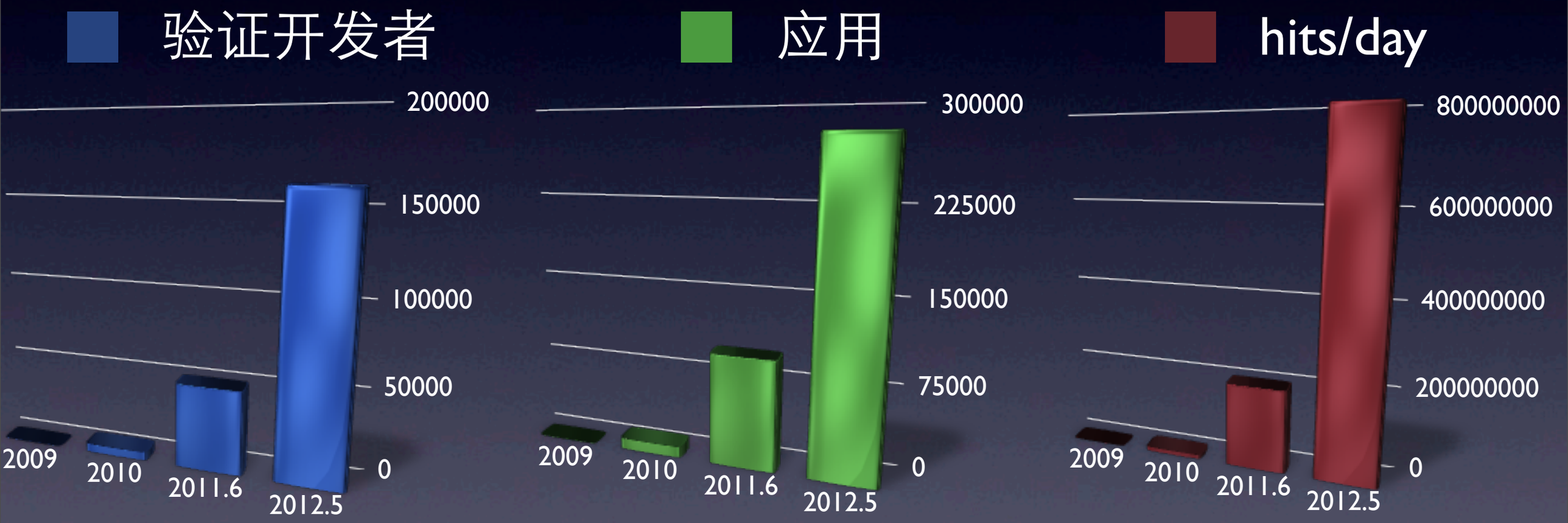
SAE安全实践

Sina App Engine team
2013.10
weibo @SinaAppEngine

SAE现状



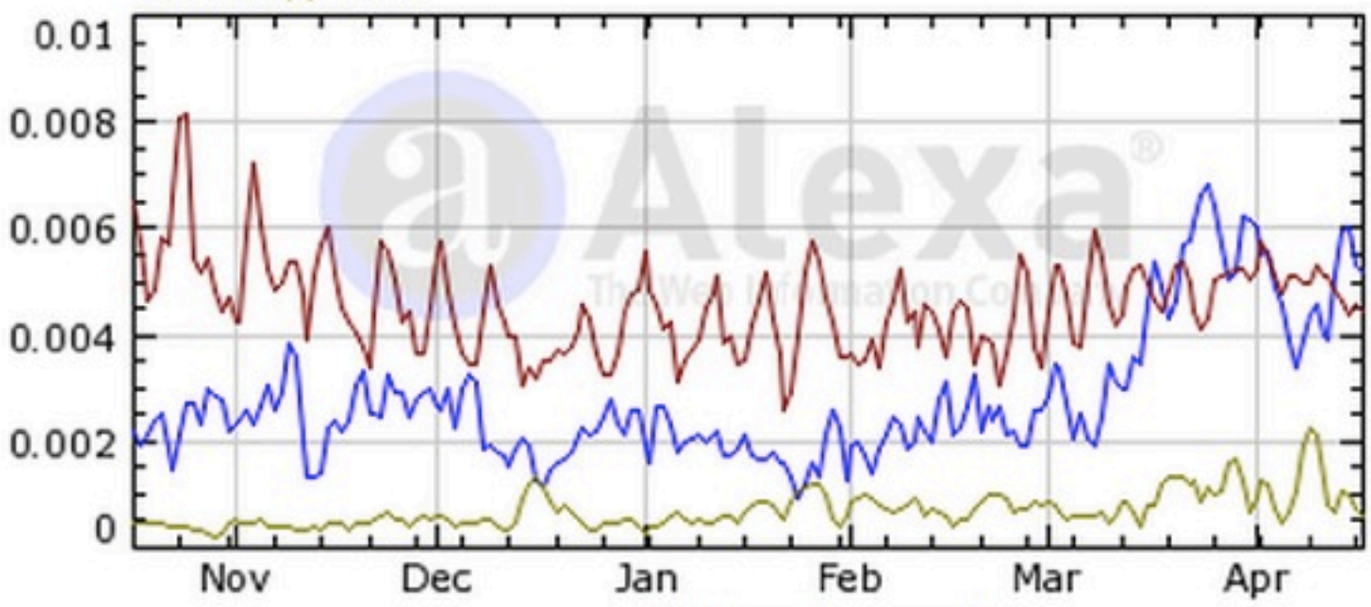
2011 SLA: 99.95%

SAE现状

Traffic Rank | Reach | **Pageviews** | Pageviews/User | Bounce % | Time on Site | Search %

Daily Pageviews (percent)

sinaapp.com appspot.com herokuapp.com



Trailing 6 months

Estimated percentage of global pageviews on sinaapp.com:

	Pageviews	Change
Yesterday	0.0053	+0.1%
7 day	0.00501	+15%
1 month	0.0052	+86%
3 month	0.00333	+49.7%

Compare **sinaapp.com** to:

appspot.com | herokuapp.com | | | Compare

SAE内置服务

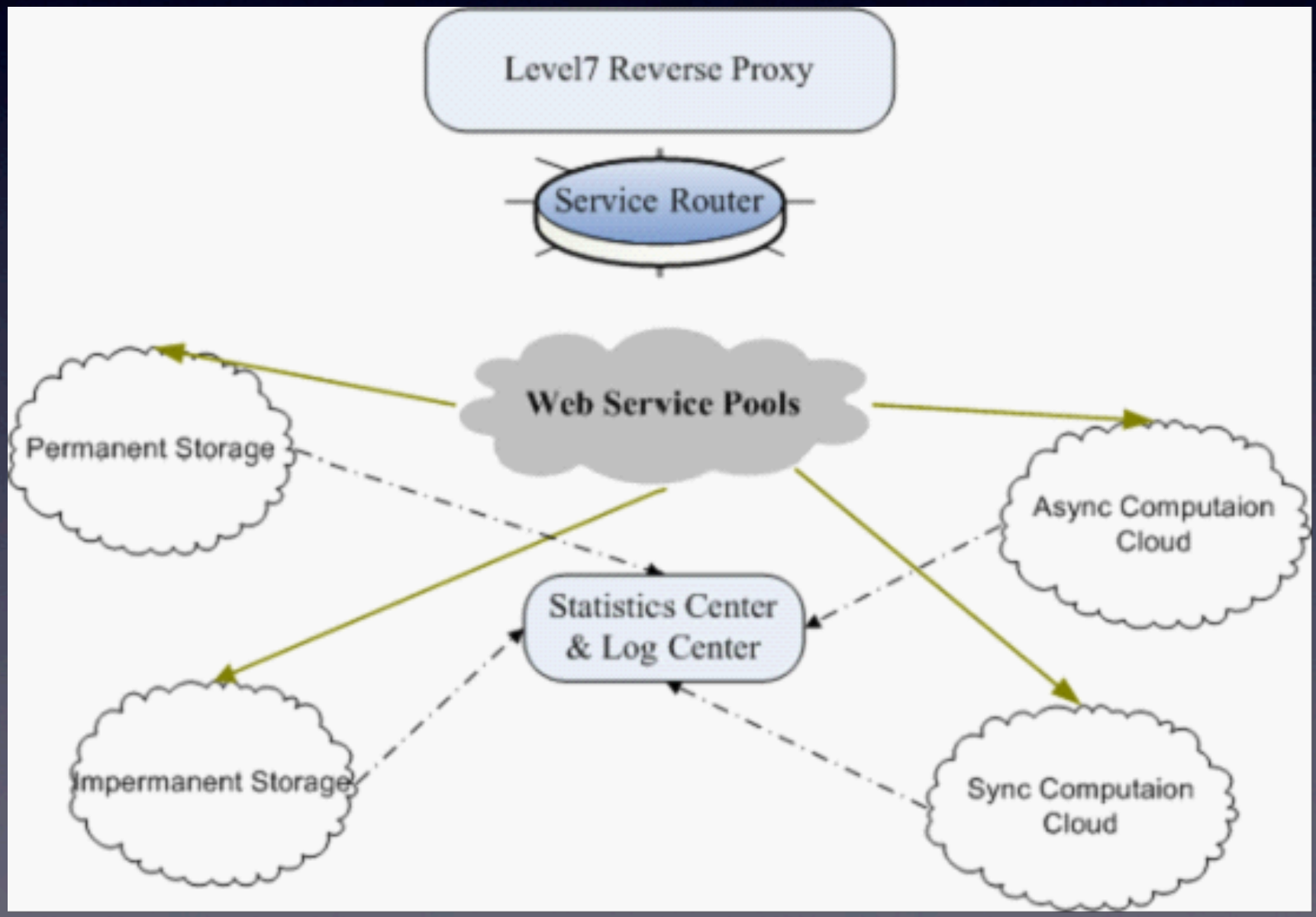
MySQL/RDC	MemcacheX	KVDB	TmpFS	Storage
Counter	Rank	CDN	Mail	Cron
TaskQueue	DeferredJob	Image	FetchURL	SocketProxy
AppConfig	Full-text Index	SMS	Word Segment	LBS

公有云计算安全的特点

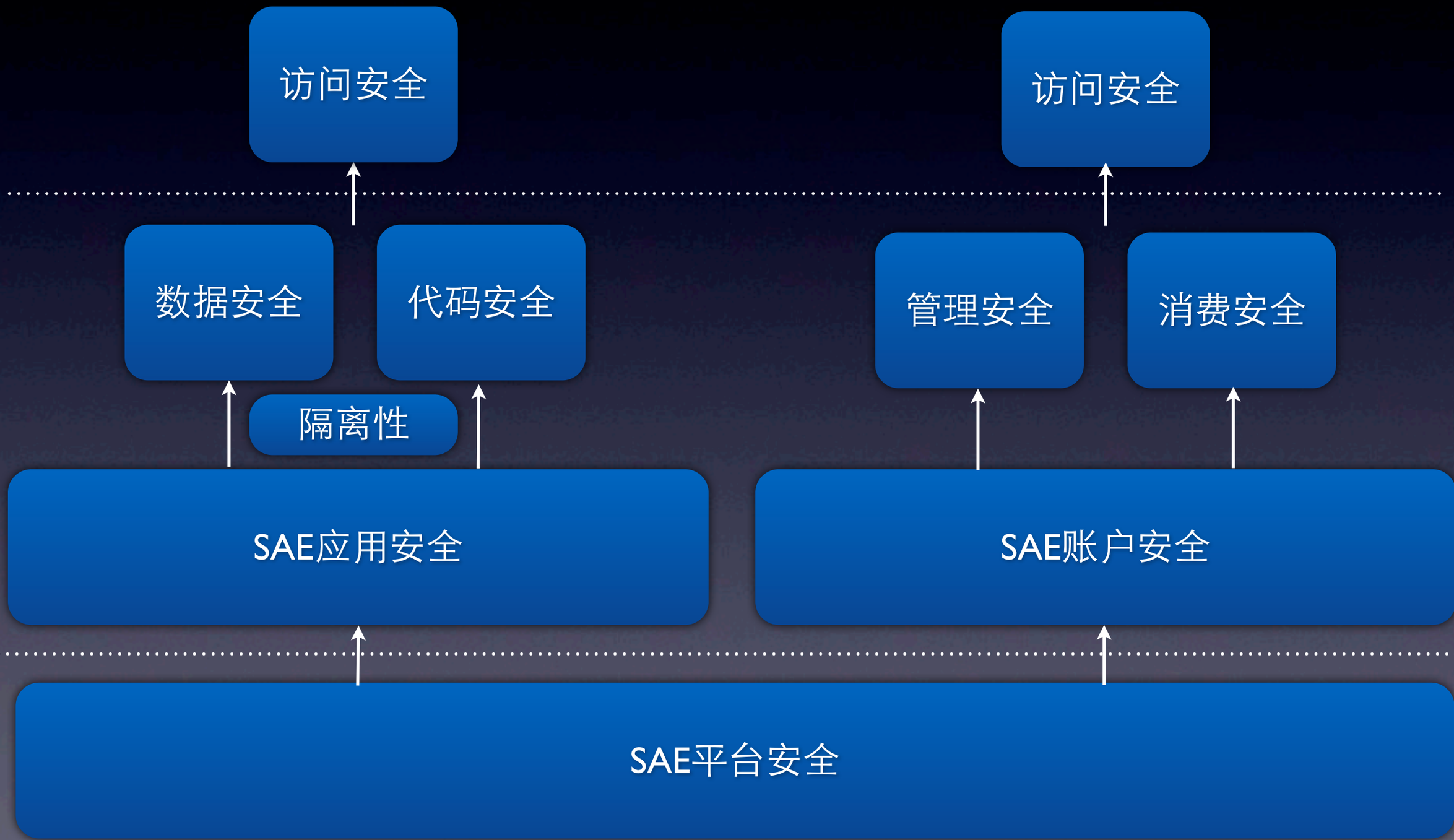
- 资源共享性
- 服务多样性
- 用户不可预知性
- 规模不可预知性

SAE安全实践

SAE整体架构图



SAE安全架构



SAE安全实践 - 隔离性

沙箱隔离：

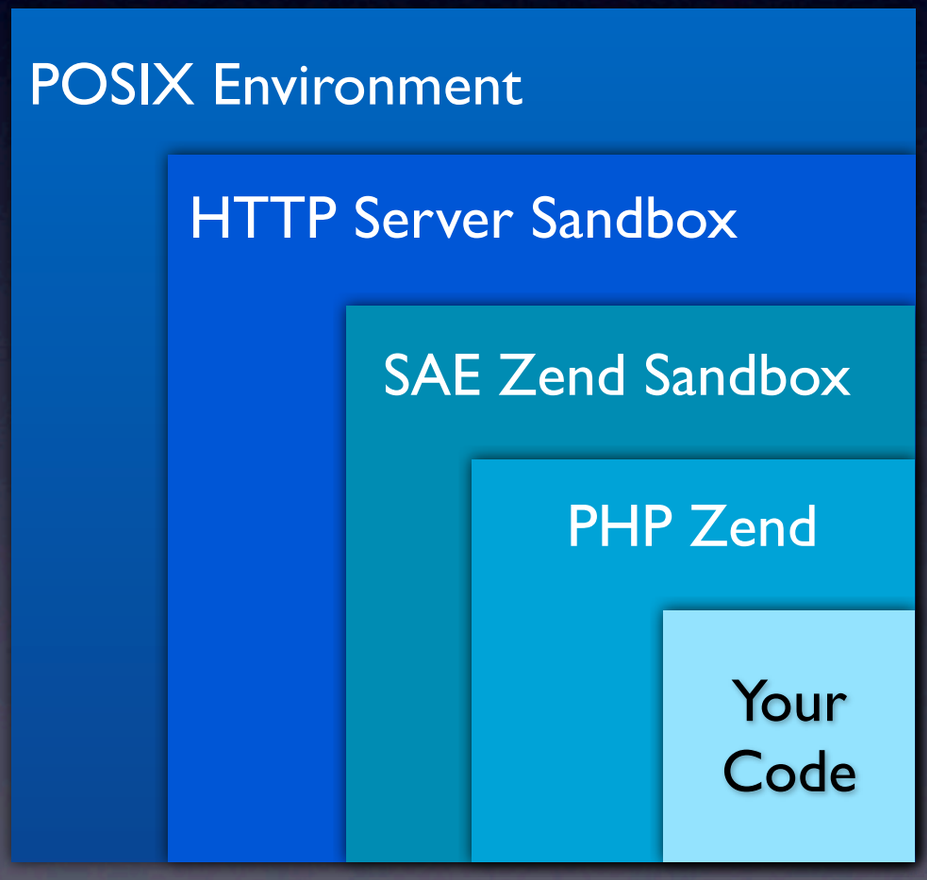
- PHP沙箱
- Python沙箱
- Java沙箱

服务隔离：

- 存储类服务（MySQL）
- 计算类服务（Image）

SAE安全实践 - 隔离性

PHP沙箱



Level 1 on Zend

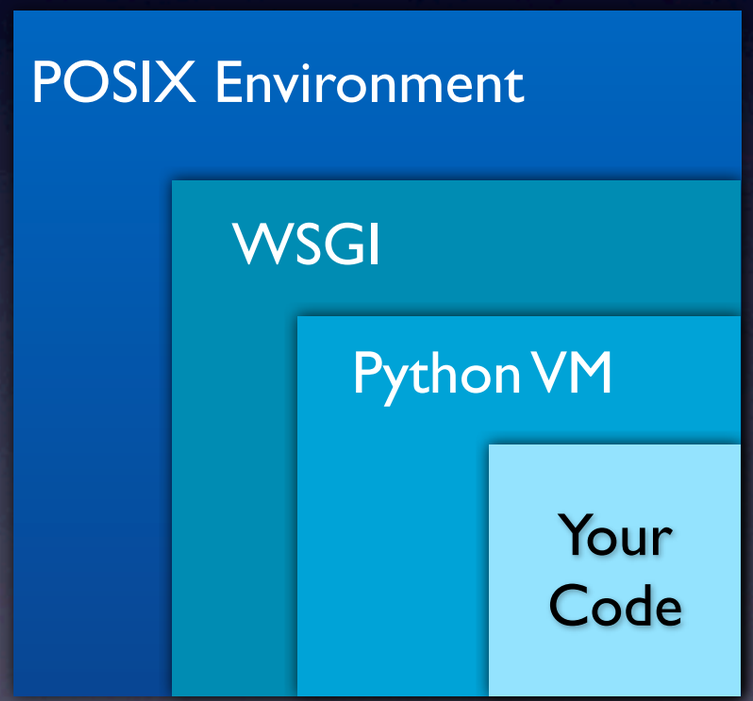
- I/O隔离
- 内存保护
- cpu控制

Level 2 on Apache

- 连接保护
- 请求控制
- libc函数保护（DLL注入）

SAE安全实践 - 隔离性

Python沙箱



Level 1 on Python VM

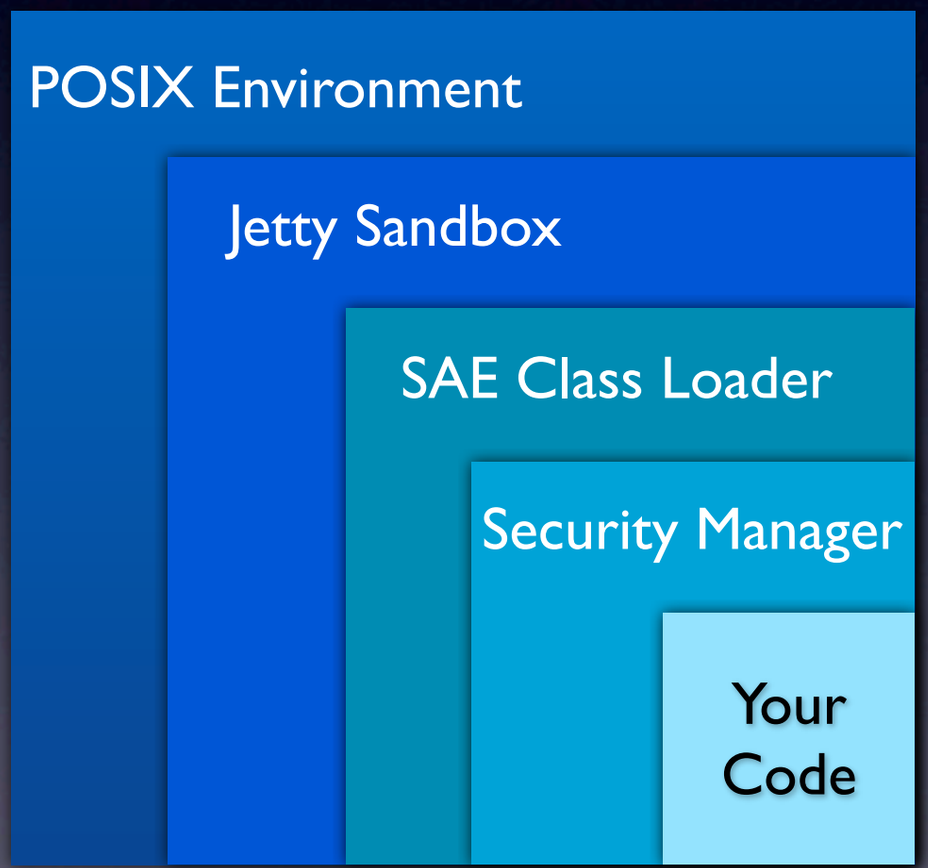
- IO隔离
- 网络隔离
- CPU控制
- libc函数保护（DLL注入）

Level 2 on Posix

- SE - Linux

SAE安全实践 - 隔离性

Java沙箱



Level 1 on JVM

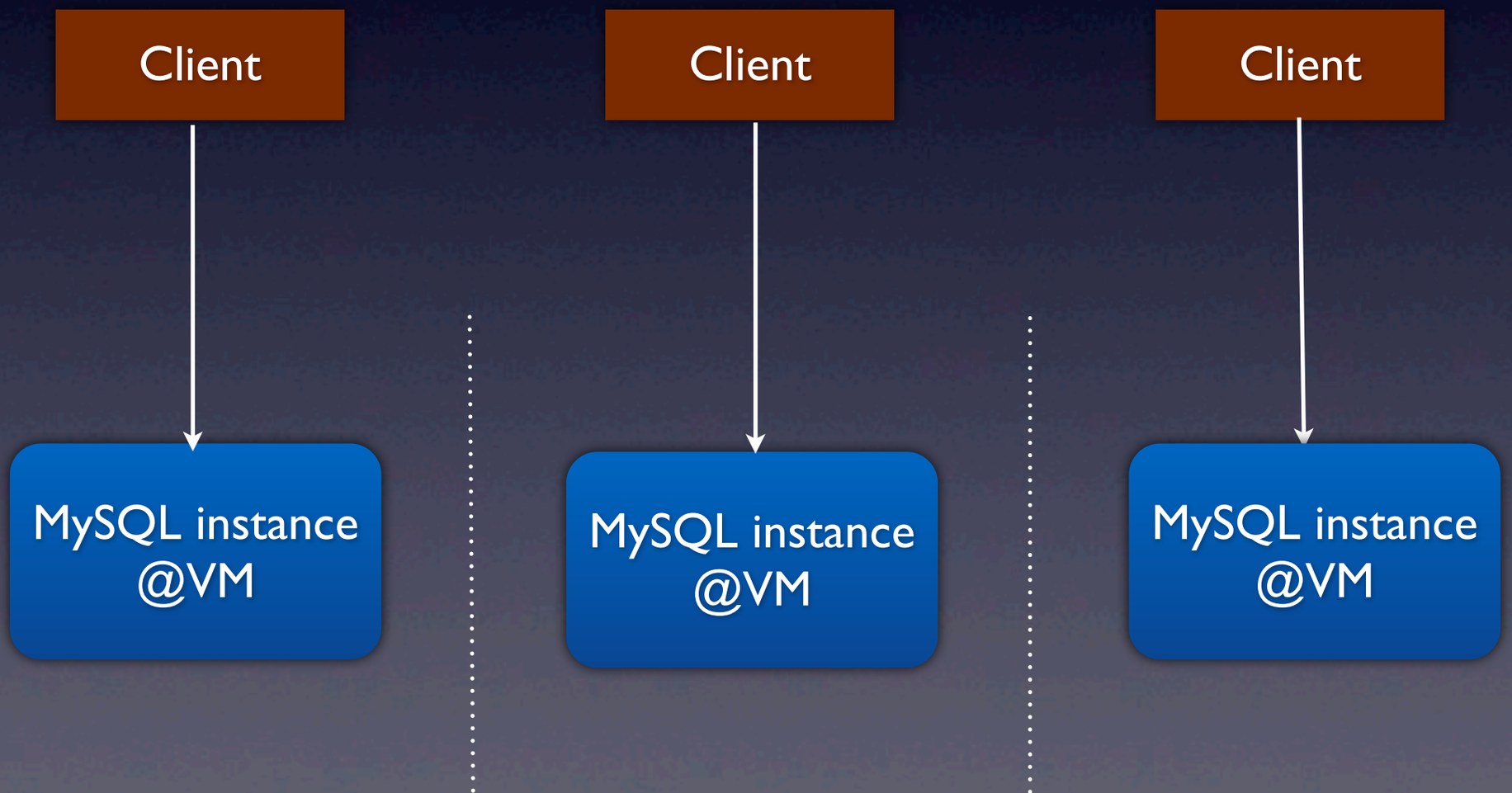
- policy控制
- SAE Class Loader
- 网络隔离
- CPU控制
- JVM迁移

Level 2 on Posix

- SE - Linux

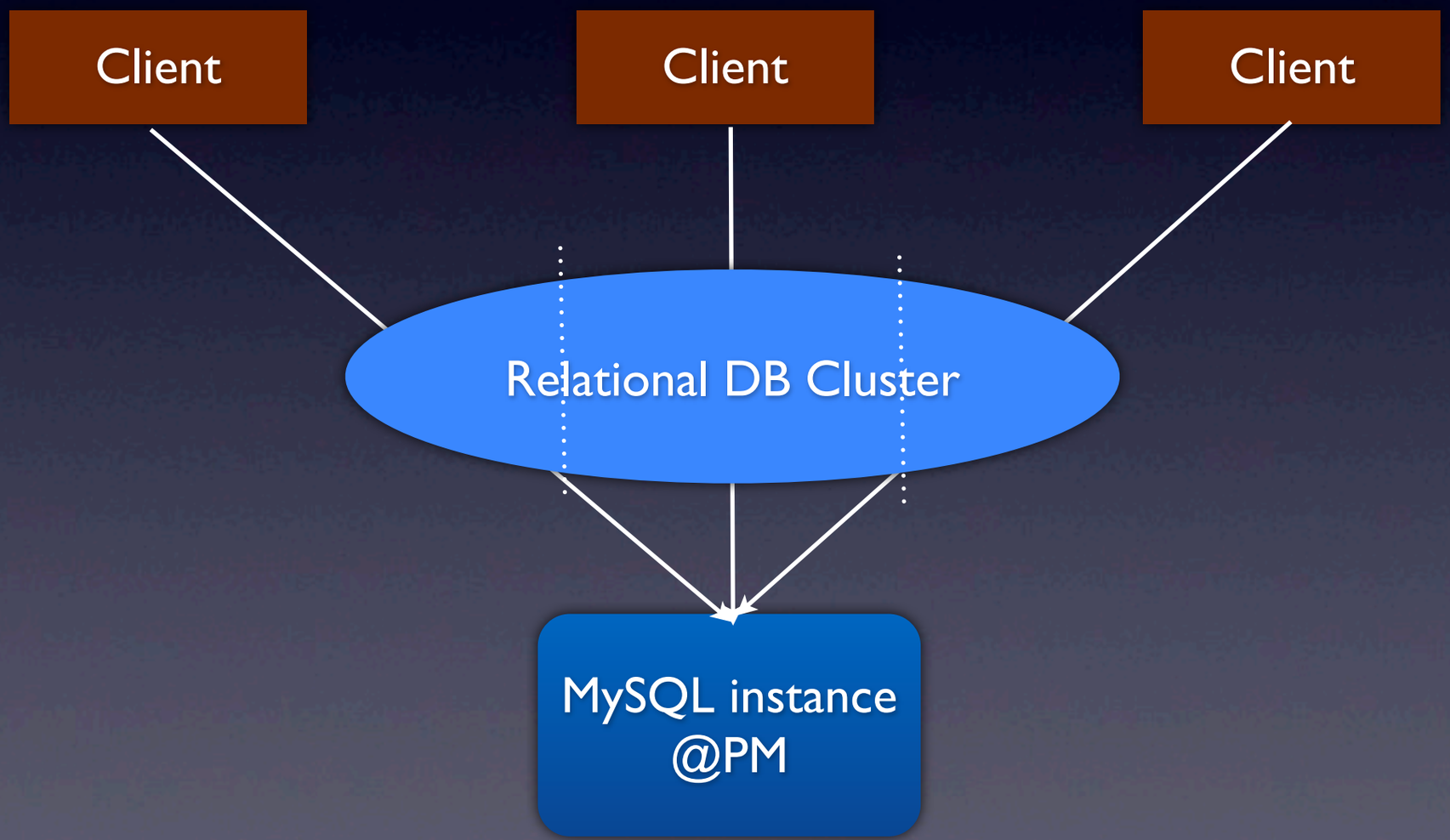
SAE安全实践 - 隔离性

MySQL隔离性 2009.11



SAE安全实践 - 隔离性

MySQL隔离性 2010.6



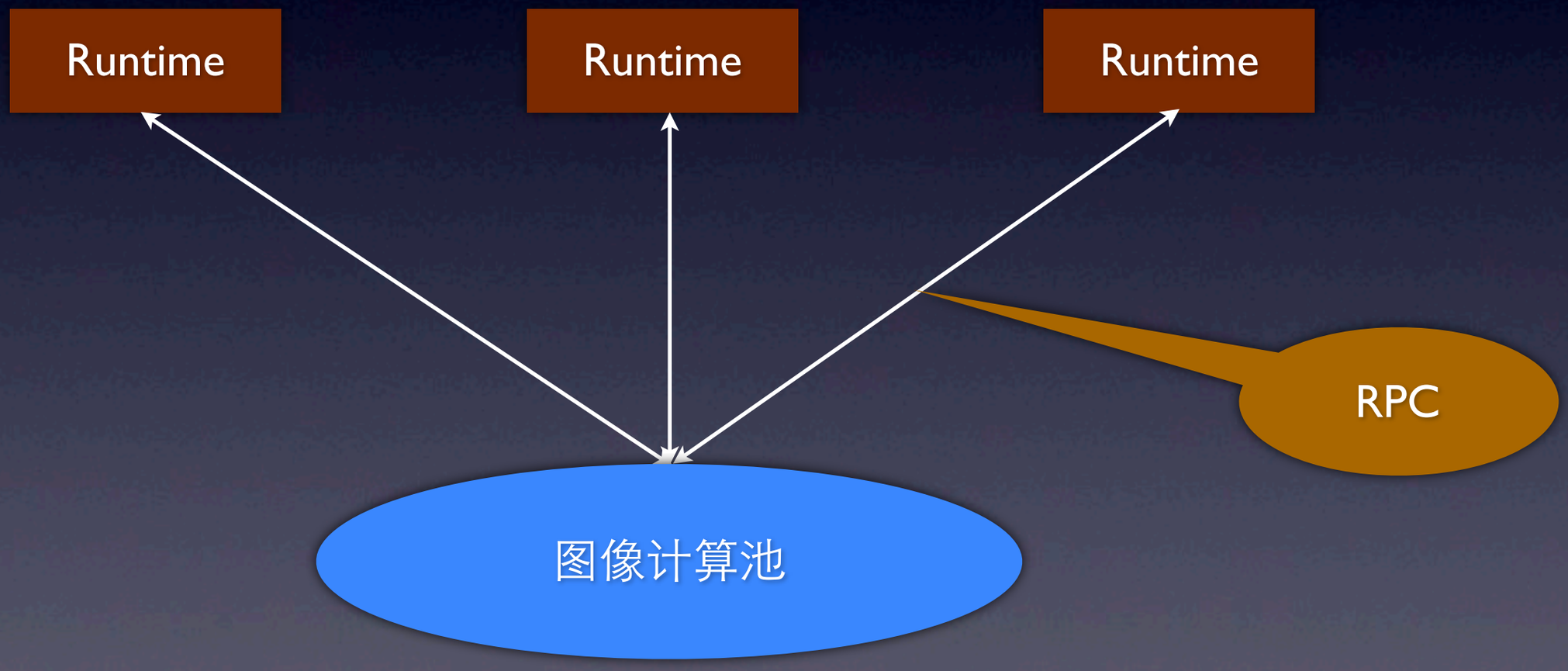
SQL预判

并发执行时间和

慢查询配额

SAE安全实践 - 隔离性

计算池隔离 - GDSmooth



SAE安全实践 - 数据安全

可靠性:

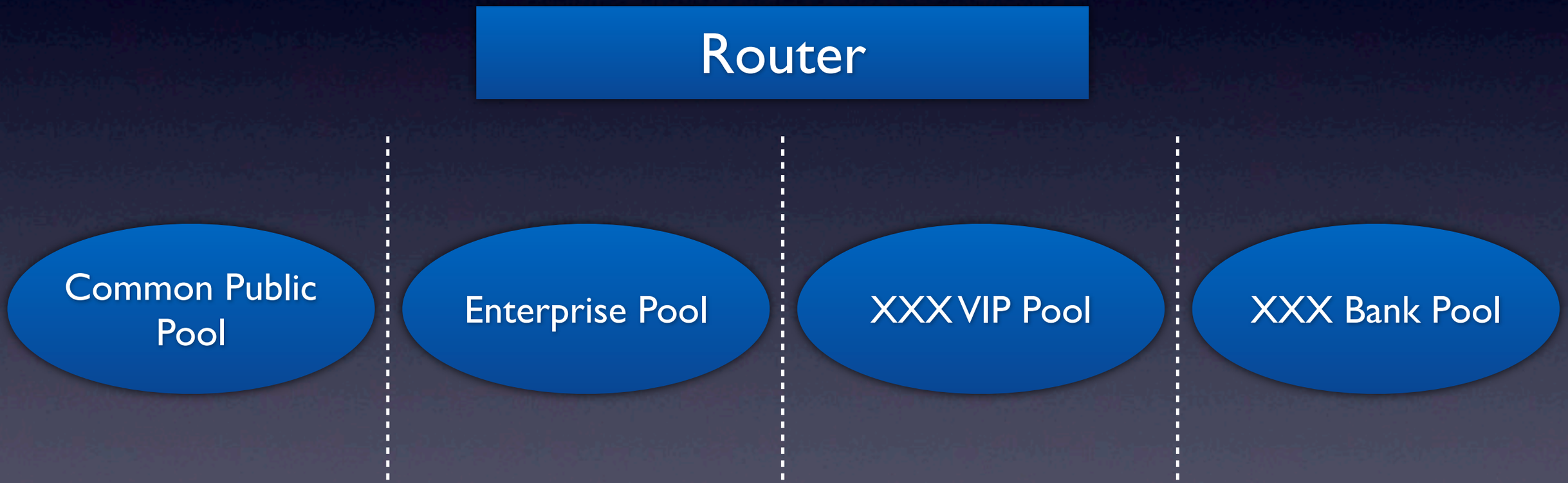
- MySQL备份机制
- KVDB备份机制
- TaskQueue备份机制
- Counter/Rank备份机制

企业数据安全:

- VPC

SAE安全实践 - 数据安全

企业VPC (Virtual Public Cloud)



SAE安全实践 - 代码安全

用户代码漏洞

用户代码丢失

用户代码泄露

SAE安全实践 - 代码安全

应用体检

SAE安全实践 - 代码安全

- SVN代码版本控制

- CodeFS
- 用户代码权限保护

SAE安全实践 - 代码安全

- 用户代码加密（PHP）

- 用户代码加密（Java）

  代码混淆器

- 用户代码加密（Python）

  .pyc

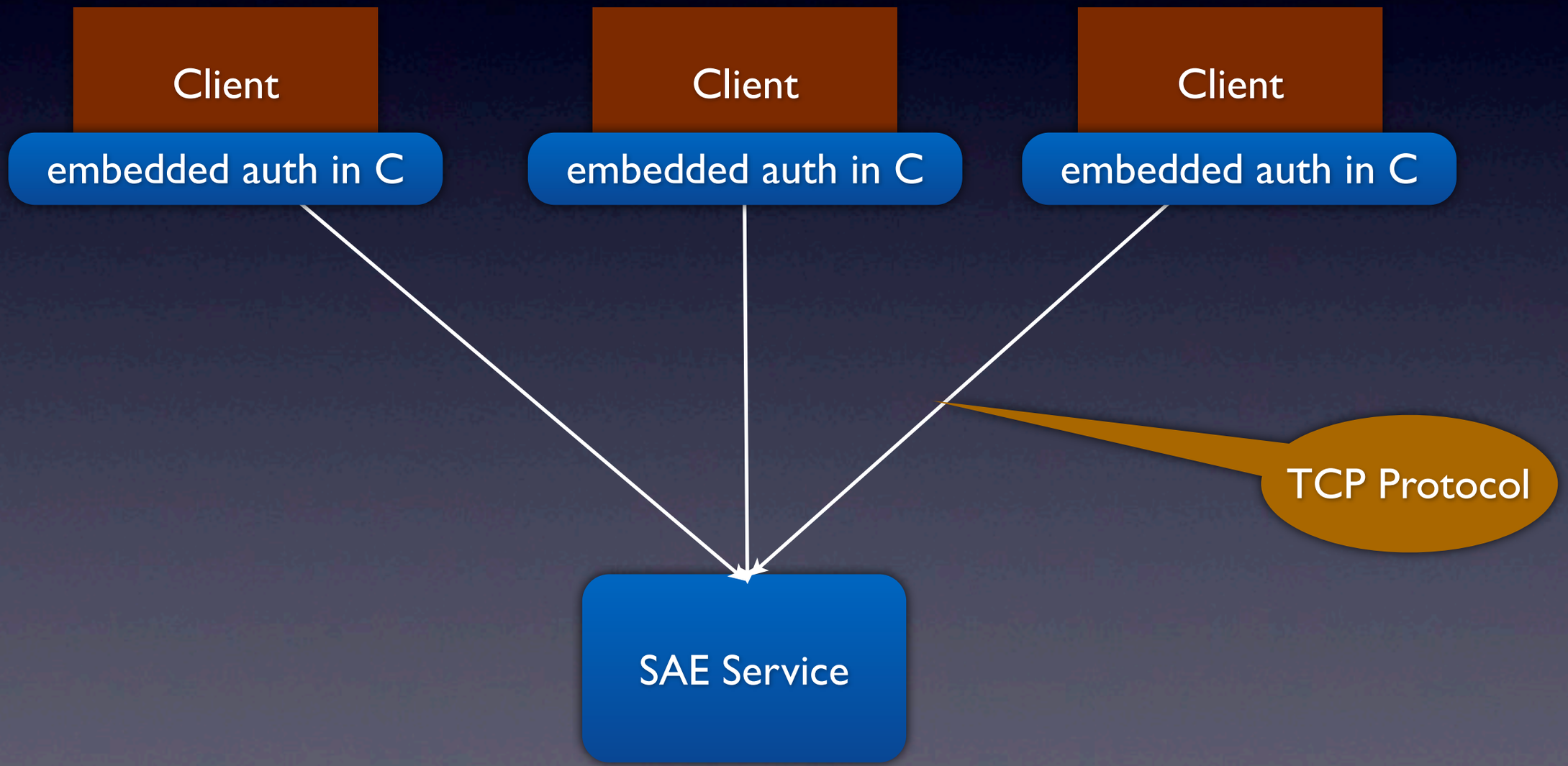
SAE安全实践 - 访问安全

对内访问安全:
验证方式
网络控制

对外访问安全:
验证方式
网络控制
防火墙

SAE安全实践 - 访问安全

两种验证方式 - Client Namespace-binding

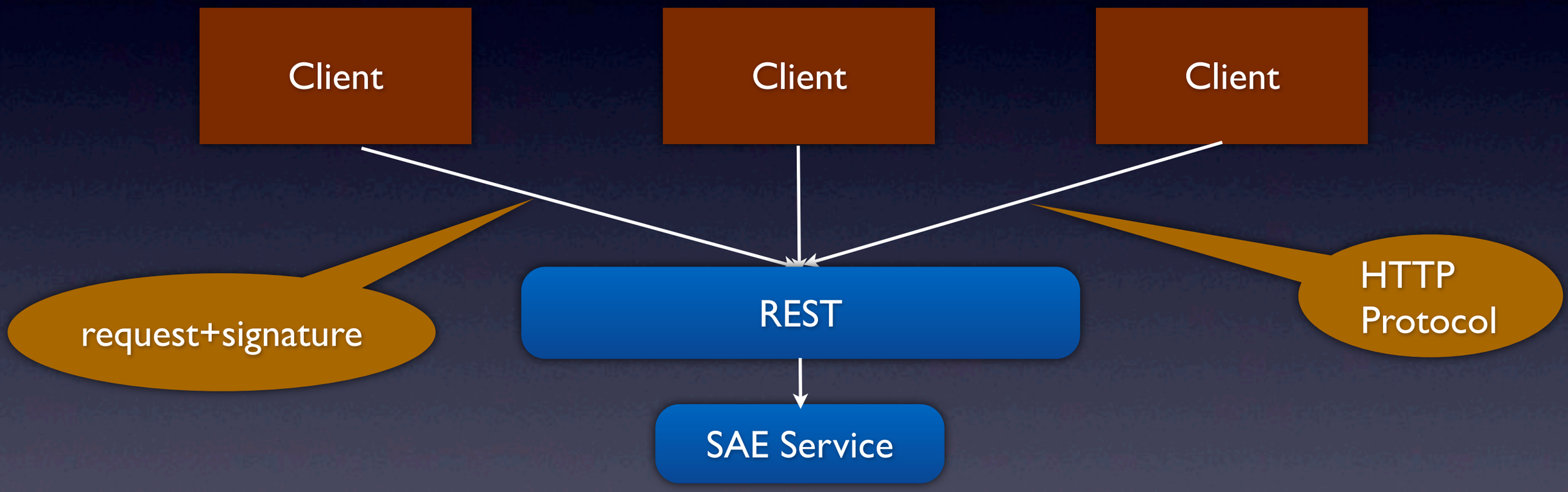


SAE安全实践 - 访问安全

MySQL跨应用授权

SAE安全实践 - 访问安全

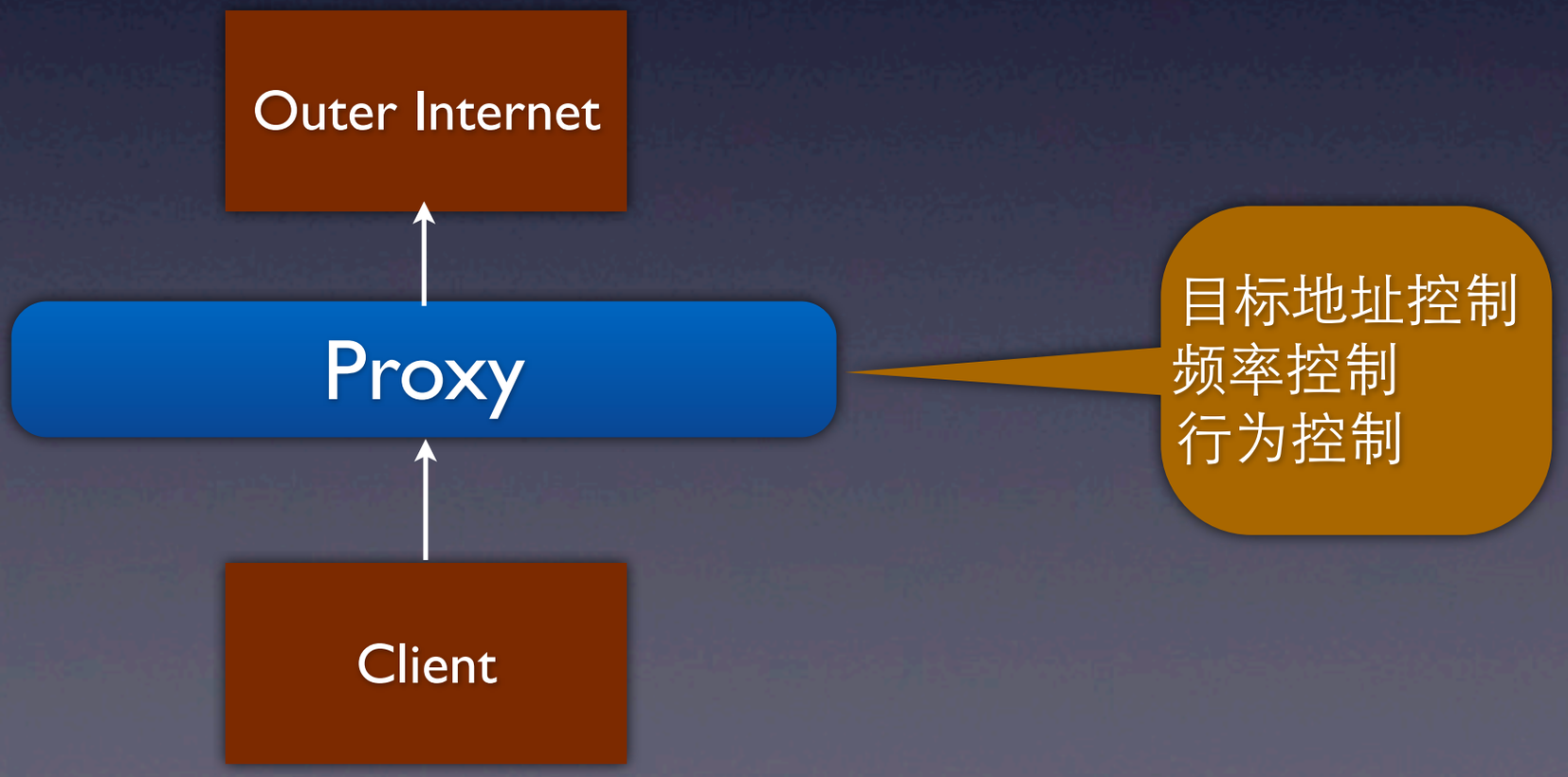
两种验证方式 - SHA256 REST signature



signature == SHA256(request+access-key+secret-key)
request间隔和排序

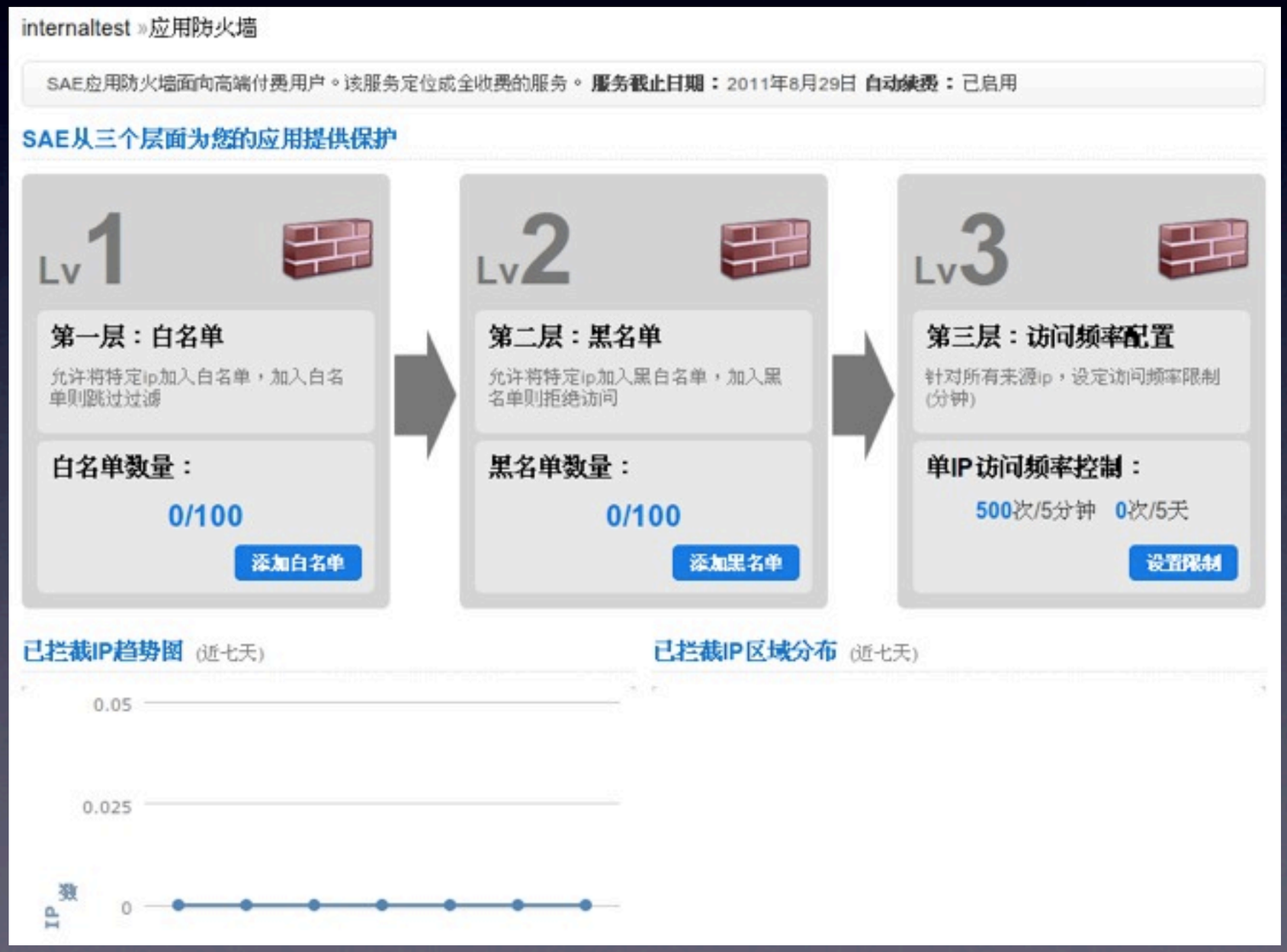
SAE安全实践 - PaaS SDN

- 网络安全控制 - FetchURL (HTTP/HTTPS)
- 网络安全控制 - SocketProxy (TCP/SSL)
- PaaS&IaaS 网络安全控制



SAE安全实践 - 访问安全

应用防火墙



- IP黑白名单
- 访问频率控制
- 流入流出流量控制

SAE安全实践 - 账户安全

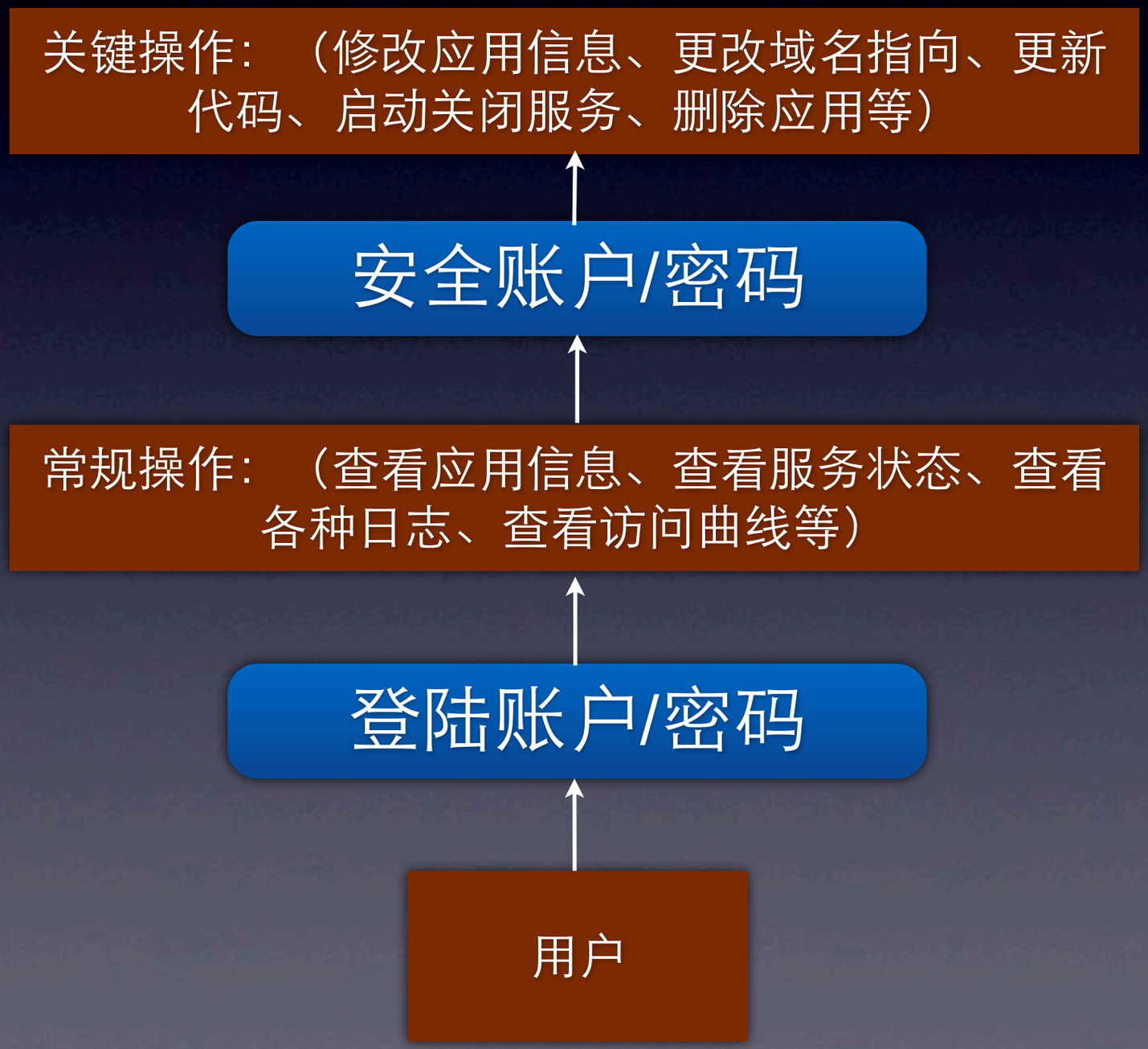
登录安全

管理安全

消费安全

SAE安全实践 - 账户安全

普通用户



SAE安全实践 - 账户安全

企业用户

关键操作：（修改应用信息、更改域名指向、更新代码、启动关闭服务、删除应用等）

↑

安全密码+动态口令

激活动态口令

↑

常规操作：（查看应用信息、查看服务状态、查看各种日志、查看访问曲线等）

↑

登陆账户/密码

↑

VIP用户

SAE安全实践 - 账户安全

SAE账户角色体系

SAE帐号	状态	操作	权限
sp***e@163.com	Active	无法删除项目创建者	创建者 (全部权限)

您可以邀请朋友加入开发，我们会将邀请链接通过电子邮件和微博私信发送给他。

如果他还没有注册SAE，使用该邮箱注册后，仍可以收到邀请。

E-mail *

角色

管理者
参与者
观察者
✓ 自定义

管理代码 管理服务 设置配额 设置应用信息

邀请语

发送邀请

SAE安全实践 - 账户安全

SAE账户角色体系

角色\权限	删除应用	除删除应用外的所有权限	部署代码	设置配额	查看数据、日志
项目所有者	*	*	*	*	*
管理者		*	*	*	*
参与者			*	*	*
观察者					*
自定义角色		?	?	?	?

SAE安全实践 - 消费安全

- 云豆保护

- 大额消费保护
- 消费审计

SAE安全实践 - 经验

- 关于信任

  可靠的技术/运维团队

  SLA保证和补偿政策：

  - SAE故障补偿政策： http://sae.sina.com.cn/?m=devcenter&catId=245
  - 没有补偿政策的SLA都是耍流氓

- 关于变更

  自身系统变更 =>灰度发布

  用户代码数据变更 => 变更跟踪、分组

Q & A

conglei@staff.sina.com.cn
weibo.com/kobe