



Безопасность Docker



Изоляция не идеальна

Контейнеры всё равно используют общие ресурсы, порой косвенно:





Изоляция не идеальна

Контейнеры всё равно используют общие ресурсы, порой косвенно:

dentry

inodes

другие





Изоляция не идеальна

Контейнеры всё равно используют общие ресурсы, порой косвенно:

- dentry

- inodes

- другие

Крутая детективная история:

<https://sysdig.com/blog/container-isolation-gone-wrong/>





Хостовая ОС



Надежные пароли





Хостовая ОС

Надежные пароли

Минимальные права





Хостовая ОС

- Надежные пароли

- Минимальные права

- Минимум ПО





Хостовая ОС

- Надежные пароли
- Минимальные права
- Минимум ПО
- SELinux/AppArmor





Хостовая ОС

- Надежные пароли
- Минимальные права
- Минимум ПО
- SELinux/AppArmor
- И т.д.





Уязвимости



ПО не идеально





Уязвимости

- ПО не идеально
- Критические уязвимости находят чаще, чем вы думаете





УЯЗВИМОСТИ

Vulnerability Details : [CVE-2019-5736](#)

runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.

Publish Date : 2019-02-11 Last Update Date : 2019-06-03

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [▼ Scroll To](#) [▼ Comments](#) [▼ External Links](#)

[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

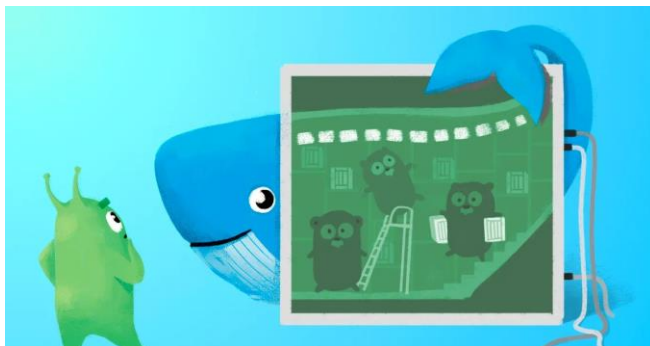
CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	216



Уязвимости. Что же делать?



Обновляться!

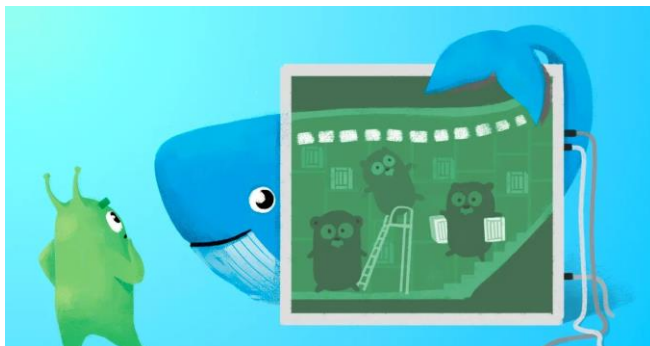




Уязвимости. Что же делать?

- Обновляться!

- Не использовать UID 0 (root) в контейнерах



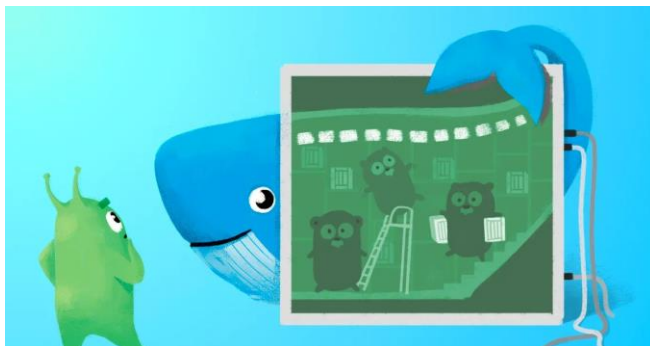


Уязвимости. Что же делать?

- Обновляться!

- Не использовать UID 0 (root) в контейнерах

- Не пользоваться образами, которым вы не доверяете





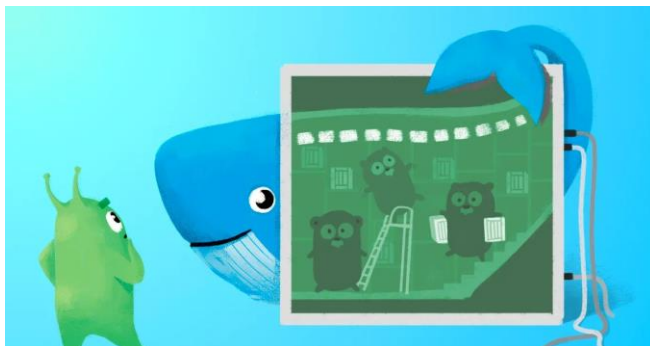
Уязвимости. Что же делать?

- Обновляться!

- Не использовать UID 0 (root) в контейнерах

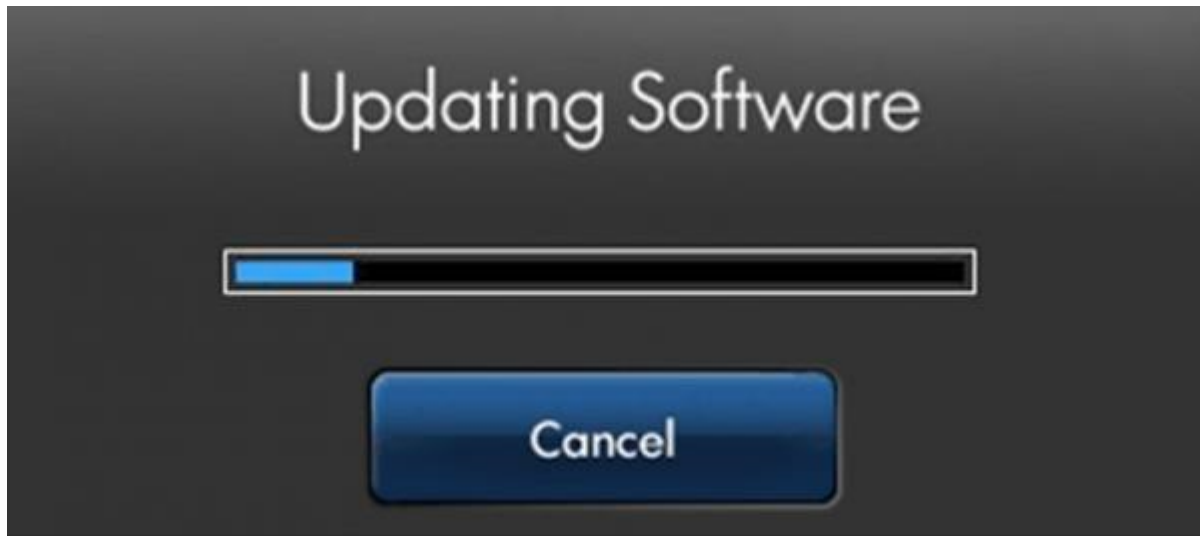
- Не пользоваться образами, которым вы не доверяете

- Использовать статические и динамические анализаторы






Уязвимости. Обновляться!



slido

Как часто обновляете ПО?

 Start presenting to display the poll results on this slide.



Уязвимости. Root.

Стараемся **не использовать** Root в контейнерах





Уязвимости. Root.

Стараемся **не использовать** Root в контейнерах

Он почти никогда не нужен





Уязвимости. Root.

Стараемся **не использовать** Root в контейнерах

Он почти никогда не нужен

Это не сложно





Уязвимости. Root.

Стараемся **не использовать** Root в контейнерах

Он почти никогда не нужен

Это не сложно

Ваши контейнеры будут работать в openshift!





Уязвимости. Root. Меняем пользователя

FROM ubuntu

RUN mkdir /app

RUN groupadd -r user && useradd -r -s /bin/false -g user
user

WORKDIR /app

COPY . /app

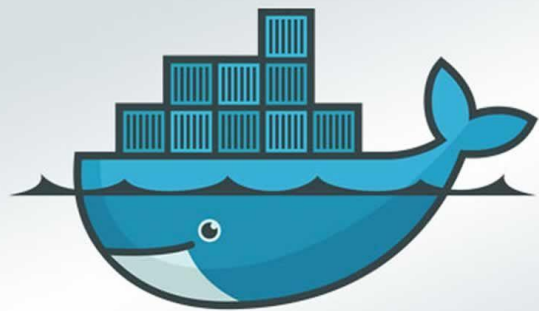
RUN chown -R user:user /app

USER user

CMD node index.js



Уязвимости. Образы



docker HUB





Уязвимости. Образы





Уязвимости. Образы

Смотрим Dockerfile





Уязвимости. Образы

Смотрим Dockerfile

Собираем сами из репозитория





Уязвимости. Образы

- Смотрим Dockerfile

- Собираем сами из репозитория

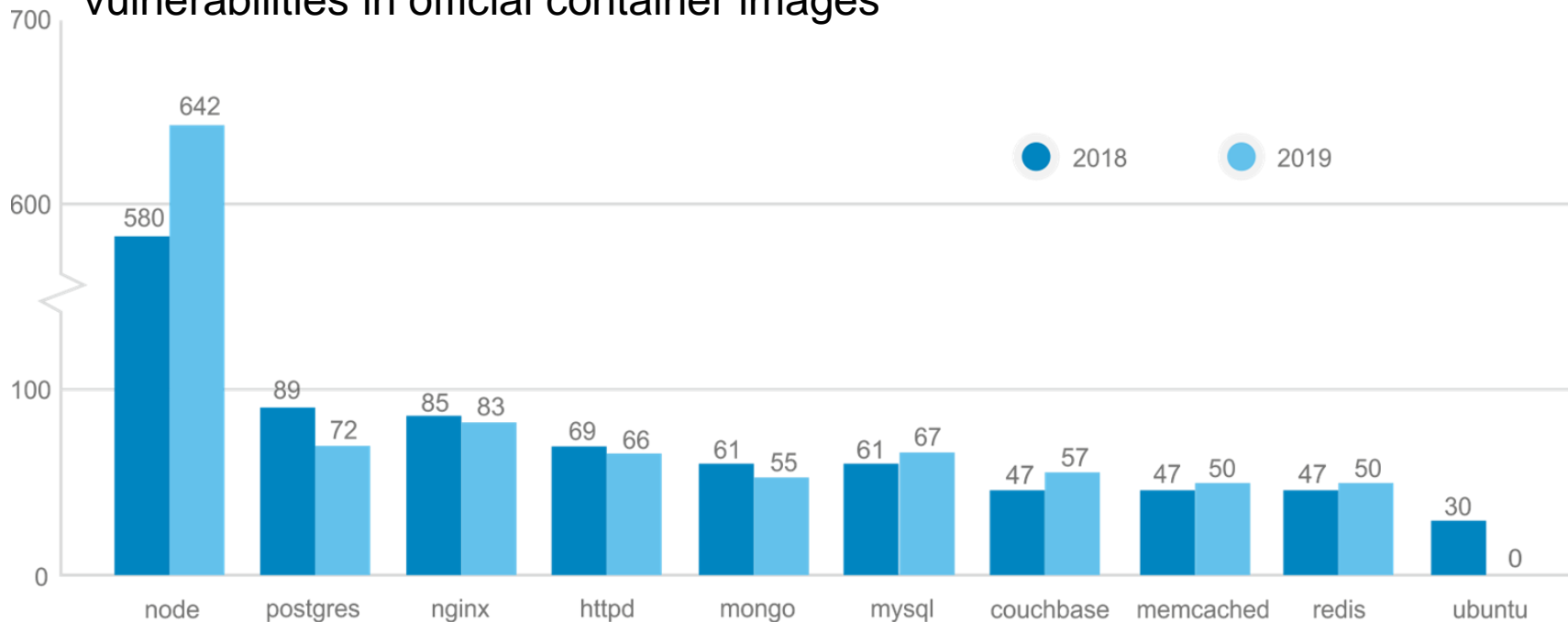
- Используем официальные образы





Уязвимости. Образы

vulnerabilities in official container images





Уязвимости. Анализаторы

Статические





Уязвимости. Анализаторы

Статические



Динамические





Уязвимости. Анализаторы

Статические



Динамические



Всё вместе
(но платно)





Уязвимости. Линтеры



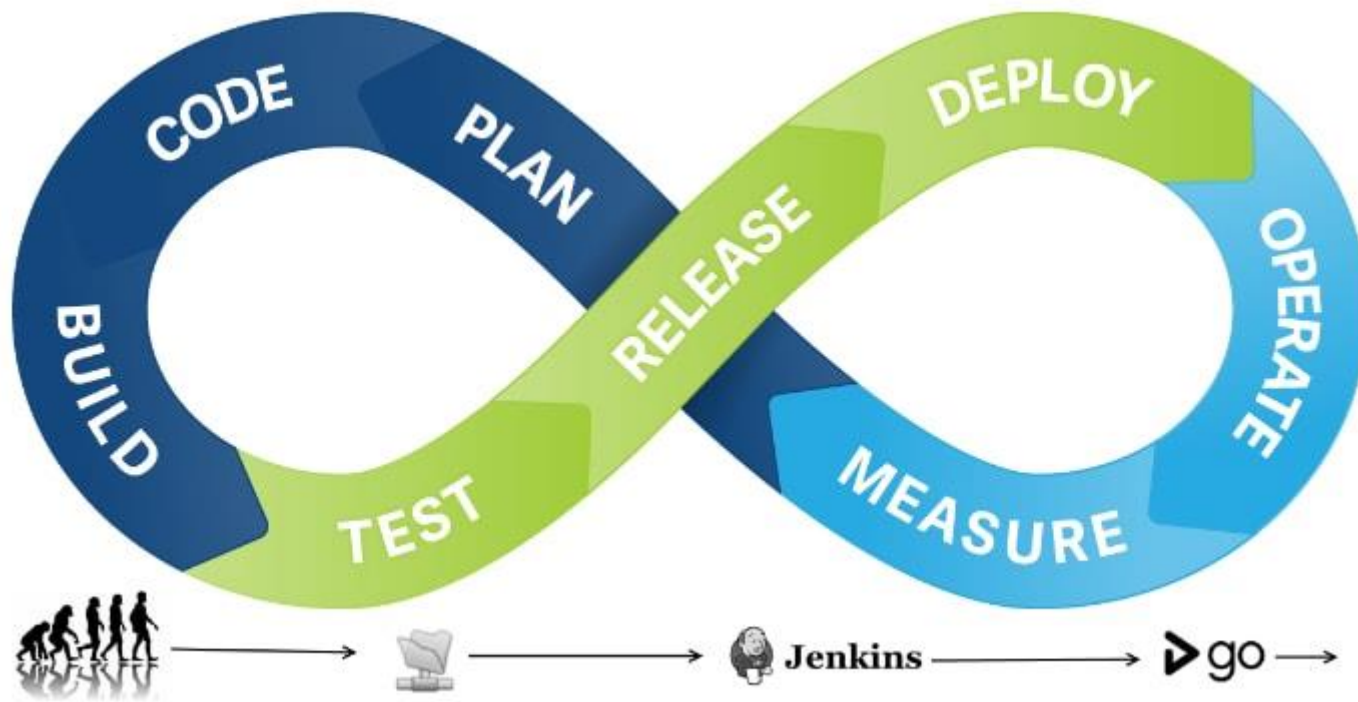
Hadolint

```
Using latest is prone to errors if the image will ever update. Pin the version explicitly to a release tag
1 FROM alpine:latest
2
MAINTAINER is deprecated
3 MAINTAINER ask@slurm.io
4
Pin versions in apk add. Instead of `apk add <package>` use `apk add <package>=<version>`
5 RUN apk add --no-cache ca-certificates curl tar && \
6     update-ca-certificates
7
Use absolute WORKDIR
8 WORKDIR "/opt"
9
Last USER should not be root
10 USER root
11
```

СЛЁРМ



Уязвимости. Линтеры и анализаторы





Capabilities

Docker run Image --priveleged





Capabilities

Docker run Image --priveleged

wget -O - http://сайт/скрипт.sh | bash





Capabilities



Docker run Image --priveleged

wget -O - http://сайт/скрипт.sh | bash

Одно и то же!



Capabilities

Иногда даже базовые Capabilities излишни





Capabilities

Иногда даже базовые Capabilities излишни
В идеале оставляем только нужные

Например:

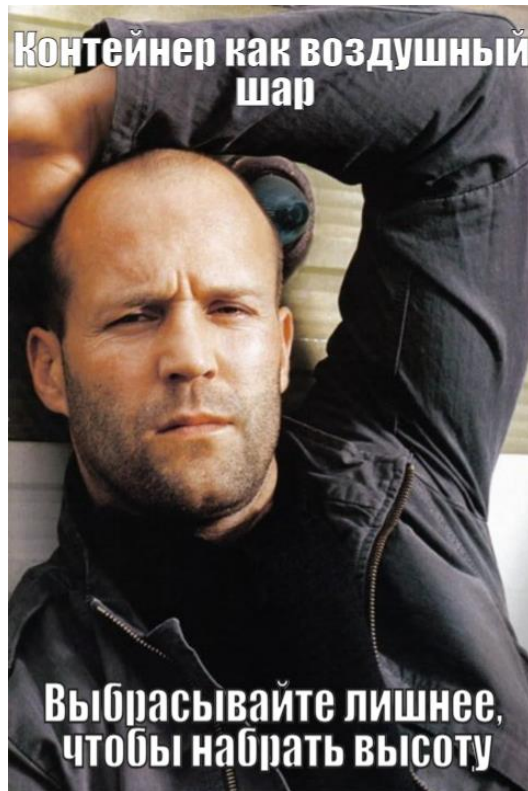
— `docker run -d --cap-drop=all --cap-add=setuid --cap-add=setgid fedora`





Минимизировать площадь атаки

Distroless

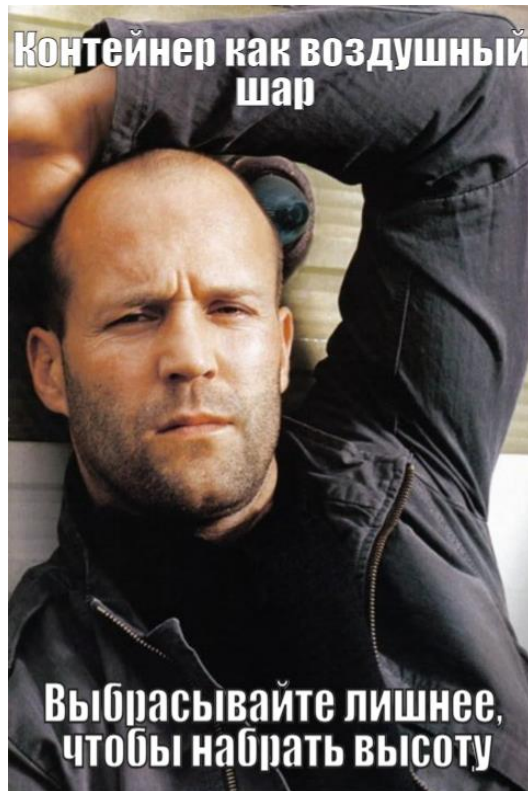




Минимизировать площадь атаки

Distroless

From: scratch



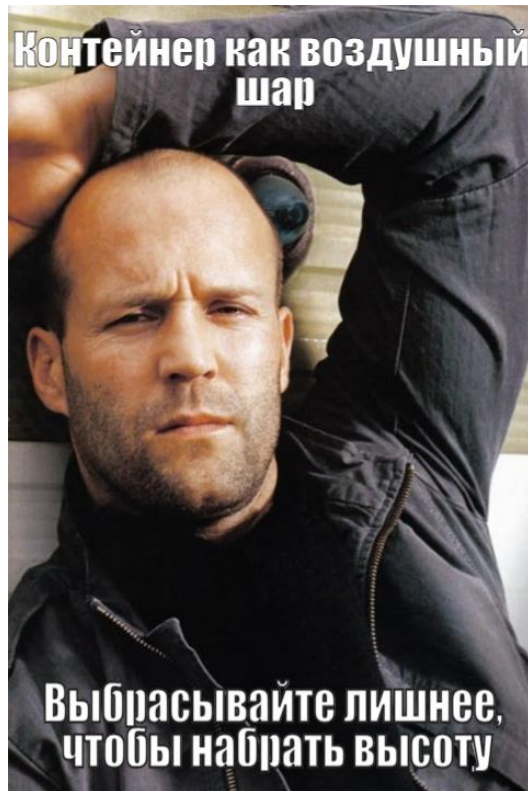


Минимизировать площадь атаки

- Distroless

- From: scratch

- From: [alpine/debian](#) тоже неплохо





Distroless

Только рантайм и ничего больше

gcr.io/distroless/static-debian10





Distroless

Только рантайм и ничего больше

gcr.io/distroless/static-debian10

gcr.io/distroless/base-debian10

gcr.io/distroless/java-debian10

gcr.io/distroless/cc-debian10

gcr.io/distroless/nodejs-debian10

<https://github.com/GoogleContainerTools/distroless>





Distroless. Пример



```
# Start by building the application.  
FROM golang:1.13-buster as build
```

```
WORKDIR /go/src/app  
ADD . /go/src/app
```

```
RUN go get -d -v ./...
```

```
RUN go build -o /go/bin/app
```

```
# Now copy it into our base image.  
FROM gcr.io/distroless/base-debian10  
COPY --from=build /go/bin/app /  
CMD ["/app"]
```

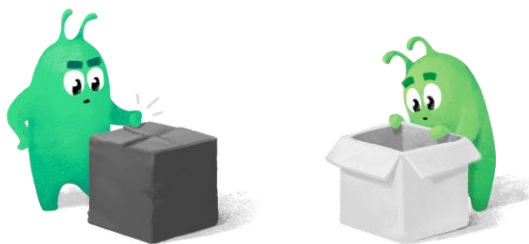


FROM: Scratch



Подписанные контейнеры

`sudo export DOCKER_CONTENT_TRUST=1`

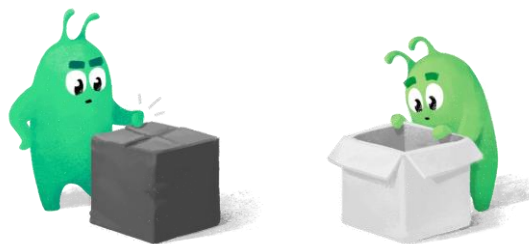




Подписанные контейнеры

`sudo export DOCKER_CONTENT_TRUST=1`

Верификация издателя и целостности контейнера





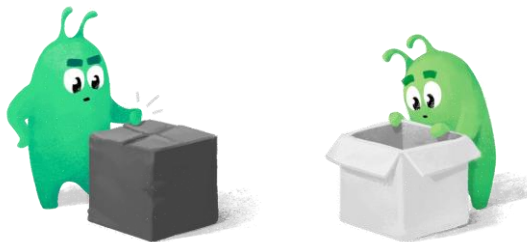
Подписанные контейнеры

- `sudo export DOCKER_CONTENT_TRUST=1`

- Верификация издателя и целостности контейнера

- Подпись отдельно для каждого тега

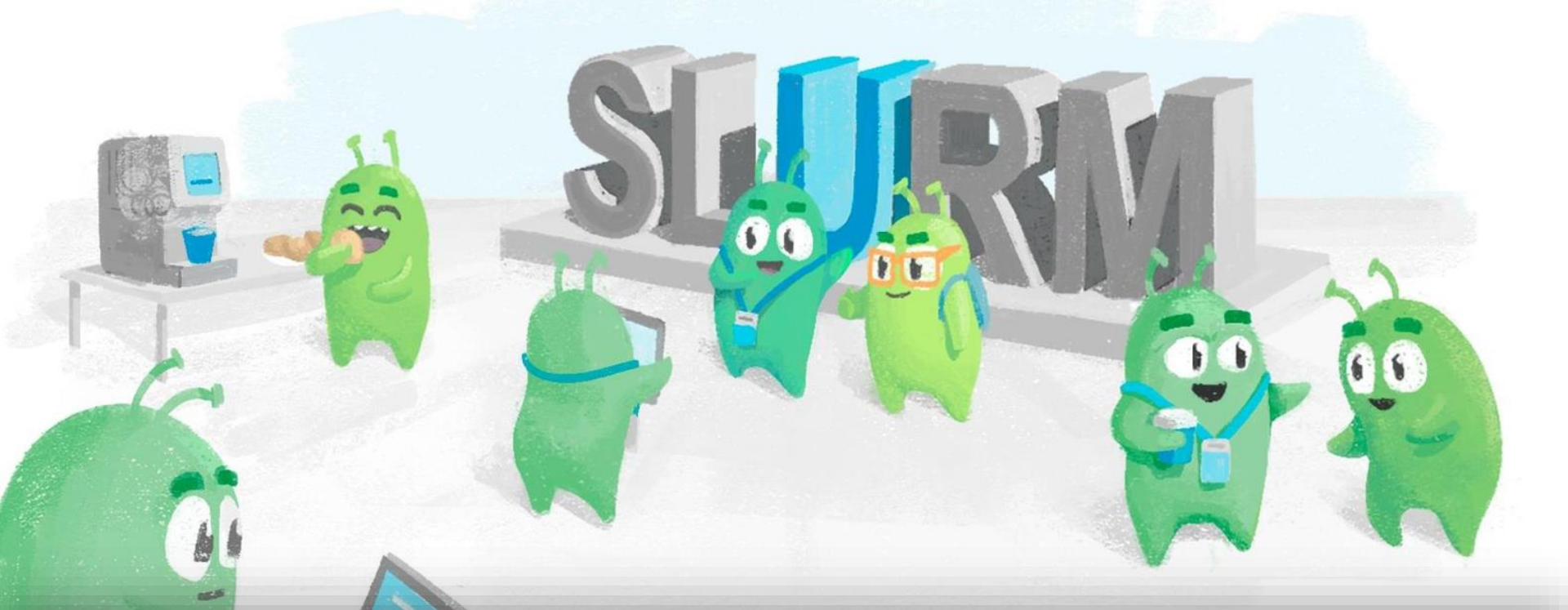
- Latest может быть не подписан, а 3.1.6 подписан



PS

Пожалуйста, не тащите sshd в контейнеры!





southbridge.io

Спасибо!

СЛЁРМ

slurm.io