云上快速构建小程序创业

主讲人：祝犁

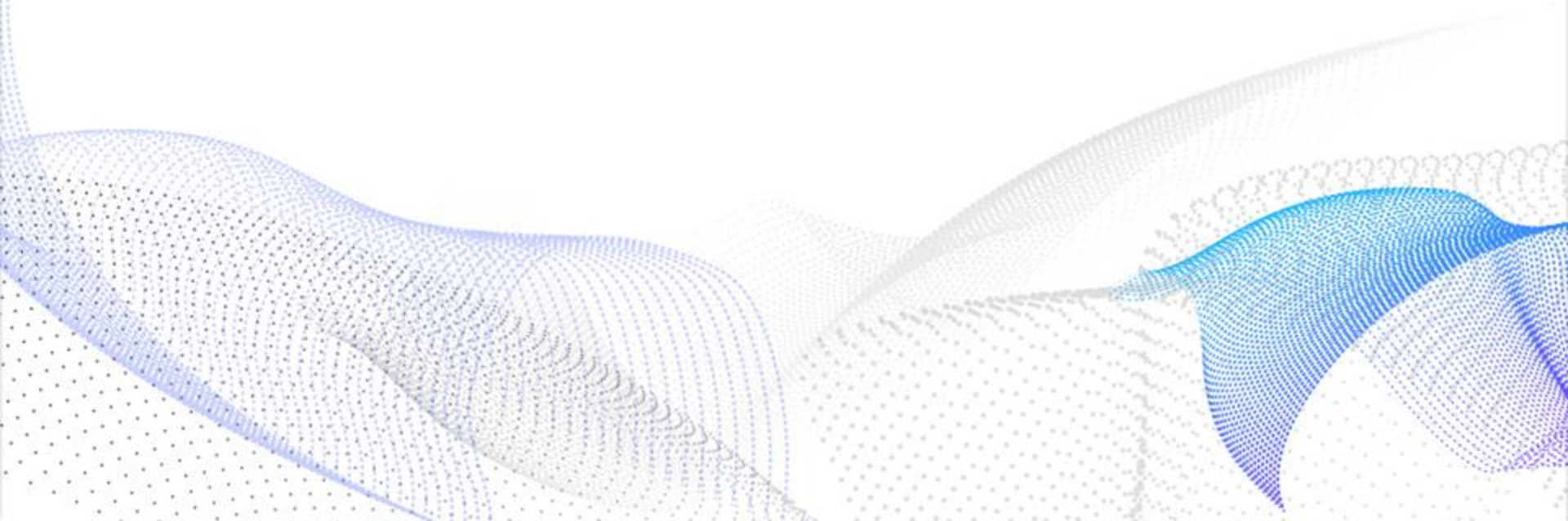
Agenda

- 云服务器选型
- 应用上云和云服务器管控
- 安全组管理
- 弹性和生命周期管理

Hello，云服务器

- 计算
  - CPU和内存
- 网络
  - 网络
  - 带宽
- 存储
  - 磁盘
  - 快照
  - 镜像
- 安全
  - 安全组
  - 秘钥对KeyPair

如何选择一款4C8G云服务器



云服务器选型-规格组简介

系列	常见规格组	CPU/内存	系统盘	数据盘	场景
通用型	n1,n2,n4	1:2 1:4	高效/SSD	高效/SSD	通用场景
内存型	e3,e4, se1	1:8	高效/SSD	高效/SSD	大量的内存操作、查找和计算的应用
均衡型	mn4	1:4	高效/SSD	高效/SSD	平衡计算、内存和网络资源有需求的应用场景
紧凑型	xn4	1:1	高效/SSD	高效/SSD	入门级计算需求, 测试环境，跳板机
企业型	sn1,sn2,se1	1:2 1:4 1:8	高效/SSD	高效/SSD	企业型,适合中大型应用
	i1	1:4	高效/SSD	高效/SSD/高性能SSD本盘	高性能数据库
	d1	1:4	高效/SSD	高效/SSD/高吞吐HDD本盘	hadoop大数据，日志
GPU	gn4,gn5,f1	1:7.5	高效/SSD	高效/SSD	适合依赖 GPU 进行学习

云服务器选型-存储

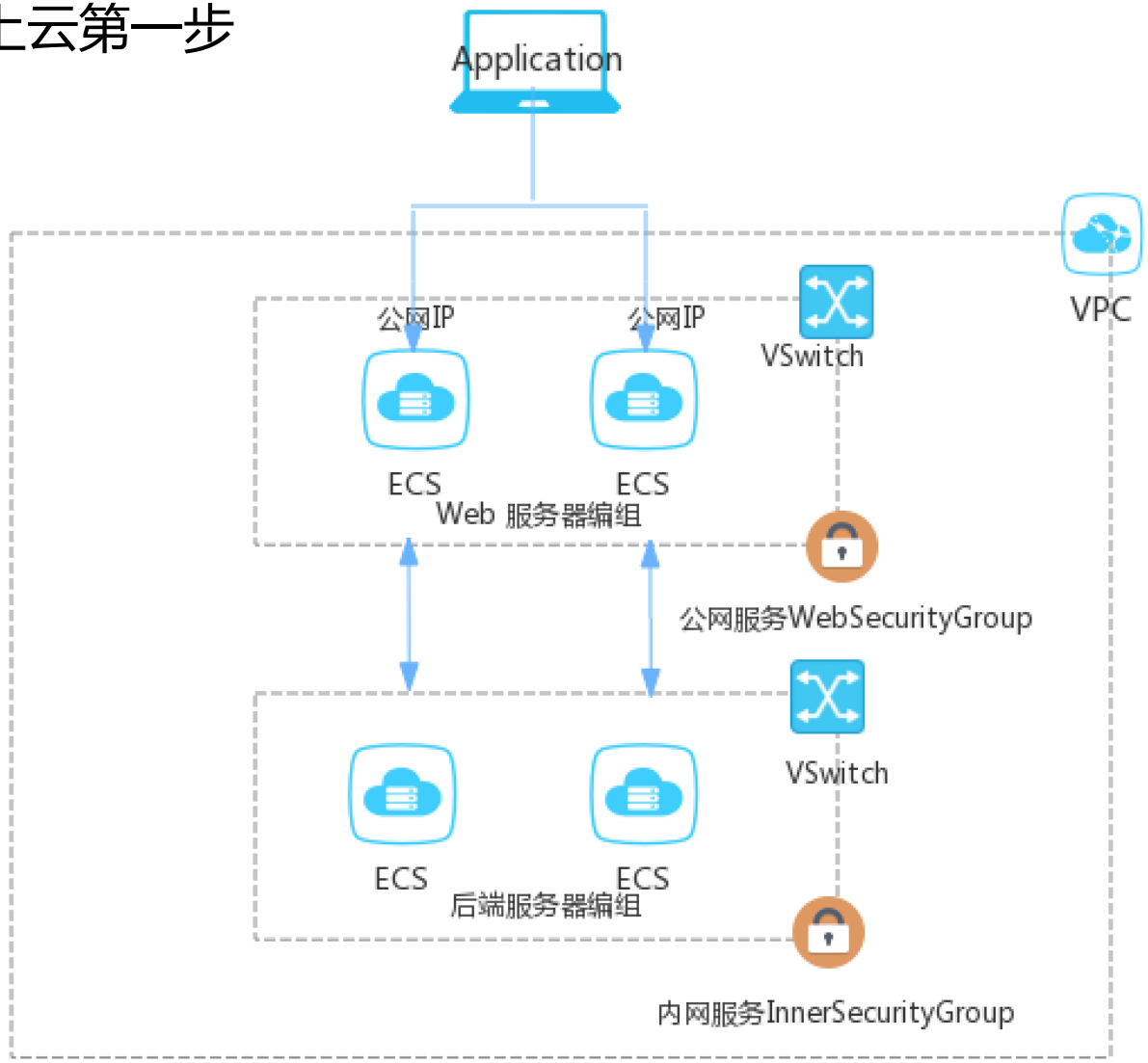
磁盘种类	可靠性	性能	容量	Latency	100GB月价
普通云盘	高	200~500 IOPS，30-50MBps	单磁盘5-2000GB	5~10ms	30元
高效云盘	高	3,000 IOPS， <=80MBps	单磁盘5-32768GB	1~3ms	35元
SSD云盘	高	20, 000 IOPS，256MBps 30 IOPS/GB，	单磁盘20-32768GB	0.5~2ms	100元
IO型实例存储（本地盘存储）	低	24万 IOPS/2000MBps	52-1556GB/Disk	0.2~0.5ms	Not For Individual Sale
容量型实例存储（本地盘存储）	低	5000MBps	6T-168T/实例	1ms	Not For Individual Sale 低至2元

4C8G的云服务器-选型规格和地域

实例规格	规格组	IO优化	存储	配置属性	网络性能	Turbo	NUMA	场景	月价
ecs.n4.xlarge	通用型n4	Y	40G高效云盘	Broadwell 2.5G DDR 4	高	Y	Y	通用入门级应用	401.60(vpc)
ecs.sn1.large	独享型sn1	Y	40G高效云盘	Broadwell 2.5G DDR 4	高	Y	Y	企业级中主频，计算密集	506.10(vpc)
ecs.c4.xlarge	计算型c4	Y	40G高效云盘	Broadwell 3.2G DDR 4	高	Y	Y	高主频，计算密集	698.00(vpc)
ecs.n1.large	通用型n1	Y	40G高效云盘	Haswell 2.5G DDR 4	中			通用入门级应用	382.60(vpc)
ecs.s3.large	1代	Y	40G高效云盘		中低			通用入门级应用	410.00
ecs.n4.xlarge（张家口）	通用型n4	Y	40G高效云盘	Broadwell 2.5G DDR 4	高	Y	Y	通用入门级应用	337.20(vpc)
ecs.sn1.large（张家口）	独享型sn1	Y	40G高效云盘	Broadwell 2.5G DDR 4	高	Y	Y	企业级中主频，计算密集	425.20(vpc)

注: 价格为华南-1，系统盘默认40GB。张家口机房有额外的20%优惠

上云第一步

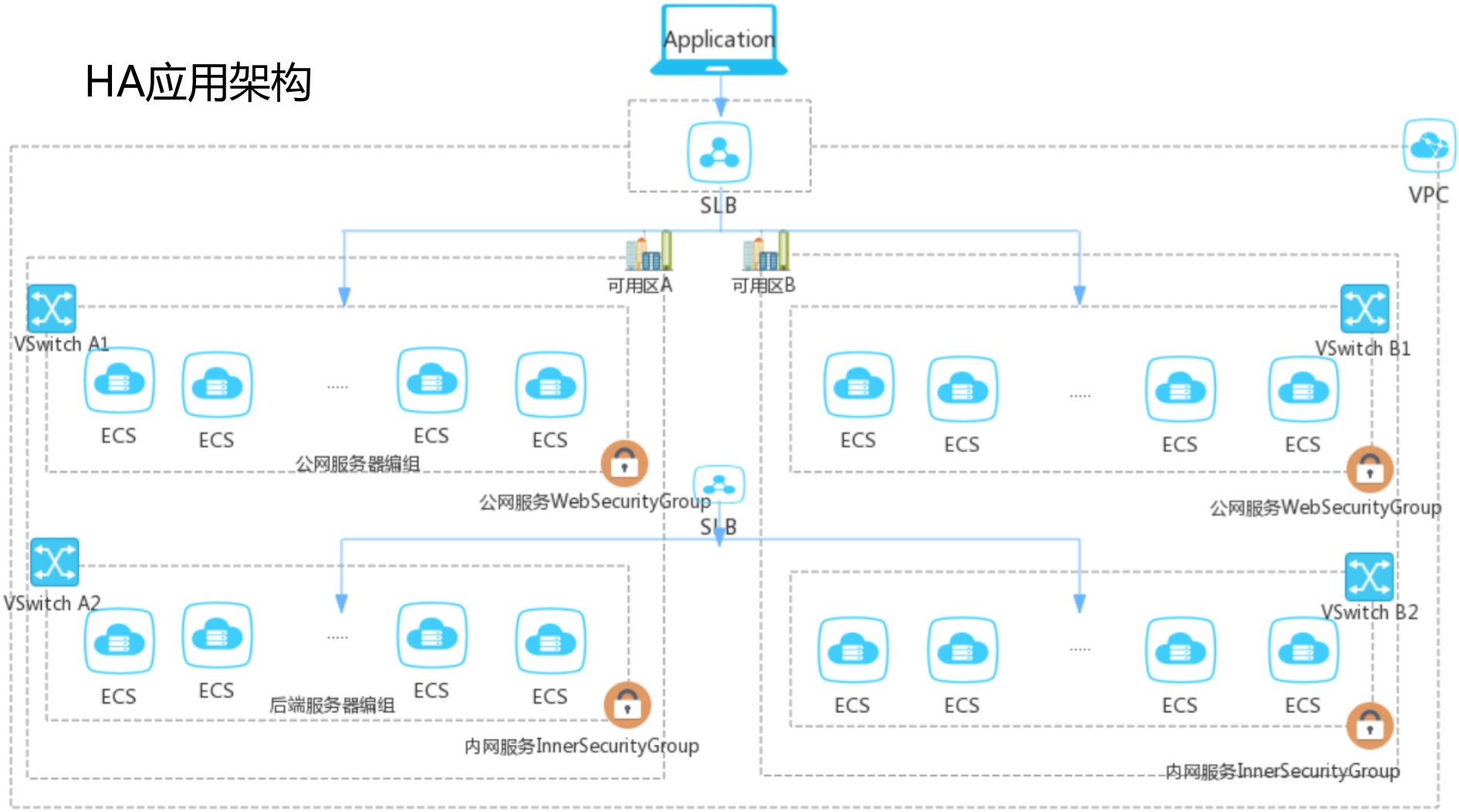


- 选择地域，例如杭州，创建VPC
- 两个子网，公网访问和内网访问
- 划分服务器编组
- 为不同的服务器编组提供不同的安全组

业务规模增长和线上大促

- 多环境
  - 测试环境，低配多套
  - 预发环境，尽量模拟生产环境，方便独立压测
  - 生产环境
- 避免单点构建HA架构
  - 负载均衡
  - 多可用区

HA应用架构


Application
SLB
VPC
可用区A
可用区B
VSwitch A1
VSwitch B1
ECS
公网服务器编组
公网服务WebSecurityGroup
SLB
VSwitch A2
VSwitch B2
后端服务器编组
内网服务InnerSecurityGroup

云服务器管控-分组管理

- 名称和描述
  - 可用性有局限
- TAG分组
  - 每个资源最多支持10个TAG
  - 支持实例、磁盘、快照、镜像、安全组
- 虚拟交换机（子网）
  - 承担不同的职责
- 划分安全组分组

云服务器管控

- ECS控制台登录的三种途径
  - 主账号
  - RAM子账号
  - STS角色扮演登录
- 操作
  - 短信风控
  - MFA多因素认证
- 监控
  - ECS查询监控信息API
  - 云监控配置监控大盘

OpenAPI权限设置

- 慎重分发主账号的AK
- RAM子账号做分权
  - 限制云资源的范围
  - 方便回收
  - 按需分配
- 子账号访问主账号资源时的鉴权规则
  - TAG授权

OpenAPI权限设置

- 授权子账号权限
  - ECS控制台操作权限
- 限制子账号可以登录和操作的范围
- 限制子账号的登陆账号源IP CIDR
  - 10.1.0.0/24

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "ecs:*",
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "*",
      "Resource": "*",
      "Effect": "Deny",
      "Condition": {
        "NotIpAddress": {
          "acs:SourceIp": [
            "YOUR COMPANY IP RANGE"
          ]
        }
      }
    }
  ]
}
```


Ooops, your files have been encrypted!
有没有恢复这些文档的方法？
当然有可恢复的方法。只能通过我们的解密服务才能恢复。我以人格担保，能够提供安全有效的恢复服务。
但这是收费的，也不能无限期的推迟。
请点击 <Decrypt> 按钮，就可以免费恢复一些文档。请您放心，我是绝不会骗你的。
但想要恢复全部文档，需要付款点费用。
是否随时都可以固定金额付款，就会恢复的吗，当然不是，推迟付款时间越长对你不利。
最好3天之内付款费用，过了三天费用就会翻倍。
还有，一个礼拜之内未付款，将会永远恢复不了。
对了，忘了告诉你，对半年以上没钱付款的穷人，会有活动免费恢复，能否轮到你，就要看您的运气怎么样了。
付款方法
我们只会接受比特币。不懂比特币是什么，请点击查看详情 <About bitcoin>。
不会购买比特币，请点击查看购买方法，<How to buy bitcoins>。
5/15/2017 17:53:09
Time Left
02:04:51:13
Your files will be lost on
5/19/2017 17:53:09
Time Left
06:04:51:13
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
@阿里云

安全组管理规则设置-封堵端口

授权策略	协议类型	端口范围	授权类型	授权对象	描述	优先级	创建时间	操作
拒绝	自定义 TCP	135/135	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
拒绝	自定义 TCP	42/42	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
拒绝	自定义 TCP	445/445	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
拒绝	自定义 TCP	137/137	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
拒绝	自定义 UDP	135/135	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
拒绝	自定义 TCP	139/139	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
拒绝	自定义 UDP	137/139	地址段访问	0.0.0.0/0	-	1	2017-05-18 22:43:53	修改描述 | 克隆 | 删除
允许	全部	-1/-1	地址段访问	0.0.0.0/0	-	100	2017-05-18 22:43:46	修改描述 | 克隆 | 删除

安全组管理

- 白名单机制
  - 尽量开通最小的权限，默认拒绝所有的访问
- 每个云服务器属于5个安全组，每个安全组100条规则
- 安全组规则变更备份和恢复

安全组管理-网段授权和组组授权

网卡类型: 内网

规则方向: 入方向

授权策略: 允许

协议类型: HTTP (80)

* 端口范围: 80/80

授权类型: 地址段访问

* 授权对象: 0.0.0.0/0 教我设置

优先级: 1

描述: 根据CIDR网段授权

长度为2-256个字符，不能以http://或https://开头。

网卡类型: 内网

规则方向: 入方向

授权策略: 允许

协议类型: HTTP (80)

* 端口范围: 80/80

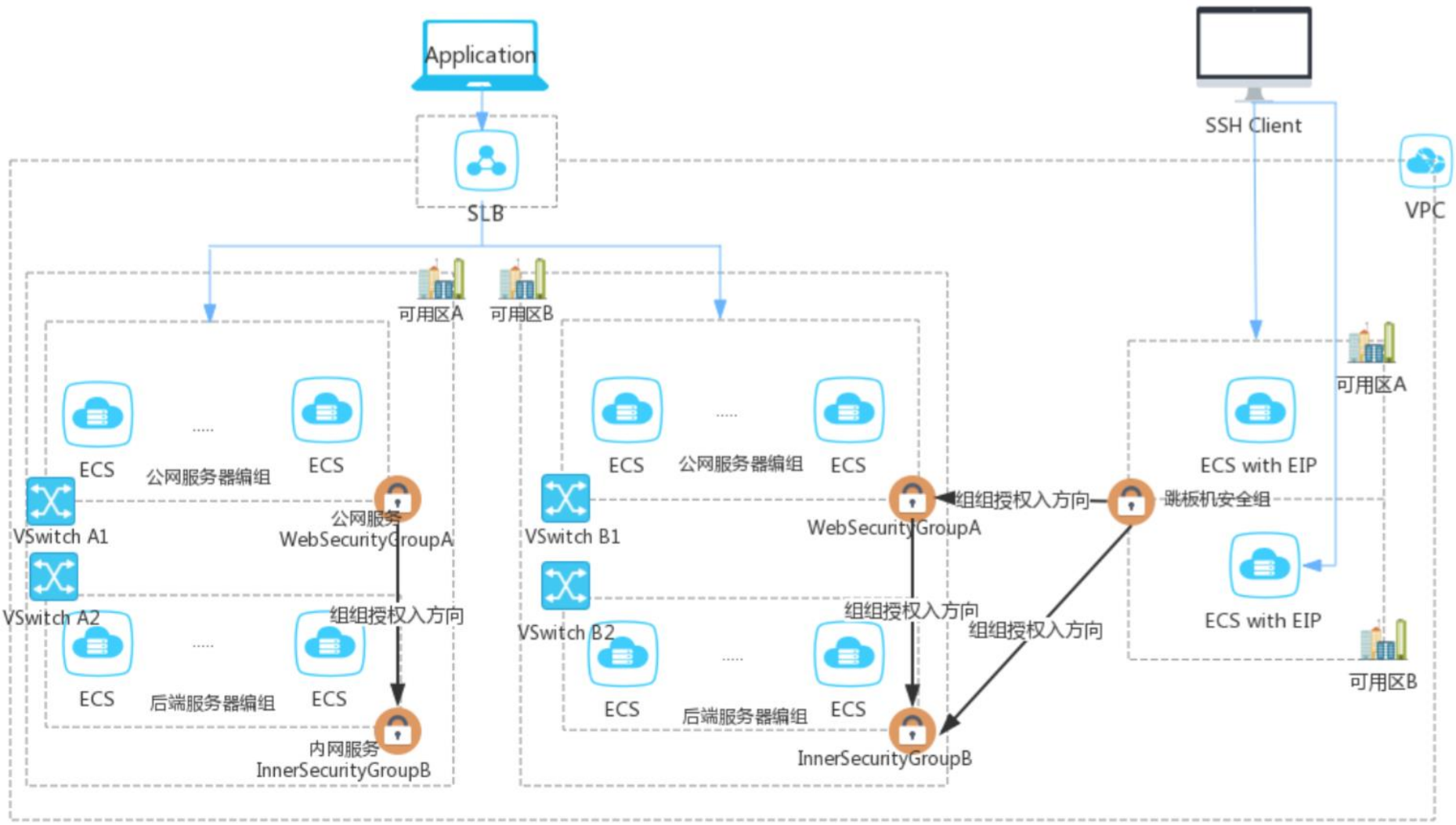
授权类型: 安全组访问 本账号授权 跨账号授权

授权对象: [redacted]

优先级: 1

描述: 跨安全组授权

长度为2-256个字符，不能以http://或https://开头。


Application
SLB
SSH Client
VPC
可用区A
可用区B
ECS
公网服务器编组
ECS
VSwitch A1
公网服务
WebSecurityGroupA
VSwitch A2
组组授权入方向
ECS
后端服务器编组
ECS
内网服务
InnerSecurityGroupB
ECS
公网服务器编组
ECS
VSwitch B1
WebSecurityGroupA
组组授权入方向
跳板机安全组
VSwitch B2
组组授权入方向
组组授权入方向
ECS
后端服务器编组
ECS
InnerSecurityGroupB
可用区A
ECS with EIP
ECS with EIP
可用区B

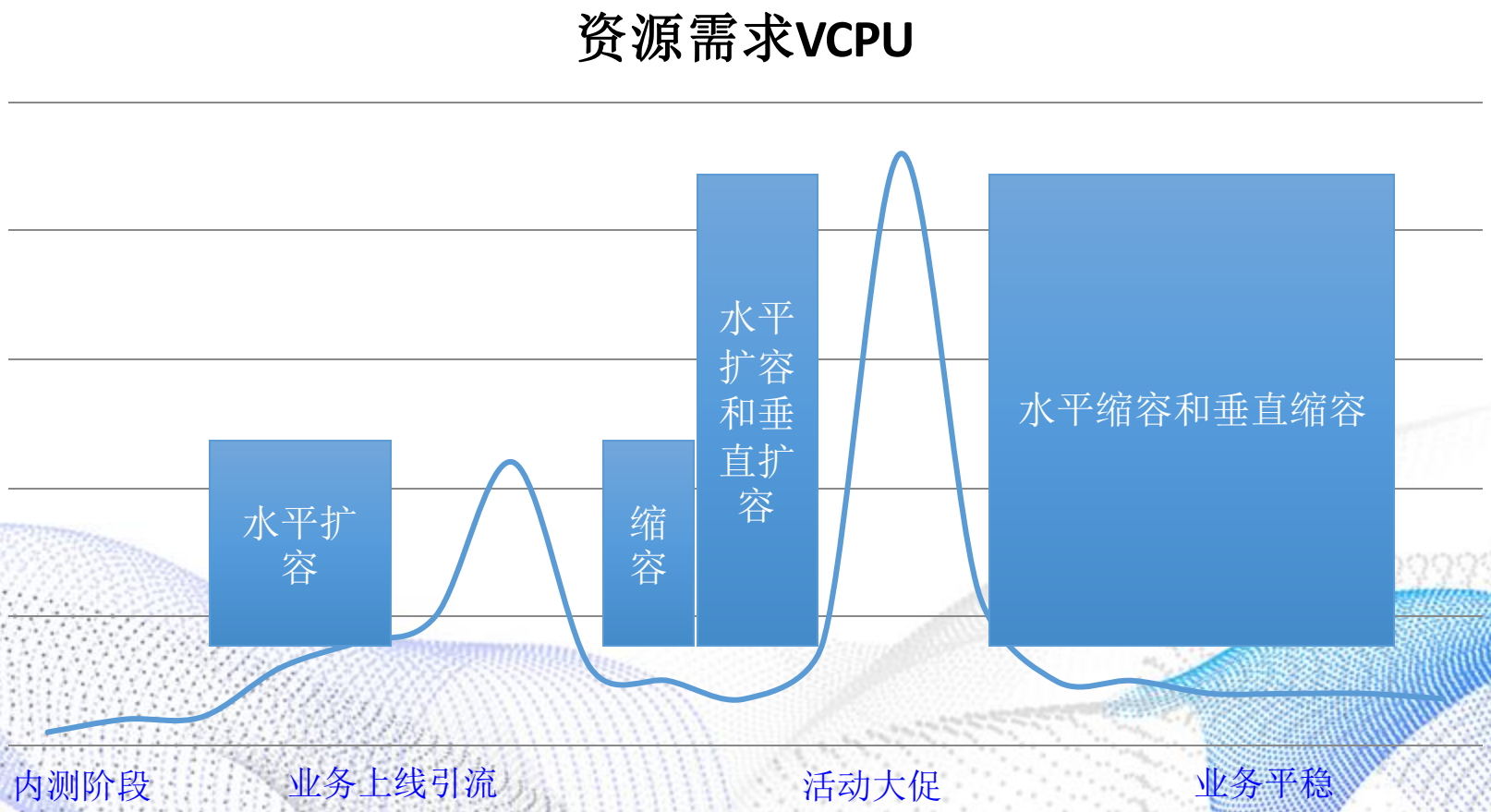
安全组管理-最佳实践

- 避免所有的资源归属于同一个安全组
  - 所有资源网络都通，不可控
  - 执行ACL变更变得不可控
- 提供公网服务的云服务器和内网服务器尽量属于不同的安全组
  - 公网服务的安全组规则应该最小集
- 不同的应用使用不同的安全组
  - Windows和Linux属于不同的安全组
- 生产环境和测试环境使用不同的安全组
- 仅对需要公网访问子网或者云服务器分配公网IP
  - 不提供公网服务不要分配

安全管理-跳板机

- 使用跳板机约束和审计可访问生产环境的权限
  - 多台跳板机避免单点
  - 使用单独的子网
  - 使用单独的安全组，限制公网入方向

弹性需求和弹性资源-成本篇



弹性计算扩容

- 新浪微博自动触发弹性创建和释放
  - 10分钟内完成上千台服务器创建
- 集团某BU弹性2小时创建8000台云服务器
  - 自动续费
  - 直接续费数千台实例

云服务器弹性能力-按需付费

- ECS控制台
- OpenAPI结合自身创建和释放
  - 创建按量和包年包月实例 CreateInstance
  - 删除按量实例 DeleteInstance
  - 设置按量实例定时释放 ModifyInstanceAutoReleaseTime
- 弹性伸缩AutoScaling
  - 定时任务
  - 报警任务

云服务器弹性能力-弹性变配

- 实例配置
  - 实时升级配置
  - 实时降级配置
  - 预约降配
  - 按量付费转包年包月
  - 设置和取消自动续费
- 带宽
  - 永久升级
  - 临时升级
  - 带宽付费方式转换，从固定带宽到按量
  - 带宽付费方式转换，从按量到固定
- 存储
  - 磁盘扩容
  - 包年包月磁盘转按量磁盘
  - 按量磁盘转包年包月

总结

- 工欲善其事必先利其器，依据场景选对地域规格很重要
- 做好服务器分组
- 良好的安全组的配置不仅仅安全，更方便梳理各个系统的边界
- 弹性能力是您的成本利器
  - 按需扩容
  - 按需缩容
  - 弹性变配

2017云栖大会·成都峰会
THE COMPUTING CONFERENCE
阿里云

飞天·智能

APSARA INTELLIGENCE

2017云栖大会·成都峰会

5月23日 成都世纪城天堂洲际大酒店