LinuxKit - от контейнеров к VM

9 сентрября 2017

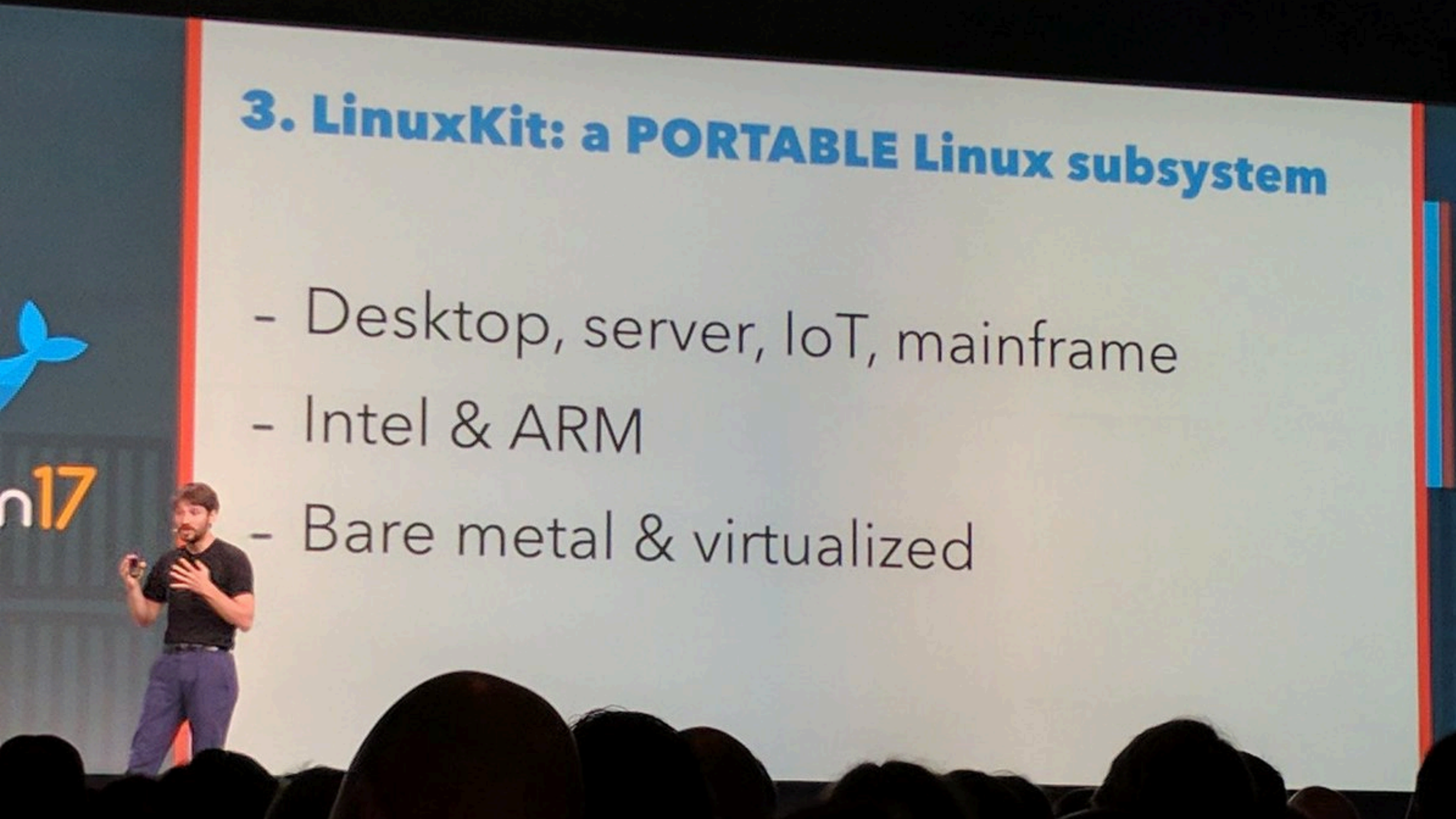
Олег Федосеев

olegfedoseev


1. LinuxKit: a SECURE Linux subsystem
Only works with containers
- Smaller attack surface
- Immutable infrastructure
- Sandboxed system services
Incubator for security innovations
- Wireguard, Landlock, KSPP
- MirageOS type safe system daemons
Community-first security process
- Linux is too big for any one company to secure it
- Participate in existing Linux security efforts
dockercon17

3. LinuxKit: a PORTABLE Linux subsystem

- Desktop, server, IoT, mainframe
- Intel & ARM
- Bare metal & virtualized




moby
project


LINUXKIT

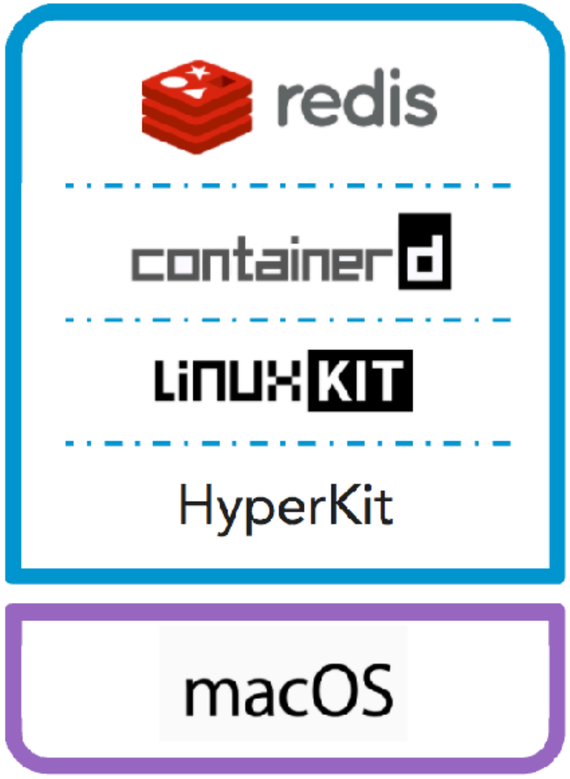
Истоки LinuxKit

- Удобный механизм дистрибуции приложений
- Одно “ядро” - Linux Containers
- Множество платформ
- Постоянный рост угрозы безопасности
- Неизменяемая инфраструктура
- UniKernels :)

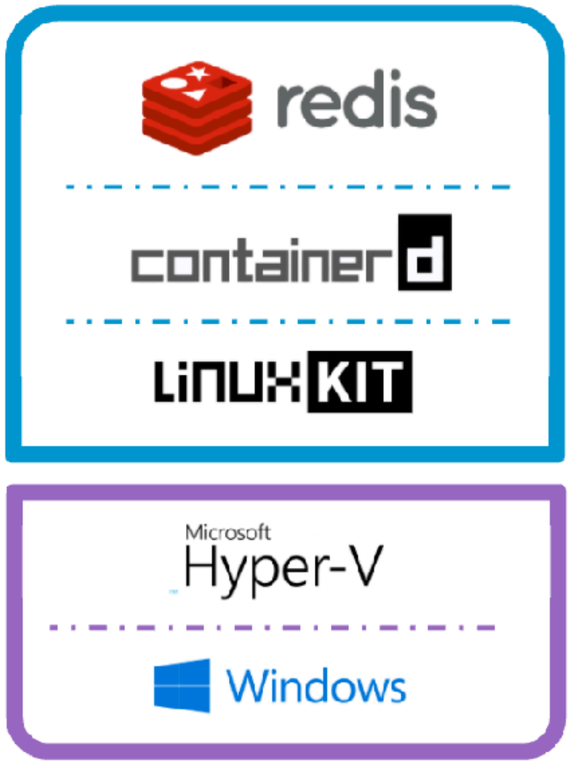
Что такое LinuxKit?

- Конструктор для сборки образа Linux
- Все сервисы в контейнерах
- Самый минимум сервисов
- Максимально ограниченные права и возможности
- Основная файловая система read-only

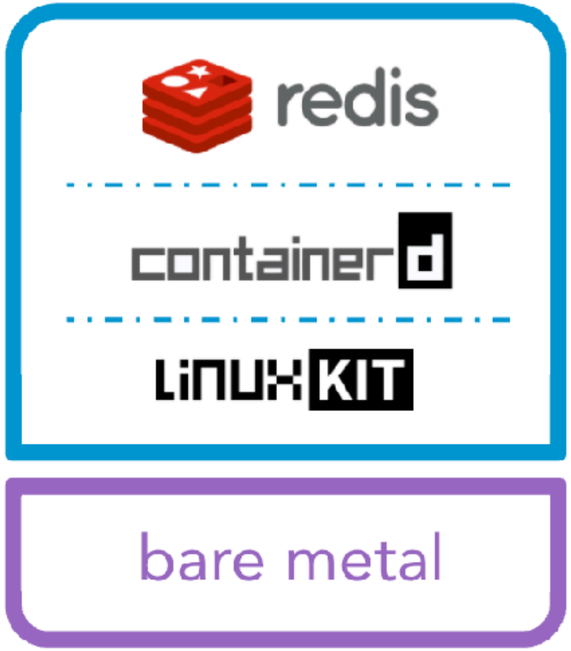
LinuxKit



"RedisOS"
for Mac



"RedisOS"
for Windows



"RedisOS"
for bare metal

```
kernel:
  image: linuxkit/kernel:4.9.47
  cmdline: "console=tty0 console=ttyS0 console=ttyAMA0"
init:
  - linuxkit/init:79973d34faf7d4654462f3408c5eb00befaf03b8
  - linuxkit/runc:a1b564248a0d0b118c11e61db9f84ecf41dd2d2a
  - linuxkit/containerd:06876ceef325e49e9ba119659357768d5df89075
onboot:
  - name: dhcpcd
    image: linuxkit/dhcpcd:f3f5413abb78fae9020e35bd4788fa93df4530b7
    command: ["/sbin/dhcpcd", "--nobackground", "-f", "/dhcpcd.conf", "-1"]
services:
  - name: getty
    image: linuxkit/getty:797cb79e0a229fcd16ebf44a0da74bcec03968ec
  - name: redis
    image: redis:3.0.7-alpine
    capabilities:
     - CAP_NET_BIND_SERVICE
     - CAP_CHOWN
     - CAP_SETUID
     - CAP_SETGID
     - CAP_DAC_OVERRIDE
    net: host
```

Описание базовой системы

```
kernel:
  image: linuxkit/kernel:4.9.47
  cmdline: "console=tty0 console=ttyS0 console=ttyAMA0"
init:
  - linuxkit/init
  - linuxkit/runc
  - linuxkit/containerd
onboot:
  - name: dhcpcd
    image: linuxkit/dhcpcd
    command: ["/sbin/dhcpcd", "--nobackground", "-f", "/dhcpcd.conf", "-1"]
```

Описание базовой системы

```
kernel:
  image: linuxkit/kernel:4.9.47
  cmdline: "console=tty0 console=ttyS0 console=ttyAMA0"
init:
  - linuxkit/init
  - linuxkit/runc
  - linuxkit/containerd
onboot:
  - name: dhcpcd
    image: linuxkit/dhcpcd
    command: ["/sbin/dhcpcd", "--nobackground", "-f", "/dhcpcd.conf", "-1"]
```

Описание базовой системы

```
kernel:
  image: linuxkit/kernel:4.9.47
  cmdline: "console=tty0 console=ttyS0 console=ttyAMA0"
init:
  - linuxkit/init
  - linuxkit/runc
  - linuxkit/containerd
onboot:
  - name: dhcpcd
    image: linuxkit/dhcpcd
    command: ["/sbin/dhcpcd", "--nobackground", "-f", "/dhcpcd.conf", "-1"]
```

Описание базовой системы

```
kernel:
  image: linuxkit/kernel:4.9.47
  cmdline: "console=tty0 console=ttyS0 console=ttyAMA0"
init:
  …
onboot:
  - name: dhcpcd
    image: linuxkit/dhcpcd
    command: ["/sbin/dhcpcd", "--nobackground", "-f", "/dhcpcd.conf",
"-1"]
```

Описание сервисов

```
services:
  - name: getty
    image: linuxkit/getty
  - name: redis
    image: redis:3.0.7-alpine
    capabilities:
     - CAP_NET_BIND_SERVICE
     - CAP_CHOWN
     - CAP_SETUID
     - CAP_SETGID
     - CAP_DAC_OVERRIDE
    net: host
```

Описание сервисов

```
services:
  - name: getty
    image: linuxkit/getty
  - name: redis
    image: redis:3.0.7-alpine
    capabilities:
     - CAP_NET_BIND_SERVICE
     - CAP_CHOWN
     - CAP_SETUID
     - CAP_SETGID
     - CAP_DAC_OVERRIDE
    net: host
```

Описание сервисов

```
services:
  - name: getty
    image: linuxkit/getty
  - name: redis
    image: redis:3.0.7-alpine
    capabilities:
     - CAP_NET_BIND_SERVICE
     - CAP_CHOWN
     - CAP_SETUID
     - CAP_SETGID
     - CAP_DAC_OVERRIDE
    net: host
```

Что внутри?

```
linuxkit:~# pstree
init---containerd-+-containerd-shim---rungetty.sh---login
                   |
                   `-containerd-shim---redis-server
```

Что внутри?

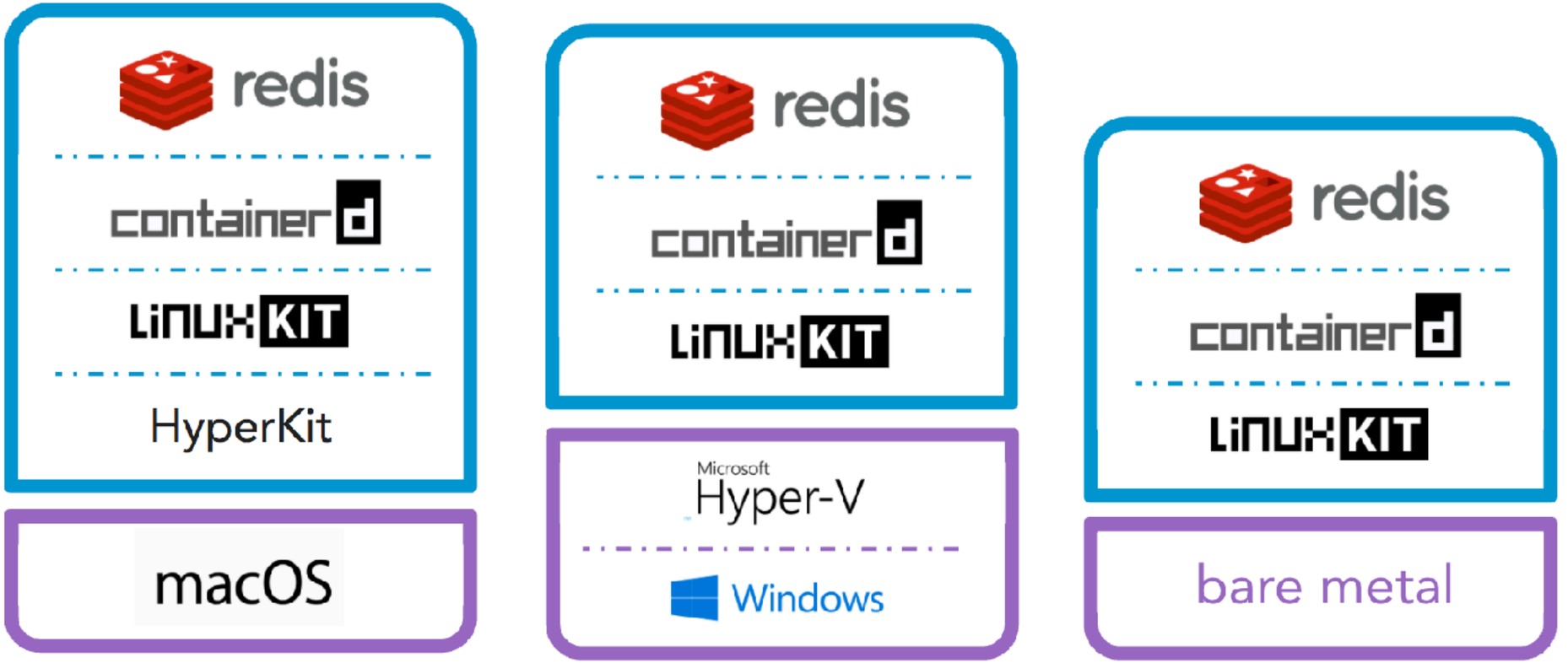
```
linuxkit:~# pstree
init---containerd-+-containerd-shim---rungetty.sh---login
                  |
                  `-containerd-shim---redis-server
```

- **init** и **containerd** как “точка входа”
- **login** для консоли
- **redis-server** основной сервис

Что внутри?

```
linuxkit:~# ctr c
CONTAINER    IMAGE    RUNTIME
getty        -        io.containerd.runtime.v1.linux
redis        -        io.containerd.runtime.v1.linux
```

LinuxKit

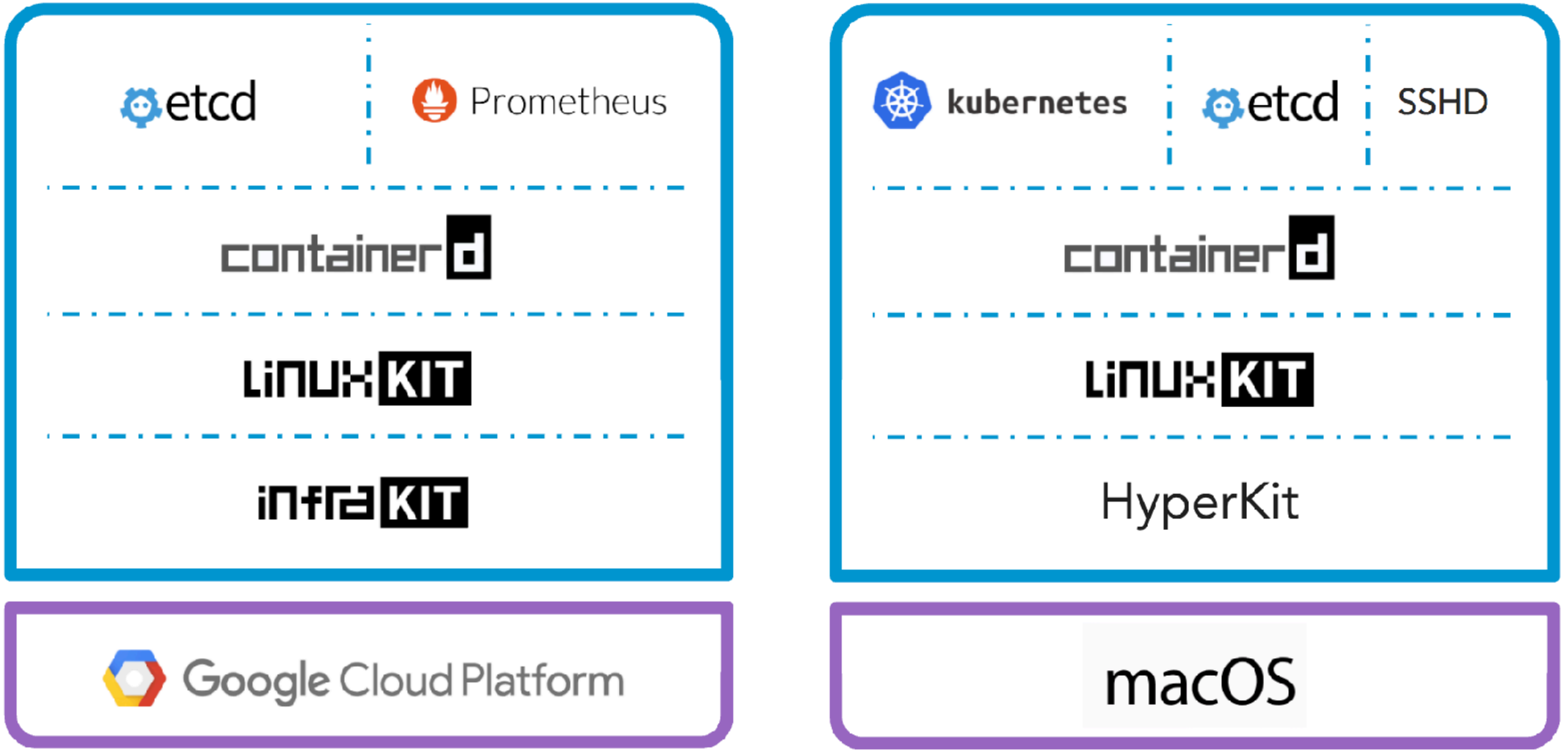


"RedisOS"
for Mac

"RedisOS"
for Windows

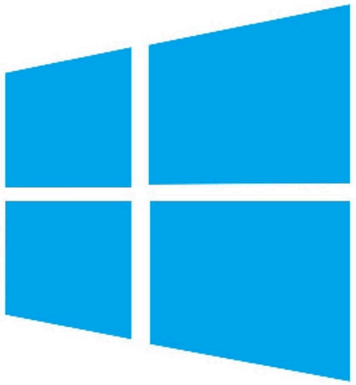
"RedisOS"
for bare metal

LinuxKit


etcd
Prometheus
containerd
LinuxKit
infraKit
Google Cloud Platform
kubernetes
etcd
SSHD
containerd
LinuxKit
HyperKit
macOS

Поддерживаемые облачные платформы

Поддерживаемые гипервизоры



Microsoft
Hyper-V

Hyperkit

Хватит теории!
Как собрать образ?

Что нужно чтобы начать?

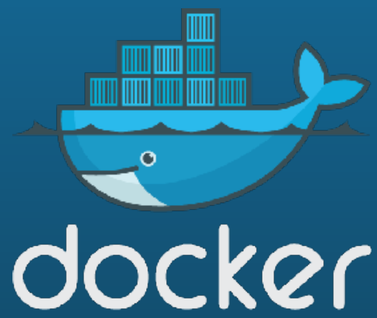
- moby tool (и опционально linuxkit)
- описание системы в yaml-файле
- ...
- Всё!

Что нужно чтобы начать?

```
go get -u github.com/moby/tool/cmd/moby
go get -u github.com/linuxkit/linuxkit/src/cmd/linuxkit

moby build examples/redis-os.yml
linuxkit run redis-os
```

А теперь демо!



Вопросы?

Олег Федосеев
olegfedoseev

t.me/DockerNsk
t.me/GDGNsk