

Inside TAE



GAE



SAE

TAE



BAE



TAE

- 定位：淘宝的受控第三方开放基础设施
- 最初需求来自店铺装修市场
 - 个性化展示和交互
 - 更复杂的后台业务逻辑
- 现在已经是一个完备的AE系统
 - PHP
 - JAVA

淘宝U站（优站）

uz.taobao.com



特色

特别的爱，只给特别的你



手工集市



足彩U站



浙江金名片



笑里藏宝



节日购



永远的经典



万佳绣



玻璃控

glass.uz.taobao.com

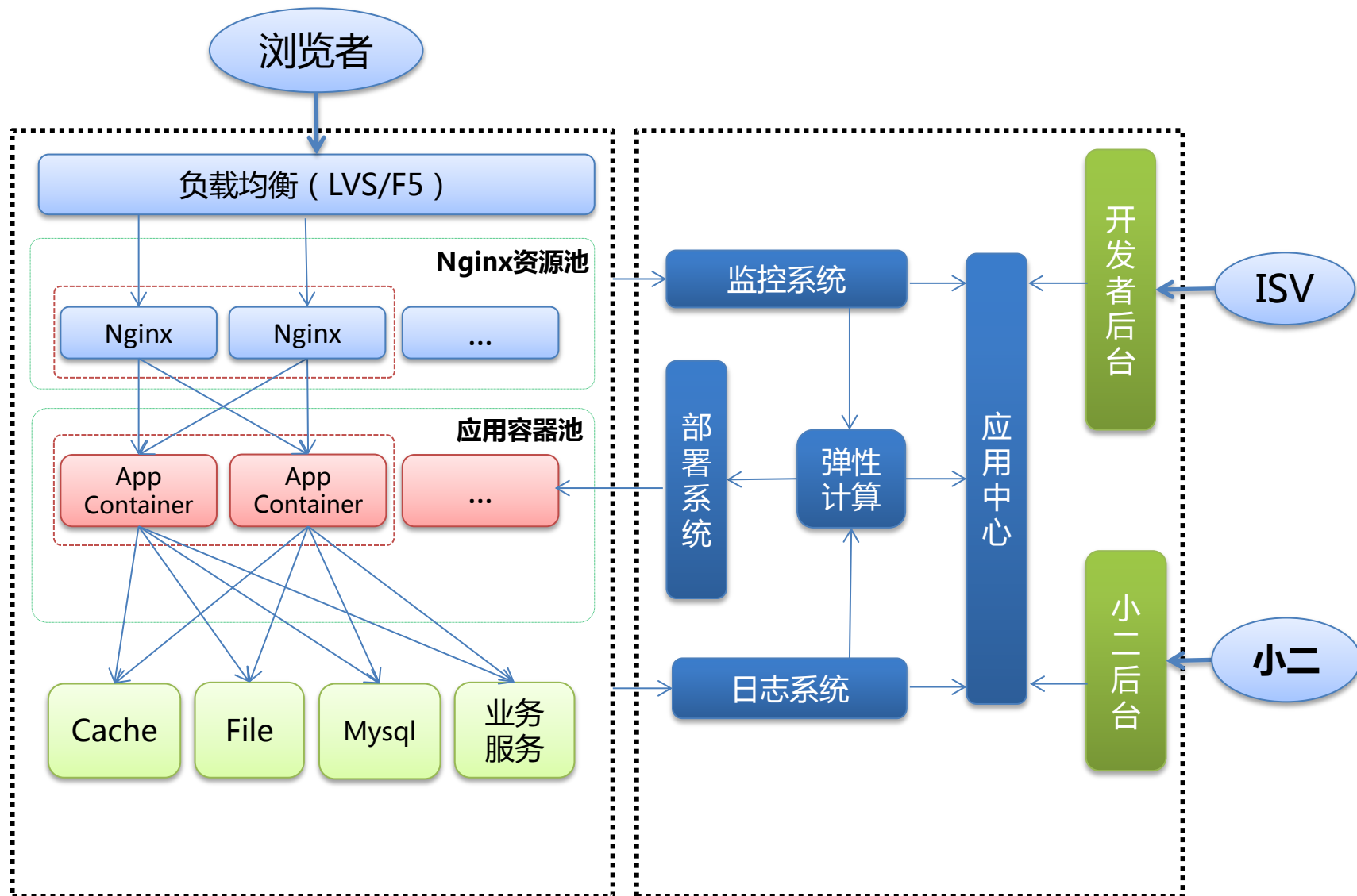


uz.taobao.com

- 800+ TAE App
- 2000+ App版本
- 日均UV 130W+, PV 1200+
- 平均单用户浏览页面**9.08**个
- 平均访问时长**7分38秒**

PHP 容器篇

系统概览




```
<?php
$a = $appEngine->find("xService");
echo "<br>".$a->someMethod();
?>
```

开发者后台

部署

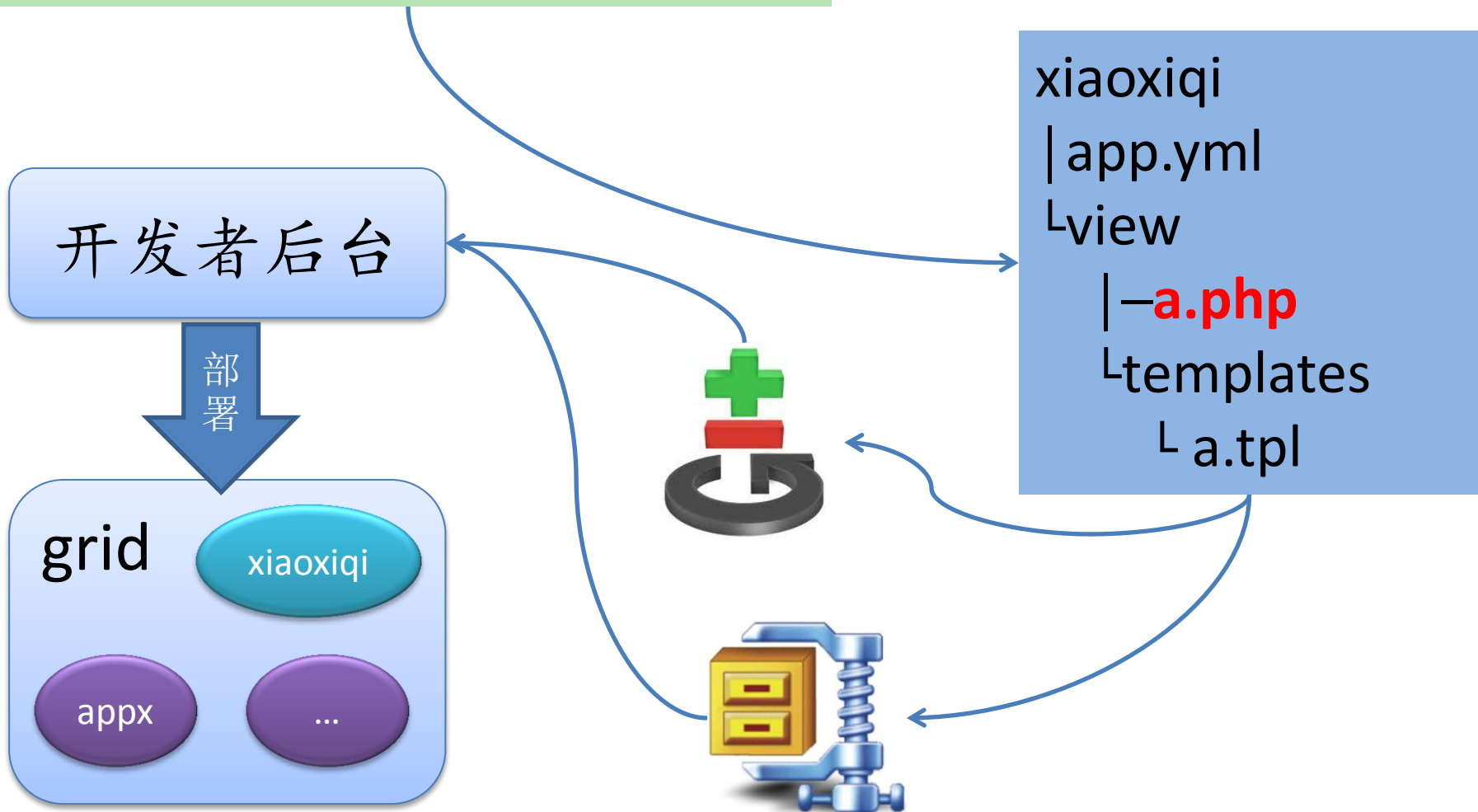
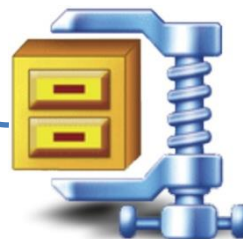
grid

xiaoxiqi

appx

...

```
xiaoxiqi
| app.yml
└ view
  | -a.php
  └ templates
    └ a.tpl
```





xiaoxiqi.uz.taobao.com/a.php

负载均衡设备

Nginx

Nginx

xiaoxiqi
| app.yml
└ view
 | -a.php
 └ templates
 └ a.tpl

grid

xiaoxiqi

appx

...

```
<?php
$a = $appEngine->find("xService");
echo "<br>".$a->someMethod();
?>
```



xiaoxiqi.uz.taobao.com/a.php

负载均衡设备

Nginx

grid

xiaoxiqi

appx

...

```
$a = $appEngine->find("xService");  
echo "<br>".$a->someMethod();
```

PhpProgram

└ BlockStatement

├ ExpressionStatement

├ ...

└ EchoStatement

└ MethodInvokeStatement

xService

app2.taogrid.taobao.com

LB/LVS

LB/LVS

LB/LVS

店铺装修

Tae Nginx

Tae Nginx

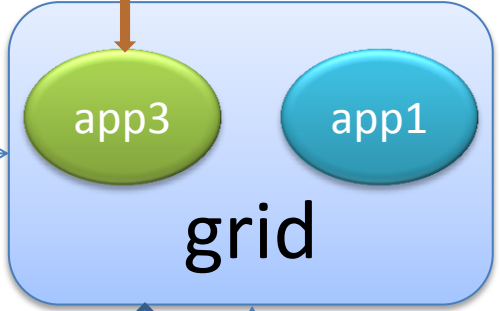
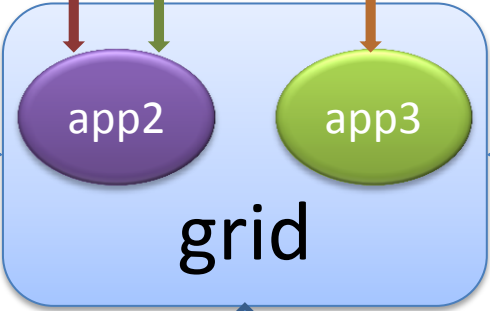
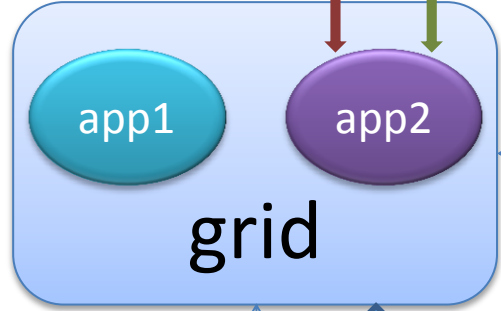
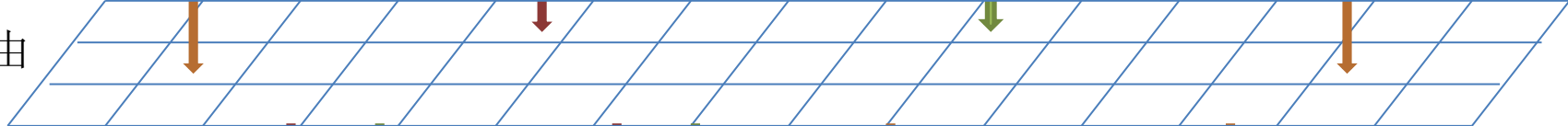
店铺浏览

RPC

HTTP

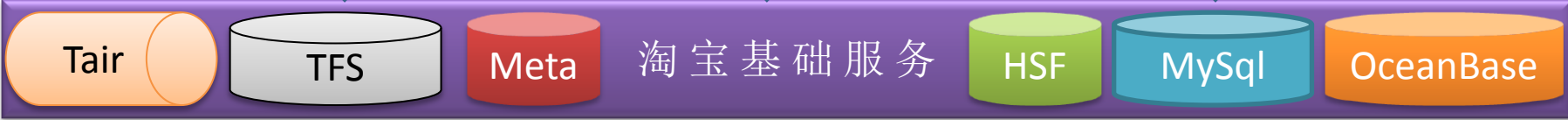
RPC

路由

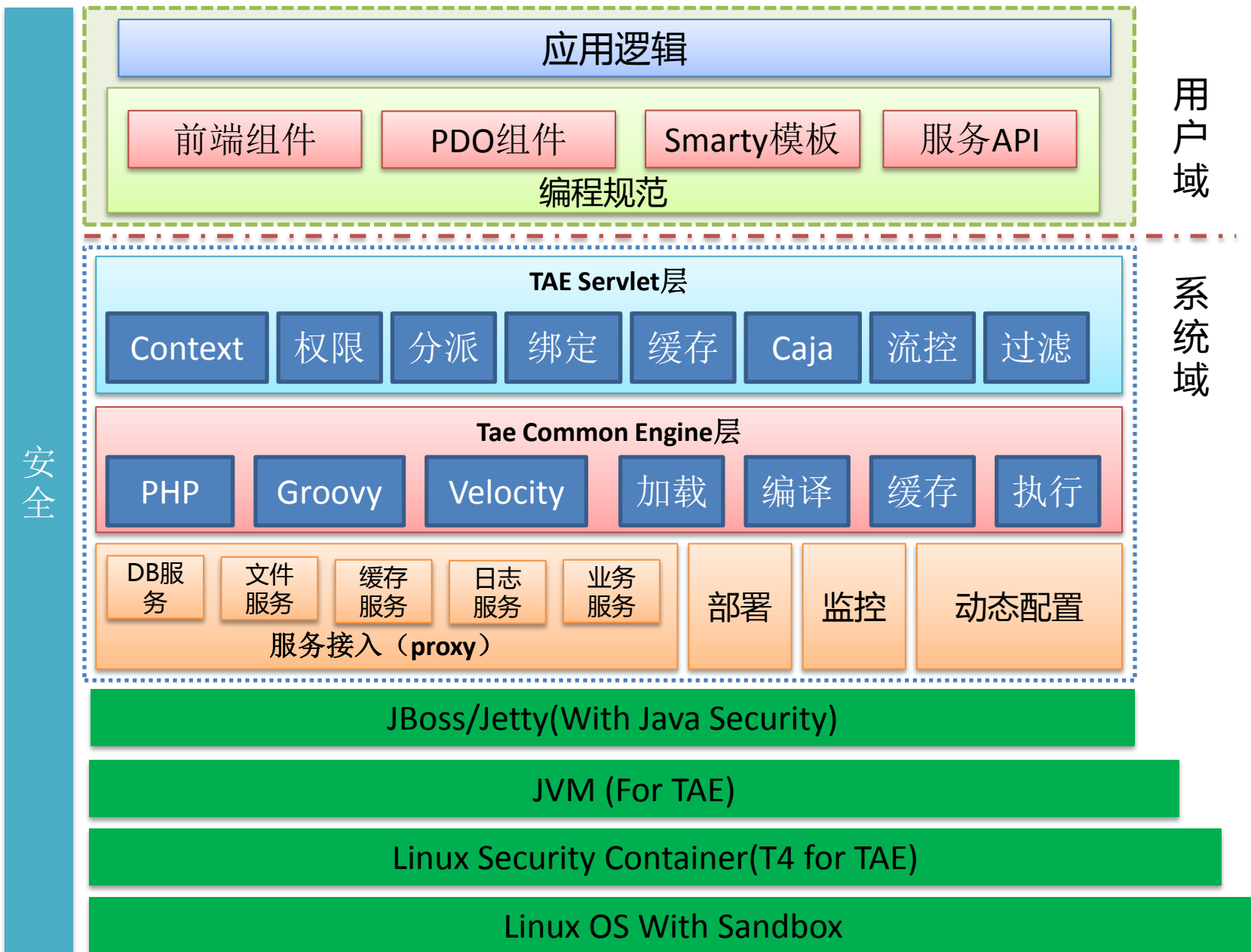


HSF

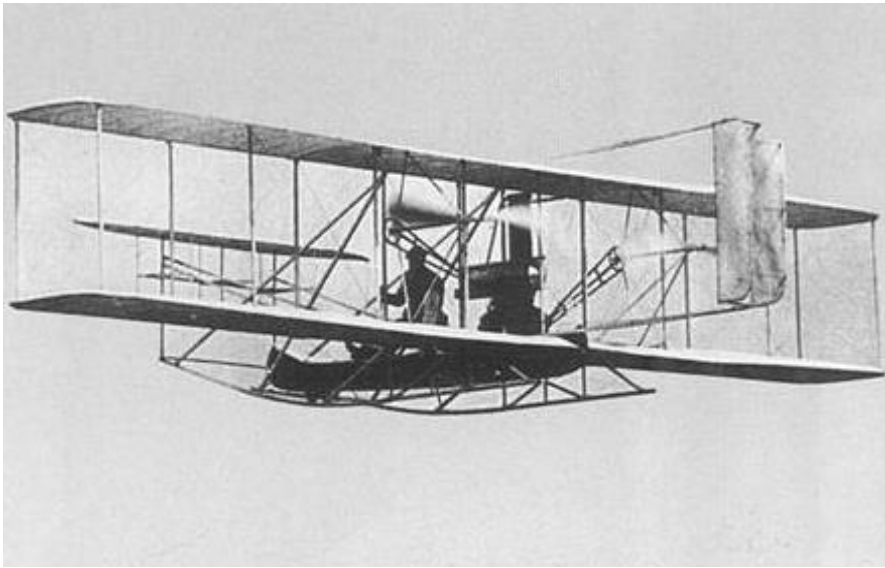
HSF



PHP容器结构



对Quercus的改进



没有大规模商用的实验室产品

能够工业化，大规模使用的产品

U站 -- 9个月 -- 800+ ISV，应用版本



PHP安全

- 没有PHP原生环境
 - 第三方代码：PHP；容器代码：java
 - 弱类型语言操作强类型语言
 - 代码执行引擎和代码本身处于不同的层级
- 前端安全
 - Caja沙箱 + HTML/CSS 白名单过滤
 - 上线前黑白盒扫描，上线后定时黑盒扫描
- 资源安全
 - 死循环；耗时操作
 - 大内存

JS安全解决方案

```
<div> ... </div>  
<script src=/a/b.js/>
```

```
return (x + y);
```

```
____.loadModule({  
  'instantiate': function (____, IMPORTS____) {  
    var dis____ = IMPORTS____;  
    var moduleResult____;  
    moduleResult____ = ____ .NO_RESULT;  
    IMPORTS____.w____ ('x', 2);  
    IMPORTS____.w____ ('y', 3);  
    return (IMPORTS____.x_v____ ? IMPORTS____.x: ____ .ri (IMPORTS____, 'x')) +  
      (IMPORTS____.y_v____ ? IMPORTS____.y: ____ .ri (IMPORTS____, 'y'));  
    return moduleResult____;  
  },  
  'cajolerName': 'com.google.caja',  
  'cajolerVersion': '4905',  
  'cajoledDate': 1340761300140  
});
```




PHP 白名单

Quercus Engine

JBOSS/Jetty

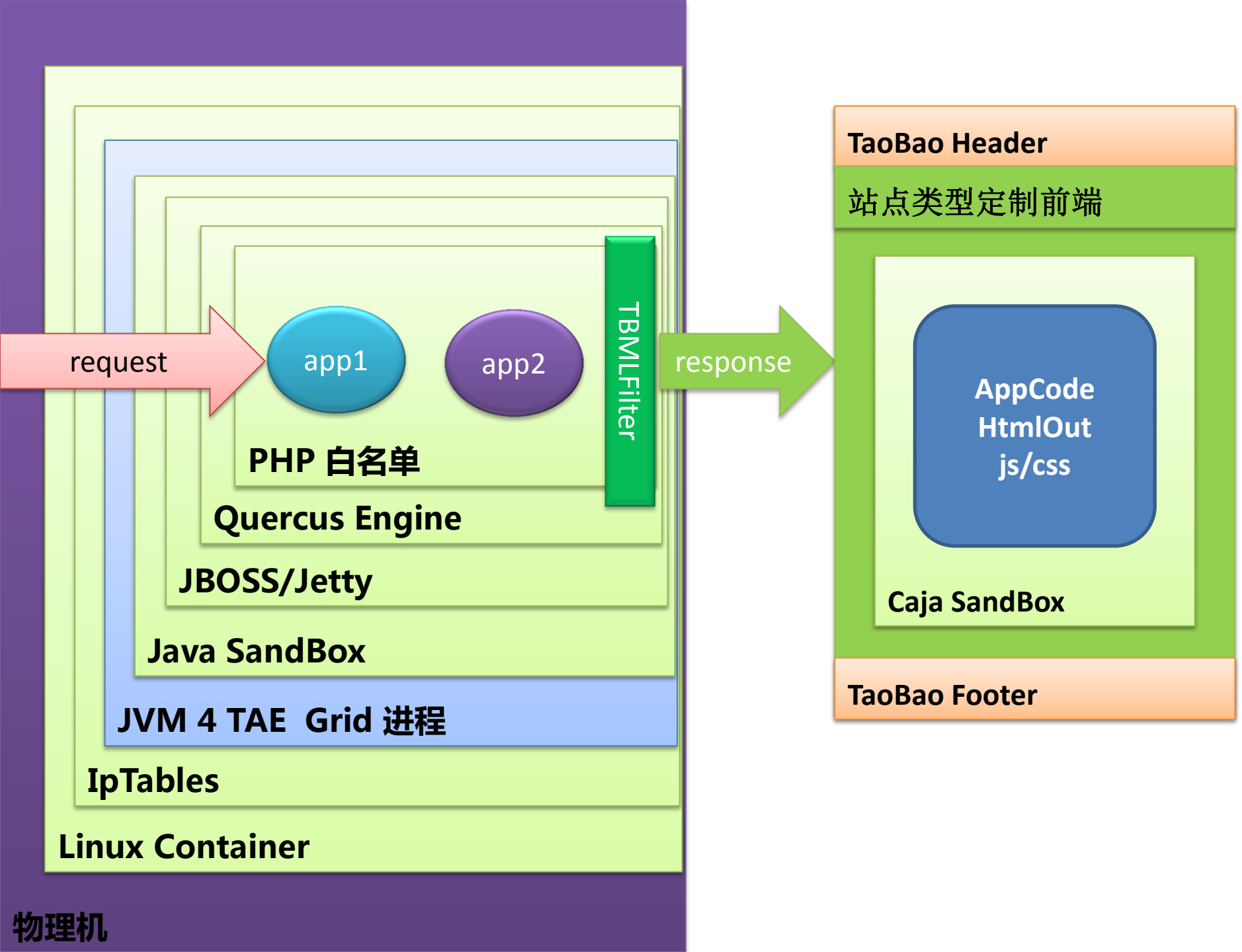
Java SandBox

JVM 4 TAE Grid 进程

IpTables

Linux Container

物理机




JAVA 容器篇

需要解决什么问题？

- 安全问题！
 - ISV代码、数据安全
 - *淘宝买家数据安全
 - *淘宝数据安全
- 提供**JAVA**运行容器

难点 - 安全

- 应用层安全问题
 - Cookie & session 泄漏用户信息
 - Html、js、css、pic 等问题
 - 调用未授权的服务
 - Sql 注入
 - XSS CSRF
- 系统层安全问题
 - 资源竞争（死循环、线程数耗尽）
 - 攻破Java沙箱
 - 系统0day

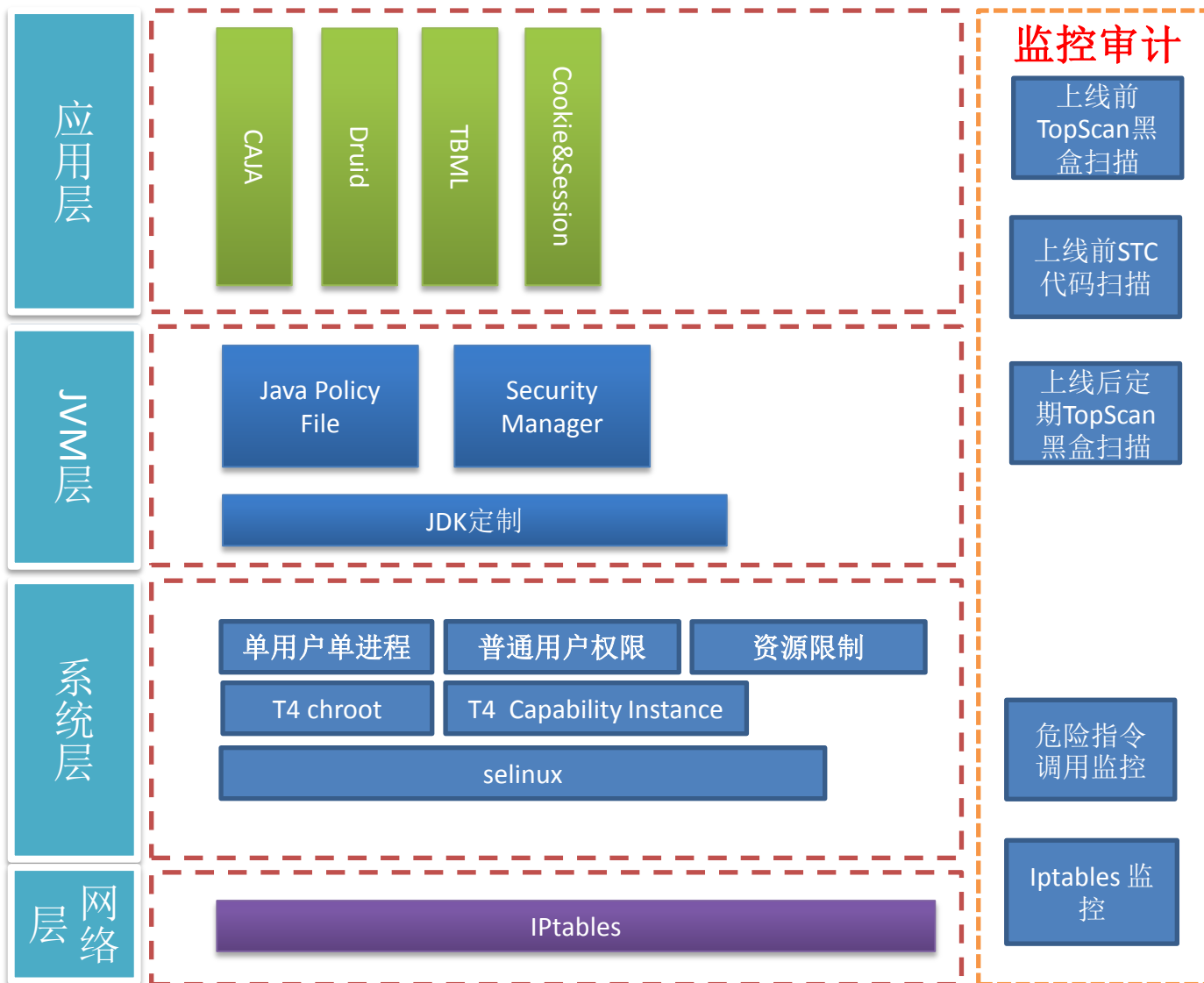


后果
很严重

难点 - 安全

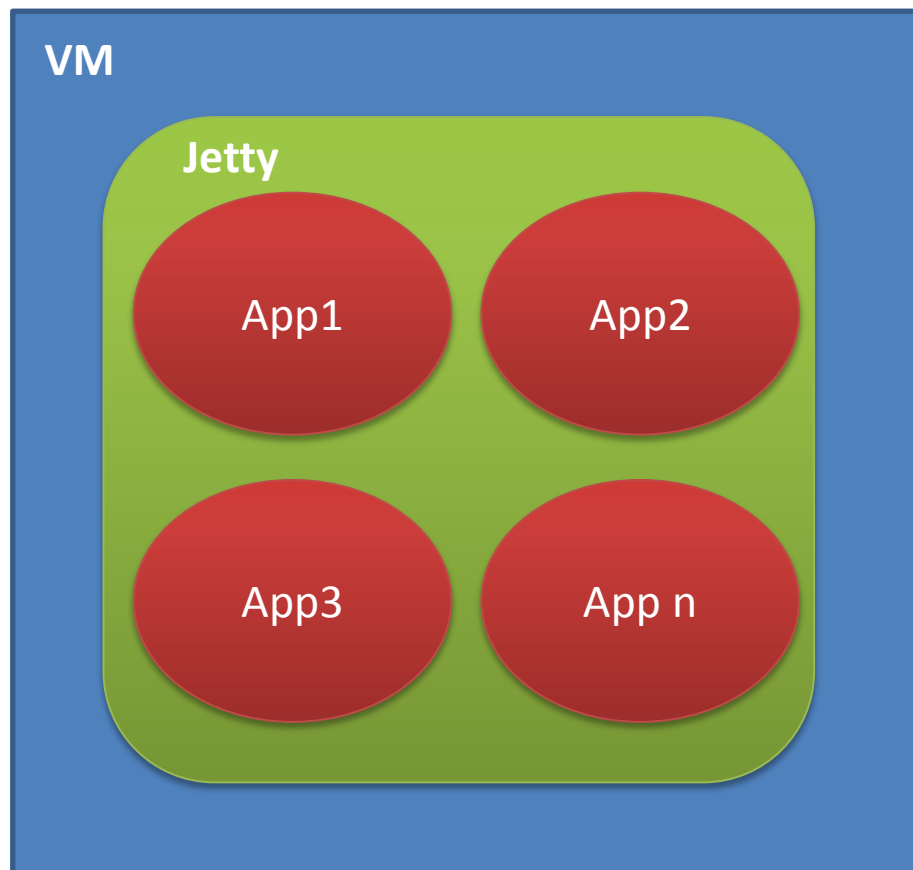
- 设计时基本考虑
 - 需要的是安全体系，每一层有具体的职责
 - “Java沙箱被by pass”是网络、系统层防御措施的基本假设
- 安全体系层级
 - 应用层
 - JVM层
 - 系统层
 - 网络层
 - 运行时监控

JAVA应用安全体系



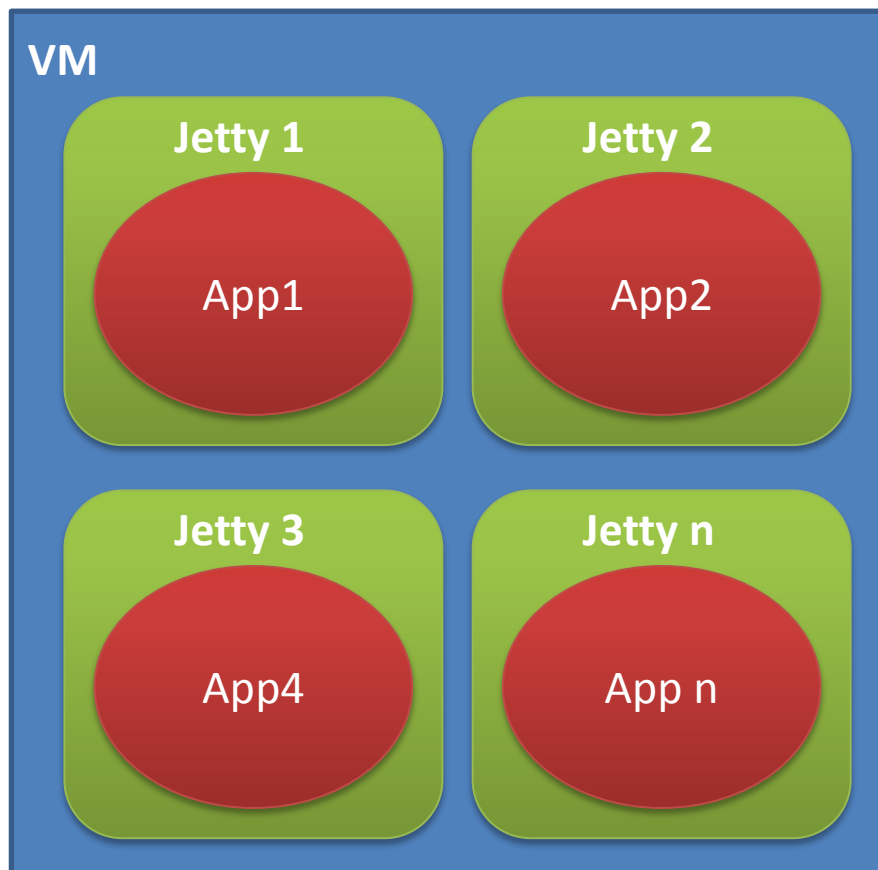
单进程多应用方案

- 单进程 \leftrightarrow 多 app
- 问题
 - 权限无法隔离
 - 资源也无法隔离



单用户单进程方案

- 单进程 \leftrightarrow 单App
- 优点
 - 资源隔离有好转
 - 可以初步做到文件访问权限隔离



- 单用户单进程

- 文件权限的设置
- 用户最小权限

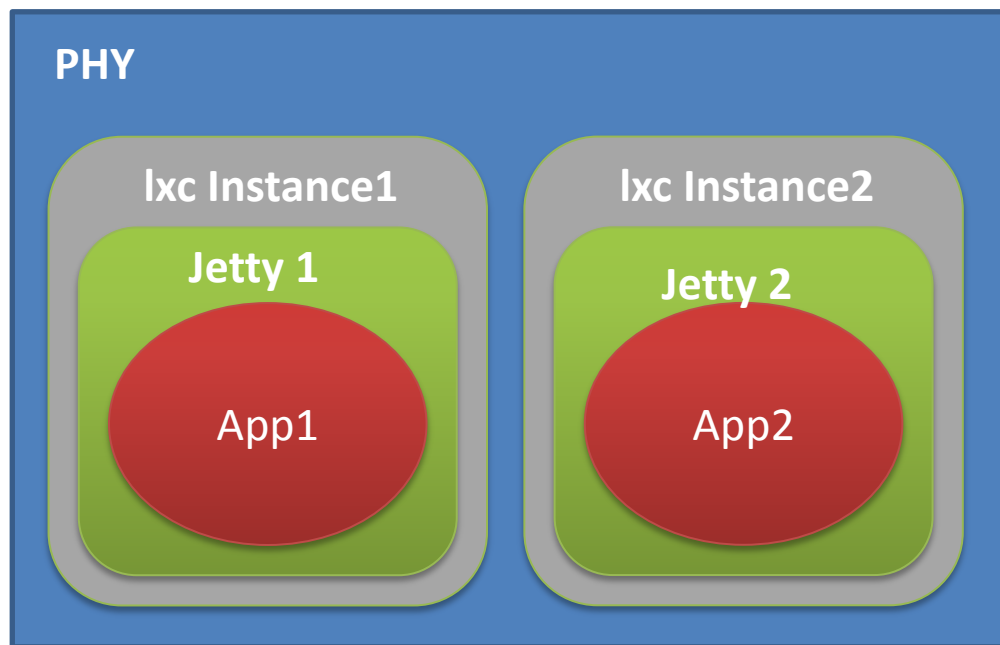
```
setfacl -m g:tae_apps:x /  
setfacl -m g:tae_apps:x /  
setfacl -d -m g:tae_apps:- /etc  
setfacl --set u::rw,g::r,o::r,g:tae_apps:- /etc/group  
setfacl --set u::rw,g::r,o::r,g:tae_apps:- /etc/passwd  
setfacl --set u::rw,g::r,o::r,g:tae_apps:- /etc/shadow  
  
setfacl -b -R /root  
setfacl -m g:tae_apps:- /root  
  
setfacl -m g:tae_apps:x /home  
setfacl -d -m g:tae_apps:- /home  
setfacl -m g:tae_apps:- /home/admin  
setfacl -m g:tae_apps:- /home/hubble  
setfacl -m g:tae_apps:- /home/tops
```

- 问题

- 用户管理需要root权限，root权限如果被拿到，其他app就危险了
- 文件权限的管理复杂
- 如果root权限需要开通，没有办法将instance的capability全部去除，那安全级别就会降低
- 资源隔离还不够彻底

单VM单用户单进程方案

- 单 Instance 单进程
 - 每个instance有且只有一个java进程
 - lxc Instance去除所有的capability
 - Instance的root帐号降级为普通帐号
- 优点
 - 安全模型更简单粗暴
 - 架构更简单，管理更方便：
不需要在instance内在搞多用户



单VM单用户单进程方案

- 问题
 - 资源问题 - 会生成大量的lxc incetance
 - 需要休眠方案
 - IP不够用
 - 需要lxc incetance无IP方案

资源问题应对方案

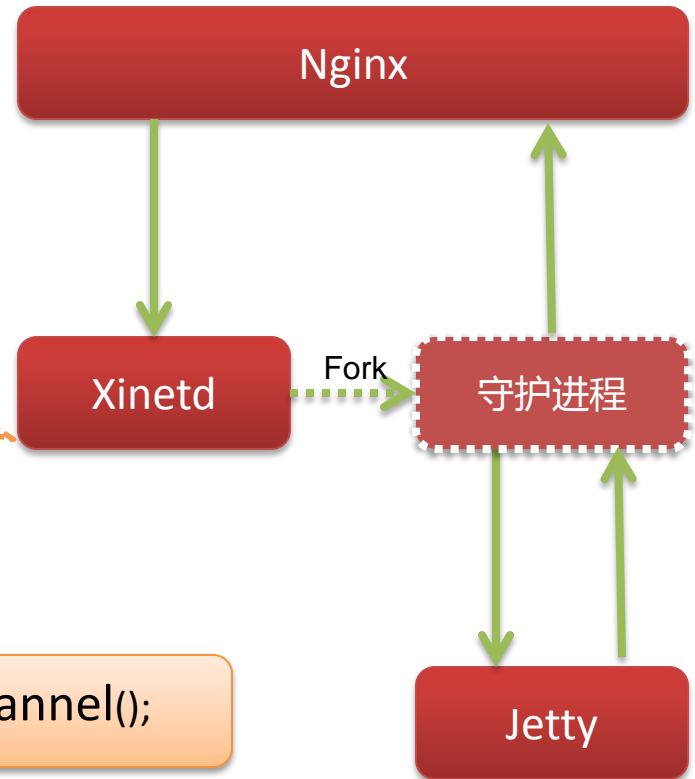
— 按需启动

将长时间不访问的应用进程关掉
当有访问时，启动进程，提供服务

— 两种方式

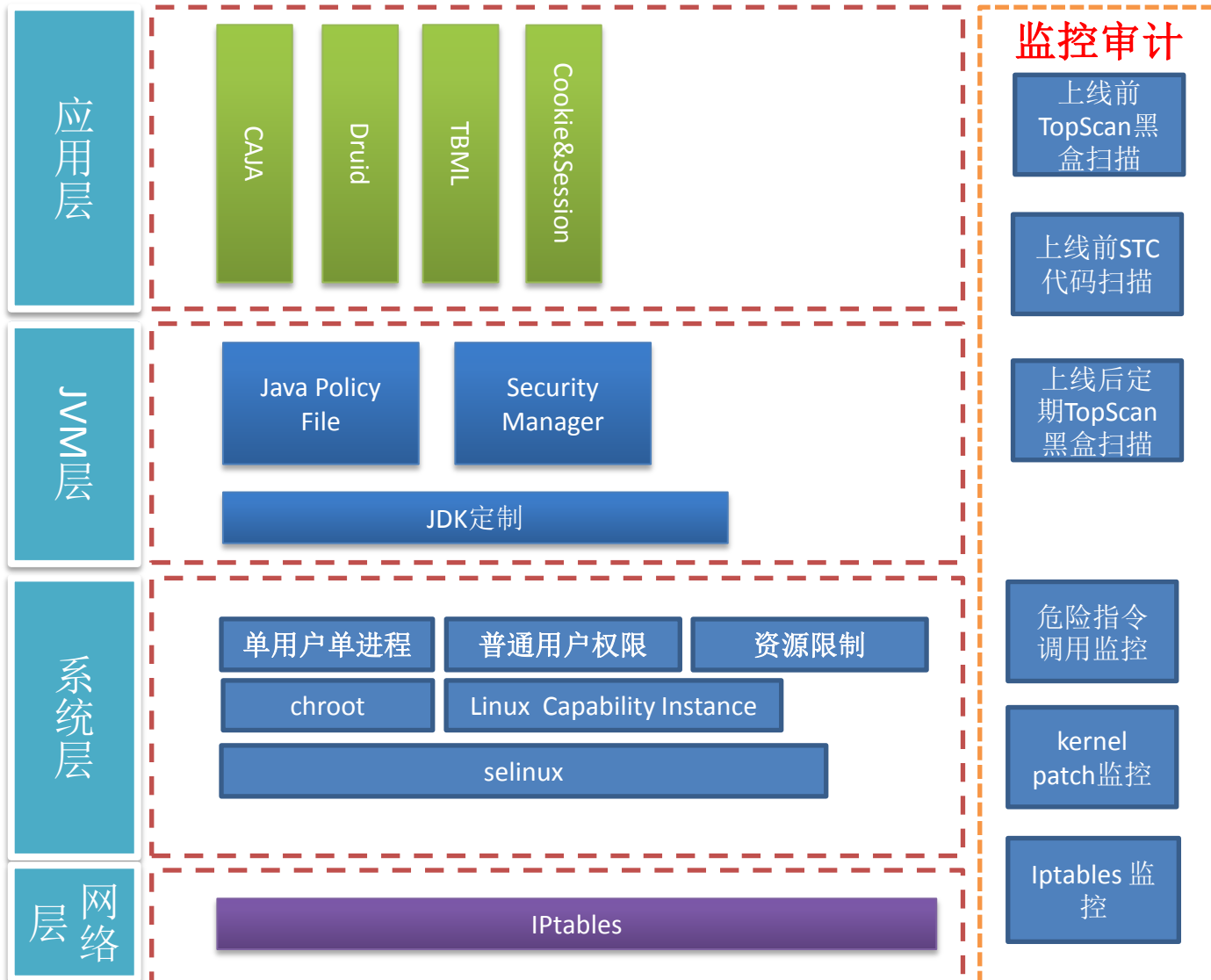
- 端口转发
- 通道 

在所有定义的服务端口监听连接

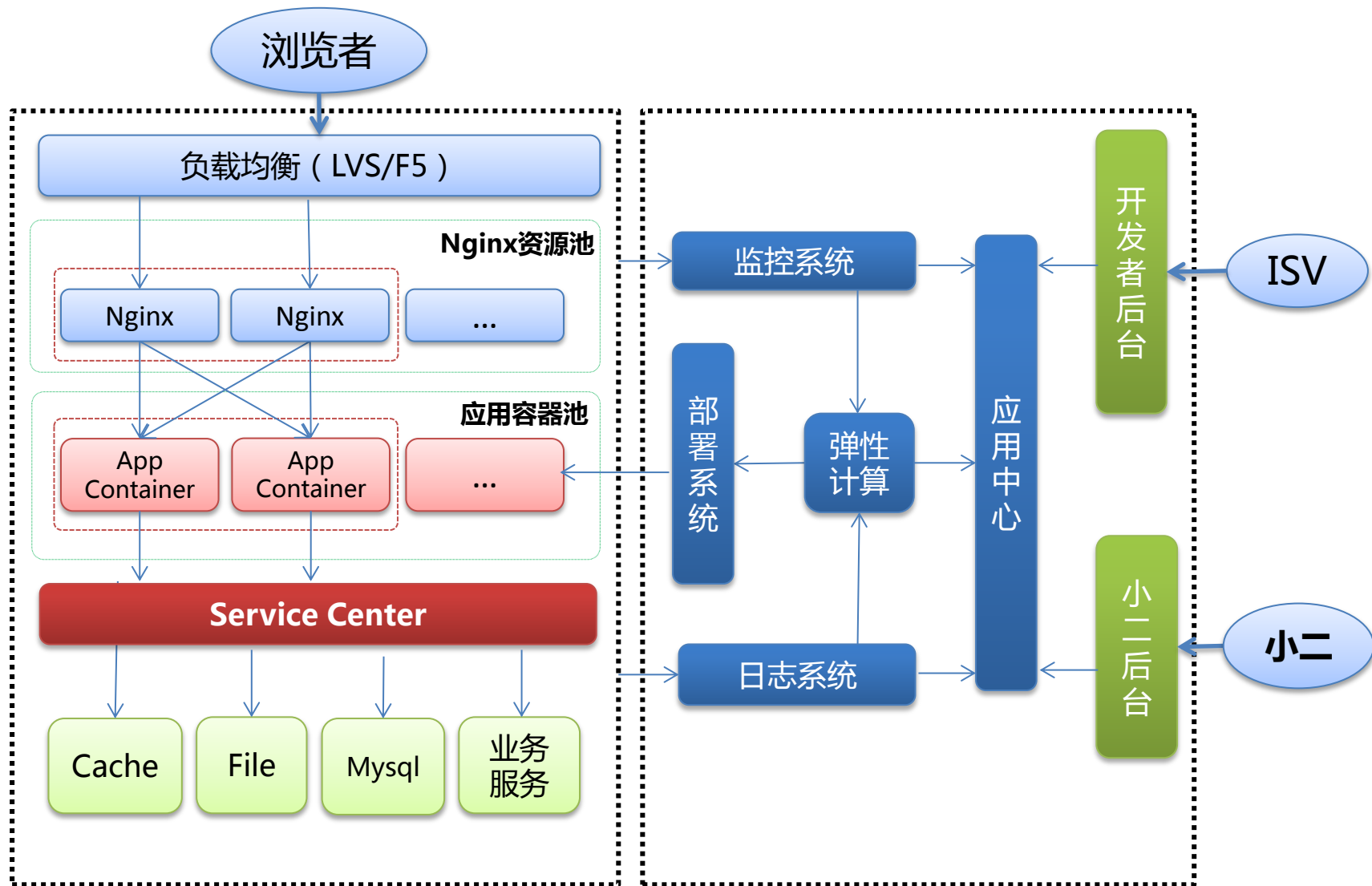


```
Channel channel = System.inheritedChannel();
```

安全体系回顾



Service Center引入



Service Center

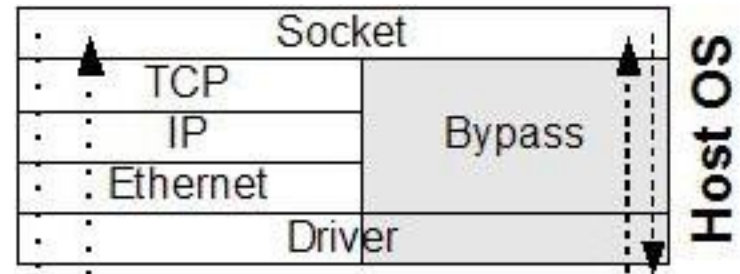
- Service Center带来的好处
 - 所有的服务调用都通过服务中心
 - 网络层设置白名单，只允许访问服务中心
- 潜在性能问题

Service Center性能

- 本地进程通讯 - Tcp Friends

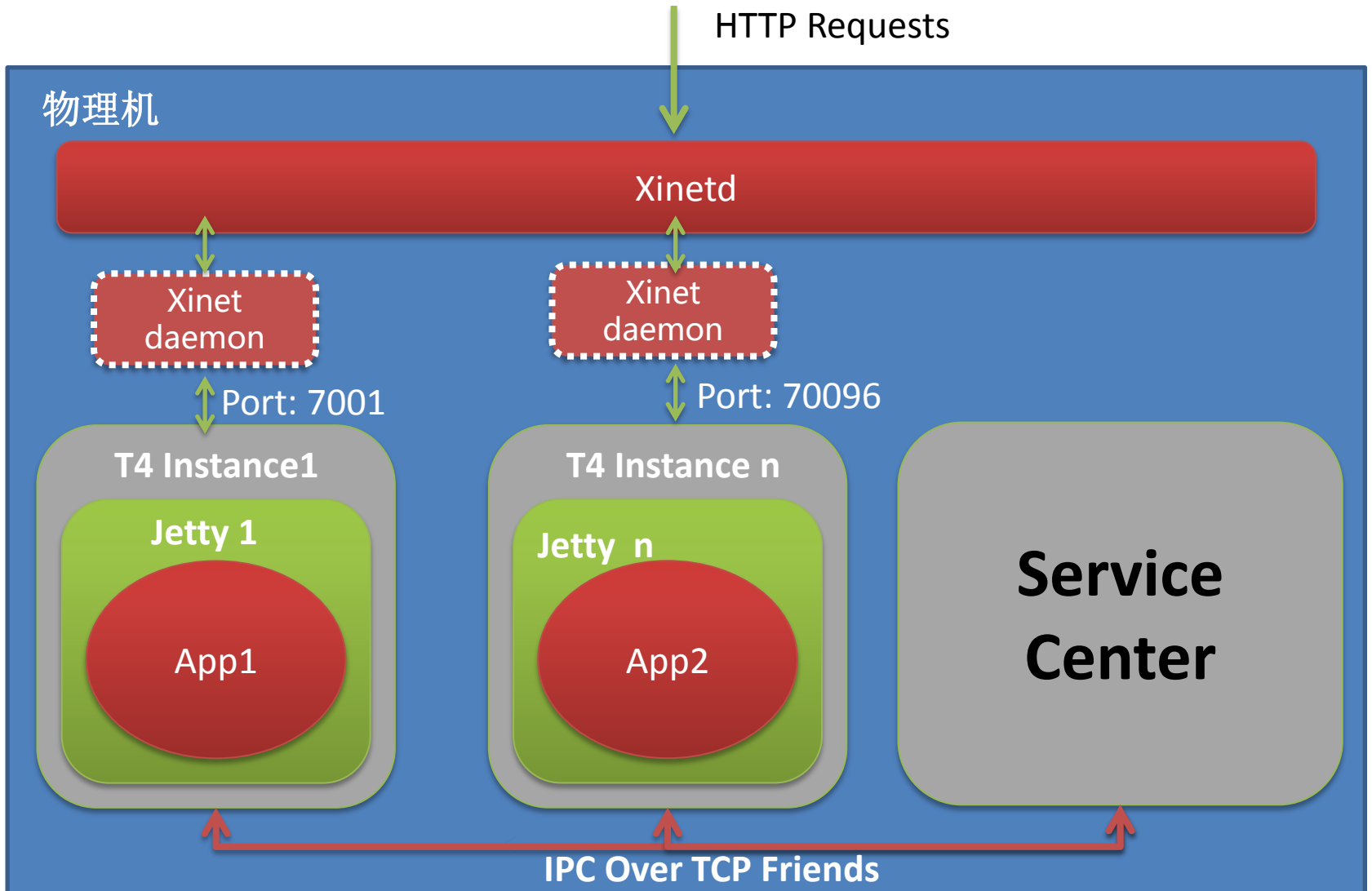
- when both endpoints of a TCP connection are on the same machine, the two sockets are marked as being "friends" in the kernel.

Data written to such a socket will be immediately queued for reading on the friend socket, bypassing the network stack entirely



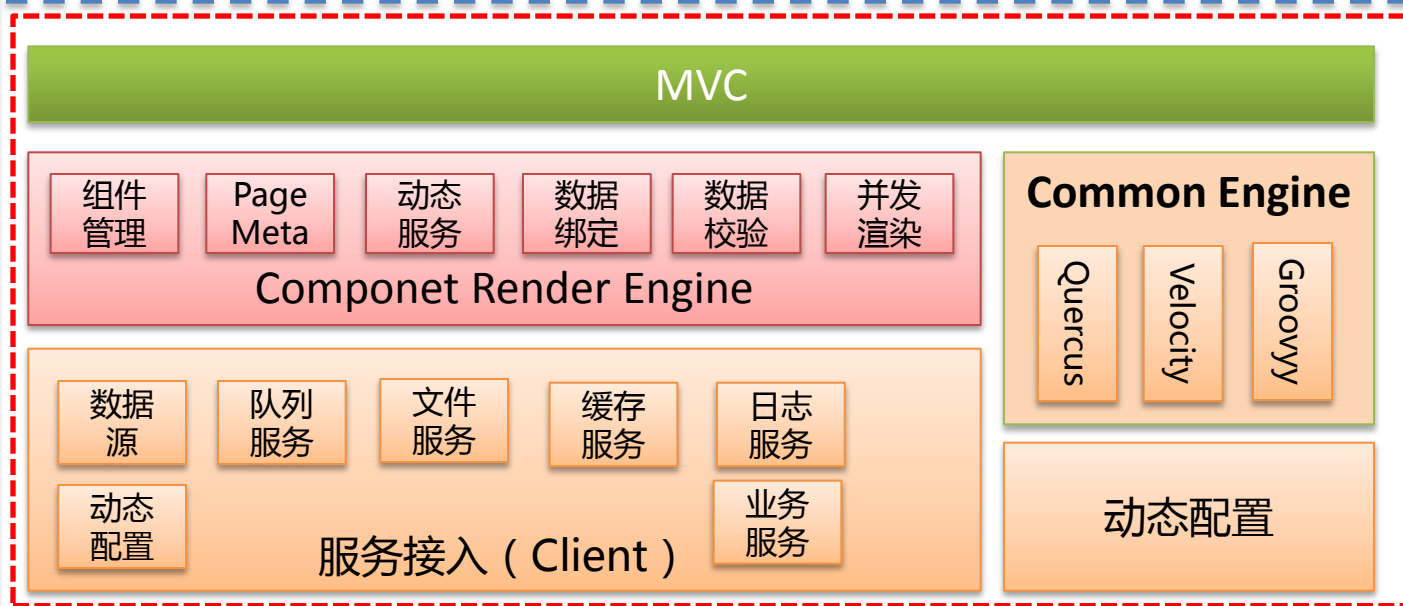
- Google 采用了类似的技术
- 每台物理机上部署一个service center，加速物理机上的instance与服务center的通讯
- 解决总线的问题，但不限于于总线

Put it together

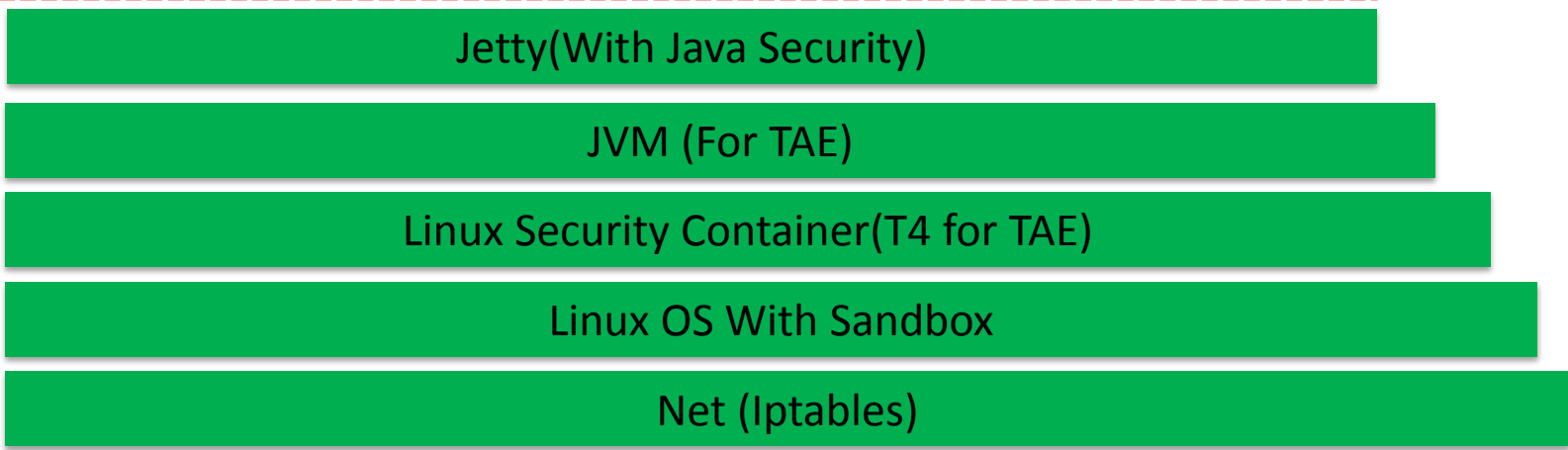




用户域



系统域



淘宝开放的三种形态



Q & A

欢迎加入TAE团队

- 这里是第三方代码的执行引擎，运行容器
- 这里涉及从前端到内核的各种技术
- 这里在支持着数千个开发团队和创业公司
- 这里客户是你的上帝，客户代码的上帝是你
- 加入我们，请联系：

– 邮箱：

linxuan@taobao.com

haomin.liuhm@taobao.com

– 微博：

淘宝林轩

ludvik_淘宝伯昊

– 微信：

床前明月光

ludvik



淘宝网
Taobao.com

THANK YOU

