

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 概述

7.2 创建bucket

7.2 应用

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

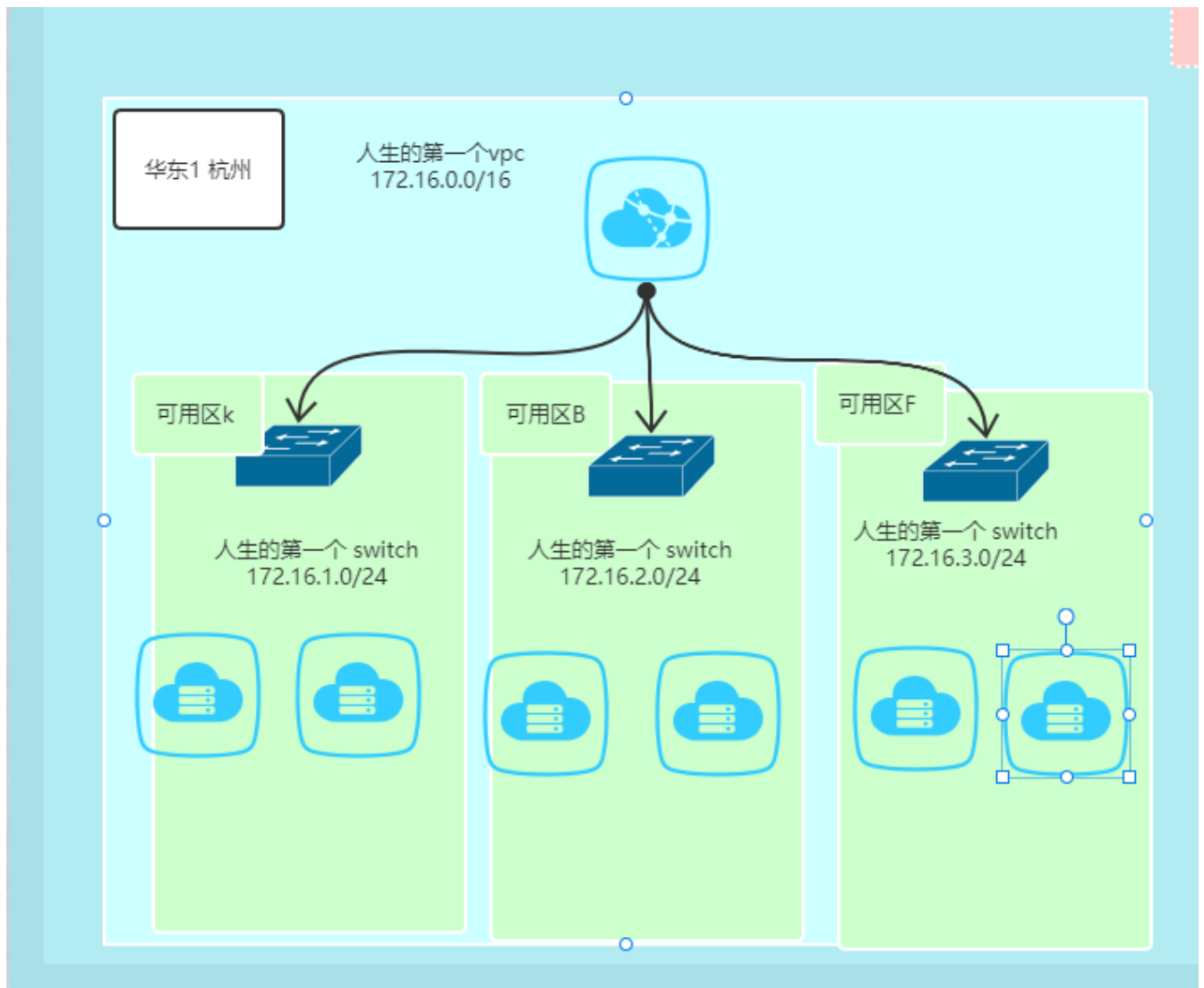
2. 术语

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](#)

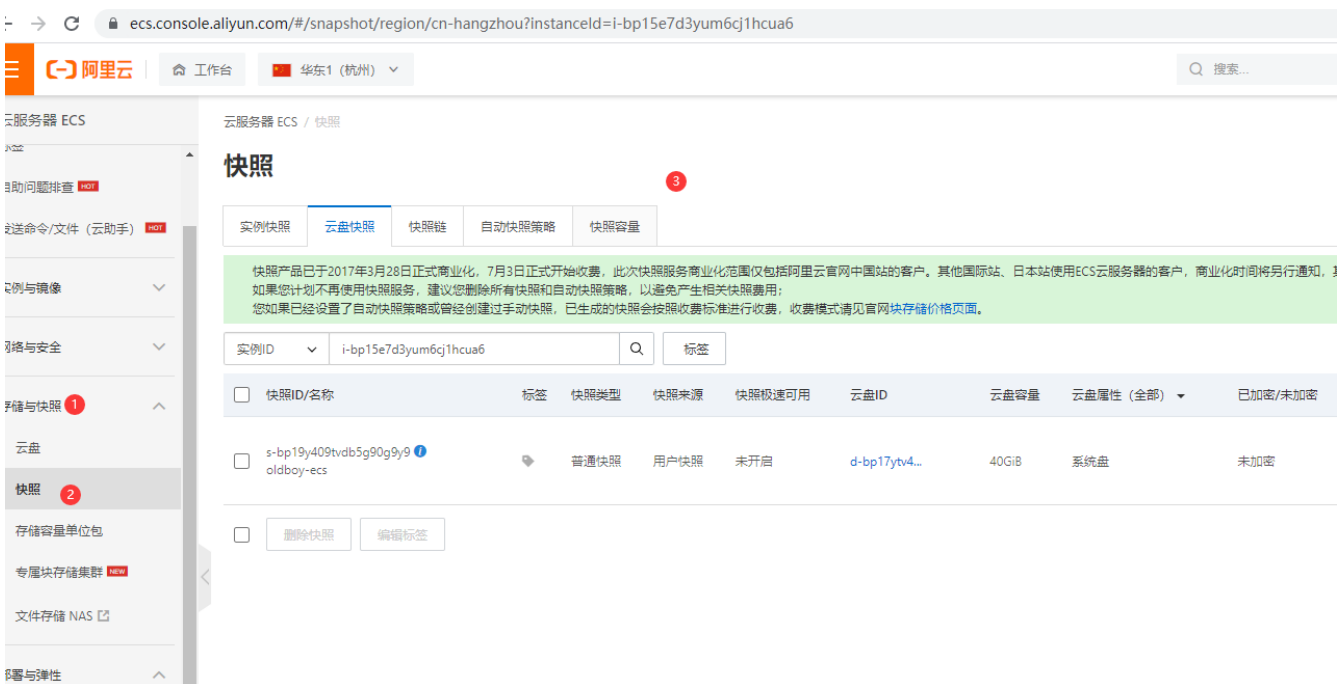
① 安全组类似防火墙功能，用于设置网络访问控制。您也可以到管理控制台 [新建安全组](#) [安全FAQ](#)

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 ①

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-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

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

云服务器 ECS

小册

自助问题排查 HOT

发送命令/文件 (云助手) HOT

实例与镜像 1

实例

镜像 2

弹性容器实例 ECI NEW

专有宿主机 DDH

云盒 NEW

超级计算集群

预留实例券

资源保障 NEW

节省计划 NEW

网络与安全

安全组

弹性网卡

密钥对

专有网络 VPC NEW

云服务器 ECS / 镜像

镜像

推荐使用镜像构建服务快速构建镜像, [点击创建](#) NEW

创建镜像

立即创建 运维编排创建

从一个已有的实例或快照创建新镜像。

更新镜像

镜像构建

选择已有镜像, 使用镜像构建服务 (ImageBuilder) 文本化定制镜像内容, 快速完成镜像的更新、共享、分发。

复制 复制

自定义镜像

公共镜像

共享镜像

镜像市场

镜像族系

搜索镜像族

全部镜像

镜像名称

输入镜像名称查询

Q

标签筛选

<input type="checkbox"/>	镜像ID/名称	镜像族系	标签	操作系统
<input type="checkbox"/>	m-bp1gq1snhhguf5dap35 web-nginx	未指定		
<input type="checkbox"/>	m-bp1gh7gke2aig3tb0fqI oldboy-76-v8	未指定		

NAS文件系统 / 文件系统列表

文件系统列表

创建文件系统

文件系统类型: 全部

文件系统ID

请输入

Q

标签筛选

C

☐

文件系统 ID/名称

标签

类型

存储规格

可用区

挂载点

使用量/总容量

计费方式

数据生命周期

加密

状态

操作

☐

02ca4462ce
nas-oldboy77

通用型NAS
NFS协议

性能型

华东 1 可用区 B

1

0 B / 1 PiB

按量付费

未启用 [配置策略](#)

不加密

✓ 运行中

[监控](#) | [管理](#) | [更多](#)

☐

[添加标签](#)

[删除标签](#)

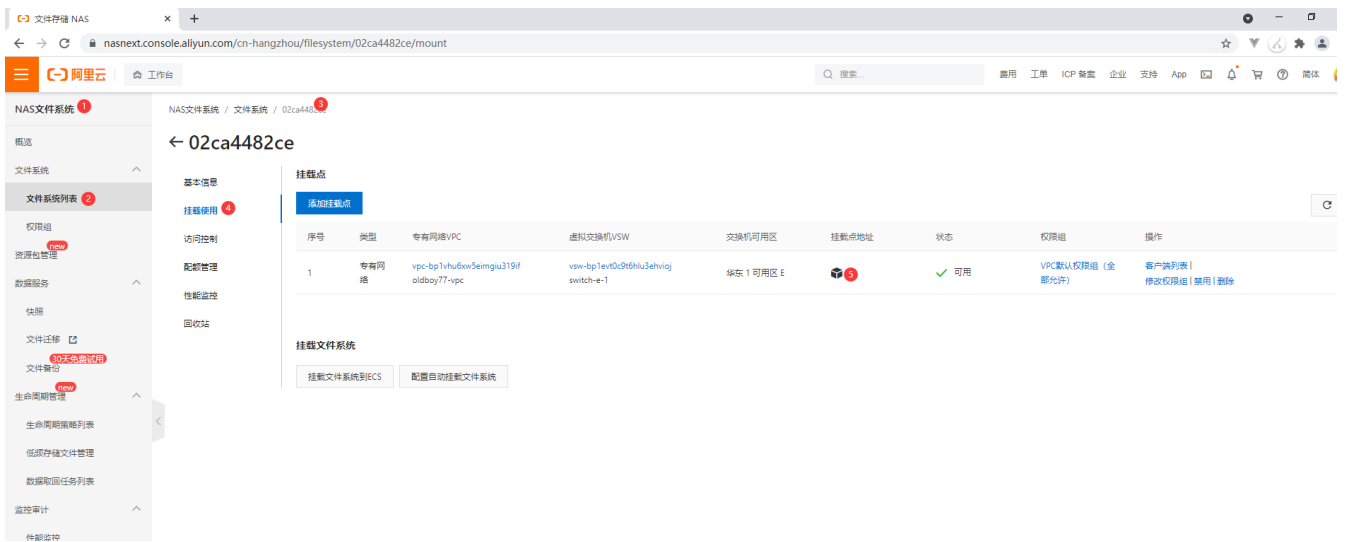
每页显示 10

共1条

[< 上一页](#)

[1](#)

[下一页 >](#)



- 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 \(DDL\)](#)

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。特殊符号包括! @ # \$ % ^ & * () _

* 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

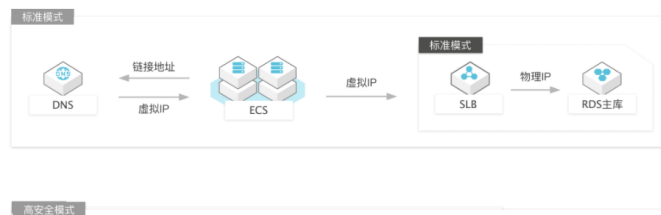
设置白名单后才显示地址

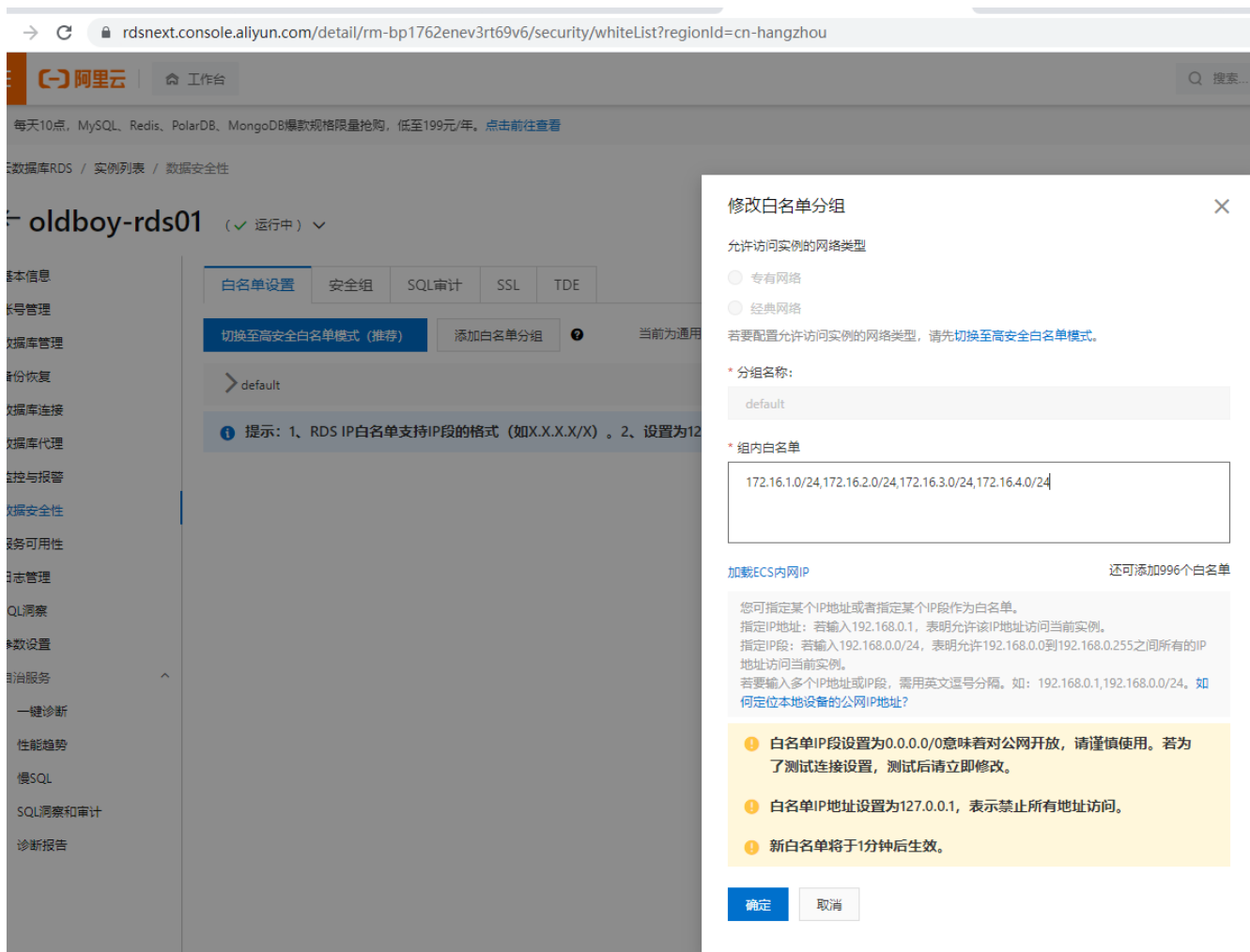
内网端口

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

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 概述

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 * 存储名称，用于区分不同存储

空间大小 * (GB)

Access Key ID * 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 * 创建空间时填写的Bucket名称

地域节点 * Endpoint

存储目录 * 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](#)