构建安全的PaaS云服务

演讲人：吴建强

职务：搜狐 安全经理

日期：2014/09/25

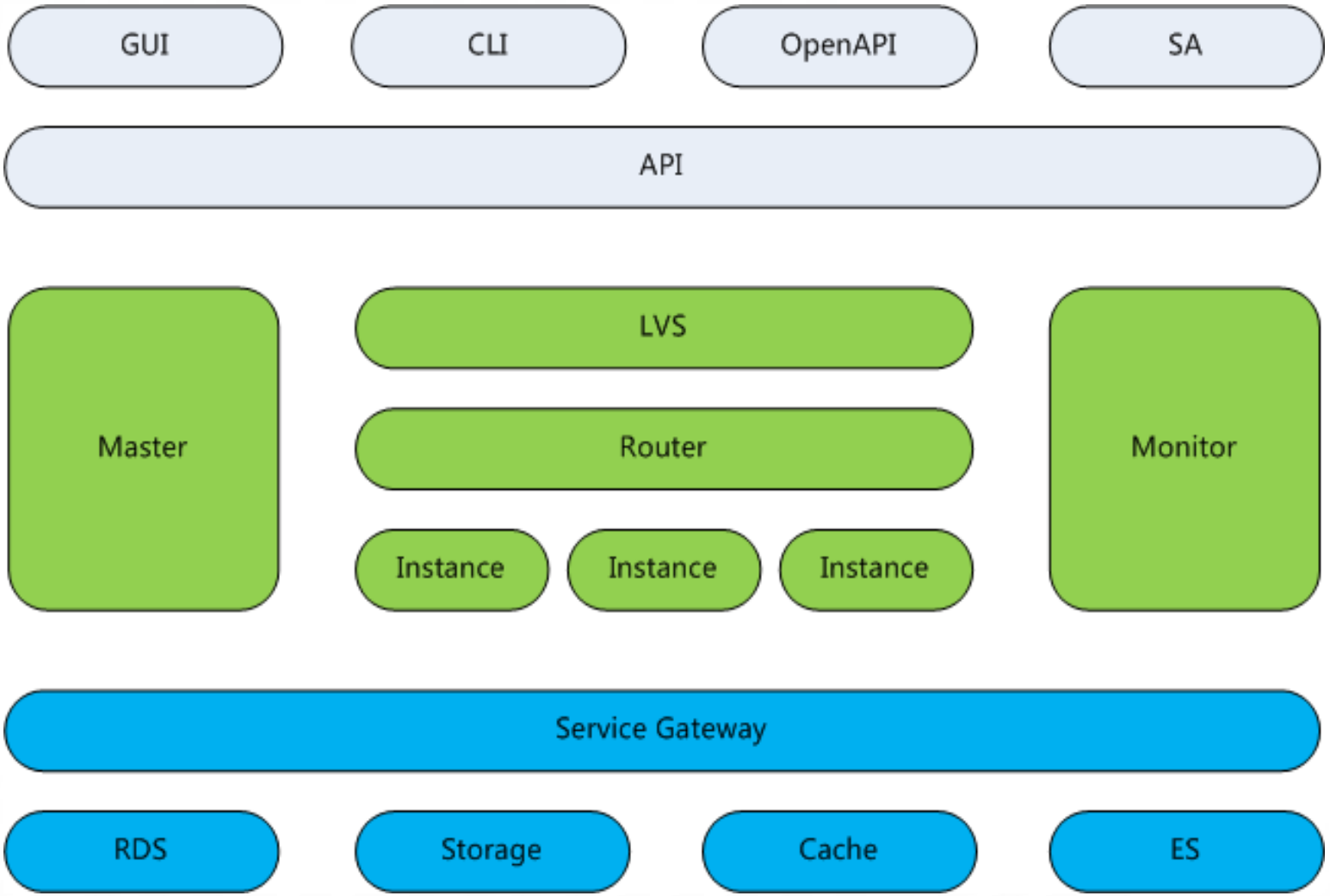
PaaS介绍

- PaaS是什么
- 为什么使用PaaS
- PaaS价值观
  - Forget servers
  - Run Anything
  - See Everything
  - Trust & Manage

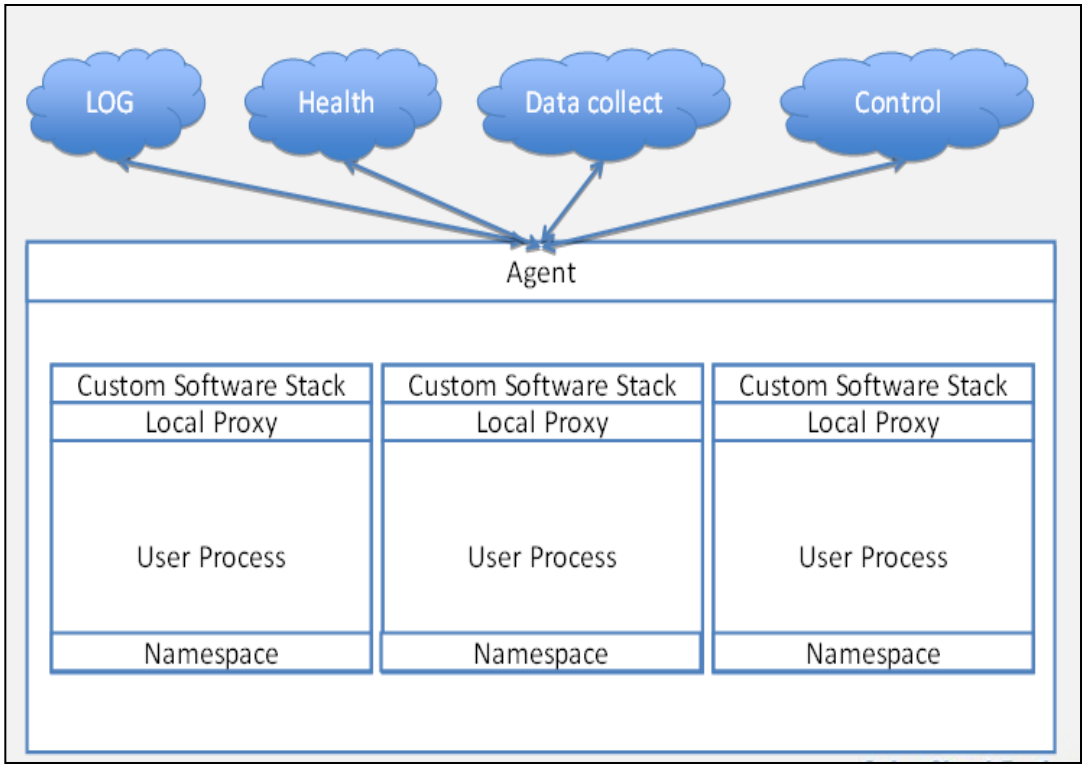
PaaS安全

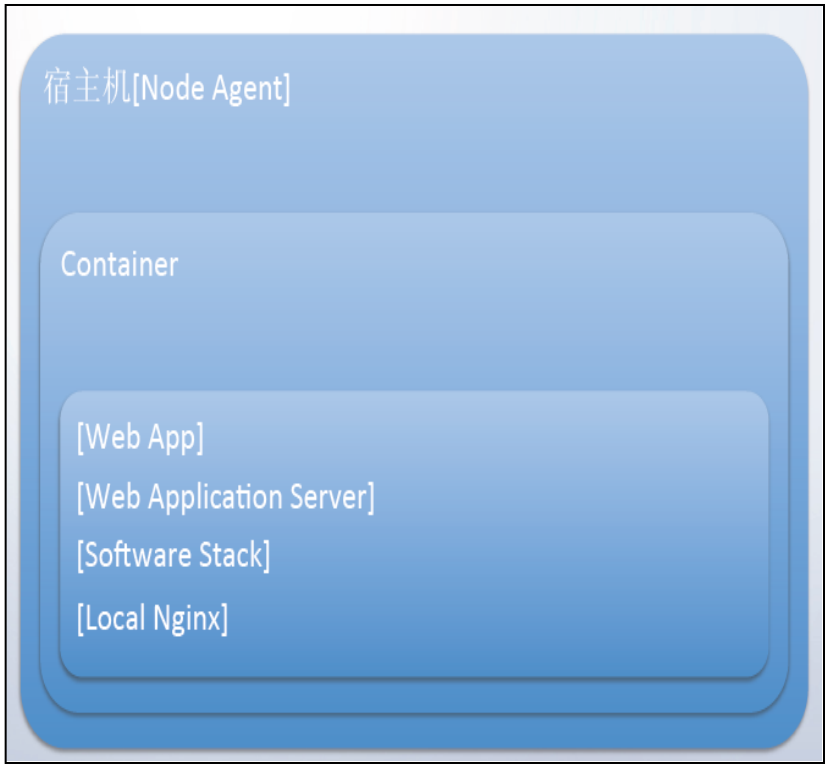
- 用户所担心的安全问题
  - 服务可用
  - 数据安全
  - 代码安全
  - 成本安全

PaaS架构


GUI
CLI
OpenAPI
SA
API
Master
LVS
Router
Instance
Instance
Instance
Monitor
Service Gateway
RDS
Storage
Cache
ES

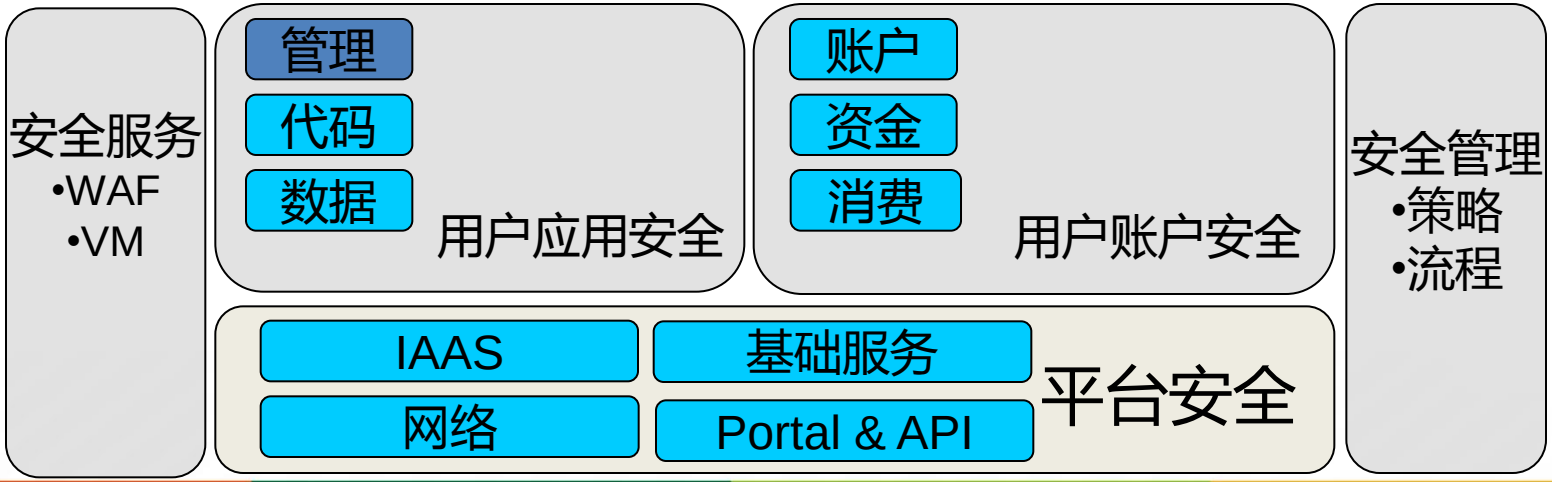
PaaS架构


LOG
Health
Data collect
Control
Agent
Custom Software Stack
Local Proxy
User Process
Namespace
Custom Software Stack
Local Proxy
User Process
Namespace
Custom Software Stack
Local Proxy
User Process
Namespace


宿主机[Node Agent]
Container
[Web App]
[Web Application Server]
[Software Stack]
[Local Nginx]

PaaS安全目标

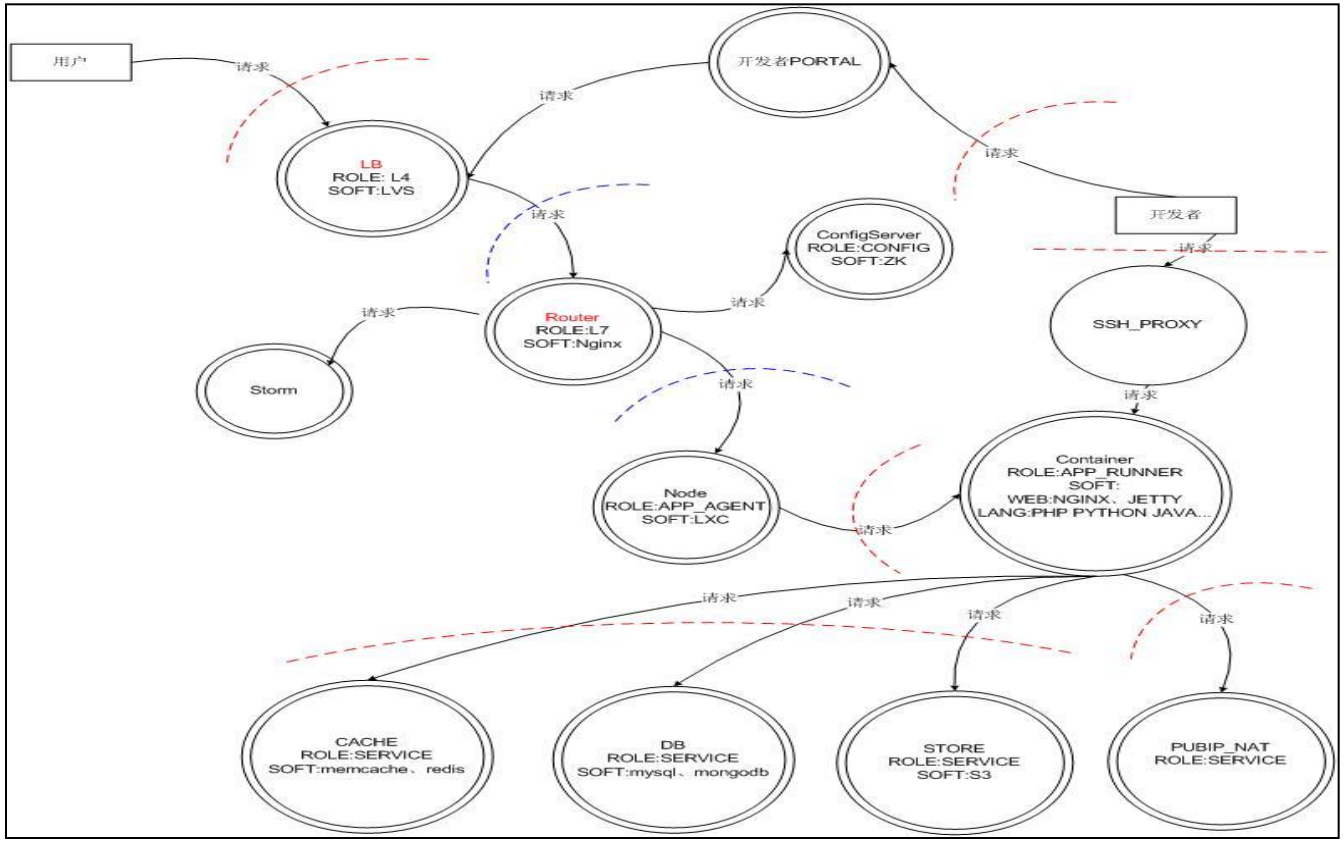
- 平台安全
- 用户安全
- 安全管理
- 安全服务



安全原则

- PDR+Defense in depth
- SD3+C
  - **Secure by Design**
  - **Secure by Default**
  - Secure in Deployment and Communication
- SDL

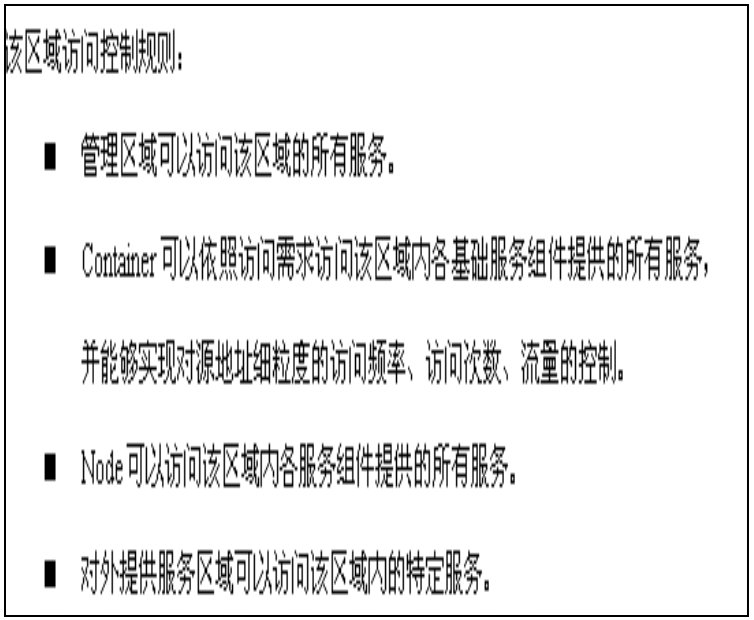
威胁建模

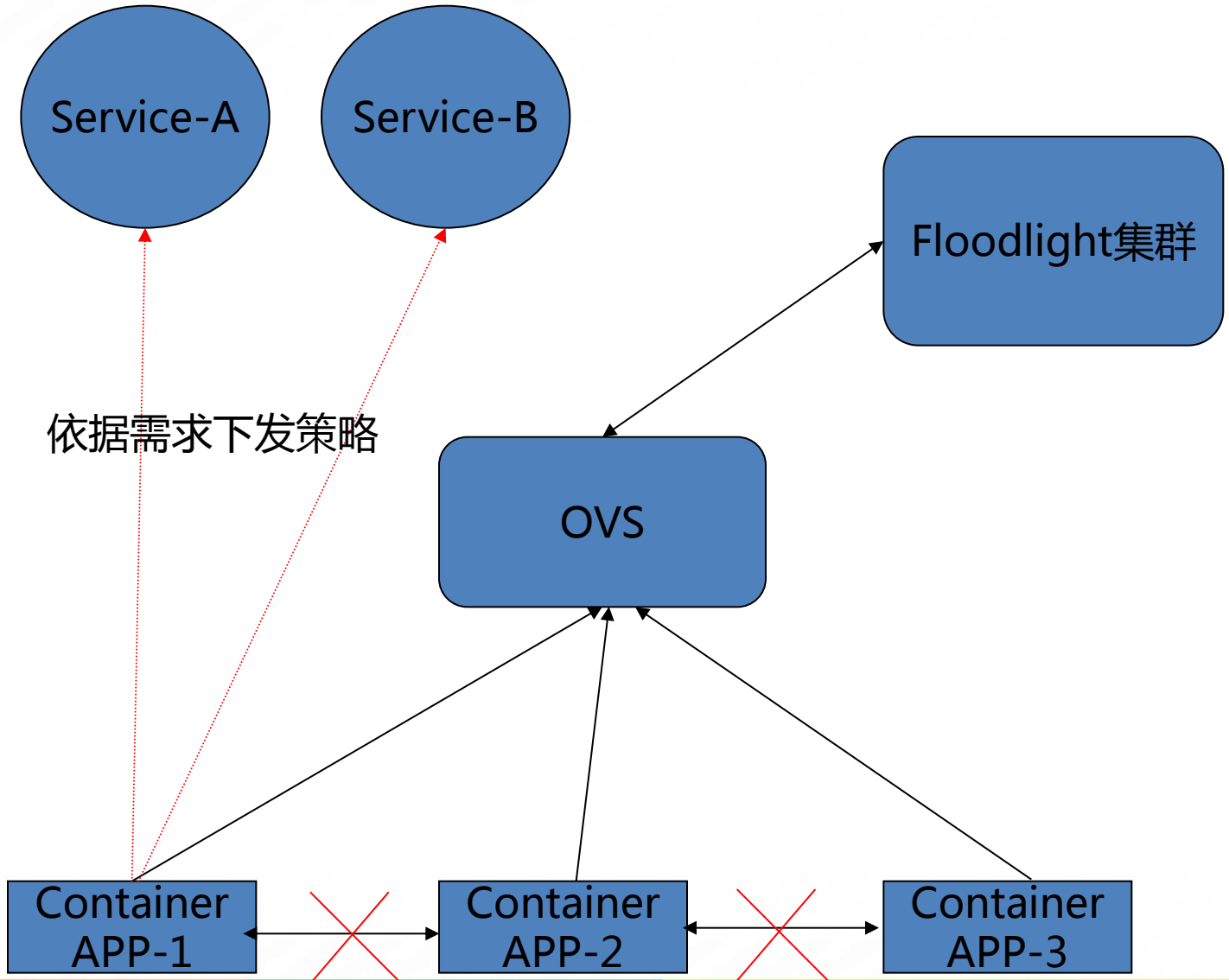


- DDOS
- Elevation of Privilege
- Information Disclosure
- Tampering

PaaS安全架构

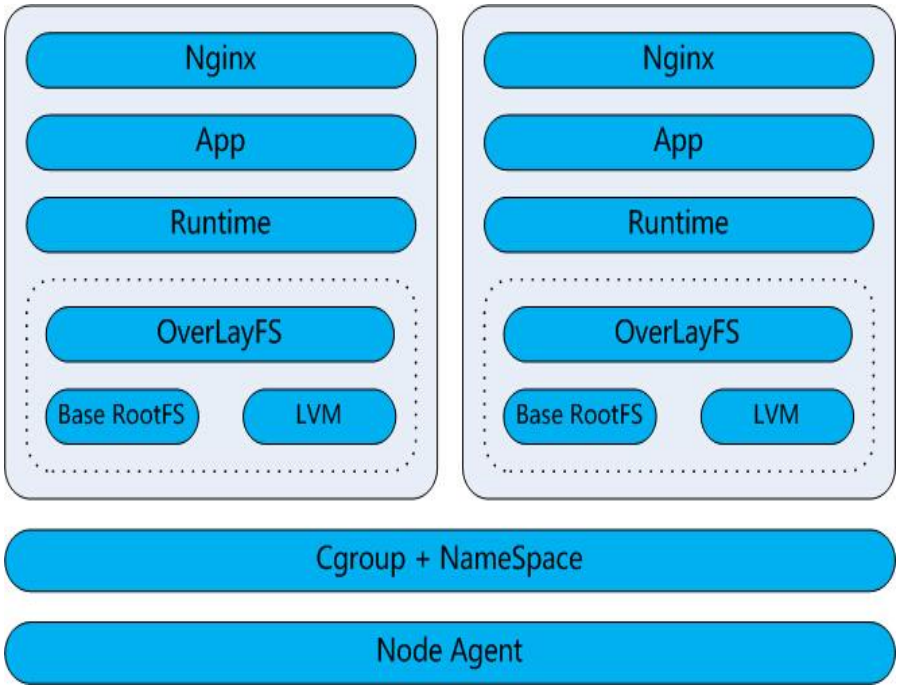
- 网络及区域安全
  - 安全域
    - 管理服务区域
    - [对内/对外]基础服务区域
    - [对内/对外]计费服务区域
    - NODE服务区域
    - Container服务区域
  - 精确到应用级别的授权




Service-A
Service-B
Floodlight集群
依据需求下发策略
OVS
Container
APP-1
Container
APP-2
Container
APP-3

PaaS安全架构

- Node(宿主)安全
  - 宿主Agent安全
  - 强制访问控制
  - 内核防溢出



PaaS安全架构

- Container(实例)安全
  - Cgroup控制
  - 取消特权Capabilities
    (Docker Container Breakout Proof-of-Concept Exploit)
  - 精简rootfs
  - 保护sys/proc
  - 最小权限运行服务进程

沙盒(sandbox)安全

– 资源隔离
  - **文件系统**

    文件系统隔离/磁盘容量
  - **内存**

    内存隔离/内存容量
  - **进程**

    进程隔离/进程创建
  - **网络**

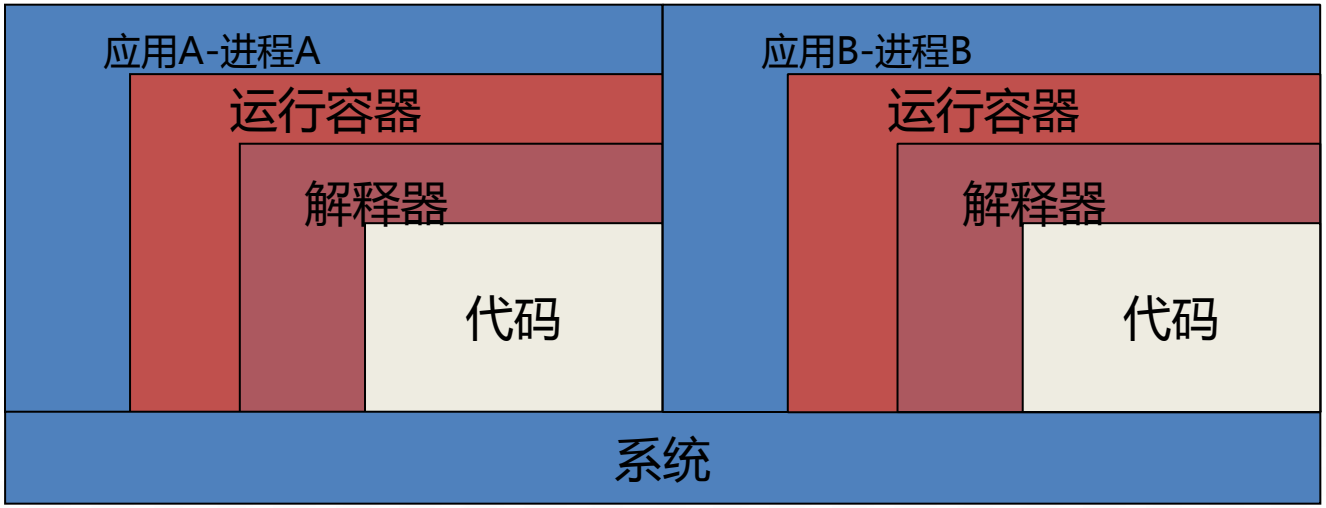
    访问控制/频率控制
  - **CPU**

    CPU时间

沙盒(sandbox)安全

– 基于解释器/运行容器(VM)/POSIX定制的沙盒
  - 对用户代码通过函数(黑名单/特性)/特权级别/访问策略进行限制
  - 多应用共享进程
  - 每个应用使用一个进程

  java: Security Manger+Policy/Javaagent+Instrument（类白名单、函数黑名单）



沙盒(sandbox)安全

- 基于解释器/运行容器(VM)/POSIX定制的沙盒
  - 威胁
    - 特权函数未在黑名单
    - 解释器漏洞
      CVE-2012-1171
      CVE-2013-1493 / CVE-2013-2465
    - 实现错误

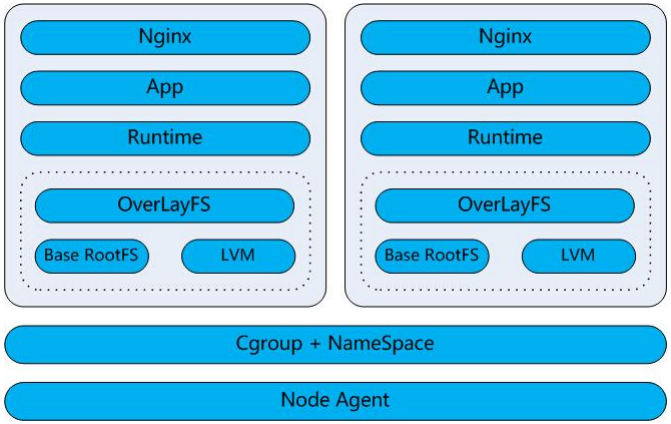
架构优缺点

优点：
轻量级/效率高/稳定性好

缺点：
兼容性差/实现复杂/隔离性差

沙盒(sandbox)安全

– 容器及虚拟机实现的沙盒
  - 每个应用使用一个虚机
    - Cgroup+NameSpace+SDN
  - 威胁
    – 提权
    – 逃逸



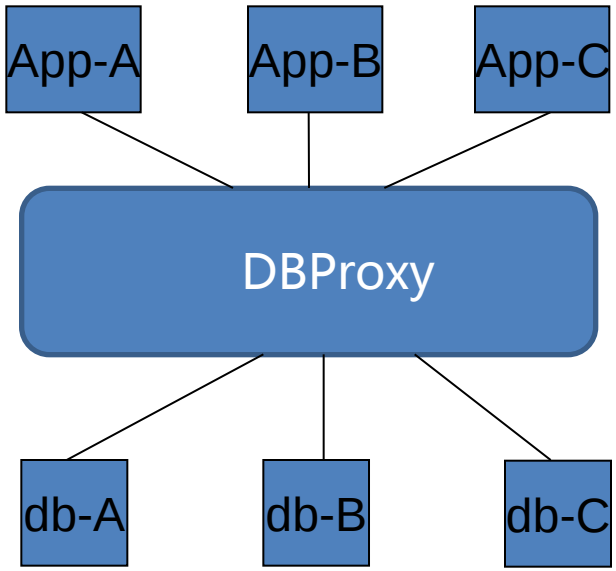
架构优缺点

优点：
兼容性好/隔离性强/通用实现

缺点：
开销高/稳定性/维护成本

数据安全

– *MySQL*



- 读写分离
- 负载均衡
- 故障转移
- 请求控制
- 资源控制
- 权限控制
- 备份机制
- SQL安全监控

XXX:9084->XXXX:3306 | readonly :XXX | 2014-06-25 13:49:35
sql: select * from XXX_account where dirname='XXX'; WAITFOR DELAY '0:0:5';--' | COMMENT:Multiple queries found

用户安全

- 登录保护
- 关键操作
  - 二次密码
  - 手机验证码
- 消费安全
  - 消费限制
  - 访问建模

安全服务

- 合作共赢-支持第三方服务接入
- DDOS
- WAF
  - 灵活自定义
- 安全监控
  - WEB监控
  - 数据库监控
- 应用安全
  - 漏洞扫描

发现恶意用户

- 黄赌毒
- 攻击入侵
  - 扫描
  - 代理
- 控制端
  - 钓鱼网站
  - XSS平台
  - 僵尸网络

发现恶意用户

- 基于内容
- 基于行为


cloudscape.sohu.com
欢迎使用搜狐云景 | 技术支持
返回首页 | 登录 | 注册
搜狐云景 Sohu Cloudscape
首页
特性
服务
文档
用户中心
现在去申请邀请码
激活账户
搜狐云景邀请码申请活动给力进行中...
注册激活邀请码
电子代金券
进行实名认
100元
大约可以支
个月
开放
作为开放的PaaS平台，我们在思考我们能为开发者带来什么，是否愿意奉献自己的成果和秘密，是
Open

Thanks!