DaoCloud

ebay | IT大咖说 不止于技术

绝不避谈DOCKER安全

孙宏亮

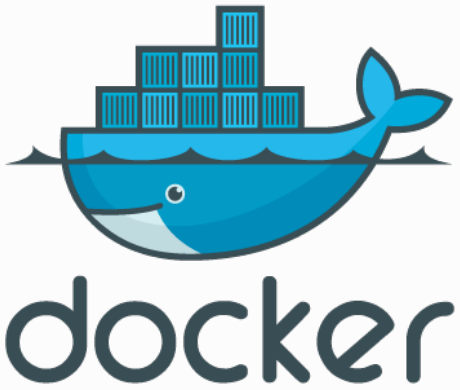
DaoCloud

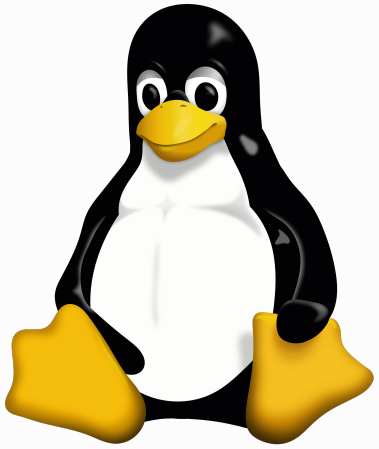
allen.sun@daocloud.io

ABOUT ME

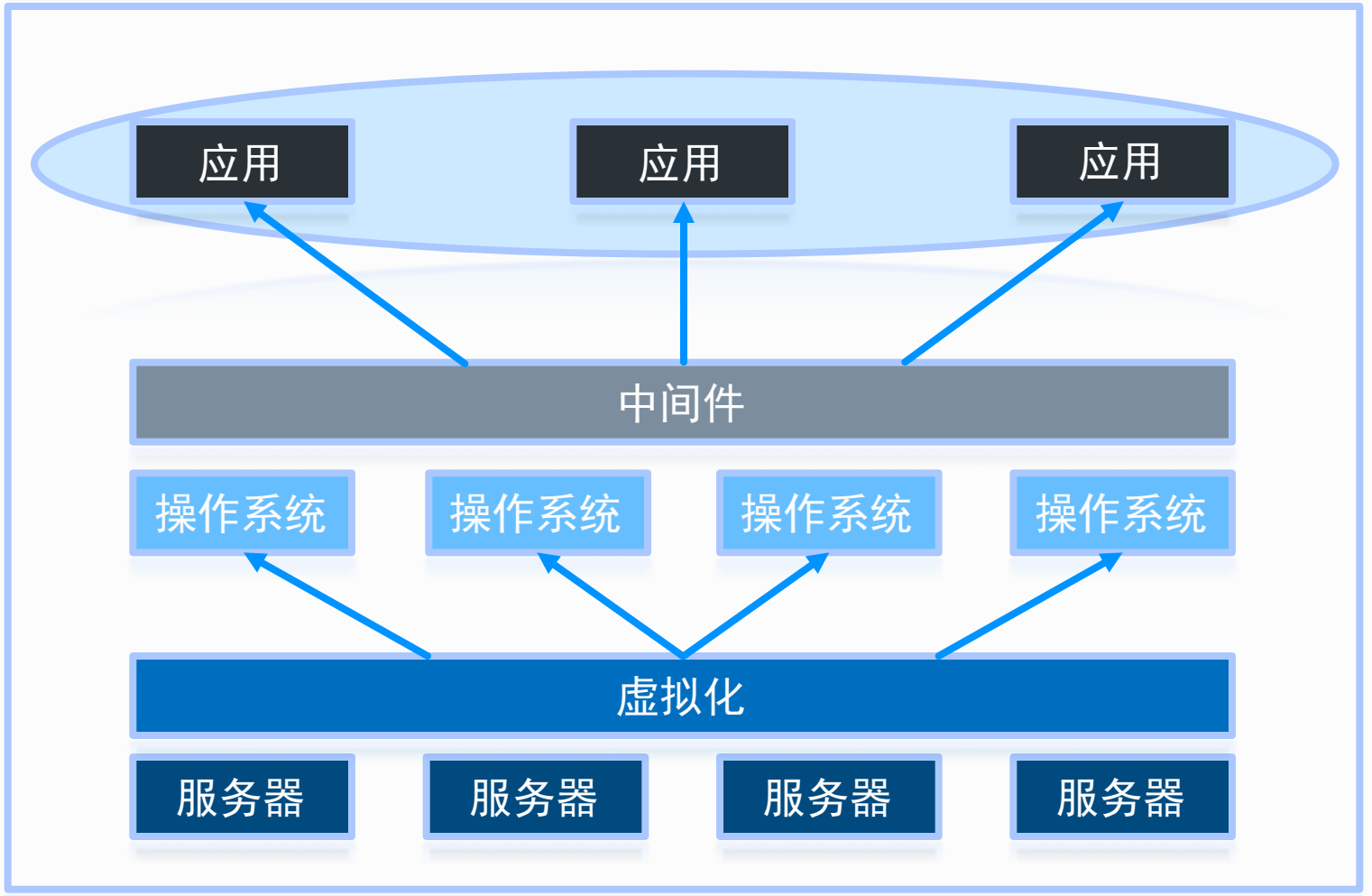
- DaoCloud
- Docker
- Linux
- GitHub: allencloud

DaoCloud





企业级IT架构



Dev

MQ/Cache

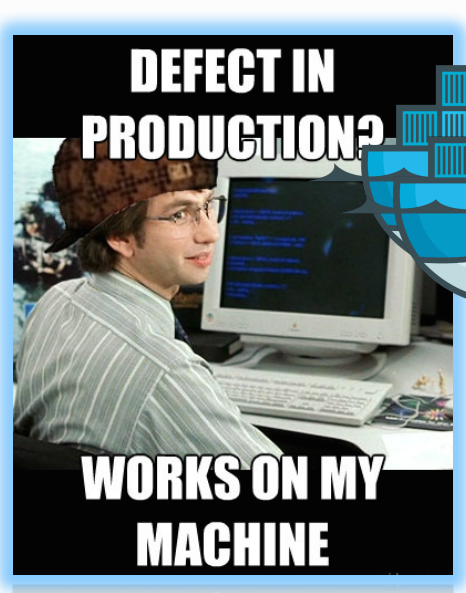
RHEL/Windows

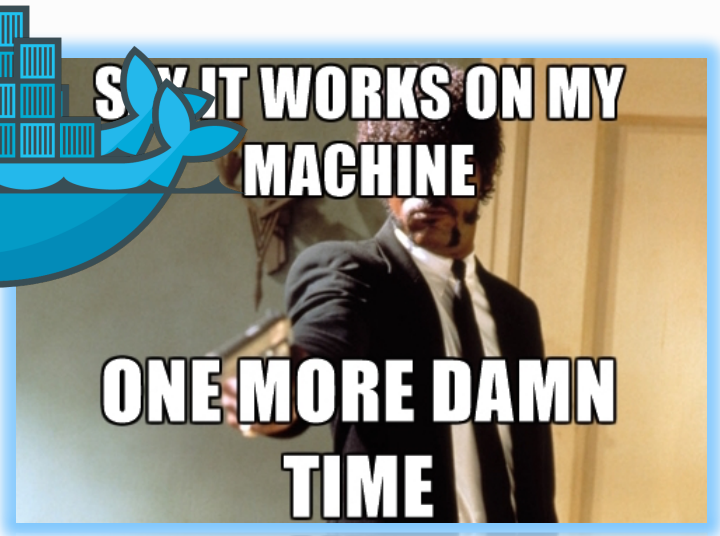
Ops

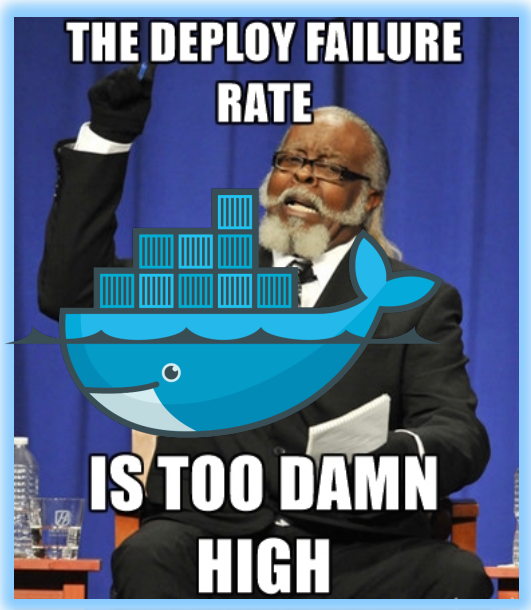
VMWare/KVM

X86/Power

企业应用交付流程







开发 → 测试 → 运维

DOCKER不为安全而生

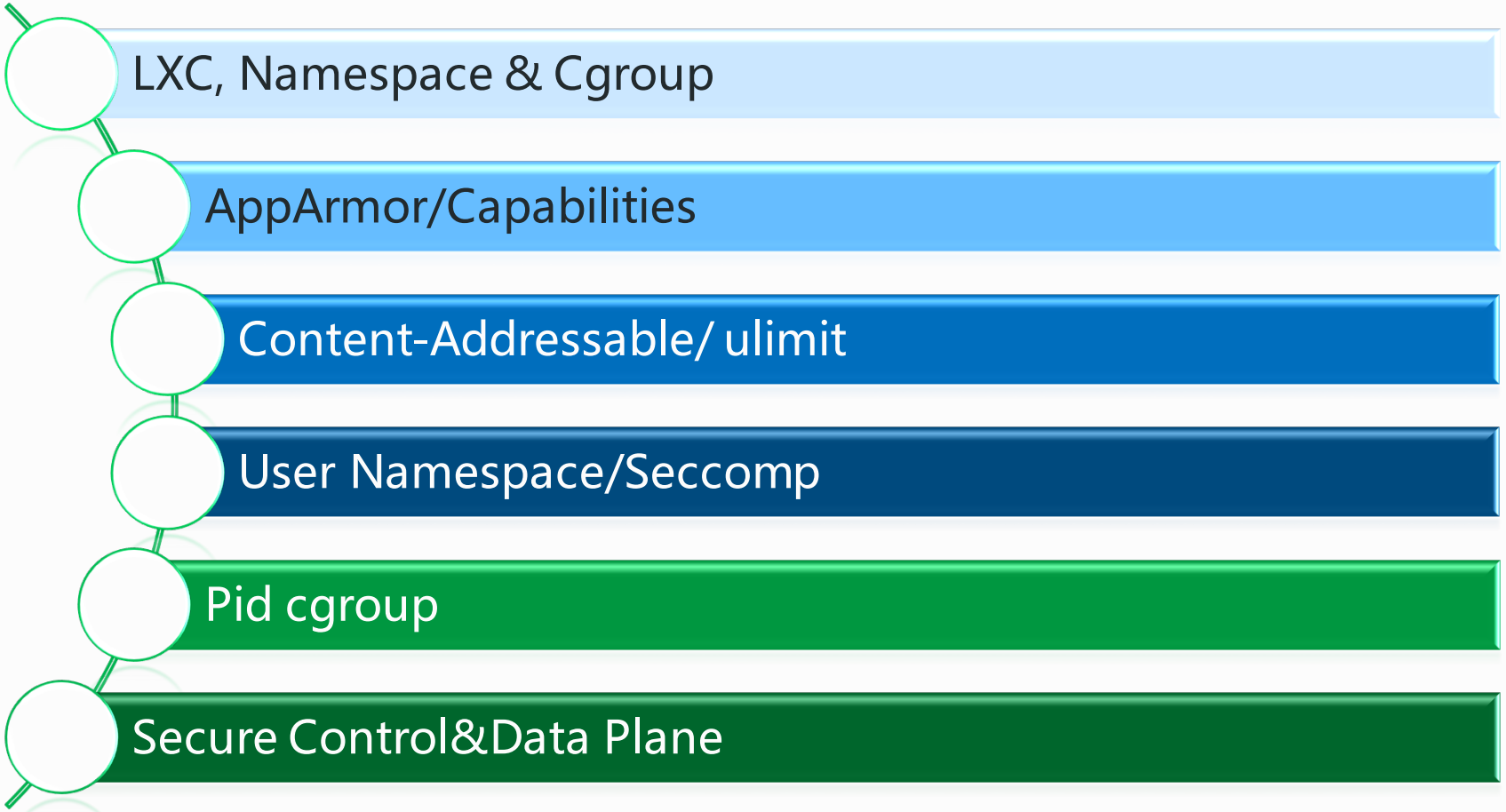
不可回避！

易用性　　标准化　　性能

外界对DOCKER的安全担忧

- 没有 VMs 安全
- 降低安全性获得性能
- 容器内root就是宿主机root
- Cgroup/Namespace不安全
- 网络隔离弱
- ……

安全发展史


LXC, Namespace & Cgroup
AppArmor/Capabilities
Content-Addressable/ ulimit
User Namespace/Seccomp
Pid cgroup
Secure Control&Data Plane

安全发展维度

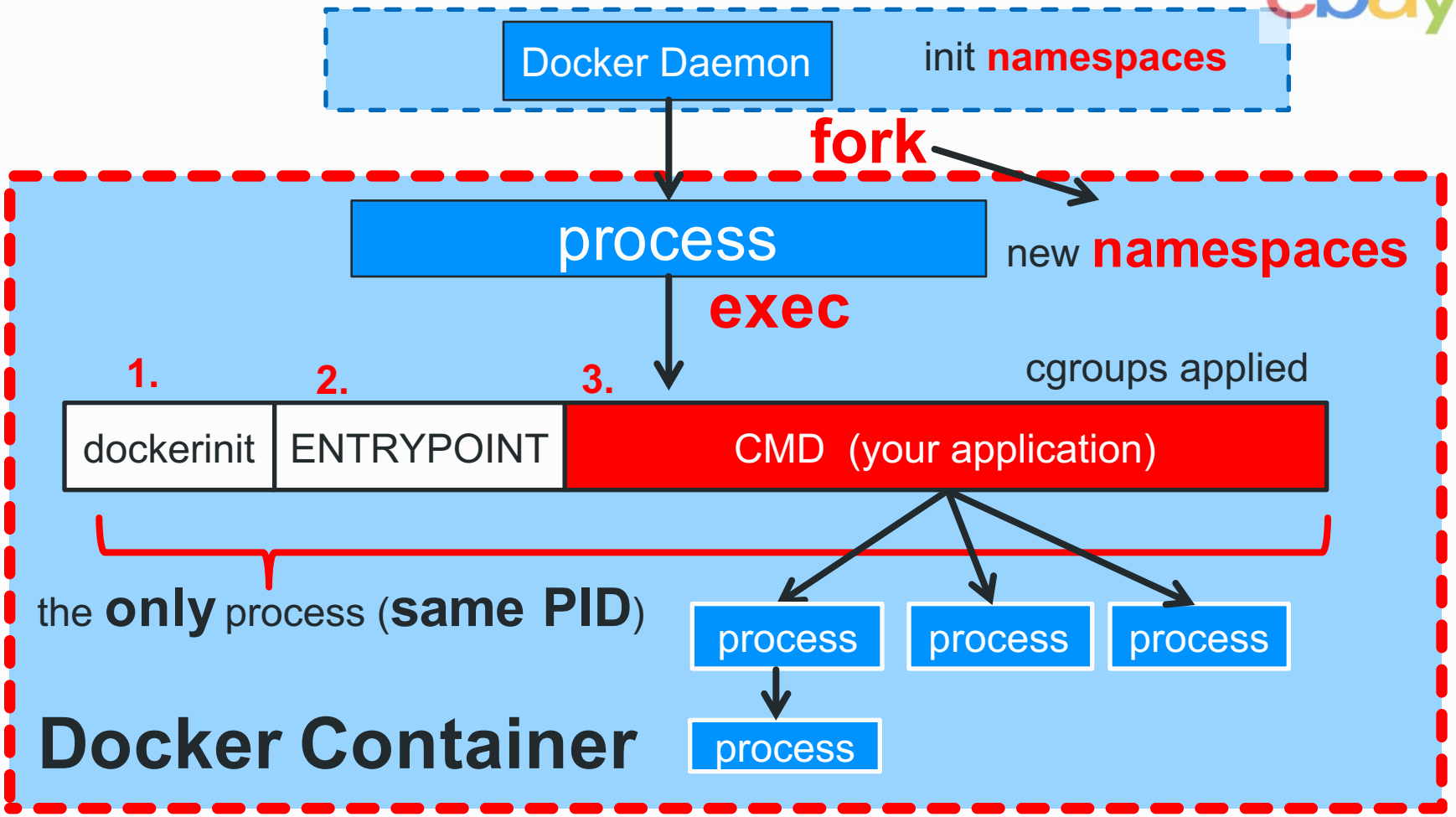
- 通信安全
  - Client—Engine
  - Engine—Registry
- 镜像安全
- 容器安全
- 应用安全

Available Container Security Features, Requirements and Defaults			
Security Feature	**LXC 2.0**	**Docker 1.11**	**CoreOS Rkt 1.3**
User Namespaces	Default	Optional	Experimental
Root Capability Dropping	Weak Defaults	Strong Defaults	Weak Defaults
Procfs and Sysfs Limits	Default	Default	Weak Defaults
Cgroup Defaults	Default	Default	Weak Defaults
Seccomp Filtering	Weak Defaults	Strong Defaults	Optional
Custom Seccomp Filters	Optional	Optional	Optional
Bridge Networking	Default	Default	Default
Hypervisor Isolation	Coming Soon	Coming Soon	Optional
MAC: AppArmor	Strong Defaults	Strong Defaults	Not Possible
MAC: SELinux	Optional	Optional	Optional
No New Privileges	Not Possible	Optional	Not Possible
Container Image Signing	Default	Strong Defaults	Default
Root Interation Optional	True	False	Mostly False

Secure By Default

"In this modern age, I believe that there is little excuse for not running a Linux application in some form of a Linux container, MAC or lightweight sandbox."

– Aaron Grattafiori, author of NCC Group's white paper



文件系统 / Pid / 网络 / IPC …

DOCKER DAEMON 安全

- Docker Daemon的控制权
- Root权限
- TLS

HUMAN FACTOR

```
// It's a bad idea to bind to TCP without tlsverify.
if proto == "tcp" && (serverConfig.TLSConfig == nil || serverConfig.T
    logrus.Warn("[!] DON'T BIND ON ANY IP ADDRESS WITHOUT setting "+
        "-tlsverify IF YOU DON'T KNOW WHAT YOU'RE DOING [!]")
}
```

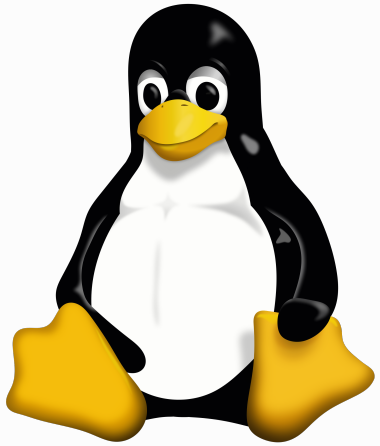
一无所有!

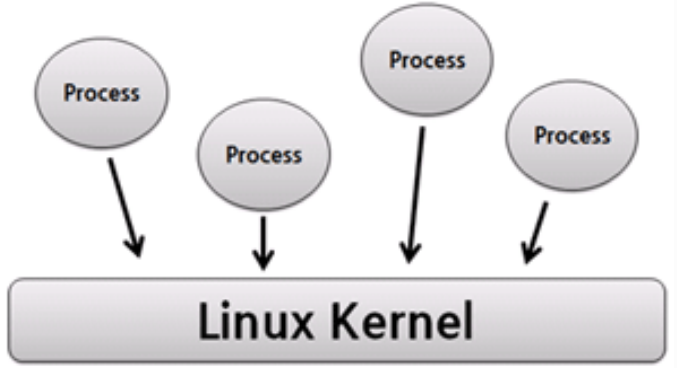

DEMO

DOCKER REGISTRY 安全

- 一个真实的故事
- 集群Registry中所有镜像的污染

DOCKER容器安全

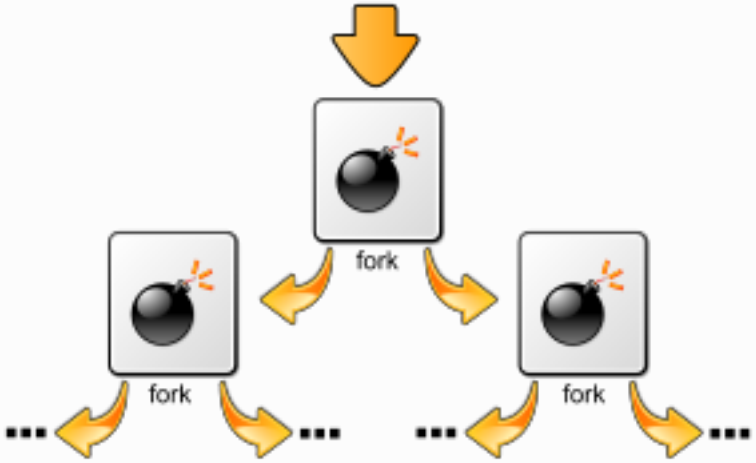




Linux为进程而设计，不为容器（进程组）而设计

FORK BOMB

- 利用系统调用fork（或其他等效的方式）
- 拒绝服务攻击；
- fork炸弹通过连续自我复制占用系统资源
- 导致系统减速或崩溃。



DOS

- Filesystem/Disk
- Processes
- Fd
- Signals

https://github.com/docker/docker/issues/15815，docker 1.8.1

- Fork Bomb
- Disk space
- Disk inode

DOCKER应用安全

- 镜像的安全（签名、校验）
- 镜像内容的攻击平面
- 应用的credential信息


DEMO

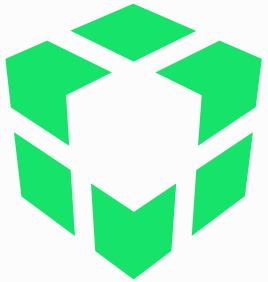
共享内核

内核也是一种资源

REFERENCE

- http://blog.etsukata.com/2014/05/docker-linux-kernel.html
- https://blog.docker.com/2016/04/docker-security/

Thank you



DaoCloud