

老男孩教育77期-阿里云-从入门到放弃

老男孩教育77期-阿里云-从入门到放弃

0. 概述

1. 阿里云架构

2. 术语

3. ecs使用指南☆☆☆☆☆

4. 创建快照

5. rds

6. ram权限控制☆☆☆☆☆

6.1 创建用户组及用户

6.2 授予权限

7. oss

7.1 nas vs oss☆☆☆☆☆

7.2 创建bucket

7.2 应用

8. slb

8.1 slb概述

8.2 clb

8.3 alb

8.4 alb clb 小结☆☆☆☆☆

9. DNS (云解析DNS)☆☆☆☆☆

10. 安全

10.1 安全组☆☆☆☆☆

10.2 云安全中心（态势感知）☆☆☆☆☆:star2:

10.3 waf防火墙☆☆☆

11. cdn

12. ess

13. 总结

0. 概述

- 阿里云架构
- 阿里云必备产品
- slb(clb),alb,cdn,waf
- ecs(镜像, 快照, 磁盘,)
- rds,oss,nas
- ess,ram...nat网关
- 态势感知

- 算钱

1. 阿里云架构

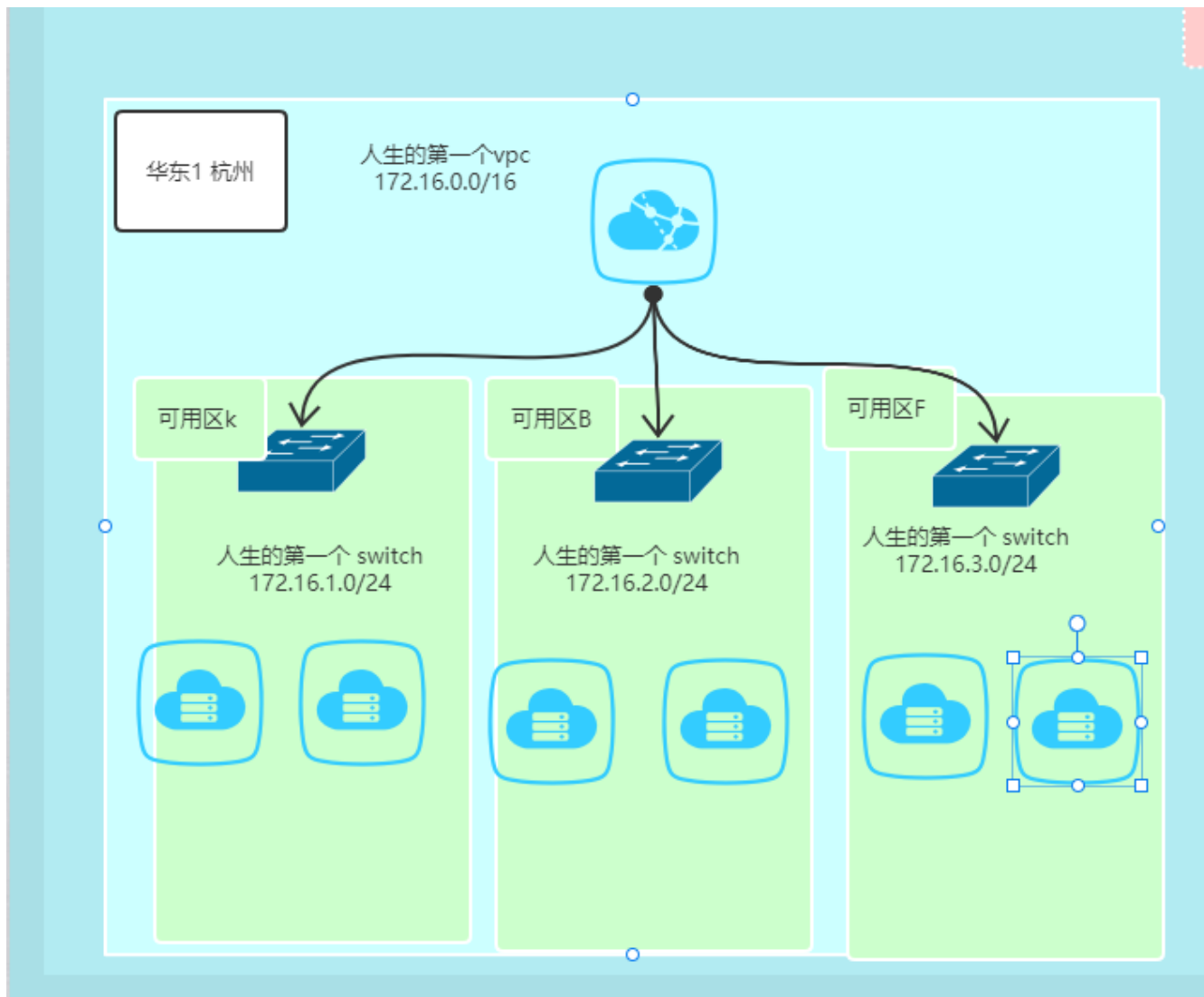
2. 术语

术语		
实例	阿里云中的一个功能	
实例id	阿里云中各种产品的唯一标记	
释放	删除	
安全组	防火墙，默认是白名单	
oss中的bucket	存放数据的空间的名字bucket	

3. ecs使用指南☆☆☆☆☆

- ☐ 创建使用ecs，vpc,安全组，实例配置
- ☐ 快照，镜像，
- ☐ 磁盘挂载与维护

	地域 (region)	可用区(zone)
含义	不同的区域，北京 上海 杭州 深圳。。。	同一个地域的不同机房
	不同地域内网，不通	同一个地域的不同可用区，内网是互通



← 创建专有网络

专有网络

地域

华东1 (杭州)

* 名称

oldboy77-vpc

12/128

* IPv4网段

建议您使用RFC私网地址作为专有网络的网段如 10.0.0.0/8 , 172.16.0.0/12 , 192.168.0.0/16 。网段配置建议

172.16.0.0/12

一旦创建成功，网段不能修改

IPv6网段

分配 (默认)

2408:4005:36c:4800::/56

系统将为您自动创建免费版的IPv6网关

描述

0/256

交换机

创建交换机

删除

名称

switch-e-1

10/128

可用区

杭州 可用区E

可用区资源

ECS

RDS

SLB

IPv4网段

网段配置建议

172

16

1

0

/

24

一旦创建成功，网段不能修改

可用IP数

252

IPv6网段

2408:4005:36c:48

1

::/

64

请输入数字0-255

专有网络架构预览



← 创建专有网络

✔ 专有网络VPC实例与相关交换机创建成功!

您已成功创建该专有网络VPC实例与相关交换机。

专有网络ID 创建状态	vpc-bp1vhu6xw5eimgiu319if ✔ 创建成功	实例名称	oldboy77-vpc
创建NAT网关 查看专有网络详情			
交换机ID 实例名称	vsw-bp1evt0c9t6hlu3ehvioj switch-e-1	可用区 创建状态	杭州 可用区E ✔ 创建成功
添加云产品 查看交换机详情			
交换机ID 实例名称	vsw-bp13kpmu9ejx0jdgizk2n switch-b-2	可用区 创建状态	杭州 可用区B ✔ 创建成功
添加云产品 查看交换机详情			

ecs-buy.aliyun.com/wizard/spm=51/b.13329450.home-res.buy.15414d15dfliq8#/postpay/cn-hangzhou?orderSource=buyWizard-console-overview

阿里云 账号全部资源

云服务器 ECS 一键购买 自定义购买

网络 经典网络 ①

如何选择网络

oldboy77-vpc / vpc-bp1vhu6xw5eimgiu319if

switch-e-1 / vsw-bp1evt0c9t6hlu3ehvioj

可用私有IP数量 252 个

如需创建新的专有网络，您可 [前往控制台创建](#)

交换机所在可用区：华东 1 可用区 E 交换机网段：172.16.1.0/24

仅单向收取流出流量费用，流入流量免费

公网流量费用按实际使用流量收费，每小时扣费。仅单向收取流出流量费用，流入流量免费。例如您在 1 小时内公网流出流量为 6.51GB，收取费用为 6.51GB * 0.8 元 / GB = 5.20 元（注：不同地域“公网流量费用”的单价略有不同，实际价格请参照“当前配置”的报价）

安全组

安全组限制
配置安全组

[重新选择安全组](#)

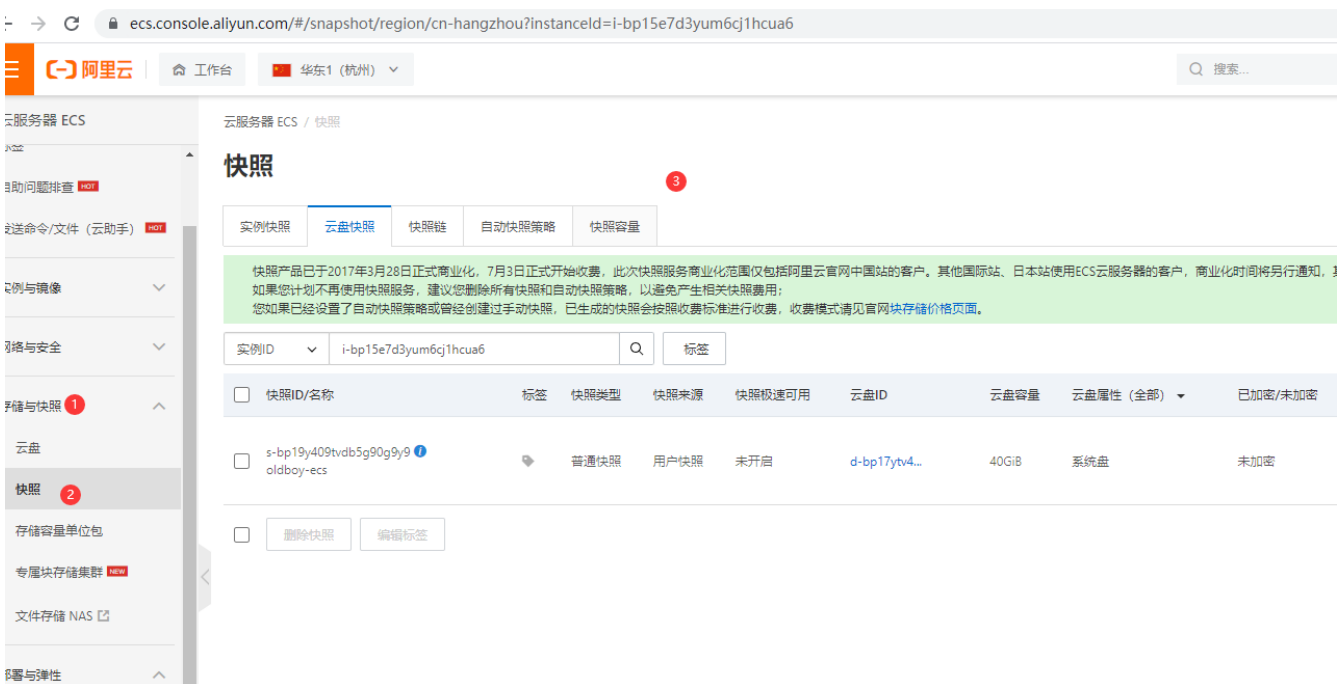
① 安全组类似防火墙功能，用于设置网络访问控制。您也可以到管理控制台 [新建安全组](#) [安全FAQ](#)

所选安全组 1)。默认安全组（自定义端口）

请确保所选安全组开放包含 22（Linux）或 3389（Windows）端口，否则无法远程登录ECS。您可以进入ECS控制台设置。[前往设置](#)

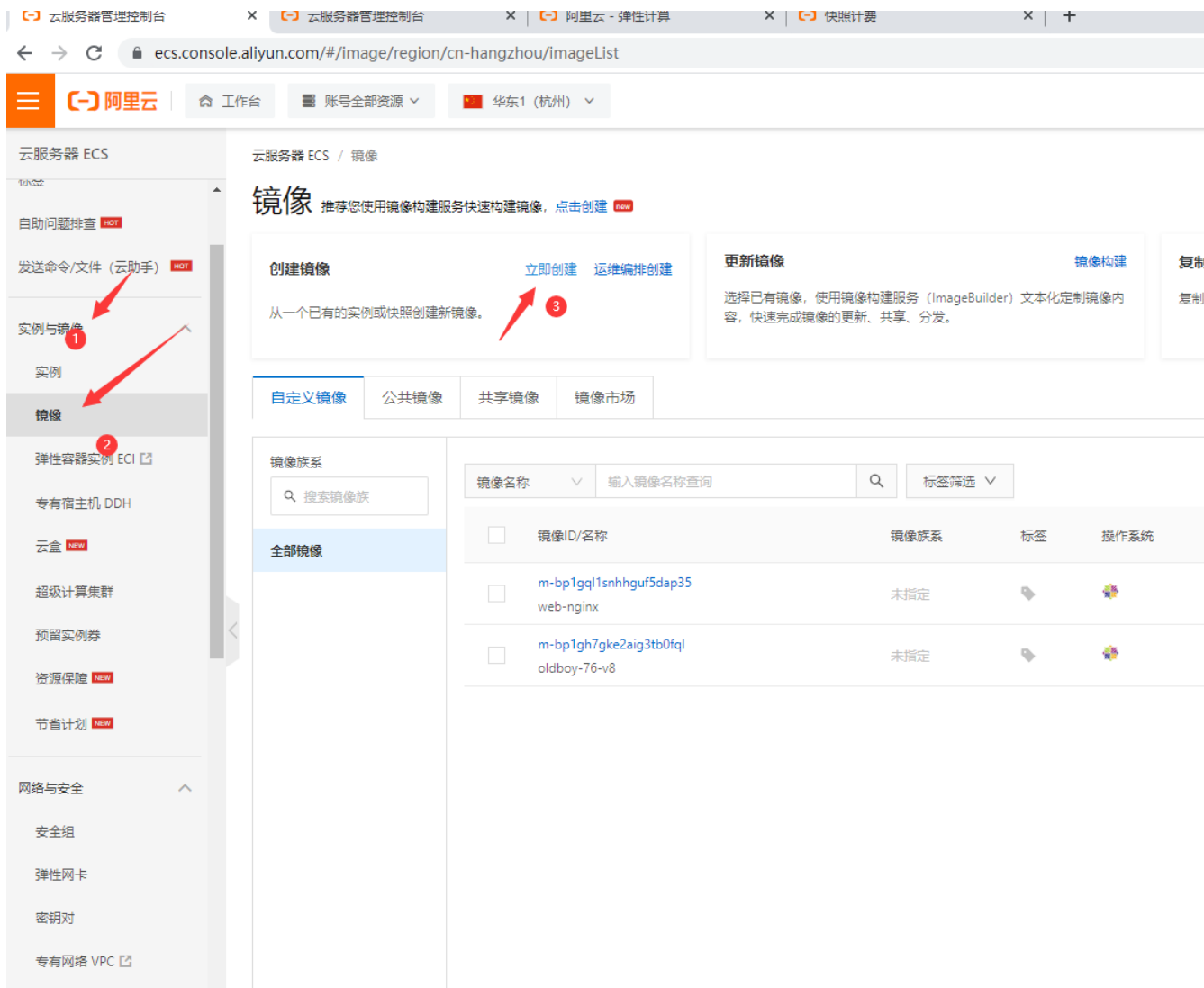
请勾选要开通的IPv4的协议/端口：① ☒ HTTP 80 端口 ☒ HTTPS 443 端口 ☒ 22 端口 ☒ 3389 端口 ☒ ICMP 协议 ②

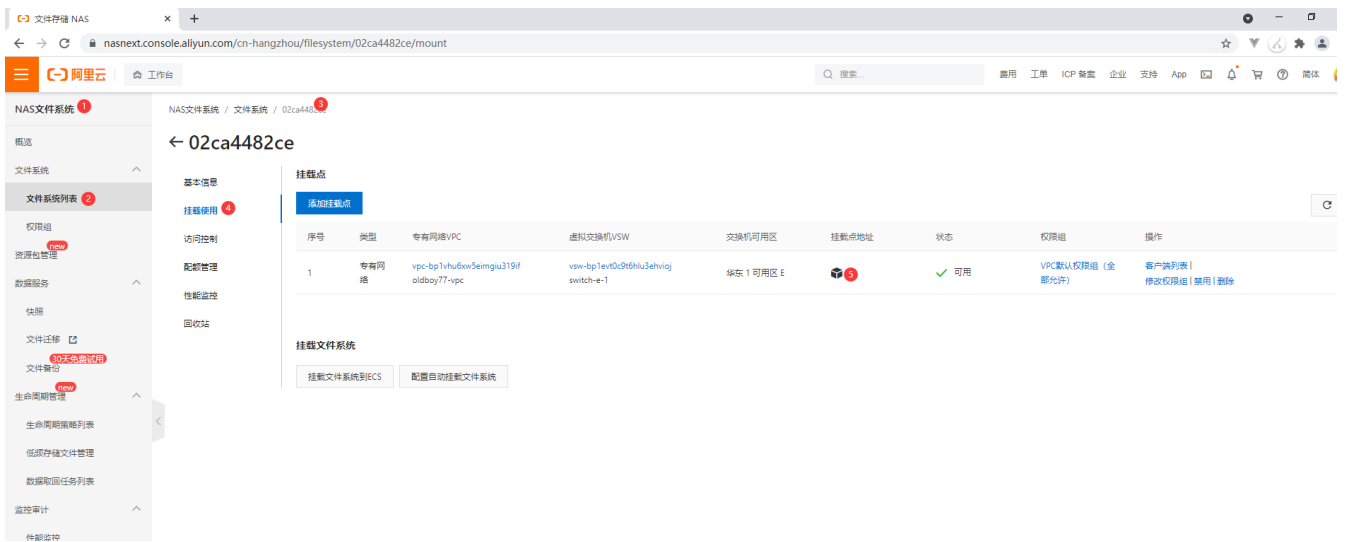
4. 创建快照



```
yum install -y nginx mariadb-server php.x86_64 php-bcmath.x86_64 php-cli.x86_64 php-common.x86_64 php-dba.x86_64 php-debug.x86_64 php-devel.x86_64 php-embedded.x86_64 php-enchant.x86_64 php-fpm.x86_64 php-gd.x86_64 php-gmp.x86_64 php-intl.x86_64 php-json.x86_64 php-ldap.x86_64 php-mbstring.x86_64 php-mysqld.x86_64 php-odbc.x86_64 php-opcache.x86_64 php-pdo.x86_64 php-pgsql.x86_64 php-process.x86_64 php-recode.x86_64 php-snmp.x86_64 php-soap.x86_64 php-xml.x86_64 php-xmlrpc.x86_64

yum install -y nc dos2unix unzip wget lrzsz bash-completion
systemctl enable nginx mariadb php-fpm.service
```





- ecs
- nas
- 快照---->镜像

5. rds



创建账号

* 数据库账号

oldboy

由小写字母、数字、下划线（_）组成，以字母开头，以字母或数字结尾，最多32个字符

* 账号类型 ?

☒ 高权限账号 ☐ 普通账号

[自定义权限](#)

* 密码

.....

必须包含三种及以上类型：大写字母、小写字母、数字、特殊符号。长度为8~32位。特殊字符包括! @ # \$

* 确认密码

.....

备注

备注说明最多256个字符

确定

取消

* 数据库账号

cloud

数据库账号重复

由小写字母、数字、下划线 (_) 组成，以字母开头，以字母或数字结尾，最多32个字符

* 账号类型 ?

☐ 高权限账号

☒ 普通账号

授权数据库:

未授权数据库

请输入



☐ cloud



☐ 1 项

已授权数据库 [查看权限列表](#)

全部设 [读写 \(DDI](#)

请输入

☐ 0 项

自定义权限

* 密码

密码不能为空

必须包含三种及以上类型：大写字母、小写字母、数字、特殊符号。长度为8~32位。特殊字符包括! @ # \$ % ^ & * () _

* 确认密码

备注

备注说明最多256个字符

确定

取消

创建数据库



* 数据库 (DB) 名称

cloud

由字母、数字、下划线 (_)、中划线 (-) 组成, 以字母或数字开头, 字母或数字结尾, 最多64个字符

* 支持字符集

utf8

授权账号

cloud(普通账号)

[创建新账号](#)

账号类型

☒ 读写 ☐ 只读 ☐ 仅DDL ☐ 仅DML

备注说明

0/256

备注说明最多256个字符

创建

取消

每天10点, MySQL、Redis、PolarDB、MongoDB爆款规格限量抢购, 低至199元/年, [点击前往查看](#)

云数据库RDS / 实例列表 / 数据库连接

[升级为PolarDB](#) [经典网络平滑迁](#)

← oldboy-rds01 (✓ 运行中) ▾

[导出数据库](#)[构建数仓](#)[操作指引](#)[重置实例](#)[备份实例](#)

基本信息

账号管理

数据库管理

备份恢复

[数据库连接](#)

数据库代理

监控与报警

数据安全

服务可用性

日常运维

SQL洞察

参数设置

自治服务

一键诊断

性能趋势

慢SQL

SQL洞察和审计

诊断报告

数据库连接

[切换交换机](#) | [切换为经典网络](#) | [修改连接地址](#) | [申请外网地址](#) | [如何连接RDS](#) | [为什么连接不上](#)

网络类型

专有网络(VPC)oldboy77-vpc / vpc-bp1vhu6wx5eimgu319tf

数据库代理状态 (原高安全模式)

未开通

内网地址

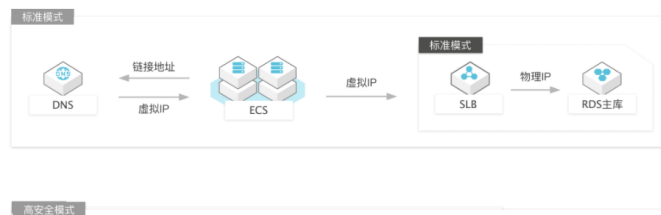
设置白名单后才显示地址

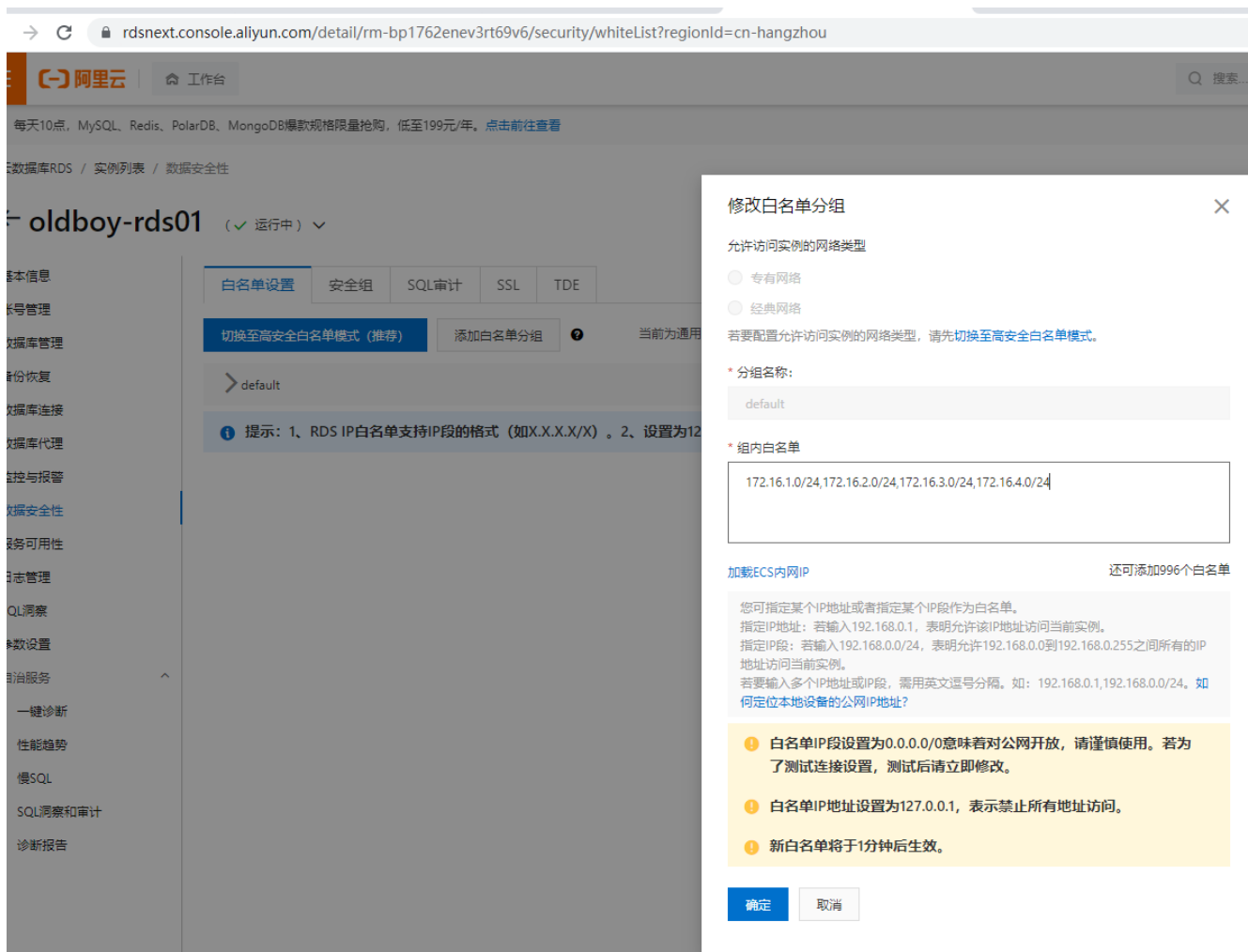
内网端口

3306

请使用内网连接本进行实例连接。连接本对应的IP地址不固定, 会发生变化。

访问模式结构图





6. ram权限控制 ☆☆☆☆☆

- 权限控制，类似于sudo
- 开发人员，新入职的运维人员，授权ram权限和用户。普通用户。
- 应用场景：
 - 创建ram用户给开发人员：access id 和secret
 - 创建ram用户权限部分阿里云功能，给某个用户、用户组
- 授权的方案：
 - 根据用户组进行授权，如果有特殊需求精确到用户授权。

6.1 创建用户组及用户



- 控制台访问-web页面查询，查看信息使用
- API调用（开发使用），开发程序代码中代用，资源

← 创建用户

用户账号信息

* 登录名称 [?]

dev-rds

@oldboyedu.onaliyun.com

* 显示名称 [?]

dev-rds

dev-oss

@oldboyedu.onaliyun.com

dev-oss

×

+ 添加用户

访问方式 [?]

☒ 控制台访问 用户使用账号密码访问阿里云控制台

☒ Open API 调用访问 启用 AccessKey ID 和 AccessKey Secret，支持通过 API 或其他开发工具访问

控制台密码

☐ 自动生成密码

☒ 自定义密码

.....



需要重置密码

☐ 用户在下次登录时必须重置密码

☒ 无需重置

MFA 多因素认证

☐ 需要开启 MFA 认证

☒ 无需开启

确定

返回

配置费用：

您没有权限询价，请联系主账号前往 RAM 控制台授权，需要授权的 Action 为 `ecs:DescribePrice`

- 用户与用户组关联

RAM 访问控制 / 用户组 / dev

← dev

组基本信息

编辑基本信息

组名称

dev

复制

显示名称

dev

备注

development开发组

组成员管理

权限管理

添加组成员

用户登录名称/显示名称	备注	加入时间
dev-oss@oldboyedu.onaliyun.com dev-oss		2021年8月23日 11:06:55
dev-rds@oldboyedu.onaliyun.com dev-rds		2021年8月23日 11:06:55

6.2 授予权限

Q 搜索... 费用 工单 ICP 备案 企业 支持 App 消息 购物车 帮助 简体

RAM 访问控制

添加权限

指定资源组的授权生效前提是该云服务已支持资源组，查看当前支持资源组的云服务。[前往查看](#)

单次授权最多支持 5 条策略，如需绑定更多策略，请分多次进行。

* 授权范围

☒ 整个云账号

☐ 指定资源组

请选择或输入资源组名称进行搜索

* 授权主体

dev@group.oldboyedu.onaliyun.co... X

* 选择权限

系统策略 自定义策略 + 新建权限策略

ecs

权限策略名称	备注
AliyunECSFullAccess	管理云服务器服务(ECS)的权限
AliyunECSReadOnlyAccess	只读访问云服务器服务(ECS)的权限
AliyunECSNetworkInterfaceM...	管理ECS弹性网卡的权限
AliyunECSAssistantReadonly...	查看云助手命令和在云服务器服务（ECS）上执行记录的权限
AliyunECSAssistantFullAcce...	管理云助手命令和向云服务器服务（ECS）内发送命令的权限

请选择权限

已选择 (0)

清空

确定

取消

- fullaccess 这个资源的所有权限都给你
- readonly 这个资源的只读权限

添加权限

授权范围 整个云账号

dev@group.oldboyedu.onaliyun.com

权限策略名称 AliyunECSReadOnlyAccess 授权成功

- oss 管理oss资源
- rds 查看rds资源
-

ram用户	dev组权限	用户自己权限
dev-oss2	ecs只读权限	
dev-rds	ecs只读权限	管理rds资源

RAM 访问控制

概览

身份管理

用户

用户组

角色

设置

SSO 管理

权限管理

授权

权限策略管理

OAuth 应用管理 (公测中)

RAM 访问控制 / 用户 / dev-rds@oldboyedu.onaliyun.com

← dev-rds@oldboyedu.onaliyun.com

用户基本信息

编辑基本信息

登录名称

dev-rds@oldboyedu.onaliyun.com

复制

UID

271756329686772880

显示名称

dev-rds

创建时间

2021年8月23日 10:46:12

备注

手机号码

邮箱

认证管理

加入的组

权限管理

个人权限

继承用户组的权限

所属组	权限策略名称	权限类型	备注
dev	AliyunECSReadOnlyAccess	系统策略	只读访问云服务器服务(ECS)的权限

RAM 访问控制

概览

身份管理

用户

用户组

角色

设置

SSO 管理

权限管理

授权

权限策略管理

OAuth 应用管理 (公测中)

RAM 访问控制 / 用户 / dev-rds@oldboyedu.onaliyun.com

← dev-rds@oldboyedu.onaliyun.com

用户基本信息

编辑基本信息

登录名称

dev-rds@oldboyedu.onaliyun.com

复制

UID

2717

显示名称

dev-rds

创建时间

2021

备注

手机号码

邮箱

认证管理

加入的组

权限管理

个人权限

继承用户组的权限

添加权限

授权范围	权限策略名称	权限策略类型	备注
整个云账号	AliyunRDSReadOnlyAccess	系统策略	只读访问云数据库服务(RDS)的权限

7. oss

7.1 nas vs oss ☆☆☆☆☆

存储类型		区别01：特点	区别02：使用方法
块存储	云盘，高效云盘，ssd,essd		
文件存储	nas (nfs、smb)	低访问量，数据量不大	配置后，linux挂载使用
对象存储	oss	较高访问量，数据库巨大 tb,pb, 容量无限	创建ram子账号 (api access id 和secret)， 给开发人员程序代码中调用

7.2 创建bucket

创建 Bucket

创建存储空间

存储类型

标准存储

低频访问存储

归档存储

标准：高可靠、高可用、高性能，数据会经常被访问到。

如何选择适合您的存储类型？

同城冗余存储

启用

关闭

OSS 将您的数据以冗余的方式存储在同一区域（Region）的 3 个可用区（Zone）中。提供机房级容灾能力。更多详情请参见 [同城冗余存储](#)。

！

同城冗余存储能提高您的数据可用性，同时会采用相对较高的计费标准。请查看 [价格详情](#)。同城冗余存储属性开启后，将不支持关闭。

版本控制

开通

不开通

！

开启版本控制特性后，针对数据的覆盖和删除操作将会以历史版本的形式保存下来。了解 [版本控制](#)。当前未开启版本控制功能，数据删除或被覆盖后将无法找回。

读写权限

私有

公共读

公共读写

私有：对文件的所有访问操作需要进行身份验证。

服务端加密方式

无

OSS 完全托管

KMS

实时日志查询

开通

不开通

OSS 与日志服务深度结合，免费提供最近 7 天内的 OSS 实时日志查询（限额 900 GB/天的日志写入额度，超出部分由日志服务单独收费。假设一条日志为 1 KB，约为 9 亿条）。开通该功能后，您可对 Bucket 的访问记录进行实时查询分析，[了解详情](#)。

定时备份

开通

不开通

混合云备份服务为 OSS 提供数据保护保障，防止误修改、误删除，可低成本长期保存历史数据。

确定

取消

7.2 应用

- web页面访问
- 程序代码访问
 - 支持使用oss作为存储
 - 创建oss,oss信息
 - 创建ram用户（api access id 和secret）
 - 在程序代码中配置oss
 - 测试

- 可道云

ecs	nginx php mariadb	
oss	oldboy-lidao007-cloud	
ram用户	可以访问（读写） oss	

#01 ecs环境准备

```
yum install -y nginx mariadb-server
```

```
yum install -y php-bcmath.x86_64 php-cli.x86_64 php-common.x86_64 php-dba.x86_64 php-dbg.x86_64 php-devel.x86_64 php-embedded.x86_64 php-embeddable.x86_64 php-enchant.x86_64 php-fpm.x86_64 php-gd.x86_64 php-gmp.x86_64 php-intl.x86_64 php-json.x86_64 php-ldap.x86_64 php-mbstring.x86_64 php-mysqlnd.x86_64 php-odbc.x86_64 php-opcache.x86_64 php-pdo.x86_64 php-pgsql.x86_64 php-process.x86_64 php-recode.x86_64 php-snmp.x86_64 php-soap.x86_64 php-xml.x86_64 php-xmlrpc.x86_64
```

#02 统一nginx php 用户

修改目录权限

```
[root@oldboy-ecs ~]# chown nginx.nginx /var/lib/php/session
[root@oldboy-ecs ~]# ll -d /var/lib/php/session
drwxrwx--- 2 nginx nginx 6 May 7 2020 /var/lib/php/session
```

#03 配置

#nginx-->php

```
[root@oldboy-ecs ~]# cat /etc/nginx/conf.d/cloud.conf
server {
    listen 80;
    server_name cloud.etiantian.org;
    root /data/cloud;
    location / {
        index index.php;
    }

    location ~ \.php$ {
        fastcgi_pass unix:/run/php-fpm/www.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }
}
```

#数据库 用户

mysql_secure_installation #一直Y

```
create database cloud charset utf8 ;
grant all on cloud.* to 'cloud'@'localhost' identified by '1';
grant all on cloud.* to 'cloud'@'%' identified by '1';
select user,host from mysql.user;
```

测试 nginx php

测试 php-mysql

```
systemctl enable nginx php-fpm.service mariadb
systemctl start  nginx php-fpm.service mariadb.service
```

系统安装

数据库类型：

SQLite

MySQL

PDO

支持集群部署,主从多数据库分离.

服务器：*

127.0.0.1

用户名：*

cloud

密码：

•

数据库：*

cloud

存储引擎：

InnoDB

系统缓存类型：

文件缓存

Redis

Memcached

用于缓存通用数据及会话session，加快系统访问

确定

- 配置可道云 访问oss

kod



桌面



文件管理



官网



更多

位置

收藏夹

个人空间

我的图片

我的文档

我的音乐

桌面

企业网盘

与我协作

工具

最近文档



个人空间



新建文件夹



上传



我的图片



我的文档



我的音乐



系统管理员

admin



个人中心



文件管理



后台管理



用户管理



插件管理



多语言 (language)



主题样式

自动



全屏



关于



App下载



免费版



退出

5 个项目

< 返回

存储类型

阿里云OSS

使用帮助

名称 *

阿里云-杭州-oss

存储名称，用于区分不同存储

空间大小 *

1024

(GB)

Access Key ID *

LTAI5tR13NcxxM4uYixyPBAW

阿里云账号的Access Key ID，请在【控制台-Access Key管理】中创建或查看

Access Key Secret *

.....

阿里云账号的Access Key Secret，获取方法同上

Bucket名称 *

oldboy-lidao007-cloud

创建空间时填写的Bucket名称

地域节点 *

oss-cn-hangzhou-internal.aliyuncs.com

Endpoint

存储目录 *

/kodbox/

文件存储目录

服务器中转（上传）

☒ 开启后，将通过服务器上传文件至对象存储；否则，将通过客户端直接上传。

服务器中转（下载）

☒ 开启后，将通过服务器获取存储文件进行下载；否则，将获取文件直链下载。

设为默认

☒ 默认项为唯一有效的系统存储，如选择开启，将自动取消其它默认存储方式，请谨慎操作。

保存

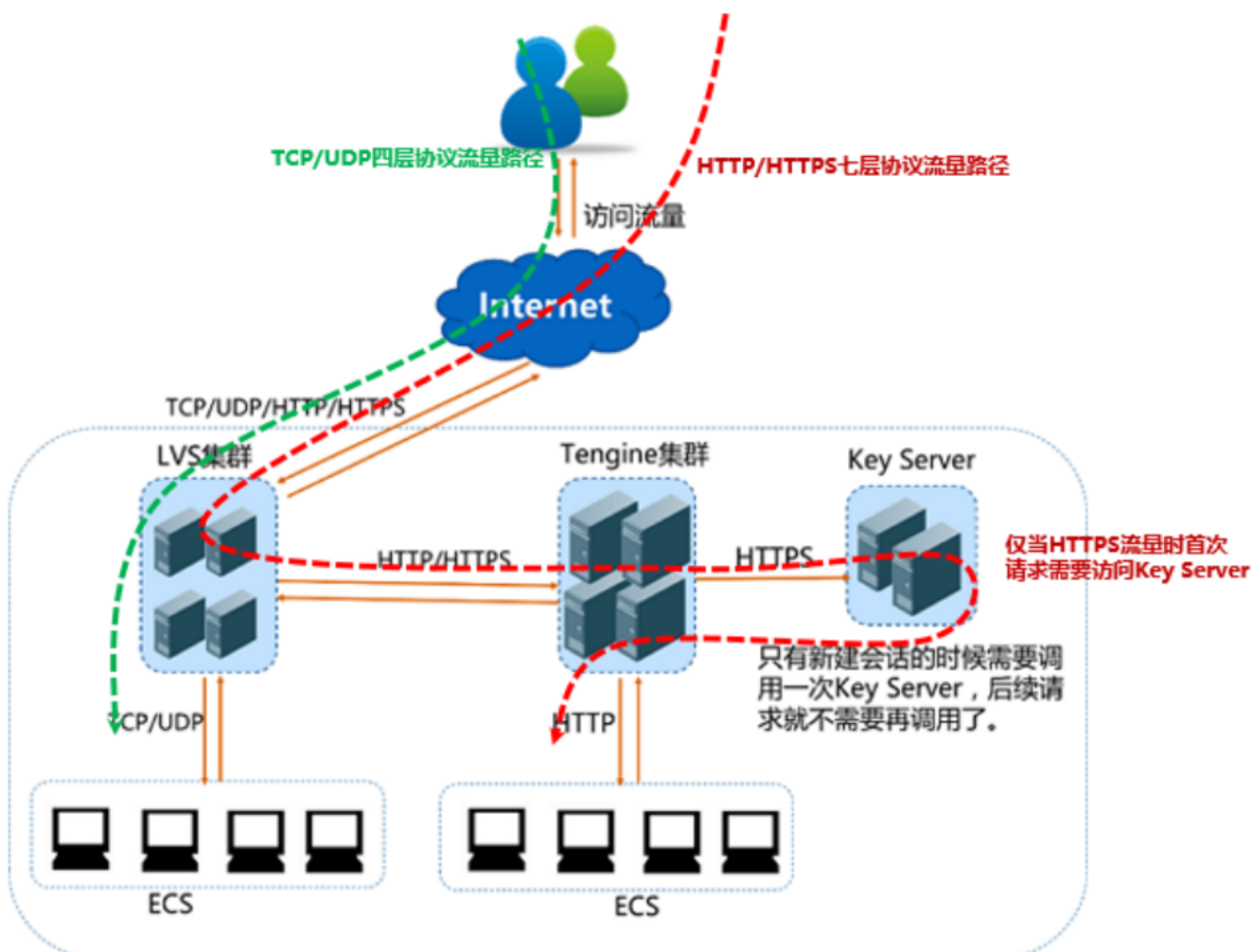
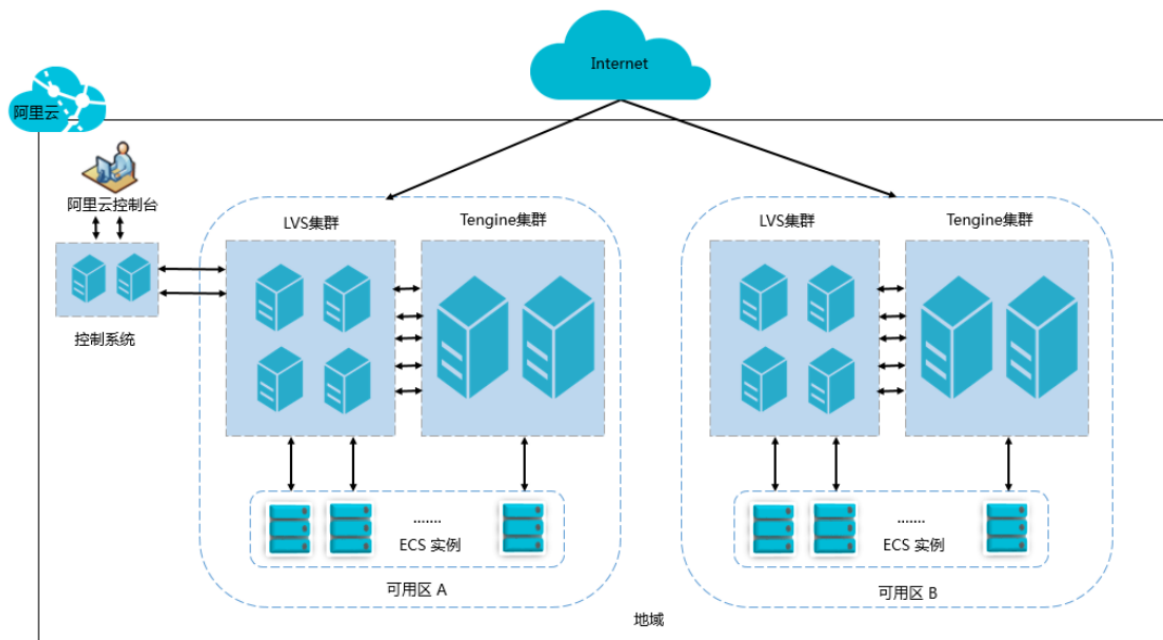
8. slb

8.1 slb概述

- 阿里云负载均衡
- clb(slb) 传统型负载均衡CLB（Classic Load Balancer）
- alb 应用型负载均衡ALB（Application Load Balancer）

	slb(clb)	alb
共同点	负载均衡功能，支持7层负载	负载均衡功能，支持7层负载
区别01	支持4层和7层	支持7层
区别02	clb 7层只支持域名或uri跳转	alb 7层负载支持更多功能，基于变量（客户浏览器，语言，其他功能。。。）

- 目标：不想使用clb和alb，想自己创建ecs *2 + keepalived 实现负载均衡高可用。
- 实现：申请keepalived,havip 未正式上市，测试



8.2 clb

← → ↺

slb.console.aliyun.com/slb/cn-hangzhou/slbs

三

阿里云

工作台

账号全部资源

华东1 (杭州)

负载均衡 SLB

概览

应用型负载均衡 ALB

实例

服务器组

健康检查

访问控制

TLS 安全策略

传统型负载均衡 CLB(原SLB)

实例管理

回收站

负载均衡 SLB / 实例管理

实例管理

创建传统型负载均衡

请选择标签

可用区: 全部

模糊搜索

请输入名称、ID或IP进行模糊搜索

实例名称/ID

服务地址

状态

启动

停止

释放设置

编辑标签

负载均衡 SLB / 实例管理

实例管理

创建传统型负载均衡

请选择标签

可用区: 全部

模糊搜索

请输入名称、ID或IP进行模糊搜索

实例名称/ID

服务地址

状态

监控

实例体检

端口/健康检查/后端服务器

操作

启动

停止

释放设置

编辑标签

clb-01

lb-bp1tz042zfjwr9h0kxy

未设置标签

121.41.11.176(公网IPv4)

运行中

点我开始配置

监听配置向导 | 添加后端服务器

每页显示 20

总共1条

上一页

下一页

负载均衡 SLB / 负载均衡业务配置向导

负载均衡业务配置向导

协议&监听

后端服务器

健康检查

配置审核

添加后端服务器用于处理负载均衡接收到的访问请求

后端服务器配置说明

请选择将监听请求转发至哪类后端服务器

虚拟服务器组

默认服务器组

主备服务器组

选择服务器组

请选择

upstream static {
server
server
server
}

upstream default {
server
server
server
}

upstream dong {
server
server
server
}


```
rm-bp1762enev3rt69v6.mysql.rds.aliyuncs.com
```

#导出数据库内容

```
mysqldump -uroot -p1 cloud >cloud.sql
```

#导入数据库内容

```
mysql -uoldboy -poldboyEDU123 cloud -h rm-6.m...s.aliyuncs.com <cloud.sql
```

```
[root@oldboy-ecs config]# pwd
```

```
/data/cloud/config
```

```
[root@oldboy-ecs config]# cat setting_user.php
```

```
<?php
```

```
$config['database'] = array (
    'DB_TYPE' => 'mysqli',
    'DB_HOST' => 'rm-bp1762enev3rt69v6.mysql.rds.aliyuncs.com',
    'DB_PORT' => 3306,
    'DB_USER' => 'cloud',
    'DB_PWD' => 'oldboyEDU123',
    'DB_NAME' => 'cloud',
    'DB_SQL_LOG' => true,
    'DB_FIELDS_CACHE' => true,
    'DB_SQL_BUILD_CACHE' => false,
);
```

```
$config['cache']['sessionType'] = 'file';
$config['cache']['cacheType'] = 'file';
```

#检查服务状态

```
[root@oldboy-ecs cloud]# systemctl is-enabled nginx mariadb.service php-fpm.service
```

```
enabled
```

```
disabled
```

```
enabled
```

```
[root@oldboy-ecs cloud]# systemctl is-active nginx mariadb.service php-fpm.service
```

```
active
```

```
inactive
```

```
active
```

云服务器 ECS / 实例 实例使用须知

实例

! 检查到安全组中包含允许对特定端口进行不受限制访问的规则，存在潜在高风险。[查看详情](#)

[创建实例](#) [高级搜索](#) [创建诊断](#) [批量操作](#) [刷新](#) [下载](#) [设置](#)

<input type="checkbox"/>	实例ID/名称	标签	监控	可用区	IP地址	状态	配置	操作
<input type="checkbox"/>	i-bp19y409tvdckh65px oldboy-ecs			杭州 可用区I	121.40.75.12 (公网) 172.16.4.22 (私有)	运行中	1 vCPU 1 GiB (I/O优化) ecs.s6-c1m1.small 100Mbps (峰值)	管理 远程连接 更改实例规格 更多
<input type="checkbox"/>	<div>启动 停止 重启 重置实例密码 续费 按量付费转包年包月 释放设置 更多</div>							

共有 1 条 每页 10 条

[更换操作系统](#)
[重新初始化云盘](#)
[创建自定义镜像](#)
[创建实例快照](#)

[购买相同配置](#)
[实例状态](#)
[实例设置](#)
[密码/密钥](#)
[资源变配](#)
[云盘和镜像](#)
[网络和安全组](#)
[运维和诊断](#)
[部署与弹性](#)

华东1（杭州）

搜索...

费用工单

创建自定义镜像

创建镜像的同时系统默认会创建相关快照，当前阿里云快照已经商业化，保有镜像会产生一定的快照费用。

请您在使用linux系统创建自定义镜像时，注意不要在/etc/fstab文件中加载数据盘的信息，否则使用该镜像创建的实例无法启动。

您可以对当前ECS实例做个完整的镜像模板，包含该实例下的所有云盘。该实例的每块云盘会新增一个快照，可以在快照列表中查询。需要等待每块云盘的快照创建完成，镜像才能可以使用，期间不要更改实例状态，如停止或重启实例，请耐心等待。

* 自定义镜像名称:

oldboy-ecs-lnmp

* 自定义镜像描述:

lnmp
无数据库
数据库连接rds
存储连接oss

镜像族系:

请输入或选择镜像族系

资源组:

请选择

标签:

请选择已有标签键或输入新键

请选择已有标签值或输入新值

创建

取消

云服务器 ECS / 实例

实例使用须知

实例

检查到安全组中包含允许对特定端口进行不受限制访问的规则，存在潜在高风险。[查看详情](#)

创建实例

选择实例属性项搜索，或者输入关键字识别搜索

Q

标签

高级搜索

创建诊断

批量操作

刷新

导出

设置

实例ID/名称	标签	监控	可用区	IP地址	状态	配置	操作
<input type="checkbox"/> i-bp19y409tydckh6n65px oldboy-ecs			杭州 可用区I	121.40.75.12 (公网) 172.16.4.22 (私有)	运行中	1 vCPU 1 GiB (I/O优化) ecs.s6-c1m1.small 100Mbps (峰值)	管理 远程连接 更改实例规格 更多
<input type="checkbox"/>							

☐ 启动

☐ 停止

☐ 重启

☐ 重置实例密码

☐ 续费

☐ 按量付费转包年包月

☐ 释放设置

☐ 更多

共有1条, 每页

购买相同配置

实例状态

实例设置

密码/密钥

资源变配

云盘和镜像

网络和安全组

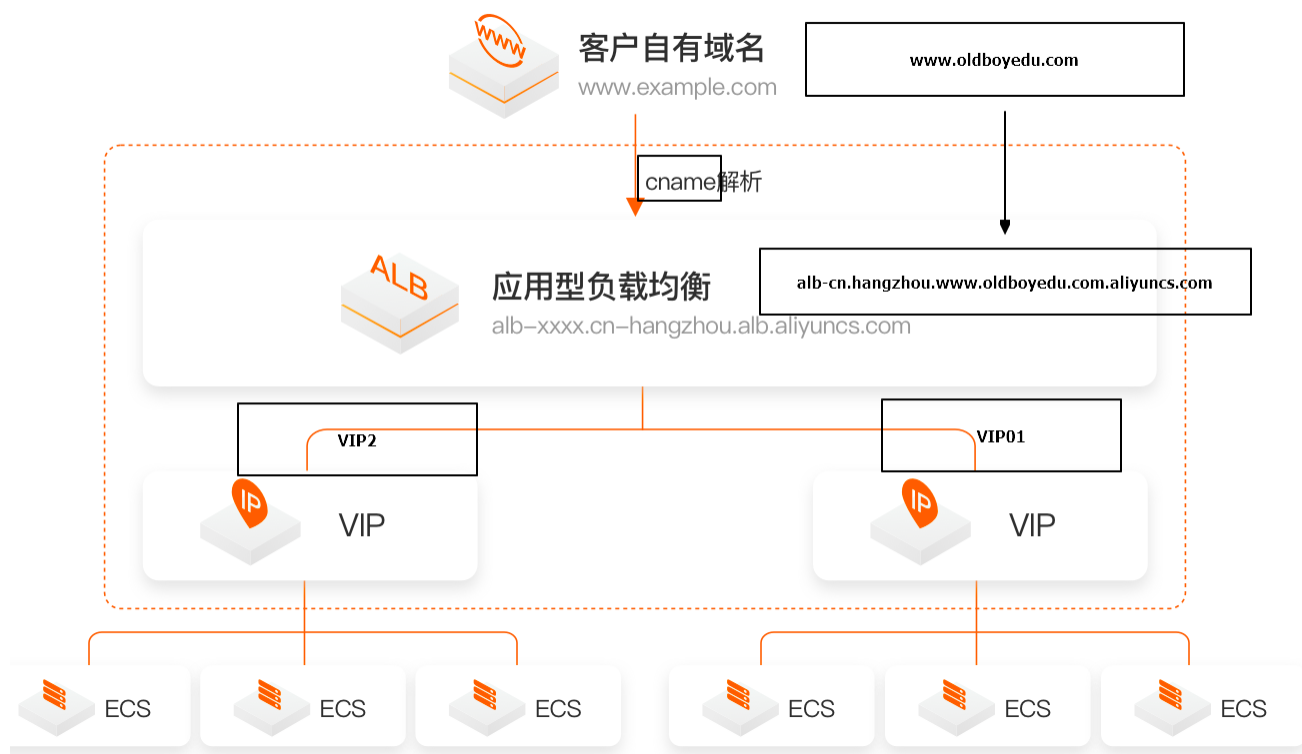
运维和诊断

部署与弹性

5tb 云盘 200元
oss 7200元 按量
oss 4,977 包年

8.3 alb

- 根据用户请求的客户端，http请求报文内容，进行分发
- 流量镜像：



操作流程



1. 准备工作

搭建负载均衡服务前，您需要根据业务需求规划 ALB实例的地域，创建专有网络VPC（Virtual Private Cloud）和后端服务器ECS实例等。

2. 步骤一：创建ALB实例

使用负载均衡服务时，您需要先创建一个 ALB实例，每一个 ALB实例代表着一个负载均衡服务实体。

3. 步骤二：创建后端服务器组

您需要创建服务器组并添加后端服务器来接收 ALB转发的客户端请求。

4. 步骤三：配置监听

您需要为实例配置监听，检查连接请求，然后根据调度算法定义的转发策略将客户端请求分发至后端服务器。

5. (可选) 步骤四：设置域名解析

ALB支持将您拥有的常用域名通过CNAME方式解析到 ALB实例的公网服务域名上，使您可以更加方便地访问各种网络资源。

/PC

oldboy77-vpc

创建一个VPC

可用区

☒杭州 可用区H

switch-h

☒杭州 可用区I

switch-i

应用型负载均衡支持多可用区部署，为保障业务高可用，请至少选择2个或以上可用区

P模式

固定IP

动态IP

此模式下每个可用区有且只有一个IP，并且IP固定保持不变，此模式下实例弹性能力受限，最大支持10万QPS

功能版本（实例费）

基础版

标准版

在基础版的功能基础上，标准版还包含诸如自定义TLS安全策略，重定向、重写等高级路由特性，详情参见[应用型负载均衡基础版和标准版功能差异](#)

实例网络类型

私网

公网

应用型负载均衡公网使用弹性公网IP，使用公网实例将收取弹性公网IP实例费与带宽、流量费用，详情参见[弹性公网IP计费文档](#)

公网计费方式

按流量计费

按固定带宽计费

阿里云

工作台

账号全部资源

华东1（杭州）

搜索

费用 工单 ICP 备案 企业 支持 App 购物车 帮助 反馈

负载均衡 SLB / 实例

实例

创建应用型负载均衡

全部可用区域

模糊搜索

请输入实例名称、ID、DNS 名称等进行查询

标签筛选

☐实例名称/实例ID

☐DNS 名称

☐运行状态

☐网络类型

☐专有网络ID

☐标签

☐监控

☐功能版本

☐操作

<input type="checkbox"/>	-	alb-s8xut4ughjjet8if.cn-hangzhou.alb.aliyuncs.com	运行中	公网	vpc-bp1vhu6m5eimgiu319if			标准版	创建实例
<input type="checkbox"/>	alb-s8xut4ughjjet8if								

☐批量释放

☐设置标签

每页显示 20 总共 1条 < 上一页 下一页 >

- 准备ecs

```
yum install -y nginx
systemctl enable nginx
systemctl start nginx
echo `hostname` `hostname -I` >/usr/share/nginx/html/index.html
cat /usr/share/nginx/html/index.html
```



```
upstream    www {  
    server  
    server  
  
}  
  
server {  
  
    location / {  
        proxy_pass http://www;  
    }  
}
```

```
}

```

负载均衡 SLB

概览

应用型负载均衡 ALB

实例

服务群组

健康检查

访问控制

TLS 安全策略

传统型负载均衡 CLB(原SLB)

实例管理

回收站

证书管理

访问控制

日志管理

所属实例

策略管理

快速链接

负载均衡 SLB / 实例 / 负载均衡业务配置向导

负载均衡业务配置向导

1 配置监听

选择负载均衡协议

HTTP

监听端口

80

监听名称

如不填写，系统默认为“协议_端口”

高级配置

修改

连接空闲超时时间

15 秒

选择请求超时时间

60 秒

Gzip数据压缩

已开启

附加HTTP头字段

开启通过X-Forwarded-For头字段获取来访者真实 IP。

WAF安全防护

☐ 为监听开启WAF安全防护

1 配置监听

2 选择服务器组

3 配置审核

添加后端服务器用于处理负载均衡接收到的访问请求

选择服务器组

服务器类型

默认 | sgp-d0vqh9pverw1stypz

后端协议

HTTP

调度算法

加权轮询

会话保持

未开启

健康检查

已开启

已添加的后端服务器

实例ID	地域	运行状态	专有网络 ID	IP地址	端口	权重	描述
oldboy-ecs001 i-bp17xgncp12ncmbj0vo9	杭州 可用区H	可用	vpc-bp1vhu6wx5eimgiu319if	172.16.3.83	80	100	-
oldboy-ecs002 i-bp17xgncp12ncmbj0voa	杭州 可用区H	可用	vpc-bp1vhu6wx5eimgiu319if	172.16.3.82	80	100	-

每页显示 20 总共 2 个 < 上一页

负载均衡 SLB

概览

应用型负载均衡 ALB

实例

服务群组

健康检查

访问控制

TLS 安全策略

传统型负载均衡 CLB(原SLB)

实例管理

回收站

证书管理

访问控制

日志管理

所属实例

策略管理

快速链接

负载均衡 SLB / 实例 / 负载均衡业务配置向导

负载均衡业务配置向导

1 配置监听

2 选择服务器组

3 配置审核

配置监听

负载均衡协议

HTTP

监听端口

80

监听名称

-

WAF安全防护

未开启

连接空闲超时时间

15 秒

选择请求超时时间

60 秒

Gzip数据压缩

已开启

附加HTTP头字段

开启通过X-Forwarded-For头字段获取来访者真实 IP。

选择服务器组

服务器组

sgp-d0vqh9pverw1stypz

已添加的后端服务器

实例ID	地域	运行状态	专有网络 ID	IP地址	端口	权重	描述
oldboy-ecs001 i-bp17xgncp12ncmbj0vo9	杭州 可用区H	可用	vpc-bp1vhu6wx5eimgiu319if	172.16.3.83	80	100	-
oldboy-ecs002 i-bp17xgncp12ncmbj0voa	杭州 可用区H	可用	vpc-bp1vhu6wx5eimgiu319if	172.16.3.82	80	100	-

每页显示 20 总共 2 个 < 上一页 下一页 >

- 根据用户浏览器类型进行转发

主机	浏览器类型	alb中的服务器组
ecs001	谷歌浏览器	谷歌组
ecs002	其他浏览器	默认组

负载均衡 SLB / 服务器组

服务器组

创建服务器组

服务器组名称 请输入服务器组名称进行查询

<input type="checkbox"/>	服务器组名称/ID	VPC	后端协议	关联的实例	类型	状态	标签	操作
<input type="checkbox"/>	谷歌组 sgp-g5w8qo25srz77kpts8	vpc-bp1vhuf6w5eimgiu319if	HTTP	-	服务器类型	可用		编辑后端服务器 编辑基本信息 编辑健康检查 更多
<input type="checkbox"/>	默认 sgp-d0vqh9pverw1sypz	vpc-bp1vhuf6w5eimgiu319if	HTTP	alb-s8xut4ugihjjet8if	服务器类型	可用		编辑后端服务器 编辑基本信息 编辑健康检查 更多

☐ 批量释放

☐ 设置标签

每页显示 20 总共2条 < 上一页 下一页 >

工作台

负载均衡 SLB / 实例 / alb-01-hangzhou-nginx | alb-s8xut4ugihjjet8if

← alb-01-hangzhou-nginx | alb-s8xut4ugihjjet8if

实例详情 监听 监控图表

创建监听

监听名称	监听协议/端口	运行状态	健康检查状态	监控	访问控制	监听默认转发规则	操作
HTTP_80 lsn-18bfyn21yhqps5uaw	HTTP:80	运行中	异常		未开启 应用	转发至默认	查看详情 查看/编辑转发规则 启动 更多

每页显示 20 共有 1 条 < 上一页 下一页 >

User-Agent:
Mozilla/5.0 (windows NT 10.0; win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131
Safari/537.36

插入转发规则

1 / 规则名称 转发到谷歌组

如果 (条件全部匹配)

HTTP标头

键是 User-Agent

值是 "Chrome"

+ 添加标头值

+ 添加转发条件

那么

转发至

服务器类型 sgp-g5w8qo25srz77kpts8 | 谷歌组

配置权重

+ 添加服务器组

+ 添加动作

+ 继续插入规则

请求方向转发规则

响应方向转发规则

提示：除了可以添加、修改、删除转发规则，也可以通过鼠标拖拽来调整规则优先级。

+ 插入新规则

保存优先级

1 / 转发到谷歌组 / rule-4c9pxae2px5e83re2x

✓ 正常

如果

✓ HTTP标头 键是 User-Agent 值是 "Chrome"

那么

转发至 谷歌组 权重: 100

优先级最低 / 监听默认规则

✓ 正常

如果

-

那么

转发至 默认

负载均衡 SLB / 实例 / alb-01-hangzhou-nginx | alb-s8xut4ughijjet8f / HTTP_80 | Isn-18bjfyit21yhgp5suw

← HTTP_80 | Isn-18bjfyit21yhgp5suw

启动

监听详情

转发规则

规则总览

转发规则：
您可以定义应用型负载均衡实例的监听转发规则，确定应用型负载均衡实例如何将请求路由到一个或多个后端服务器组中的后端服务器。
提示：除了可以添加、修改、删除转发规则，也可以通过鼠标拖拽来调整规则优先级。

客户端

ALB

请求方向规则 1

则 0

管理

后端服务

请求方向规则 (1)

1 如果 HTTP标头键是User-Agent值是 "Chrome" 那么 转发至 谷歌组 权重: 100

请求方向转发规则

响应方向转发规则

8.4 alb clb 小结 ✨ ✨ ✨ ✨ ✨

应用场景	slb(clb)	alb
共同点	负载均衡功能，支持7层负载	负载均衡功能，支持7层负载
区别01	支持4层和7层	支持7层
区别02	clb 7层只支持域名或uri跳转	alb 7层负载支持更多功能，基于变量（客户浏览器，语言，其他功能。。。）

9. DNS (云解析DNS) ✨ ✨ ✨ ✨ ✨

- Domain Name Sever/System 域名解析系统/服务 域名--dns->ip
- 域名（购买）-----> ip(ecs,slb)
 - dns解析服务（自己搭建,中小型公司使用这些服务搭建内部DNS系统，用来解析域名、主机。。。）
 - bind9
 - dnsmasq
 -
 - 域名运营商解析（简单配置）
 - 万网（阿里云）☒ ， 腾讯，新网
 - godaddy

术语		
记录	一条dns信息 域名-->ip (也可以是其他东西)	
记录类型	具体要如何解析域名	

- DNS记录类型

- A记录 #域名---->ipv4
- AAAA记录 #域名---->ipv6
- CNAME记录 #别名记录 域名---->域名 (CDN,alb, WAF)
- MX记录 #搭建/配置企业邮箱 使用 # baidu.com lidao@baidu.com
- TXT记录 #域名---->字符串 # 验证域名的所有者 (验证后删除)

#A记录 域名--->ip

###主机记录就是域名前缀，常见用法有：

#www: 解析后的域名为www.aliyun.com。

#@: 直接解析主域名 aliyun.com。 ping oldboylinux.com #配置@oldboylinux.com

#*: 泛解析，匹配其他所有域名 *.aliyun.com。

ping a.oldboylinux.com

ping b.oldboylinux.com

mail: 将域名解析为mail.aliyun.com，通常用于解析邮箱服务器。

二级域名: 如: abc.aliyun.com, 填写abc。

手机网站: 如: m.aliyun.com, 填写m。

TTL: Time To Live #缓存时间

操作成功

记录类型:

A- 将域名指向一个IPv4地址

主机记录:

aliyun

.oldboylinux.com ?

解析线路:

默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路设置结果

* 记录值:

47.97.219.137

* TTL:

10 分钟

#CNAME 别名记录

[root@oldboy-ecs001 ~]# dig baidu.oldboylinux.com

```
;<<>> DiG 9.11.26-RedHat-9.11.26-4.el8_4 <<>> baidu.oldboylinux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30614
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 1546ab793a3c1f8e010000006124663d47072d00622c6ad8 (good)
;; QUESTION SECTION:
;baidu.oldboylinux.com.      IN  A

;; ANSWER SECTION:
baidu.oldboylinux.com.  600 IN  CNAME  www.jd.com.
www.jd.com.           9  IN  CNAME  www.jd.com.gs1b.qianxun.com.
www.jd.com.gs1b.qianxun.com. 22 IN  CNAME  www.jdcdn.com.
www.jdcdn.com.        239 IN CNAME  img20.360buyimg.com.s.galileo.jcloud-cdn.com.
img20.360buyimg.com.s.galileo.jcloud-cdn.com. 3132 IN CNAME img2x-sched.jcloud-cdn.com.
img2x-sched.jcloud-cdn.com. 29  IN  A      222.186.184.3

;; Query time: 159 msec
;; SERVER: 100.100.2.136#53(100.100.2.136)
;; WHEN: Tue Aug 24 11:23:41 CST 2021
;; MSG SIZE rcvd: 284
```

记录类型:

CNAME- 将域名指向另外一个域名

主机记录:

baidu

.oldboylinux.com ?

解析线路:

默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路设置结果

* 记录值:

www.baidu.com

* TTL:

10 分钟

#TXT记录

```
[root@oldboy-ecs001 ~]# dig TXT check.oldboylinux.com

; <<>> DiG 9.11.26-RedHat-9.11.26-4.el8_4 <<>> TXT check.oldboylinux.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1838
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 347feae0f1c3179cb6ba56ad6124675509d61c3a08013040 (good)
;; QUESTION SECTION:
;check.oldboylinux.com.      IN  TXT

;; ANSWER SECTION:
check.oldboylinux.com.  600 IN  TXT "this is test, this test is ok."

;; Query time: 2 msec
;; SERVER: 100.100.2.136#53(100.100.2.136)
;; WHEN: Tue Aug 24 11:28:21 CST 2021
;; MSG SIZE rcvd: 122
```

修改记录X

记录类型:

TXT- 文本长度限制512, 通常做SPF记录 (反垃圾邮件)▼

主机记录:

check

.oldboylinux.com?

解析线路:

默认 - 必填! 未匹配到智能解析线路时, 返回【默认】线路设置结果▼?

* 记录值:

this is test, this test is ok.

* TTL:

10 分钟▼

10. 安全

- 安全组
- 系统自动安装安全插件 (监控插件)
- 阿里云安全中心: 云盾, 态势 (态势) 感知
- waf 应用防火墙

10.1 安全组 ❄❄❄❄❄

- 阿里云的防火墙 (iptables filter表)
- 默认是白名单, 防止端口或ip访问

云服务器管理控制台

ecs.console.aliyun.com/?spm=5176.100251.favorite.decs.72014f15xUAfOJ#/home

阿里云 | 工作台

搜索...

费用 工单 ICP 备案

云服务器 ECS

专有宿主机 DDH

云盘

超级计算集群

预留实例券

资源保障

节省计划

网络与安全

安全组

弹性网卡

密钥对

专有网络 VPC

前缀列表

存储与快照

云盘

快照

存储容量单位包

专属块存储集群

地域	可用区	实例数	状态	规格	公网带宽	公网IP	内网带宽	内网IP	公网带宽	公网IP
华北2 (北京)	可用区A	0	空闲	ecs.g6.large	0	0	0	0	0	0
华东1 (杭州)	可用区A	2	运行中	ecs.g6.large	0	0	0	0	0	0
华北6 (乌兰察布)	可用区A	1	空闲	ecs.g6.large	0	0	0	0	0	0
新加坡	可用区A	1	空闲	ecs.g6.large	0	0	0	0	0	0

我的权益

5年老用户 升级专享6.3折

立即领取

使用规则

5年老用户 续费专享6.3折

立即领取

使用规则

我的教程

快速搭建网站

部署开发环境

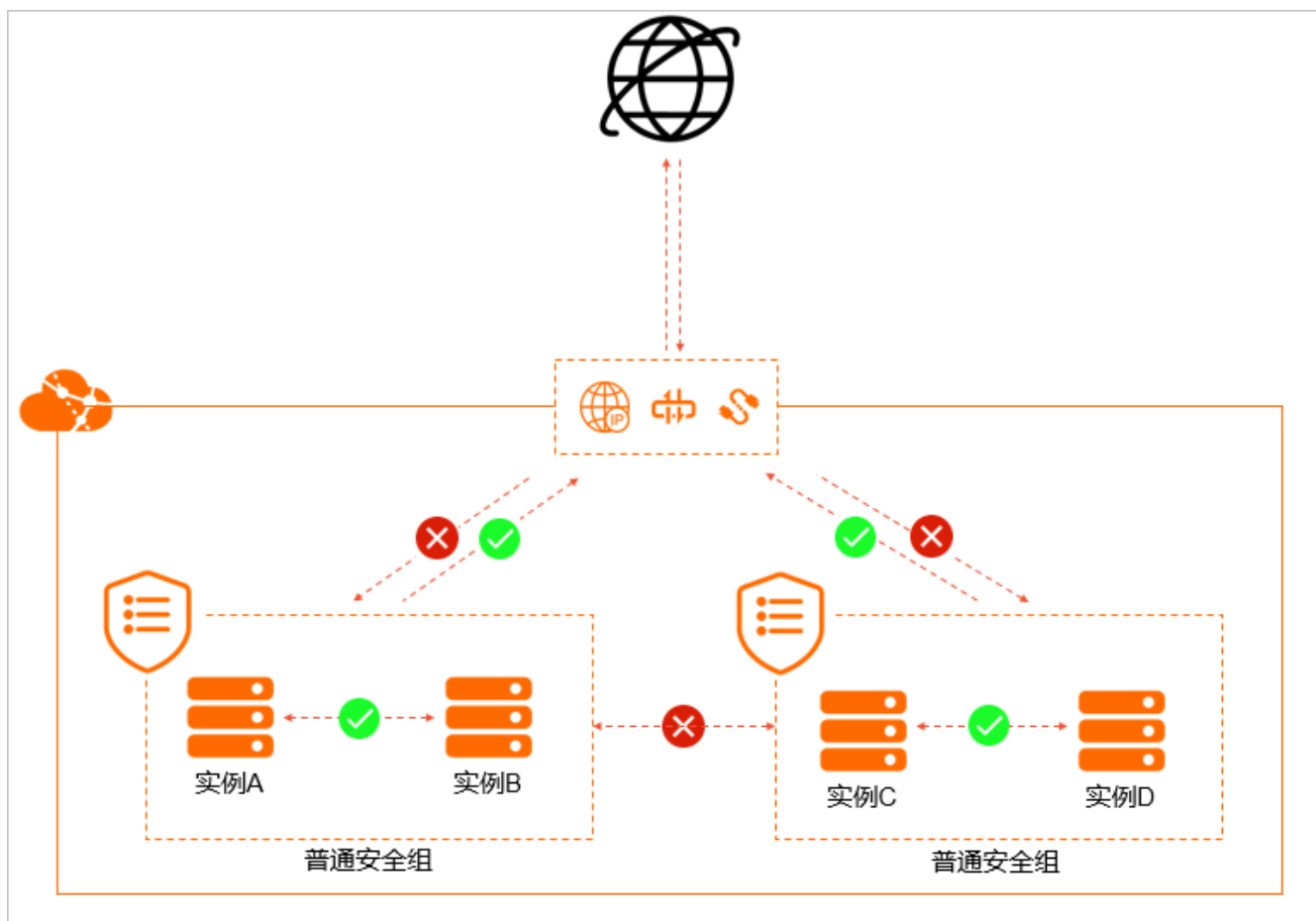
搭建云上博客

搭建小程序

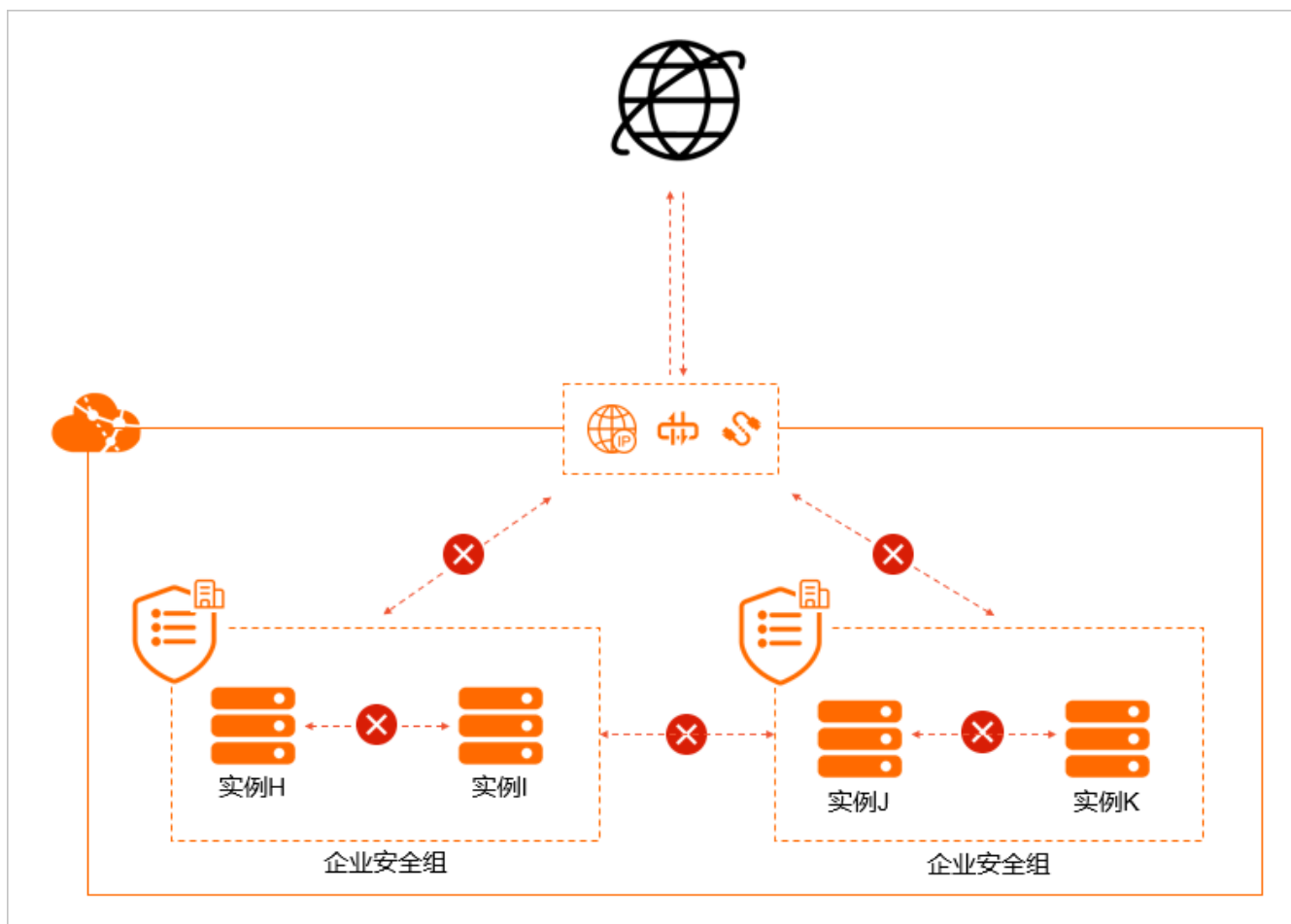
云上服务器迁移

云上高可用架构

- 普通安全组



- 企业级安全组



- 普通安全组---->企业级安全组



目标安全组

安全组类型 ☐ 普通安全组 ☒ 企业级安全组

选择安全组

安全组ID	安全组名称	可加入IP数	操作
<input type="text" value="sg-bp1d57d3d18x2fltsv1e"/>	安全组-企业级	65536	删除
<div>增加 已选安全组: 1 / 5</div>			

所选实例 共 2 个实例将执行替换安全组操作。

实例ID/名称	原安全组数量	替换后安全组数量
i-bp17xgncp12ncmbj0voa oldboy-ecs002	1	1
i-bp17xgncp12ncmbj0vo9 oldboy-ecs001	1	1

替换安全组

取消




<

安全组规则

安全组内实例列表

安全组内弹性网卡

云服务器 ECS / 安全组 / sg-bp1d57d3d18x2ftsv1e

← 安全组-企业级  oldboy77-vpc / vpc-bp1vhu6xw5eimgiu319if

基本信息

安全组ID/名称: sg-bp1d57d3d18x2ftsv1e/ 安全组-企业级



网络: vpc-bp1vhu6xw5eimgiu319if

安全组类型: 企业级安全组

描述:

标签:

资源组:

访问规则  导入安全组规则  导出

入方向

出方向

手动添加





快速添加

全部编辑

🔍 输入端口或者授权对象进行搜索

授权策略	优先级 ①	协议类型	端口范围 ①	授权对象 ①	描述
<input type="checkbox"/>  允许	1	自定义 TCP	目的: 9999/9999	源: 172.16.0.0/12	
<input type="checkbox"/>  允许	1	自定义 TCP	目的: 80/80	源: 0.0.0.0/0	
<input type="checkbox"/>  允许	1	自定义 TCP	目的: 443/443	源: 0.0.0.0/0	
<input type="checkbox"/>  允许	1	自定义 TCP	目的: 22/22	源: 0.0.0.0/0	
<input type="checkbox"/>  允许	1	自定义 TCP	目的: 3389/3389	源: 0.0.0.0/0	
<input type="checkbox"/>  允许	1	全部 ICMP(IPv4)	目的: -1/-1	源: 0.0.0.0/0	
<input type="checkbox"/>  删除					

10.2 云安全中心（态势感知） :star2:

- 查看异常登录
- 查看漏洞信息: 
 - 解决: 升级 (rpm包, 编译安装,yum)
 - 检查: 漏洞影响的软件及版本 (范围)

10.3 waf防火墙

- 防火墙
 - 开源软件-iptables 4
 - 硬件防火墙-深信服, 奇安信
 - 开源软件(nginx lua)、公有云服务- waf防火墙应用防火墙 (SQL注入, CC)
- 用户输入域名---->ip 用户访问ip对应网站信息
- 用户--->waf---->cdn---->slb---->网站集群
- 用户--->waf----->ecs

本页目录(4)

步骤1：购买WAF实例

步骤2：网站接入

步骤3：配置网站防护策略

步骤4：查看安全报表

#服务器地址需要为公网可达的IP，支持IPv4和IPv6，暂不支持只配置IPv6。

同时配置IPv4和IPv6时，如勾选协议跟随，则来自IPv6的地址将总是转发到IPv6的源站，来自IPv4的地址将总是转发到IPv4的源站。如不勾选协议跟随，则不做区分，混合回源（即IPv4有可能回源到IPv4和IPv6，IPv6同理）。

只配置IPv4时，IPv4和IPv6请求都将通过IPv4回源。

如有IPv6回源需求，需要确保“网站接入”中域名列表的“IPv6状态”已开启。

如果当前版本不支持IPv6，请升级您的版本。

#获取waf的cname

```
irtluyrkeu8wat4fbrf0cq37k3gioz3.yundunwaf5.com
```

```
aliyun.oldboyedu.com ---> ip ecs
```

```
aliyun.oldboyedu.com ---> irtluyrkeu8wat4fbrf0cq37k3gioz3.yundunwaf5.com ---> ip ecs
```

添加记录

导入/导出

请求量统计

新手引导

全部记录

精确搜索

输入关键字

高级搜索

<input type="checkbox"/>	主机记录	记录类型	解析线路(isp)	记录值	TTL	状态	备注	操作
<input type="checkbox"/>	aliyun	CNAME	默认	irtluyrkeu8wat4fbrf0cq37k3gioz3.yundunwaf5.com	10 分钟	正常		修改 暂停 删除 备注

#如果您需要对经过WAF的请求进行标记（用以区分没有经过WAF的请求），

#可以自定义一个特殊的标记，

如ALIWAF-TAG: Yes（ALIWAF-TAG为Header字段名，Yes为Header字段值）。

请不要填写标准的HTTP头部字段（如User-agent等），否则会导致标准字段被自定义的字段值覆盖。

```
> Frame 1004: 945 bytes on wire (7560 bits), 945 bytes captured (7560 bits)
> Ethernet II, Src: ee:ff:ff:ff:ff:ff (ee:ff:ff:ff:ff:ff), Dst: Xensourc_0e:de:28 (00:16:3e:0e:de:28)
> Internet Protocol Version 4, Src: 47.98.74.70, Dst: 172.16.3.83
> Transmission Control Protocol, Src Port: 45934, Dst Port: 80, Seq: 1, Ack: 1, Len: 891
▼ Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: aliyun.oldboyedu.com\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36\r\n
    X-True-IP: 123.112.22.232\r\n
    X-Real-IP: 123.112.22.232\r\n
    Web-Server-Type: nginx\r\n
    WL-Proxy-Client-IP: 123.112.22.232\r\n
    X-Forwarded-For: 123.112.22.232\r\n
    X-Forwarded-Proto: http\r\n
    X-Forwarded-Cluster: waf,\r\n
    EagleEye-TraceId: 2f624a4616297958982315751e468f\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
  > Cookie: Hm_lvt_9aa800f882f575237396648643111698=1625626576,1627468880,1628064983\r\n
    If-None-Match: "61244866-1a"\r\n
    If-Modified-Since: Tue, 24 Aug 2021 01:16:22 GMT\r\n
    eagleeye-rpcid: 0.1\r\n
    User-Waf996: yes\r\n
  \r\n
  [Full request URI: http://aliyun.oldboyedu.com/]
  [HTTP request 1/4]
  [Response in frame: 1007]
  [Next request in frame: 1010]
```

#tcpdump 抓包保存

```
tcpdump -nn port 80 -w /tmp/80.pcap
```

wireshark 查看

```
http.request.method == GET #只过滤出 http get请求
```

11. cdn

- 目标：网站加速，网站静态资源（html,js,css,图片，视频。。。缓存到cdn上面）
- 实现：内容分发网络，类似于分布式缓存加上调度器（智能DNS),缓存+加速
- 使用：
 - 产品：阿里云，腾讯云。。。。
 - 公司：蓝汛，网宿。。。

阿里云

工作台

账号全部资源

搜索

常用工具ICP备案企业支持App扫码购物车帮助

CDN

概览

尊敬的用户，受CA政策影响，CDN HTTPS免费证书申请成功后会受到较大影响，已申请证书到期前不受影响，建议您尽快到SSL证书产品重新进行证书申请并部署。[详细请见公告](#)

尊敬的用户，阿里云CDN将于2021年8月30日下架并停服CDN图片鉴黄资源包。如果您是CDN图片鉴黄资源包年包用户，请勿续费。如果您是CDN图片鉴黄资源包年包用户，请您在8月30日前提交工单申请退款。如您仍有图片鉴黄的需求，请登录阿里云官网[鉴黄](#)了解更多详情。如有疑问，欢迎联系阿里云。

基础数据

带宽峰值3.61Mbps

总流量7.76GB

HTTPS请求数26.03万次

QUIC请求数0次

安全

CDN WAF拦截次数开通

频次控制拦截次数开通

证书

已过期11个

即将过期0个

热门服务

全部域名17个

创建我的CDN

管理

刷新预热

计费方式按流量计费

变更计费方式

用量查询

费用中心

资源包管理

请点击“查看”，到费用中心的资源包概览页面，选择“CDN/全站加速资源包”查询详细情况。

购买

资源包用量查看和续费

源站		
回源		

新增源站信息

* 源站信息

- ☐ OSS域名
- ☒ IP
- ☐ 源站域名
- ☐ 函数计算域名

IP

118.31.79.50

* 优先级

- ☒ 主
- ☐ 备

* 权重

10

* 端口

80

确定

取消

← 添加域名

1

域名信息

2

推荐配置

基础信息

* 加速域名

aliyun.oldboyedu.com

加速域名是指接入CDN，用于加速源站的域名，也是您最终暴露给终端用户访问的域名。CDN支持添加泛域名如*.test.com”。[了解更多](#)

业务信息

* 业务类型

图片小文件

* 加速区域

☒ 仅中国内地

☐ 全球

☐ 全球（不包含中国内地）

! 加速区域含中国内地时，加速域名必须备案。由于工信部备案系统有数据延迟，刚完成备案的域名请在8个小时以后再配置。[什么是ICP备案?](#)

不同加速区域价格有差别，请按您的实际需求选择。[价格详情](#)

资源分组

选择资源组

源站信息

* 源站信息

新增源站信息

源站类型	域名	优先级	权重	端口	操作
IP	118.31.79.50	主	10	80	编辑 删除

添加缓存过期时间



类型

☐ 目录

☒ 文件后缀名

后缀名

jpg,txt,html,jpeg

文件后缀如输入多个须以半角逗号分隔如jpg,txt

过期时间

10

天

过期时间最多为3年

权重

1

最大99，最小1

确定



取消

发件nasnkey的时候会保留URL中?之后的参数，这样可以有效提高文件缓存命中率，提升效率及效率。通过配置过

✔ 恭喜您完成添加向导，请前往域名注册商配置CNAME！

重要：您还需要完成加速域名的CNAME解析设置

您需要在域名解析中添加CNAME记录，CDN加速方能生效，请前往您的域名注册商添加CNAME。

域名	aliyun.oldboyedu.com
CNAME记录值	aliyun.oldboyedu.com.w.kunlunaq.com 
主机记录	aliyun 
记录类型	CNAME

打开CNAME配置向导

返回域名列表

#刷新

强制删除CDN所有节点上的缓存资源，当您向CDN节点请求资源时，CDN会直接回源站获取对应的资源并返回给您，同时将资源重新缓存到CDN节点。刷新功能会降低缓存命中率。

#预热

源站主动将对应的资源缓存到CDN节点，当您首次请求资源时，即可直接从CDN节点获取到最新的资源，无需再回源站获取。预热功能会提高缓存命中率。

基础服务计费	后付费模式		预付费模式
	按流量计费	小时流量计费	下行流量资源包
	按带宽计费	日峰值带宽计费	

增值服务计费	后付费模式		预付费模式
	HTTP请求	静态HTTPS请求数	静态HTTPS资源包
	QUIC请求	静态QUIC请求数	
	WAF防护	边缘WAF请求数	边缘WAF资源包
	图片鉴黄	图片鉴黄处理数量	图片鉴黄资源包
	实时日志	实时日志推送数量	

#假设	日带宽峰值	10Mb	流量1天	10GB	1个月	300GB	1年	3650GB
			1天					
#方案01	按流量计费	1天10GB流量	1个月300G	费用/月=300*0.24	=72	一年	864	
#方案02	日峰值带宽计费	1天 10*0.6	=6	1月	180	1年		
#方案03	购买资源包							

	1天	1个月	1年
方案01 按流量计费	10GB流量	72	864 3650GB
方案02 日峰值带宽计费	10Mb 6	180	2,160
方案03 购买资源包			900 5TB

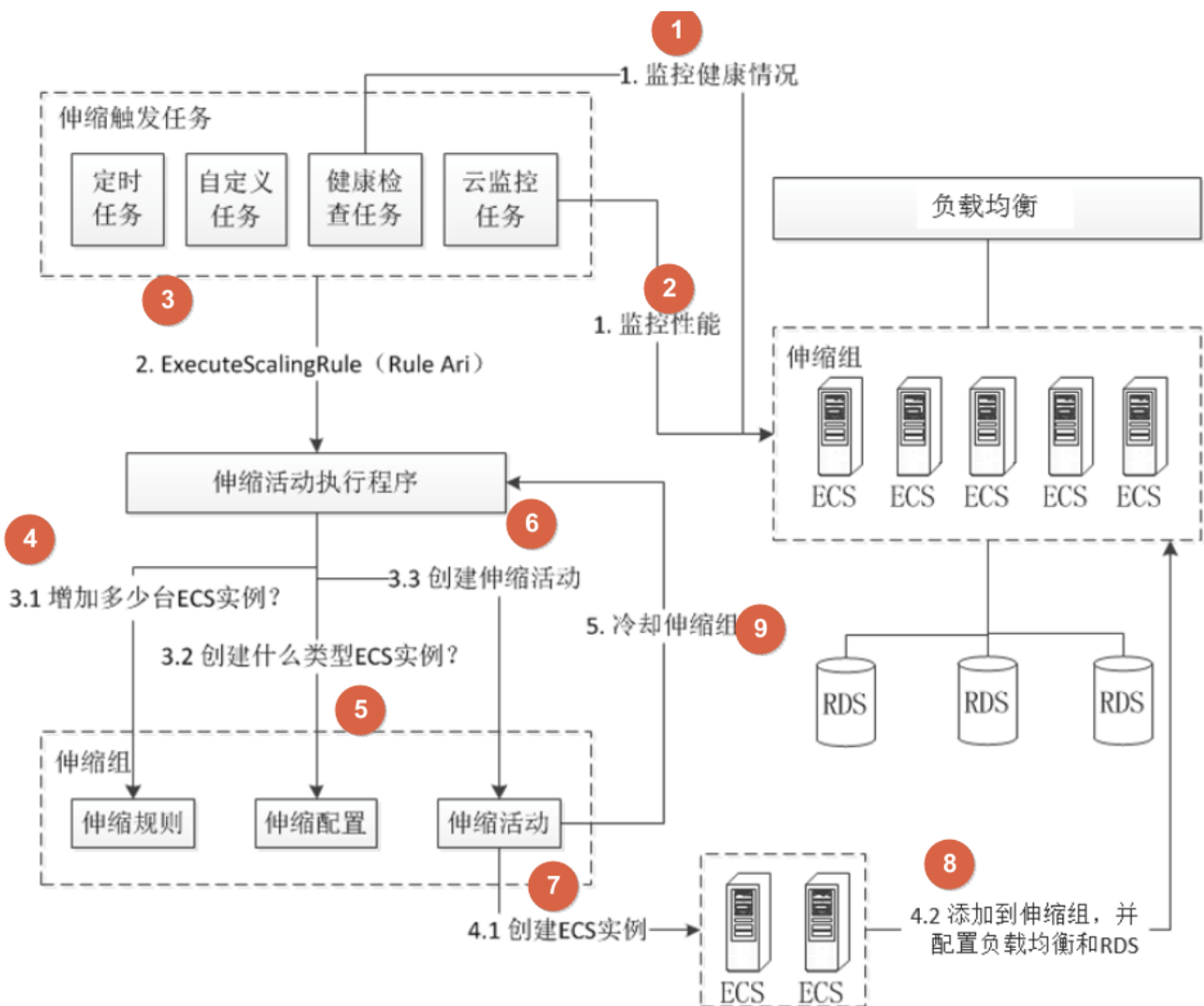
#https 请求加速	1天 40w次	1年 1.5e次
#按照次数 按量		
#资源包 包年		

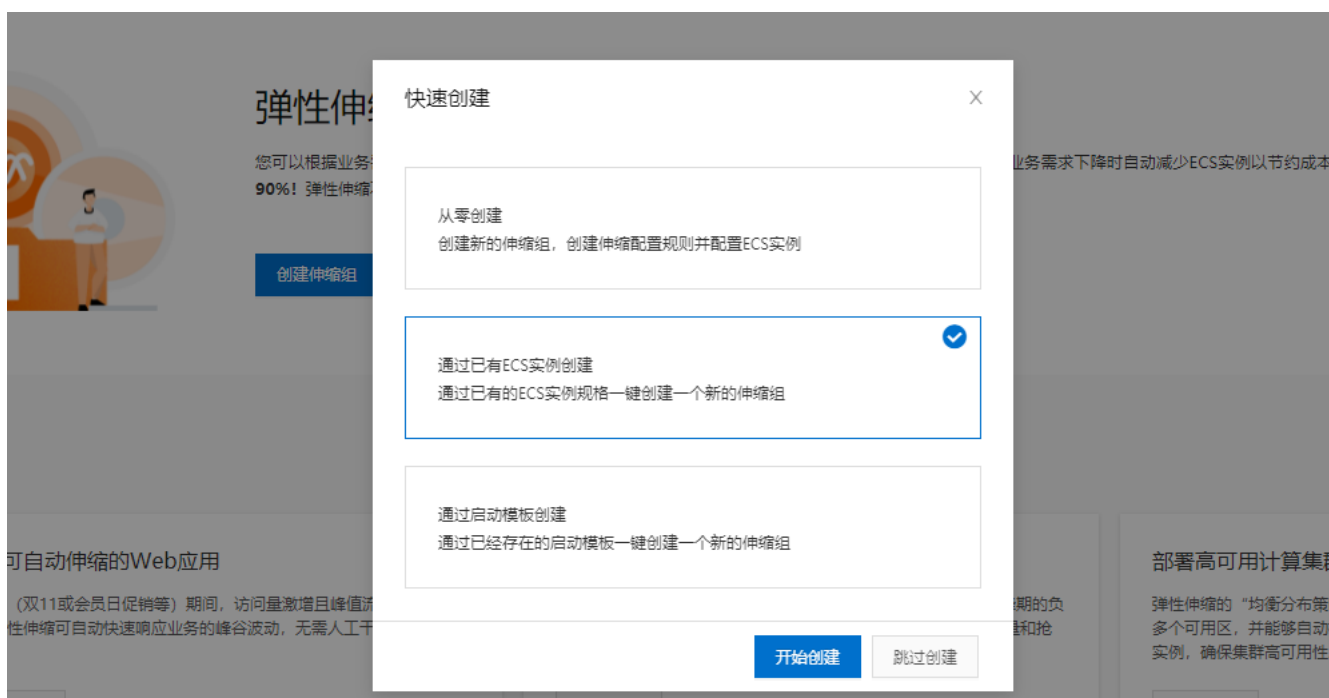
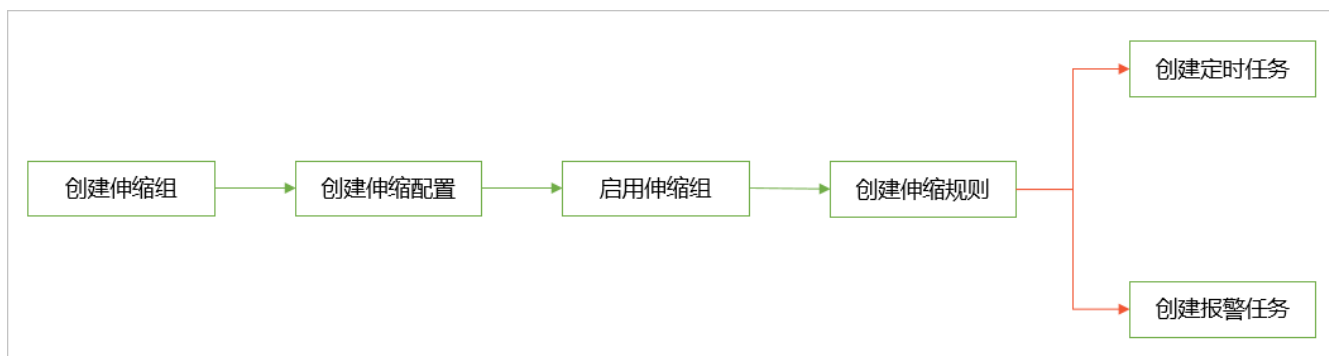
	1天	1月	1年
按照次数 按量	40*0.05=2	60	720 1.5亿
资源包 包年			324 1亿
搭配	1天40w次 1年1.5e次 https 资源包+按量 324+240=564		

- 小结
 - cdn加速原理
 - cdn配置流程
 - cdn费用计算

12.ess

- ess 弹性伸缩 Auto Scaling
- 根据指标（系统负载，带宽，连接数。。。）动态调整集群中服务器的数量。
- 预防：活动，推广，突然火爆。





* 伸缩组名称

ecs-web-static

名称2~64个字符，以大小写字母、数字或中文开头，可包含点号（.）、下划线（_）或中划线（-）

组内实例配置信息来源 ?

☐ 启动模板 ☒ 选择已有实例 ☐ 从零开始创建 [查看组内实例配置信息来源说明](#)

* 选择已有实例

i-bp171s3hnu79f7ed9qtc / oldboy-ecs

! 该实例不会自动加入到伸缩组内，若需加入，请使用下面的添加已有实例来实现。

实例ID/名称 [i-bp171s3hnu79f7ed9qtc / oldboy-ecs](#)
镜像ID centos_7_9_x64_20G_alibase_20210623.vhd ?
实例规格 ecs.s6-c1m1.small
安全组ID [sg-bp1d9ypyhv7ferjplnw / 阿里云-杭州-ecs-安全组-secure-group](#)
网络类型: 专有网络
专有网络ID [vpc-bp1vhu6xw5eimgiu319if / oldboy77-vpc](#)
虚拟交换机ID [vsw-bp14z55fs40pat8oqwk6l / switch-i](#)

标签 ?

标签键 标签值
web static

创建伸缩组

X

请选择或输入完整的标签键 : 请选择或输入完整的标签值

实例移出策略 ?

先筛选 最早伸缩配置对应的实例 [如何保证手工添加的ECS实例不被移出伸缩组](#)
再从结果中移出 最早创建的实例

暂停的流程 ?

请选择需要暂停的流程

开启伸缩组保护 ?

☐

实例的健康检查 ?

☒

* 组内最小实例数 ?

1
0到2000之间

* 组内最大实例数 ?

6
0到2000之间 [查看配额说明](#)

组内期望实例数 ?

2 [前往查看组内期望实例数详情](#)

* 默认冷却时间 (秒) ?

10
0到18000之间

网络类型

☒ 专有网络 ☐ 经典网络

扩容策略

☐ 优先级策略 ☒ 均衡分布策略 ☐ 成本优化策略

实例回收模式

☒ 释放模式 ☐ 停机回收模式

当ECS实例状态不健康时，该实例会被移出伸缩组并释放。请不要在伸缩组内的实例中保存应用状态信息和相关数据等信息，避免数据丢失风险。

* 专有网络

vpc-bp1vhu6xw5eimgiu319if / oldboy77-vpc

[创建专有网络](#)

* 选择交换机

vsw-bp14z55fs40pat8oqwk6l / switch-i X
vsw-bp12p0lq7i90gjq6j73m1 / switch-h X
vsw-bp1evt0c9t6hlu3ehvioj / switch-e-1 X
vsw-bp13kpmu9ejx0jdgk2n / switch-b-2 X

[创建交换机](#)

已选4个交换机，当前伸缩组最多只能选择10个交换机。

添加已有实例

请选择已有实例，支持已有实例ID搜索

已选0台实例

关联传统型负载均衡CLB（原SLB）

请选择传统型负载均衡，支持传统型负载均衡ID搜索

[创建传统型负载均衡](#)

已选0台实例

关联传统型负载均衡CLB（原SLB）

lb-bp12cjbvm3fmg6zd91l / auto_named_slb X

[创建传统型负载均衡](#)

请先选择传统型负载均衡CLB后编辑对应的服务器组，已选1个传统型负载均衡CLB，当前伸缩组最多可配置30个，[查看配额说明](#)

当前每个传统型负载均衡CLB实例后端可以挂载的服务器数量限额为200。
伸缩组关联传统型负载均衡CLB实例后，在伸缩组中的ECS实例都会自动加入到传统型负载均衡CLB实例的后端服务器组，建议您使用生命周期挂钩来确保服务可用。请参考[使用文档](#)。

只有配置过监听的负载均衡才能被伸缩组使用。

▼ lb-bp12cjbvm3fmg6zd91l / auto_named_slb

服务器组：1默认，0虚拟

[移出](#)

服务器组	端口 (1-65535)	权重 (1-100)	操作
默认服务器组	-	在伸缩配置里指定	删除
添加虚拟服务器组		添加默认服务器组	

#优先级策略

优先吧扩容的ecs增加到指定的虚拟交换机中。 虚拟交换机ecs满了才会更换。

根据您定义的虚拟交换机扩容。

当优先级较高的虚拟交换机所在可用区无法创建ECS实例时，自动使用下一优先级的虚拟交换机创建ECS实例。

#均衡分布策略 均衡

让ess添加ecs尽可能分布在不同的 可用区

在伸缩组指定的多可用区（即指定多个专有网络交换机）之间均匀分配ECS实例。如果由于库存不足等原因可用区之间变得不平衡，您可以进行再均衡操作来平衡资源的可用区分步。

只有设置了多个专有网络交换机时该策略才能生效

创建便宜的抢占式实例，然后创建按量

- 添加告警任务

三

阿里云

工作台

华东1 (杭州)

弹性伸缩

伸缩组管理

自动触发任务管理

定时任务

报警任务

问题诊断

垂直伸缩

标签

一步一步创建弹性伸缩

常见问题

配额申请

弹性伸缩 / 报警任务

报警任务

系统监控自定义监控

创建报警任务

报警任务ID

请输入报警任务ID

搜索

报警任务名称/ID

状态 (全部)

监控资源

创建报警任务

描述

系统负载高之后添加ecs

描述为2~255个字符

* 监控资源

asg-bp12o63alqt70tdm3024 / ecs-web-static

监控类型

系统监控

* 监控项

(Agent) 系统平均负载

统计周期

1

分钟

* 统计办法

Average (平均值)

>=

阈值

0.5

重复几次后报警

1

次

生效周期

不设置

Cron表达式

* 报警触发规则

请选择报警触发规则，支持名称搜索

创建伸缩规则

#简单规则 增加、删除、一步到位

定义了伸缩组扩缩容的行为，当由报警任务触发时，需要等待冷却时间结束

#目标追踪规则 3台ecs 负载0.8 目标降低到0.4 增加1台

通过自动计算实例扩缩容数量将指定指标维持在目标值附近

#预测规则

用户可以配置要预测的性能监控，监控目标值等一系列参数，对伸缩组进行预测

#步进规则 与第2个类似

根据一组步长调整增加或减少组的当前容量，这些步长调整根据警报违规的大小而变化

创建伸缩规则

* 规则名称

名称2~64个字符，以大小写字母、数字或中文开头，可包含点号（.）、下划线（_）或中划线（-）

* 伸缩规则类型 ☒ 简单规则 ☐ 步进规则 ☐ 目标追踪规则 ☐ 预测规则

* 执行的操作

增加“或”减少“选项最多只能支持500台，否则报错
调整至N台”以及“增加或减少N%”一次只能触发500台实例的伸缩活动

冷却时间 秒

- ① 在扩容或缩容时，可以通过[生命周期挂钩](#)在以下场景中完成ECS实例的定制化配置：
扩容时，对伸缩组新创建的ECS实例，在加入伸缩组前进行个性化配置，比如在ECS内运行特定脚本等；
缩容时，对伸缩组即将释放的ECS实例，在释放之前进行个性化配置，比如将ECS内的日志进行拷贝等；

确认

取消

弹性伸缩

伸缩组管理

自动触发任务管理

定时任务

报警任务

问题诊断

垂直伸缩

标签

一步一步创建弹性伸缩

常见问题

弹性伸缩 / 报警任务

产品动态 帮助文档

报警任务

系统监控 自定义监控

创建报警任务

报警任务ID

请输入报警任务ID

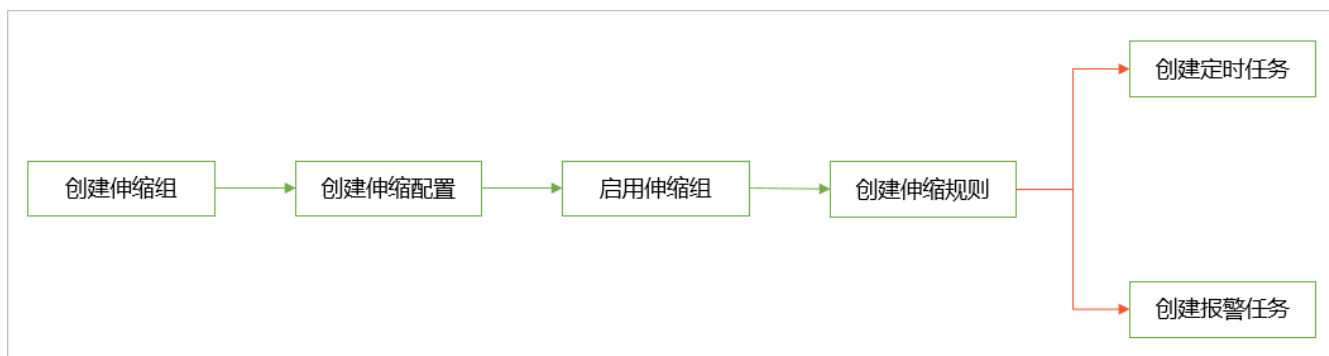
搜索

报警任务名称/ID	状态 (全部)	监控资源	监控类型	统计周期	生效周期	触发伸缩的条件	报警触	操作
ecs-web-系统负载高 asg-bp12o63alq70ldm3024_c52b9f12-db3f-424c-af45-10b6b6099172	正常	伸缩组 asg-bp12o63alq70ldm3024	系统监控	1分钟	全不生效	(Agent) 系统平均负载 Average (平均值) 连续 1 次 >= 0.5	伸缩组 bp12o 报警触	停用 删除 修改 修改触发规则

共有 1 条

< 1 >

10 条/页



13. 总结

- 阿里云架构
- DNS,CDN,WAF,SLB(CLB) ALB , ECS, RDS,NAS/OSS, ESS
- EIP,NAT网关（共享上网，端口映射）
- VPC互联