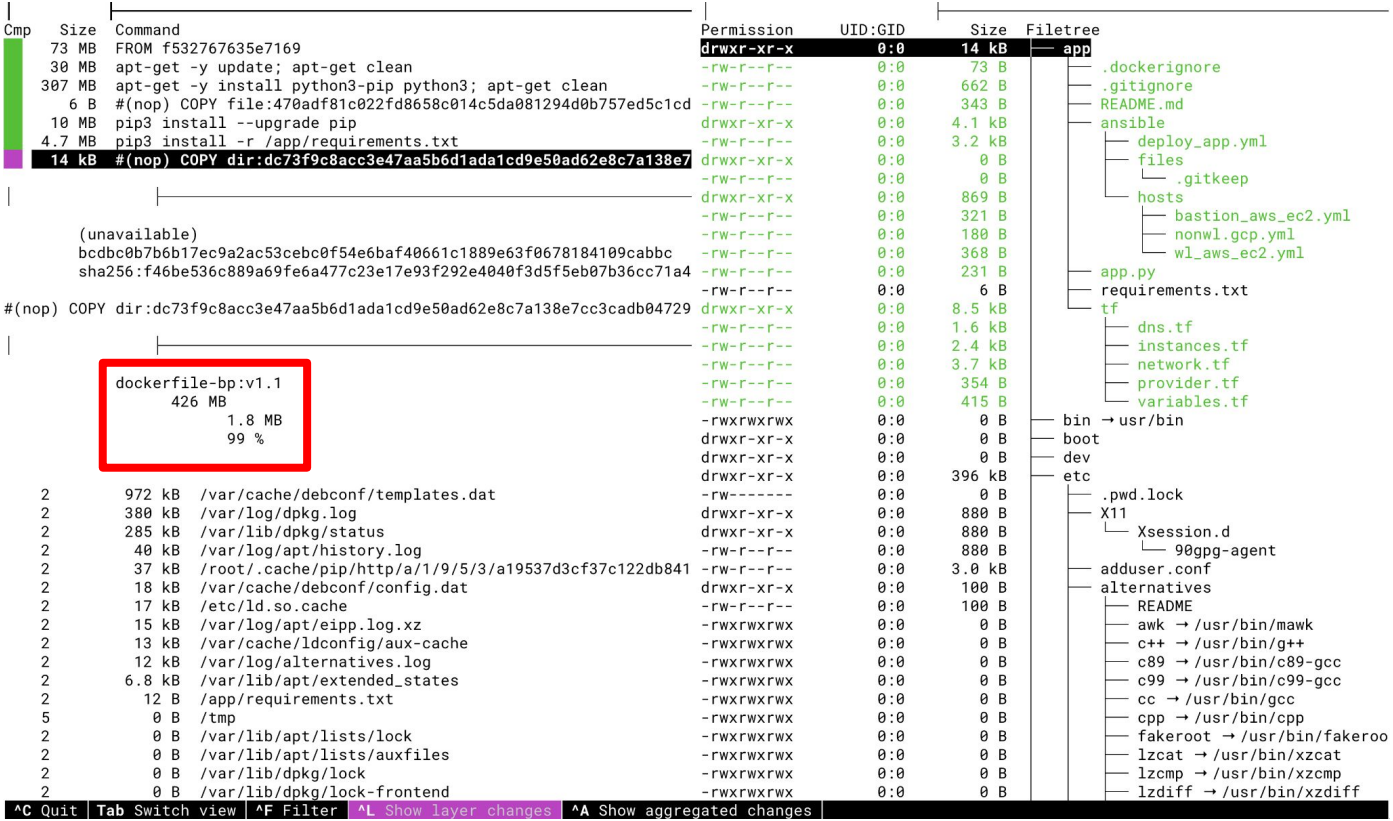
dive dockerfile-bp:v1



.dockerignore

```
$ cat .dockerignore
Dockerfile*
.git
tf/.terraform*
bitbucket-pipelines.yml
environment.jpeg

$ time docker build -t dockerfile-bp:v1.1 -f Dockerfile-v1 --no-cache .
Sending build context to Docker daemon  29.7kB
Step 1/11 : FROM ubuntu
 ---> fb52e22af1b0
Step 2/11 : RUN apt-get -y update; apt-get clean
 ---> Running in 18104df613da


Successfully built 7e5b47ec9a60
Successfully tagged dockerfile-bp:v1.1

real    0m52.181s
user    0m4.011s
sys     0m1.538s
```

dive dockerfile-bp:v1.1



DOCKER_BUILDKIT=1

Build images with BuildKit

- Now default on Docker Desktop
- Limitation: Only supported for building Linux containers

```
$ DOCKER_BUILDKIT=1 docker build -t dockerfile-bp:v1.2 -f Dockerfile-v1 --no-cache .
[+] Building 35.8s (13/13) FINISHED
 => [internal] load build definition from Dockerfile-v1                                                0.0s
 => => transferring dockerfile: 40B                                                                    0.0s
 => [internal] load .dockerignore                                                                      0.0s
 => => transferring context: 113B                                                                      0.0s
 => [internal] load metadata for docker.io/library/ubuntu:latest                                       0.0s
 => CACHED [1/8] FROM docker.io/library/ubuntu                                                         0.0s
 => [internal] load build context                                                                      0.1s
 => => transferring context: 743B                                                                      0.0s
 => [2/8] RUN apt-get -y update; apt-get clean                                                         3.7s
 => [3/8] RUN apt-get -y install python3-pip python3; apt-get clean                                   23.7s
 => [4/8] COPY ./requirements.txt /app/requirements.txt                                               0.0s
 => [5/8] WORKDIR /app                                                                                 0.0s
 => [6/8] RUN pip3 install --upgrade pip                                                               3.2s
 => [7/8] RUN pip3 install -r /app/requirements.txt                                                    2.8s
 => [8/8] COPY . /app                                                                                  0.0s
 => exporting to image                                                                                 2.2s
 => => exporting layers                                                                                2.2s
 => => writing image sha256:a8ec44a3a73b03dec1f5ebe03b7563d74dc3867e02857b95ae0c64235874c96e           0.0s
 => => naming to docker.io/library/dockerfile-bp:v1.2                                                  0.0s
```

hadolint

```
 1  FROM ubuntu
 2
 3  RUN apt-get -y update; apt-get clean
 4  RUN apt-get -y install python3-pip python3; apt-get clean
 5
 6  COPY ./requirements.txt /app/requirements.txt
 7
 8  WORKDIR /app
 9
10  RUN pip3 install --upgrade pip
11
12  RUN pip3 install -r /app/requirements.txt
13  COPY . /app
14
15  ENTRYPOINT [ "python" ]
16
17  EXPOSE 80
18
19  CMD [ "app.py" ]
```

```
$ hadolint Dockerfile-v1
Dockerfile-v1:1 DL3006 warning: Always tag the version of an image explicitly
Dockerfile-v1:3 DL3009 info: Delete the apt-get lists after installing something
Dockerfile-v1:4 DL3059 info: Multiple consecutive `RUN` instructions. Consider consolidation.
Dockerfile-v1:4 DL3008 warning: Pin versions in apt get install. Instead of `apt-get install <package>` use `apt-get install
<package>=<version>`
Dockerfile-v1:4 DL3015 info: Avoid additional packages by specifying `--no-install-recommends`
Dockerfile-v1:10 DL3013 warning: Pin versions in pip. Instead of `pip install <package>` use `pip install <package>==<version
>` or `pip install --requirement <requirements file>`
Dockerfile-v1:10 DL3042 warning: Avoid use of cache directory with pip. Use `pip install --no-cache-dir <package>`
Dockerfile-v1:12 DL3059 info: Multiple consecutive `RUN` instructions. Consider consolidation.
Dockerfile-v1:12 DL3042 warning: Avoid use of cache directory with pip. Use `pip install --no-cache-dir <package>`
```

Dockerfile-v2

```
FROM ubuntu:20.10

RUN apt-get -y update && \
    apt-get -y install --no-install-recommends python3-pip=20.1.1-2 python3=3.8.6-0ubuntu1 && \
    rm -rf /var/lib/apt/lists/* && \
    apt-get clean

COPY ./requirements.txt /app/requirements.txt

WORKDIR /app

RUN pip3 install --no-cache-dir --upgrade pip && \
    pip3 install --no-cache-dir -r /app/requirements.txt

COPY . /app

ENTRYPOINT [ "python" ]

EXPOSE 80

CMD [ "app.py" ]
```

Build Dockerfile-v2

```
$ DOCKER_BUILDKIT=1 docker build -t dockerfile-bp:v2 -f Dockerfile-v2 --no-cache .
[+] Building 26.0s (11/11) FINISHED
 => [internal] load build definition from Dockerfile-v2                                                                0.0s
 => => transferring dockerfile: 40B                                                                                    0.0s
 => [internal] load .dockerignore                                                                                      0.0s
 => => transferring context: 34B                                                                                       0.0s
 => [internal] load metadata for docker.io/library/ubuntu:20.10                                                        0.0s
 => [internal] load build context                                                                                      0.1s
 => => transferring context: 664B                                                                                      0.0s
 => CACHED [1/6] FROM docker.io/library/ubuntu:20.10                                                                   0.0s
 => [2/6] RUN apt-get -y update &&     apt-get -y install --no-install-recommends python3-pip=20.1.1-2 python3=3.8.6-0ubuntu1 &&     rm -rf /  18.7s
 => [3/6] COPY ./requirements.txt /app/requirements.txt                                                               0.0s
 => [4/6] WORKDIR /app                                                                                                 0.0s
 => [5/6] RUN pip3 install --no-cache-dir --upgrade pip &&     pip3 install --no-cache-dir -r /app/requirements.txt    6.5s
 => [6/6] COPY . /app                                                                                                  0.0s
 => exporting to image                                                                                                 0.6s
 => => exporting layers                                                                                                0.6s
 => => writing image sha256:aceb70211c5cda1b3a0459bc503d918d1ae15a4a783540974c397027e767343f                           0.0s
 => => naming to docker.io/library/dockerfile-bp:v2                                                                    0.0s
```

```
$ docker images --filter "reference=dockerfile-bp:*"
REPOSITORY      TAG       IMAGE ID       CREATED          SIZE
dockerfile-bp   v2        aceb70211c5c   41 seconds ago   132MB
dockerfile-bp   v1.2      a8ec44a3a73b   12 hours ago     426MB
dockerfile-bp   v1.1      7e5b47ec9a60   12 hours ago     426MB
dockerfile-bp   v1        50caddc65bcf   28 hours ago     1.01GB
```

dive dockerfile-bp:v2

```
Cmp   Size  Command
    79 MB  FROM e26c83a411971f8
   811 B  set -xe          && echo '#!/bin/sh' > /usr/sbin/policy-rc.d
     7 B  mkdir -p /run/systemd && echo 'docker' > /run/systemd/containe
    40 MB  RUN /bin/sh -c apt-get -y update &&     apt-get -y install --n
     6 B  COPY ./requirements.txt /app/requirements.txt # buildkit
     0 B  WORKDIR /app
    13 MB  RUN /bin/sh -c pip3 install --no-cache-dir --upgrade pip &&
    14 kB  COPY . /app # buildkit

        (unavailable)
        a06f35a9be1d0e41078f2ec853a7accfce1afabf38029f9089b25864cc878269
        sha256:020903ff2587e5b3ad813bd91ee0da2bef569312d6f38a312822a99a9af

RUN /bin/sh -c apt-get -y update &&     apt-get -y install --no-install-re

            dockerfile-bp:v2
                 132 MB
                       1.6 MB
                       99 %

    2        1.0 MB  /var/cache/debconf/templates.dat
    2        325 kB  /var/log/dpkg.log
    2        209 kB  /var/lib/dpkg/status
    2         36 kB  /var/log/apt/history.log
    2         18 kB  /var/cache/debconf/config.dat
    2         14 kB  /etc/ld.so.cache
    2         12 kB  /var/cache/ldconfig/aux-cache
    2         11 kB  /var/log/apt/eipp.log.xz
    2        1.2 kB  /var/lib/apt/extended_states
    2         300 B  /var/lib/dpkg/diversions
    2          12 B  /app/requirements.txt
    2           0 B  /var/lib/dpkg/lock-frontend
    2           0 B  /var/lib/dpkg/triggers/Lock
    2           0 B  /var/cache/debconf/passwords.dat
    2           0 B  /var/lib/dpkg/triggers/Unincorp
    2           0 B  /var/cache/apt/archives/partial
```

```
Permission     UID:GID       Size  Filetree
-rwxrwxrwx         0:0        0 B  ├── bin → usr/bin
drwxr-xr-x         0:0        0 B  ├── boot
drwxr-xr-x         0:0        0 B  ├── dev
drwxr-xr-x         0:0     364 kB  ├⊕ etc
drwxr-xr-x         0:0        0 B  ├── home
-rwxrwxrwx         0:0        0 B  ├── lib → usr/lib
-rwxrwxrwx         0:0        0 B  ├── lib32 → usr/lib32
-rwxrwxrwx         0:0        0 B  ├── lib64 → usr/lib64
-rwxrwxrwx         0:0        0 B  ├── libx32 → usr/libx32
drwxr-xr-x         0:0        0 B  ├── media
drwxr-xr-x         0:0        0 B  ├── mnt
drwxr-xr-x         0:0        0 B  ├── opt
drwxr-xr-x         0:0        0 B  ├── proc
drwx------         0:0     3.3 kB  ├── root
-rw-r--r--         0:0     3.1 kB  │   ├── .bashrc
-rw-r--r--         0:0      161 B  │   └── .profile
drwxr-xr-x         0:0        7 B  ├── run
drwxrwxrwx         0:0        0 B  │   ├── lock
drwxr-xr-x         0:0        0 B  │   ├── mount
drwxr-xr-x         0:0        7 B  │   ├── systemd
-rw-r--r--         0:0        7 B  │   │   └── container
-rw-rw-r--        0:43        0 B  │   └── utmp
-rwxrwxrwx         0:0        0 B  ├── sbin → usr/sbin
drwxr-xr-x         0:0        0 B  ├── srv
drwxr-xr-x         0:0        0 B  ├── sys
drwxrwxrwx         0:0        0 B  ├── tmp
drwxr-xr-x         0:0     114 MB  ├⊕ usr
drwxr-xr-x         0:0     4.3 MB  └⊕ var
```

```
^C Quit | Tab Switch view | ^F Filter | Space Collapse dir | ^Space Collapse all dir | ^A Added | ^R Removed | ^M Modified | ^U Unmodified | ^B Attributes | ^
```

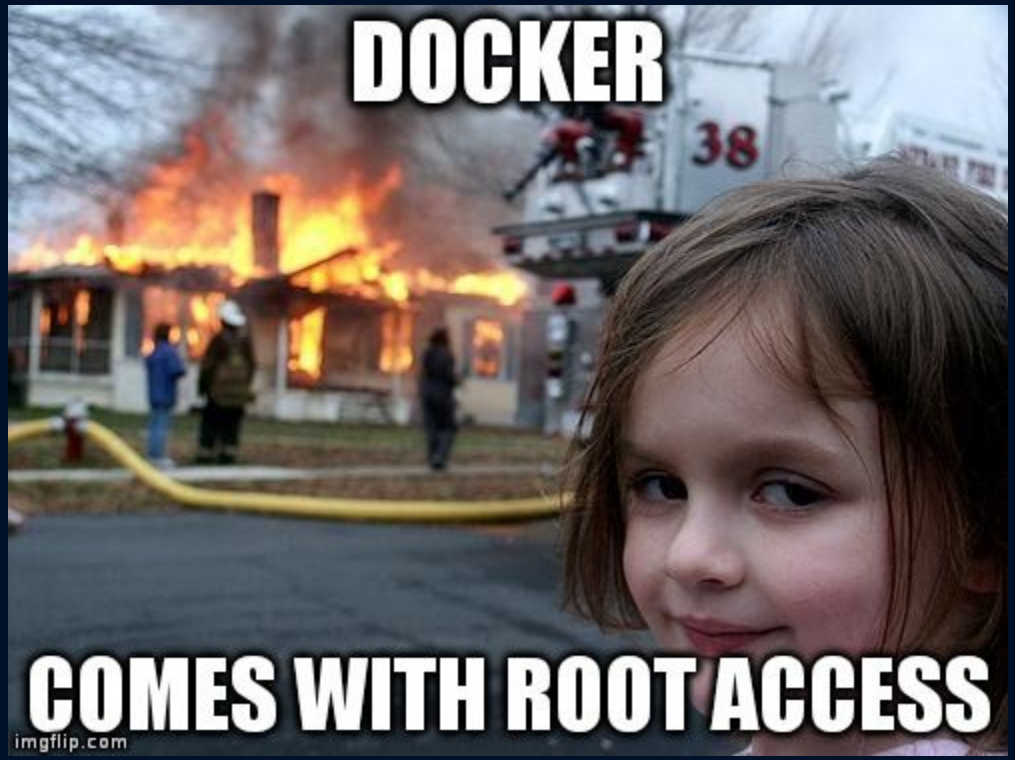
Dockerfile-v3

```
FROM python:3.9-slim-buster

COPY ./requirements.txt /app/requirements.txt
WORKDIR /app
RUN pip install --no-cache-dir -r /app/requirements.txt
COPY . /app

ENTRYPOINT [ "python" ]
EXPOSE 80
CMD [ "app.py" ]
```

```
$ docker images --filter "reference=dockerfile-bp:*"
REPOSITORY      TAG       IMAGE ID       CREATED              SIZE
dockerfile-bp   v3        390c9252e4e0   About a minute ago   125MB
dockerfile-bp   v2        aceb70211c5c   7 minutes ago        132MB
dockerfile-bp   v1.2      a8ec44a3a73b   12 hours ago         426MB
dockerfile-bp   v1.1      7e5b47ec9a60   12 hours ago         426MB
dockerfile-bp   v1        50caddc65bcf   28 hours ago         1.01GB
```

```
$ DOCKER_BUILDKIT=1 docker build -t dockerfile-bp:v3 -f Dockerfile-v3 --no-cache .
[+] Building 7.1s (11/11) FINISHED
 => [internal] load build definition from Dockerfile-v3                                                0.0s
 => => transferring dockerfile: 260B                                                                   0.0s
 => [internal] load .dockerignore                                                                      0.0s
 => => transferring context: 34B                                                                       0.0s
 => [internal] load metadata for docker.io/library/python:3.9-slim-buster                              1.9s
 => [auth] library/python:pull token for registry-1.docker.io                                          0.0s
 => CACHED [1/5] FROM docker.io/library/python:3.9-slim-buster@sha256:85c310e75457e15f1517bfe8530c49d  0.0s
 => [internal] load build context                                                                      0.0s
 => => transferring context: 664B                                                                      0.0s
 => [2/5] COPY ./requirements.txt /app/requirements.txt                                               0.0s
 => [3/5] WORKDIR /app                                                                                 0.0s
 => [4/5] RUN pip install --no-cache-dir -r /app/requirements.txt                                      4.7s
 => [5/5] COPY . /app                                                                                  0.0s
 => exporting to image                                                                                 0.2s
 => => exporting layers                                                                                0.1s
 => => writing image sha256:390c9252e4e08759b3c4c9a955d1545494975f8b4178e2571a2399f031b9f488           0.0s
 => => naming to docker.io/library/dockerfile-bp:v3                                                    0.0s
```

KUBERMATIC



Dockerfile-v4: Security Update

```
FROM python:3.9-slim-buster

COPY ./requirements.txt /app/requirements.txt
WORKDIR /app
RUN groupadd --gid 5000 appuser && \
    useradd --home-dir /app --create-home --uid 5000 --gid 5000 --shell /bin/bash appuser && \
    pip install --no-cache-dir -r /app/requirements.txt

USER appuser
COPY . /app

ENTRYPOINT [ "python" ]
EXPOSE 80
CMD [ "app.py" ]
```

```
$ docker images --filter "reference=dockerfile-bp:*"
REPOSITORY      TAG       IMAGE ID       CREATED          SIZE
dockerfile-bp   v4        a1ece0d2b869   59 seconds ago   126MB
dockerfile-bp   v3        390c9252e4e0   7 minutes ago    125MB
dockerfile-bp   v2        aceb70211c5c   13 minutes ago   132MB
dockerfile-bp   v1.2      a8ec44a3a73b   12 hours ago     426MB
dockerfile-bp   v1.1      7e5b47ec9a60   12 hours ago     426MB
dockerfile-bp   v1        50caddc65bcf   29 hours ago     1.01GB
```

```
$ DOCKER_BUILDKIT=1 docker build -t dockerfile-bp:v4 -f Dockerfile-v4 --no-cache .
[+] Building 6.2s (11/11) FINISHED
 => [internal] load build definition from Dockerfile-v4                                                                                0.0s
 => => transferring dockerfile: 402B                                                                                                   0.0s
 => [internal] load .dockerignore                                                                                                      0.0s
 => => transferring context: 34B                                                                                                       0.0s
 => [internal] load metadata for docker.io/library/python:3.9-slim-buster                                                              1.6s
 => [auth] library/python:pull token for registry-1.docker.io                                                                          0.0s
 => [internal] load build context                                                                                                      0.1s
 => => transferring context: 664B                                                                                                      0.0s
 => CACHED [1/5] FROM docker.io/library/python:3.9-slim-buster@sha256:85c310e75457e15f1517bfe8530c49d41f505443afbba8ea133706e88378be7e  0.0s
 => [2/5] COPY ./requirements.txt /app/requirements.txt                                                                               0.0s
 => [3/5] WORKDIR /app                                                                                                                 0.0s
 => [4/5] RUN groupadd --gid 5000 appuser &&     useradd --home-dir /app --create-home --uid 5000 --gid 5000 --shell /bin/bash appuser &&  4.1s
 => [5/5] COPY . /app                                                                                                                  0.0s
 => exporting to image                                                                                                                 0.2s
 => => exporting layers                                                                                                                0.2s
 => => writing image sha256:4172cebcd41ac1ae9f6fd62a075435be117d9327261d89530cf141853892d321                                           0.0s
 => => naming to docker.io/library/dockerfile-bp:v4                                                                                    0.0s
```

What difference does it make?

```
koray@koray-test:~$ docker run -d -p 8080:8080 dockerfile-bp:v3
2e310379a903732f995a129f59d1e2a7e22151dbb4046e73127a32d7781fe750

koray@koray-test:~$ docker run -d -p 8081:8080 dockerfile-bp:v4
f3a7402bb89505ff49c62601afb2381a06069b32de7f7acabdc51cd8bbfccac4

koray@koray-test:~$ docker ps
CONTAINER ID   IMAGE               COMMAND           CREATED          STATUS
f3a7402bb895   dockerfile-bp:v4    "python app.py"   8 seconds ago    Up 7 seconds
2e310379a903   dockerfile-bp:v3    "python app.py"   18 seconds ago   Up 17 seconds

koray@koray-test:~$ ps aux | grep python
root         407  0.0  0.4  28416 16920 ?        Ss   09:44   0:00 /usr/bin/python3 /u
root        5472  0.8  0.7  37112 28308 ?        Ss   10:00   0:00 python app.py
5000        5571  1.2  0.7  37112 28288 ?        Ss   10:01   0:00 python app.py
```

Dockerfile-v5

```
FROM python:3.9-alpine

COPY ./requirements.txt /app/requirements.txt
WORKDIR /app
RUN addgroup --gid 5000 appuser && \
    adduser -D -h /app -u 5000 -G appuser -s /bin/sh appuser && \
    pip install --no-cache-dir -r /app/requirements.txt

USER appuser
COPY . /app

ENTRYPOINT [ "python" ]
EXPOSE 80
CMD [ "app.py" ]
```

```
$ docker images --filter "reference=dockerfile-bp:*"
REPOSITORY      TAG       IMAGE ID       CREATED          SIZE
dockerfile-bp   v5        1da204f0714c   10 seconds ago   56.2MB
dockerfile-bp   v4        a1ece0d2b869   9 minutes ago    126MB
dockerfile-bp   v3        390c9252e4e0   15 minutes ago   125MB
dockerfile-bp   v2        aceb70211c5c   21 minutes ago   132MB
dockerfile-bp   v1.2      a8ec44a3a73b   12 hours ago     426MB
dockerfile-bp   v1.1      7e5b47ec9a60   12 hours ago     426MB
dockerfile-bp   v1        50caddc65bcf   29 hours ago     1.01GB
```

```
$ DOCKER_BUILDKIT=1 docker build -t dockerfile-bp:v5 -f Dockerfile-v5 --no-cache .
[+] Building 6.4s (10/10) FINISHED
 => [internal] load build definition from Dockerfile-v5                                                                    0.0s
 => => transferring dockerfile: 40B                                                                                        0.0s
 => [internal] load .dockerignore                                                                                          0.0s
 => => transferring context: 34B                                                                                           0.0s
 => [internal] load metadata for docker.io/library/python:3.9-alpine                                                       0.8s
 => CACHED [1/5] FROM docker.io/library/python:3.9-alpine@sha256:964a1afa20dd4a3723002560124dd96f2a9e853f7ef5b86f5c2354af336fca37  0.0s
 => [internal] load build context                                                                                          0.1s
 => => transferring context: 664B                                                                                          0.0s
 => [2/5] COPY ./requirements.txt /app/requirements.txt                                                                    0.0s
 => [3/5] WORKDIR /app                                                                                                     0.0s
 => [4/5] RUN addgroup --gid 5000 appuser &&     adduser -D -h /app -u 5000 -G appuser -s /bin/sh appuser &&     pip install --no-cache-dir -r  5.1s
 => [5/5] COPY . /app                                                                                                      0.0s
 => exporting to image                                                                                                     0.2s
 => => exporting layers                                                                                                    0.2s
 => => writing image sha256:1da204f0714c02b9381cc9ab585ec515492178e2d6aaf702d6d9001fed39739e                               0.0s
 => => naming to docker.io/library/dockerfile-bp:v5                                                                        0.0s
```

Go Application - Dockerfile-go-v1

```
FROM golang:1.16

ENV GOPRIVATE "bitbucket.org/koksay"

ARG ssh_key

RUN groupadd --gid 5000 appuser && \
    useradd --home-dir /app --create-home --uid 5000 --gid 5000 --shell /bin/bash appuser

WORKDIR /app
USER appuser
ADD . /app/

RUN mkdir /app/.ssh && echo "${ssh_key}" > /app/.ssh/id_rsa \
    && git config --global url."git@bitbucket.org:".insteadOf "https://bitbucket.org/" \
    && ssh-keyscan bitbucket.org >> /app/.ssh/known_hosts \
    && chmod 400 /app/.ssh/id_rsa \
    && go build -o server main.go \
    && rm /app/.ssh/id_rsa

EXPOSE 8080

ENTRYPOINT ["./server"]
```

```
$ docker build -t dockerfile-bp-go:v1 --build-arg ssh_key="$(cat demo_key)" -f Dockerfile-go-v1 .
Sending build context to Docker daemon  10.24kB
Step 1/10 : FROM golang:1.16
1.16: Pulling from library/golang
```

```
$ docker images --filter "reference=dockerfile-bp-go:*"
REPOSITORY          TAG       IMAGE ID       CREATED         SIZE
dockerfile-bp-go    v1        5409ca247864   3 minutes ago   923MB
```

KUBERMATIC

skopeo

```
$ skopeo inspect --config docker-daemon:dockerfile-bp-go:v1 | jq '.history[] | select(.comment=="buildkit.dockerfile.v0")'
{
  "created": "2021-09-15T10:56:22.9819587Z",
  "created_by": "ENV GOPRIVATE=bitbucket.org/koksay",
  "comment": "buildkit.dockerfile.v0",
  "empty_layer": true
}
{
  "created": "2021-09-15T10:56:22.9819587Z",
  "created_by": "ARG ssh_key",
  "comment": "buildkit.dockerfile.v0",
  "empty_layer": true
}
{
  "created": "2021-09-15T10:56:22.9819587Z",
  "created_by": "RUN |1 ssh_key=-----BEGIN OPENSSH PRIVATE KEY-----\nb3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn\n
zs1GY8JfEPLvP9Tr9Mqs1IxzFBg9wP39oI6Sbkzc5T/VE7B6v\nAs+MKwKYdQZH7TW6RKTNoAFue0dg8rwueb6BdO5bq/Khbn/5Ojm/3DEpdsUdr3TUcdA3E9\nDsmo3/OVIy/szbkET(
01lDVgkPJfHrUBMI+EJV2u/NgdoYwQ8\n57TG3GDnGThC2LVLct9an1WsDb4I8c7W+6ueNR2aT3ZVs7fai1ydQnDHdWmt8jVu/UO/py\nlRn0bpz89PhVX5JC3BqVErilmAFmLEcd+u7
4MT56F5zzEzB6\n+QjtpFvAit78Pij0SSZp/b391Ng9WsA6+WMycT0C4w6W0+M9GwVR9c4RcPeJJA3FAkvYUd\nucpbHziTWwnfOb4w1cBTeK/ownf/8YROCloVvQ+/FOBliUtbeVE9L(
T3Tk4QzAXqbjHLMvqcpbhI8S7PhcSTmZCN9vFAAAFkJQFpkCUBaZAAAAAB3NzaC1yc2\nEAAAGBAK7887NRmPCXxDy7z/U6/TKrNSMcxQYPcD9/aCOkm5M3OU/1ROwerwLPjCsCmHUG\r
nm+gXTuW6vyoW5/+To5v9wxKXbFHa901HHQNxPQ7JqN/zlSMv\n7M25BExupDYR30F5vPcgE15i79qC9NZQ1YJDyXx61ATCPhCVdrvzYHaGMEPOe0xtxg5xk4\nQti1S3LfWp9VrA2+C
cnUJwx3VprfI1bv1Dv6cpUZ9G6c/PT4\nVV+SQtwalRK4pZgBZixHHfru0kNEmtpelmIMRZRf8UK9y6ODE+ehec8xMwevkI7aRbwIre\n/D4o9Ekmaf29/dTYPVrAOvljMnE9AuMOltP
FHbnKWx84k1sJ\n3zm+MNXAU3iv6MJ//GETgpaFb0PvxTgZYlLW3lRPS+tgxEMGKpioOjNVrxH0+k905OEMw\nF6m4xyzL6nKW4SPEuz4XEk5mQjfbxQAAAAMBAAEAAAGAGRcyBlM73
gT+rkwhbYLrv8caU6mycTzREVEbIwujOpxk8dFTXQZYaYnrAogwkX2EGHbFbzPCNzx6\nAzMcVEn1hagS7vHCmObik1Msoo3Bb0PPBbQQldJf5SbHcs2ofjgCrpenHB9TWweJ9wZc5/\r
qL1BrPzn/jZfjaw1TIGmWYOk/wDrziaDm/W0QDFQGQk11U9F+\n5l8FWhg0gFNVdjNp+qHIhJey8WlcG/Zpm8jUXGfinh+u0F208CdqV4QbmEcOz/sQqHcE2P\nt3tH1TIludY9/4AhN/
9vdDMsI/fJgD4DbqJ38L7ujFM9qmXIU\nToIsqoqhKxNV+mdMoqkM0S3EDyMc+m/tQjSEKgCfL5WI75gPzhceC3jbpz0QR7CfHNB8Ff\nHMHHB7xTPtxpgA26199WZypKX5yrIsFqFMb
IX8tVTXt9AAAA\nwQDR5kPZCQOin79fz6+YPOIcqRCmZxcsuu7ics108ngt/w6qAVGgRQJCPhJFQuH0cnb4IM\natf+hLNJuaDyCulvsKd665Gi2VlzsUMdgJQO1odxAddsAMHOyGy3r
otp4WS2FSQpP/cNg11WAr17rVmpktu43kgIyvtOkteWnnmRXvnM8S3jSdEZRmr5qp62\n9jRdyXGqy7ek2zztG1oQoVT0Kmn3oaeiTf1zhljnsa/V6QzcUAAADBANiOm/L5lIVnhk22\r
NxUvpQt18bOTjS2B/GRqspJ6EQvA8b4r/r8JS2KzBUo2mii8f\n1WKC6f1PdRz2qs5LckkTEUhFFNVfa0dv/12BHz/j1cH7NHTqG0tsUlIsidAinSM1tMPv2E\nkBtAymWfw3W+d4RH5
9XRPm6Nf5uw0OPA4qrLUI000rRHDXk8\nx01BSgEH2rKZo0ISmZLfjFJskUeK+z2wAAAMEAztwb9sJtN3GqqS2/mn9IfcRcMrxYAkCi\nAPkXovucxAeWr/DS7Le0ygizDWBu0RcEhW0
CsHRg8uec2COM\niJOYIsdjxqLuTcZKUGVeBysHUIzfDlr/qSraYYCz7VzgyfbyZ7r718Mgnhh8K+GPCbOVlp\n50RVem6IqxJC7cOHB0ivTbzzcDKaM0ZqOj0A2I/wfyyip+rOYUF+hr
T0l0XGTrZDfAAAAGWtvcmF5b2tzYXlAdGF0b29pbmUubG9jYWwB\n-----END OPENSSH PRIVATE KEY----- /bin/sh -c groupadd --gid 5000 appuser &&     useradd
ate-home --uid 5000 --gid 5000 --shell /bin/bash appuser # buildkit"
  "comment": "buildkit.dockerfile.v0"
}
```

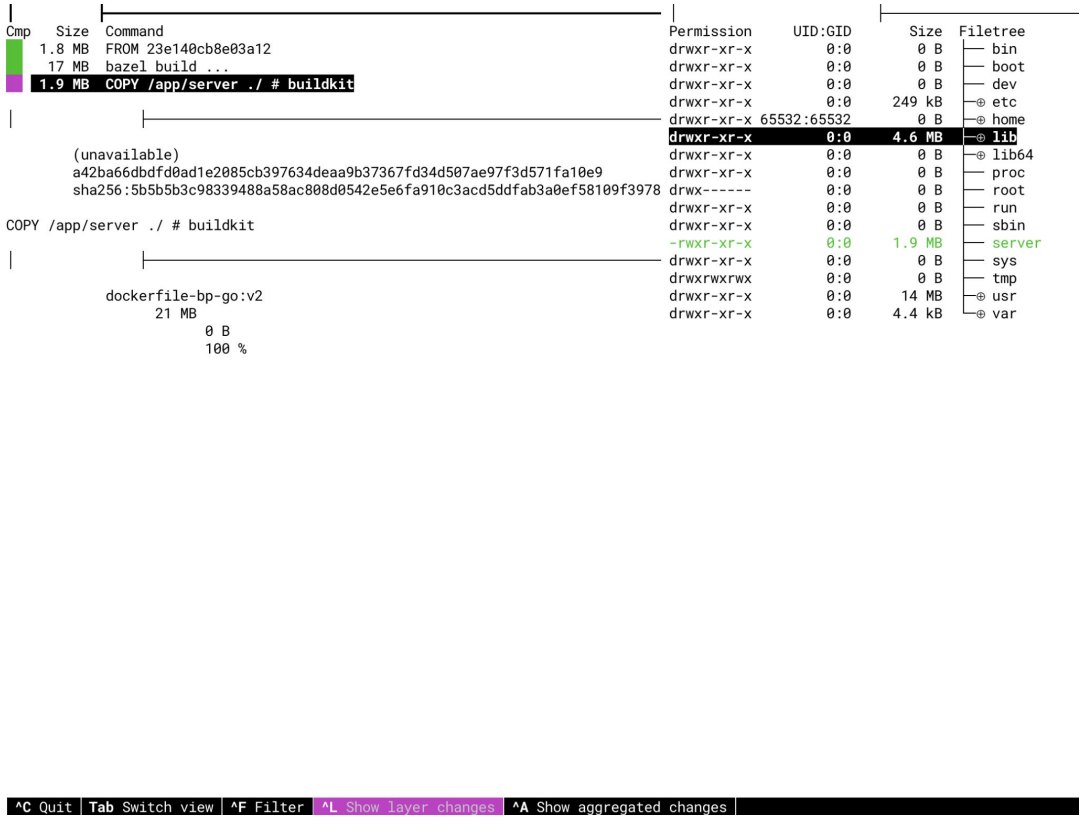
```
$ skopeo copy docker-daemon:dockerfile-bp-go:v1 dir:/tmp/skopeo
Getting image source signatures
Copying blob 688e187d6c79 done
Copying blob 00bcea93703b done
Copying blob ccb9b68523fd done
Copying blob 685934357c89 done
Copying blob 9d52e952d0a7 done
Copying blob 762eb5b089c5 done
Copying blob c92e53084342 done
Copying blob 96549fae219a done
Copying blob b565f2b413b8 done
Copying blob 52d125839c21 done
Copying blob 82040f8d3c83 done
Copying blob d16517152cae done
Copying blob cdc6a93cfae5 done
Copying config ffaf6d35ed done
Writing manifest to image destination
Storing signatures
```

Multi-stage Builds - Dockerfile-go-v2

```
# Build Stage
FROM golang:1.16 as 🔨 builder

ENV GOPRIVATE "bitbucket.org/koksay"

ARG ssh_key
WORKDIR /app
COPY . /app/
RUN mkdir -p /root/.ssh && echo "${ssh_key}" > /root/.ssh/id_rsa \
    && git config --global url."git@bitbucket.org:".insteadOf "https://bitbucket.org/" \
    && ssh-keyscan bitbucket.org >> /root/.ssh/known_hosts \
    && chmod 400 /root/.ssh/id_rsa \
    && go build -o server main.go

# Run Stage
FROM gcr.io/distroless/base:nonroot
COPY --from=builder /app/server /app/

EXPOSE 8080

ENTRYPOINT ["/app/server"]
```

```
$ docker images --filter "reference=dockerfile-bp-go:*"
REPOSITORY          TAG       IMAGE ID       CREATED          SIZE
dockerfile-bp-go    v2        6670c294e23c   21 seconds ago   21.1MB
dockerfile-bp-go    v1        846447cb43b4   27 hours ago     923MB
```

dive dockerfile-bp-go:v2



Multi stage build - Node

```dockerfile
# Build Stage
FROM node:lts as 🔨 builder

ARG NPM_TOKEN
ENV NODE_OPTIONS "--max-old-space-size=4096"
ENV PATH /usr/src/app/node_modules/.bin:$PATH

WORKDIR /usr/src/app
COPY . /usr/src/app

RUN printf "//registry.npmjs.org/:_authToken=${NPM_TOKEN}\n" > ~/.npmrc \
    && printf "registry=https://registry.npmjs.org\n" >> ~/.npmrc \
    && npm ci \
    && npm run build

# Run Stage
FROM nginx:mainline-alpine
COPY --from=builder /usr/src/app/dist /usr/share/nginx/html

COPY nginx.conf /etc/nginx/nginx.conf

CMD ["nginx", "-g", "daemon off;"]
```

KUBERMATIC

Vulnerability Scanning

- Use container scanning tools (e.g. docker scan - snyk, Anchore, Xfrog xray)

```
$ docker scan dockerfile-bp-go:v1

Testing dockerfile-bp-go:v1...

Organization:      korayoksay
Package manager:   deb
Project name:      docker-image|dockerfile-bp-go
Docker image:      dockerfile-bp-go:v1
Platform:          linux/amd64
Base image:        golang:1.16.8-bullseye
Licenses:          enabled

Tested 203 dependencies for known issues, found 80 issues.

According to our scan, you are currently using the most secure version of the selected base image
```

```
$ docker scan dockerfile-bp-go:v2

Testing dockerfile-bp-go:v2...



Organization:      korayoksay
Package manager:   deb
Project name:      docker-image|dockerfile-bp-go
Docker image:      dockerfile-bp-go:v2
Platform:          linux/amd64
Licenses:          enabled

Tested 6 dependencies for known issues, found 25 issues.
```

```
$ docker scan dockerfile-bp:v3

Testing dockerfile-bp:v3...

Organization:      korayoksay
Package manager:   deb
Project name:      docker-image|dockerfile-bp
Docker image:      dockerfile-bp:v3
Platform:          linux/amd64
Base image:        python:3.9.7-slim-buster
Licenses:          enabled

Tested 94 dependencies for known issues, found 71 issues.

Base Image               Vulnerabilities  Severity
python:3.9.7-slim-buster  71              2 critical, 9 high, 9 medium, 51 low

Recommendations for base image upgrade:

Alternative image types
Base Image            Vulnerabilities  Severity
python:3.10.0rc1-slim  39              1 critical, 0 high, 2 medium, 36 low
python:3.10-rc-slim    39              1 critical, 0 high, 2 medium, 36 low
```

```
$ docker scan dockerfile-bp:v5

Testing dockerfile-bp:v5...

Organization:      korayoksay
Package manager:   apk
Project name:      docker-image|dockerfile-bp
Docker image:      dockerfile-bp:v5
Platform:          linux/amd64
Base image:        python:3.9.7-alpine3.14
Licenses:          enabled

✓ Tested 37 dependencies for known issues, no vulnerable paths found.

According to our scan, you are currently using the most secure version of the selected base image
```

Best Practices

- Use **non-root user** to run the containers!
- Use **`.dockerignore`** files!
- Use BuildKit (**`export DOCKER_BUILDKIT=1`**)
- Use **hadolint** (or any other linter)
  - Always use a tag with the base image (not :latest)
  - Combine RUN statements
  - Pin the package versions with apt/yum/apk
  - Remove cached files (e.g. pip --no-cache-dir / apt -> rm -rf /var/lib/apt/lists/*)
- Use analysis tools (e.g. **dive**, **skopeo**)
- Use **multi staged builds**
- Base images: **slim** | **alpine** | **distroless**
- Use image scanners (e.g. **snyk**, **anchore**, **jfrog xray**)

KUBERMATIC

Any Questions?

KUBERMATIC

Thank you!

koray@kubermatic.com

@kubermatic

kubermatic/kubermatic