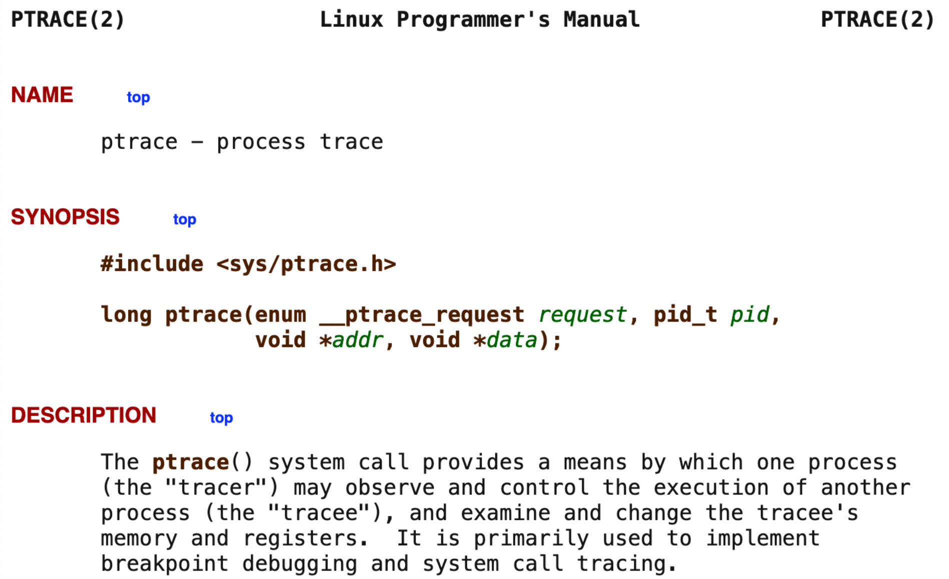
Минимизация образов корневых файловых систем Docker контейнеров

Ирина Николаева   Иван Ганкевич

Санкт-Петербургский государственный университет

GRID’21

Motivation



PTRACE(2) Linux Programmer's Manual PTRACE(2)

NAME top

ptrace - process trace

SYNOPSIS top

```
#include <sys/ptrace.h>

long ptrace(enum __ptrace_request request, pid_t pid,
            void *addr, void *data);
```

DESCRIPTION top

The **ptrace**() system call provides a means by which one process (the "tracer") may observe and control the execution of another process (the "tracee"), and examine and change the tracee's memory and registers. It is primarily used to implement breakpoint debugging and system call tracing.

Chainsaw usage example

1. Generate a list of all files in the root file system.

   ```
   chainsaw-blacklist /
   ```

2. Generate a list of files that some-app reads/writes.

   ```
   chainsaw-whitelist /bin/some-app
   ```

3. Compute set difference between the two lists.

   ```
   chainsaw-diff
   ```

4. Remove all the files from the resulting list.

   ```
   chainsaw-cut
   ```

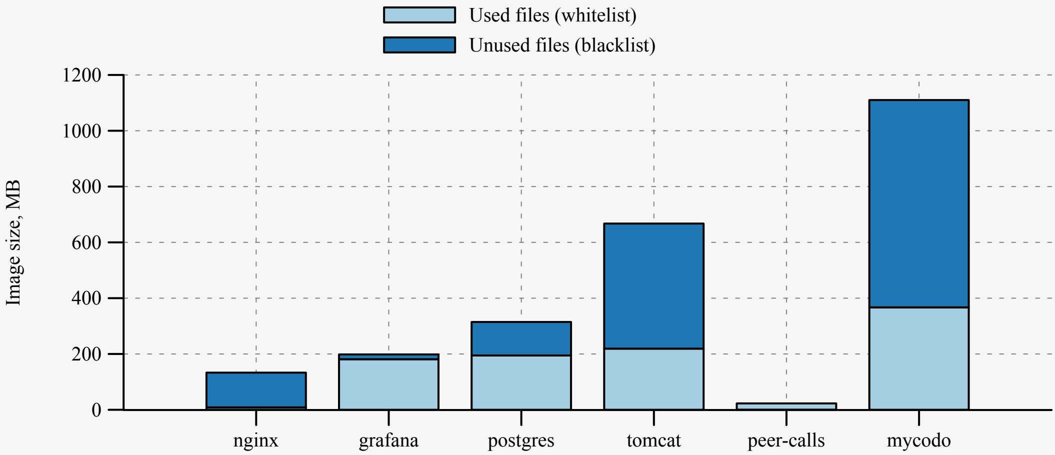
Dockerfile example

```
FROM image as build

RUN dnf install -y git python && \
    pip3 install ninja meson && \
    git clone https://github.com/igankevich/chainsaw && \
    cd chainsaw && \
    meson build && \
    ninja -C build && \
    ninja -C build install && \
    chainsaw-blacklist / && \
    chainsaw-whitelist some-app && \
    chainsaw-diff && \
    chainsaw-cut diff

FROM scratch
COPY --from=build / /
ENTRYPOINT ["some-app"]
```

Tested images

Name	Description	Language
NGINX	reverse proxy server	C
Grafana	time series visualisation	TypeScript
Postgres	SQL database	C++
Tomcat	web application server	Java
peer-calls	video conference service	Go
MyCodo	mushroom monitoring system	Python

Results


Used files (whitelist)
Unused files (blacklist)
Image size, MB
1200
1000
800
600
400
200
0
nginx
grafana
postgres
tomcat
peer-calls
mycodo

Results (table)

Image	Language	Orig. size (MB)	Resulting size (MB)
nginx	C	133.12	8.64
grafana	TypeScript	198.41	181.18
postgres	C++	314.68	194.57
tomcat	Java	667.44	219.11
peer-calls	Go	22.06	22.93
mycodo	Python	1110.00	366.99

Conclusion

- Minimised scratch images is an alternative to layer-based images.
  - Layer-based images is the scaffolding.
  - Minimised scratch images is the final product.
- `ptrace` is good enough to produce a list of opened files for minimised images.
- Chainsaw works only for the final images.

Chainsaw: https://github.com/igankevich/chainsaw