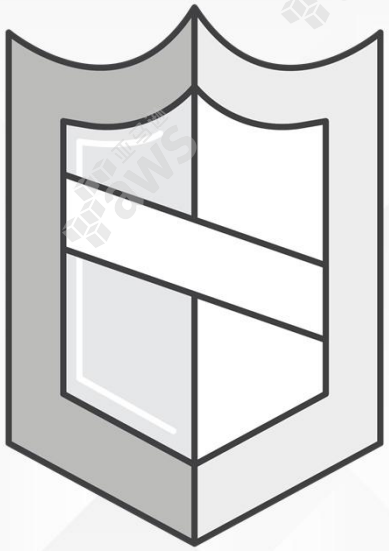

AWS Summit
AWS技术峰会2015 · 上海
亚马逊
aws

ELB应用场景与使用技巧

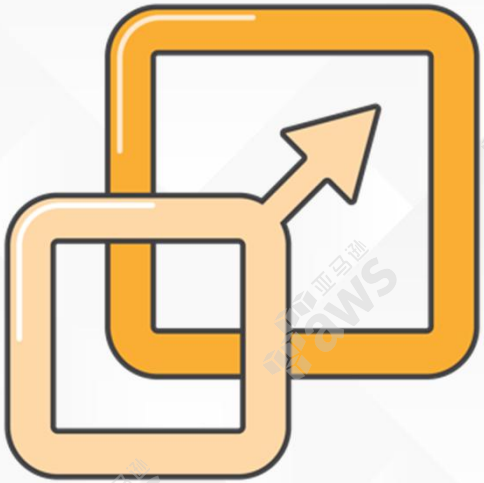
姜可舒

亚马逊 aws

弹性负载均衡 Elastic Load Balancing



安全性

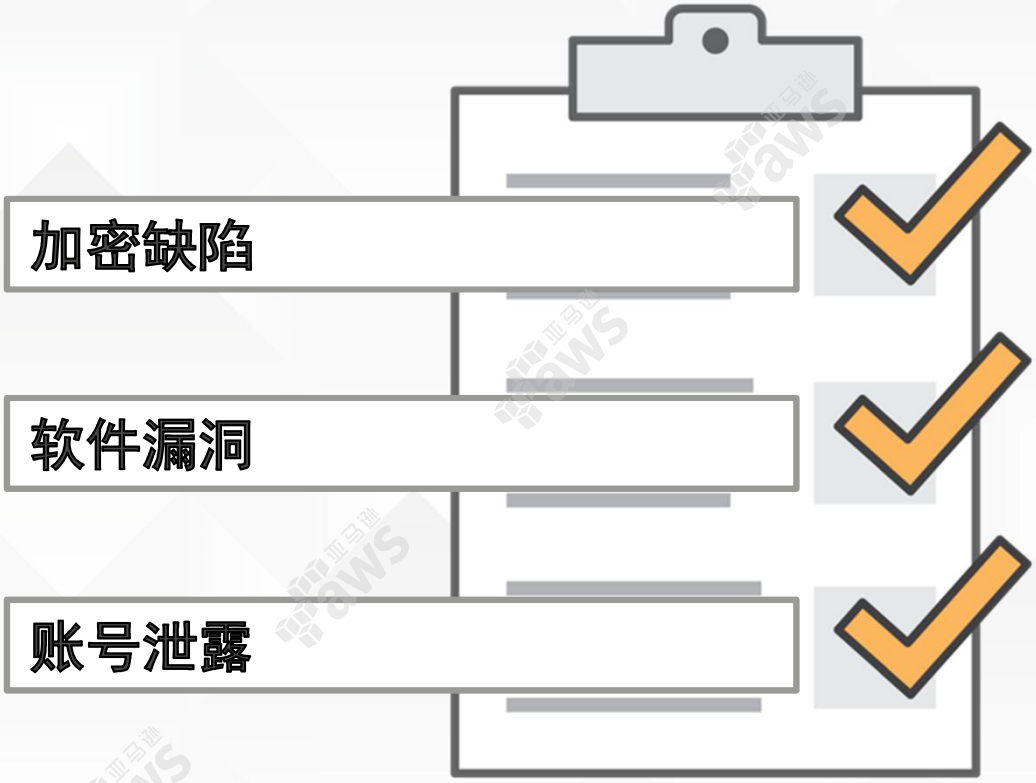


扩展性

高可用

安全性

安全威胁模型分析



SSL/TLS 安全策略

- 同步消除POODLE隐患
- 同步消除LogJam隐患
- 同步消除Heartbleed隐患
- 遵循安全规范更新，移除RC4

SSL/TLS 加密套件

- 完全正向保密(perfect forward secrecy)优先
- 优先级：AES > 3DES > RC4
- 优先级：GCM > CBC + HMAC

SSL/TLS 加密套件

- 向下兼容及折中
  - 较早的固件或者嵌入式系统
  - 控制器，网络爬虫…
- 访问日志分析
- 强烈推荐ELBSecurityPolicy-2015-05及更新版本

ELB访问日志

2015-05-13T23:39:43.945958Z my-loadbalancer
192.168.131.39:2817 10.0.0.1:80 0.000086 0.001048 0.001337
200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1”
"curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2

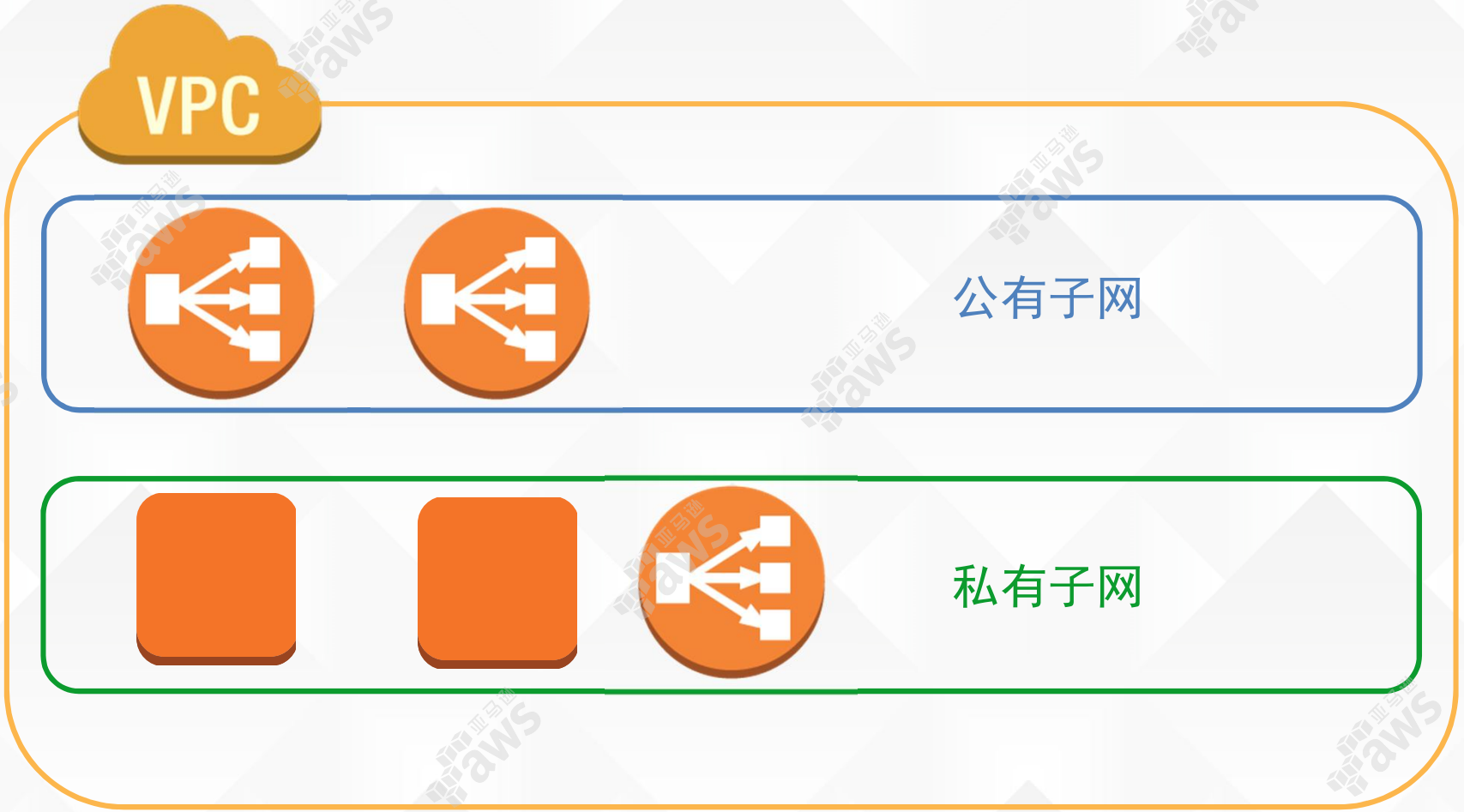
ELB访问日志

2015-05-13T23:39:43.945958Z my-loadbalancer
192.168.131.39:2817 10.0.0.1:80 0.000086 0.001048 0.001337
200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1”
"curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2

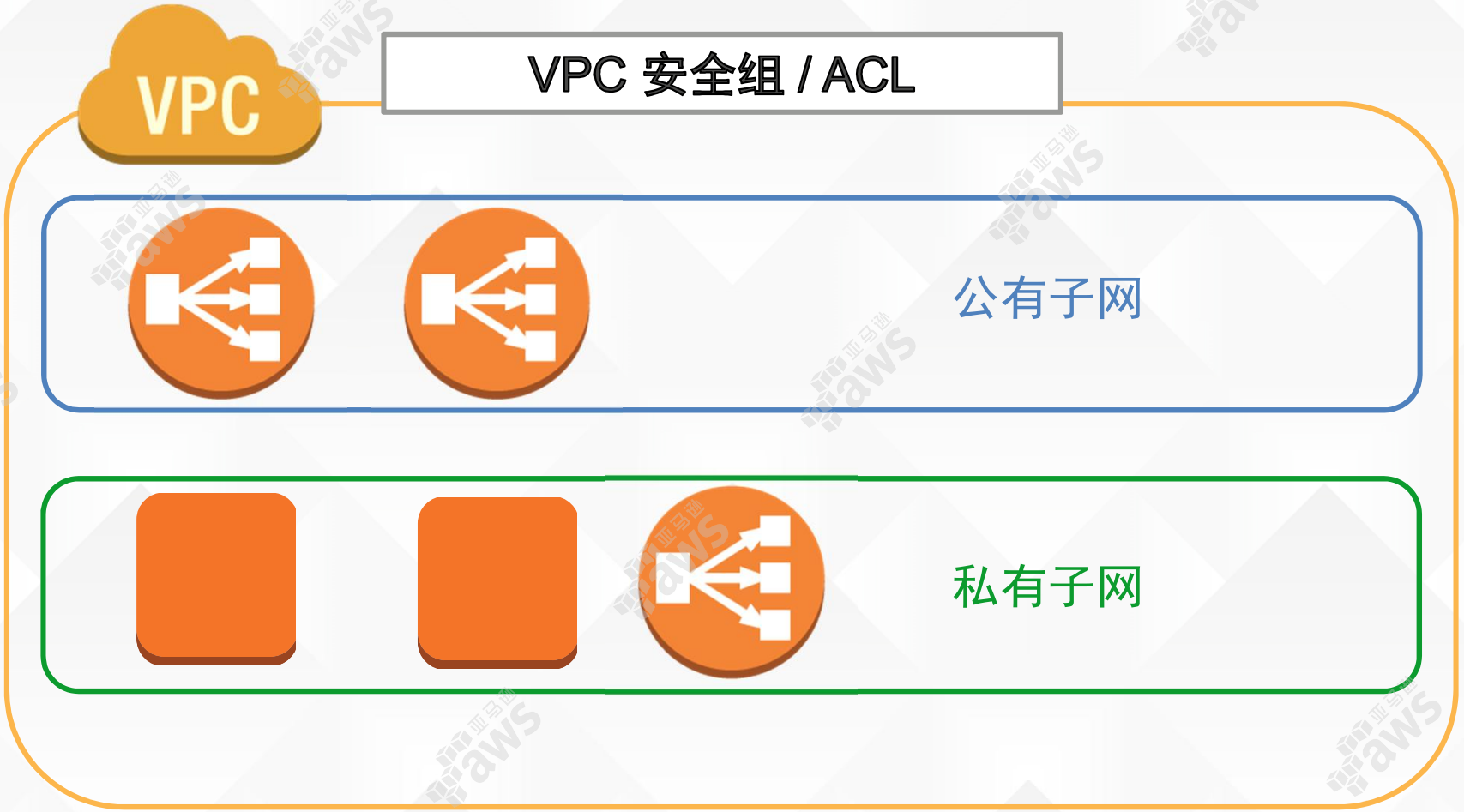
ELB访问日志

2015-05-13T23:39:43.945958Z my-loadbalancer
192.168.131.39:2817 10.0.0.1:80 0.000086 0.001048 0.001337
200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1”
"curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2

ELB及安全隔离



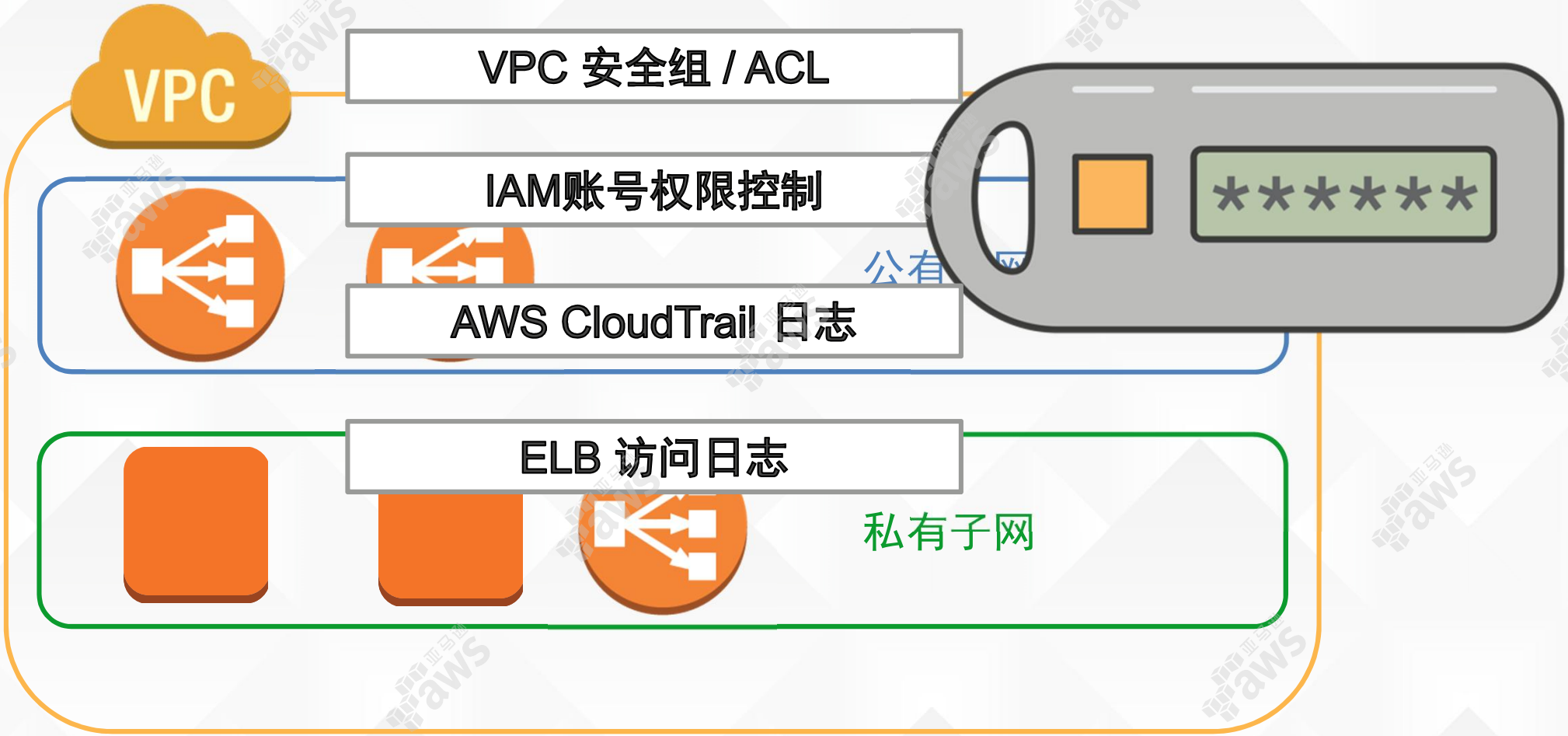
ELB及安全隔离



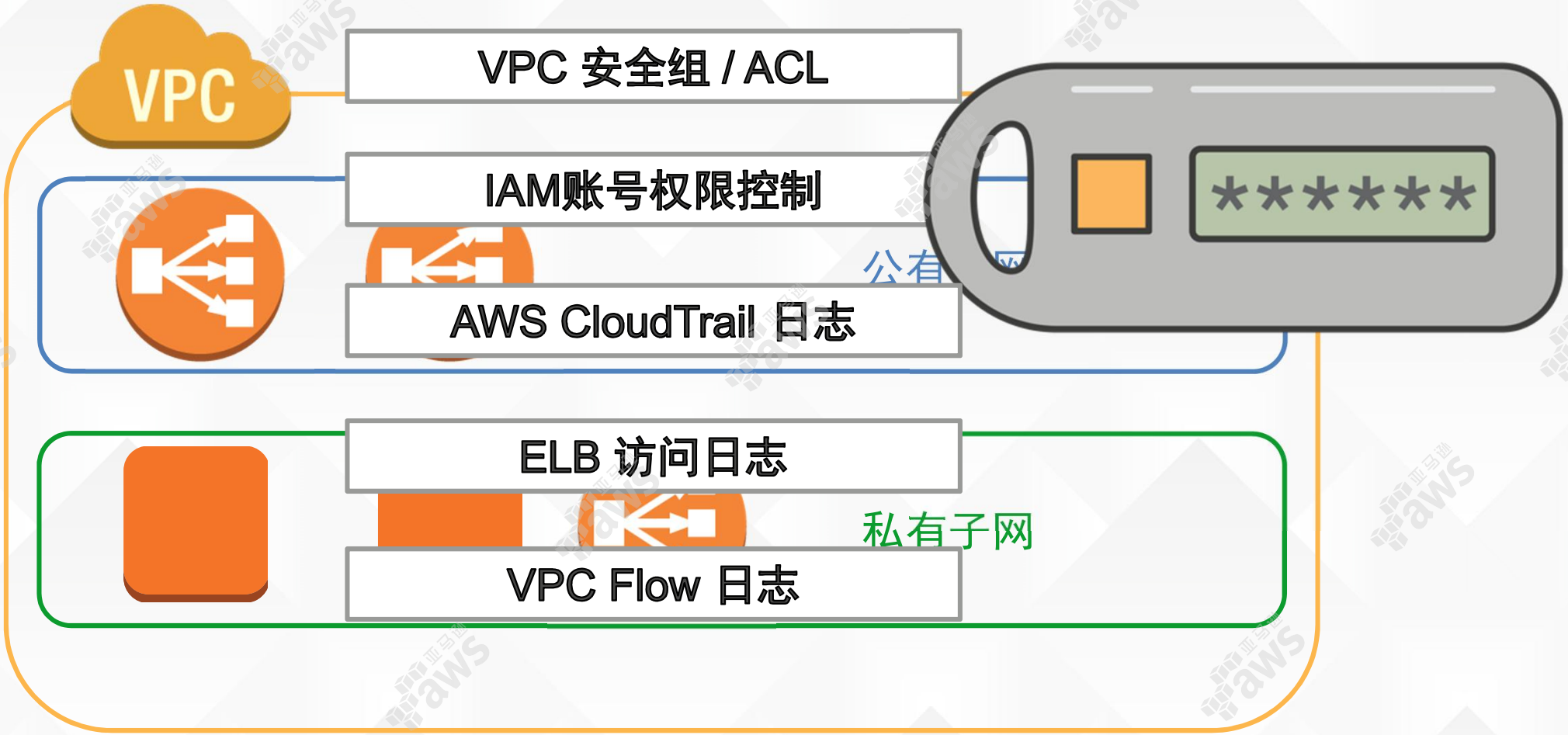
ELB及安全隔离

ELB及安全隔离

ELB 及安全隔离



ELB 及安全隔离


VPC
VPC 安全组 / ACL
IAM账号权限控制
AWS CloudTrail 日志
公有
******
ELB 访问日志
VPC Flow 日志
私有子网

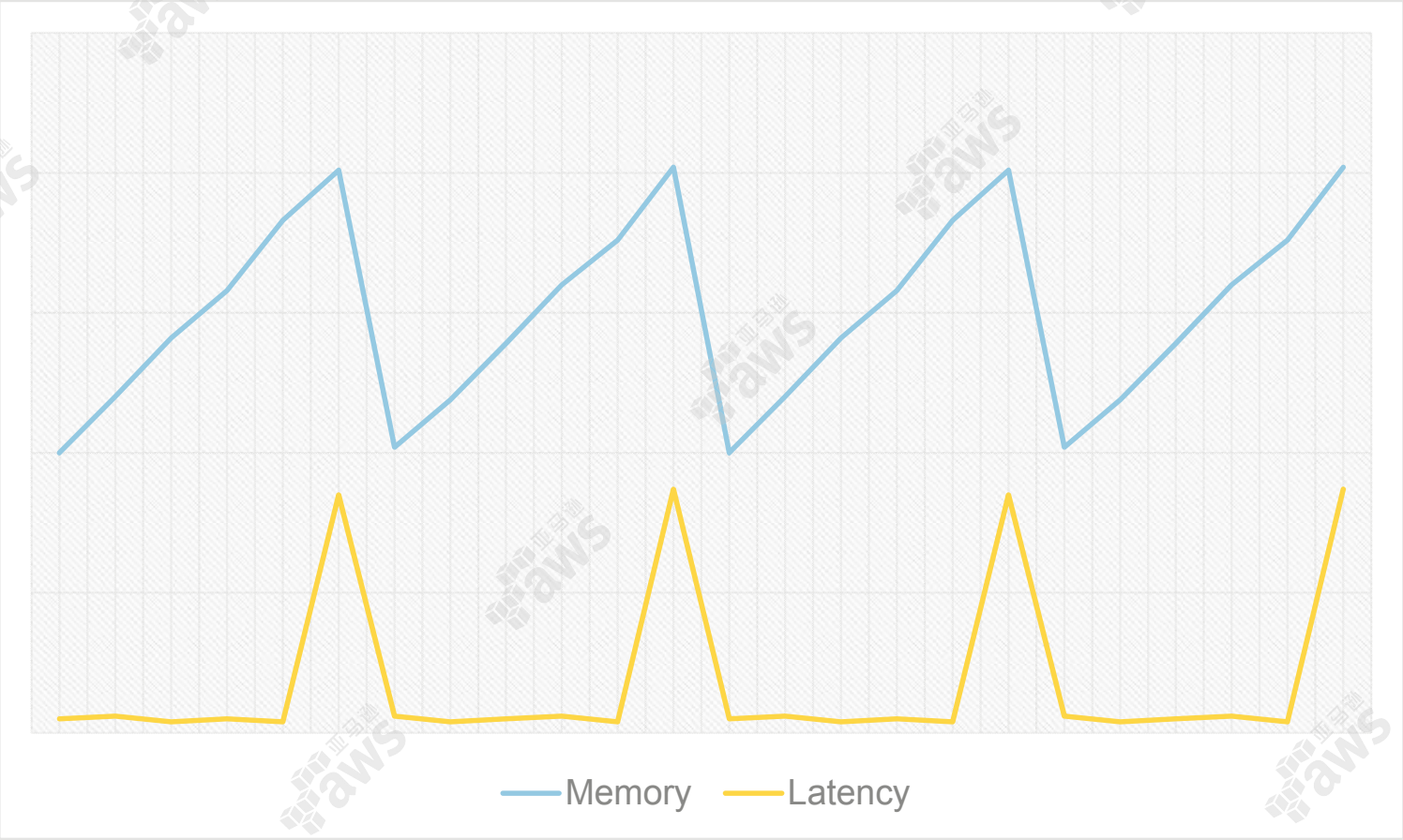
扩展性

扩展性

Latency = Load / Throughput

时延 = 负载 / 吞吐能力

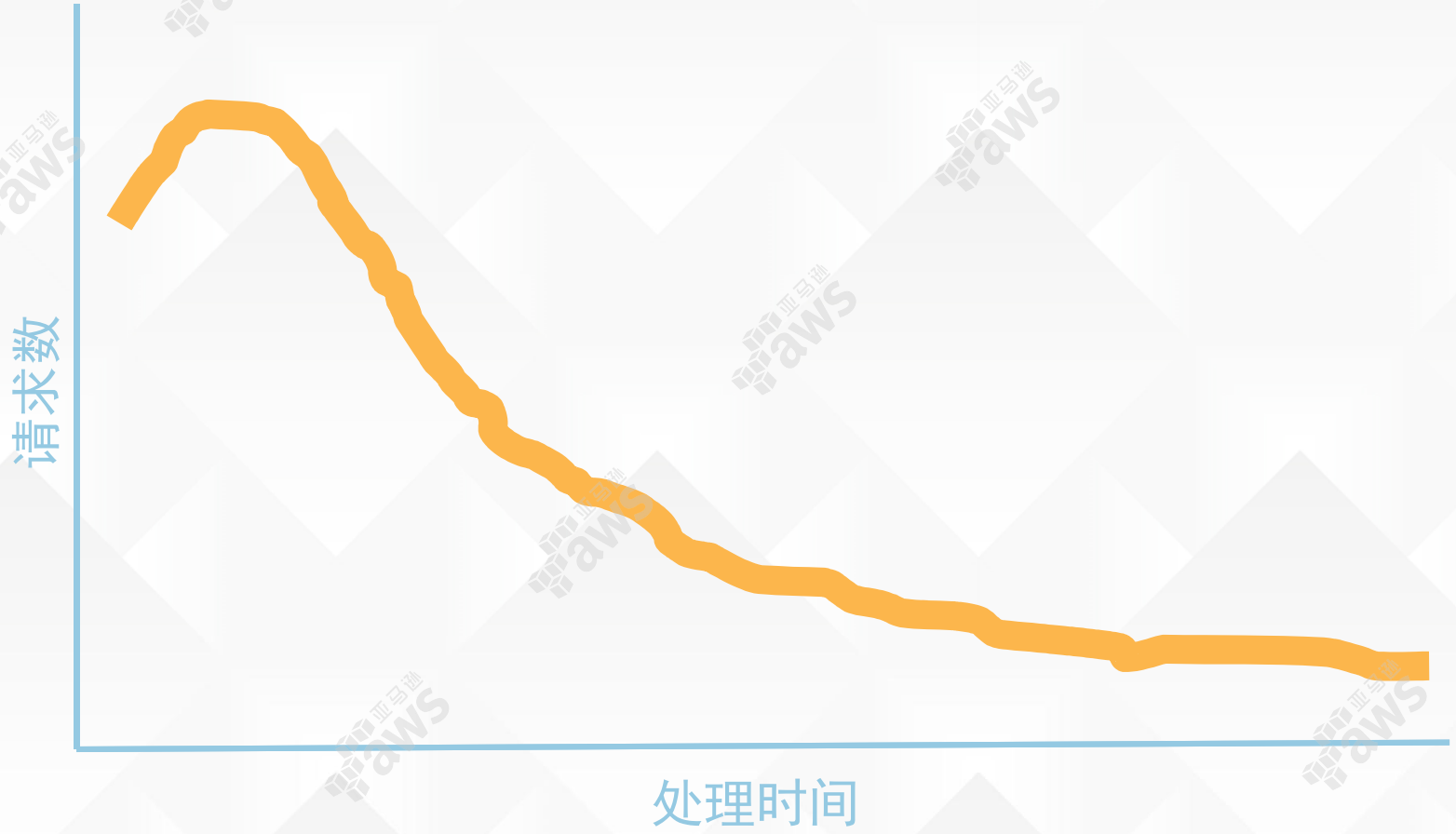
扩展性



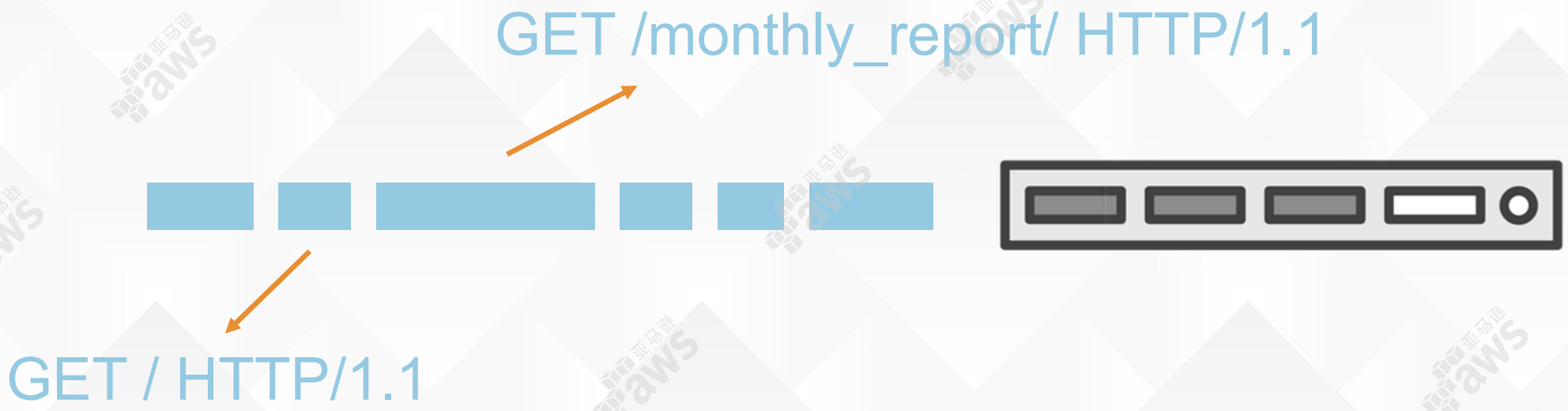
扩展性

命中及未命中缓存

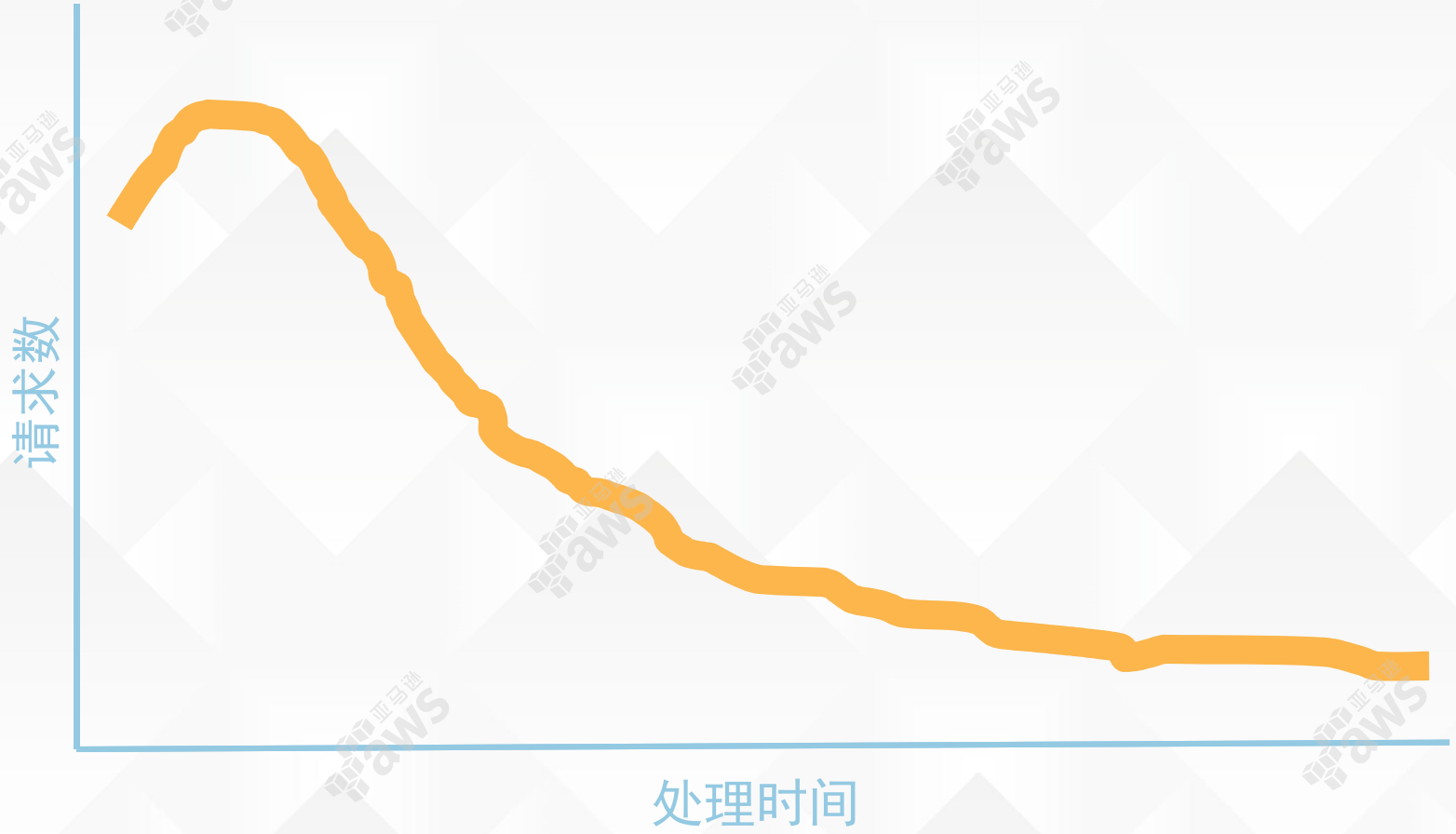
扩展性



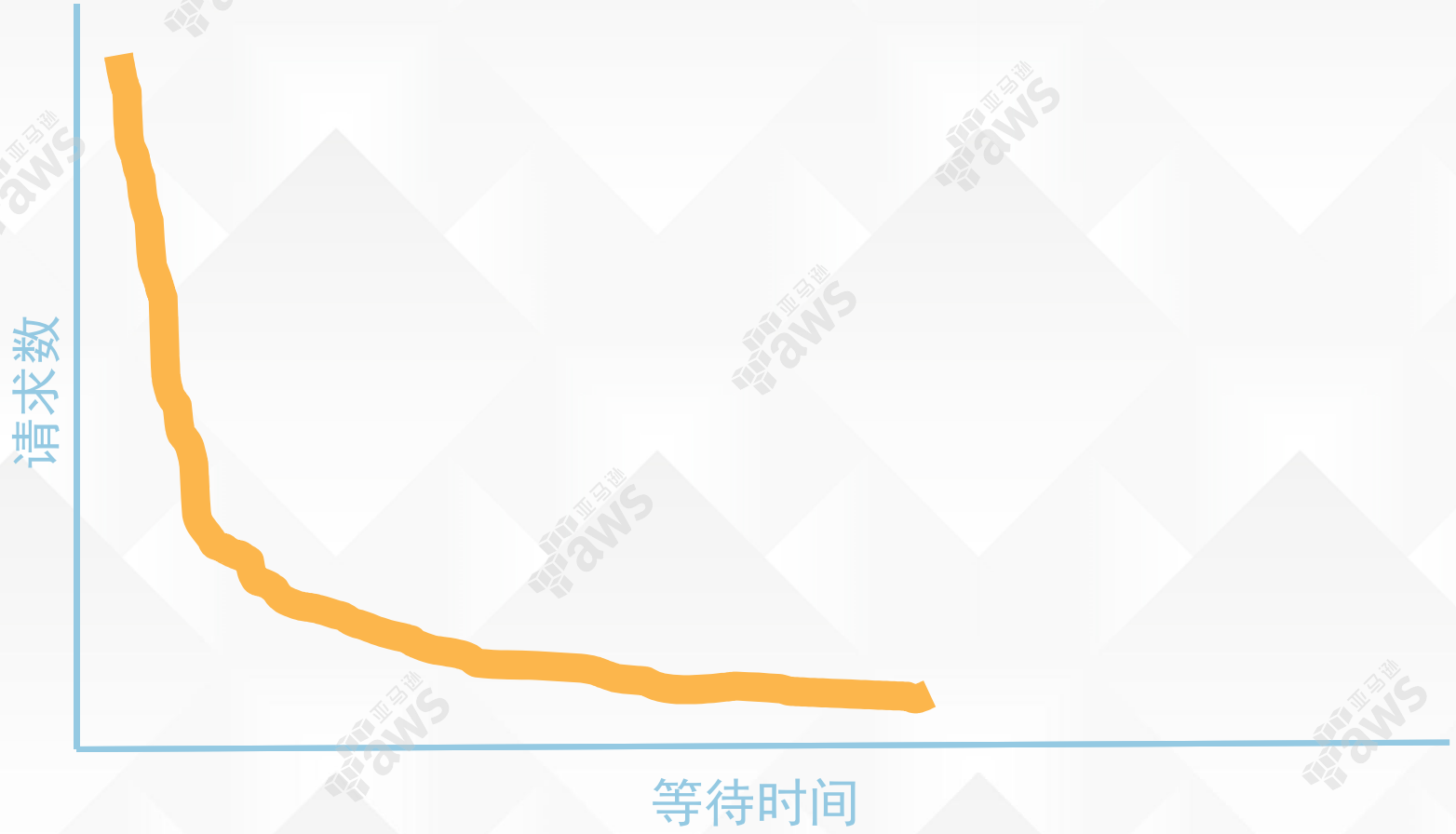
扩展性



扩展性

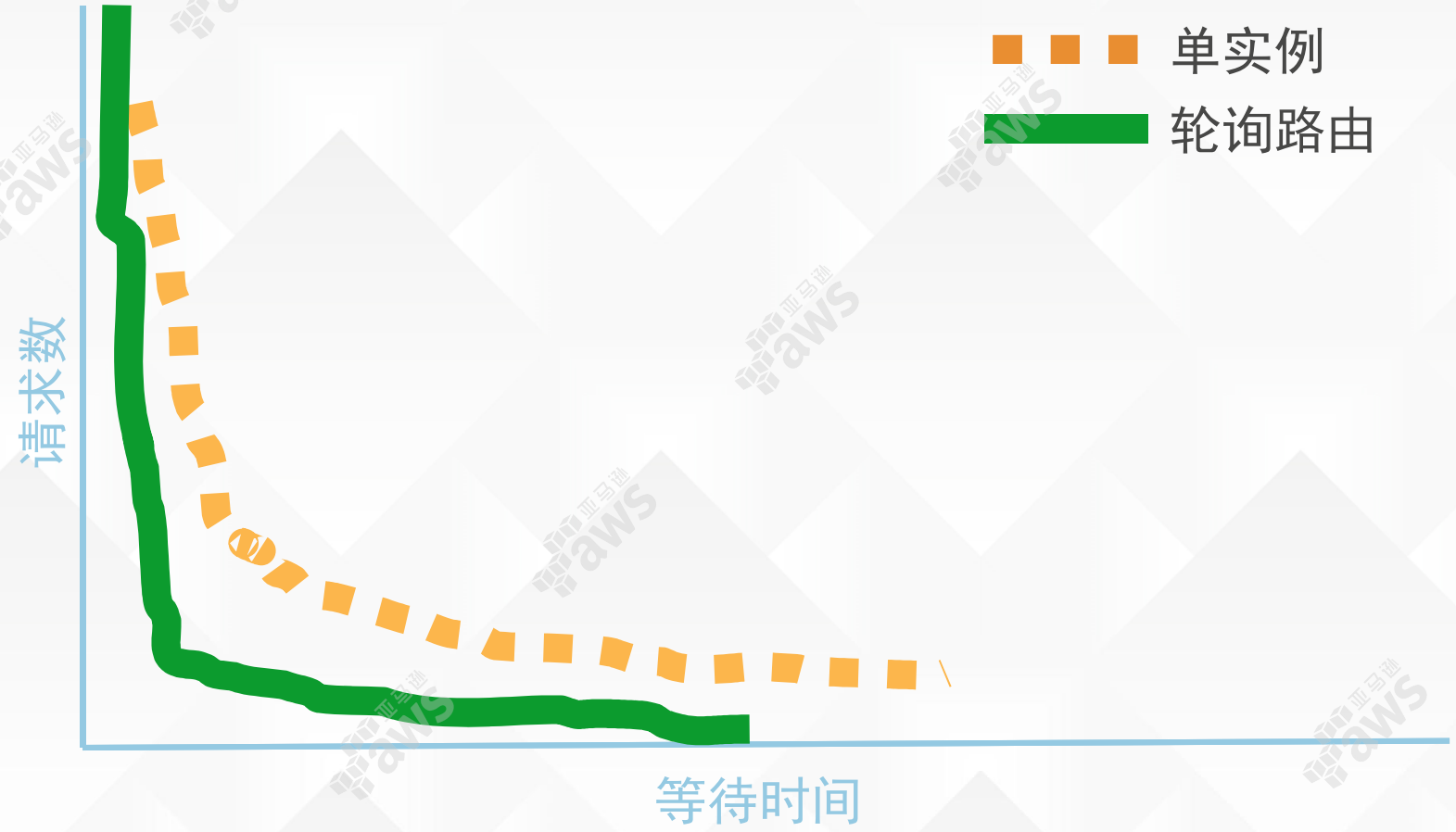


扩展性



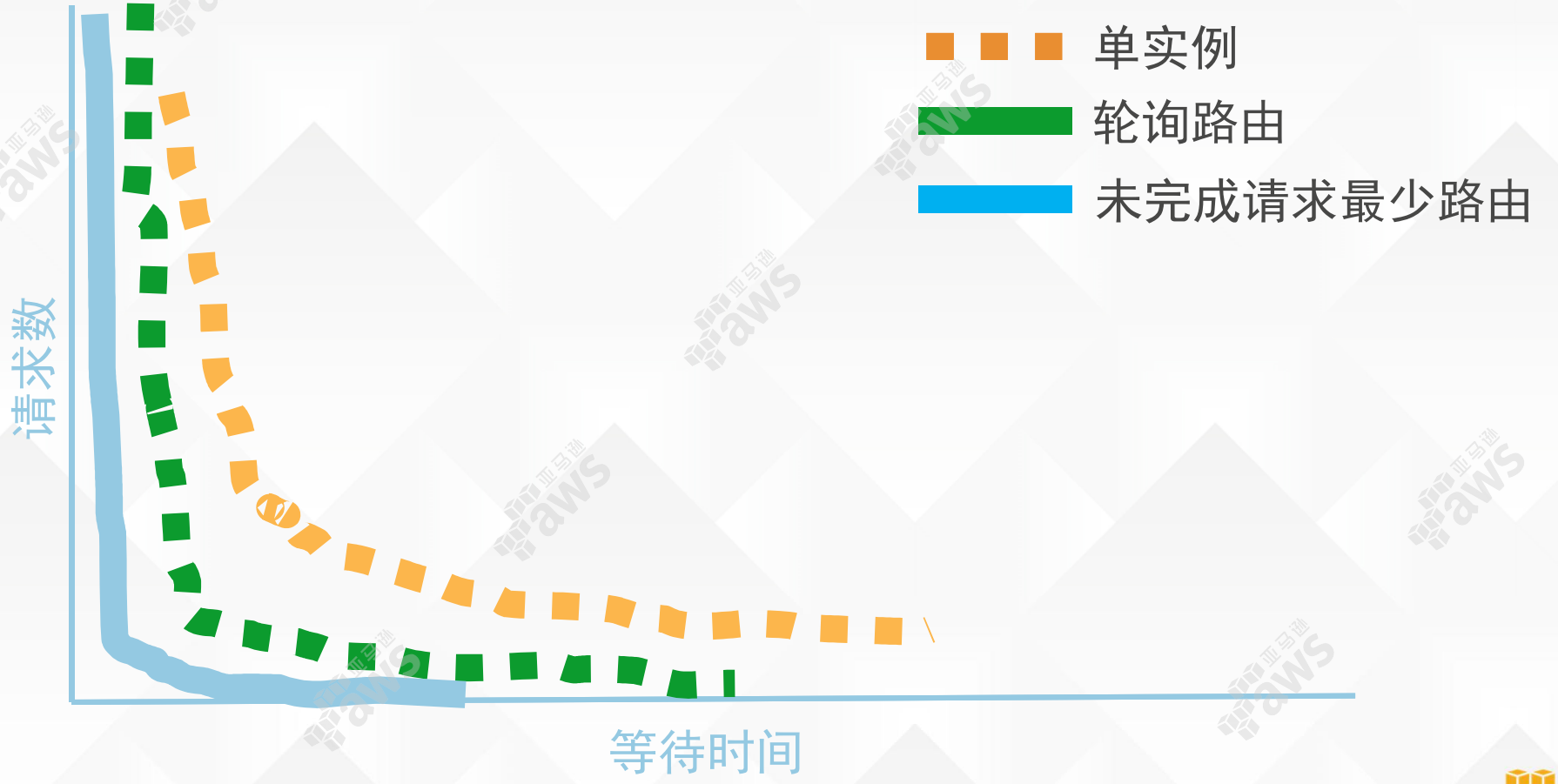
扩展性

扩展性



扩展性

扩展性



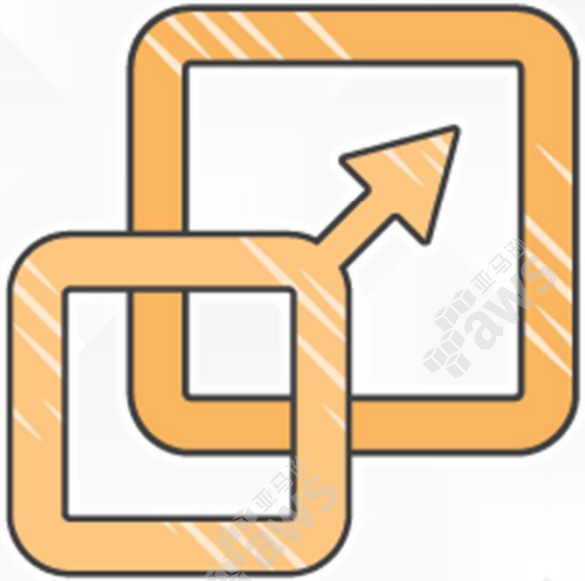
ELB的自动扩展策略分为主动模式，基于添加的后端实例容量，和被动模式，基于收到的负载

CloudWatch和Auto Scaling

Auto Scaling可以使用全部ELB监控指标

允许您基于ELB角度监控的实时应用情况动态扩展

需要根据所有监控指标合理设置Auto Scaling
收缩策略



CloudWatch监控指标

13个CloudWatch监控指标

洞悉ELB以及应用的健康以及运行状态

利用CloudWatch报警迅速通知异常并进行响应

所有监控指标粒度均为1分钟

运行状况良好的主机数 HealthyHostCount

可用区内以ELB视角观察到的健康实例数量

较为常见的导致实例不健康的原因是健康检查超时

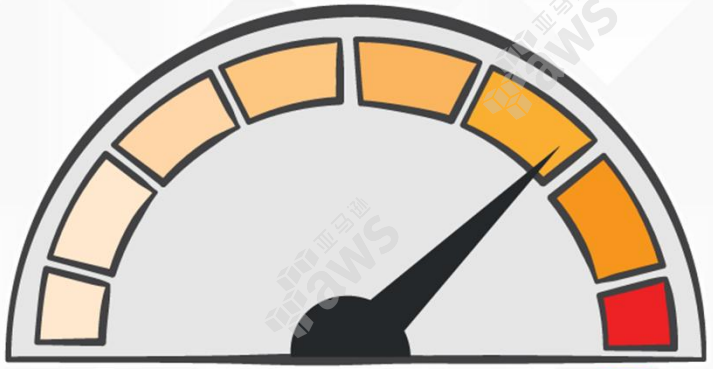
建议根据可用区查询

延迟 Latency

测量请求发送给后端实例至收到响应的时间开销

在故障分析时，分析最小值、平均值以及最大值，从而判断总体请求延迟情况

通过ELB访问日志，详细分析单个请求



波动队列SurgeQueue 和 溢出spillovers

波动队列长度表示无法及时被发送给后端实例的请求数量

最大长度为1,024每个ELB节点, 超出队列长度ELB会返回503错误

通常的原因是ELB无法与后端实例创建连接

表示应用处理能力需要扩展

访问日志 Access logs

- timestamp
- elb name
- client:port
- backend:port
- request_processing_time
- backend_processing_time
- response_processing_time
- elb_status_code
- backend_state_code
- received_bytes
- sent_bytes
- “request”
- “User-Agent”
- Ciphersuite
- SSL/TLS protocol version

2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000086 0.001048 0.001337 200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1” "curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2

全球扩展

结合Route 53进行多个Region的基于延迟或者地理位置的路由

可以有效降低应用延迟

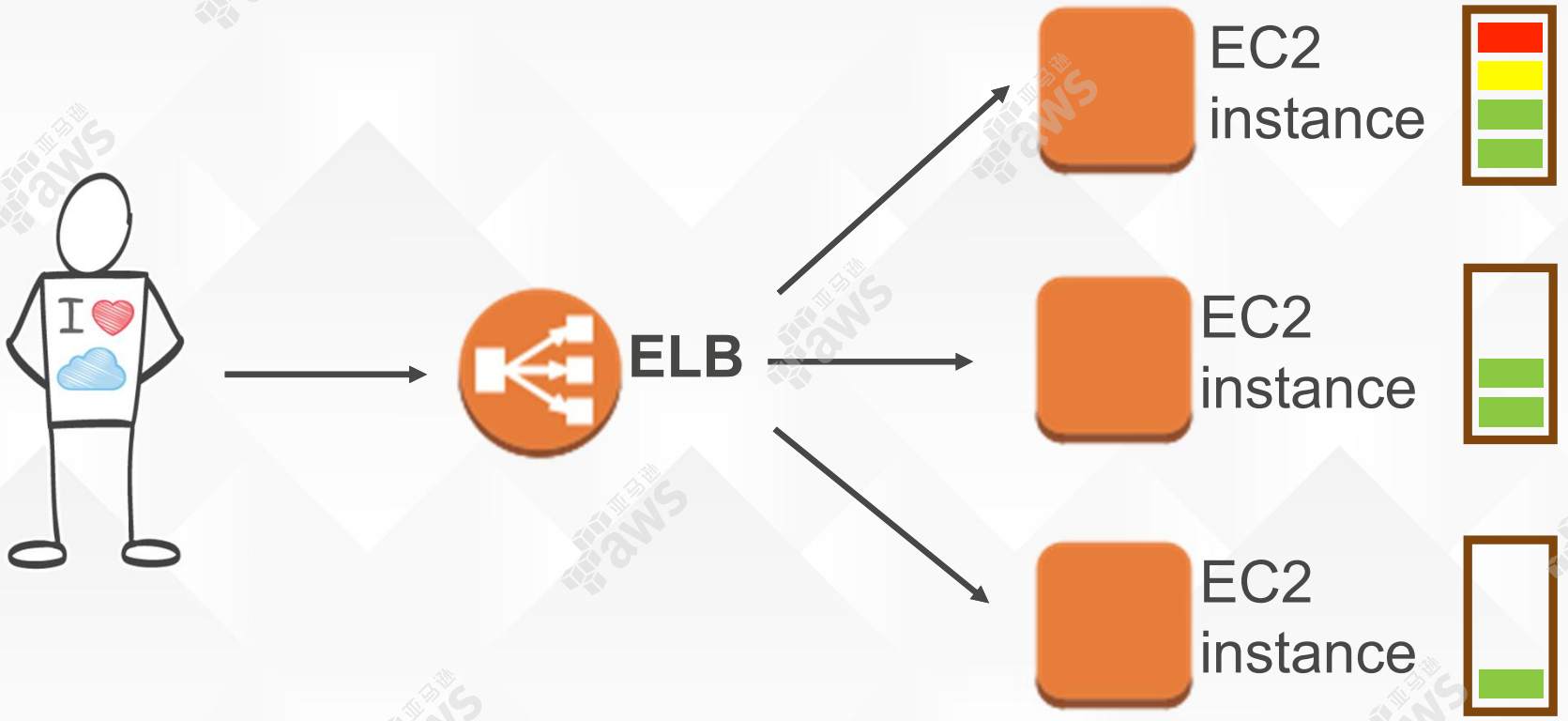
在线广告服务

交易平台

可用性

在进行系统维护时，在线替换后端实例，实现无缝切换

健康检查



健康检查

支持TCP及HTTP健康检查

自定义检查频率及失败阈值

HTTP检查必须返回2XX

如何进行更深层的健康检查

超过空闲超时时长 (Idle Timeout)后，不再被使用的连接会被ELB关闭

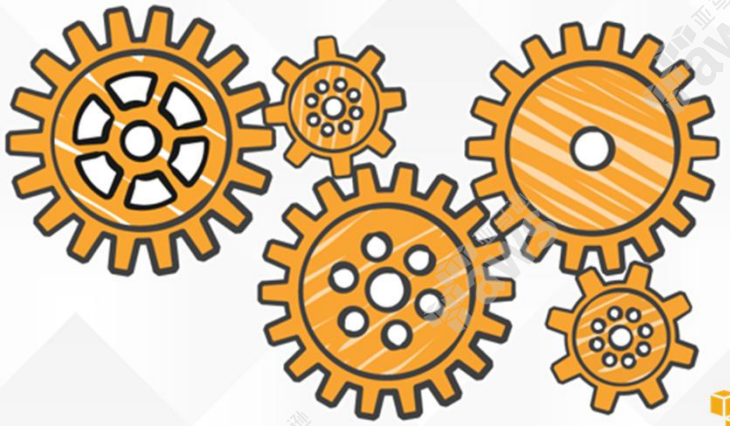
空闲超时 Idle timeouts

空闲连接会被保持的时长

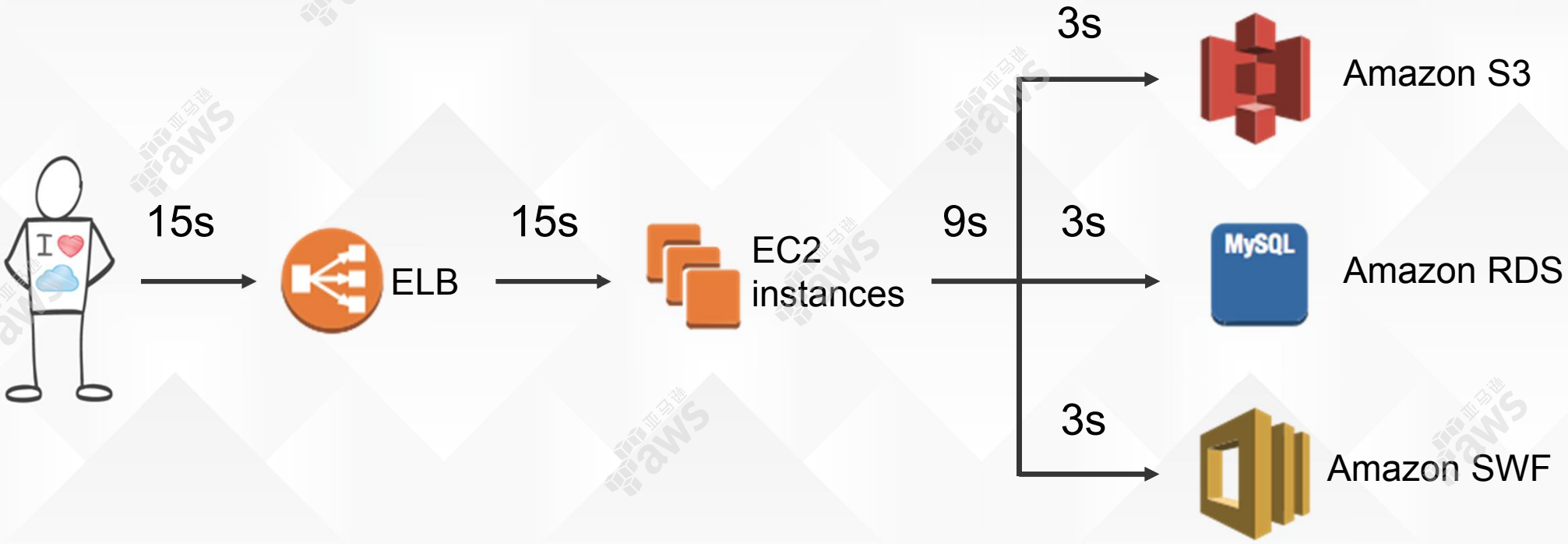
同时作用于客户端至ELB及ELB至后端实例的连接

默认为60秒，允许范围为最低1秒，最高3600秒

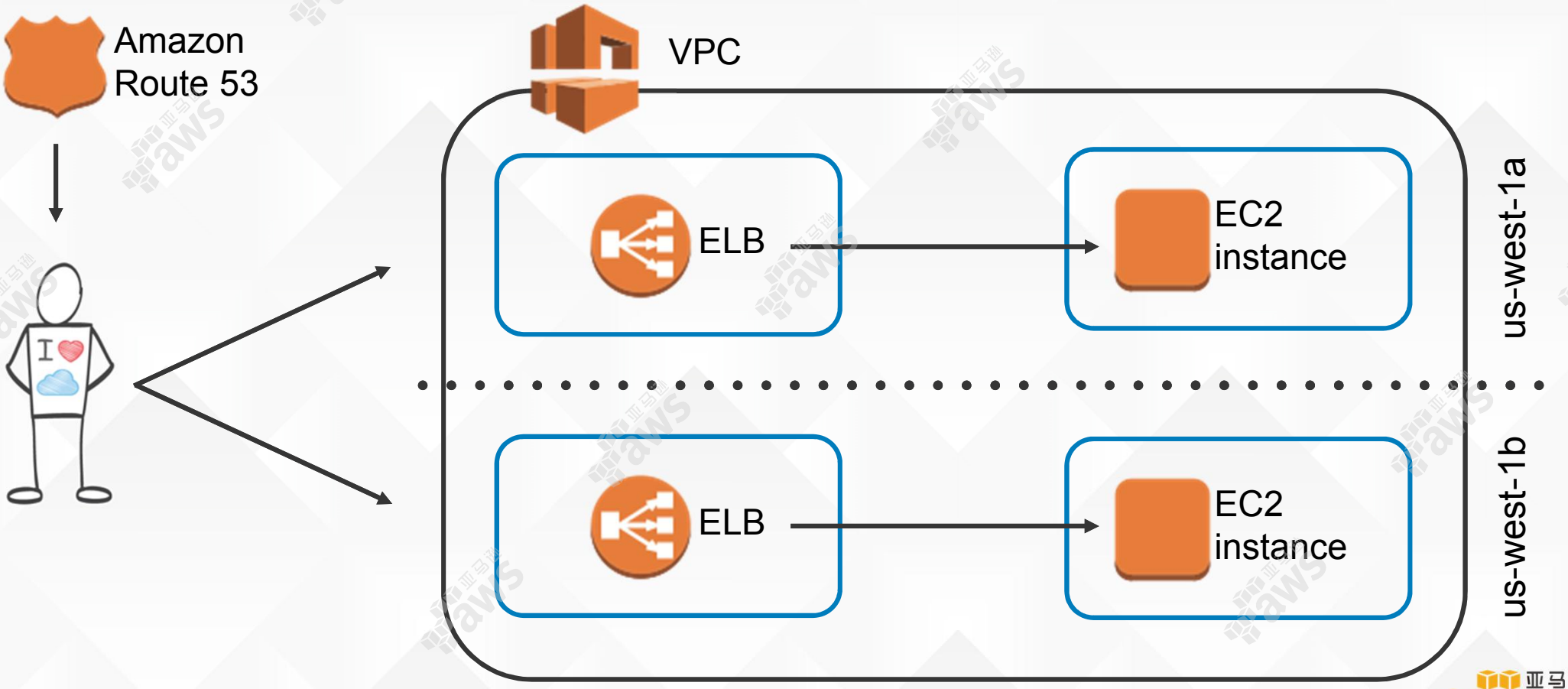
ELB超时时间<=应用超时时间



连接超时 Idle timeouts



多可用区部署


Amazon
Route 53
VPC
ELB
EC2
instance
ELB
EC2
instance
us-west-1a
us-west-1b

Route 53健康检查保障可用性

当某个可用区故障时，所有ELB自动扩展

Route 53发现可用区故障后，自动切走流量

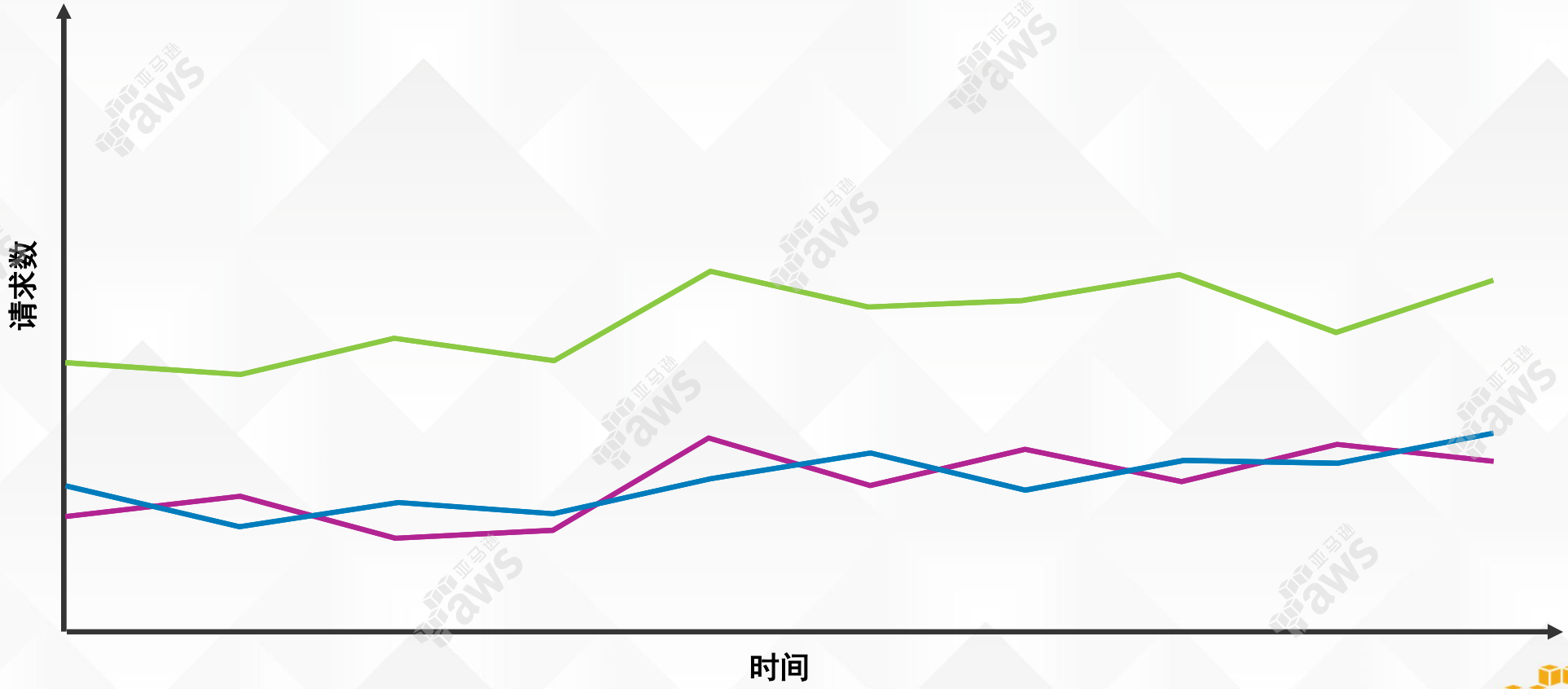
150秒内完成

不需要额外的控制层

为ELB添加至少2个位于不同可用区的子网

如何解决添加多可用区后可能会遇到的问题

负载不均衡



DNS 缓存以及分布

通常情况下DNS TTL会被遵守

有可能出现DNS数量不足，导致ELB节点收到的请求分布不均匀

移动网络通常有更多的DNS服务器

企业网络通常DNS服务器数量较少

DNS优化

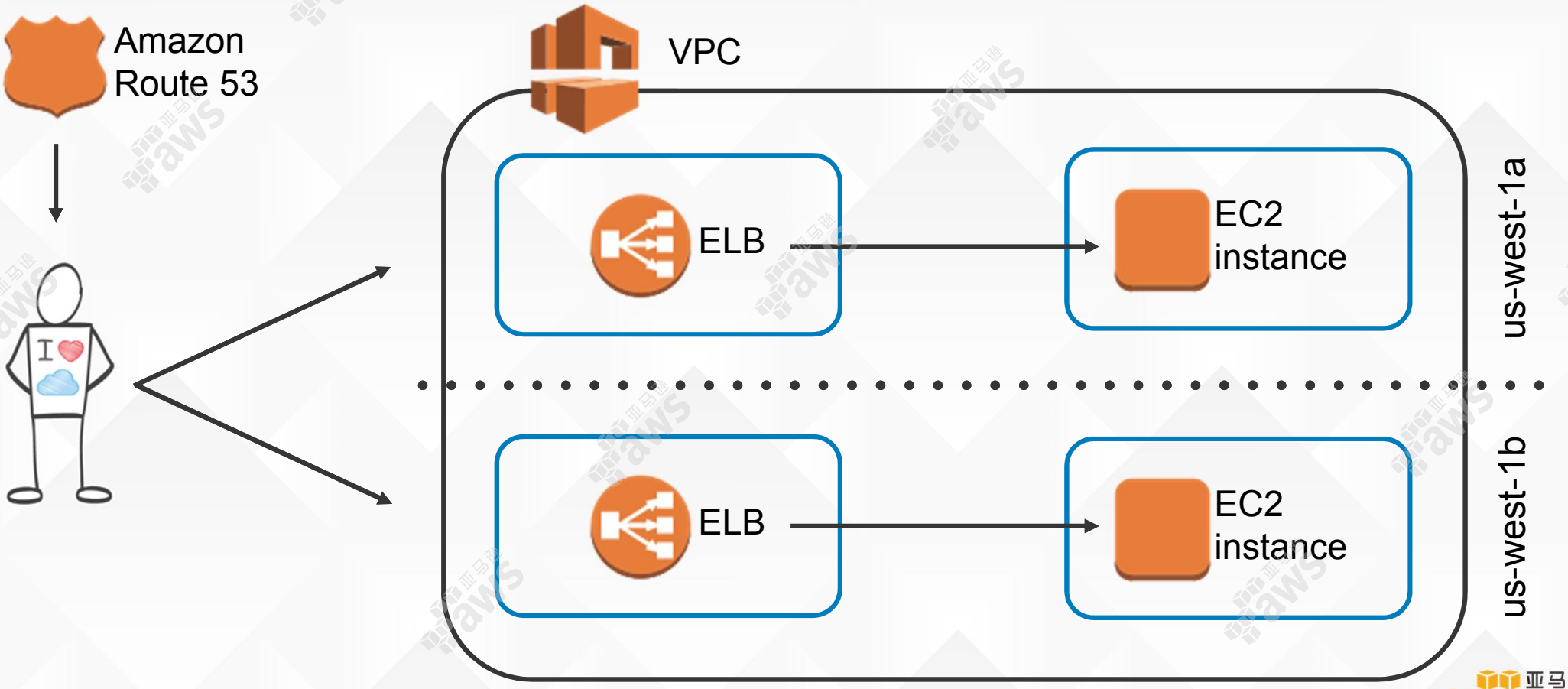
DNS缓存经常会造成客户端在一定时间内使用某一个特定IP地址

在Route 53上使用通配符作为CNAME或者ALIAS

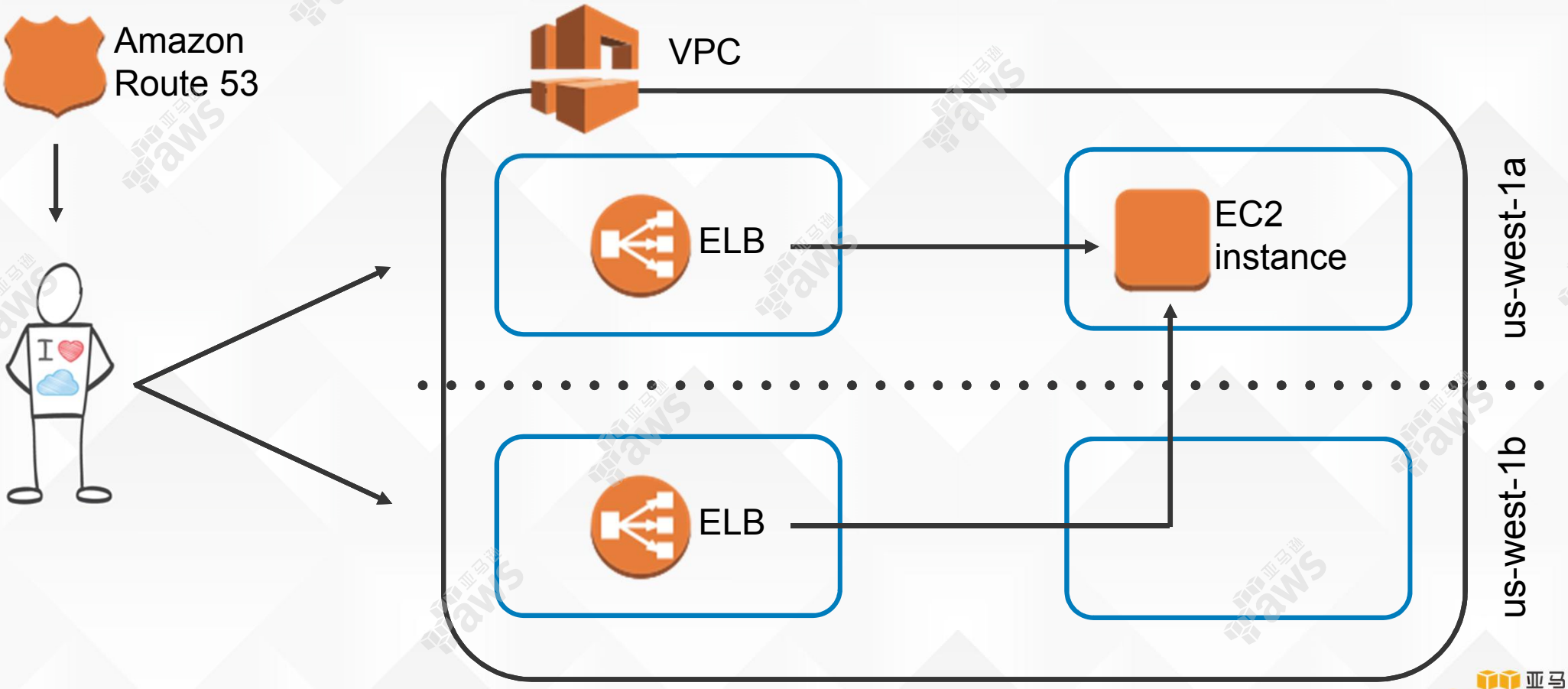
```
// Create a wildcard CNAME or ALIAS in Route 53.
*.example.com ALIAS … elb-12345.us-east-1.elb.amazon.com
*.example.com CNAME elb-12345.us-east-1.elb.amazon.com

// prepend random content for each lookup made by the application.
PROMPT> dig +short 25a8ade5-6557-4a54-a60e-8f51f3b195d1.example.com
192.0.2.1
192.0.2.2
```

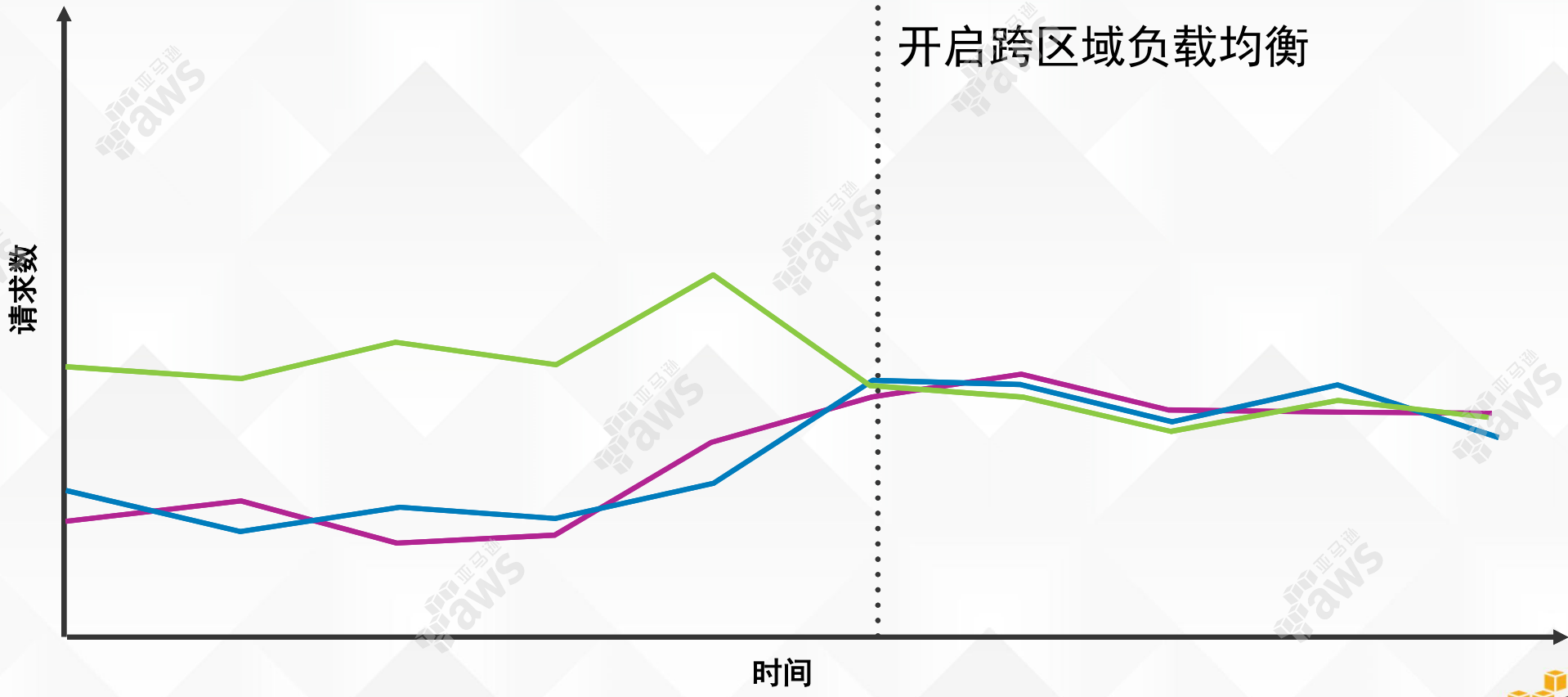
多可用区部署


Amazon
Route 53
VPC
ELB
EC2
instance
ELB
EC2
instance
us-west-1a
us-west-1b

多可用区部署



负载变化



跨区域负载均衡 Cross-zone load balancing

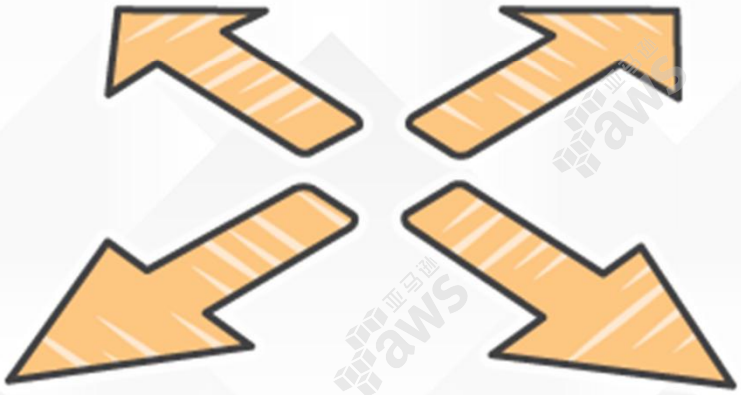
缓解DNS缓存造成的不均衡

消除后端实例负载不均衡

请求均匀地分发至多个可用区

开启前需要确认连接数限制

跨区域分发请求没有额外的带宽费用

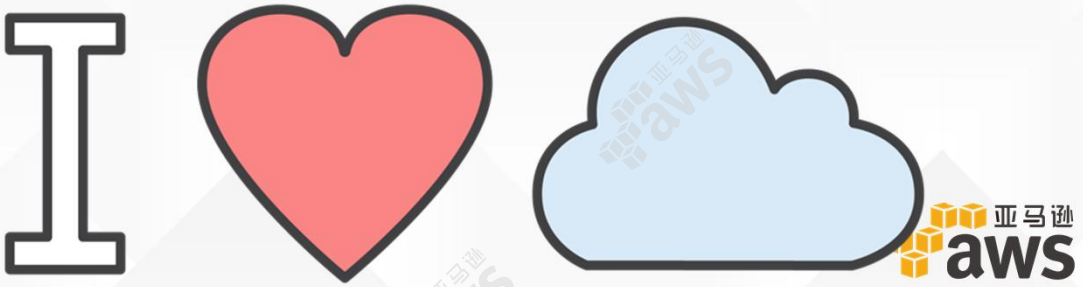


ELB 和 DevOps

可以被AWS CloudFormation, AWS Opsworks,
AWS Elastic Beanstalk, Amazon EC2 Container Service,
Amazon API Gateway, Asgard集成

可以作为蓝/绿部署网关

通过代码自动化管理ELB



Thank You