

# 可视化架构运维实践

(上册)

## 云上架构生命周期管理 所见即所得

最佳实践能力中心



在云计算越来越趋于基础设施化的今天，大中小客户使用云时通常会遇到的一些挑战，阿里云提供了大量的云服务，将云服务配置成客户的应用架构需要一定的专业知识，客户云资源分散在不同的云服务中，不便于从应用架构的角度来开通、运维、管理资源，阿里云空中架构师云速搭 CADT 是一款为上云应用提供自助式云架构管理的产品。



阿里云开发者“藏经阁”

海量电子手册免费下载

# 前言

所见即所得（英语：What You See Is What You Get，缩写：WYSIWYG）是由菲利普·威尔逊（Flip Wilson）所提出的一种电脑文本编辑器方面的技术，使得编辑文字时在屏幕上直接呈现最终显示效果，如打印到纸张上的效果，故也称可视化操作。

在云计算越来越趋于基础设施化的今天，大中小客户使用云时通常会遇到的一些挑战，阿里云提供了大量的云服务，将云服务配置成客户的应用架构需要一定的专业知识，客户云资源分散在不用的云服务中，不便于从应用架构的角度来开通、运维、管理资源，阿里云空中架构师云速搭 CADT 是一款为上云应用提供自助式云架构管理的产品。

云速搭 CADT 是一款为上云应用提供自助式云架构管理的产品，显著地降低应用云上管理的难度和时间成本。本产品提供丰富的预制应用架构模板，同时也支持自助拖拽方式定义应用云上架构；支持较多阿里云服务的配置和管理。用户可以方便的对云上架构方案的成本、部署、运维、回收进行全生命周期的管理。



# 目录

1. 可视化运维工具云速搭 CADT 基本功能介绍	13
2. 云速搭使用技巧	15
2.1. 分享自定义模板给其他用户使用	15
2.2. 使用自定义镜像创建 ECS	22
2.3. 为 ECS 定义多个安全组	24
2.4. 资源探查	26
3. 云速搭部署基础资源	31
3.1. 云速搭架构设计入门	31
3.1.1. 设计应用架构	32
3.1.2. 配置资源参数	34
3.1.2. 部署应用	46
3.2. 云速搭部署 EIP 实现共享带宽/流量包管理	55
3.2.1. 云速搭架构设计	55
3.2.2. 设计应用架构	57
3.2.3. 共享流量包部署	58
3.2.4. 共享宽带包部署	63
3.3. 云速搭部署 CLB 实现负载分发	72
3.3.1. 云速搭创建 CLB 架构设计	72
3.3.2. 通过云速搭 CADT 部署资源	74
3.3.3. 验证通过 CLB 转发到 ECS 实现负载分发	84
3.3.4. 验证 CLB 挂载 SSL 证书实现 https 转发	88
3.4. 云速搭部署和导入公网型负载均衡 CLB	91
3.4.1. 云速搭架构设计入门	91
3.4.2. CADT 部署公网型 CLB	92
3.4.3. 创建基础网络资源	92
3.4.4. 新建公网型 CLB	94
3.4.5. 导入已保有公网型 CLB	96
3.4.6. 保存架构图	97
3.4.7. 执行导入和部署	98
3.4.7.1. 执行导入和部署	98
3.4.7.2. 执行部署新资源	99

3.5.云速搭部署 ALB 实现负载分发.....	102
3.5.1.云速搭部署 ALB 架构设计.....	102
3.5.2.通过云速搭 CADT 部署资源.....	105
3.5.3.验证通过 ALB 转发到 ECS 实现负载分发.....	115
3.5.4.验证通过 ALB 转发到 CLB 实现负载分发.....	119
3.5.5.验证通过 ALB 转发到 ACK 集群实现负载分发.....	128
3.6.云速搭-NAT 网关部署及应用.....	142
3.6.1.云速搭架构设计.....	142
3.6.2.设计应用架构.....	143
3.6.3.配置资源参数.....	145
3.6.4.NAT 部署.....	157
3.6.4.1.NAT+ECS 粒度.....	162
3.6.4.2.NAT+VPC 粒度.....	164
3.6.4.3.NAT+VSW 粒度.....	165
3.6.4.4.NAT 共享流量包.....	166
3.7.云速搭部署智能接入网关 SAG APP.....	167
3.7.1.云速搭架构设计入门.....	167
3.7.2.设计过程.....	168
3.7.3.部署过程.....	170
3.7.4.验证过程.....	172
3.8.云速搭部署云企业网 CEN.....	178
3.8.1.云速搭架构设计入门.....	178
3.8.2.设计过程.....	179
3.8.3.部署过程.....	187
3.8.4.验证过程.....	190
3.9.云速搭部署 NAS 文件系统.....	193
3.9.1.云速搭架构设计.....	193
3.9.2.通过云速搭 CADT 部署资源.....	195
3.9.3.验证 ECS 挂载 NAS 文件系统.....	204
3.10.云速搭部署混合云备份 HBR.....	207
3.10.1.云速搭架构设计入门.....	207
3.10.2.设计过程.....	208
3.10.3.部署过程.....	215
3.10.4.验证过程.....	219
3.11.云速搭部署 Web 应用防火墙 WAF.....	224
3.11.1.部署按量的 WAF 服务.....	224
3.11.1.1.创建应用.....	224
3.11.1.2.部署应用.....	227

3.11.2.开通包年包月的 WAF 服务	232
3.11.2.1.创建应用	232
3.11.2.2.部署应用	234
3.12.云速搭部署堡垒机	239
3.12.1.云速搭架构设计入门	239
3.12.2.应用架构设计	240
3.12.3.资源参数配置	243
3.12.4.部署应用	247
3.13.云速搭部署云防火墙	253
3.13.1.云速搭架构设计入门	253
3.13.2.创建应用	254
3.13.3.部署应用	257
3.14.云速搭部署云安全中心	261
3.14.1.云速搭架构设计入门	261
3.14.2.应用架构设计	262
3.14.3.部署应用	269
3.15.云速搭部署安全组	276
3.15.1.云速搭架构设计入门	276
3.15.2.应用架构设计	277
3.15.3.部署应用	285
3.15.4.CADT 部署企业安全组	295
3.16.云速搭部署 ECS 最佳实践	300
3.16.1.云速搭架构设计	300
3.16.2.准备工作	300
3.16.3.应用架构设计	303
3.16.4.部署应用	312
3.17.云速搭部署 GPU 云服务器	318
3.17.1.云速搭架构设计	318
3.17.2.应用架构设计	320
3.17.3.部署应用	327
3.18.云速搭部署 ECS 部署集	334
3.18.1.云速搭架构设计	334
3.18.2.应用架构设计	335
3.18.3.部署应用	344
3.19.云速搭部署弹性裸金属服务器	351
3.19.1.云速搭架构设计	351
3.19.2.应用架构设计	352
3.19.3.部署应用	358

3.20.云速搭部署 DTS 应用	365
3.20.1.云速搭架构设计	365
3.20.2.应用架构设计	366
3.20.3.配置资源参数	372
3.20.4.部署应用	375
3.20.5.DTS 实现 RDS 数据同步	381
3.21.云速搭部署风险识别 SAF 最佳实践	392
3.21.1.云速搭架构设计	392
3.21.2.CADT 设计部署风险识别服务	393
3.21.3.基于已有应用部署	398
<b>4.云速搭部署容器、大数据、数据库</b>	<b>401</b>
4.1.云速搭部署 Elasticsearch 应用	401
4.1.1.云速搭架构设计入门	401
4.1.2.应用架构设计	402
4.1.3.部署应用	409
4.2.云速搭部署 Flink 应用	415
4.2.1.云速搭架构设计入门	415
4.2.2.应用架构设计	416
4.2.3.配置资源参数	421
4.2.4.部署应用	424
4.3.云速搭部署云数据库 RDS	430
4.3.1.云速搭架构设计入门	430
4.3.2.设计应用架构	431
4.3.3.MySQL 部署	434
4.3.4.SQL Server 部署	444
4.3.5.PostgreSQL 部署	450
4.3.6.PolarDB 部署	455
4.4.云速搭部署数据库审计	462
4.4.1.云速搭架构设计入门	462
4.4.2.应用架构设计	463
4.4.3.部署应用	469
4.5.云速搭部署 SLS 实现日志采集处理分析	475
4.5.1.云速搭架构设计入门	475
4.5.2.通过云速搭 CADT 部署资源	477
4.5.3.Logtail 日志采集处理分析	485
4.5.3.1.创建日志服务 Project 和 Logstore	485

4.5.3.2. 安装 Logtail 日志采集客户端	489
4.5.3.3. 配置主账号 AliUid	490
4.5.3.4. 配置接入日志库	491
4.5.3.5. 云服务器上模拟产生 Nginx 文本日志	498
4.5.3.6. 通过日志服务仪表盘进行可视化分析	501
4.6. 云速搭部署 Redis 应用	504
4.6.1. 云速搭架构设计入门	504
4.6.2. 应用架构设计	505
4.6.3. 配置资源参数	508
4.6.4. 部署应用	510
4.7. 云速搭部署 ADB 应用	516
4.7.1. 云速搭架构设计入门	516
4.7.2. 应用架构设计	517
4.7.3. 配置资源参数	520
4.7.4. 部署应用	522
4.8. 云速搭部署 MongoDB 应用	528
4.8.1. 云速搭架构设计入门	528
4.8.2. 应用架构设计	529
4.8.3. 配置资源参数	533
4.8.4. 部署应用	534
4.9. 云速搭部署 EMR	540
4.9.1. 云速搭架构设计入门	540
4.9.2. 应用架构设计	541
4.9.3. 部署应用	547
4.9.4. 导入已保有 EMR 应用架构	554
4.10. 云速搭部署 ACK 集群	560
4.10.1. 云速搭架构设计	560
4.10.2. 通过 CADT 创建 ACK 集群	563
4.10.2.1. 手动创建 ACK 集群	563
4.10.2.2. 基于官方模板新建 ACK 集群	571
4.10.3. 部署应用	572
4.10.4. 导入已保有 ACK 应用架构	578
<b>5. 资源组合部署</b>	<b>585</b>
5.1. 云速搭部署 E-HPC+NAS 应用	585
5.1.1. 云速搭架构设计入门	585
5.1.2. 应用架构设计	586

5.1.3. 部署应用	593
5.1.4. 部署结果验证	598
5.2. 云速搭部署挂载 CPFS 的 E-HPC	600
5.2.1. 云速搭架构设计入门	600
5.2.2. 部署 CPFS 和 ECS	603
5.2.2.1. 创建基础网络资源	603
5.2.2.2. 创建 CPFS	606
5.2.2.3. 创建 ECS 并挂载 EIP	607
5.2.2.4. 保存架构图	610
5.2.2.5. 执行部署	610
5.2.2.6. 记录用于制作镜像的 ECS 私网 IP	614
5.2.2.7. 确认 CPFS 挂载点状态并记录初始密码	614
5.2.3. 制作镜像	616
5.2.3.1. 允许远程登录 CPFS 管理节点	616
5.2.3.2. 远程登录 CPFS 客户端管理节点 qr001	617
5.2.3.3. 配置 CPFS 管理节点对客户端节点的免密钥登录	618
5.2.3.4. 记录 CPFS 管理节点的 Quorum 和 Contact 内容	620
5.2.3.5. 远程登录用于制作镜像的 ECS 实例	620
5.2.3.6. 在用于制作镜像的 ECS 上安装 CPFS 客户端	621
5.2.3.7. 制作自定义镜像	623
5.2.4. 部署 E-HPC	625
5.2.4.1. 创建 E-HPC	625
5.2.4.2. 执行部署	627
5.2.4.3. 确认 E-HPC 集群运行正常	628
5.3. 云速搭基于资源组部署云资源	629
5.3.1. 云速搭架构设计入门	629
5.3.2. 权限管理	631
5.3.2.1. 创建用户和用户组	631
5.3.2.2. 创建资源组	635
5.3.2.3. 资源组授权	637
5.3.2.4. 添加授权架构	639
5.3.3. 云资源部署	641
5.3.3.1. 设计资源架构	641
5.3.3.2. 部署资源	643
5.3.4. 权限验证	646
5.3.4.1. 验证资源组支持的产品权限	646
5.3.4.2. 自定义策略管理产品	650
5.3.4.3. 查看 CADT 架构	654

5.3.4.4.查看应用组监控.....	655
5.3.4.5.跨资源组转移资源.....	656
5.4.云速搭部署 Hologres 应用.....	658
5.4.1.云速搭架构设计.....	658
5.4.2.应用架构设计.....	659
5.4.3.配置资源参数.....	664
5.4.4.部署应用.....	666
5.5.云速搭部署 WAF 和 SLB 透明接入应用.....	674
5.5.1.云速搭架构设计入门.....	674
5.5.2.设计 WAF 和 SLB 透明接入架构.....	675
5.5.3.部署应用.....	685
5.5.4.透明接入.....	690
5.6.云速搭部署 ESS 实现弹性伸缩.....	691
5.6.1.通过云速搭创建 ESS.....	691
5.6.2.通过云速搭 CADT 部署资源.....	693
5.6.3.验证 ESS 弹性伸缩能力.....	706
5.7.云速搭部署云上网络组网.....	714
5.7.1.组网设计.....	714
5.7.2.绘制基础网络资源.....	717
5.7.3.绘制网关资源.....	723
5.7.4.绘制云企业网.....	726
5.7.5.绘制说明类图标.....	728
5.7.6.保存架构图.....	728
5.7.7.执行部署.....	729
5.7.8.检查 CEN 网络资源挂载情况.....	731
5.8.云速搭部署高可用虚拟 IP HaVIP.....	733
5.8.1.云速搭架构设计入门.....	733
5.8.2.设计过程.....	734
5.8.3.部署过程.....	744
5.8.4.验证过程.....	747
5.9.单账号跨 VPC 共享 NAT 网关.....	755
5.9.1.云速搭 CADT 架构设计.....	755
5.9.2.CADT 部署单账户跨 VPC 共享 NAT 网关.....	756
5.9.3.验证过程.....	761
<b>6.云速搭权限管理及场景设计.....</b>	<b>767</b>
6.1.前置条件.....	767

6.2.云速搭权限管理概述.....	768
6.3.权限管理场景设计.....	769
6.3.1.企业 IT 管理场景.....	769
6.3.2.设计权限管控策略.....	769
6.3.3.权限管控策略实现.....	770
6.4.权限管理策略配置.....	773
6.4.1.创建资源组.....	773
6.4.2.创建 RAM 用户组.....	774
6.4.3.为 RAM 用户组授权.....	776
6.4.4.创建 RAM 用户并加入用户组.....	779
6.4.5.CADT 应用加入资源组.....	781
6.5.权限场景验证.....	785
6.5.1.角色权限验证.....	785
6.5.2.资源组归属验证.....	791
6.6.自定义权限（可选）.....	794
6.6.1.创建自定义权限策略 cadt-full-access.....	794
6.6.2.创建自定义权限策略 cadt-read-only.....	801
6.6.3.使用自定义策略.....	802
<b>7.最佳实践及官方模板.....</b>	<b>803</b>
7.1.企业上云等保三级合规最佳实践.....	803
7.1.1.场景描述.....	803
7.1.2.应用范围.....	803
7.1.3.架构设计.....	803
7.2.云服务器基准性能测试.....	805
7.2.1.场景描述.....	805
7.2.2.解决问题.....	805
7.2.3.架构设计.....	805
7.3.PAI 平台搭建企业级个性化推荐系统.....	807
7.3.1.场景描述.....	807
7.3.2.适用客户.....	807
7.3.3.架构设计.....	807
7.4.基于 ECI 的 ACK 集群高弹性架构.....	810
7.4.1.场景描述.....	810
7.4.2.解决问题.....	810
7.4.3.架构设计.....	810
7.5.阿里云最佳实践频道.....	812
7.6.云速搭 CADT 官方模板计.....	823

<b>8.客户成功.....</b>	<b>814</b>
8.1.最佳实践助力正元智慧上云提效.....	814
8.1.1.客户简介.....	814
8.1.2.客户需求.....	814
8.1.3.客户价值.....	815
8.1.4.客户之声.....	816
8.1.5.查看详情.....	817
8.2.最佳实践助力复星星选项目极速上线成功.....	819
8.2.1.客户简介.....	819
8.2.2.客户需求.....	819
8.2.3.客户价值.....	819
8.2.4.客户之声.....	820
8.2.5.查看详情.....	821
8.3.云速搭助力青莲实现极速项目交付.....	822
8.3.1.客户简介.....	822
8.3.2.客户需求.....	822
8.3.3.客户价值.....	822
8.3.4.查看详情.....	823
8.4.北京乘云至达使用云速搭 CADT 工具快速交付项目.....	824
8.4.1.客户简介.....	824
8.4.2.客户需求.....	824
8.4.3.客户价值.....	824
8.4.4.客户之声.....	825
8.4.5.查看详情.....	826
<b>9.相关资源.....</b>	<b>827</b>

# 1. 可视化运维工具云速搭 CADT 基本功能介绍

## 1、快速生成云上架构

云速搭提供丰富的预制应用架构模板，同时也支持自助拖拽方式定义应用云上架构，显著地降低应用云上管理的难度和时间成本。

- 官方模板  
提供完整可直接部署的资源配置，减少用户操作，用户可根据官方模板配置所需架构图。
- 分享模板  
用户可将绘制的架构图分享给其他用户。
- 自助拖拽  
用户在编辑页面绘制配置所需要使用的相关服务架构图。

## 2、自动化资源部署

在云速搭中对应用架构的可行性进行自动化验证，包括资源关联关系，资源规格等。

- 资源验证  
用户根据绘制的架构图查询对应资源配置是否合法，以及资源是否可用。
- 资源询价  
用户根据架构图查询所要使用的产品价格，可以方便的计算当前部署架构的总成本，支持按照预付费，后付费等多种方式和多种时长计算。
- 资源部署  
一键完成用户配置的所有资源的部署，支持分阶段部署模式，部署失败的资源可以再次进行部署。

## 3、资源探查生成云上架构

利用阿里云配置审计服务提供的资源数据（需先开通配置审计功能），采用交互式自动化探查应用拓扑，快速生成云上架构图，并导入为 CADT 应用，便于用户管理应用架构，提高运维效率。

- 资源信息获取

CADT 通过配置审计获取用户的云上资源及资源间关联关系（需用户授权确认）。

- 生成云资源架构

用户勾选属于云上应用的资源，CADT 将自动生成该应用的拓扑图，并保证资源数据的完整性和正确性。

- 导入云资源为应用

将生成的架构图保存并执行导入操作，将生成 CADT 应用，可以利用 CADT 对应用进行全生命周期管理。

## 2.云速搭使用技巧

### 2.1.分享自定义模板给其他用户使用

#### 操作前提

已获取合作伙伴或其他用户的账号 ID。关于如何查看账号 ID，请参考[如何查看账号 ID](#)。

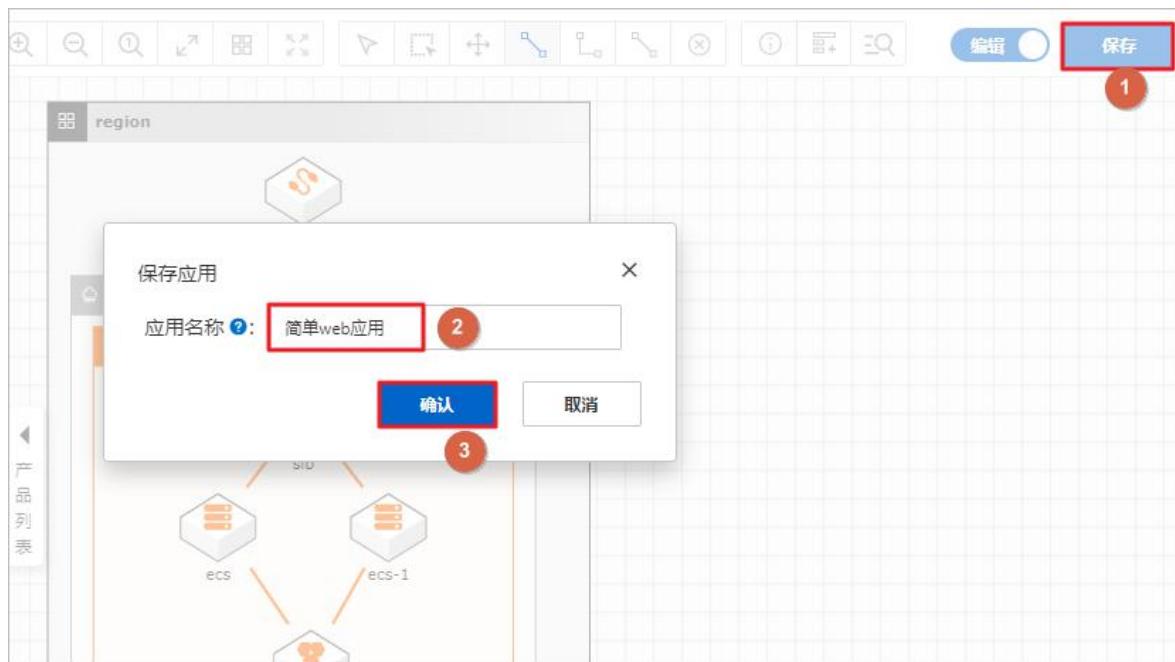
#### 创建自定义模板

步骤 1 登录[云速搭 CADT](#) 控制台。

步骤 2 通过[新建 > 新建空白应用](#)，搭建如下图所示的应用架构作为示例：



步骤3 保存自定义应用，输入应用名称，并单击确认。



步骤4 保存成功后，通过菜单栏下的应用 > 我的应用可以查看到新建的应用。





步骤 5 选择该应用，单击**另存为模板**。



步骤 6 设置模板名称，并根据实际需要选择地域标签及是否需要设置为默认模板，并单击确认。



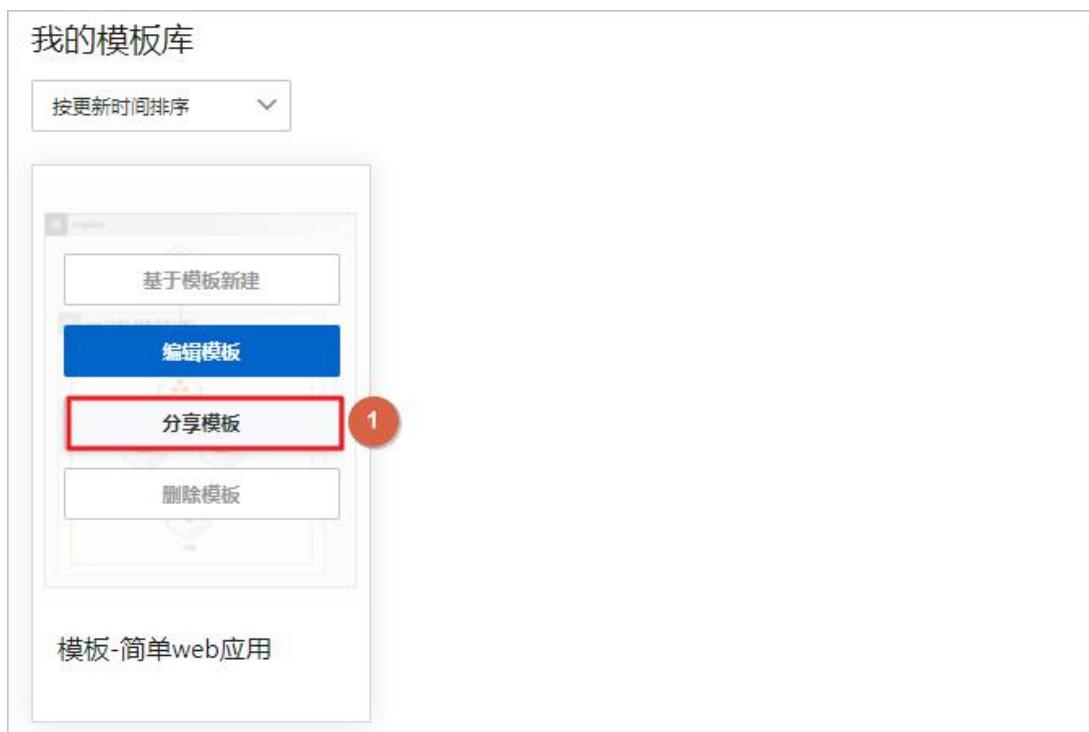
步骤 7 模板添加成功后，从菜单栏下的新建 > 我的模板库新建下可以看到自定义模板。



## 分享模板

步骤 1 分享者登录[云速搭 CADT](#) 控制台。

步骤 2 在[我的模板库](#)页面，选择需要分享的模板，单击分享模板。

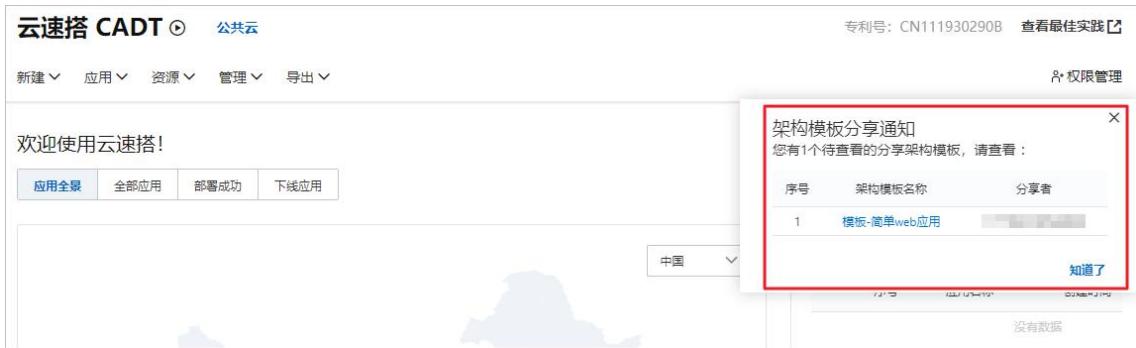


步骤 3 输入对应用户 ID，单击授权。



## 被授权用户查看分享结果

步骤 1 被授权用户登录**云速搭 CADT** 控制台，可以看到架构模板分享通知，包括架构模板名称和分享者。



步骤 2 通过菜单栏下的**新建 > 我的模板库新建**进入**我的模板库**页面，可以看到其他用户分享给自己的模板。



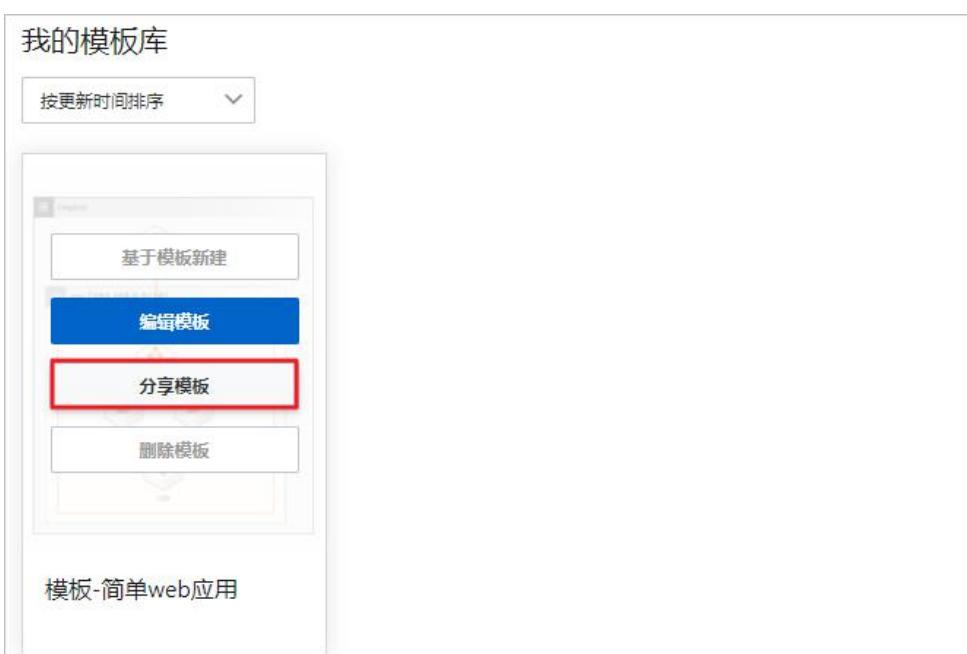
步骤 3 被授权用户可以基于其他用户分享给自己的模板定制应用。



## 撤销模板分享

如果分享者需要撤销被授权用户使用模板的权限，执行以下操作：

步骤 1 分享者登录云速搭 CADT 控制台，在我的模板库页面，选择对应的模板，单击**分享模板**。



步骤 2 在**分享模板**对话框中，选择需要撤销使用权限的用户，单击**撤销并确认**即可。



## 2.2. 使用自定义镜像创建 ECS

云速搭 CADT 支持通过自定义镜像创建 ECS 实例，本文为您介绍具体操作。

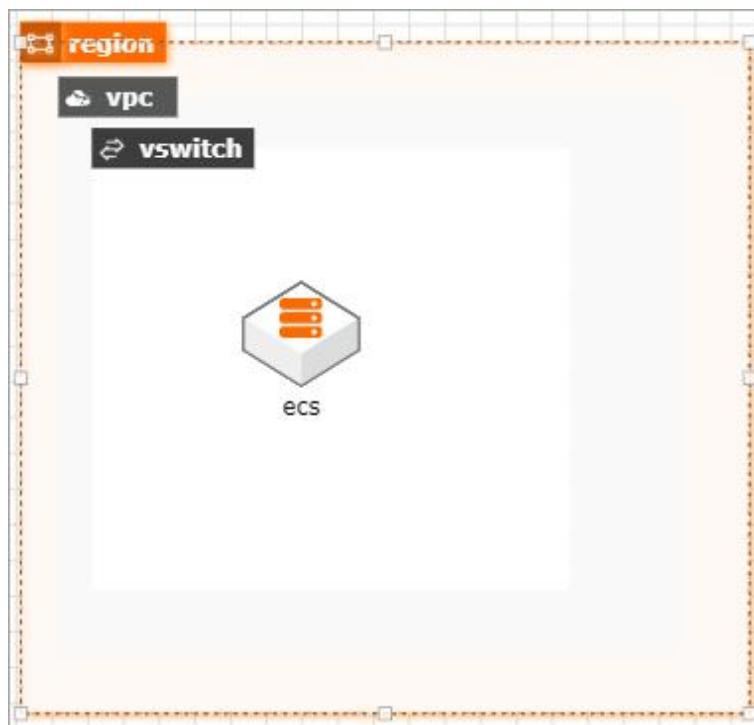
### 操作前提

已在对应地域创建自定义镜像，如未创建，请参考[创建自定义镜像](#)。

### 操作步骤

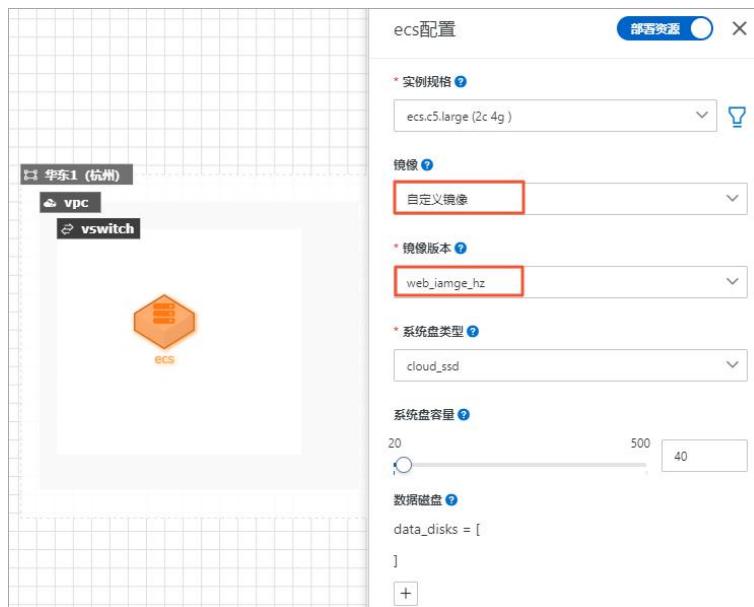
步骤 1 登录[云速搭 CADT](#)控制台。

步骤 2 在菜单栏处选择**新建 > 新建空白应用**，作为演示，此处创建一个单 Region 单可用区下的 ECS 实例。



步骤 3 依次完成专有网络 VPC、交换机（VSwitch）的配置，在配置 ECS 实例时，注意以下两项参数配置：

- 镜像：选择**自定义镜像**
- 镜像版本：CDT 自动为您同步该地域下的全部自定义镜像，选择对应的版本即可。



步骤 4 配置完成，保存应用，按照页面提示完成部署。

## 2.3.为 ECS 定义多个安全组

云速搭 CADT 支持创建安全组资源，可以为 ECS 定义多个安全组。

### 操作步骤

1. 登录[云速搭 CADT](#) 控制台。
2. 在菜单栏处选择**新建 > 新建空白应用**，作为演示，此处创建一个单 Region 单可用区下的 ECS 实例，然后依次完成专有网络 VPC、交换机（VSwitch）和 ECS 参数配置，可以看到，此时 ECS 无法选择到**安全组**。



3. 从左侧菜单栏中找到**安全组**资源拖拽到架构图中，设置名称为 sg1，然后双击打开 ECS 配置框，此时在 ECS 安全组配置中可以选到 sg1。



4. 以同样方式，再添加一个安全组 sg2，然后在 ECS 配置项**安全组**处添加 sg2，即为 ECS 实例添加了两个安全组。以此类推，可以为 ECS 实例创建多个安全组。



## 2.4. 资源探查

云速搭 CADT 支持探查云上已保有资源，自动生成应用架构，可视化运维管理。

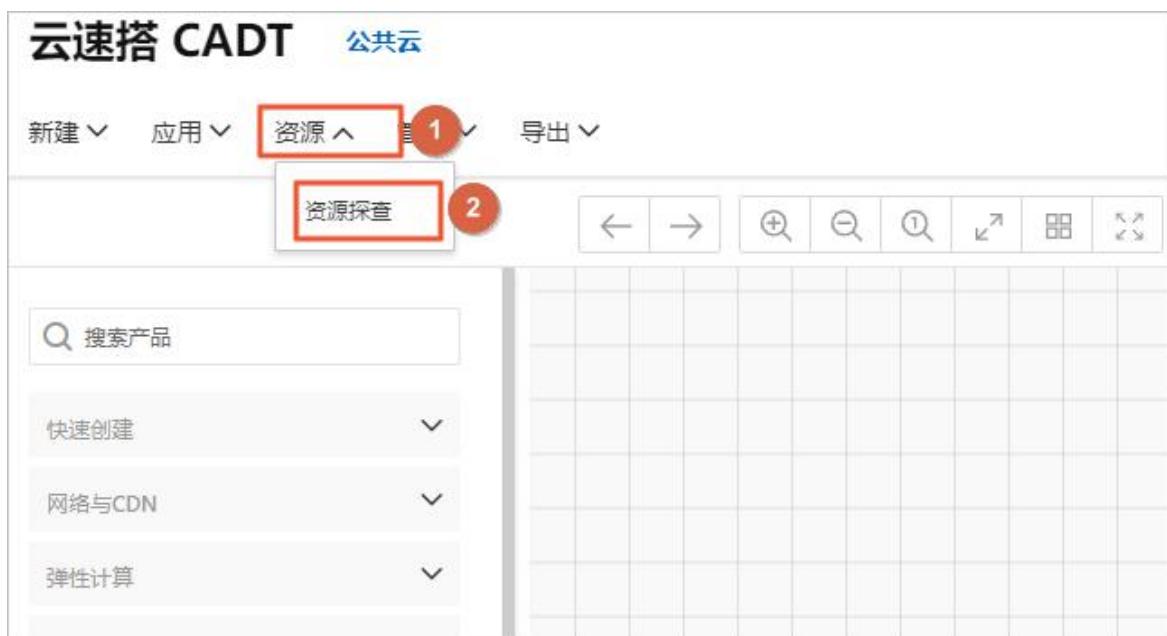
### 探查资源

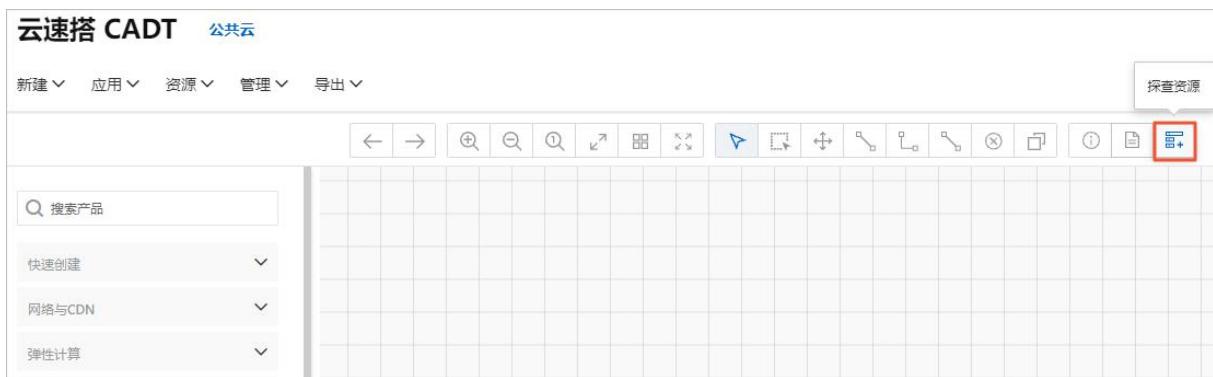
1. 登录云速搭 CADT 管理控制台。

在菜单栏下单击新建 > 新建空白应用，打开一个空白画布。



在当前画布下，单击资源 > 资源探查或者直接单击工具栏中的探查资源按钮。





在选择探查资源对话框中，单击探查资源。



选择探查的区域（不选择默认探查全部区域），单击确定。



等待资源探查完成。



2. 资源探查的结果以**全局资源、区域资源、专有网络资源和交换机资源**进行展示，您可以根据资源所属区域和依赖查询显示。

### 全局资源



**区域资源：**由于探查的是全局资源，CADT 会将您云上各区域下的所有已保有资源探查出来，根据实际需要选择查询显示。

探查结果: 成功

全局资源	<b>区域资源</b>	专有网络资源	交换机资源
区域:	华北2 (北京)		
<input type="checkbox"/> 华北2 (北京) <input type="checkbox"/> 华东2 (上海) <input type="checkbox"/> 华东1 (杭州) <input type="checkbox"/> 美国东部 1 (弗吉尼亚) <input type="checkbox"/> 华南1 (深圳) <input type="checkbox"/> 亚太东南 1 (新加坡)		资源名称 <input type="text"/>	资源ID
		cadt-case	cadt-case

专有网络资源：查询显示特定区域下依赖 VPC 的资源，如安全组。

探查结果: 成功

全局资源	区域资源	<b>专有网络资源</b>	1 交换机资源
区域:	华北2 (北京)	VPC:	vpc-[REDACTED] / vpc-[REDACTED] 2
<input type="checkbox"/> 资源类型 <input type="checkbox"/>		资源名称 <input type="text"/>	资源ID
<input type="checkbox"/> security_group		sg-[REDACTED]	sg-[REDACTED]

交换机资源：查询显示特定区域下依赖依赖交换机的资源，如云服务器 ECS。

探查结果: 成功

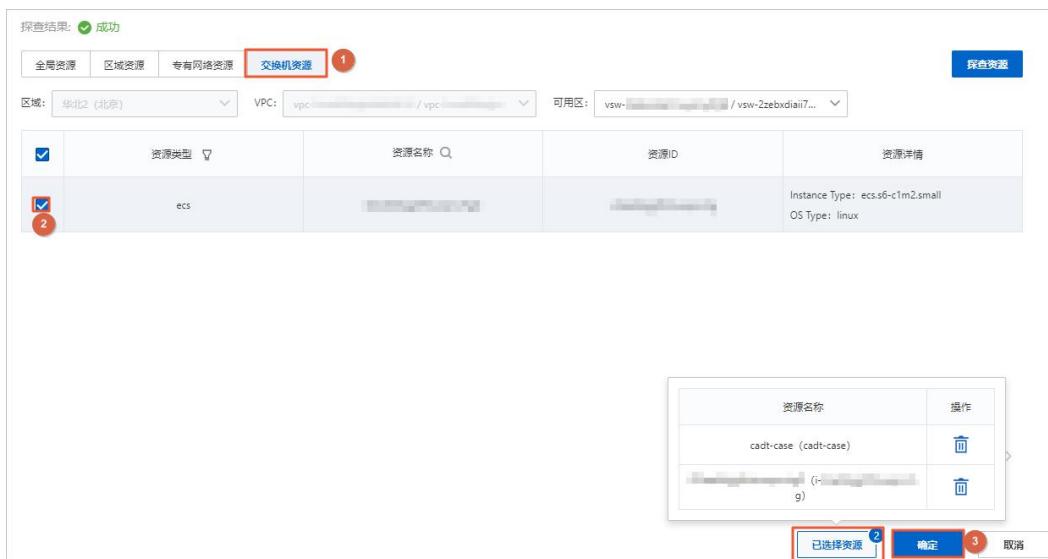
全局资源	区域资源	专有网络资源	<b>交换机资源</b> 1	2
区域:	华北2 (北京)	VPC:	vpc-[REDACTED] / vpc-[REDACTED]	可用区: vsw-[REDACTED] / vsw-[REDACTED]
<input type="checkbox"/> 资源类型 <input type="checkbox"/>		资源名称 <input type="text"/>	资源ID	资源详情
<input type="checkbox"/> ecs		[REDACTED]	[REDACTED]	Instance Type: ecs.s6-c1m2.small OS Type: linux

## 生成应用架构

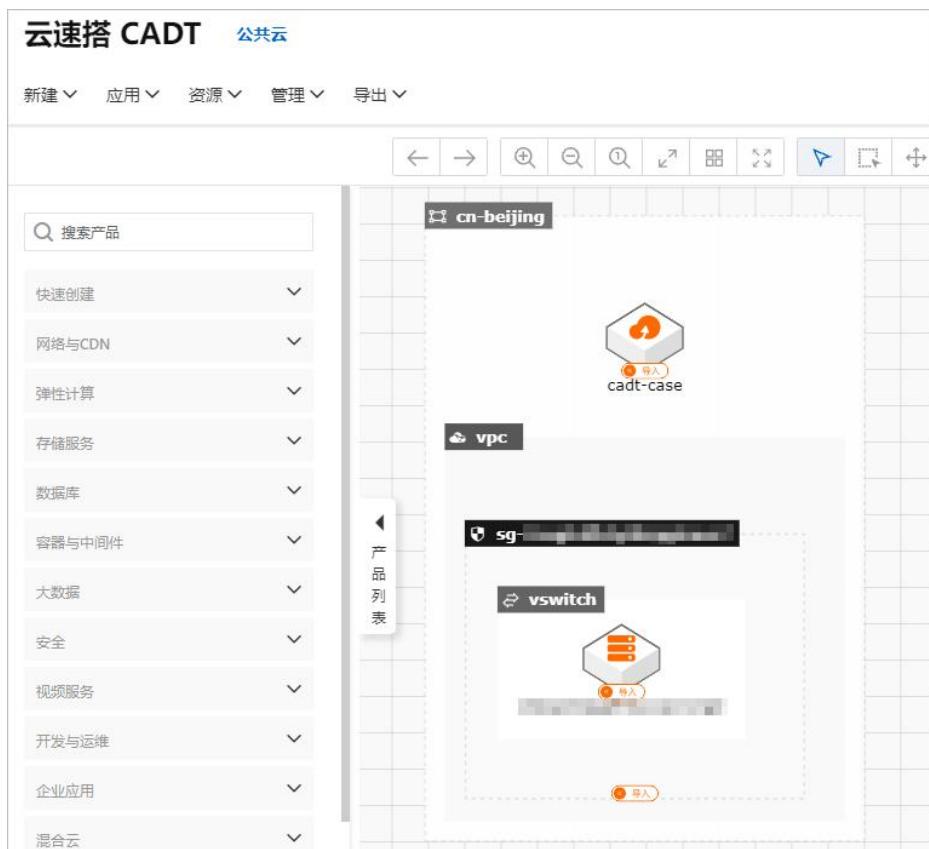
资源探查完成后，CADT 可以将所需的已保有资源生成对应的应用架构，可视化管理云上应用，直观便捷。

1. 在对应的页签下勾选需要生成应用架构的资源，例如选择探查出的对象存储 OSS Bucket 和 ECS 实例，单击**确定**。

**说明：**在已选择资源下可以看到要生成架构图的资源，可以根据情况进行去除。



单击**确定**后，应用架构自动生成，可以更加直观地进行运维管理。



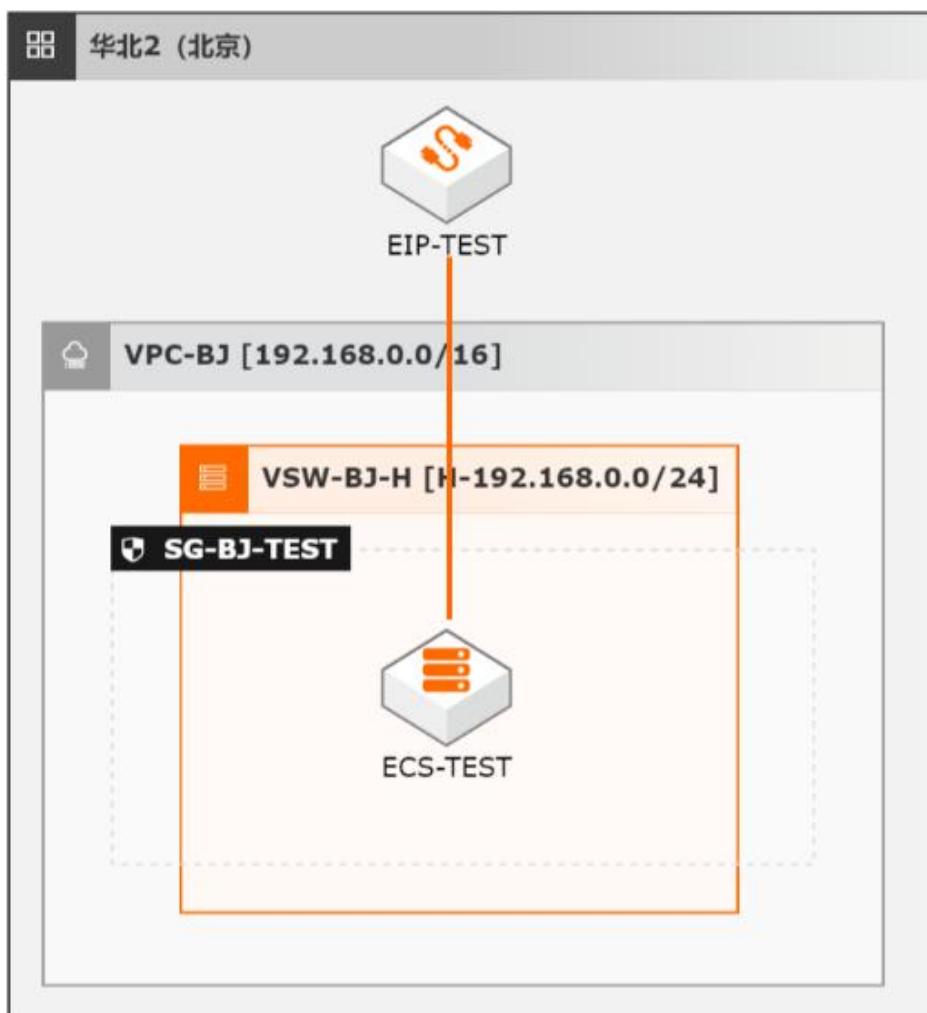
## 3.云速搭部署基础资源

### 3.1.云速搭架构设计入门

作者 | 阿里云资深技术专家 游圣

#### 方案架构

- 通过云速搭实现最简单架构，设计一个 ECS+EIP 简单架构，实现 ECS 可以被公网通过 ssh 访问，ECS 可以访问公网。
- 具备一个默认安全组，通过安全组进行详细的安全策略配置。



## 理解资源级别

每个阿里云资源都有对应的资源级别，在 CADT 进行架构设计时要遵循资源级别开展。本架构中使用的资源及对应的资源级别如下表所示，在进行架构设计时需要用到。

云资源	资源级别
EIP	Region
ECS	VSW
安全组	VPC

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

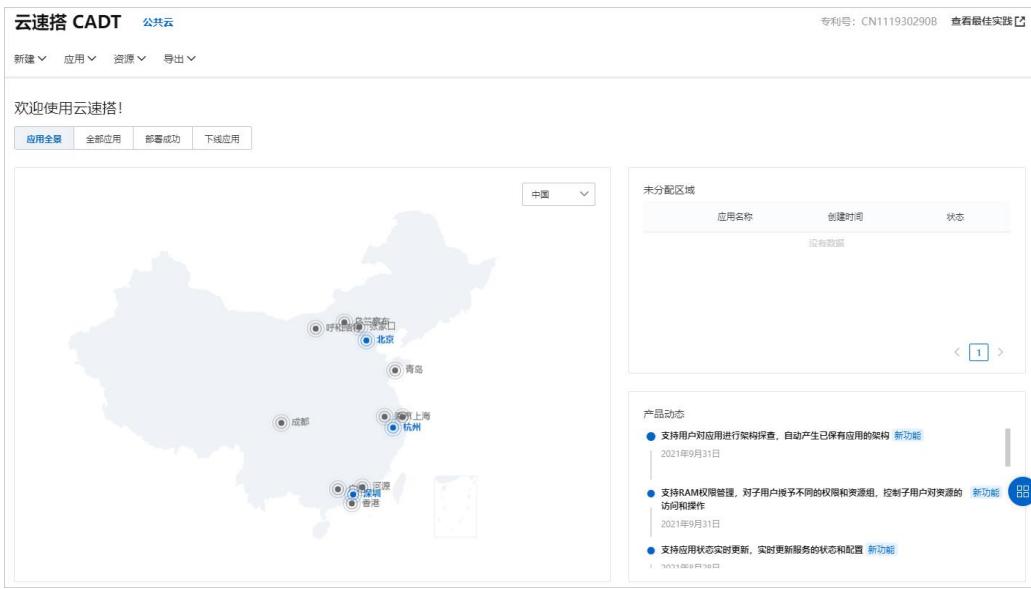
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	VPC-BJ	192.168.0.0/16
AZ	北京 H 可用区	192.168.0.0/24
安全组	SG-BJ-TEST	-

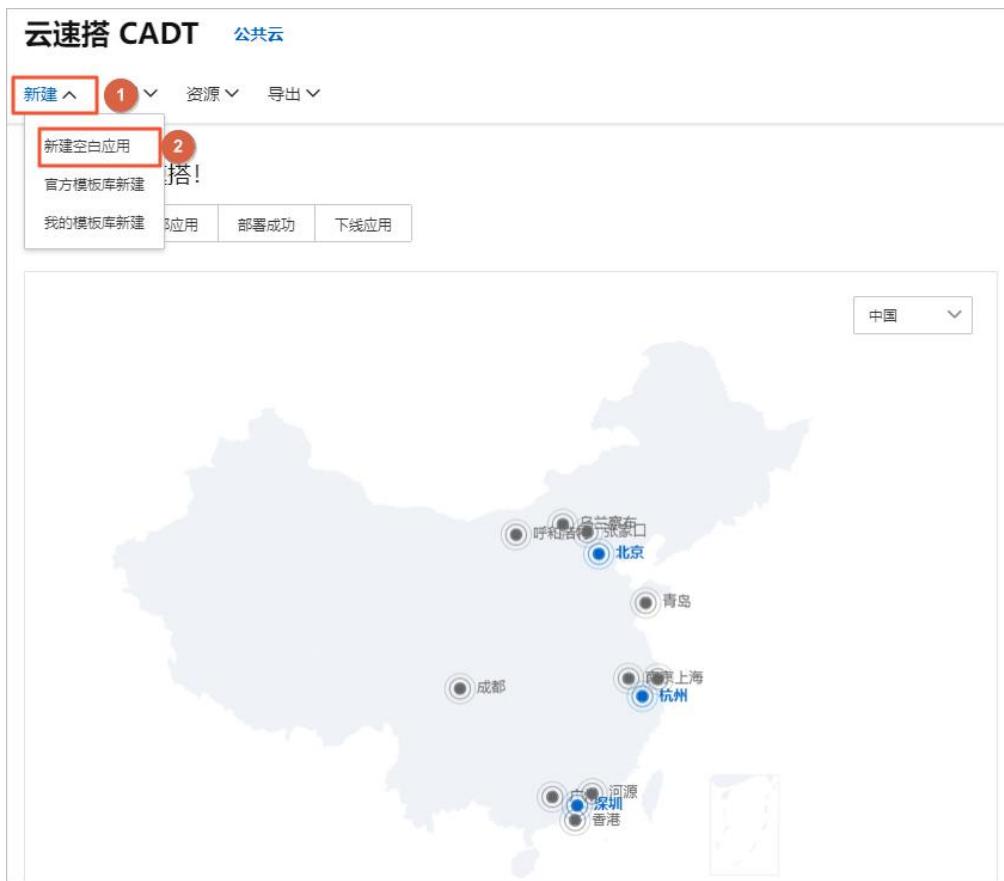
### 3.1.1. 设计应用架构

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

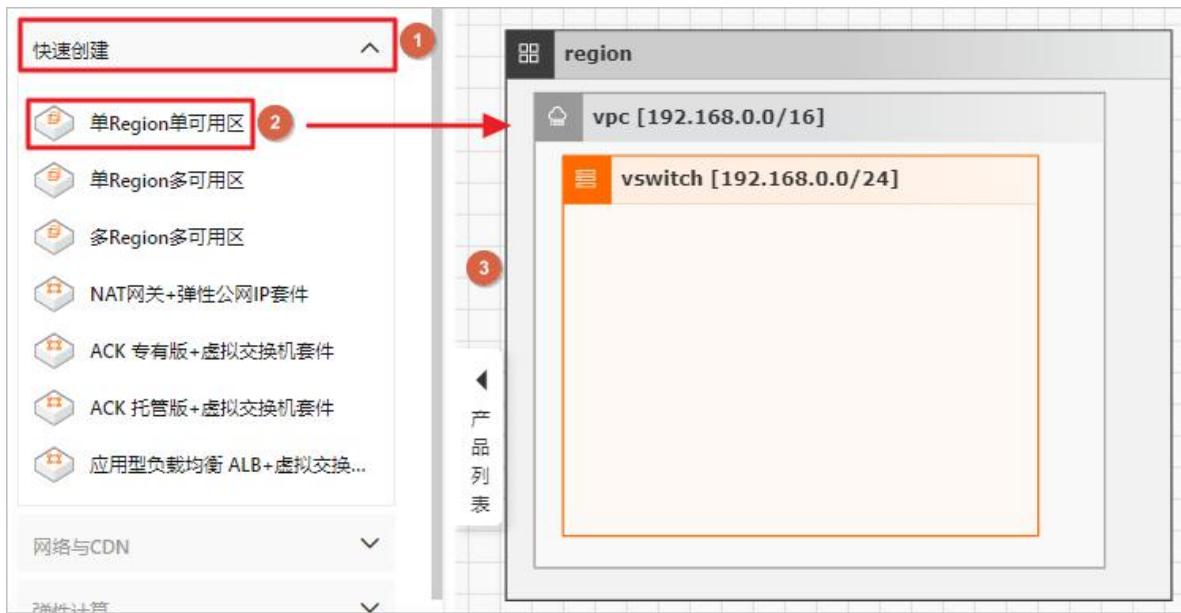
**说明：**如果提示需要开通服务，请根据提示进行开通。



步骤 2 在菜单栏单击新建 > 新建空白应用，打开一个空白画布。



步骤 3 一个完整的应用架构需要先构建网络环境，从左侧工具栏**快速创建**下选择合适的网络拓扑类型，本场景适用**单 Region 单可用区**，单击选中并拖拽到右侧空白画布中。



### 3.1.2. 配置资源参数

#### 操作说明

- 操作方式：在 CADT 双击资源即可配置资源参数。
- 配置顺序：需按**资源级别和依赖**依次进行 Region → AZ → VPC，完成所有配置后，当再次修改应用架构高级别资源参数时，需要再次双击打开低级别资源参数配置框，确认参数配置完整正确。

#### 操作步骤

步骤 1 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 **Region** 框，并在右侧弹框列表中选择**华北 2（北京）** 区域。



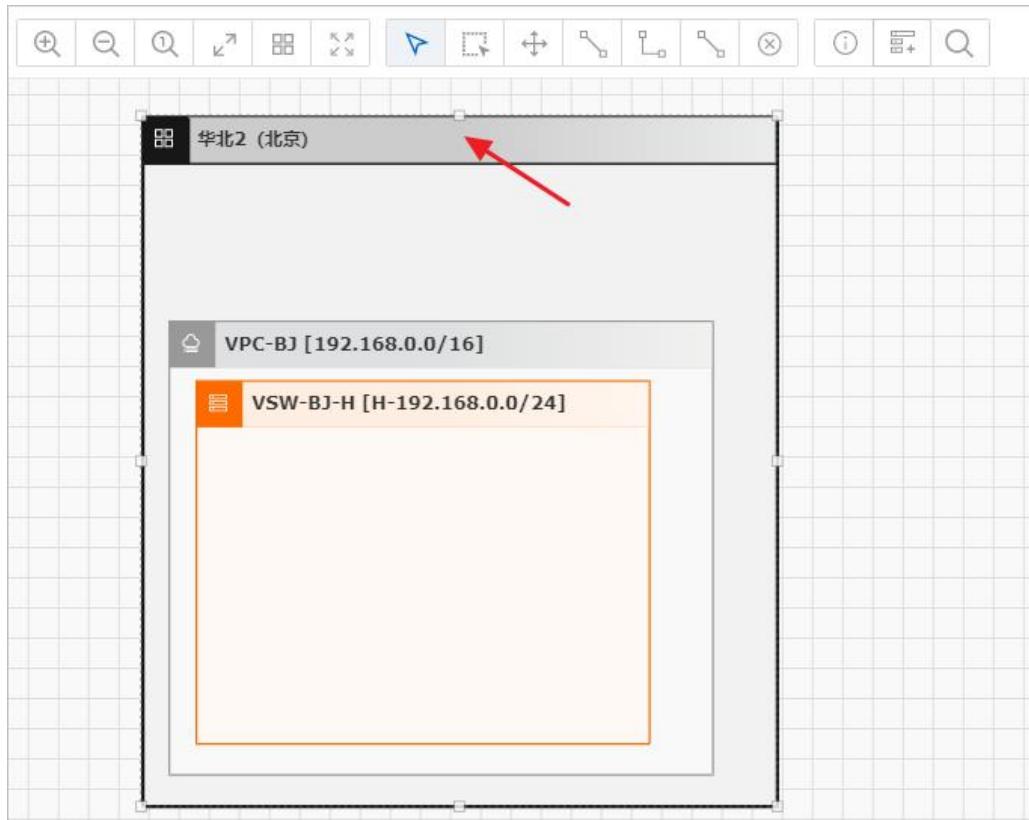
2. 双击配置 VPC：



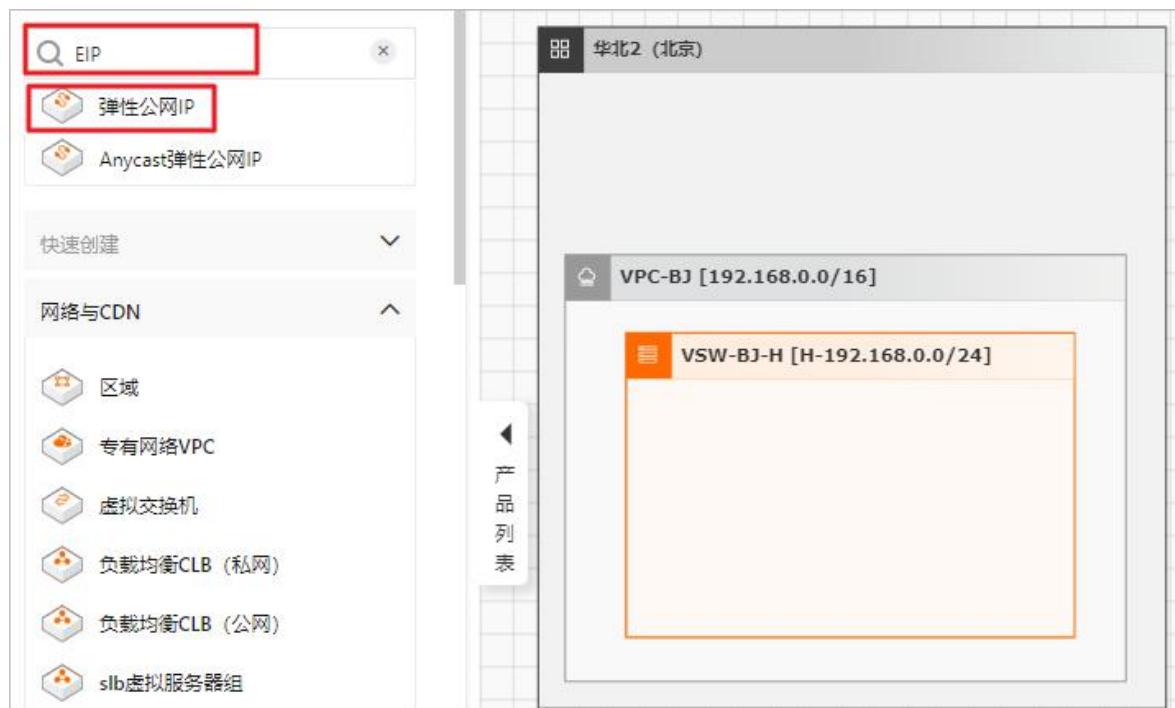
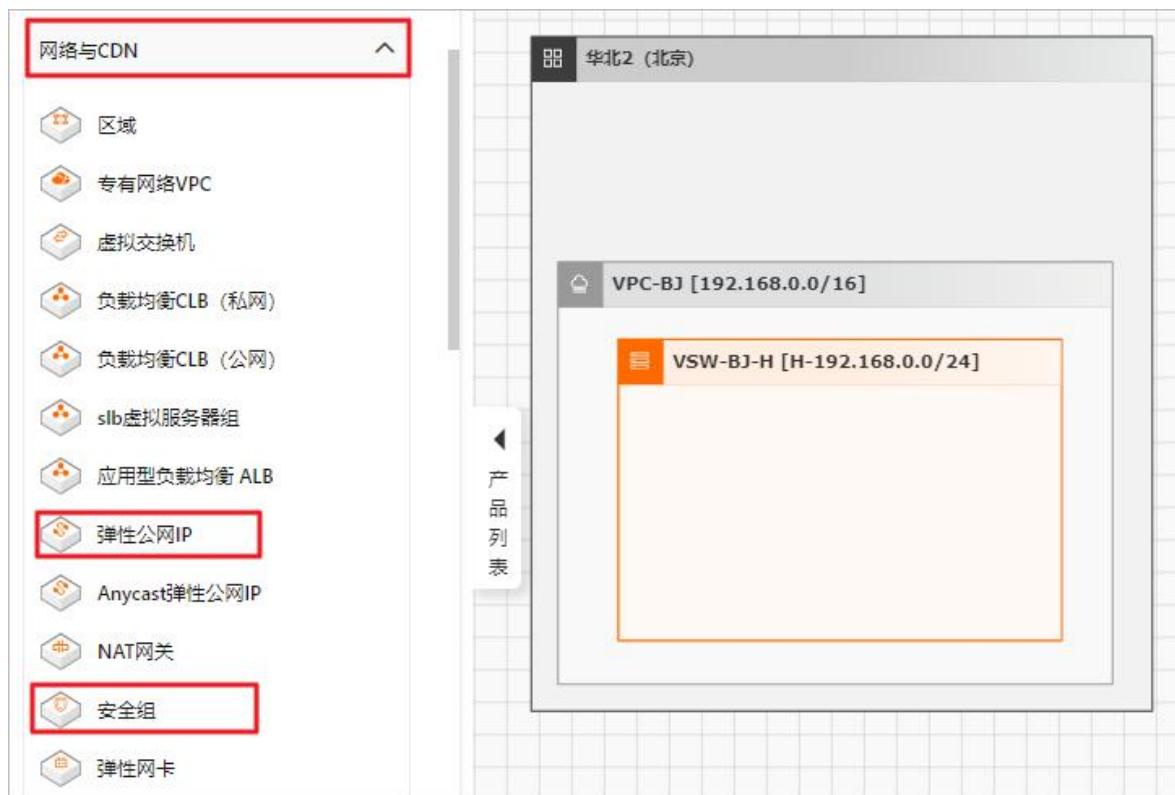
3. 双击配置 VSW：



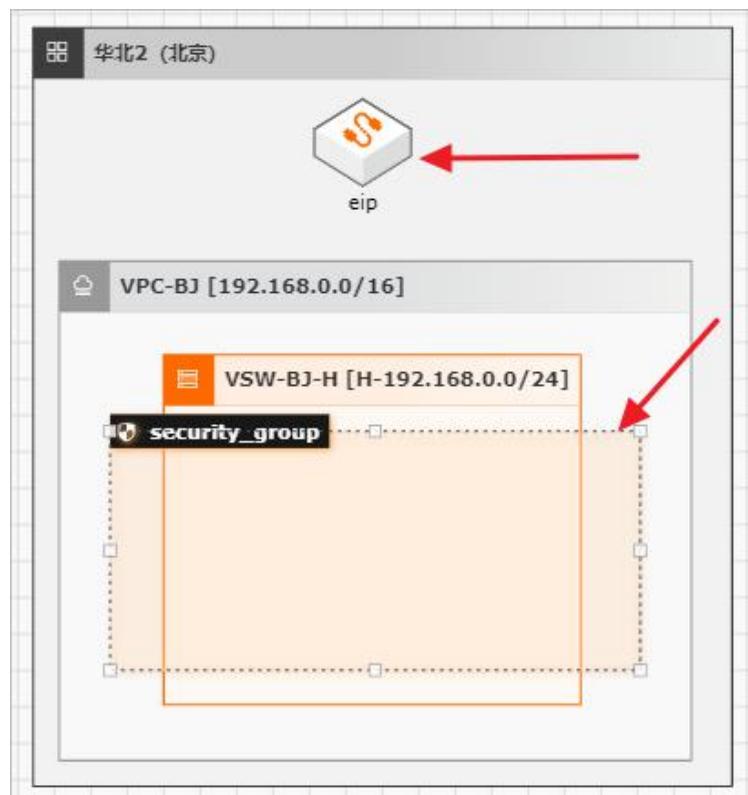
步骤 2 按照红色箭头位置拖动，可使北京 Region 区域框变大，便于后续其他资源拖入。



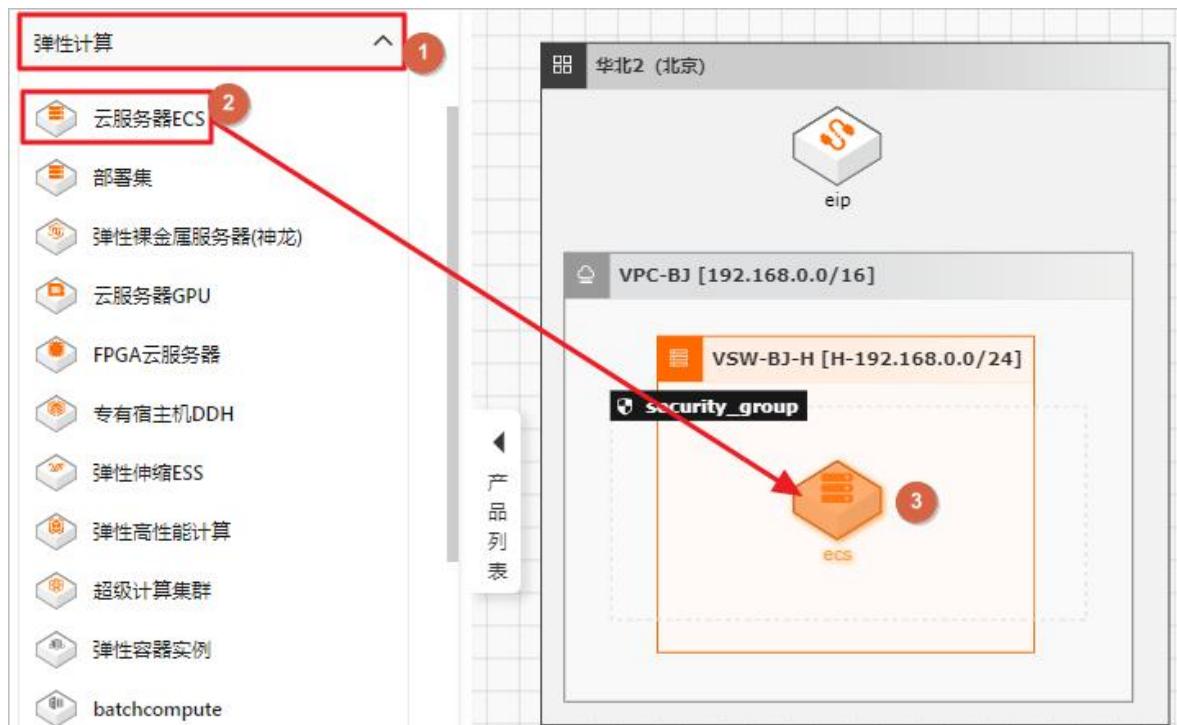
步骤 3 从左侧产品列表对应分类下找到**弹性公网 IP** 和 **安全组**，或通过搜索栏输入关键字快速定位。



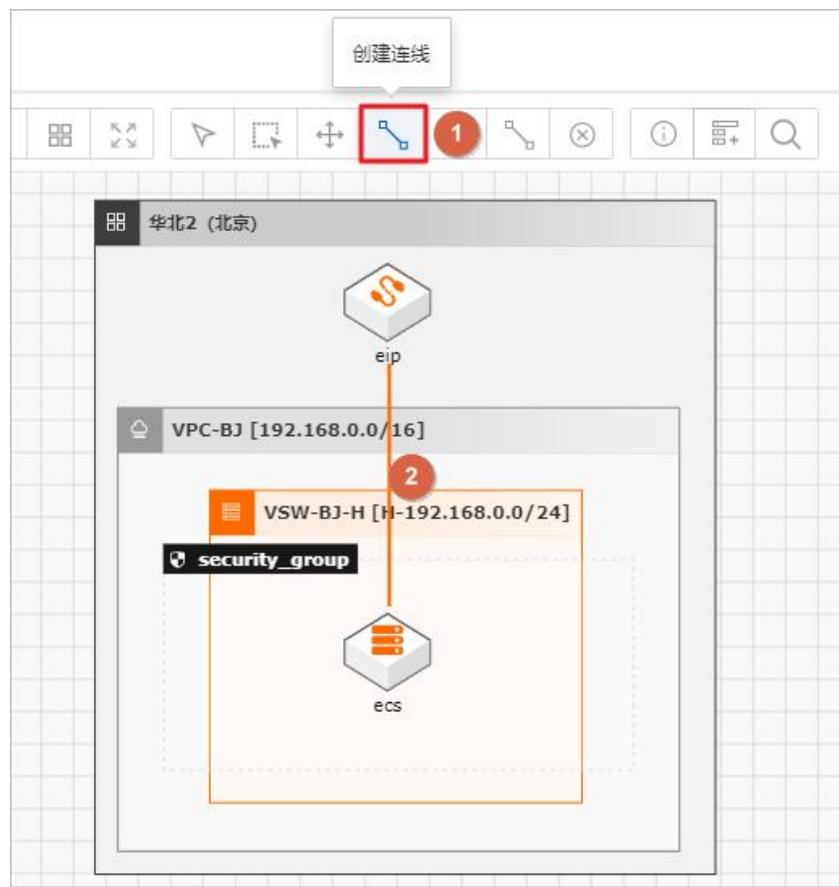
步骤 4 根据资源级别拖入对应位置，如下图所示：



步骤 5 从产品列表选择 ECS 拖入到安全组。



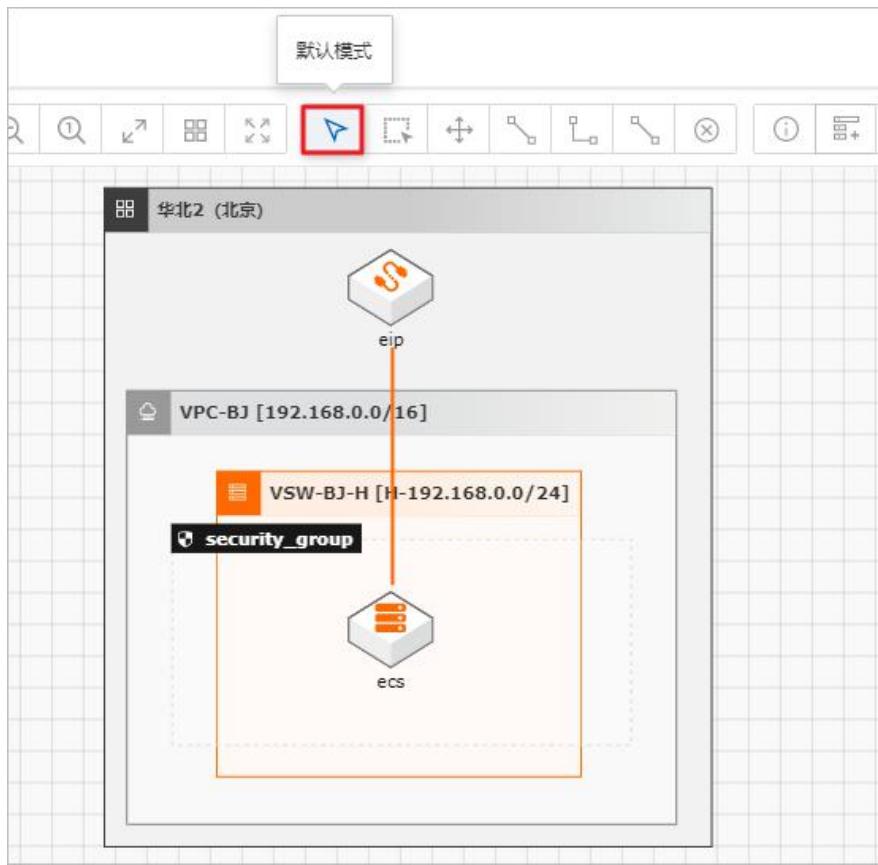
步骤 6 单击创建连线按钮，将 EIP 和 ECS 连接到一起。



**说明：**双击连线，可以根据需要设置连线显示样式。



步骤 7 创建完连线后，切换为**默认模式**。



步骤 8 双击 EIP 图标，参考下图在右侧进行 EIP 配置。

1	购买方式	新购	2
3	EIP名	EIP-TEST	4
5	购买数量	1	6
* 商品类型		按量付费	
线路类型		BGP(多线)	

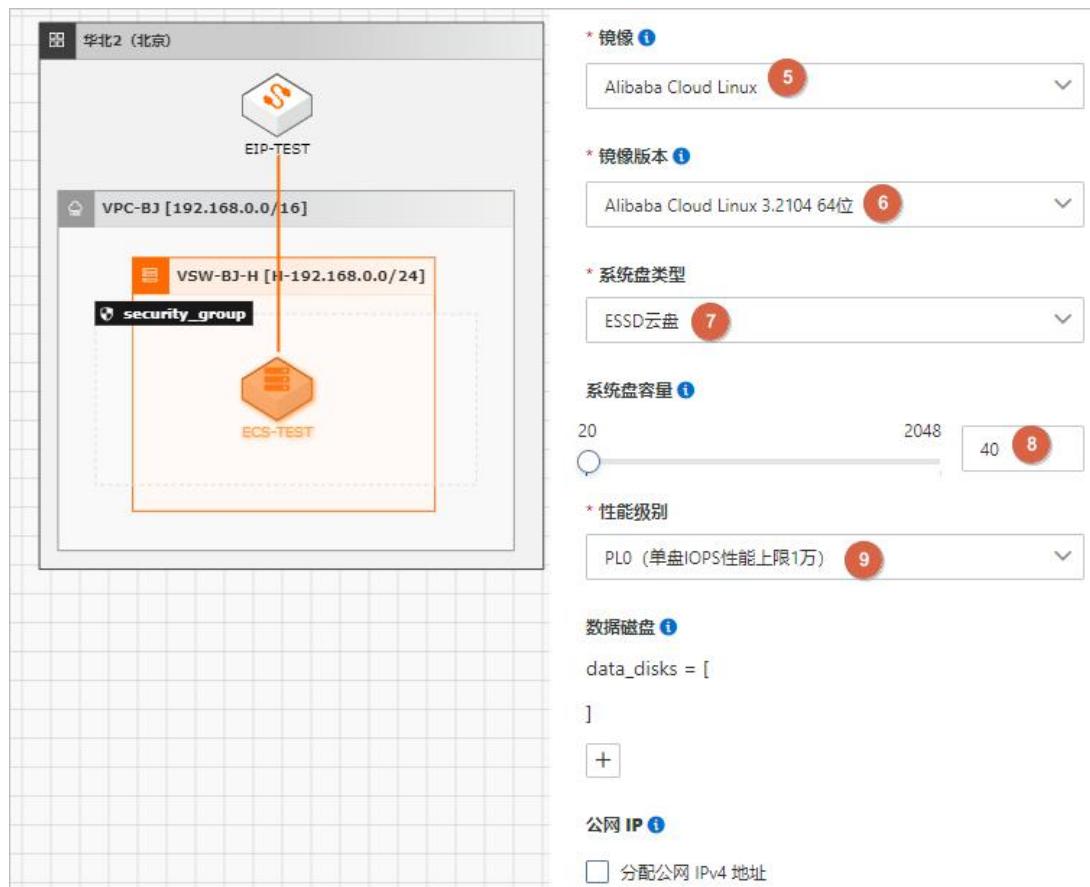
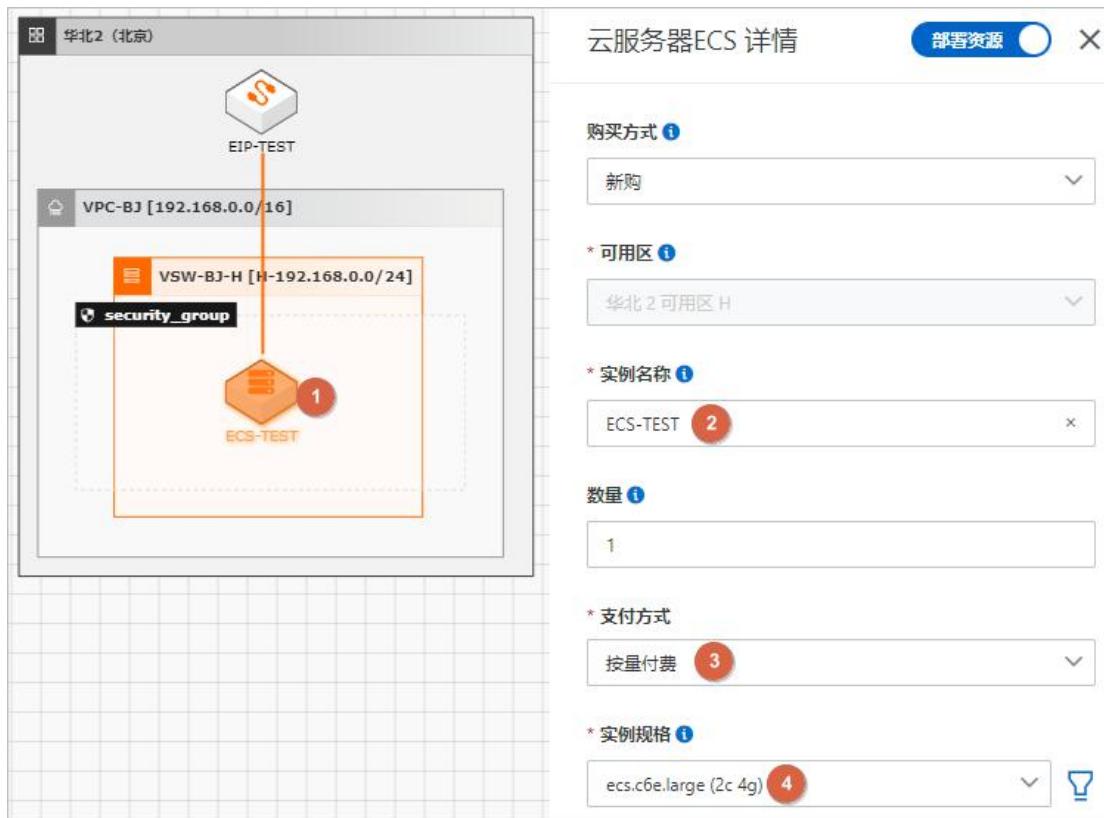


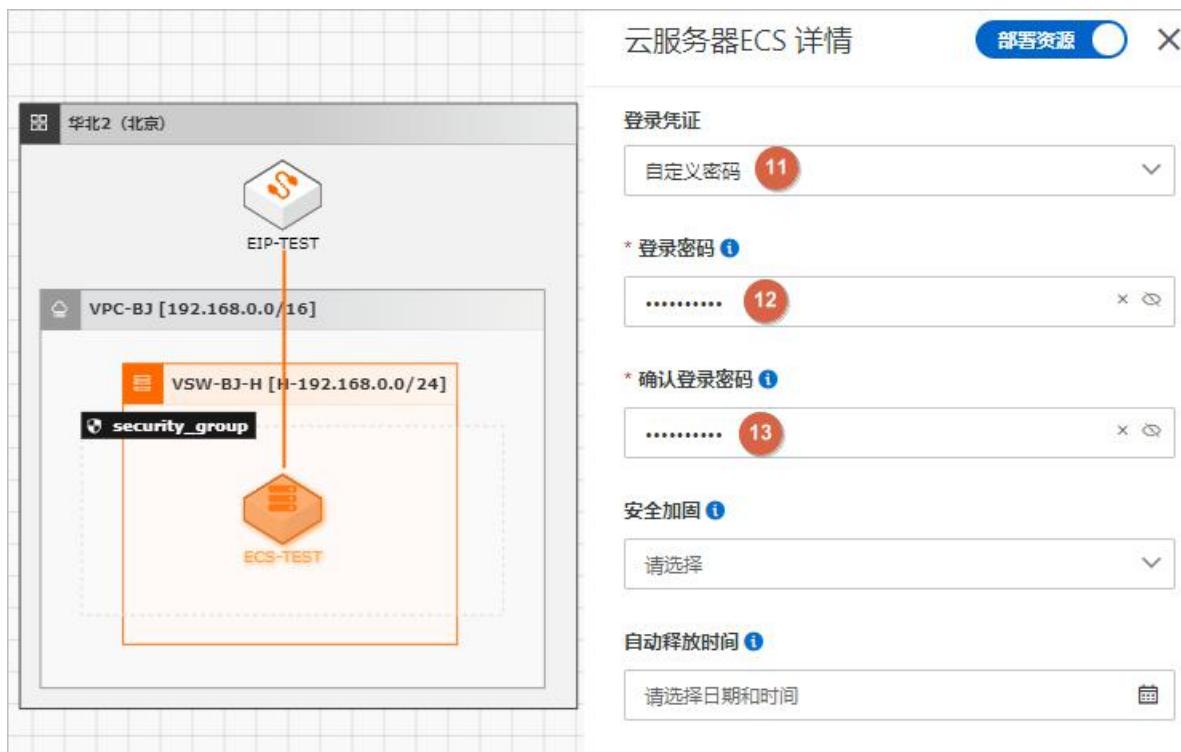
步骤 9 双击 ECS 图标，参考下图进行 ECS 配置。

**说明：**按照从上往下的顺序依次进行输入和选择，其中**支付方式**（按量付费或包年包月）决定了可选择的实例规格，不同支付方式的实例规格在各个可用区分布不同。

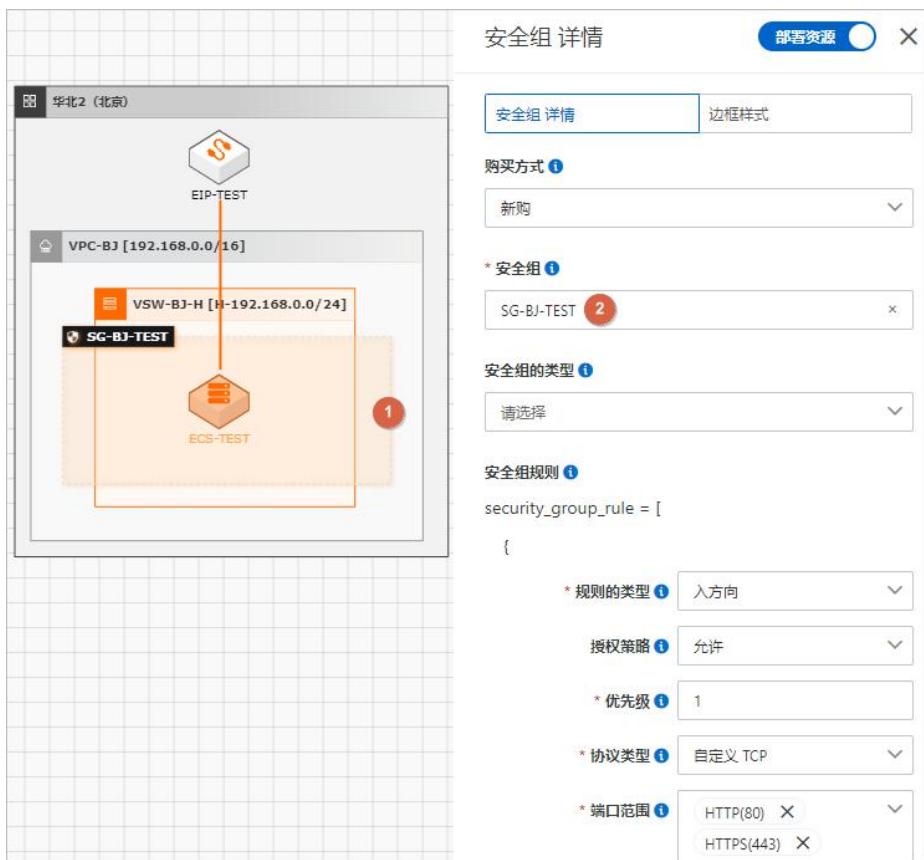
本示例配置如下表所示：

配置项	参数说明
购买方式	新购
可用区	已根据当前 ECS 实例所在可用区自动选择
实例名称	ECS-TEST
数量	1
支付方式	按量付费
实例规格	c6e.large
操作系统	Alibaba Cloud Linux 3.2104 64 位
系统盘	ESSD 云盘
性能级别	PL0
主机名	ECS-TEST
登录凭证	选择 <b>自定义密码</b> ，需要连续两次输入密码。

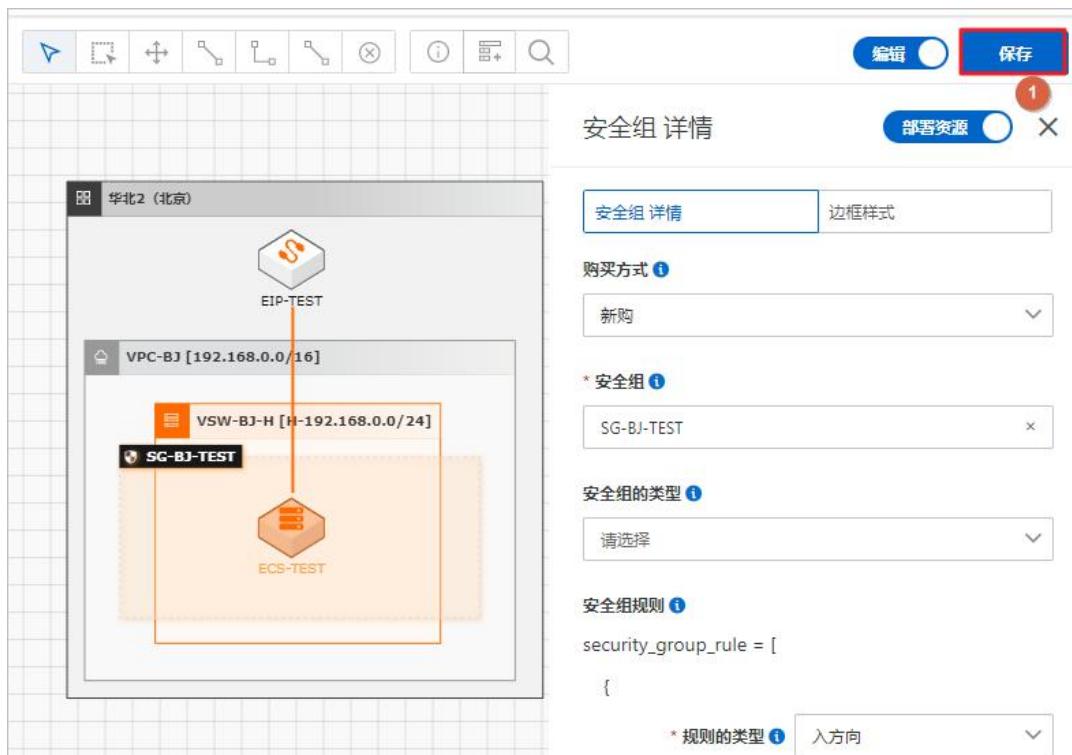




步骤 10 双击安全组图标，这里只配置安全组名称，其他配置保持默认，可以滚动鼠标进行查看。



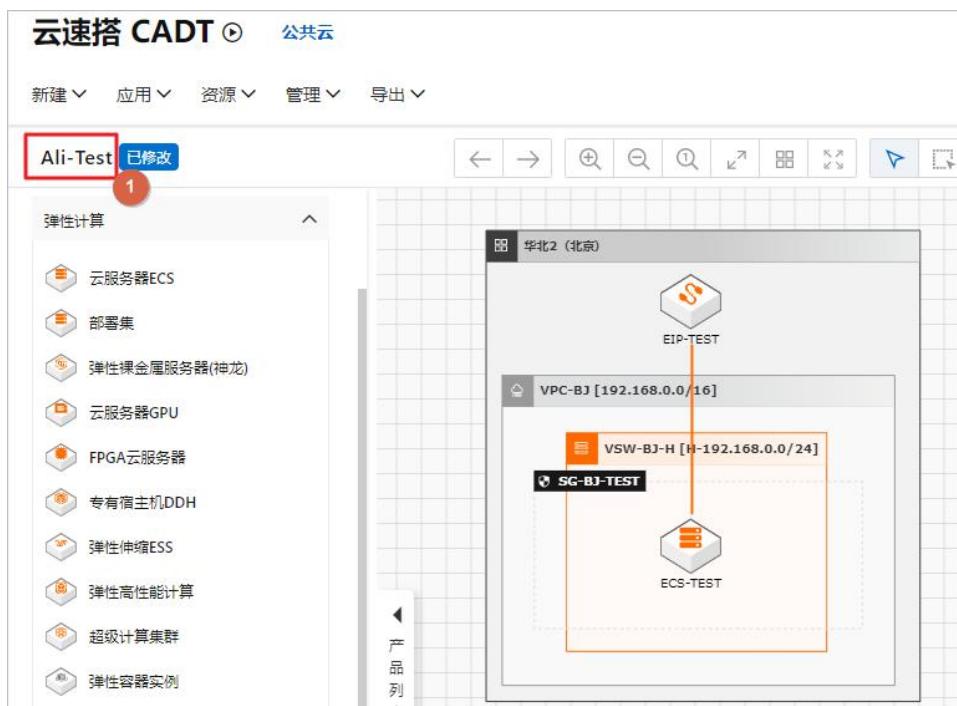
步骤 11 配置完成，单击右上角**保存**按钮，将创建的架构保存为应用。



步骤 12 设置应用名称“Ali-Test”，单击确认。



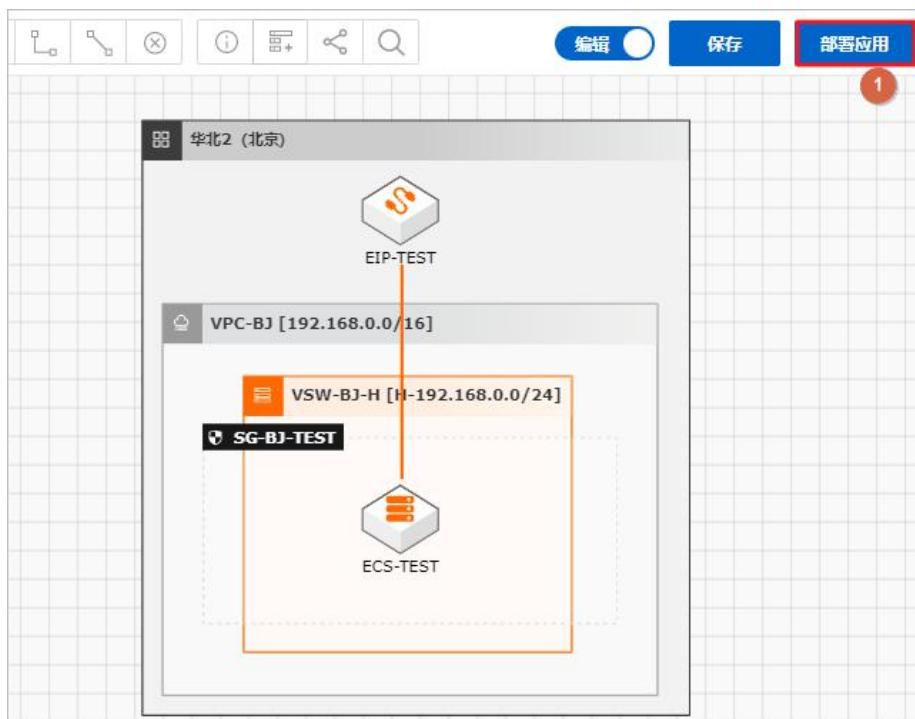
**说明：**左上角会显示保存后的应用名称，每一个架构在云上都是要支持应用的，所以保存后就会形成一个应用架构。



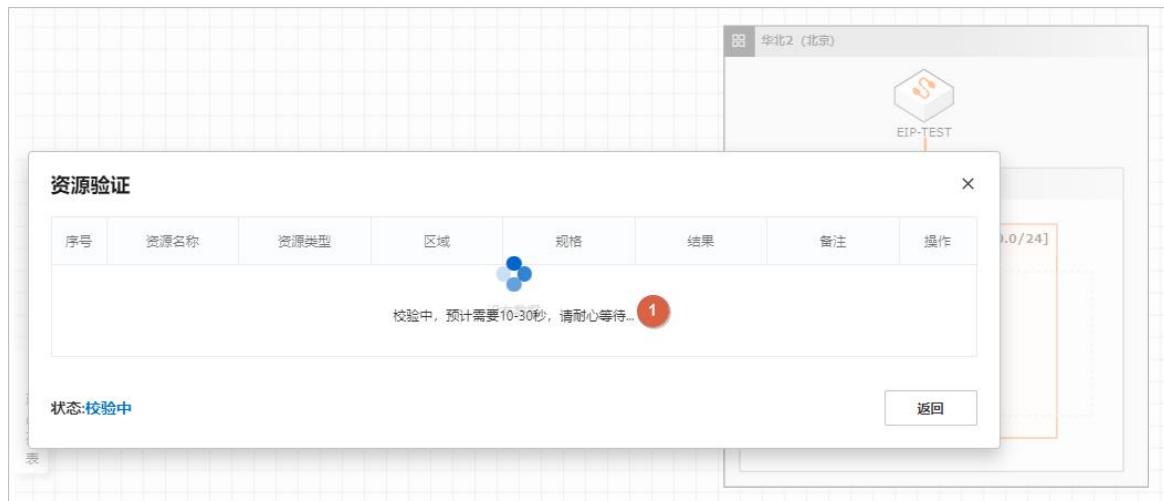
至此，架构设计阶段工作完成。

### 3.1.2. 部署应用

步骤 1 单击右上角的**部署应用**。



步骤 2 进入**资源验证**阶段，这个阶段会对架构中的资源在可用区下的库存情况进行查询，同时可以对资源规格进行 review。资源验证是实时进行的，请耐心等待。



步骤3 当出现检验成功时，可以查看一下相关的信息，确认一下是否是和自己的设计相符，如果相符单击下一步：价格清单。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	VPC-BJ [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
2	EIP-TEST	eip	北京	public	成功	校验通过	定位
3	SG-BJ-TEST	security.group	北京		成功	校验通过	定位
4	VSW-BJ-H [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
5	ECS-TEST	ecs	北京	ecs.c6e.large	成功	校验通过	定位

状态:校验成功 1

下一步: 价格清单 2

返回

步骤4 进入核算价格阶段，这里会将架构中的云资源按照**免费**、**按量付费**和**包年包月**进行区分，如果产品享受折扣这里会自动将账号对应的优惠显示出来。

状态为**计价成功**时，可以单击**查看报告**。

**导出价格清单**

1 免费 2 按量付费

**资源成本占比**

资源预算

- 计算 计算: 0.02元/时
- 网络 网络: 0.45元/时

**价格列表**

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	状态	操作
1	EIP-TEST	eip	北京	BGP	1	0.02元/时	首0.02元/时	0.02元/时	新购	定位
2	ECS-TEST	ecs	北京	ecs.c6e.large	1	0.45元/时	首0.45元/时	0.45元/时	新购	定位

状态: 计价成功 3

上一步: 资源校验 4

查看报告 5

下一步: 确认订单

步骤 5 会实时生成一个应用架构成本分析报告。



步骤 6 如果确认价格符合预期，可以单击**下一步：确认订单**。

确认订单阶段会列出架构中所有的产品及其价格，需要用户确认无误后勾选接受《云速搭服务条款》，此时**下一步：支付并创建**才会高亮，可以单击进行实际的资源购买和部署。

**确认订单**

免费  按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	ECS-TEST	ecs	北京	ecs.c6e.large	1	0.45元/时	0.45元/时	新购
2	EIP-TEST	eip	北京	BGP	1	0.02元/时	0.02元/时	新购

《云速搭服务条款》  
2 部署前，请阅读并勾选服务条款

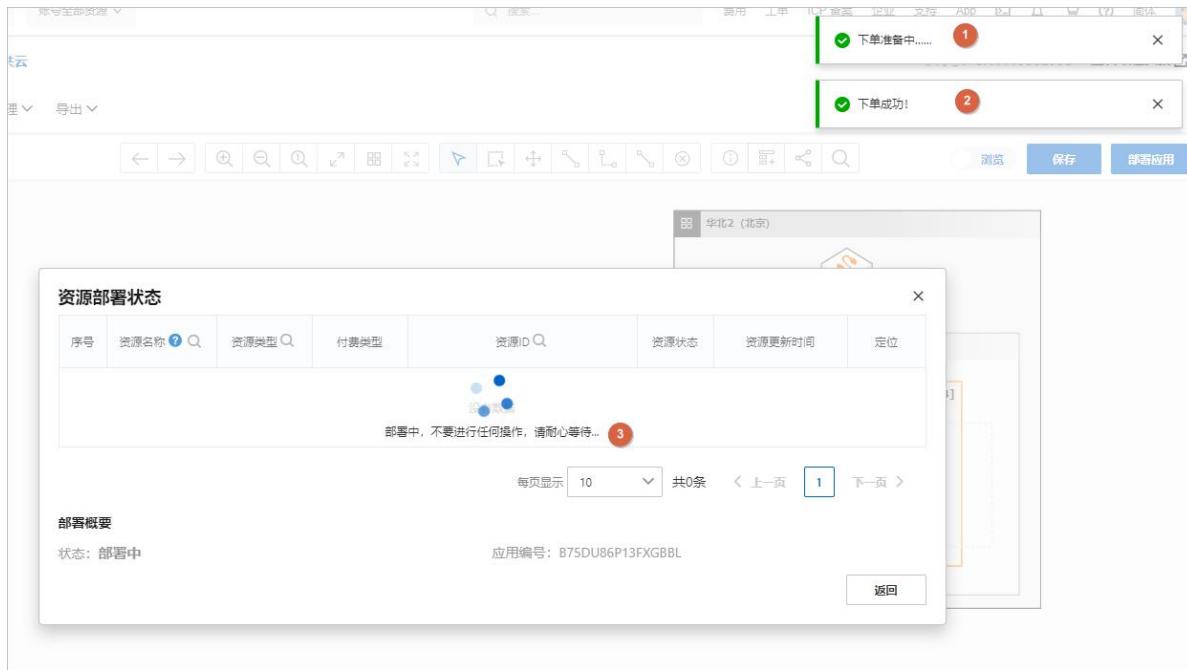
按量付费：0.45元/时 ①

状态：计价成功

上一步：价格清单 下一步：支付并创建 3

步骤 7 这时进入订单准备并进行下单，右上角会有提示，请耐心等待，不要关闭窗口。

**说明：**这里的方案编号是这个应用的唯一标识，如果提交工单，需要提供这个方案编号。



步骤 8 耐心等待一段时间后，部署成功，这里可以看到 VPC、VSW、EIP、ECS、安全组已经部署成功。

资源部署状态							
序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	VPC-BJ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zemz8wzpronpqiez7etf	运行中	2022-01-20 10:13:50	定位
2	VSW-BJ-H [H-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze71kofgcrkziu09wzl	运行中	2022-01-20 10:14:38	定位
3	EIP-TEST	eip (弹性公网IP)	按量付费	eip-2ze12he2ls880wfsw9p1x	运行中	2022-01-20 10:14:37	定位
4	SG-BJ-TEST	security.group (安全组)	-	sg-2ze2z8y274io78nusch5	运行中	2022-01-20 10:14:38	定位
5	ECS-TEST	ecs (弹性云服务器)	按量付费	i-2ze0wnm5f3mpqxx7l63c	运行中	2022-01-20 10:15:23	定位

每页显示 10 共 5 条 < 上一页 1 下一页 >

**部署概要**

状态：部署成功 ① 订单编号：212674768190833

应用编号：B75DU86P13FXGBBL

2 3 查看报告 返回

步骤 9 单击查看报告，可以实时生成应用架构方案部署报告。



步骤 10 部署成功后，资源右上角都会有一个绿色的状态灯，部署成功的架构图会默认进入浏览状态，这时是不能对架构图进行修改的，防止误操作。

单击屏幕下方的**资源清单**，显示所有资源信息。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC-BJ [192.168.0.0/16]	vpc (专有网络VPC)	免费	vpc-2zemz8wzpronpqez7eff	新建	运行中	2022-01-20 10:13:50	定位	详情 监控   变更日志 操作
2	VSW-BJ-H [H-192.168.0.0/24]	vswitch (虚拟交换机)	免费	vsw-2ze71kofgcrkzlu09wzlt	新建	运行中	2022-01-20 10:14:38	定位	详情 监控   变更日志 操作

步骤 11 单击 EIP-TEST，直接跳转到 EIP 控制台。

The screenshot shows the Cloud Speed Stack Resource Catalog interface. At the top, there's a network diagram with nodes: EIP-TEST, VPC-BJ [192.168.0.0/16], VSW-BJ-H [192.168.0.0/24], SG-BJ-TEST, and ECS-TEST. Below the diagram is a table of resources:

应用操作	导出资源清单	序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
		2	VSW-BJ-H [192.168.0.0/24]	(虚拟交换机)	免费	vsw-zze12he2ls880wfs...	新建	运行中
		3	EIP-TEST	eip (弹性公网IP)	按量付费	eip-2ze12he2ls880wfs...	新建	运行中
		4	SG-BJ-TEST	security group (安全组)	免费	sg-2ze2z8y274io78nus...	新建	运行中

A red arrow points to the 'EIP-TEST' row in the table.

步骤 12 可以在 EIP 控制台查看资源信息，这里可以看到 EIP-TEST 绑定了一个 ECS 实例，实例 ID i-2ze0wnm5f3mpqxx7l63c

The screenshot shows the EIP control console for the resource 'eip-2ze12he2ls880wfs...'. It has tabs for '实例信息' (Instance Information) and '监控运维' (Monitoring and Maintenance). The '实例信息' tab is active.

### 基本信息

实例 ID	eip-2ze12he2ls880wfs... <a href="#">复制</a>	实例名称	EIP-TEST <a href="#">编辑</a>
IP地址	47.95.204.235 <a href="#">2</a>	DDoS安全防护	
标签		带宽包服务	未加入共享带宽
IP状态	已分配	绑定实例类型	ECS 实例
绑定实例ID	i-2ze0wnm5f3mpqxx7l63c <a href="#">1</a> <a href="#">复制</a>	资源组	default resource group
删除保护	未开启 <a href="#">开启删除保护</a>	云防火墙防护	未开通 <a href="#">申请7天免费试用</a>
描述	-		

### 付费信息

计费方式	按流量计费 <a href="#">3</a>	带宽值	5 Mbps <a href="#">4</a>
EIP原有计费方式	后付费	创建时间	2022年1月20日 10:13:49

步骤 13 在资源清单单击 ECS-TEST。



步骤 14 可以在 ECS 控制台查看相应信息，这里可以看到 ECS ID 为 i-2ze097s8uciox4qxi53，与 EIP 中绑定信息相符，这里安全组 ID 为 sg-2ze0mehvqbjupirq5wm。

**ECS-TEST** 运行中

实例ID	i-2ze0wnm5f3mpqxx7l63c	远程连接	地域	华北2 (北京)
资源组:	-		所在可用区	北京 可用区H
弹性公网IP	47.95.204.235	解绑弹性IP	主机名	ECS-TEST
安全组	sg-2ze2z8y274io78nusch5	加入安全组	创建时间	2022年1月20日 10:14:00
描述	-	修改实例描述	自动释放时间	-
CPU&内存	2核 4 GiB	云盘	1	重新初始化云盘
操作系统	Alibaba Cloud Linux 3.2104 64位	更换操作系统	快照	0
实例规格	ecs.c6e.large	更改实例规格	镜像ID	aliyun_3_x64_20G_alibase_20210910.vhd
实例规格族	ecs.c6e		当前使用带宽	5Mbps (峰值)
标签				
网络信息				
网络类型	专有网络	专有网络	vpc-2zemz8wzprnppqiez7etf	绑定辅助弹性网卡   更换专有网络
弹性网卡	eni-2ze3yjc3n8nuq1mjtlw1	虚拟交换机	vsw-2ze71kofgrkziu09wzlt	
主私网IP	192.168.0.64	弹性IP实例ID	eip-2ze12he2ls880wfsw9p1x	
IPv6 地址	-	辅助私网IP	-	
付费信息				
付费类型	按量	带宽计费方式	按使用流量	按量付费转包年包月   为按量付费购买预留实例券

步骤 15 单击资源清单中的安全组。

The screenshot shows a network topology and a resource list table.

**Network Diagram:**

- A top-level EIP labeled "EIP-TEST" is connected to a VPC labeled "VPC-BJ [192.168.0.0/16]".
- The VPC contains a subnet labeled "VSW-BJ-H [192.168.0.0/24]".
- The subnet contains an ECS instance labeled "ECS-TEST".
- A security group labeled "SG-BJ-TEST" is associated with the subnet.

**Resource List Table:**

序号	资源名称	资源类型	付费类型	资源ID
4	SG-BJ-TEST	security.group (安全组)	免费	sg-2ze2z8y274io78nusch5
5	ECS-TEST	ecs (云服务器ECS)	按量付费	i-2ze0wnm5f3mpqxx7l63c

步骤 16 跳转到安全组后，可以看到安全组的访问规则信息。

The screenshot shows the configuration page for the "SG-BJ-TEST" security group.

**基本信息:**

- 安全组ID/名称: sg-2ze2z8y274io78nusch5 / SG-BJ-TEST
- 安全组类型: 普通安全组
- 描述:
- 资源组:
- 网络: vpc-2zemz8wzpronzpqiez7etf
- 组内连通策略: 组内互通 设置成组内隔离
- 标签:

**访问规则:**

- 入方向 出方向
- 手动添加 快速添加 全部编辑 搜索框: 输入端口或者授权对象进行搜索

授权策略	优先级	协议类型	端口范围	授权对象	描述
<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: 3389/3389	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	

步骤 17 可以单击**安全组内实例列表**，查看该安全组内包含的实例信息，这里可以看到 ECS-TEST。

The screenshot shows the Alibaba Cloud ECS console interface. At the top, it displays the security group name "SG-BJ-TEST" and its VPC ID "VPC-BJ / vpc-2zemz8wzprnpqjiez7etf". Below this, there is a tip about using prefix lists for security group rule management. The main area is titled "安全组内实例列表" (Instances in Security Group). It includes a search bar with dropdown options for "实例名称" (Instance Name) and "输入实例名称模糊查询" (Search by Instance Name). A table lists the instances:

实例ID/名称	专有网络	可用区	IP地址
i-2ze0wmn5f3mpqxx7l63c ECS-TEST <span style="color:red;">②</span>	vpc-2zemz8wzprnpqjiez7etf vsw-2ze71kofgcrkzu09wzlt	北京 可用区H	47.95.204.235 (弹性) 192.168.0.64 (私有)

At the bottom of the table, there is a button labeled "移出安全组" (Remove from Security Group).

至此一个简单的“架构设计-价格测算-部署-架构核查”就完成了。

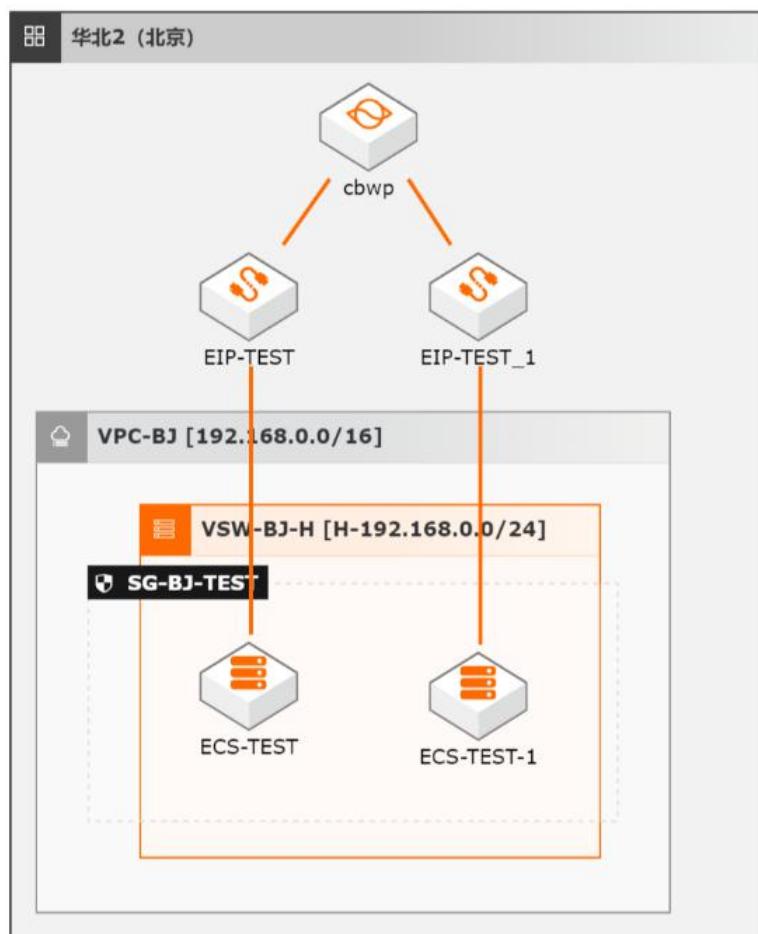
## 3.2.云速搭部署 EIP 实现共享带宽/流量包管理

作者 | 阿里云解决方案架构师 嘉辽

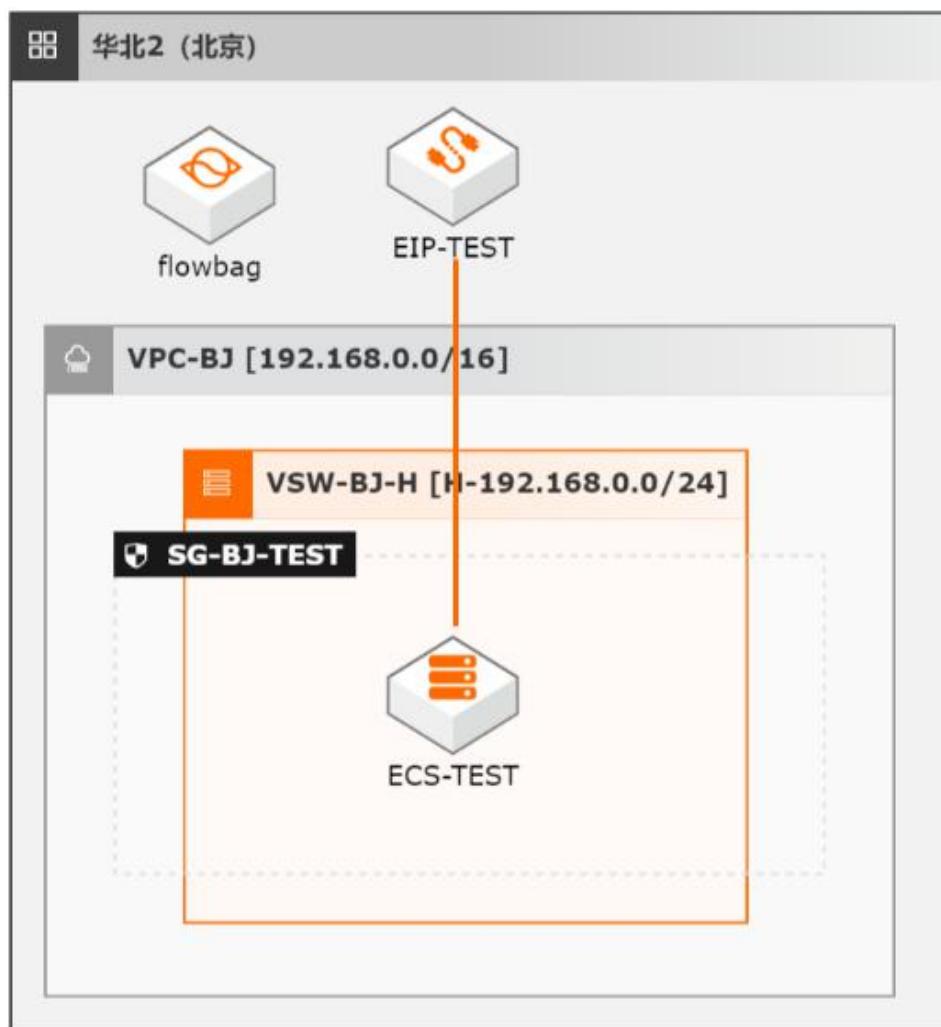
### 3.2.1.云速搭架构设计

#### 方案架构

- 通过云速搭设计、部署一个“ECS+EIP+共享带宽”的架构，多个 EIP 可以使用共享带宽的资源。



- 通过云速搭部署共享流量包，可以自动抵扣按流量计费的云服务器 ECS、弹性公网 IP 和负载均衡 SLB 多地域产生的 IPv4 流量（不含 EIP 精品流量）费用。



## 理解资源级别

每个阿里云资源都有对应的资源级别，在 CADT 进行架构设计时要遵循资源级别开展。

本架构中使用的资源及对应的资源级别如下表所示，在进行架构设计时需要用到。

云资源	资源级别
EIP	Region
共享带宽	Region
共享流量包	全局
ECS	VSW
安全组	VPC

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

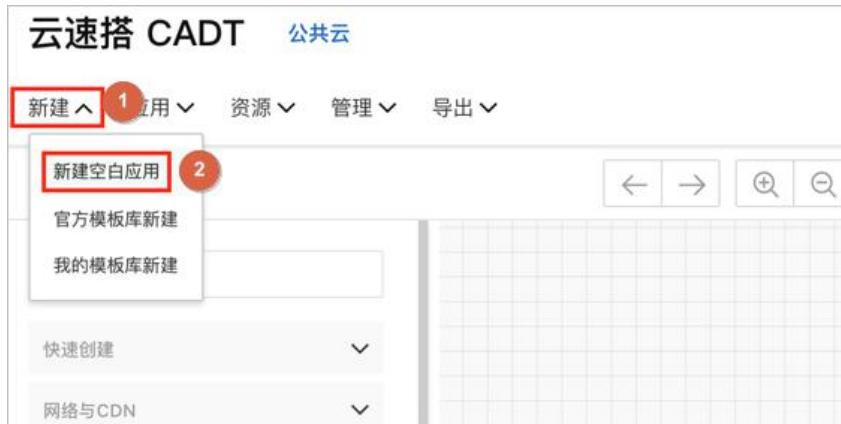
资源分类	资源名称	网段
Region	北京	-
VPC	VPC-BJ	192.168.0.0/16
Vswitch	VSW-BJ-H	192.168.0.0/24
安全组	SG-BJ-TEST	-

### 3.2.2.设计应用架构

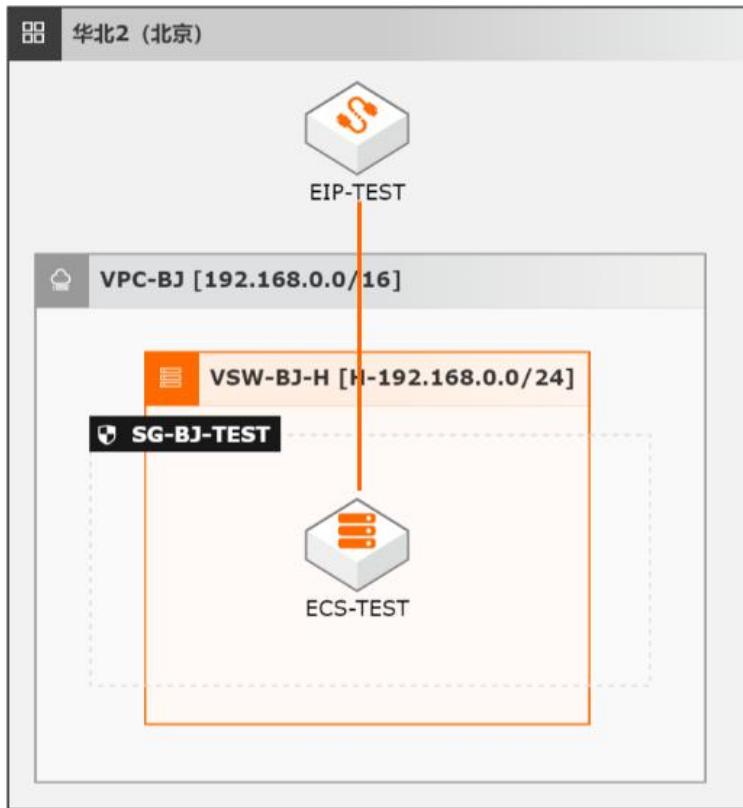
步骤 1 登录云速搭 CADT 管理控制台。[\(https://bpstudio.console.aliyun.com/\)](https://bpstudio.console.aliyun.com/)

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在菜单栏单击新建 > 新建空白应用，打开一个空白画布。



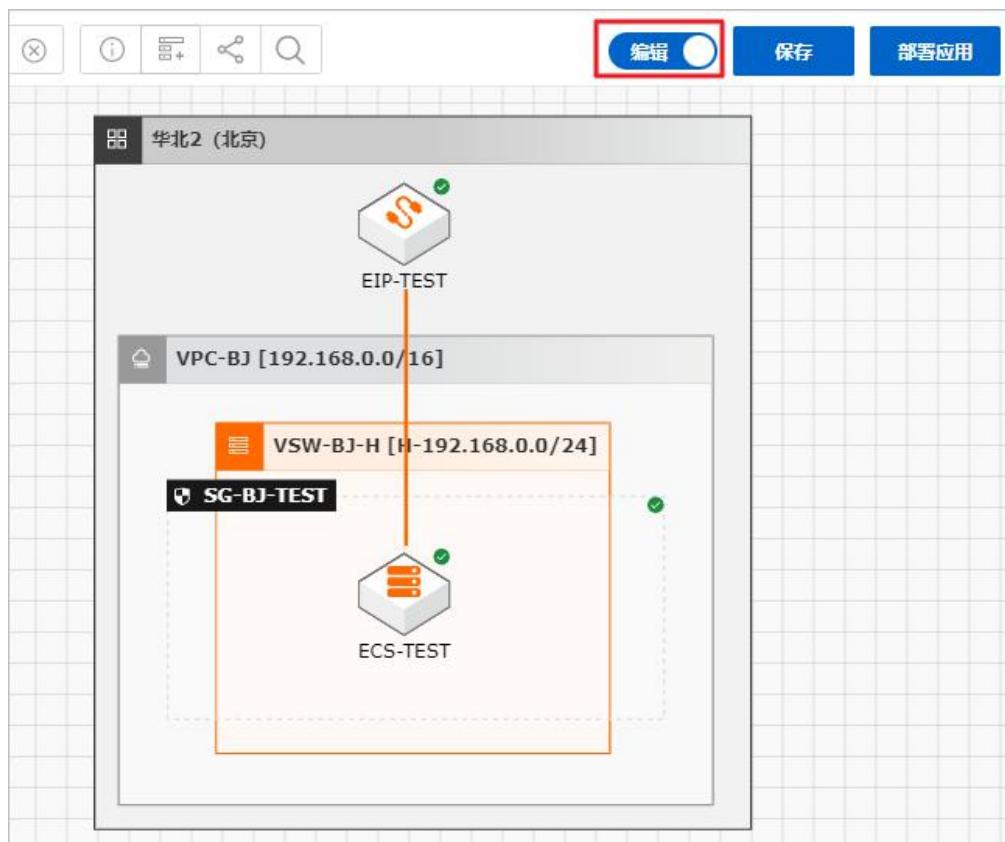
步骤 3 请根据《云速搭架构涉及入门》(<https://bp.aliyun.com/detail/239>) 第 2 章节完成以下架构配置。



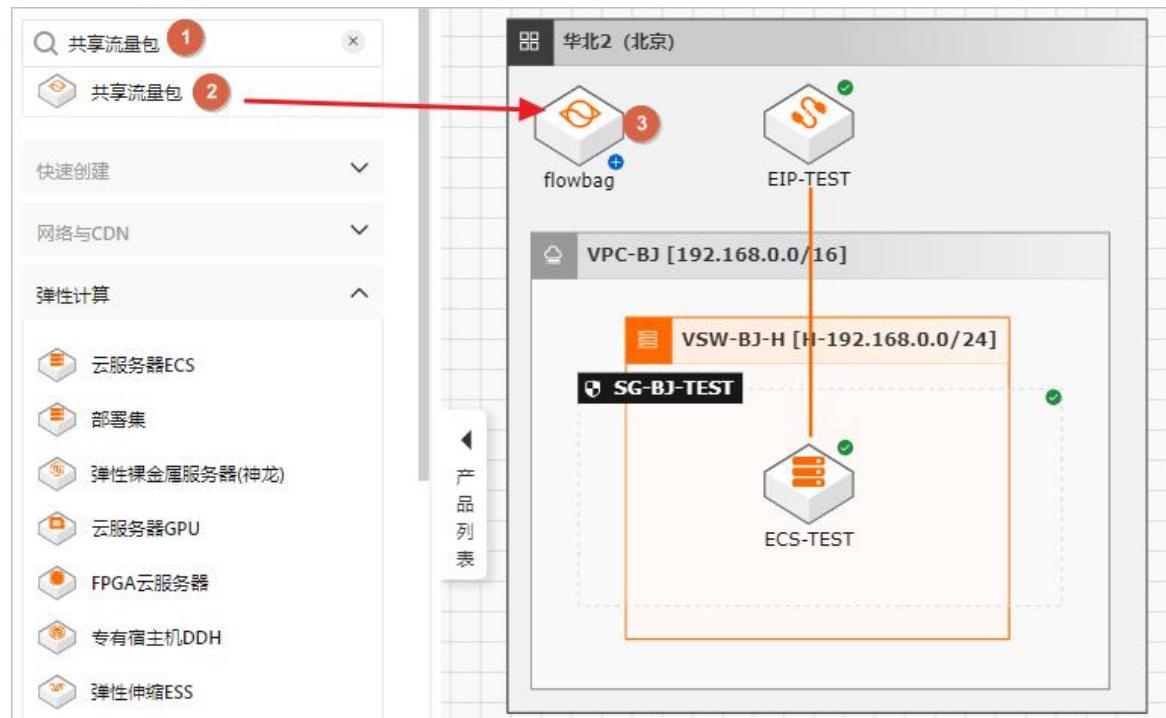
### 3.2.3. 共享流量包部署

共享流量包产品是一款流量套餐产品，使用方便，价格实惠。在购买共享流量包产品后会立刻生效，并自动抵扣按流量计费的云服务器 ECS、弹性公网 IP（EIP）、负载均衡（SLB）和 NAT 网关产生的 IPv4 流量（不包含 EIP 精品流量）费用，直到流量包用完或到期为止。

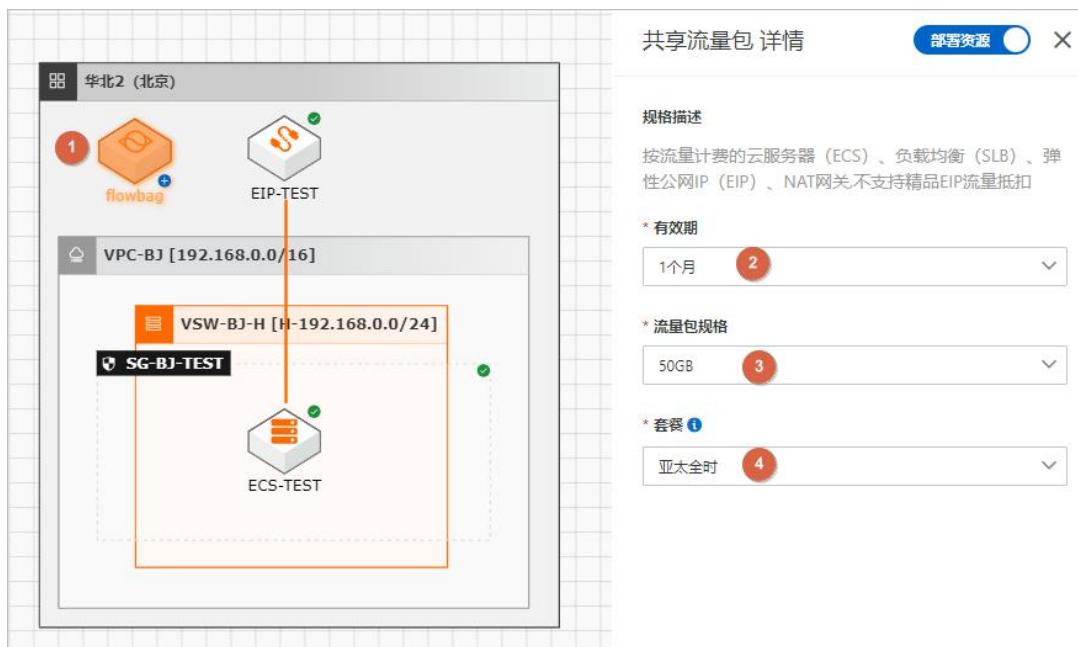
步骤 1 应用部署完成后，默認為浏览模式，切换为编辑模式继续进行应用架构设计。



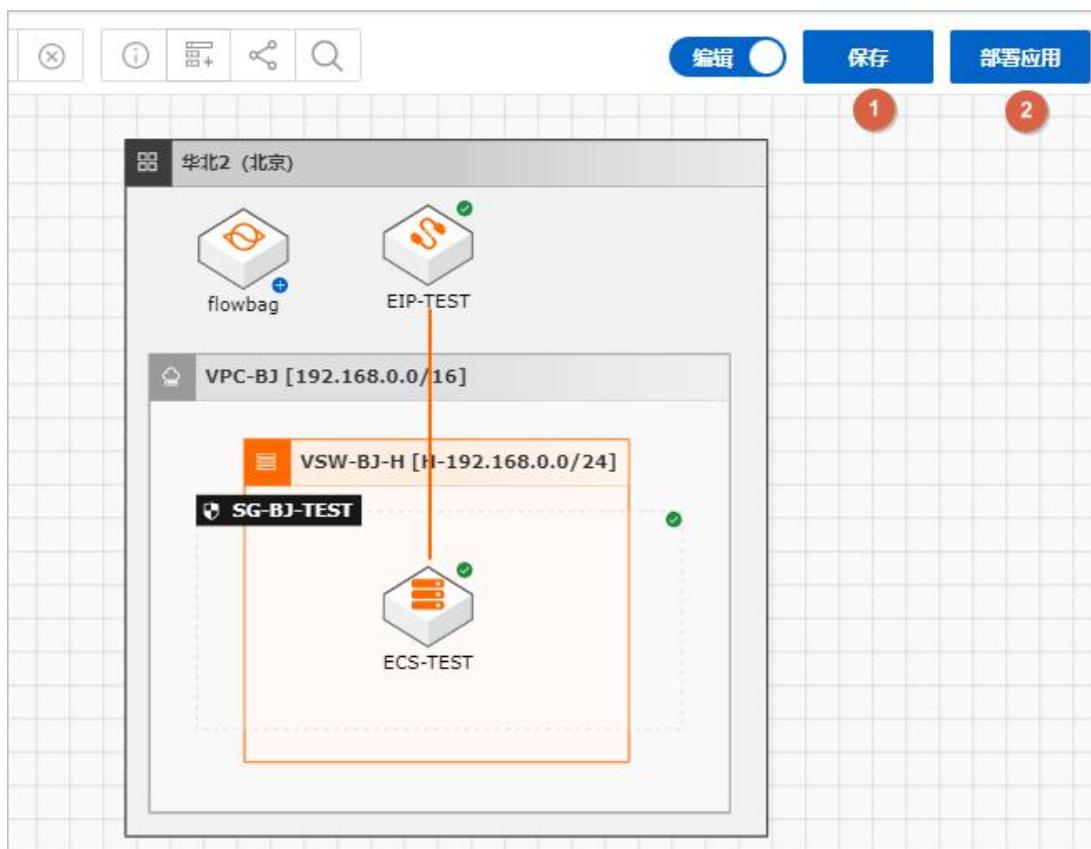
步骤 2 在左侧搜索框输入资源名称：共享流量包，选中共享流量包图标，由于共享流量包属于全局资源，可以放在 region 中，拖动共享流量包图标至 region 中。



步骤3 双击共享流量包图标，进行参数配置。



步骤4 点击保存，然后点击部署应用。



步骤 5 重新进行资源验证、询价、订单确认及下单部署。

### 资源验证

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	VPC-BJ [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	<a href="#">定位</a>
2	EIP-TEST	eip	北京	public	成功	校验通过	<a href="#">定位</a>
3	SG-BJ-TEST	security.group	北京		成功	校验通过	<a href="#">定位</a>
4	VSW-BJ-H [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	<a href="#">定位</a>
5	ECS-TEST	ecs	北京	ecs.c6e.large	成功	校验通过	<a href="#">定位</a>
6	flowbag	flowbag		50	成功	校验通过	<a href="#">定位</a>

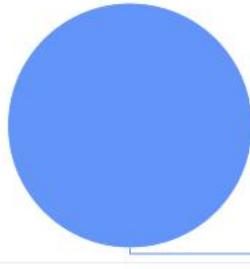
状态: 资源验证成功(架构调整)

[下一步: 价格清单](#) [返回](#)

### 导出价格清单

免费 [包年包月](#) [按量付费](#)

#### 资源成本占比



资源预算  
● 网络 网络:    元

100%

#### 价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	状态	操作
1	flowbag	flowbag		50	1	1月	37.00元/月	省 <span style="background-color: #ccc; color: #ccc;">  </span> 元/月	<span style="background-color: #ccc; color: #ccc;">  </span> 元/月	新购	<a href="#">定位</a>

状态: 询价成功(架构调整)

[上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

**确认订单**

免费	包年包月

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
1	flowbag	flowbag		50	1	1月	37.00元/月	元/月	新购

《云速搭服务条款》

① 部署前, 请阅读并勾选服务条款

包年包月: **元**

状态: 淘价成功(架构调整)

[查看新购资源配置](#) [上一步: 价格清单](#) [下一步: 支付并创建](#)

**确认订单**

免费	包年包月

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
1	flowbag	flowbag		50	1	1月	37.00元/月	元/月	新购

《云速搭服务条款》

部署前, 请阅读并勾选服务条款

包年包月: **元**

状态: 淘价成功(架构调整)

[查看新购资源配置](#) [上一步: 价格清单](#) [下一步: 支付并创建](#)

2

3

您创建的应用中包含如下包年包月资源:

flowbag

这些资源未到期前无法进行释放, 请确认!

[确认](#) [取消](#)

步骤 6 等待共享流量包创建完成即可。

**资源部署状态**

序号	资源名称 <a href="#">?</a>	资源类型 <a href="#">Q</a>	付费类型	资源ID <a href="#">Q</a>	资源状态	资源更新时间	定位
2	VSW-BJ-H [H-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze71kofgcrkz109wzlt	运行中	2022-01-20 10:14:38	定位
3	EIP-TEST	eip (弹性公网IP)	按量付费	eip-2ze12he2ls880wfsw9p1x	运行中	2022-01-20 10:14:37	定位
4	SG-BJ-TEST	security.group (安全组)	-	sg-2ze2z8y274io78nusvh5	运行中	2022-01-20 10:14:38	定位
5	ECS-TEST	ecs (云服务器ECS)	按量付费	i-2ze0wnm5f3mpqxx7l63c	运行中	2022-01-20 10:15:23	定位
6	flowbag	flowbag (共享流量包)	按量付费	flowpack-cn-2r4j6bs001c	运行中	2022-01-20 10:58:41	定位

每页显示 [10](#) 共6条 [< 上一页](#) [1](#) [下一页 >](#)

**部署概要**

状态: 部署成功

应用编号: B75DU86P13FXGBBL

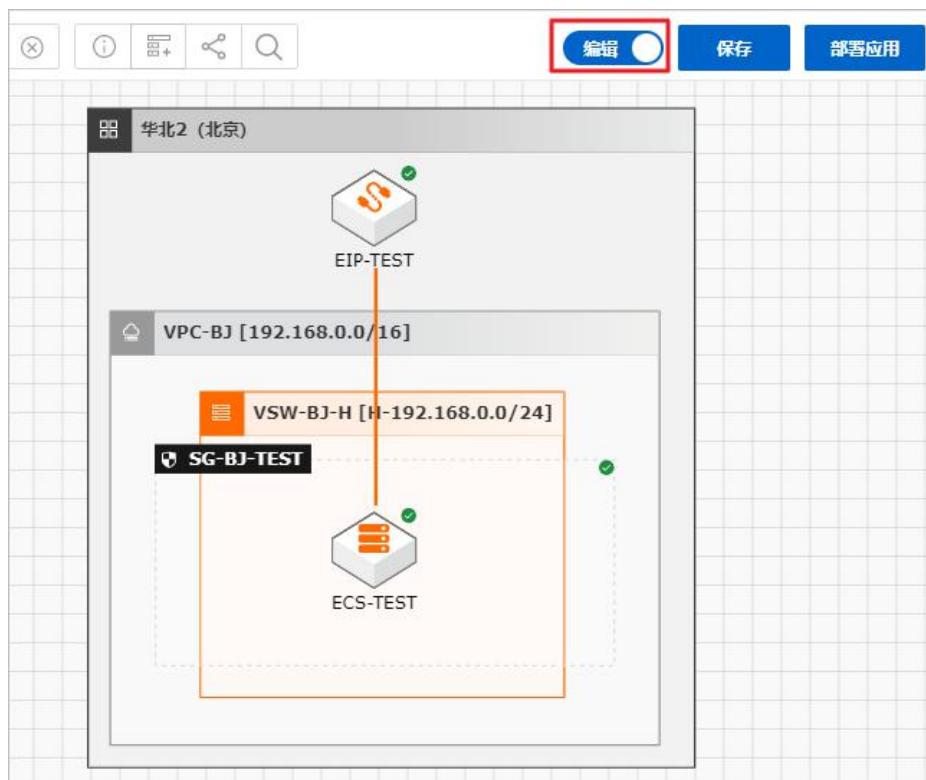
订单编号: 212674768190833, 212675686010833

[查看报告](#) [返回](#)

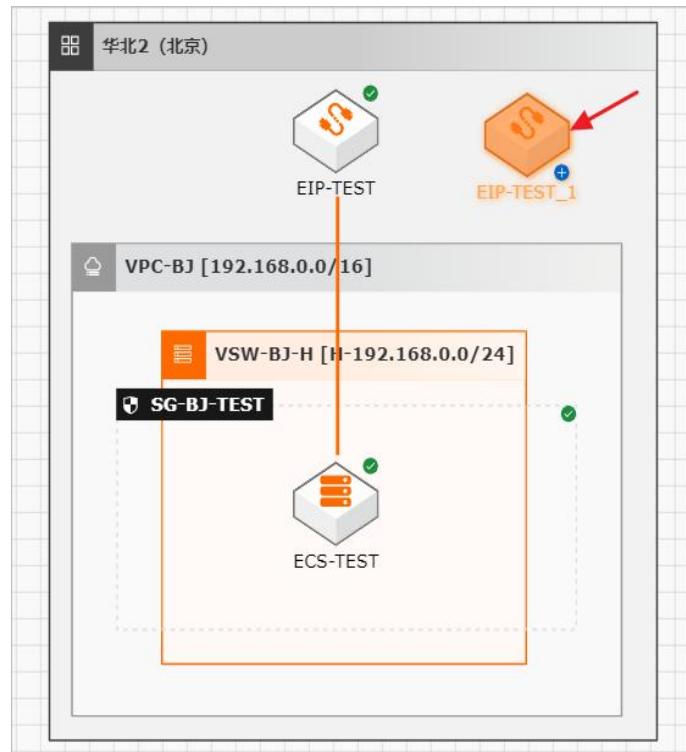
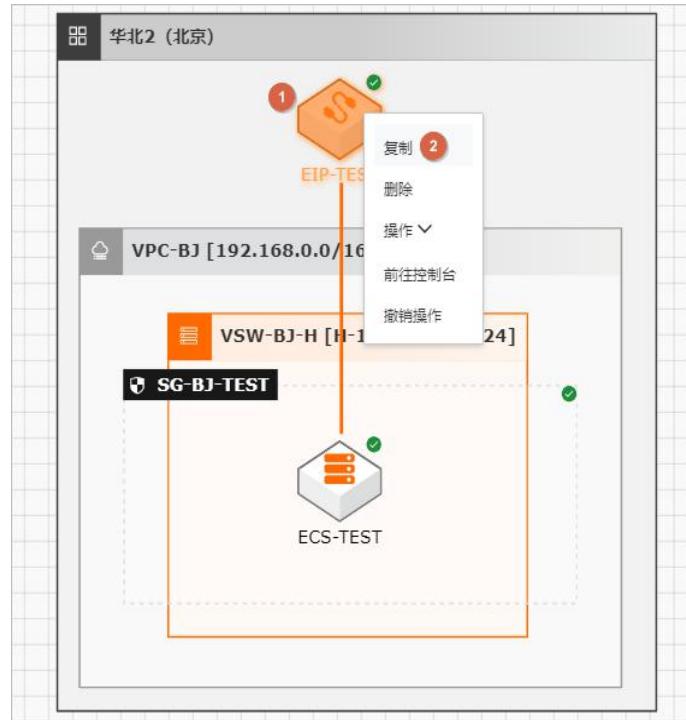
### 3.2.4. 共享宽带包部署

共享带宽提供地域级带宽共享和复用功能。创建共享带宽实例后，您可以将弹性公网 IP (EIP) 添加到共享带宽实例中，复用共享带宽中的带宽，节省公网带宽使用成本。如果没有选择共享流量包，也可以考虑使用共享带宽包。

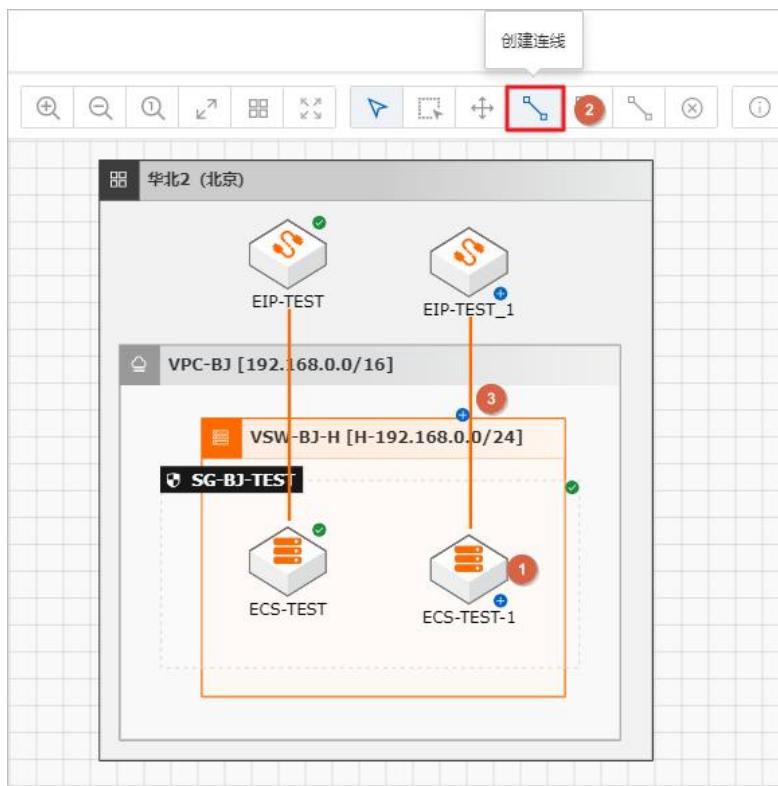
步骤 1 紧接 3.2.1.章节，切换为编辑模式继续进行应用架构设计。



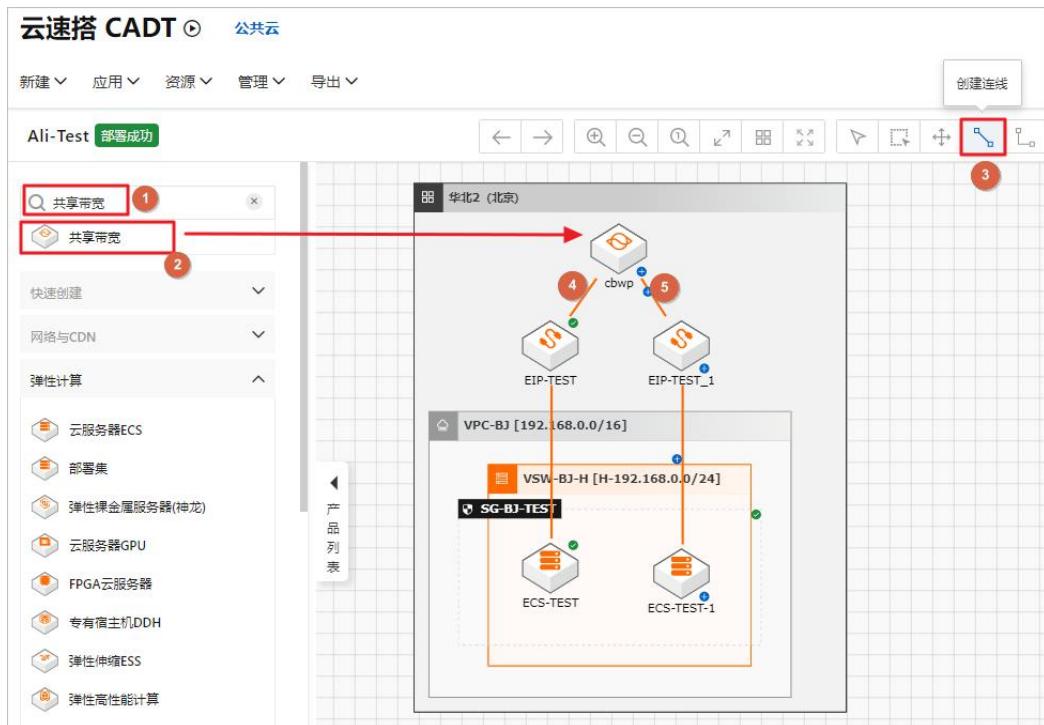
步骤 2 如下图所示，新增一个 ECS 和 EIP，可以复制 EIP 和 ECS，在画板中选中实例图标，然后右键，选择**复制**，得到一个新的资源实例。



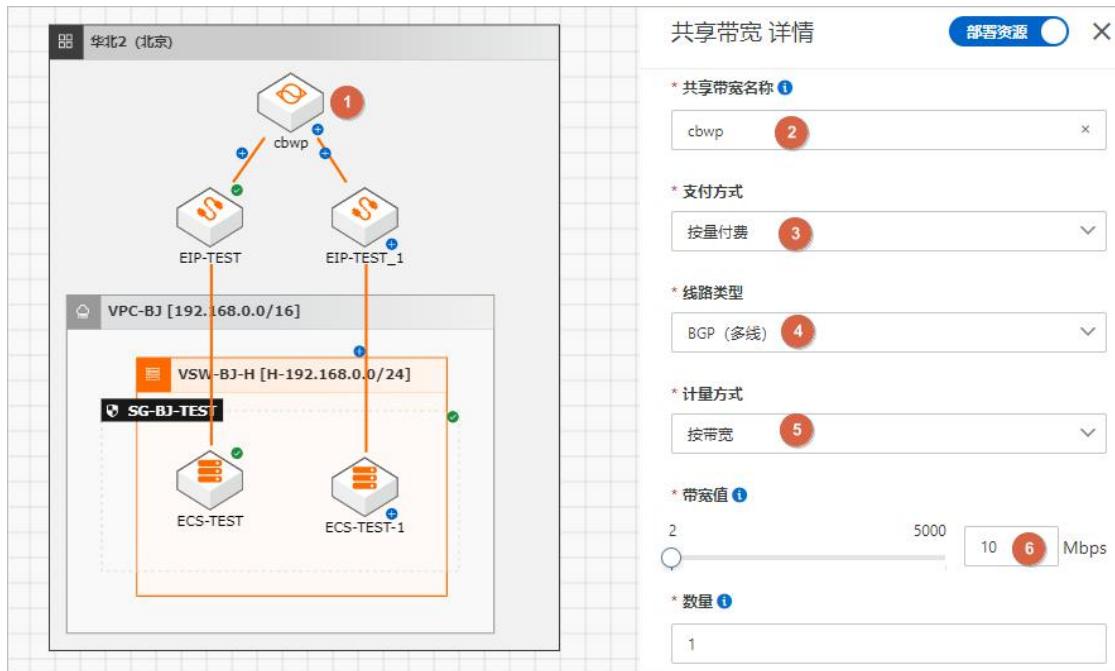
步骤 3 按照相同方式复制一个新的 ECS 实例，并且通过实线将 EIP 和 ECS 连接。



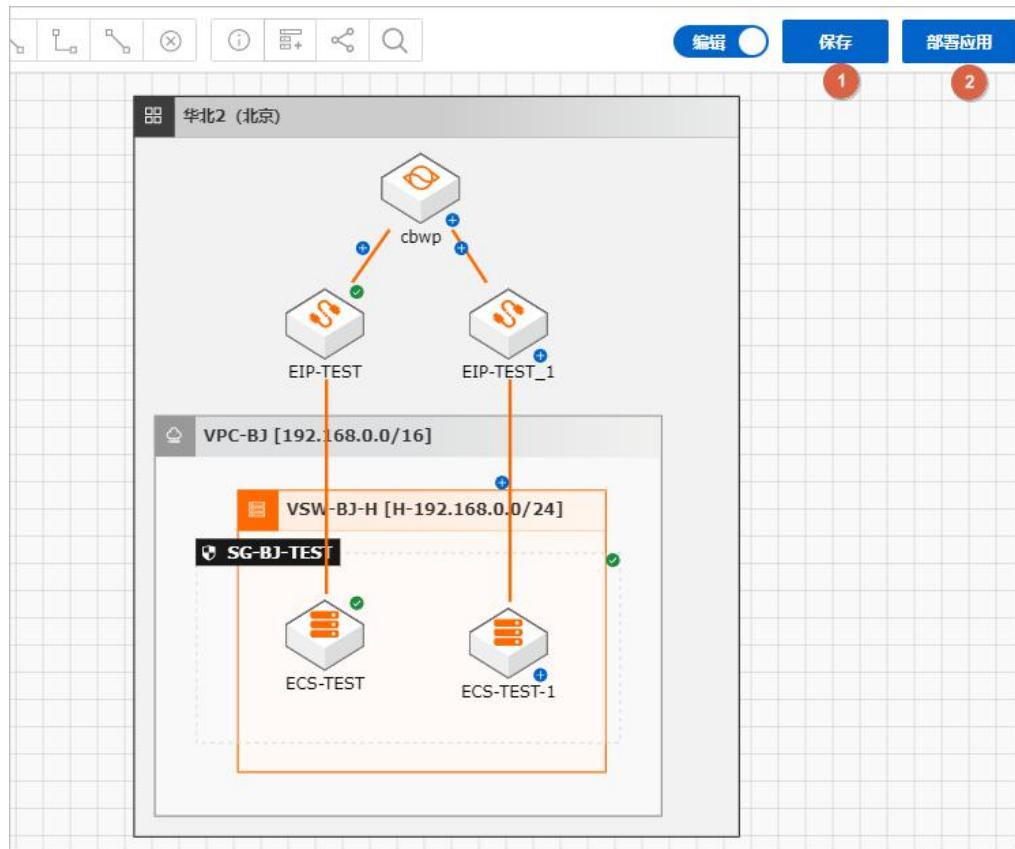
步骤 4 在左侧搜索框输入资源名称：共享带宽，选中共享带宽图标，由于共享带宽属于 region 资源级别，因此放在 region 中，拖动共享带宽图标至 region 中，可以调整边框上下大小，并且分别通过联系将共享流量包与 EIP 连接。



步骤 5 双击共享带宽图标，进入参数配置。



步骤 6 点击保存并部署应用。



步骤 7 重新进行资源验证、询价、订单确认、下单部署。

### 资源验证

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	VPC-BJ [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
2	EIP-TEST	eip	北京	public	成功	校验通过	定位
3	SG-BJ-TEST	security.group	北京		成功	校验通过	定位
4	VSW-BJ-H [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
5	ECS-TEST	ecs	北京	ecs.c6e.large	成功	校验通过	定位
6	flowbag	flowbag		50	成功	校验通过	定位
7	cbwp	cbwp	北京	BGP	成功	校验通过	定位

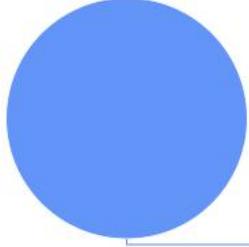
状态: 资源验证成功(架构调整)

[下一步: 价格清单](#) [返回](#)

### 导出价格清单

免费 [包年包月](#) 按量付费

#### 资源成本占比



资源预算  
● 网络 网络: 100%

#### 价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	状态	操作
1	flowbag	flowbag		50	1	1月	37.00元/月	省 10 元/月	37.00元/月	已保有产品	定位

状态: 询价成功(架构调整)

[上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

确认订单
×

		免费	按量付费						
序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态	
1	ECS-TEST-1	ecs	北京	ecs.c6e.large	1	0.45元/时	元/时	新购	
2	cbwp	cbwp	北京	BGP	1	33.60元/时	元/时	新购	
3	EIP-TEST_1	eip	北京	BGP	1	0.02元/时	元/时	新购	

《云速搭服务条款》

部署前, 请阅读并勾选服务条款

按量付费:  元/时

状态: 询价成功(架构调整)
查看新购资源配置
上一步: 价格清单
下一步: 支付并创建

步骤 8 部署成功后，点击返回。

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	VPC-BJ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zemz8wzprnppqiez7etf	运行中	2022-01-20 10:13:50	定位
2	VSW-BJ-H [H-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze71kofgcrkziu09wzlt	运行中	2022-01-20 10:14:38	定位
3	EIP-TEST	eip (弹性公网IP)	按量付费	eip-2ze12he2ls880wfsw9p1x	运行中	2022-01-20 10:14:37	定位
4	SG-BJ-TEST	security.group (安全组)	-	sg-2ze2z8y274io78nusch5	运行中	2022-01-20 10:14:38	定位
5	ECS-TEST	ecs (云服务器)	按量付费	i-2ze0wnm5f3mpqxx7l63c	运行中	2022-01-20 10:15:23	定位

步骤 9 在资源清单中点击共享带宽，跳转到共享带宽页面，记录实例 ID

The screenshot shows a network diagram and a resource list. The network diagram illustrates a connection between two EIPs (EIP-TEST and EIP-TEST\_1) and two ECS instances (ECS-TEST and ECS-TEST-1) via a shared bandwidth (cbwp). The resources are organized into a VPC (VPC-BJ) and a subnet (VSW-BJ-H). The resource list table below shows two entries: 'ECS-TEST-1' and 'cbwp'. The 'cbwp' entry is highlighted with a red border.

应用操作	导出资源清单					
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
8	ECS-TEST-1	ecs (云服务器ECS)	按量付费	i-2ze4yve5p2dkdsutuv4f	新建	运行中
9	cbwp	cbwp (共享带宽)	按量付费	cbwp-2zeuc6ftxxr4neoj8ncl9	新建	运行中

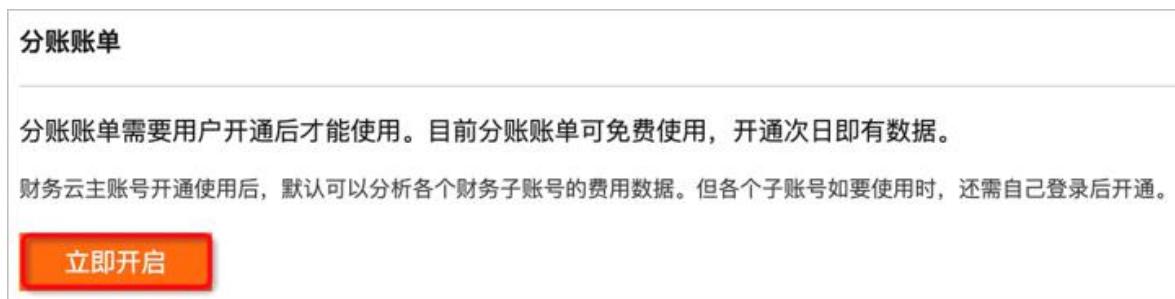
This screenshot shows the detailed configuration of a shared bandwidth named 'cbwp'. The left sidebar lists various networking components like NAT gateways and VPC NAT gateways. The main panel displays the 'Basic Information' tab for the selected 'cbwp-2zeuc6ftxxr4neoj8ncl9' instance. It shows details such as the instance ID, name, and line type (BGP multi-line). The 'Billing Information' tab indicates a pay-as-you-go model with a bandwidth of 10 Mbps. The 'Monitoring' tab features two line charts: 'Network Incoming Bandwidth bps' and 'Network Outgoing Bandwidth bps', both showing stable values around 150-200 bps over a one-hour period.

步骤 10 共享带宽已经绑定了两个 EIP

步骤 11 在共享带宽中找到创建的实例，点击共享带宽实例 > 更多操作 > 查看账单。

步骤 12 在账单详情中，点击分账账单。

### 步骤 13 选择立即开启



### 步骤 14 通过搜索共享带宽的实例 ID 搜索账单信息，信息可能有延时。

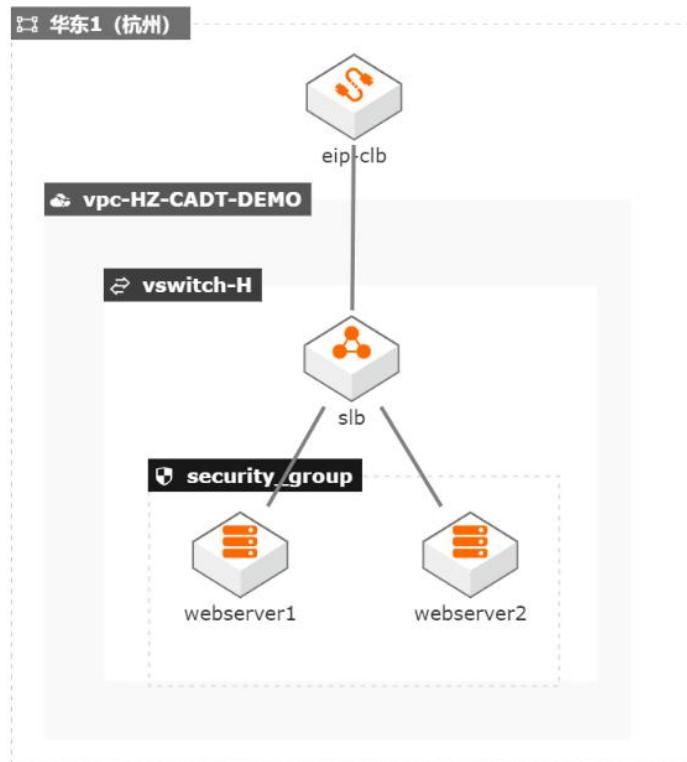
## 3.3.云速搭部署 CLB 实现负载分发

作者 | 阿里云解决方案架构师 洁谦

### 3.3.1. 云速搭创建 CLB 架构设计

#### 方案架构

- 通过云速搭构建一个基于 tcp (或 https) 的负载均衡业务架构，实现终端浏览器发起 tcp (https) 请求后，经过 CLB 负载分发到后端两台 ECS 服务器。
- 具备一个安全组，通过安全组对 ECS 进行详细的安全策略配置。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下图，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
EIP	Region
ECS	VSW
安全组	VPC
CLB	VSW

## 资源规划清单

资源类别	配置项	配置明细	说明
区域	区域	华东 1 (杭州)	本最佳实践全部资源部署在杭州（主数据中心）
专有网络 VPC	状态	新购（根据实际情况选择新购或已保有，本最佳实践新购 VPC）	云上选择专有网络（VPC）以保障安全性。 选择离原系统公网 IP 近的云上区域减少网络延迟。
	VPC 名	vpc-HZ-CADT-DEMO	选择资源丰富、离用户近的区域保障项目顺利实施。
	网段	172.10.0.0/16	网络规划留足可用 IP 数即可。
虚拟交换机	状态	新购（根据实际情况选择新购或已保有，本最佳实践新购交换机）	
	vswitch 名	vswitch_H	
	可用区	华东 1 可用区 H	
	IPv4 网段	172.10.0.0/24	
ECS	可用区	默认（华东 1 可用区 H）	根据 ECS 所在的 vswitch
	ECS 名	WebServer1	http 后端服务
	主机名	WebServer1	http 后端服务
	支付方式	后付费	按量付费
	实例规格	4 核 CPU, 16GB 内存 (ecs.g6.xlarge)	云上业务系统规格按照原规格购买。
	镜像	CentOS	
	镜像版本	CentOS 7.6 64 位	

资源类别	配置项	配置明细	说明
ECS	系统盘	cloud_ssd	ESSD 云盘
	硬盘容量	40GiB	
	公网带宽	按流量付费	
	出网带宽	10	
	登陆密码	*****	初始 root 用户密码，创建成功后由业务方分别登录修改密码。
	安全加固	Active	
CLB	支付方式	按量计费	
	实例规格	简约型 I (slb.s1.small)	
	主可用区	华东 1 可用区 H	
	备可用区	华东 1 可用区 I	
	实例类型	私网	
	计费类型	按使用流量计费	
	IP 版本	IPv4	

### 3.3.2.通过云速搭 CADT 部署资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录 CADT 控制台，如果提示需要开通服务，请根据提示进行开通。

步骤 2 单击新建 > 新建空白应用。



步骤 3 从左侧**快速创建**下选择“单 Region 单可用区”模板到右侧画布区域。



步骤 4 分别双击 region、vpc、vswitch 进行设置。

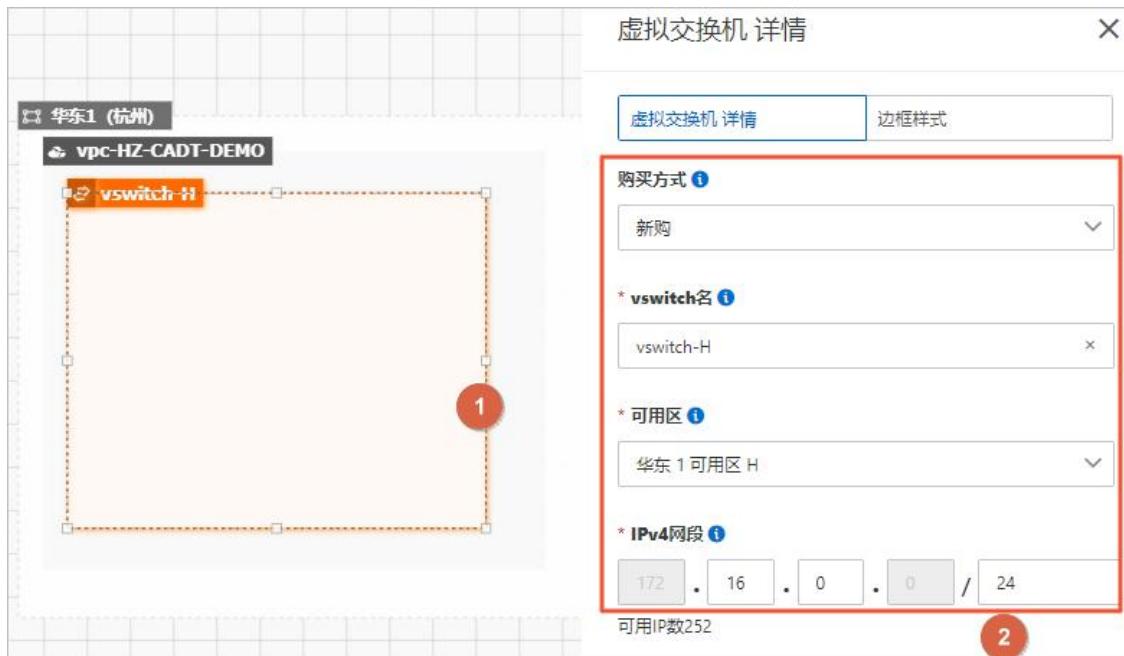
- 配置 region：



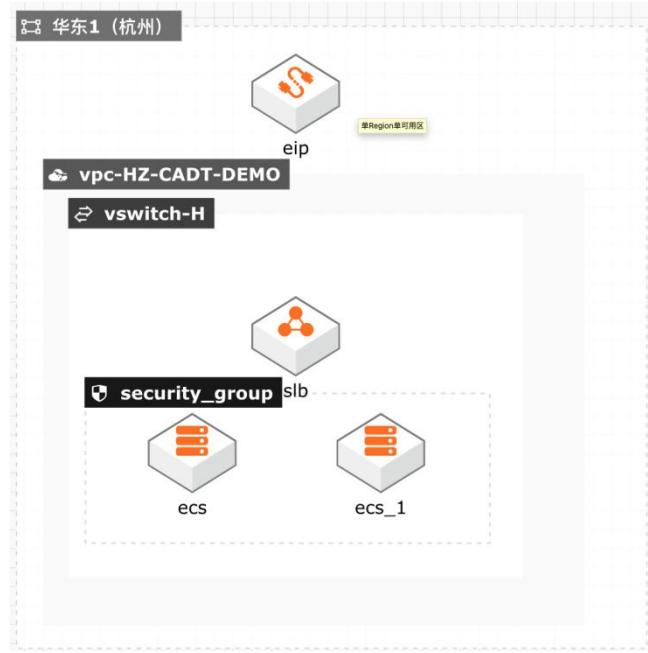
- 配置 vpc：



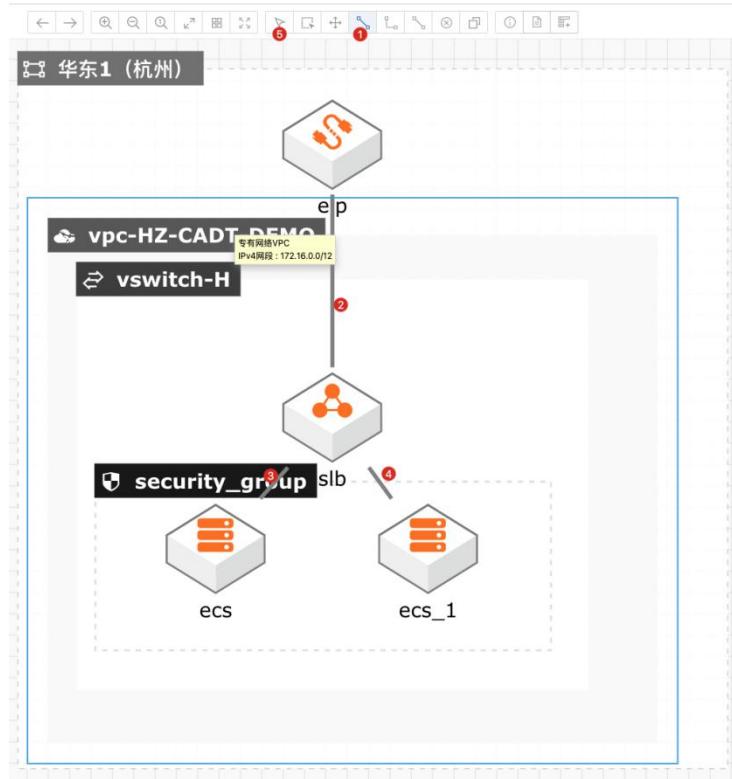
- 配置 vswitch:



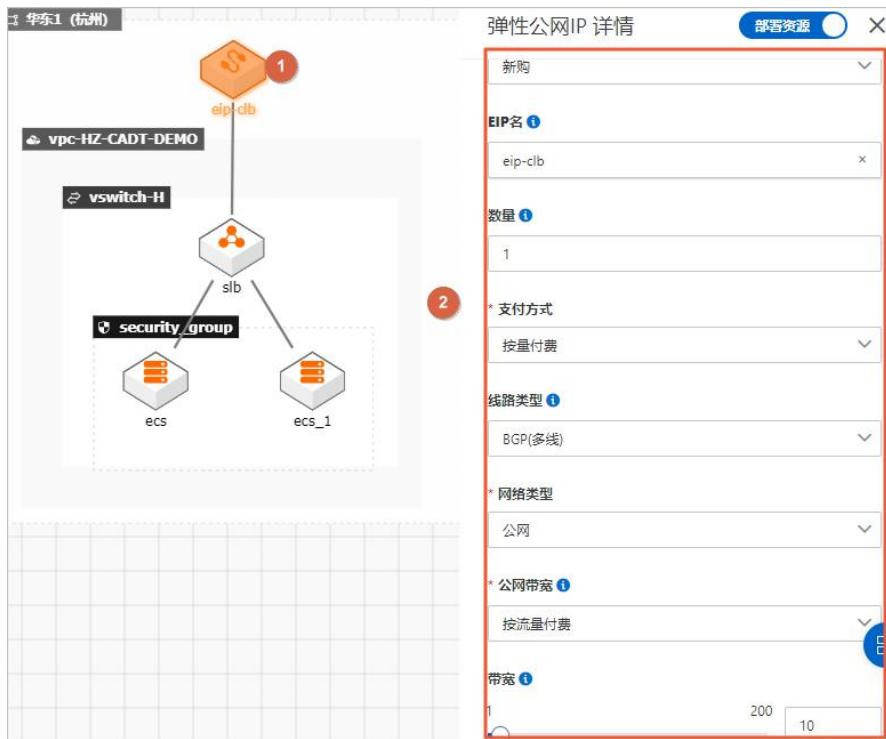
步骤 5 在画布区域调整 region、vpc、vswitch 图层到合适大小后，分别从左侧产品列表中选择安全组、ECS、EIP、CLB（私网）拖入对应区域中（参考[理解资源级别](#)，根据架构资源级别设计）。



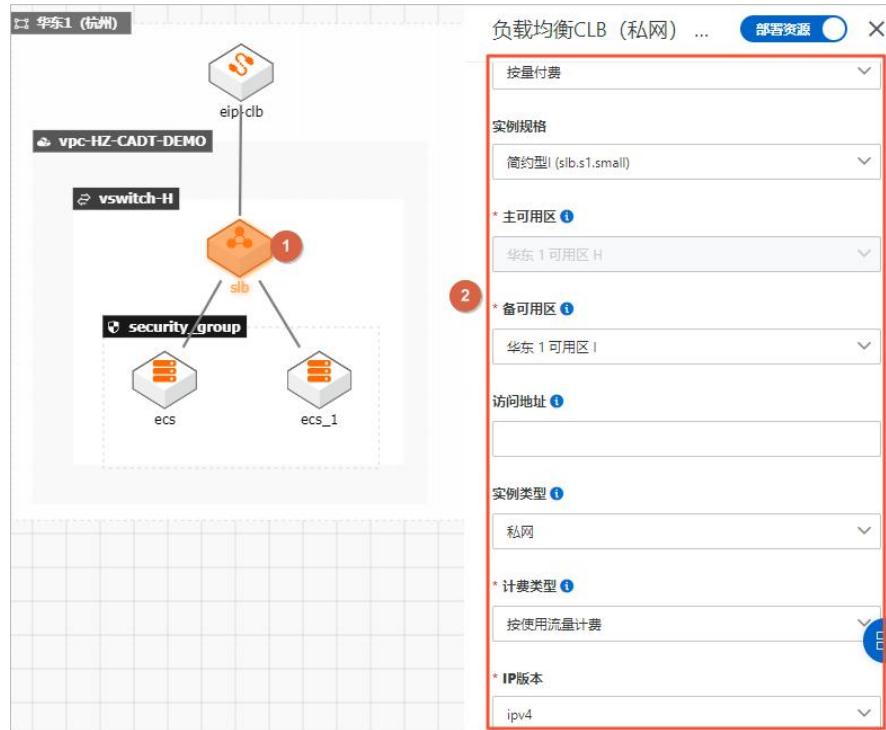
步骤 6 单击**创建连线**按钮，将 CLB 与两台 ECS 连接，EIP 与 CLB 连接。创建完连线后，需要切换回**默认模式**。



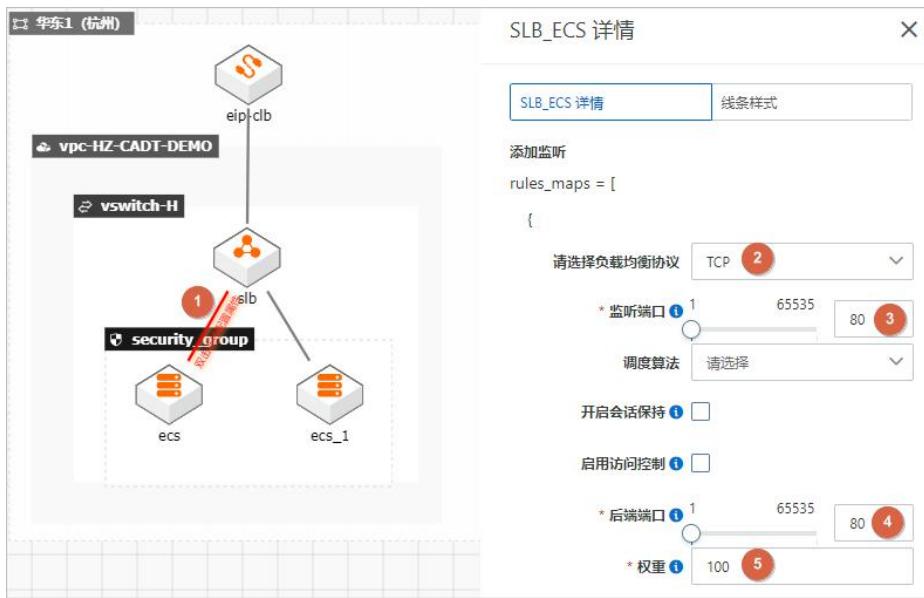
步骤 7 双击 EIP 进行规格配置。



步骤 8 双击 CLB 进行实例规格配置。



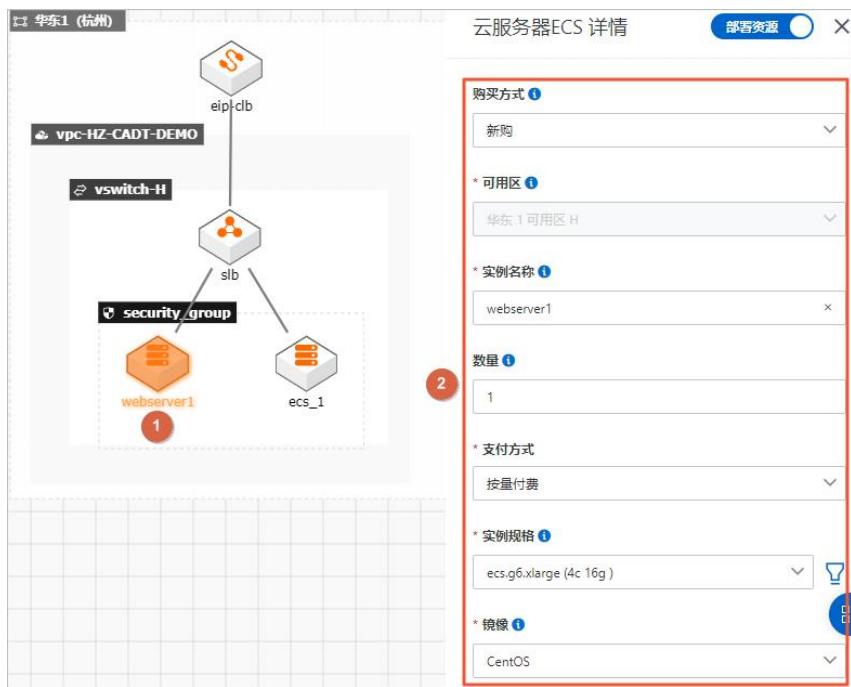
步骤 9 双击 CLB-ECS 之间的连线，配置监听信息。



同样方法配置另一条 CLB-ECS 连线。

步骤 10 配置 ECS。

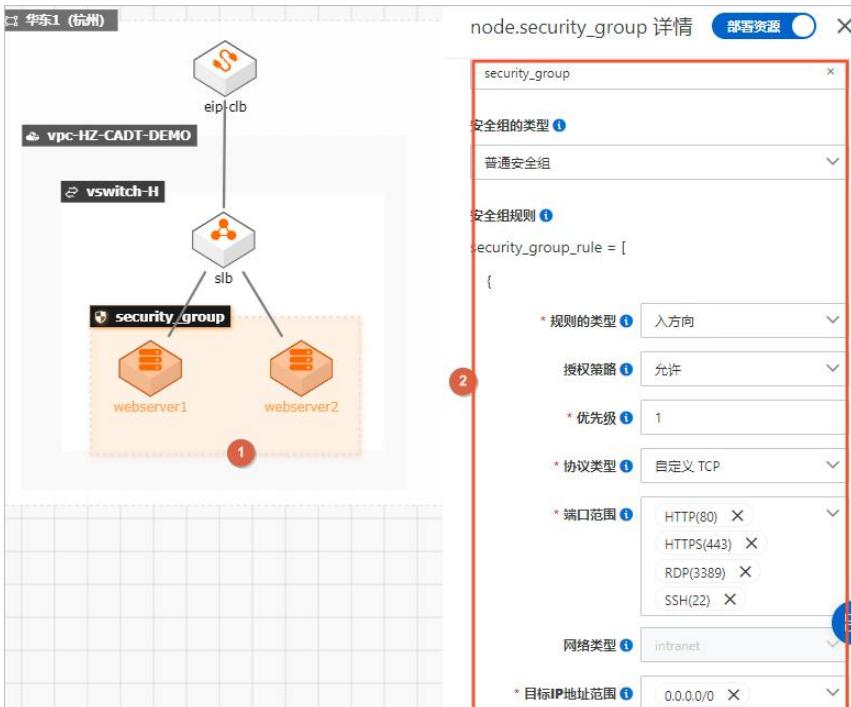
配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	webserver1
支付方式	按量付费
实例规格	ecs.g6.xlarge(4c 16g)
镜像	CentOS
镜像版本	CentOS 7.6 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
公网 IP	分配公网 IPv4 地址
宽带计费模式	按流量付费
带宽（峰）值	10 Mbps
主机名	webserver1
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>



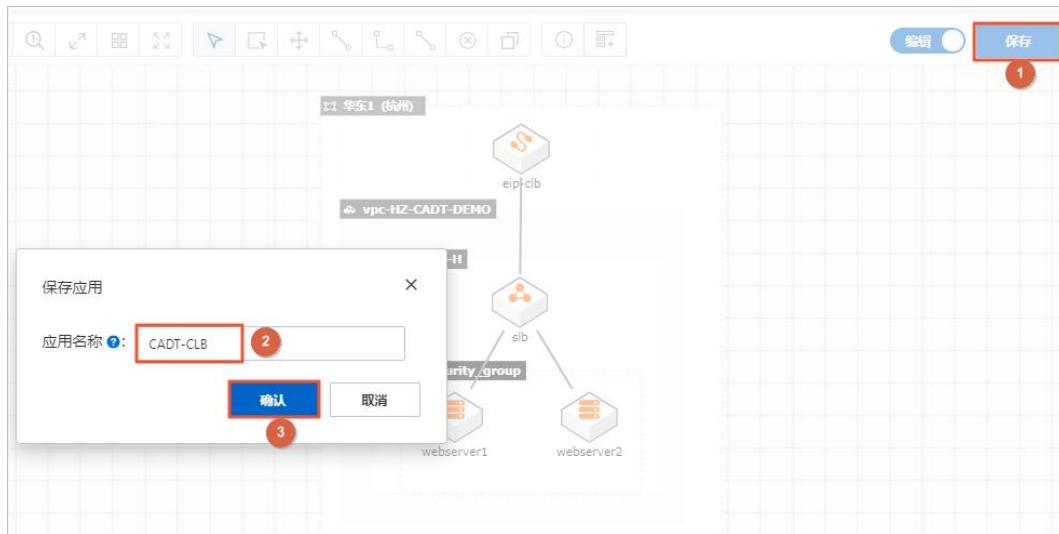
按照同样配置项配置另外一台 ECS，实例名称设定为 webserver2。

为方便后续 ECS 上部署应用，将两台 ECS 开通公网 IP。（企业环境建议内网 ECS 通过 NAT 网关主动访问互联网，日常 SSH 登录通过堡垒机跳转。）

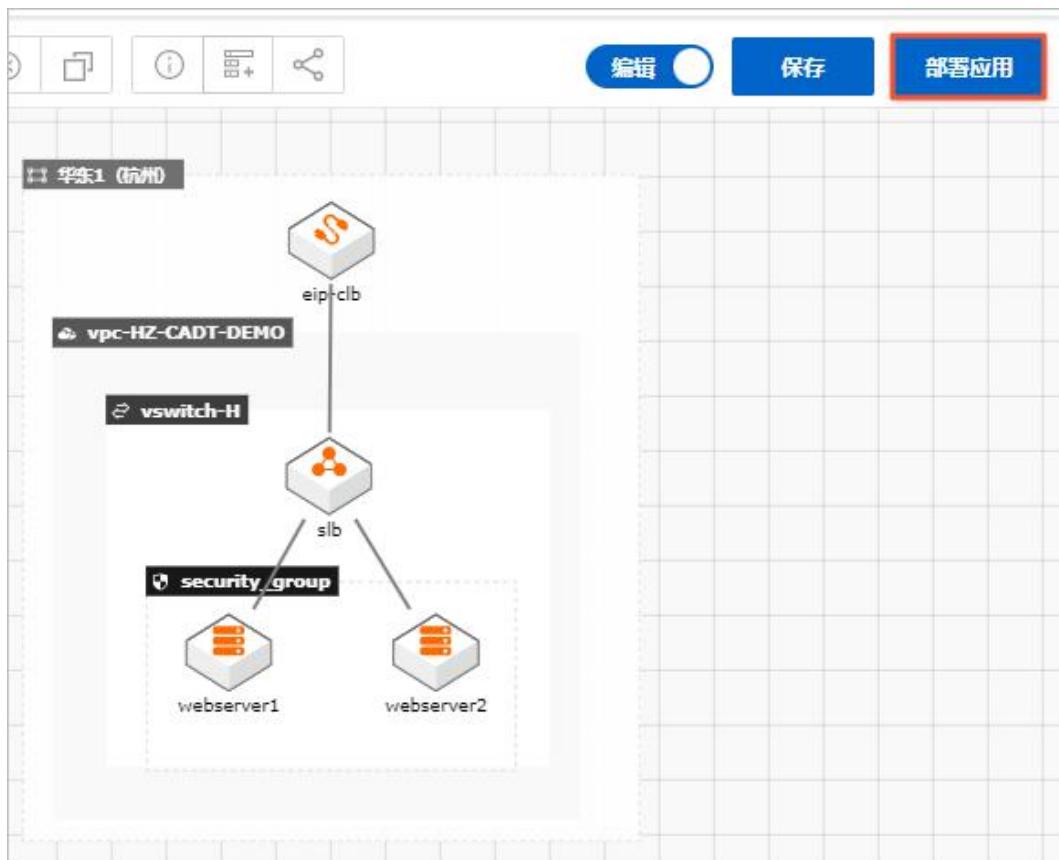
步骤 11 双击安全组，配置安全组策略，放行 22、80、443 端口。



步骤 12 配置完成后，单击右上角**保存**按钮，输入应用名称，单击**确认**。



步骤 13 保存完成后，单击**部署应用**。



步骤 14 等待资源验证成功，单击**下一步：价格清单**。

**资源验证**

资源名称	资源类型	区域	规格	结果	备注	操作
webserver1	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
webserver2	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
slb	clb	杭州	slb.s1.small	成功	校验通过	定位
security_group	security.group	杭州	normal	成功	校验通过	定位
eip-clb	eip	杭州	public	成功	校验通过	定位

状态: **校验成功**

① **下一步: 价格清单** **返回**

步骤 15 计价成功后，单击**下一步：确认订单**。

**导出价格清单**

**免费** **按量付费**

**资源成本占比**

资源预算

- 计算 计算: 0 元/时
- 网络 网络: 0 元/时

**价格列表**

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
eip-clb	eip	杭州	public	1	0 元/时	省 0 元/时	0 元/时	定位
slb	clb	杭州	slb.s1.small	1	0 元/时	省 0 元/时	0 元/时	定位
webserver1	ecs	杭州	ecs.g6.xlarge	1	0 元/时	省 1.2 元/时	0 元/时	定位
webserver2	ecs	杭州	ecs.g6.xlarge	1	0 元/时	省 1.2 元/时	0 元/时	定位

状态: **计价成功**

**上一步: 资源校验** **查看报告** ① **下一步: 确认订单**

步骤 16 核对订单无误后，勾选《云速搭服务条款》，并单击**下一步：支付并创建**，进行应用部署。

确认订单

免费 按量付费

资源名称	资源类型	区域	规格	数量	原价	实付	状态
webserver2	ecs	杭州	ecs.g6.xlarge	1	1元/时	1元/时	新购
webserver1	ecs	杭州	ecs.g6.xlarge	1	1元/时	1元/时	新购
slb	clb	杭州	slb.s1.small	1	1元/时	1元/时	新购
eip-clb	eip	杭州	public	1	2元/时	2元/时	新购

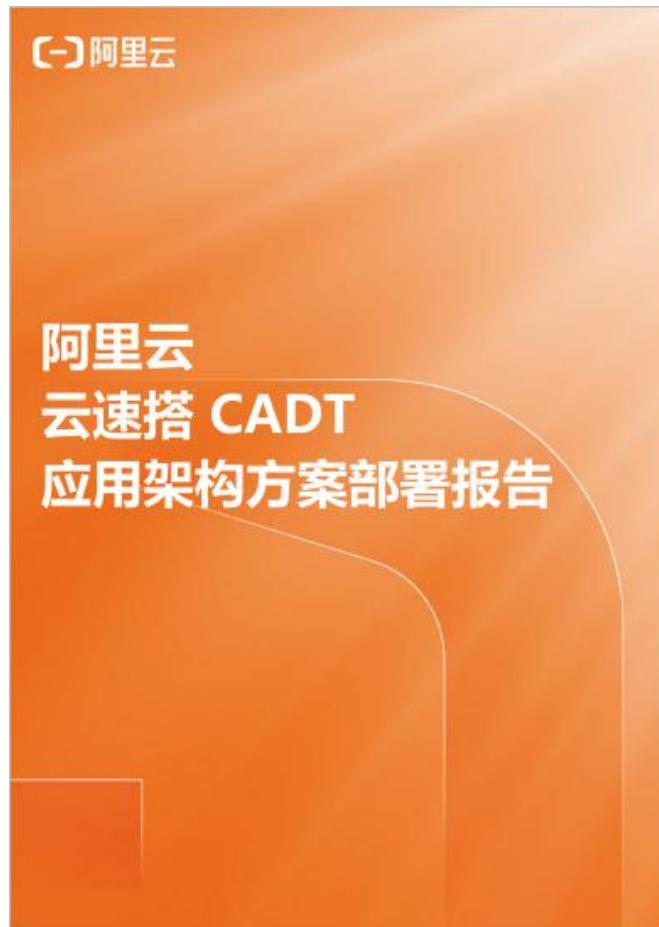
《云速搭服务条款》①  
部署前,请阅读并勾选服务条款

按量付费: 10元/时

状态: 计价成功

上一步: 价格清单 ② 下一步: 支付并创建

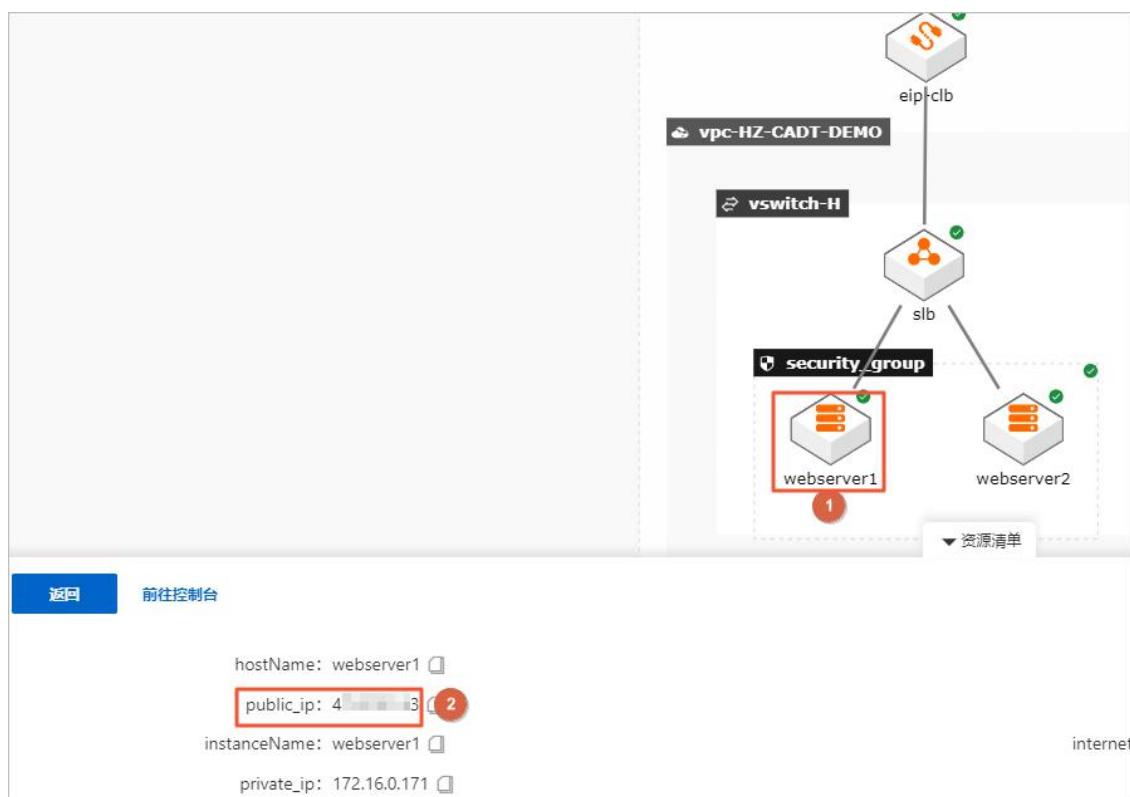
步骤 17 部署成功后, 单击查看报告, 可以查看详细的应用部署报告。



### 3.3.3.验证通过 CLB 转发到 ECS 实现负载分发

步骤 1 通过公网 IP 登录 ECS (webserver1)

1. 双击 webserver1 这台 ECS 实例，复制该 ECS 的公网 IP。



2. SSH 登录到该 ECS，执行下面指令，安装 httpd 服务，并启动服务。

```
yum install -y httpd  
systemctl start httpd  
systemctl status httpd
```

3. 确认 httpd 正常启动：

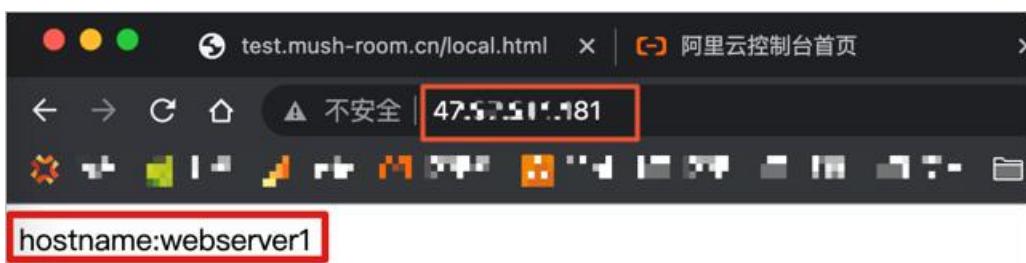
```
[root@webserver1 ~]# systemctl start httpd
[root@webserver1 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since 四 2021-10-21 16:52:24 CST; 5s ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Main PID: 2110 (httpd)
      Status: "Processing requests..."
     CGroup: /system.slice/httpd.service
             ├─2110 /usr/sbin/httpd -DFOREGROUND
             ├─2111 /usr/sbin/httpd -DFOREGROUND
             ├─2112 /usr/sbin/httpd -DFOREGROUND
             ├─2113 /usr/sbin/httpd -DFOREGROUND
             ├─2114 /usr/sbin/httpd -DFOREGROUND
             └─2115 /usr/sbin/httpd -DFOREGROUND

10月 21 16:52:24 webserver1 systemd[1]: Starting The Apache HTTP Server...
10月 21 16:52:24 webserver1 httpd[2110]: AH00558: httpd: Could not reliably determine...ge
10月 21 16:52:24 webserver1 systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

#### 4. 创建一个 html 文件：

```
cat <<EOF > /var/www/html/index.html
<html>
hostname: `hostname` 
</html>
EOF
cat /var/www/html/index.html
```

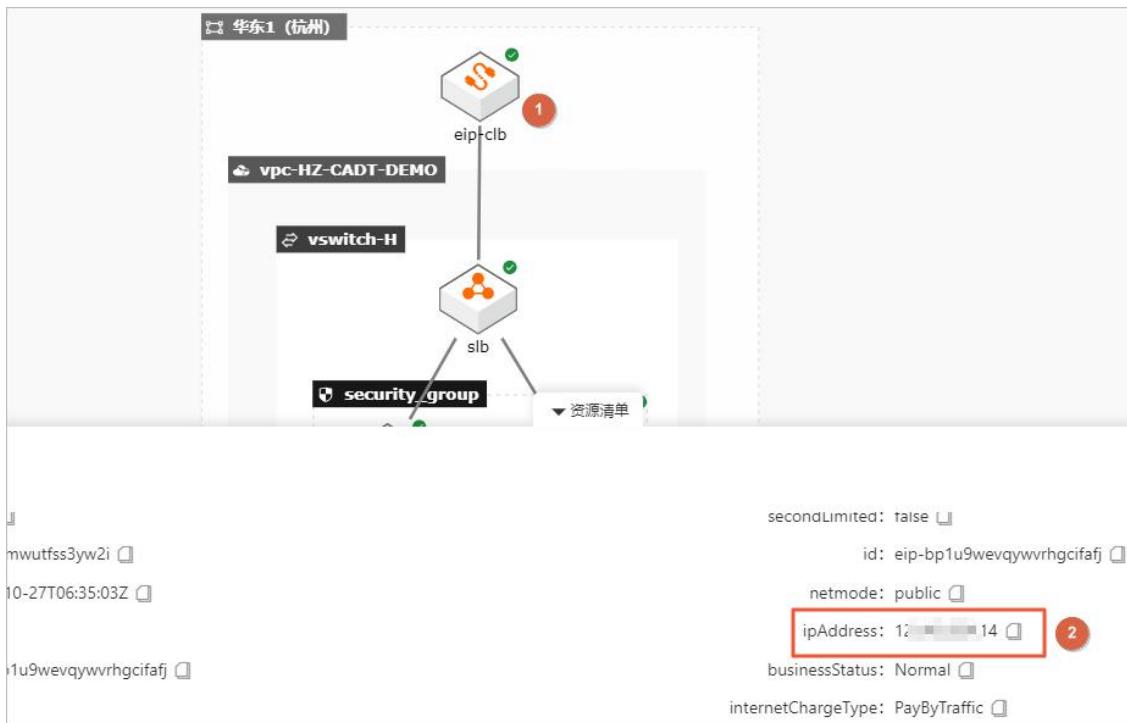
#### 5. 浏览器输入 `http://<ECS public ipAddress>/`, 验证 ECS 上 http 服务正常。



步骤 2 另外一台 ECS 按照上述流程也配置完成 http 服务。

步骤 3 配置域名，添加 A 解析记录。

- 本步骤前提为已申请域名且已通过备案，本例已申请并备案域名备用。双击 EIP，在下方详情页面找到并复制公网 IP 地址。



2. 登录云解析 DNS 控制台 <https://dns.console.aliyun.com/>，单击目标域名的解析设置。

The screenshot shows the AliCloud DNS console interface:

**左侧导航栏 (Left Navigation Bar):**

- 云解析DNS
- 域名解析 (1)** (highlighted with a red box and circled with a red number "1")
- PrivateZone
- 全局流量管理 (旧版)
- 全局流量管理
- IP地理位置库
- 辅助DNS
- 公共DNS
- 操作日志

**右侧内容区 (Main Content Area):**

- 域名解析** (Domain Resolution)
- 公告: .com/.net/.cn/.xin/.top/.xyz/.vip/.club/.shop/.wang/.ren等域名注册成功后必须进行域名实名认证，否则会造成解析不生效，实名认证审核通过后的1-2个工作日解析可恢复。
- 【金秋十月】云解析新用户限时活动: 新购、续费同享75折!
- [0元试用] 阿里云DNS全系列产品 新用户免费试用
- 权威域名 (highlighted with a blue box)
- 缓存加速域名
- 请求量统计
- 版本套餐管理
- 更多服务
- 全部域名
- 域名快速搜索
- 操作
- 域名: mush...om.cn (highlighted with a red box)
- 标签
- 记录数: 363
- DNS服务器状态: 正常
- 付费版本: 免费版
- 解析设置 (2)** (highlighted with a red box and circled with a red number "2")

3. 单击添加记录。

The screenshot shows the "解析设置" (Resolution Settings) page for the domain mush-room.cn:

**顶部信息 (Top Information):**

- 当前分配的DNS服务器是: dns27.hichina.com, dns28.hichina.com

**底部操作栏 (Bottom Operation Bar):**

- 添加记录** (highlighted with a red box)
- 导入/导出
- 请求量统计
- 新手引导
- 全部记录
- 精确搜索

4. 添加一条 A 记录。

记录类型: ①

A- 将域名指向一个IPV4地址

主机记录: ②

test-clb .mush-room.cn ③

解析线路: ④

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: ⑤

127.0.0.1:200

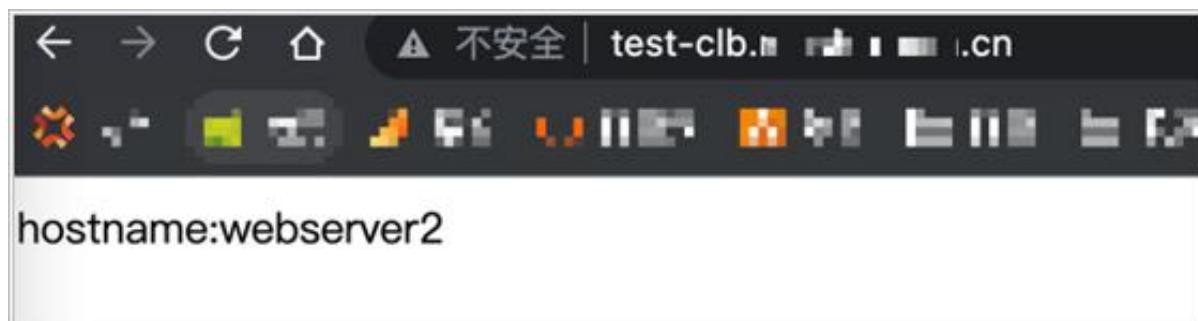
\* TTL: ⑥

10 分钟

取消 确认

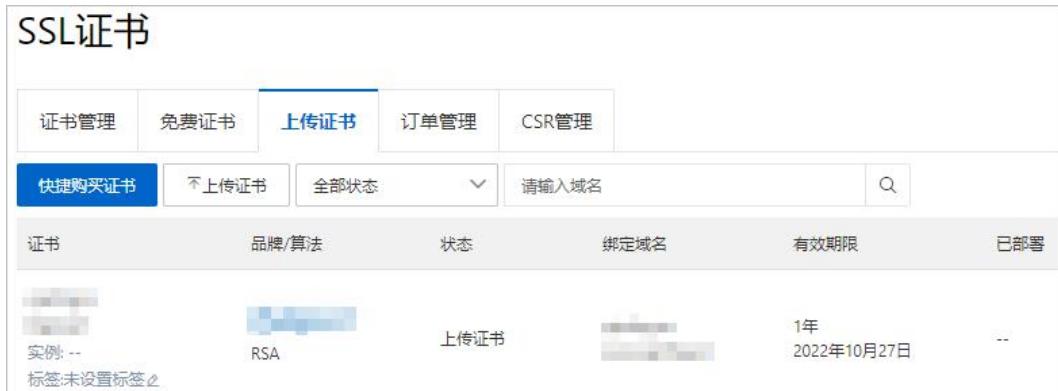
步骤 4 CLB 功能验证。

域名解析配置完成后, 等待解析生效 (一般 10 分钟内), 使用浏览器访问刚添加解析的域名。反复刷新页面可以看到请求被随机分发到 webserver1 和 webserver2 上。



### 3.3.4. 验证 CLB 挂载 SSL 证书实现 https 转发

步骤 1 为了验证 CADT 配置 CLB 的 https 监听，事先针对测试域名准备一个自签名证书。SSL 证书相关内容请查阅：<https://help.aliyun.com/product/28533.html>



步骤 2 重新部署测试环境，首先释放当前资源，单击资源清单 > 释放全部资源。

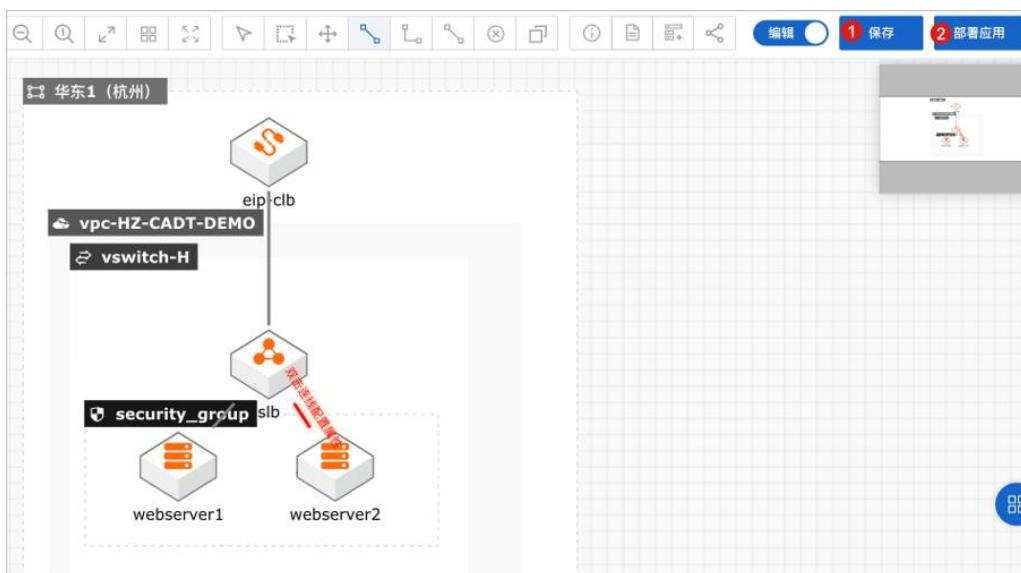


步骤3 释放成功后，双击CLB-ECS连线，配置https监听。



同样方法配置另一条线的监听。

步骤4 保存架构图，单击**部署应用**。

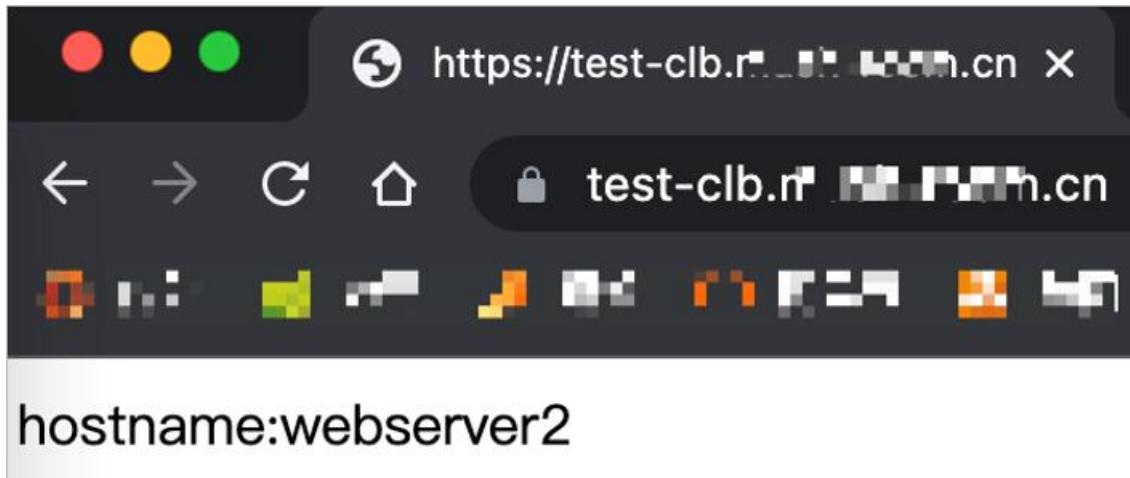


步骤5 验证CLB https转发。

1. 参考[验证通过CLB转发到ECS实现负载分发](#)步骤1，在两台ECS部署httpd服务。
2. 参考[验证通过CLB转发到ECS实现负载分发](#)步骤2，在云解析DNS控制台修改之前添加的A解析记录为新的EIP地址。

The screenshot shows the 'DNS解析' (DNS Resolution) section of the Hichina management console. The left sidebar includes options like '解析设置' (Resolution Settings), 'DNS安全' (DNS Security), '权重配置' (Weight Configuration), '自定义线路' (Custom Path), and '解析日志' (Resolution Log). The main area is titled '解析设置 mush-room.cn' and displays a table of DNS records. The table has columns for '主机记录' (Host Record), '记录类型' (Record Type), '解析线路(Isp)' (Resolution Path), '记录值' (Record Value), 'TTL' (Time-to-Live), '状态' (Status), '备注' (Remarks), and '操作' (Operations). Three records are listed: one for 'dev' with value '127.0.0.1' and another for 'mush-room' with value '127.0.0.1'. A new record 'test-clb' is being added at the bottom, highlighted with a red border. The status bar at the top indicates the current DNS servers are dns27.hichina.com and dns28.hichina.com.

步骤 6 浏览器输入 <https://<测试域名>>，反复刷新页面可以看到请求被分发到 webserver1 和 webserver2 上。



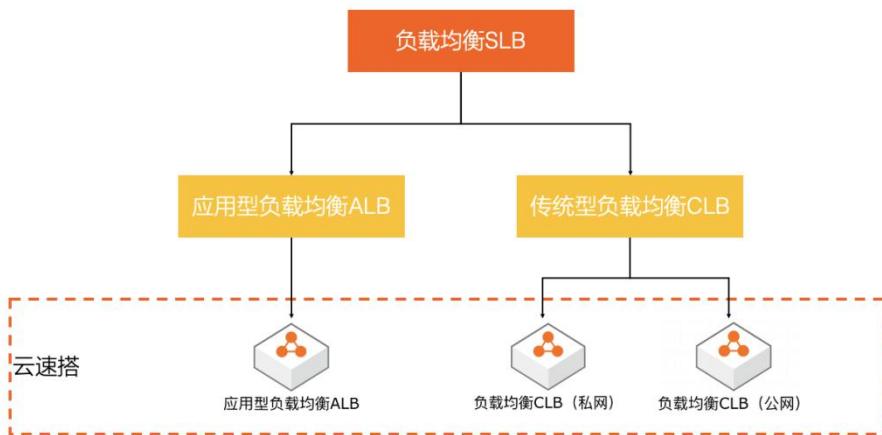
## 3.4.云速搭部署和导入公网型负载均衡 CLB

作者 | 阿里云解决方案架构师 天裴

### 3.4.1. 云速搭架构设计入门

#### 方案简介

- 云速搭已经支持全部类型的负载均衡实例。



- 本最佳实践讲解如何通过云速搭导入一个已保有的公网型负载均衡 CLB，并部署一个新的公网型 CLB。



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
公网型负载均衡 CLB	Region

### 已保有公网型 CLB

为演示将保有的公网型 CLB 导入 CADT 应用架构，请事先创建一个公网型 CLB 实例，详细操作可以参考 [https://help.aliyun.com/document\\_detail/86454.html](https://help.aliyun.com/document_detail/86454.html)

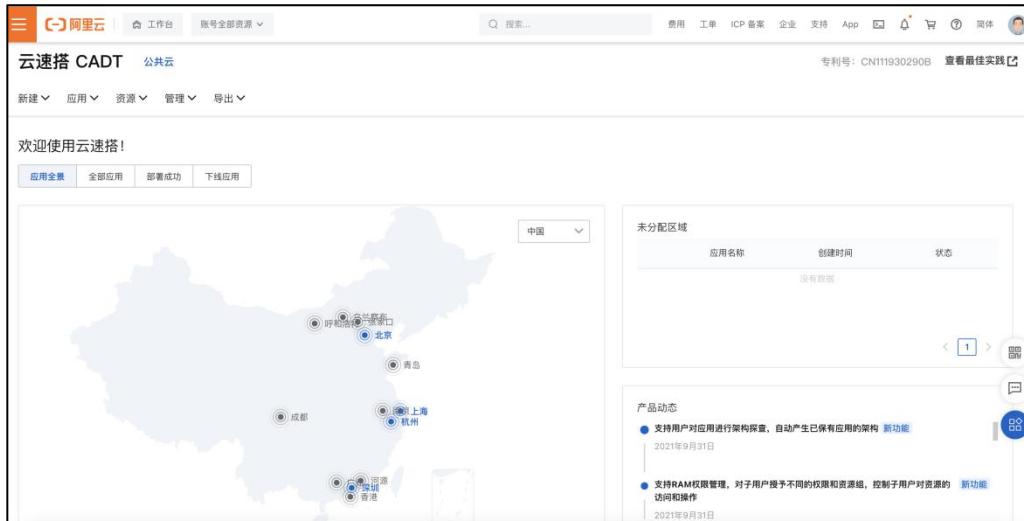
在本例中，我们已经通过控制台在深圳创建了一个公网型 CLB 实例（主可用区：华南 1 可用区 D；备可用区：华南 1 可用区 E）

### 3.4.2.CADT 部署公网型 CLB

### 3.4.3. 创建基础网络资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/> 登录 CADT 控制台。

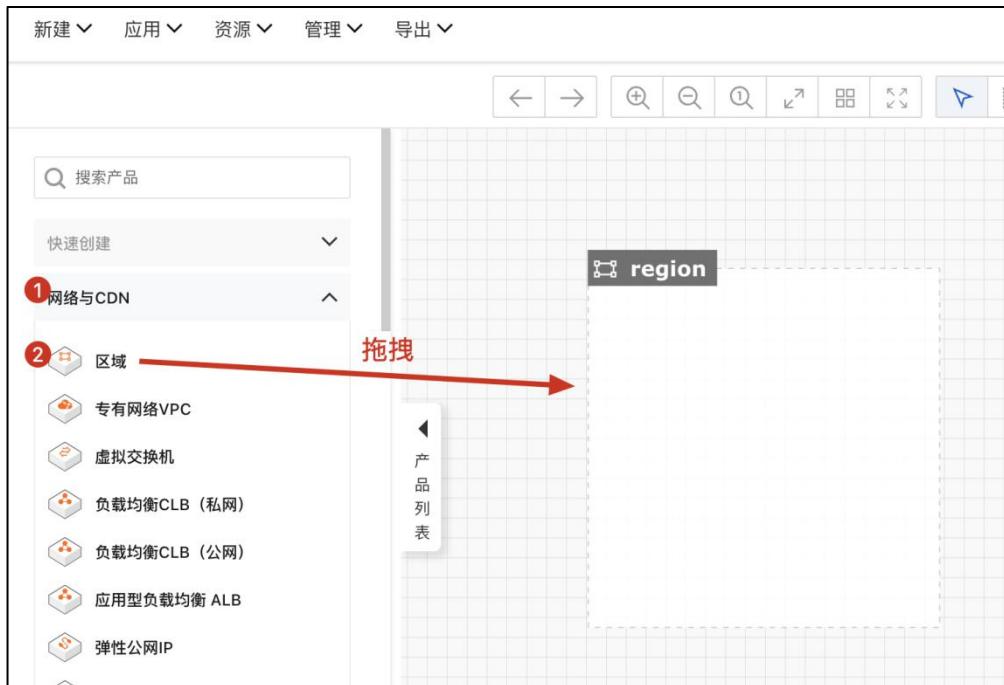
**说明：**如果提示需要开通服务，请根据提示进行开通。



步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



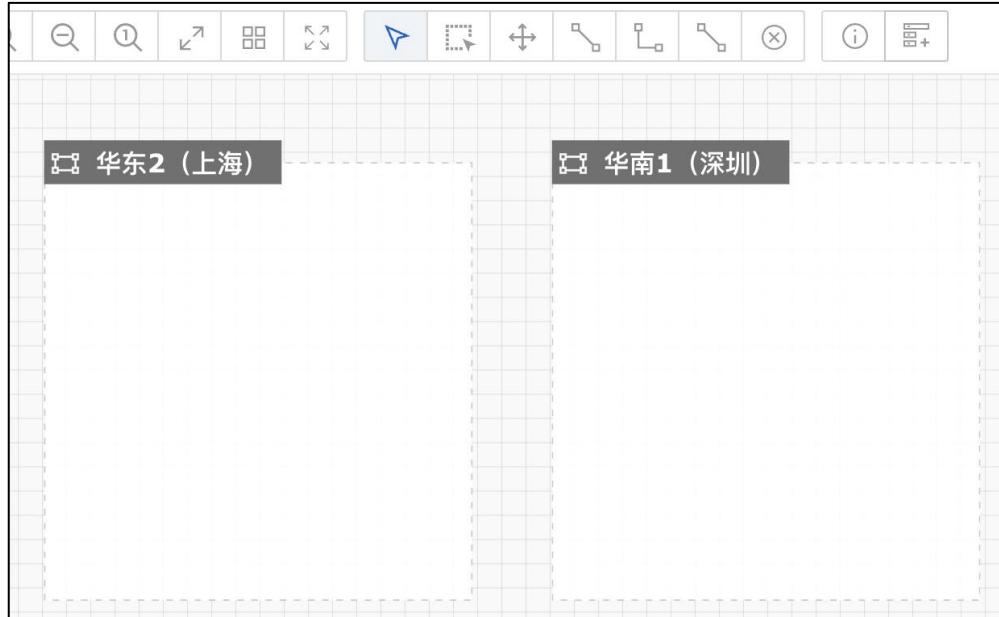
步骤 3 从左侧网络产品列表找到**区域**，单击拖入到画布区域中，松开鼠标。



步骤 4 在 `region` 对象的任意位置双击鼠标，开启配置清单，选择华东 2（上海）。

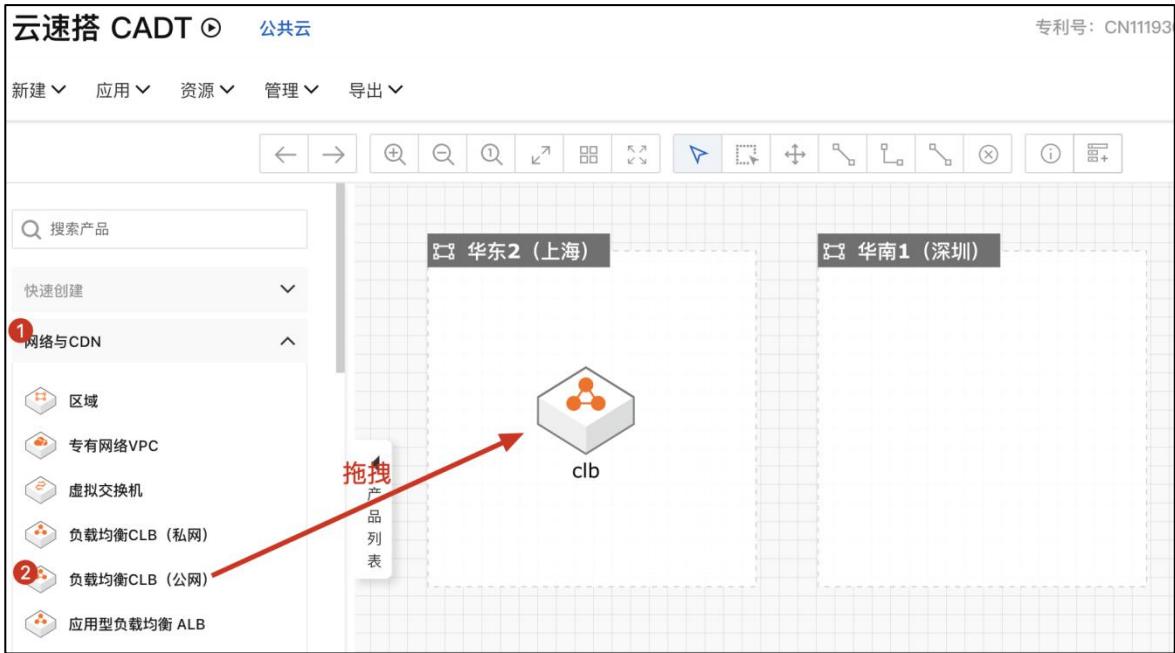


步骤 5 重复步骤 3~4，拖入一个新的区域，并选择华南 1 (深圳)。



### 3.4.4.新建公网型 CLB

步骤 1 从左侧网络产品列表找到**负载均衡 CLB (公网)**，单击拖入到上海区域中。



步骤 2 双击 clb 图标，开启配置。



步骤 3 按以下配置项完成配置后，关闭配置页面。

配置型	内容
购买方式	新购
实例名称	自定义，本例使用“新建公网型 CLB”
支付方式	按量付费（方便测试后释放资源）
实例规格	根据业务需要选择，本例选择 简约型 I (slb.s1.samll)
主可用区	华东 2 可用区 G
备可用区	华东 2 可用区 E
访问地址	(非必填)
实例类型	公网
计费类型	根据业务需要选择，本例选择 按使用流量计费
IP 版本	根据业务需要选择，本例选择 IPV4
打标	非必填
资源组	非必填

完成配置后关闭配置清单。

### 3.4.5. 导入已保有公网型 CLB

步骤 1 从左侧网络产品列表找到 **负载均衡 CLB (公网)**，单击拖入到深圳区域中。



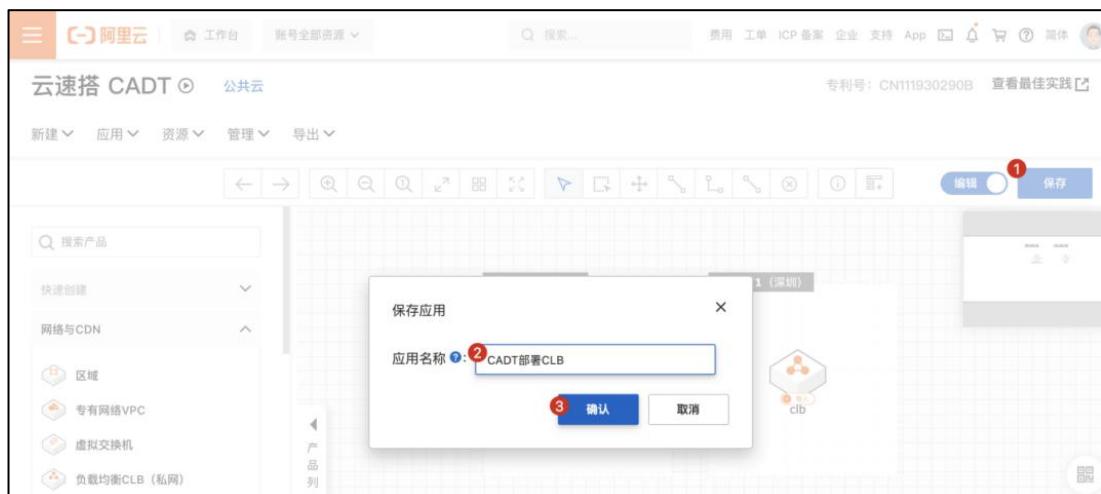
步骤 2 双击 clb 图标，开启配置。

**注意：**这里要首先选择已保有 CLB 的主可用区（本例为华南 1 可用区 D），接着选择已保有 CLB 的备可用区（本例为华南 1 可用区 E），这样才可以在实例名下拉菜单中找到已保有的 CLB 实例。



### 3.4.6.保存架构图

步骤 1 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写**应用名称**，并单击**确认**。

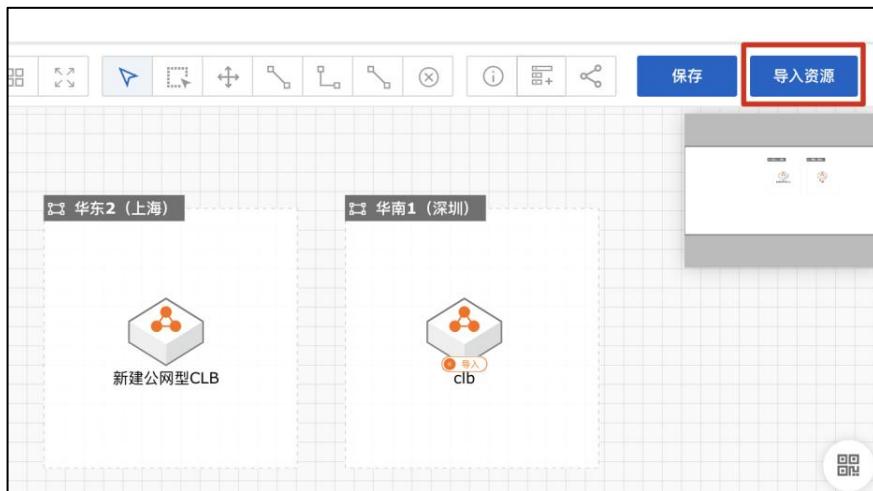


## 3.4.7.执行导入和部署

由于在架构图中同时拥有**导入的保有资源**和**新建资源**，我们需要首先将保有资源导入，再创建新的资源。

### 3.4.7.1.执行导入和部署

步骤 1 单击导入资源。



步骤 2 确认待导入清单，单击导入。



**说明：**资源导入 CADT 仅仅是将已保有的资源纳入 CADT 管控，对资源本身不会有任何影响。  
片刻后即可完成导入。

步骤 3 完成导入后单击返回。



### 3.4.7.2. 执行部署新资源

完成保有 CLB 导入后，就可以创建新的 CLB。

步骤 1 单击右上角的**部署应用**。



步骤 2 开始进行资源验证，如果有校验错误提示，根据提示进行修改，直至校验成功后单击**下一步：价格清单**。



步骤 3 待询价成功后，核对方案价格（也可以单击**查看报告**导出 PDF 版的报价清单），单击**下一步：确认订单**。

**导出价格清单**

免费 按量付费

资源成本占比

资源预算  
● 网络 网络: 100% 元/时

10...

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	新建公网型CLB	clb	上海	slb.s1.small	1	0.01元/时	0.01元/时	0.01元/时	定位

状态: **询价成功(架构调整)**

上一步: 资源校验 查看报告 下一步: 确认订单

步骤 4 勾选《云速搭服务条款》，单击**下一步：支付并创建**。

**确认订单**

免费 按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	新建公网型clb	clb	上海	slb.s1.small	1	0.01元/时	0.01元/时	新购

《云速搭服务条款》

部署前，请阅读并勾选服务条款

按量付费: 0.01元/时

状态: **计价成功**

上一步: 价格清单 下一步: 支付并创建

步骤 5 进入部署流程，这里会进行扣费并开始创建资源。



步骤 6 等待资源部署完成, 单击[返回](#)。



步骤 7 资源部署完成后, 可打开[资源清单](#)查看所有的资源信息。

The screenshot shows the 'Resource Catalog' interface for CLB. At the top, there are deployment status indicators: '部署成功' (Deployment successful) and various navigation icons. Below is a map view with regions: 华东2 (上海) and 华南1 (深圳). Each region contains a CLB icon with a green checkmark. A red box highlights the '▼ 资源清单' (Resource Catalog) button at the bottom center of the map area.

历史版本 释放全部资源 同步资源数

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	clb	clb	按量付费	lb-wz9ikwd8l1006t5fsls6h	已保有	运行中	-	定位	<a href="#">详情</a>   <a href="#">监控</a>
2	新建公网型CLB	clb	按量付费	lb-uf6rkvime4h8onw3loofi	新建	运行中	2021-11-02 20:54:33	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更</a>

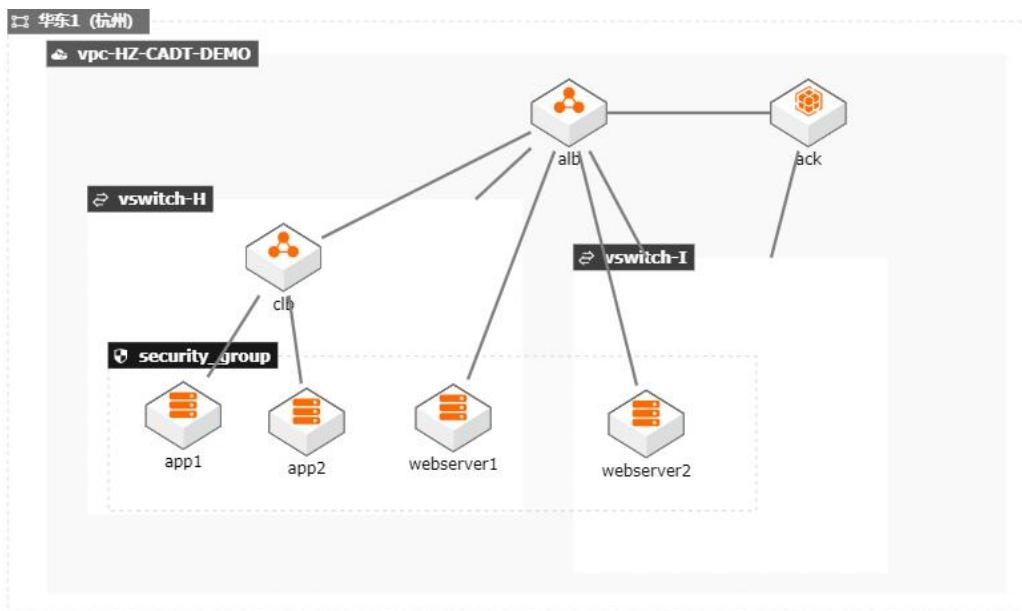
## 3.5.云速搭部署 ALB 实现负载分发

作者 | 阿里云解决方案架构师 洁谦

### 3.5.1. 云速搭部署 ALB 架构设计

#### 方案架构

- 通过云速搭构建一个基于 http(s)的负载均衡业务架构，实现终端浏览器发起 http(s)请求后，经过 ALB 监听配置的转发规则，分别负载分担到后端 ECS 服务器、CLB 和 ACK 集群。
- 具备一个安全组，通过安全组对 ECS 进行详细的安全策略配置。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下图，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
ECS	VSW
安全组	VPC
ALB	VPC
CLB	VSW
ACK	VPC

## 资源规划清单

资源类别	配置项	配置明细	说明
区域	区域	华东 1 (杭州)	本最佳实践全部资源部署在杭州（主数据中心）
专有网络 VPC	状态	新购（根据实际情况选择新购或已保有，本最佳实践新购 VPC）	云上选择专有网络（VPC）以保障安全性。 选择离原系统公网 IP 近的云上区域减少网络延迟。
	VPC 名	vpc-HZ-CADT-DEMO	
	网段	172.10.0.0/16	选择资源丰富、离用户近的区域保障项目顺利实施。 网络规划留足可用 IP 数即可。
虚拟交换机	状态	新购（根据实际情况选择新购或已保有，本最佳实践新购交换机）	
	vswitch 名	vswitch_H	
	可用区	华东 1 可用区 H	
	IPv4 网段	172.10.0.0/24	
	vswitch 名	vswitch_I	
	可用区	华东 1 可用区 I	
	IPv4 网段	172.10.1.0/24	

资源类别	配置项	配置明细	说明
ECS	可用区	默认 (华东 1 可用区 H /I)	根据 ECS 所在的 vswitch
	ECS 名	WebServer1	http 后端服务
	主机名	WebServer1	http 后端服务
	支付方式	后付费	按量付费
	实例规格	4 核 CPU, 16GB 内存 (ecs.g6.xlarge)	云上业务系统规格按照原规格购买。
	镜像	CentOS	
	镜像版本	CentOS 7.6 64 位	
	系统盘	cloud_ssd	ESSD 云盘
	硬盘容量	40GiB	
	公网带宽	按流量付费	
CLB	出网带宽	10	
	登陆密码	*****	初始 root 用户密码, 创建成功后由业务方分别登录修改密码。
	安全加固	Active	
ACK	支付方式	按量计费	
	实例规格	简约型 I (slb.s1.small)	
	主可用区	华东 1 可用区 H	
	备可用区	华东 1 可用区 I	
	实例类型	私网	
	计费类型	按使用流量计费	
	IP 版本	IPv4	
Pod 网络	集群规格	Pro 版	
	Kubernetes 版本	1.18.8-aliyun.1	
	容器运行时	Docker 19.03.5	
	Worker 部署可用区	cn-hangzhou-i	
	网络插件	Flannel	
	Pod 网络 CIDR	192.168.0.0/17	

资源类别	配置项	配置明细	说明
ACK	Service CIDR	192.168.128.0/17	
	节点 IP 数量	32	
	Worker 付费类型	按量付费	
	Worker 实例规格	ecs.g6.xlarge(4c 16g)	
	Worker 数量	2	
	Worker 系统盘类型	cloud_essd	
	性能级别	PL0	
	worker 系统盘大小	120	
	woker 操作系统	Alibaba Cloud Linux	
	woker 登录方式	设置密码	
	登录密码	<输入自定义密码>	

### 3.5.2. 通过云速搭 CADT 部署资源

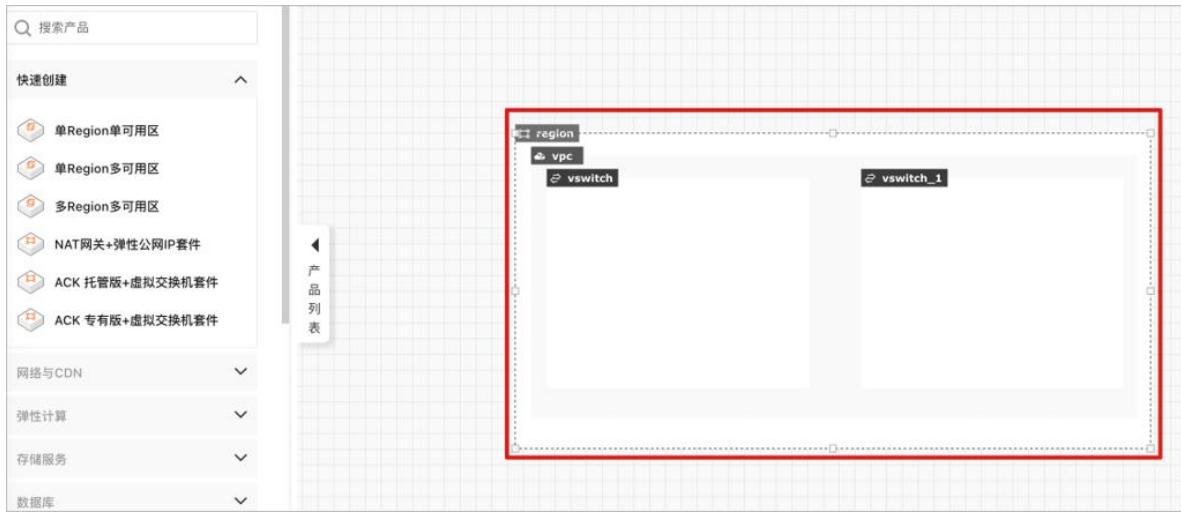
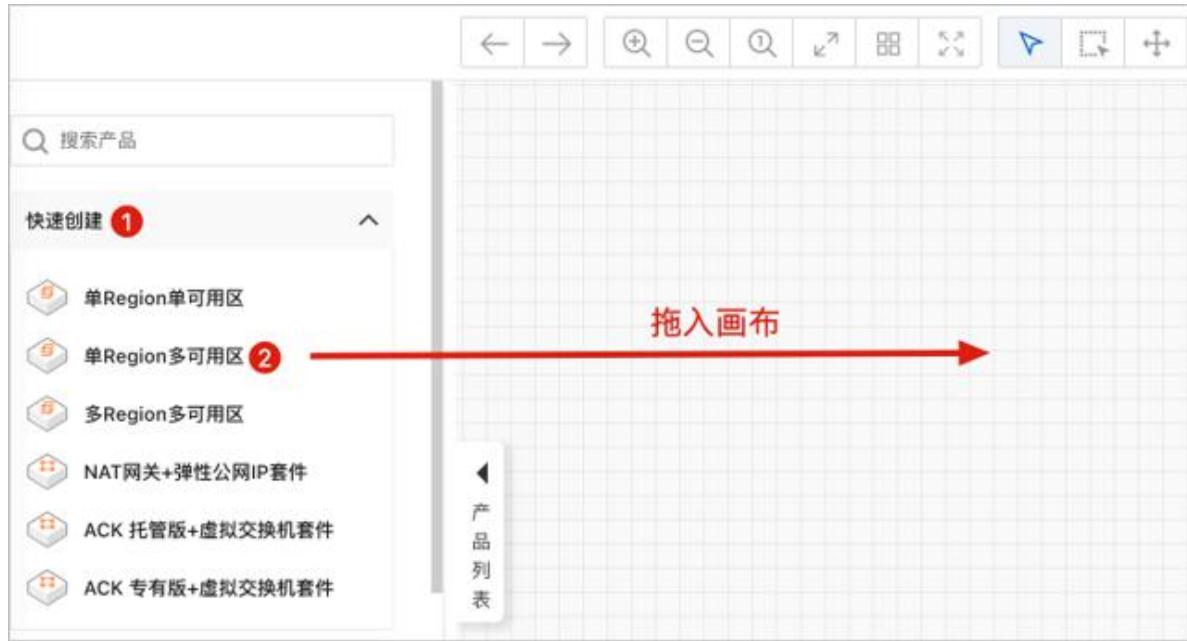
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录 CADT 控制台，如果提示需要开通服务，请根据提示进行开通。

步骤 2 单击新建 > 新建空白应用。



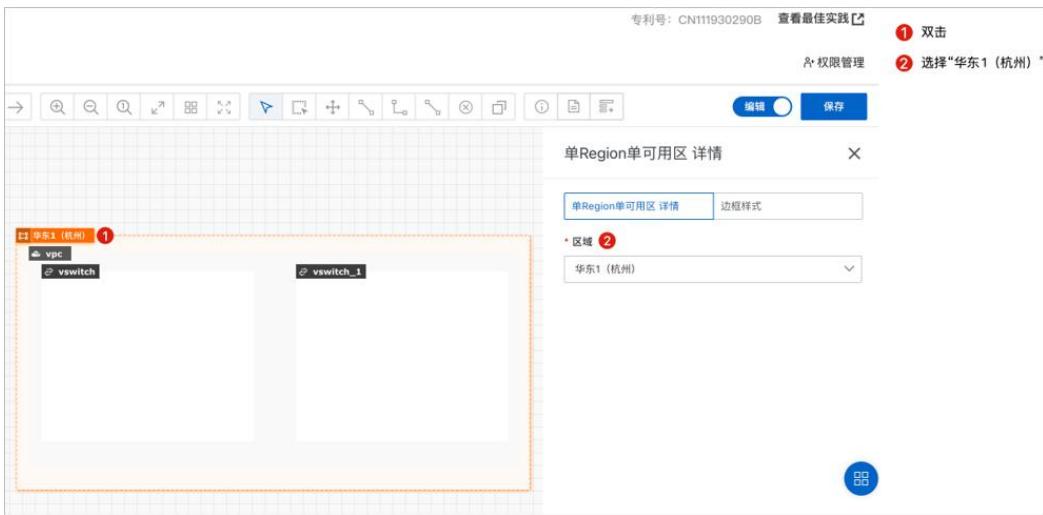
步骤3 从左侧**快速创建**下选择“单 Region 多可用区”模板到右侧画布区域。

由于应用型负载均衡 ALB 支持多可用区部署，为保障业务高可用，部署时需至少选择 2 个或以上可用区，所以在部署 ALB 前需要在该地域至少有两个不同可用区的 vswitch。



步骤4 分别双击 region、vpc、vswitch 进行设置

- 配置 region：



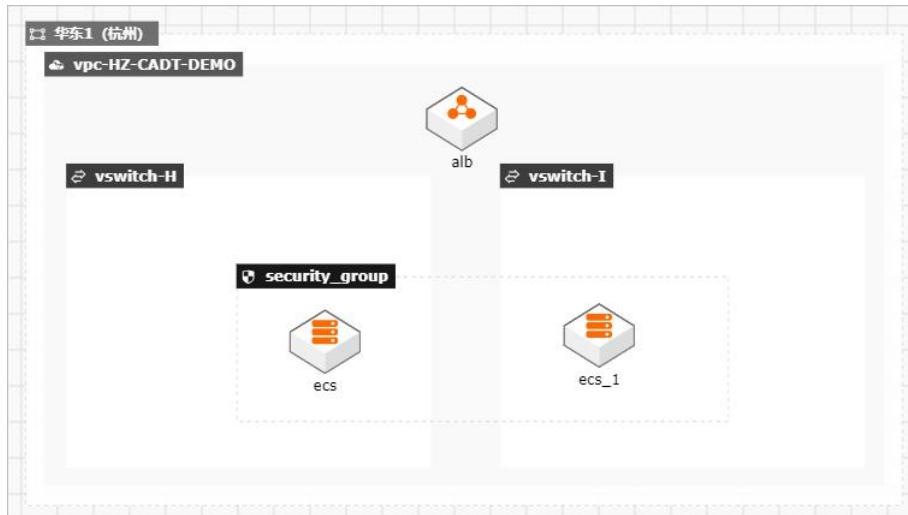
- 配置 vpc:



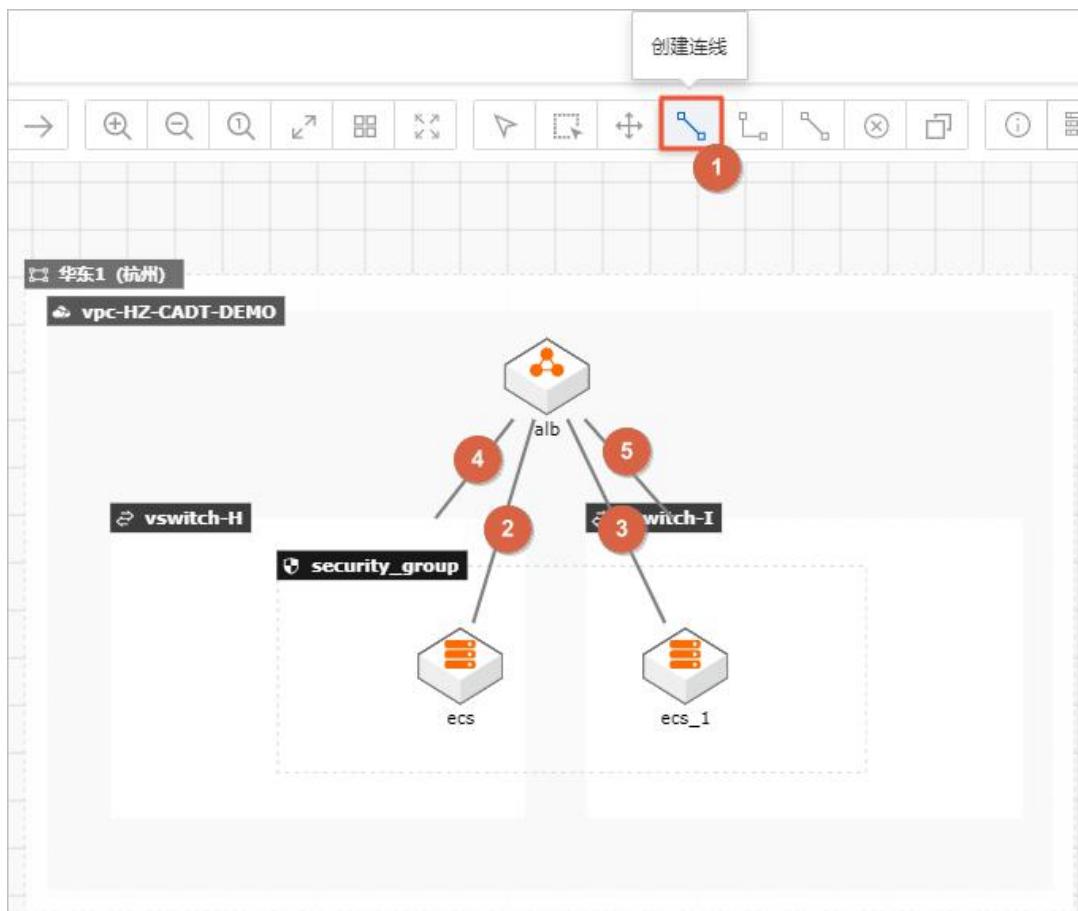
- 配置两个 vswitch, 一个可用区 H, 另一个可用区 I:



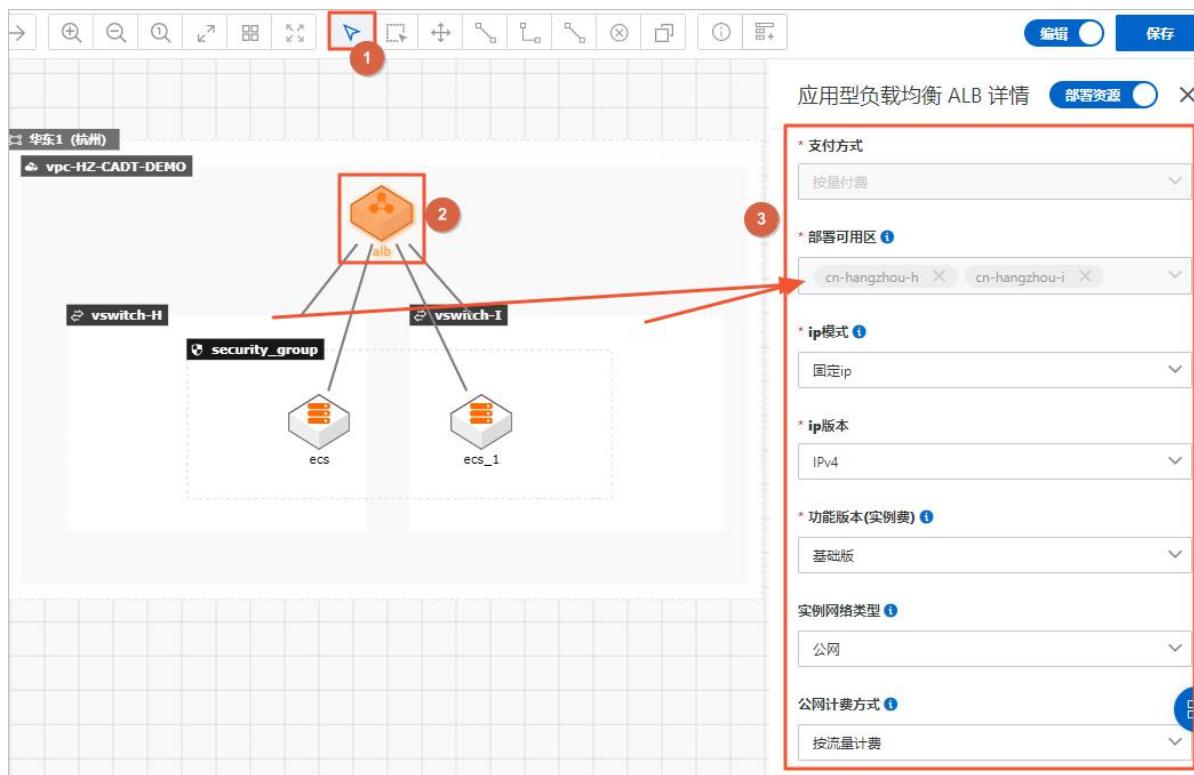
步骤5 在画布区域调整region、vpc、vswitch图层到合适大小后，分别从左侧产品列表中选择安全组、ECS、ALB拖入对应区域中（参考[理解资源级别](#)，根据架构资源级别设计）。



步骤6 单击**创建连线**按钮，将ALB与两台ECS、两台vswitch连接在一起。



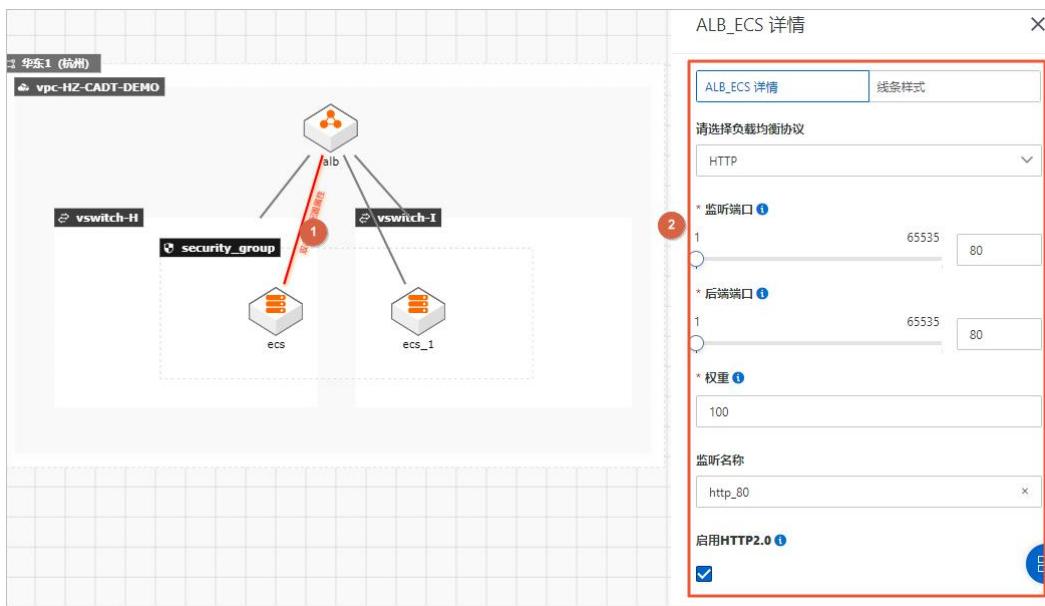
步骤 7 切换回**默认模式**，双击 ALB 进行配置，此时可以看到“部署可用区”已自动添加两个 switch 所在的可用区。



步骤 8 双击 ALB-ECS 之间的连线，配置监听信息。

配置项	配置明细
选择负载均衡协议	HTTP
监听端口	80
后端端口	80
权重	100
监听名称	自定义，例如 http_80
服务器组名称	自定义，例如 webserver
选择后端协议	HTTP
选择调度算法	加权轮询

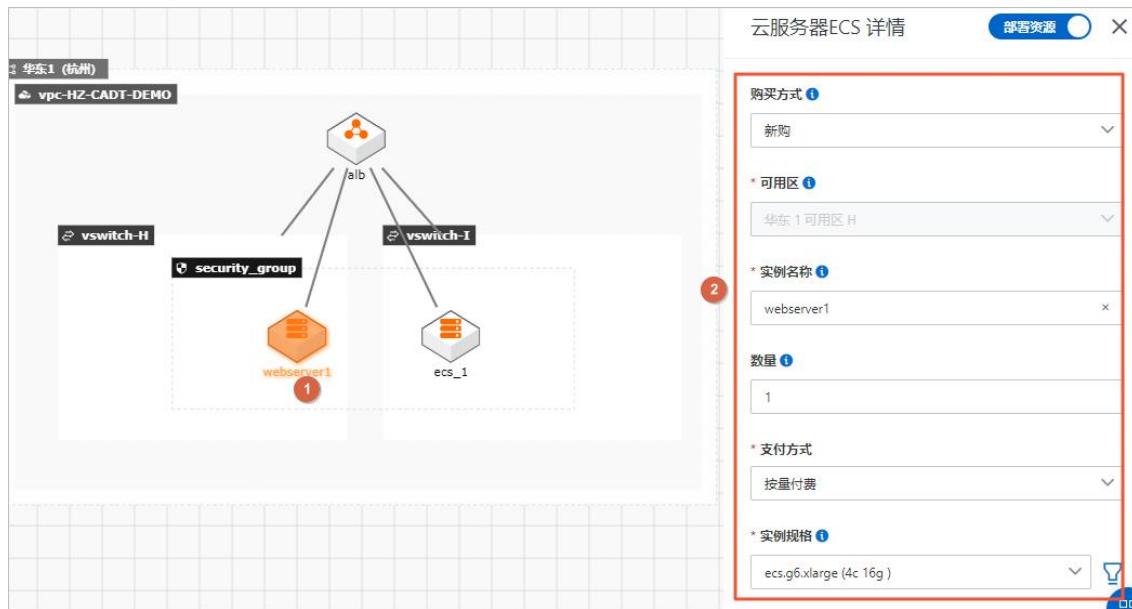
其他配置保持默认即可。



同样方法配置另一条 ALB-ECS 连线。

步骤 9 配置 ECS。

配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	webserver1
支付方式	按量付费
实例规格	ecs.g6.xlarge(4c 16g)
镜像	CentOS
镜像版本	CentOS 7.6 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
公网 IP	分配公网 IPv4 地址
宽带计费模式	按流量付费
带宽 (峰) 值	10 Mbps
主机名	webserver1
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>



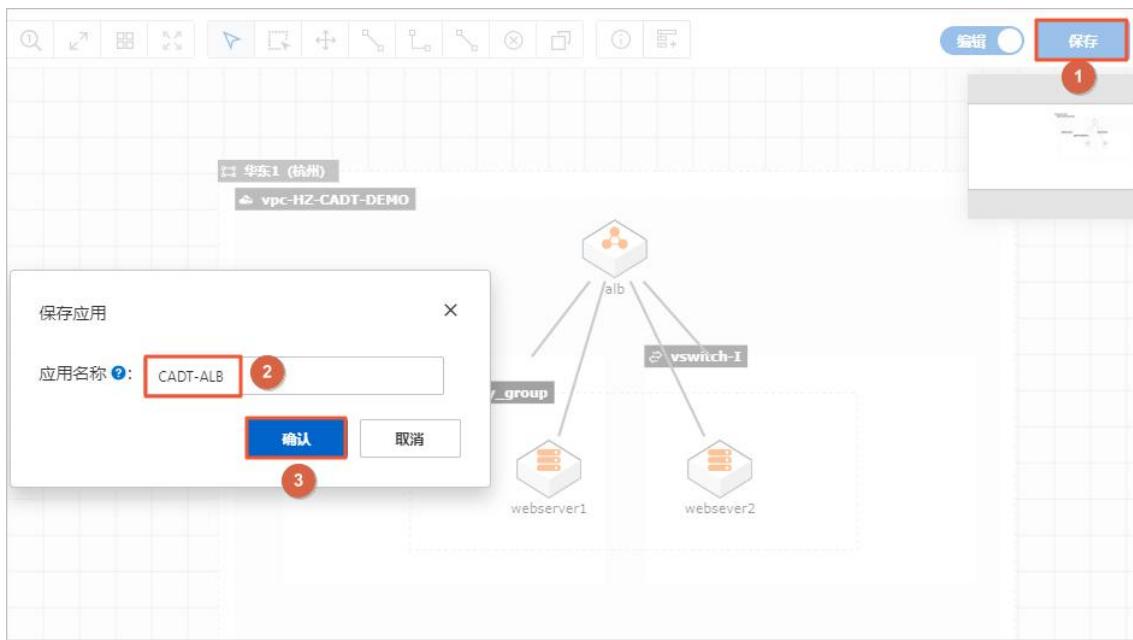
按照同样配置项配置另外一台 ECS，实例名称定为 webserver2。

为方便后续 ECS 上部署应用，将两台 ECS 开通公网 IP。（企业环境建议内网 ECS 通过 NAT 网关主动访问互联网，日常 SSH 登录通过堡垒机跳转。）

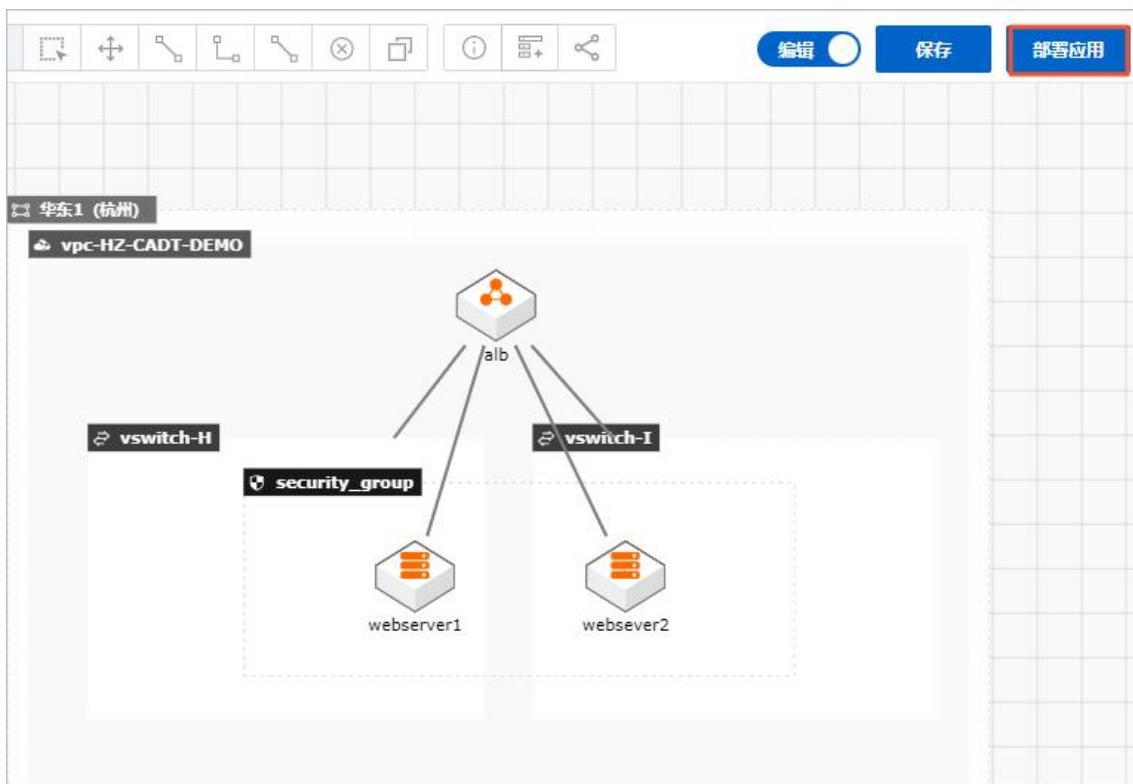
步骤 10 双击安全组，配置安全组策略，放行 22、80、443 端口。



步骤 11 配置完成后，单击右上角**保存**按钮，输入应用名称，单击**确认**。



步骤 12 保存完成后，单击**部署应用**。



步骤 13 等待资源验证成功，单击下一步：价格清单。

**资源验证**

资源名称	资源类型	区域	规格	结果	备注	操作
vswitch-l	vswitch	杭州	172.16.1.0/24	成功	校验通过	定位
vswitch-H	vswitch	杭州	172.16.0.0/24	成功	校验通过	定位
webserver1	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
webserver2	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
alb	alb	杭州	基础型	成功	校验通过	定位
vpc-HZ-CADT-DEMO	vpc	杭州	172.16.0.0/12	成功	校验通过	定位
security_group	security.group	杭州	normal	成功	校验通过	定位
弹性伸缩组	auto-scaling-group	华东	弹性伸缩组	弹性伸缩组	弹性伸缩组	弹性伸缩组

状态: **校验成功**

① **下一步: 价格清单** **返回**

步骤 14 计价成功后，单击下一步：确认订单。

**导出价格清单**

**免费** **按量付费**

**资源成本占比**

资源预算

- 计算 计算: 1.2 元/时
- 网络 网络: 0.8 元/时

**价格列表**

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
alb	alb	杭州	基础型	1	1.2元/时	0.0元/时	1.2元/时	定位
webserver2	ecs	杭州	ecs.g6.xlarge	1	1.2元/时	0.0元/时	1.2元/时	定位
webserver1	ecs	杭州	ecs.g6.xlarge	1	1.2元/时	0.0元/时	1.2元/时	定位

状态: **计价成功**

① **上一步: 资源校验** **查看报告** **下一步: 确认订单**

步骤 15 核对订单无误后，勾选《云速搭服务条款》，并单击下一步：支付并创建进行应用部署。

**确认订单**

免费	按量付费						
资源名称	资源类型	区域	规格	数量	原价	应付	状态
webserver1	ecs	杭州	ecs.g6.xlarge	1	1元/时	1元/时	新购
webserver2	ecs	杭州	ecs.g6.xlarge	1	1元/时	1元/时	新购
alb	alb	杭州	基础型	1	0.5元/时	0.5元/时	新购

《云速搭服务条款》①  
部署前，请阅读并勾选服务条款

**按量付费：0.1300元/时**

状态：**计价成功**

② [上一步：价格清单](#) [下一步：支付并创建](#)

步骤 16 部署成功后，单击**查看报告**，可以查看详细的应用部署报告。

**资源部署状态**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
vpc-HZ-CADT-DEMO	vpc	-	vpc- <a href="#">XXXXXXXXXX</a>	运行中	2021-10-22 11:21:53	定位
security_group_alb_demo	security.group	-	sg- <a href="#">XXXXXXXXXX</a>	运行中	2021-10-22 11:21:53	定位
vswitch-H	vswitch	-	vsw- <a href="#">XXXXXXXXXX</a>	运行中	2021-10-22 11:21:53	定位
vswitch-I	vswitch	-	vsw- <a href="#">XXXXXXXXXX</a>	运行中	2021-10-22 11:21:53	定位

**部署概要**

状态：部署成功  
方案编号：SBV2CXXXXX03B

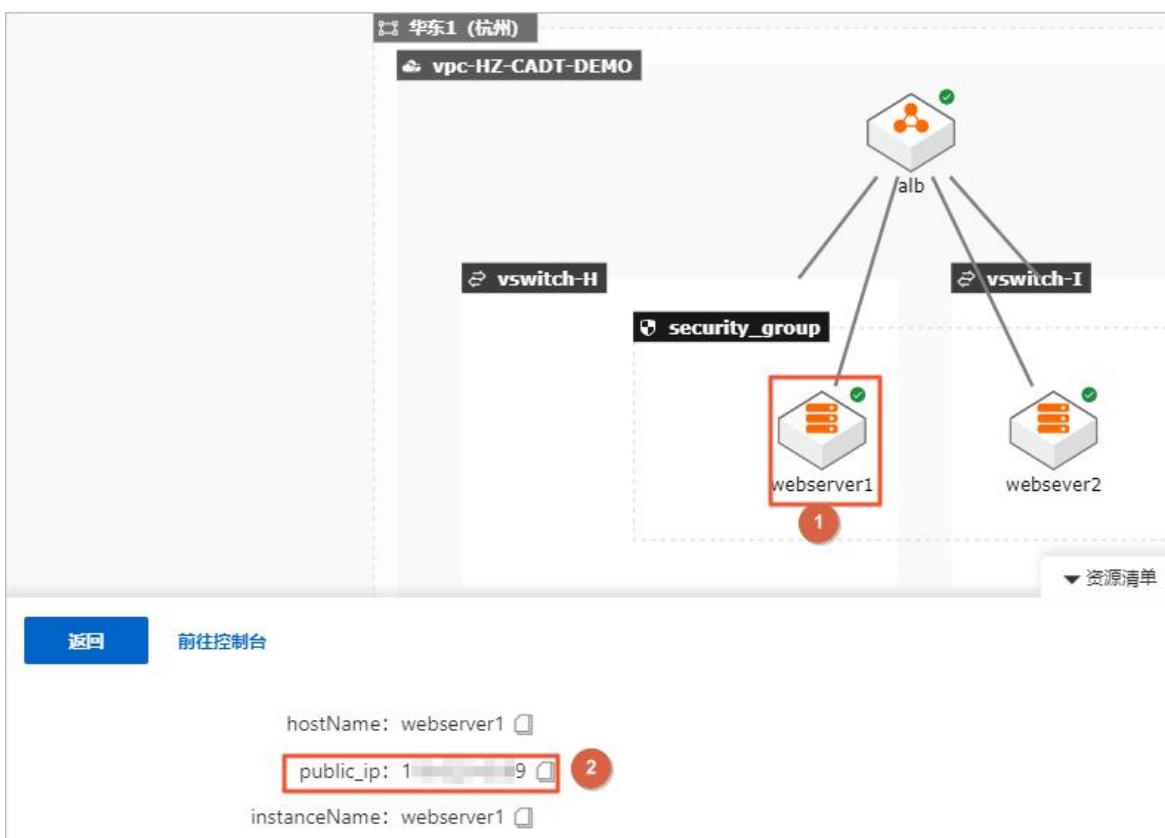
订单编号：2113751777781212233917726141

[可查看详细报告](#) [查看报告](#) [返回](#)

### 3.5.3.验证通过 ALB 转发到 ECS 实现负载分发

步骤 1 通过公网 IP 登录 ECS (webserver1)。

1. 双击 webserver1 这台 ECS 实例，复制该 ECS 的公网 IP。



2. SSH 登录到该 ECS，执行下面指令，安装 httpd 服务，并启动服务。

```
yum install -y httpd  
systemctl start httpd  
systemctl status httpd
```

3. 确认 httpd 正常启动

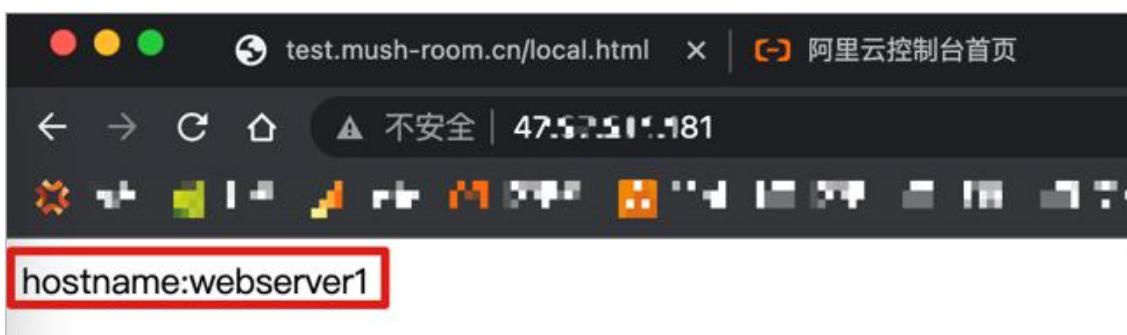
```
[root@webserver1 ~]# systemctl start httpd
[root@webserver1 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since 四 2021-10-21 16:52:24 CST; 5s ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Main PID: 2110 (httpd)
      Status: "Processing requests..."
     CGroup: /system.slice/httpd.service
             ├─2110 /usr/sbin/httpd -DFOREGROUND
             ├─2111 /usr/sbin/httpd -DFOREGROUND
             ├─2112 /usr/sbin/httpd -DFOREGROUND
             ├─2113 /usr/sbin/httpd -DFOREGROUND
             ├─2114 /usr/sbin/httpd -DFOREGROUND
             └─2115 /usr/sbin/httpd -DFOREGROUND

10月 21 16:52:24 webserver1 systemd[1]: Starting The Apache HTTP Server...
10月 21 16:52:24 webserver1 httpd[2110]: AH00558: httpd: Could not reliably determine...ge
10月 21 16:52:24 webserver1 systemd[1]: Started The Apache HTTP Server.
Hint: Some lines were ellipsized, use -l to show in full.
```

#### 4. 创建一个 html 文件：

```
cat <<EOF > /var/www/html/index.html
<html>
hostname: `hostname` 
</html>
EOF
cat /var/www/html/index.html
```

#### 5. 浏览器输入 http://<ECS public ipAddress>/，验证 ECS 上 http 服务正常。



#### 6. 另外一台 ECS 按照上述流程也配置完成 http 服务。

步骤 2 配置域名 CNAME 解析。

1. 本步骤前提为已申请域名且已通过备案，本例已申请并备案域名备用。双击 ALB，在下方详情页面找到并复制 cname 地址。

ALB configuration details:

```

cd31x0e","zoneId":"cn-hangzhou-i","loadBalancerAddress":16.62.71.239"}]} deletionProtectionConfig: enabled":false
dNSName: alb-[REDACTED].w.cn-hangzhou.alb.aliyuncs.com

```

2. 登录云解析 DNS 控制台 <https://dns.console.aliyun.com/>，单击目标域名的解析设置。

Cloud DNS Control Panel - Domain Parsing:

**操作**

- 域名解析 (1)
- PrivateZone
- 全局流量管理 (旧版)
- 全局流量管理
- IP地理位置库
- 辅助DNS
- 公共DNS
- 操作日志

**域名解析**

公告: .com/.net/.cn/.xin/.top/.xyz/.vip/.club/.shop/.wang/.ren等域名注册成功后必须进行域名实名认证,否则会造成解析不生效。实名认证审核通过后的1-2个工作日解析可恢复。

【金秋十月】云解析新用户限时活动: 新购、续费同享75折!

【0元试用】阿里云DNS全系列产品 新用户免费试用!

权威域名 缓存加速域名 请求量统计 版本套餐管理 更多服务

添加域名 批量自动续费 批量操作 全部域名 域名快速搜索

操作	付费版本	DNS服务器状态	记录数	标签	域名
正常	免费版	正常	363		mush-room.cn

请勿使用顶级域名做解析

**操作**

② 解析设置

3. 单击添加记录。

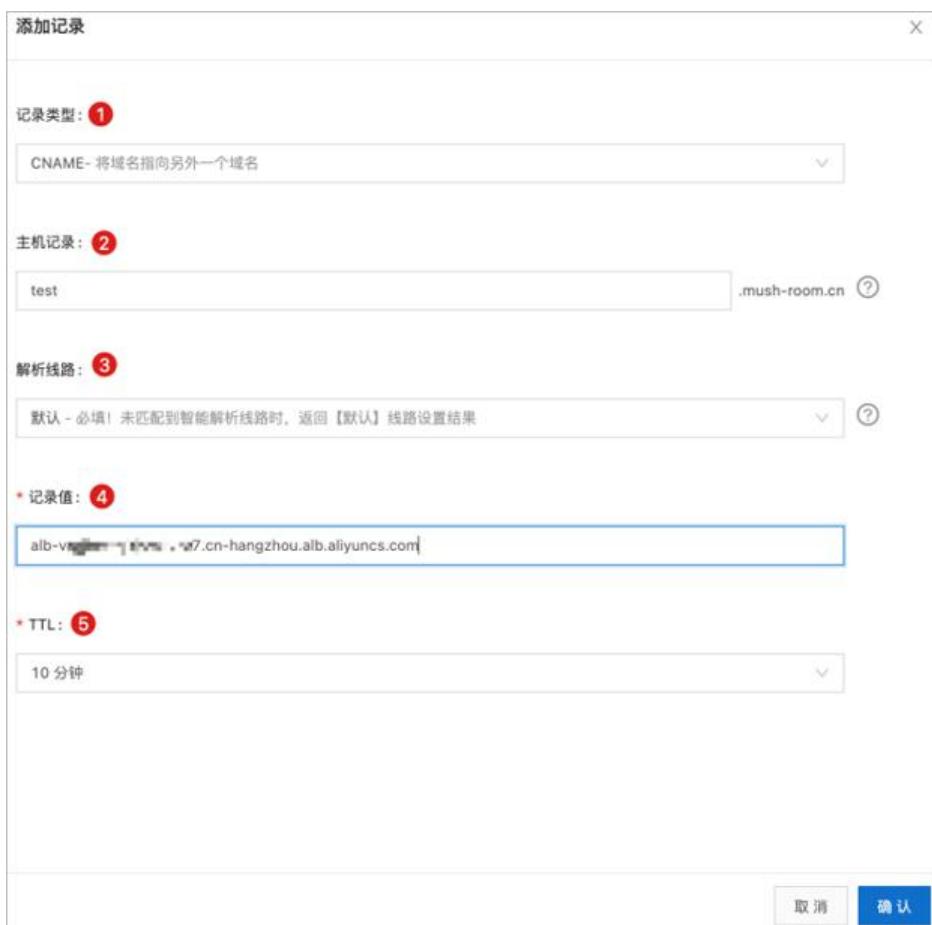
Cloud DNS / Domain Parsing / Configuration Settings

解析设置 mush-room.cn

当前分配的DNS服务器是: dns27.hichina.com, dns28.hichina.com

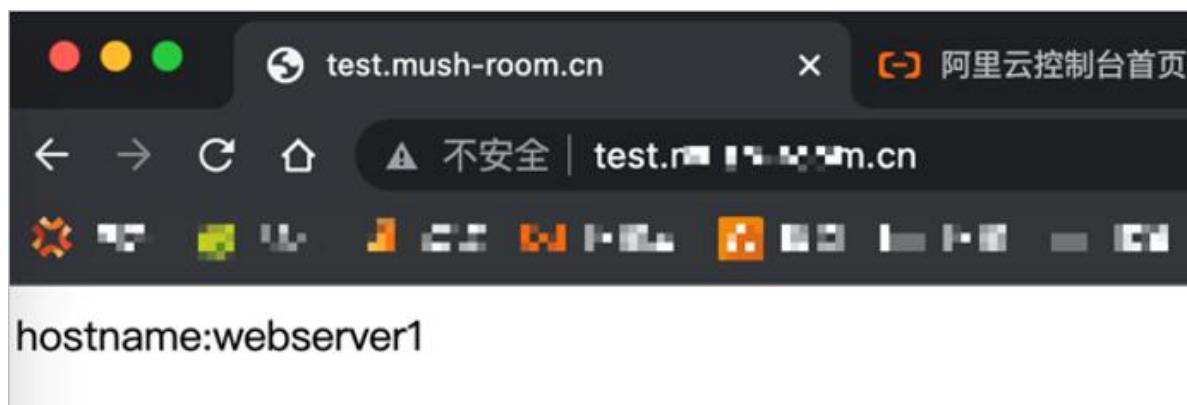
添加记录 导入/导出 请求量统计 新手引导

#### 4. 添加一条 CNAME 记录。



### 步骤 3 ALB 功能验证

域名 CNAME 解析配置完成后，等待解析生效（一般 10 分钟内），使用浏览器访问刚添加解析的域名。反复刷新页面可以看到在请求被负载到 webserver1 和 webserver2 上。



### 3.5.4.验证通过 ALB 转发到 CLB 实现负载分发

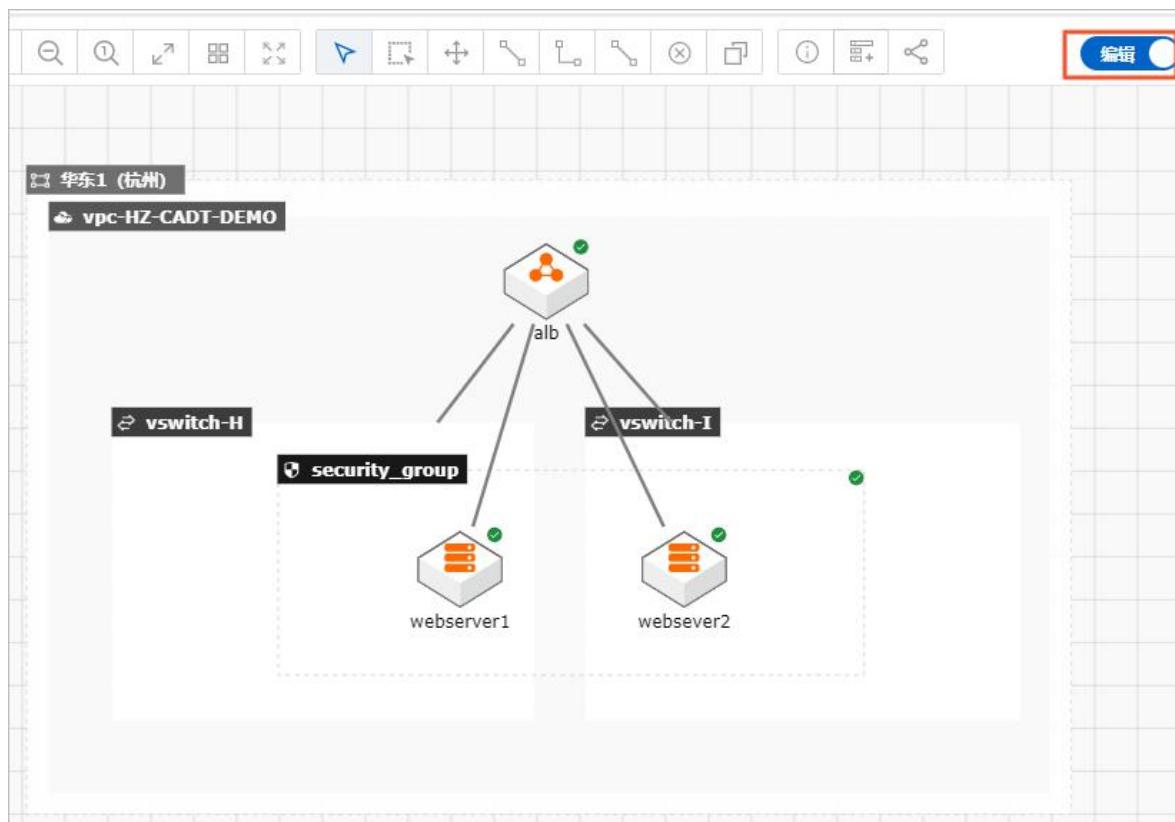
步骤 1 登录云速搭 CADT 控制台（<https://bpstudio.console.aliyun.com/>），单击应用 > 我的应用，进入我的应用页面。



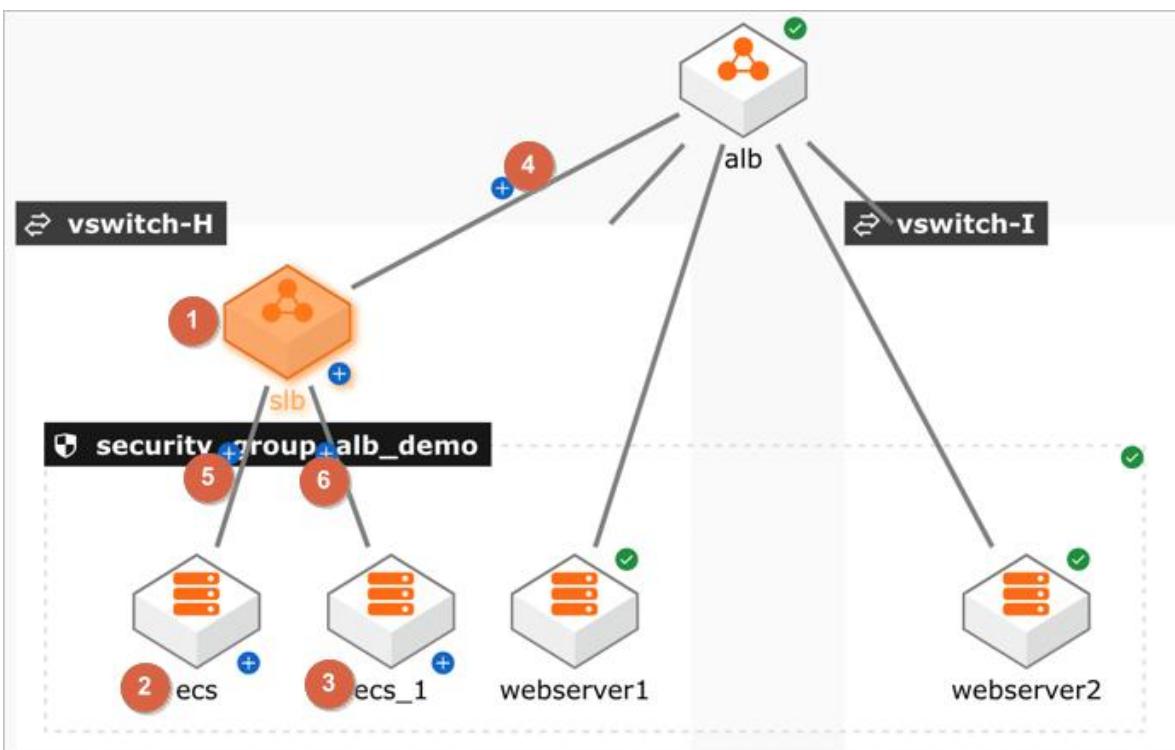
步骤 2 找到 DEMO 的应用架构图，单击编辑架构图。



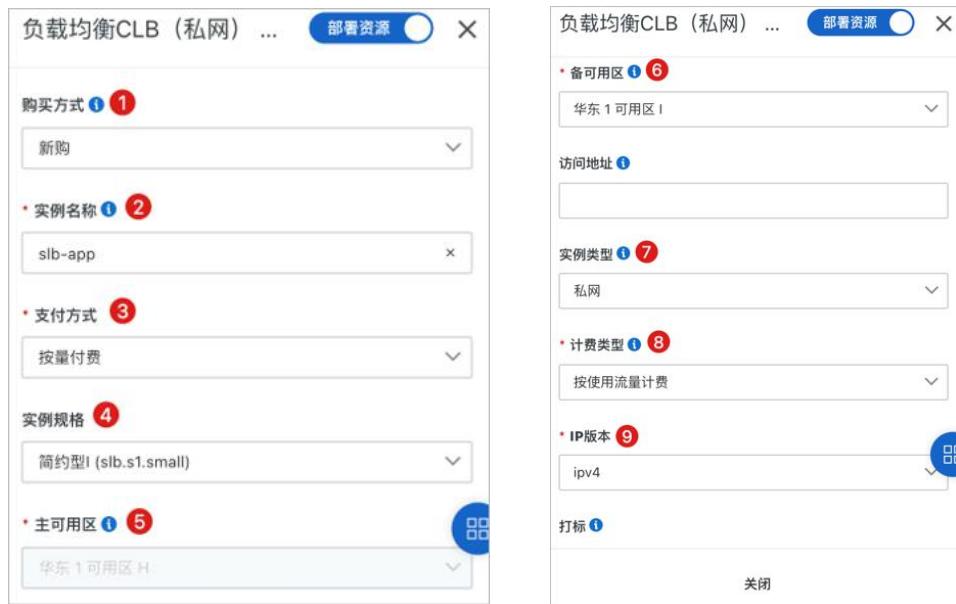
步骤 3 切换到编辑模式。



步骤 4 在 vswitch-H 中添加一个 CLB（私网）和两台 ECS，并通过连线将 CLB 与两台 ECS 相连。同时将 ALB 与 CLB 相连，然后保存。编辑后的架构如下图所示：



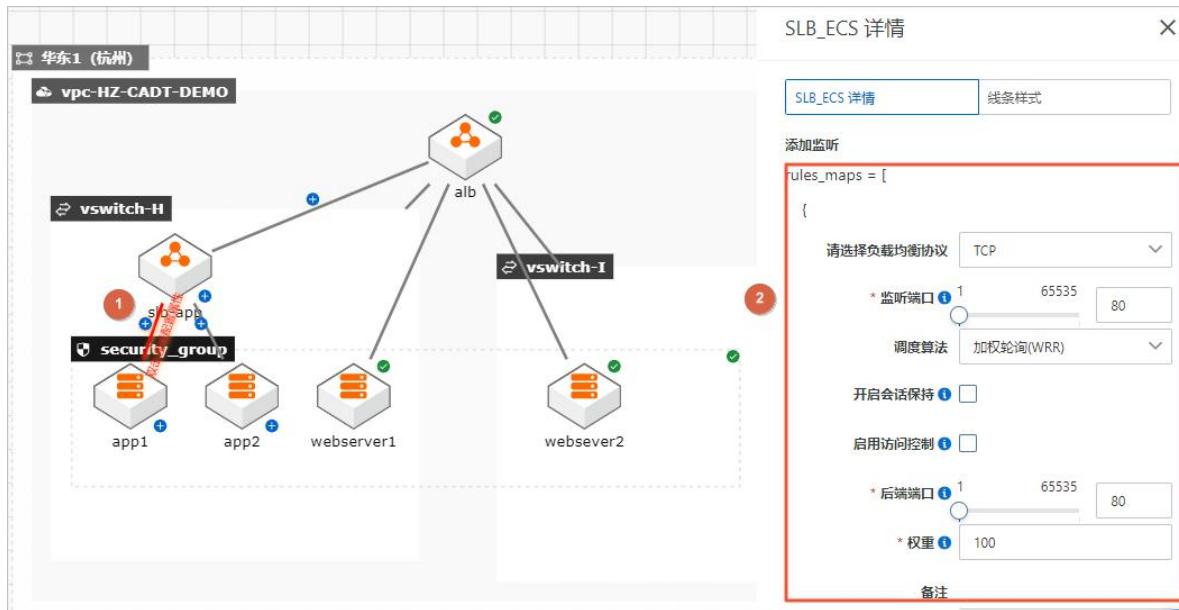
步骤 5 双击 CLB 进行配置：



步骤 6 双击 ECS 进行配置参考章节 2 步骤 8，实例名称分别设置为“app1”和“app2”。

配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	app1
支付方式	按量付费
实例规格	ecs.g6.xlarge(4c 16g)
镜像	CentOS
镜像版本	CentOS 7.6 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
公网 IP	分配公网 IPv4 地址
宽带计费模式	按流量付费
带宽（峰）值	10 Mbps
主机名	app1
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>

步骤 7 双击 CLB 和 ECS 之间的连线，进行监听配置。



同样方法配置完另一条连线。

步骤 8 配置完成后，单击**保存**，然后单击**部署应用**，开始进行部署。

资源验证完成后，单击**下一步：价格清单**。

资源名称	资源类型	区域	规格	结果	备注	操作
vswitch-l	vswitch	杭州	172.16.1.0/24	成功	校验通过	定位
vswitch-H	vswitch	杭州	172.16.0.0/24	成功	校验通过	定位
webserver2	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
webserver1	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
alb	alb	杭州	基础型	成功	校验通过	定位
vpc-HZ-CADT-DEMO	vpc	杭州	172.16.0.0/12	成功	校验通过	定位
security_group	security.group	杭州	normal	成功	校验通过	定位

状态: 资源验证成功(架构调整)

**下一步：价格清单** **返回**

**导出价格清单**

免费 按量付费

资源成本占比

资源预算

- 计算 计算: [redacted] 元/时
- 网络 网络: [redacted] 元/时

价格列表

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
slb-app	clb	杭州	slb.s1.small	1	0.10元/时	省 [redacted] 元/时	[redacted] 元/时	定位
app2	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	省 [redacted] 元/时	[redacted] 元/时	定位
app1	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	省 [redacted] 元/时	[redacted] 元/时	定位
alb	alb	杭州	基础型	1	0.05元/时	省 [redacted] 元/时	[redacted] 元/时	定位

状态: **询价成功(架构调整)**

上一步: 资源校验 查看报告 **下一步: 确认订单**

**确认订单**

免费 按量付费

资源名称	资源类型	区域	规格	数量	原价	实付	状态
webserver1	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	[redacted]	已保有产品
webserver2	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	[redacted]	已保有产品
alb	alb	杭州	基础型	1	0.05元/时	[redacted]	已保有产品
app2	ecs	杭州	ecs.g6.large	1	0.42元/时	[redacted]	新购
app1	ecs	杭州	ecs.g6.large	1	0.42元/时	[redacted]	新购
slb-app	clb	杭州	slb.s1.small	1	0.10元/时	[redacted]	新购

《云速搭服务条款》

部署前, 请阅读并勾选服务条款

按量付费: **1.56元/时**

状态: **询价成功(架构调整)**

查看新购资源配置 上一步: 价格清单 **下一步: 支付并创建**

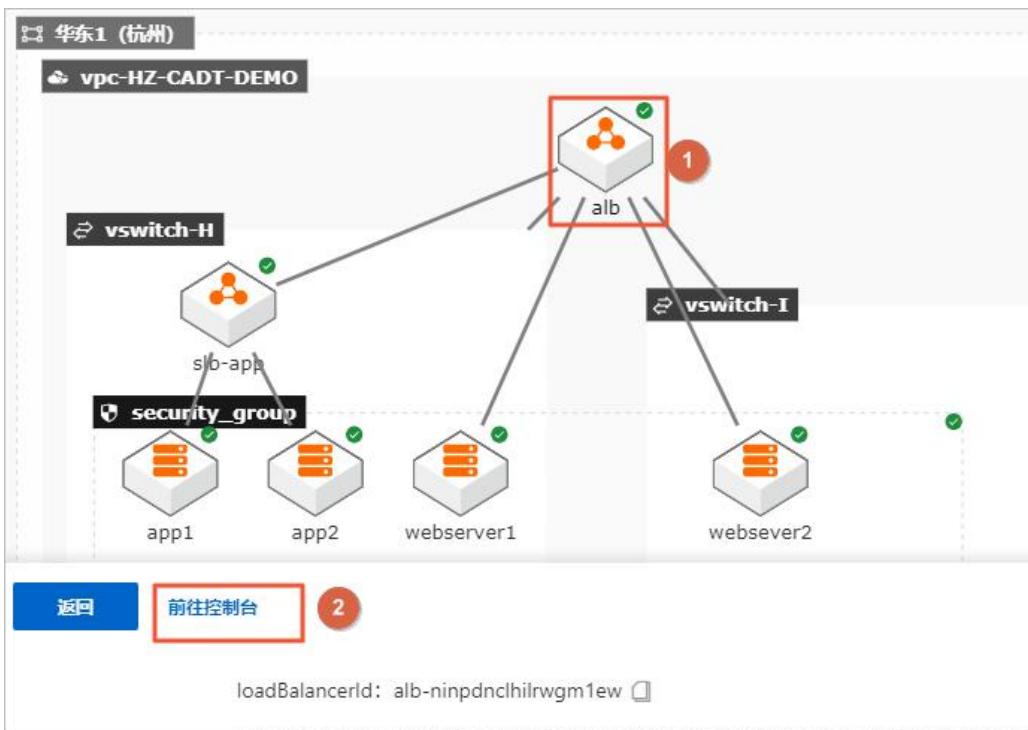
**说明:** 架构调整后, 再次部署, 只会针对新增或删除的实例进行操作。

步骤 9 部署完成后，在新添加的 app1 和 app2 两台 ECS 上执行以下指令：

```
yum install -y httpd  
systemctl start httpd  
systemctl status httpd  
  
mkdir /var/www/html/app  
touch /var/www/html/index.html  
cat <<EOF > /var/www/html/app/index.html  
<html>  
This is an app within CLB.<br/>  
hostname: `hostname`  
</html>  
EOF  
  
cat /var/www/html/app/index.html
```

步骤 10 ALB 添加服务器组

1. CADT 架构图双击 ALB，前往控制台。



2. 在左侧导航栏选择**服务器组**，创建服务器组。

The screenshot shows the Alibaba Cloud SLB console. On the left sidebar, '服务器组' (Server Groups) is selected, indicated by a red box and a red number '1'. The main content area is titled '服务器组' (Server Groups). A large red box highlights the '创建服务器组' (Create Server Group) button, which is step 2 in the process. Below it, there is a search bar labeled '请输入服务器组名称进行查询' (Enter server group name for search) and a dropdown menu labeled '服务器组名称' (Server Group Name). A table lists existing server groups: 'webserver' (VPC, HTTP), 'sgp-21...' (VPC, HTTP), and 'sgp-31...' (VPC, HTTP).

服务器组名称/ID	VPC	后端协议
webserver	vpc-	HTTP
sgp-21...	b...	HTTP
sgp-31...	b...	HTTP

\* 服务器组类型 ①

IP类型

\* 服务器组名称 ②

CLB-app

\* VPC ③

vpc-HZ-CADT-DEMO | vpc-bp1i4pp4ecvrezpt80ntv

选择后端协议 ④

HTTP

选择调度算法 ⑤

加权轮询

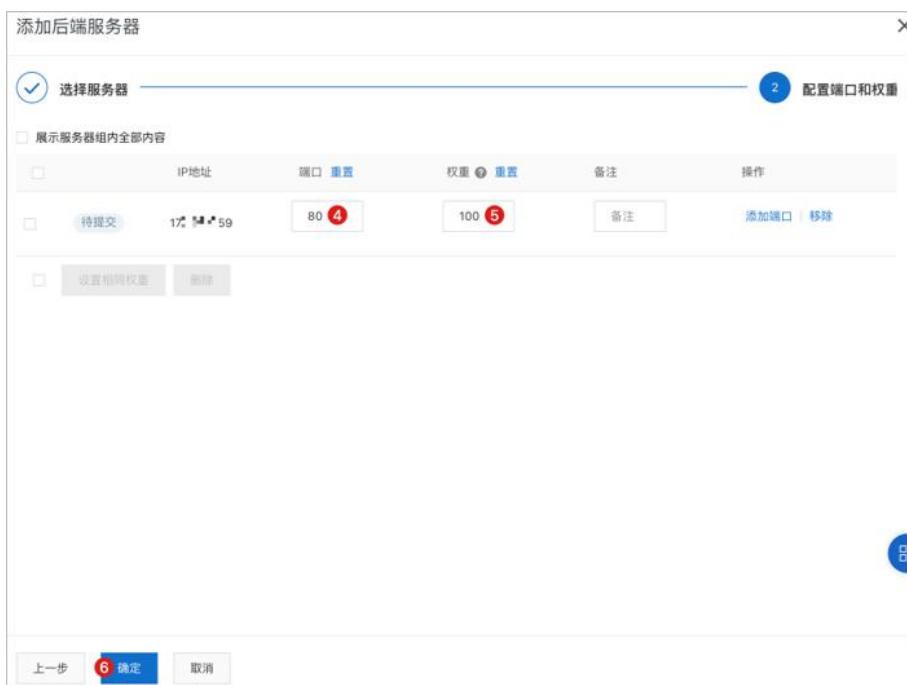
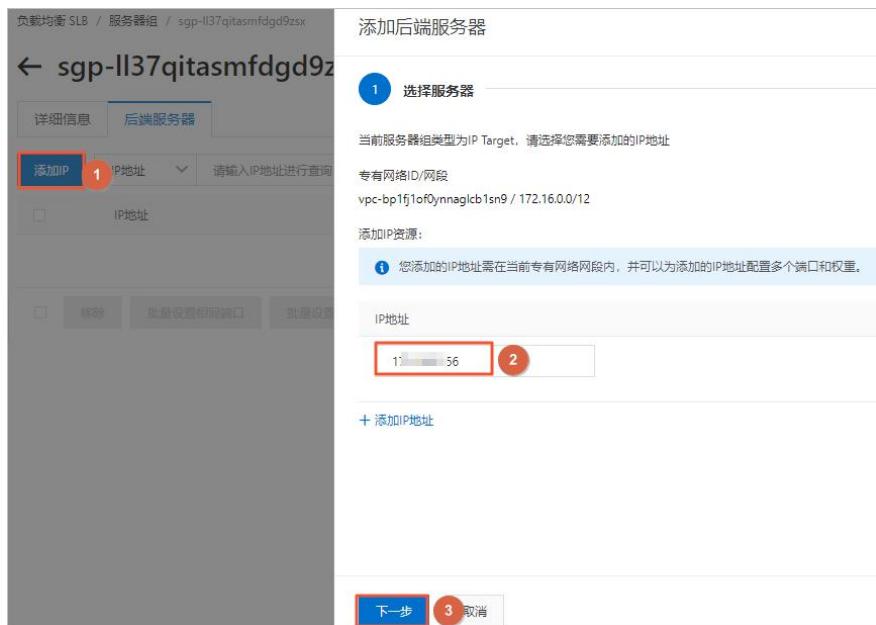
\* 选择资源组 ⑥

default resource group

开启会话保持

创建 取消

3. 然后添加后端服务器，单击添加 IP，输入 CLB 的私网 IP 地址（可在 CADT 架构图双击 CLB 在下方详情获取）。



步骤 11 ALB 配置转发规则。

1. 实例里找到对应的 ALB 实例，单击实例 ID 进入详情页。

实例名称/实例ID	DNS 名称	运行状态	网络类型
alb-rnit3ao74qdyi3gur6	alb-rnit3ao74qdyi3gur6.cn-hangzhou-1a.com	运行中	公网

2. 打开监听页面，单击监听器的查看/编辑转发规则。

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-lbq6zmkn41nyhc	HTTP:80	运行中	正常	未开启	启用	转发至 webserver	<a href="#">查看详情</a>   <a href="#">查看/编辑转发规则</a>

3. 新增两条转发规则如下，将路径 “/” 转发到 webserver1 和 webserver2，将路径 “/app” 转发到 CLB。

如果 (条件全部匹配)	那么
路径 是 /	转发至 服务器类型 sgp-edn3lbq6zmkn41nyhc   webserver
+ 添加路径 + 添加转发条件	+ 添加动作

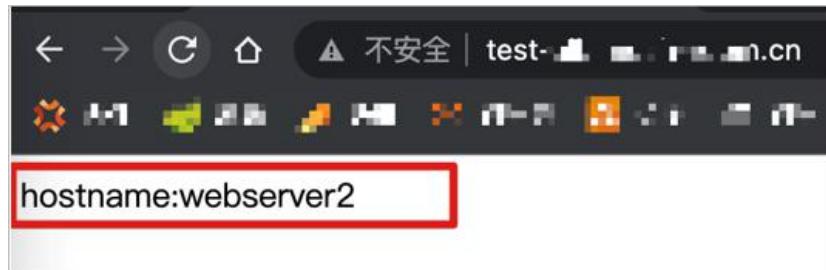
如果 (条件全部匹配)	那么
路径 是 /app/	转发至 IP类型 sgp-li37qitasmf9g9zsx   CLB-app
+ 添加路径 + 添加转发条件	+ 添加动作

[继续插入规则](#)

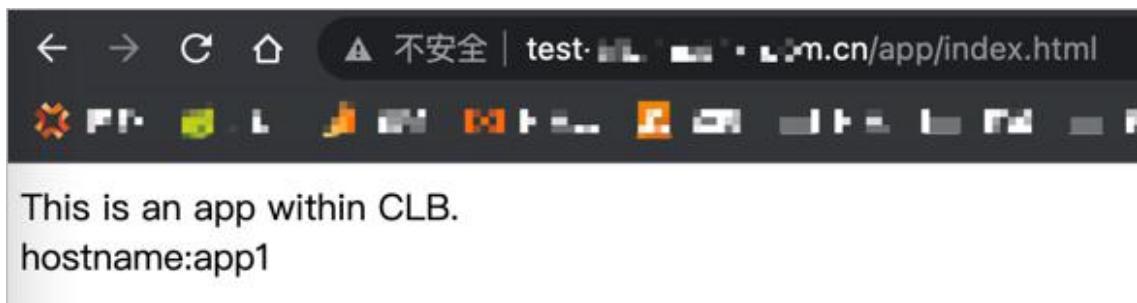
[确定](#) [取消](#)

步骤 12 验证转发效果

- 在浏览器输入 <http://<测试域名>/>，反复刷新可以发现请求在 webserver1 和 webserver2 上轮询。



- 在浏览器输入 <http://<测试域名>/app/index.html>，反复刷新可以发现请求在 app1 和 app2 上轮询。



### 3.5.5. 验证通过 ALB 转发到 ACK 集群实现负载分发

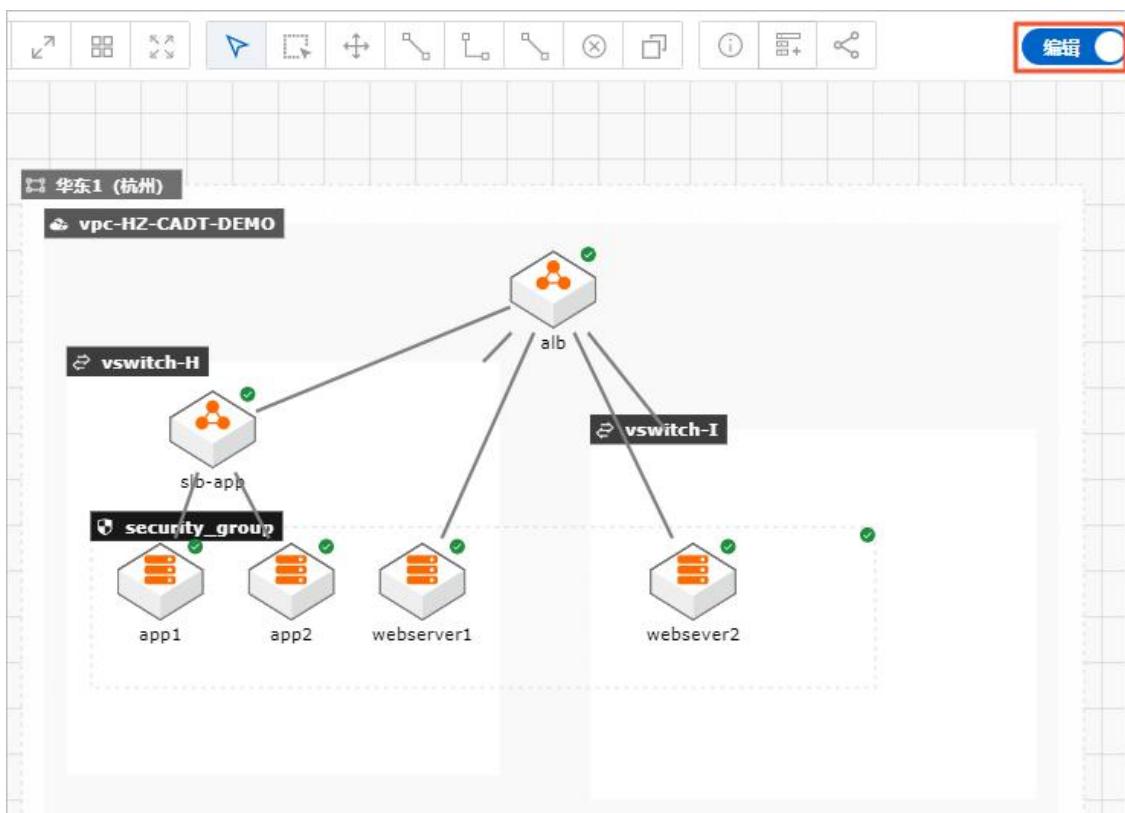
步骤 1 登录云速搭 CADT 控制台（<https://bpstudio.console.aliyun.com/>），单击**应用 > 我的应用**，进入我的应用页面。



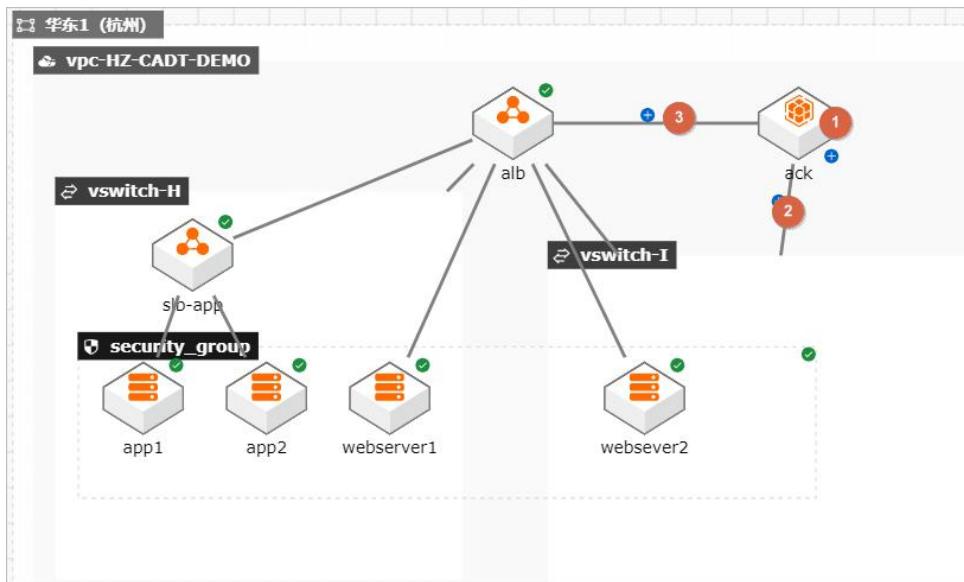
找到 DEMO 的应用架构图，单击**编辑架构图**。



步骤 2 切换到**编辑模式**。



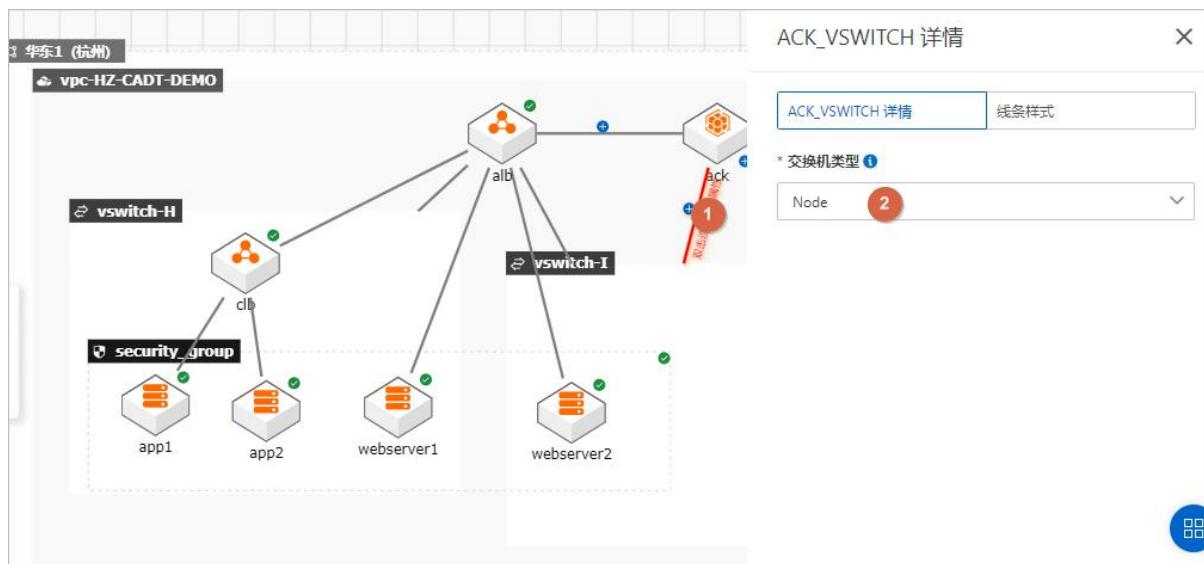
步骤 3 从左侧的云产品列表中搜索**ACK 托管版**，拖入架构图画布中，并使用连线的方式将 ACK 连接到 vswitch-I（以此选择 ACK worker 节点部署的可用区）；然后再用连线将 ALB 与 ACK 连接起来。



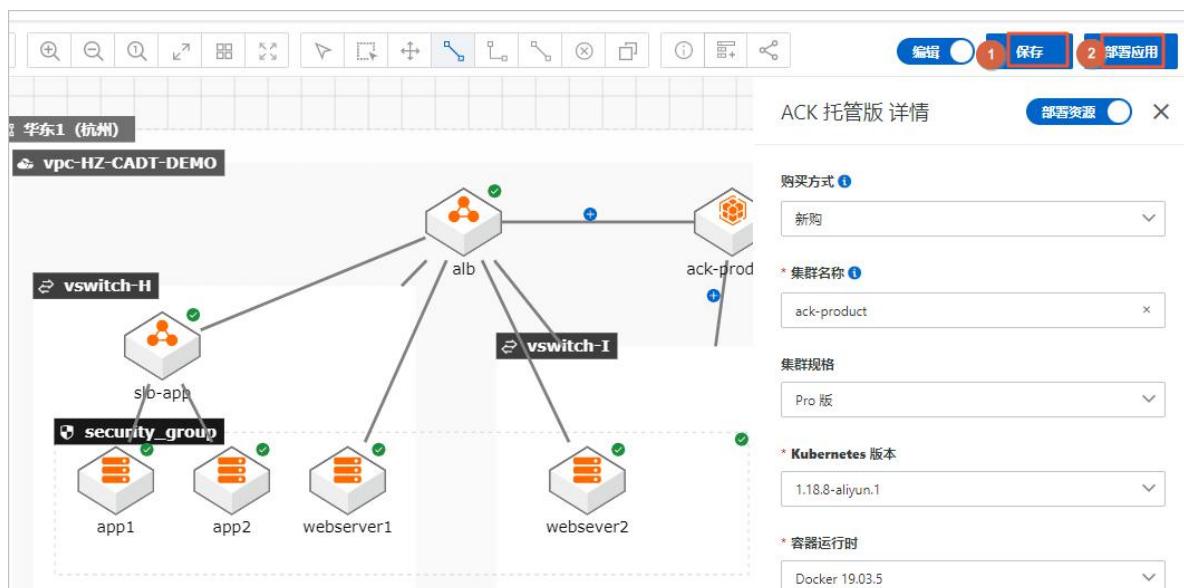
#### 步骤 4 ACK 配置

配置项	配置明细
集群名称	ack-product
集群规格	Pro 版
Kubernetes 版本	1.18.8-aliyun.1
容器运行时	Docker 19.03.5
Worker 部署可用区	cn-hangzhou-i
网络插件	Flannel
Pod 网络 CIDR	192.168.0.0/17
Service CIDR	192.168.128.0/17
节点 IP 数量	32
Worker 付费类型	按量付费
Worker 实例规格	ecs.g6.xlarge(4c 16g)
Worker 数量	2
Worker 系统盘类型	cloud_essd
性能级别	PL0
worker 系统盘大小	120
woker 操作系统	Alibaba Cloud Linux
woker 登录方式	设置密码
登录密码	<输入自定义密码>

步骤 5 双击 ACK 和交换机之间的连线，选择交换机类型。



步骤 6 配置完成后，先进行**保存**，然后单击**部署应用**。



步骤 7 按界面提示操作，直到支付创建资源。

### 资源验证

资源名称	资源类型	区域	规格	结果	备注	操作
webserver1	ecs	华东	ecs.g6.xlarge	成功	校验通过	定位
webserver1	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
alb	alb	杭州	基础型	成功	校验通过	定位
vpc-HZ-CADT-DEMO	vpc	杭州	172.16.0.0/12	成功	校验通过	定位
security_group	security.group	杭州	normal	成功	校验通过	定位
app2	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
app1	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
slb-app	clb	杭州	slb.s1.small	成功	校验通过	定位

状态: 资源验证成功(架构调整)

[下一步: 价格清单](#) [返回](#)

### 导出价格清单

[免费](#) [按量付费](#)

#### 资源成本占比

资源预算

- 计算 计算: 50元/时
- 网络 网络: 50元/时

#### 价格列表

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
ack-product	ack	杭州	ecs.g6.xlarge	2	2.50元/时	省 50元/时	2.00元/时	定位
slb-app	clb	杭州	slb.s1.small	1	0.10元/时	省 0元/时	0.10元/时	定位
app2	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	省 0元/时	1.04元/时	定位
app1	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	省 0元/时	1.04元/时	定位

状态: 询价成功(架构调整)

[上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

**确认订单**

资源名称	资源类型	区域	规格	数量	原价	应付	状态
webserver1	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	元/时	已保有产品
webserver2	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	元/时	已保有产品
alb	alb	杭州	基础型	1	0.05元/时	元/时	已保有产品
slb-app	clb	杭州	slb.s1.small	1	0.10元/时	元/时	已保有产品
app1	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	元/时	已保有产品
app2	ecs	杭州	ecs.g6.xlarge	1	1.04元/时	元/时	已保有产品
ack-product	ack	杭州	ecs.g6.xlarge	2	2.50元/时	元/时	新购

《云速搭服务条款》  
部署前, 请阅读并勾选服务条款  
**1**

按量付费: **元/时**  
**2**

状态: **询价成功(架构调整)**

[查看新购资源配置](#) [上一步: 价格清单](#) [下一步: 支付并创建](#)

步骤 8 部署完成后, 双击 ACK 资源名称, 跳转到控制台。

**资源部署状态**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
webserver1	ecs	按量付费	i-bp12qqpsd4bxp896kr5m	运行中	2021-10-28 14:42:55	<a href="#">定位</a>
clb	clb	按量付费	lb-bp1tfk5l55x9i7rhpcy0l	运行中	2021-10-28 15:25:20	<a href="#">定位</a>
app1	ecs	按量付费	i-bp1hex2e9zt154sn4ajf	运行中	2021-10-28 15:26:01	<a href="#">定位</a>
app2	ecs	按量付费	i-bp1hmr9w2y2o75mxvhcy	运行中	2021-10-28 15:26:01	<a href="#">定位</a>
ack-product	ack	-	ca7aaa1def4cd426d997ffa9f375cdb1e	运行中	2021-10-28 16:24:31	<a href="#">定位</a>

**部署概要**

状态: 部署成功  
订单编号: 211319570670833, 211320229530833  
方案编号: NYX447TYTUZ7YUSC

[查看报告](#) [返回](#)

步骤 9 ACK 创建一个简单的 http 应用

1. 单击集群名称, 进入新创建的 ACK 集群。

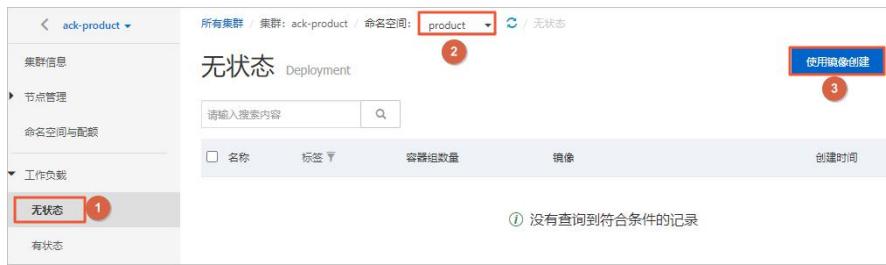
The screenshot shows the 'Container Service - Kubernetes' interface. In the top left, it says '容器服务 - Kubernetes'. The top right says '容器服务 ACK / 集群'. On the left, there's a sidebar with '概览', '集群' (selected), '授权管理', and a '市场' section with '容器镜像服务' and '编排模板'. Under '编排模板', the 'ack-product' cluster is listed. The main area is titled '集群列表' and shows a message: '云原生AI套件已开启全面公测, 移步了解详情'. Below is a table with columns: '集群名称/ID', '标签', '集群类型', '地域', '集群状态', and '节点数'. The 'ack-product' row is selected and highlighted with a red box.

2. 创建命名空间“product”。

This screenshot shows the 'Create Namespace' dialog box. On the left, the sidebar has 'Namespace and Quotas' selected (marked with a red box). The main area has a 'Namespace' tab selected. It shows a table with 'Name' and 'Label' columns. A new row is being created with 'product' in the 'Name' field (marked with a red box and number 3). Below the table is a 'Labels' section with 'Variable Name', 'Variable Value', and 'Operation' buttons. At the bottom are 'Confirm' and 'Cancel' buttons (marked with a red box and number 4).

This screenshot shows the 'Create Namespace' dialog box again. The 'Name' field contains 'product' (marked with a red box and number 1). Below it is a note: 'Length is 1 ~ 63 characters, only numbers, lowercase letters and underscores (-), and the first and last characters must be letters or numbers'. The 'Labels' section is identical to the previous screenshot. At the bottom are 'Confirm' and 'Cancel' buttons (marked with a red box and number 2).

3. 在 product 命名空间下创建无状态工作负载。



4. 应用名称“http-product”，单击下一步。

应用名称	http-product
副本数量	2
类型	无状态 (Deployment)
标签	<a href="#">添加</a>
注解	<a href="#">添加</a>
时区同步	<input type="checkbox"/> 容器与节点使用相同时区
<a href="#">返回</a> <a href="#" style="background-color: #0072bc; color: white; border: 1px solid #0072bc; padding: 5px;">下一步</a>	

5. 选择镜像，切换到 Docker 官方镜像，搜索选中 httpd，镜像 tag 选择“2.4.50”。

容器1	<a href="#">添加容器</a>		
镜像名称:	httpd	<a href="#">选择镜像</a> (1)	
镜像Tag:	2.4.50	<a href="#">选择镜像Tag</a> (2)	
<input type="button" value="优先使用本地镜像(IfNotPresent)"/> (3)			
<a href="#">设置镜像密钥</a>			
资源限制:	CPU 如: 0.5	Core 内存 如: 128 MiB	Ephemeral-Storage 如: 2 GiB
<small>建议根据实际使用情况设置, 防止由于资源约束而无法调度或引发内存不足 (OOM) 错误</small>			
所需资源:	CPU 0.25	Core 内存 512 MiB	Ephemeral-Storage 2 GiB
<small>建议根据实际使用情况设置, 防止因资源不足导致应用不可用</small>			
容器启动项:	<input type="checkbox"/> stdIn <input type="checkbox"/> tty		
特权容器:	<input checked="" type="radio"/> <input type="radio"/>		
Init Container:	<input type="checkbox"/>		
<b>端口</b> <a href="#">新增</a>			
名称	容器端口	协议	
http	80		(4)
<a href="#">上一步</a> <a href="#" style="background-color: #0072bc; color: white; border: 1px solid #0072bc; padding: 5px;">下一步</a>			



## 6. 创建服务 (Service)



**创建服务**

名称:	http-product-svc ①								
命名空间:	product								
类型:	负载均衡 ② 私网访问 ③ 新建SLB ④ 简约型I (slb.s1.small) ⑤ 修改 ⑥ 请根据业务选择SLB规格, SLB计费详情请参考产品定价: 自动新建的SLB在Service删除时会被删除。								
外部流量策略:	Cluster ⑤								
端口映射:	● 添加 ⑥ <table border="1"> <tr> <th>名称 ①</th> <th>服务端口</th> <th>容器端口</th> <th>协议</th> </tr> <tr> <td>http</td> <td>80</td> <td>80</td> <td>TCP ⑦</td> </tr> </table>	名称 ①	服务端口	容器端口	协议	http	80	80	TCP ⑦
名称 ①	服务端口	容器端口	协议						
http	80	80	TCP ⑦						
注解:	● 添加								
标签:	● 添加								
⑦ 创建 取消									

服务端口	容器端口	协议
80	80	TCP

路由 (Ingress) [创建](#)

指标伸缩  开启

定时伸缩  开启

升级方式  开启

节点亲和性 [添加](#) ⚪ 亲和与反亲和性

应用亲和性 [添加](#)

应用反亲和性 [添加](#)

调度容忍 [添加](#)

Pod标签 [添加](#)

Pod注解 [添加](#)

上一步 [创建](#)

7. 查看应用确认，pod 启动正常。

步骤 10 添加一个 CNAME 解析记录。

参考章节 3 步骤 2，解析记录主机名 product-lab，CNAME 填写 ALB 的 cname 地址。

记录类型: ①  
CNAME- 将域名指向另外一个域名

主机记录: ②  
product-alb .mush-room.cn ③

解析线路: ③  
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 ④

\* 记录值: ④  
alb-...7.cn-hangzhou.alb.aliyuncs.com

\* TTL: ⑤  
10 分钟

取消 确认

步骤 11 ALB 添加服务器组

1. 进入 ALB 控制台，服务器组 > 创建服务器组。

负载均衡 SLB		负载均衡 SLB / 服务器组		
极宽		服务器组		
应用型负载均衡 ALB		② 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
实例		<input type="checkbox"/>	服务器组名称/ID	VPC
服务器组 ①		<input type="checkbox"/>	clb-app sgp-0...5	vpc-b...67
健康检查		<input type="checkbox"/>	webserver sgp-c...mz	vpc-l...67
访问控制				HTTP

创建服务器组

\* 服务器组类型 ① IP类型

\* 服务器组名称 ② product-ack

\* VPC ③ vpc-HZ-CADT-DEMO | vpc-l...p67

选择后端协议 ④ HTTP

选择调度算法 ⑤ 加权轮询

\* 选择资源组 ⑥ default resource group

开启会话保持

配置健康检查

开启健康检查

高级配置 [修改](#)

健康检查协议	HTTP	健康检查方法	HEAD
健康检查协议版本	HTTP1.1	健康检查端口	后端服务器端口
健康检查路径	/	健康检查域名	后端服务器内网IP
健康状态返回码	http_2xx	响应超时时间	5 秒
间隔时间	3 秒	健康阈值	2 次
不健康阈值	3 次		

[创建](#) [取消](#)

2. 创建后添加后端服务器，单击“添加 IP”。



3. 此处 IP 填写 ACK 中刚才创建的服务所挂载 LB 的 IP

名称	标签	类型	创建时间	集群 IP	内部端点	外部端点
http-product-svc	service.beta.kubernetes.io/hash:6f6a60493bb9460bf5038c240a3452b101ecf2ac111812591d29d905	LoadBalancer	2021-10-28 16:48:48	192.168.147.211	http-product-svc:80 TCP	172.16.147.211:31585 TCP



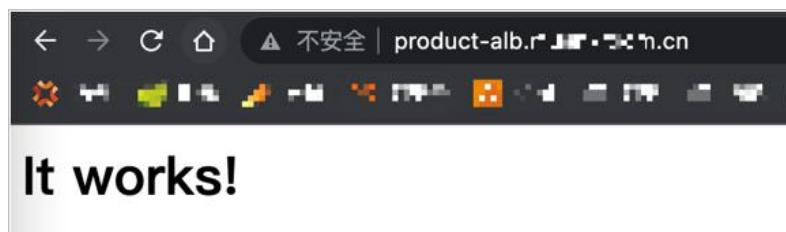
步骤 12 配置 ALB 转发规则，参考章节 4 步骤 11。

根据域名转发到 ACK 集群的应用上。

规则	如果	那么
1 / auto_named_rule / rule-mc... 7/077 正常	域名 是 product-alb.***.cn	转发至 product-ack 权重: 100
2 / auto_named_rule / rule-or... 7/07z 正常	路径 是 /	转发至 webserver 权重: 100
3 / auto_named_rule / rule-lcq... awv.gregk0 正常	路径 是 /app/*	转发至 clb-app 权重: 100
优先级最低 / 监听默认规则 正常	-	缺省转发到 ECS 转发至 webserver

步骤 13 验证转发效果。

浏览器输入 <http://product-lab.xxx.xxx>



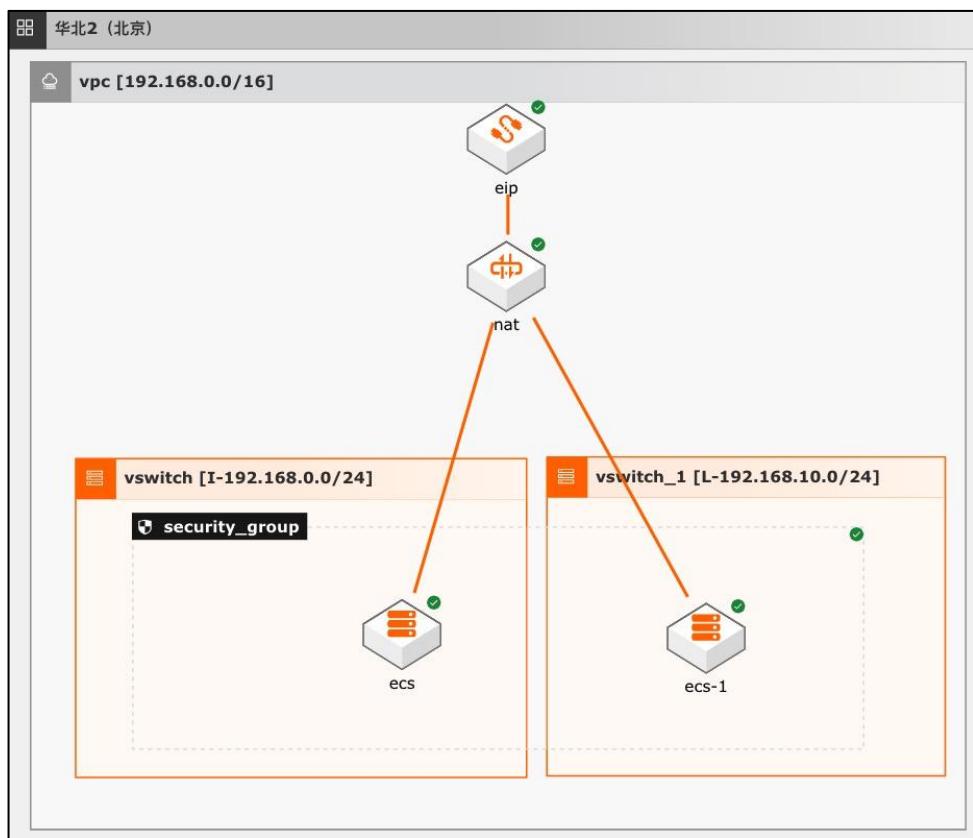
## 3.6.云速搭-NAT 网关部署及应用

作者 | 阿里云解决方案架构师 嘉辽

### 3.6.1.云速搭架构设计

#### 方案架构

通过云速搭设计一个 ECS+EIP+NAT 网关的架构，通过配置 SNAT 规则实现相应的 ECS 可以访问互联网。



#### 理解资源级别

每个阿里云资源都有对应的资源级别，在 CADT 进行架构设计时要遵循资源级别开展。本架构中使用的资源及对应的资源级别如下表所示，在进行架构设计时需要用到。

云资源	资源级别
EIP	Region
NAT 网关	VPC
共享流量包	地域
ECS	AZ
安全组	VPC

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-bj	192.168.0.0/16
AZ1	北京 I 可用区	192.168.0.0/24
AZ2	北京 L 可用区	192.168.10.0/24
安全组	Security-group	-

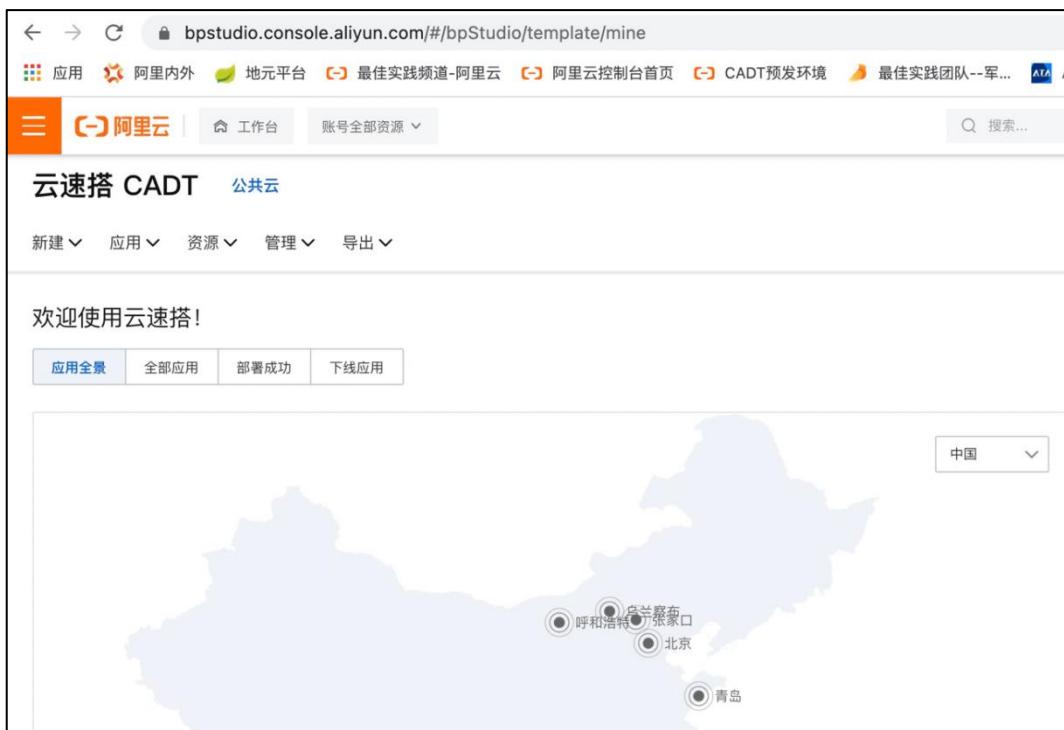
## 3.6.2.设计应用架构

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

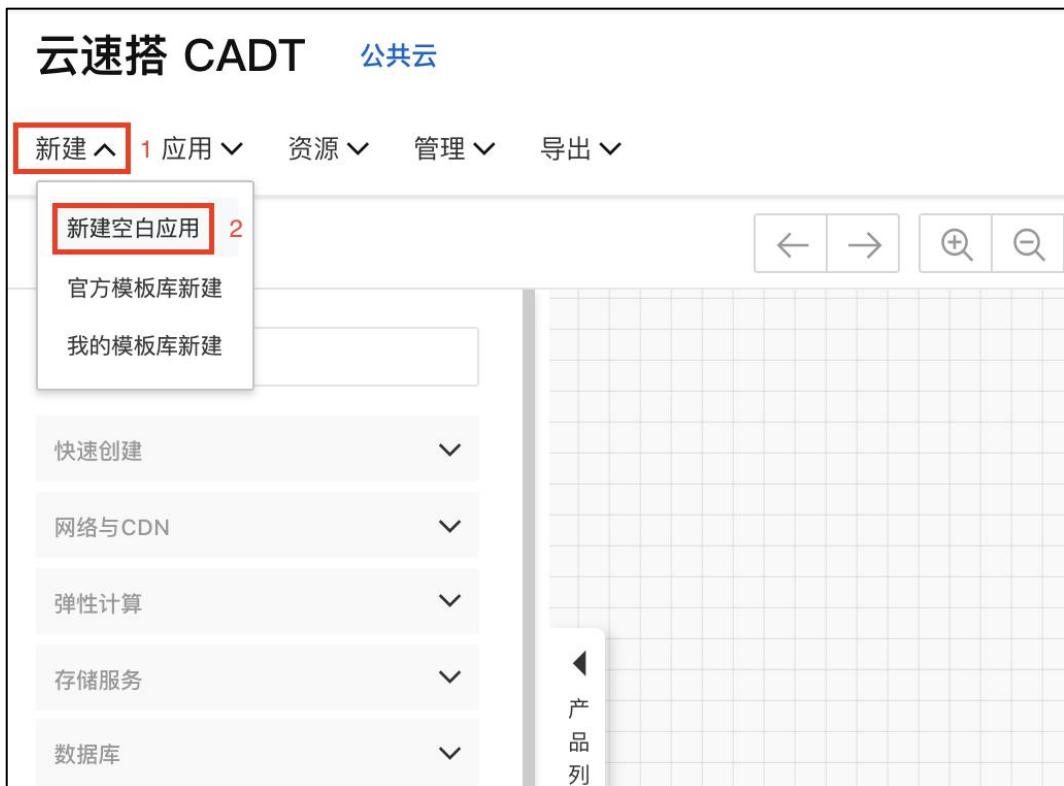
资源分类	资源名称	网段
Region	北京	-
VPC	vpc-bj	192.168.0.0/16
AZ1	北京 I 可用区	192.168.0.0/24
AZ2	北京 L 可用区	192.168.10.0/24
安全组	Security-group	-

步骤 1 登录 <https://bpstudio.console.aliyun.com/>

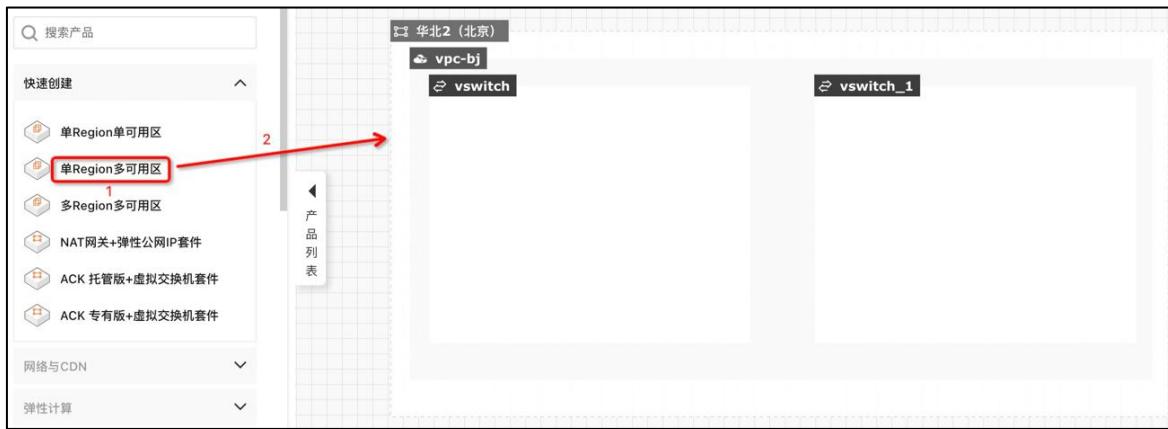


**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在菜单栏单击新建 > 新建空白应用，打开一个空白画布。



步骤3 从左侧工具栏**快速创建**下选择合适的网络拓扑类型，本场景适用**单 Region 多可用区**，单击选中并拖拽到右侧空白画布中。



### 3.6.3.配置资源参数

步骤4 依次双击 Region、VPC、vswitch 进行配置。

双击 **Region**，出现右边提示窗，在区域下拉菜单中选择**华北2（北京）**



双击 **vpc** 选项，在右边提示窗的 VPC 名选项中输入 **vpc-bj**



两双击 **vswitch** 选项，在右边提示窗的 **vswitch** 选项中输入 **vswitch-bj**，可用区选择北京可用区 **I**，网段用默认的 **192.168.0.0/24**。



在 vswitch1 中完成如下配置



步骤 5 在左侧搜索框输入资源名称 eip，选中弹性公网 IP，由于 EIP 属于 Region 资源级别，本例放在 Region 中，拖动弹性公网图标至 Region 中。



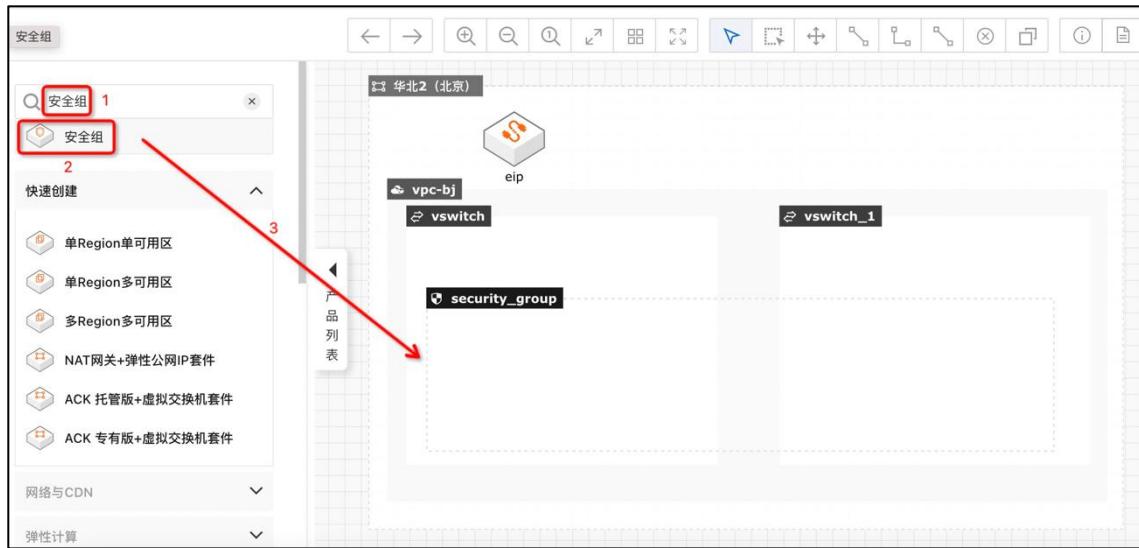
步骤 6 双击 EIP 图标，弹出右侧窗口，进行相应参数配置

配置项	参数说明
购买方式	新购
EIP 名	eip
数量	1
支付方式	按量付费
线路类型	BGP (多线)
网络类型	公网
公网带宽	按流量付费
带宽	5Mb





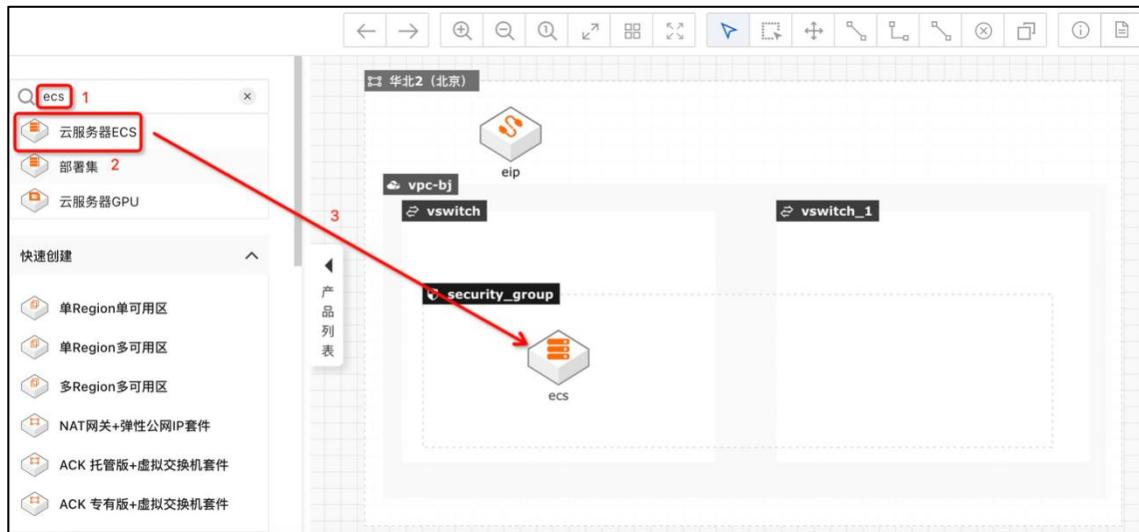
步骤 7 在左侧搜索框输入资源名称安全组，选中安全组图标，由于安全组属于 VPC 资源级别，本次实例中两个 vswitch 中的 ecs 共用同一个安全组，拖动弹性公网图标至 VPC 中，注意，安全组可以向左或者向后拖动边框超过 vswitch 的边界



步骤 8 双击安全组图标，保持默认参数即可



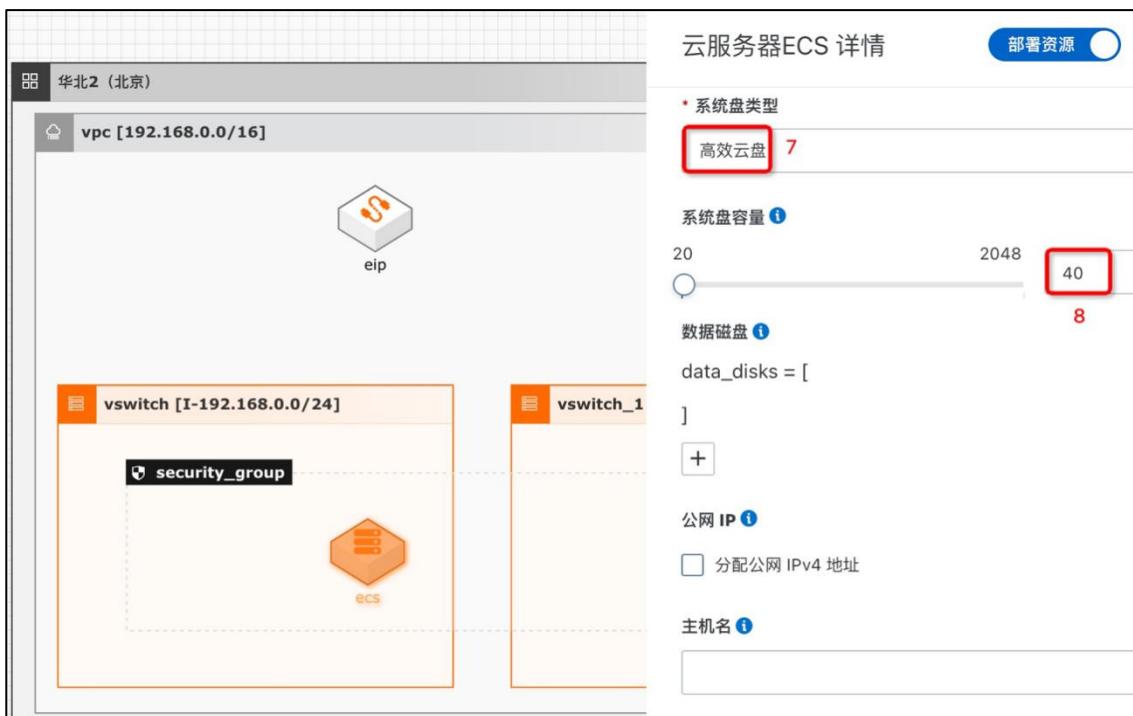
步骤 9 在左侧搜索框输入资源名称 ecs，选中 ecs 图标，由 ecs 属于 vswitch 资源级别，因此放在 vswitch 中，拖动 ecs 图标至 vswitch 中，注意同时也要放在安全组中，适当可以调整安全组上下左右的宽度



步骤 10 双击 ECS 图标，进行参数配置

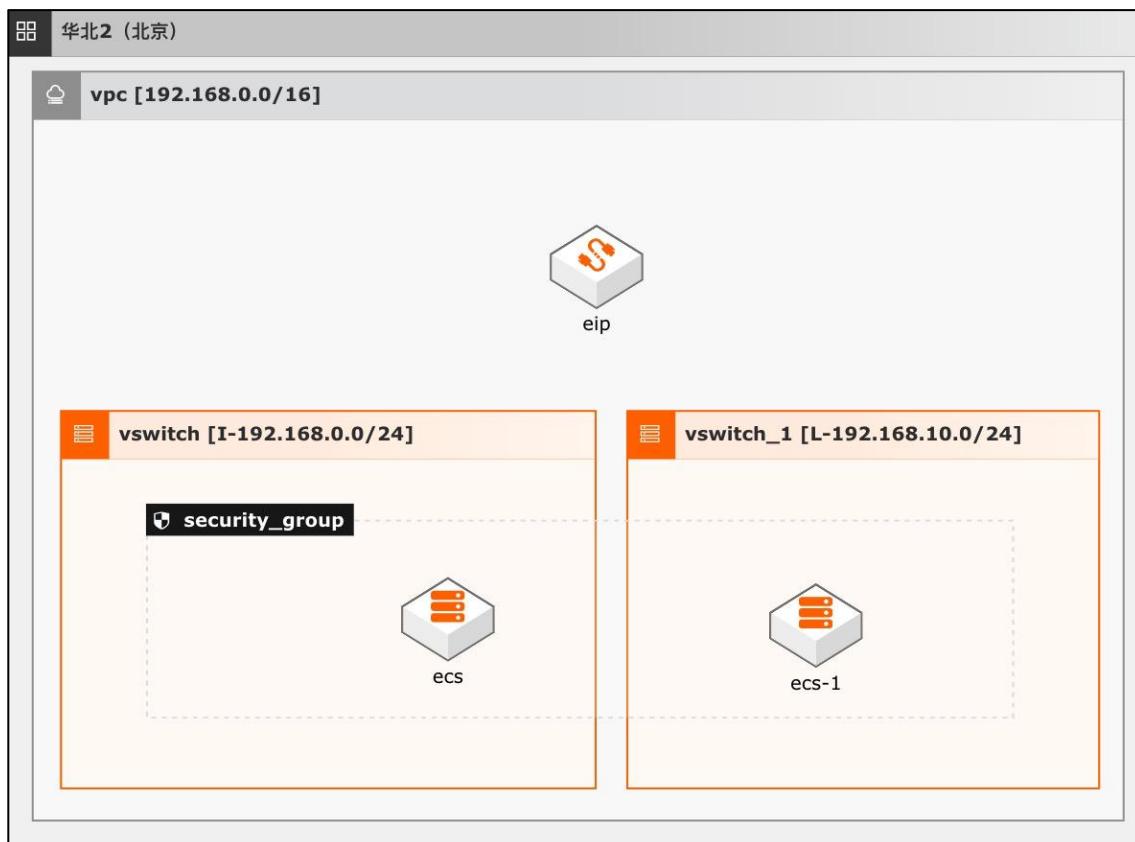
配置项	参数说明
购买方式	新购
可用区	自动填充当前 ecs 所在的 vswitch, 无需修改
实例名称	ecs
数量	1
支付方式	按量付费
实例规格	ecs.c6.2xlarge(8c 16g), 支持关键字搜索
操作系统	Alibaba Cloud Linux 3.2104 64 位
系统盘类型	高效云盘
系统盘容量	40G
主机名	ecs-bj
登录凭证	选择自定义密码, 需要连续两次输入密码。



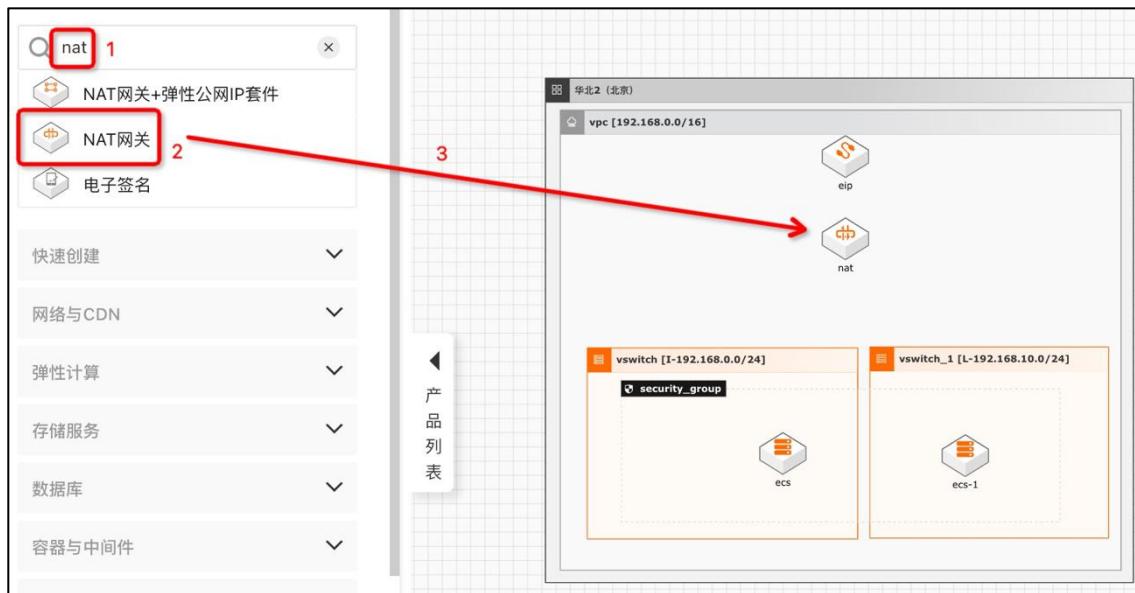


**注意：**标注\*是必填项，参数较多，需要将进度条拖动到最下面，完成必填参数的配置。

步骤 11 在另一个 vswitch 中按照上述步骤同样创建一台 ECS



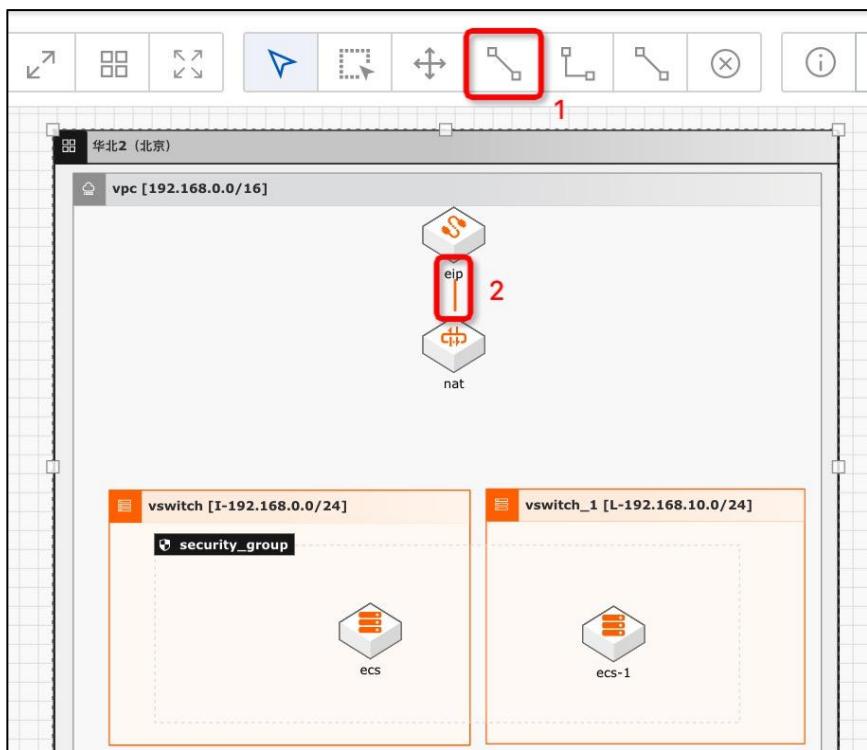
步骤 12 在左侧搜索框输入资源名称 NAT 网关，选中 NAT 网关图标，由 NAT 网关属于 VPC 资源级别，因此放在 VPC 中，拖动 NAT 网关图标至 VPC 中



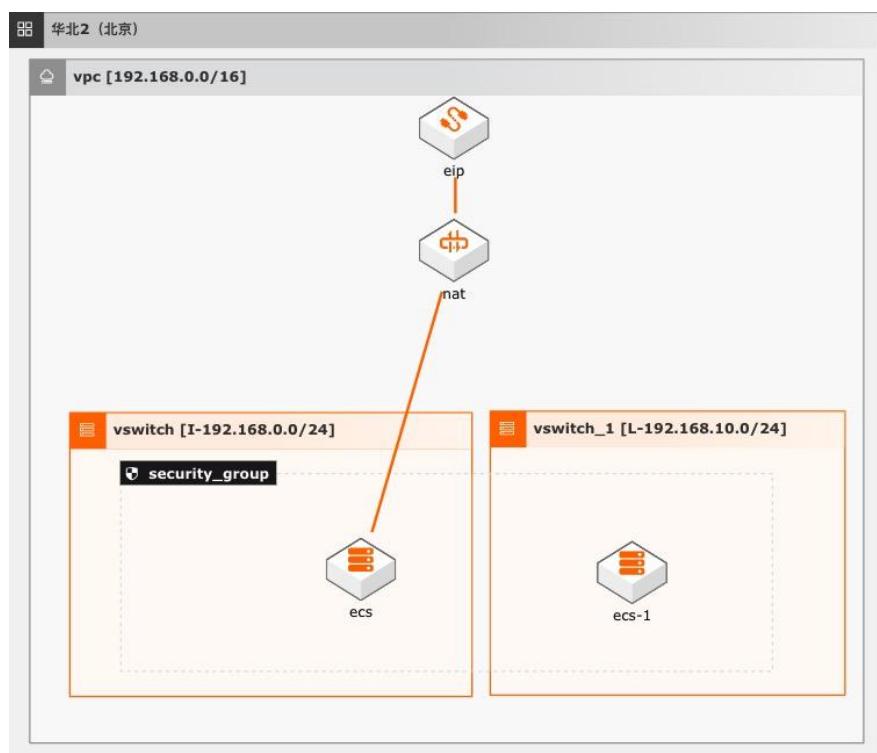
步骤 13 双击 NAT 网关图标，进行 NAT 网关配置



步骤 14 通过实现将 EIP—NAT 网关连接起来



步骤 15 将 nat 网关与 ecs 通过实线连接



步骤 16 双击实线，配置 snat 和 dnat 规则

**NAT\_ECS 详情**

```
rules_maps = [
  {
    "条目名称": [
      {"* 创建条目类型": "SNAT", "1": "SNAT"},  

      {"* 选择公网IP地址": "eip", "2": "eip"}  

    ],  

    "+": "3"
  }
]
```

**NAT\_ECS 详情**

```
{
  "条目名称": [
    {"* 内网端口": "22", "4": "22"},  

    {"* 创建条目类型": "DNAT", "5": "DNAT"},  

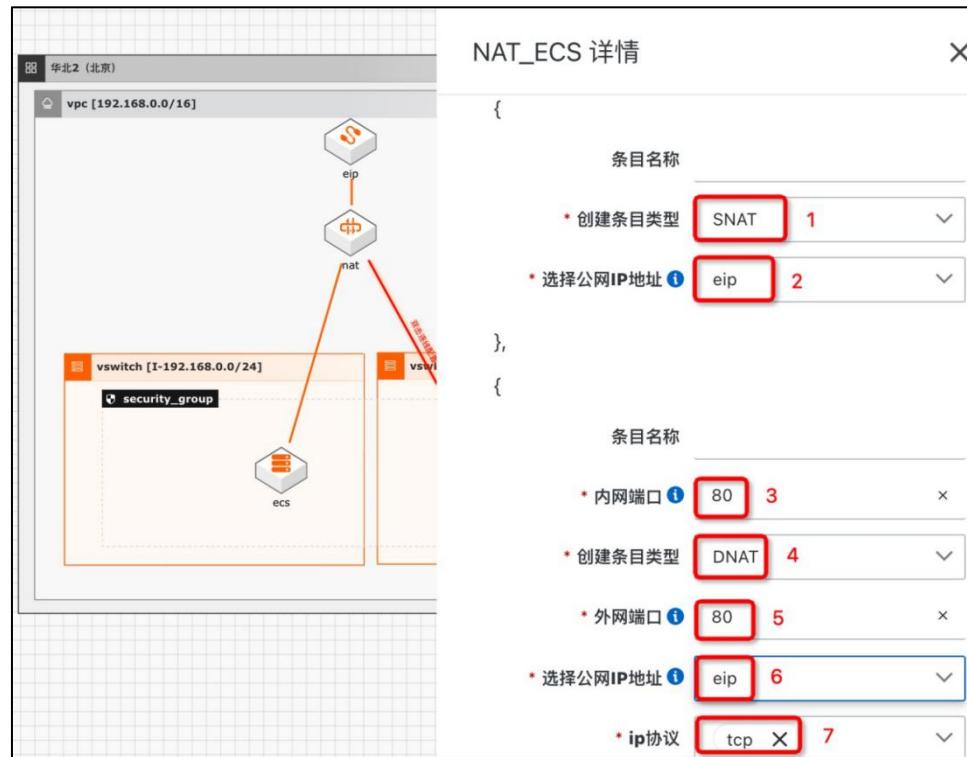
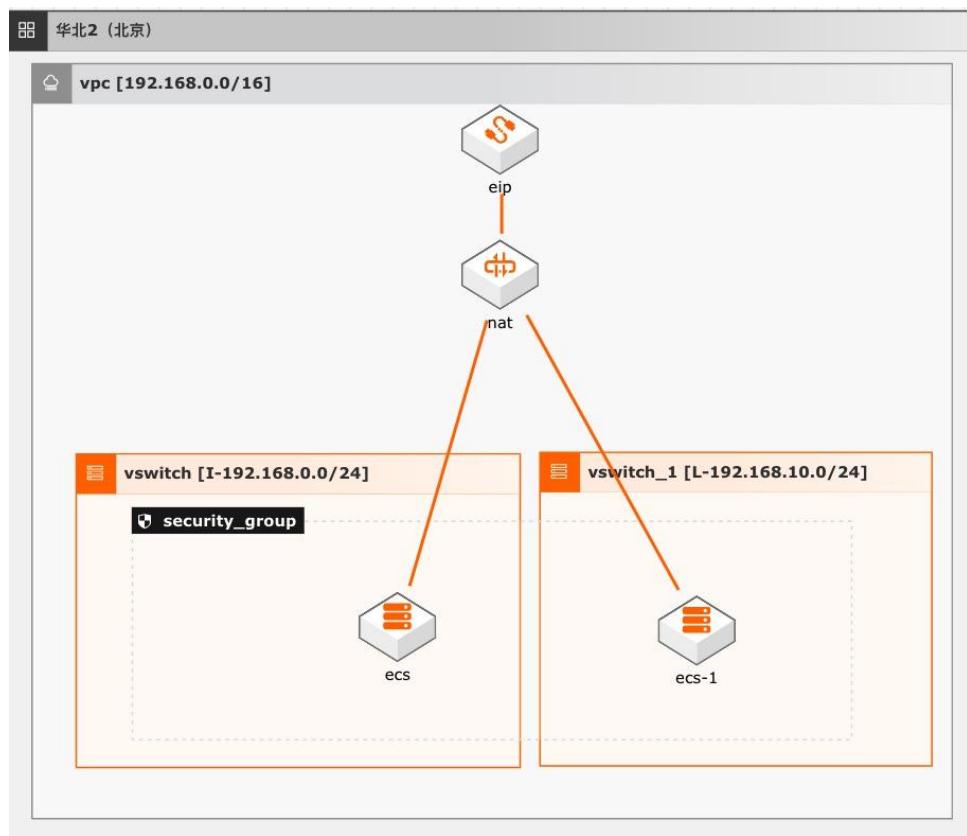
    {"* 外网端口": "22", "6": "22"},  

    {"* 选择公网IP地址": "eip", "7": "eip"},  

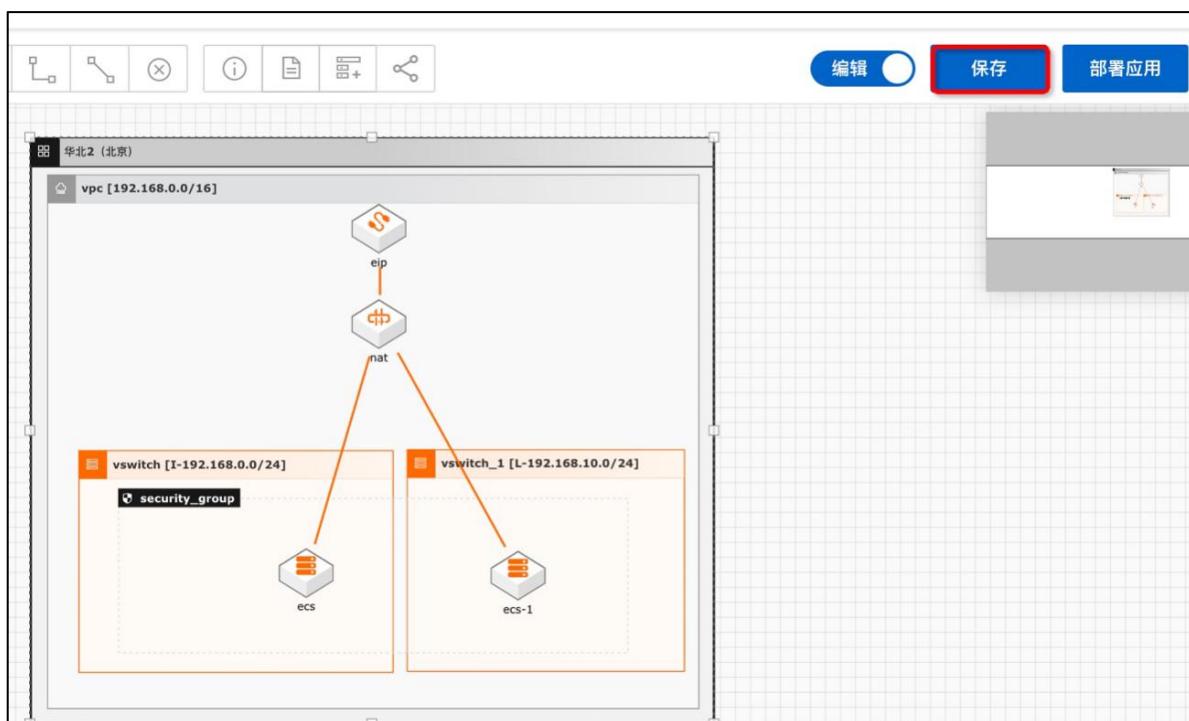
    {"* ip协议": "tcp", "8": "tcp"}  

  ]
}
```

步骤 17 另一台 ecs 也按照上面配置



步骤 18 完成以上资源配置后，单击**保存**。



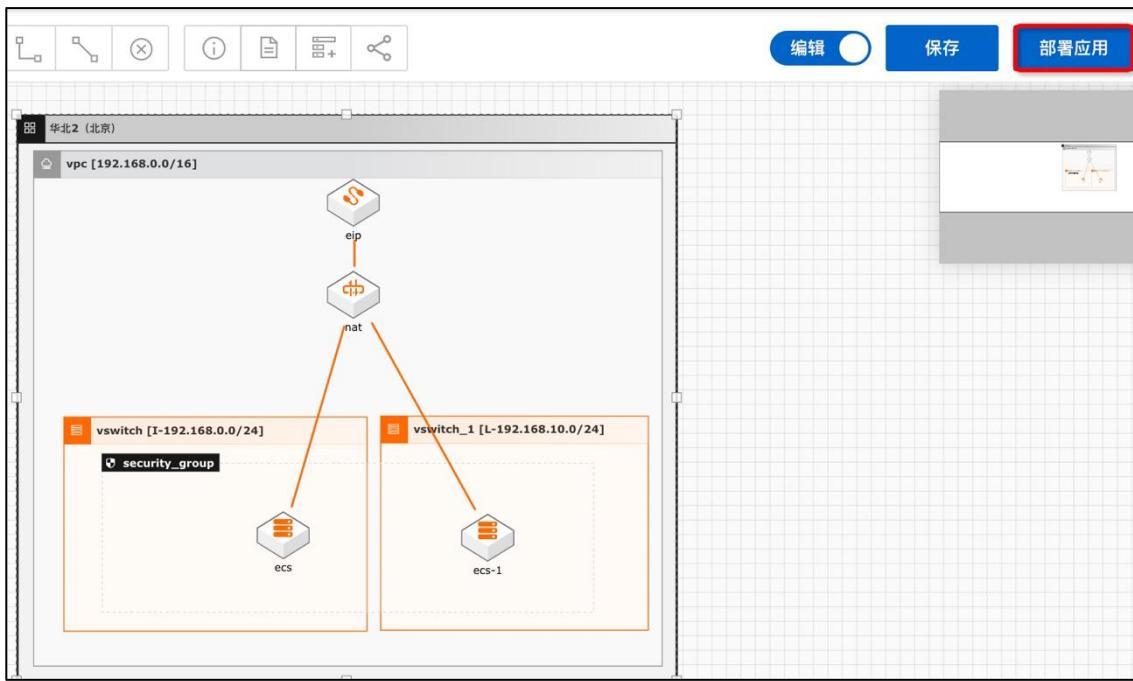
步骤 19 应用名称设置为 nat-test，单击确认。



至此，架构设计阶段工作完成。

### 3.6.4.NAT 部署

步骤 20 单击右上角的**部署应用**。



### 步骤 21 进行资源校验

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	ecs	ecs	北京	ecs.c6.2xlarge	成功	校验通过	定位
2	security_group	security.group	北京		成功	校验通过	定位
3	vswitch_1 [L-192.168.10.0/24]	vswitch	北京	192.168.10.0/24	成功	校验通过	定位
4	eip	eip	北京	public	成功	校验通过	定位
5	vpc [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
6	ecs-1	ecs	北京	ecs.c6.2xlarge	成功	校验通过	定位
7	vswitch [I-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位

状态: **校验成功**

**下一步: 价格清单** 部署应用 [返回](#)

步骤 22 勾选《匀速搭服务条款》，然后单击**下一步：支付并创建**，进行资源部署。

**导出价格清单**

免费 按量付费

资源成本占比

资源预算

- 计算 计算: [REDACTED] 元/时
- 网络 网络: [REDACTED] 元/时

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	状态	操作
1	eip	eip	北京	BGP	1	[REDACTED]	[REDACTED]	[REDACTED]	新购	定位
2	ecs-1	ecs	北京	ecs.c6.2xlarge	1	[REDACTED]	[REDACTED]	[REDACTED]	新购	定位
3	ecs	ecs	北京	ecs.c6.2xlarge	1	[REDACTED]	[REDACTED]	[REDACTED]	新购	定位

状态: **计价成功**

上一步: 资源校验 查看报告 下一步: 确认订单

**确认订单**

免费 按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	nat	nat	北京		1	[REDACTED]	[REDACTED]	新购
2	ecs	ecs	北京	ecs.c6.2xlarge	1	[REDACTED]	[REDACTED]	新购
3	ecs-1	ecs	北京	ecs.c6.2xlarge	1	[REDACTED]	[REDACTED]	新购
4	eip	eip	北京	BGP	1	[REDACTED]	[REDACTED]	新购

《云速搭服务条款》

部署前, 请阅读并勾选服务条款

按量付费: [REDACTED]

状态: **计价成功**

上一步: 价格清单 下一步: 支付并创建

步骤 23 等待提示部署成功, 单击**返回**。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2ze4vgi50f3nhejideylt	运行中	2021-12-24 19:32:25	定位
2	vswitch [l-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zeib5daoiy4sn1u2x2n0	运行中	2021-12-24 19:32:56	定位
3	vswitch_1 [l-192.168.10.0/24]	vswitch (虚拟交换机)	-	vsw-2ze6piobbk1998wfij8z7	运行中	2021-12-24 19:32:56	定位
4	security_group	security.group (安全组)	-	sg-2zeihv02860l49mzag9j	运行中	2021-12-24 19:32:56	定位

每页显示 10 共8条 < 上一页 1 下一页 >

**部署概要**

状态: 部署成功 1 订单编号: 212139296740519, 212142241960519, 212145638870519, 212146029950519

应用编号: J6Q6W660LIM7258D 2

查看报告 返回

步骤 24 打开资源清单，在资源名称中点击各个资源可以跳转到相应产品控制台，已单击 ecs。

**应用操作** 应用操作 **导出资源清单**

序号	资源名称	资源类型	付费类型	资源ID	来源
6	ecs	ecs (云服务器ECS)	按量付费	i-2ze7qrzz6lv9hg5iqatu	新建
7	ecs-1	ecs (云服务器ECS)	按量付费	i-2zeihv02860l49msgowr	新建

步骤 25 在 ECS 控制台中记录 ecs 的 ip 地址，同样方式记录另一台 ecs\_1 的 ip 地址。

**云服务器 ECS**

**← ecs**

**实例详情** 监控 安全组 云盘 快照 一致性组 快照 弹性网卡 远程命令/文件 操作记录 健康诊断 事件

**基本信息**

ecs 运行中

实例ID	i-2ze7qrzz6lv9hg5iqatu	远程连接	地域	华北2 (北京)
资源组	-	所在可用区	北京 可用区1	
公网IP	-	绑定弹性IP	主机名	i2ze7qrzz6lv9hg5iqatuZ
安全组	sg-2zeihv02860l49mzag9j	加入安全组	创建时间	2021年12月24日19:32:00
标签	-	编辑标签	自动释放时间	-
描述	-	修改实例描述		

CPU&内存 8核 16 GB 云盘 1

操作系统 Alibaba Cloud Linux 3.2104 64位 更换操作系统 快照 0

实例规格 ecs.c6.2xlarge 改变实例规格 镜像ID aliyun\_3\_x64\_20G\_alibase\_20210910.vhd

实例规格族 ecs.c6 当前使用带宽 0Mbps (峰值)

**网络信息**

网络类型	专有网络	专有网络	vpc-2ze4vgi50f3nhejideylt
弹性网卡	eni-2zebk7pwijq5cc9gcept	虚拟交换机	vsw-2zeib5daoiy4sn1u2x2n0
主私网IP	192.168.0.151	弹性IP实例ID	-
IPv6地址	-	辅助私网IP	-

实例名称	IP 地址
ecs	192.168.0.151
ecs-1	192.168.10.111

步骤 26 单击 nat 跳转到控制台，看到 nat 网关相应信息。

应用操作		导出资源清单				
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
7	ecs-1	ecs (云服务器ECS)	按量付费	i-2zeihv02860i49msgowr	新建	运行中
8	nat	nat (NAT网关)	按量付费	ngw-2ze6idnqpf7vcf2wi5dex	新建	运行中

专有网络 / 公网NAT网关 / ngw-2ze6idnqpf7vcf2wi5dex

← ngw-2ze6idnqpf7vcf2wi5dex

基本信息	绑定的弹性公网IP (1)	DNAT管理	SNAT管理	监控
实例ID	ngw-2ze6idnqpf7vcf2wi5dex	复制		
描述	- 编辑			
地域	华北2 (北京)			
状态	可用			
弹性网卡ID	eni-2zegg6q2j01r5ay4wadx	复制		
最大带宽	5120 Mbps			
标签	暂无标签	添加		

付费信息

付费类型	后付费
计费方式	按使用量计费

步骤 27 单击绑定的弹性公网 IP，可以看到 CADT 中创建的 EIP 已经自动挂载给 NAT 网关。

专有网络 / 公网NAT网关 / ngw-2ze6idnqpf7vcf2wi5dex					
← ngw-2ze6idnqpf7vcf2wi5dex					
<a href="#">基本信息</a> <a href="#">绑定的弹性公网IP (1)</a> <a href="#">DNAT管理</a> <a href="#">SNAT管理</a> <a href="#">监控</a>					
<a href="#">绑定弹性公网IP</a>					
<input type="checkbox"/>	弹性公网IP地址	实例ID/名称	监控	状态	带宽
<input type="checkbox"/>	101.200.82.157	eip-2zeqdji8q0vu7xc4usy18 eip	已分配	5 Mbps 按使用流量计费	
<input type="checkbox"/>	<a href="#">解绑</a>				

### 3.6.4.1.NAT+ECS 粒度

步骤 28 单击 nat 实例名称，然后在 SNAT 管理中可以看到 CADT 配置的 snat 条目信息。

专有网络 / 公网NAT网关

**公网NAT网关**

实例ID/名称	标签	监控	最大吞吐量	规格/类型	专有网络
ngw-2ze58998edd5c5yvr3ff0 nat			5120 Mbps <a href="#">申请调整</a>	- 增强型	vpc-2zeif1jtmr5uh4gyynan vpc

专有网络 / 公网NAT网关 / ngw-2ze58998edd5c5yvr3ff0

**← ngw-2ze58998edd5c5yvr3ff0**

基本信息	绑定的弹性公网IP (1)	DNAT管理	SNAT管理	监控
<b>基本信息</b>				
实例ID	<a href="#">ngw-2ze58998edd5c5yvr3ff0 复制</a>			
描述	<a href="#">编辑</a>			
地域	华北2 (北京)			
状态	<span style="color: green;">✓ 可用</span>			
弹性网卡ID	<a href="#">eni-2zegi703xuqnfxbnix5i 复制</a>			
最大带宽	5120 Mbps			
标签	<a href="#">暂无标签</a> <a href="#">添加</a>			
<b>付费信息</b>	<a href="#">查看账单</a>			
付费类型	后付费			
计费方式	按使用量计费			

← ngw-2ze58998edd5c5yvr3ff0

基本信息	绑定的弹性公网IP (1)	DNAT管理	SNAT管理	监控
<b>SNAT表信息</b>				
SNAT表ID	<a href="#">stb-2zexsqjoz18a9ois46lmg 复制</a>			
<b>SNAT条目列表</b>				
创建SNAT条目	条目ID	请输入		
		<input type="text"/>		
<input type="checkbox"/>	SNAT条目ID		源网段	ECS/交换机/VPC的ID
<input type="checkbox"/>	snat-2zeqw2ib3tx4qyex7pcua	-	192.168.10.96/32	i-2ze8vyma0m0b808x45sf ecs_1
<input type="checkbox"/>	snat-2zenxldf7t0belaad6g5p	-	192.168.0.9/32	i-2zeisdcaaffyreaukfp ecs

步骤 29 SNAT 功能验证，通过登录 ecs，然后访问 [www.baidu.com](http://www.baidu.com)，如下图所示，可以正常访问互联网

```
>_ 2. root@iZ2ze8vyma0m0b808x45sfZ:~ ×
[root@iZ2ze8vyma0m0b808x45sfZ ~]# ping www.baidu.com
PING www.a.shifen.com (110.242.68.4) 56(84) bytes of data.
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=1 ttl=50 time=12.2 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=2 ttl=50 time=12.1 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=3 ttl=50 time=12.1 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=4 ttl=50 time=12.1 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=5 ttl=50 time=12.1 ms
```

步骤 30 在 DNAT 管理中可以看到 CADT 中配置的 dnat 条目

DNAT条目ID	公网IP地址	公网端口
fwd-2ze2luxwuru0oyyd17z53	101.200.82.157	80
fwd-2zesoxr5ypapgyzxoe5fc	101.200.82.157	22

步骤 31 DNAT 功能验证，通过远程访问公网 ip 的 22 端口，如下图所示，成功跳转到 ECS 中

```
jialiao@B-C1KDLVDL-0253 ~ % ssh root@101.200.82.157 1
The authenticity of host '101.200.82.157 (101.200.82.157)' can't be established.
ECDSA key fingerprint is SHA256:2XaDbQCa4MzcjtAe40QckJ94kaGhxfkTY9LX4BuPiOs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes 2
Warning: Permanently added '101.200.82.157' (ECDSA) to the list of known hosts.
root@101.200.82.157's password: 3、输入ECS的root密码

Welcome to Alibaba Cloud Elastic Compute Service !

Updates Information Summary: available
 7 Security notice(s)
    1 Critical Security notice(s)
    6 Moderate Security notice(s)
Run "dnf upgrade-minimal --security" to apply all updates.
[root@iZ2zeisdcaoaffyreaukfPZ ~]#
```

### 3.6.4.2.NAT+VPC 粒度

删除 2.3.1 中的 snat 规则，通过 nat 网关其他配置，实现 VPC 下所有的 ECS 均能访问互联网。

步骤 32 在 SNAT 条目列表中，选择“创建 SNAT 条目”，选择 VPC 粒度，使用单 IP 地址，下拉框中选择创建的 EIP，然后单击确定创建。



步骤 33 等待配置完成

SNAT条目列表			
创建SNAT条目	条目ID	请输入	搜索
<input type="checkbox"/> SNAT条目ID			
<input type="checkbox"/> snat-2ze199gzzvh1z9zocky6	-	192.168.0.0/16	vpc-2ze4vgi50f3nhejideylt

步骤 34 登录 ecs 进行测试

```
[root@iZ2zeihv02860l49msgowrz ~]# ping www.baidu.com
PING www.a.shifen.com (110.242.68.4) 56(84) bytes of data.
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=1 ttl=50 time=12.4 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=2 ttl=50 time=12.3 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=3 ttl=50 time=12.3 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=4 ttl=50 time=12.3 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=5 ttl=50 time=12.3 ms
```

同样方式登录 ecs-1 进行验证，也能访问互联网。

### 3.6.4.3.NAT+VSW 粒度

通过配置相关规则，实现 VPC 下 vswitch 的 ECS 能访问互联网，vswitch\_1 的 ECS 无法访问互联网。

步骤 35 删除刚才创建的 SNAT 规则，创建新的 SNAT 规则，选择交换机粒度，选择交换机 vswitch，如下进行配置，单击确定创建。

The screenshot shows the SNAT management interface for a specific NAT gateway. The top navigation bar includes links for '专有网络 / 公网NAT网关 / ngw-2zeeyckfoqsfnetqbkqd2'. Below the navigation is a header with tabs: '基本信息' (Basic Information), '绑定的弹性公网IP (1)' (1 Elastic Public IP Bound), 'DNAT管理' (DNAT Management), 'SNAT管理' (SNAT Management) [selected], and '监控' (Monitoring). The main area is titled 'SNAT表信息' (SNAT Table Information) and shows a SNAT table ID 'stb-2zemfyfcxyef3oi4dtx2x' with a '复制' (Copy) button. Below this is a 'SNAT条目列表' (SNAT Rule Item List) section. A blue button labeled '创建SNAT条目' (Create SNAT Rule Item) is highlighted with a red box. To its right are search fields for '条目ID' (Rule ID) and '请输入' (Enter), and a magnifying glass icon. The table below lists columns: 'SNAT条目ID' (SNAT Rule ID), '源网段' (Source Network Segment), and 'ECS/交换机/VPC的ID' (ECS/switch/VPC ID).

The screenshot shows the 'Create SNAT Rule Item' dialog. At the top is a back arrow and the title '创建SNAT条目'. Below is a note about SNAT rule types and their functions. The 'SNAT条目粒度' (SNAT Rule Item Granularity) section contains two radio buttons: 'vpc粒度' (vpc granularity) and '交换机粒度' (switch granularity) [selected]. A note next to '交换机粒度' states: '指定交换机下的ECS通过配置的公网IP访问互联网'. The '选择交换机' (Select Switch) field contains the value 'vsw-2zeib5daoiy4sn1u2x2...' with a red box around it and the number '2' to its right. A note below says: '如您选择多个交换机，将会为您创建多条SNAT条目，使用相同的公网IP地址。' The '交换机网段' (Switch Network Segment) is set to '192.168.0.0/24'. The '选择公网IP地址' (Select Public IP Address) section has a radio button for '使用单IP' (Use Single IP) [selected] with the value '101.200.82.157' [boxed with red box and number 4] and another for '使用多IP'. The '条目名称' (Rule Item Name) field is empty. The bottom right corner shows '0/128'.

步骤 36 配置完成，分别登录两台 ECS 进行验证。

SNAT条目列表			
创建SNAT条目	条目ID	请输入	搜索
<input type="checkbox"/>	SNAT条目ID	源网段	ECS/交换机/VPC的ID
<input type="checkbox"/>	snat-2ze32g0o4281dvt1ybvvh	192.168.0.0/24	vsw-2zeib5daoly4sn1u2x2n0 vswitch

```
[root@iZ2ze7qrzz6lv9hg5iqatuZ ~]# ip add 1
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:06:f2:52 brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.151/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
            2 valid_lft 315358550sec preferred_lft 315358550sec
        inet6 fe80::216:3eff:fe06:f252/64 scope link
            valid_lft forever preferred_lft forever
[root@iZ2ze7qrzz6lv9hg5iqatuZ ~]# ping www.baidu.com
PING www.a.shifen.com (110.242.68.4) 56(84) bytes of data. 3
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=1 ttl=50 time=10.8 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=2 ttl=50 time=10.7 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=3 ttl=50 time=10.7 ms
64 bytes from 110.242.68.4 (110.242.68.4): icmp_seq=4 ttl=50 time=10.7 ms
```

```
>_ 2. root@iZ2zeihv02860l49msgowrZ:~ x
[root@iZ2zeihv02860l49msgowrZ ~]# ip add 1
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:16:3e:37:20:50 brd ff:ff:ff:ff:ff:ff
        inet 192.168.10.111/24 brd 192.168.10.255 scope global dynamic noprefixroute eth0
            2 valid_lft 315358649sec preferred_lft 315358649sec
        inet6 fe80::216:3eff:fe37:2050/64 scope link
            valid_lft forever preferred_lft forever
[root@iZ2zeihv02860l49msaowrZ ~]# ping www.baidu.com
PING www.a.shifen.com (110.242.68.3) 56(84) bytes of data. 3
```

验证结果：在 vswitch 中的 ecs 可以访问互联网，而在 vswitch\_1 中的 ecs-1 无法访问互联网。

### 3.6.4.4.NAT 共享流量包

参考 <https://bp.aliyun.com/detail/251> 最佳实践的 2.5 小节。

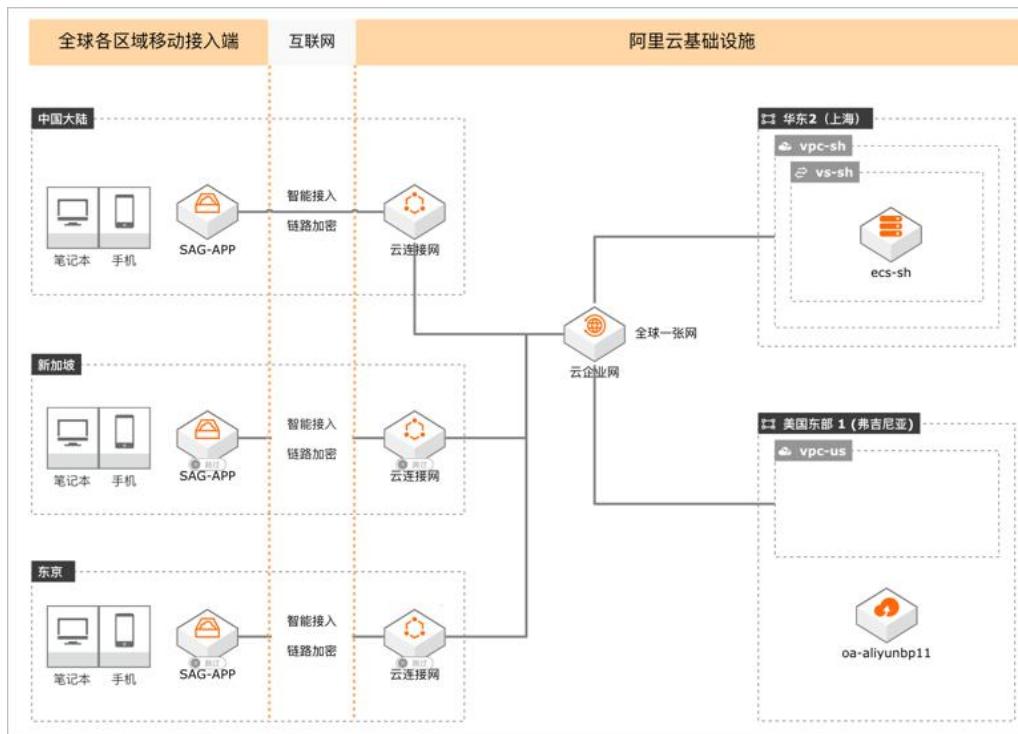
## 3.7.云速搭部署智能接入网关 SAG APP

作者 | 阿里云解决方案架构师 厉博

### 3.7.1.云速搭架构设计入门

#### 方案架构

本篇最佳实践通过 CADT 在华东 2 上海和美西弗吉尼亚创建跨地域的 VPC，在 VPC 内部署 ECS 模拟办公系统应用。通过 CADT 购买 SAG APP 版并挂载到云连接网 CCN，通过云企业网 CEN 将云上跨地域的 VPC 和云连接网 CCN 打通，实现内网互联互通。登录 SAG 客户端之后，就可以通过内网 IP 访问云上资源。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
CEN	全局资源
ECS	vswitch 交换机
安全组	VPC 专有网络
SAG APP	全局资源
CCN	全局资源

### 3.7.2.设计过程

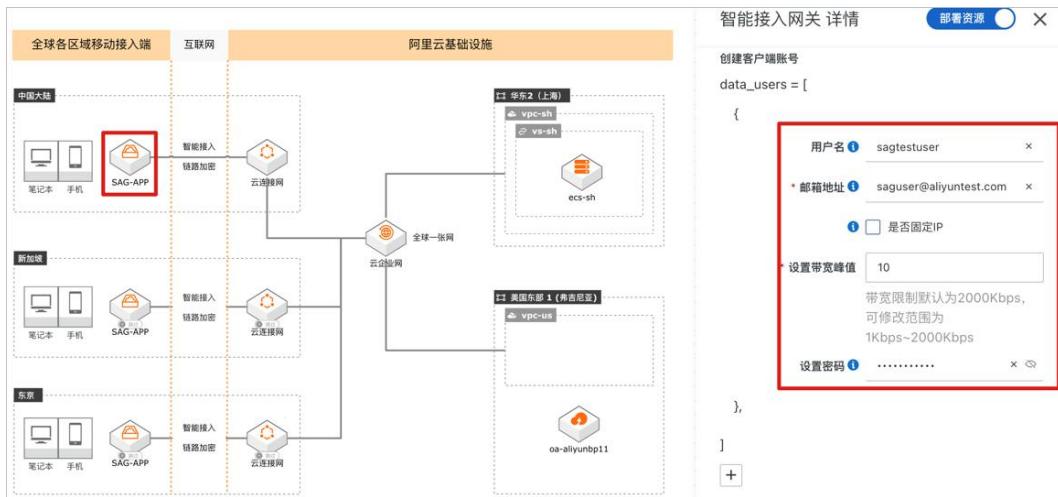
步骤 1 访问 CADT 控制台 <https://bpstudio.console.aliyun.com>，打开官方模板库：



步骤 2 输入 SAG 关键字模糊搜索，找到《中小企业上云多地域办公组网 SAG》模板，单击基于方案新建。



步骤3 双击架构图中的SAG-APP，在右侧的配置栏输入SAG客户端账号、邮箱地址。请输入真实有效的邮箱地址，并设置密码，用于后续进行登录测试。



步骤4 双击 OSS 图标，修改 OSS bucket 名称，本实践以“oa-aliyunbp11”作为示例。



步骤5 将设计好的架构**保存**为应用。



### 3.7.3.部署过程

步骤 6 单击应用 > 部署应用。



步骤 7 资源验证成功之后，单击下一步：价格清单。

资源验证						
资源名称	资源类型	区域	规格	结果	备注	操作
SAG-APP	sag		5	成功	校验通过	定位
vpc-sh	vpc	上海	192.168.10.0/24	成功	校验通过	定位
vpc-us	vpc	美国硅谷	172.16.10.0/24	成功	校验通过	定位
默认安全组	security.group	上海		成功	校验通过	定位
默认安全组	security.group	美国硅谷		成功	校验通过	定位
云企业网	cen			成功	校验通过	定位
oss-16181967516 571	oss	美国硅谷	Standard	成功	校验通过	定位
云连接网	ccn			成功	校验通过	定位

状态:校验成功
下一步: 价格清单
返回

步骤 8 确认各项产品价格无误，单击下一步：确认订单。

可以单击查看报告会实时生成一个应用架构成本分析报告。

**导出价格清单**

免费    **包年包月**    按量付费

资源成本占比



资源预算  
● 网络 网络: ... 元

10...

价格列表

资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
云连接网	ccn	上海		1	-				定位
云企业网	cen			1	1月	...元/月	省...元/月	...元/月	定位
SAG-APP	sag	上海	5	1	1月	...元/月	省...元/月	...元/月	定位

状态: 计价成功

上一步: 资源校验    查看报告    **下一步: 确认订单**

步骤 9 勾选《云速搭服务条款》，并单击**下一步：支付并创建**。

**确认订单**

免费    **包年包月**    按量付费

资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
SAG-APP	sag	上海	5	1	1月	...元/月	...元/月	新购
云企业网	cen			1	1月	...元/月	...元/月	新购
oss-16181967 516571	oss	美国硅谷	Standard	1	-			新购
云连接网	ccn	上海		1	-			新购

**《云速搭服务条款》** ①

部署前，请阅读并勾选服务条款

包年包月: ... 元 按量付费: ... 元/时 ②

状态: 计价成功

上一步: 价格清单    **下一步: 支付并创建**

步骤 10 再次确认，注意架构图中 SAG、CEN 是按月购买的，无法提前释放。



步骤 11 大概 3 分钟左右，资源部署成功。

资源部署状态						
资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
SAG-APP	sag	-	sag-xsua78toh28o96bpss	运行中	2021-10-08 09:39:17	定位
oss-1618196 7516571	oss	按量付费	oss-16181967516571	运行中	2021-10-08 09:39:17	定位
云企业网	cen	-	cen-6w3u4iq2cxad8wx1ql	运行中	2021-10-08 09:39:17	定位
vpc-sh	vpc	-	vpc-uf6s1o2fa6kmq4y7k8kdm	运行中	2021-10-08 09:39:42	定位
vpc-us	vpc	-	vpc-rj93y1g83mefgeoxyewic	运行中	2021-10-08 09:39:42	定位

**部署概要**

状态： 部署成功 订单编号： 211028174380125, 211028075370125  
方案编号：A7PRCB210X62ZL6B

### 3.7.4.验证过程

用户可按照实际业务部署应用，这里通过在 ECS 上部署 httpd 服务模拟办公系统。

步骤 12 访问 ECS 控制台 <https://ecs.console.aliyun.com/#/server/region/cn-shanghai>，查看创建好的 ECS，勾选该 ECS，单击更多 > 发送远程命令。

云服务器 ECS / 实例

## 实例

创建实例 选择实例属性项搜索，或者输入关键字识别搜索

实例ID/名称 标签 监控 可用区 IP地址

1 i-uf6fxgyhdpj1lulo7xw8 ecs-sh 上海 可用区G 192.168.10.246 (私有)

启动 停止 重启 重置实例密码 换费 按量付费转包年包月 释放设置 更多▲

更多 ▾ ②

发送远程命令 ③

- 重开机
- 实例设置
- 密码/密钥
- 资源变配
- 云盘和镜像
- 网络和安全组

步骤 13 输入以下命令安装 web 服务，配置 index.html 主页。

```
yum install -y httpd
cd /var/www/html
echo "Hello world, This is OA system." > index.html
service httpd start
netstat -an|grep :80|grep LISTEN
```

发送命令

实例ID: i-uf6fxgyhdpj1lulo7xw8

命令类型: Shell

保留命令:

命令内容:

```
1 yum install -y httpd
2 cd /var/www/html
3 echo "Hello world, This is OA system." > index.html
4 service httpd start
5 netstat -an|grep :80|grep LISTEN
```

命令输出:

```
✓ 1. i-uf6fxgyhdpj1lulo7xw8
Verifying : mailcap-2.1.41-2.1.a17.noarch 2/5
Verifying : apr-util-1.5.2-6.2.a17.x86_64 3/5
Verifying : apr-1.4.8-7.1.a17.x86_64 4/5
Verifying : httpd-tools-2.4.6-97.1.a17.x86_64 5/5

Installed:
httpd.x86_64 0:2.4.6-97.1.a17

Dependency Installed:
apr.x86_64 0:1.4.8-7.1.a17      apr-util.x86_64 0:1.5.2-6.2.a17
httpd-tools.x86_64 0:2.4.6-97.1.a17      mailcap.noarch 0:2.1.41-2.1.a17

Complete!
tcp6      0      0 ::1:80          ::*              LISTEN
✓ 执行成功 2021年10月8日09:55:13
```

执行 取消 ②

步骤 14 登录云企业网控制台。<https://cen.console.aliyun.com/cen/list>，查看创建好的云企业网实例，单击创建的 CEN 实例 ID。

The screenshot shows the 'Cloud Enterprise Network Instances' page. At the top, there is a notice about the requirement to submit material from November 15, 2018. Below the notice, there are buttons for 'Create Cloud Enterprise Network Instance', 'Tag Filter', and 'Refresh'. There is also a search bar with dropdowns for 'Instance Name' and 'Region'. The main table lists instances with columns: Instance ID/Name, Tag, Status, Network Instance, Bandwidth Pack, Cross-Region Bandwidth, and Description. The first row, which has a red box around its 'Instance ID/Name' cell, shows the instance ID 'cen-6w3u4iq2cxd8wx1ql' and the status 'Available'.

步骤 15 可以发现 VPC 和 CCN 已经都加载进来了。

The screenshot shows the 'Basic Information' tab of a CEN instance. It displays the instance ID 'cen-6w3u4iq2cxd8wx1ql', name 'Cloud Enterprise Network', status 'Available', and enablement of the 'Multi-path Routing Function'. Below this, the 'Network Instance Management' section shows the 'Load Network Instance' tab selected. A red box highlights the 'Instance ID/Name' column of the table, which lists three network instances: 'ccn-bf5pgoq69vcd6ojhd1' (Cloud Connection Network), 'vpc-uf6s1o2fa6kmq4y7k8kdm' (VPC), and 'vpc-rj93y1g83mefgeoxyewic' (VPC). All three instances are marked as 'Loaded' (已加载).

步骤 16 访问 SAG 控制台 (<https://smarttag.console.aliyun.com/software/cn-shanghai/software>)，SAG 实例已挂载云连接网 CCN，状态为可用。私网网段已正确设置。

The screenshot shows the 'APP Instance Management' page. It features a search bar with 'Create Intelligent Access Gateway APP', 'Buy APP Traffic Package', 'View APP Traffic Package Details', and a search input field. The main table lists instances with columns: Instance ID/Name, Cloud Connection Network ID/Name, Status, Monitoring, Private Network Segment, and Total Account Number. The first row, which has a red box around its 'Instance ID/Name' cell, shows the instance ID 'sag-xsua78toh28o96bpss' and the status 'Available'.

步骤 17 单击 SAG 实例 ID，在**客户端账号管理**页签下可以查看到创建好的账号信息。可以在操作栏进行重置密码操作。

客户端IP地址	监控	用户名	当月流量统计	连接带宽限制	应用加速带宽峰值	邮箱账号	在线状态	上线时间	操作
(随机IP)		sagtestuser1	-	2 Mbps	-	l...h@alibaba-inc.com	不在线	-	<a href="#">删除</a> <a href="#">重置密码</a> <a href="#">更多</a>

步骤 18 进入邮箱，可用看到用户名和密码，记录好信息。点击下载客户端。

尊敬的阿里云用户：

您好，感谢您使用阿里云智能接入网关软件版产品，您的管理员已为您创建了一个账号或修改了您的密码，请您妥善保管好您的账号密码。

智能接入网关实例ID：sag-xsua78toh28o96bpss

企业码：

用户名：sagtestuser1

密码：[REDACTED]

您可以[点击](#)下载安装阿里云网络客户端。您可以通过上述账号登录客户端修改密码。若在使用过程中忘记密码，您可以联系您的网络管理员咨询或重置密码。更多帮助请联系您的管理员或参考[操作指导](#)。

阿里云计算有限公司

此为系统邮件请勿回复

步骤 19 跳转到客户端下载页面 ([https://help.aliyun.com/document\\_detail/102544.html](https://help.aliyun.com/document_detail/102544.html))。目前支持：Windows, Android, iOS, MacOS。根据实际情况选择终端类型下载对应的客户端并完成安装。

默认 CEN 内的网络有 1K 的网络带宽用于验证连通性。若想正常的跨域访问业务，则需要购买对应的带宽包。此处略。登录 SAG 客户端后，就可以通过内网 IP 访问到云上 WebServer 服务。

步骤 20 以 MacOS 客户端为例，输入 SAG ID，用户名和密码，单击登录。

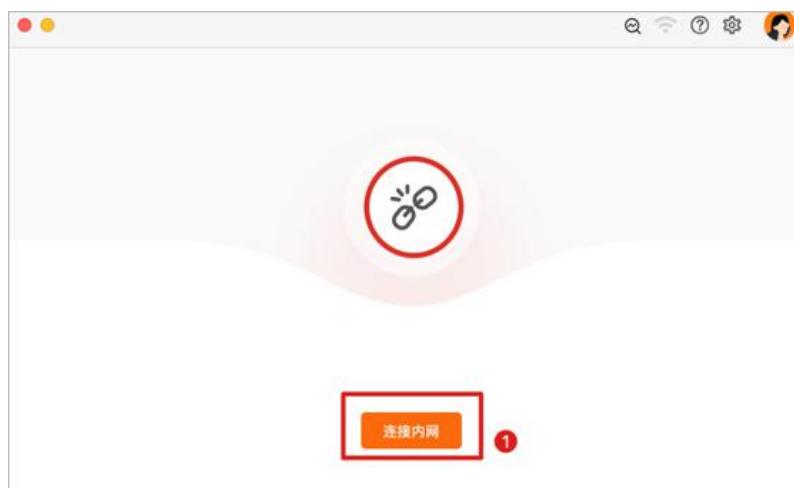
**说明：**用户名和密码就是之前邮件中的信息。



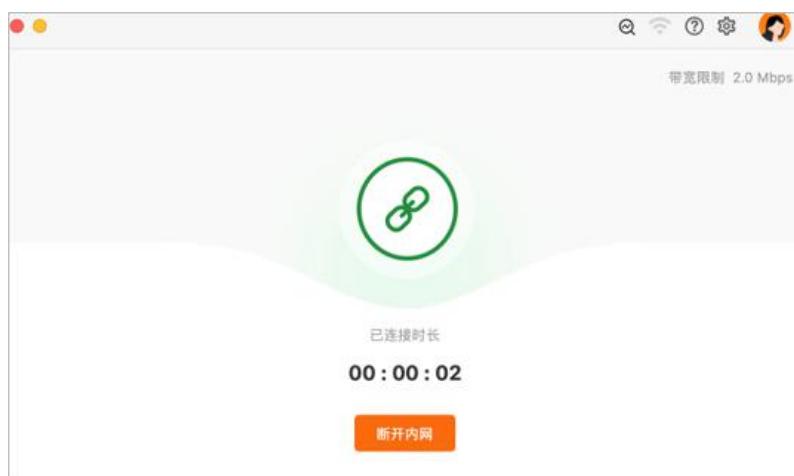
步骤 21 单击**登录**, 进行连接, 并按提示单击**同意、允许**。



步骤 22 单击连接内网。

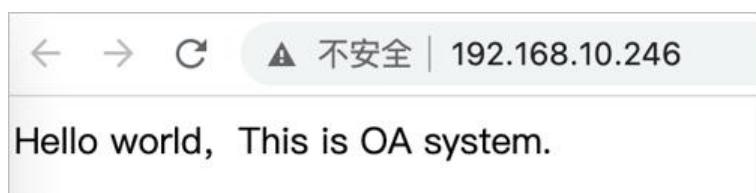


步骤 23 如下已连接阿里云网络。



到这里表示已经连接上阿里云了。

步骤 24 打开浏览器输入 WebServer 的内网 IP 地址: <http://192.168.10.246> (以实际地址为准)  
可以访问到 web 页面:



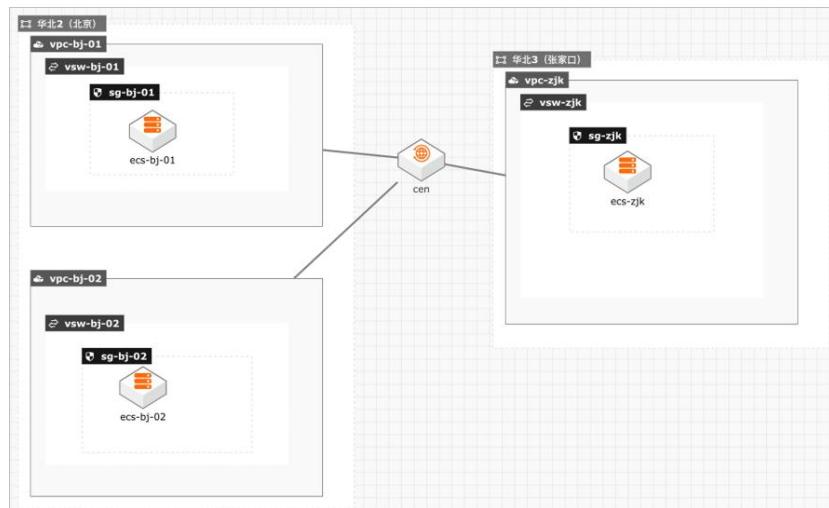
## 3.8.云速搭部署云企业网 CEN

作者 | 阿里云解决方案架构师 厉博

### 3.8.1.云速搭架构设计入门

#### 方案架构

通过云速搭 CADT 设计一个多地域多 VPC 组网的架构，大致实现的架构如下图所示：通过 CEN 将位于不同 VPC，不同地域的 ECS 实现网络互通。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region
CEN	全局资源
ECS	VSW
安全组	VPC

### 3.8.2.设计过程

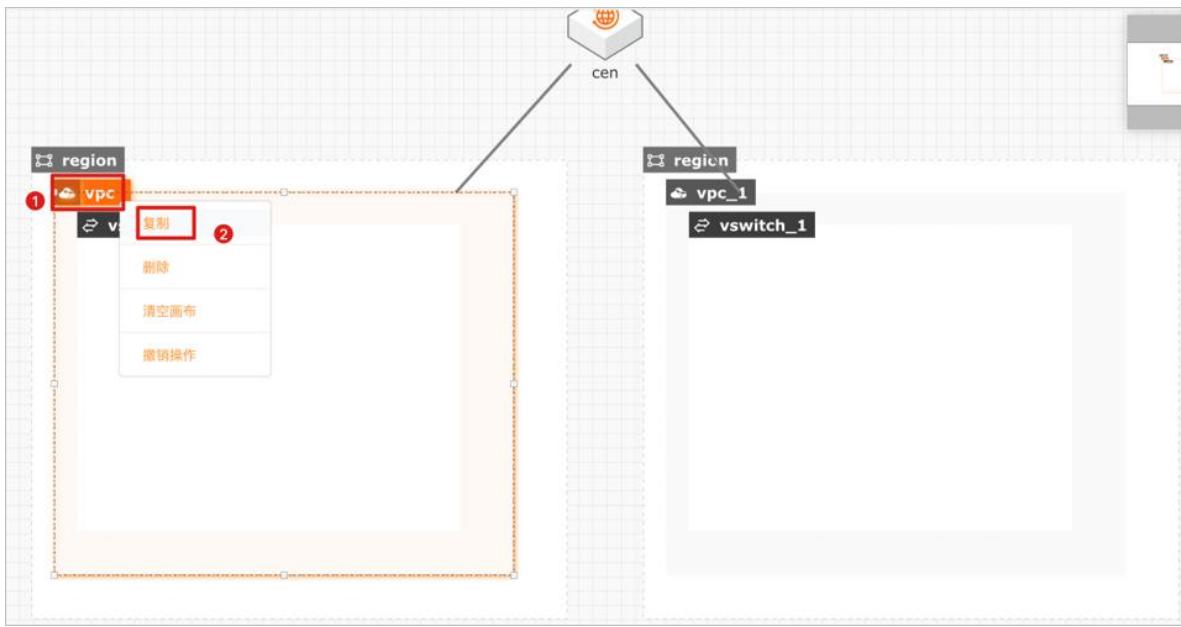
步骤 1 在 CADT 控制台单击新建 > 新建空白应用。



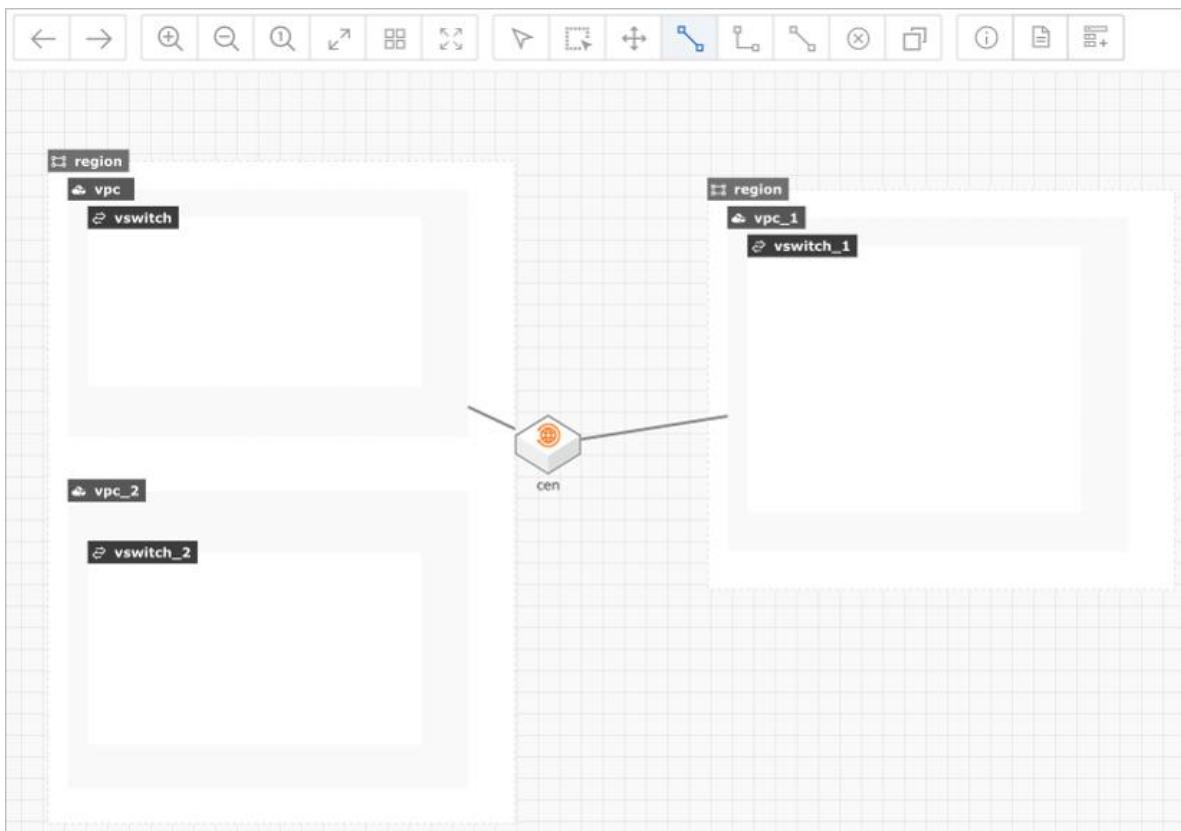
步骤 2 从快速创建下拖动一个“多 Region 多可用区”模板到右侧画板中。



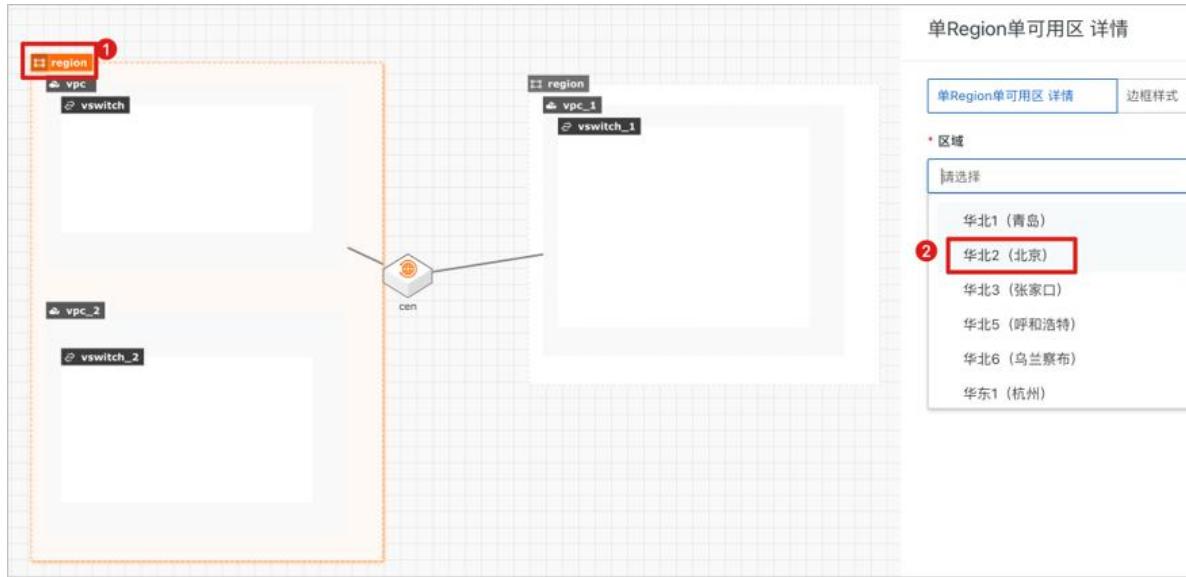
步骤 3 调整架构，右键复制 VPC。



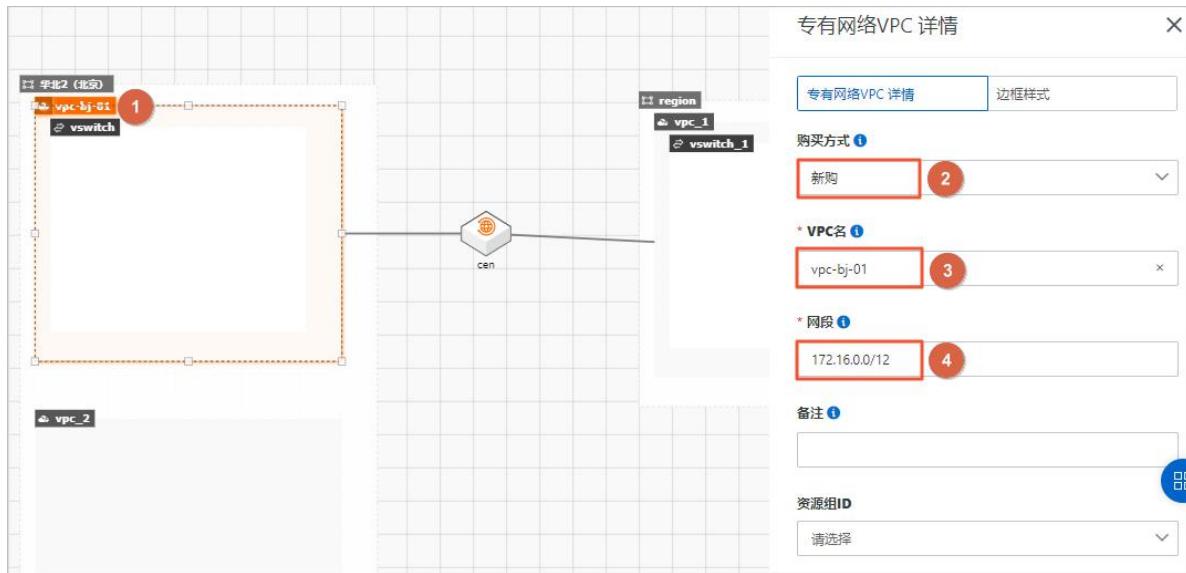
步骤 4 得到如下架构：



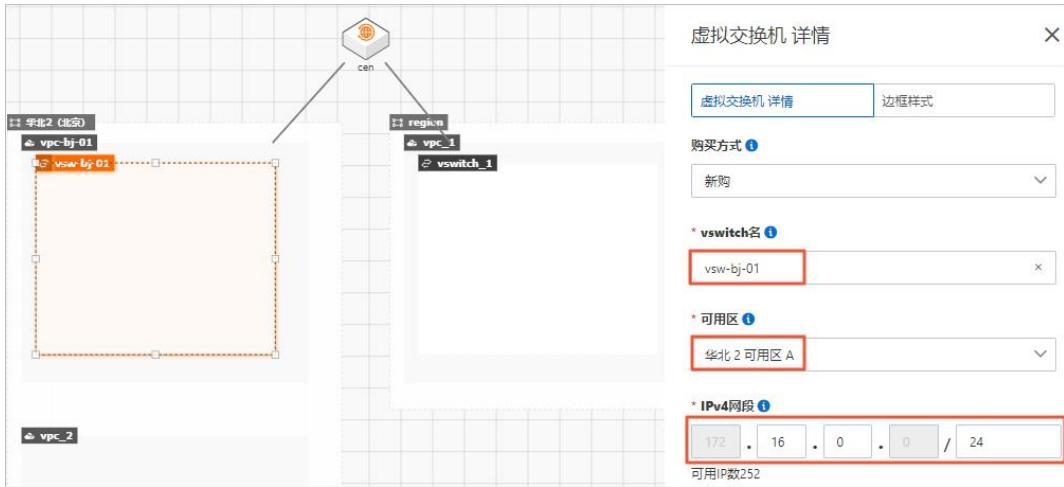
步骤 5 单击架构图左侧的 region，设置为“华北 2-北京”。



步骤 6 单击 VPC，设置 VPC 名 (vpc-bj-01) 以及网段 (172.16.0.0/12)。



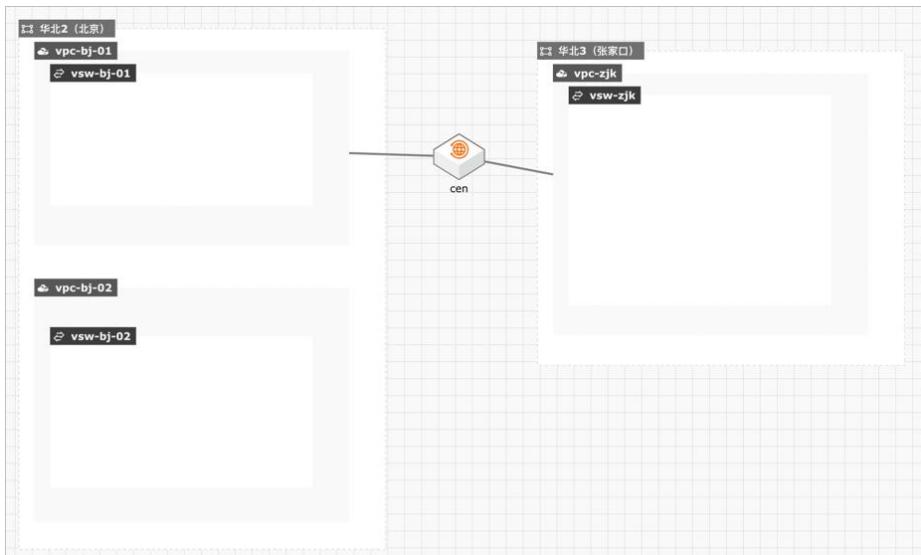
步骤 7 单击 vswitch，设置交换机名称 (vsw-bj-01) 以及网段 (172.16.0.0/24)，可用区选择可用区 A。



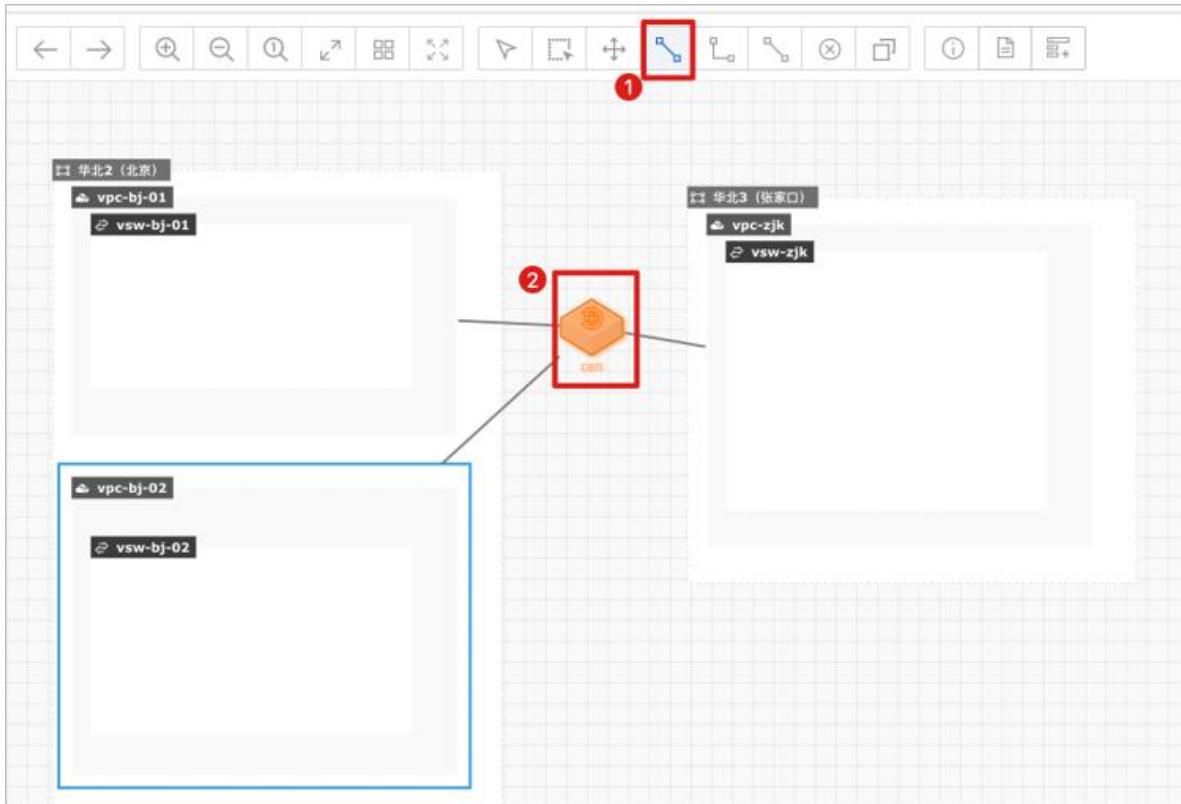
步骤 8 同上设置其他网络属性

区域	VPC	交换机	可用区
华北 2 (北京)	vpc-bj-01 172.16.0.0/12	vsw-bj-01 172.16.0.0/24	A
华北 2 (北京)	vpc-bj-02 172.16.1.0/12	vsw-bj-02 172.16.1.0/24	A
华北 3 (张家口)	vpc-zjk 172.16.2.0/12	vsw-zjk 172.16.2.0/24	A

步骤 9 得到如下架构：

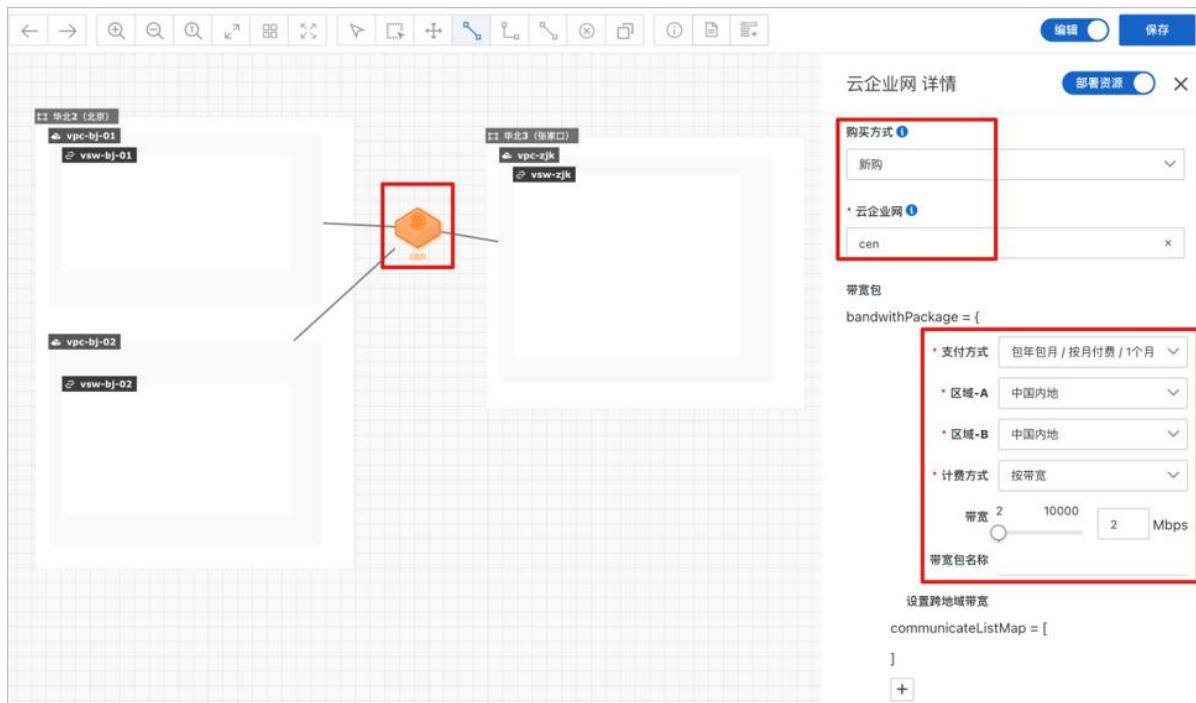


步骤 10 单击**创建连线**，在 CEN 和 vpc-bj-02 之间连线。



步骤 11 双击 cen，编辑右侧参数。

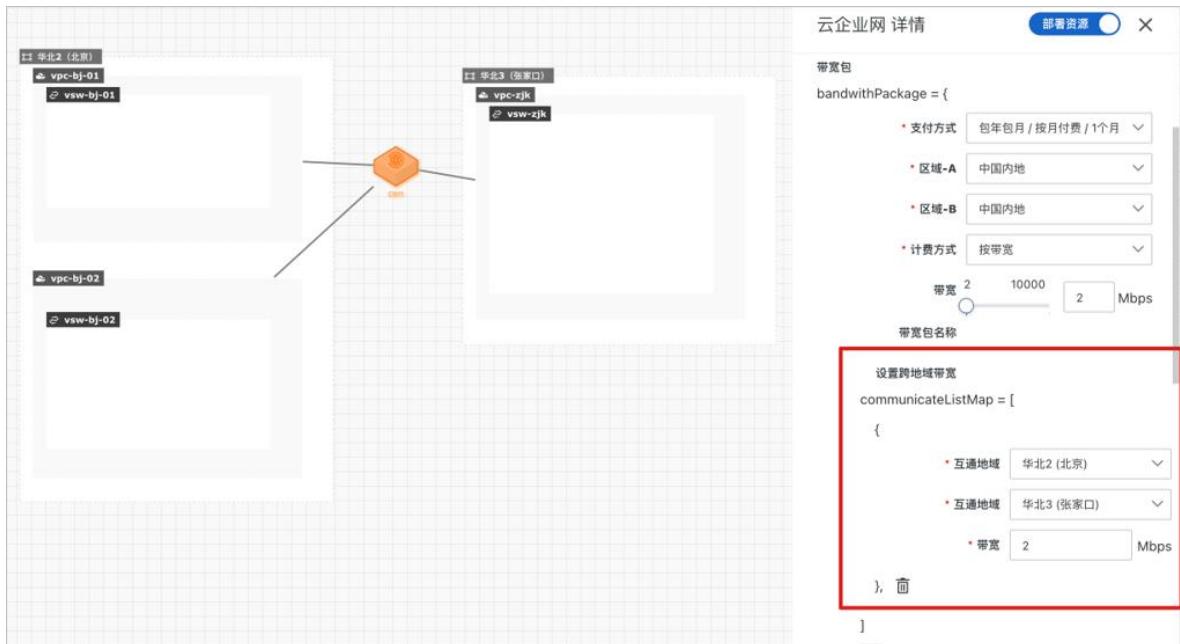
- 购买方式：新购
- 云企业网：cen 名称，此处按默认
- 带宽包：
  - 支付方式：包年包月/按月付费/1 个月
  - 区域-A：中国内地
  - 区域-B：中国内地
  - 计费方式：按带宽
  - 带宽：2Mbps（按实际需求填写）
  - 带宽包名称：（可选）



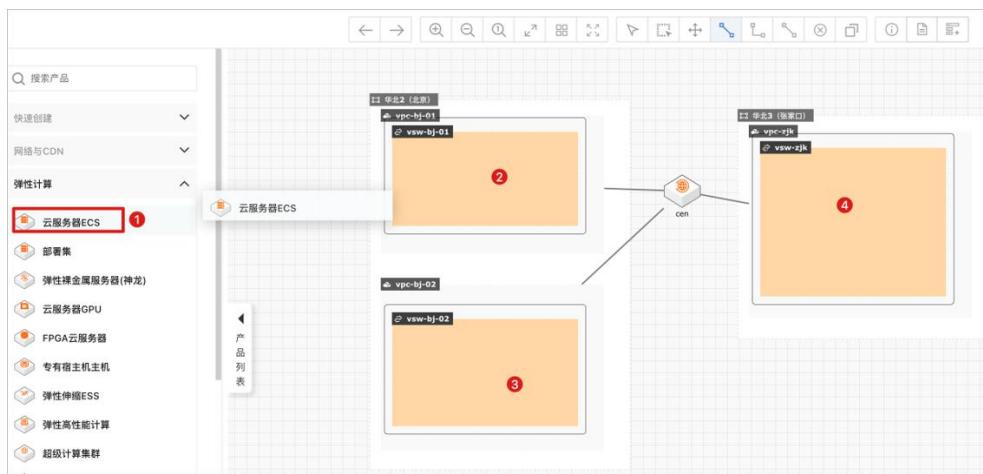
步骤 12 要实现跨地域网络实例互通，在购买带宽包后，您还需要设置跨地域互通带宽。

每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。

例如，一个此场景中的云企业网实例绑定了一个带宽值为 2Mbps，互通区域为中国内地和中国内地的带宽包。可以在该带宽包内设置华北 2 到华北 3 地域的跨地域互通带宽，但所有跨地域互通带宽之和不大于 2Mbps。

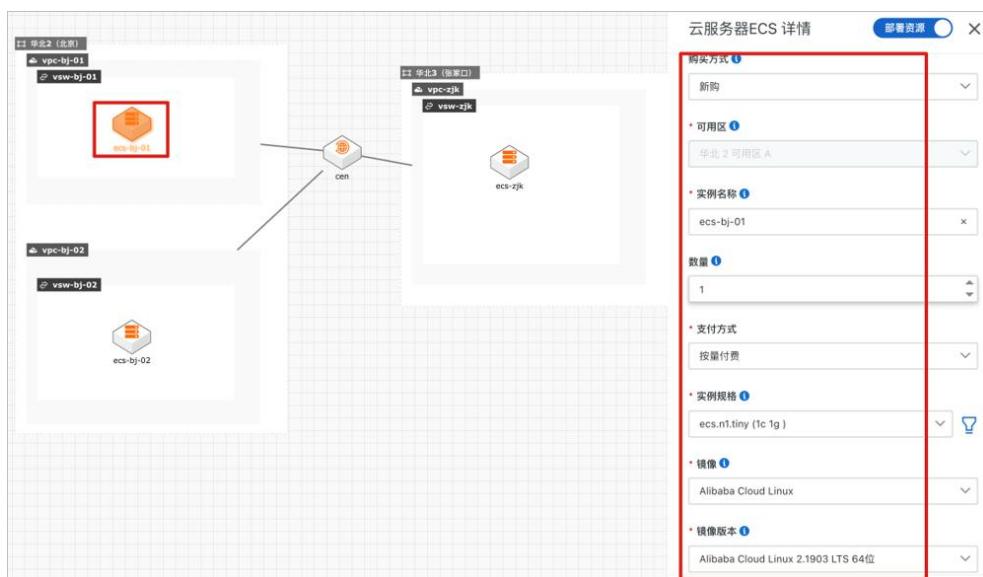


步骤 13 从左侧拖拽 ECS 到右侧三个交换机中。

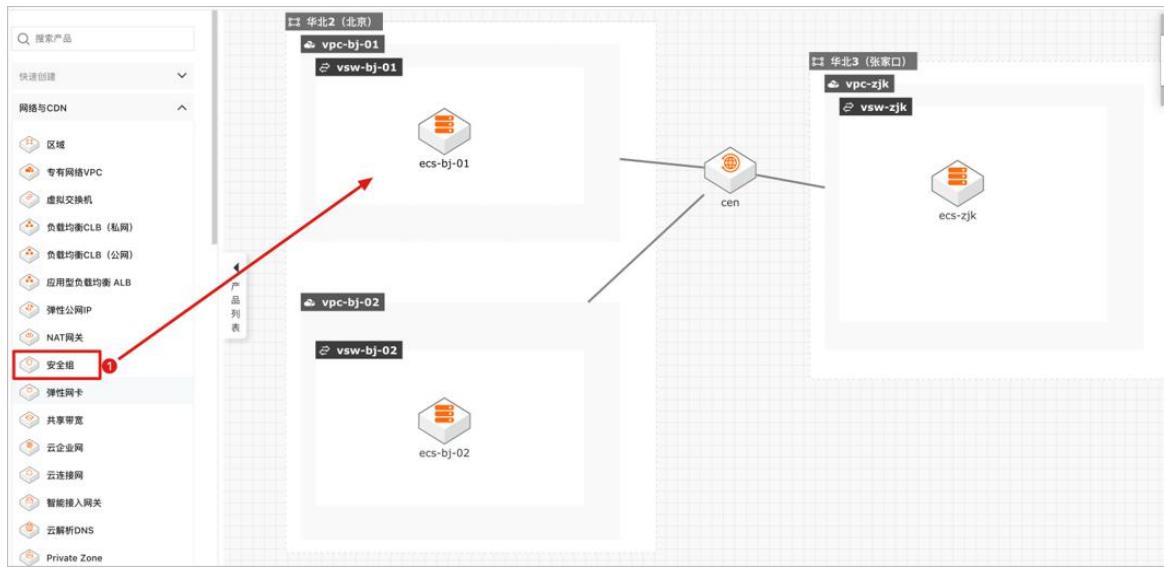


步骤 14 配置 ECS 的规格。

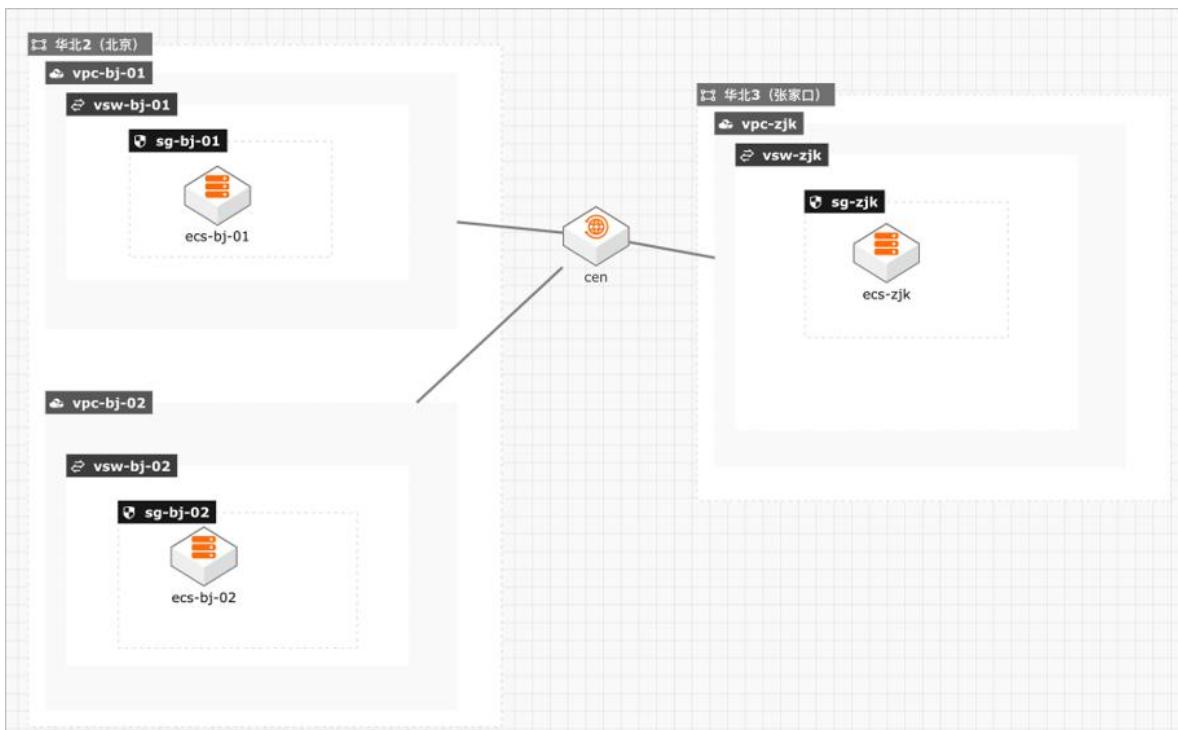
- 购买方式：新购
- 实例名称：ecs-bj-01
- 数量：1
- 支付方式：按量付费
- 实例规格：ecs.n1.tiny(1c 1g)
- 镜像：Alibaba Cloud Linux
- 镜像版本：Alibaba Cloud Linux 2.1903 LTS 64 位
- 系统盘类型：高效云盘
- 登录凭证：稍后创建



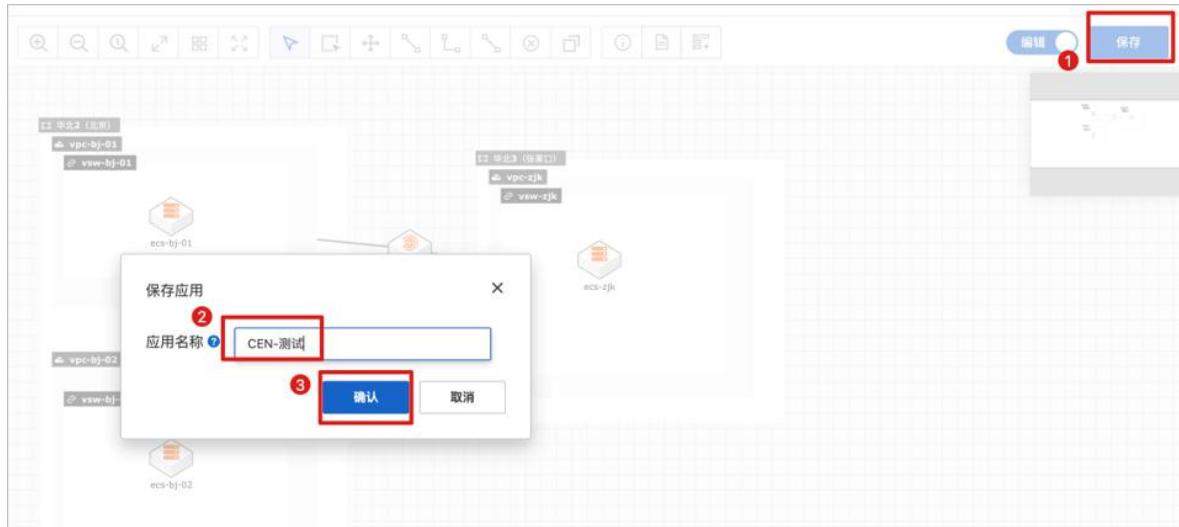
步骤 15 从左侧拖入安全组到每个 ECS 上。



步骤 16 配置安全组，输入名称，规则保持默认。

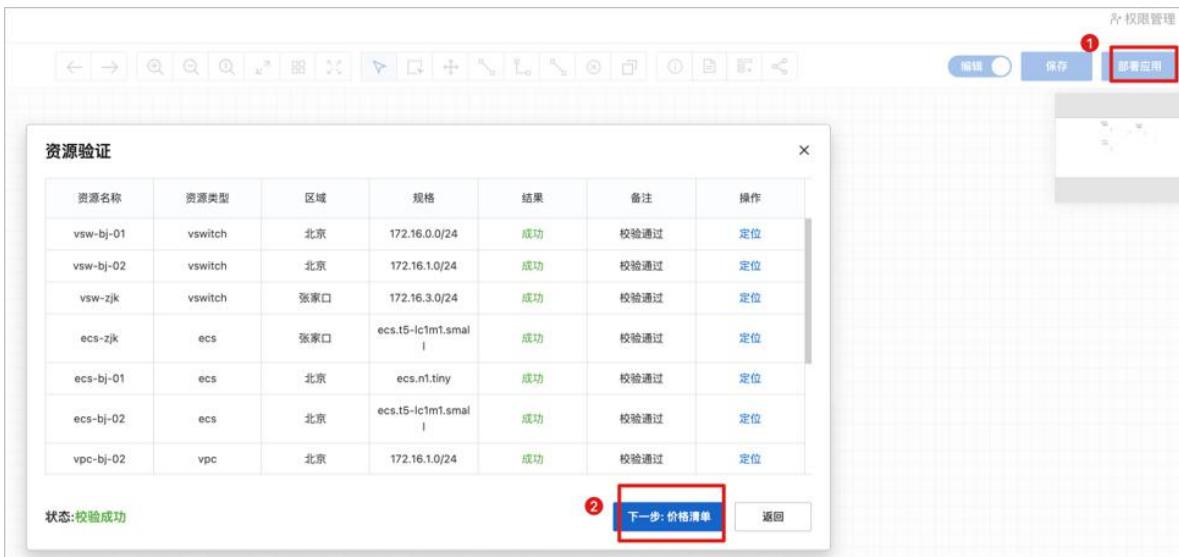


步骤 17 保存架构为应用。



### 3.8.3. 部署过程

步骤 18 保存后单击部署应用，系统将对资源配置进行校验。若校验成功，单击下一步：价格清单。



步骤 19 确认价格无误后，单击下一步：确认订单；可以单击查看报告得到一份报价清单。



步骤 20 勾选《云速搭服务条款》，确认价格后，单击下一步：支付并创建。

**确认订单**

免费 包年包月 按量付费

资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
cen	cen			1	1月	440.00元/月	340 元/月	新购

《云速搭服务条款》  
部署前，请阅读并勾选服务条款 ①

包年包月: 100 元 按量付费: 0.030元/时 ②

状态: 计价成功 上一步: 价格清单 下一步: 支付并创建

步骤 21 再次确认。



步骤 22 等待资源部署完成，部署过程为后台调用进程。



步骤 23 部署成功。



### 3.8.4.验证过程

步骤 1 展开应用下的资源清单，单击资源名称 cen，跳转到 CEN 控制台。



步骤 2 可以看到，CEN 实例加载了三个 VPC。

实例ID/名称	所属地域	实例类型	所属账号	加载时间	状态
vpc-2ze0s9lnkpq6dbqabzrb7 vpc-bj-01	华北2 (北京)	专有网络 (VPC)	1254528490571584	2021年10月21日17:51:00	● 已加载
vpc-2zekh85072poc0uz7macq vpc-bj-02	华北2 (北京)	专有网络 (VPC)	1254528490571584	2021年10月21日17:52:00	● 已加载
vpc-8vbd9tuometlxs2yjh5 vpc-zjk	华北3 (张家口)	专有网络 (VPC)	1254528490571584	2021年10月21日17:51:00	● 已加载

步骤3 单击带宽包管理，可以看到带宽包购买成功并已完成绑定。

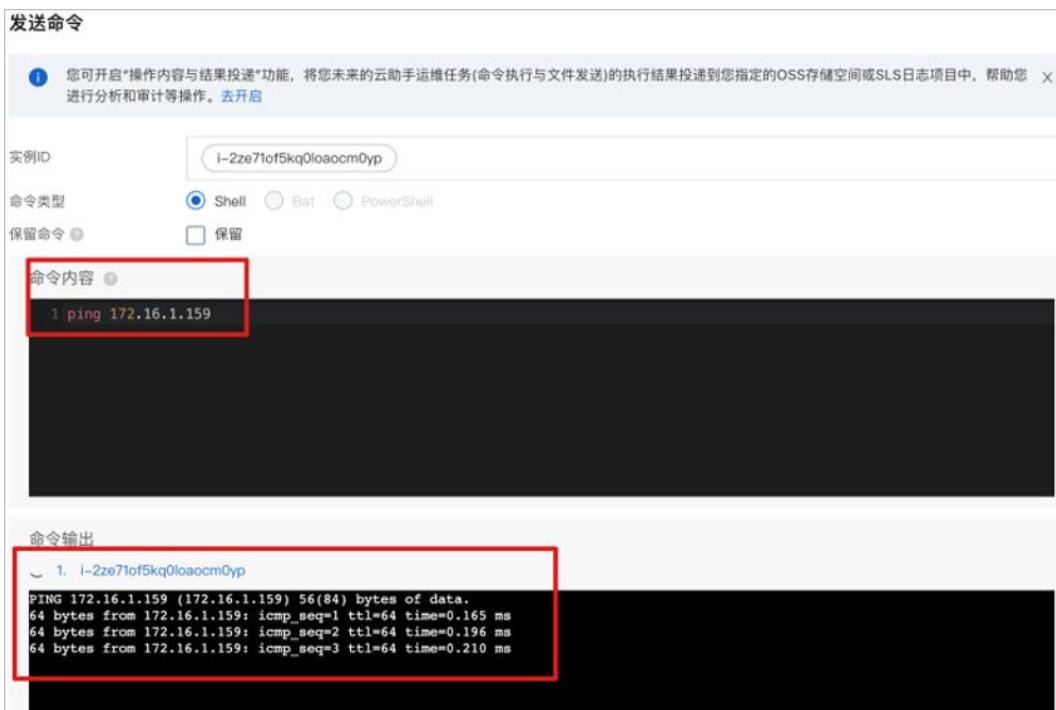
带宽包ID	标签	互通区域	带宽	已分配带宽	监控	付费类型	状态
cenbwp-o4rtclhvpa4k2g5dp5		中国内地=中国内地	2 Mbps 降配 升配	2 Mbps	预警设置	预付费 2021年11月22日00:00:00	已绑定 到期

步骤4 单击跨地域互通带宽管理，已正确设置。

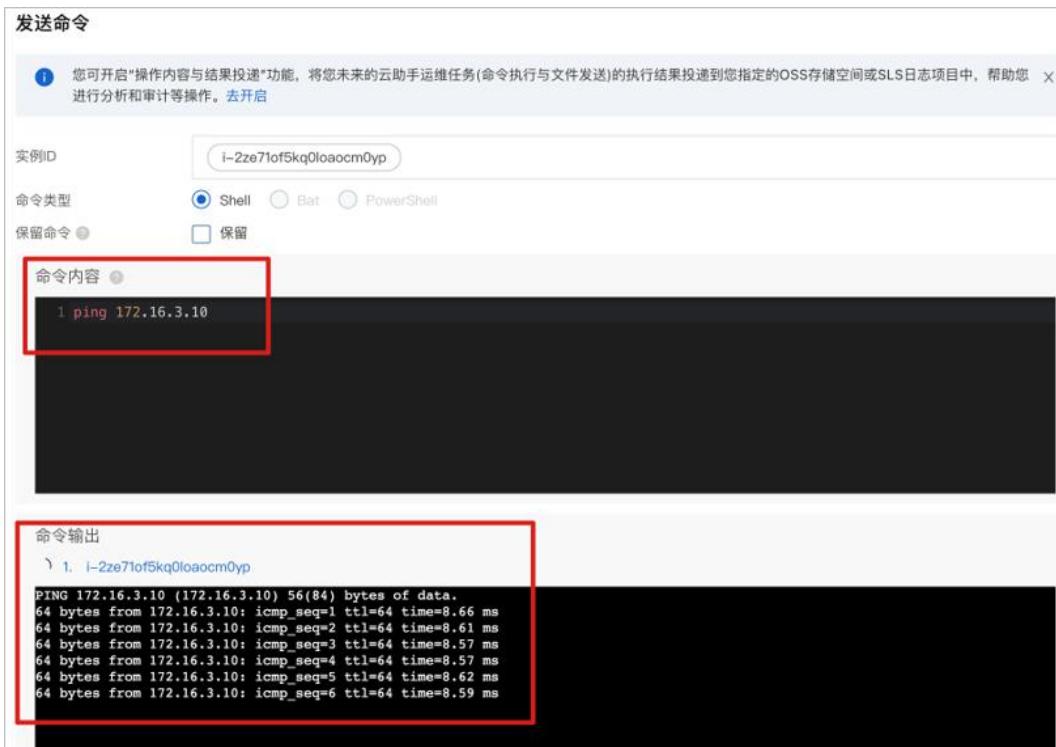
互通区域	监控	互通地域	带宽	状态
中国内地 (cenbwp-o4rtclhvpa4k2g5dp5)	预警设置	华北2 (北京) = 华北3 (张家口)	2 Mbps 修改	● 可用

步骤5 进入 ECS 控制台 <https://ecs.console.aliyun.com/#/server/region/cn-beijing>，记录 ECS IP 地址。

步骤 6 在 ecs-bj-01 上 ping ecs-bj-02 的 IP 地址，得到如下结果。说明 VPC 之间网络已经互通。



步骤 7 继续验证 ecs-bj-01 到 ecs-zjk



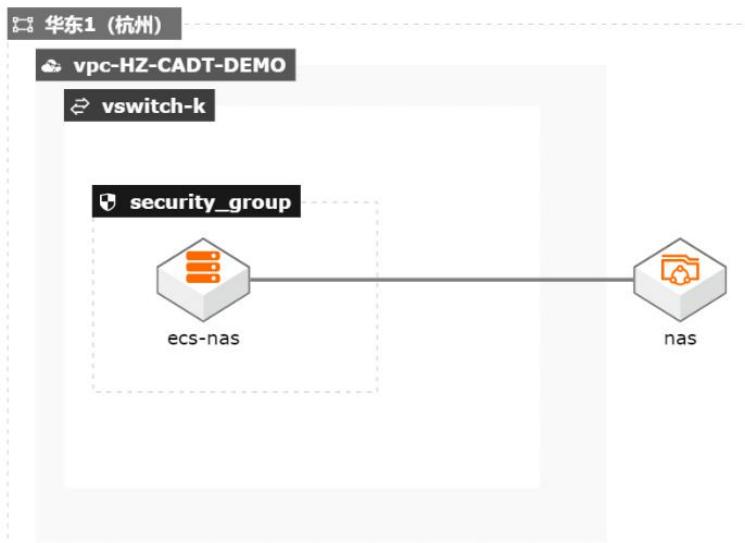
## 3.9.云速搭部署 NAS 文件系统

作者 | 阿里云解决方案架构师 浩谦

### 3.9.1.云速搭架构设计

#### 方案架构

- 通过云速搭构建一个 NAS，并将 NAS 文件系统挂载到 ECS 的目录上。
- 具备一个安全组，通过安全组对 ECS 进行详细的安全策略配置。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
ECS	VSW
NAS	Region
安全组	VPC

## 资源规划清单

资源类别	配置项	配置明细	说明
区域	区域	华东 1 (杭州)	本最佳实践全部资源部署在杭州 (主数据中心)
专有网络 VPC	状态	新购 (根据实际情况选择新购或已保有, 本最佳实践新购 VPC)	云上选择专有网络 (VPC) 以保障安全性。 选择离原系统公网 IP 近的云上区域减少网络延迟。
	VPC 名	vpc-HZ-CADT-DEMO	选择资源丰富、离用户近的区域保障项目顺利实施。
	网段	172.10.0.0/16	网络规划留足可用 IP 数即可。
虚拟交换机	状态	新购 (根据实际情况选择新购或已保有, 本最佳实践新购交换机)	
	vswitch 名	vswitch-k	
	可用区	华东 1 可用区 K	
	IPv4 网段	172.10.3.0/24	
ECS	可用区	默认 (华东 1 可用区 K)	ECS 创建在 vswitch-k 下, 无需选择。
	ECS 名	ecs-nas	
	主机名	ecs-nas	
	支付方式	后付费	按量付费
	实例规格	4 核 CPU, 16GB 内存 (ecs.g6.xlarge)	云上业务系统规格按照原规格购买。
	镜像	CentOS	
	镜像版本	CentOS 7.6 64 位	
	系统盘	cloud_ssd	ESSD 云盘
	硬盘容量	40GiB	
	公网带宽	按流量付费	
	出网带宽	10	分配公网 IP

资源类别	配置项	配置明细	说明
ECS	登录密码	*****	初始 root 用户密码，创建成功后由业务方分别登录修改密码。
	安全加固	Active	
NAS	NAS 名称	nas	
	支付方式	按量付费	
	可用区	华东 1 可用区 K	NAS 创建在 vswitch-k 下，无需选择。
	存储规格	容量型	
	协议类型	nfs	
	是否加密	不加密	

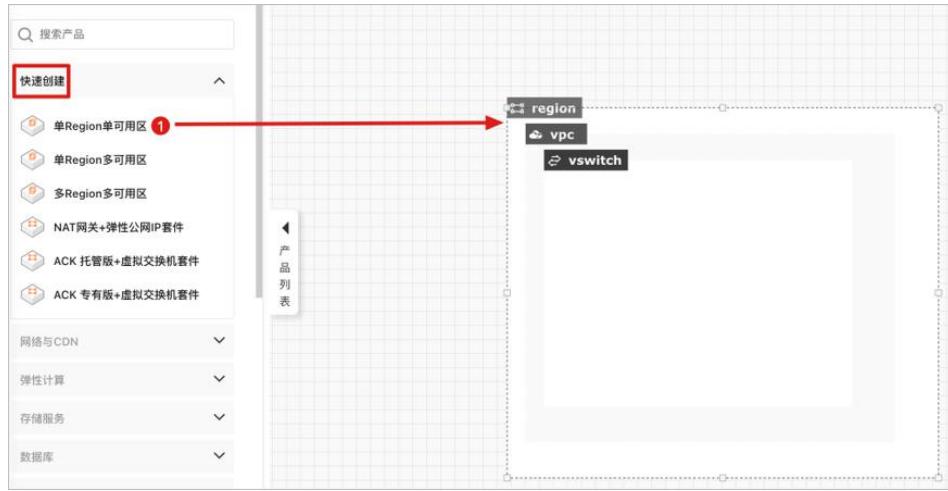
### 3.9.2.通过云速搭 CADT 部署资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录 CADT 控制台。如果提示需要开通服务，请根据提示进行开通。

步骤 2 单击新建 > 新建空白应用。



步骤 3 从左侧**快速创建**下选择“单 Region 单可用区”模板到右侧画布区域。



步骤 4 分别双击 region、vpc、vswitch 进行设置。

- 配置 region：



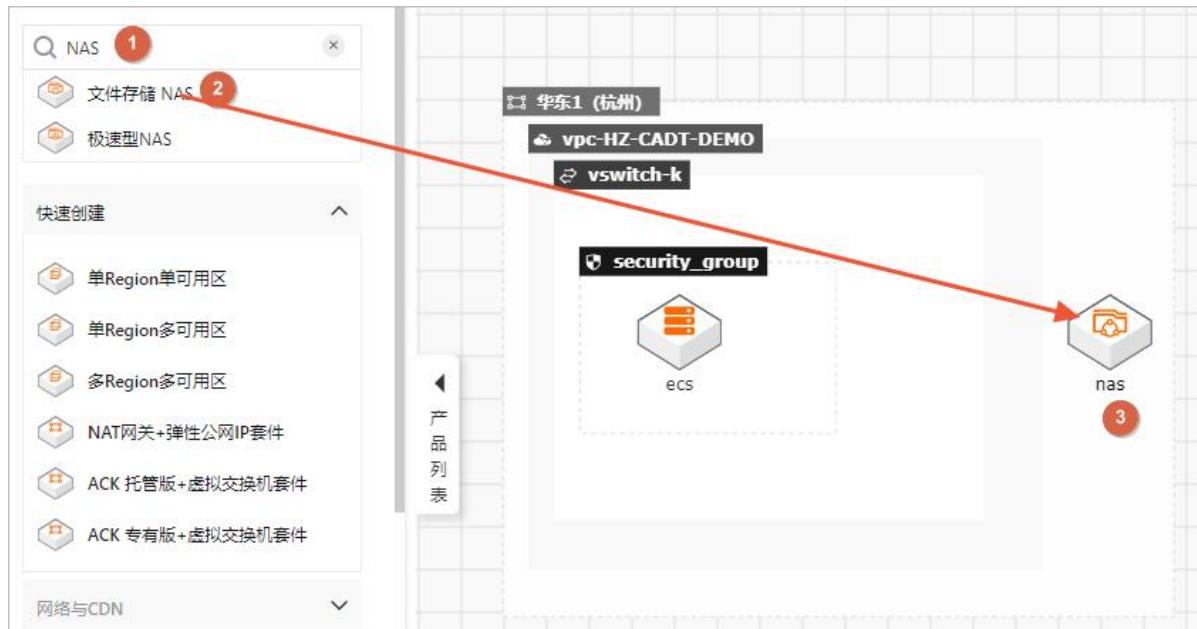
- 配置 vpc：



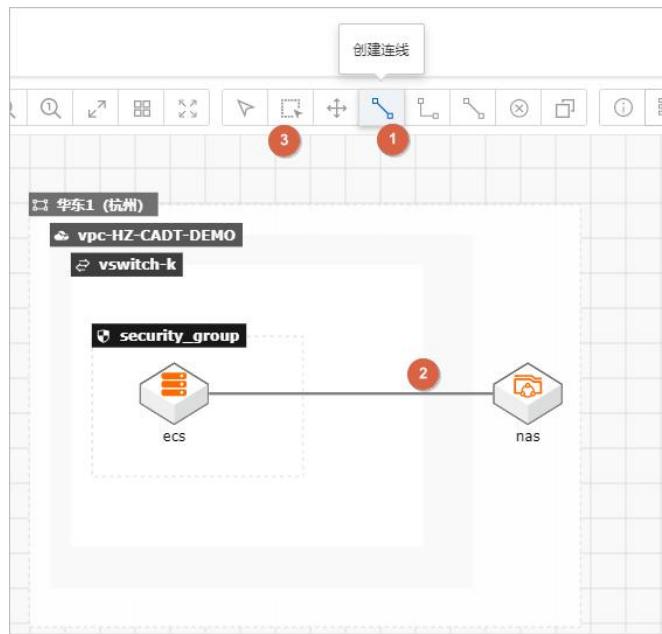
- 配置 vswitch:



步骤 5 在画布区域调整 region、vpc、vswitch 图层到合适大小后，分别从左侧产品列表中选择安全组、ECS、NAS 拖入对应区域中（参考[理解资源级别](#)，根据架构资源级别设计）。

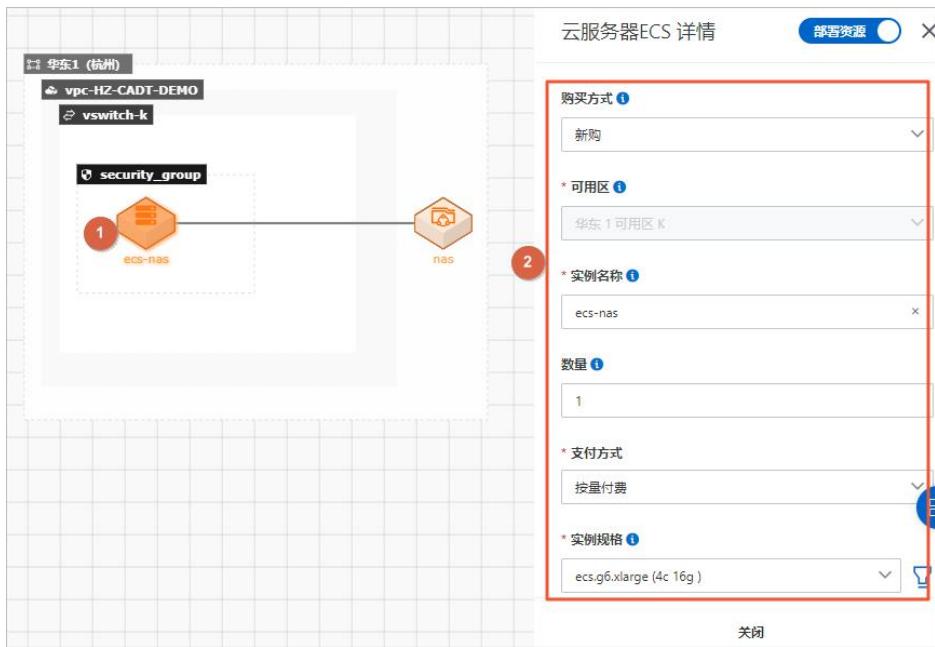


步骤 6 单击**创建连线**按钮，将 NAS 与 ECS 连接在一起。创建完连线后，切换为**默认模式**。

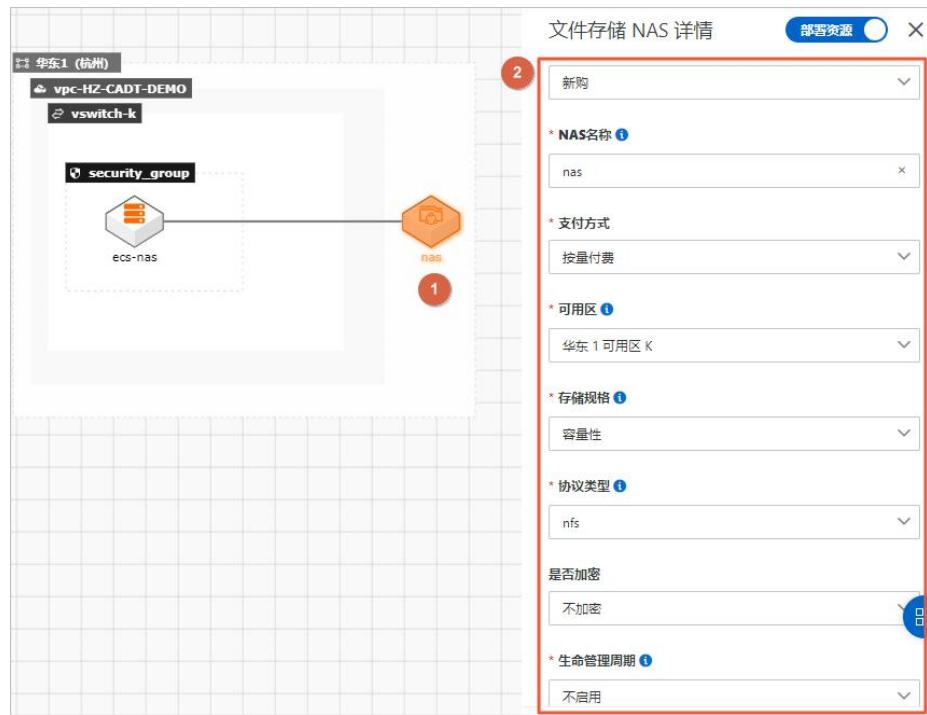


步骤 7 双击 ECS，配置资源规格：

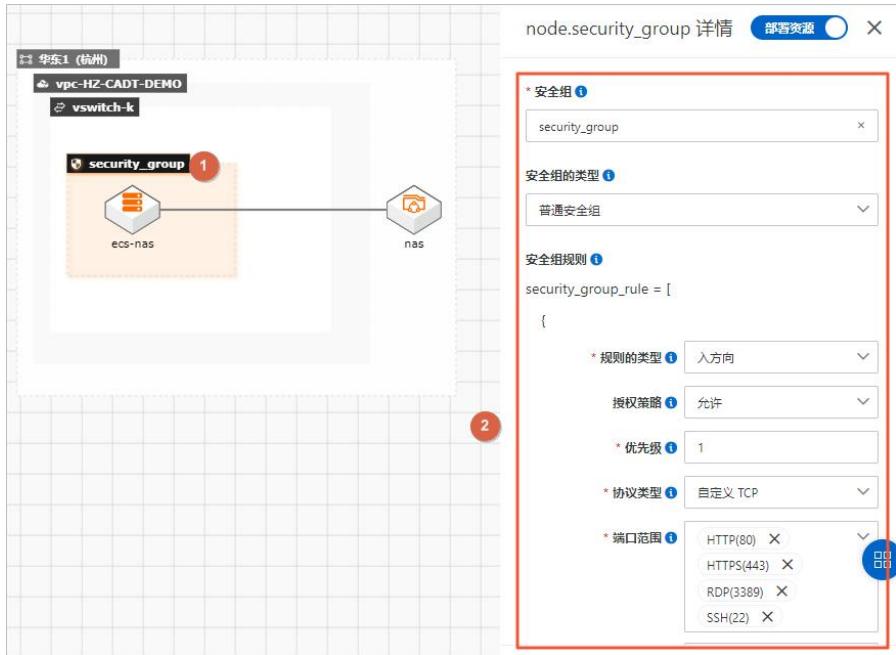
配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs-nas
支付方式	按量付费
实例规格	ecs.g6.xlarge(4c 16g)
镜像	CentOS
镜像版本	CentOS 7.6 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
公网 IP	分配公网 IPv4 地址
宽带计费模式	按流量付费
带宽 (峰) 值	10 Mbps
主机名	ecs-nas
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>



步骤 8 双击 NAS，配置资源规格：



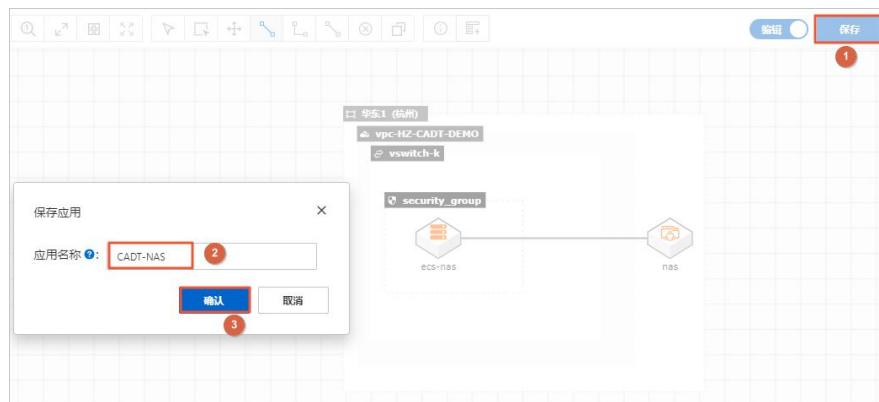
步骤 9 双击安全组，配置安全组策略，放行 22、80、443 端口。



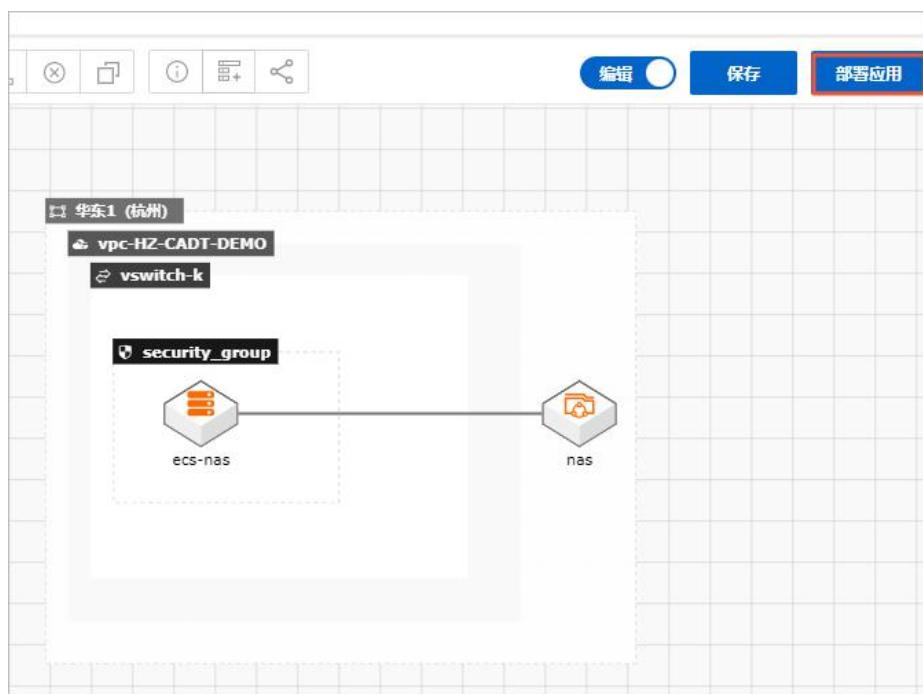
步骤 10 双击 ECS 与 NAS 之间连线，配置权限组：



步骤 11 配置完成后，单击右上角的**保存**按钮，输入应用名称后，单击**确认**。



步骤 12 保存完成后，单击**部署应用**。



步骤 13 等待资源验证成功，单击**下一步：价格清单**。

资源名称	资源类型	区域	规格	结果	备注	操作
nas	nas	杭州	hybrid	成功	校验通过	定位
vswitch-k	vswitch	杭州	172.16.3.0/24	成功	校验通过	定位
ecs-nas	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位

状态:校验成功

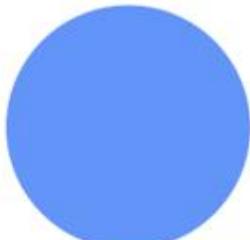
1 下一步: 价格清单 返回

步骤 14 显示计价成功后，单击**下一步：确认订单**。

**导出价格清单**

免费 按量付费 ×

资源成本占比



资源预算  
● 计算 计算: 0.00 元/时

100%

价格列表

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
ecs-nas	ecs	杭州	ecs.g6.xlarge	1				<a href="#">定位</a>
nas	nas	杭州	hybrid	1				<a href="#">定位</a>

状态: 计价成功

[上一步: 资源校验](#) 查看报告 ① [下一步: 确认订单](#)

步骤 15 核对订单无误后，勾选《云速搭服务条款》，单击**下一步：支付并创建**进行应用部署。

**确认订单**

免费 按量付费 ×

资源名称	资源类型	区域	规格	数量	原价	实付	状态
nas	nas	杭州	hybrid	1			<span style="color: green;">新购</span>
ecs-nas	ecs	杭州	ecs.g6.xlarge	1			<span style="color: green;">新购</span>

**《云速搭服务条款》** ①  
部署前，请阅读并勾选服务条款

按量付费:

状态: 计价成功

[上一步: 价格清单](#) ② [下一步: 支付并创建](#)

步骤 16 部署成功后可以查看报告。

资源部署状态

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
nas	nas	按量付费	Od4... 65	运行中	2021-10-25 10:26:20	定位
vswitch-k	vswitch	-	vsw-b... 5... zn	运行中	2021-10-25 10:26:49	定位
ecs-nas	ecs	按量付费	i-bp... k	运行中	2021-10-25 10:26:49	定位
security_group _alb_demo	security.group	-	sg-b... u	保有资源导入架构	-	定位
vpc-HZ-CADT-	vpc	-	vpc-h... atv	保有资源导入架构	-	定位

部署概要

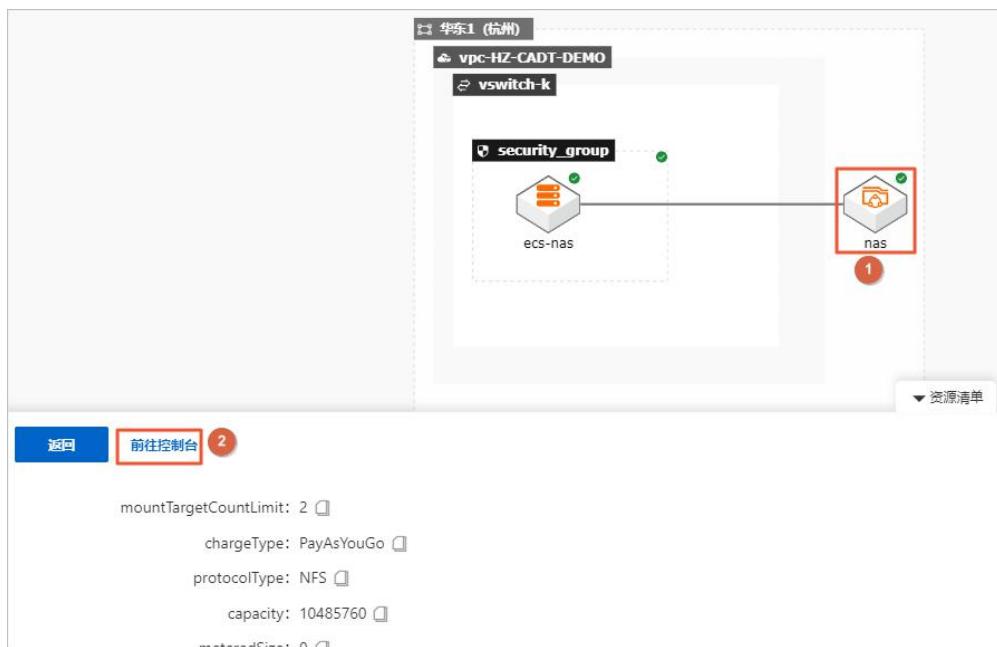
状态: 部署成功 方案编号: K...HV

[查看报告](#) [返回](#)



### 3.9.3.验证 ECS 挂载 NAS 文件系统

步骤 17 应用部署成功后，双击 NAS 实例，单击前往控制台。



步骤 18 挂载 NAS 文件系统到 ECS 实例。

1. 打开文件系统列表页面，单击新创建的文件系统 ID。

NAS文件系统		文件系统列表			
概览		NAS文件系统 / 文件系统列表			
文件系统					
文件系统	1	创建文件系统	文件系统类型: 全部	文件系统ID	请输入
权限组				标签	类型
new		文件系统 ID/名称			
资源包管理		0d...nas.j55	nas		通用型NAS
数据服务					NFS协议

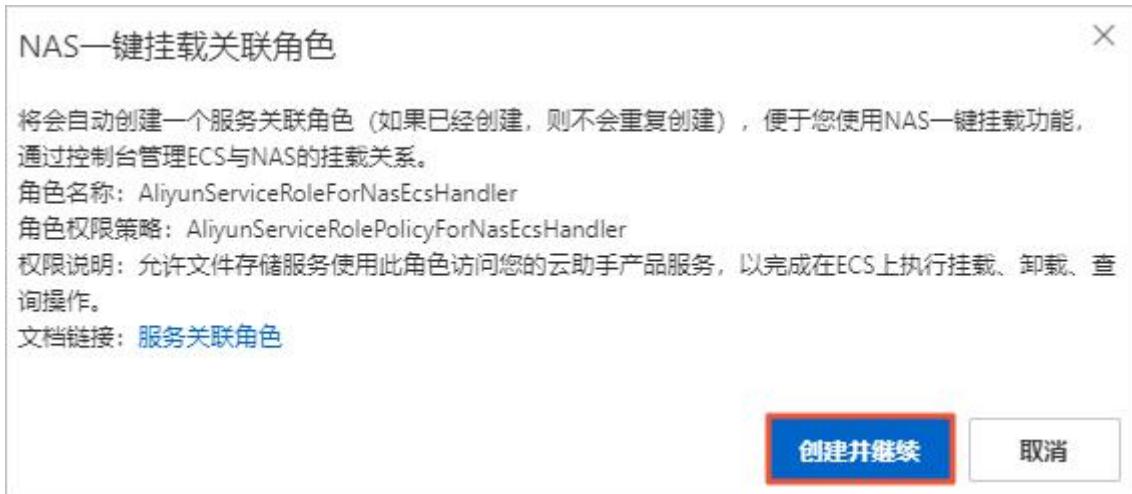
2. 在左侧选择挂载使用，在挂载点操作列下，单击挂载。

基本信息		挂载点								
挂载使用		添加挂载点								
访问控制		序号	类型	专有网络VPC	虚拟交换机VSW	交换机可用区	挂载点地址	状态	权限组	操作
配额管理	1	1	专有网络	vpc-bp1o1yxka6vqs8l0g4f	vsw-vp1o1yxka6vqs8l0g4f	华东1 可用区K	ecs_nas	可用		挂载   卸载   查询   客户端修改权限组   禁用   删除

3. ECS 实例里选择刚创建的 ECS 实例 “ecs-nas”，挂载路径输入 /mnt。



如果提示需要创建 NAS 一键挂载关联角色，单击**创建并继续**即可。



4. 等待挂载状态变为已挂载，即完成了 NAS 文件系统的挂载。

挂载点						
添加挂载点						
序号	类型	专有网络VPC	虚拟交换机VSW	交换机可用区	挂载点地址	状态
1	专有 网络	vpc- bp119rviancoxudlsogh vpc-HZ-CADT-DEMO	vsw- bp1o1yxsk6vqs8i80g4f vswitch-k	华东1可用区 K		可用
实例ID/名称		i-bp1cw5y5uvwkxlbluk7h/ecs-nas				
ECS ID	i-bp1cw5y5uvwkxlbluk7h				名称	ecs-nas
IP地址	172.16.3.41 (私有) / 121.40.119.28 (公网)				可用区	华东1可用区
挂载状态	挂载路径	NAS目录	自动挂载	协议类型	挂载参数	
	/mnt	/	on	NFSv3	rw,relatim	

步骤 19 NAS 文件系统挂载验证。

登录 ECS 服务器，执行：

```
df -h
```

文件系统	容量	已用	可用	已用%	挂载点
/dev/vda1	40G	2.1G	36G	6%	/
devtmpfs	7.7G	0	7.7G	0%	/dev
tmpfs	7.7G	0	7.7G	0%	/dev/shm
tmpfs	7.7G	480K	7.7G	1%	/run
tmpfs	7.7G	0	7.7G	0%	/sys/fs/c
group					
tmpfs	1.6G	0	1.6G	0%	/run/user
/0					
0d4...5-aet4.cn-hangzhou.nas.aliyuncs.com:/	10P	0	10P	0%	/mnt

查看挂载信息，可以看到 NAS 文件系统已经挂载到/mnt 上。

## 3.10.云速搭部署混合云备份 HBR

作者 | 阿里云解决方案架构师 厉博

### 3.10.1.云速搭架构设计入门

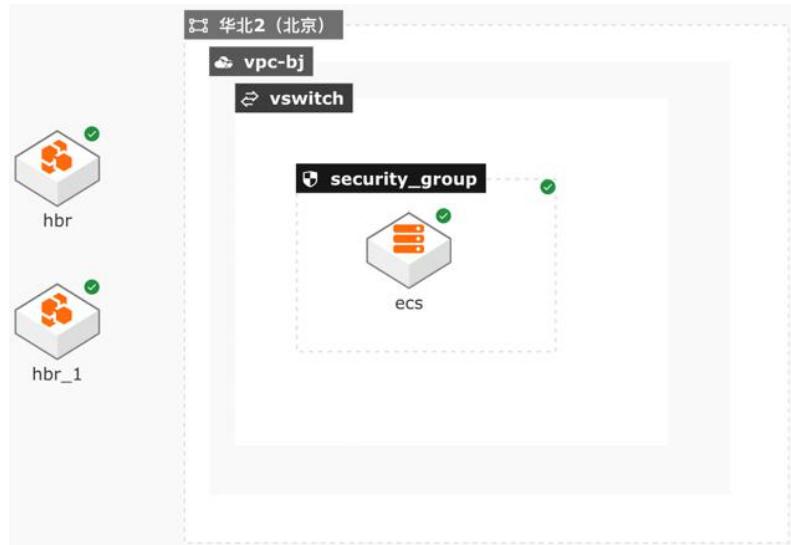
#### 方案架构

混合云备份 HBR (Hybrid Backup Recovery) 作为阿里云统一灾备平台，是一种简单易用、敏捷高效、安全可靠的公共云数据管理服务，可以为阿里云 ECS 整机、ECS 数据库、文件系统、NAS、OSS 以及自建机房内的文件、数据库、虚拟机、大规模 NAS 等提供备份、容灾保护以及策略化归档管理。

产品架构如下图所示：



本实践以 ECS 文件备份为例，通过 CADT 设计备份架构，并一键部署演示环境。Demo 架构如下图所示：



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

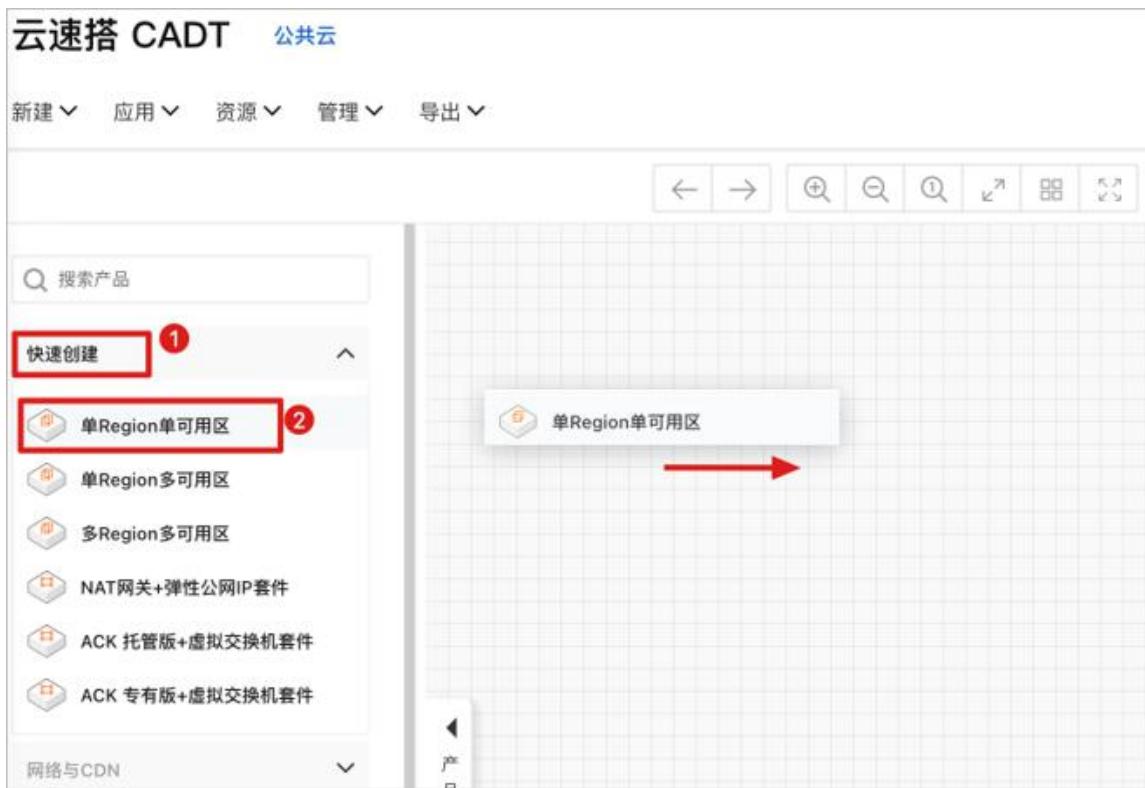
云资源	架构级别
VPC	Region 地域
HBR	全局资源
ECS	vswitch 交换机
安全组	VPC 专有网络

### 3.10.2.设计过程

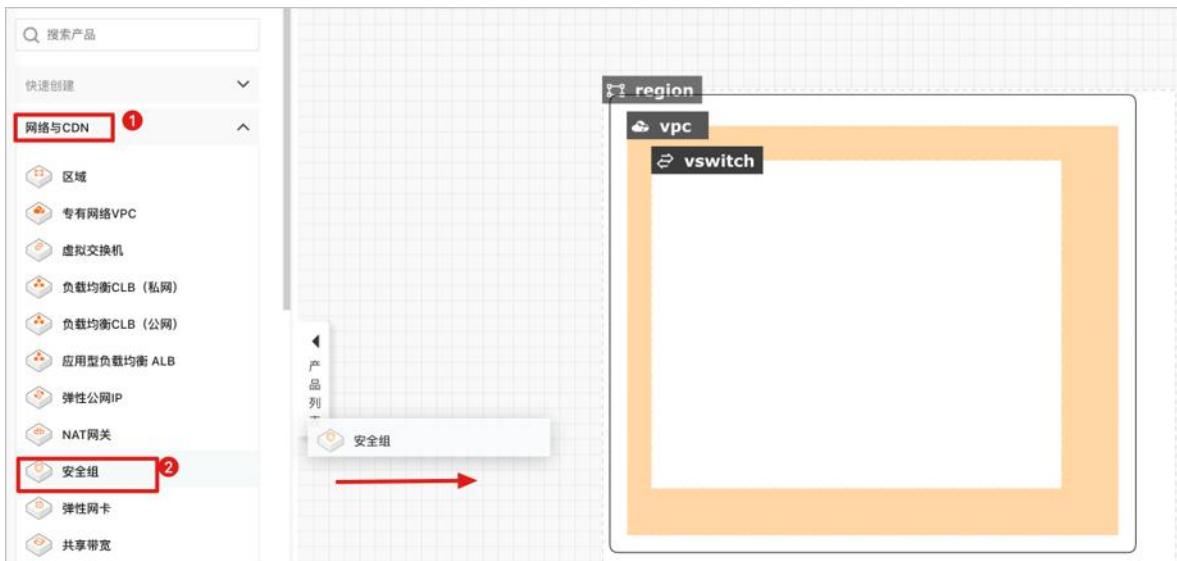
步骤 1 在云速搭 CADT 控制台单击新建 > 新建空白应用。



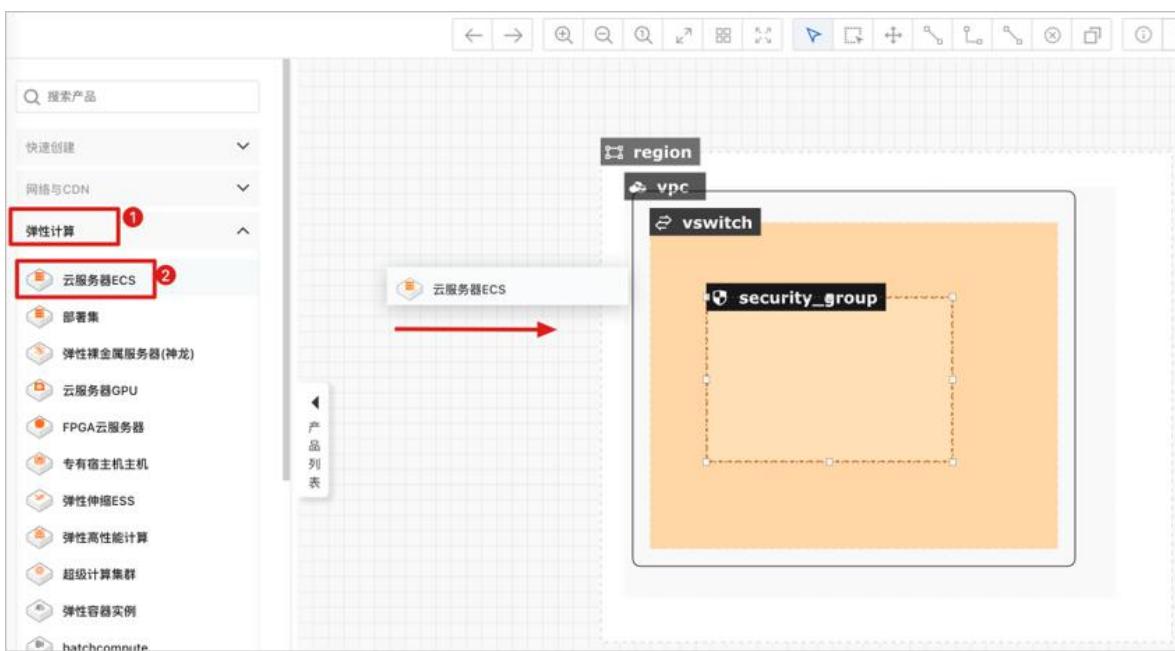
步骤 2 在左侧产品列表的**快速创建**下，拖动一个“单 Region 单可用区”模板到右侧画板中。



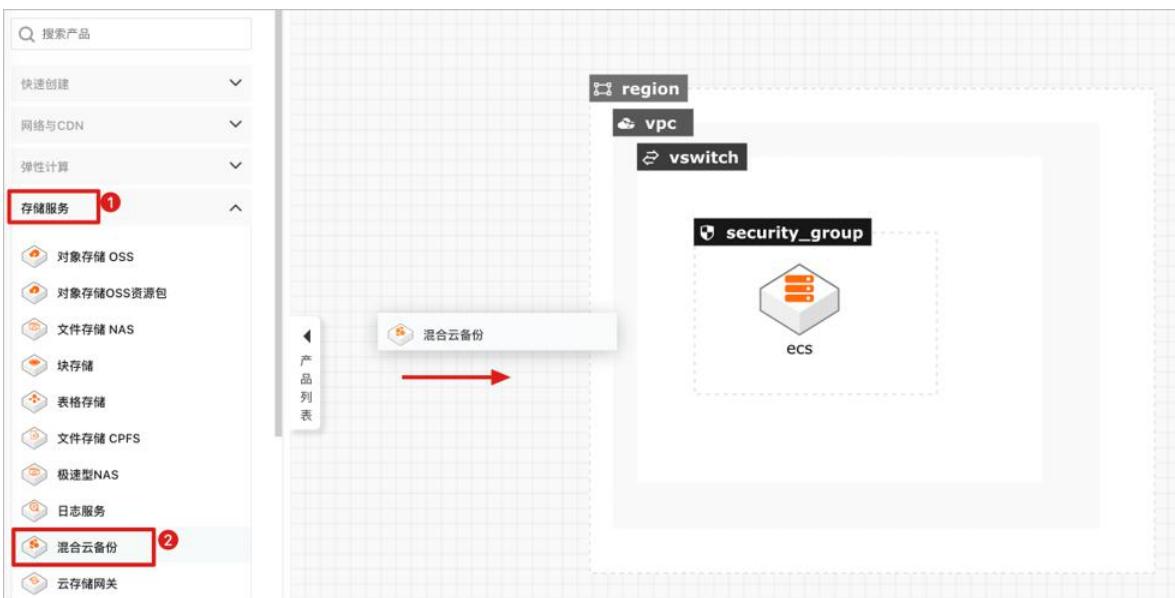
步骤 3 添加一个安全组到右侧画板高亮处，高亮处表示安全组是 VPC 级别的资源。



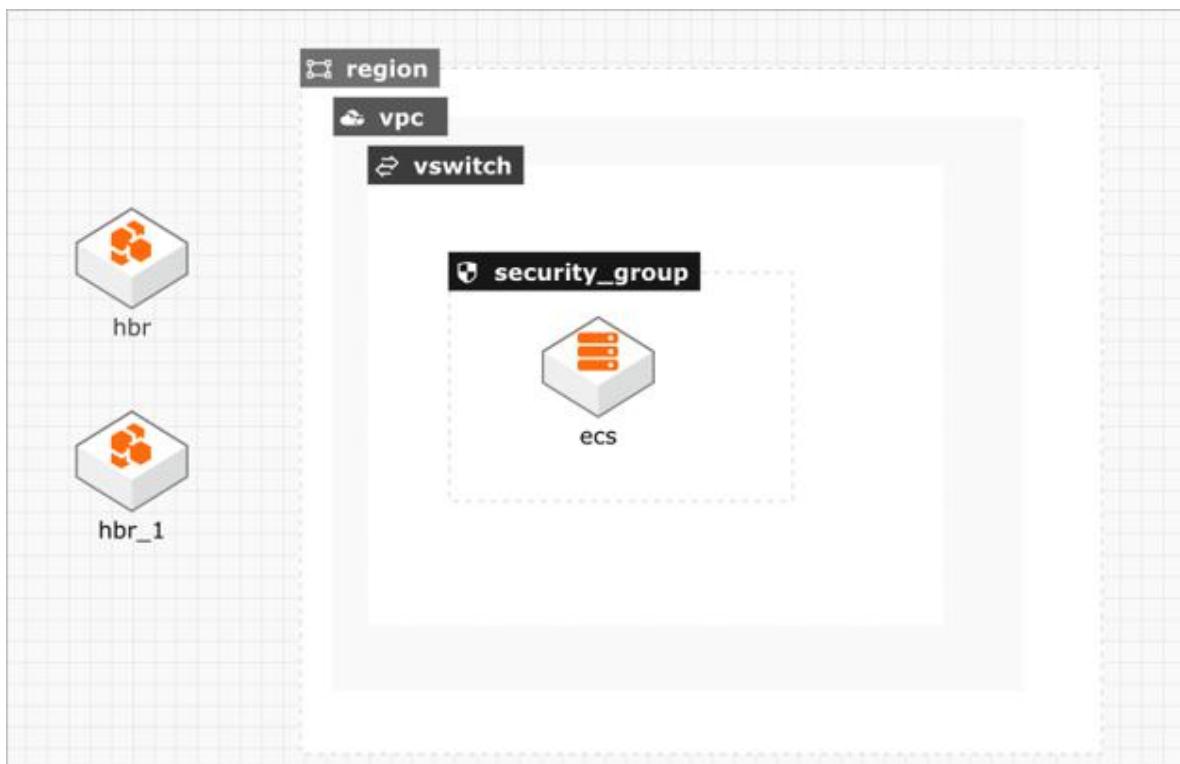
步骤 4 添加一个 ECS 到右侧画板的安全组内。



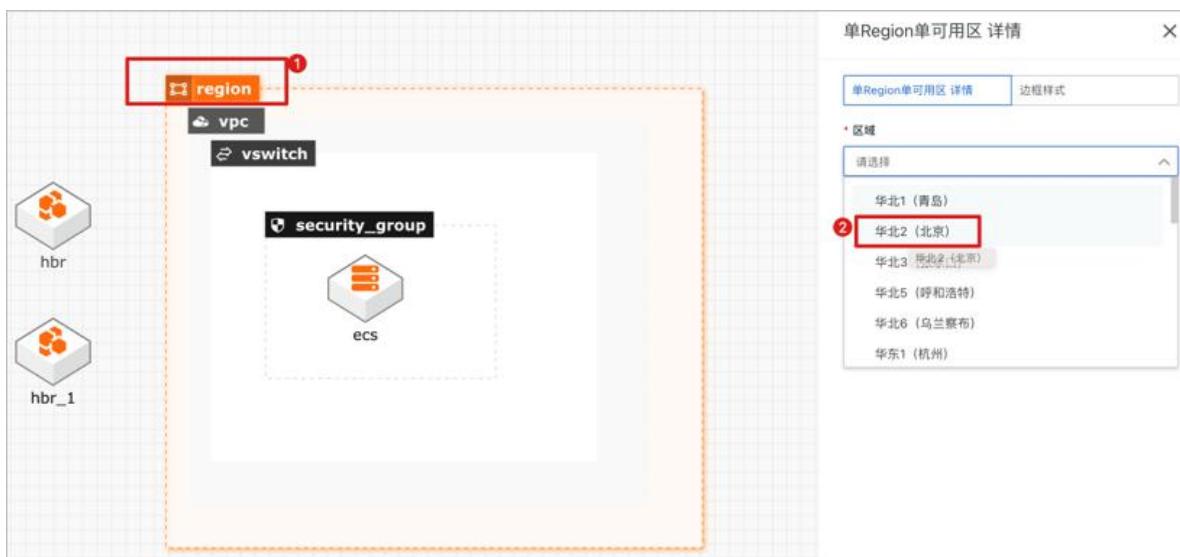
步骤 5 以同样方式，添加两个混合云备份到右侧画板中。



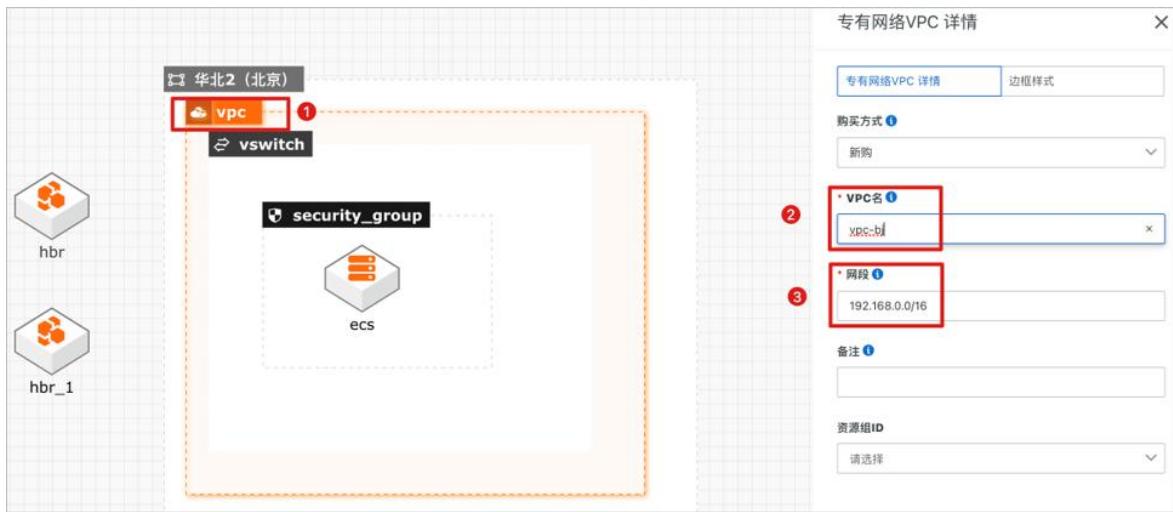
步骤 6 得到架构如下图所示：



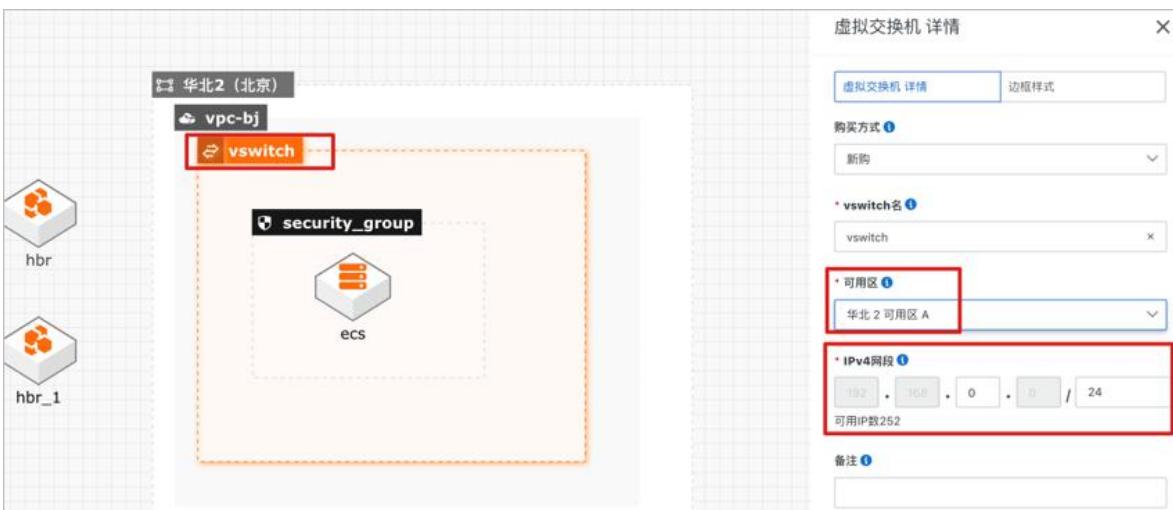
步骤 7 单击架构图中的 region，设置为“华北 2（北京）”。



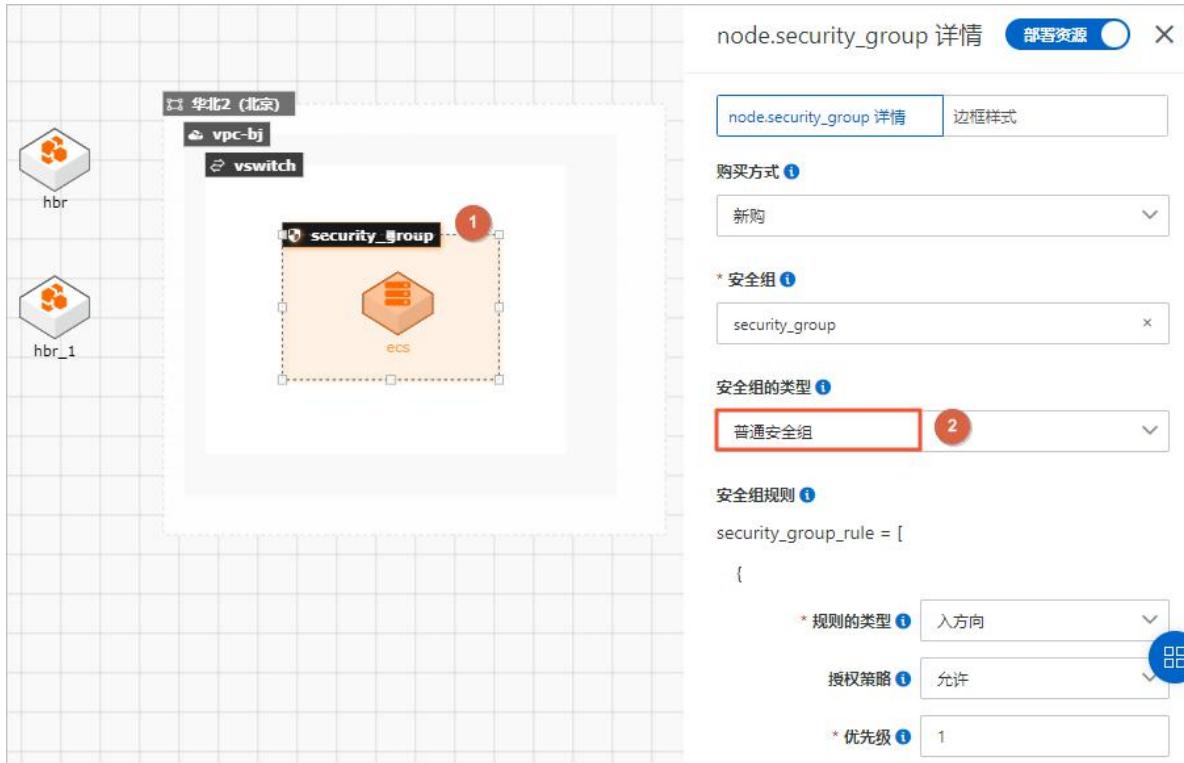
步骤 8 单击 VPC，设置 VPC 名 (vpc-bj) 以及网段 (192.168.0.0/16)。



步骤 9 单击 vswitch，设置交换机网段为“192.168.0.0/24”，可用区选择“华北 2 可用区 A”。

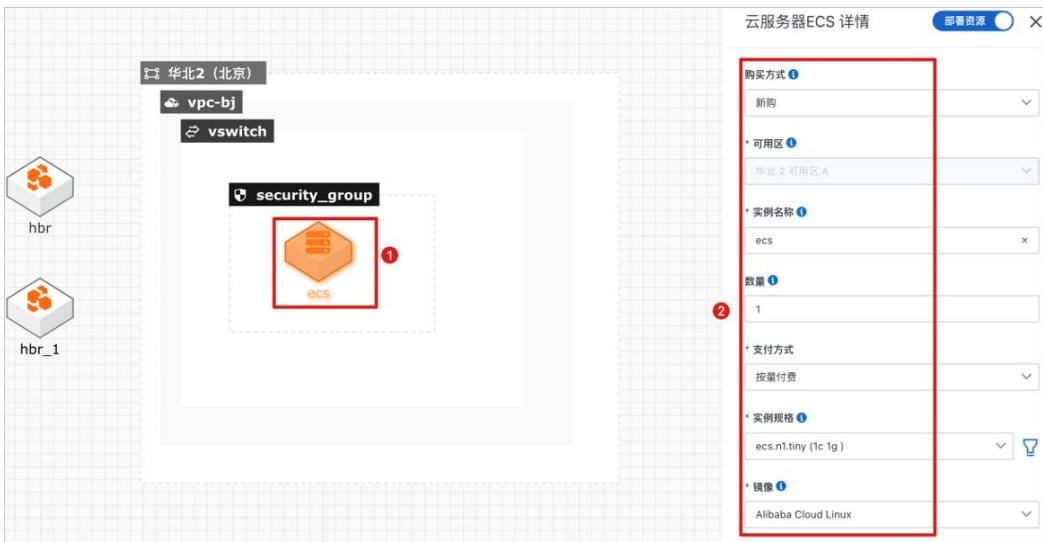


步骤 10 单击安全组，选择安全组类型为普通安全组，其他配置保持默认。



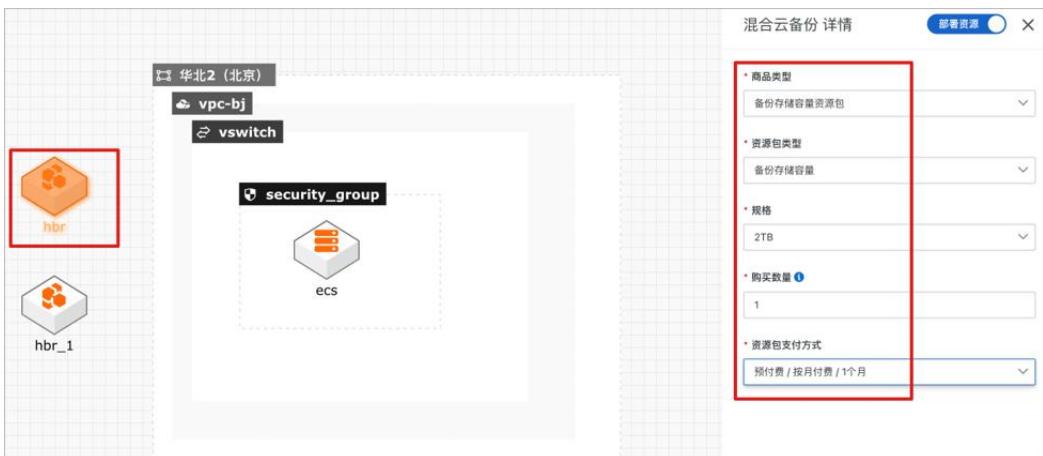
步骤 11 单击 ECS，配置 ECS 的规格。

- 购买方式：新购
- 实例名称：ecs-bj-01
- 数量：1
- 支付方式：按量付费
- 实例规格：ecs.n1.tiny(1c 1g)
- 镜像：Alibaba Cloud Linux
- 镜像版本：Alibaba Cloud Linux 2.1903 LTS 64 位
- 系统盘类型：高效云盘
- 登录凭证：稍后创建



步骤 12 单击 hbr，设置混合云备份的存储容量包。

- 商品类型：备份存储容量资源包
- 资源包类型：备份存储容量
- 规格：2TB
- 购买数量：1
- 资源包支付方式：预付费/按月付费/1 个月

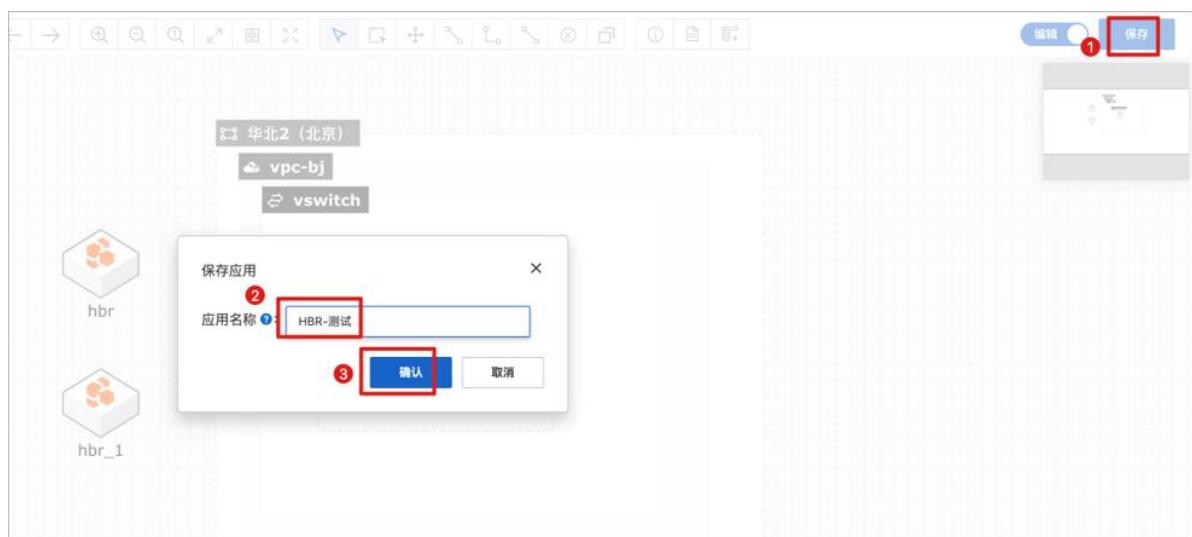


步骤 13 单击 hbr\_1，设置文件备份客户端。

- 商品类型：文件备份软件资源包
- 资源包类型：文件备份软件
- 规格：1 个客户端
- 购买数量：1
- 资源包支付方式：预付费/按月付费/1 个月



步骤 14 保存架构。



### 3.10.3.部署过程

步骤 15 保存后单击**部署应用**，系统将对资源配置进行校验。



校验成功，单击**下一步：价格清单**。

资源验证						
资源名称	资源类型	区域	规格	结果	备注	操作
vswitch	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
ecs	ecs	北京	ecs.n1.tiny	成功	校验通过	定位
vpc-bj	vpc	北京	192.168.0.0/16	成功	校验通过	定位
hbr	hbr		FPT_hbr_backups storage_bag_absolute_1583828157	成功	校验通过	定位
hbr_1	hbr		FPT_hbr_filelic_b ag_absolute_158 5915869	成功	校验通过	定位
security_group	security.group	北京		成功	校验通过	定位

状态:校验成功

**下一步：价格清单** **返回**

步骤 16 确认价格无误后，单击**下一步：确认订单**。

**说明：**可以单击**查看报告**得到一份报价清单。

**导出价格清单**

免费 包年包月 按量付费

资源成本占比

资源预算  
● 云 云: 119元

100%

价格列表

资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
hbr	hbr		kupstorage_bag_absolute_1583828157	1	1月	545.59元/月	省 119元/月	426.59元/月	定位
hbr	hbr		FPT_hbr_filelic_bag_absolute_1585915869	1	1月	45.00元/月	省 119元/月	45.00元/月	定位

状态: 计价成功

上一步: 资源校验 查看报告 下一步: 确认订单

步骤 17 勾选《云速搭服务条款》，确认价格后，单击下一步：支付并创建。

**确认订单**

免费 包年包月 按量付费

资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
	hbr		FPT_hbr_filelic_bag_absolute_1585915869	1	1月	45.00元/月	45.00元/月	新购
	hbr		FPT_hbr_backupstorage_bag_absolute_1583828157	1	1月	545.59元/月	545.59元/月	新购

《云速搭服务条款》 ①  
部署前，请阅读并勾选服务条款

包年包月: 119元 按量付费: 45元/时 ②

状态: 计价成功 上一步: 价格清单 下一步: 支付并创建

步骤 18 再次确认。

资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
	hbr		FPT_hbr_filelic_bag_absolute_1585915869	1	1月	45.00元/月	45.00元/月	新购
	hbr		FPT_hbr_backupstorage_bag_absolute_1583828157	1	1月	545.59元/月	545.59元/月	新购

《云速搭服务条款》  
部署前, 请阅读并勾选服务条款

包年包月: **45.00 元** 按量付费: **545.59 元/时**

状态: **计价成功**

您创建的应用中包含如下包年包月资源:  
hbr  
这些资源未到期前无法进行释放, 请确认!

**确认** **取消**

**上一步: 价格清单** **下一步: 支付并创建**

步骤 19 等待资源部署完成, 部署过程为后台调用进程。

华北2 (北京)

vpc-bj

资源部署状态

部署中, 不要进行任何操作, 请耐心等待...

部署摘要

状态: 部署中 方案编号: T2E8HK5A31B2H2P3

返回

hbr\_1

步骤 20 部署成功。

**资源部署状态**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
hbr_1	hbr	包年包月	HBR_FILELIC_BAG-cn-zvp2ejiat0002t	运行中	2021-10-22 08:59:19	定位
vpc-bj	vpc	-	vpc-2zer0wploit0636yjmqh8	运行中	2021-10-22 09:00:00	定位
vswitch	vswitch	-	vsw-2ze3yssjhhlz4thviosn	运行中	2021-10-22 09:00:01	定位
security_group	security.group	-	sg-2ze2su0gt8ghwzpjw6z1	运行中	2021-10-22 09:00:01	定位
ecs	ecs	按量付费	i-2ze65movyg2au2273gul	运行中	2021-10-22 09:00:56	定位

**部署概要**

状态: 部署成功 订单编号 : 211233829070125, 211234027640125  
方案编号: T2E8HK5A31B2H2P3

[查看报告](#) [返回](#)

### 3.10.4.验证过程

步骤 21 单击展开应用下面的**资源清单**, 然后单击资源名称 hbr, 跳转到混合云备份 HBR 控制台。

**HBR-测试 部署成功**

**华北2 (北京)**

- vpc-bj
- vswitch
- security\_group
- ecs

**资源清单**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间
hbr	hbr	包年包月	HBR_BACKUPSTORAGE_BAG-cn-7mz2ejiat0003a	运行中	2021-10-22 08:59:19
hbr_1	hbr	包年包月	HBR_FILELIC_BAG-cn-zvp2ejiat0002t	运行中	2021-10-22 08:59:19
vpc-bj	vpc	-	vpc-2zer0wploit0636yjmqh8	运行中	2021-10-22 09:00:00

步骤 22 在资源包管理页面中可以看到备份存储容量资源包和文件备份软件已生效。

资源包类型	生效时间	过期时间	容量	状态
备份存储容量资源包	2021-10-26 11:07:47	2021-11-27 00:00:00	2 TB	有效
文件备份软件	2021-10-26 11:07:46	2021-11-27 00:00:00	1 个	有效

步骤 23 在左侧导航栏选择备份 > ECS 文件备份，安装客户端。

**说明：**首次使用按页面提示完成授权即可：

①混合云备份服务授权

将会自动创建一个服务关联角色（如果已经创建，则不会重复创建），以完成相应功能。  
角色名称：AliyunServiceRoleForHbrEcsBackup  
角色权限策略：AliyunServiceRolePolicyForHbrEcsBackup  
权限说明：允许备份服务组件访问您ECS和VPC资源的权限，使用该权限查询VPC和ECS资源，通过云助手部署备份客户端，管理恢复的ECS实例和快照等。  
文档链接：[混合云备份服务关联角色](#)

返回 确定授权

①

③ 备份 更多...

④ 安装客户端

安装中：

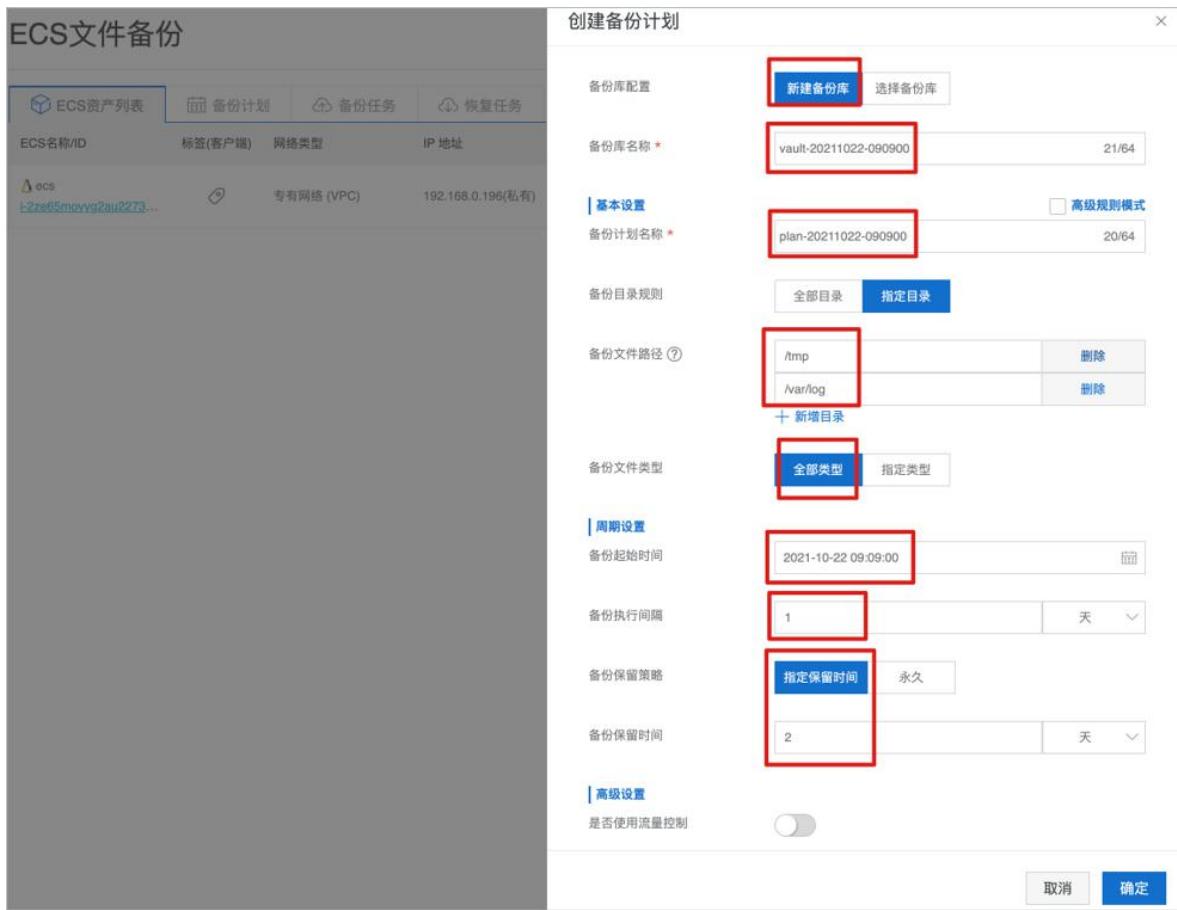
ECS名称/ID	标签(客户端)	网络类型	IP 地址	ECS状态	云助手	客户端状态
ecs i-2ze65movyg2au2273...	--	专有网络 (VPC)	192.168.0.196(私有)	正在运行	有	正在安装

安装成功：

ECS名称/ID	标签(客户端)	网络类型	IP 地址	ECS状态	云助手	客户端状态
ecs i-2ze65movyg2au2273...	已激活 Ver. 2.6.2	专有网络 (VPC)	192.168.0.196(私有)	正在运行	有	已激活 Ver. 2.6.2

步骤 24 单击操作列下的**备份**，备份 /tmp 目录

ECS名称/ID	标签(客户端)	网络类型	IP 地址	ECS状态	云助手	客户端状态	操作
ecs i-2ze3hzcu4cizz1...	已激活 Ver. 2.6.2	专有网络 (VPC)	192.168.0.163(私有)	正在运行	有	已激活 Ver. 2.6.2	<b>备份</b>



步骤 25 立即执行备份。

已保护的ECS	备份路径	备份库名/ID	计划名称/ID	执行计划	保留时间	状态	操作
ecs i-2ze65movyq2au22...	/tmp /var/log	vault-20211022-090900 v-00007xsh8j7zwq1s...	plan-20211022-090900 plan-000a9dyej5ihd...	开始: 2021-10-22 09:09:01 间隔: 1天	2 天	完成	<span style="color: green;">立即执行</span>

备份执行中：

ECS文件备份

刷新

ECS资产列表 备份计划 备份任务 恢复任务

已保护的ECS	备份路径	备份库名/ID	备份ID/计划ID	备份数据量	备份库使用量	备份速度	时间段	状态	操作
全部客户端	备份实例选择在这里	vault-20211022-...	job-000a9dyej5t...	总量: 0 B	0 B	0 B/s	2021-10-22 09:12:16 ~ ..	执行中	取消
ecs	/tmp	vault-20211022-...	job-000a9dyej5t...	总量: 0 B	0 B	<0.1% 空间节省	2021-10-22 09:12:16 ~ ..	0%	
j-2ze65movyg2...	/var/log	v-0007jxsh8j7z...	plan-000a9dyej...	完成: 0 B					

步骤 26 执行完成。

ECS文件备份

ECS资产列表 备份计划 备份任务 恢复任务

已保护的ECS	备份路径	备份库名/ID	备份ID/计划ID	备份数据量	备份库使用量	备份速度	时间段	状态
全部客户端	备份实例选择在这里	vault-20211022-...	job-000a9dyej5t...	总量: 16.19 MB	14.19 MB	5.4 MB/s	2021-10-22 09:12:16 ~ 2021-10-22 09:12:19	完成
ecs	/tmp	vault-20211022-...	job-000a9dyej5t...	总量: 16.19 MB	14.19 MB	5.4 MB/s	2021-10-22 09:12:16 ~ 2021-10-22 09:12:19	100%
j-2ze65movyg2...	/var/log	v-0007jxsh8j7z...	plan-000a9dyej...	完成: 16.19 MB				

## 3.11.云速搭部署 Web 应用防火墙 WAF

作者 | 阿里云解决方案架构师 敬海

### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
WAF	全局资源

### 应用架构规划

在进行应用架构设计时，可以提前进行资源规划。

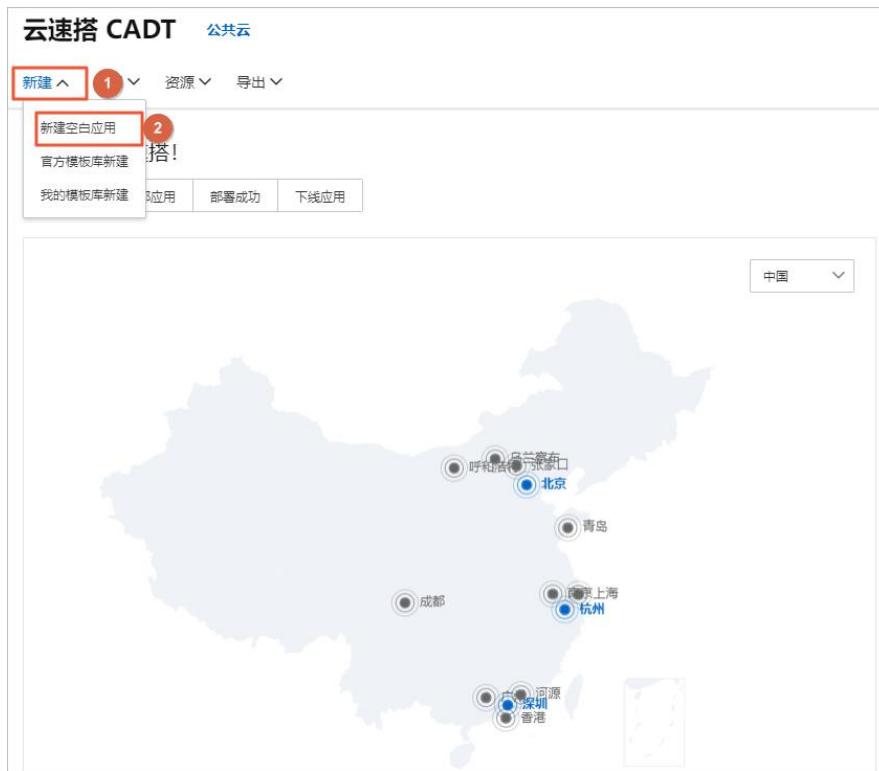
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
全局资源	WAF	-

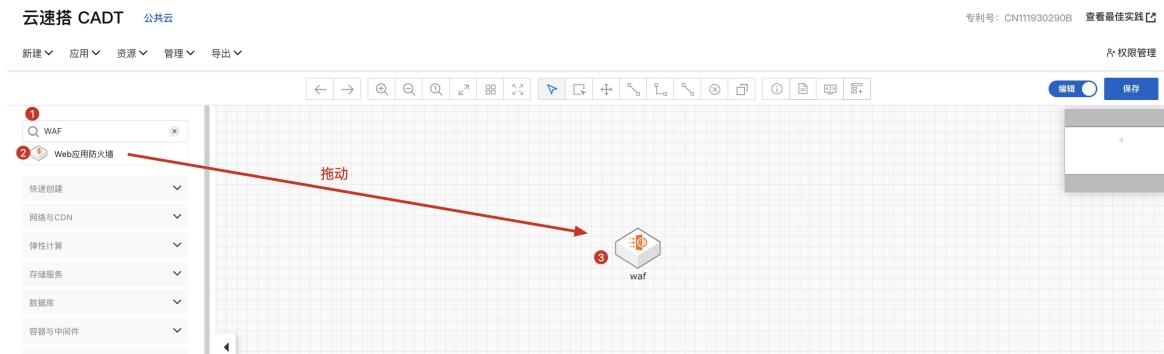
### 3.11.1.部署按量的 WAF 服务

#### 3.11.1.1.创建应用

步骤 1 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤 2 从左侧产品列表的**快速创建**分类下，找到**Web 应用防火墙**，单击后拖入到画布区域中，松开鼠标左键。



步骤 3 双击 WAF 进行配置。

Web应用防火墙 详情

部署资源   X

购买方式 i

新购

\* 实例名称 i

waf

\* 支付方式

① 按量付费

\* 套餐选择

云WAF

\* 地域

中国内地

\* WAF版本

② 按量2.0

支付方式选择按量付费。

步骤 4 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写应用名称，并单击**确认**。



### 3.11.1.2.部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、ECS 是否有库存等，一般需要几十秒左右。

Resource Verification						
Resource Name	Resource Type	Region	Specification	Result	Notes	Action
waf	waf			Success	Verified	Locate

State: Verified successful

[Next: Price List](#) [Return](#)

步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息，由于 WAF 这里选择了按量付费，点击计费方式，在弹出的窗口，查看计费详情。

The screenshot shows the Alipay Cloud Pricing Platform interface. On the left, there's a sidebar with 'Export Price List' and tabs for 'Free' and 'Billing Method'. Below it is a section titled 'Resource Cost Contribution' with a note 'No cost contribution at present'. A red arrow points from this note to the right panel. The right panel has a header 'Billing Method 2.0' with a note about the upgrade to version 2.0. It includes sections for 'Billing Period' (from the day the WAF instance is activated until its expiration), 'Billing Method' (bill by actual usage after domain connection), and a note about total fees being the sum of function item fees and traffic fees. At the bottom, there are buttons for 'Previous Step: Resource Verification' and 'Next Step: Confirm Order'.

步骤 4 可以单击**查看报告**，查看应用的价格信息。



步骤 5 单击**下一步：确认订单**，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

**确认订单**

资源名称	资源类型	区域	规格	数量	原价	实付	状态
waf	waf	杭州		1			新购

**《云速搭服务条款》**  
部署前, 请阅读并勾选服务条款

状态: **计价成功**

步骤 6 单击**下一步: 支付并创建**, 就会进入部署流程, 这里会进行扣费并开始创建资源。

**注意:** 部署流程一旦开始后, 无法取消。

**资源部署状态**

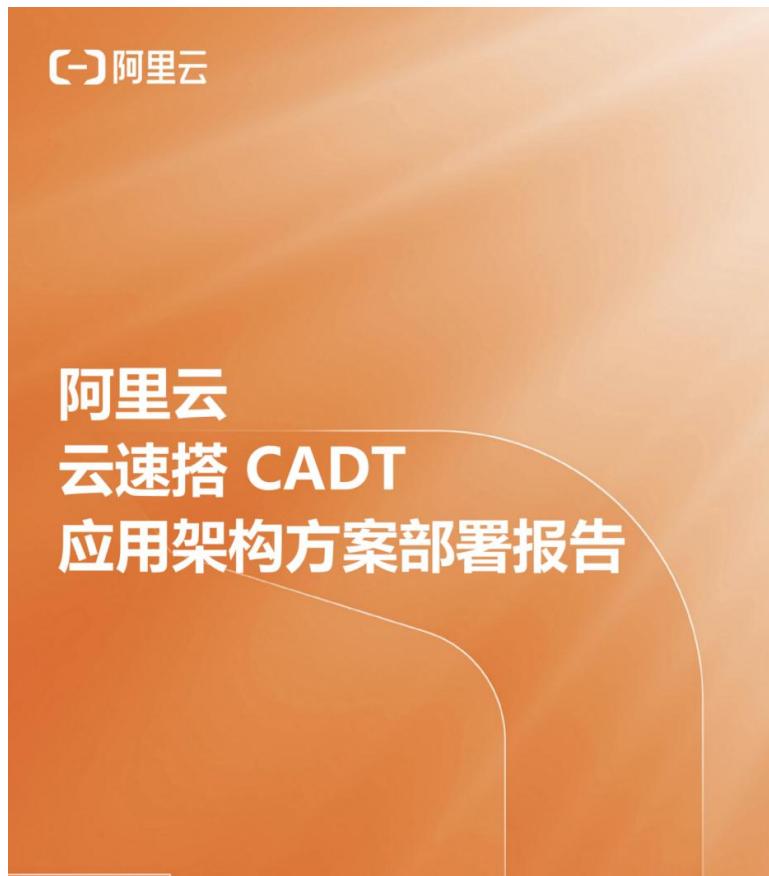
资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位

部署中, 不要进行任何操作, 请耐心等待...

**部署概要**

状态: 部署中 方案编号: HC80P8WFYBEU3C3E

步骤 7 部署完成后, 单击**查看报告**, 可以查看本次的部署报告。



步骤 8 单击返回，然后单击资源清单。

The screenshot shows a table with the following data:

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位	操作
waf	waf	按量付费	waf_elasticity-cn-7mz2ev7qw03c	运行中	2021-10-28 16:43:10	定位	详情   监控   变更日志

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 9 单击 WAF 后，跳转到 WAF 控制台查看。

这里可以看到按量 waf 已经开通。

## 步骤 10 配置 WAF

参考 <https://bp.aliyun.com/detail/39> 中第六章的内容，配置 WAF。

## 步骤 11 释放 WAF 应用

对于按量的 WAF，如果不使用后，可以释放资源。

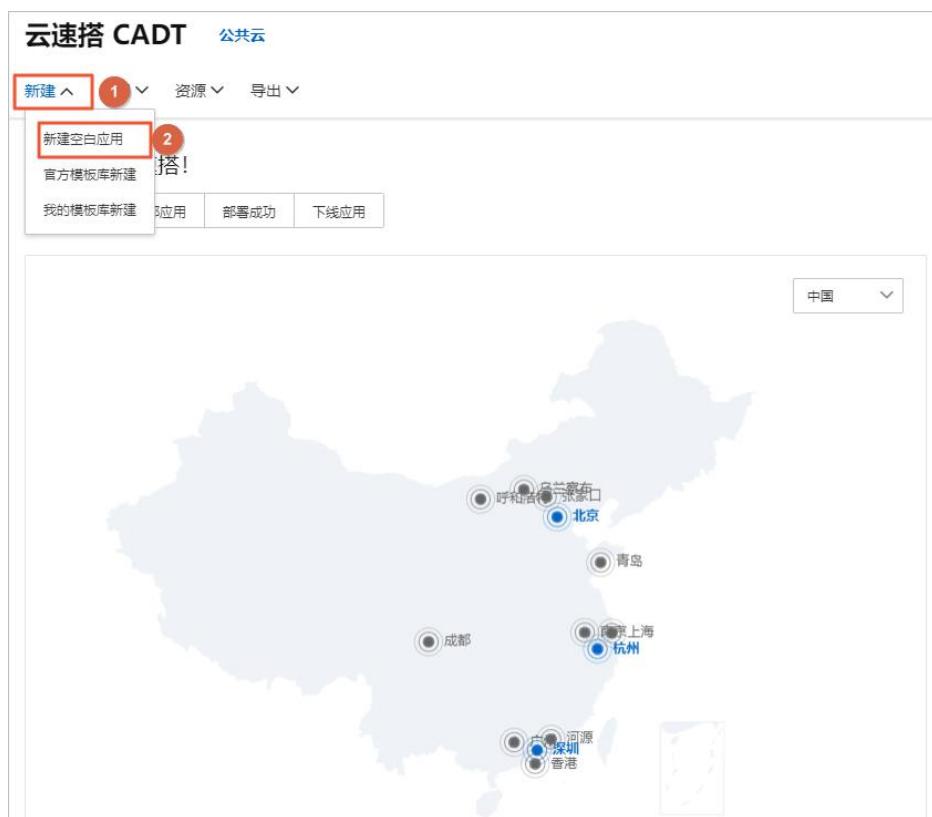
首先在控制台删除 WAF 的相关配置，然后在 CADT 中释放 CADT 资源。

在弹出的窗口中，输入验证码，然后点击确定，释放后如下：

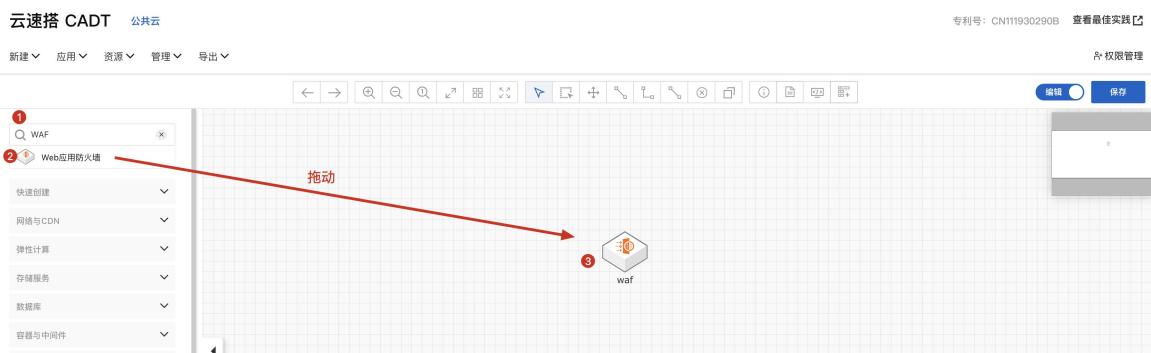
## 3.11.2.开通包年包月的 WAF 服务

### 3.11.2.1.创建应用

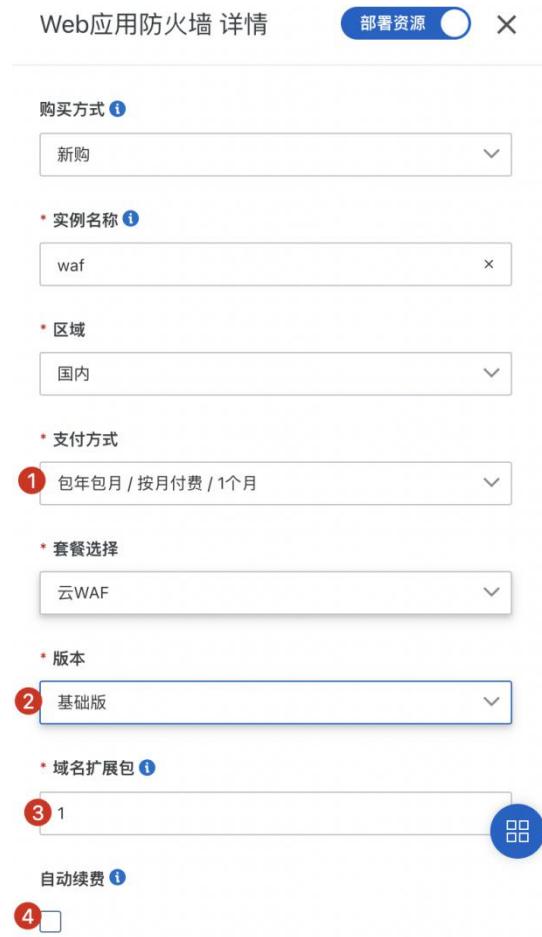
步骤 1 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤 2 从左侧产品列表的**快速创建**分类下，找到**Web 应用防火墙**，单击后拖入到画布区域中，松开鼠标左键。



步骤3 双击WAF进行配置，以购买基础版为例：



支付方式选择按量付费。

步骤4 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写应用名称，并单击**确认**。



### 3.11.2.2.部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、ECS 是否有库存等，一般需要几十秒左右。

资源验证						
资源名称	资源类型	区域	规格	结果	备注	操作
waf	waf		version_basic_advanced	成功	校验通过	定位

状态:校验成功

下一步: 价格清单

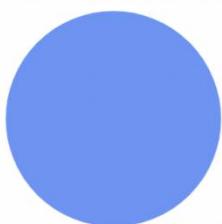
返回

步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息查看。

导出价格清单

免费 包年包月

资源成本占比



资源预算  
● 安全 安全: 0.01元

100%

价格列表

资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
waf	waf	杭州	version_basic _advanced	1	1月	108.25元/月	0.01元	108.25元	<a href="#">定位</a>

状态: 计价成功

上一步: 资源校验 查看报告 下一步: 确认订单

步骤 4 可以单击[查看报告](#), 查看应用的价格信息。



**步骤5 单击下一步：确认订单，**在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。



**步骤6 单击下一步：支付并创建，**就会进入部署流程，这里会进行扣费并开始创建资源。



**注意：**部署流程一旦开始后，无法取消。



步骤 7 部署完成后, 点击**查看报告**, 可以查看本次的部署报告。



步骤 8 单击返回，然后单击资源清单。

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位	操作
waf	waf	包年包月	waf-cn-tl32ev9ij3k	运行中	2021-10-28 17:23:24	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 9 单击 waf 后，跳转到 waf 控制台查看。

域名	插入模式	源站信息	快速操作	操作
没有查询到符合条件的记录				

这里可以看到按量 waf 已经开通。

步骤 10 配置 waf

参考 <https://bp.aliyun.com/detail/39> 中第六章的内容，配置 waf。

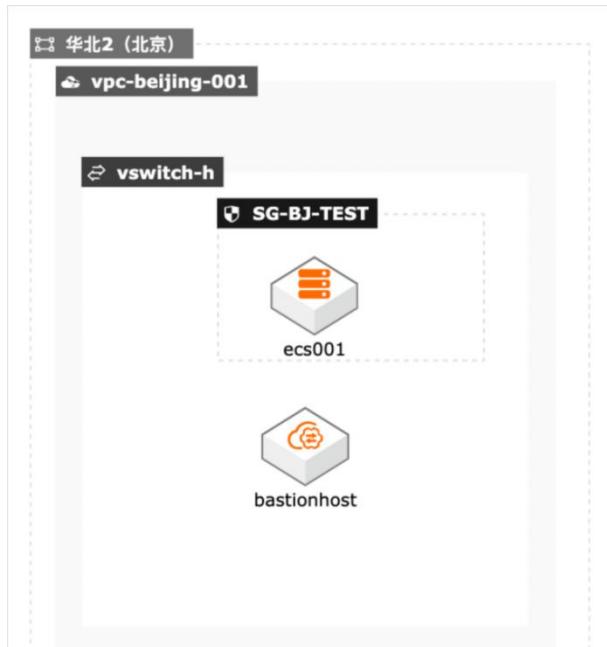
## 3.12.云速搭部署堡垒机

作者 | 阿里云解决方案架构师 敬海

### 3.12.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现堡垒机的部署。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
堡垒机	vswitch 交换机
ECS	vswitch 交换机

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

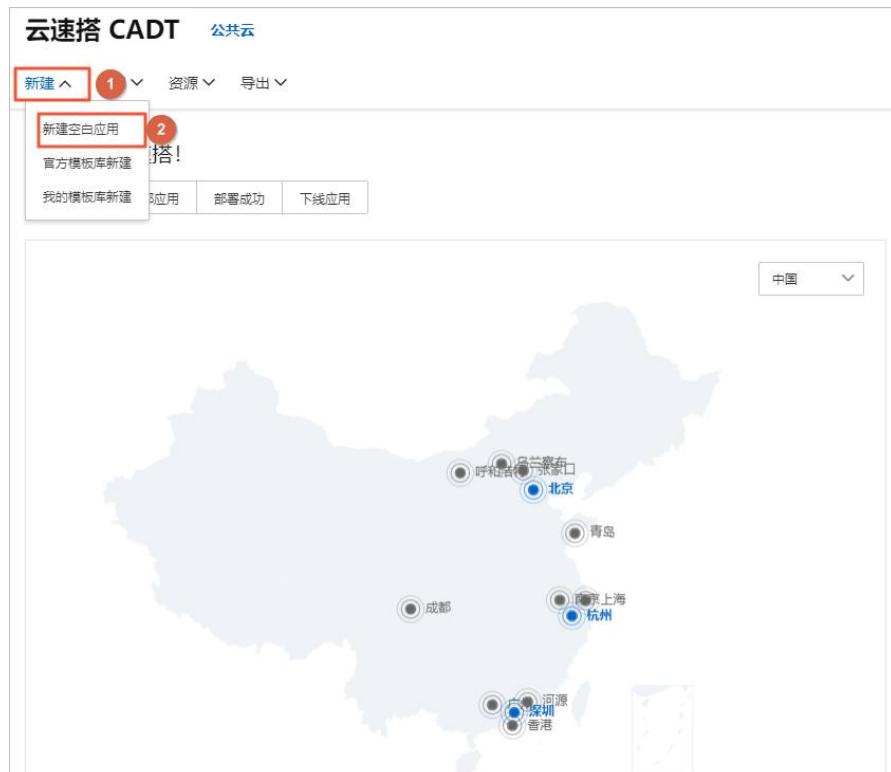
资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
安全组	SG-BJ-TEST	-

### 3.12.2.应用架构设计

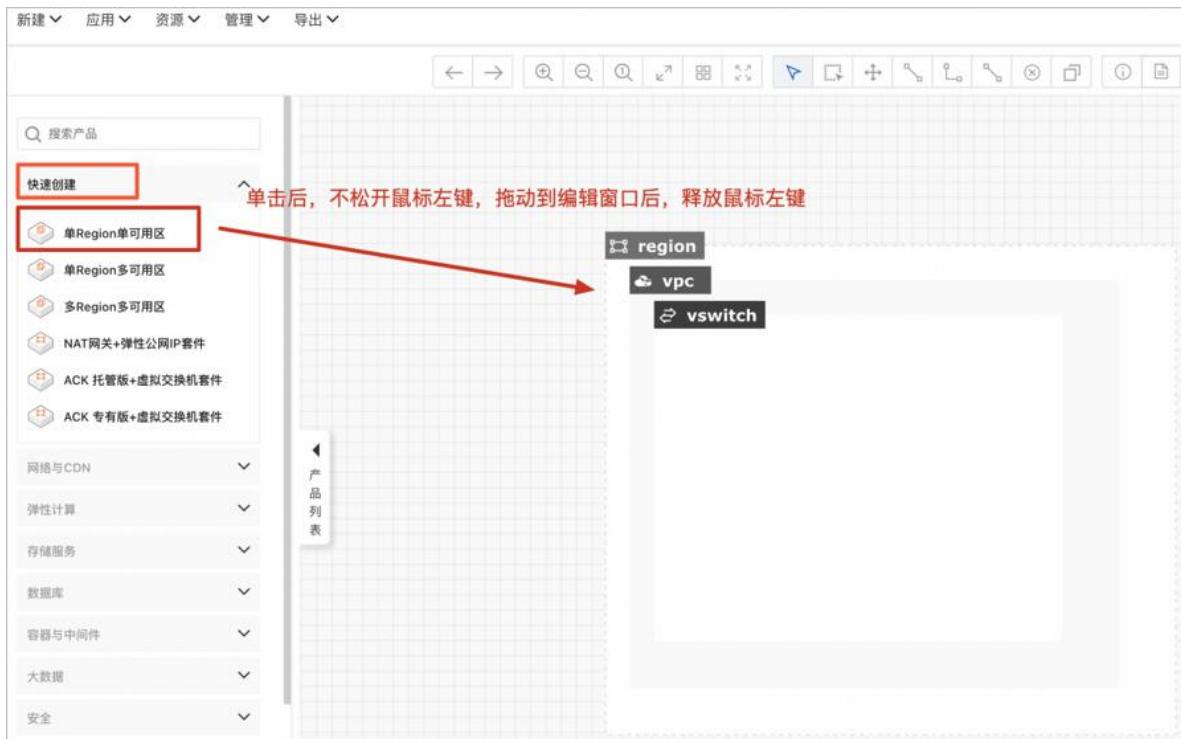
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

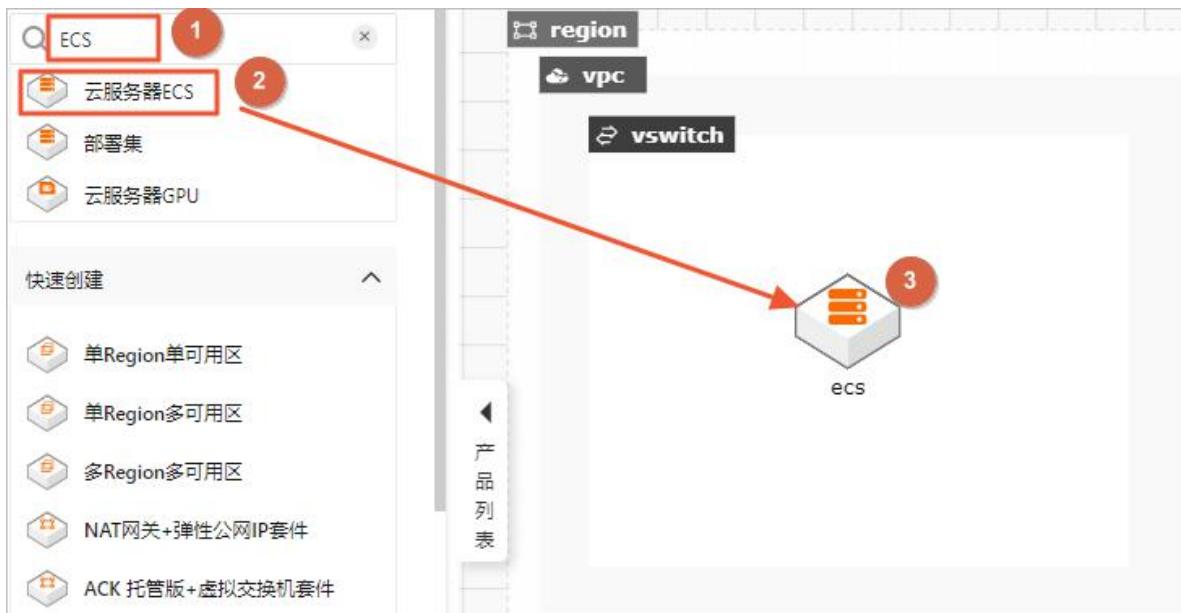
步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤3 从左侧产品列表的**快速创建**分类下，找到**单Region单可用区**，单击后拖入到画布区域中，松开鼠标左键。



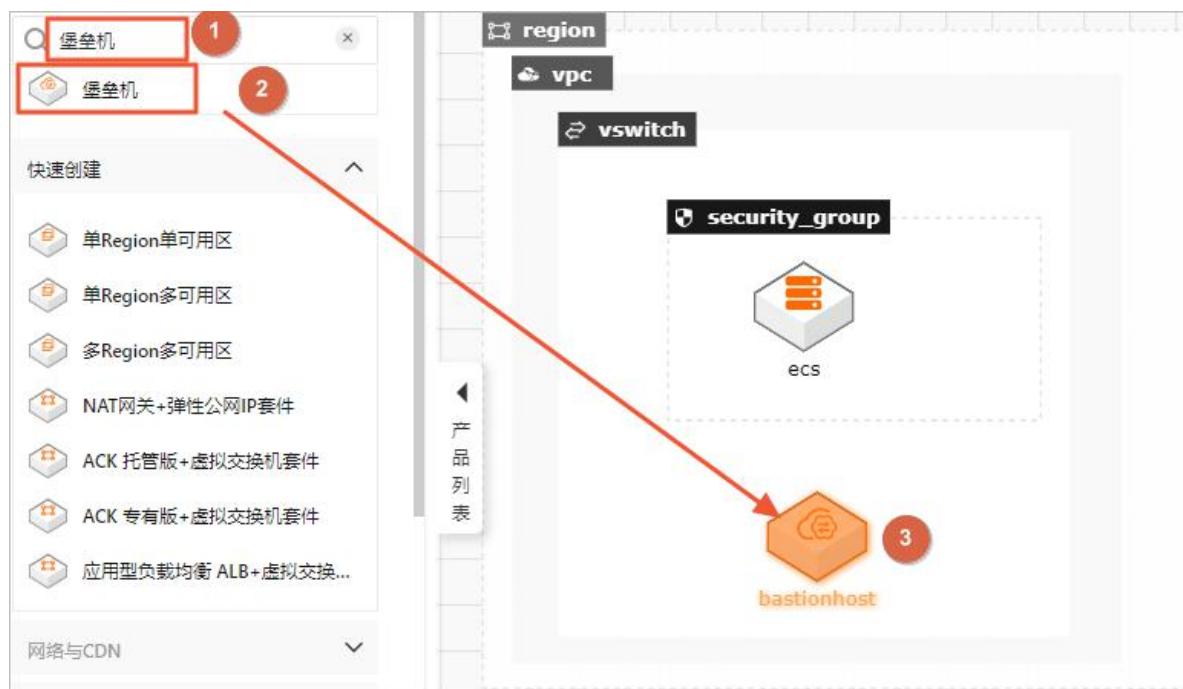
步骤4 搜索 ECS，拖到 vswitch 中。



步骤5 搜索安全组，拖入一个安全组，将 ECS 放在安全组的框内。



步骤 6 搜索堡垒机，拖到 vswitch 中。



### 3.12.3.资源参数配置

双击资源图标，进行参数配置：

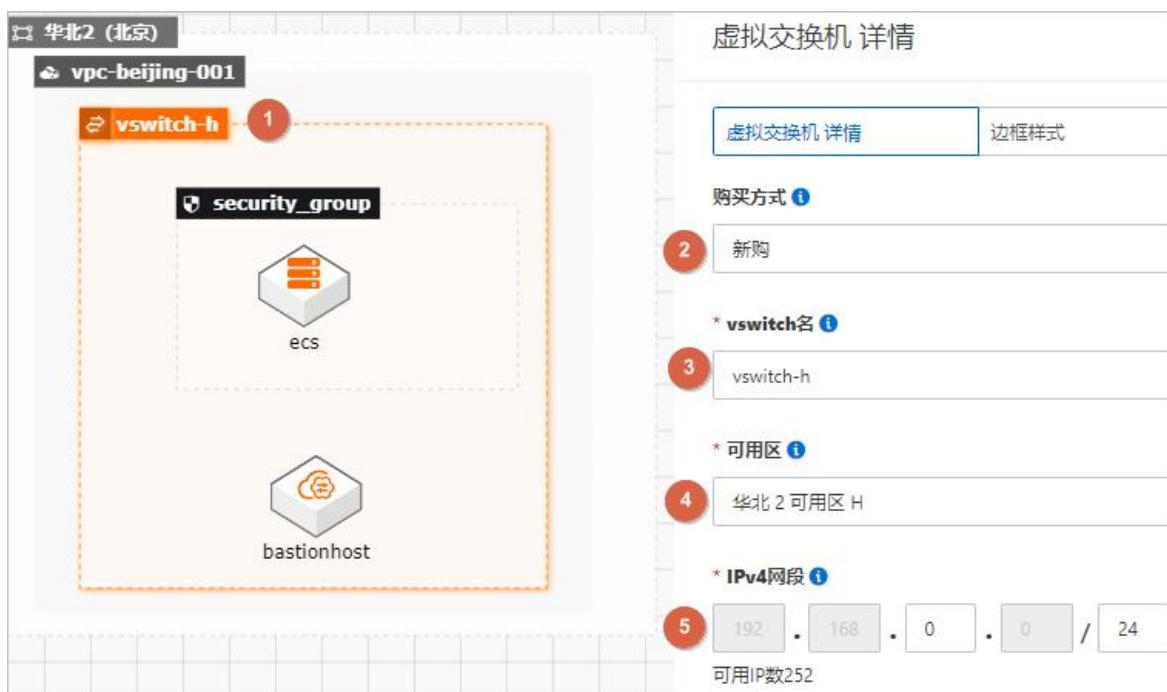
步骤 7 双击配置 Region，选择华北 2（北京）。



步骤 8 双击 VPC，配置 VPC 参数。



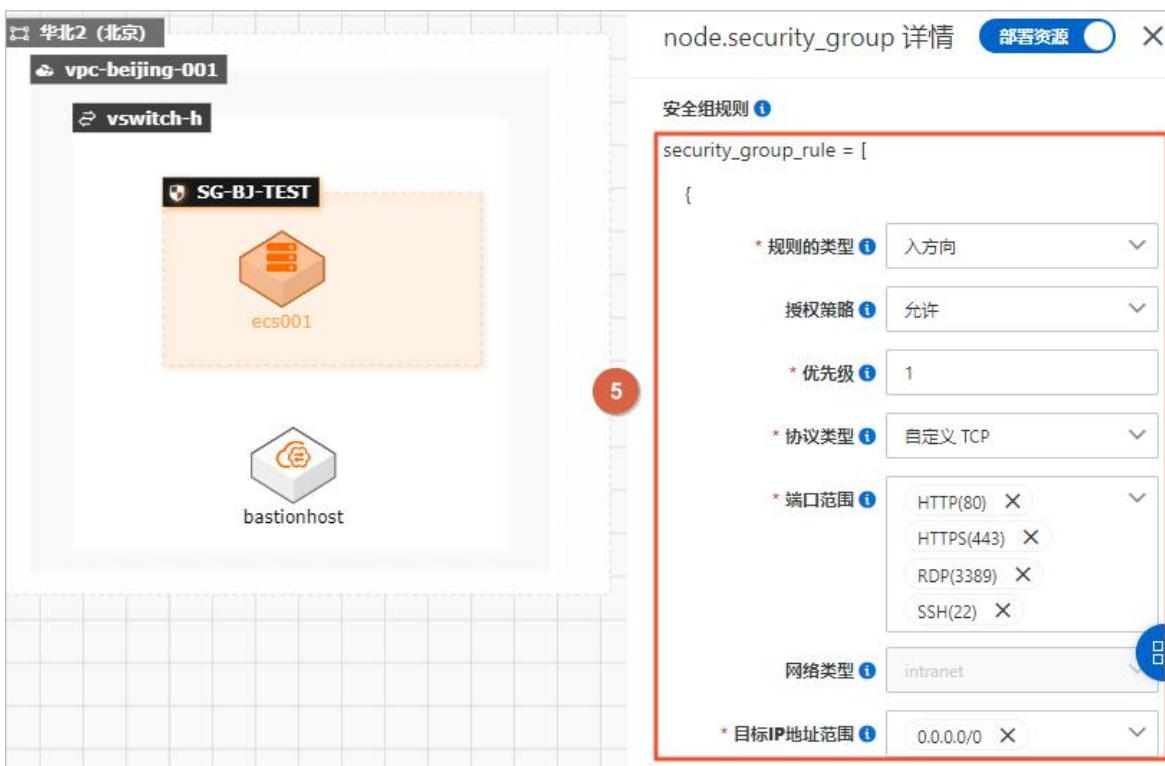
步骤 9 双击 Vswitch，配置 vswitch 参数。



步骤 10 双击 ECS 配置实例信息，ECS 实例信息参考下表：

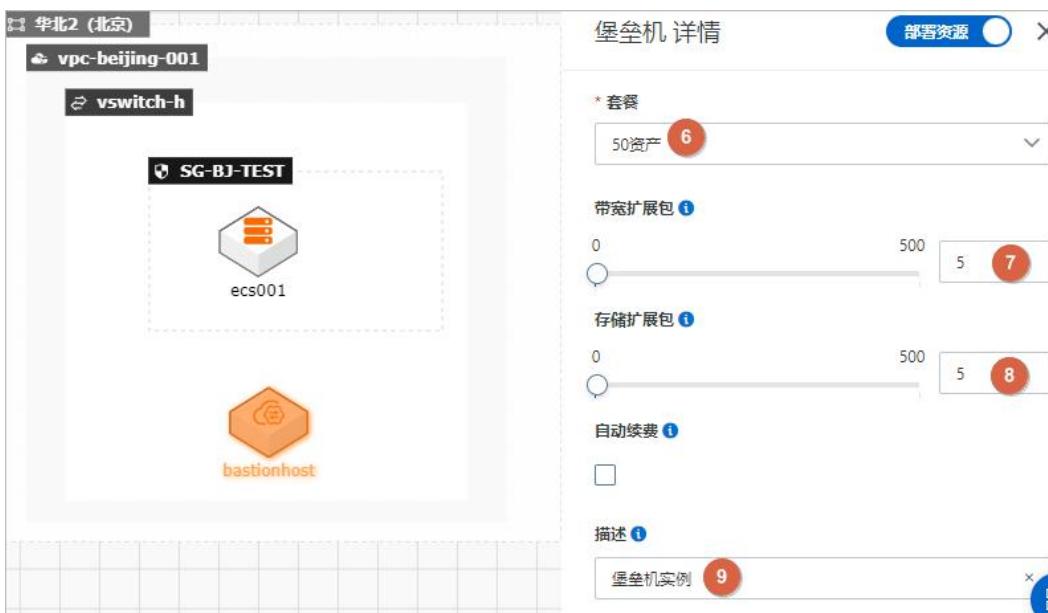
配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs001
支付方式	按量付费
实例规格	ecs.c6a.large(2c 4g)
镜像	CentOS
镜像版本	CentOS 7.6 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
主机名	ecs001
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>

步骤 11 双击安全组，修改安全组参数。

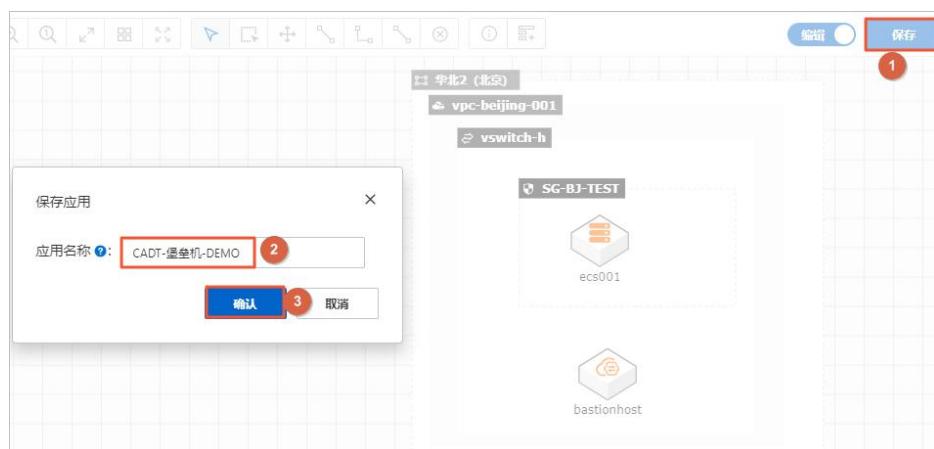


步骤 12 双击堡垒机图标，并配置其参数。

堡垒机计费方式详见：[https://help.aliyun.com/document\\_detail/52924.html](https://help.aliyun.com/document_detail/52924.html)

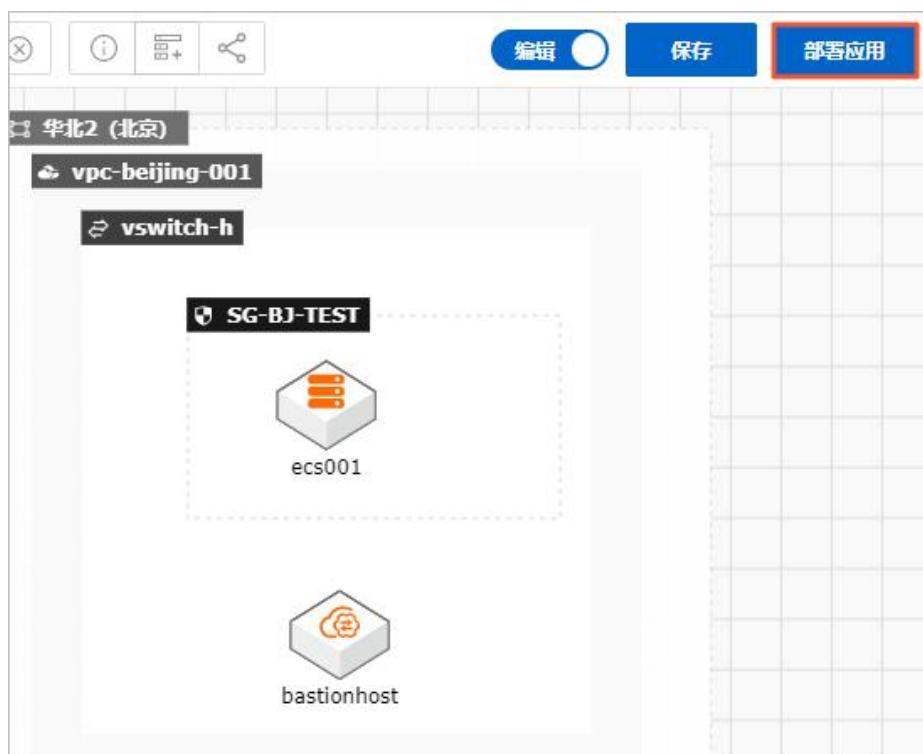


步骤 13 配置完成，单击右上角的**保存**，并设置应用名称。



### 3.12.4.部署应用

步骤 14 应用保存完成后，单击右上角的**部署应用**。



步骤 15 弹出如下校验页面，这里会校验参数配置是否合法、ECS 是否有库存等，一般需要十几秒左右。

校验成功，单击**下一步：价格清单**。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-h	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	ecs001	ecs	北京	ecs.c6a.large	成功	校验通过	定位
3	vpc-beijing-001	vpc	北京	192.168.0.0/16	成功	校验通过	定位
4	默认安全组	security.group	北京		成功	校验通过	定位
5	SG-BJ-TEST	security.group	北京	normal	成功	校验通过	定位
6	bastionhost	bastionhost	北京	cloudbastion	成功	校验通过	定位

状态:校验成功

下一步: 价格清单

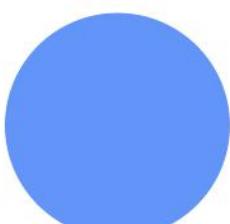
返回

步骤 16 在导出价格清单对话框中会拉取应用所有配置的价格信息，可以查看计费详情。分别查看包年包月和按量付费资源的价格：

**导出价格清单**

免费 **包年包月** 按量付费

资源成本占比



资源预算  
● 安全 安全: 100 元

100%

价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
1	bastionhost	bastionhost	北京	cloudbastion	1	1月	3420.00元/月			<a href="#">定位</a>

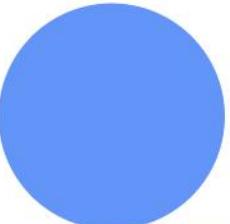
状态: **计价成功**

上一步: 资源校验 查看报告 **下一步: 确认订单**

**导出价格清单**

免费 包年包月 **按量付费**

资源成本占比



资源预算  
● 计算 计算: 0.34 元/时

100%

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	ecs001	ecs	北京	ecs.c6a.large	1	0.34元/时			<a href="#">定位</a>

状态: **计价成功**

上一步: 资源校验 查看报告 **下一步: 确认订单**

步骤 17 可以单击**查看报告**, 查看应用的价格信息。



步骤 18 单击**下一步：确认订单**, 在新的窗口中, 勾选《云速搭服务条款》, 这里会显示价格信息, 按量的会按小时扣除, 包年包月的会一次性扣除 (如有)。

单击**下一步：支付并创建**, 就会进入部署流程, 这里会进行扣费并开始创建资源。

The screenshot shows the "确认订单" (Confirm Order) step of the deployment process. It includes:

- A table listing resources:序号 资源名称 资源类型 区域 规格 数量 购买时长 原价 实付 状态  
1 bastionhost bastionhost 北京 cloudbastion 1 1月 3420.00元/月 [redacted] 新购
- A checked checkbox for "《云速搭服务条款》" (Cloud Speed Stack Service Terms).
- A callout box showing resource details:
  - 您创建的应用中包含如下包年包月资源:
  - bastionhost
  - 这些资源未到期前无法进行释放, 请确认!
- Buttons: 确认 (Confirm) and 取消 (Cancel).
- Bottom status: 状态: 计价成功 (Status: Pricing successful).
- Buttons: 上一步: 价格清单 (Previous Step: Price List) and 下一步: 支付并创建 (Next Step: Pay and Create).

**注意：**部署流程一旦开始后，无法取消。



步骤 19 部署完成后，单击查看报告，可以查看本次的部署报告。

资源部署状态							
序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001	vpc	-	vpc-2ze08v1qm3t5ggk1ufc7l	运行中	2021-11-01 17:05:24	定位
2	默认安全组	security.group	-	sg-2zefiis08efdjom1khua	运行中	2021-11-01 17:05:25	定位
3	vswitch-h	vswitch	-	vsw-2zegsq9oa1bzcg29ftg32	运行中	2021-11-01 17:05:52	定位
4	ecs001	ecs	按量付费	i-2zeb7b8tz2dsq8b1gbfp	运行中	2021-11-01 17:06:48	定位
5	bastionhost	bastionhost	包年包月	bastionhost-cn-tl32f2u0l03	运行中	2021-11-01 19:28:08	定位

部署概要  
状态: 部署成功  
方案编号: F1AZLC13M43XYAUG  
订单编号: 211355149540159, 211359309820159  
[查看报告](#) [返回](#)



步骤 20 单击返回，然后单击资源清单。

The screenshot shows the Cloud Speed Stack deployment interface. At the top, it says "CADT-堡垒机-DEMO [部署成功]". Below that is a navigation bar with icons for back, forward, search, and other operations. The main area displays a hierarchical tree structure under "华北2 (北京) / vpc-beijing-001". Under "vswitch-h", there are two resources: "ecs001" and "bastionhost". A "资源清单" (Resource List) button is located at the bottom of the tree view. Below the tree is a table with the following data:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	vpc-beijing-001	vpc	-	vpc-2ze0by1qm3t5ggk1ufc7l	新建	运行中	2021-11-01 17:05:24	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
2	sg-default	security group	-	sg-2zeffis08efdfjom1khuq	新建	运行中	2021-11-01 17:05:25	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
3	vswitch-h	vswitch	-	vsw-2zegsq9oa1bzcg29ftg32	新建	运行中	2021-11-01 17:05:52	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
4	ecs001	ecs	按量付费	i-2zeb7b8tz2dsq8b1gbfp	新建	运行中	2021-11-01 17:06:48	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
5	bastionhost	bastionhost	按量付费	bastionhost-cn-tl32f2u0l03	新建	运行中	2021-11-01 17:06:48	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 21 单击堡垒机后，跳转到堡垒机控制台查看。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
1	vpc-beijing-001	vpc	-	vpc-2ze0by1qm3t5ggk1ufc7l	新建	运行中
2	sg-default	security group	-	sg-2zeffis08efdfjom1khuq	新建	运行中
3	vswitch-h	vswitch	-	vsw-2zegsq9oa1bzcg29ftg32	新建	运行中
4	ecs001	ecs	按量付费	i-2zeb7b8tz2dsq8b1gbfp	新建	运行中
5	bastionhost	bastionhost	包年包月	bastionhost-cn-tl32f2u0l03	新建	运行中

步骤 22 启用堡垒机：

The screenshot shows the "实例" (Instance) configuration page for a bastion host. The top navigation bar includes "产品手册" and "购买堡垒机". The main area shows a summary card for "bastionhost-cn-tl32f2u0l03" which is currently "未初始化" (Not Initialized). The card includes sections for "标签" (Tags), "出口IP" (Exit IP), "版本" (Version), "规格" (Specs), and "到期时间" (Expiration Time). A prominent red box highlights the "启用" (Enable) button in the bottom right corner of the card.



步骤 23 等待几分钟后，堡垒机创建成功。



步骤 24 等待堡垒机启动后，参照如下链接使用堡垒机。

<https://bp.aliyun.com/detail/39> 中第十章《开通并配置堡垒机》中的内容。

## 3.13.云速搭部署云防火墙

作者 | 阿里云解决方案架构师 敬海

### 3.13.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现云防火墙的示例架构，开通一个典型的网络服务。云防火墙选型查看如下文档：

[https://help.aliyun.com/document\\_detail/162300.html](https://help.aliyun.com/document_detail/162300.html)



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
云防火墙	全局资源

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

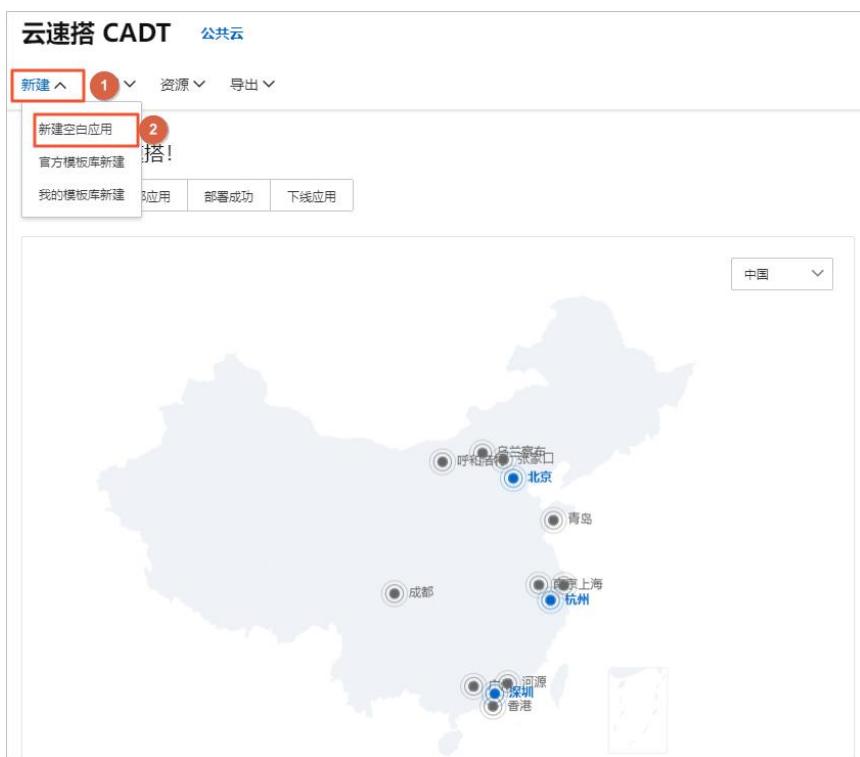
资源分类	资源名称	网段
全局资源	云防火墙	-

### 3.13.2.创建应用

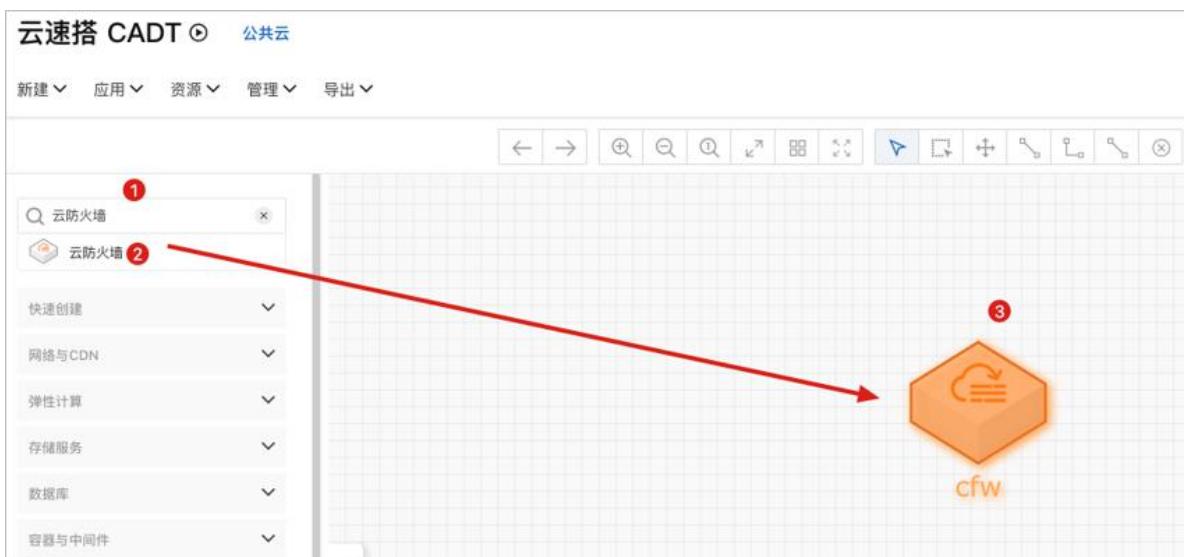
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤3 从左侧产品列表搜索框处，找到**云防火墙**，单击后拖入到画布区域中，松开鼠标左键。



步骤4 双击云防火墙图标进行配置。



**\* 可防护公网IP数**

20  个

互联网边界隔离防护功能可保护的公网IP数如上所示，继续购买可增加防火墙能保护的公网IP数量，可随时扩容

**\* 公网流量处理能力**

10  Mbps

公网流量处理能力是指云防火墙可防护的公网方向流量峰值，建议与您业务的公网带宽保持一致，可随时扩容

**\* 日志审计**

是

云防火墙默认存储7天日志，如需要更长时间日志存储或满足等保要求，建议选购日志分析服务

**\* 日志存储容量**

1000  GB

存储容量选购参考：10M公网带宽，存储6个月日志，推荐购买1000GB日志存储容量

**\* 专家服务**

否

专家服务：提供钉钉群交流，配置接入服务，策略优化服务，重要时期安全保障

**\* 购买时长**

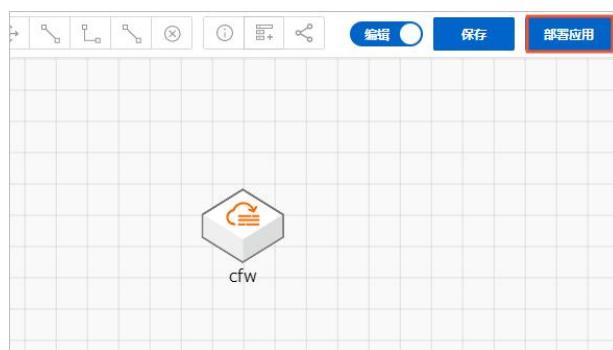
预付费 / 按月付费 / 1个月

步骤 5 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写应用名称，并单击**确认**。



### 3.13.3.部署应用

步骤 6 应用保存完成后，单击右上角的**部署应用**。



步骤 7 等待校验成功，单击**下一步：价格清单**。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	cfw	vipcloudfw		2	成功	校验通过	定位

状态:校验成功

**下一步：价格清单** **返回**

步骤 8 在导出价格清单页面，会拉取应用所有配置的价格信息，可以查看计费详情。

**导出价格清单**

免费 **包年包月**

资源成本占比

资源预算  
● 安全(云盾) 安全(云盾) 10...

价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
1	cfw	vipcloudfw		2	1	1月	3300.00元/月	10%	3000元	定位

状态: 计价成功

**上一步：资源校验** **查看报告** **下一步：确认订单**

步骤 9 可以单击**查看报告**, 查看应用的价格信息。



步骤 10 单击**下一步：确认订单**, 在新的窗口中, 勾选《云速搭服务条款》, 这里会显示价格信息, 按量的会按小时扣除, 包年包月的会一次性扣除 (如有)。

**确认订单**

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
1	cfw	vipcloudfw		2	1	1月	3300.00元/月	3300.00元	新购

《云速搭服务条款》

1 部署前, 请阅读并勾选服务条款

包年包月: 3300元

状态: 计价成功

上一步: 价格清单

2 下一步: 支付并创建

步骤 11 单击**下一步：支付并创建**, 就会进入部署流程, 这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后, 无法取消。



步骤 12 部署完成后，如下图所示：



步骤 13 部署完成后，单击查看报告，可以查看本次的部署报告。



步骤 14 单击返回，然后单击资源清单。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	cfw	vipcloudfw	包年包月	vipcloudfw-cn-7pp2f6cw303	新建	运行中	2021-11-03 17:07:42	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 15 单击云防火墙后，跳转到云防火墙控制台查看。

这里可以看到云防火墙已经开通。

步骤 16 配置云防火墙。

参考 <https://bp.aliyun.com/detail/39> 中第 8 章的内容，配置云防火墙。

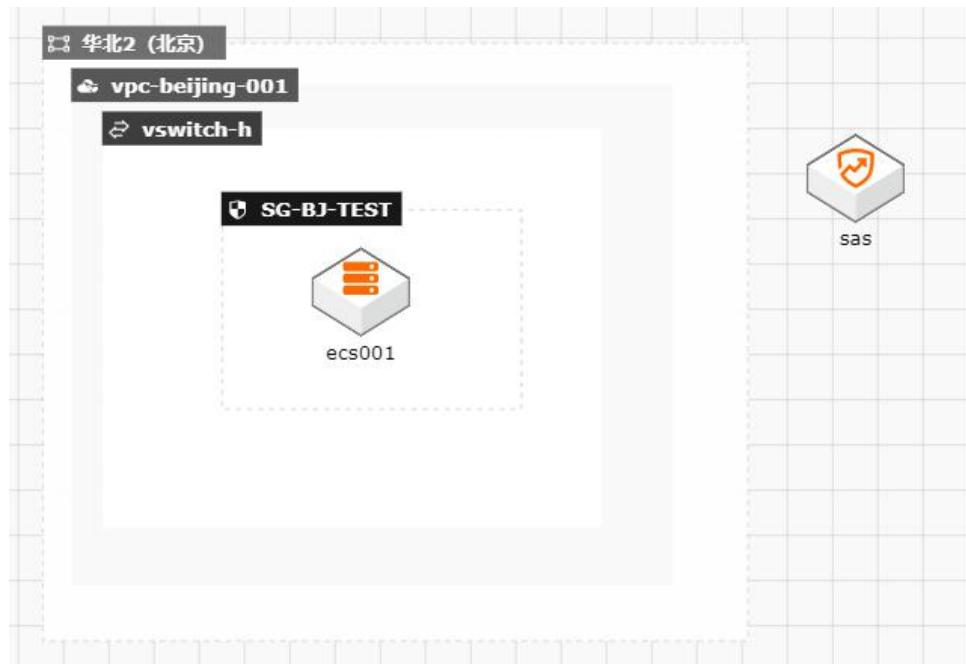
## 3.14.云速搭部署云安全中心

作者 | 阿里云解决方案架构师 敬海

### 3.14.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现云安全中心的部署。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
云安全中心	全局级别
ECS	vswitch 级别

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
安全组	SG-BJ-TEST	-

### 3.14.2.应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

云速搭 CADT 公共云

专利号: CN111930290B 查看最佳实践

新建 应用 资源 导出

欢迎使用云速搭!

应用全景 全部应用 部署成功 下线应用

中国

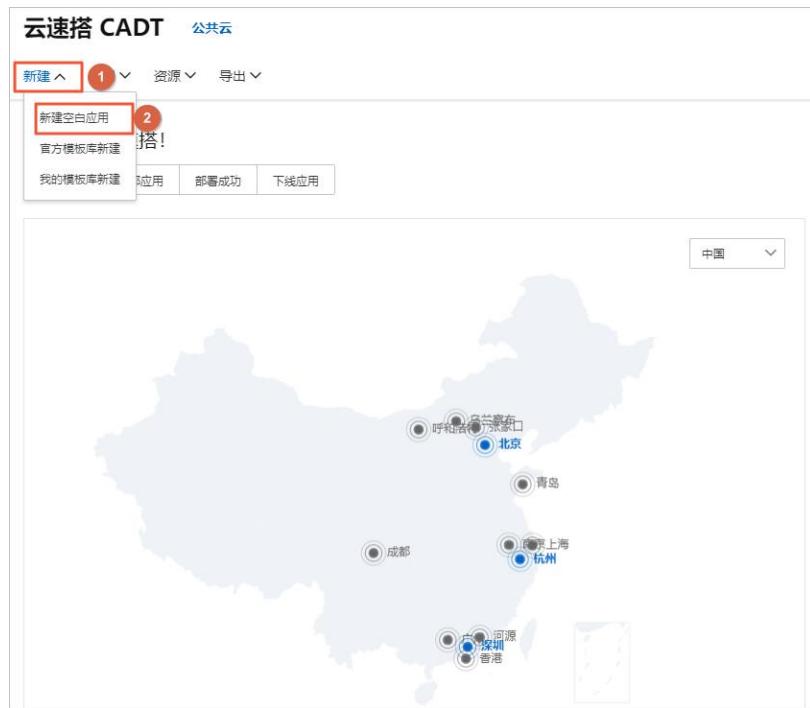
未分配区域

应用名称	创建时间	状态
无数据		

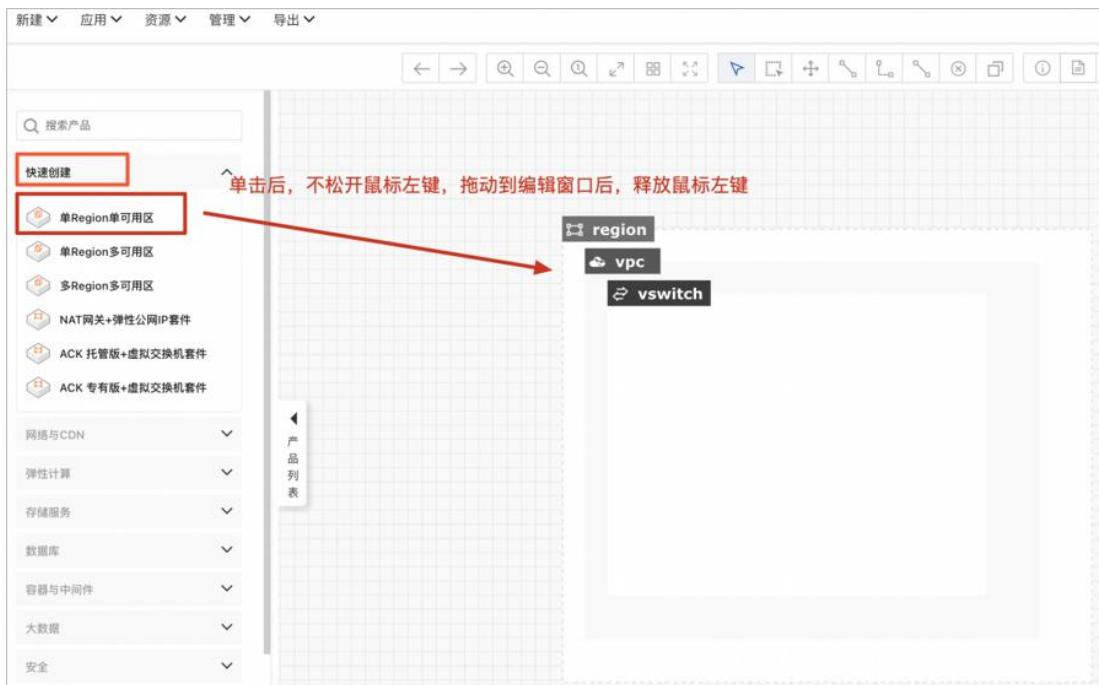
产品动态

- 支持用户对应用进行架构探查，自动产生已有应用的架构 [新功能](#)  
2021年9月31日
- 支持RAM权限管理，对子用户授予不同的权限和资源组，控制子用户对资源的 [新功能](#)  
访问和操作  
2021年9月31日
- 支持应用状态实时更新，实时更新服务的状态和配置 [新功能](#)  
2021年9月31日

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

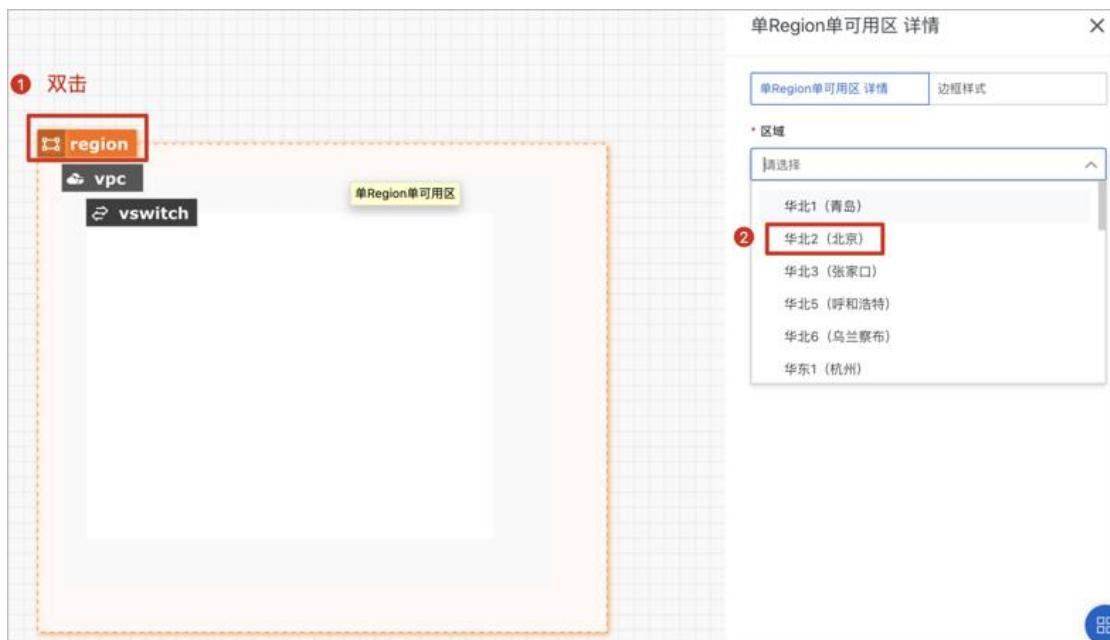


步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。



步骤4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北2（北京）。



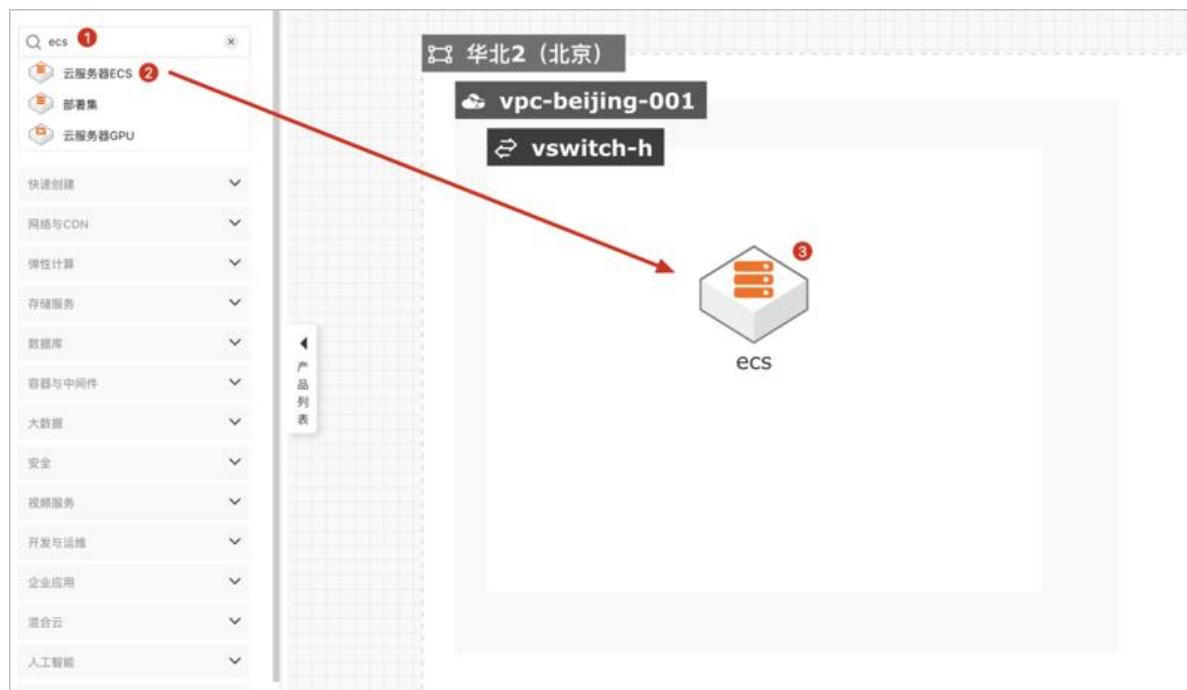
2. 双击 VPC，配置 VPC 参数。



3. 双击 Vswitch，配置 vswitch 参数。



步骤 5 左侧搜索 ECS，拖到 vswitch 中。

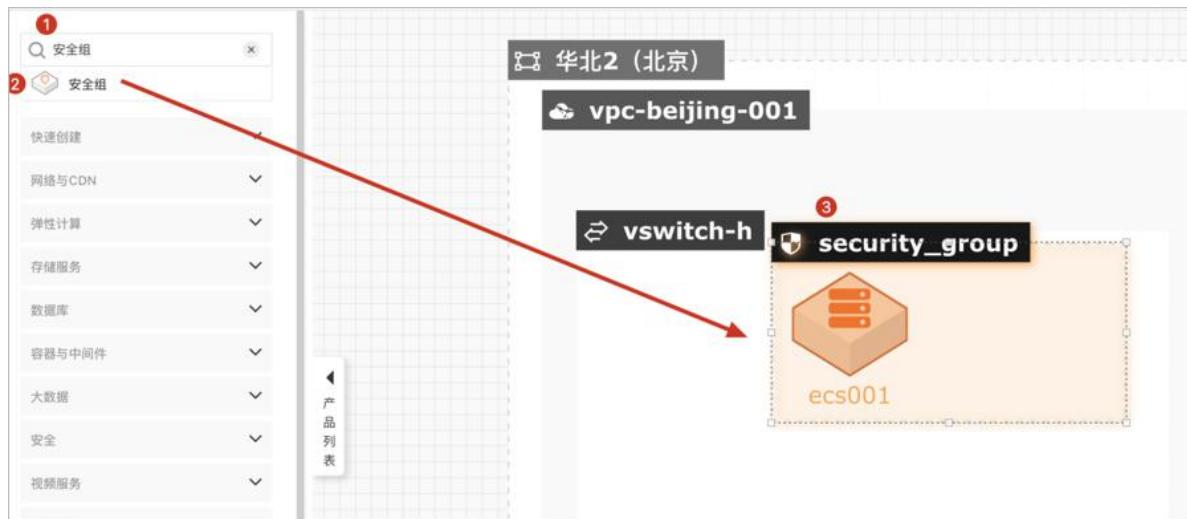


步骤 6 双击 ECS，配置参数。

配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs001
支付方式	按量付费
实例规格	ecs.c6a.large(2c 4g)
镜像	Alibaba Cloud Linux
镜像版本	Alibaba Cloud Linux 3.2104 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
主机名	ecs001
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>



步骤 7 搜索安全组，拖入一个安全组，将 ECS 放在安全组的框内。

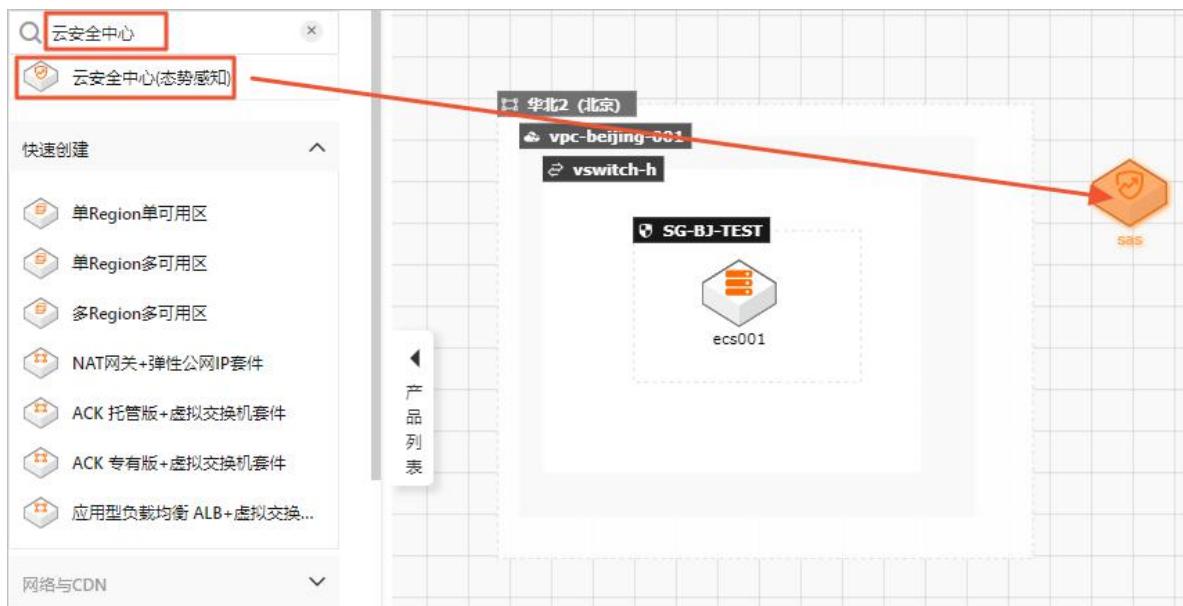


步骤 8 双击安全组，修改安全组参数：

- 安全组名称：自定义
- 安全组类型：普通安全组
- 安全组规则根据实际需要进行配置，本示例保持默认



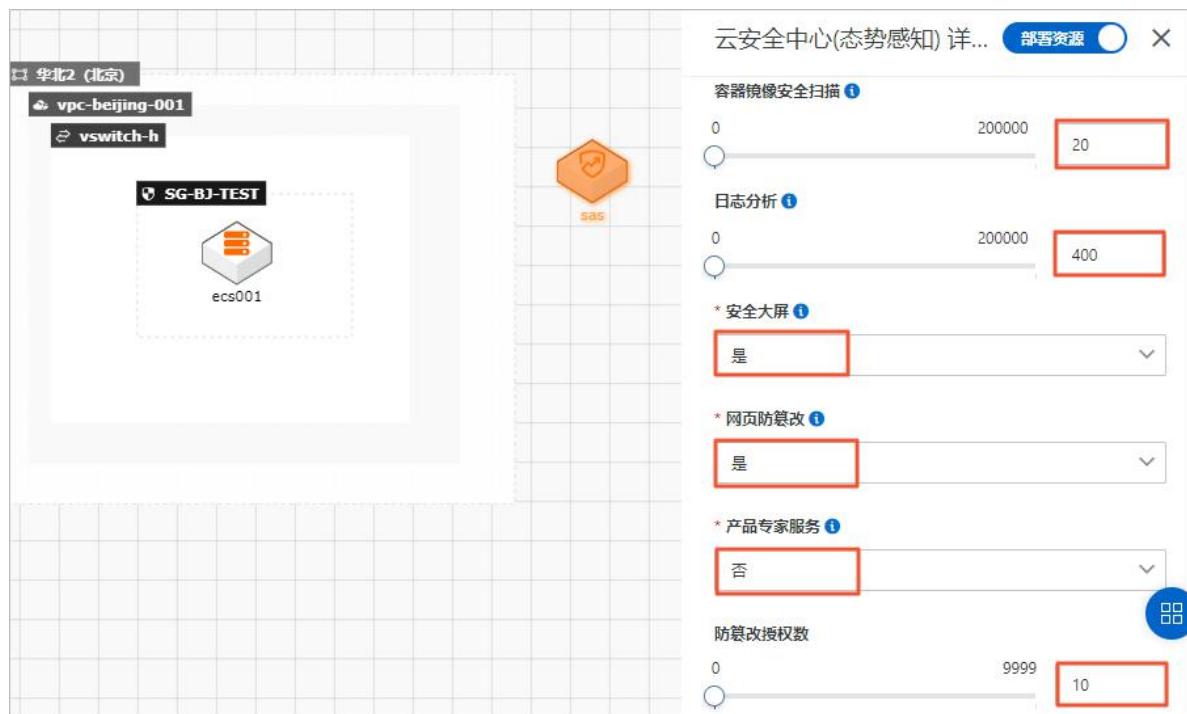
步骤 9 从左侧搜索框处找到云安全中心，并拖动到右侧架构图中（云安全中心属于全局资源，可以放到架构图中的任意位置），如下图所示。



步骤 10 双击云安全中心图标，并配置其参数。

云安全中心计费方式详见：[https://help.aliyun.com/document\\_detail/57357.html](https://help.aliyun.com/document_detail/57357.html)



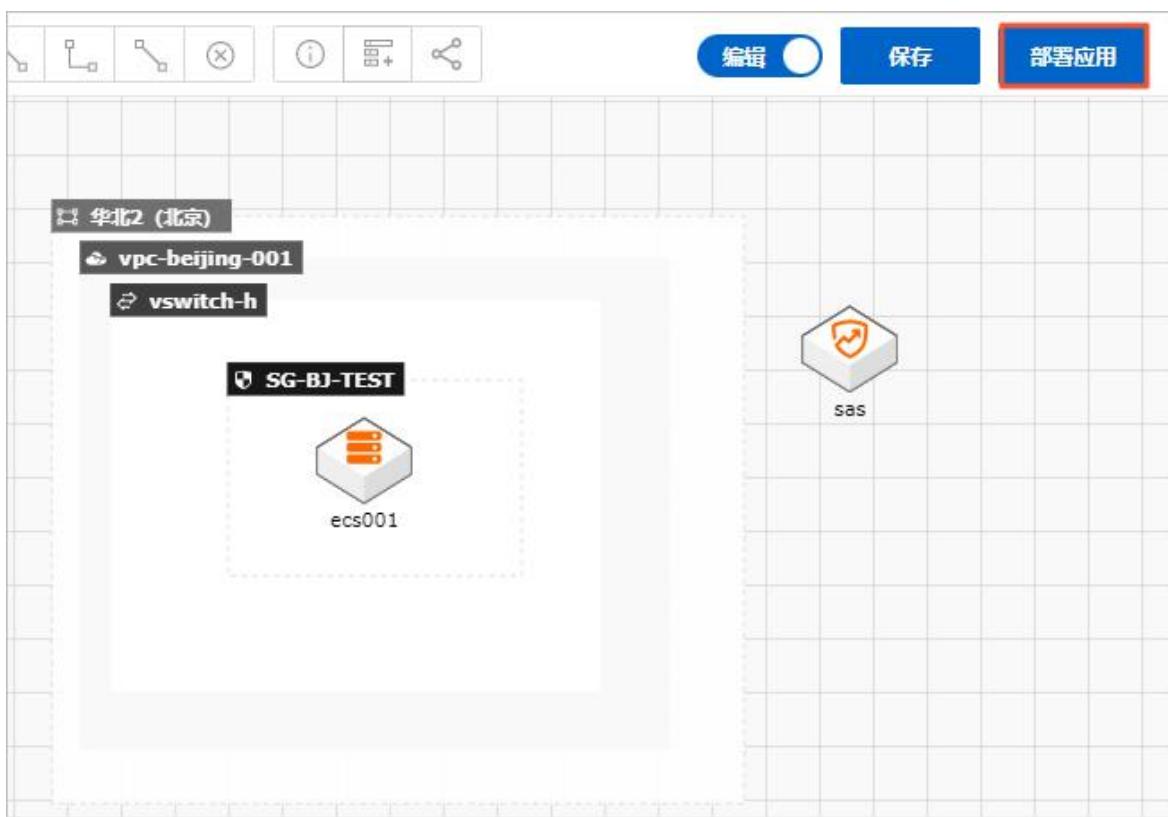


步骤 11 单击右上角的保存，填写应用名称。



### 3.14.3. 部署应用

步骤 12 应用保存完成后，单击右上角的部署应用。



步骤 13 等待校验成功，单击**下一步：价格清单**。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-h	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	sas	sas		level3	成功	校验通过	定位
3	ecs001	ecs	北京	ecs.c6a.large	成功	校验通过	定位
4	vpc-beijing-00 1	vpc	北京	192.168.0.0/16	成功	校验通过	定位
5	SG-BJ-TEST	security.group	北京	normal	成功	校验通过	定位

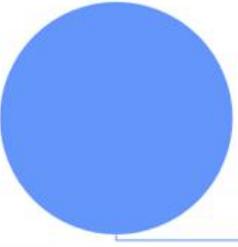
状态:校验成功 下一步: 价格清单 返回

步骤 14 在**导出价格清单**对话框中，会拉取应用所有配置的价格信息，可以查看计费详情。分别查看包年包月和按量付费的资源价格。

**导出价格清单**

免费 **包年包月** 按量付费

资源成本占比



资源预算  
● 安全 安全: 10... 元

价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
1	sas	sas		level3	1	1月	18303.00元/月	18303.00元/月	18303.00元/月	<a href="#">定位</a>

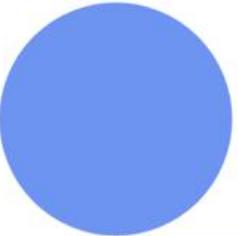
状态: **计价成功**

上一步: 资源校验 [查看报告](#) **下一步: 确认订单**

**导出价格清单**

免费 **按量付费**

资源成本占比



资源预算  
● 计算 计算: 10... 元/时

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	ecs001	ecs	北京	ecs.c6a.large	1	0.34元/时	0.34元/时	0.34元/时	<a href="#">定位</a>

状态: **计价成功**

上一步: 资源校验 [查看报告](#) **下一步: 确认订单**

步骤 15 可以单击**查看报告**, 查看应用的价格信息。



步骤 16 单击**下一步：确认订单**，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

**确认订单**

免费	<b>包年包月</b>	按量付费

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
1	sas	sas		level3	1	1月	18303.00元/月	元/月	新购

《云速搭服务条款》  
部署前，请阅读并勾选服务条款

包年包月：**18303元** 按量付费：**CC10元/H**

状态：**计价成功**

[上一步：价格清单](#) [下一步：支付并创建](#)

步骤 17 单击**下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。



Resource Deployment Status							
序号	Resource Name	Resource Type	Billing Type	Resource ID	Resource Status	Resource Update Time	Location
1	sas	sas	By Year/Month	sas-rl0iwirmk743	Running	2021-11-02 20:12:02	Location
2	vpc-beijing-001	vpc	-	vpc-2zerq6w28u324dw39s9dm	Running	2021-11-02 20:12:47	Location
3	SG-BJ-TEST	security.group	-	sg-2zec8bx9mvo2lbvtes31	Running	2021-11-02 20:12:47	Location
4	vswitch-h	vswitch	-	vsw-2zemacor8m70e43wnl0id	Running	2021-11-02 20:12:47	Location
5	ecs001	ecs	Pay-as-you-go	i-2zefngf8dolyh6xei42i	Running	2021-11-02 20:13:13	Location

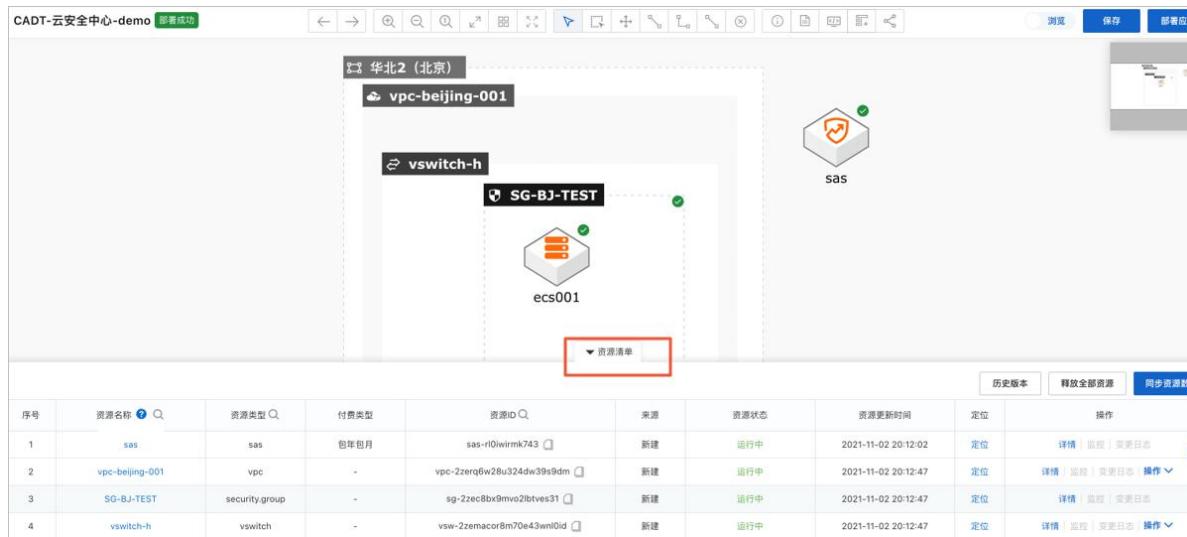
**Deployment Summary**  
Status: Deployment successful  
Order number: 211375101180159  
Scheme number: 63R7XUZJBO4CJ2IM

[View Report](#) [Return](#)

步骤 18 部署完成后，单击[查看报告](#)，可以查看本次的部署报告。



步骤 19 单击返回，然后单击资源清单。

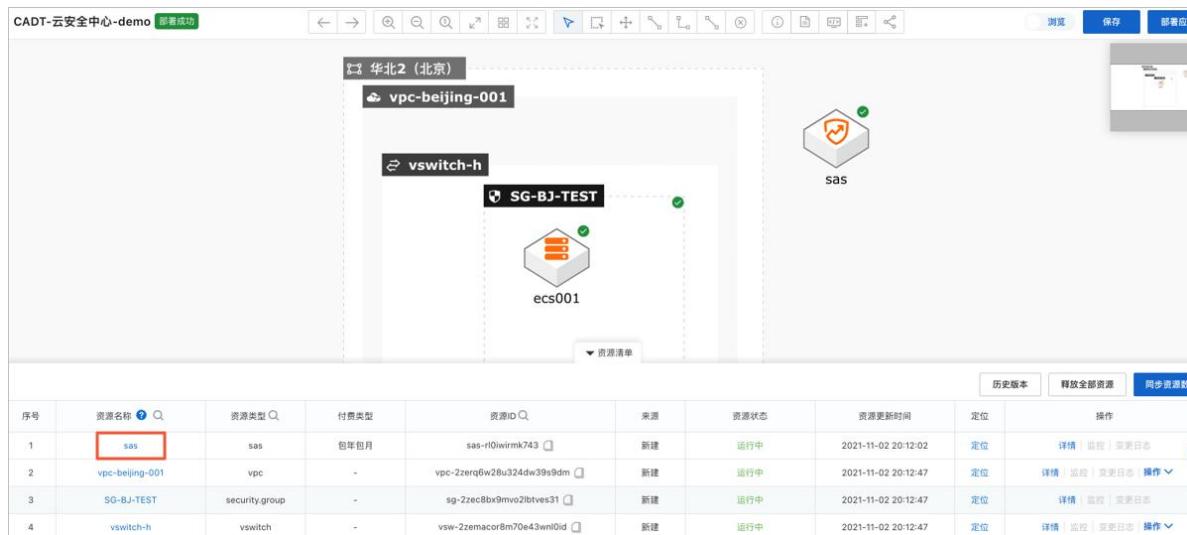


The screenshot shows the CADT Cloud Security Center interface. At the top, there's a toolbar with various icons. Below it is a navigation bar with '华北2 (北京)' and a network diagram showing a VPC (vpc-beijing-001) connected to a security group (SG-BJ-TEST) which contains an ECS instance (ecs001). A red box highlights the '资源清单' button at the bottom of the diagram. To the right of the diagram is a sidebar with a 'sas' icon. Below the diagram is a table listing resources:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	sas	sas	包年包月	sas-rI0wirmk743	新建	运行中	2021-11-02 20:12:02	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>
2	vpc-beijing-001	vpc	-	vpc-2zerq6w28u324dw39s9dm	新建	运行中	2021-11-02 20:12:47	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>
3	SG-BJ-TEST	security.group	-	sg-22ec8bx9nvo2lbves3t	新建	运行中	2021-11-02 20:12:47	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>
4	vswitch-h	vswitch	-	vsw-2zermacor8m70e43wnl0d	新建	运行中	2021-11-02 20:12:47	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 20 单击云安全中心后，跳转到云安全中心控制台查看详情。



This screenshot is identical to the one above, but the first row ('sas') in the resource list table is highlighted with a red box. This indicates that the user has selected the 'sas' resource to view its details.

云安全中心

总资产 4 资产中心

勒索家族 REvil (Sodinokibi) 近期通过供应链攻击以及Kaseya远程代码执行漏洞 (CVE-2021-30116) 进行大肆传播，云安全中心默认支持此勒索的防御。请确保您已经在设置页面启用了防病毒功能，以防止您的资产遭受损失。

**安全评分**

发现 6 条风险

根据高级版威胁检测能力评估

立即处理

已累计保护您的资产 0 天

立即升级 换费

授权数/防护资产数 5/5 (10核) 未防护资产(ECS)

网站 容器

开启威胁检测功能，领取20 元代金券！ 等级保护合规

立即领取

步骤 21 等待云安全中心启动后，参考如下链接使用云安全中心。

<https://bp.aliyun.com/detail/39> 中第九章《开通并配置云安全中心》

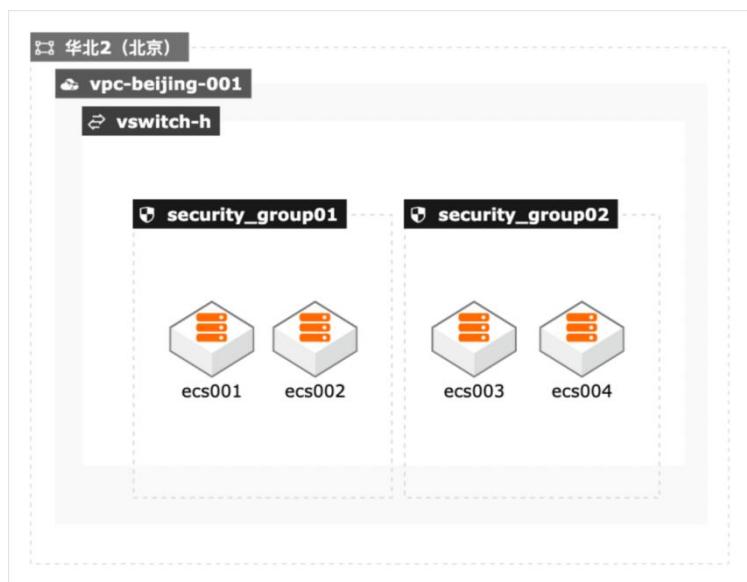
## 3.15.云速搭部署安全组

作者 | 阿里云解决方案架构师 敬海

### 3.15.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现安全组和企业安全组的部署。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
安全组	VPC 级别
ECS	vswitch 交换机

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
安全组	security_group01	-
安全组	security_group02	

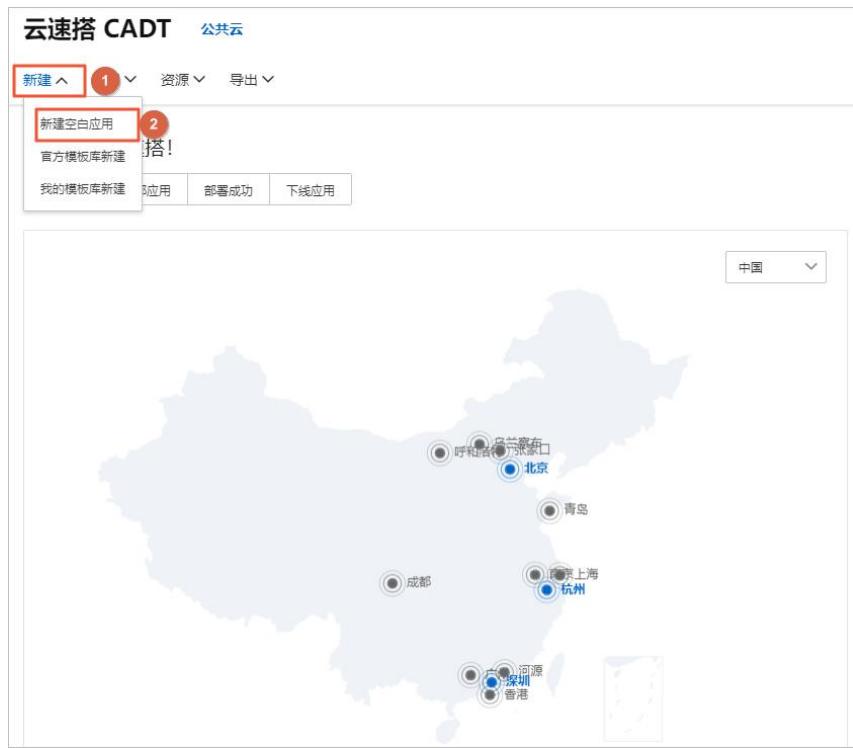
### 3.15.2.应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

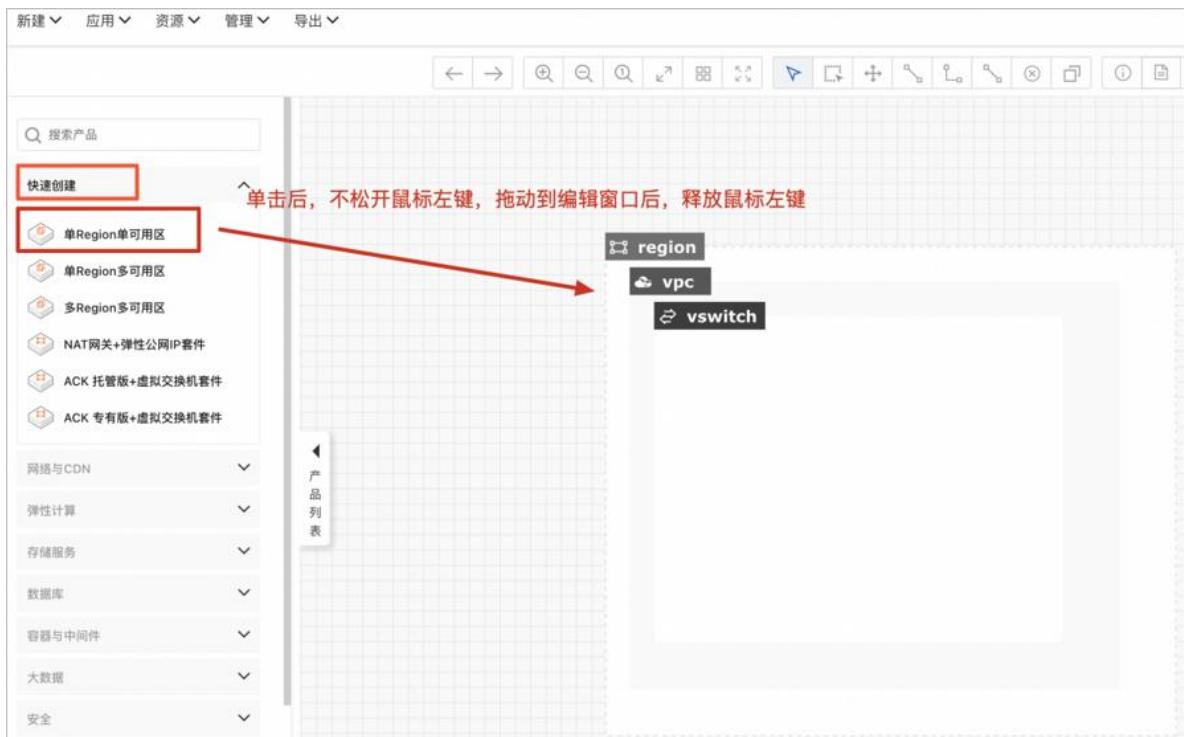
**说明：**如果提示需要开通服务，请根据提示进行开通。

The screenshot displays the Cloud Speed Stack CADT Control Console. At the top, there's a header bar with the title '云速搭 CADT' and a dropdown menu for '公共云'. On the right side of the header, it says '专利号: CN111930290B' and '查看最佳实践'. Below the header, there are navigation buttons for '新建' (Create), '应用' (Application), '资源' (Resources), and '导出' (Export). A message '欢迎使用云速搭!' (Welcome to Cloud Speed Stack!) is displayed. The main area features a map of China with several cities marked: Beijing, Shanghai, Hangzhou, Shenzhen, Hong Kong, Chongqing, Chengdu, and Jinan. To the right of the map, there are two sections: '未分配区域' (Unassigned Regions) and '产品动态' (Product News). The '未分配区域' section shows a table with columns for '应用名称' (Application Name), '创建时间' (Creation Time), and '状态' (Status), with a note '没有数据' (No data). The '产品动态' section lists three items: 1. 支持用户对应用进行架构探查, 自动生成已保存应用的架构 [New Feature]. Date: 2021年9月31日. 2. 支持RAM权限管理, 对子用户授予不同的权限和资源组, 控制子用户对资源的访问和操作 [New Feature]. Date: 2021年9月31日. 3. 支持应用状态实时更新, 实时更新服务的状态和配置 [New Feature]. Date: 2021年9月30日.

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

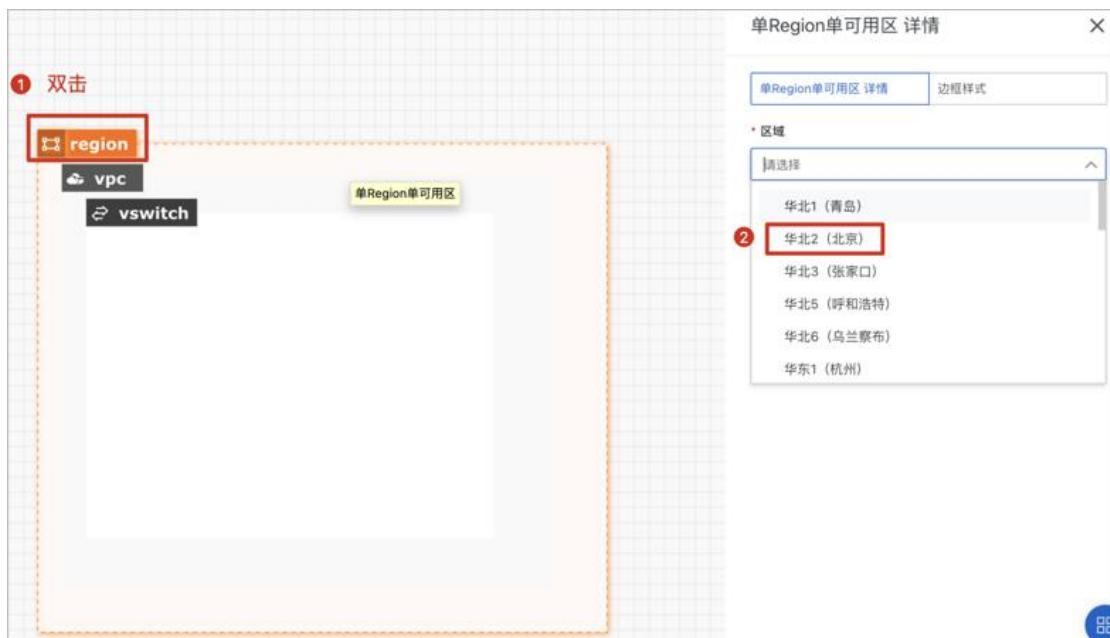


步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

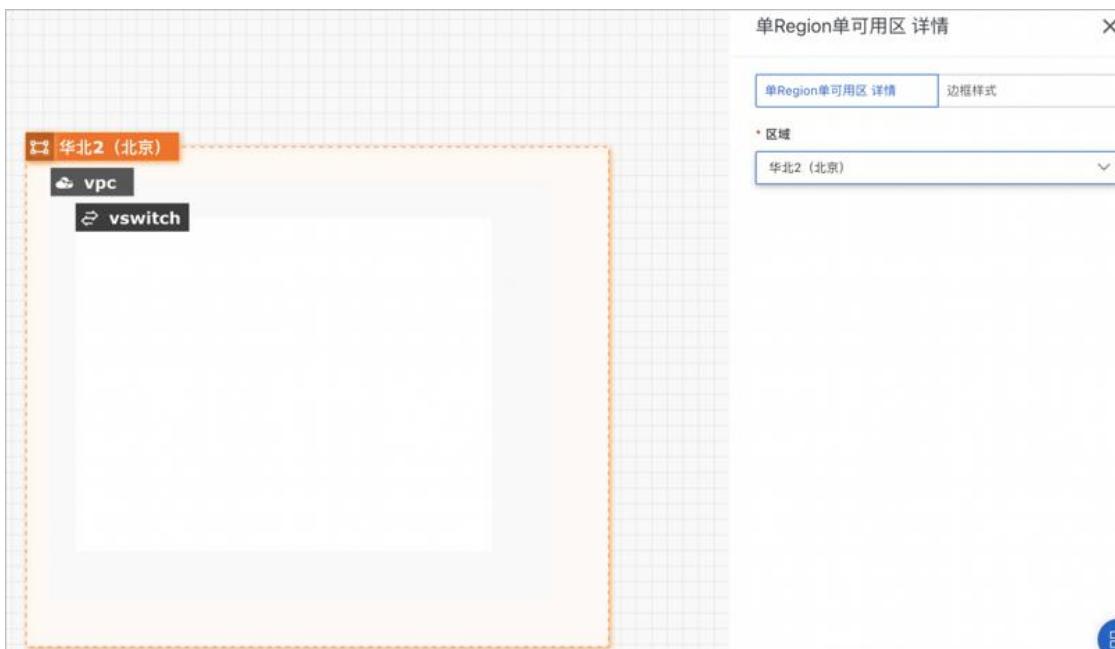


步骤4 依次双击Region、VPC、vswitch进行配置。

1. 双击region，在右侧弹出窗口中，选择华北2（北京）。



选择后，如下图所示：



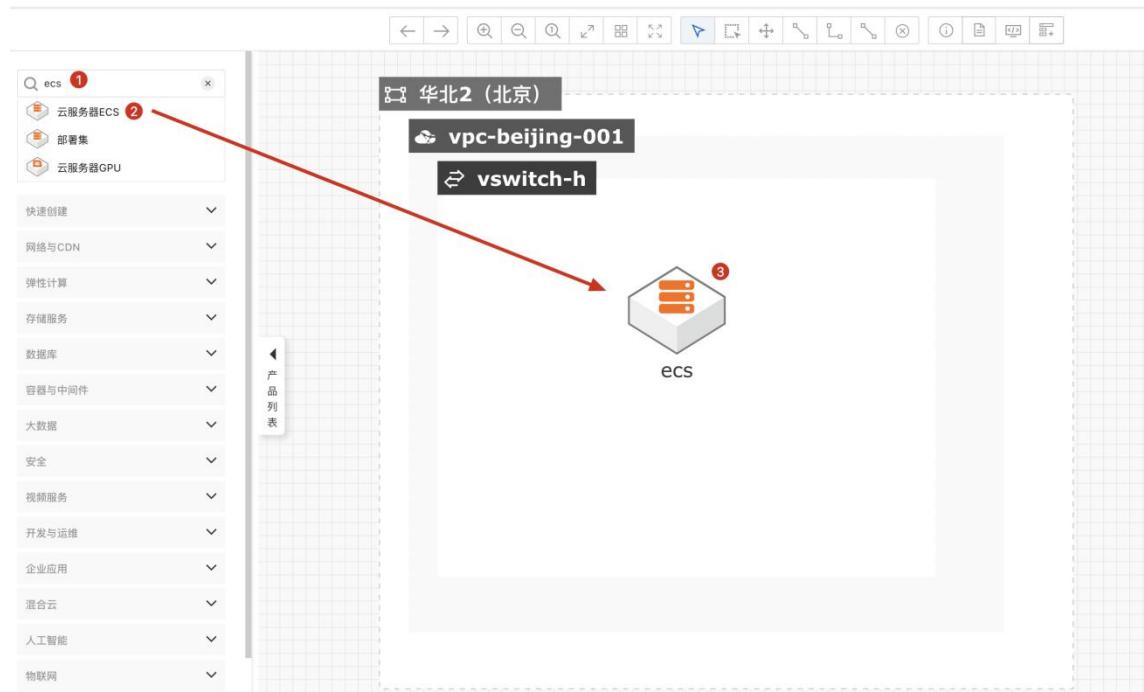
2. 双击VPC，配置VPC参数。



3. 双击 Vswitch，配置 vswitch 参数。



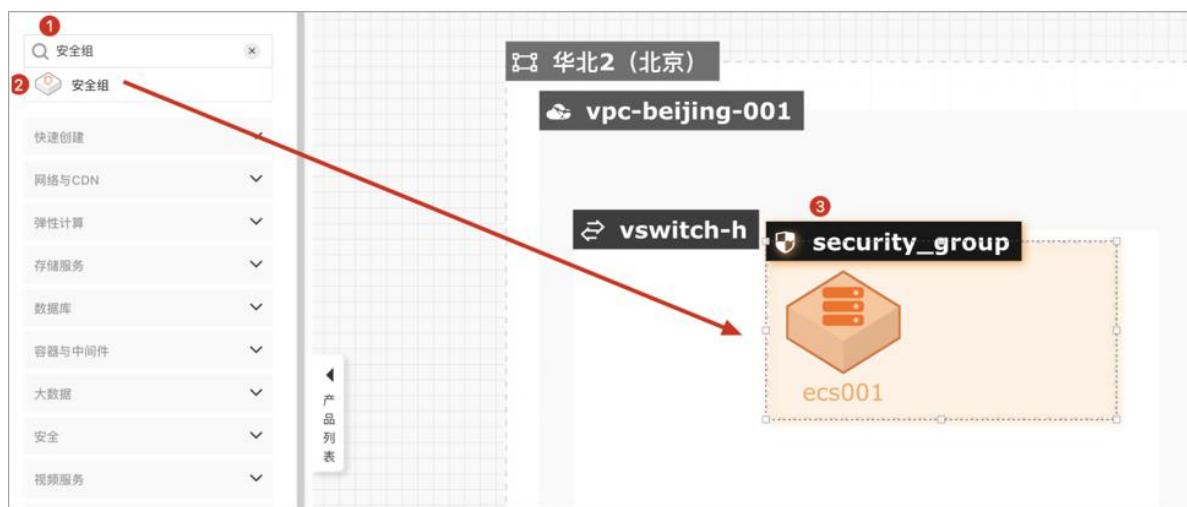
步骤 5 左侧搜索 ECS，拖到 vswitch 中。



步骤 6 双击 ECS，选择参数

配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs001
支付方式	按量付费
实例规格	ecs.c6a.large(2c 4g)
镜像	Alibaba Cloud Linux
镜像版本	Alibaba Cloud Linux 3.2104 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
主机名	ecs001
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>

步骤 7 搜索安全组，拖入一个安全组，将 ECS 放在安全组的框内。



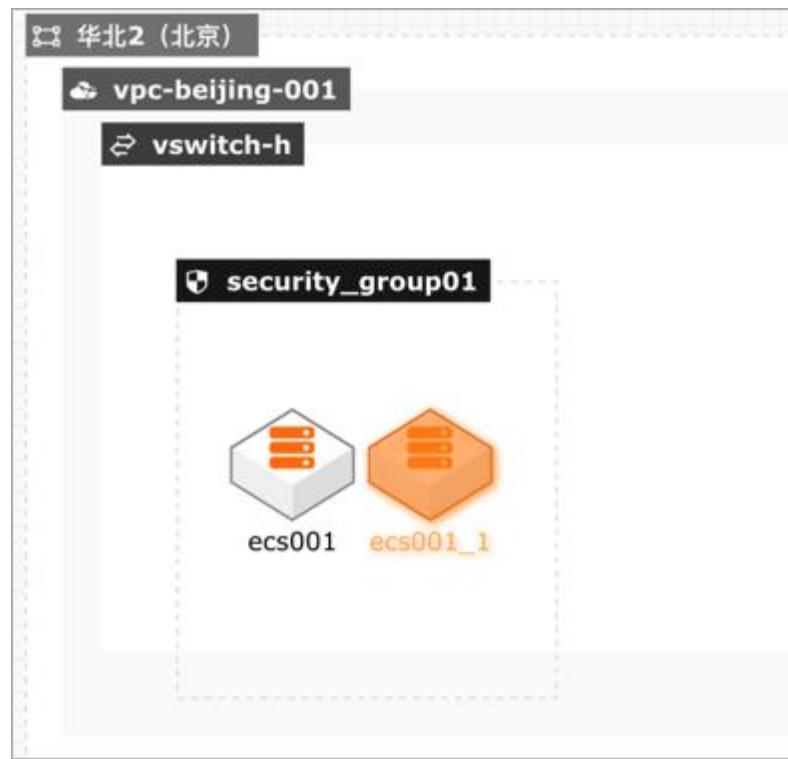
步骤 8 双击安全组，修改安全组参数。

The screenshot shows the configuration details for the 'node.security\_group'. It includes fields for the security group name ('security\_group01'), type ('普通安全组'), and a detailed view of a security rule. The rule configuration is as follows:

- 规则的类型:** 入方向
- 授权策略:** 允许
- 优先级:** 1
- 协议类型:** 全部ICMP(IPv4)
- 端口范围:** -1/-1
- 网络类型:** intranet
- 目标IP地址范围:** 0.0.0.0/0

At the bottom, there is a button labeled '删除这条规则' (Delete this rule).

步骤 9 右键 ECS 图标，选择复制。



步骤 10 单击 ecs001\_1 修改其名称为 ecs002，主机名也修改为 ecs002。

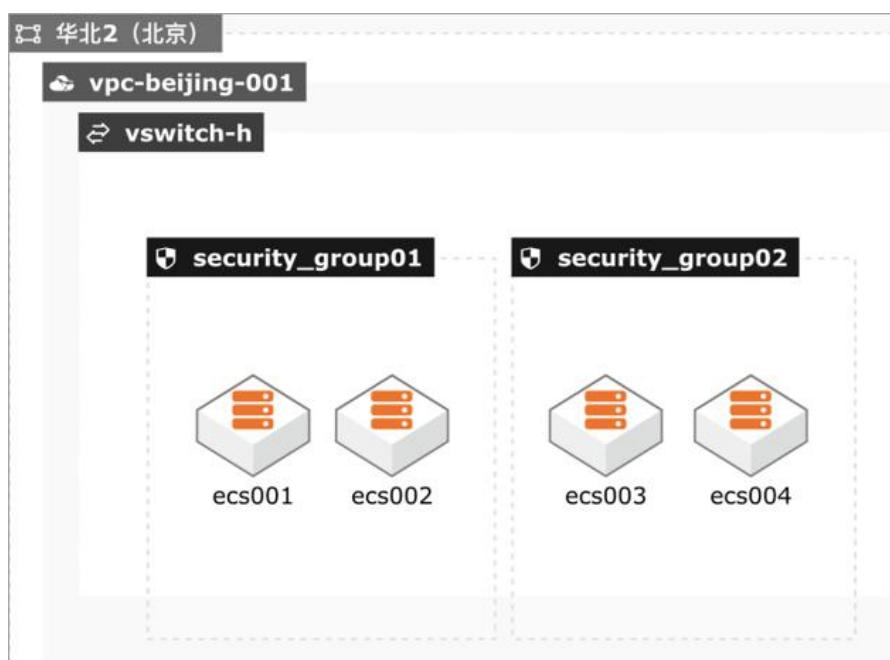
A screenshot of a dialog box for modifying an instance. It has a field labeled "\* 实例名称" (Instance Name) with the value "ecs002". There is also a close button "x" in the top right corner.



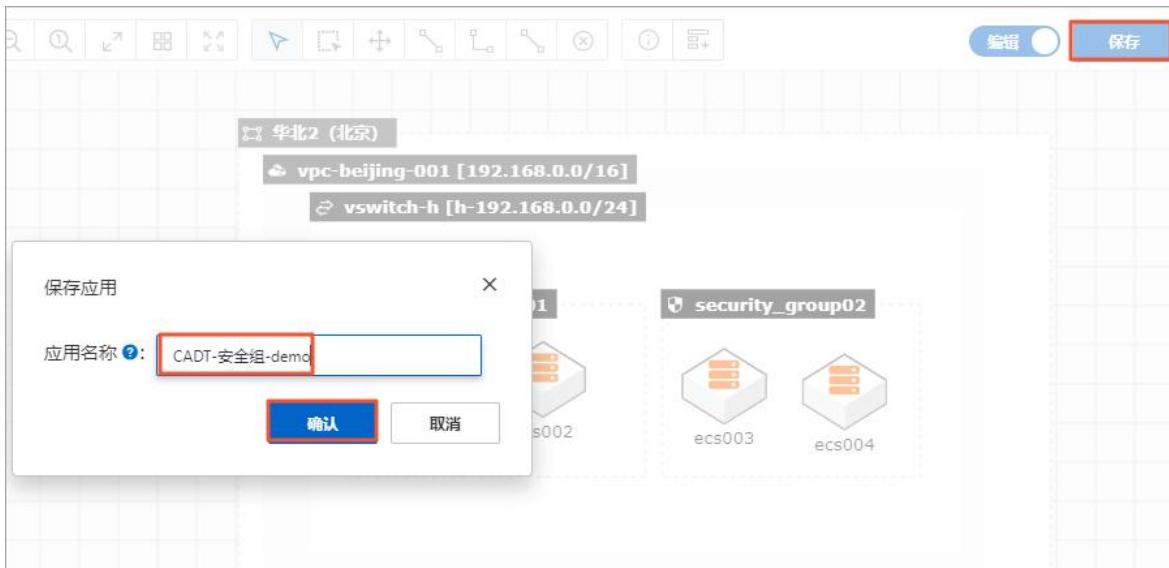
修改完成后如下图所示：



步骤 11 参考以上步骤，扩展成如下架构图：

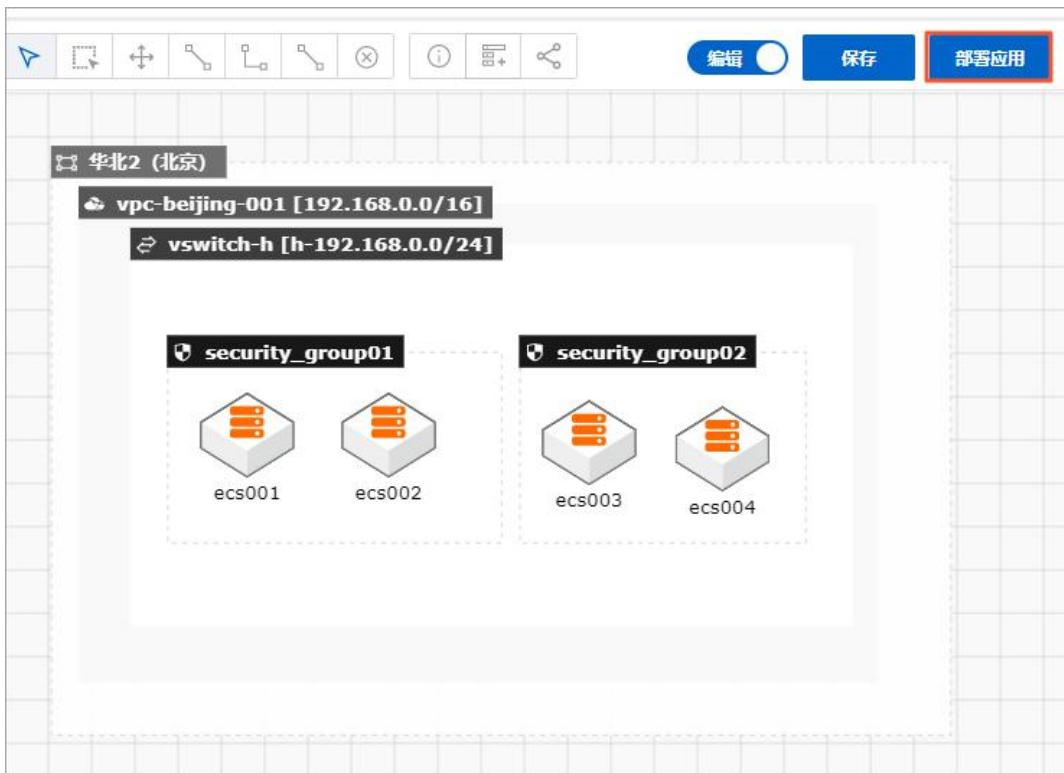


步骤 12 单击右上角的保存，填写应用名称。



### 3.15.3. 部署应用

步骤 13 应用保存完成后，单击右上角的部署应用。

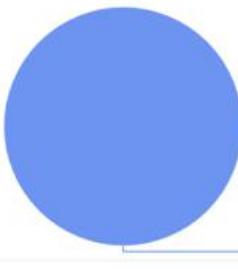


步骤 14 弹出如下校验页面，这里会校验参数配置是否合法、ECS 是否有库存等，一般需要几十秒左右。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-h	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	ecs003	ecs	北京	ecs.c6a.large	成功	校验通过	定位
3	vpc-beijing-001	vpc	北京	192.168.0.0/16	成功	校验通过	定位
4	security_group02	security.group	北京	normal	成功	校验通过	定位
5	ecs001	ecs	北京	ecs.c6a.large	成功	校验通过	定位
6	security_group01	security.group	北京		成功	校验通过	定位
7	ecs002	ecs	北京	ecs.c6a.large	成功	校验通过	定位
8	ecs004	ecs	北京	ecs.c6a.large	成功	校验通过	定位

状态:校验成功
下一步: 价格清单
返回

步骤 16 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息，查看计费详情。分别查看包年包月的价格和按量付费的价格。

导出价格清单																	
免费		按量付费															
资源成本占比																	
 资源预算 <input checked="" type="radio"/> 计算 计算: <span style="background-color: #e0f2e0;">  </span> 元/时																	
价格列表																	
序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作								
1	ecs004	ecs	北京	ecs.c6a.large	1	0.34元/时	省 <span style="background-color: #e0f2e0;">  </span> /时	元/时	定位								
2	ecs003	ecs	北京	ecs.c6a.large	1	0.34元/时	省 <span style="background-color: #e0f2e0;">  </span> /时	元/时	定位								
3	ecs001	ecs	北京	ecs.c6a.large	1	0.34元/时	省 <span style="background-color: #e0f2e0;">  </span> /时	元/时	定位								
4	ecs002	ecs	北京	ecs.c6a.large	1	0.34元/时	省 <span style="background-color: #e0f2e0;">  </span> /时	元/时	定位								

状态: 计价成功
上一步: 资源校验
查看报告
下一步: 确认订单

步骤 16 可以单击**查看报告**, 查看应用的价格信息。



步骤 17 单击**下一步：确认订单**, 在新的窗口中, 勾选《云速搭服务条款》, 这里会显示价格信息, 按量的会按小时扣除, 包年包月的会一次性扣除 (如有)。

**确认订单**

免费  按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	ecs002	ecs	北京	ecs.c6a.large	1	0.34元/时	0.34元/时	新购
2	ecs001	ecs	北京	ecs.c6a.large	1	0.34元/时	0.34元/时	新购
3	ecs003	ecs	北京	ecs.c6a.large	1	0.34元/时	0.34元/时	新购
4	ecs004	ecs	北京	ecs.c6a.large	1	0.34元/时	0.34元/时	新购

**《云速搭服务条款》**  
部署前, 请阅读并勾选服务条款

按量付费: 0.34元/时

状态: **计价成功**

[上一步: 价格清单](#) [下一步: 支付并创建](#)

步骤 18 单击**下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。

**资源部署状态**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
				部署中	不要进行任何操作，请耐心等待...	

**部署概要**

状态：部署中 方案编号：HC80P8WFYBEU3C3E

[返回](#)

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
4	security_group0_2	security.group	-	sg-2zefrzfyz6mmj2iepl7o	运行中	2021-11-12 16:12:36	定位
5	ecs003	ecs	按量付费	i-2ze78zfakirexl7gxizw	运行中	2021-11-12 16:13:14	定位
6	ecs001	ecs	按量付费	i-2zeiomrd9angh17ufk0c	运行中	2021-11-12 16:13:14	定位
7	ecs004	ecs	按量付费	i-2zebpf4cjh3prct08tom	运行中	2021-11-12 16:13:14	定位
8	ecs002	ecs	按量付费	i-2ze8q3x4yum821xrrgo1	运行中	2021-11-12 16:13:14	定位

**部署概要**

状态：部署成功 方案编号：6Y8EUT13Z1I2ZWM

[查看报告](#) [返回](#)

步骤 19 部署完成后，单击**查看报告**，可以查看本次的部署报告。



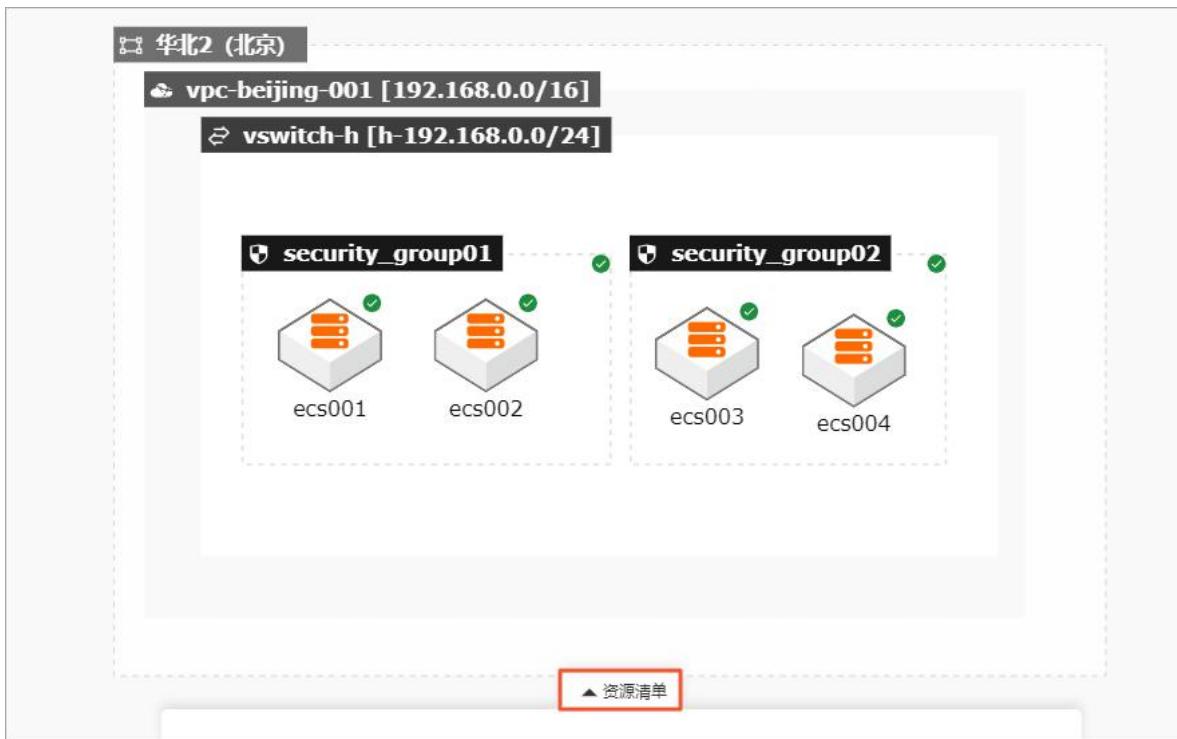
步骤 20 单击返回，然后单击资源清单。

资源部署状态							
序号	资源名称 <a href="#">?</a> <a href="#">Q</a>	资源类型 <a href="#">Q</a>	付费类型	资源ID <a href="#">Q</a>	资源状态	资源更新时间	定位
1	vpc-beijing-001 [1 92.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zew760ist4bvbjklwyp <a href="#">D</a>	运行中	2021-11-17 17:06:09	<a href="#">定位</a>
2	security_group02	security.group (node.security_group)	-	sg-2zee5xbe74yev5ccd40u <a href="#">D</a>	运行中	2021-11-17 17:06:09	<a href="#">定位</a>
3	vswitch-h [h-192.1 68.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zekvt3vkhwvc59im9oq <a href="#">D</a>	运行中	2021-11-17 17:06:55	<a href="#">定位</a>
4	security_group01	security.group (node.security_group)	-	sg-2ze8e0o1xz2v3r862ung <a href="#">D</a>	运行中	2021-11-17 17:06:09	<a href="#">定位</a>

**部署概要**

状态: 部署成功 方案编号: J6X7J76CJ12P35UJ

[查看报告](#) [返回](#)



序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
4	security_group01	(node.security_group)	-	sg-00000000000000000	新建	运行中	2021-11-17 17:06:55	定位	详情 监控 变更日志 操作
5	ecs004	ECS (云服务器ECS)	按量付费	i-2ze69inctxw1h2ep1sovuv	新建	运行中	2021-11-17 17:06:55	定位	详情 监控 变更日志 操作
6	ecs002	ECS (云服务器ECS)	按量付费	i-2ze3ccvju3wzlynzscq	新建	运行中	2021-11-17 17:06:55	定位	详情 监控 变更日志 操作

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 21 单击安全组后，跳转到安全组控制台查看。

The screenshot shows the VPC configuration for 'vpc-beijing-001'. It displays two security groups, 'security\_group01' and 'security\_group02', each associated with two ECS instances (ecs001, ecs002 and ecs003, ecs004). A resource list below shows the details of these resources.

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间
3	vswitch-h [h-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zekvt3vkhwy59im9oq	新建	运行中	2021-11-17 17:06
4	<b>security_group01</b>	security_group (node.security_group)	-	sg-2ze8e0o1xz2v3r862ung	新建	运行中	2021-11-17 17:06

This screenshot shows the 'security\_group01' configuration. It includes basic information like the security group ID and type, and a detailed view of its rules. The rules table lists four entries allowing traffic from 0.0.0.0/0 to specific ports (3389, 22/22, 80/80, 443/443) on port 1.

授权策略	优先级	协议类型	端口范围	授权对象	描述
<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	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: 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	

步骤 22 登录 ecs，验证安全组规则，单击 ecs001，跳转到控制台。

This screenshot shows a list of ECS instances. The instance 'ecs001' is highlighted with a red box, indicating it is the target for further action.

序号	资源名称	资源类型	付费类型	资源ID	来源
5	ecs003	ecs	按量付费	i-2ze78zfakirel7gixzw	新建
6	<b>ecs001</b>	ecs	按量付费	i-2zeiomrd9angh17ufk0c	新建
7	ecs004	ecs	按量付费	i-2zebpf4cjh3prct08tom	新建
8	ecs002	ecs	按量付费	i-2ze8q3x4y়um821xrrgo1	新建

步骤 23 单击远程连接。

← ecs001 ▾

实例详情	监控	安全组	云盘	实例快照	快照	弹性网卡	远程命令/文件	操作记录	健康诊断
基本信息									
ecs001 ✅ 运行中					诊断健康状态 NEW   启动   重启   停止				
实例ID	i-2zeiomrd9angh17ufk0c	远程连接	地域	华北2 (北京)					
资源组:	-		所在可用区	北京 可用区H					
公网IP	-	绑定弹性IP	主机名	ecs001					
安全组	sg-2zee8hlgm9k49qg52yja	加入安全组	创建时间	2021年11月12日 16:12:00					
标签	-	编辑标签	自动释放时间	-					
描述	-	修改实例描述							

远程连接与命令 ②

X

Workbench远程连接

通过网页可以对ECS实例进行远程控制，支持复制粘贴文本，支持多操作系统用户登录同一台实例，支持可视化查看系统文件资源。

立即登录

VNC远程连接 ②

立即登录

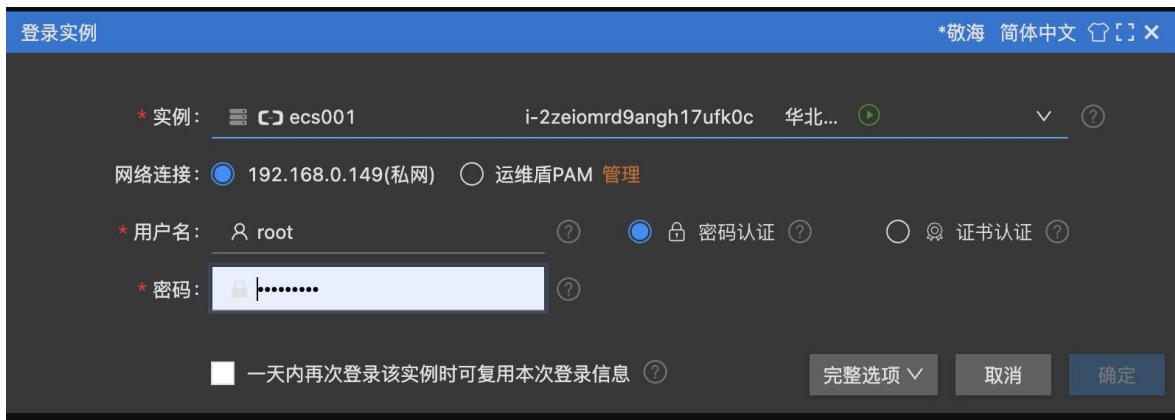
发送远程命令 (云助手) 推荐

发送远程命令可以帮助您在实例内部快速执行命令，即无需远程连接登录实例，即可完成查看硬盘空间、安装软件、启动停止服务等操作。该功能通过 云助手 的命令执行功能实现，如果您的实例还没有安装或激活云助手客户端，请先 安装或者激活。

发送远程命令

取消

步骤 24 在新打开的页面，输入用户名和密码，单击确定。



步骤 25 登录后如下图所示：

```
Welcome to Alibaba Cloud Elastic Compute Service !
Last login: Fri Nov 12 16:18:08 2021 from 100.104.192.167
[root@ecs001 ~]#
```

步骤 26 在 ECS 控制台，查看各个 ecs 的内网 ip 地址。

实例 ID / 名称	状态	标签	操作系统	监控	可用区	配置
i-2ze8q3x4yum821xrrgo1 ecs002	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)
i-2zebpf4cjh3prct08tom ecs004	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)
i-2zeiomrd9angh17ufk0c ecs001	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)
i-2ze78zfakirexl7gxizw ecs003	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)

按照 [https://help.aliyun.com/document\\_detail/25387.html](https://help.aliyun.com/document_detail/25387.html) 这里的描述，普通安全组中：

- 在安全组未添加安全组规则时，不同安全组内的实例之间内网隔离。
- 在安全组未添加安全组规则时，拒绝所有入方向的访问请求。

这里应该两个安全组内的是可以 ping 通的，组之间是不通的。

我们在 ecs001 上分别 ping 另外三个节点，来看效果。

步骤 27 修改/etc/hosts 如下：

```
[root@ecs001 ~]# vim /etc/hosts
[root@ecs001 ~]# cat /etc/hosts
::1      localhost      localhost.localdomain  localhost6      localhost6.localdomain6
127.0.0.1    localhost      localhost.localdomain  localhost4      localhost4.localdomain4

192.168.0.149  ecs001
192.168.0.151  ecs002
192.168.0.148  ecs003
192.168.0.150  ecs004

[root@ecs001 ~]#
```

效果如下：

```
[root@ecs001 ~]# ping ecs002
PING ecs002 (192.168.0.151) 56(84) bytes of data.
64 bytes from ecs002 (192.168.0.151): icmp_seq=1 ttl=64 time=0.479 ms
64 bytes from ecs002 (192.168.0.151): icmp_seq=2 ttl=64 time=0.189 ms
64 bytes from ecs002 (192.168.0.151): icmp_seq=3 ttl=64 time=0.128 ms
^C
--- ecs002 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2080ms
rtt min/avg/max/mdev = 0.128/0.265/0.479/0.153 ms
[root@ecs001 ~]# ping ecs003
PING ecs003 (192.168.0.148) 56(84) bytes of data.

^C
--- ecs003 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3100ms

[root@ecs001 ~]# ping ecs004
PING ecs004 (192.168.0.150) 56(84) bytes of data.
```

是符合预期的。

### 3.15.4.CADT 部署企业安全组

释放以上应用，将安全组修改为企业安全组，再次进行效果验证。

步骤 28 打开资源清单，单击释放全部资源。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
5	ecs003	ecs	按量付费	i-2ze78zfakirext7gxizw	新建	运行中	2021-11-12 16:13:14	定位	详情 监控 变更日志
6	ecs001	ecs	按量付费	i-2zeiomrd9angh17ulk0c	新建	运行中	2021-11-12 16:13:14	定位	详情 监控 变更日志

步骤 29 单击确定。



步骤 30 输入校验码。



步骤 31 等待释放完成，单击返回按钮。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001	vpc	-	vpc-2zerdfjjsoi1sgr53a85h	已删除	2021-11-12 17:22:02	定位
2	vswitch-h	vswitch	-	vsw-2ze67yc3gow8300iuii59	已删除	2021-11-12 17:22:02	定位
3	security_group01	security.group	-	sg-2zee8hlgm9k49qg52yja	已删除	2021-11-12 17:21:14	定位
4	security_group02	security.group	-	sg-2zefrzfyz6mmj2iepl7o	已删除	2021-11-12 17:21:14	定位
5	ecs003	ecs	按量付费	i-2ze78zfakirexl7gxizw	已删除	2021-11-12 17:20:40	定位

**部署概要**

状态: 释放成功

方案编号: 6Y8EUT13Z1Z4ZWM

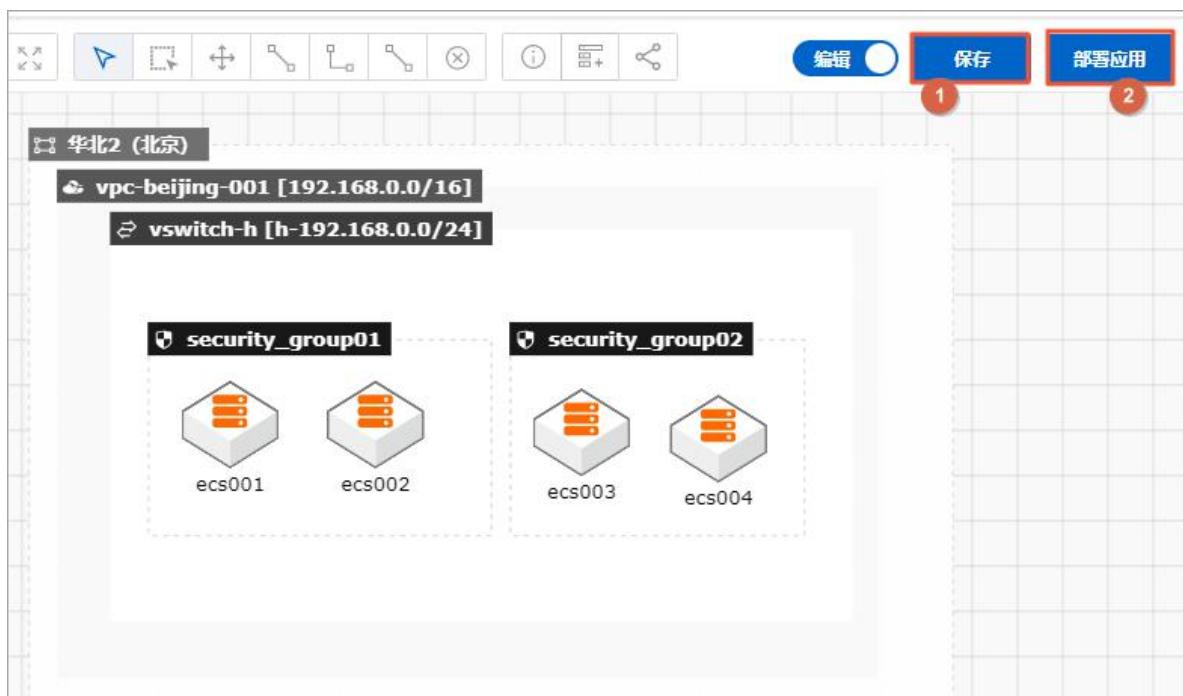
**返回**

步骤 32 切换到编辑模式。

步骤 33 分别双击两个安全组，修改安全组类型为企业级安全组。



步骤 34 重新保存并部署。



部署完成后，如下图所示：



### 步骤 35 校验企业安全组隔离效果

1. 重新部署后，各个 ecs 的内网 ip 地址如下：

实例 ID / 名称	状态	标签	操作系统	监控	可用区	配置	IP 地址
i-2zej9jlwf5e1vn805pkd ecs002	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)	192.168.0.49 (私有)
i-2zeiomrd9angi8mj03te ecs004	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)	192.168.0.48 (私有)
i-2zeiomrd9angi8mj03td ecs001	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)	192.168.0.47 (私有)
i-2zeg6twivvbluk52fsx ecs003	运行中				北京 可用区H	2 核 4 GiB (I/O 优化) ecs.c6a.large 0 Mbps (峰值)	192.168.0.46 (私有)

2. 登录 ecs001，分别 ping 其他几个节点，查看效果。

3. 修改/etc/hosts 如下

```
[root@ecs001 ~]# vim /etc/hosts
[root@ecs001 ~]# cat /etc/hosts
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

192.168.0.47    ecs001
192.168.0.49    ecs002
192.168.0.46    ecs003
192.168.0.48    ecs004
```

4. 检查 ping 效果，都不通，符合预期。

```
[root@ecs001 ~]# ping ecs002
PING ecs002 (192.168.0.49) 56(84) bytes of data.
^C
--- ecs002 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2058ms

[root@ecs001 ~]# ping ecs003
PING ecs003 (192.168.0.46) 56(84) bytes of data.
^C
--- ecs003 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1033ms

[root@ecs001 ~]# ping ecs004
PING ecs004 (192.168.0.48) 56(84) bytes of data.
^C
--- ecs004 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1029ms

[root@ecs001 ~]#
```

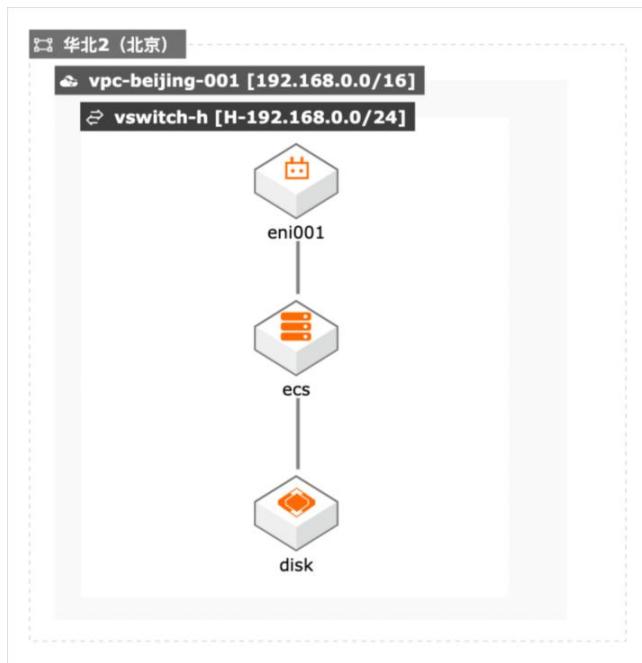
## 3.16.云速搭部署 ECS 最佳实践

作者 | 阿里云解决方案架构师 敬海

### 3.16.1.云速搭架构设计

#### 方案架构

通过云速搭实现 ECS 的部署，具体为使用自定义镜像，秘钥登录，外接 eni 和云盘的一个 ECS 实例的部署。



### 3.16.2.准备工作

#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
ECS	vswitch 交换机

## 地域和可用区规划

地域规划在华北 2 (北京)，可用区选择 cn-beijing-h 可用区。

## 检查自定义镜像

步骤 1 打开对应地域的镜像列表

<https://ecs.console.aliyun.com/image/region/cn-beijing/imageList>

步骤 2 确保这里有自定义镜像，这里以图中的镜像为例。

镜像名称	镜像ID/名称	镜像族系	标签	操作系统	平台	系统位数	状态(全部)	进度	创建时间	操作
m-2zeqjv6bn7b9p2mjme imagenet2012-full	m-2zeqjv6bn7b9p2mjme	未指定	未指定	CentOS	64位	可用	100%	2021年9月17日 16:13:01	创建实例 复制镜像 共享镜像	

## 创建密钥

步骤 3 在对应的地域创建秘钥。(<https://ecs.console.aliyun.com/keyPair/region/cn-beijing>)

阿里云 | 工作台 | 账号全部资源 | 华北2 (北京) | 搜索...

概览  
事件  
标签  
自助问题排查  
应用管理  
我的常用  
实例与镜像  
网络与安全  
安全组  
弹性网卡  
**密钥对** ②  
专有网络 VPC

**密钥对**

创建密钥对 密钥对名称 输入密钥对名称查询 标签

密钥对名称	标签	密钥对指纹
key1203		

没有查询到符合条件的结果

创建密钥对 [返回密钥对列表](#)

1  
\*密钥对名称: key1203  
长度为2~128个字符。不能以特殊字符及数字开头，只可包含特殊字符中的点号(.)、下划线(\_)、连字符(-)和空格。

\*创建类型:  自动创建密钥对  导入已有密钥对  
创建完成后请一定下载私钥，您只有一次下载私钥的机会。

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

2 确定 取消

步骤 4 创建成功后如下图所示：

云服务器 ECS / 密钥对

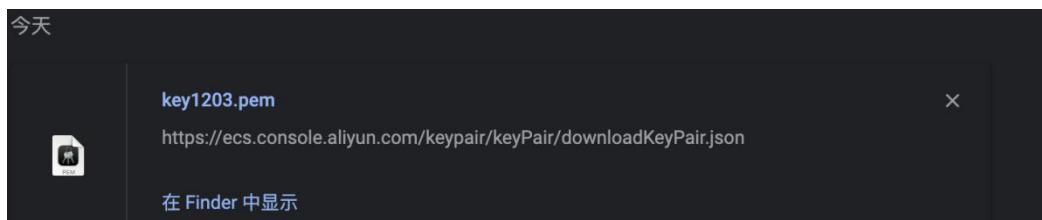
**密钥对**

创建密钥对 密钥对名称 输入密钥对名称查询 标签

密钥对名称	标签	密钥对指纹	密钥对创建时间	操作
key1203		[REDACTED]	2021年12月3日 11:39	<a href="#">锁定密钥对</a>   <a href="#">解绑密钥对</a>

共有1条, 每页显示: 50

步骤 5 浏览器自动下载了如下 pem 文件，保存备用。



## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
ECS	ecs001	

### 3.16.3.应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通

云速搭 CADT 公共云

专利号: CN111930290B 查看最佳实践

新建 应用 资源 导出

欢迎使用云速搭!

应用全量 全部应用 部署成功 下线应用

中国

未分配区域

应用名称	创建时间	状态
没有数据		

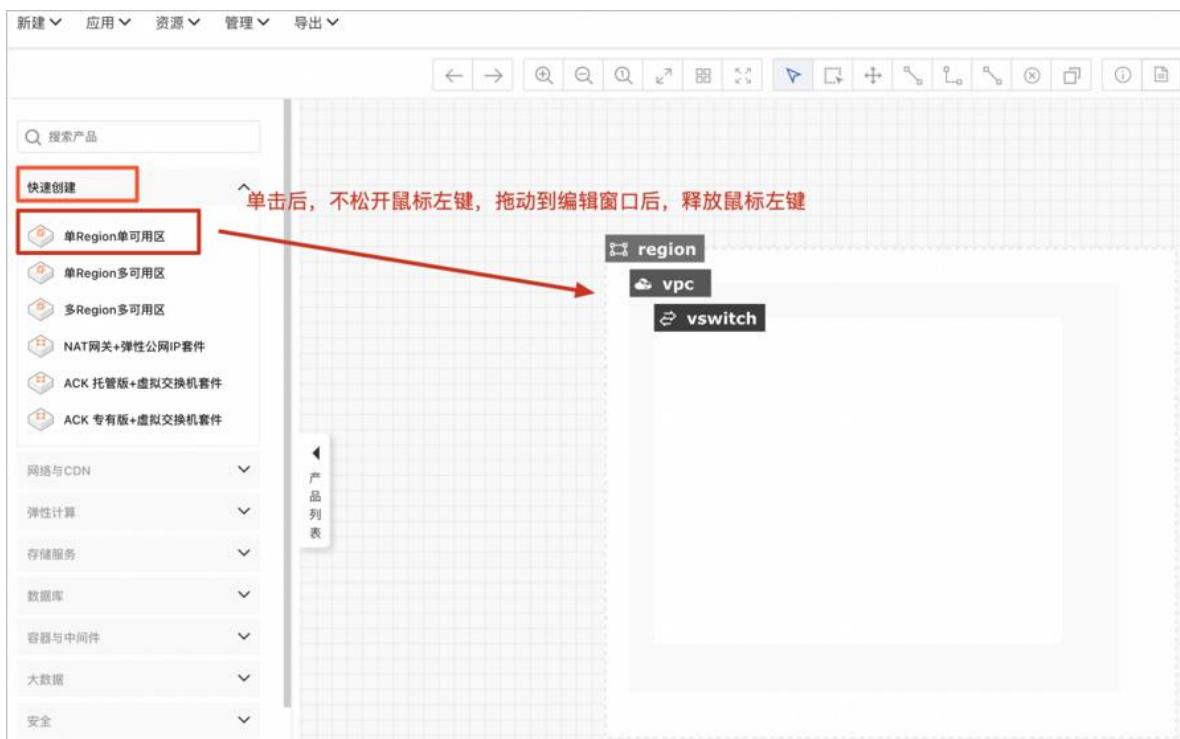
产品动态

- 支持用户对应用进行架构探查，自动生成已有应用的架构 新功能 2021年9月31日
- 支持RAM权限管理，对子用户授予不同的权限和资源组，控制子用户对资源的访问和操作 新功能 2021年9月31日
- 支持应用状态实时更新，实时更新服务的状态和配置 新功能 2021年9月30日

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

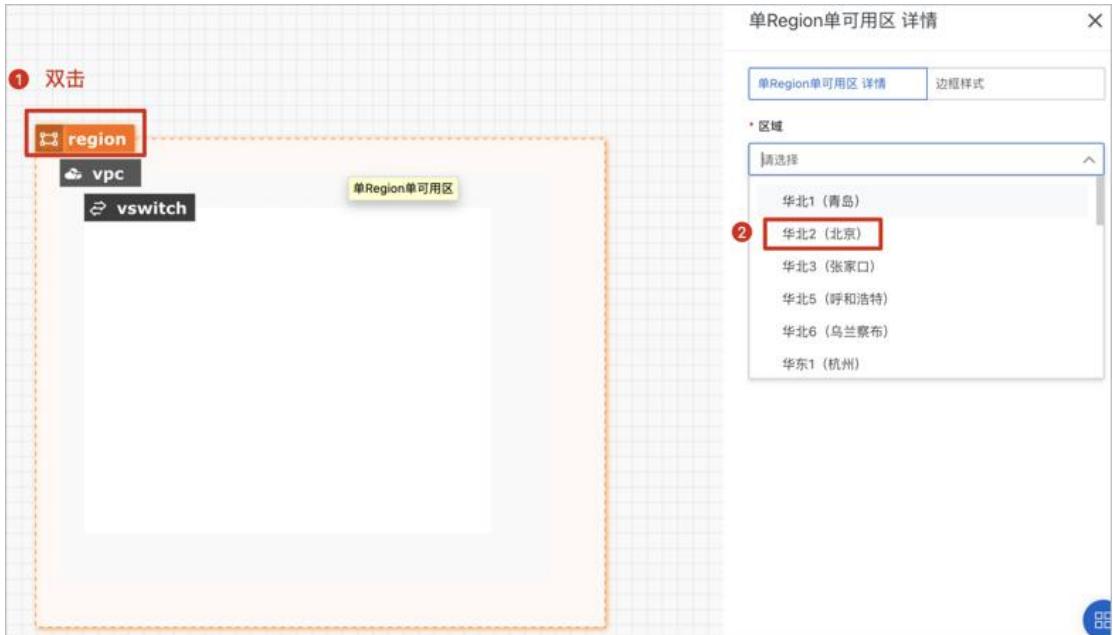


步骤 3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

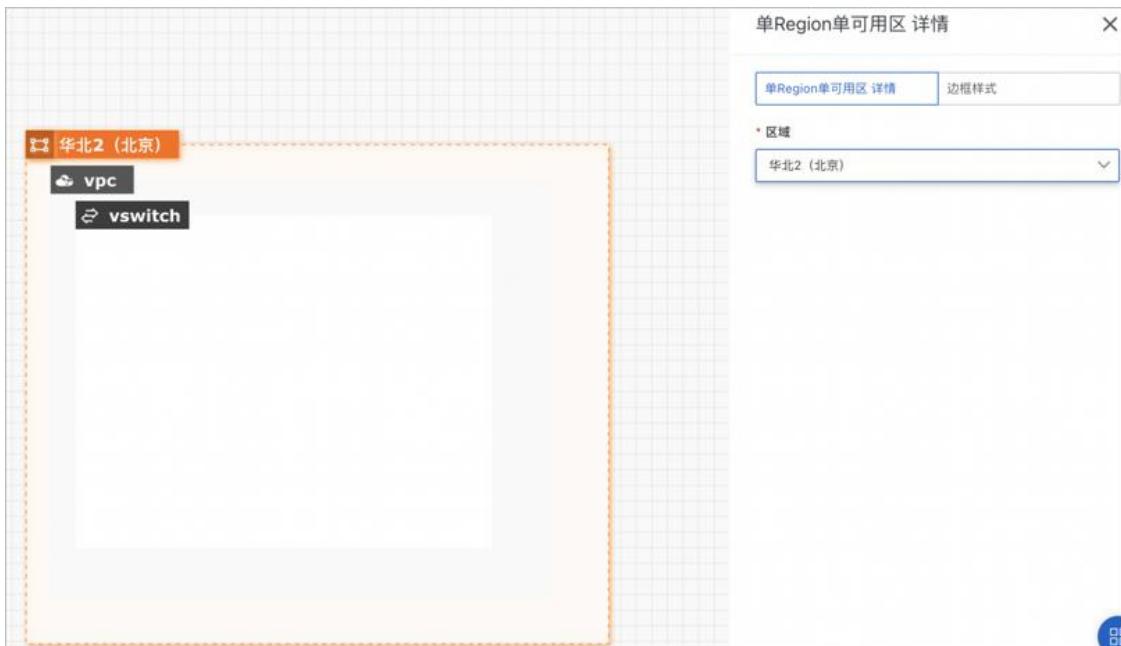


步骤 4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



选择后，如下图所示：



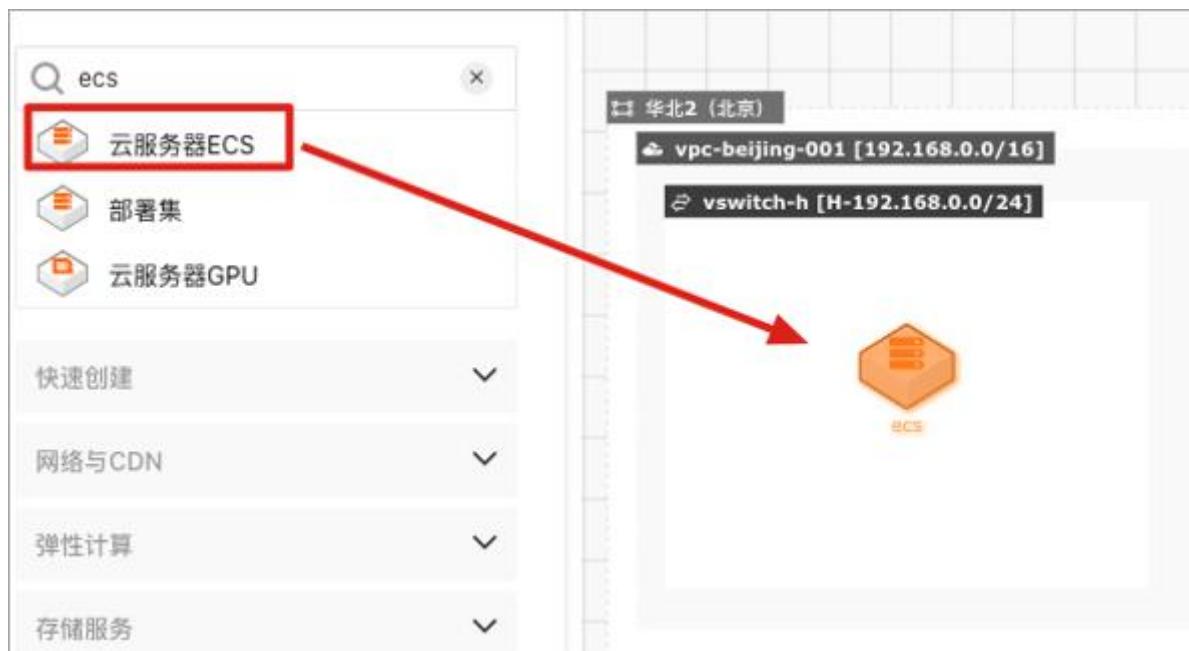
2. 双击 VPC，配置 VPC 参数。



3. 双击 vswitch，配置 vswitch 参数。



步骤 5 搜索 ecs，并拖入一个 ecs 到 vswitch-h 中。



步骤 6 双击 ECS，配置参数：

This screenshot shows the configuration page for creating a new ECS instance. The fields filled in are:

- 可用区**: 华北 2 可用区 H
- 实例名称**: ecs
- 数量**: 1
- 支付方式**: 按量付费
- 实例规格**: ecs.c6a.large (2c 4g)
- 镜像**: 自定义镜像
- 镜像版本**: imangenet2012-full/m-2zecjv6bnl7b9p2rmjme[linux]
- 系统盘类型**: ESSD云盘
- 系统盘容量**: 500
- 性能级别**: PL0 (单盘IOPS性能上限1万)
- 数据磁盘**: data\_disks = [ ]
- 公网 IP**: 分配公网 IPv4 地址 (checked)
- 带宽计费模式**: 按流量付费
- 带宽 (峰) 值**: 100 (with a plus sign icon)

**带宽 (峰) 值** i

1
——
100
1
Mbps

**主机名** i

×

**有序后缀** i

**资源标签**

无数据原因如下：

- 1.当前vswitch所选可用区下无可售资源
- 2.以上属性配置组合下无可售资源

请填写标签键
:
请填写标签值
面

+
(1/20)

1.资源标签键不可以重复，最长为64个字符。

**登录凭证**

使用密钥
▼

密钥
key1203
▼

**安全加固** i

请选择
▼

**自动释放时间** i

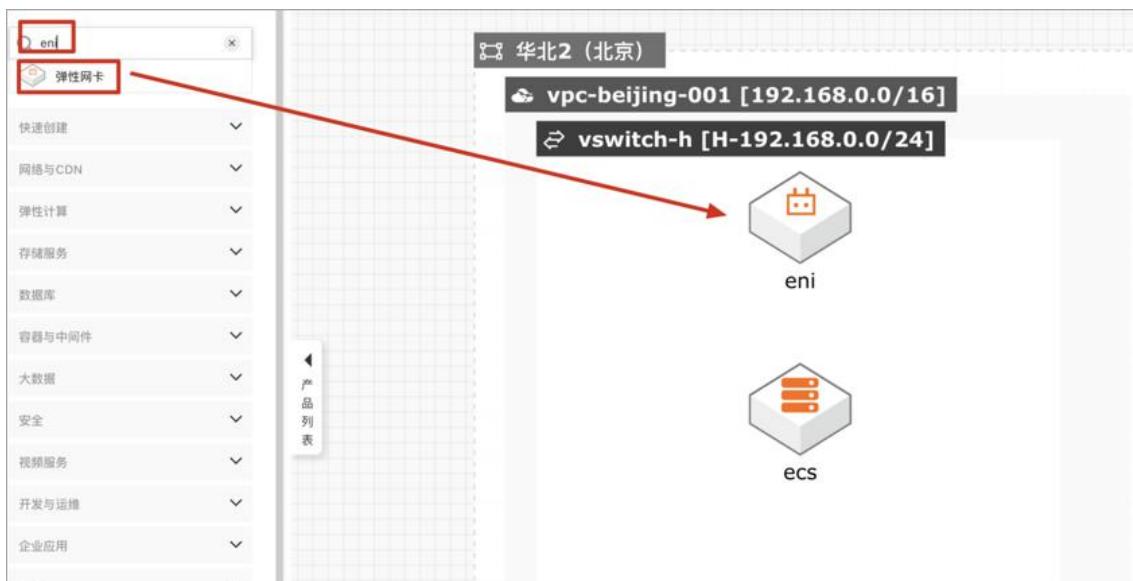
请选择日期和时间
面

**实例自定义数据** i

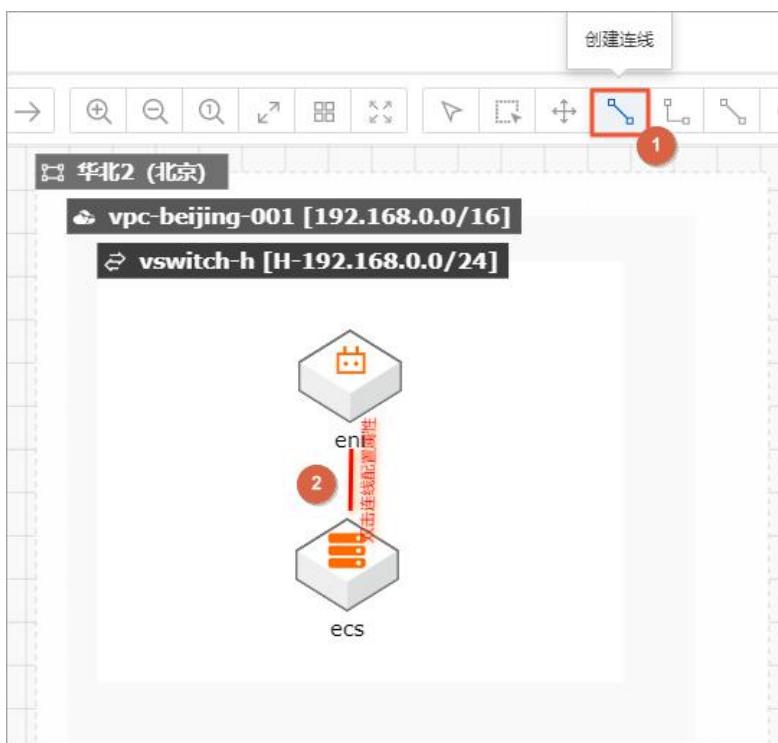
**实例私网IP地址** i

关闭

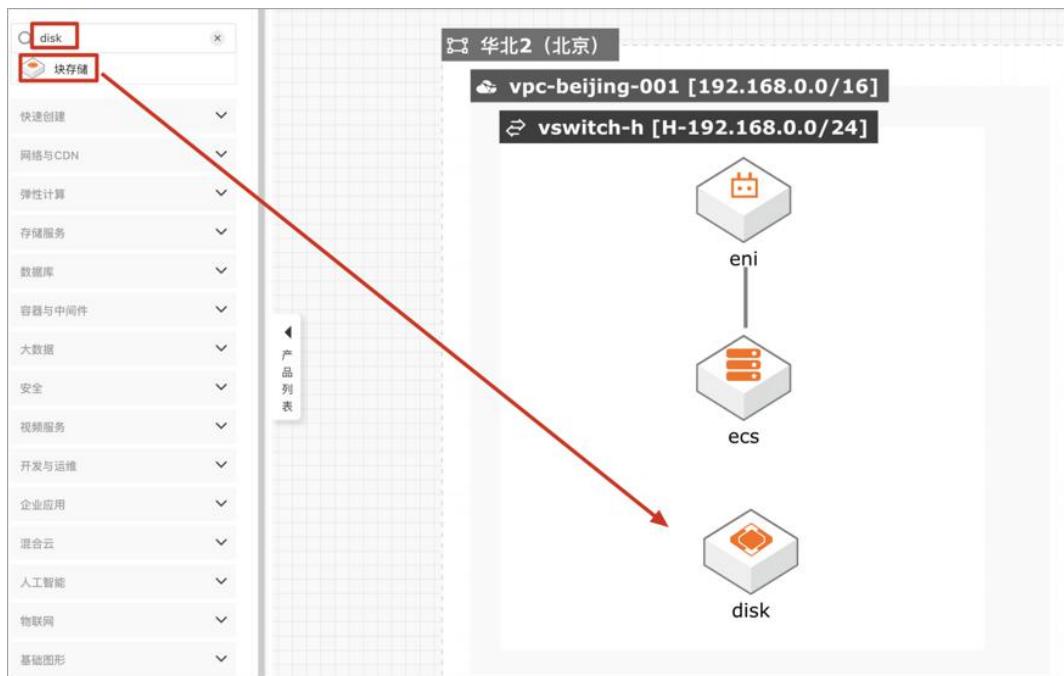
步骤 7 搜索 eni，拖入 vswitch 中。



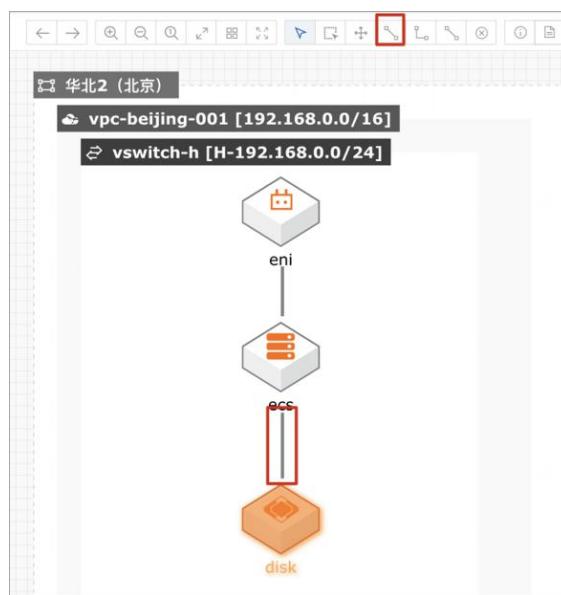
步骤 8 切换到连线模式，将 eni 和 ecs 连接起来。



步骤 9 搜索 disk，并拖入 vswitch 中。



步骤 10 切换到连线模式，将 ecs 和 disk 连接起来。



步骤 11 双击 eni 配置 eni 的参数

\* 网卡名称

主私网IP

辅助私网IP   
private\_ips = [  
]  
+

辅助私网IP数量

标签映射  :   
+  
(1/20)

1. 标签映射键不可以重复,最长为64个字符;  
2. 标签映射值可以为空,最长为128个字符;  
3. 标签映射键和标签映射值都不能以"aliyun", "acs:", "http://"或 "https://"开头;

关闭

步骤 12 双击 disk, 配置 disk 参数。

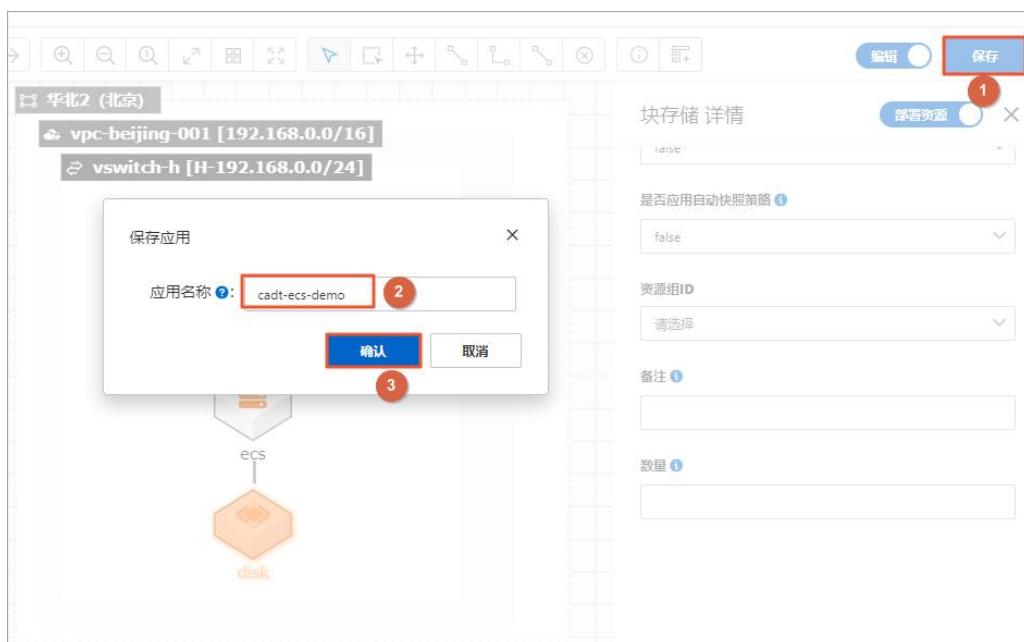
The left form is titled "购买方式" (Purchase Method) and includes fields for:

- 新购 (New Purchase)
- disk名 (Disk Name): disk
- 可用区 (Availability Zone): 华北 2 可用区 H
- 分类 (Category): ESSD 云盘
- 数据盘大小 (Data Disk Size): 100 GiB
- 性能级别 (Performance Level): PLO (单盘IOPS性能上限1万)
- 快照id (Snapshot ID): (empty)
- 磁盘是否加密 (Disk Encryption): false

The right form is titled "快照id" (Snapshot ID) and includes fields for:

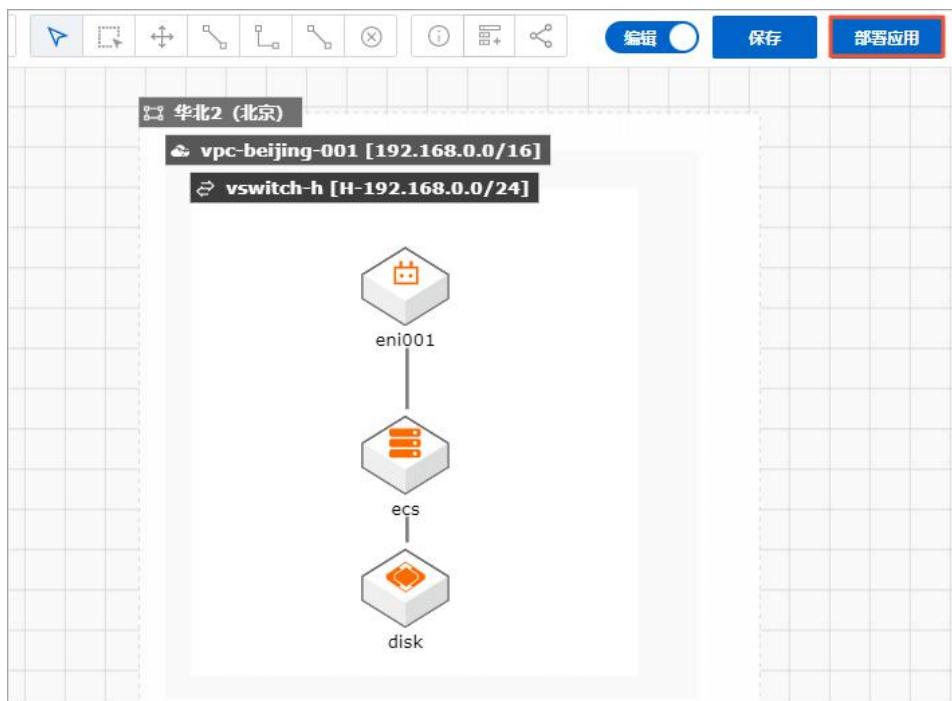
- 快照id (Snapshot ID): (empty)
- 磁盘是否加密 (Disk Encryption): false
- 删除自动快照 (Delete Auto Snapshot): false
- 是否与实例一起释放 (Release with Instance): false
- 是否应用自动快照策略 (Apply Auto Snapshot Policy): false
- 资源组ID (Resource Group ID): 请选择 (Select)

步骤 13 单击右上角的**保存**, 填写应用名称为 **cadt-ecs-demo**



## 3.16.4.部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、ECS 是否有库存等，一般需要几十秒左右。

等待校验成功，单击**下一步：价格清单**。

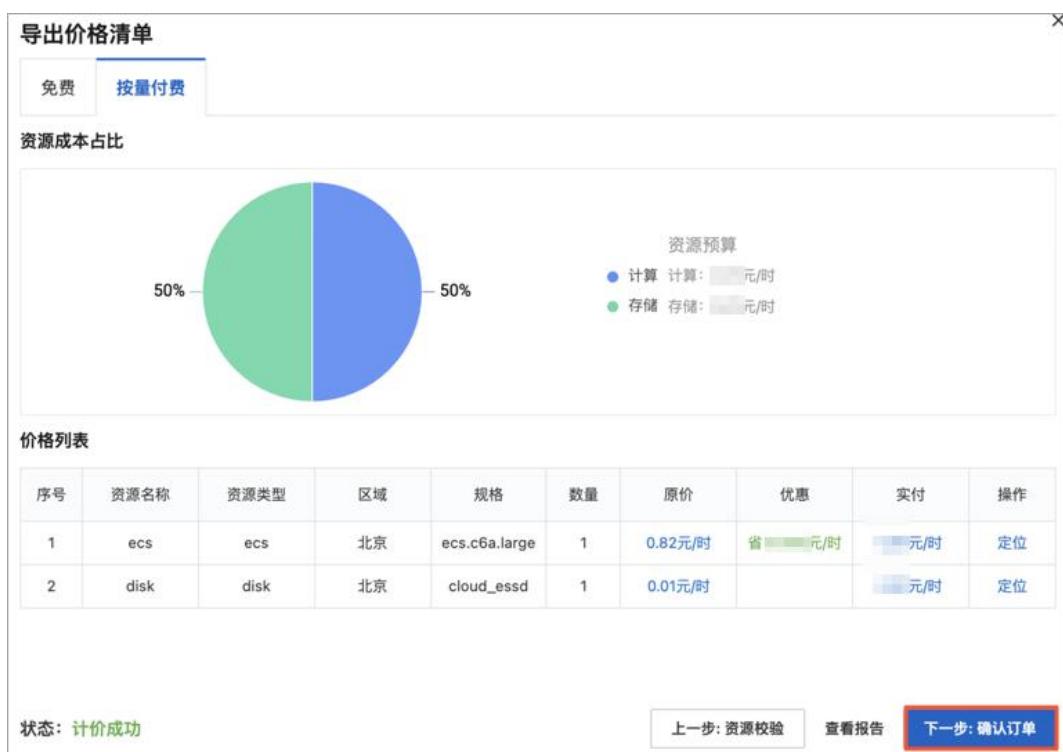
**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-h [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	<a href="#">定位</a>
2	vpc-beijing-001 [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	<a href="#">定位</a>
3	默认安全组	security.group	北京		成功	校验通过	<a href="#">定位</a>
4	disk	disk	北京	cloud_essd	成功	校验通过	<a href="#">定位</a>
5	eni001	eni	北京		成功	校验通过	<a href="#">定位</a>
6	ecs	ecs	北京	ecs.c6a.large	成功	校验通过	<a href="#">定位</a>

状态:校验成功

[下一步：价格清单](#) [返回](#)

步骤3 在**导出价格清单**对话框，会拉取应用所有配置的价格信息，查看计费详情。分别查看包年包月的价格和按量付费的价格。



步骤4 可以单击**查看报告**，查看应用的价格信息。



**步骤5 单击下一步：确认订单**，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。



**步骤6 单击下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。



**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zew8i7m8zhnag2m7z9do	运行中	2021-12-03 19:38:28	定位
2	vswitch-h [H-19 2.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zegryxcw656hea4fig48	运行中	2021-12-03 19:38:28	定位
3	默认安全组	security.group (安全组)	-	sg-2zeepwbl6gf9a4utda68	运行中	2021-12-03 19:38:28	定位
4	ecs	ecs (云服务器ECS)	按量付费	i-2zeg3fmje9byyr5sy7p5	运行中	2021-12-03 19:39:12	定位
5	disk	disk (磁盘)	-	d-2ze30npopuzpzzov3yop	运行中	2021-12-03 19:38:44	定位

每页显示 10 共6条 < 上一页 1 下一页 >

**部署概要**

状态: 部署成功 方案编号: 48FRBDYSTNUF3UHH

[查看报告](#) [返回](#)

步骤 7 部署完成后，单击[查看报告](#)，可以查看本次的部署报告。



步骤 8 单击[返回](#)，然后打开[资源清单](#)。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zew8i7m8znhnq2m7z9do	运行中	2021-12-03 19:38:28	定位
2	vswitch-h [H-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zegryxcw656hea4fig48	运行中	2021-12-03 19:38:28	定位
3	默认安全组	security.group (安全组)	-	sg-2zeepwbl6gf9a4utda68	运行中	2021-12-03 19:38:28	定位
4	ecs	ecs (云服务器ECS)	按量付费	i-2zeg3fmje9byyrsy7p5	运行中	2021-12-03 19:39:12	定位
5	disk	disk (块存储)	-	d-2ze30npopuzpzzov3yop	运行中	2021-12-03 19:38:44	定位

每页显示 10 共6条 < 上一页 1 下一页 >

**部署概要**

状态: 部署成功 方案编号: 48FRBDYSTNUF3UHH

[查看报告](#) [返回](#)

**云速搭 CADT** 公共云

专利号: CN111930290B 查看最佳实践

新建 应用 资源 管理 导出

cadt-ecs-demo01 部署成功

vswitch-h [H-192.168.0.0/24]

eni001  
ecs  
disk

资源清单

导出资源清单

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
4	ecs	ecs (云服务器ECS)	按量付费	i-2zeg3fmje9byyrsy7p5	新建	运行中	2021-12-03 19:39:12	定位	详情 监控 变更日志 操作
5	disk	disk (块存储)	-	d-2ze30npopuzpzzov3yop	新建	运行中	2021-12-03 19:38:44	定位	详情 监控 变更日志 操作
6	eni001	eni (弹性网卡)	-	eni-2zehhkzw8hs9ml119rf	新建	运行中	2021-12-03 19:38:44	定位	详情 监控 变更日志

每页显示 10 共6条 < 上一页 1 下一页 >

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 9 单击 ECS 后，跳转到 ECS 控制台查看。

1. 检查镜像 id

基本信息

诊断健康状态 DOWN | 启动 | 重启 | 停止 | 配置安全组规则 | 重置实例密码

实例ID	i-2zeg3fmje9byyr5sy7p5	远程连接	地域	华北2 (北京)
资源组:	-		所在可用区	北京 可用区H
公网IP	8.141.149.227	转换为弹性公网IP	主机名	ecs001
安全组	sg-2zeepwbl6gf9a4utda68	加入安全组	创建时间	2021年12月3日 19:38:00
标签	-	编辑标签	自动释放时间	-
描述	-	修改实例描述	释放设置	

CPU&内存	2核 4 GiB	云盘	2	重新初始化云盘
操作系统	CentOS 7.7 64位	快照	0	
实例规格	ecs.c6a.large	更改实例规格	镜像ID	m-2zecjv6bnl7b9p2rmjme
实例规格族	ecs.c6a		当前使用带宽	10Mbps (峰值)
			创建自定义镜像	
			按量付费实例更改带宽	

## 2. 检查外挂的云盘

云盘

创建云盘 挂载云盘

<input type="checkbox"/> 云盘ID/云盘名称	标签	云盘种类 (全部) ▾	云盘状态 (全部) ▾	付费类型 (全部) ▾	可卸载 (全部) ▾	可用区	云盘属性 (全部) ▾	已加密/未加		
<input type="checkbox"/> d-2ze30nipopuzpzzov3yop disk		ESSD云盘	PL0	100GiB (3000 IOPS)	使用中	按量付费	支持	北京 可用区H	数据盘	未加密

## 3. 使用秘钥登录

```
jh@MAC ~ $ chmod 400 key1203.pem
jh@MAC ~ $ ssh -i key1203.pem root@8.141.149.227
The authenticity of host '8.141.149.227 (8.141.149.227)' can't be established.
ECDSA key fingerprint is SHA256:eQyDCxfTFh9Dho0mMPogi77E5Ta8Q6hfB8Cm8P0v0u0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '8.141.149.227' (ECDSA) to the list of known hosts.
Last login: Tue Mar 17 09:36:19 2020 from 106.11.34.17
```

Welcome to Alibaba Cloud Elastic Compute Service !

```
[root@ecs001 ~]#
```

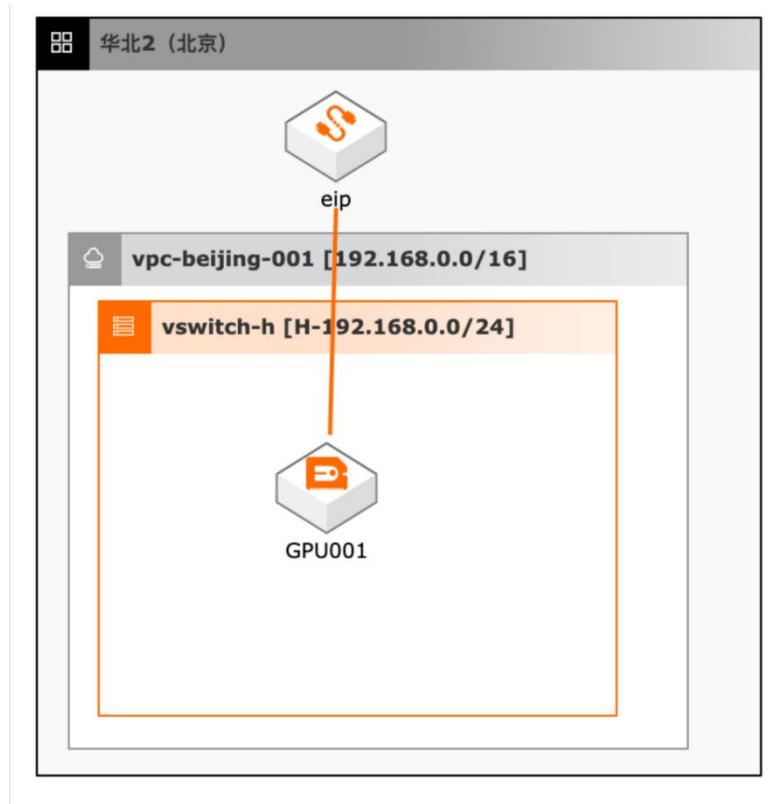
## 3.17.云速搭部署 GPU 云服务器

作者 | 阿里云解决方案架构师 敬海

### 3.17.1.云速搭架构设计

#### 方案架构

通过云速搭实现 GPU 云服务器的部署。这里使用 ECS 的 UserData 特性自动安装 GPU 驱动，A IACC 等组件，减少配置工作量。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
GPU 云服务器	vswitch 交换机

## 地域和可用区规划

地域规划在华北 2 (北京)，可用区选择 cn-beijing-h 可用区。

## 准备 userData 脚本

这里使用 GPU 的 Userdata 如下：

```
#!/bin/sh

#Please input version to install
IS_INSTALL_AIACC_TRAIN="TRUE"
IS_INSTALL_AIACC_INFERENCE="TRUE"
DRIVER_VERSION="450.80.02"
CUDA_VERSION="11.0.2"
CUDNN_VERSION="8.0.4"
IS_INSTALL_RAPIDS="FALSE"

INSTALL_DIR="/root/auto_install"

#using .deb to install driver and cuda on ubuntu OS
#using .run to install driver and cuda on ubuntu OS
auto_install_script="auto_install_v3.3.sh"

script_download_url=$(curl http://100.100.100.200/latest/meta-data/source-address | head -1)"/opsx/ecs/linux/binary/script/${auto_install_script}"
echo $script_download_url
mkdir $INSTALL_DIR && cd $INSTALL_DIR
```

```
wget -t 10 --timeout=10 $script_download_url && sh ${INSTALL_DIR}/${auto_install_script} $DRIVER_VERSION $CUDA_VERSION $CUDNN_VERSION $IS_INSTALL_AIACC_TRAIN $IS_INSTALL_AIACC_INFERENCE $IS_INSTALL_RAPIDS
```

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
GPU 云服务器	GPU001	

## 3.17.2.应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

The screenshot shows the Cloud Speed Stack CADT Control Console. At the top, there are navigation tabs: 新建 (Create), 应用 (Application), 资源 (Resources), and 导出 (Export). On the right, there are links for 专利号: CN1119302908 and 查看最佳实践 (View Best Practice).

The main area features a map of China with city markers for Beijing, Shanghai, Hangzhou, Shenzhen, Hong Kong, Chongqing, Chengdu, and others. Below the map is a button labeled 中国 (China) with a dropdown arrow.

To the right of the map is a section titled "未分配区域" (Unassigned Region) which lists "应用名称" (App Name), "创建时间" (Creation Time), and "状态" (Status). It currently displays "没有数据" (No Data).

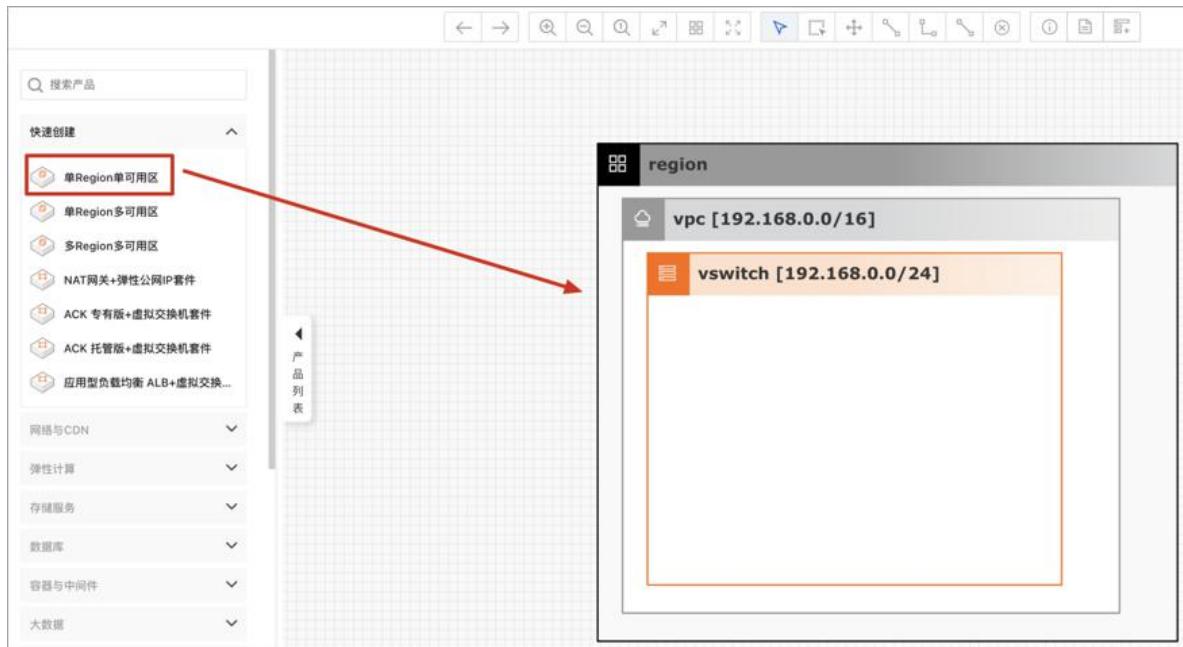
At the bottom right, there is a "产品动态" (Product Dynamics) section with three bullet points:

- 支持用户对应用进行架构探查，自动生成已保有的应用的架构 [新功能](#)
- 2021年9月31日
- 支持RAM权限管理，对子用户授予不同的权限和资源组，控制子用户对资源的访问和操作 [新功能](#)
- 2021年9月31日
- 支持应用状态实时更新，实时更新服务的状态和配置 [新功能](#)
- 2021年10月10日

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

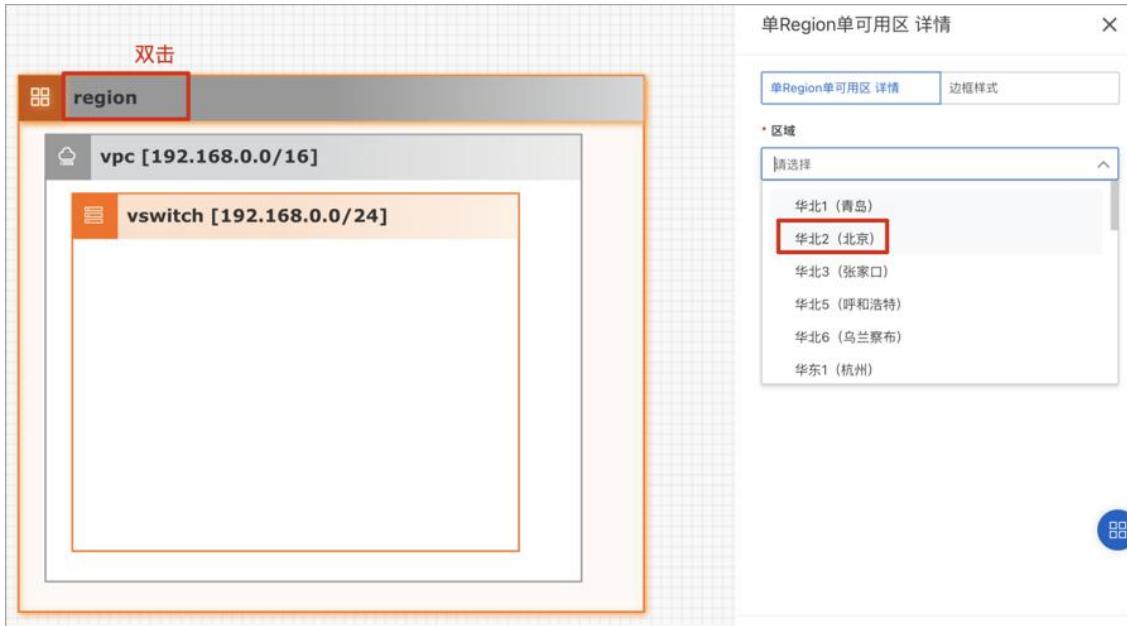


步骤 3 从左侧产品列表的快速创建分类下，找到单 Region 单可用区，单击后拖入到画布区域中，松开鼠标左键。

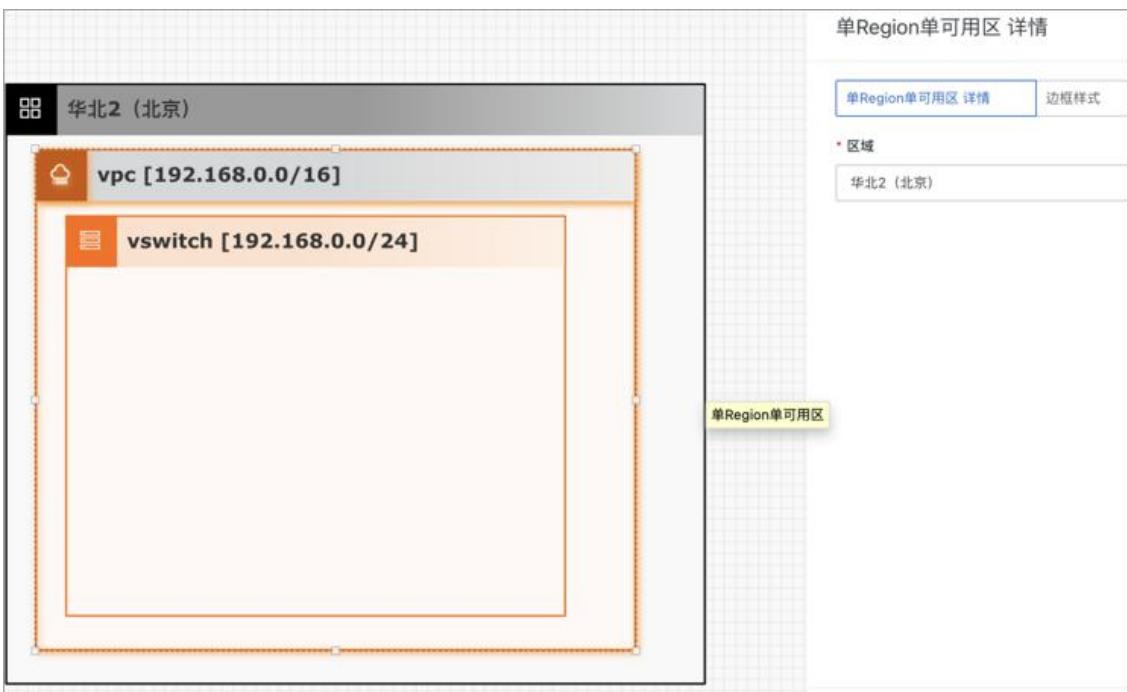


步骤 4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



选择后，如下图所示：



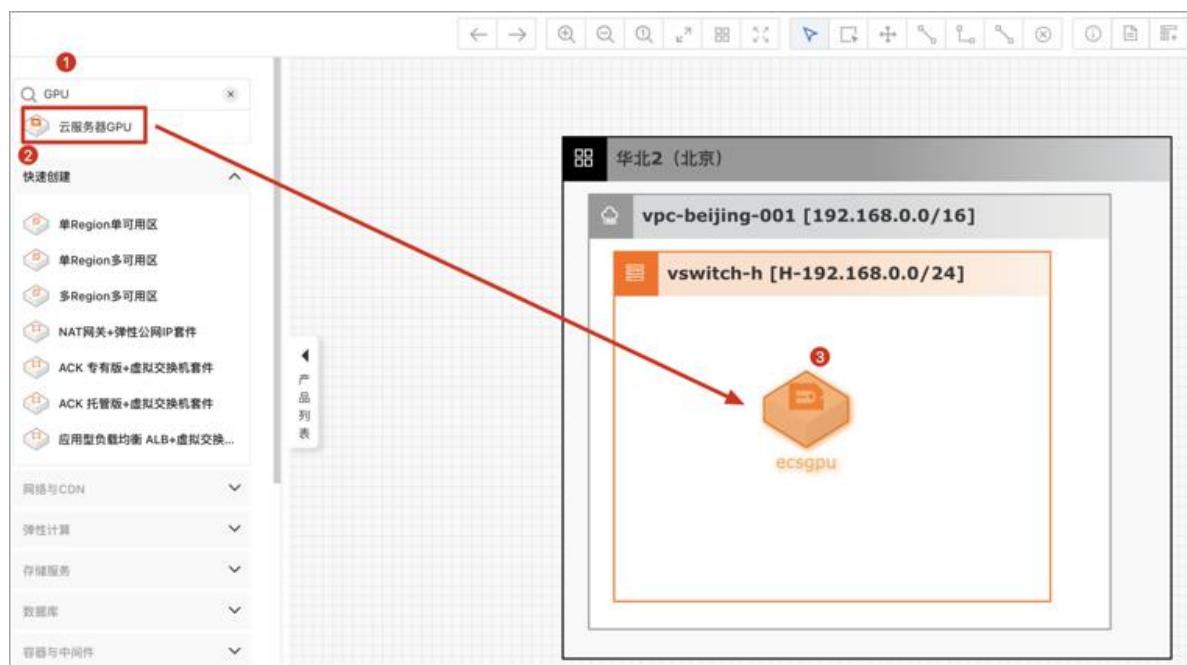
2. 双击 VPC，配置 VPC 参数。



3. 双击 Vswitch，配置 vswitch 参数。



步骤 5 搜索 GPU，拖入一个 GPU 云服务器到 vswitch-h 中。



步骤 6 双击 GPU 云服务器，配置参数。

\* 可用区 ①

华北 2 可用区 H

\* GPU ①

GPU001

\* 支付方式

按量付费

\* 实例规格

ecs.gn6v-c8g1.2xlarge (8c 32g)

镜像 ①

CentOS

\* 镜像版本 ①

CentOS 8.4 64位

\* 系统盘类型 ①

ESSD 云盘

系统盘容量 ①

20

2048

120

\* 性能级别

PL0 (单盘IOPS性能上限1万)

数据磁盘 ①

data\_disks = [  
]  
+

资源标识 ①

请填写标签键

:

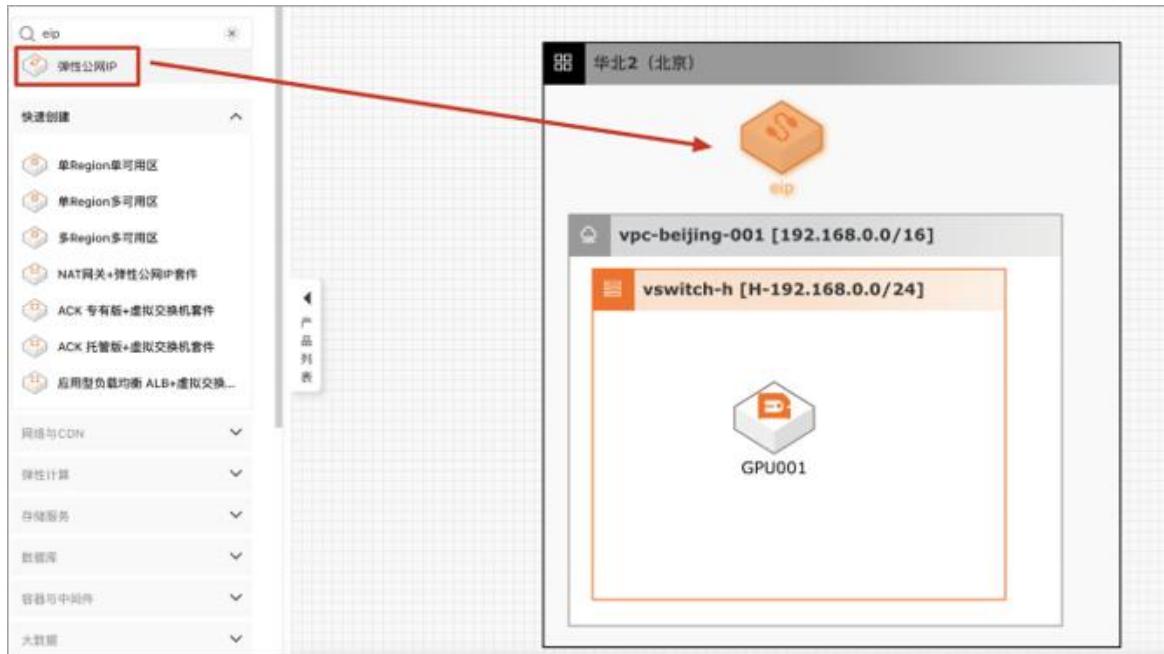
请填写标签值

[+]  
(1/20)

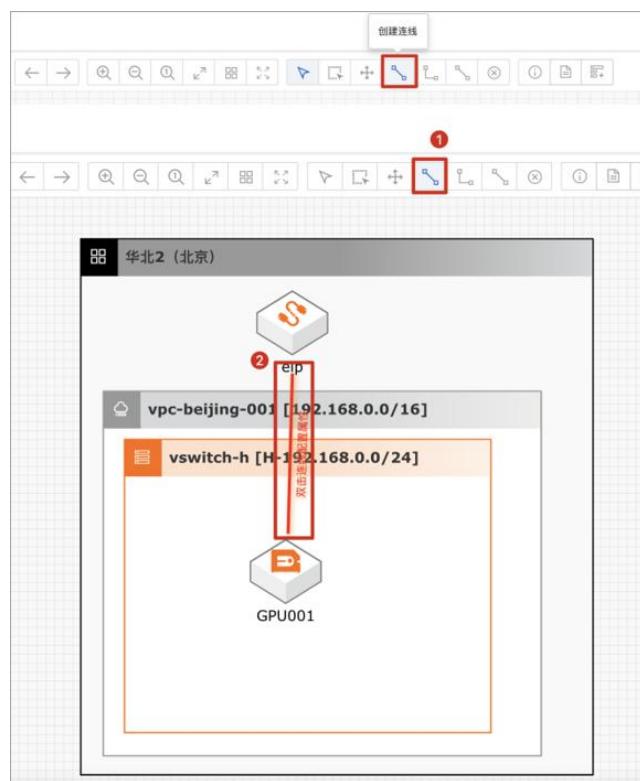
1. 资源标识键不可以重复,最长为64个字符;  
 2. 资源标识值可以为空,最长为128个字符;  
 3. 资源标识键和资源标识值都不能以"aliyun", "acs:", "http://"或 "https://"开头;



步骤 7 搜索 eip，拖入地域中。



步骤 8 切换到连线模式，将 eip 和 GPU 云服务器连接起来



步骤 9 双击 eip，并配置 eip 参数如下

购买方式 ①  
新购

EIP名 ①  
eip

购买数量 ①  
1

\* 商品类型  
按量付费

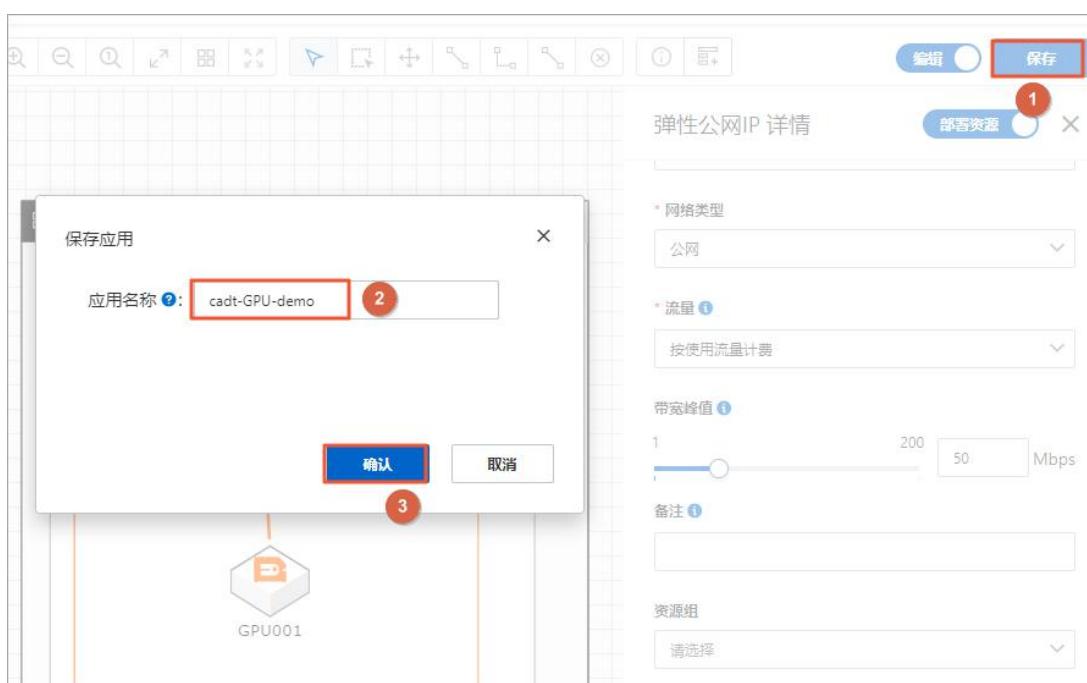
线路类型 ①  
BGP(多线)

\* 网络类型  
公网

\* 流量 ①  
按使用流量计费

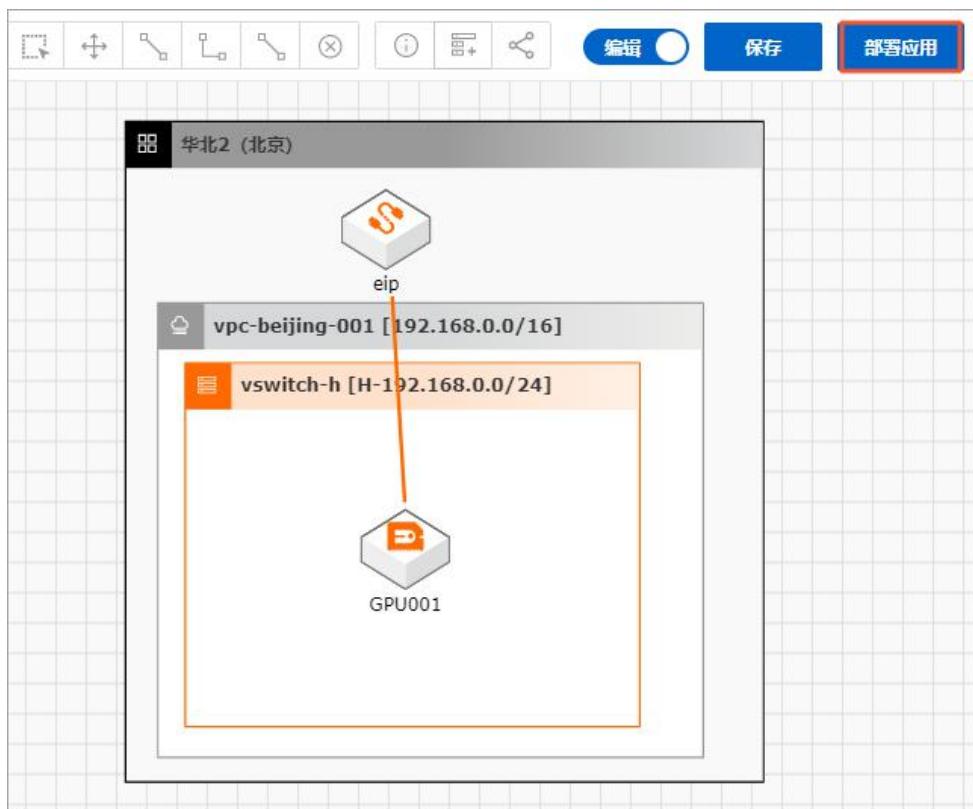


步骤 10 单击右上角的**保存**，填写应用名称为 **cadt-GPU-demo**



### 3.17.3. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、GPU 云服务器是否有库存等，一般需要几十秒左右。

等待校验成功，单击下一步：价格清单。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-h [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	默认安全组	security.group	北京		成功	校验通过	定位
3	vpc-beijing-001 [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
4	eip	eip	北京	public	成功	校验通过	定位
5	GPU001	ecsgpu	北京	ecs.gn6v-c8g1.2x large	成功	校验通过	定位

状态:校验成功

下一步: 价格清单

返回

步骤 3 在导出价格清单对话框中，会拉取应用所有配置的价格信息，查看计费详情。



可以单击[查看报告](#), 查看应用的价格信息。



**步骤4 单击下一步：确认订单**，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

The screenshot shows a 'Confirm Order' dialog box. At the top, there are two tabs: 'Free' and 'Pay by Quantity' (按量付费), with 'Pay by Quantity' selected. Below the tabs is a table listing resources:

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	GPU001	ecsgpu	北京	ecs.gn6v-c8g1.2xlarge	1	26.59元/时	26.59元/时	新购
2	eip	eip	北京	BGP	1	0.02元/时	0.02元/时	新购

Below the table, there is a checked checkbox labeled 'Check Service Terms'. A note below it says 'Please read and check the service terms before deployment.'.

In the middle section, it says 'Pay by Quantity: 26.59 元/时'.

At the bottom left, it says 'Status: Pricing successful'. On the right, there are two buttons: 'Previous Step: Price List' and 'Next Step: Pay and Create' (highlighted with a red box).

**步骤5 单击下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。

The screenshot shows a 'Resource Deployment Status' page. At the top, there is a search bar with fields for 'Resource Name', 'Resource Type', 'Payment Type', and 'Resource ID'. Below the search bar, a message says 'Deploying, do not perform any operations, please wait...'.

In the middle section, there is a summary table with the following data:

状态	方案编号
部署中	HC80P8WFYBEU3C3E

At the bottom right, there is a 'Return' button.

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	Free	vpc-2zekmt2d3wow1kw05fqg	运行中	2021-12-10 15:08:00	定位
2	eip	eip (弹性公网IP)	按量付费	eip-2zekk41eno0ppnep65qj0	运行中	2021-12-10 15:08:00	定位
3	默认安全组	security.group (安全组)	Free	sg-2zees9oqwpupv568gqez	运行中	2021-12-10 15:08:01	定位
4	vswitch-h [H-19 2.168.0.0/24]	vswitch (虚拟交换机)	Free	vsw-2zewvrmfi80ize6jvw6dn	运行中	2021-12-10 15:08:35	定位
5	GPU001	ecs (云服务器)	按量付费	i-2ze79x94z4zeibvekg	运行中	2021-12-10 15:08:56	定位

每页显示 10 共5条 < 上一页 1 下一页 >

**部署概要**

状态: 部署成功 订单编号: 211863802470159  
方案编号: ZBZC0WVDYLAKCOCC

[查看报告](#) [返回](#)

步骤 6 部署完成后，单击[查看报告](#)，可以查看本次的部署报告。



步骤 7 单击返回，然后打开资源清单。

The screenshot shows the CADT interface with the following details:

- Top Bar:** Includes '新建' (New), '应用' (Apply), '资源' (Resources), '管理' (Management), '导出' (Export), '专利号: CIN11930290B 查看最佳实践' (Patent No: CIN11930290B View Best Practice), and '权限管理' (Permission Management).
- Project:** 'cadt-GPU-demo' with a status of '部署成功' (Deployment successful).
- Diagram:** A network diagram titled '学之3 (北京)' showing a connection between an 'eip' and a 'vswitch-h [H:192.168.0.0/24]' interface, which is connected to a 'GPU001' instance.
- Resource List:**

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
4	vswitch-h	vswitch (虚拟交换机)	免费	vsw-2zeewvmf180ize6jvw6dn	新建	运行中	2021-12-10 15:08:35	定位	详情 监控 变更日志 操作
5	GPU001	ecs (云服务器ECS)	按量付费	i-2ze79x94z4zeibveglkg	新建	运行中	2021-12-10 15:08:56	定位	详情 监控 变更日志 操作
- Bottom Buttons:** '历史版本' (History), '释放全部资源' (Release All Resources), and '同步资源数据' (Sync Resource Data).

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 8 单击 GPU 云服务器后，跳转到 GPU 云服务器控制台查看。

## 1. 检查 eip 绑定

The screenshot shows the ECS instance detail page for 'GPU001' with the following details:

- Basic Information:**
  - Instance ID: i-2ze79x94z4zeibveglkg
  - Region: 华北2 (北京)
  - Remote Connection: 远程连接
  - 弹性公网IP: 101.201.79.68 (highlighted with a red box)
  - 安全组: sg-2zees9oqwpuv568gqez
  - 标签: -
  - 描述: -
- Actions:** Includes '诊断健康状态' (Diagnose Health Status), '启动' (Start), '重启' (Restart), '停止' (Stop), '配置安全组规则' (Configure Security Group Rules), '重置实例密码' (Reset Instance Password), '修改实例主机名' (Change Instance Hostname), '修改设置' (Modify Settings), and '释放设置' (Release Settings).

## 2. 远程登陆

```
jh@MAC ~ $ ssh root@101.201.79.68
The authenticity of host '101.201.79.68 (101.201.79.68)' can't be established.
ECDSA key fingerprint is SHA256:xJ4ZZKqe2BEX7ejI6T4LqztPrbEGlZzmCf2DjxXUaOE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '101.201.79.68' (ECDSA) to the list of known hosts.
root@101.201.79.68's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Activate the web console with: systemctl enable --now cockpit.socket

% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total Spent   Left Speed
100  21  100  21    0     0  2100      0 --::-- --::-- --::--  2100
CHECKING AUTO INSTALL, DRIVER_VERSION=450.80.02 CUDA_VERSION=11.0.2 CUDNN_VERSION=8.0.4 INSTALL AIACC-Training=TRUE INSTALL AIAC
C-Inference=TRUE , PLEASE WAIT .....
The script automatically downloads and installs a NVIDIA GPU driver and CUDA, CUDNN library. if you choose install perseus, pers
eus environment will install as well.
1. The installation takes 15 to 20 minutes, depending on the intranet bandwidth and the quantity of vCPU cores of the instance.
Please do not operate the GPU or install any GPU-related software until the GPU driver is installed successfully.
2. After the GPU is installed successfully, the instance will restarts automatically.

Install may have some INSTALL_ERROR, please check log /root/auto_install/auto_install.log !
[root@iZZze79x94z4zeibveglkgZ ~]#
```

3. 可以发现，userdata 中的脚本正在执行中。

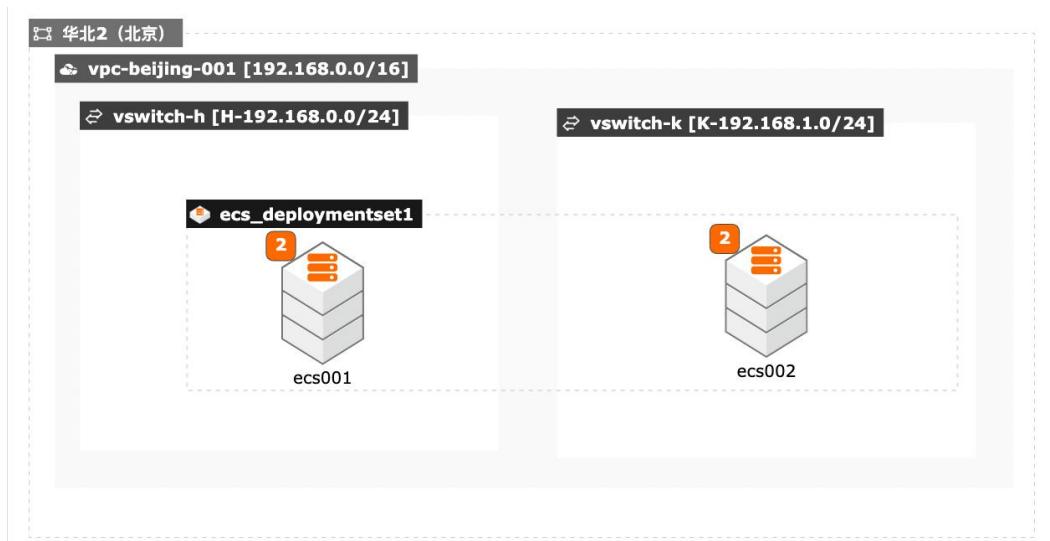
## 3.18.云速搭部署 ECS 部署集

作者 | 阿里云解决方案架构师 敬海

### 3.18.1.云速搭架构设计

#### 方案架构

通过云速搭实现 ECS 部署集的部署。



ECS 部署集概述请参考：[https://help.aliyun.com/document\\_detail/91258.html](https://help.aliyun.com/document_detail/91258.html)

注意几点限制：

- 在部署集中创建 ECS 实例时，一个可用区内最多能创建 20 台 ECS 实例（该数值根据您使用云服务器 ECS 的情况而变化），一个阿里云地域下能创建的 ECS 实例数量为  $20 * \text{可用区数量}$ 。
- 部署集现阶段能创建的 ECS 实例规格族仅支持：
  - c6、g6、r6、c5、g5、ic5、r5
  - hfc6、hfg6、hfr6、hfc5、hfg5
  - d2、d2s、d2c、d1、d1ne
  - i2、i2g、i1
  - selne、sn1ne、sn2ne

## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
AZ	vswitch-k	192.168.1.0/24
ECS 部署集	ecs_deploymentset1	

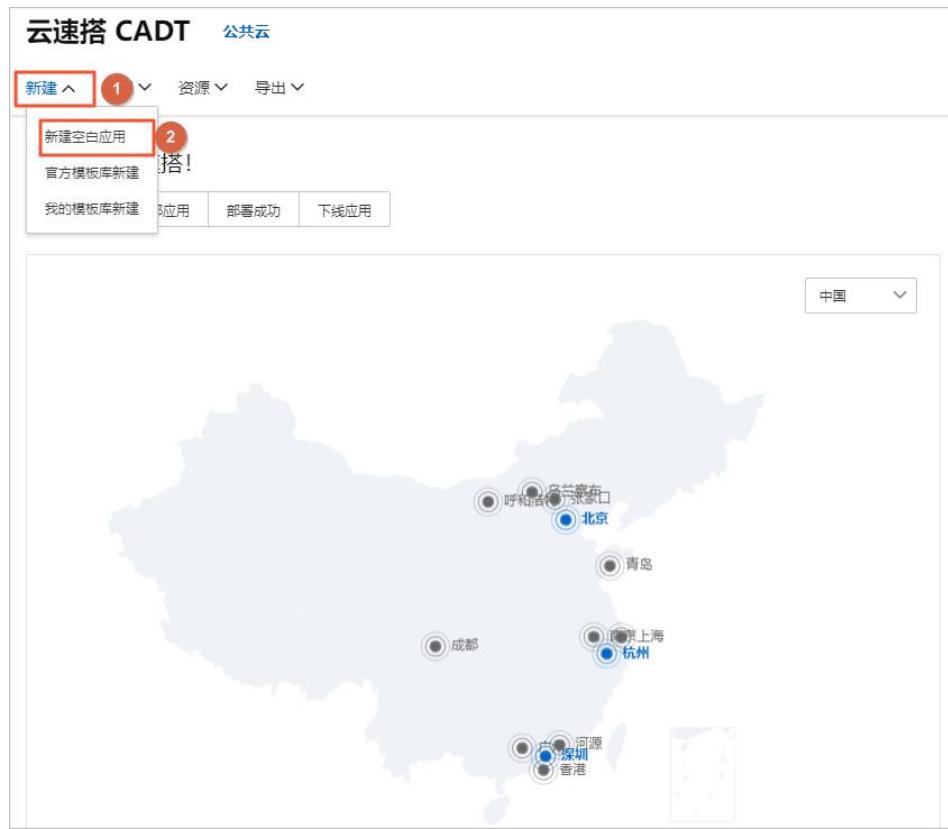
云资源	架构级别
VPC	Region 地域
ECS 部署集	VPC 级别
ECS	vswitch 交换机

## 3.18.2.应用架构设计

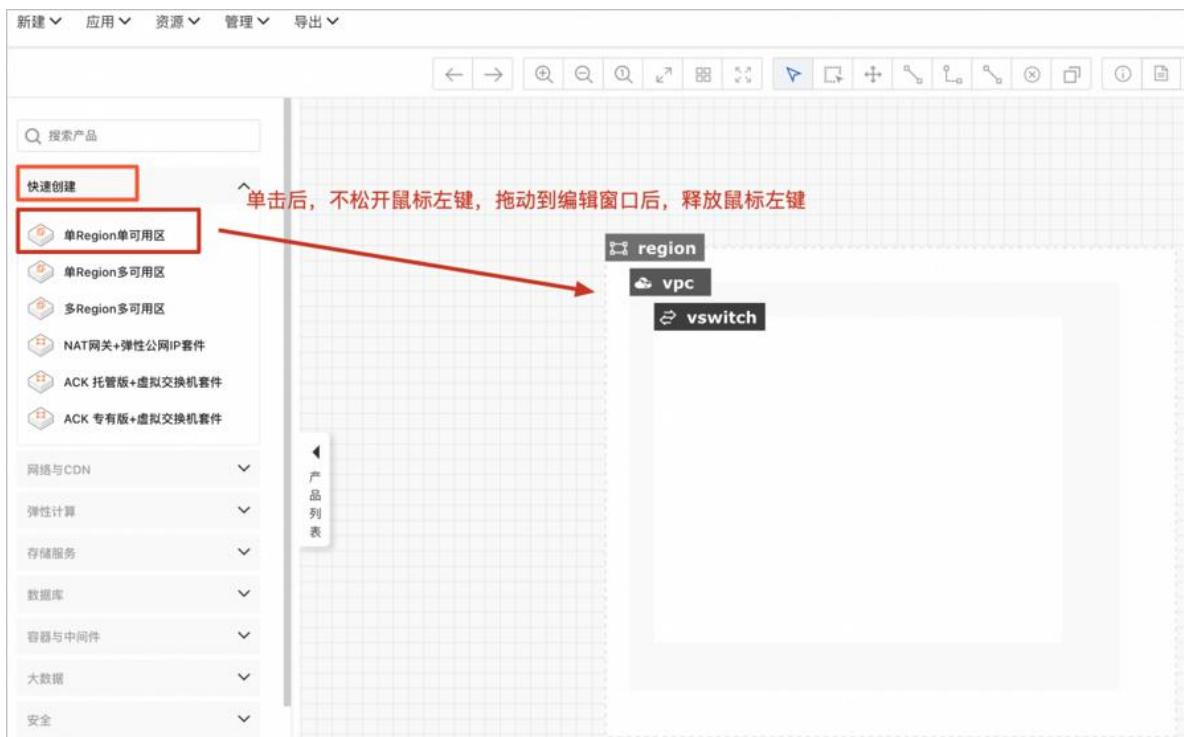
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

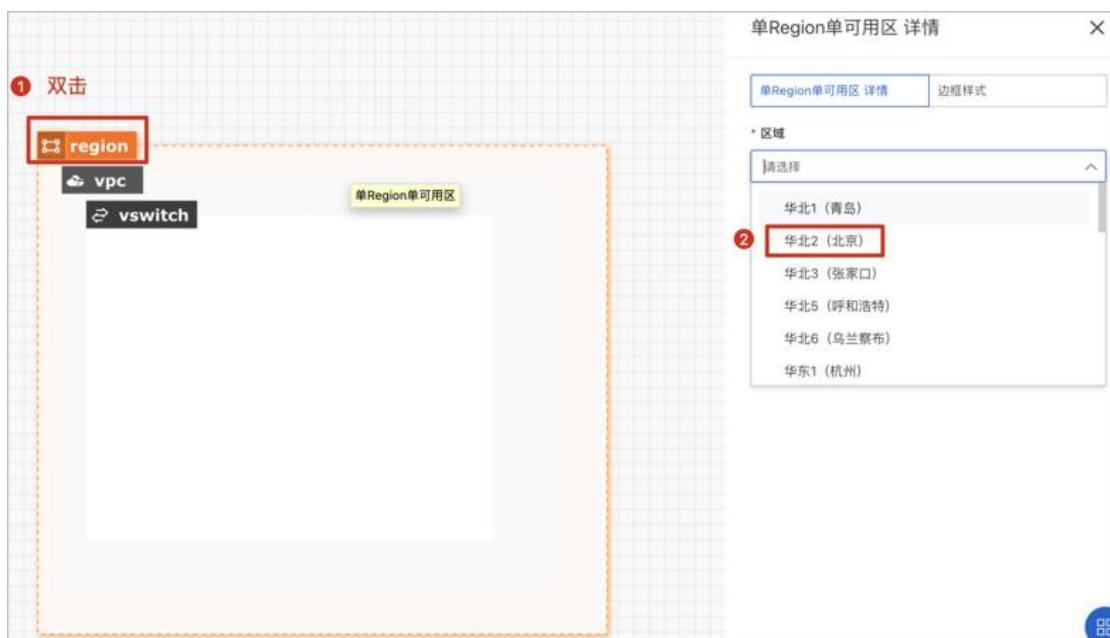


步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

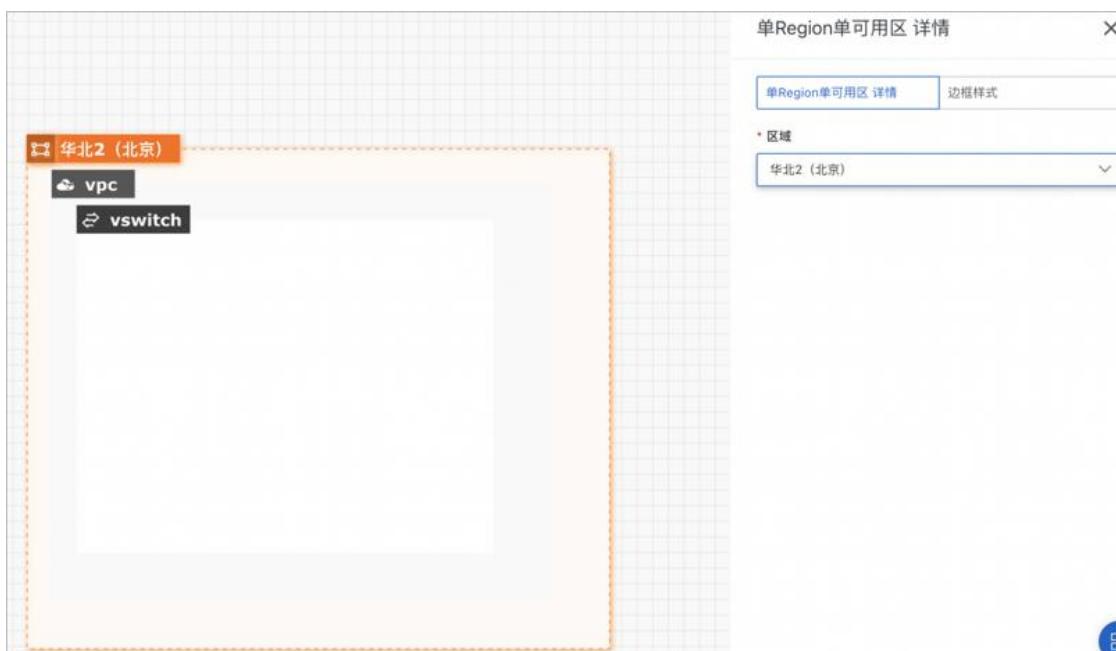


步骤4 依次双击Region、VPC、vswitch进行配置。

1. 双击region，在右侧弹出窗口中，选择华北2（北京）。



选择后，如下图所示：



2. 双击VPC，配置VPC参数。



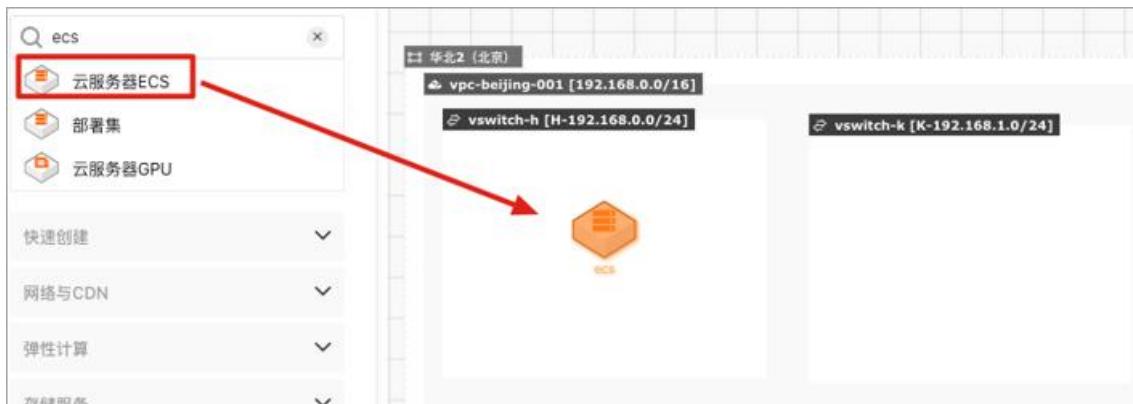
3. 双击 Vswitch，配置 vswitch 参数。



4. 同样的步骤，再拖入一个 vswitch，并设置如下参数。



步骤 5 搜索 ecs，并拖入 vswitch-h 中一个 ecs



步骤 6 双击 ECS，配置参数：

**购买方式** ?

**\* 可用区** ?

**\* 实例名称** ?

×

**数量** ?

**\* 支付方式**

**\* 实例规格** ?

💡

**\* 镜像** ?

**\* 镜像版本** ?

**\* 系统盘类型**

**系统盘容量** ?

20 2048

**\* 性能级别**

**数据磁盘** ?

`data_disks = [  
]  
+`

**公网 IP** ?

分配公网 IPv4 地址

**主机名** ?

×

**有序后缀** ?

**资源标签**

无数据原因如下：  
1.当前vswitch所选可用区下无可售资源  
2.以上属性配置组合下无可售资源

:  💡

+

**登录凭证**

**\* 登录密码** ?

× ?

**\* 确认登录密码** ?

× ?

**安全加固** ?

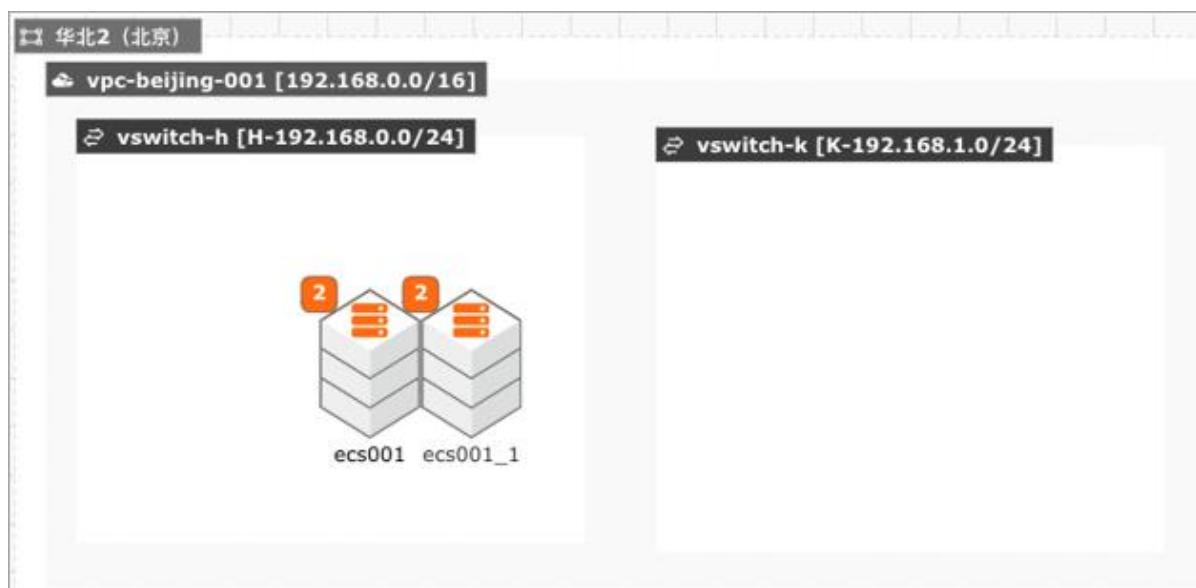
**自动释放时间** ?

💡

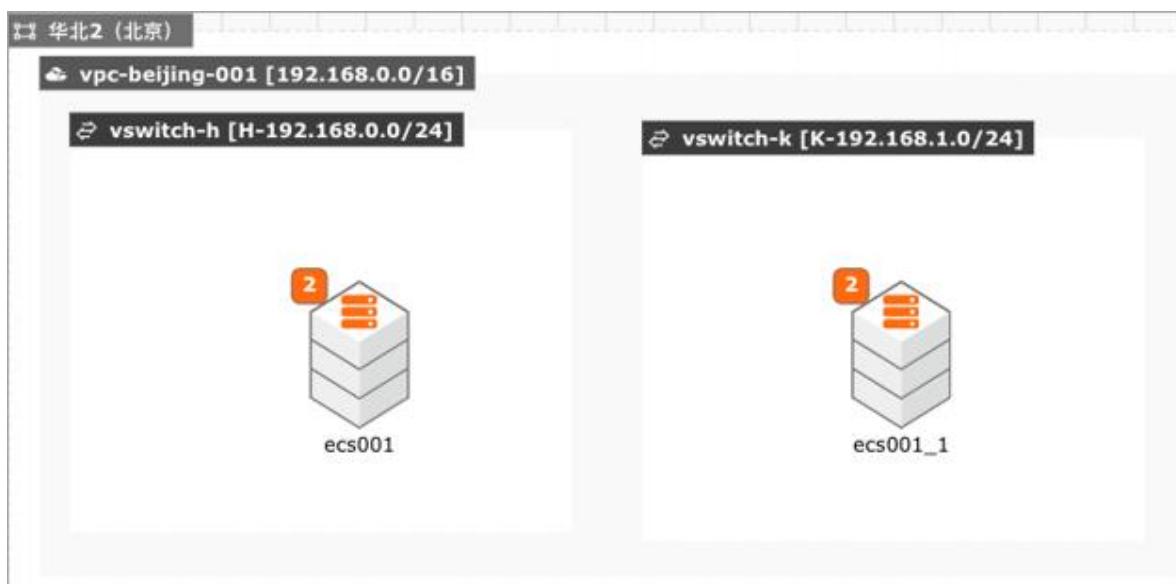
步骤 7 单击 ECS 图标，选择右键，单击**复制**。



步骤 8 出现复制后的 ecs 图标



步骤 9 将其拖动到另一个 vswitch 中。



步骤 10 修改复制的 ecs 的参数。

The screenshot shows the configuration page for creating a new ECS instance. The left panel contains fields for basic parameters like region, availability zone, instance name, quantity, payment method, and instance type. The right panel contains more detailed settings such as image, system disk type and capacity, performance level, data disks, and public IP allocation.

购买方式	新购
* 可用区	华北 2 可用区 K
* 实例名称	ecs002
数量	2
* 支付方式	按量付费
* 实例规格	ecs.c6.large (2c 4g)
* 镜像	Alibaba Cloud Linux
* 镜像版本	Alibaba Cloud Linux 3.2104 64位
* 系统盘类型	ESSD 云盘
系统盘容量	20 2048 40
* 性能级别	PL0 (单盘IOPS性能上限1万)
数据磁盘	data_disks = [ ]
公网 IP	<input type="checkbox"/> 公网/内网 IP 从本地址

**主机名**

**有序后缀**

**资源标签**

请填写标签键	:	请填写标签值
+		
(1/20)		
1. 资源标签键不可以重复,最长为64个字符; 2. 资源标签值可以为空,最长为128个字符; 3. 资源标签键和资源标签值都不能以"aliyun", "acs:", "http://"或 "https://"开头; 4. 最多只能设置20个;		

**系统盘标签**

请填写标签键	:	请填写标签值
--------	---	--------

**登录凭证**

自定义密码

**\* 登录密码**

\*\*\*\*\*

**\* 确认登录密码**

\*\*\*\*\*

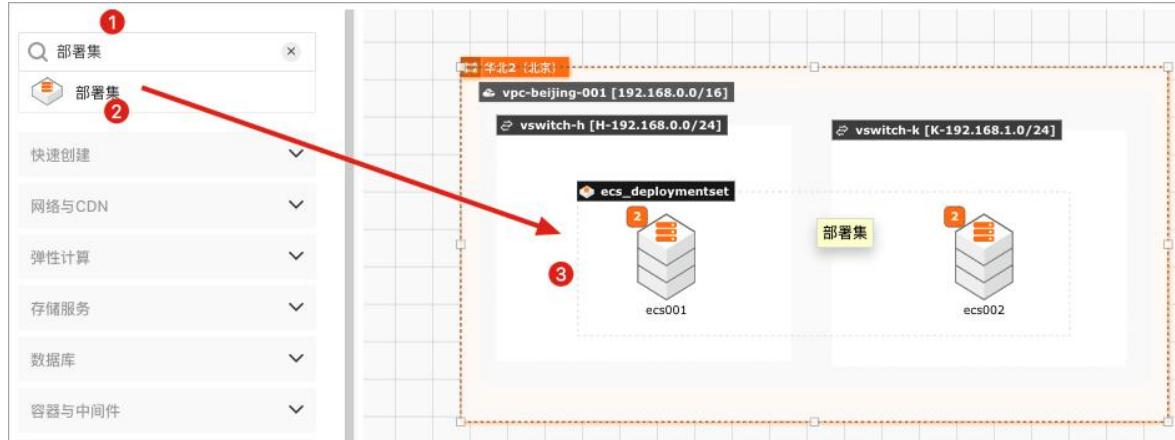
**安全加固**

请选择

**自动释放时间**

请选择日期和时间

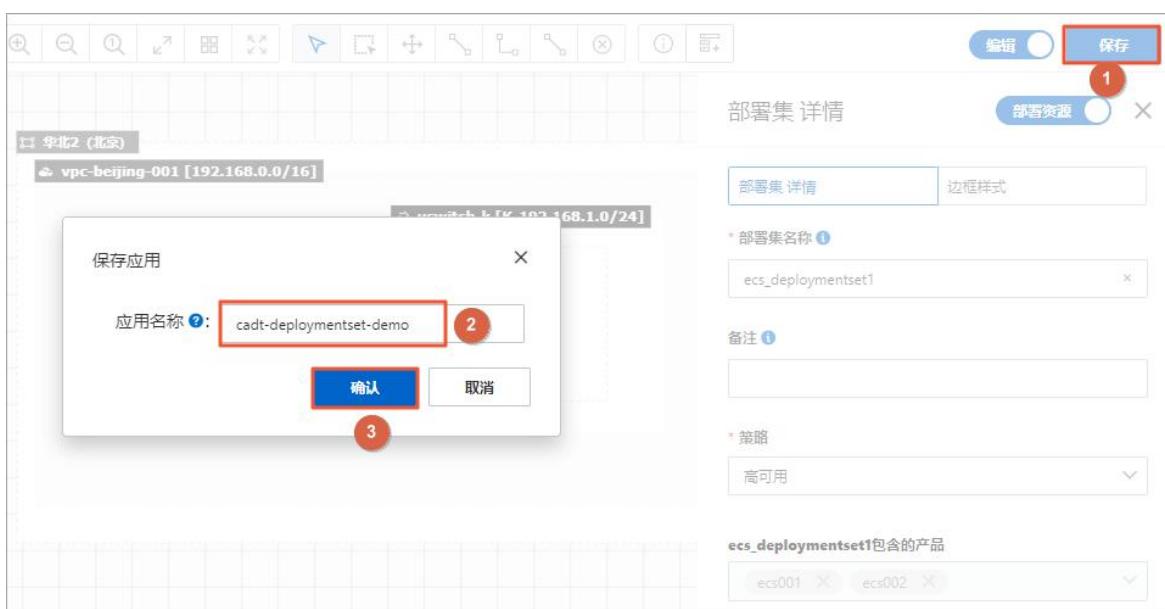
步骤 11 搜索 ECS 部署集，拖入一个 ECS 部署集，将所有 ECS 放在 ECS 部署集的框内。



步骤 12 双击 ECS 部署集，修改 ECS 部署集参数。

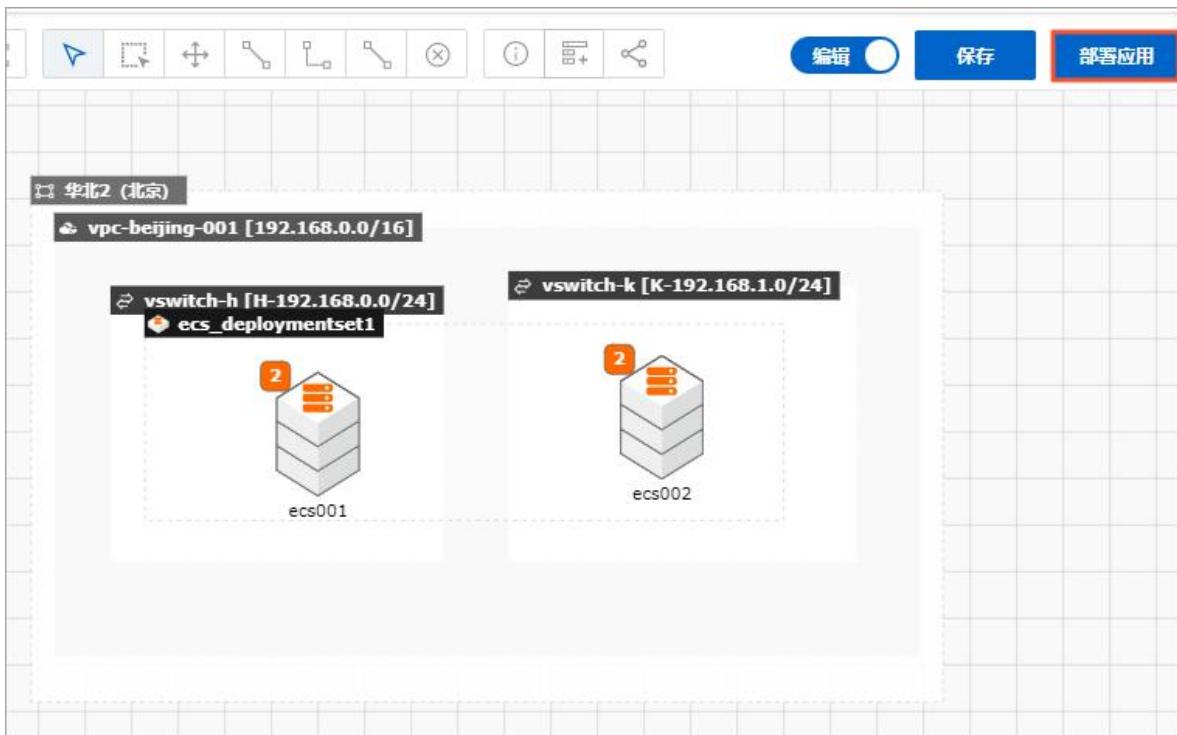


步骤 13 配置完成，单击右上角的**保存**，填写应用名称为 **cadt-deploymentset-demo**



### 3.18.3.部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、ECS 是否有库存等，一般需要几十秒左右。

等待校验成功，单击**下一步：价格清单**。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-h [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	vpc-beijing-001 [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
3	默认安全组	security.group	北京		成功	校验通过	定位
4	ecs002	ecs	北京	ecs.c6.large	成功	校验通过	定位
5	vswitch-k [K-192.168.1.0/24]	vswitch	北京	192.168.1.0/24	成功	校验通过	定位
6	ecs001	ecs	北京	ecs.c6a.large	成功	校验通过	定位

状态:校验成功
下一步: 价格清单
返回

步骤 3 在**导出价格清单**对话框，会拉取应用所有配置的价格信息，可以查看计费详情。

可以单击**查看报告**，查看应用的价格信息。



确认无误，单击**下一步：确认订单**。

**导出价格清单**

免费  按量付费

**资源成本占比**

资源预算  
● 计算 计算: [redacted] 元/时

100%

**价格列表**

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	ecs001	ecs	北京	ecs.c6a.large	2	0.67元/时	省 [redacted] 元/时	[redacted] 元/时	定位
2	ecs002	ecs	北京	ecs.c6.large	2	0.86元/时	省 [redacted] 元/时	[redacted] 元/时	定位

状态: **计价成功**

[上一步: 资源校验](#) [查看报告](#) **下一步: 确认订单**

步骤4 在确认订单对话框中，勾选《云速搭服务条款》，单击下一步：支付并创建。



步骤5 进入部署流程，这里会进行扣费并开始创建资源。

注意：部署流程一旦开始后，无法取消。



步骤6 部署完成后，单击查看报告，可以查看本次的部署报告。



步骤 7 单击返回，然后打开应用底部的资源清单。

华北2 (北京)

vpc-beijing-001 [192.168.0.0/16]

vswitch-h [H-192.168.0.0/24]

ecs\_deploymentset1

vswitch-k [K-192.168.1.0/24]

ecs001

2

ecs002

2

资源清单

导出资源清单

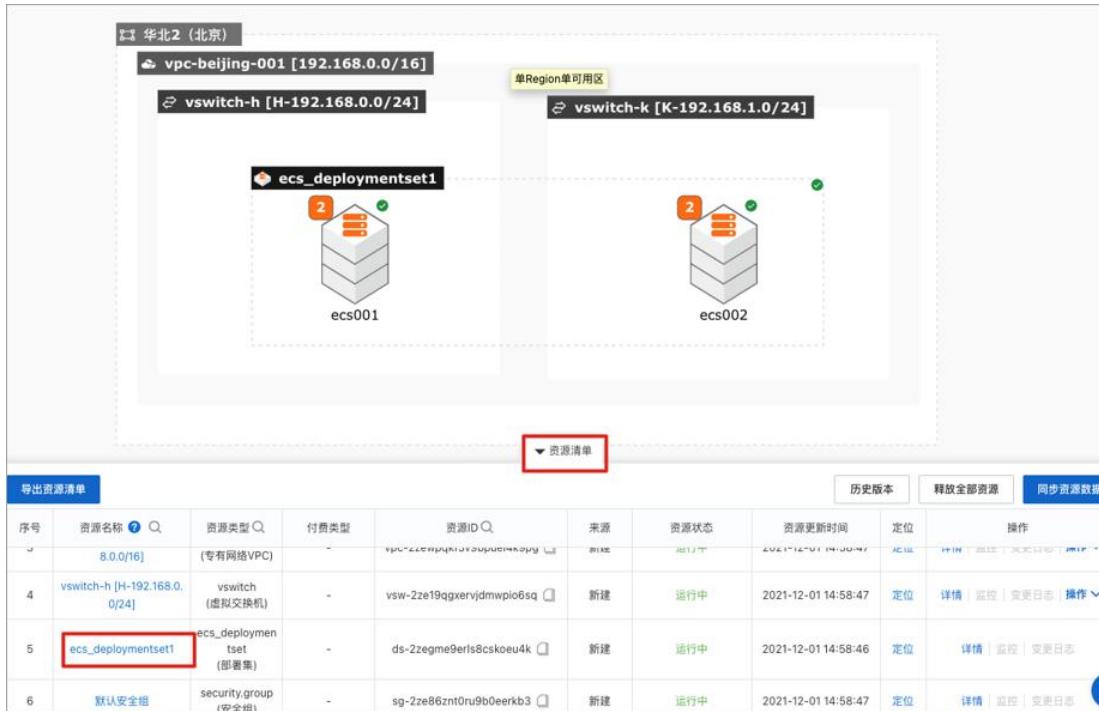
历史版本

释放全部

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位
1	vswitch-h [H-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zepppusuki7my2p3npm	新建	运行中	2021-12-02 15:47:49	定位
2	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zev3k5nsgy92dt34tq	新建	运行中	2021-12-02 15:47:28	定位

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 8 单击 ECS 部署集后，跳转到 ECS 部署集控制台查看。



The screenshot shows the Alibaba Cloud ECS console under the 'Deployment Set' section. It lists a single deployment set named 'ecs\_deploymentset1' with an ID of 'ds-2zegme9erls8cskoeu4k'. The table shows the following details:

部署集ID	部署集名称	部署集描述	实例数量	创建时间	操作
ds-2zegme9erls8cskoeu4k	ecs_deploymentset1		4	2021年12月1日 14:58	<a href="#">创建实例</a>   <a href="#">修改信息</a>   <a href="#">删除</a>

步骤 9 单击部署集 id，查看实例列表如下图所示：

The screenshot shows the 'Instance List' page for the deployment set 'ecs\_deploymentset1'. It lists four instances:

实例ID/名称	可用区	状态	网络类型	操作
i-2ze0w238qjk727g6ioj9 ecs001002	可用区 H	● 运行中	专有网络	<a href="#">修改部署集</a>   <a href="#">管理</a>
i-2ze0w238qjk727g6ioj8 ecs001001	可用区 H	● 运行中	专有网络	<a href="#">修改部署集</a>   <a href="#">管理</a>
i-2zea7hmxwo2u3epvcx5j ecs002001	可用区 K	● 运行中	专有网络	<a href="#">修改部署集</a>   <a href="#">管理</a>
i-2zeiqv9r10ibiooo4imy ecs002002	可用区 K	● 运行中	专有网络	<a href="#">修改部署集</a>   <a href="#">管理</a>

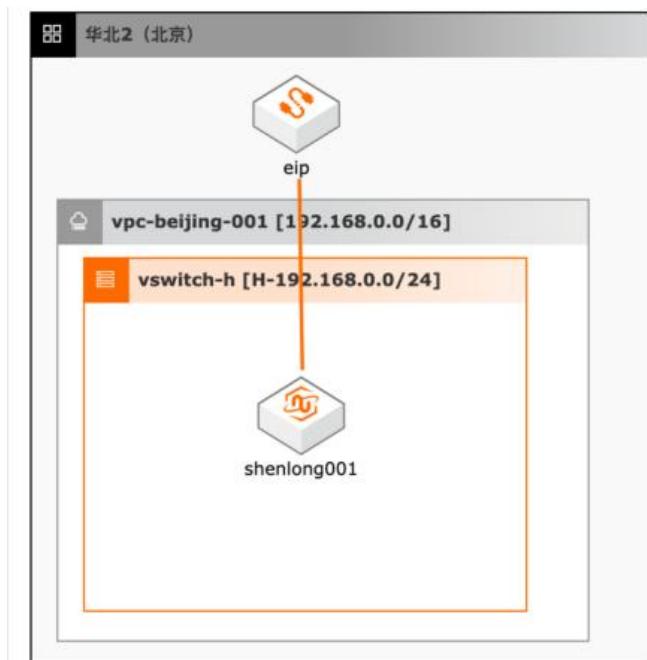
## 3.19.云速搭部署弹性裸金属服务器

作者 | 阿里云解决方案架构师 敬海

### 3.19.1.云速搭架构设计

#### 方案架构

通过云速搭实现弹性裸金属服务器的部署。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
弹性裸金属服务器	vswitch 交换机

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
弹性裸金属服务器	shenlong001	

### 3.19.2.应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

云速搭 CADT 公共云

专利号: CN111930290B 查看最佳实践

新建 应用 资源 导出

欢迎使用云速搭!

应用全貌 全部应用 部署成功 下线应用

中国

未分配区域

应用名称	创建时间	状态
无数据		

< 1 >

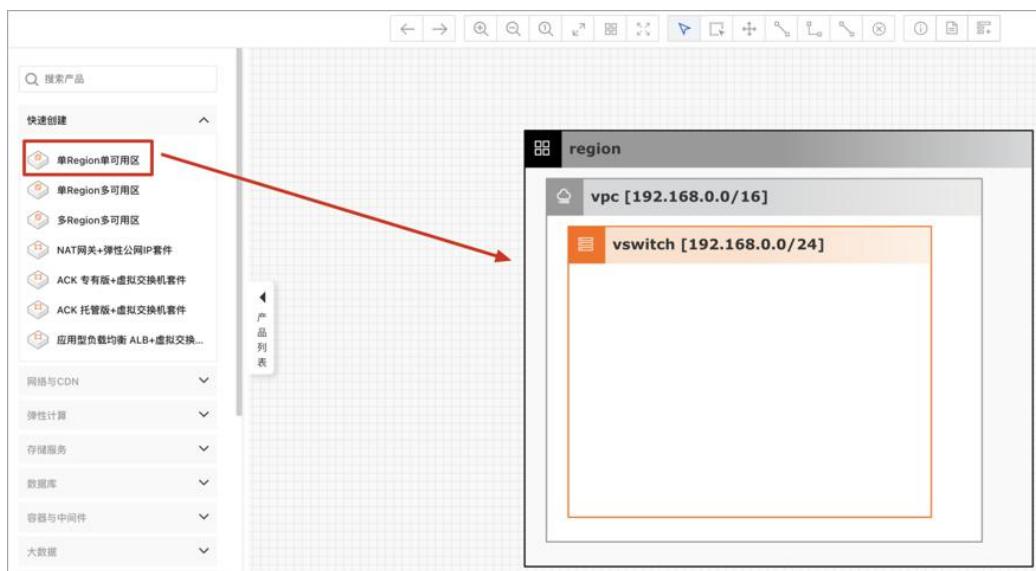
产品动态

- 支持用户对应用进行架构审查，自动产生已保有的应用的架构 [新功能](#)
- 2021年9月31日
- 支持RAM权限管理，对子用户授予不同的权限和资源组，控制子用户对资源的 [新功能](#) 访问和操作
- 2021年9月31日
- 支持应用状态实时更新，实时更新服务的状态和配置 [新功能](#)
- 2021年9月30日

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

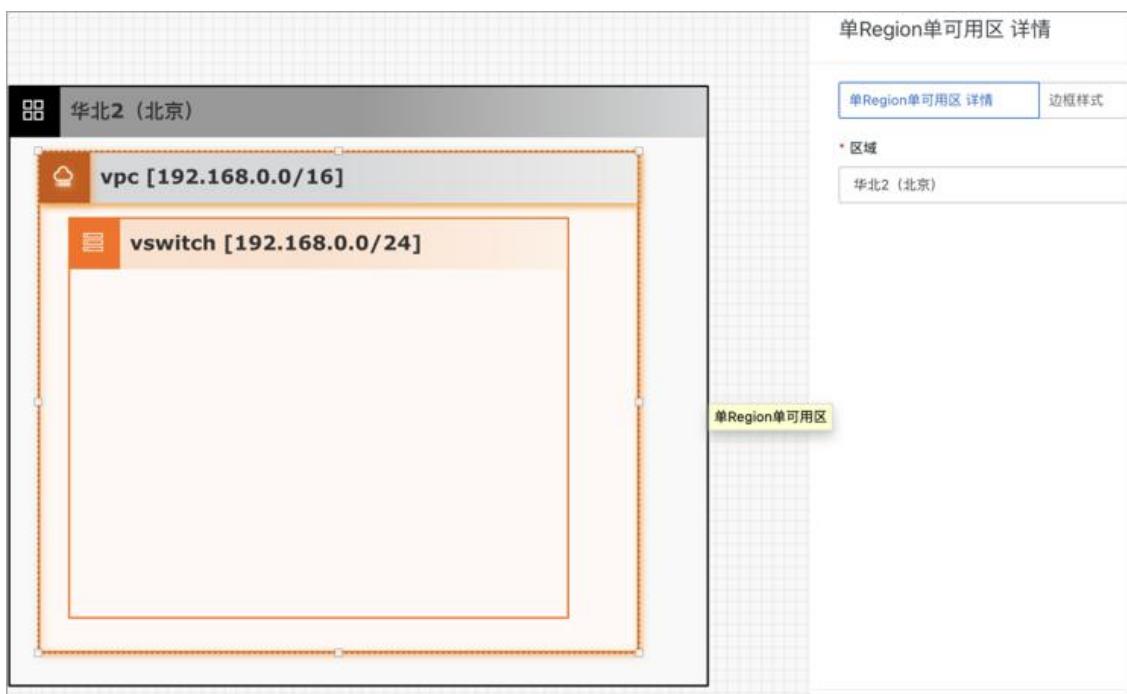


步骤4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北2（北京）。



选择后，如下图所示：



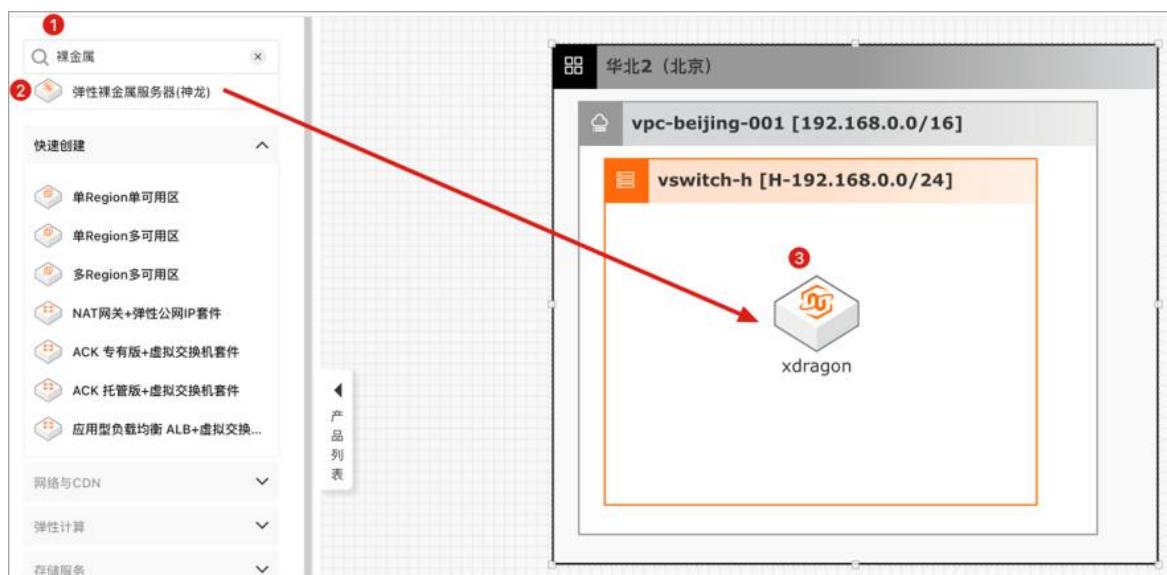
2. 双击 VPC，配置 VPC 参数。



3. 双击 Vswitch，配置 vswitch 参数。



步骤 5 搜索裸金属，拖入到 vswitch-h 中。



步骤 6 双击弹性裸金属服务器，配置参数。

可用区 !

华北 2 可用区 H

\* 弹性裸金属服务器(神龙) !

shenlong001

\* 支付方式

按量付费

\* 实例规格

ecs.ebmhfc6.20xlarge (80c 192g)

镜像 !

CentOS

\* 镜像版本 !

CentOS 8.4 64位

\* 系统盘类型 !

ESSD 云盘

系统盘容量 !

20
( )
2048
40

\* 性能级别

PL0 (单盘IOPS性能上限1万)

数据磁盘 !

data\_disks = [  
]

+

公网 IP !

分配公网 IPv4 地址

登录凭证 !

自定义密码

\* 登录密码 !

.....

\* 确认登录密码 !

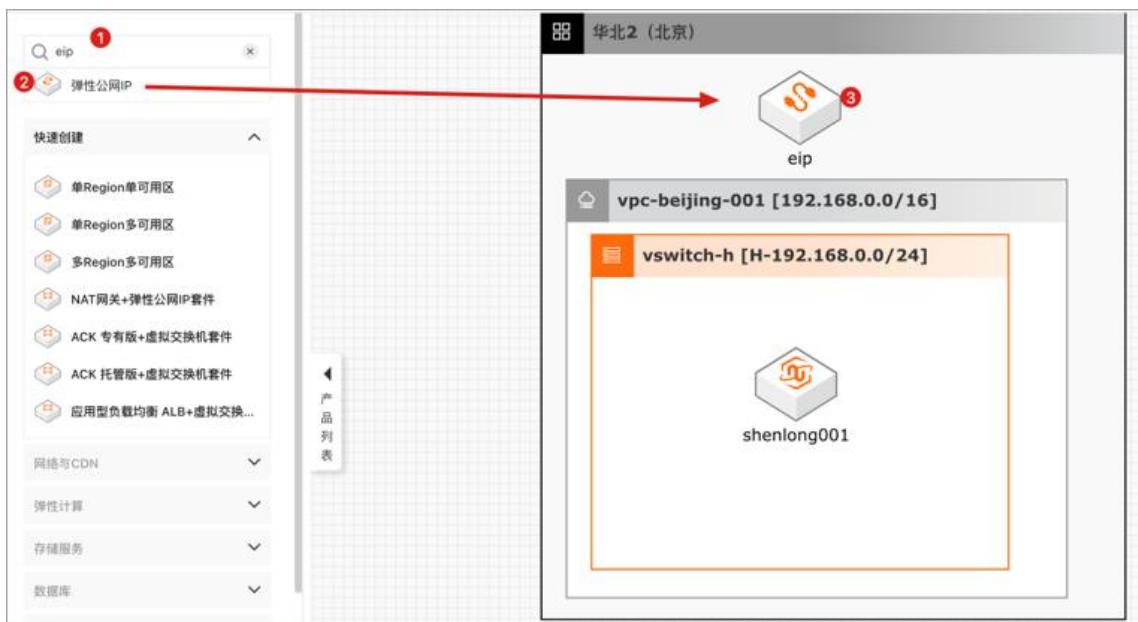
.....

安全加固 !

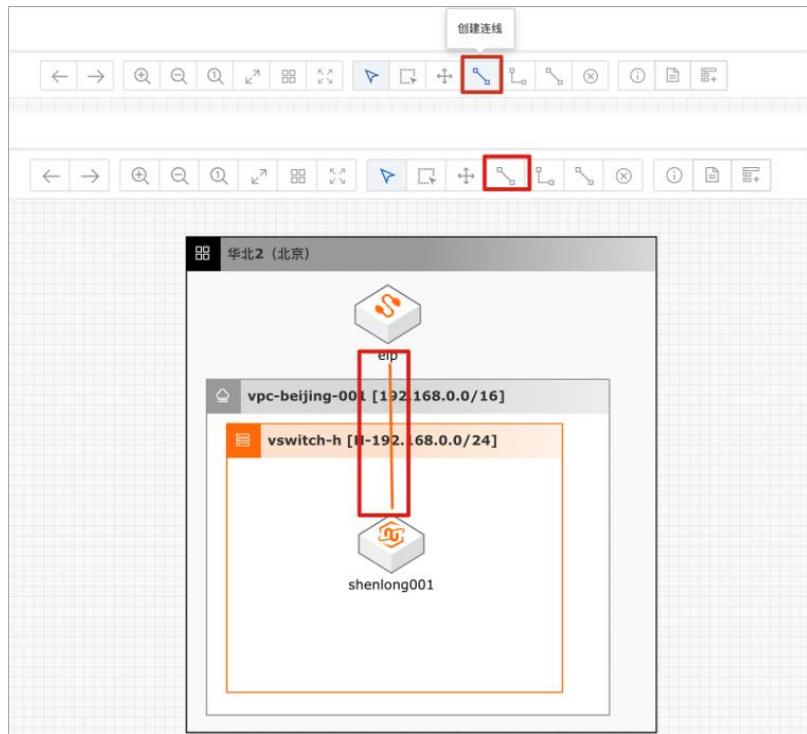
请选择

实例自定义数据 !

步骤 7 搜索 eip，拖入地域中。



步骤 8 切换到连线模式，将 eip 和弹性裸金属服务器连接起来。



步骤 9 双击 eip，并配置 eip 参数如下：

The screenshot shows the "EIP名" (EIP Name) configuration dialog. It contains the following fields:

- 购买方式**: 新购 (Purchase Method)
- EIP名**: eip (EIP Name)
- 购买数量**: 1 (Purchase Quantity)
- 商品类型**: 按量付费 (Pay-as-you-go)
- 线路类型**: BGP(多线) (BGP Multi-line)
- 网络类型**: 公网 (Public Network)
- 流量**: 按使用流量计费 (Charge by usage)

带宽峰值 1

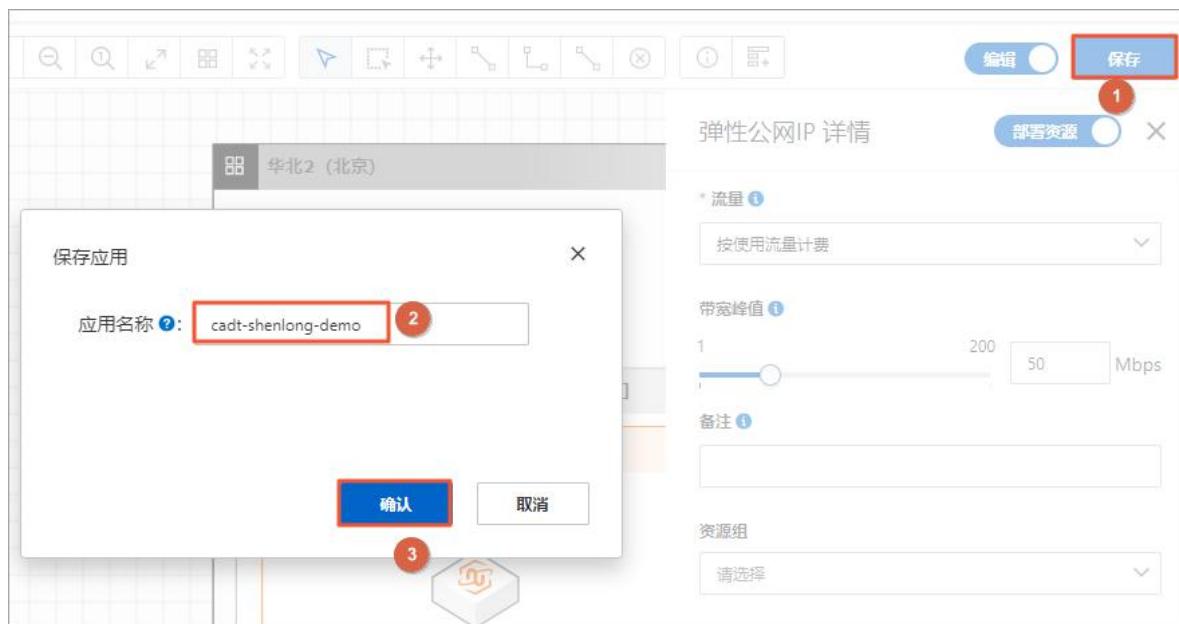
1 200 50 Mbps

备注 1

资源组

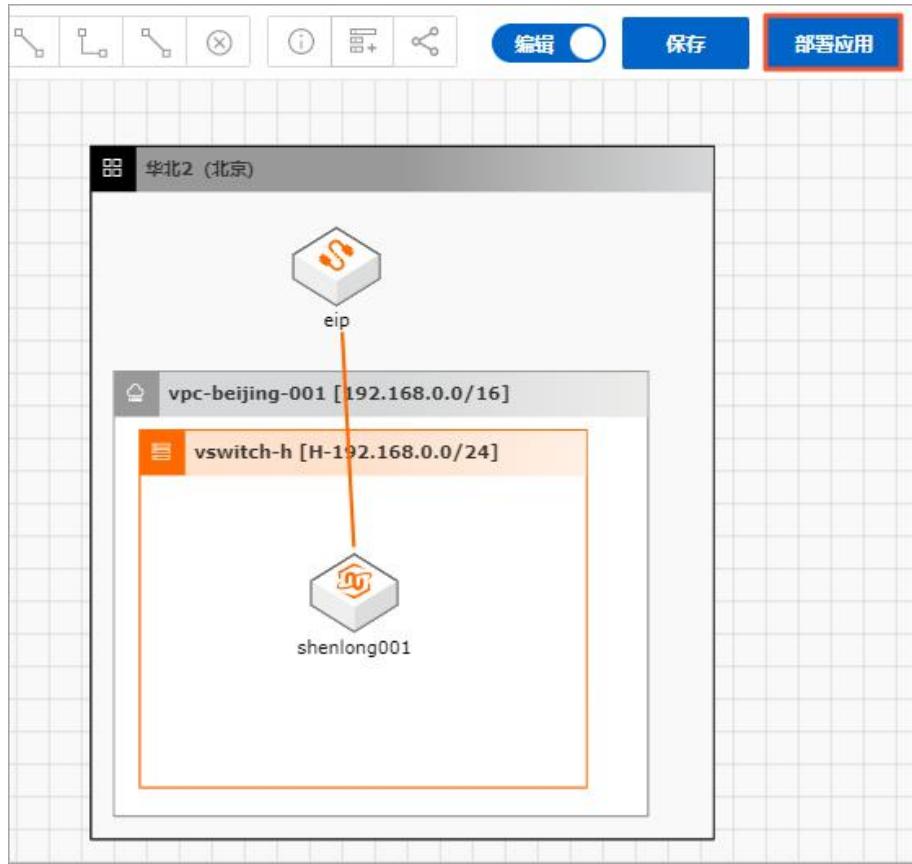
请选择

步骤 10 单击右上角的**保存**，填写应用名称为 **cadt-shenlong-demo**



### 3.19.3. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、弹性裸金属服务器是否有库存等，一般需要几十秒左右。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	eip	eip	北京	public	成功	校验通过	定位
2	默认安全组	security.group	北京		成功	校验通过	定位
3	vswitch-h [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
4	vpc-beijing-001 [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
5	shenlong001	xdragon	北京	ecs.ebmhf6.20xlarge	成功	校验通过	定位

状态:校验成功
下一步: 价格清单
返回

步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息，查看计费详情。



可以单击[查看报告](#), 查看应用的价格信息。



**步骤4 单击下一步：确认订单**，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。



**步骤5 单击下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。



**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	Free	vpc-2ze0hauu43x5re4bamjt5	运行中	2021-12-10 15:50:42	定位
2	eip	eip (弹性公网IP)	按量付费	eip-2zettfnrb6bt7yoq733l6	运行中	2021-12-10 15:50:42	定位
3	vswitch-h [H-19 2.168.0.0/24]	vswitch (虚拟交换机)	Free	vsw-2zer8yj8y8sgivusvz1de	运行中	2021-12-10 15:51:13	定位
4	默认安全组	security.group (安全组)	Free	sg-2ze79x94z4zeivlpavw	运行中	2021-12-10 15:50:42	定位
5	shenlonna001	ecs (云服务器ECS)	按量付费	i-2ze49gaboehverdohar7	运行中	2021-12-10 15:52:06	定位

每页显示  共5条 < 上一页  下一页 >

**部署概要**

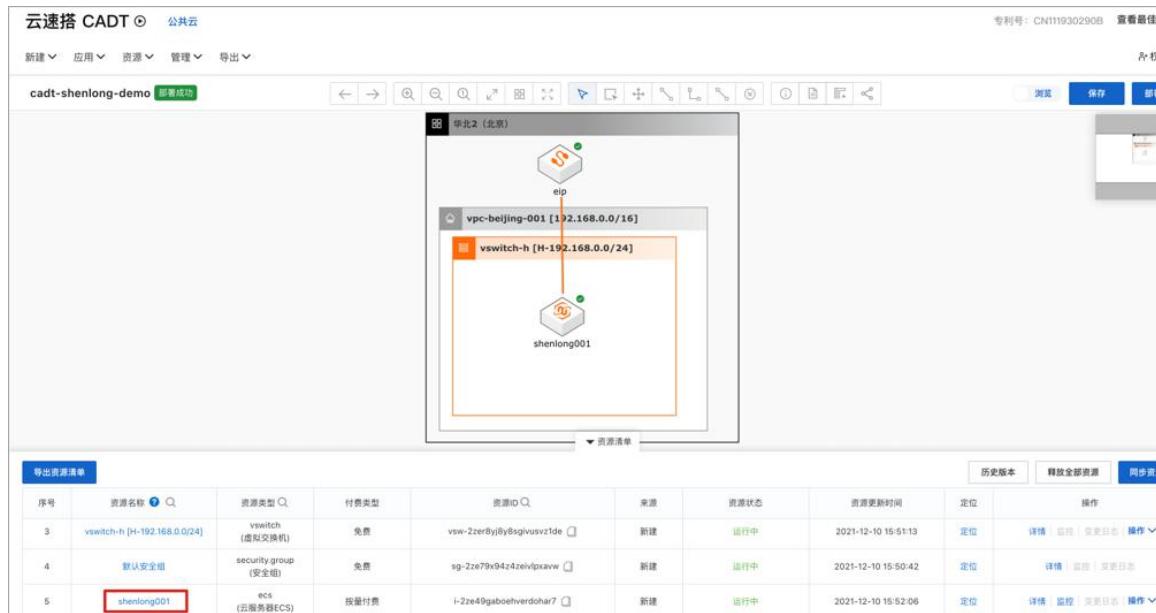
状态: 部署成功 订单编号: 211862351900159  
方案编号: BVHRK45FUZF9UR48

[查看报告](#) [返回](#)

步骤 6 部署完成后，单击**查看报告**，可以查看本次的部署报告。



步骤 7 单击返回，然后单击资源清单。



这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 8 单击弹性裸金属服务器后，跳转到弹性裸金属服务器控制台查看。

## 1. 检查 eip 绑定

The screenshot shows the ECS instance detail page for "shenlong001" with the following details:

- 基本信息:** Instance ID: i-2ze49gaboevhverdohar7, Status: 运行中 (Running).
- 弹性公网IP:** 123.57.146.163 (highlighted with a red box).
- 安全组:** sg-2ze79x94z4zeivlpxavw.
- 远程连接:** Available options include: 诊断健康状态 (Diagnose Health Status), 启动 (Start), 重启 (Restart), 配置安全组规则 (Configure Security Group Rule), and 重置实例密钥 (Reset Instance Key).

## 2. 远程登陆

```
root@iZ2ze49gaboehverdohar7Z:~ Last login: Fri Dec 10 15:14:21 on ttys000
jh@MAC ~ $ ssh root@123.57.146.163
The authenticity of host '123.57.146.163 (123.57.146.163)' can't be established.
ECDSA key fingerprint is SHA256:/HC3TJbpsjXSMs+hjN3XGsy6UNTqhIZPLyysFFwth4U.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '123.57.146.163' (ECDSA) to the list of known hosts.
root@123.57.146.163's password:

Welcome to Alibaba Cloud Elastic Compute Service !

Activate the web console with: systemctl enable --now cockpit.socket
[root@iZ2ze49gaboehverdohar7Z ~]#
```

## 3.20.云速搭部署 DTS 应用

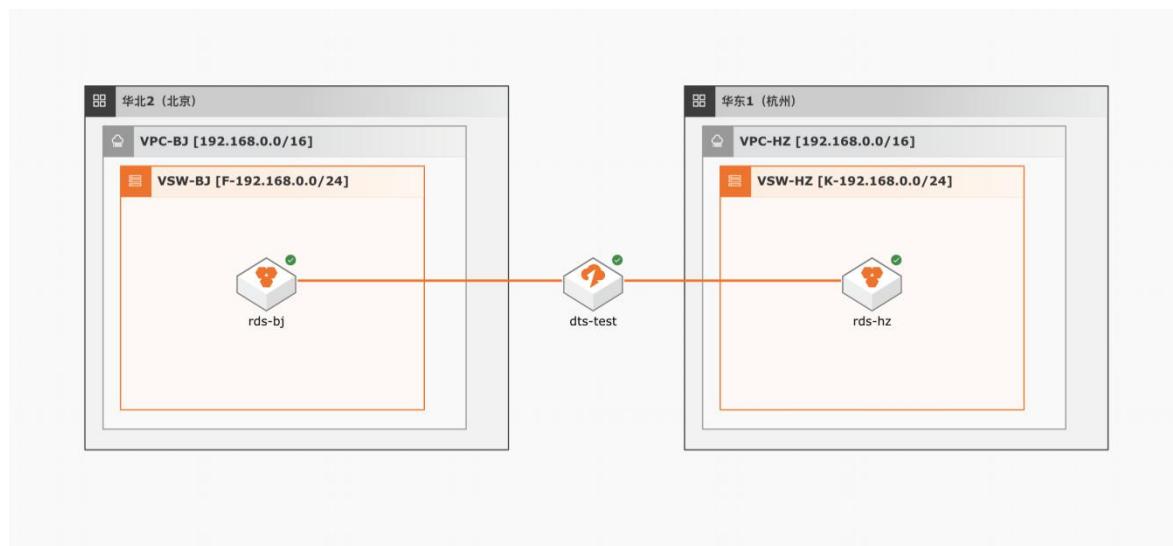
作者 | 阿里云解决方案架构师 袁影

### 3.20.1.云速搭架构设计

#### 方案架构

通过云速搭实现一个 DTS 和两个 RDS 实例的创建，并通过配置同步策略，将源 RDS 数据库库中的数据同步到目标 RDS 数据库中，其中产品架构及原理请参考文档：

[https://help.aliyun.com/document\\_detail/26598.html](https://help.aliyun.com/document_detail/26598.html)



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
DTS	全局
RDS	Vswitch 交换机

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

区域一：

资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC-BJ	192.168.0.0/16
AZ	VSW-BJ	192.168.0.0/24 (可用区 F)

区域二：

资源分类	资源名称	网段
Region	华东 1 (杭州)	-
VPC	VPC-HZ	192.168.0.0/16
AZ	VSW-HZ	192.168.0.0/24 (可用区 K)

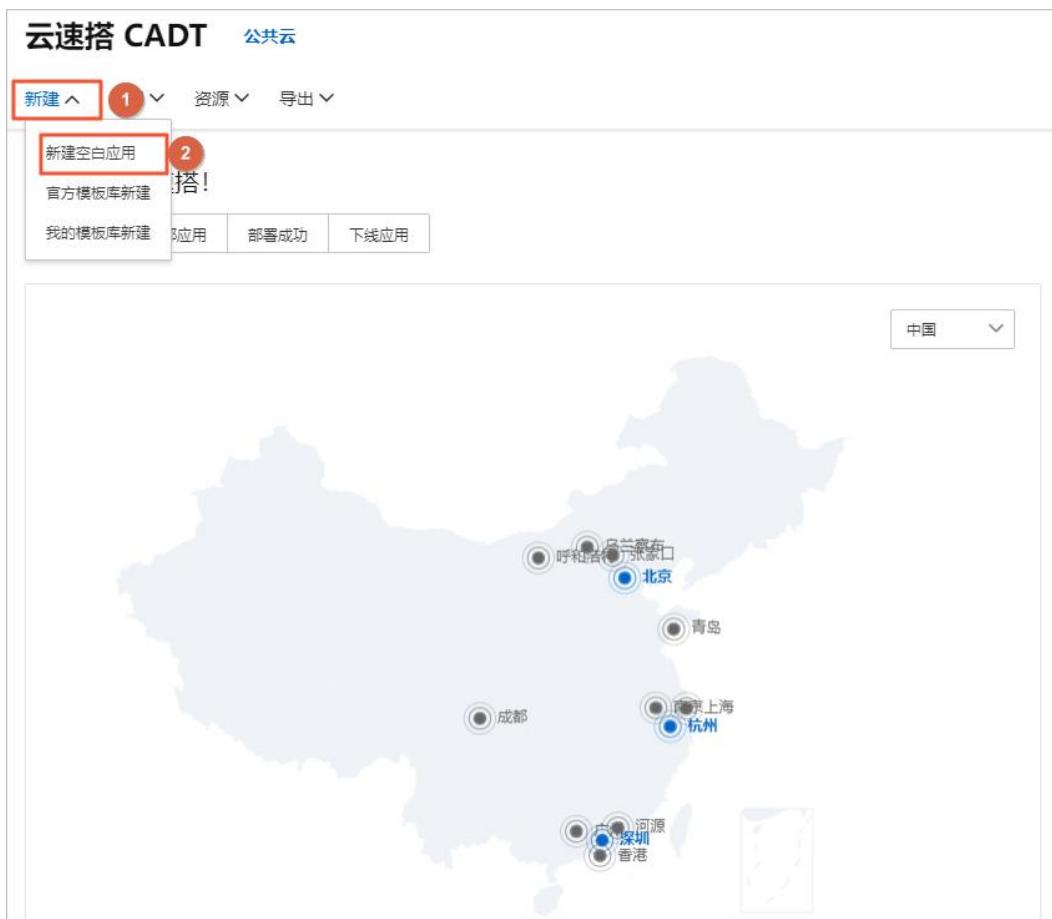
## 3.20.2.应用架构设计

在进行应用架构设计时，可以提前进行资源规划。

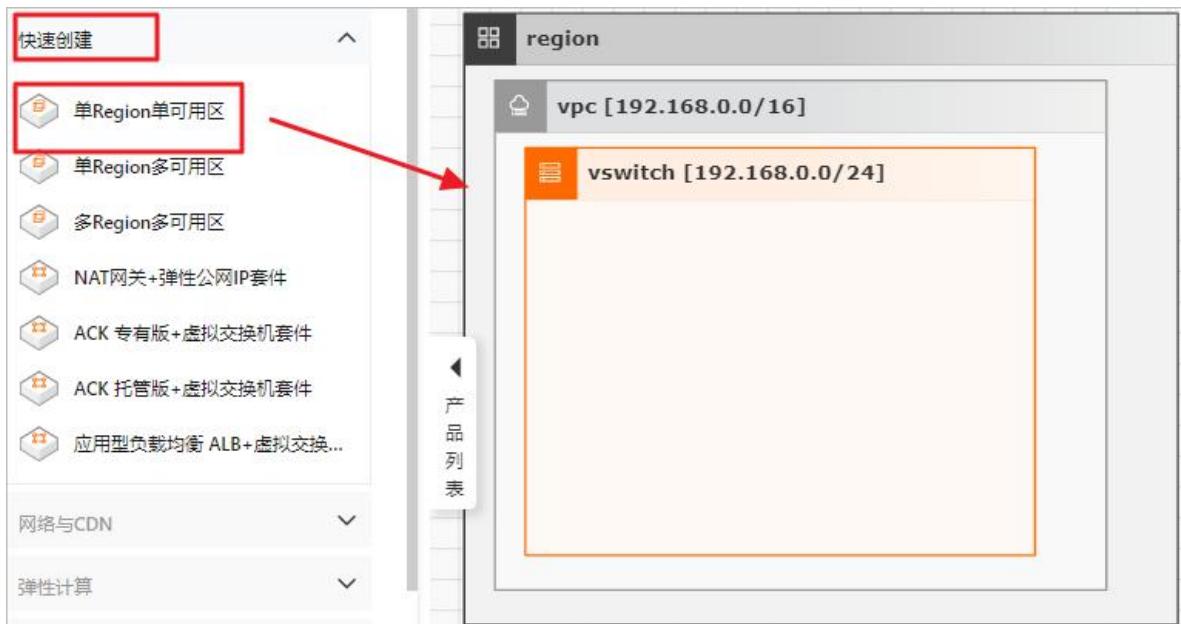
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC-BJ	192.168.0.0/16
AZ	VSW-BJ	可用区 F 区, 192.168.0.0/24
Region	华东 1 (杭州)	-
VPC	VPC-HZ	192.168.0.0/16
AZ	VSW-HZ	可用区 K 区, 192.168.0.0/24

步骤 1 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤 2 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。



依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



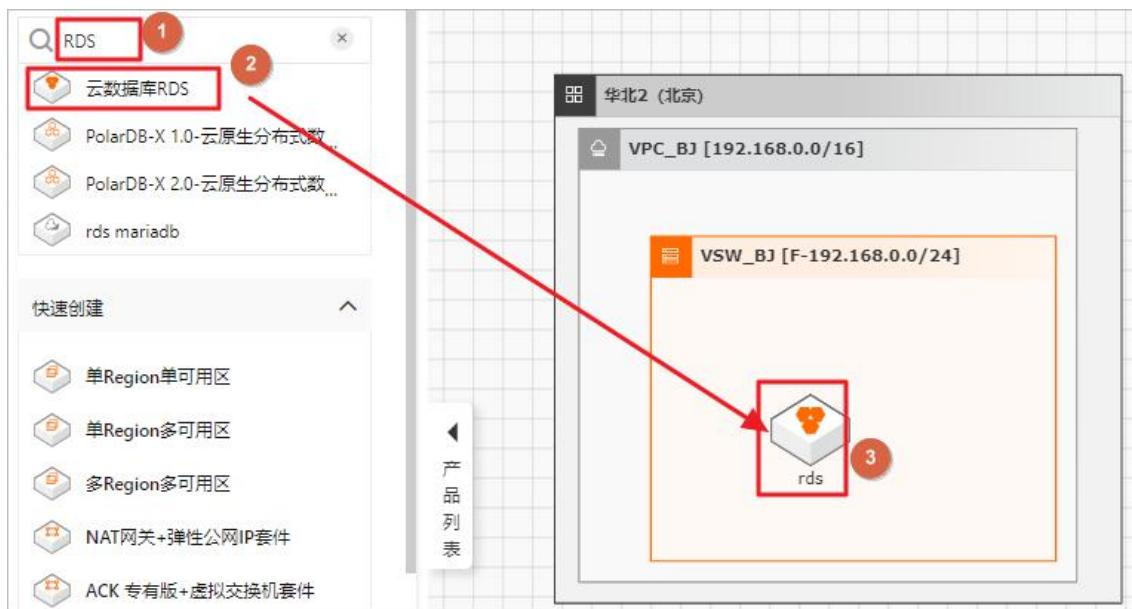
2. 双击 VPC，配置 VPC 参数。



2. 双击 vswitch，配置 vswitch 参数，可用区选择：华北 2 可用区 F。



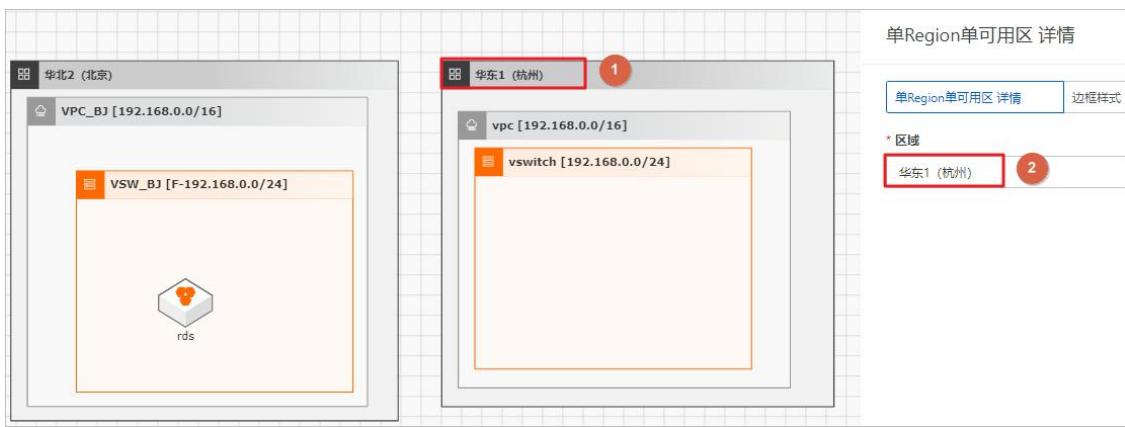
4. 在左侧搜索框中输入 rds，选定 RDS 图元，拖动到图中。



步骤 3 再从左侧产品列表的快速创建分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华东 1（杭州）。



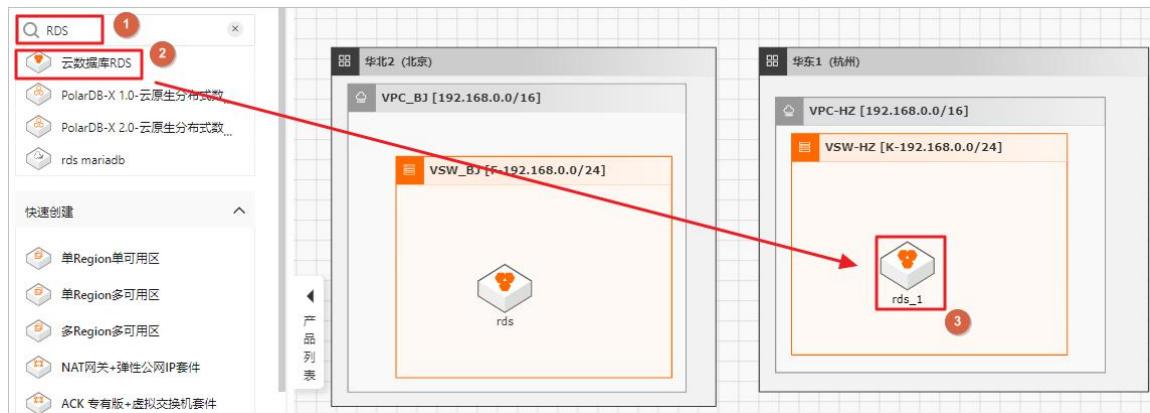
2. 双击 VPC，配置 VPC 参数。



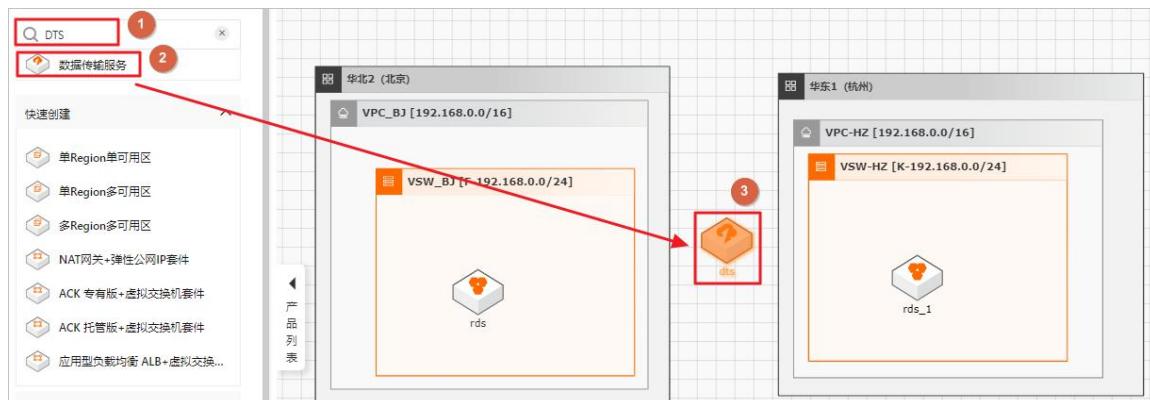
3. 双击 vswitch，配置 vswitch 参数，可用区选择：华东 1 可用区 K。



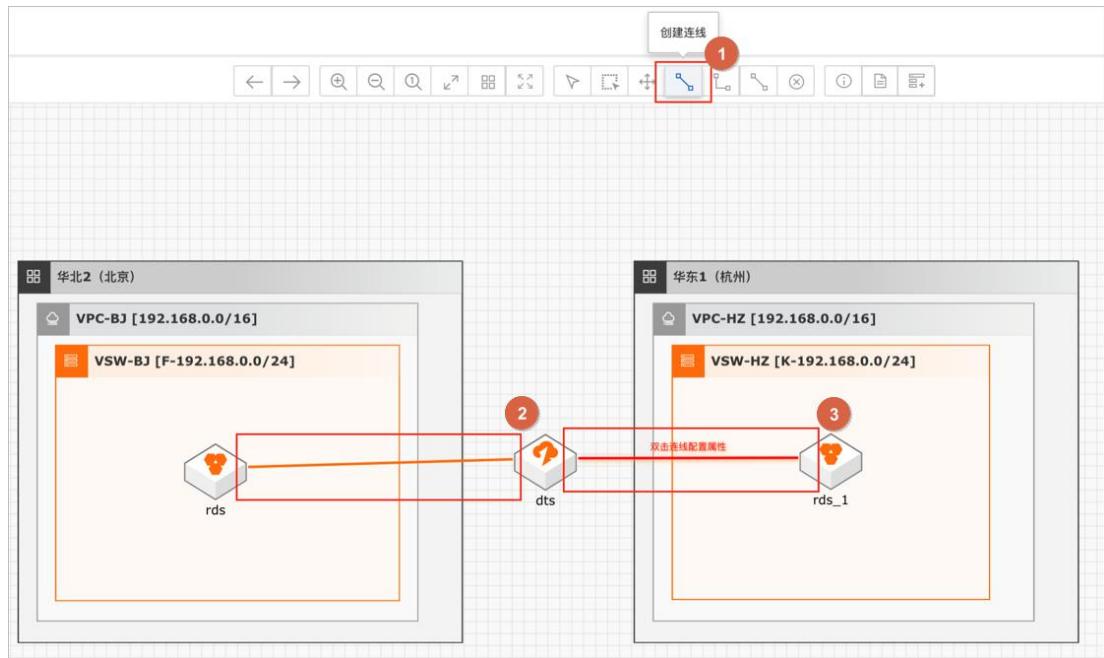
4. 在左侧搜索框中输入 rds，选定 RDS 图元，拖动到图中。



步骤 4 从左侧搜索框输入 dts，选定 DTS 图元，单击后拖入到画布区域中，松开鼠标左键。



步骤 5 在画布中间的工具栏中，点击创建连线图标，分别将 rds 与 dts、dts 和 rds\_1 建立连线。

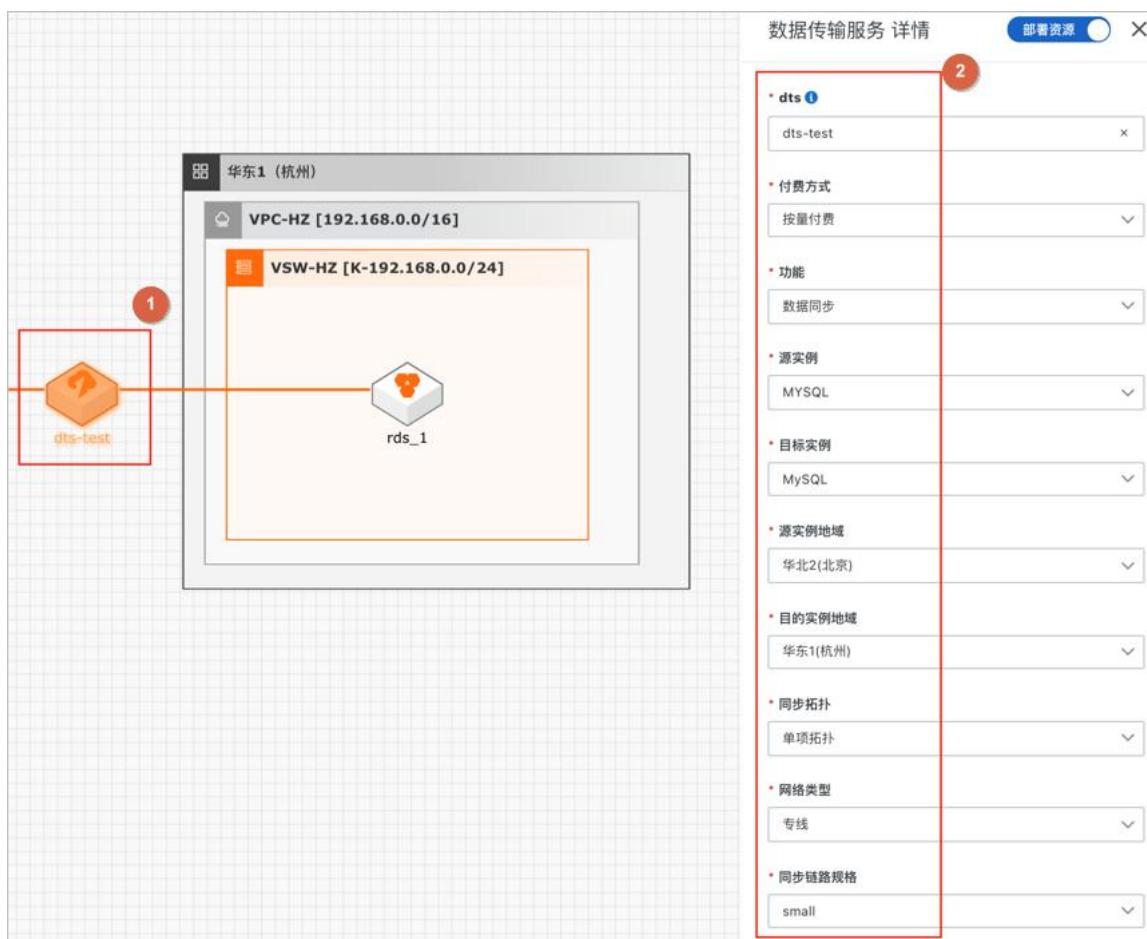


### 3.20.3.配置资源参数

步骤 1 分别双击 dts、dts 图标，配置相关参数，参数配置参考下表。

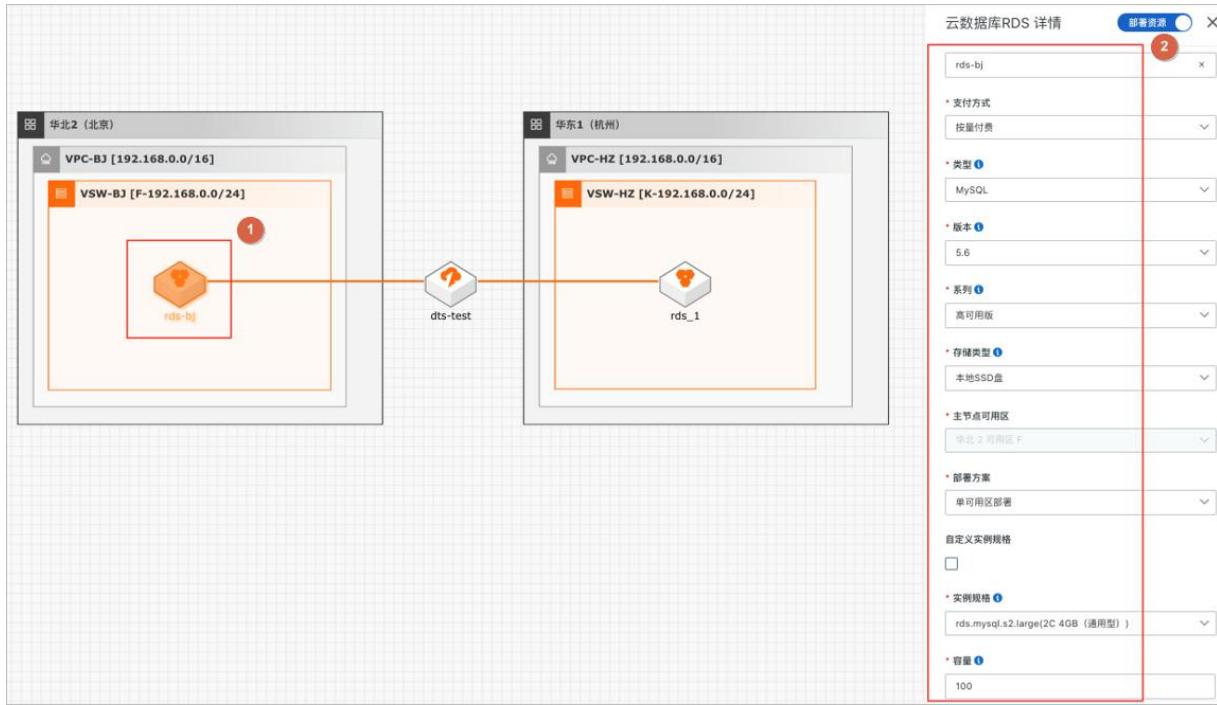
表一：DTS 参数配置

配置项	参数说明
dts 实例名	dts-test
付费方式	按量付费
功能	数据同步
源实例	MYSQL
目标实例	MYSQL
源实例地域	华北 2(北京)
目的实例地域	华东 1(杭州)
同步拓扑	单项拓扑
网络类型	专线
同步链路规格	small
数量	1



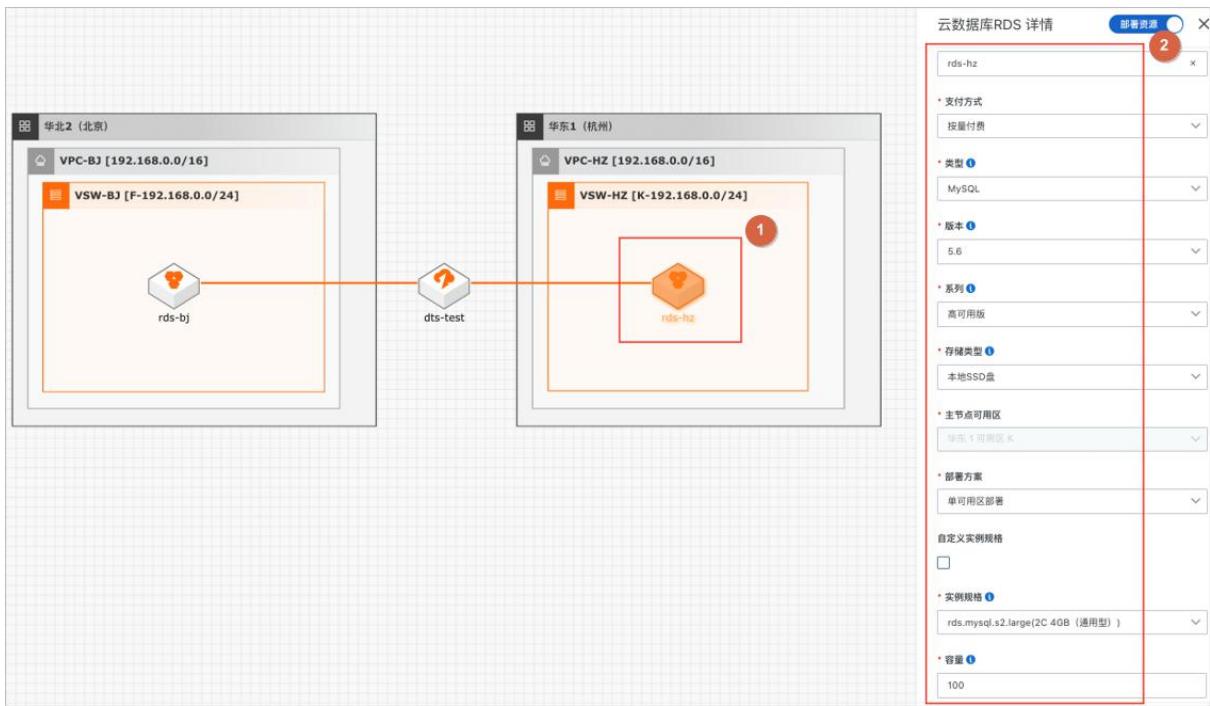
表二：RDS（北京）参数配置

配置项	参数说明
实例名	rds-bj
支付方式	按量付费
类型	MySQL
版本	5.6
系列	高可用版
存储类型	本地 SSD 盘
部署方案	单可用区部署
实例规格	rds.mysql.s2.large(2C 4GB (通用型))
容量	100

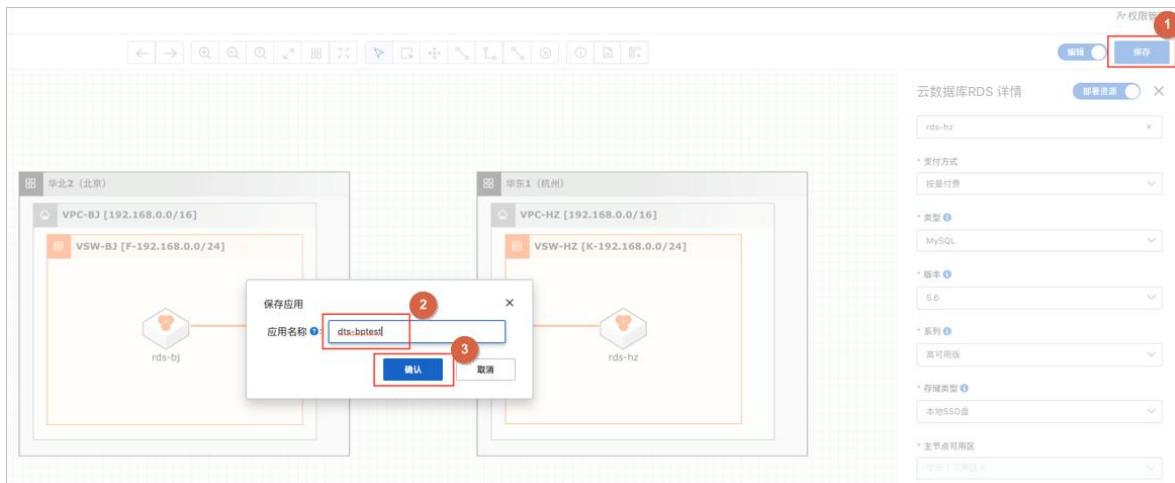


表三：RDS（杭州）参数配置

配置项	参数说明
实例名	rds-hz
支付方式	按量付费
类型	MYSQL
版本	5.6
系列	高可用版
存储类型	本地 SSD 盘
部署方案	单可用区部署
实例规格	rds.mysql.s2.large(2C 4GB (通用型))
容量	100

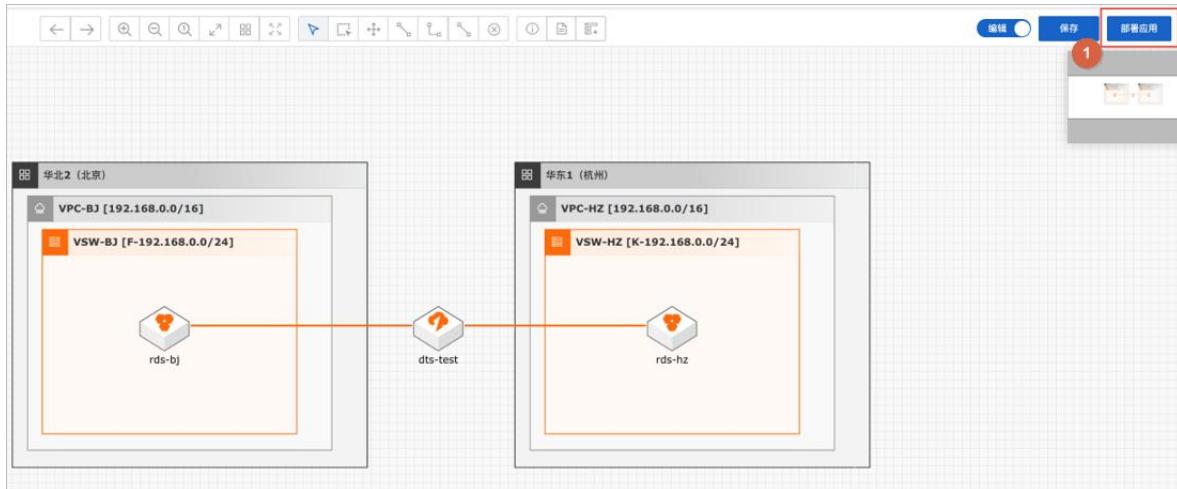


步骤 2 完成以上资源配置后，单击**保存**，并设置**应用名称**，最后单击**确认**。



### 3.20.4. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、是否有库存等，一般需要几十秒左右。

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	VSW-HZ [K-192.168.0.0/24]	vswitch	杭州	192.168.0.0/24	成功	校验通过	定位
2	VSW-BJ [F-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
3	rds-hz	rds	杭州	MySQL	成功	校验通过	定位
4	VPC-HZ [192.168.0.0/16]	vpc	杭州	192.168.0.0/16	成功	校验通过	定位
5	rds-bj	rds	北京	MySQL	成功	校验通过	定位
6	VPC-BJ [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位

状态:校验成功

**下一步: 价格清单**

**返回**

步骤 3 等待校验成功，单击**下一步: 价格清单**。这里会拉取应用所有配置的价格信息。

导出价格清单

免费 按量付费

资源成本占比

资源预算

- 大数据 大数据: 1.21 元/时
- 数据库 数据库: 2.48 元/时

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	状态	操作
1	dts-test	dts		rds.mysql.s2.large	1	2.48元/时	省 1.21 元/时	1.21 元/时	新购	定位
2	rds-hz	rds	杭州	rds.mysql.s2.large	1	1.21元/时	省 1.21 元/时	1.21 元/时	新购	定位
3	rds-bj	rds	北京	rds.mysql.s2.large	1	1.21元/时	省 1.21 元/时	1.21 元/时	新购	定位

状态: 计价成功

上一步: 资源校验

查看报告

下一步: 确认订单

1

步骤 4 可以单击**查看报告**, 查看应用的价格信息。



步骤 5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。



步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

#### 注意：

- 部署流程一旦开始后，无法取消。
- 部署时间预计 2 分钟左右，请耐心等待。



步骤 7 部署完成后，如下图所示。

**资源部署状态**

序号	资源名称 <a href="#">?</a> <a href="#">Q</a>	资源类型 <a href="#">Q</a>	付费类型	资源ID <a href="#">Q</a>	资源状态	资源更新时间	定位
3	VPC-HZ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-bp1k9s6pfa9st4v9njl7 <a href="#">D</a>	运行中	2022-01-04 10:39:07	定位
4	VSW-HZ [K-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-bp1k0xm22wodvx1edf5t0 <a href="#">D</a>	运行中	2022-01-04 10:39:07	定位
5	dts-test	dts (数据传输服务)	按量付费	dtszmoo1pq4p4ilbe4 <a href="#">D</a>	运行中	2022-01-04 10:39:06	定位
6	rds-bj	rds (云数据库RDS)	按量付费	rm-2ze3n5l587og47fm3 <a href="#">D</a>	运行中	2022-01-04 10:40:39	定位
7	rds-hz	rds (云数据库RDS)	按量付费	rm-bp1z392145dvx0oer <a href="#">D</a>	运行中	2022-01-04 10:40:39	定位

每页显示 [10](#) 共7条 < 上一页 [1](#) 下一页 >

**部署概要**

状态: 部署成功 订单编号: 21233363999042812334333170425212334134140425  
应用编号: VAS84TX9WTJ49YBD

[查看报告](#) [返回](#)

步骤 8 单击**查看报告**, 可以查看本次的部署报告。



步骤 9 单击返回，然后单击资源清单。

The screenshot shows the Cloud Speed Stack CADT interface. At the top, there are tabs for '新建' (Create), '应用' (Application), '资源' (Resource), '管理' (Management), and '导出' (Export). Below the tabs, the title 'dts-bptest' is displayed. The main area shows two network segments: '华北2 (北京)' and '华东1 (杭州)'. Each segment contains a VPC network diagram with subnets and resources like 'VSW-BJ' and 'rds-bj' in the first, and 'VSW-HZ' and 'rds-hz' in the second. Below the diagrams is a table titled '资源清单' (Resource List) with the following data:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位
4	VSW-HZ [K-192.168.0.0/24]	vswitch (虚拟交换机)	免费	vsw-bp1kxm22wodvxtedf5t0	新建	运行中	2022-01-04 10:39:07	定位
5	<b>dts-test</b>	dts (数据传输服务)	按量付费	dtszmoo1pq4p4ibe4	新建	运行中	2022-01-04 10:39:06	定位
6	rds-bj	rds (云数据库RDS)	按量付费	rm-2ze3n5i587og47fm3	新建	运行中	2022-01-04 10:40:39	定位
7	rds-hz	rds (云数据库RDS)	按量付费	rm-bplz39214sdvx0er	新建	运行中	2022-01-04 10:40:39	定位

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。

步骤 10 单击资源名称 **dts-test**，可跳转到对应的控制台。

The screenshot shows the Alibaba Cloud RDS for MySQL instance configuration page for the 'beijing-hangzhou-small' instance. On the left, there is a sidebar with navigation links: '作业配置' (Job Configuration), '同步初始化' (Sync Initialization), '性能监控' (Performance Monitoring), '增量同步性能' (Incremental Sync Performance), '监控报警' (Monitoring & Alarming), '任务日志' (Task Log), and '更多' (More). The main content area is divided into sections: '基本信息' (Basic Information) and '付费信息' (Billing Information).

**基本信息** section:

同步实例ID: dtszmoo1pq4p4ibe4	同步作业名称: beijing-hangzhou-small
源实例类型: RDS For MySQL	源RDS实例ID: 未配置
连接方式: 非加密连接	
状态: 未配置	
数据库类型: MySQL	
目标实例类型: RDS For MySQL	目标RDS实例ID: 未配置
连接方式: 非加密连接	
数据库类型: MySQL	

**付费信息** section:

源实例类型: RDS For MySQL	源实例地区: 华北2 (北京)
目标实例类型: RDS For MySQL	目标实例地区: 华东1 (杭州)
链接规格: small	
付费方式: 按量付费	创建时间: 2022年01月04日 10:38:16

## 3.20.5.DTS 实现 RDS 数据同步

### 配置源站 RDS 数据库

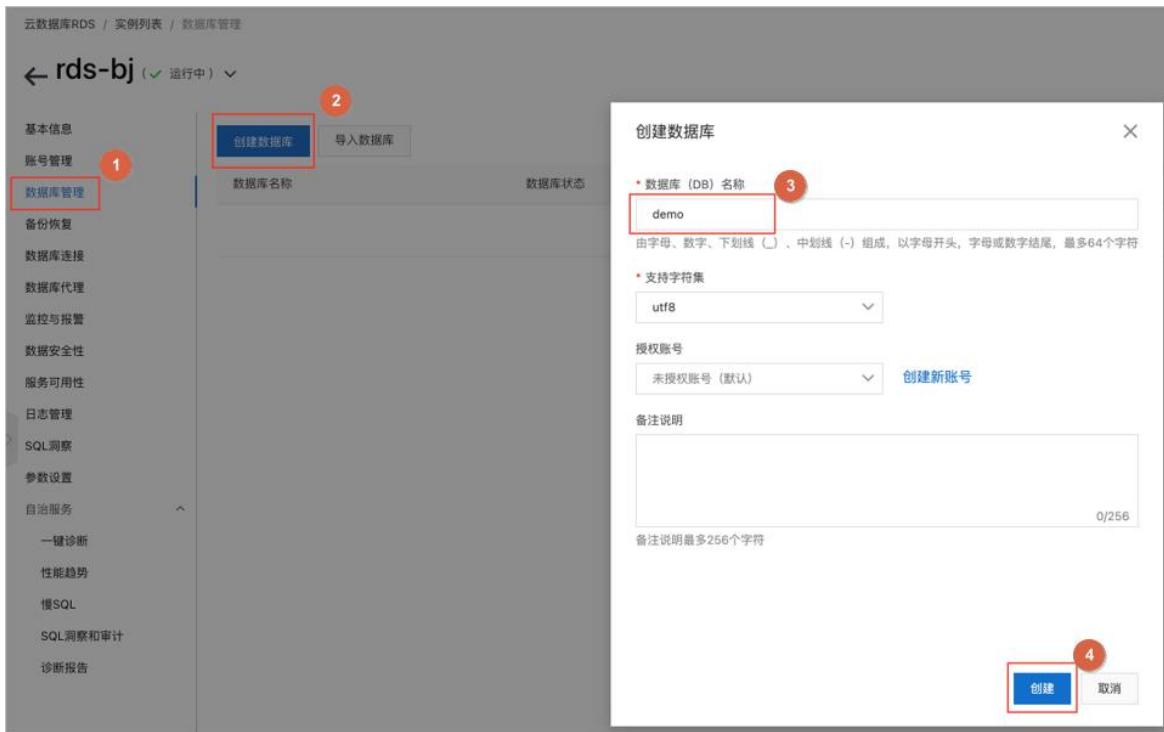
步骤 1 在 CADT 的资源列表页，点击 **rds-bj**，跳转到 RDS 的管理控制台。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位
4	VSW-HZ [K-192.168.0.0/24]	vswitch (虚拟交换机)	免费	vsw-bj1k0xm22wodvxlledf5t0	新建	运行中	2022-01-04 10:39:07	定位
5	dts-test	dts (数据传输服务)	按量付费	dtsznootpq4lp4lbe4	新建	运行中	2022-01-04 10:39:06	定位
6	<b>rds-bj</b>	rds (云数据库RDS)	按量付费	rm-2xe3n5i587eg47m3	新建	运行中	2022-01-04 10:40:39	定位
7	rds-hz	rds (云数据库RDS)	按量付费	rm-bpl239214sdvvdoer	新建	运行中	2022-01-04 10:40:39	定位

步骤 2 配置源数据库账号及数据库

#### 1. 增加 RDS 账号

## 2. 创建数据库实例



## 3. 登录数据库



4. 在 DMS 管理控制台登录数据库，输入账号、密码，测试连接成功后，点击**登录**



## 5. 执行建表 SQL，创建数据库表

```
CREATE TABLE `user` (
  `id` int NOT NULL AUTO_INCREMENT,
  `name` varchar(64) NULL COMMENT '姓名',
  `age` smallint NULL COMMENT '年龄',
  `email` varchar(64) NULL COMMENT '邮箱',
  `telephone` int(11) NULL COMMENT '手机',
  `remark` text NULL COMMENT '备注',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB
DEFAULT CHARACTER SET=utf8;
```

执行成功后，刷新表结构，可以看到数据表 user：

The screenshot shows the DMS Data Management Service interface with the SQL window open. A red box highlights the 'SQLConsole' tab. Another red box highlights the '执行(F8)' (Execute) button. A third red box highlights the '执行结果1' (Execution Result 1) tab. The SQL code for creating the 'user' table is pasted into the SQLConsole tab, and its execution results are shown in the Execution Result tab.

```

CREATE TABLE `user` (
  `id` int NOT NULL AUTO_INCREMENT,
  `name` varchar(64) NULL COMMENT '姓名',
  `age` smallint NULL COMMENT '年龄',
  `email` varchar(64) NULL COMMENT '邮箱',
  `telephone` int(11) NULL COMMENT '手机',
  `remark` text NULL COMMENT '备注',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB
DEFAULT CHARACTER SET=utf8;
  
```

Execution Result 1:

```

---共(1)条语句执行---

[语句1]:
CREATE TABLE `user` (
  `id` int NOT NULL AUTO_INCREMENT,
  `name` varchar(64) NULL COMMENT '姓名',
  `age` smallint NULL COMMENT '年龄',
  `email` varchar(64) NULL COMMENT '邮箱',
  `telephone` int(11) NULL COMMENT '手机',
  `remark` text NULL COMMENT '备注',
  PRIMARY KEY (`id`)
) ENGINE=InnoDB
DEFAULT CHARACTER SET=utf8
[Success], 耗时: 31(ms)
影响行数: 0
  
```

[消息] : 执行成功, 当前返回 [0] 行, 耗时 [31ms]

## 6. 右击 user 表，数据方案->测试数据构建，构建测试数据

The screenshot shows the DMS Data Management Service interface with the SQL window open. A red box highlights the '右击弹出' (Right-clicked) context menu for the 'user' table. Another red box highlights the '数据方案' (Data Scheme) item in the context menu. A third red box highlights the '测试数据构建' (Test Data Build) item in the expanded '数据方案' submenu. A fourth red box highlights the '测试数据构建' (Test Data Build) item in the expanded 'Test Data Build' submenu.

测试数据构建 - user

\* 配置算法:

序号	列名	类型	默认值	约束	生成方式
1	id	int(11)		PK, 自增, 非空	随机 (自增, 步长 1)
2	name	varchar(64)			随机 (变长字符串)
3	age	smallint(6)			随机 (区间 [1, 100])
4	email	varchar(64)			随机 (变长字符串)
5	telephone	int(11)			随机 (区间 [1, 1000])
6	remark	text			随机 (变长字符串)

预览测试数据

\* 生成行数:

\* 冲突处理:  遇到数据冲突则跳过  遇到数据冲突则替换

5 提交申请

✓ 执行

进度: 

完成

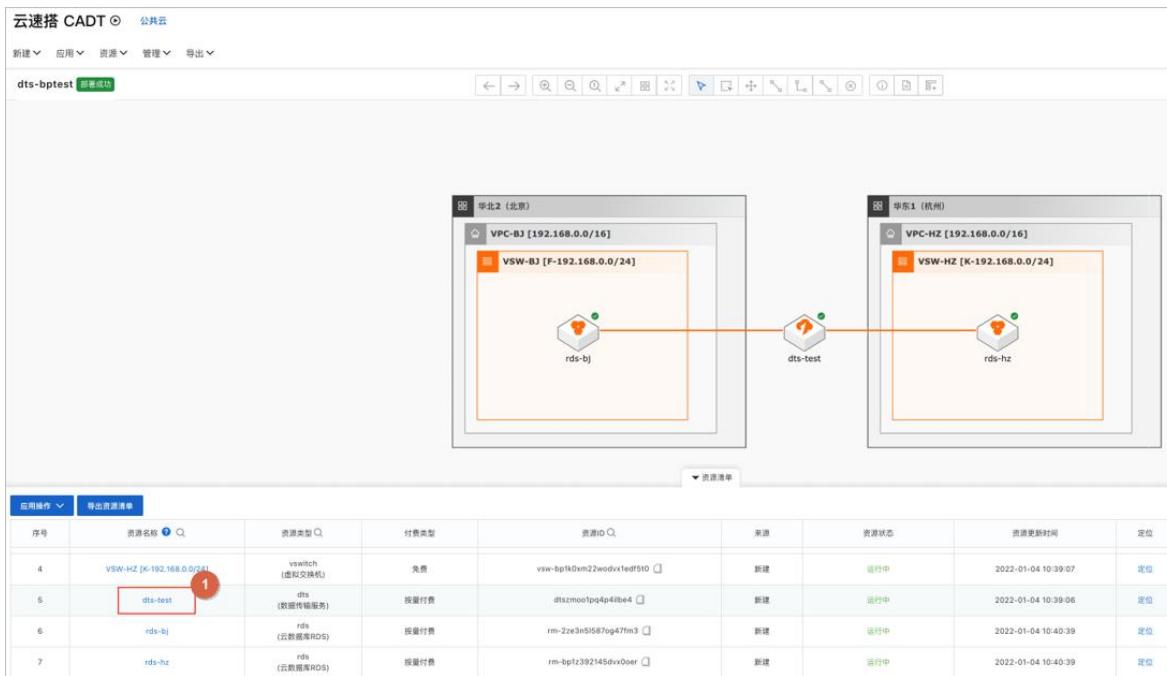
[2022-01-04 14:40:23]: 获取数据库链接成功  
[2022-01-04 14:40:23]: 单个SQL大小设置为(byte):16777216  
[2022-01-04 14:40:23]: 开始准备测试数据。总行数: 10000  
[2022-01-04 14:40:23]: 已经构建 2,000 行数据, 耗时: 737 (ms)  
[2022-01-04 14:40:24]: 已经构建 7,000 行数据, 耗时: 1,059 (ms)  
[2022-01-04 14:40:24]: 已经构建 10,000 行数据。耗时: 1,304 (ms)  
[2022-01-04 14:40:24]: 测试数据构建成功

4 完成

6 任务执行完成

## 使用 DTS 同步数据到目标 RDS 数据库

步骤 1 在 CADT 的资源列表页，点击 **dts-test**，跳转到 DTS 的管理控制台。



## 步骤 2 在 DTS 控制台点击配置同步作业

The screenshot shows the DTS configuration interface for a sync job named 'beijing-hangzhou-small'. The top navigation bar includes links for '工作台' (Workbench), '搜索...' (Search), '费用' (Cost), '工单' (Ticket), 'ICP 备案' (ICP Record Filing), '企业' (Enterprise), '支持' (Support), 'App', and '帮助' (Help).

The main area displays basic information for the sync job:

同步实例ID: dtszmoo1pq4p4lbe4	同步作业名称: beijing-hangzhou-small
源实例类型: RDS For MySQL	源RDS实例ID: 未配置
连接方式: 非加密连接	
状态: 未配置	
数据库类型: MySQL	
目标实例类型: RDS For MySQL	目标RDS实例ID: 未配置
连接方式: 非加密连接	
数据库类型: MySQL	

A sidebar on the left lists configuration sections: '作业配置' (Job Configuration), '同步初始化' (Sync Initialization), '性能监控' (Performance Monitoring), '增量同步性能' (Incremental Sync Performance), '监控报警' (Monitoring & Alarming), and '任务日志' (Task Log). A red circle with the number '1' highlights the '配置同步作业' (Configure Sync Job) button at the top right of the main panel.

## 步骤 3 配置源和目的数据库

创建同步作业 < 返回数据同步列表

1.选择同步通道的源及目标实例 > 2.选择同步对象 > 3.高级设置 > 4.预检查

同步作业名称: beijing-hangzhou-small

**源实例信息**

实例类型: RDS实例  
实例地区: 华北2 (北京)  
实例ID: rm-2ze3n5l587og47fm3 (1)  
连接方式: 非加密连接 (radio) SSL安全连接

**目标实例信息**

实例类型: RDS实例  
实例地区: 华东1 (杭州)  
实例ID: rm-bp1z392145dvv0oer (2)  
连接方式: 非加密连接 (radio) SSL安全连接

取消 授权白名单并进入下一步 (3) 体验新版控制台

阿里云 | 工作台

创建同步作业 < 返回数据同步列表

1.选择同步通道的源及目标实例 > 2.选择同步对象 > 3.高级设置 > 4.预检查

正在创建同步账号, 创建过程需要30秒左右, 请耐心等待.....

100% (1)

授权白名单并进入下一步 (3) 体验新版控制台

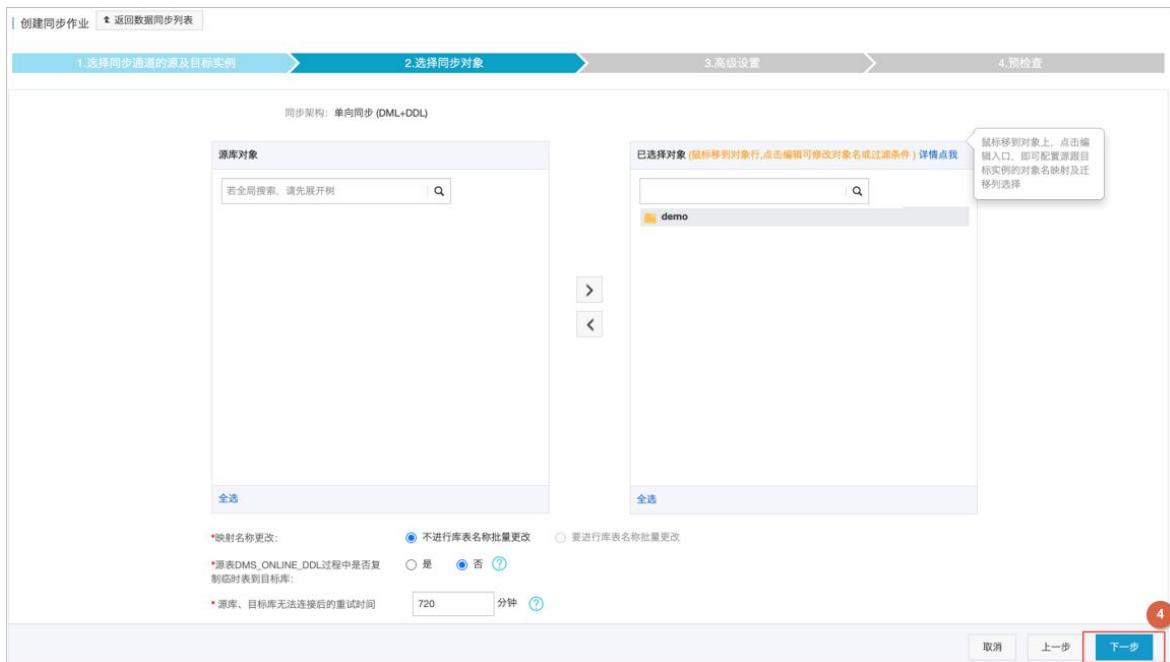
同步作业名称: beijing-hangzhou-small

**源实例信息**

实例类型: RDS实例  
实例地区: 华北2 (北京)  
实例ID: rm-2ze3n5l587og47fm3  
连接方式: 非加密连接 (radio) SSL安全连接

**目标实例信息**

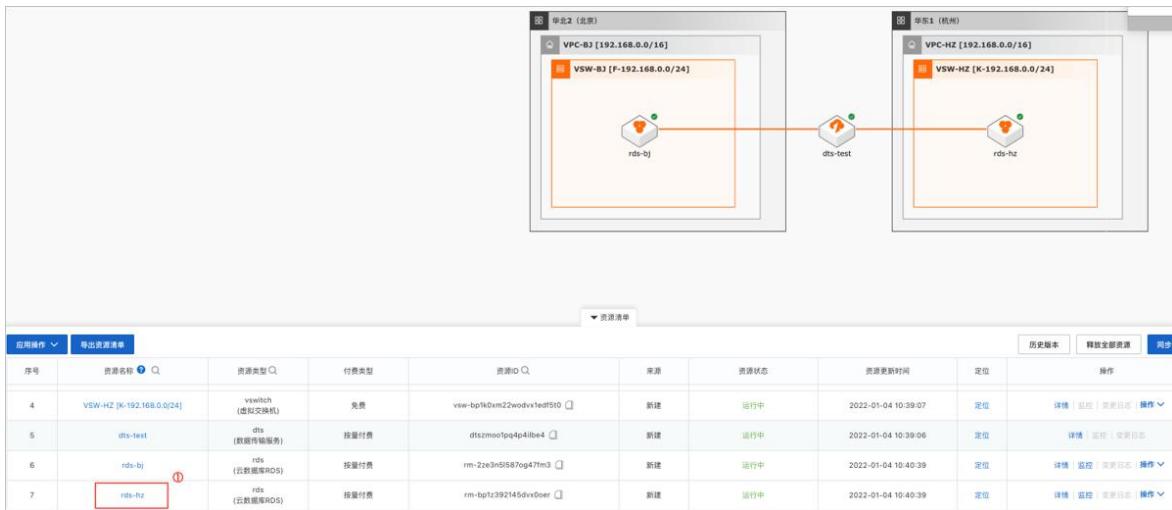
实例类型: RDS实例  
实例地区: 华东1 (杭州)  
实例ID: rm-bp1z392145dvv0oer  
连接方式: 非加密连接 (radio) SSL安全连接





## 检查目标 RDS 数据库

步骤 1 在 CADT 的资源列表页，点击 rds-hz，跳转到目标 RDS 的管理控制台。



## 步骤 2 重置自动创建的账号 (dtssyncwriter) 的密码

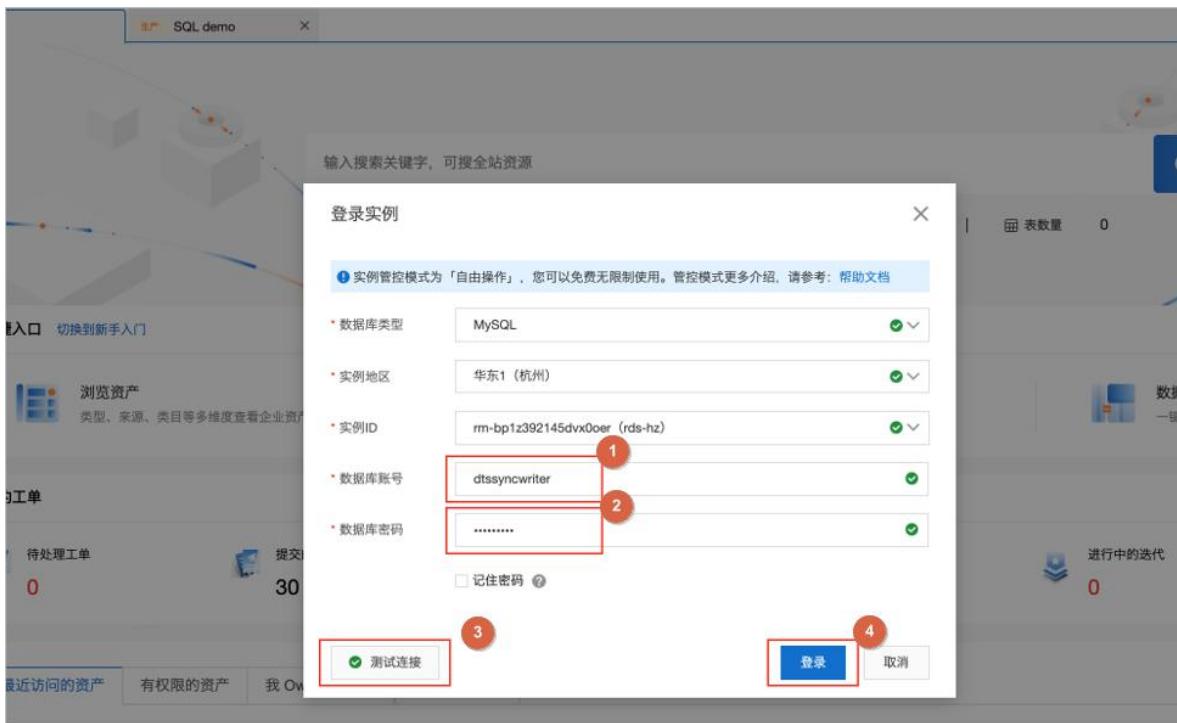
The screenshot shows the AliCloud RDS console interface. On the left, there's a sidebar with various management tabs like '基本信息', '账号管理' (highlighted with a red box and circled with a red number 1), '数据库管理', '备份恢复', '数据库连接', '数据库代理', '监控与报警', '数据安全性', '服务可用性', and '日志管理'. The main area shows a list of accounts for the instance 'rds-hz'. One account, 'dtssyncwriter', is selected. On the right, there are buttons for '登录数据库', '构建数仓', '操作指引', and '重启实例'. A red box and circled red number 2 highlight the '重置密码' (Reset Password) button in the '操作' column for the selected account.

This screenshot shows a modal dialog titled 'Reset Account Password'. It contains fields for 'New Password' and 'Confirm New Password', both highlighted with a red box and circled with a red number 3. At the bottom, there are '确定' (Confirm) and '取消' (Cancel) buttons, with the '确定' button highlighted with a red box and circled with a red number 4.

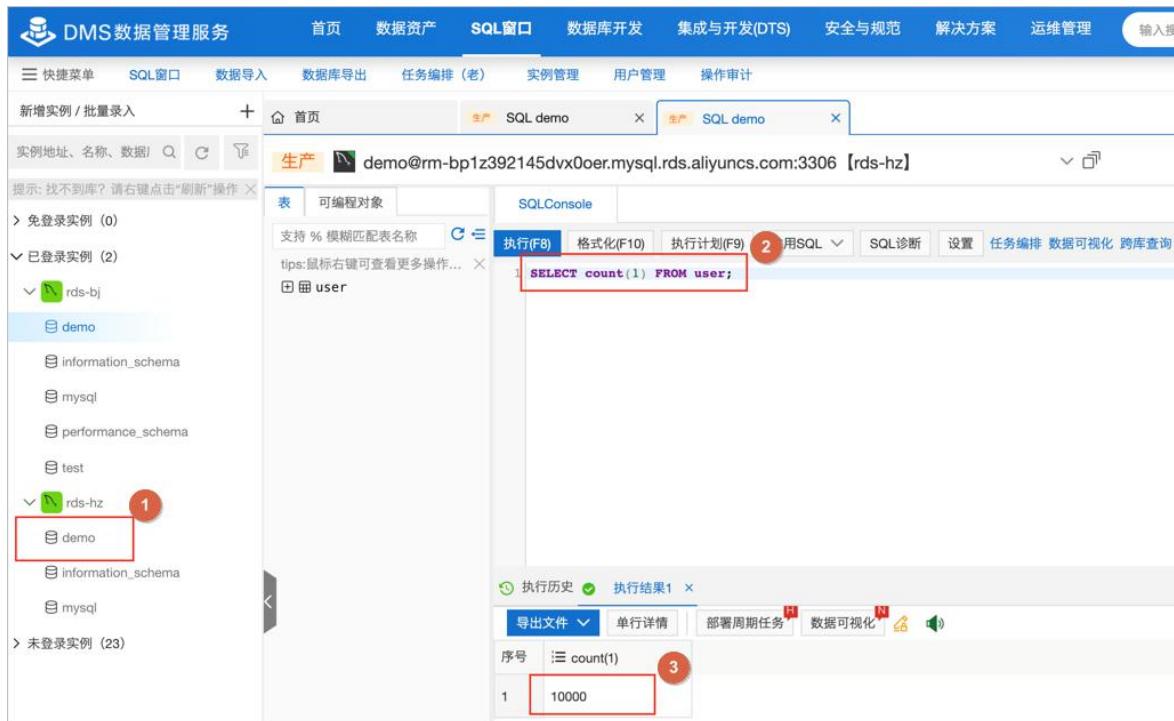
## 步骤 3 用账号 (dtssyncwriter) 登录数据库

The screenshot shows the same RDS console interface as the previous step. The '登录数据库' (Login Database) button in the top right corner is highlighted with a red box and circled with a red number 1.

在 DTS 控制台输入步骤 2 的账号、密码。



步骤 4 检查 rds-hz 数据库的数据与 rds-bj 数据库的数据一致性。



经过检查，发现 rds-hz 自动创建了 demo 数据库，以及数据表 user，自动同步了 10000 条源表里的记录到目标数据库中。

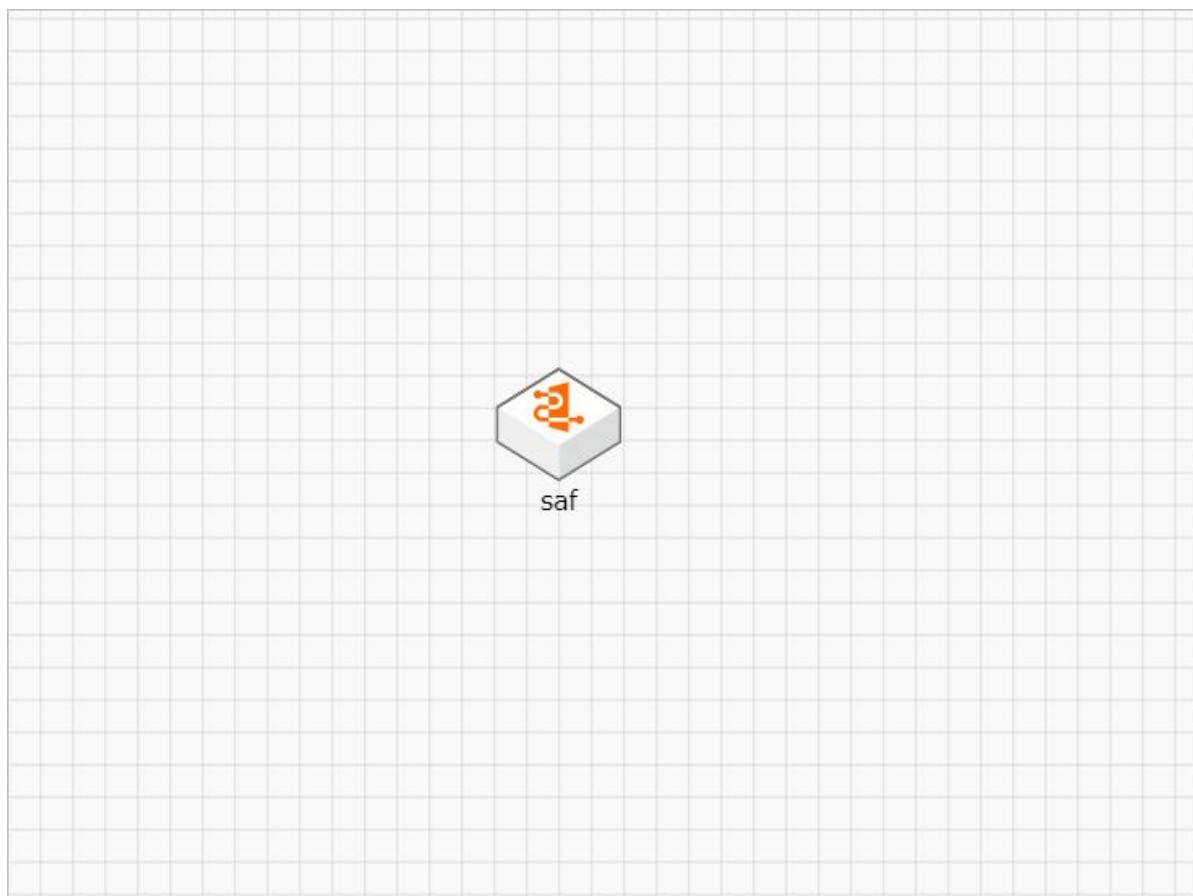
## 3.21.云速搭部署风险识别 SAF 最佳实践

作者 | 阿里云解决方案架构师 七凌

### 3.21.1.云速搭架构设计

#### 方案架构

通过云速搭 CADT 实现风险识别服务的部署，并可以基于已有的应用，多次部署，方便快捷。



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	资源级别
风险识别	全局

### 3.21.2.CADT 设计部署风险识别服务

步骤 15 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

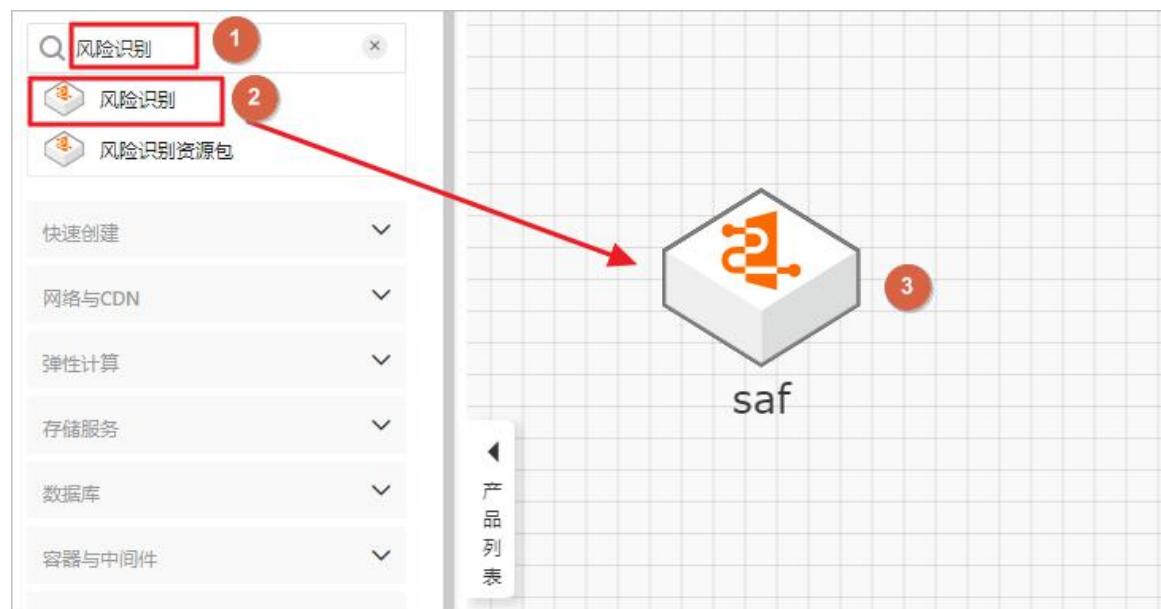
**说明：**如果提示需要开通服务，请根据提示进行开通。

The screenshot displays the Cloud Speed Stack CADT Control Console. At the top, there's a navigation bar with '新建' (New), '应用' (Application), '资源' (Resource), and '导出' (Export) dropdowns. To the right, it shows '专利号: CN111930290B' and a '查看最佳实践' (View Best Practice) button. Below the navigation, a welcome message '欢迎使用云速搭!' (Welcome to Cloud Speed Stack!) is displayed. A map of China highlights several cities: Beijing, Shanghai, Guangzhou, Shenzhen, Hangzhou, Chongqing, Chengdu, and Dalian. On the right side, there are two main sections: '未分配区域' (Unassigned Region) and '产品动态' (Product News). The '未分配区域' section has a table with columns '应用名称' (App Name), '创建时间' (Creation Time), and '状态' (Status), showing '没有数据' (No data). The '产品动态' section lists three items: 1. 支持用户对应用进行架构探查, 自动产生已保有应用的架构 (Support users to probe application architecture, automatically generate architecture for existing applications) - dated 2021年9月31日 (September 31, 2021). 2. 支持RAM权限管理, 对子用户授予不同的权限和资源组, 控制子用户对资源的访问和操作 (Support RAM permission management, grant different permissions and resource groups to sub-users, control sub-users' access and operations to resources) - dated 2021年9月31日 (September 31, 2021). 3. 支持应用状态实时更新, 实时更新服务的状态和配置 (Support real-time update of application status, real-time update of service status and configuration) - dated 2021年9月30日 (September 30, 2021).

步骤 16 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤 17 从左侧**产品列表**搜索关键字找到**风险识别**服务，选中并拖拽到右侧空白画布中。



步骤 18 双击风险识别图标，根据实际需求配置资源参数。

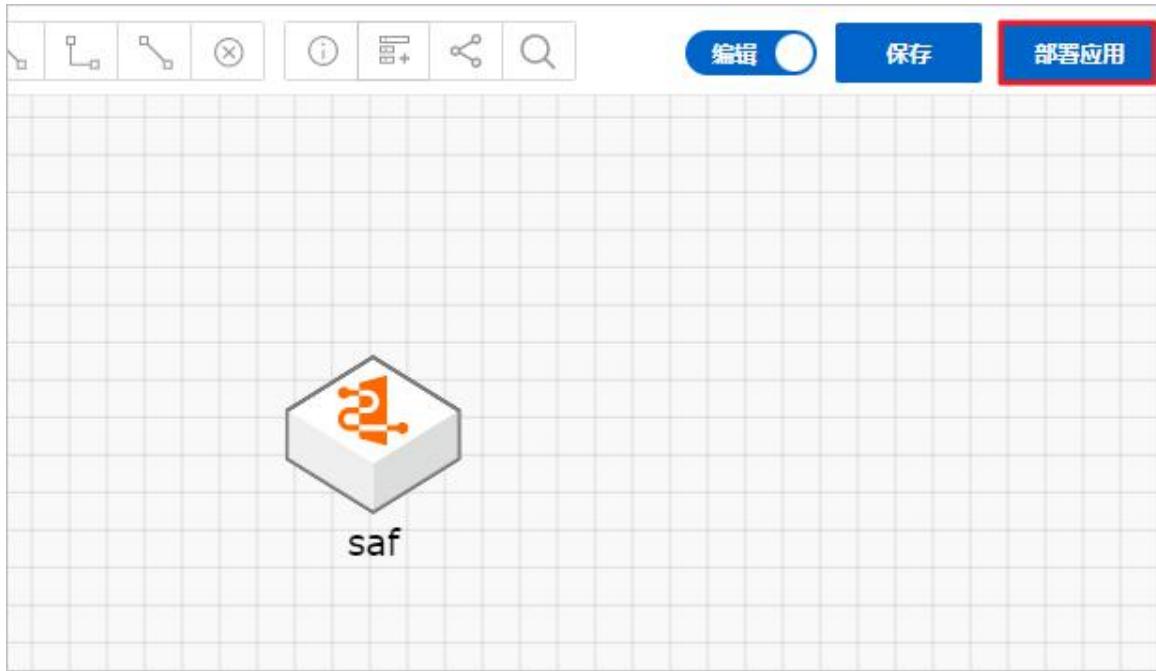
配置项	参数说明
支付方式	包年包月/购买时长/1个月
产品类型	反欺诈服务
规格	进阶版



步骤 19 部署前需要将设计好的架构保存为应用，单击右上角的**保存**，并设置**应用名称**，例如：“风险识别一月”。



步骤 20 保存为应用后，单击**部署应用**。



步骤 21 等待资源校验成功，单击**下一步：价格清单**。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	saf	风险识别		2	成功	校验通过	定位

状态: **校验成功**

**下一步：价格清单** **返回**

A screenshot of the 'Resource Verification' dialog box. The title bar says '资源验证'. Below it is a table with columns: 序号 (Index), 资源名称 (Resource Name), 资源类型 (Resource Type), 区域 (Region), 规格 (Specification), 结果 (Result), 备注 (Remarks), and 操作 (Operation). There is one row of data: Index 1, Resource Name saf, Resource Type 风险识别 (Risk Identification), Region (empty), Specification 2, Result 成功 (Success), Remarks 校验通过 (Verification Passed), and Operation 定位 (Locate). At the bottom left, it says '状态: **校验成功**' (Status: **Verification Passed**). At the bottom right are two buttons: '下一步：价格清单' (Next Step: Price List) and '返回' (Return).

步骤 22 在**导出价格清单**对话框中，CADT 会为您计算出应用所含资源的价格，包括**原价**、**优惠**以及最终的**实付价格**，在这里您需要确认下所购风险识别服务的**原价**、**优惠**以及**实付价格是否正确**，确认无误，再单击**下一步：确认订单**。



步骤 23 在确认订单对话框中，勾选《云速搭服务条款》，单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

### 3.21.3.基于已有应用部署

在云速搭 CADT 上，如果您有多次部署相同应用的需求时，无需再重新设计架构、配置参数，可以基于已有的应用一键下单购买。

步骤 1 单击应用 > 我的应用，进入我的应用页面。



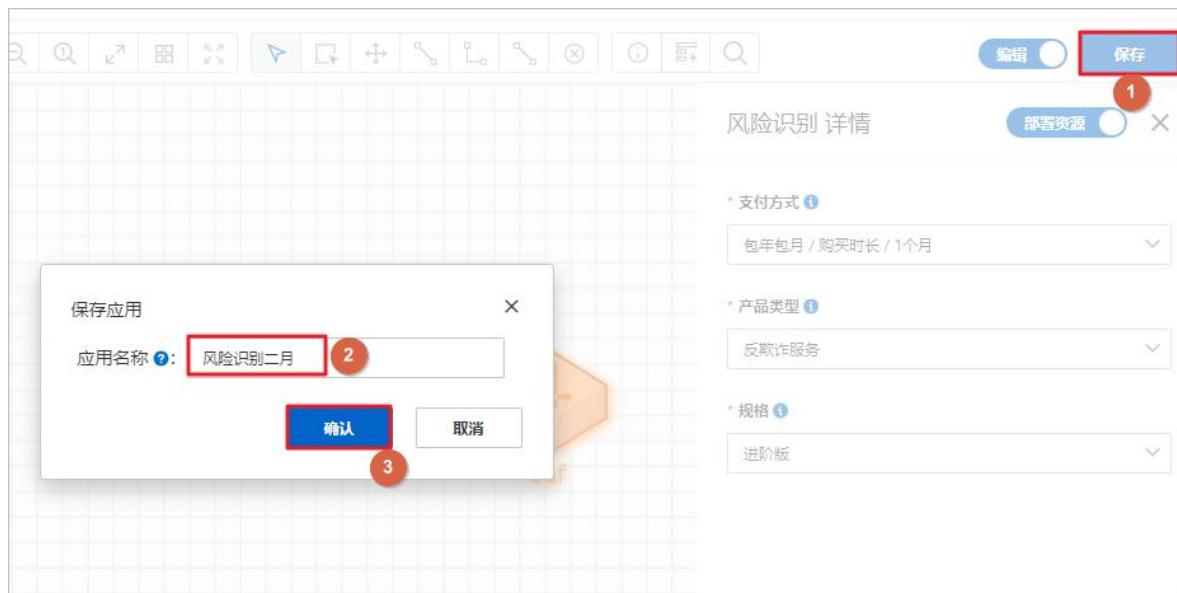
步骤 2 找到刚才创建的“风险识别一月”应用，单击复制架构图。

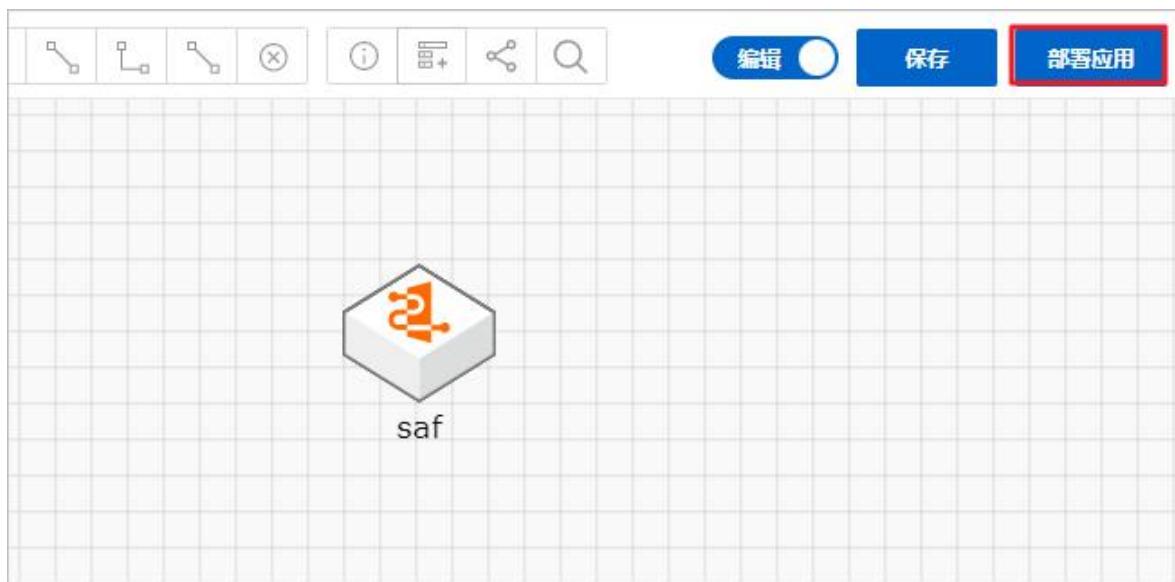


步骤3 CADT会自动将应用及其资源配置信息复制到画布中。



步骤4 此时，只需要单击右上角的保存，设置不同的应用名称，即可按界面提示进行资源部署。





## 4.云速搭部署容器、大数据、数据库

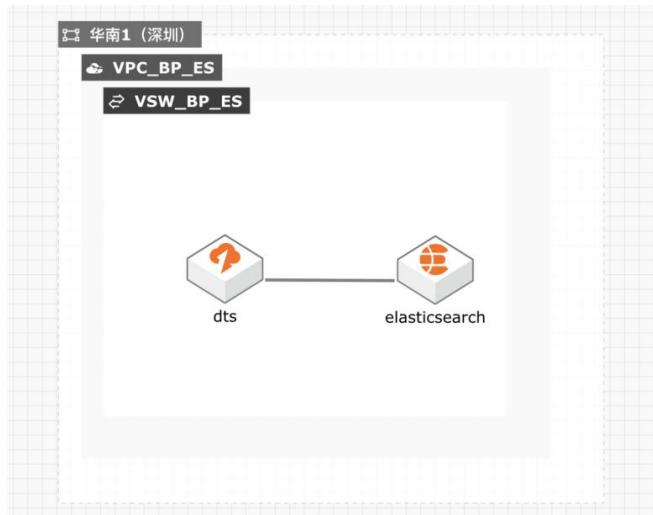
### 4.1.云速搭部署 Elasticsearch 应用

作者 | 阿里云解决方案架构师 袁影

#### 4.1.1.云速搭架构设计入门

##### 方案架构

通过云速搭实现一个 DTS+Elasticsearch 的搜索引擎架构，构建一个快速分析和检索业务数据的系统。



##### 理解资源级别

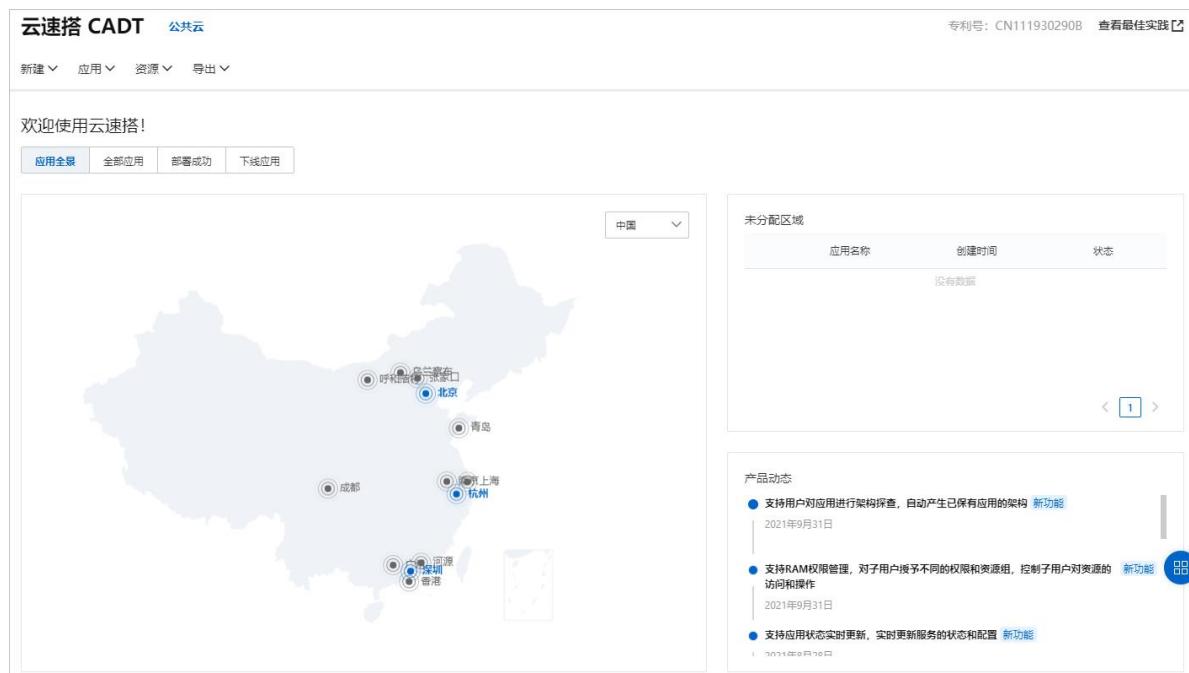
每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
DTS	Region
Elasticsearch	VSW

## 登录云速搭 CADT

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。



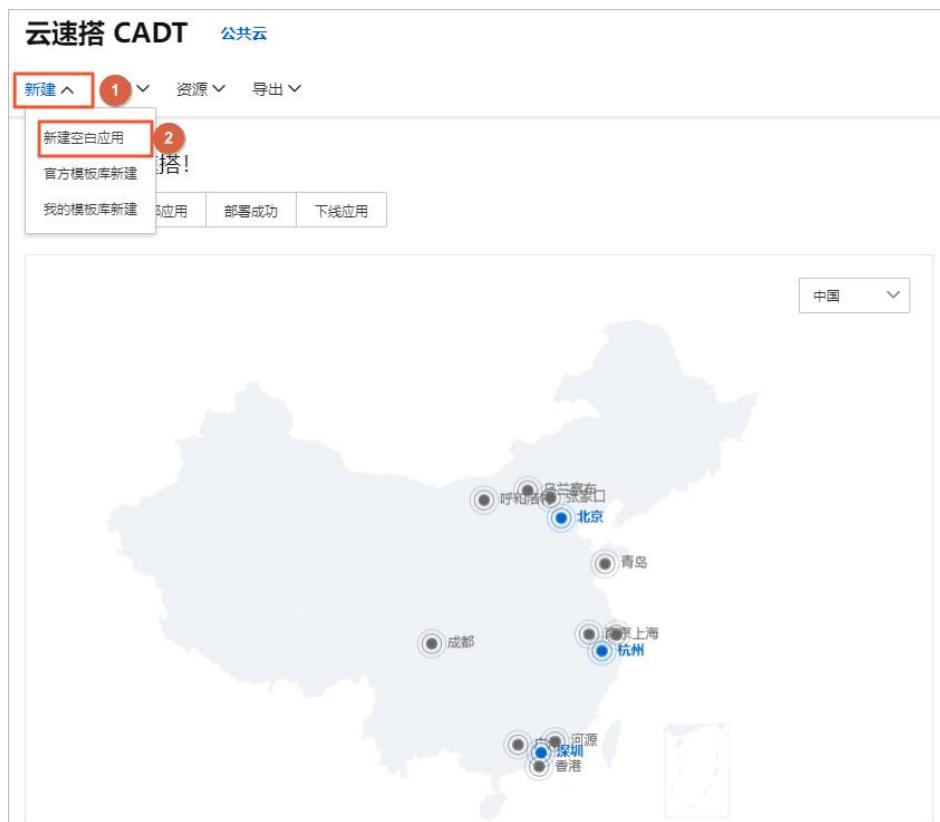
### 4.1.2. 应用架构设计

在进行应用架构设计时，可以提前进行资源规划。

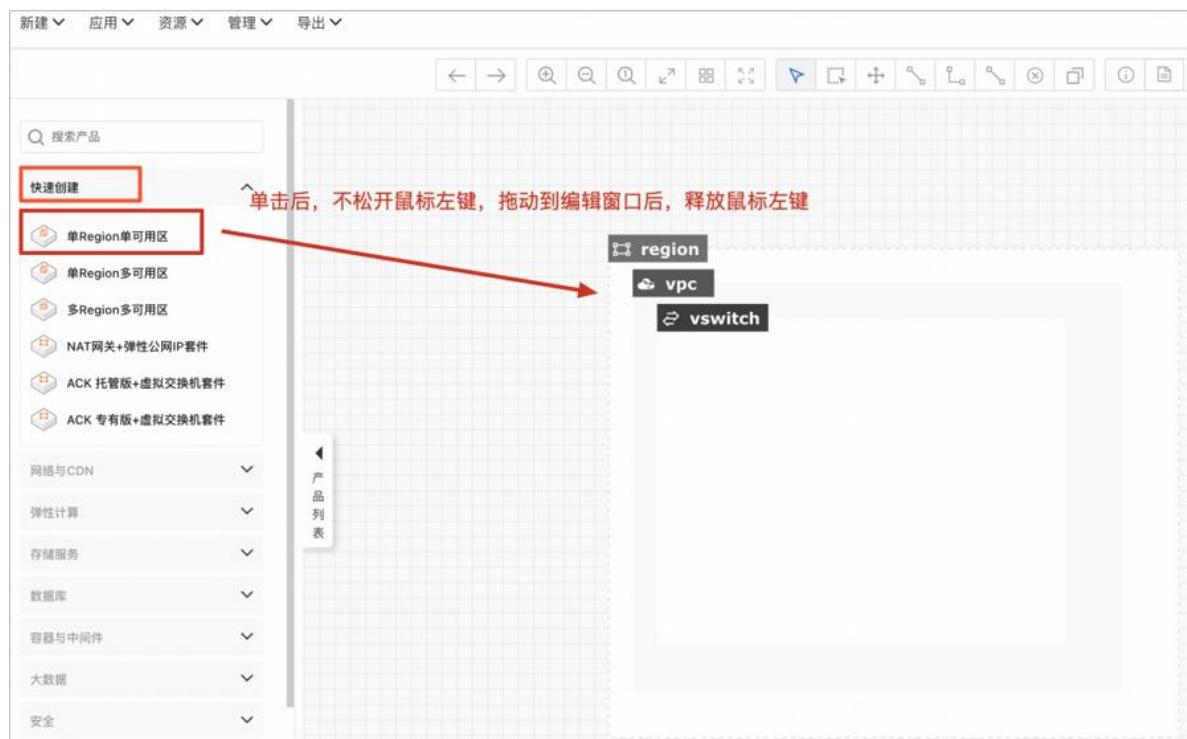
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	深圳	-
VPC	VPC_BP_ES	192.168.0.0/16
AZ	VPC_BP_ES	可用区 E 区, 192.168.0.0/24

步骤 1 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

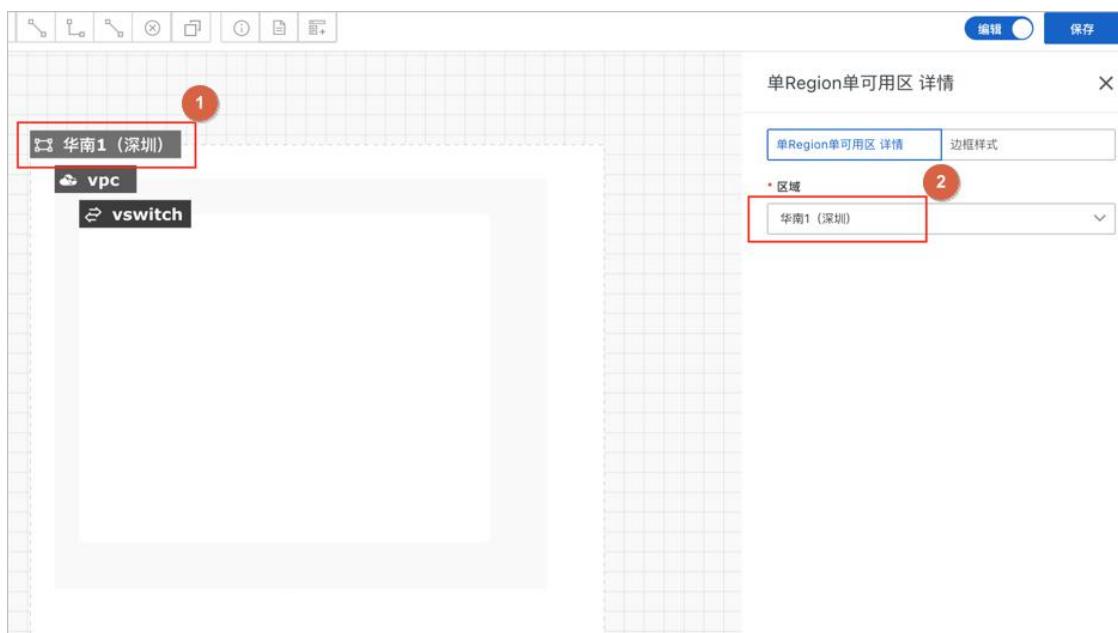


步骤 2 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。



步骤3 依次双击Region、VPC、vswitch进行配置。

1. 双击region，在右侧弹出窗口中，选择华南1（深圳）。



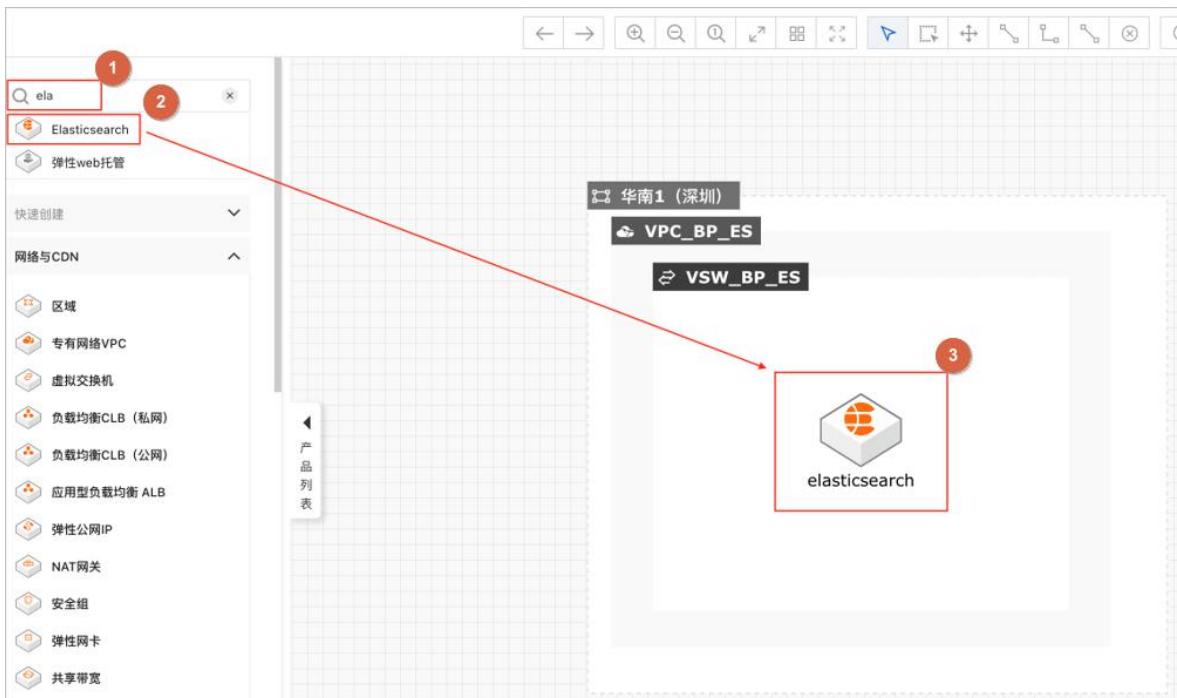
2. 双击VPC，配置VPC参数。



3. 双击vswitch，配置vswitch参数，可用区选择：深圳 可用区 E。



步骤 4 在左侧搜索框中输入 elasticseach，选定 Elasticsearch 图元，拖动到 vswitch 中。



步骤 5 双击 elasticsearch 组件，配置参数，这里输入一些示例配置。

**Elasticsearch 详情**

**部署资源**  X

**购买方式**  新购

**阿里云Elasticsearch** elasticsearch

**支付方式** 按量付费

**可用区** 华南1可用区E

**选择服务** 通用商业版

**版本** 6.7 (推荐)

**场景初始化配置** 通用场景

**可用区数量** 单可用区

**数据节点**

**Elasticsearch 详情**

**部署资源**  X

**数据节点规格族** 云盘型

**数据节点规格** elasticsearch.sn1ne.large(2核4G)

**提示**  
指定节点存储类型以及存储容量，单节点存储容量乘以节点数即为该Elasticsearch实例的总存储大小。  
在配置存储时，请考虑索引、分配、副本以及预留资源使用水位的影响。

**数据节点存储类型** 高效云盘

高效云盘提供较为低廉的存储能力，适合大规模数据量的日志及分析场景。6.7版本、7.4版本支持单节点最大容量20TB

**云盘加密**

**数据单节点存储空间**  
20 20480 100 GiB  
 SSD云盘最大2048GiB，高效云盘超过2048GiB时，只能取：2560、3072、3584、4096、4608、5120(7.4或者增强版实例超过5120GiB时，可取5632、6144、8192、10240、12288、14336、16384、18432、20480)

**Elasticsearch 详情**

**部署资源**  X

**数据节点数量** 2 50 2

两个节点集群有脑裂风险，请谨慎选择

**Kibana节点**

**Kibana节点规格** elasticsearch.sn1ne.large(2核4G)

**专有主节点**

**冷数据节点**

**协调节点**

**弹性数据节点**

**登录密码**  X 取消

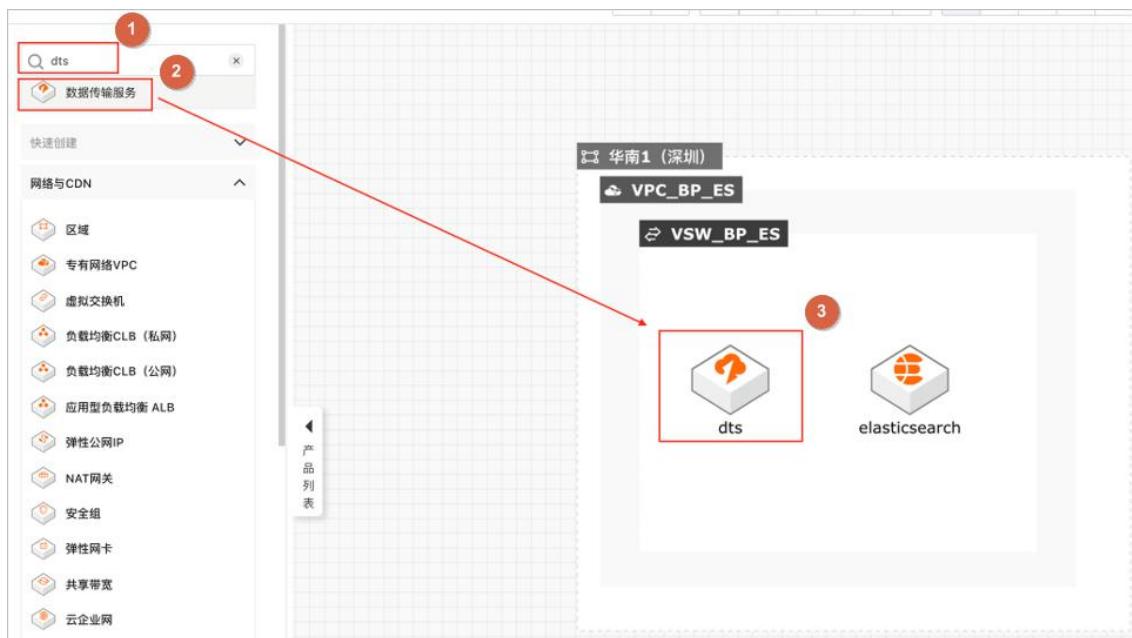
大写、小写、数字、特殊字符占三种，长度为8–32位；特殊字符为=+!@#\$%^&\*()\_-

**确认登录密码**  X 取消

大写、小写、数字、特殊字符占三种，长度为8–32

关闭 部署

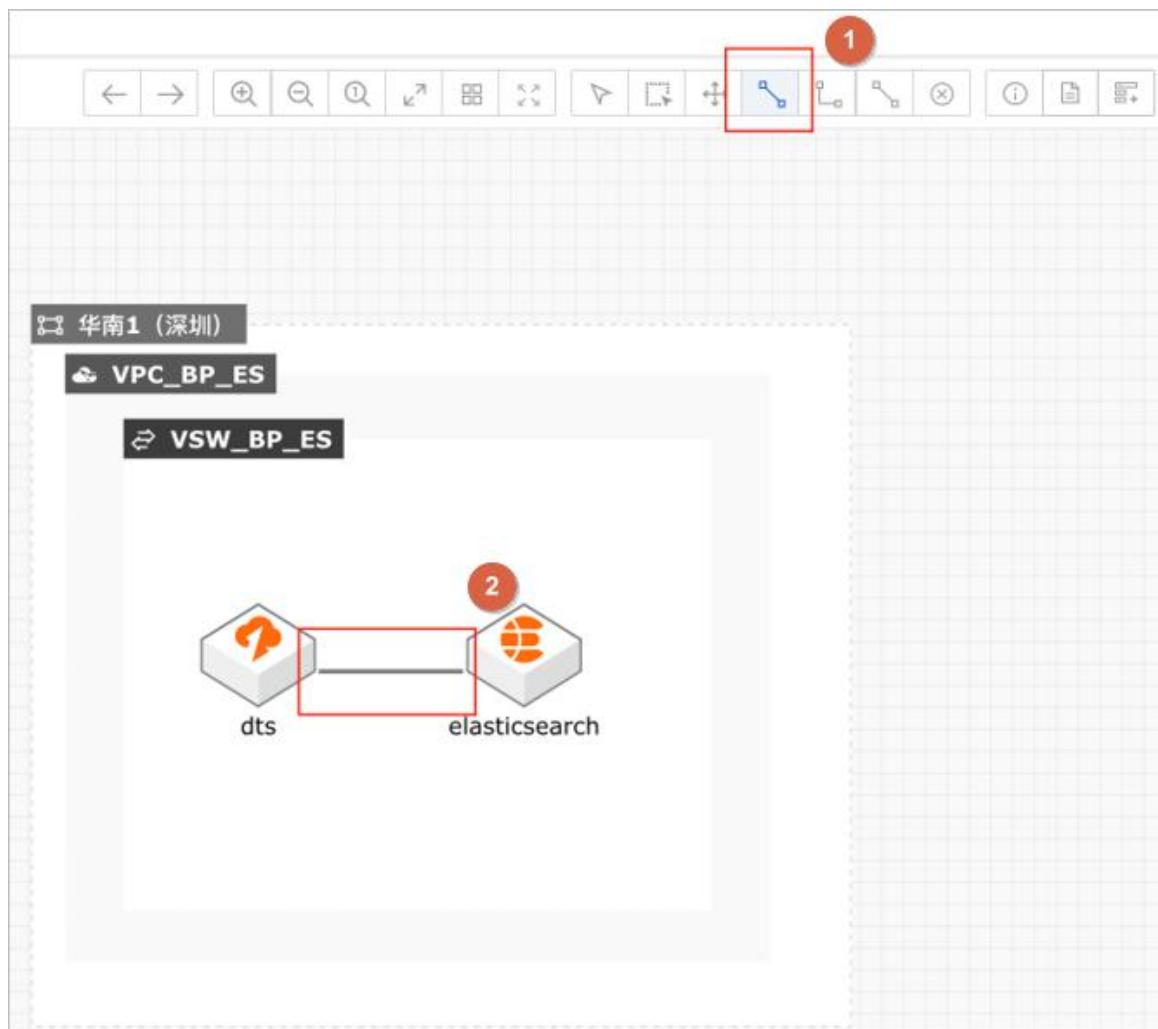
步骤 6 在左侧搜索框中输入 DTS，选定数据传输服务，拖动到图中，并配置相关参数。



步骤 7 双击 DTS 图标，配置 DTS 参数。



步骤 8 单击**创建连线**按钮，切换到连线模式，将 DTS 和 elasticsearch 连接起来，后续通过在 DTS 实例中配置相关数据源即可将其他数据导入到 elasticsearch 中。

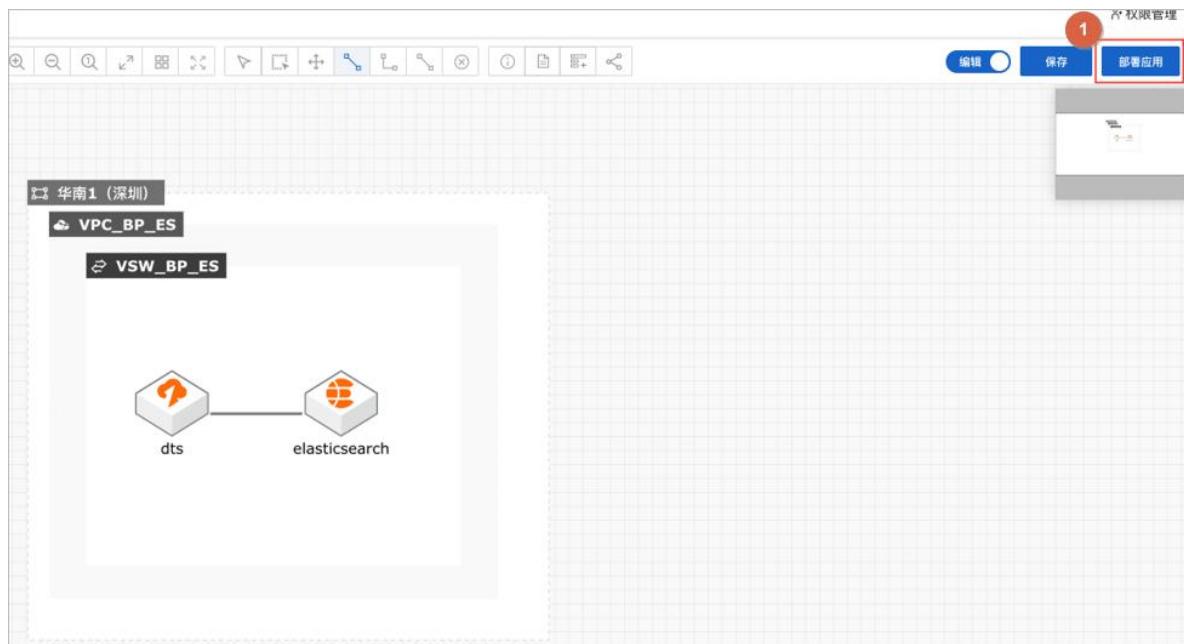


步骤 9 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写应用名称，并单击**确认**。



### 4.1.3. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、dts 和 elastic search 是否有库存等，一般需要几十秒左右。

等待校验成功，单击**下一步：价格清单**。

资源验证						
资源名称	资源类型	区域	规格	结果	备注	操作
VSW_BP_ES	vswitch	深圳	192.168.0.0/24	成功	校验通过	定位
dts	dts		data_synchronou s	成功	校验通过	定位
elasticsearch	elasticsearch	深圳	6.7	成功	校验通过	定位
VPC_BP_ES	vpc	深圳	192.168.0.0/16	成功	校验通过	定位

状态:计价成功

**下一步：价格清单**   **返回**

步骤 3 在**导出价格清单**页面会拉取应用所有配置的价格信息。



步骤 4 可以单击**查看报告**, 查看应用的价格信息。



步骤 5 单击下一步：确认订单。



步骤 6 在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

**确认订单**

免费 按量付费

资源名称	资源类型	区域	规格	数量	原价	实付	状态
dts	dts		data_synchronous	1	2.48元/时	[redacted] 元/时	新购
elasticsearch	elasticsearch	深圳	6.7	1	5.09元/时	[redacted] 元/时	新购

《云速搭服务条款》

部署前，请阅读并勾选服务条款

按量付费: [redacted] 元/时

状态: 计价成功

2

上一步: 价格清单 下一步: 支付并创建

步骤 7 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

#### 注意：

1. 部署流程一旦开始后，无法取消。
2. Elasticsearch 的部署时间比较长（预计 60 分钟，默认是小时级别），请耐心等待。

The screenshot shows the 'Resource Deployment Status' interface. At the top, there are search and filter fields for 'Resource Name', 'Resource Type', 'Billing Type', and 'Resource ID'. Below these is a progress bar with three dots indicating the deployment status. A tooltip message reads: '部署中, 不要进行任何操作, 请耐心等待...' (Deployment in progress, no operations are allowed, please wait patiently...). The main content area is titled 'Deployment Summary' and shows the deployment status as 'Deploying' and the scheme number as 'CH8GVH081PRB6IJ0'. There is a 'Return' button at the bottom right.

步骤 8 部署完成后，如下图所示。

The screenshot shows the 'Resource Deployment Status' interface after deployment completion. The table lists four resources: 'dts', 'VPC\_BP\_ES', 'VSW\_BP\_ES', and 'elasticsearch'. Each row includes columns for resource name, type, billing type, ID, status, update time, and location. All resources are shown as 'Running' (运行中). The deployment status is now 'Deployment successful' (部署成功) and the scheme number is 'CH8GVH081PRB6IJ0'. The order number is '211329658180425211329557800425'. There are 'View Report' and 'Return' buttons at the bottom right.

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
dts	dts	按量付费	dtslby10ni929rib1r	运行中	2021-10-29 14:22:58	<a href="#">定位</a>
VPC_BP_ES	vpc	-	vpc-wz9l3926c255nib38fj6j	运行中	2021-10-29 14:22:59	<a href="#">定位</a>
VSW_BP_ES	vswitch	-	vsw-wz95xxf4duxk96fuudx2x	运行中	2021-10-29 14:23:52	<a href="#">定位</a>
elasticsearch	elasticsearch	-	es-cn-i7m2ewvyt003xighz	运行中	2021-10-29 15:15:51	<a href="#">定位</a>

步骤 9 单击查看报告，可以查看本次的部署报告。



步骤 10 单击返回，然后打开资源清单。

**资源部署状态**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
dts	dts	按量付费	dtsliby10ni929rib1r	运行中	2021-10-29 14:22:58	定位
VPC_BP_ES	vpc	-	vpc-wz9l3926c255nib38fj6j	运行中	2021-10-29 14:22:59	定位
VSW_BP_ES	vswitch	-	vsw-wz95xxf4duxk96fuudx2x	运行中	2021-10-29 14:23:52	定位
elasticsearch	elasticsearch	-	es-cn-i7m2ewvyt003xighz	运行中	2021-10-29 15:15:51	定位

**部署概要**

状态：部署成功  
订单编号：211329658180425211329557800425  
方案编号：CH8GVH081PRB6IJ0

[查看报告](#) [返回](#)



这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。

步骤 11 单击资源名称 **elasticsearch**，可跳转到对应的控制台。

This screenshot shows the detailed configuration page for an Elasticsearch instance named 'es-cn-i7m2ewvyt003xighz'. The left sidebar contains navigation links for basic information, configuration management, ES cluster configuration, plugin configuration, security configuration, data backup, visualization control, monitoring and logs, cluster monitoring, log queries, intelligent monitoring, cluster overview, health diagnosis, and history reports. The main content area is divided into sections: '基本信息' (Basic Information), '运行状态' (Operational Status), and '节点可视化' (Node Visualization). In the '基本信息' section, it shows the instance ID, version (6.7.0), location (Guangzhou), and various network and port settings. The '运行状态' section displays the status as '正常' (Normal) and provides creation time and maintenance time information. The '节点可视化' section shows a green circular node icon.

此外，本实践创建的 DTS，可以将其他数据库的海量数据同步到 elasticsearch 中，充分发挥 elasticsearch 对海量数据快速查询的能力。

步骤 12 配置 elasticsearch。

可参考 <https://bp.aliyun.com/detail/71> 中第 3 章的“数据同步及搜索”，这里演示了如何通过 DTS 将其他数据同步到 elasticsearch 中数据分析。

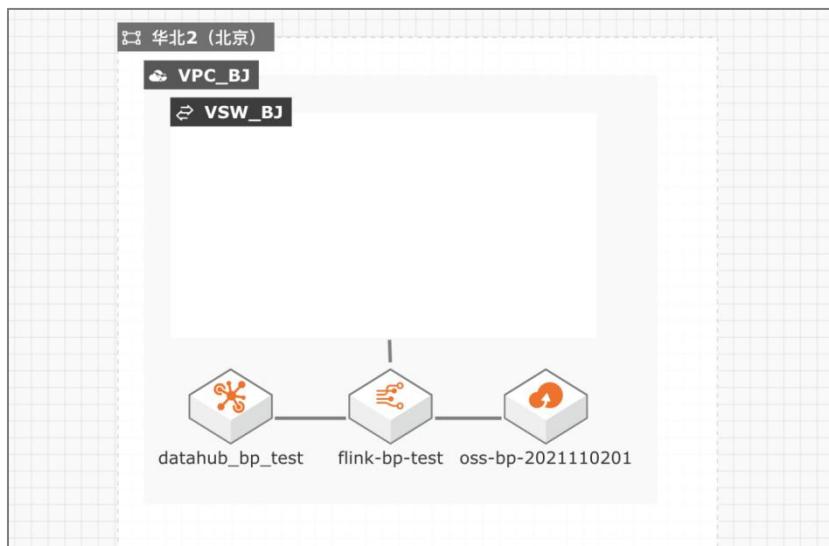
## 4.2. 云速搭部署 Flink 应用

作者 | 阿里云解决方案架构师 袁影

### 4.2.1. 云速搭架构设计入门

#### 方案架构

通过云速搭实现一个 DataHub+Flink 的实时流计算引擎架构，利用 DataHub 收集原始数据，推送到 Flink 进行基于流式数据的分析和应用。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
Flink	VSW
DataHub	Region
OSS	Region

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

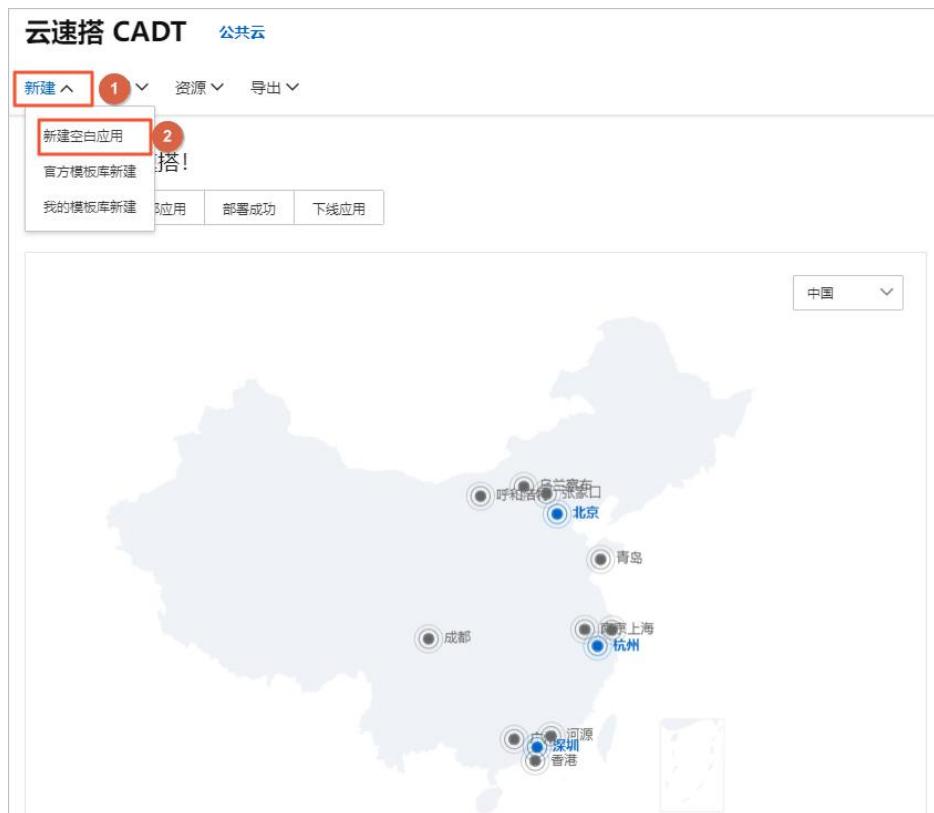
资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC_BJ	192.168.0.0/16
AZ	华北 2 可用区 F	192.168.0.0/24

### 4.2.2. 应用架构设计

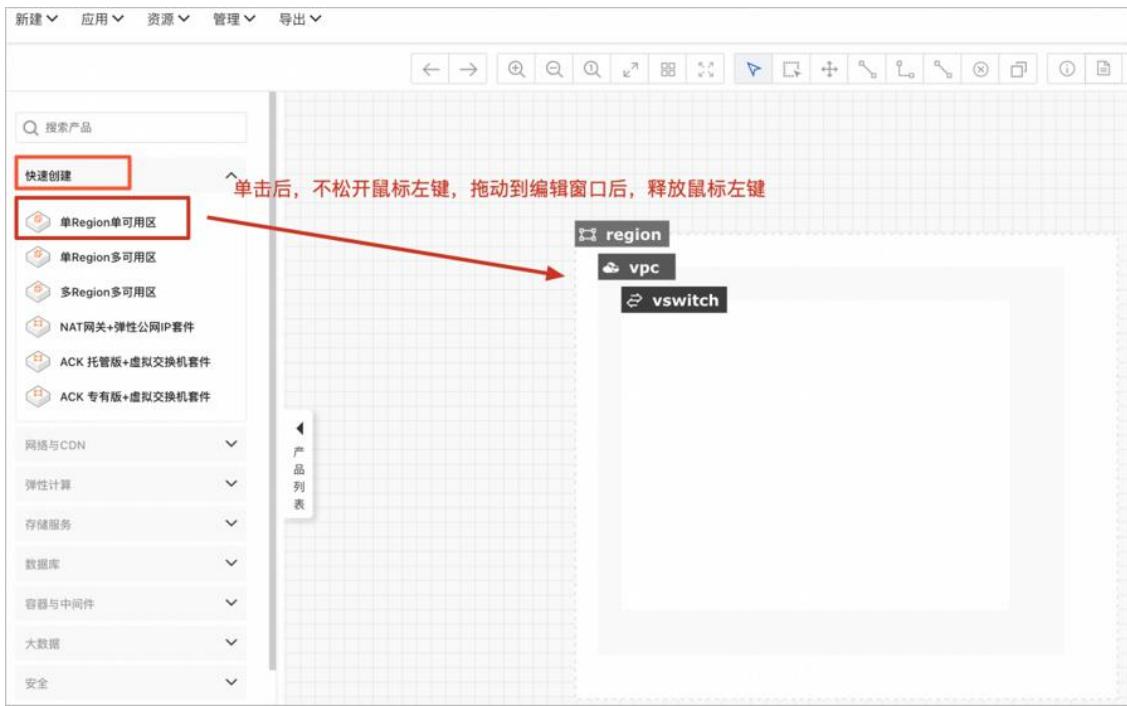
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

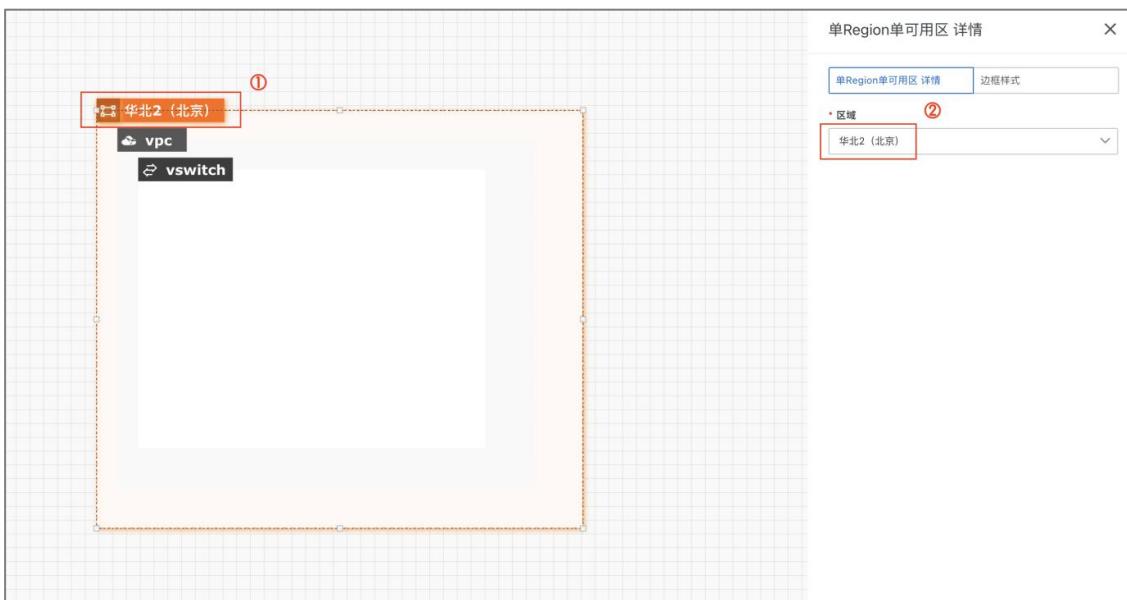


步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。



步骤4 依次双击 Region、VPC、vswitch 进行配置。

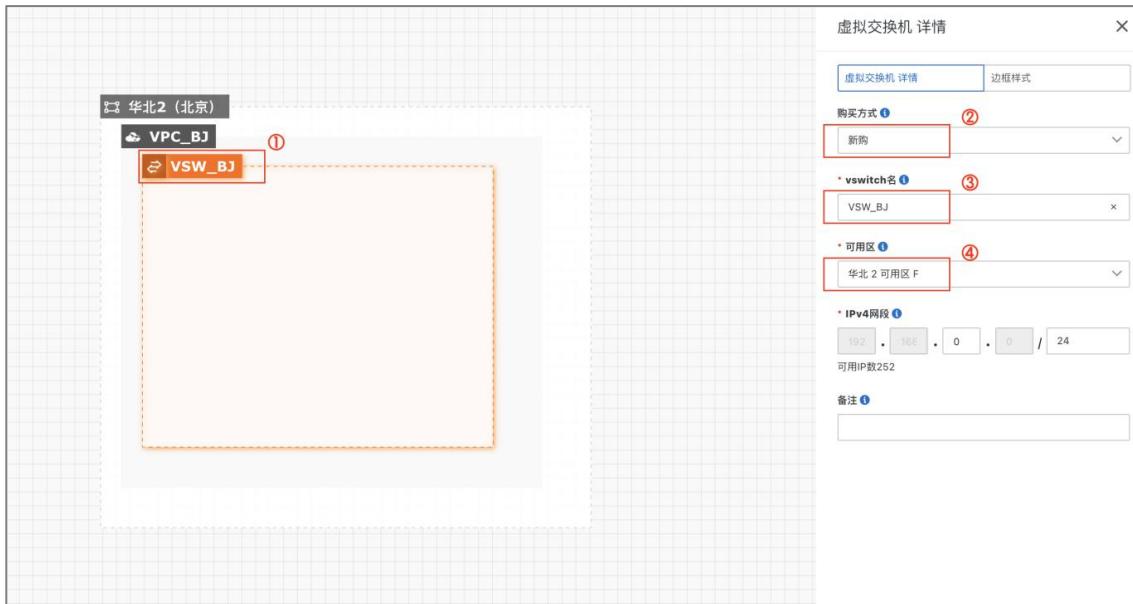
1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



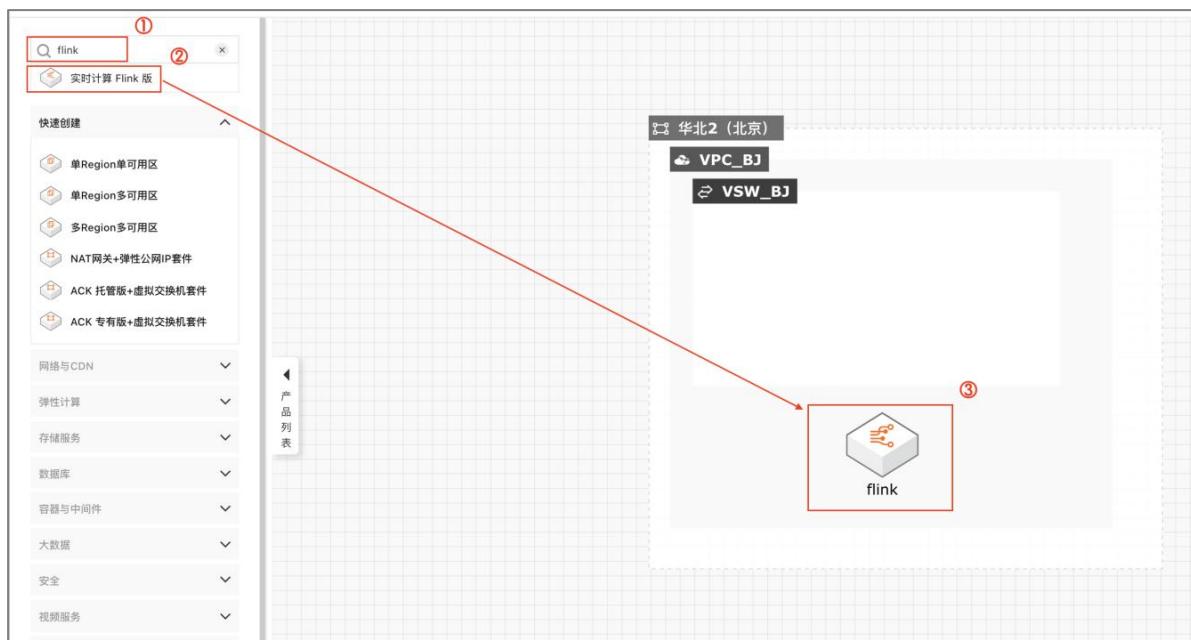
2. 双击 VPC，配置 VPC 参数。



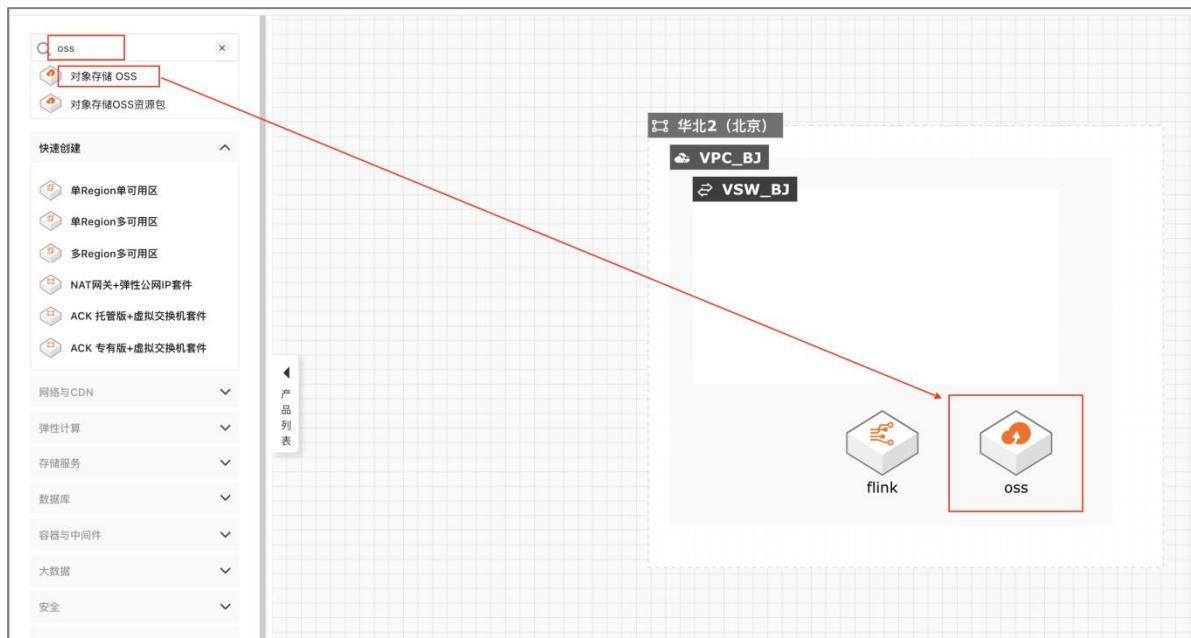
3. 双击 vswitch，配置 vswitch 参数，可用区选择：华北 2 可用区 F。



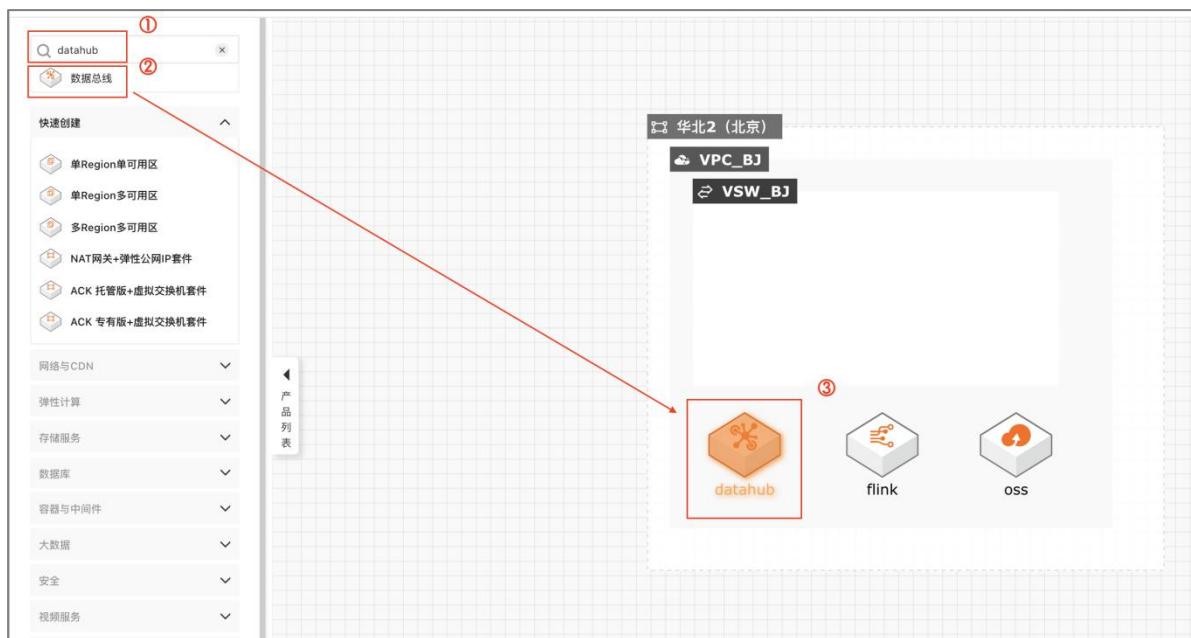
步骤 5 在左侧搜索框中输入 flink，选定 flink 图元，拖动到 vswitch 下方。



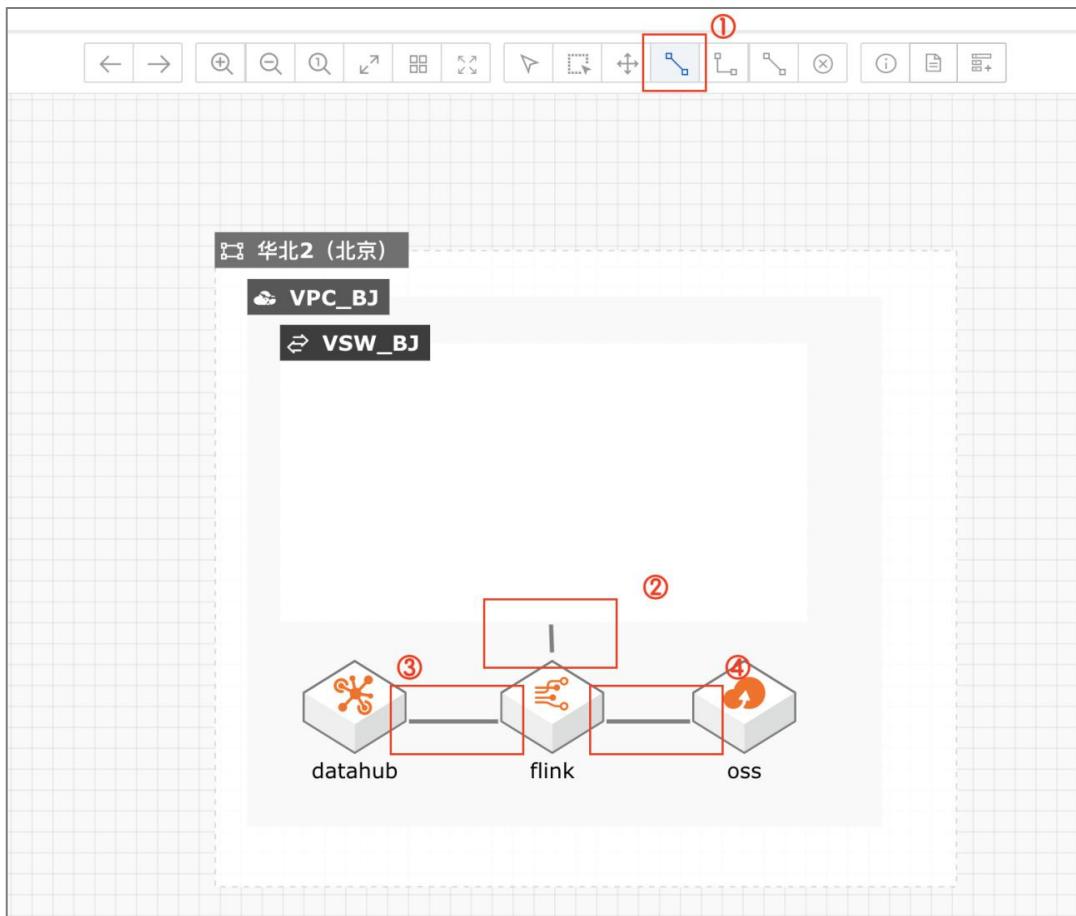
步骤 6 在左侧搜索框中输入 oss，选定**对象存储 OSS**，拖动到图中。



步骤 7 在左侧搜索框中输入 datahub，选定**数据总线**，拖动到图中。

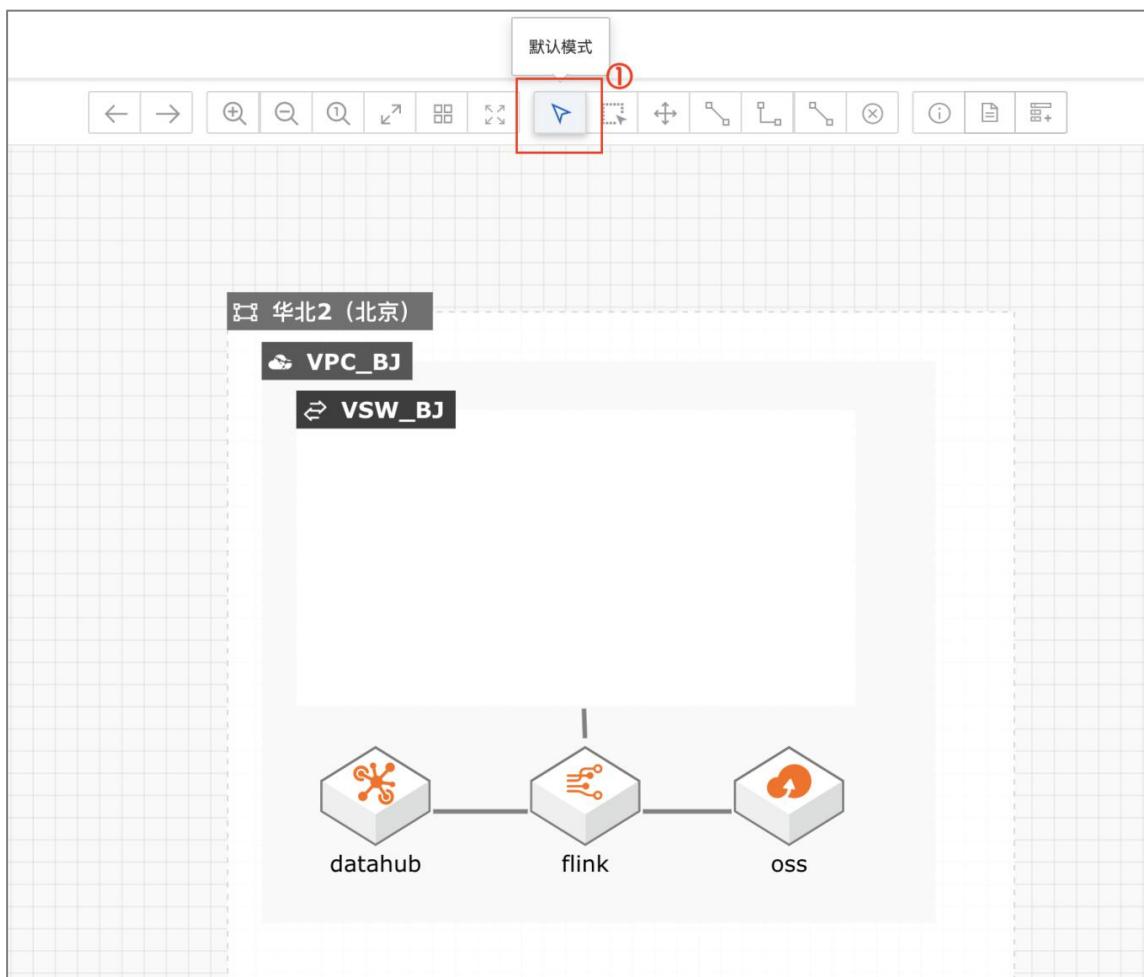


步骤 8 单击**创建连线**按钮，切换到连线模式，依次将 flink 和 VSW\_BJ 连接、将 datahub 与 flink 连接、将 flink 与 oss 连接。



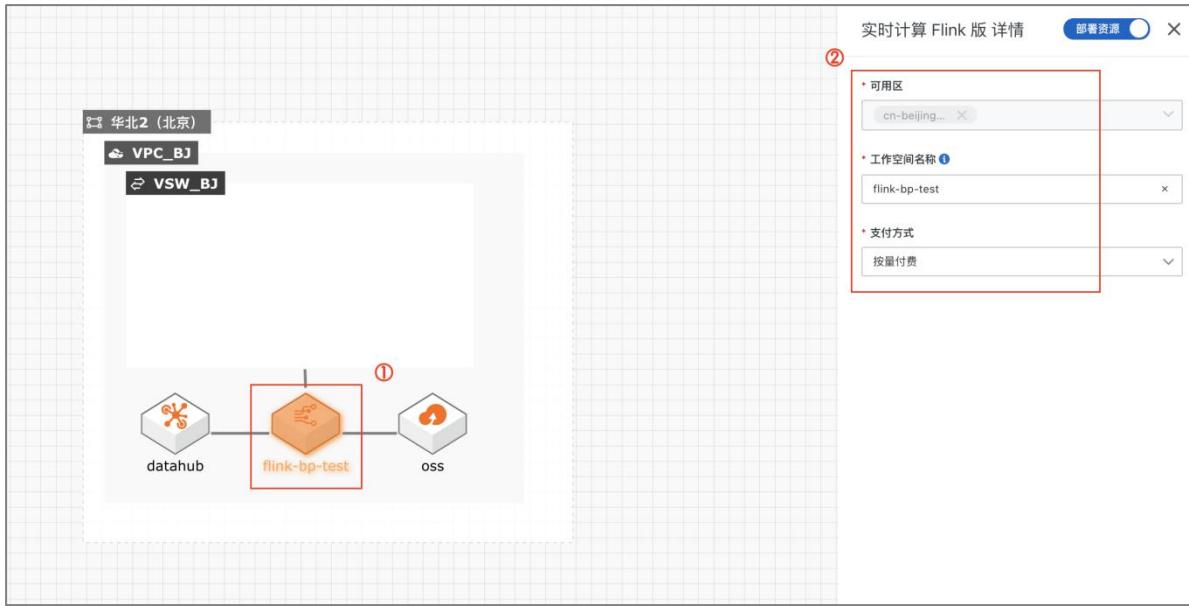
### 4.2.3.配置资源参数

步骤 1 切换回默认模式。



步骤 2 双击 flink 图标，参考下表进行参数配置。

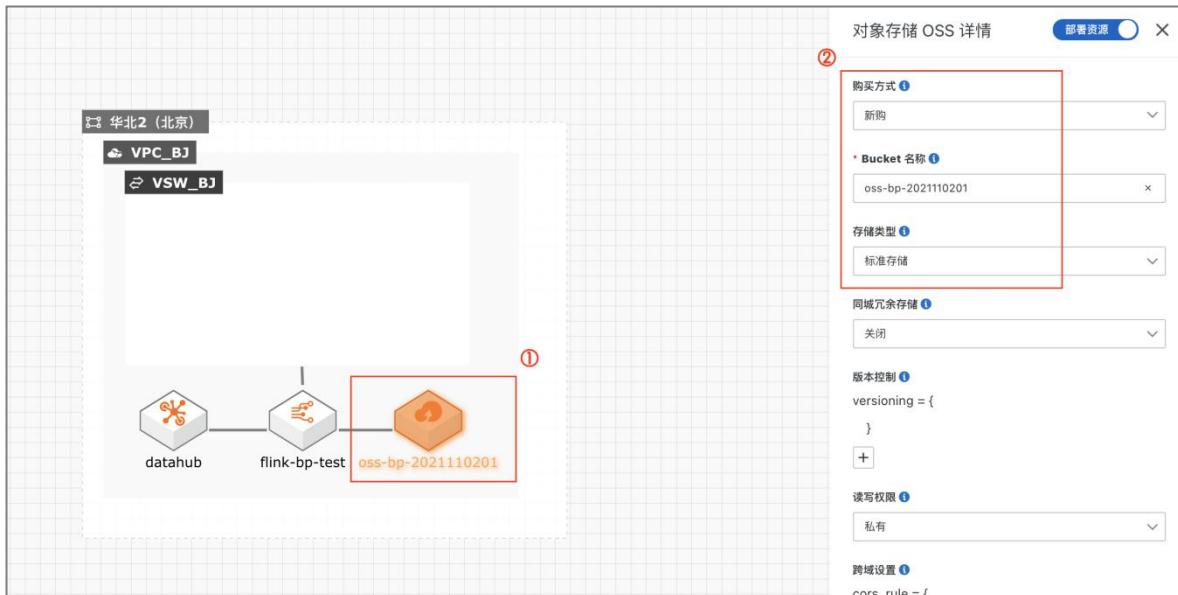
配置项	参数说明
可用区	因为创建了与 vswitch 的接线，已自动绑定，无需修改
工作空间名称	flink-bp-test
支付方式	按量付费



步骤3 双击 oss 图标，参考下表进行参数配置。

注意：oss 的项目名称需要保持阿里云全局唯一，请修改成其他名称。

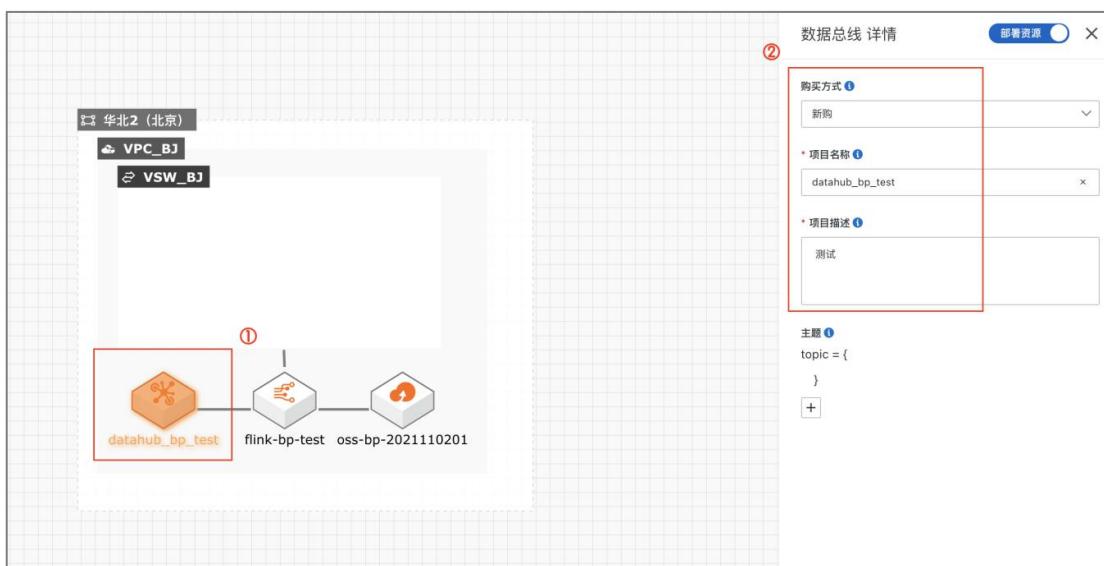
配置项	参数说明
购买方式	新购
项目名称	oss-bp-2021110201
存储类型	标准存储



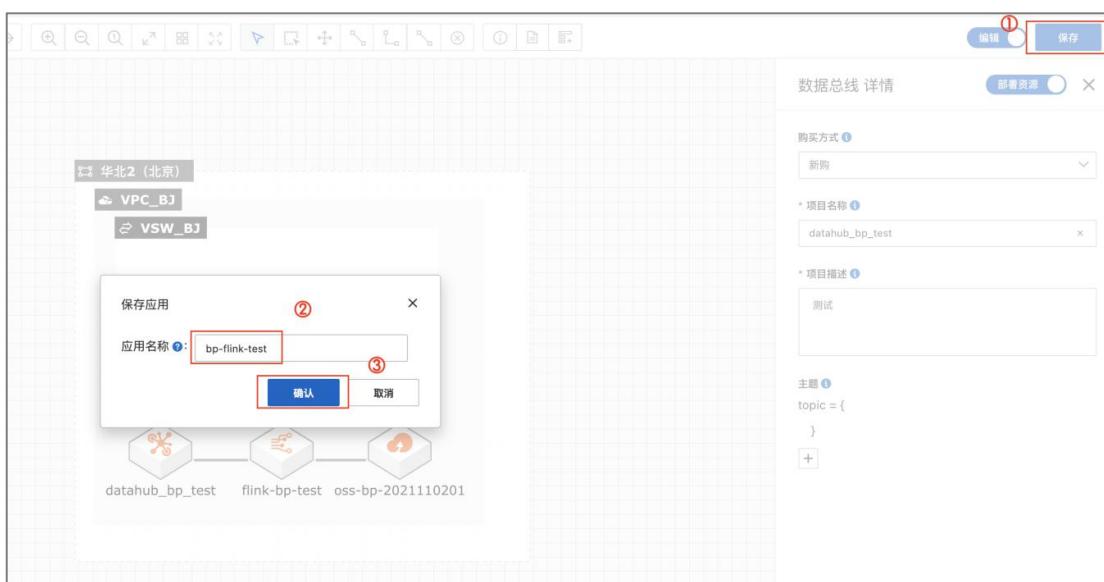
步骤4 双击 datahub 图标，参考下表进行参数配置。

配置项	参数说明
购买方式	新购
项目名称	datahub_bp_test
项目描述	测试

注意：datahub 的项目名称需要保持账号内唯一。

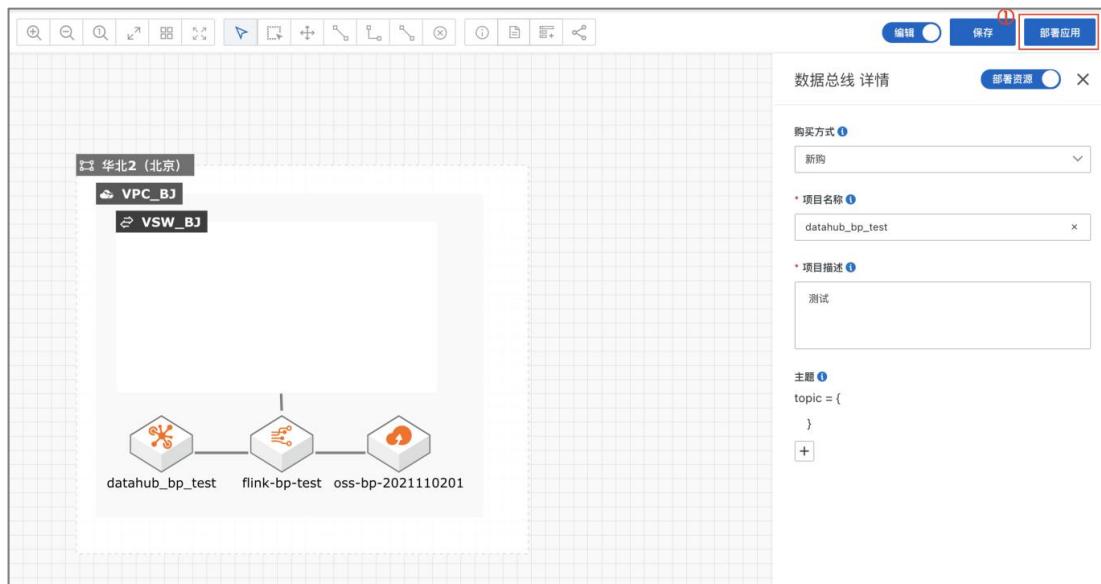


步骤5 完成以上资源配置后，单击保存，并设置应用名称，最后单击确认。



## 4.2.4. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、datahub 和 flink、oss 是否有库存等，一般需要几十秒左右。

等待校验成功，单击**下一步：价格清单**。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	flink-bp-test	实时计算 Flink 版	北京		成功	校验通过	定位
2	VSW_BJ	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
3	VPC_BJ	vpc	北京	192.168.0.0/16	成功	校验通过	定位
4	datahub_bp_te st	datahub	北京		成功	校验通过	定位
5	oss-bp-202111 0201	oss	北京	Standard	成功	校验通过	定位

状态:校验成功

① **下一步：价格清单** 返回

步骤 3 在导出价格清单页面，会拉取应用所有配置的价格信息，可以单击**查看报告**，查看应用的价格信息。

导出价格清单

免费 按量付费

资源成本占比

资源预算  
● 大数据 大数据: 元/时

100%

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	datahub_bp_test	datahub	北京		1				定位
2	flink-bp-test	实时计算 Flink 版	北京		1	0.01元/时	省  元/时	元/时	定位

状态: 计价成功

① 上一步: 资源校验 查看报告 下一步: 确认订单



步骤 4 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

**确认订单**

免费	包年包月	按量付费						
序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	flink-bp-test	实时计算 Flink 版	北京		1	■■■元/时	■■■元/时	新购
2	datahub_bp_test	datahub	北京		1			新购

①  《云速搭服务条款》  
部署前，请阅读并勾选服务条款

按量付费: ■■■元/月  
②

状态: 计价成功

上一步: 价格清单    下一步: 支付并创建

步骤 5 单击**下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**

1. 部署流程一旦开始后，无法取消。
2. 部署时间预计 5~10 分钟左右，请耐心等待。

**资源部署状态**

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位

部署中，不要进行任何操作，请耐心等待...

**部署概要**

状态: 部署中      方案编号: X8HZVP3FBS6YN8FT

返回

步骤 6 部署完成后，如下图所示。

**资源部署状态**

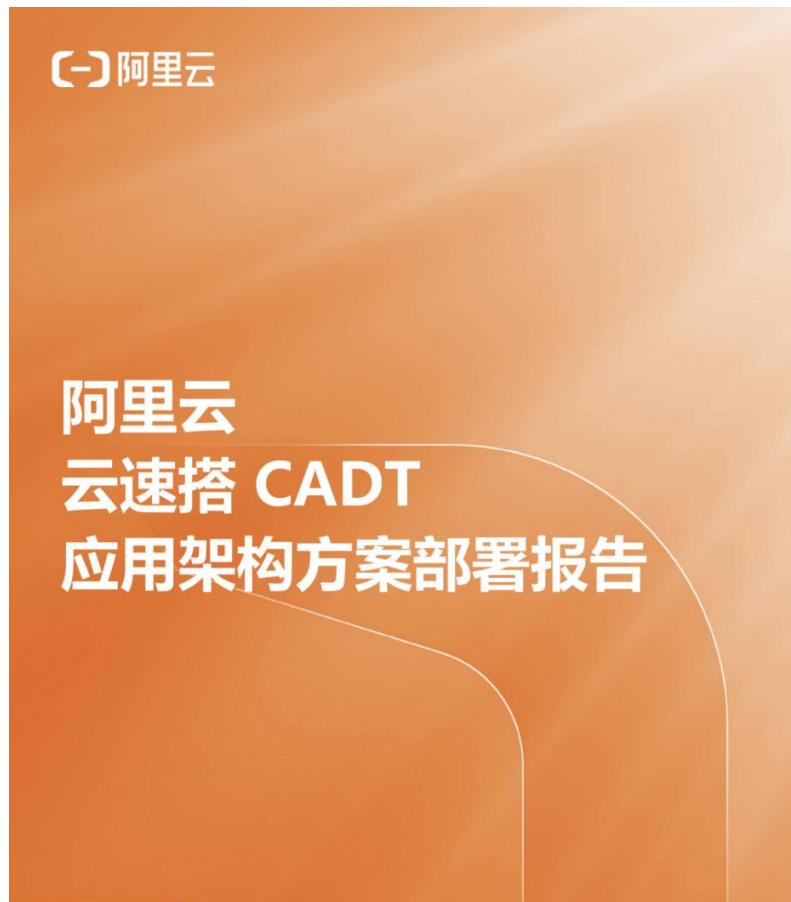
序号	资源名称 <a href="#">?</a> <a href="#">Q</a>	资源类型 <a href="#">Q</a>	付费类型	资源ID <a href="#">Q</a>	资源状态	资源更新时间	定位
1	VPC_BJ	vpc	-	vpc-2ze0iiipxblpnb0j7yglw <a href="#">Q</a>	运行中	2021-11-03 13:30:29	<a href="#">定位</a>
2	datahub_bp_test	datahub	按量付费	datahub_bp_test <a href="#">Q</a>	运行中	2021-11-03 13:30:04	<a href="#">定位</a>
3	oss-bp-2021110201	oss	按量付费	oss-bp-2021110201 <a href="#">Q</a>	运行中	2021-11-03 13:30:04	<a href="#">定位</a>
4	VSW_BJ	vswitch	-	vsw-2zefch4pu4zjwjnjft1j <a href="#">Q</a>	运行中	2021-11-03 13:31:12	<a href="#">定位</a>
5	flink-bp-test	实时计算 Flink	-	sc_flinkserverlesspost_public_cn-2r4 <a href="#">Q</a>	运行中	2021-11-03 13:34:58	<a href="#">定位</a>

**部署概要**

状态: 部署成功 订单编号 : 211380722610425  
方案编号: X8HZVP3FBS6YN8FT

[查看报告](#) [返回](#)

步骤 7 单击[查看报告](#), 可以查看本次的部署报告。



步骤 8 单击返回，然后单击资源清单。

The screenshot shows the Cloud Speed Deployment interface for the 'bp-flink-test' project. At the top, there's a toolbar with various icons. Below it is a navigation bar with tabs like '华北2 (北京)', 'VPC\_BJ', and 'VSW\_BJ'. A main panel displays three resources: 'datahub\_bp\_test', 'flink-bp-test', and 'oss-bp-2021110201', connected by arrows. Below this is a 'Resource List' section with a table:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC_BJ	vpc	-	vpc-2ze0ilipxbjpnbl07yglw	新建	运行中	2021-11-03 13:30:29	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
2	datahub_bp_test	datahub	按量付费	datahub_bp_test	新建	运行中	2021-11-03 13:30:04	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
3	oss-bp-2021110201	oss	按量付费	oss-bp-2021110201	新建	运行中	2021-11-03 13:30:04	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。

步骤 9 单击资源名称 **flink-bp-test**，可跳转到对应的控制台。

The screenshot shows the Cloud Speed Deployment interface for the 'bp-flink-test' project. The 'flink-bp-test' resource is highlighted with a red box and a circled '1' above it. The rest of the interface is identical to the previous screenshot, including the navigation bar, top-level resources tree, and resource list table.

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
1	VPC_BJ	vpc	-	vpc-2ze0ilipxbjpnbl07yglw	新建	运行中
2	datahub_bp_test	datahub	按量付费	datahub_bp_test	新建	运行中
3	oss-bp-2021110201	oss	按量付费	oss-bp-2021110201	新建	运行中
4	VSW_BJ	vswitch	-	vsw-2ze0ch4pu4zjwjqnftl	新建	运行中
5	flink-bp-test	实时计算 Flink 版	-	sc_flinkserverlesspost_public_cn-2r42f62va02	新建	运行中

Flink 全托管

工作空间 / 订单实例 ID	工作空间状态	已使用 / 已购买 CU	付费类型	时间	操作
flink-bp-test sc_flinkserverlesspost_public_cn-2r...	运行中	0.00 / -	按量付费	创建时间: 2021-11-03 13:30 到期时间: -	控制台   其他

此外，本实践创建的 datahub，可以将海量数据同步到实时流计算引擎 flink 中，并进行相关的作业开发。

#### 步骤 10 开发配置 Flink

可参考 <https://bp.aliyun.com/detail/155> 中第 4 章的“实时数仓搭建”。

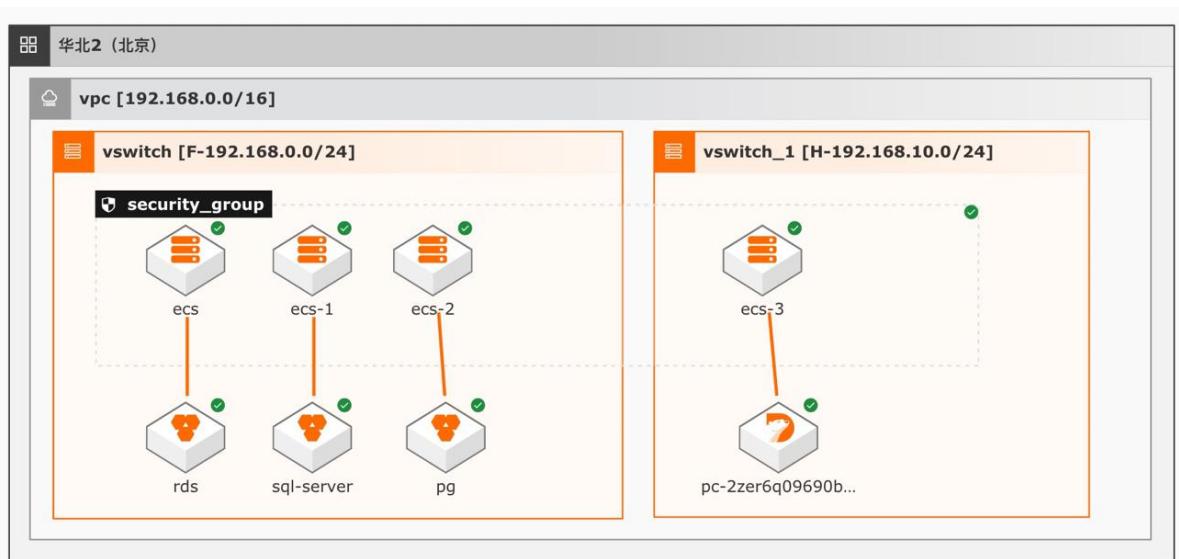
## 4.3. 云速搭部署云数据库 RDS

作者 | 阿里云解决方案架构师 嘉辽

### 4.3.1. 云速搭架构设计入门

#### 方案架构

通过云速搭设计一个 ECS+RDS 的通用架构：



#### 理解资源级别

每个阿里云资源都有对应的资源级别，在 CADT 进行架构设计时要遵循资源级别开展。

本架构中使用的资源及对应的资源级别如下表所示，在进行架构设计时需要用到。

云资源	资源级别
RDS	VSW
PolarDB	VSW
ECS	VSW
安全组	VPC

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc	192.168.0.0/16
AZ	北京 H 可用区	192.168.0.0/24
AZ	北京 H 可用区	192.168.10.0/24
安全组	sg-bj	-

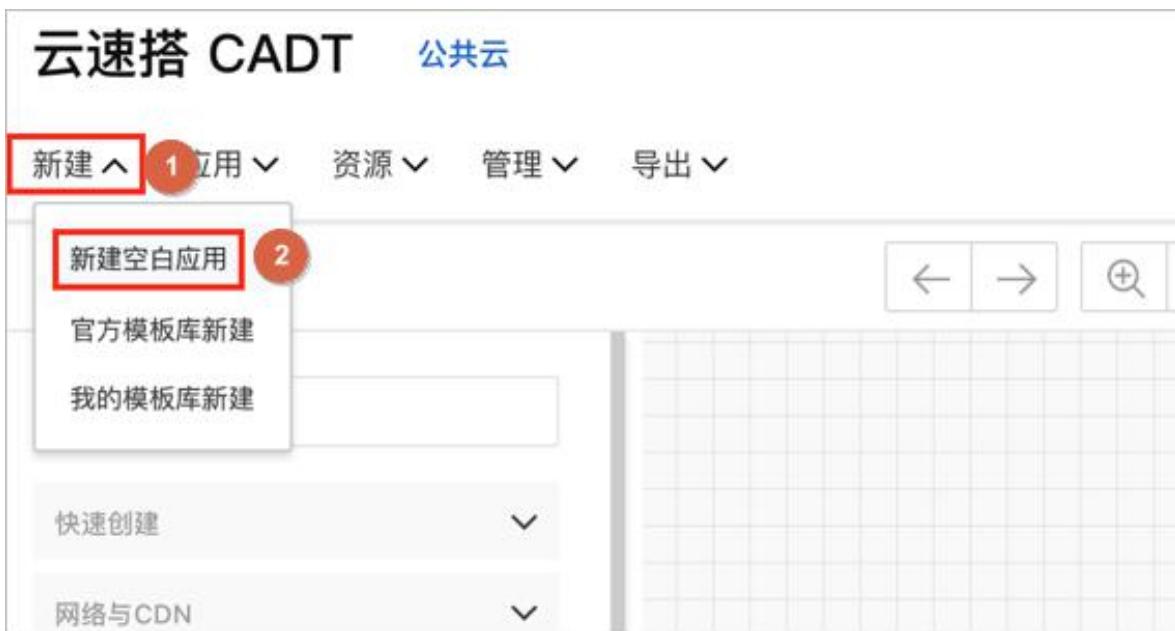
### 4.3.2.设计应用架构

步骤 1 登录 <https://bpstudio.console.aliyun.com/>，访问云速搭 CADT。

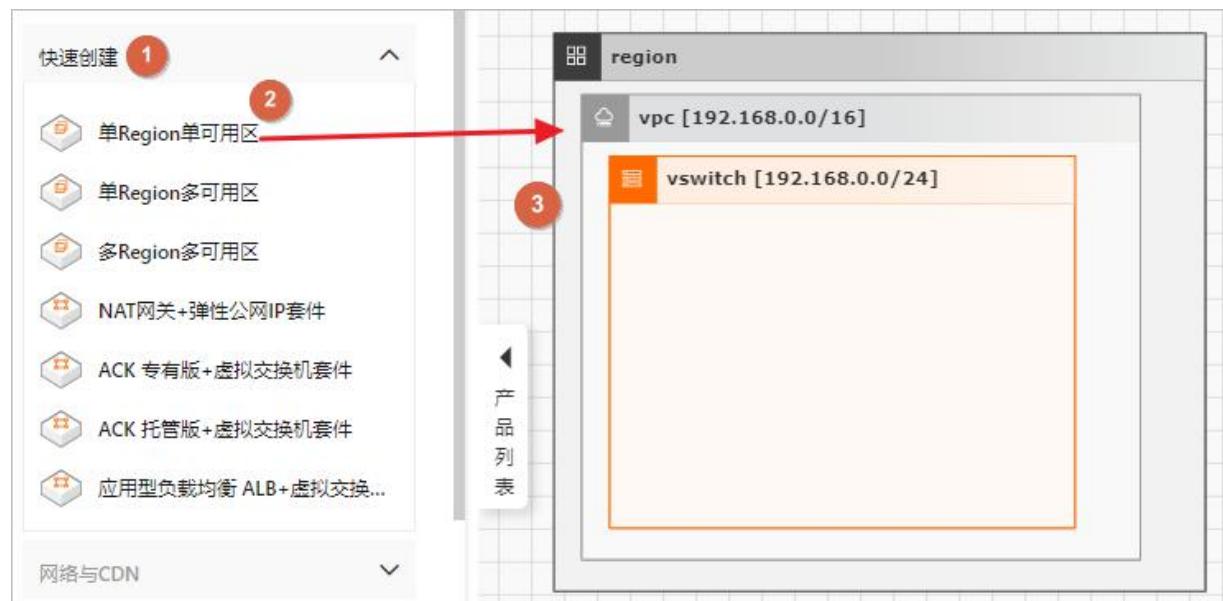
**说明：**如果提示需要开通服务，请根据提示进行开通。



步骤 2 在菜单栏单击新建 > 新建空白应用，打开一个空白画布。



步骤 3 从左侧工具栏**快速创建**下选择合适的网络拓扑类型，本场景适用**单 Region 单可用区**，单击选中并拖拽到右侧空白画布中。

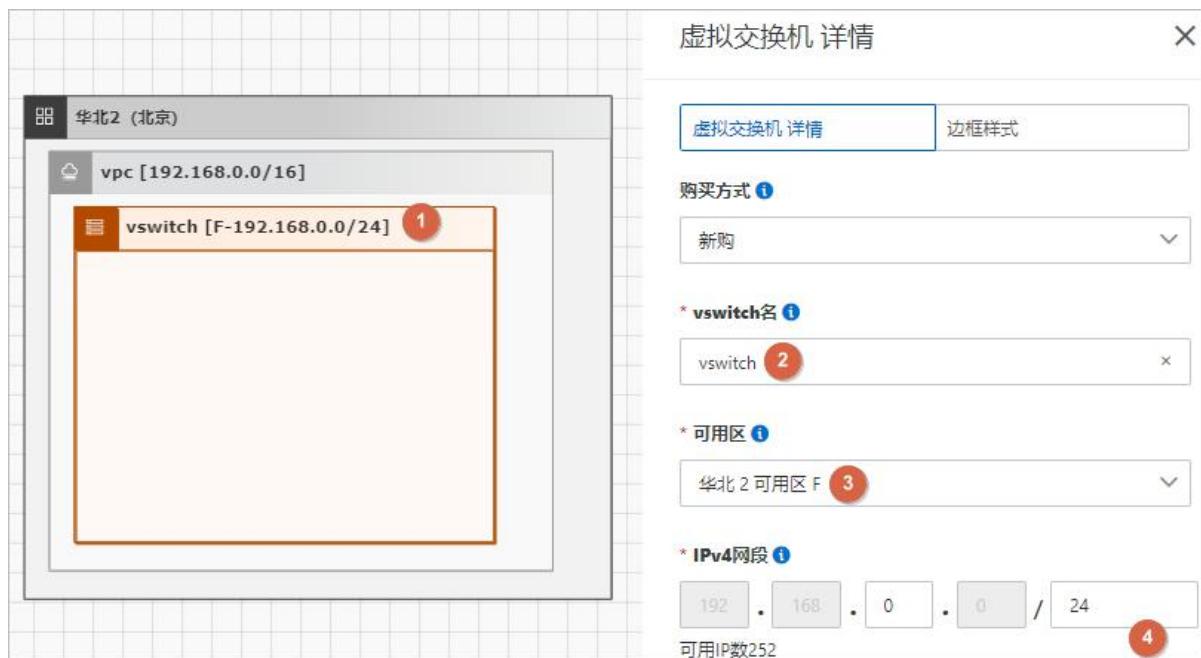


步骤 4 依次双击 Region、vpc、vswitch 进行配置。

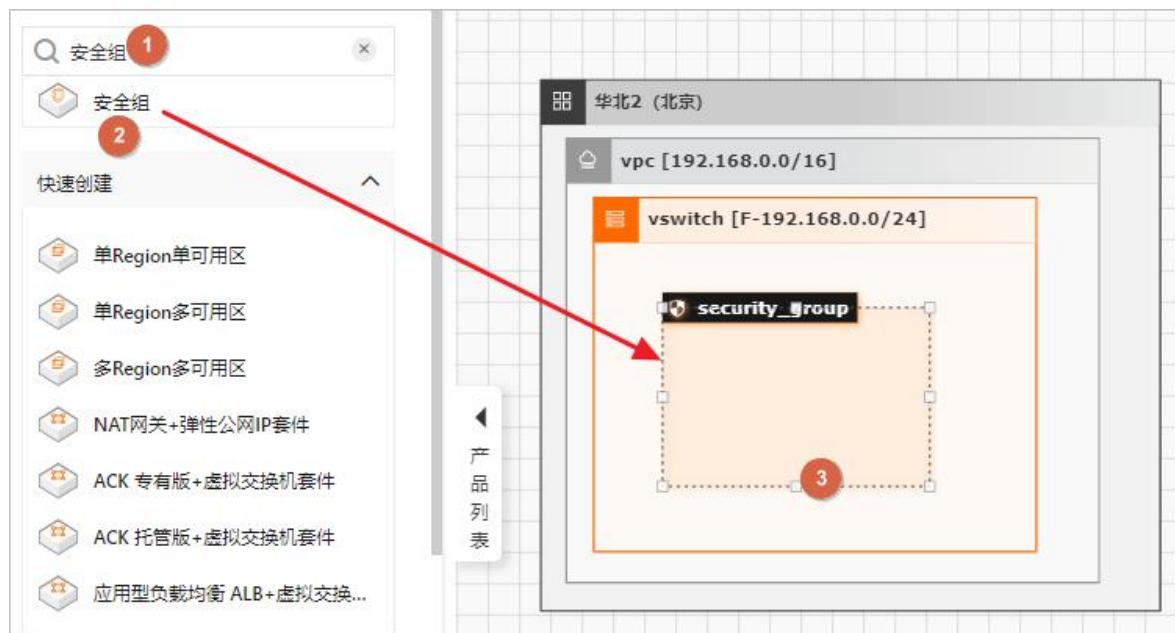
1. 双击 **Region**，出现右边提示窗，在区域下拉菜单中选择**华北 2（北京）**



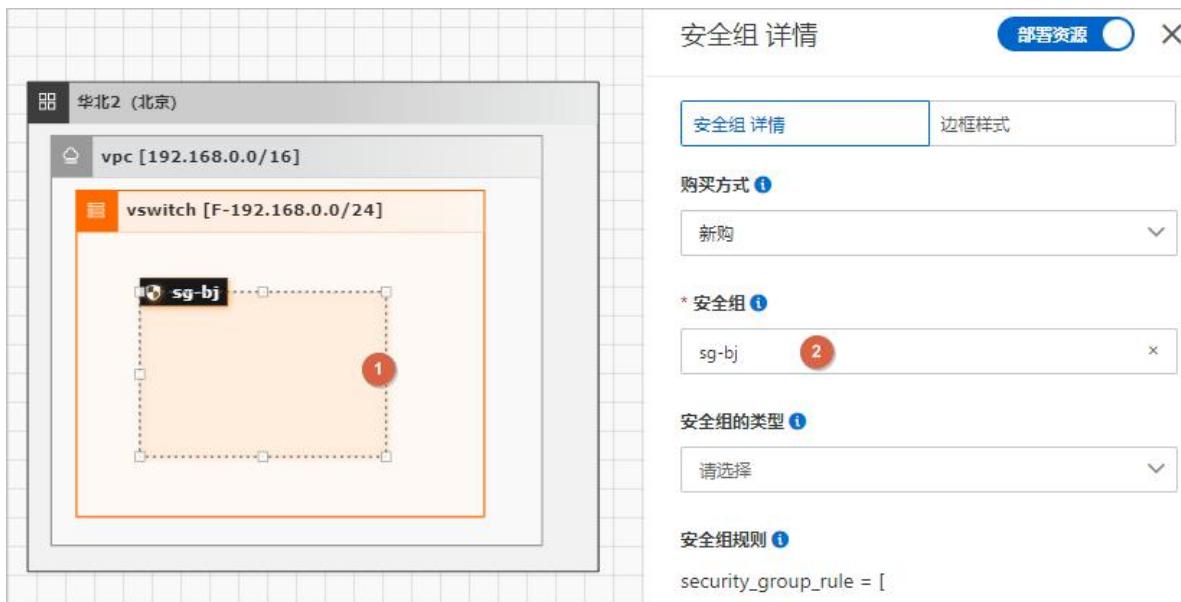
2. 双击 VPC 保持默认配置即可。
3. 双击 **vswitch**, 在右边提示窗的 vswitch 选项中输入 **vswitch**, 可用区选择北京可用区 F



步骤 5 在左侧搜索框输入资源名称**安全组**, 选中安全组图标, 拖动至 VPC 中。



步骤 6 双击安全组，对安全组重命名，其余保持默认配置即可。



### 4.3.3. MySQL 部署

步骤 1 在左侧搜索框输入资源名称 ecs，选中 ecs 图标，拖动 ecs 图标至 vswitch 中，注意同时也要放在安全组中。（ecs 属于 vswitch 资源级别，因此放在 vswitch 中。）



步骤 2 双击 ECS 图标，进行参数配置

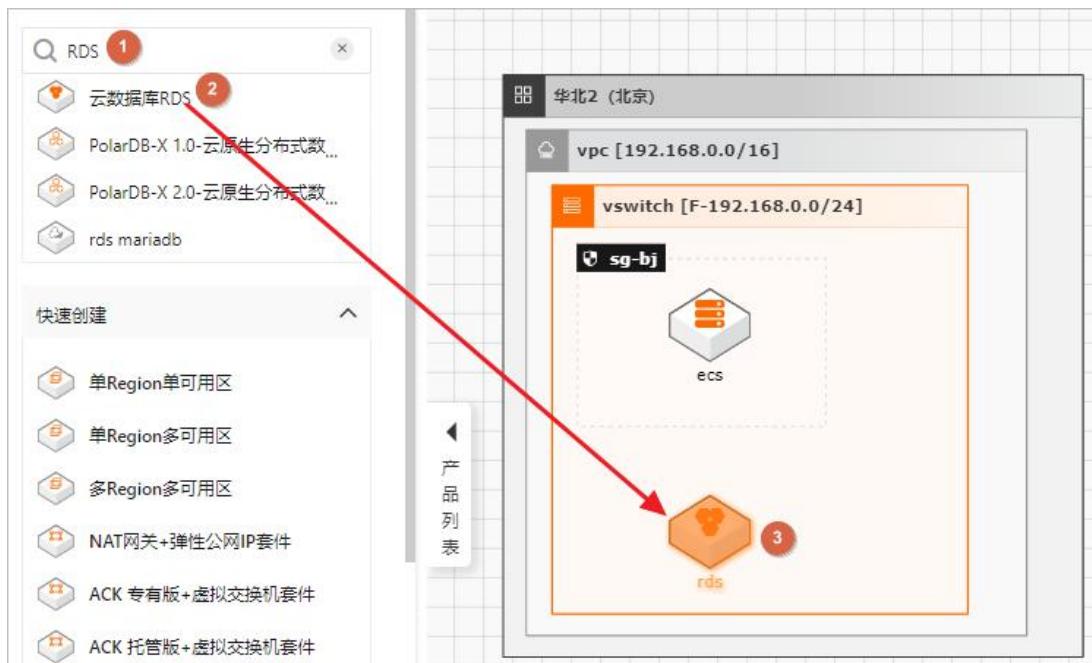
配置项	参数说明
购买方式	新购
可用区	自动填充当前 ecs 所在的 vswitch，无需修改
实例名称	ecs
数量	1
支付方式	按量付费
实例规格	ecs.n4.large(2c 4g)，支持关键字搜索
操作系统	Alibaba Cloud Linux 3.2104 64 位
系统盘类型	高效云盘
系统盘容量	40G
主机名	ecs
登录凭证	选择 <b>自定义密码</b> ，需要连续两次输入密码。



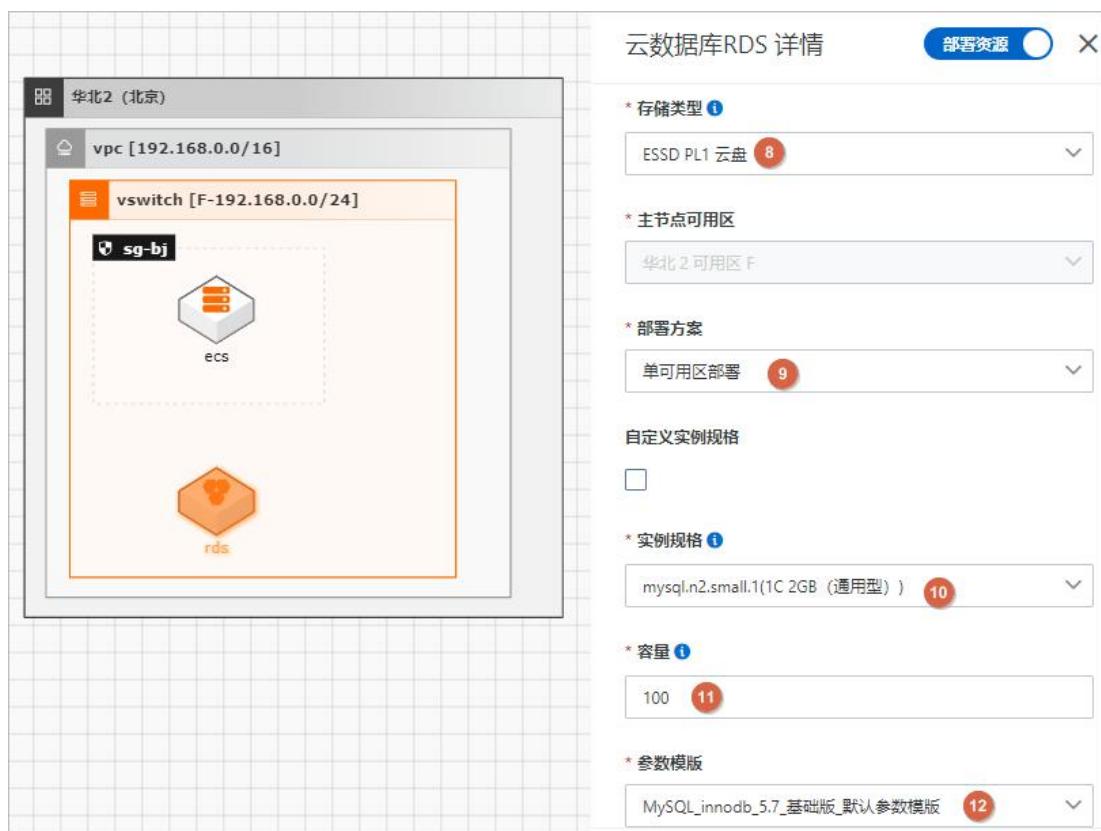
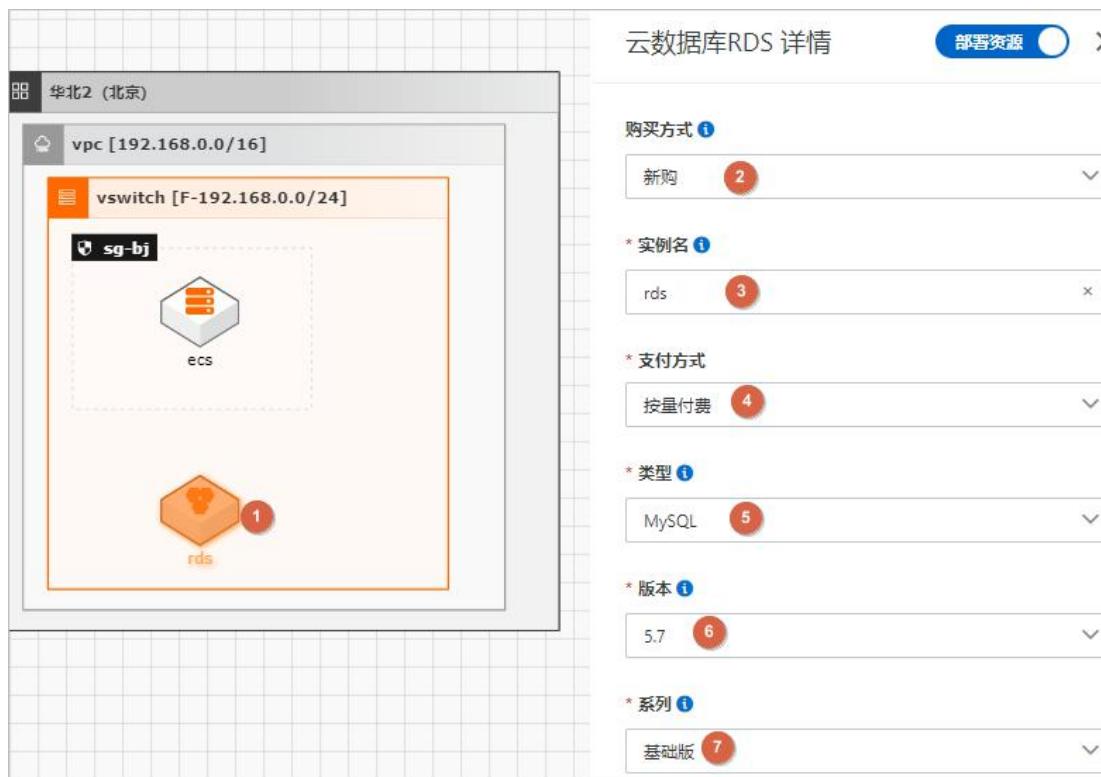


**注意：**标注\*是必填项，参数较多，需要将进度条拖动到最下面，完成必填参数的配置。

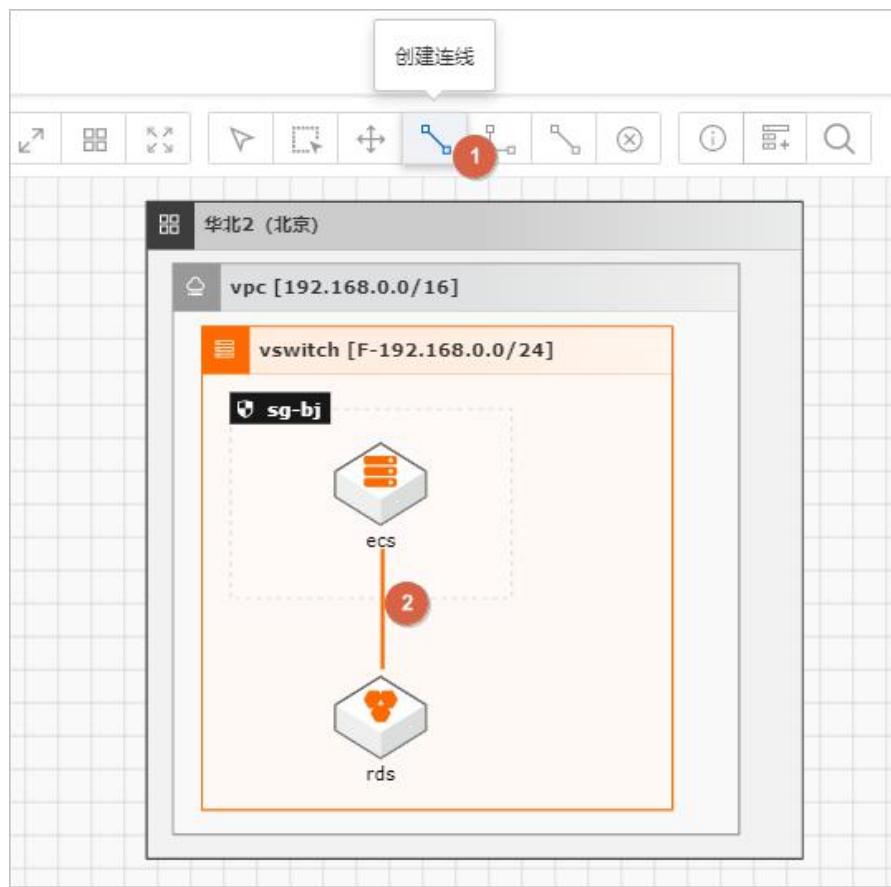
步骤 3 在左侧搜索框输入资源名称 rds，选中 RDS 图标，拖动 RDS 图标至 vswitch 中。（RDS 属于 vswitch 资源级别，因此放在 vswitch 中）



步骤 4 双击 RDS 图标，进行参数设置。



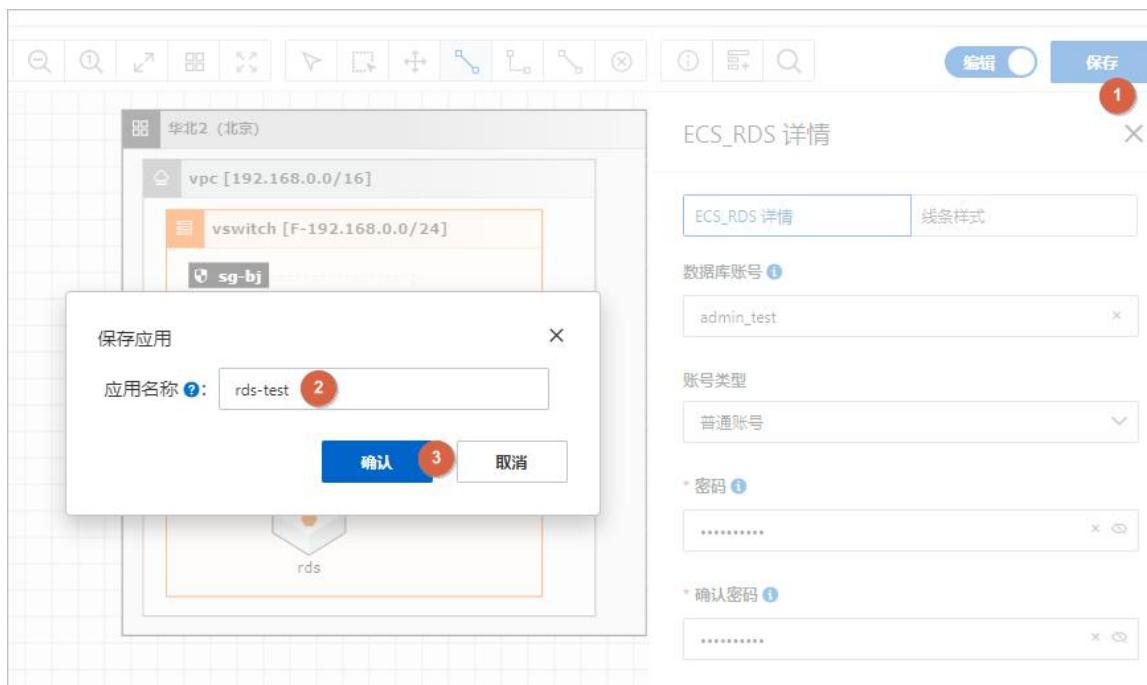
步骤 5 将 ecs 和 rds 用实线连接。



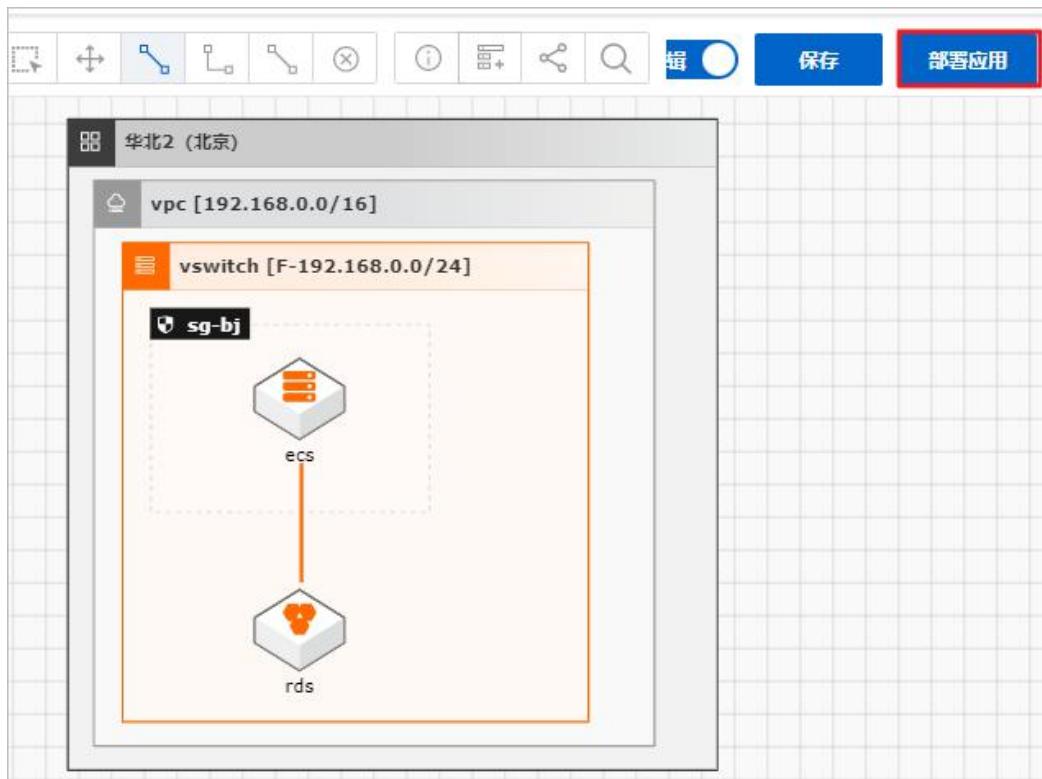
步骤 6 双击连接线进行数据库账号参数的配置。

The screenshot shows the 'ECS\_RDS 详情' configuration dialog. On the left, there's a preview of the network topology with a red circle labeled '1' pointing to a connection line between the 'ecs' and 'rds' nodes. On the right, the configuration dialog has several tabs: 'ECS\_RDS 详情' (selected), '线条样式', '数据库账号' (with a red circle labeled '2'), '账号类型' (with a red circle labeled '3'), and '密码' and '确认密码' fields (each with a red circle labeled '4' and '5' respectively).

步骤 7 上述配置完成后，单击保存，并设置应用名称。



步骤 8 保存成功后，单击右上角的**部署应用**。



步骤 9 进行资源校验。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	rds	rds	北京	MySQL	成功	校验通过	定位
2	ecs	ecs	北京	ecs.n4.large	成功	校验通过	定位
3	vswitch [F-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
4	vpc [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
5	sg-bj	security-group	北京		成功	校验通过	定位

状态:校验成功

[下一步: 价格清单](#)
[返回](#)

步骤 10 校验成功后，可以看到价格清单，单击**下一步：确认订单**。

导出价格清单													
免费		按量付费											
<b>资源成本占比</b>													
 <div style="display: flex; justify-content: space-between;"> <span>资源预算</span> <span>● 计算 计算: 100 元/时</span> <span>● 数据库 数据库: 100 元/时</span> </div>													
<b>价格列表</b>													
序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	状态	操作			
1	ecs	ecs	北京	ecs.n4.large	1	0.73元/时	省 0.37元/时	0.36元/时	新购	定位			
2	rds	rds	北京	mysql.n2.small	1	0.34元/时	省 0.17元/时	0.17元/时	新购	定位			

状态:计价成功

[上一步: 资源校验](#)
[查看报告](#)
[下一步: 确认订单](#)

步骤 11 勾选《云速搭服务条款》，然后单击**下一步：支付并创建**。

**确认订单**

免费	按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	rds	rds	北京	mysql.n2.small.1	1	0.34元/时	0.34元/时	新购
2	ecs	ecs	北京	ecs.n4.large	1	0.73元/时	0.73元/时	新购

《云速搭服务条款》  
部署前, 请阅读并勾选服务条款

按量付费: **0.34 元/时**

状态: **计价成功**

[上一步: 价格清单](#) [下一步: 支付并创建](#)

步骤 12 资源部署中, 耐心等待, 直到提示“部署成功”, 然后单击**返回**。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位

部署中, 不要进行任何操作, 请耐心等待..

每页显示 **10** 共0条 < 上一页 **1** 下一页 >

**部署概要**

状态: 部署中 应用编号: A61YQS0UCCWRCMY3

[返回](#)

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zep8248m07l7cxj9gbw3	运行中	2022-01-20 14:19:38	定位
2	vswitch [F-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zepdjkniav75agflae7	运行中	2022-01-20 14:19:39	定位
3	sg-bj	security.group (安全组)	-	sg-2zehra2eiej9crarfh4k	运行中	2022-01-20 14:19:39	定位
4	ecs	ecs (云服务器ECS)	按量付费	i-2zehra2eiej9ct9n0yfg	运行中	2022-01-20 14:20:25	定位
5	rds	rds (云数据库RDS)	按量付费	rm-2ze079wjskbed895h	运行中	2022-01-20 14:22:21	定位

每页显示 **10** 共5条 < 上一页 **1** 下一页 >

**部署概要**

状态: 部署成功 订单编号: 212678782610833  
应用编号: A61YQS0UCCWRCMY3

[查看报告](#) [返回](#)

步骤 13 打开资源清单，单击 rds，跳转到 rds 控制台。

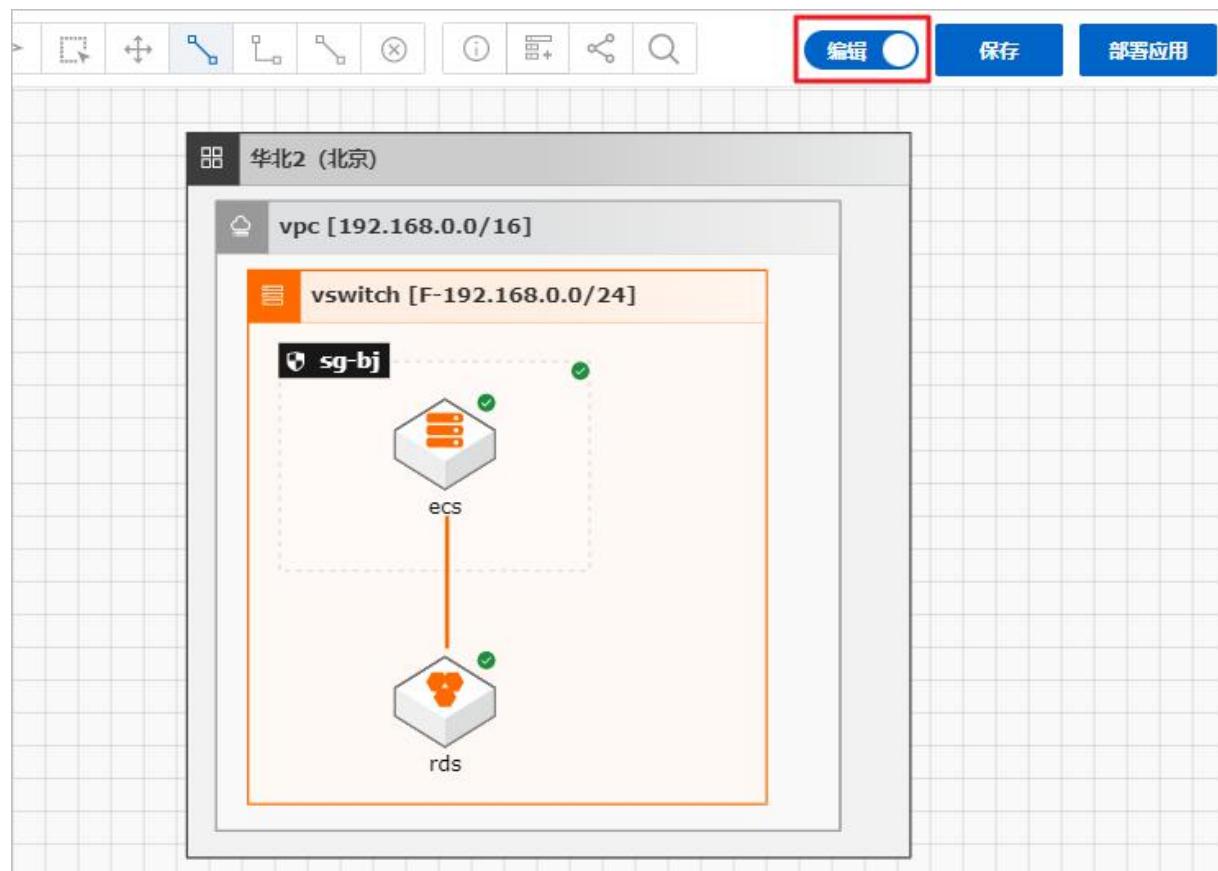
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间
4	ecs	ecs (云服务器ECS)	按量付费	i-2zefra2eiej9ct9n0yfg	新建	运行中	2022-01-20 14:20:25
5	rds	rds (云数据库RDS)	按量付费	rm-2ze079wjskbed895h	新建	运行中	2022-01-20 14:22:21

步骤 14 在账号管理中可以看到在 CADT 中创建的账号信息。

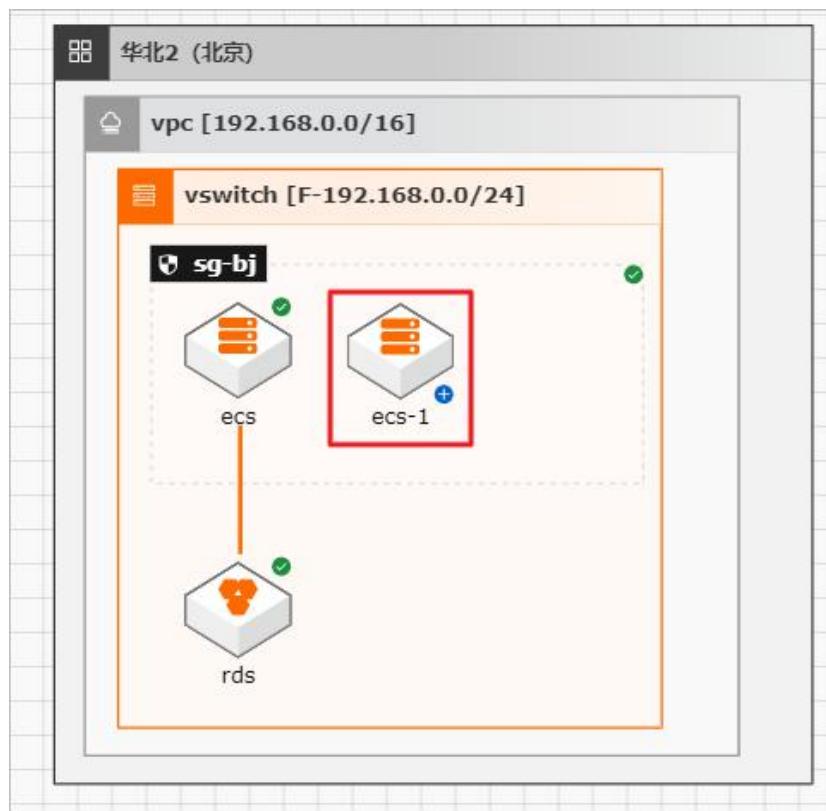
账号	类型	状态	所属数据库	账号描述
admin_test	普通账号	已激活	--	--

### 4.3.4.SQL Server 部署

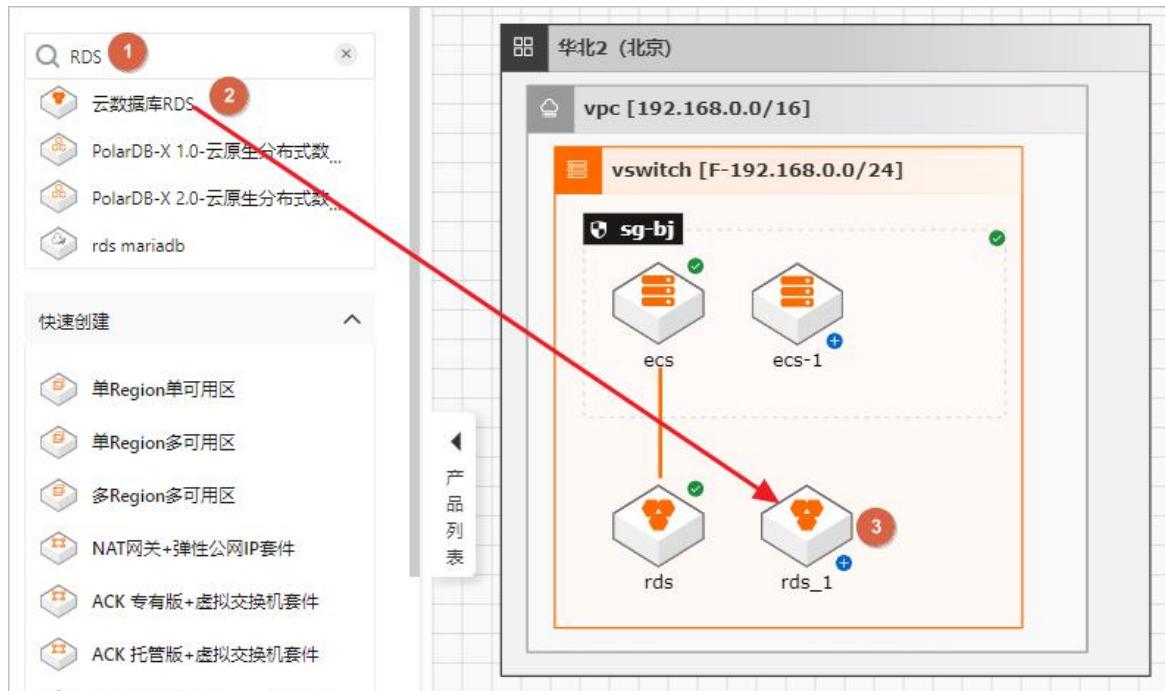
步骤 1 切换模式为编辑模式。



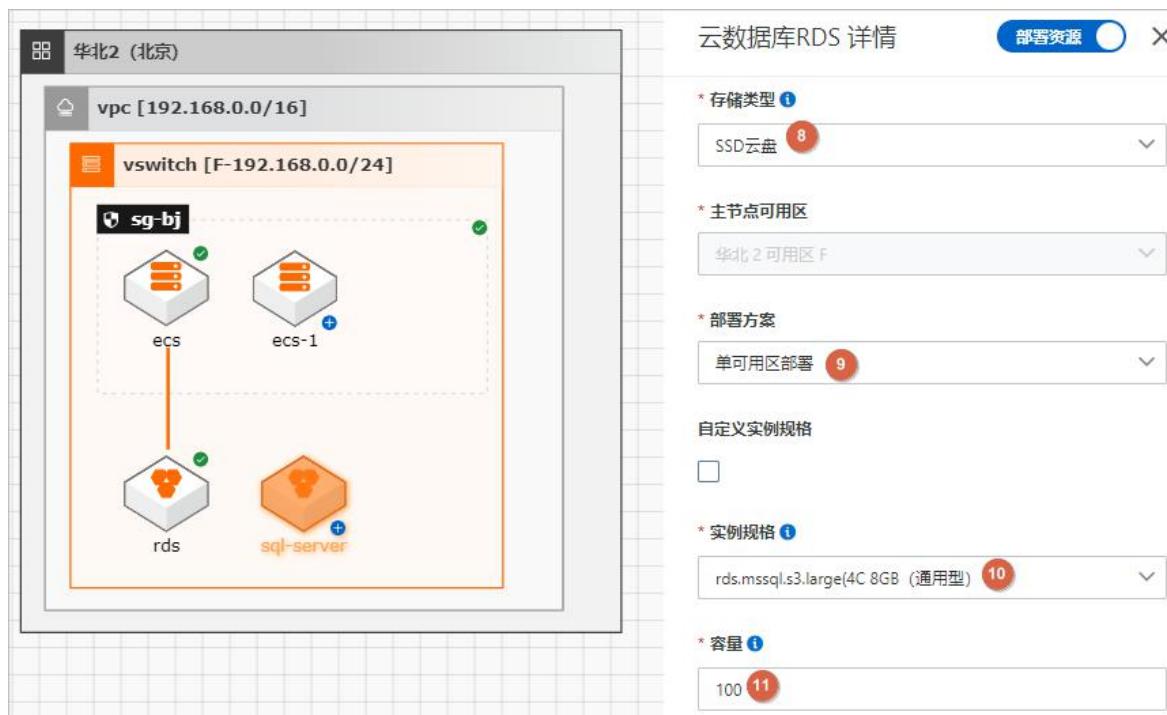
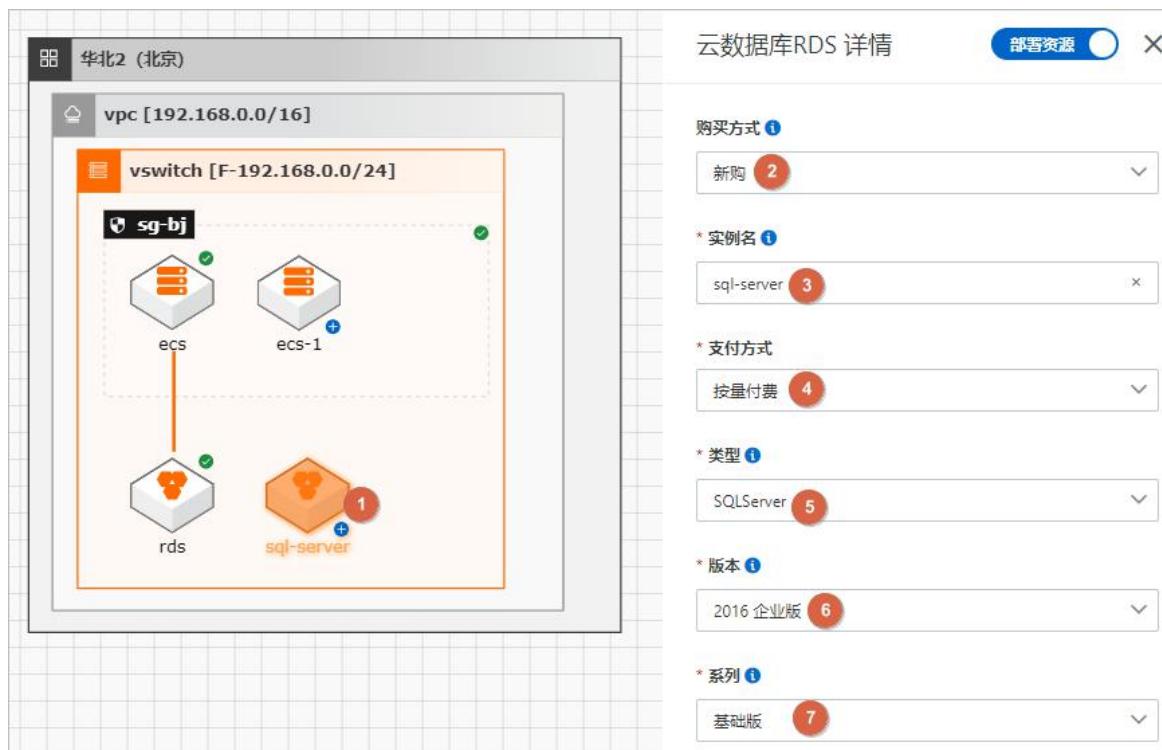
步骤 2 参考 2.2 章节中的步骤一和步骤二，将 ECS 拖动到画布中并且完成配置，也可以直接右键复制 ecs 得到 ecs\_1。



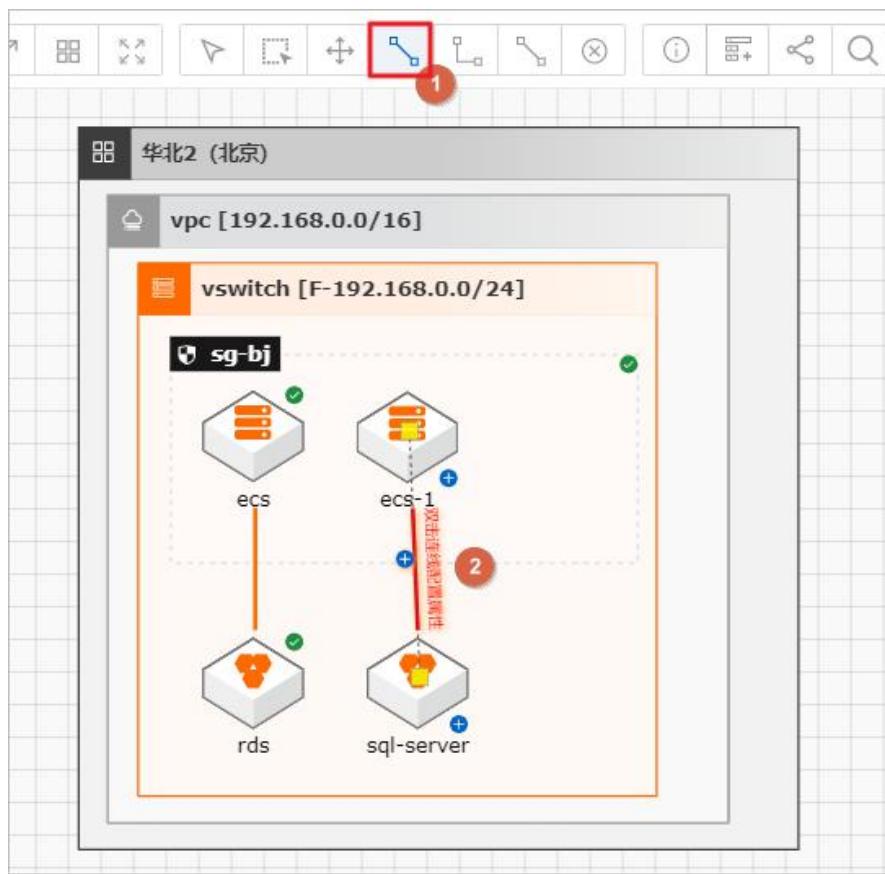
步骤 3 在左侧搜索框输入资源名称 rds，选中 RDS 图标，拖动 RDS 图标至 vswitch 中。



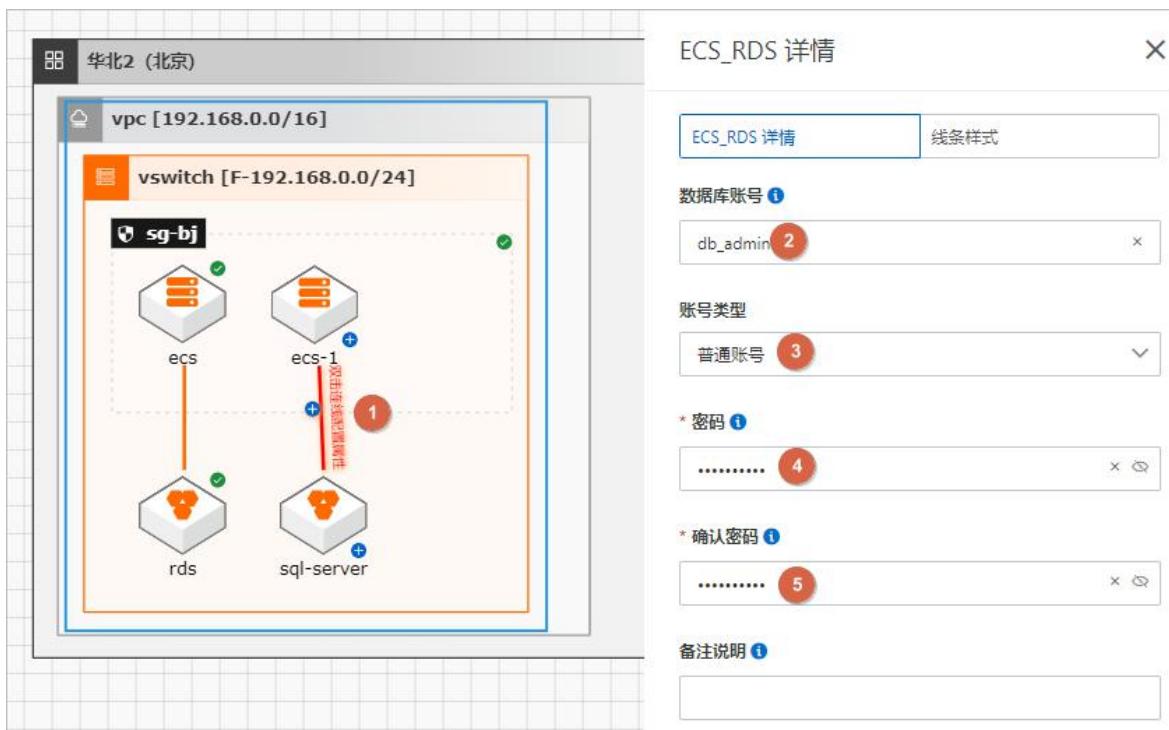
步骤 4 双击 RDS 图标，进行参数设置。



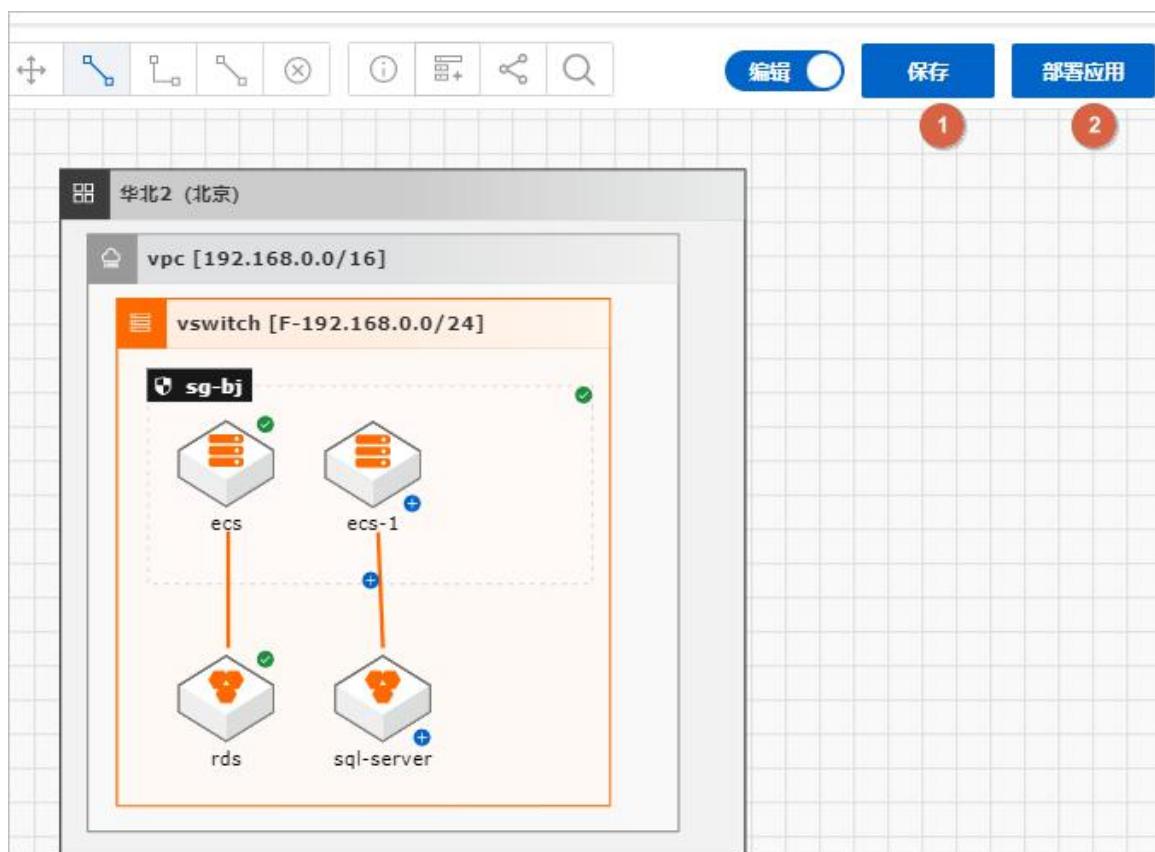
步骤 5 将 ecs 和 sql server 用连线连接。



步骤 6 双击连接线，进行属性配置。



步骤 7 单击保存，部署应用。



步骤 8 同样需要进行资源校验、订单确定、部署等步骤等环节，等待部署完成。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	rds	rds	北京	MySQL	成功	校验通过	定位
2	ecs	ecs	北京	ecs.n4.large	成功	校验通过	定位
3	vswitch [F-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
4	vpc [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
5	sg-bj	security.group	北京		成功	校验通过	定位
6	sql-server	rds	北京	SQLServer	成功	校验通过	定位
7	ecs-1	ecs	北京	ecs.n4.large	成功	校验通过	定位

状态: 资源验证成功(架构调整)

下一步: 价格清单    返回

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zep8248m07l7cxj9gwb3	运行中	2022-01-20 14:19:38	定位
2	vswitch [F-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zepdjknhahv75agflae7	运行中	2022-01-20 14:19:39	定位
3	sg-bj	security.group (安全组)	-	sg-2zefra2eiej9crarfh4k	运行中	2022-01-20 14:19:39	定位
4	ecs	ecs (云服务器ECS)	按量付费	i-2zefra2eiej9ct9n0yfg	运行中	2022-01-20 14:20:25	定位
5	rds	rds (云数据库RDS)	按量付费	rm-2ze079wjskbed895h	运行中	2022-01-20 14:22:21	定位

每页显示 10 共7条 < 上一页 1 下一页 >

**部署概要**

状态: 部署成功 订单编号 : 212678782610833, 212679384420833  
应用编号: A61YQS0UCCWRCMY3

查看报告 返回

步骤 9 在资源清单中, 资源名称中单击 sql-server

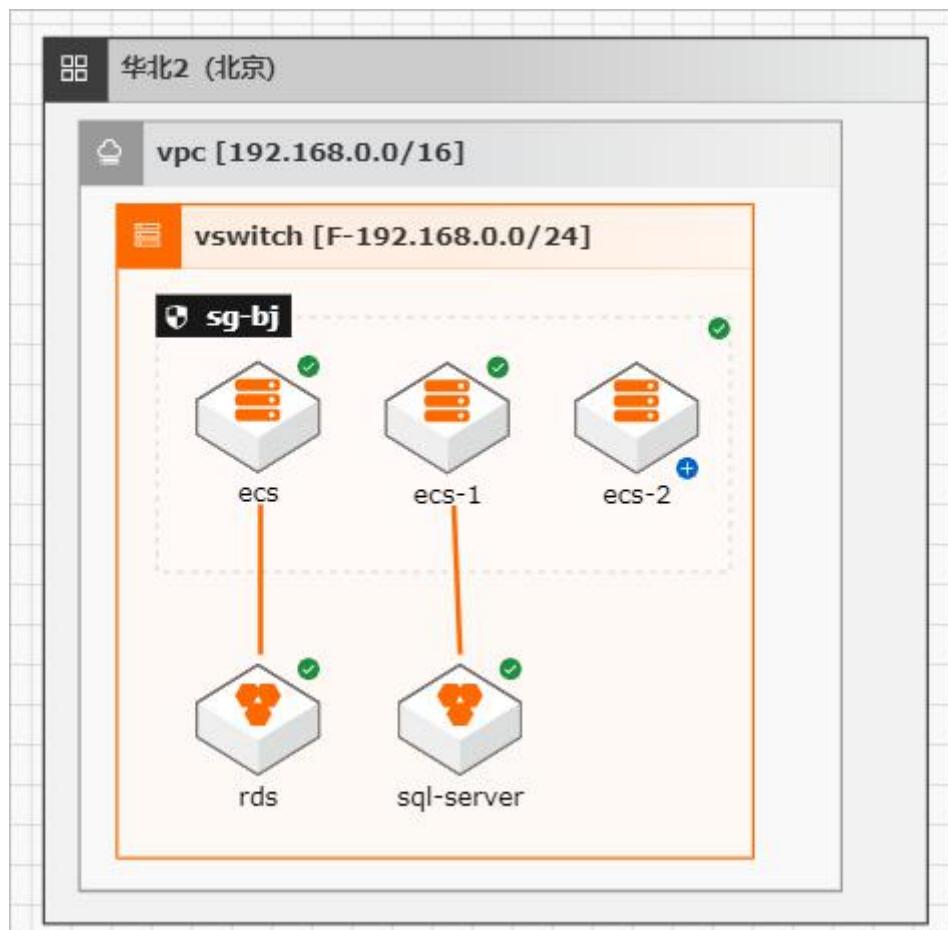
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间
6	ecs-1	ecs (云服务器ECS)	按量付费	i-2ze45o6isellwkwl0i2o	新建	运行中	2022-01-20 14:3
7	sql-server	rds (云数据库RDS)	按量付费	rm-2zed178f86ds7v98s	新建	运行中	2022-01-20 14:4

步骤 10 在账号管理中, 可以看到在 CDA 中创建的账号信息。

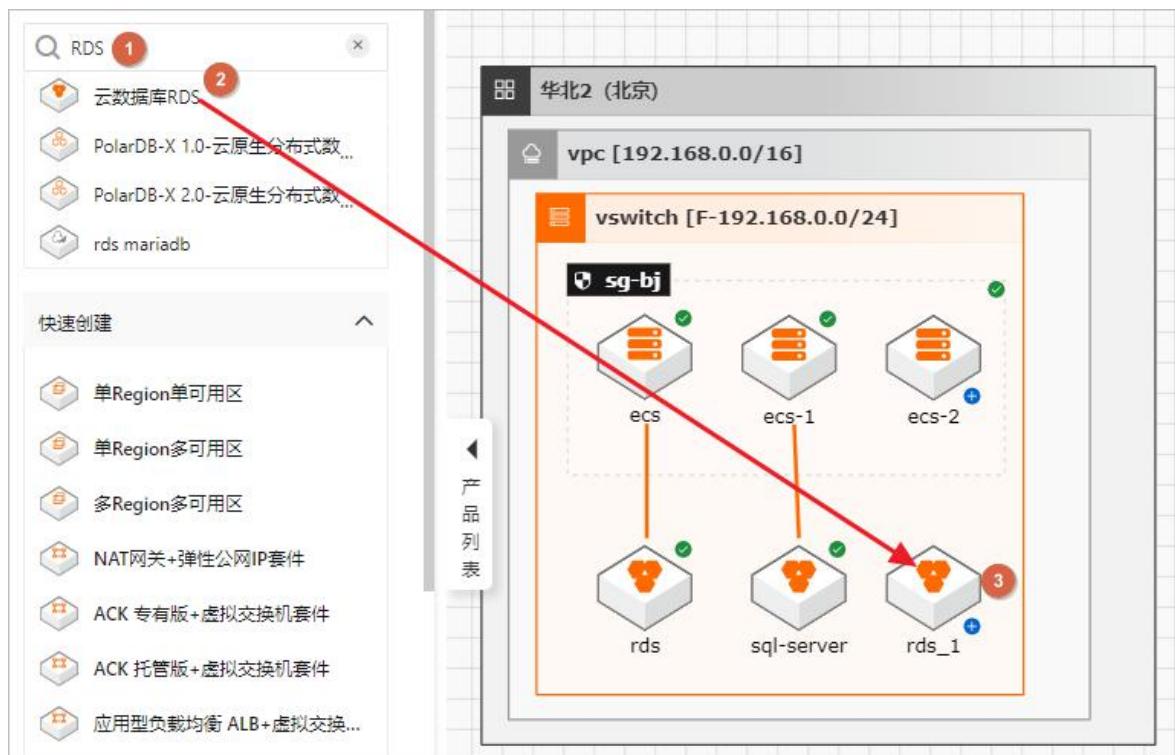
The screenshot shows the 'sql-server' instance management interface. On the left, there's a sidebar with tabs: 基本信息 (Basic Information), 账号管理 (Account Management) which is highlighted with a red box, 数据库管理 (Database Management), 备份恢复 (Backup Recovery), 数据库连接 (Database Connection), and 监控与报警 (Monitoring and Alarming). The main area has a '用户账号' (User Accounts) tab selected. A '创建账号' (Create Account) button is visible. Below it is a table with columns: 账号 (Account), 类型 (Type), 状态 (Status), and 所属数据库 (Database). One row is shown: db\_admin, 普通账号 (Normal Account), 已激活 (Activated), and --. A blue '登录数据库' (Log in to Database) button is at the top right.

### 4.3.5. PostgreSQL 部署

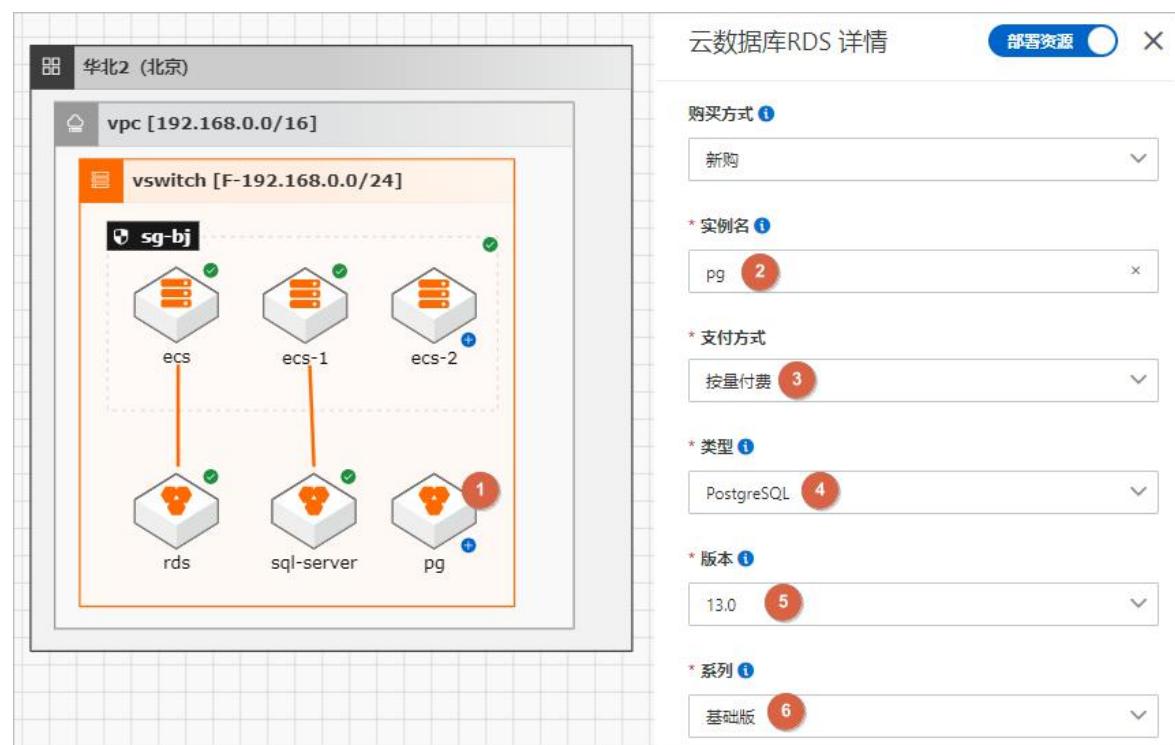
步骤 1 参考 2.2 章节中的步骤一和步骤二，将 ECS 拖动画布中并且完成配置，也可以直接右键复制 ecs 得到 ecs\_2。

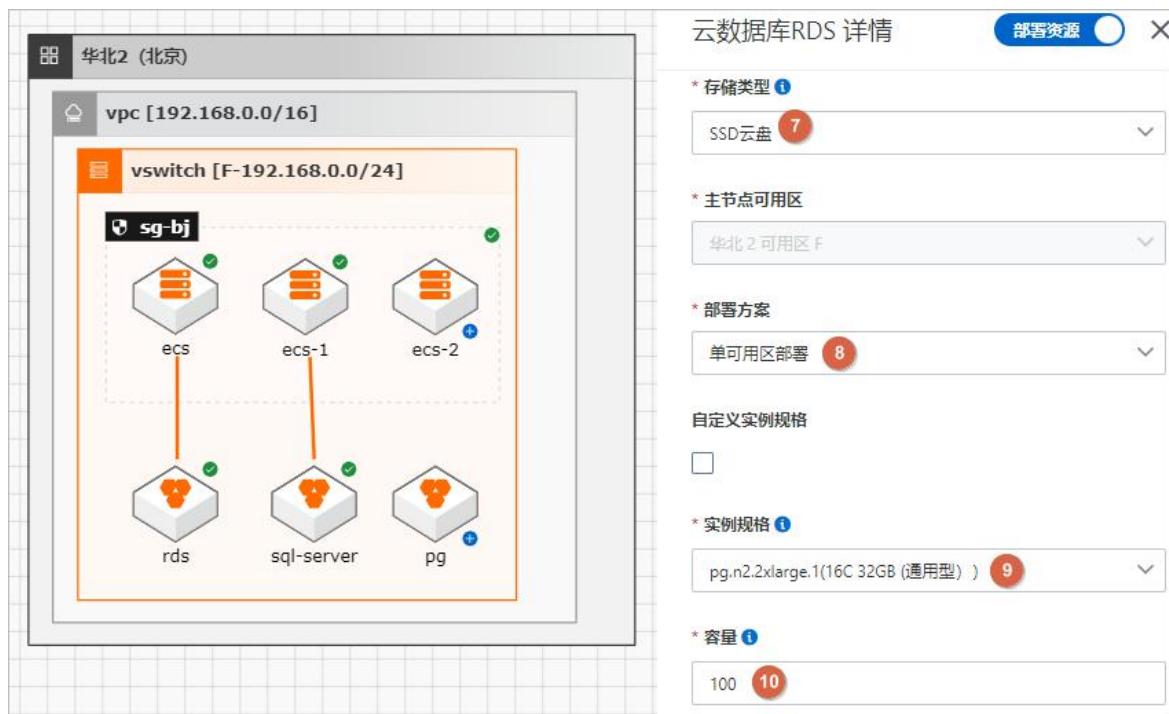


步骤 2 在左侧搜索框输入资源名称 rds，拖动 RDS 图标至 vswitch 中。

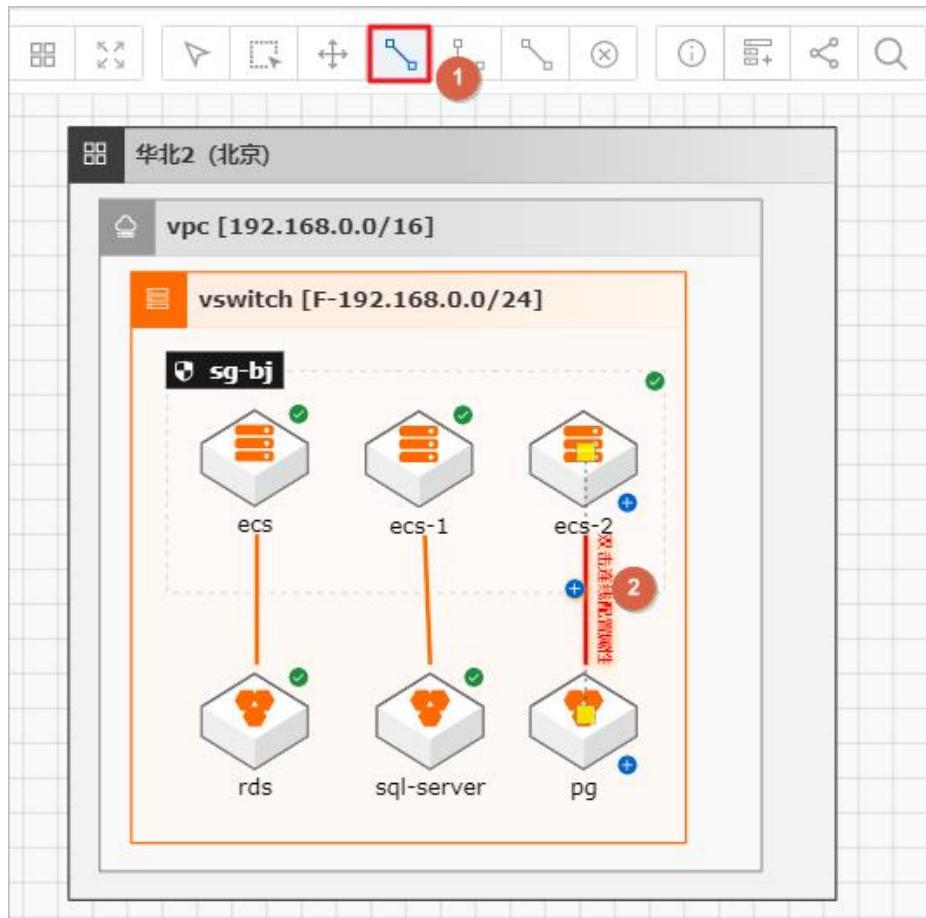


步骤 3 双击 RDS 图标，进行参数设置。

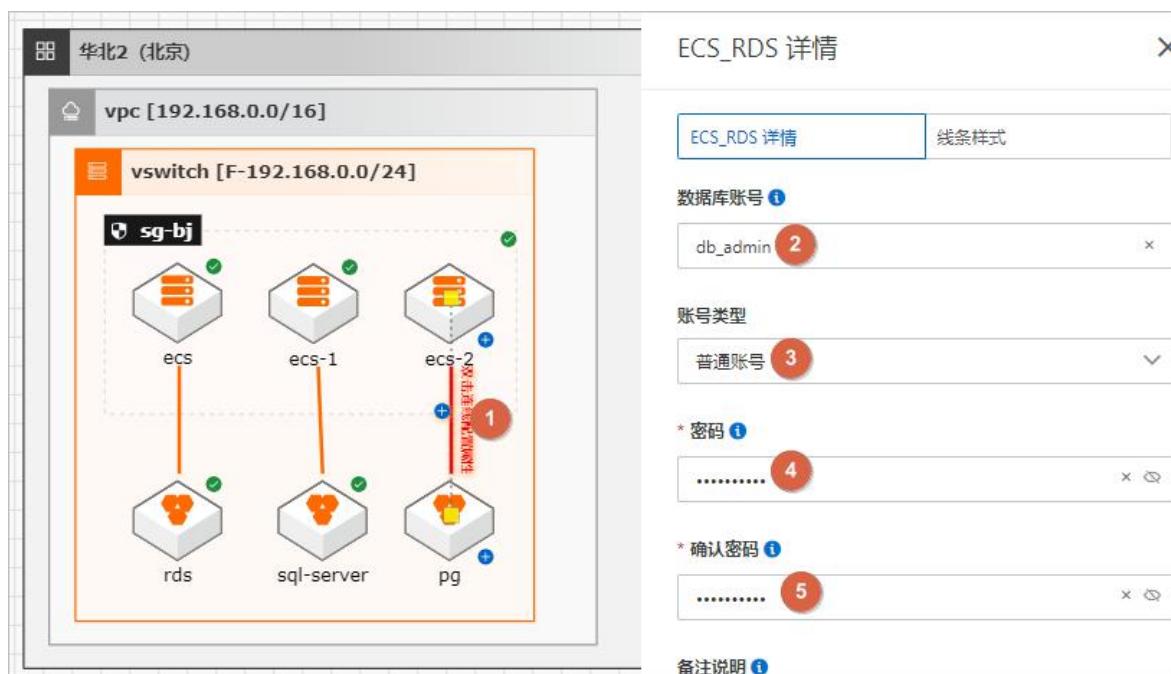




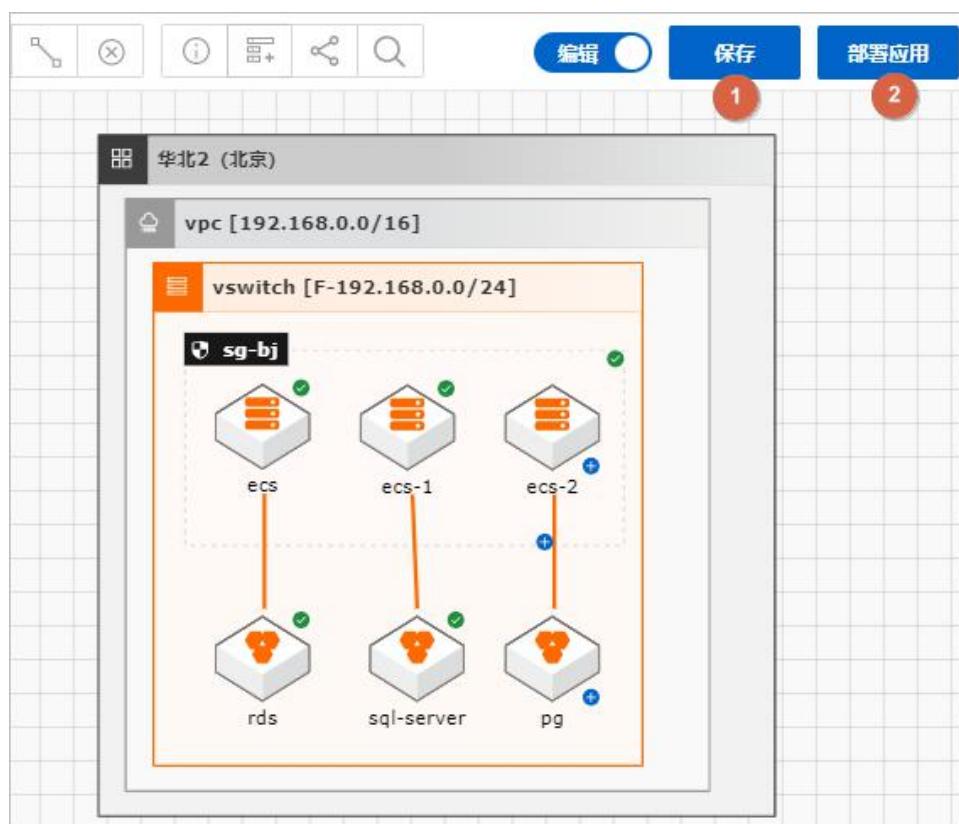
步骤 4 将 ecs 与 pg 用连线连接。



步骤 5 双击连线，进行账号信息配置。



步骤 6 单击保存，部署应用。



步骤 7 同样需要进行资源校验、订单确定、部署等步骤等环节，等待部署完成。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zep8248m07l7cxj9gwb3	运行中	2022-01-20 14:19:38	定位
2	vswitch [F-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zepdjknhav75agflae7	运行中	2022-01-20 14:19:39	定位
3	sg-bj	security.group (安全组)	-	sg-2zebra2eiej9crarfh4k	运行中	2022-01-20 14:19:39	定位
4	ecs	ecs (云服务器ECS)	按量付费	i-2zebra2eiej9ct9n0yfg	运行中	2022-01-20 14:20:25	定位
5	rds	rds (云数据库RDS)	按量付费	rm-2ze079wjskbed895h	运行中	2022-01-20 14:22:21	定位

每页显示 10 共9条 < 上一页 1 下一页 >

**部署概要**

状态：部署成功 订单编号：212678782610833, 212679384420833, 212681820400833  
应用编号：A61YQS0UCCWRRCMY3

查看报告 返回

步骤 8 在资源清单中，资源名称中单击 pg。

华北2 (北京)

vpc [192.168.0.0/16]

vswitch [F-192.168.0.0/24]

sg-bj

ecs  
ecs-1  
ecs-2

资源清单

应用操作 导出资源清单

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间
8	ecs-2	ecs (云服务器ECS)	按量付费	i-2ze6r3rvh4a0fhf6kwqy	新建	运行中	2022-01-
9	pg	rds (云数据库RDS)	按量付费	pgm-2ze05w042261y92y	新建	运行中	2022-01-

步骤 9 在账号管理中，可以看到在 CADT 中创建的账号信息。

基本信息

**账号管理**

数据库管理

备份恢复

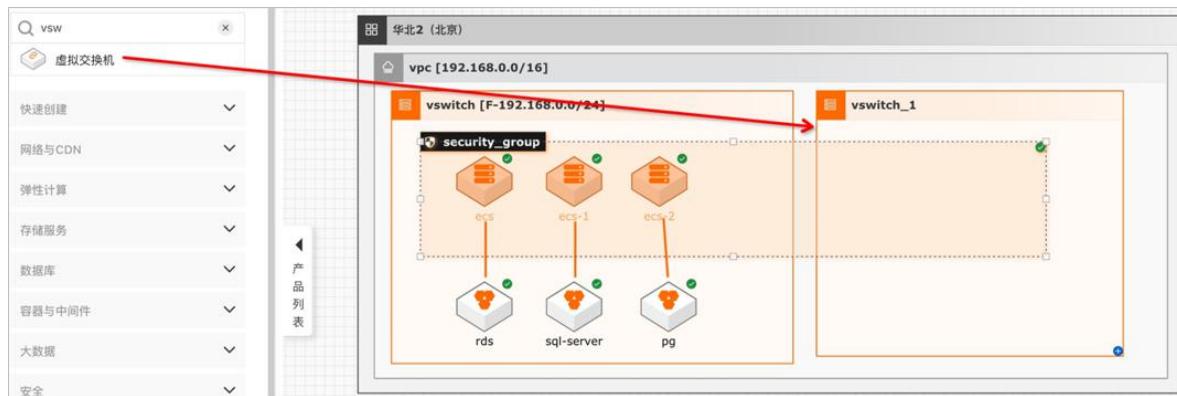
数据库连接

监控与报警

用户账号	服务账号	AD域服务信息	AD域修改记录
<b>创建账号</b>			
账号	类型	状态	
db_admin	普通账号	<b>✓ 已激活</b>	

### 4.3.6.PolarDB 部署

步骤 1 创建一个新的可用区。



虚拟交换机 详情

购买方式 **i**

新购

\* vswitch名 **i**

vswitch\_1

\* 可用区 **i**

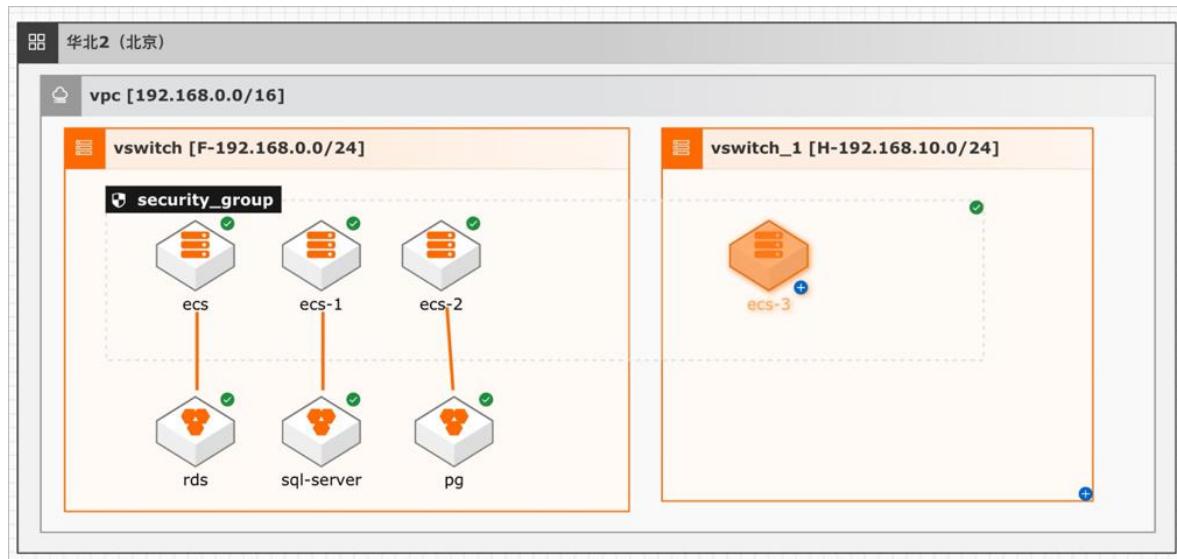
华北 2 可用区 H

\* IPv4网段 **i**

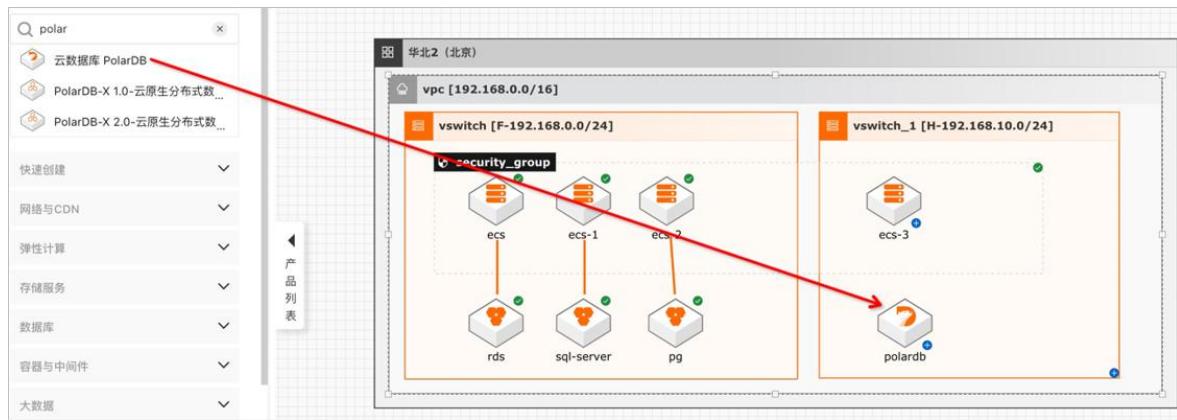
192 . 168 . 10 . 10 / 24

可用IP数252

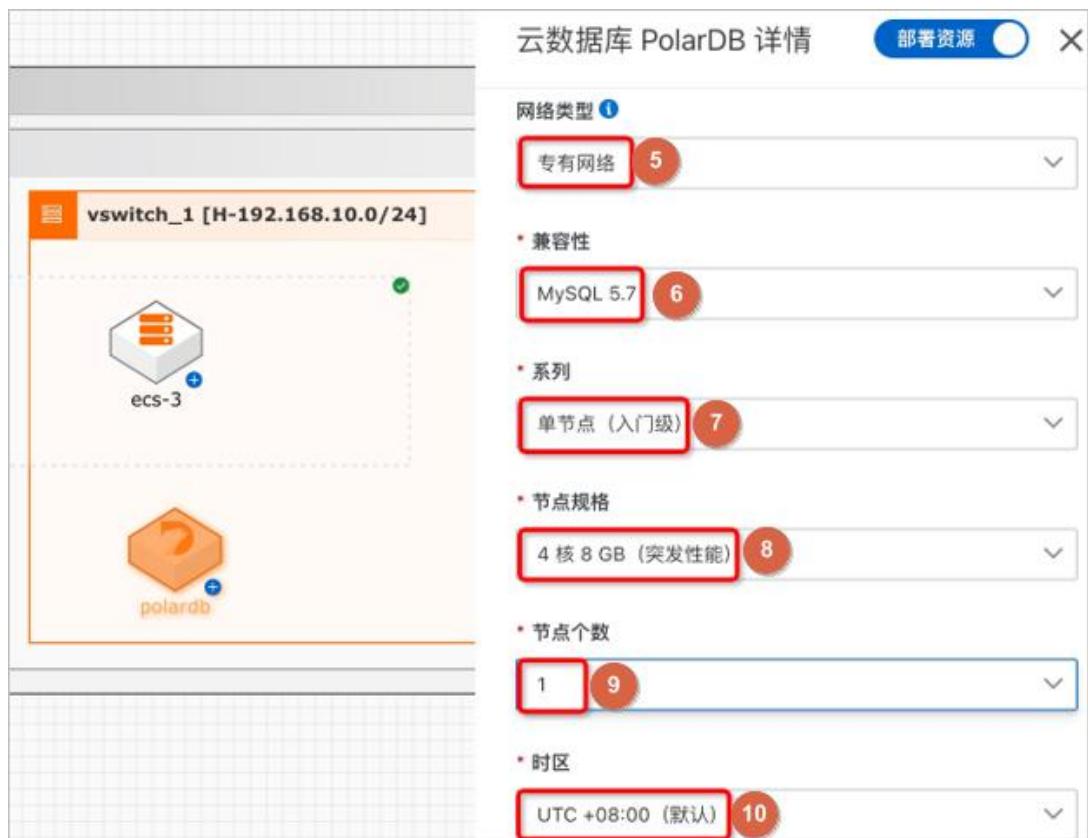
步骤 2 参考 2.2 章节中的步骤一和步骤二，将 ECS 拖动画布中并且完成配置，也可以直接右键复制 ecs 得到 ecs\_3。



步骤 3 在左侧搜索框输入资源名称 polar，拖动云数据库 PolarDB 图标至 vswitch 中。

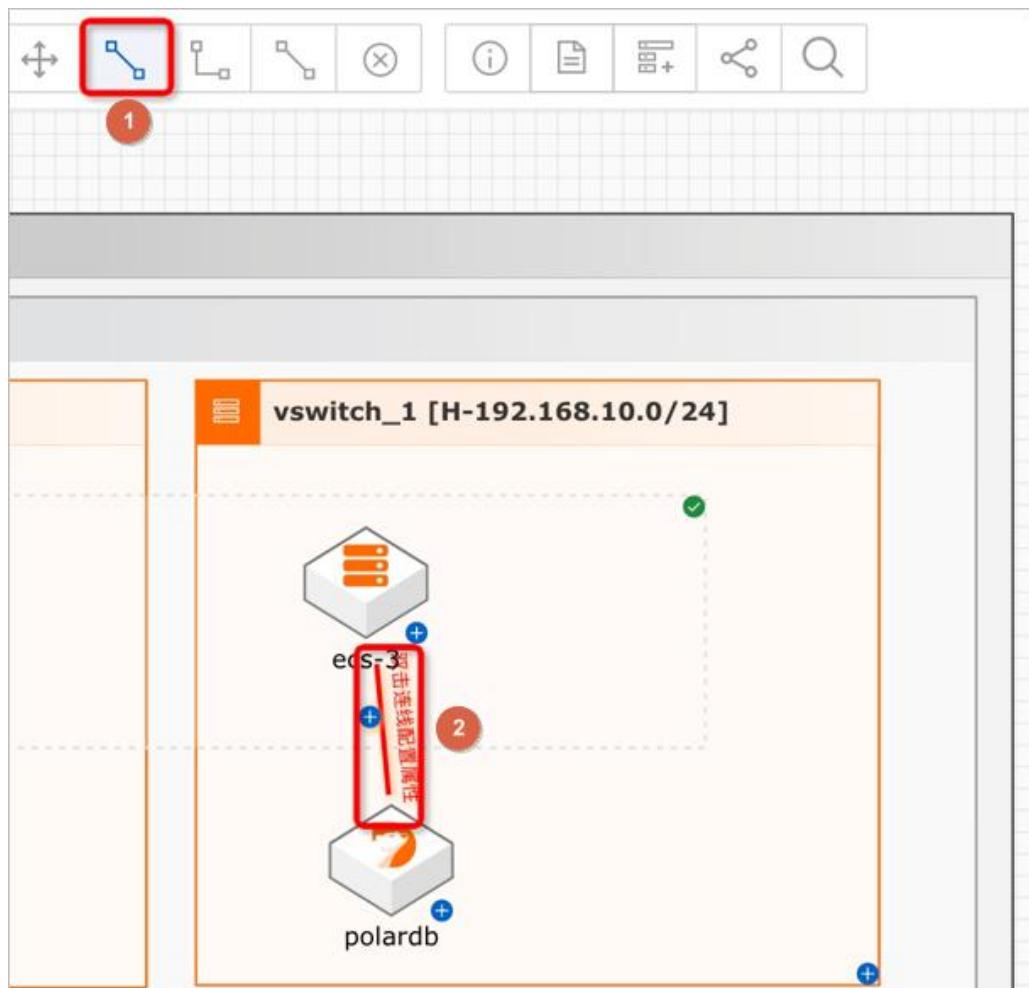


步骤4 双击 polaradb 图标，进行参数配置。

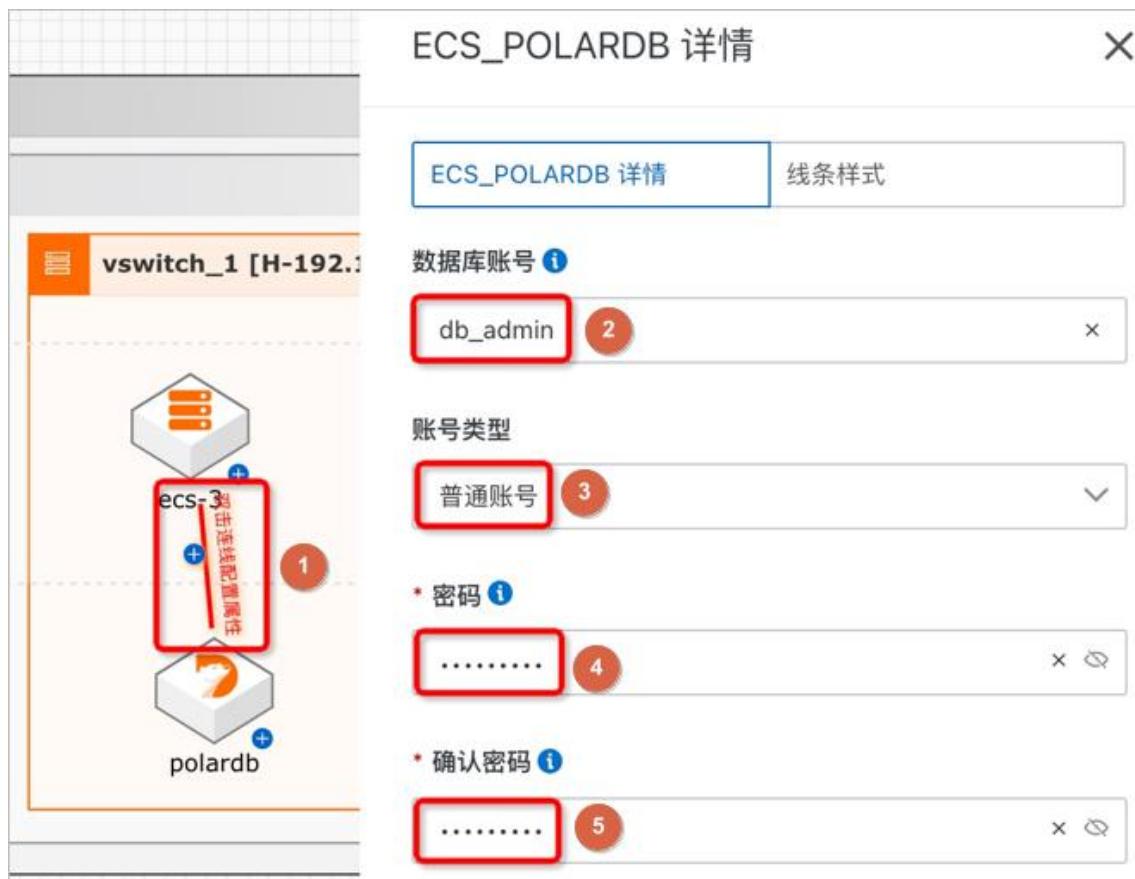




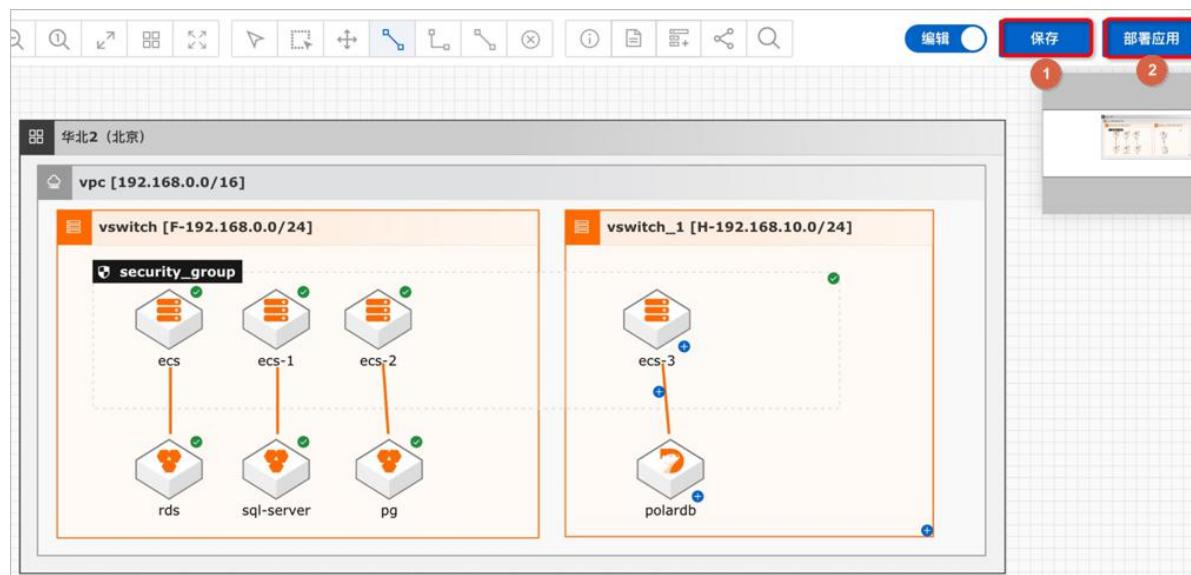
步骤 5 将 ecs 和 polardb 用连线连接。



步骤 6 双击连线，创建账号。



步骤 7 单击保存，部署应用。



步骤 8 同样需要进行资源校验、订单确定、部署等步骤等环节，等待部署完成。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc	vpc	-	vpc-2ze44vj2k4pb1duxec5ug	运行中	2021-11-01 16:35:30	定位
2	vswitch	vswitch	-	vsw-2zem54kfiud6pjgzz4l8	运行中	2021-11-01 16:35:30	定位
3	sg-bj	security.group	-	sg-2zeb7b8tz2dspuhz3qbo	运行中	2021-11-01 16:35:30	定位
4	ecs	ecs	按量付费	i-2zegcjzk7qg5qjludqdy	运行中	2021-11-01 16:35:53	定位
5	rds	rds	按量付费	rm-2zeioq3u400x93mih	运行中	2021-11-01 16:38:19	定位

**部署概要**

状态：部署成功

订单编号：211352190620519, 211359298550519, 211369103240519,  
211371418010519

方案编号：G1NBFPUCKVFUC

[查看报告](#) [返回](#)

步骤 9 在资源清单中单击 polardb 进行页面跳转

**pc-2zer6q09690b554jp** 运行中

[登录数据库](#)

**基本信息**

配置与管理	地域	华北2 (北京)	VPC	vpc-2zew7mf42lmmppgzkueep
集群白名单	数据分布的可用区	北京 可用区H	交换机	vsw-2zei5j1cu1ruijcrcj6
安全管理	兼容性	100% 兼容 MySQL 5.7	可维护窗口	02:00-03:00 <a href="#">编辑</a>
账号管理	系列	单节点	内核版本	5.7.1.0.16

**白名单与账号**

您需要设置PolarDB集群的IP白名单，并创建集群的初始账号，才能连接和使用该集群。

**访问白名单**

您已经设置2个集群白名单，[前往查看](#)

**链接地址**

步骤 10 步骤 10 在账号管理中可以看到在 CADT 中创建的账号信息

The screenshot shows the 'Account Management' page of the CADT interface. At the top, there is a breadcrumb navigation '集群 / 账号管理' and a back arrow pointing to 'pc-2ze4bw5i93tg437s9'. To the right of the back arrow is a green button labeled '运行中' (Running). On the far right is a blue button labeled '登录数据库' (Login Database). Below the header, there are several buttons: '创建账号' (Create Account), '自定义权限' (Custom Permissions), '模糊搜索 (当前页)' (Fuzzy Search (Current Page)), and a search input field with placeholder text '请输入' (Please Enter). A red box highlights the 'db\_admin' account in the list. The list includes columns: '账号名' (Account Name), '状态' (Status), '所属数据库' (Database), '备注' (Remarks), and '类型' (Type). The account 'db\_admin' is listed with a status of '可用' (Available) indicated by a green checkmark, and it is categorized as a '普通账号' (Normal Account). A red number '2' is displayed below the account list. On the left side, there is a sidebar with the following items: '基本信息' (Basic Information), '配置与管理' (Configuration and Management), '集群白名单' (Cluster Whitelist), '安全管理' (Security Management), '账号管理' (Account Management) which is highlighted with a red box and has a red number '1' next to it, '数据库管理' (Database Management), and '备份恢复' (Backup and Recovery).

## 4.4.云速搭部署数据库审计

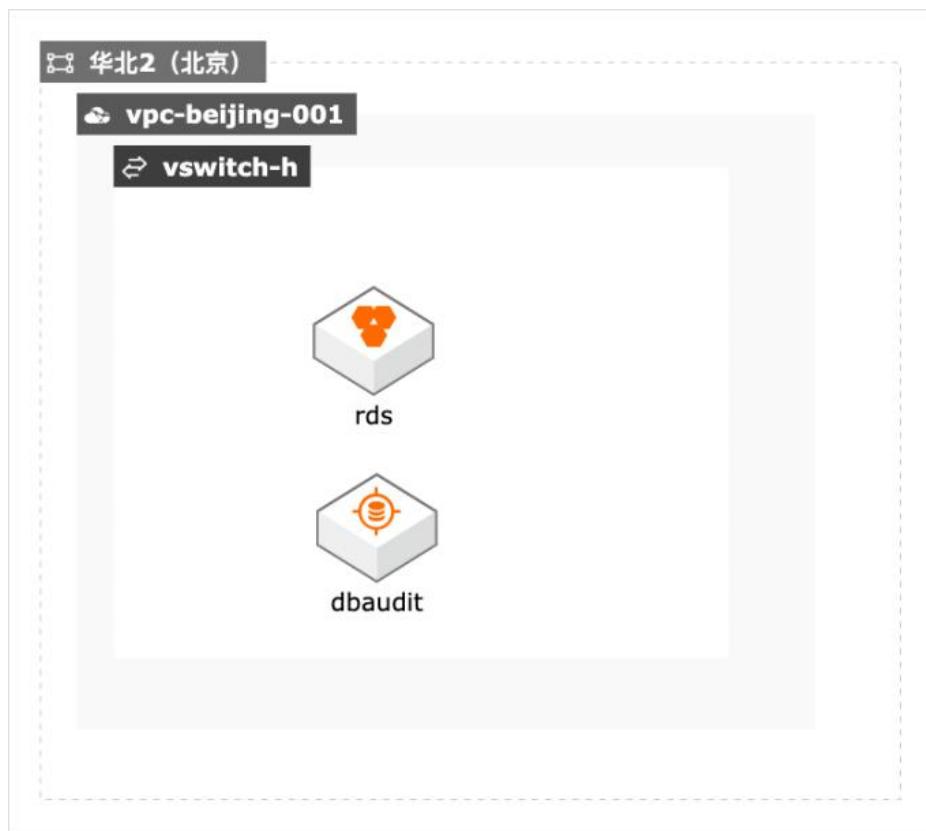
作者 | 阿里云解决方案架构师 敬海

### 4.4.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现数据库审计的部署。

数据库审计计费方式见 [https://help.aliyun.com/document\\_detail/52483.htm](https://help.aliyun.com/document_detail/52483.htm)



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

云资源	架构级别
数据库审计	vswitch 级别
RDS	vswitch 级别

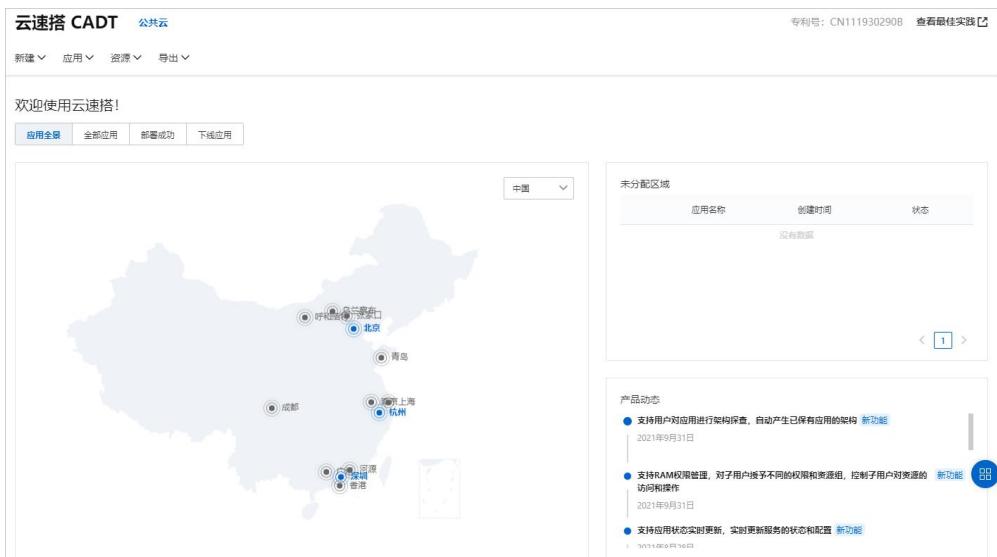
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
RDS	rds	-
数据库审计	dbaudit	-

### 4.4.2. 应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

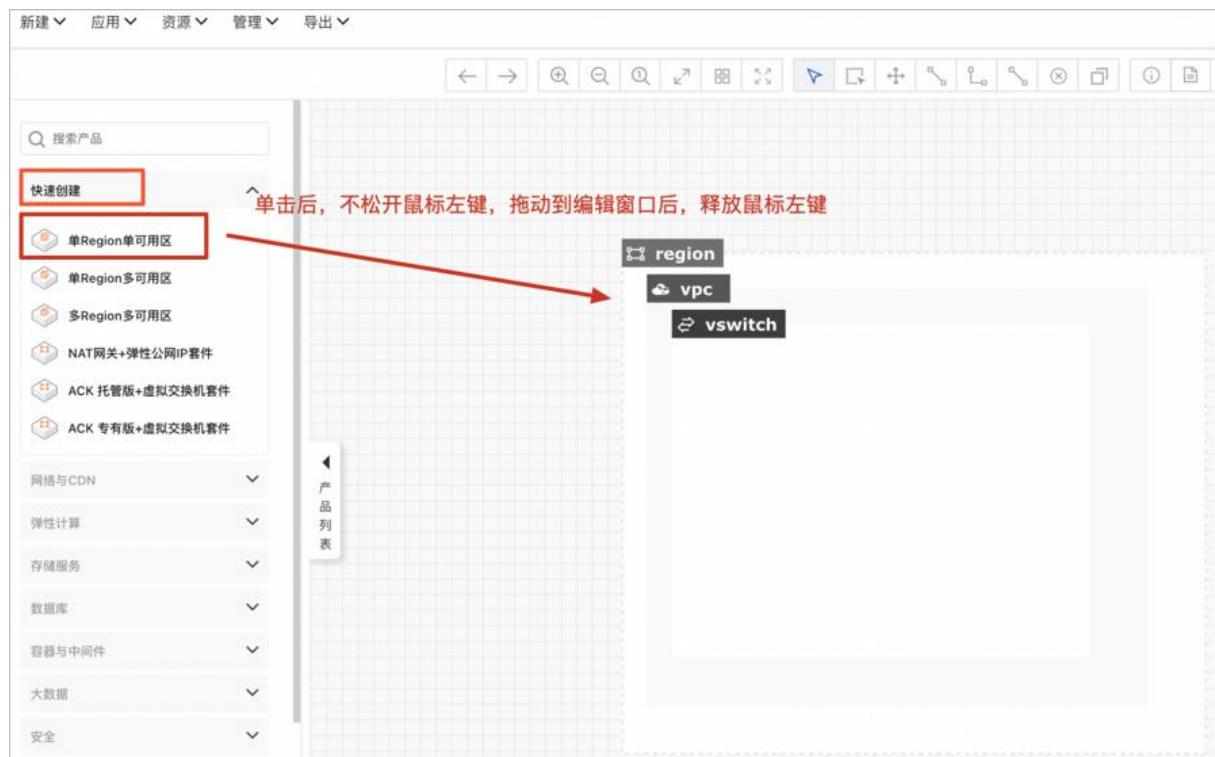
说明：如果提示需要开通服务，请根据提示进行开通。



步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

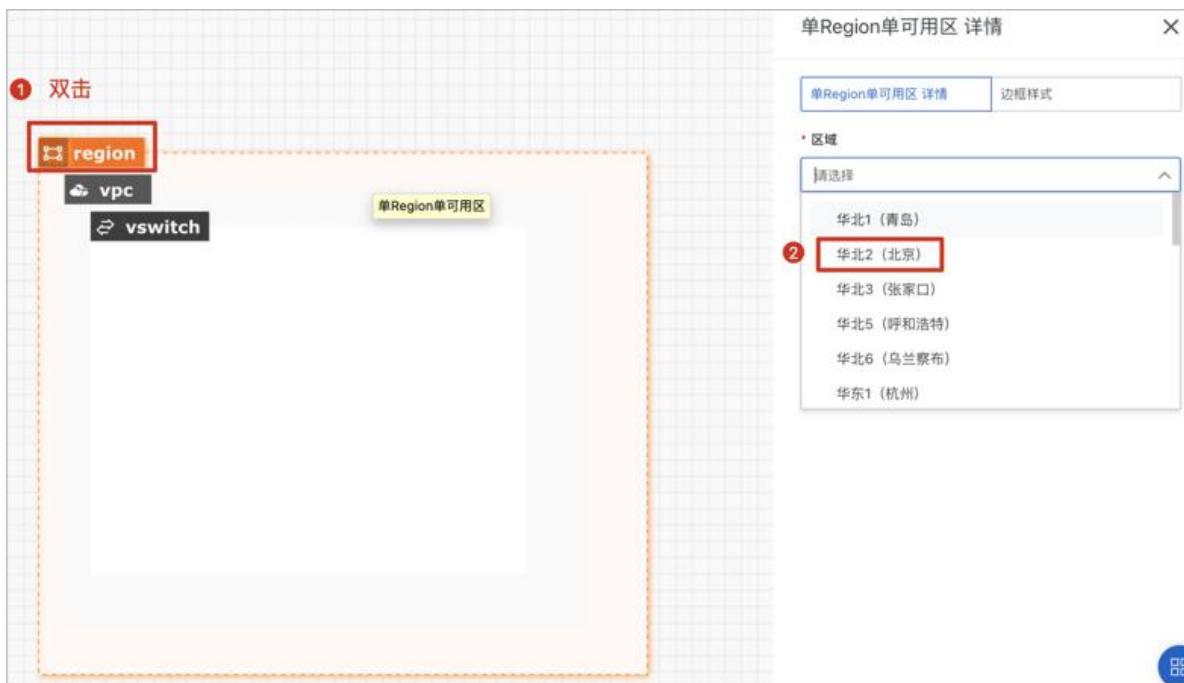


步骤 3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

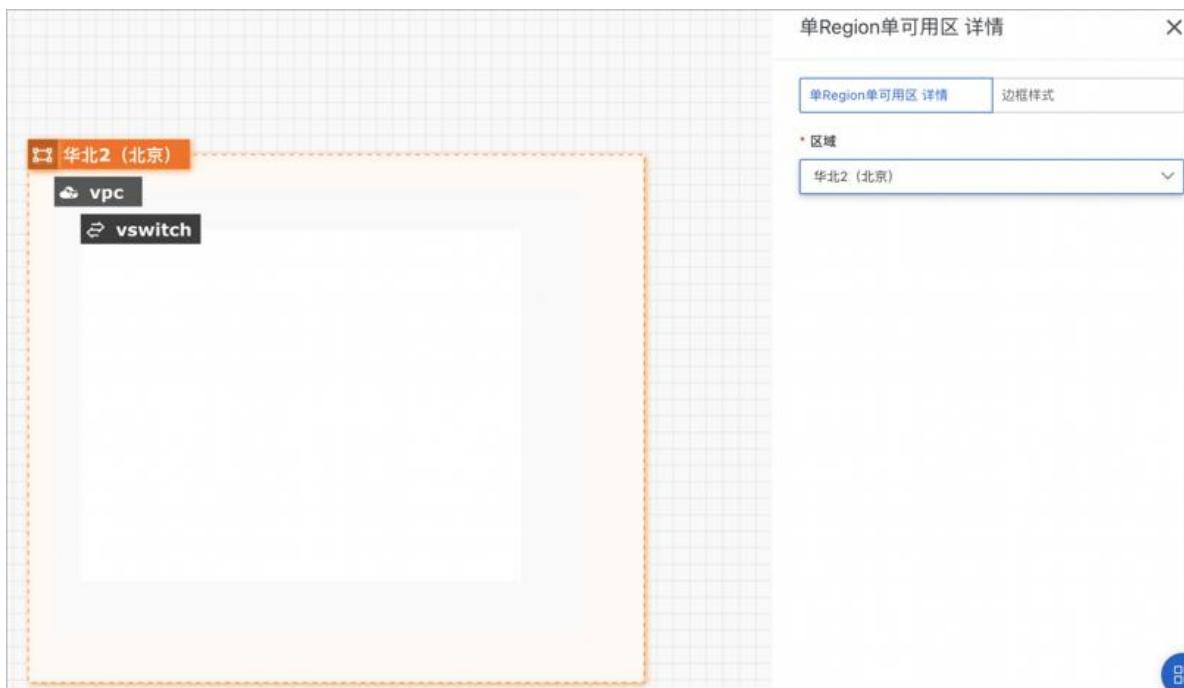


步骤 4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



选择后，如下图所示：



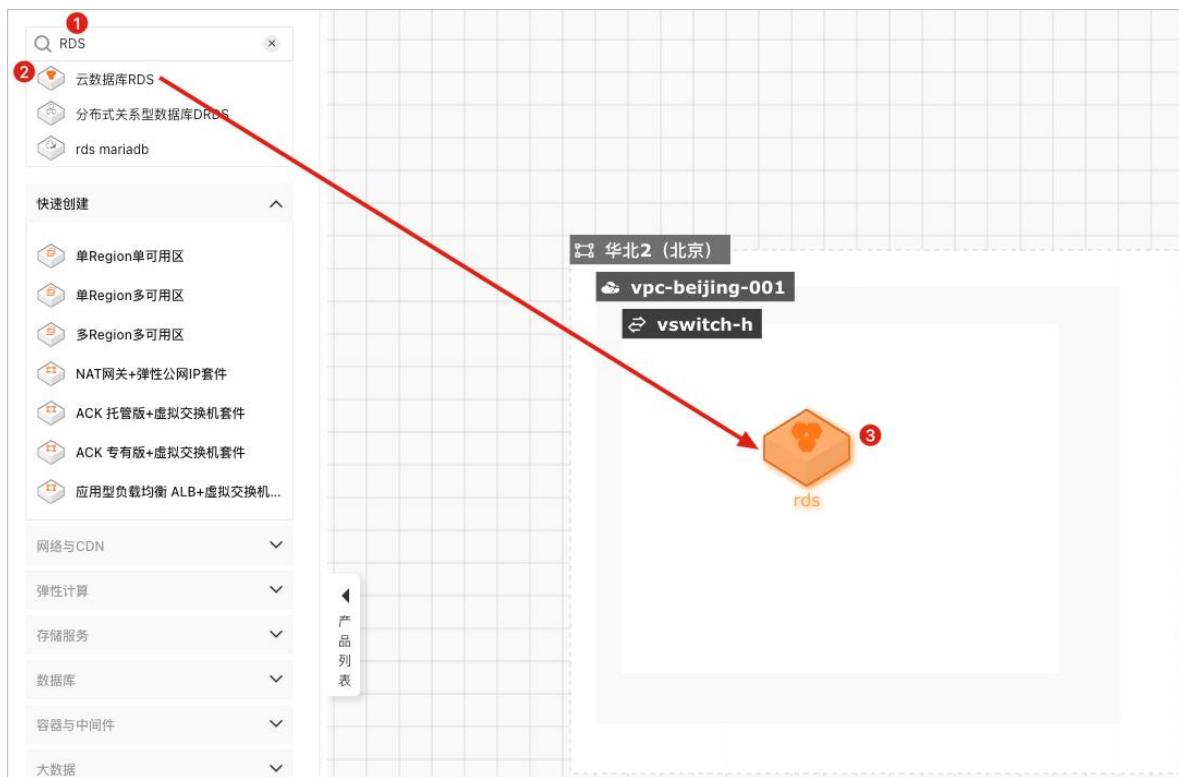
2. 双击 VPC，配置 VPC 参数。



3. 双击 Vswitch，配置 vswitch 参数。



步骤 5 左侧搜索 RDS，拖到 vswitch 中。

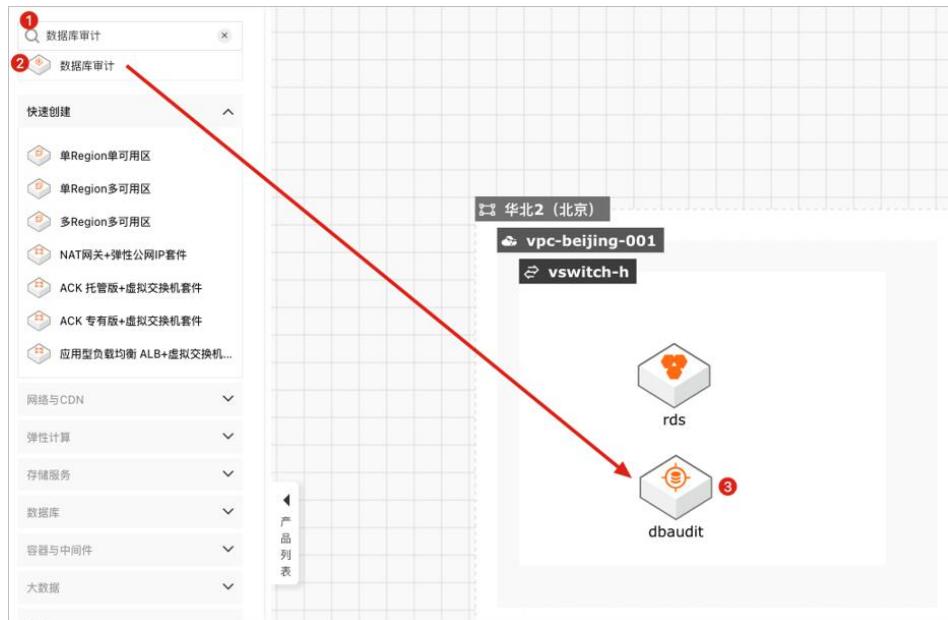


步骤 6 双击 RDS，配置参数：

购买方式 ① 新购 ①	* 主节点可用区 华北 2 可用区 H
* 实例名 ② rds ②	* 部署方案 单可用区部署 ⑧
* 支付方式 按量付费 ③ ③	自定义实例规格 <input type="checkbox"/>
* 类型 ④ MySQL ④	* 实例类型 ⑤ mysql.n2.small.1(1核 2GB (通用型)) ⑨
* 版本 ⑥ 5.7 ⑤	* 容量 ⑦ 100 ⑩
* 分类 ⑥ 基础版 ⑥	白名单ip ⑧ security_ips = [ " 192.168.0.0/24 ⑪ ] ]
* 存储类型 ⑦ SSD云盘 ⑦	

步骤 7 搜索数据库审计，拖入 vswitch 的框内。

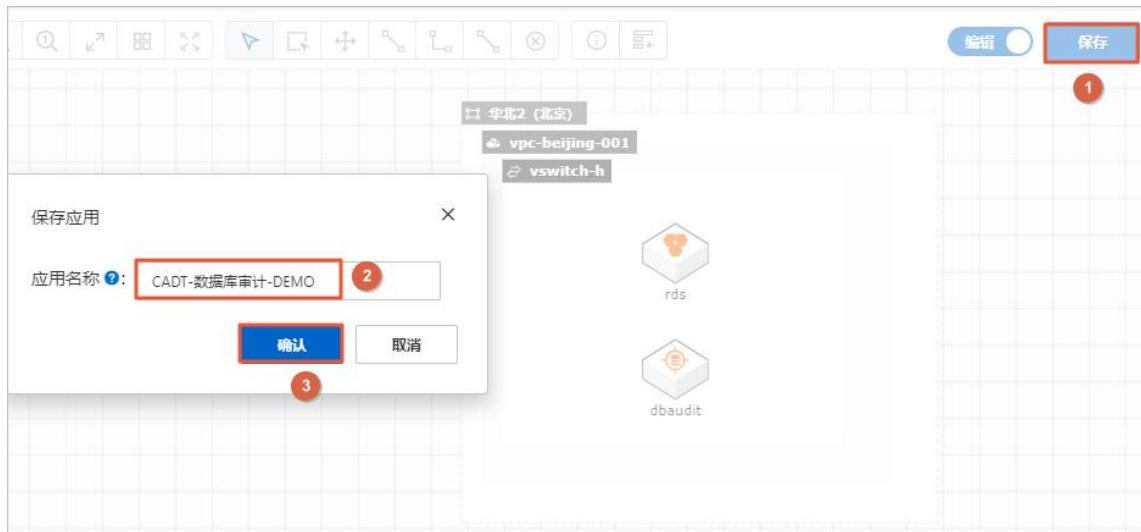
数据库审计服务需要部署在 VPC 的某个 vswitch 中，通常建议和要审计的数据库在一个 vswitch 中。



步骤 8 双击数据库审计图标，修改参数。

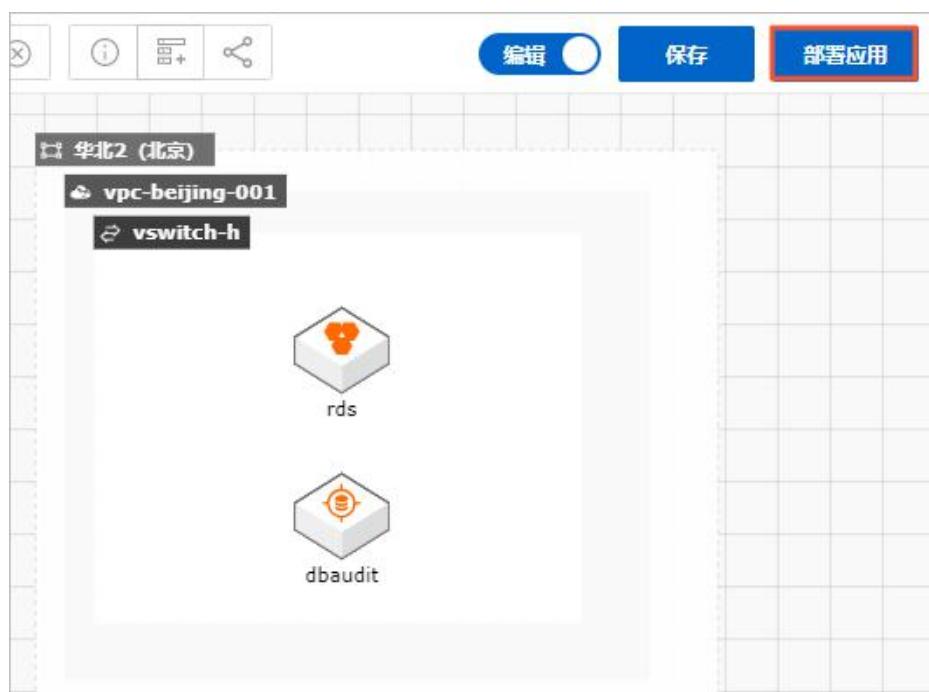


步骤 9 配置完成，单击右上角的保存，填写应用名称。



### 4.4.3. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、ECS 是否有库存等，一般需要几十秒左右。等待校验成功，单击**下一步：价格清单**。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	rds	rds	北京	MySQL	成功	校验通过	定位
2	vswitch-h	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
3	vpc-beijing-001	vpc	北京	192.168.0.0/16	成功	校验通过	定位
4	dbaudit	dbaudit	北京	alpha	成功	校验通过	定位

状态:校验成功

下一步: 价格清单 返回

步骤3 在**导出价格清单**对话框中，会拉取应用所有配置的价格信息，查看计费详情。分别查看包年包月的价格和按量付费的价格。

**导出价格清单**

包年包月 免费 按量付费

资源成本占比



资源预算  
● 数据安全 数据安全: 10... 元

价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
1	dbaudit	dbaudit	北京	alpha	1	1月	3000.00元/月			定位

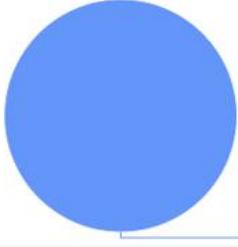
状态: 计价成功

上一步: 资源校验 查看报告 下一步: 确认订单

导出价格清单

免费 包年包月 按量付费

资源成本占比



资源预算  
● 数据库 数据库: [redacted] 元/时

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	rds	rds	北京	mysql.n2.small.1	1	0.30元/时	省 [redacted] 元/时	[redacted] 元/时	<a href="#">定位</a>

状态: 计价成功

[上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

步骤 4 可以单击[查看报告](#), 查看应用的价格信息。



步骤 5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。



步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。



步骤 7 部署完成后，单击查看报告，可以查看本次的部署报告。

**资源部署状态**

序号	资源名称 <input type="text"/>	资源类型 <input type="text"/>	付费类型	资源ID <input type="text"/>	资源状态	资源更新时间	定位
1	vpc-beijing-001	vpc	-	vpc-2zeu8u4u9995vdpsiiid	运行中	2021-11-08 14:41:40	定位
2	vswitch-h	vswitch	-	vsw-2ze9rtcdauh60h6z5f7n6	运行中	2021-11-08 14:41:40	定位
3	rds	rds	按量付费	rm-2zexf2ieds69azn1o	运行中	2021-11-08 14:44:20	定位
4	dbaudit	dbaudit	包年包月	dbaudit-cn-7pp2iumy0q	运行中	2021-11-10 11:02:13	定位

**部署概要**

状态：部署成功 订单编号：211445111440159, 211464196160159  
方案编号：0B503E5BD4QO766K

[查看报告](#) [返回](#)



步骤 8 单击返回，然后单击资源清单。

序号	资源名称 <input type="text"/>	资源类型 <input type="text"/>	付费类型	资源ID <input type="text"/>	来源	资源状态	资源更新时间	定位	操作
1	vpc-beijing-001	vpc	-	vpc-2zeu8u4u9995vdpsiiid	新建	运行中	2021-11-08 14:41:40	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
2	vswitch-h	vswitch	-	vsw-2ze9rtcdauh60h6z5f7n6	新建	运行中	2021-11-08 14:41:40	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
3	rds	rds	按量付费	rm-2zexf2ieds69azn1o	新建	运行中	2021-11-08 14:44:20	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
4	dbaudit	dbaudit	包年包月	dbaudit-cn-7pp2iumy0q	新建	运行中	2021-11-10 11:02:13	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 9 单击数据库审计后，跳转到数据库审计控制台查看。



序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	vpc-beijing-001	vpc	-	vpc-2zeu8u4u9995vdpsilcd	新建	运行中	2021-11-08 14:41:40	定位	详情   监控   变更日志   操作
2	vswitch-h	vswitch	-	vsw-2ze9rtcdauh60h6z57h6	新建	运行中	2021-11-08 14:41:40	定位	详情   监控   变更日志   操作
3	rds	rds	按量付费	rm-2zexf2ieds69azn1o	新建	运行中	2021-11-08 14:44:20	定位	详情   监控   变更日志   操作
4	dbaudit	dbaudit	包年包月	dbaudit-cn-7pp2fiumy0q	新建	运行中	2021-11-10 11:02:13	定位	详情   监控   变更日志

步骤 10 启用数据库审计实例。



步骤 11 等待数据库审计启动后，参照如下链接使用数据库审计。

<https://bp.aliyun.com/detail/39> 中第 11 章《开通并配置数据库审计》中的内容。

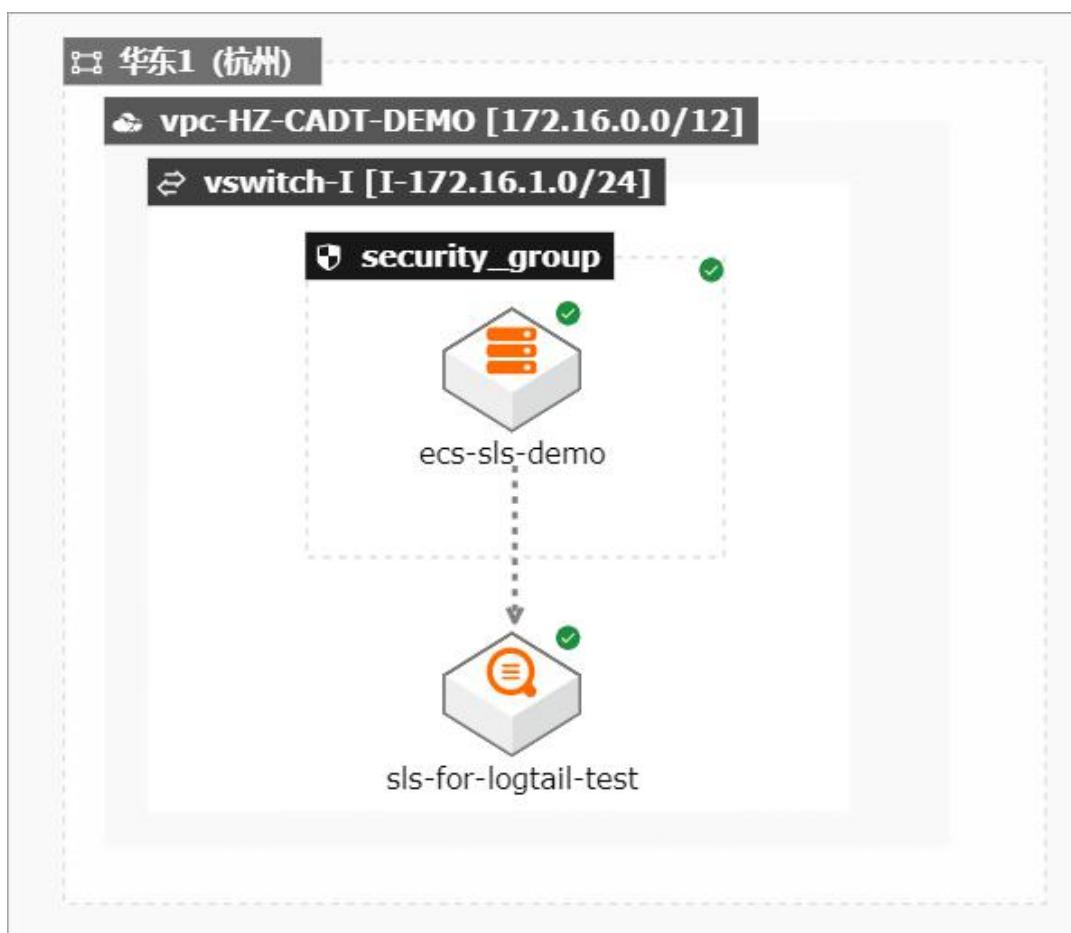
## 4.5.云速搭部署 SLS 实现日志采集处理分析

作者 | 阿里云解决方案架构师 洁谦

### 4.5.1. 云速搭架构设计入门

#### 方案架构

- 通过云速搭部署 ECS+SLS，在 ECS 上安装 logtail 收集 nginx 应用日志写入 SLS。通过日志生成器模拟 nginx 日志生成，并通过 SLS 进行日志分析。
- 具备一个安全组，通过安全组对 ECS 进行详细的安全策略配置。



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下图，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
SLS	Region
ECS	VSW
安全组	VPC

## 资源规划清单

资源类别	配置项	配置明细	说明
区域	区域	华东 1 (杭州)	本最佳实践全部资源部署在杭州 (主数据中心)
专有网络 VPC	状态	新购 (根据实际情况选择新购或已保有，本最佳实践新购 VPC)	云上选择专有网络 (VPC) 以保障安全性。 选择离原系统公网 IP 近的云上区域减少网络延迟。
	VPC 名	vpc-HZ-CADT-DEMO	
	网段	172.10.0.0/16	选择资源丰富、离用户近的区域保障项目顺利实施。 网络规划留足可用 IP 数即可。
虚拟交换机	状态	新购 (根据实际情况选择新购或已保有，本最佳实践新购交换机)	
	vswitch 名	vswitch-1	
	可用区	华东 1 可用区 I	
	IPv4 网段	172.10.1.0/24	

资源类别	配置项	配置明细	说明
ECS	可用区	默认（华东 1 可用区 I）	ECS 创建在 vswitch-1 下，无需选择。
	ECS 名	ecs-sls-demo	
	主机名	ecs-sls-demo	
	支付方式	后付费	按量付费
	实例规格	4 核 CPU, 16GB 内存 (ecs.g6.xlarge)	云上业务系统规格按照原规格购买。
	镜像	CentOS	
	镜像版本	CentOS 7.6 64 位	
	系统盘	ESSD 云盘	ESSD 云盘
	硬盘容量	40GiB	
	公网带宽	按流量付费	
	出网带宽	10	分配公网 IP
	登陆密码	*****	初始 root 用户密码，创建成功后由业务方分别登录修改密码。
	安全加固	Active	

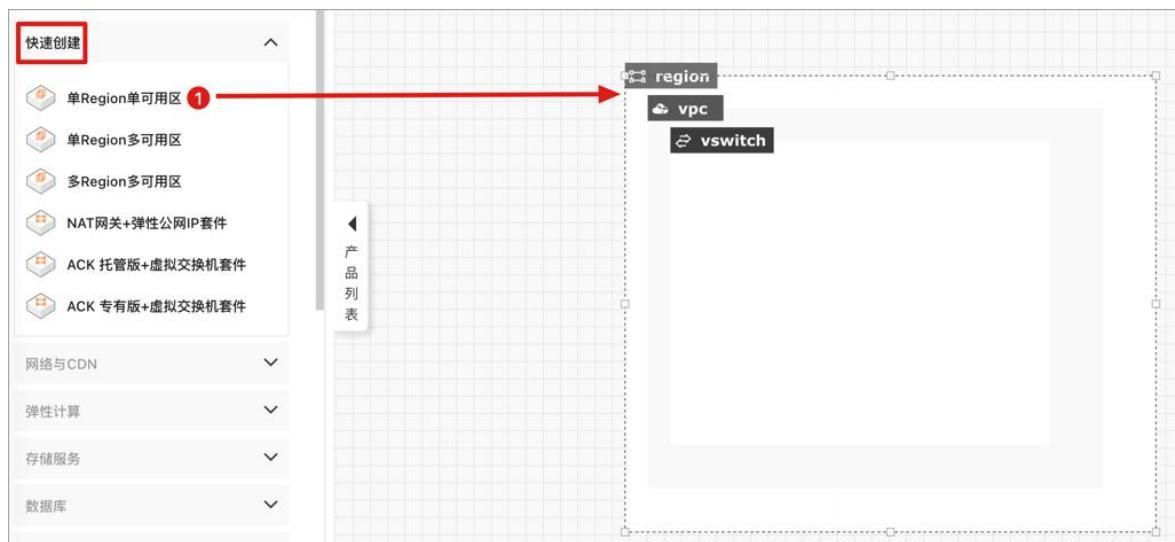
### 4.5.2. 通过云速搭 CADT 部署资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录 CADT 控制台，如果提示需要开通服务，请根据提示进行开通。

步骤 2 单击新建 > 新建空白应用



步骤3 拖入单 Region 单可用区到画布区域。



步骤4 分别双击 region、vpc、vswitch 进行设置

配置 region：



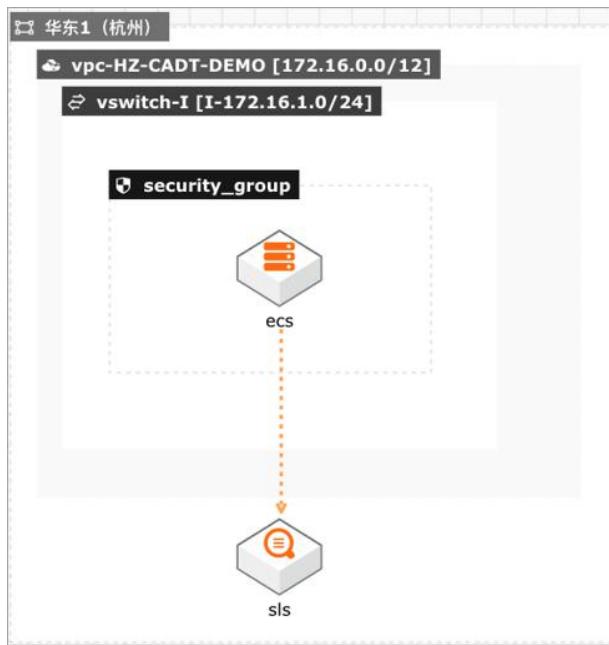
配置 vpc：



配置 vswitch:



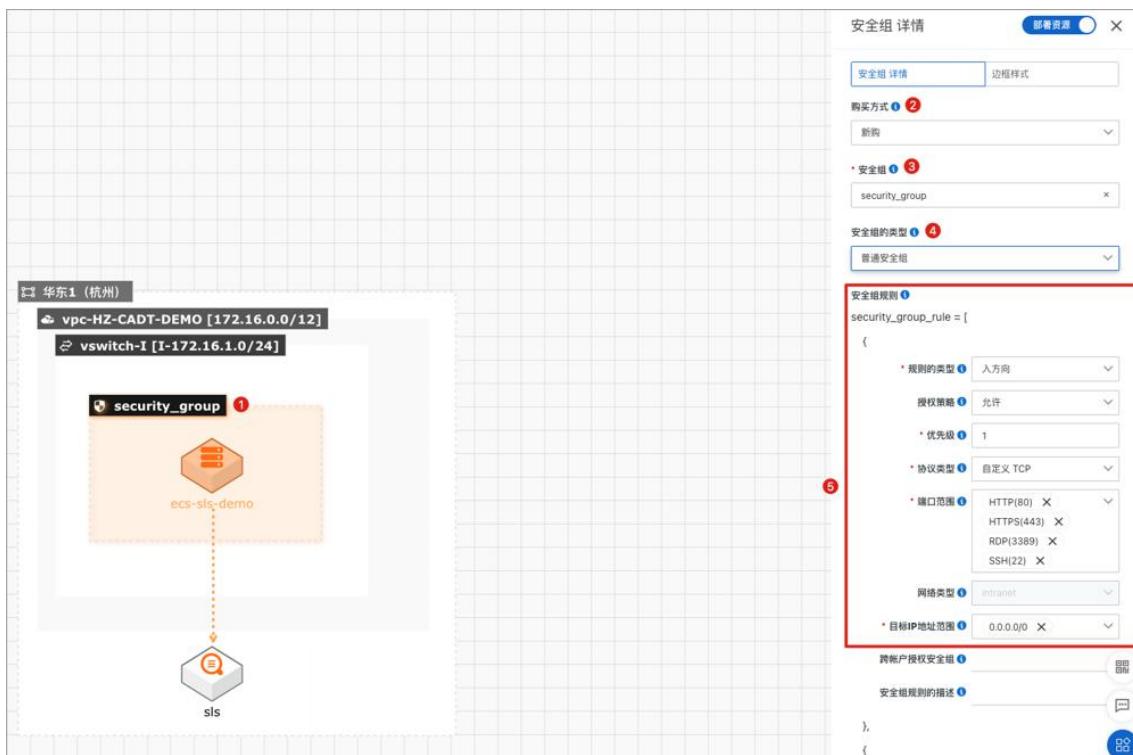
步骤 5 在画布区域调整 region、vpc、vswitch 图层到合适大小后，分别从左侧产品列表中选择安全组、ECS、SLS 拖入对应区域中（参考 1.1，根据架构资源级别）



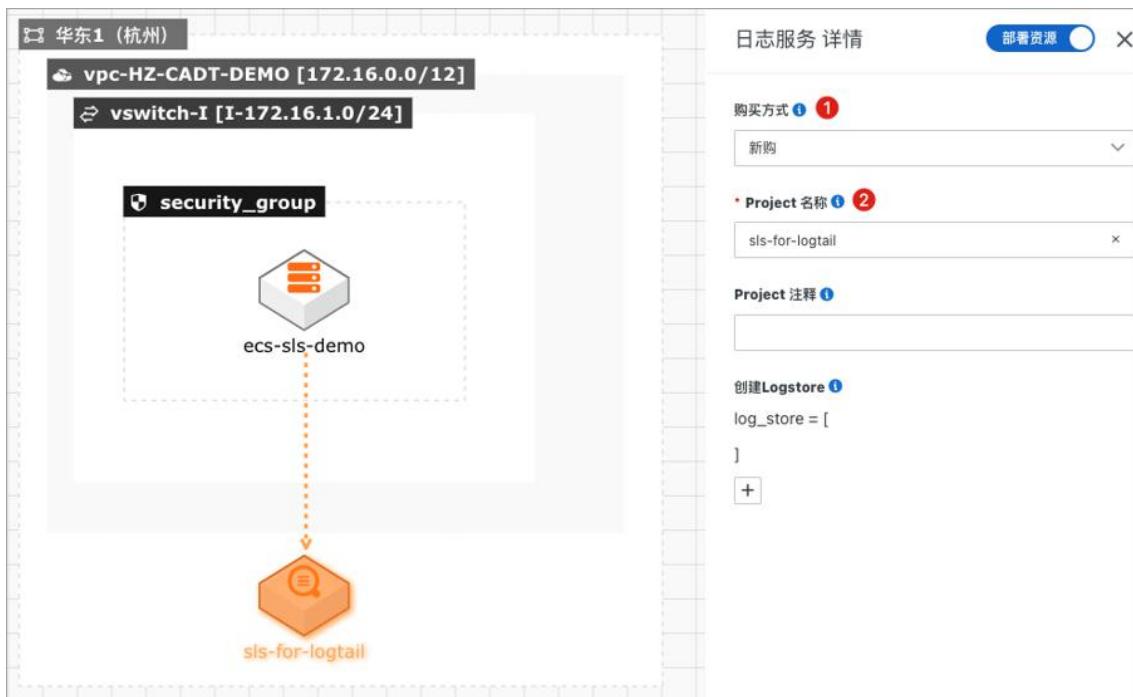
步骤 6 双击 ECS 配置实例信息，ECS 实例信息如下：

配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs-sls-demo
数量	1
支付方式	按量付费
实例规格	ecs.g6.xlarge(4c 16g)
镜像	CentOS
镜像版本	CentOS 7.6 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
公网 IP	分配公网 IPv4 地址
宽带计费模式	按流量付费
带宽（峰）值	10 Mbps
主机名	ecs-sls-demo
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>

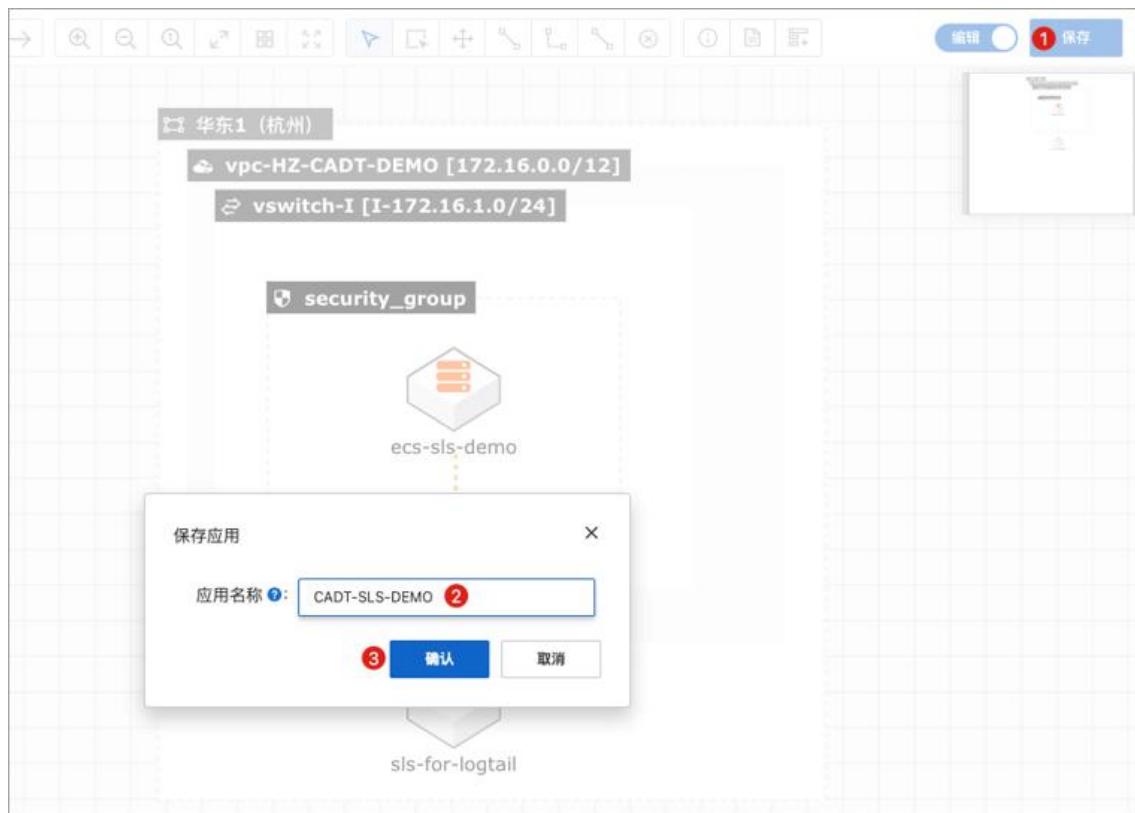
步骤 7 双击安全组，配置安全组策略，放行 22、80、443 端口



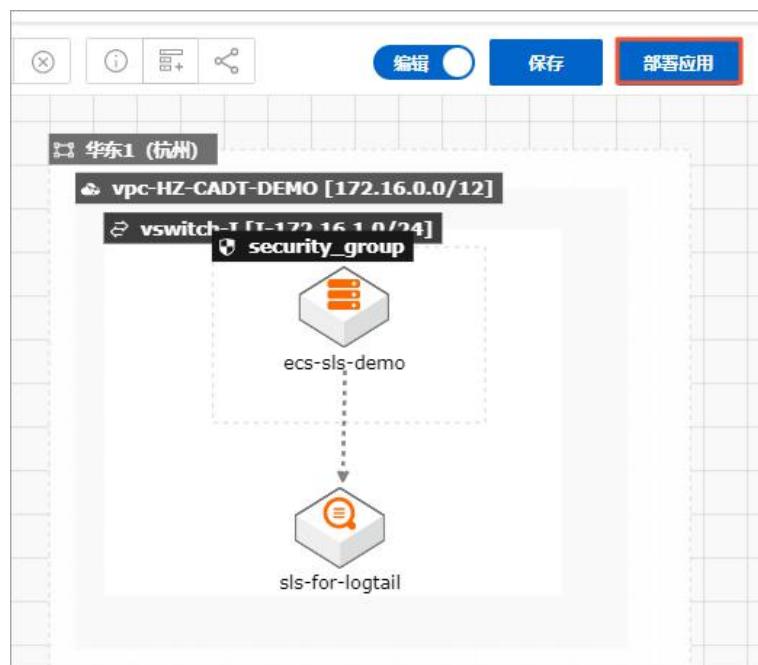
步骤 8 双击 SLS 完成实例配置。



步骤 9 配置完成后，单击**保存**，输入应用名称。



步骤 10 单击**部署应用**。



步骤 11 等待资源校验成功，单击下一步：价格清单。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vpc-HZ-CADT-DEMO [172.16.0.0/12]	vpc	杭州	172.16.0.0/12	成功	校验通过	定位
2	ecs-sls-demo	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
3	security_group	security.group	杭州	normal	成功	校验通过	定位
4	vswitch-I [1-172.16.0.0/24]	vswitch	杭州	172.16.1.0/24	成功	校验通过	定位
5	sls-for-logtail	sls	杭州		成功	校验通过	定位

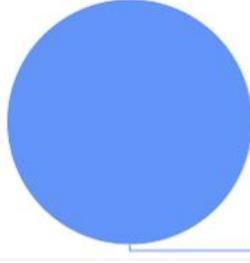
状态:校验成功

**下一步: 价格清单** 返回

**导出价格清单**

免费 包年包月 **按量付费**

资源成本占比



资源预算  
● 计算 计算: 10 元/时

10...

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	ecs-sls-demo	ecs	杭州	ecs.g6.xlarge	1	1 元/时	省 10%	( 1 元/时)	定位

状态: 计价成功

上一步: 资源校验 查看报告 **下一步: 确认订单**

**确认订单**

免费	包年包月	按量付费							
序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
1	sls-for-logtail	sls	杭州	-	1	-	-	-	新购

《云速搭服务条款》  
部署前, 请阅读并勾选服务条款 ①

按量付费: 1.00 元/时

状态: 计价成功 ② 上一步: 价格清单 ③ 下一步: 支付并创建

步骤 12 单击**查看报告**, 可以导出应用架构方案部署报告。

**资源部署状态**

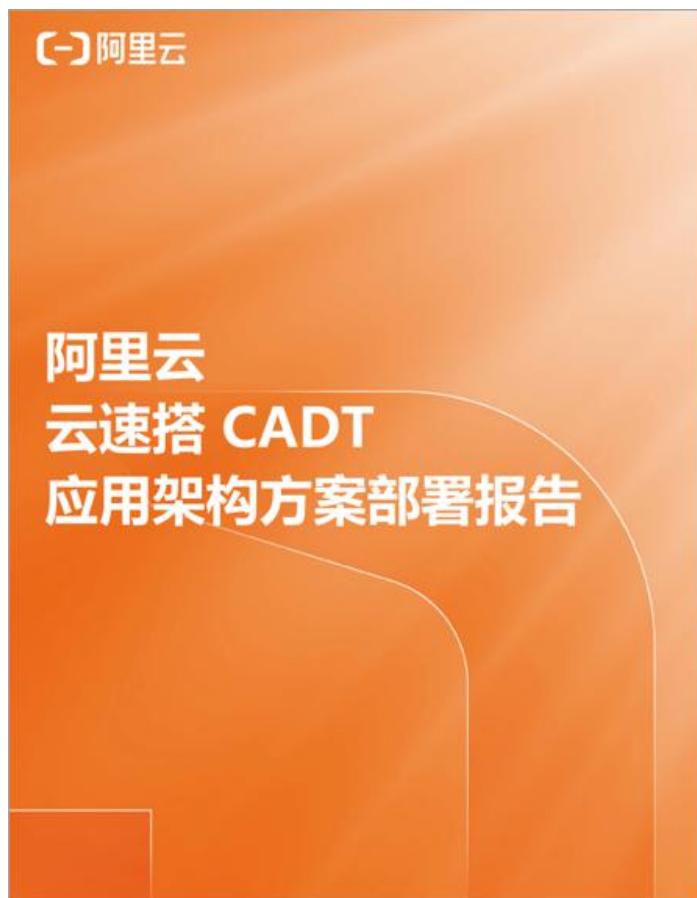
序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-HZ-CADT-DEMO [172.16.0.0/12]	vpc (专有网络VPC)	-	vpc-bp1 3qt9n	运行中	2021-12-02 11:36:19	定位
2	sls-for-logtail	sls (日志服务)	按量付费	sls-bp1 3h77ac	运行中	2021-12-02 11:36:19	定位
3	vswitch-l [1-172.16.1.0/24]	vswitch (虚拟交换机)	-	vsw-bp1 3h77ac	运行中	2021-12-02 11:37:10	定位
4	security_group	security.group (安全组)	-	sg-bp1 3h77ac	运行中	2021-12-02 11:36:19	定位

每页显示 10 共5条 < 上一页 ④ 1 下一页 >

**部署概要**

状态: 部署成功 方案编号: 1GO4YIY8YKAPXDO8 ⑤

**查看报告** ⑥ 返回

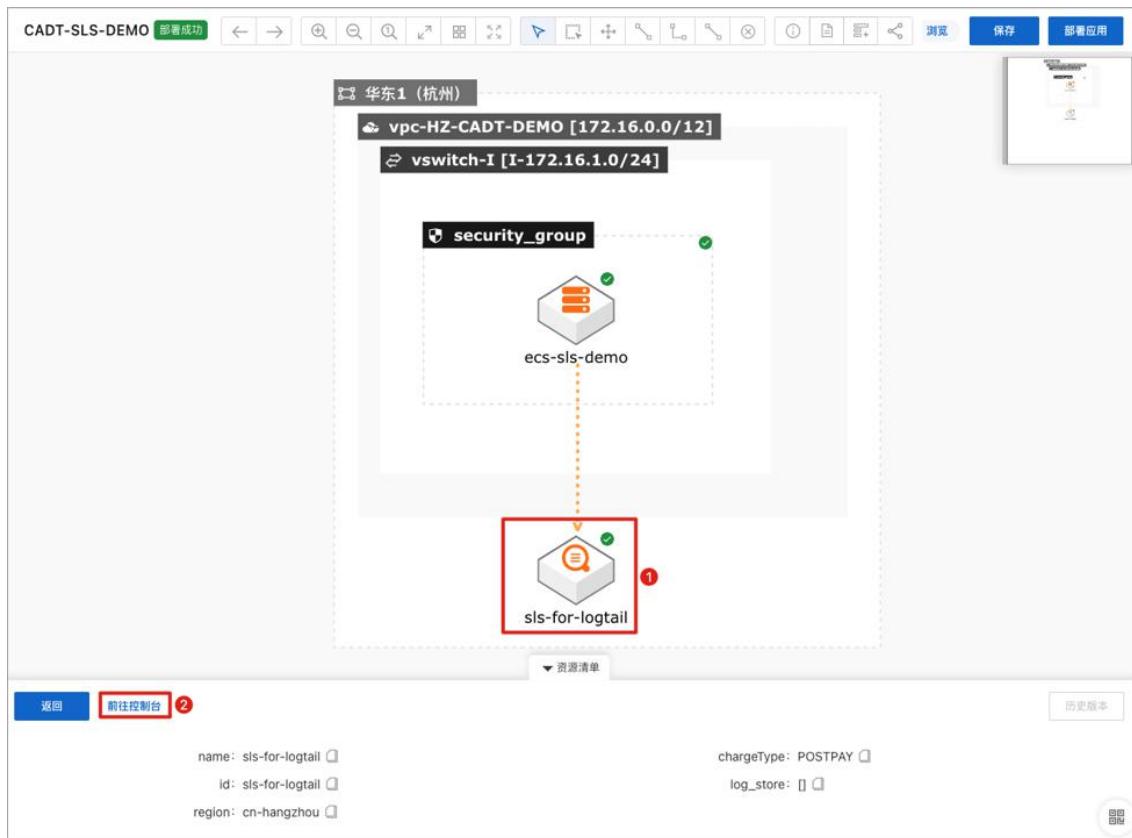


### 4.5.3. Logtail 日志采集处理分析

#### 4.5.3.1. 创建日志服务 Project 和 Logstore

步骤 1 在 CADT 中双击 sls-for-logtail，在下方资源清单单击前往控制台。

(后续所有步骤中，进入实例控制台，均通过此方法，不再赘述)



## 步骤 2 创建 Logstore。

1. 展开左侧日志存储功能栏，在日志库页签下，单击添加图标。



2. 在创建 Logstore 对话框中，将 Logstore 名称设置为 demo-access-log-store，并单击确认。

**说明：**创建 Logstore 用于保存第三方云服务器接入日志。



3. 在创建成功对话框中，单击取消。



成功创建日志库，您可以在日志库列表中看到新建的日志库(**demo-access-log-store**)。



步骤3 为 demo-access-log-store 日志库开启索引。

1. 在日志库列表中，单击 demo-access-log-store，进入日志库。
2. 在 demo-access-log-store 日志库页面，单击开启索引。



3. 在查询分析侧边页，单击确定。



4. 在查询分析设置对话框中，单击确定。



成功开启 demo-access-log-store 日志库的索引。

### 4.5.3.2. 安装 Logtail 日志采集客户端

步骤 1 登录 ECS 服务器 (ecs-sls-demo)，运行如下命令，下载 Logtail 安装文件。

```
wget  
http://logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com/linux64/logtail.sh  
-O logtail.sh; chmod 755 logtail.sh;
```

```
[root@ecs-sls-demo ~]# wget http://logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com/linux64/logtail.sh -O logtail.sh; chmod 755 logtail.sh;  
--2021-12-03 13:59:56-- http://logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com/linux64/logtail.sh  
Resolving logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com (logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com)... 106.14.229.15  
Connecting to logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com (logtail-release-cn-shanghai.oss-cn-shanghai.aliyuncs.com)|106.14.229.15|:80... connected.  
.HTTP request sent, awaiting response... 200 OK  
Length: 31141 (30K) [application/x-sh]  
Saving to: 'logtail.sh'  
  
100%[=====] 31,141 --.-K/s in 0.008s  
2021-12-03 13:59:56 (3.72 MB/s) - 'logtail.sh' saved [31141/31141]  
  
[root@ecs-sls-demo ~]# ls  
logtail.sh
```

步骤 2 运行以下命令，安装 Logtail。

```
./logtail.sh install cn-hangzhou-internet
```

```

2021-11-02 21:00:18 (20.7 MB/s) - 已保存 "logtail-linux64.tar.gz" [27355227/27355227]
logtail-linux64.tar.gz download success
install logtail files success
agent stub for telegraf has been installed
systemd 219
+PAM +AUDIT +SELINUX +IMA -APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL +XZ +LZ4 -SECCOMP +BLKID
+ELFUTILS +KMOD +IDN
use systemd for startup
Created symlink from /etc/systemd/system/default.target.wants/iologtailed.service to /etc/systemd/system/iologtailed.service
.
systemd startup done
ilogtail is running
install logtail success
start logtail success
{
    "UUID" : "3574949A-7548-4463-AF2D-137C146CAA46",
    "hostname" : "ecs-logtail", (for 内部 GTM) v2.2 20190605.pptx
    "instance_id" : "D55F1C44-3BDC-11EC-A9A6-00163E19B66D_192.168.10.3_1635858020",
    "ip" : "192.168.10.3",
    "logtail_version" : "1.0.25",
    "os" : "Linux; 3.10.0-957.21.3.el7.x86_64; #1 SMP Tue Jun 18 16:35:19 UTC 2019; x86_64",
    "update_time" : "2021-11-02 21:00:20"
}
  基于 Elasticsearch 的日志采集与分析-20211015.docx

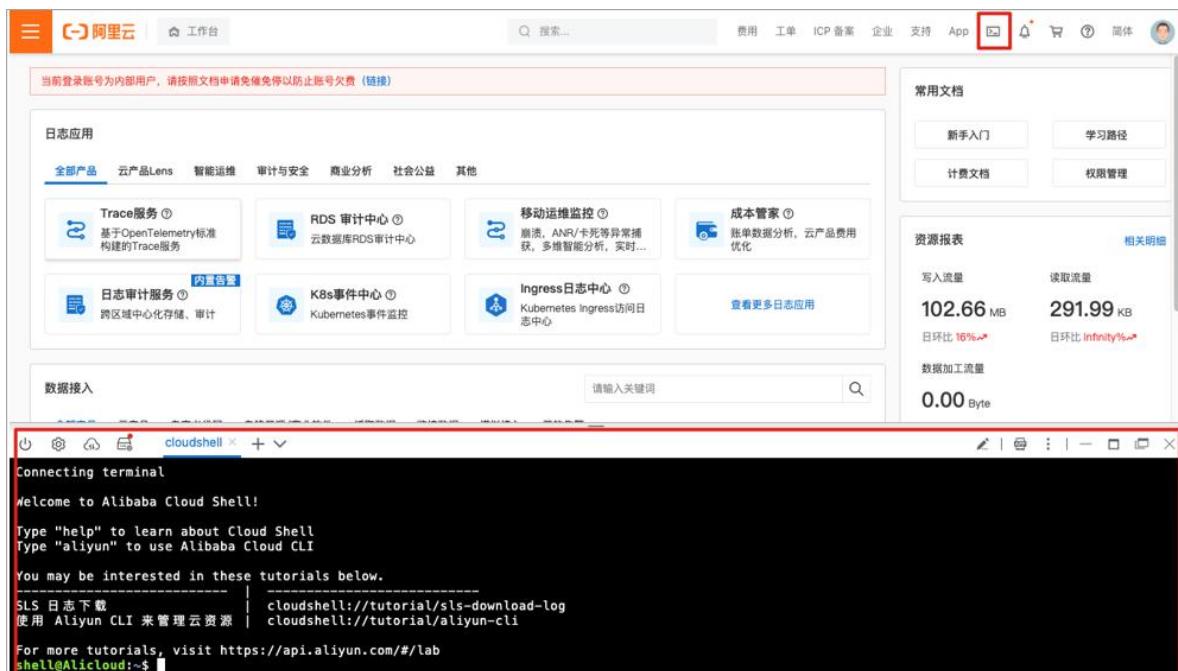
```

### 4.5.3.3.配置主账号 AliUid

查看主账号 AliUid：

步骤 1 登录阿里云日志服务控制台。（<https://sls.console.aliyun.com/lognext/profile>）

步骤 2 单击下图所示标识进入 Cloud Shell 界面。



步骤3 运行以下命令，获取主账号 AliUid。

```
echo $ALIBABA_CLOUD_ACCOUNT_ID
```

```
shell@Alicloud:~$ echo $ALIBABA_CLOUD_ACCOUNT_ID
179***:590
```

步骤4 登录第三方云服务器，配置主账号 AliUid 作为用户标识。

```
touch /etc/ilogtail/users/1*****
```

```
[root@ecs-sls-demo ~]# touch /etc/ilogtail/users/1*****
[root@ecs-sls-demo ~]#
```

#### 4.5.3.4.配置接入日志库

创建机器组：

步骤1 进入 sls-for-logtail Project。

展开左侧**机器组**功能栏，并选择**创建机器组**。

**说明：**创建机器组用于接收采集模式的配置信息。

步骤 2 在创建机器组对话框中，完成以下配置，并单击确认。

首选在云服务器执行命令获取 IP 地址：

```
cat /usr/local/ilogtail/app_info.json
```

```
[root@ecs-sls-demo ~]# cat /usr/local/ilogtail/app_info.json
{
    "UUID" : "A[REDACTED]5F6",
    "hostname" : "ecs-sls-demo",
    "instance_id" : "4[REDACTED]17E_172.16.1.149_16385
11223",
    "ip" : "172.16.1.149",
    "logtail_version" : "1.0.25",
    "os" : "Linux; 3.10.0-957.21.3.el7.x86_64; #1 SMP Tue Jun 18 16:35:19 UT
C 2019; x86_64",
    "update_time" : "2021-12-03 14:00:23"
}
[root@ecs-sls-demo ~]#
```

配置项	说明
机器组名称	demo-log-group
机器组标识	IP 地址*
IP 地址	在云服务器执行命令 cat /usr/local/ilogtail/app_info.json 获取 IP 地址



\*注：

1.由于本实践仅有一台云服务器，因此**机器组配置**里使用了**IP 地址**作为**机器组标识**，在 VPC 等自定义网络环境或者有多台服务器需要进行弹性伸缩的场景下，建议使用**用户自定义标识**作为**机器组标识**

2.关于**用户自定义标识**的配置，请查阅阿里云官网文档：

[https://help.aliyun.com/document\\_detail/28983.html](https://help.aliyun.com/document_detail/28983.html)

成功创建机器组，您可以在**机器组**列表中看到新建的机器组（**demo-log-group**）。

The screenshot shows the SLS Logtail interface. On the left, there's a sidebar with icons for clock, list, heart rate, and cube. The main area has a title bar with 'sls-for-logtail' and '切换'. Below it, there's a search bar with placeholder 'demo-access...'. Underneath, there's a section titled 'Machine Group' with a sub-section 'demo-access-log-store'. A red box highlights the 'demo-log-group' entry. To the right, there's a log viewer with a query editor containing the SQL: '1 \* | select Status,count(1) as c group by Status order by c desc'. The results table shows 4 rows. At the bottom, there's a footer with '日志总条数: 0' and '查询状态: 结果精确'.

步骤 3 在日志存储功能栏，展开 demo-access-log-store 日志库菜单，并单击添加图标。

The screenshot shows the SLS Logtail interface. On the left, there's a sidebar with icons for clock, list, heart rate, and cube. The main area has a title bar with 'sls-for-logtail' and '切换'. Below it, there's a search bar with placeholder '搜索logstore'. Underneath, there's a section titled '日志库' with a sub-section 'demo-access-log-store'. A red box highlights the '数据接入' item under the 'demo-access-log-store' menu. Another red box highlights the '+' icon at the top right of the '日志库' menu. The menu also includes other items like 'logtail配置', '数据导入', '模拟接入', '数据处理', '加工', '快速查询', '告警', '导出', and '数据消费'.

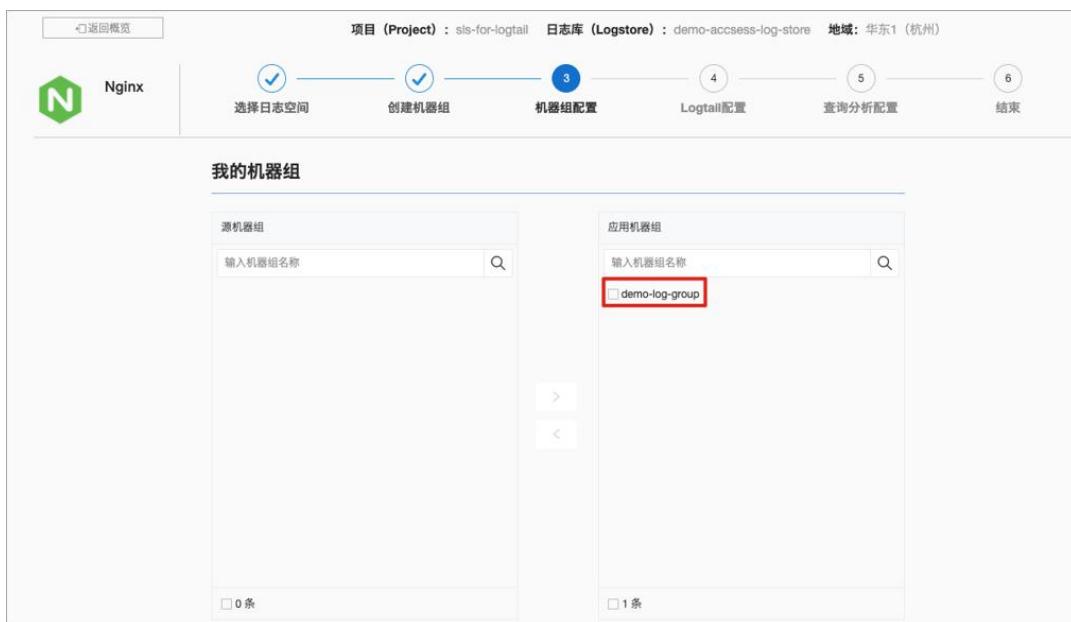
步骤 4 在**接入数据**对话框中，选择**Nginx-文本日志**，单击图标进入 Nginx 数据接入配置向导。



步骤 5 在创建机器组向导页，单击使用现有机器组。



步骤 6 在机器组配置向导页，选择应用 demo-log-group 机器组，并单击下一步。



步骤 7 在 **Logtail 配置**向导页，完成以下配置，并单击**下一步**。

配置项	说明
配置名称	accesslog-config
日志路径	/var/log/nginx access.log*（通配符匹配所有 access log）
模式	NGINX 配置模式
NGINX 日志配置	main 格式
丢弃解析失败数据	开启

NGINX 日志配置：

```
log_format main '$remote_addr - $remote_user [$time_local] "$request"
'$request_time $request_length '
'$status $body_bytes_sent "$http_referer"
'"$http_user_agent"';
```

日志样例：

```
106.11.31.2 - - [23/Sep/2021:16:15:29 +0800] "GET /nginx-logo.png HTTP/1.1" 200 368
"http://123.56.121.18/abc.test" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36" "-"
```

### 注意：

- 1.日志服务会自动读取您的 NGINX 键；
- 2.**NGINX 配置模式**请匹配您的原始日志格式，一定要注意**空格和单、双引号**；
- 3.对于单行/多行日志的采集解析支持，logtail 提供了完整正则模式，可以参考：  
<https://yq.aliyun.com/articles/680070>

Nginx

选择日志空间

创建机器组

机器组配置

Logtail配置

5

6

查询分析配置

结束

\* 配置名称:

[导入其他配置](#)

\* 日志路径:  /.../

指定文件夹下所有符合条件的文件都会被监控到(包含所有层次的目录)，文件名称可以是完整名，也支持通配符模式匹配。Linux文件路径只支持“/”开头，例: /tmp/a/b/c/app.log。Windows文件路径只支持盘符开头，例如: C:\Program Files\Intel\...\Log

设置采集屋名称:

黑名单配置可以在采集时根据指定的目录或文件，目录和文件名可以是完整匹配，也支持通配符模式匹配。比如指定按目录过滤 /tmp/mydir 可以过滤掉该目录下的所有文件，按文件过滤 /tmp/mydir/file 可以过滤掉目录下特定文件，而保留对其他文件的采集。[帮助文档](#)

是否为Docker文件:

如果是Docker容器内部文件，可以直接配置内部路径与容器Tag，Logtail会自动监测容器创建和销毁，并根据Tag进行过滤采集指定容器的日志。具体说明参考 [帮助文档](#)

模式:  NGINX配置模式

\* NGINX日志配置:

```
log_format main '$remote_addr - $remote_user [$time_local] "$request"
$request_time $request_length"
$status $body_bytes_sent "$http_referer"
$http_user_agent';
```

标准NGINX配置文件日志配置部分，通常以log\_format开头 [帮助文档](#)

正则表达式: `(\$[^"]+\"\$[^"]*\")*(\$[^"]+\"\$[^"]*\")*\$[^"]+\"\$[^"]*\")*(\$[^"]+\"\$[^"]*\")*`

\* 日志样例: `106.11.31.2 -- [23/Sep/2021:16:15:29 +0800] "GET /nginx-logo.png HTTP/1.1" 200 368
http://123.56.121.18/abc.test" "Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 "`

填写日志样例来验证您的配置是否匹配

验证成功

校验

✓ 验证成功

NGINX键名称:

Key	Value
remote_addr	106.11.31.2
remote_user	-
time_local	23/Sep/2021:16:15:29
request_method	GET
request_uri	/nginx-logo.png
request_time	200
request_length	368
status	"http://123.56.121.18/abc.test"
body_bytes_sent	
http_referer	Mozilla/5.0 (Macintosh; Intel Mac OS X 11_1_0) /
http_user_agent	-

丢弃解析失败日志:

开启后，解析失败的日志不上传到日志服务；关闭后，日志解析失败时上传原始日志。

最大监控目录深度:  Logtail限制说明请参考 [帮助文档](#)

最大目录监控深度范围0-1000，0代表只监控本层目录

高级选项: 展开 ▼

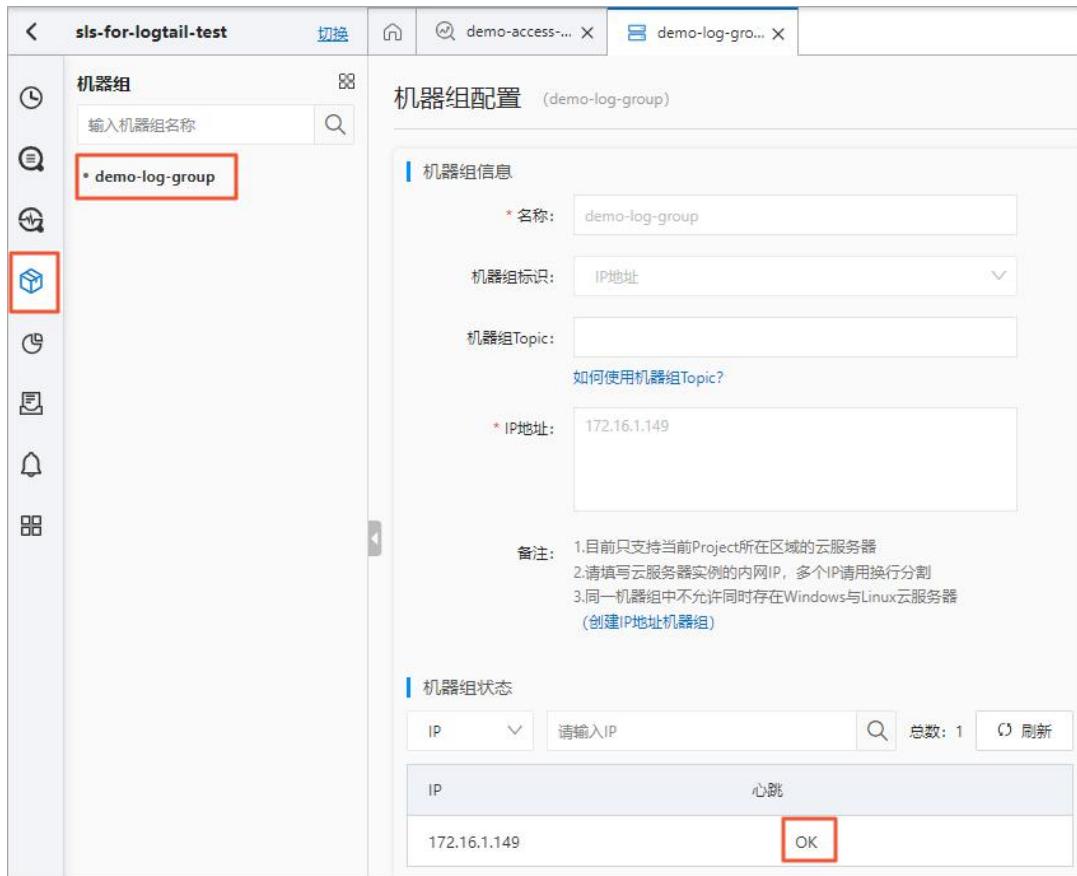
上一步
下一步

步骤 8 在查询分析配置环节，单击下一步。



步骤 9 检查机器组心跳状态。

打开机器组功能栏，查看 **demo-log-group** 机器组的心跳状态。



可以看到机器组心跳状态是 OK。

#### 4.5.3.5. 云服务器上模拟产生 Nginx 文本日志

步骤 1 安装 ruby 和关联包。

执行如下命令，进行安装：

```
yum install ruby
gem sources --add https://gems.ruby-china.com/
gem sources --remove https://rubygems.org/
gem install apache-loggen -v 0.0.5
```

```

Installed:
  ruby.x86_64 0:2.0.0.648-36.el7

Dependency Installed:
  libyaml.x86_64 0:0.1.4-11.el7_0
  ruby-libs.x86_64 0:2.0.0.648-36.el7
  rubygem-io-console.x86_64 0:0.4.2-36.el7
  rubygem-psych.x86_64 0:2.0.0-36.el7
  rubygems.noarch 0:2.0.14.1-36.el7

Complete!
[root@ecs-sls-demo ~]# gem sources --add https://gems.ruby-china.com/
https://gems.ruby-china.com/ added to sources
[root@ecs-sls-demo ~]# gem sources --remove https://rubygems.org/
https://rubygems.org/ removed from sources
[root@ecs-sls-demo ~]# gem install apache-loggen -v 0.0.5
Fetching: apache-loggen-0.0.5.gem (100%)
Successfully installed apache-loggen-0.0.5
Parsing documentation for apache-loggen-0.0.5
Installing ri documentation for apache-loggen-0.0.5
1 gem installed
[root@ecs-sls-demo ~]#

```

## 步骤 2 启动日志发生器

### 1. 安装 git

```
yum install -y git
```

### 2. 下载日志发生器

```
git clone https://code.aliyun.com/best-practice/cadt-sls.git
```

```

[root@ecs-sls-demo ~]# git clone https://code.aliyun.com/best-practice/cadt-sls.git
Cloning into 'cadt-sls'...
remote: Counting objects: 4, done.
remote: Total 4 (delta 0), reused 0 (delta 0)
Unpacking objects: 100% (4/4), done.
[root@ecs-sls-demo ~]# ls
cadt-sls  logtail.sh
[root@ecs-sls-demo ~]#

```

### 3. 解压

```

cd cadt-sls/log-gen
tar zxvf nginx-log-generator-master.tar.gz

```

### 4. 执行以下命令，启动日志发生器

```
mv nginx-log-generator-master /root/  
cd /root/nginx-log-generator-master  
.start_log_generator.sh
```

```
[root@ecs-sls-demo ~]# cd /root/nginx-log-generator-master/  
[root@ecs-sls-demo nginx-log-generator-master]# ./start_log_generator.sh
```

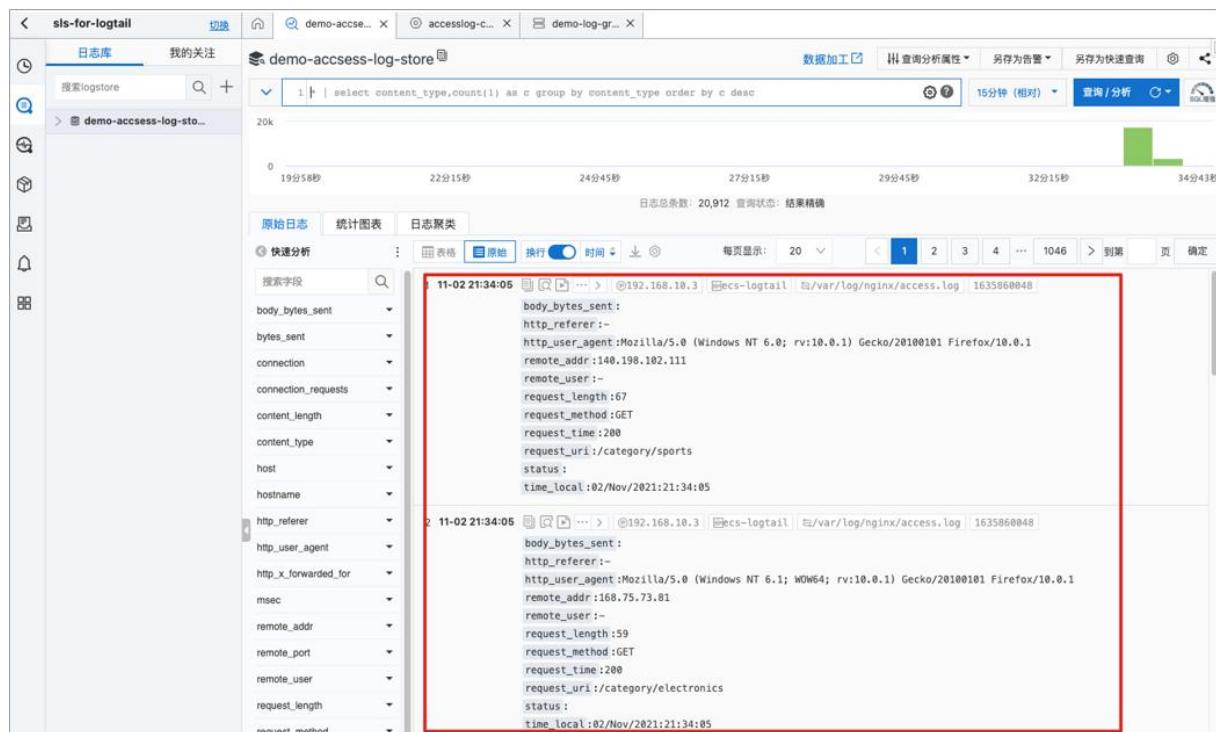
### 步骤3 停止日志发生器。

日志发生器稍微执行数分钟，执行以下命令停止日志发生器。

```
./stop_log_generator.sh
```

```
[root@ecs-sls-demo nginx-log-generator-master]# ./stop_log_generator.sh  
[root@ecs-sls-demo nginx-log-generator-master]#
```

### 步骤4 查看日志库已接收到的日志正确解析发送到 SLS。

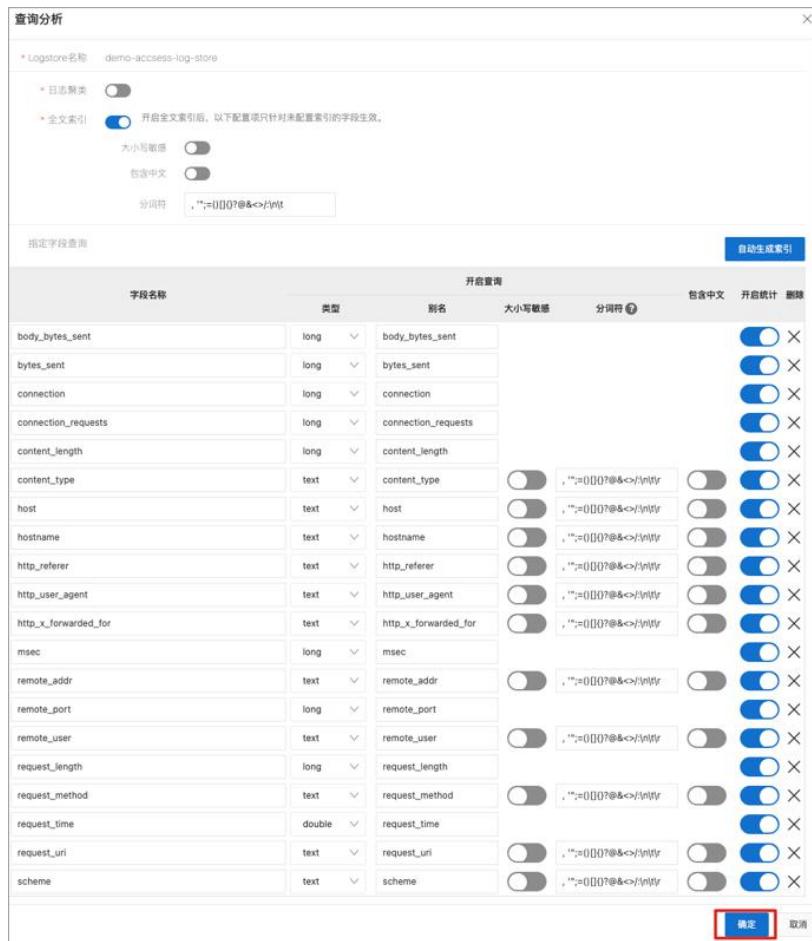


### 4.5.3.6. 通过日志服务仪表盘进行可视化分析

步骤 1 登录日志服务控制台，进入 Project sls-for-logtail。

步骤 2 进入日志目标库（**demo-access-log-store**），选择时间段（确保该时间段内有日志），在查询分析属性进行索引设置。

步骤 3 可以看到**指定字段查询**已经自动按照 Nginx 模版配置好了，并单击**确定**。



**注意：**查询分析设置的**修改操作**只会对**新写入的数据**生效，如果您需要提前对查询分析设置的某些字段分析统计生效，请使用**指定字段查询的自定义**方式在日志写入到日志库之前进行开启统计查询。

步骤 4 再次启动日志发生器和停止日志发生器。

执行以下命令，启动日志发生器。

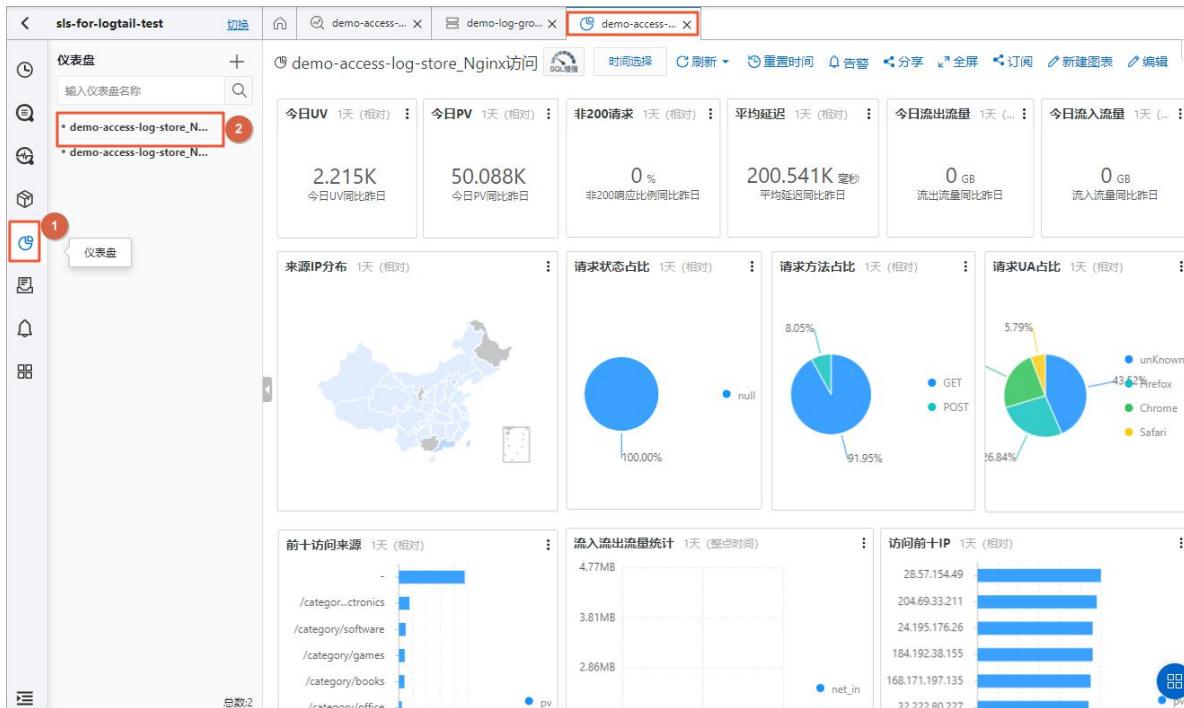
```
cd /root/nginx-log-generator-master
./start_log_generator.sh
```

```
[root@ecs-sls-demo nginx-log-generator-master]# ./start_log_generator.sh
[root@ecs-sls-demo nginx-log-generator-master]#
```

### 步骤 5 查询可视化仪表盘。

进入 **demo-access-log-store** 日志库，单击**仪表盘**查询系统自动帮您生成的仪表盘，当然您也可以根据自己的需要自定义仪表盘，本实践不再赘述。

This screenshot shows the SIS log analysis interface. On the left, there's a sidebar with various icons and a search bar. The '仪表盘' (Dashboard) icon is highlighted with a red box. In the main area, a search result for 'demo-access-log-store' is displayed, with another red box highlighting the '仪表盘' link under the '日志库' (Log Store) section.



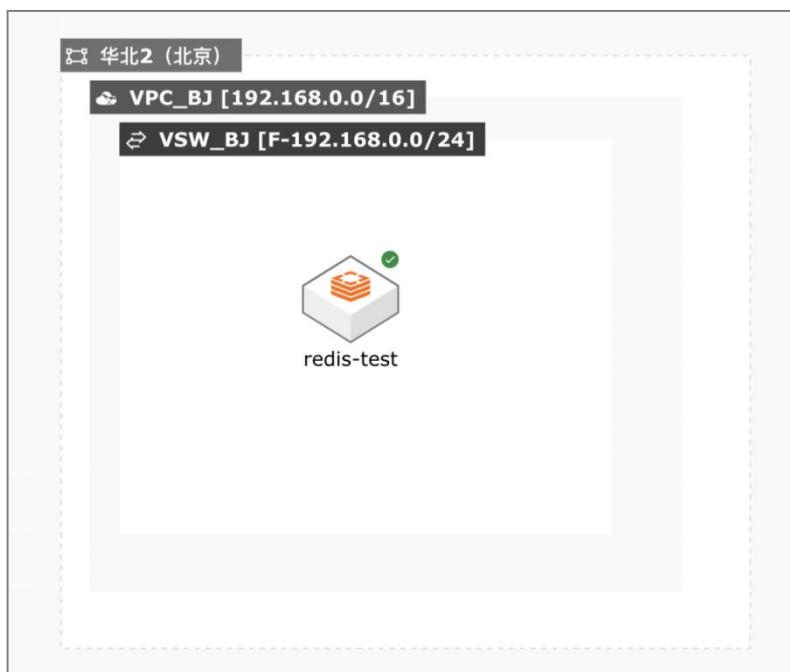
## 4.6. 云速搭部署 Redis 应用

作者 | 阿里云解决方案架构师 袁影

### 4.6.1. 云速搭架构设计入门

#### 方案架构

通过云速搭实现一个云数据库 Redis 的产品实例，其中产品的选型请参考文档：  
[https://help.aliyun.com/document\\_detail/223808.html](https://help.aliyun.com/document_detail/223808.html)。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
Redis	VSW

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

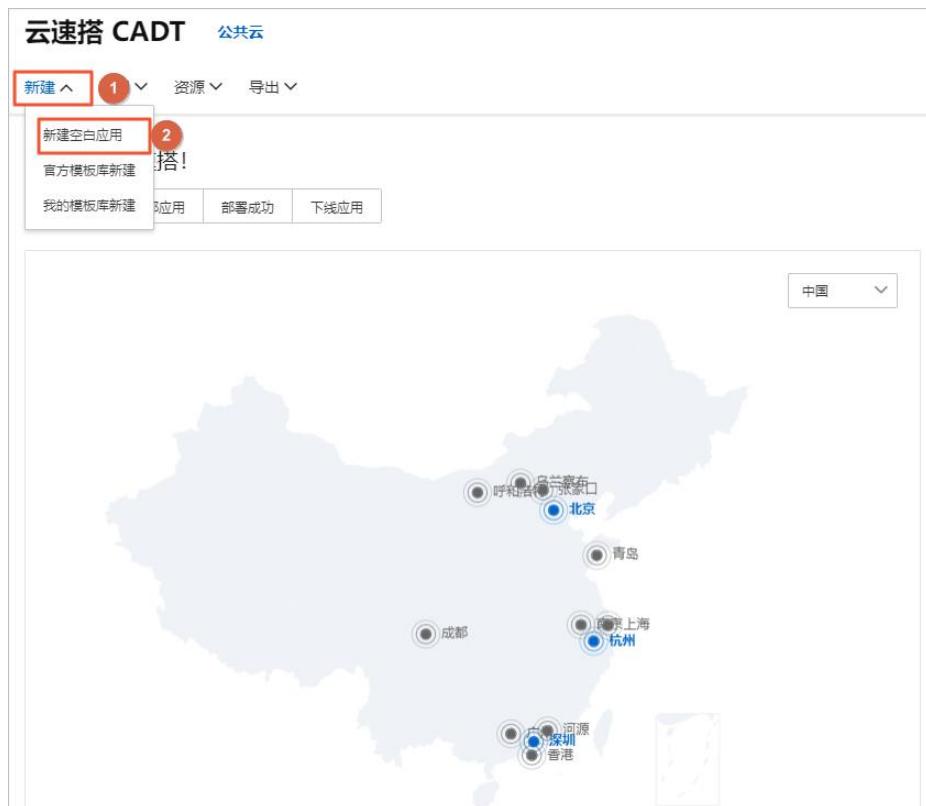
资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC_BJ	192.168.0.0/16
AZ	VSW_BJ	可用区 F 区, 192.168.0.0/24

## 4.6.2.应用架构设计

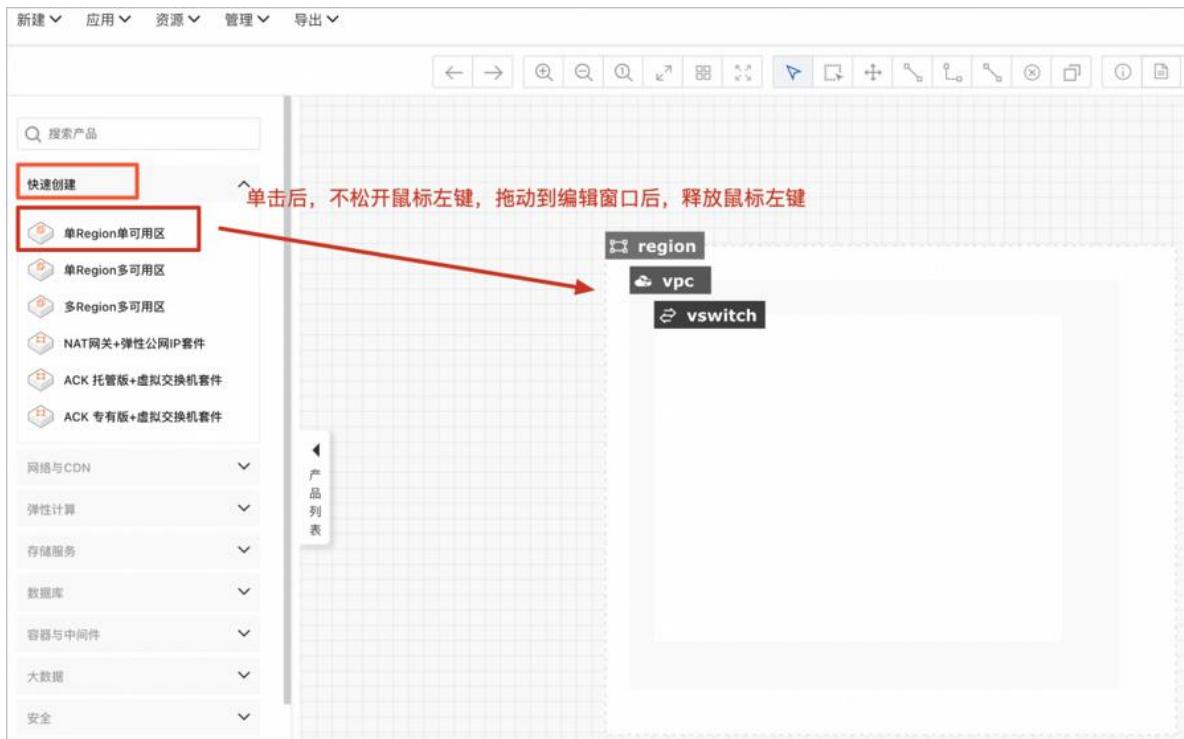
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤3 从左侧产品列表的**快速创建**分类下，找到单Region单可用区，单击后拖入到画布区域中，松开鼠标左键。

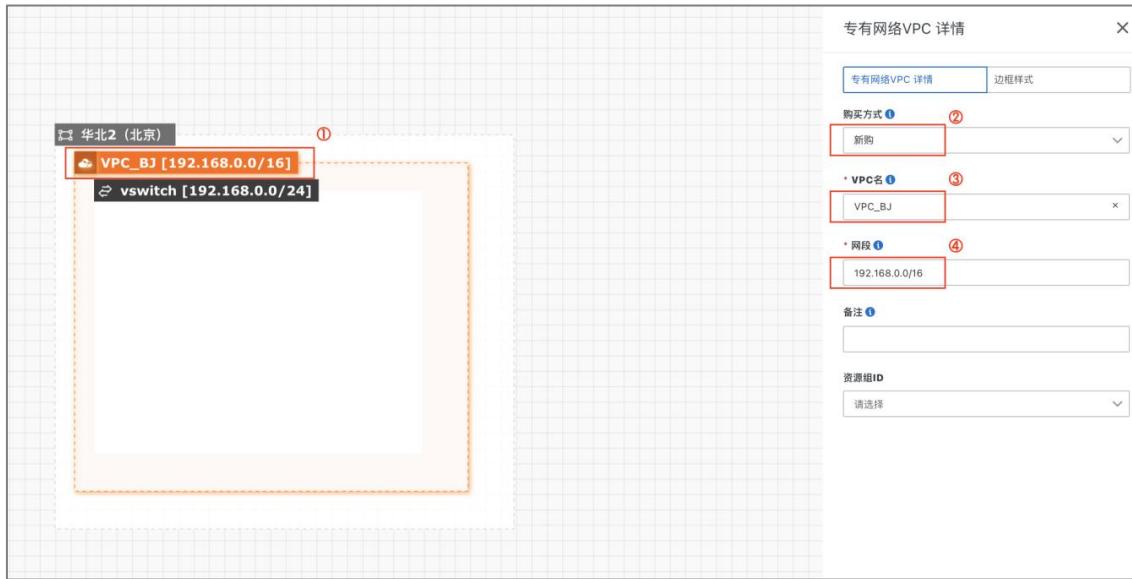


步骤4 依次双击 Region、VPC、vswitch 进行配置。

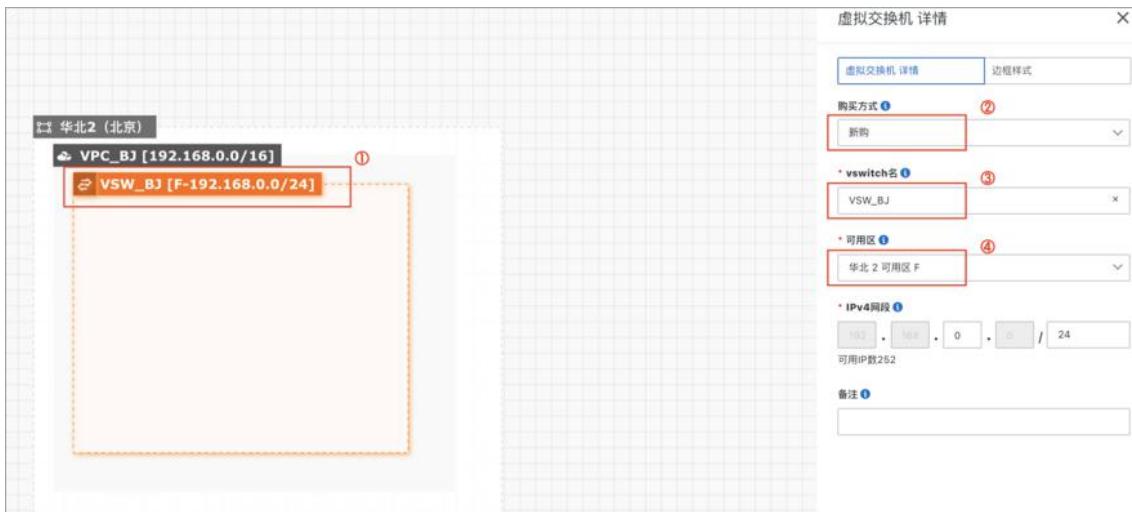
1. 双击 region，在右侧弹出窗口中，选择华北2（北京）。



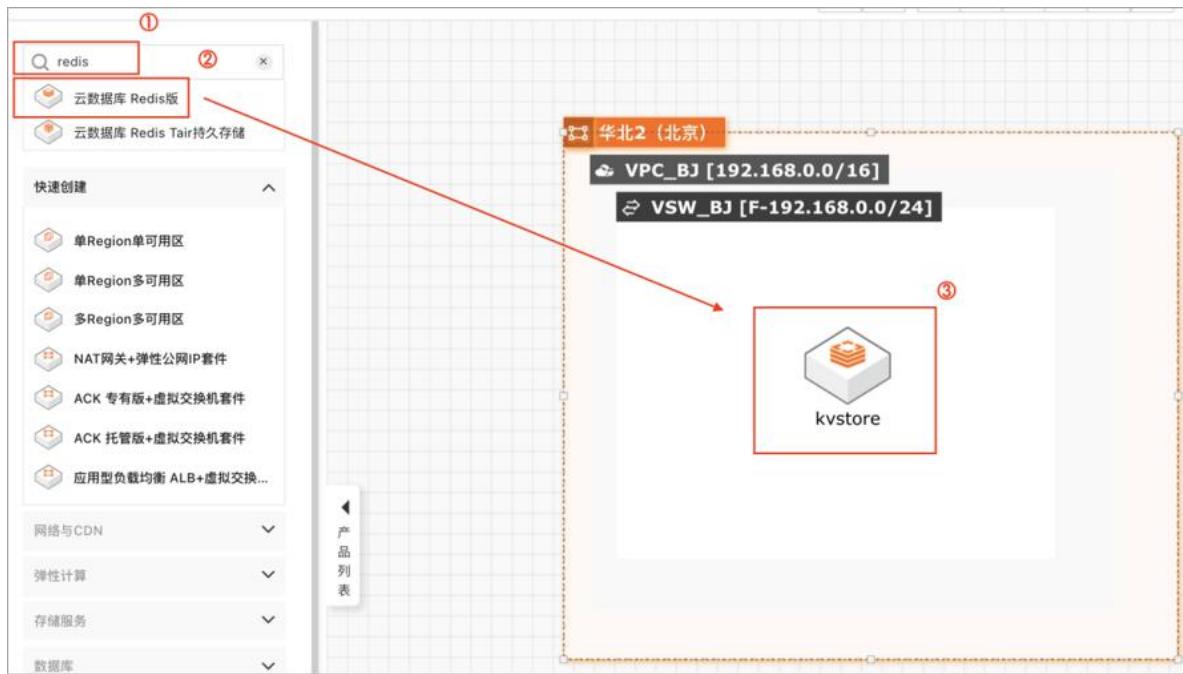
2. 双击 VPC，配置 VPC 参数。



3. 双击 vswitch，配置 vswitch 参数，可用区选择：华北 2 可用区 F。



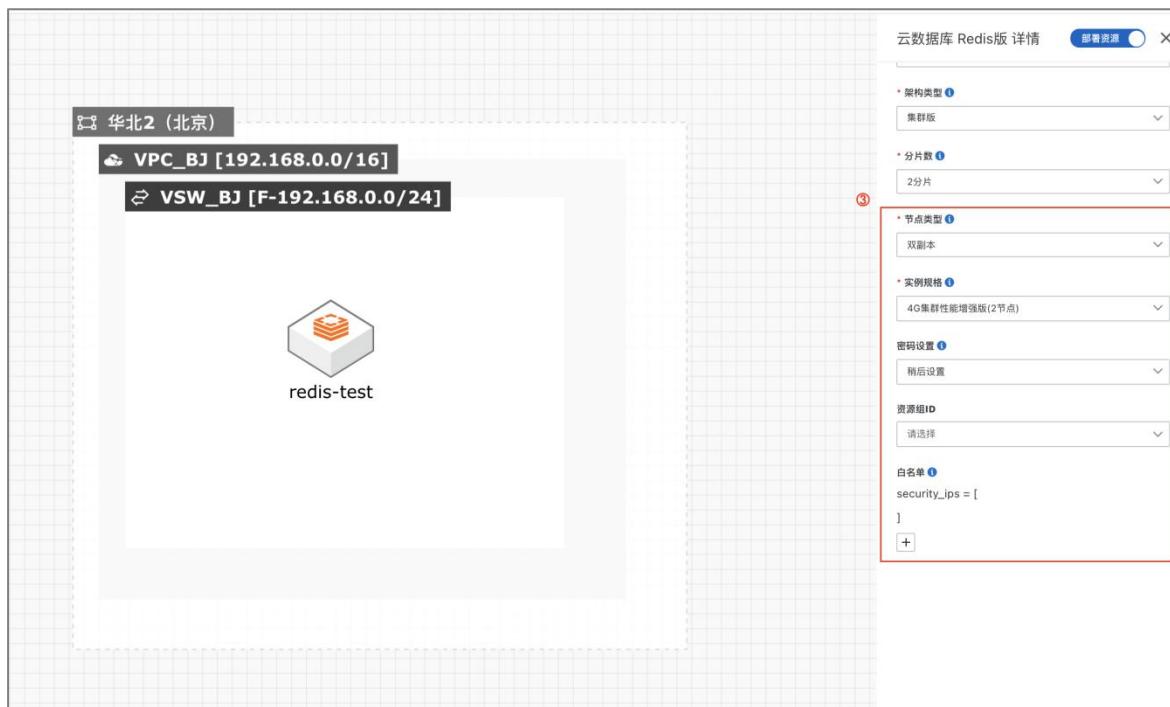
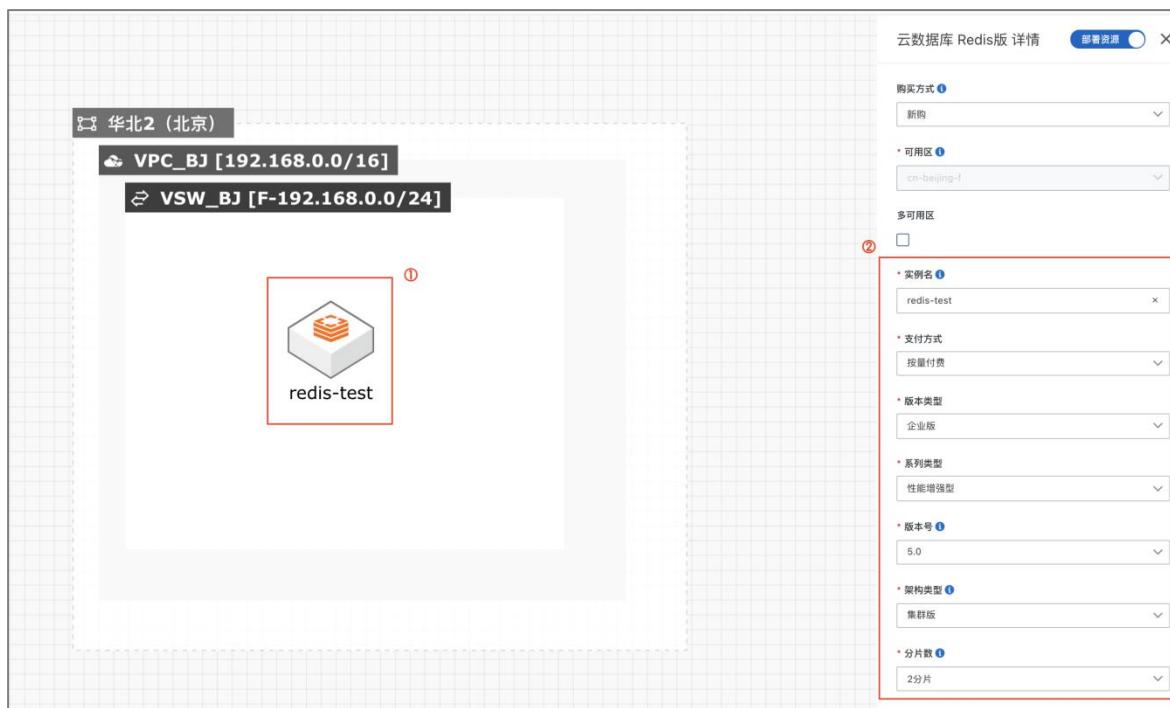
步骤 5 在左侧搜索框中输入 redis，选定 redis 图元，拖动到 VSW\_BJ 中。



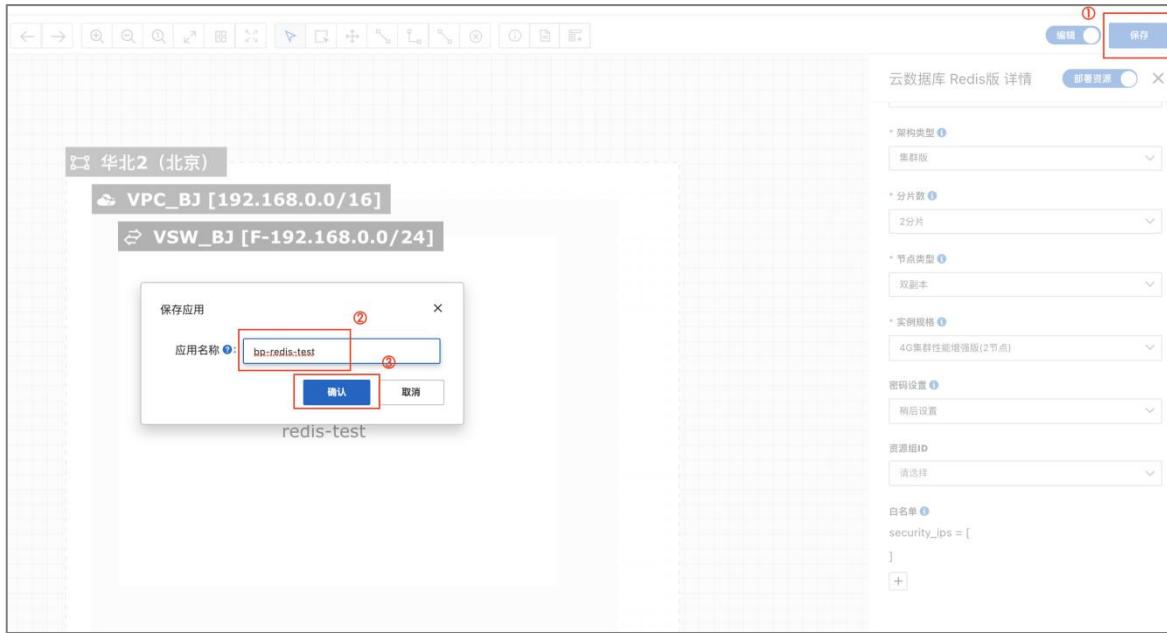
### 4.6.3.配置资源参数

步骤 1 双击 redis 图标，参考下表进行参数配置。

配置项	参数说明
实例名	redis-test
支付方式	按量付费
版本类型	企业版
系列类型	性能增强型
版本号	5.0
架构类型	集群版
分片数	2 分片
节点类型	双副本
实例规格	4G 集群性能增强版(2 节点)
密码设置	稍后设置

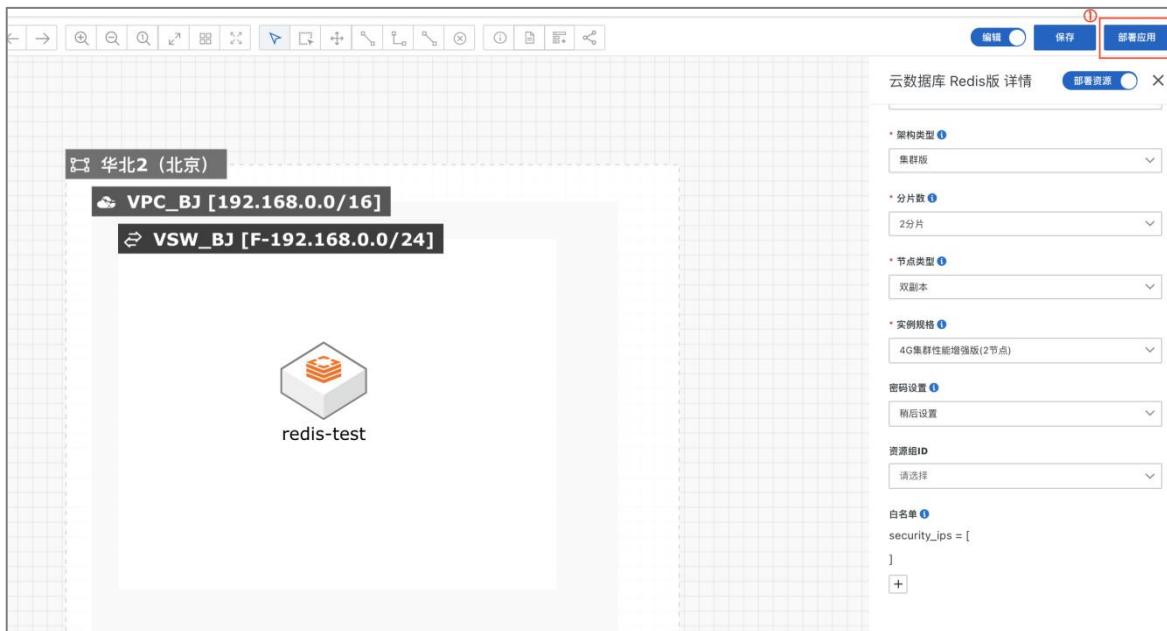


步骤 2 完成以上资源配置后，单击**保存**，并设置**应用名称**，最后单击**确认**。



#### 4.6.4. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、Redis 是否有库存等，一般需要十几秒左右。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	redis-test	kvstore	北京	4G集群性能增强版 (2节点) (QPS:480000 Connections:60000)	成功	校验通过	定位
2	VPC_BJ [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
3	VSW_BJ [F-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位

状态: **校验成功**

① **下一步: 价格清单** 返回

步骤 3 等待校验成功，单击**下一步: 价格清单**。这里会拉取应用所有配置的价格信息。

**导出价格清单**

**免费** **按量付费**

**资源成本占比**

资源预算  
● 数据库 数据库: 10... 元/时

**价格列表**

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	redis-test	kvstore	北京	4G集群性能增强版 (2节点) (QPS:480000 Connections:60000)	1	10...	10...	10...	定位

状态: **计价成功**

① **上一步: 资源校验** 查看报告 **下一步: 确认订单**

步骤 4 可以单击**查看报告**，查看应用的价格信息。



步骤 5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

### 确认订单

免费
**按量付费**

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	redis-test	kvstore	北京	4G集群性能增强版（2节点）(QPS:480000 Connections:60000)	1	1.76元/时	1.76 元/时	新购

**《云速搭服务条款》**

部署前，请阅读并勾选服务条款

按量付费：**1.76元/时**
②

状态：**计价成功**
[上一步：价格清单](#)
**下一步：支付并创建**
③

步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

#### 注意：

1. 部署流程一旦开始后，无法取消。
2. 部署时间预计 **5~10 分钟**左右，请耐心等待。

**资源部署状态**

序号	资源名称  	资源类型 	付费类型	资源ID 	资源状态	资源更新时间	定位
1		vpc (专有网络VPC)	-	vpc-2ze6gz0zq73ek3th511w 	运行中	2021-12-06 15:48:18	定位
2		vswitch (虚拟交换机)	-	部署中, 不要进行任何操作, 请耐心等待。 	运行中	2021-12-06 15:48:18	定位

每页显示  共2条 < 上一页 **1** 下一页 >

**部署概要**

状态: 部署中 方案编号: U5NPF6S743HOD99T [返回](#)

步骤 7 部署完成后, 如下图所示。

**资源部署状态**

序号	资源名称  	资源类型 	付费类型	资源ID 	资源状态	资源更新时间	定位
1	VPC_BJ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2ze6gwz0zq73ek3th511w 	运行中	2021-12-06 15:48:18	定位
2	VSW_BJ [F-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze2vlxtnm3zx6wwc43u4 	运行中	2021-12-06 15:48:18	定位
3	redis-test	kvstore (云数据库 Redis版)	按量付费	r-2zeq2fx5z7gomh7jw7 	运行中	2021-12-06 15:55:21	定位

每页显示  共3条 < 上一页 **1** 下一页 >

**部署概要**

状态: 部署成功 订单编号: 211783287110425  
方案编号: U5NPF6S743HOD99T [查看报告](#) [返回](#)

步骤 8 单击**查看报告**, 可以查看本次的部署报告。



步骤 9 单击返回，然后单击资源清单。

带此资源清单									
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC_BJ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-22ed6pew0zq74ek3th51w	新建	运行中	2021-12-06 15:48:18	定位	<a href="#">详情</a> <a href="#">返回</a> <a href="#">变更日志</a> <a href="#">操作</a>
2	VSW_BJ [F-192.168.0.0/24]	vsw (虚拟交换机)	-	vsw-2ze2v0xsm3z8wwc43u4k	新建	运行中	2021-12-06 15:48:18	定位	<a href="#">详情</a> <a href="#">返回</a> <a href="#">变更日志</a> <a href="#">操作</a>
3	redis-test	redis (云数据库 Redis版)	按量付费	r-2zaeqj7t57gpmh7je7	新建	运行中	2021-12-06 15:50:21	定位	<a href="#">详情</a> <a href="#">返回</a> <a href="#">变更日志</a> <a href="#">操作</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。

步骤 10 单击资源名称 **redis-test**，可跳转到对应的控制台。

The screenshot shows the 'Basic Information' tab of a Redis instance named 'redis-test'. Key details include:

- Instance ID: r-2zeq2fx5z7gomh7jw7
- Region: Beijing (可用区 F)
- Network Type: VPC Network
- Version: Redis 5.0 Enterprise
- Max Connections: 60,000
- Bandwidth: 4G (2 nodes)
- Status: Running (绿色)
- Deployment Segment: 未开启 (Not Enabled)

The 'Connection Information' tab lists connection methods:

连接类型	连接地址	端口号 (Port)	操作
直连访问	r-2zeq2fx5z7gomh7jw7.redis.rds.aliyuncs.com	6379	申请连接地址
专有网络			修改连接地址
公网访问			申请连接地址

A note at the bottom says: 提示：请使用以上访问连接串进行实例连接。VIP在业务维护中可能会变化。

## 步骤 11 业务系统使用 Redis

可参考 [https://help.aliyun.com/document\\_detail/151116.html](https://help.aliyun.com/document_detail/151116.html)。

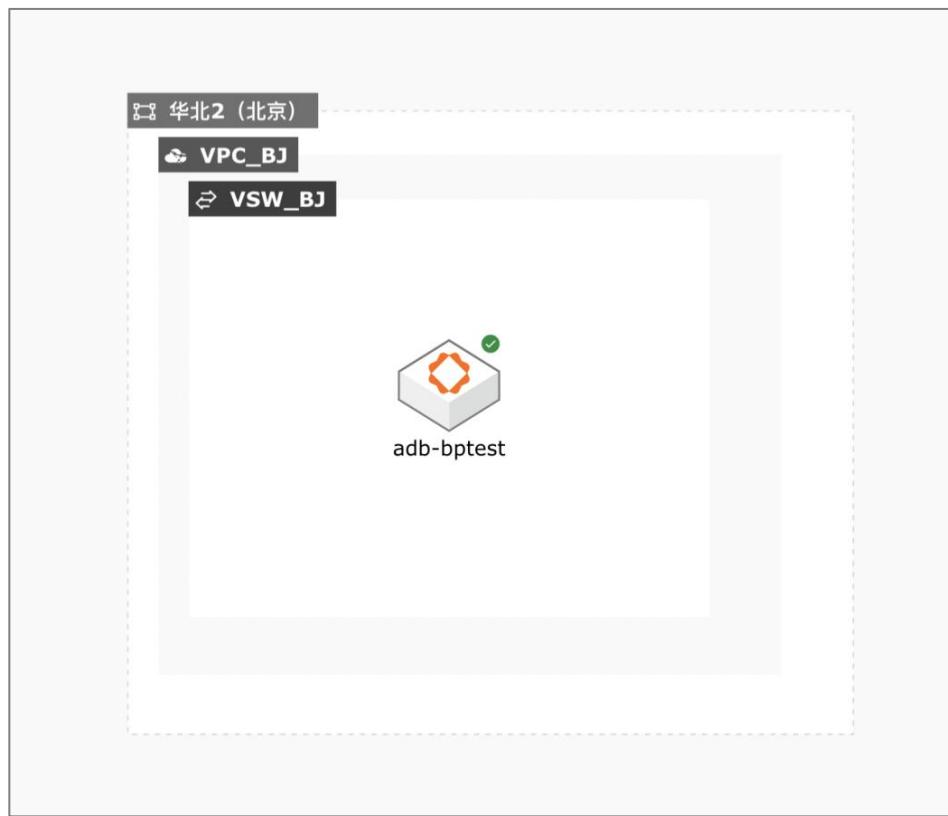
## 4.7. 云速搭部署 ADB 应用

作者 | 阿里云解决方案架构师 袁影

### 4.7.1. 云速搭架构设计入门

#### 方案架构

通过云速搭实现一个云原生数据仓库 AnalyticDB MySQL 版的产品实例，其中产品的选型请参考文档：[https://help.aliyun.com/document\\_detail/205001.html](https://help.aliyun.com/document_detail/205001.html)。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
ADB	VSW

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC_BJ	192.168.0.0/16
AZ	VSW_BJ	可用区 F 区, 192.168.0.0/24

## 4.7.2.应用架构设计

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

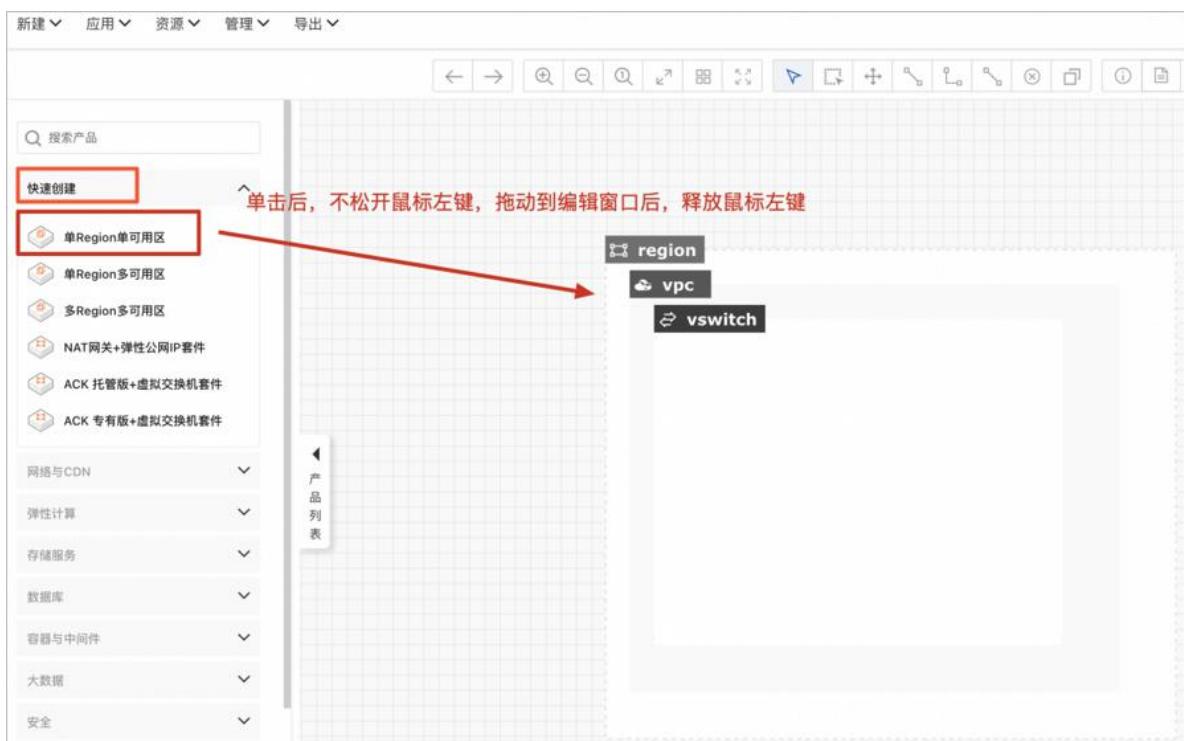
The screenshot shows the Cloud Speed Stack (CADT) Control Console. At the top, there's a header bar with 'Cloud Speed Stack CADT 公共云' and a patent number '专利号: CN111930290B'. Below the header, there are navigation tabs: '新建' (Create), '应用' (Application), '资源' (Resource), and '导出' (Export). A message '欢迎使用云速搭!' (Welcome to Cloud Speed Stack!) is displayed. The main area features a map of China with several cities marked: Beijing, Shanghai, Hangzhou, Shenzhen, Hong Kong, Guangzhou, Chongqing, Chengdu, and Jinan. To the right of the map, there's a section titled '未分配区域' (Unassigned Regions) which is currently empty ('没有数据'). Below this, there's a '产品动态' (Product Updates) section with three items:

- 支持用户对应用进行架构探查, 自动产生已保有的应用的 架构 新功能 (Support users to probe application architecture, automatically generate the architecture of existing applications. New feature)
- 2021年9月31日 (September 31, 2021)
- 支持RAM权限管理, 对子用户授予不同的权限和资源组, 控制子用户对资源的 访问和操作 新功能 (Support RAM permission management, grant different permissions and resource groups to sub-users, control sub-users' access to resources. New feature)
- 2021年9月31日 (September 31, 2021)
- 支持应用状态实时更新, 实时更新服务的状态和配置 新功能 (Support real-time application status update, real-time update service status and configuration. New feature)
- 2021年9月30日 (September 30, 2021)

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

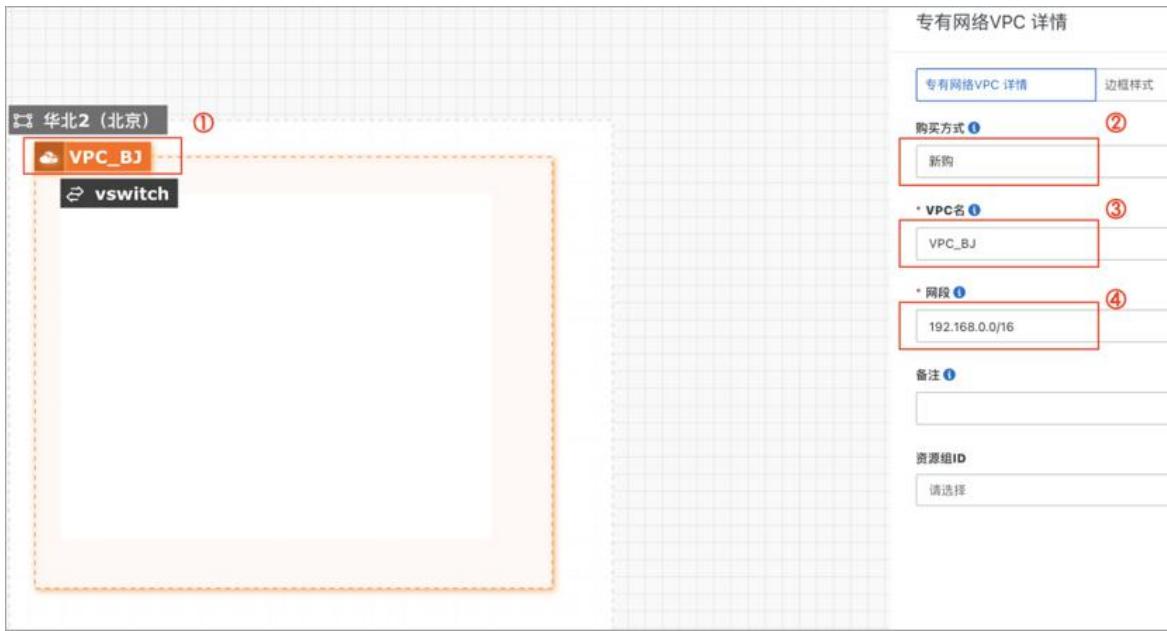


步骤4 依次双击 Region、VPC、vswitch 进行配置。

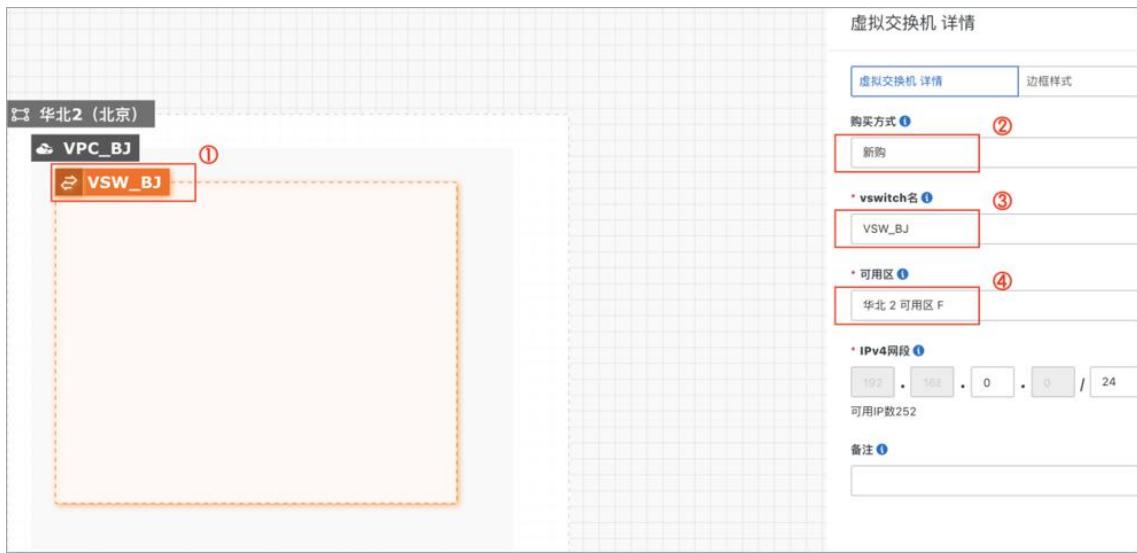
1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



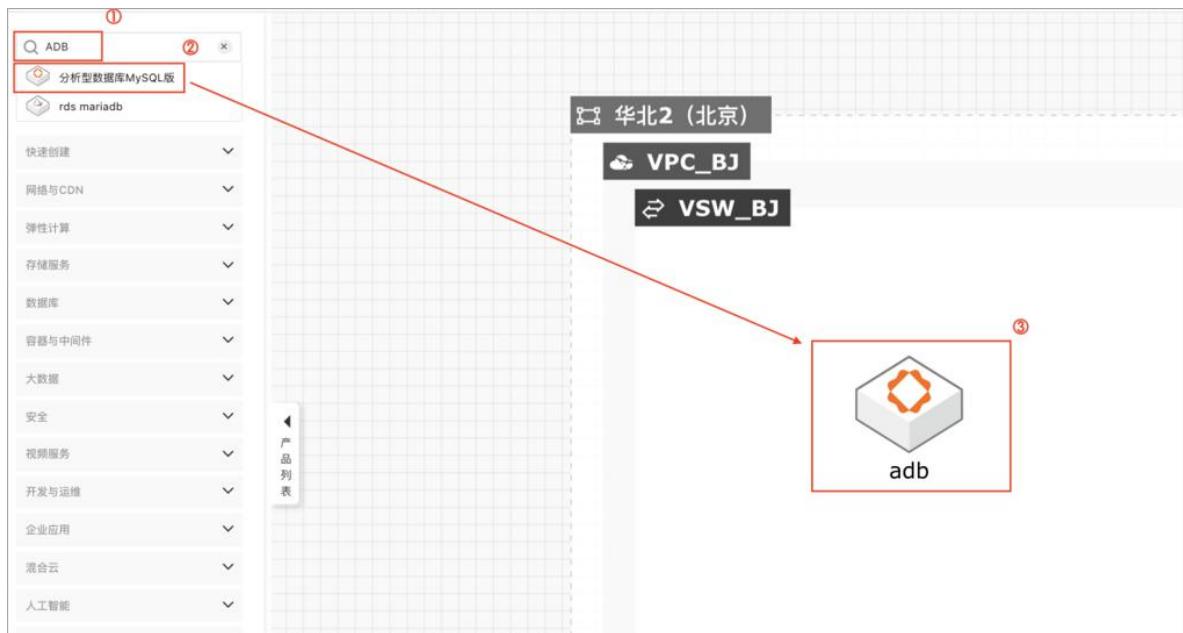
2. 双击 VPC，配置 VPC 参数。



3. 双击 vswitch，配置 vswitch 参数，可用区选择：华北 2 可用区 F。



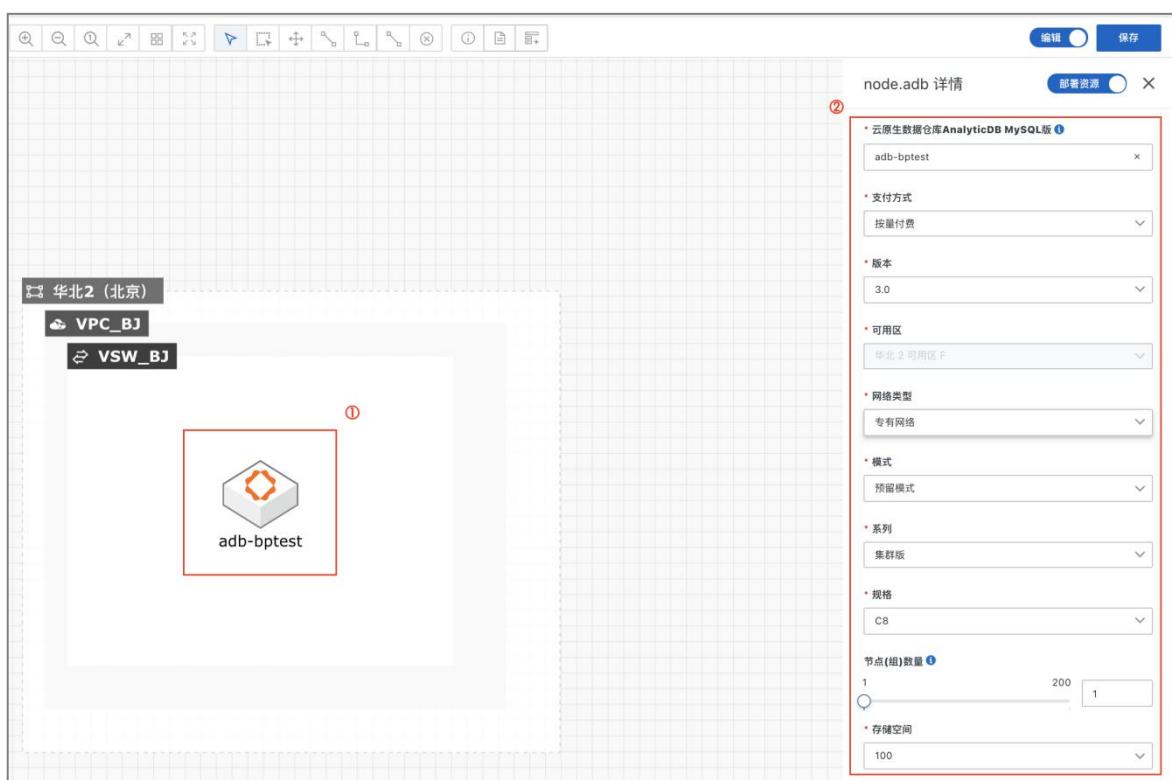
步骤 5 在左侧搜索框中输入 ADB，选定 ADB 图元，拖动到 VSW\_BJ 中。



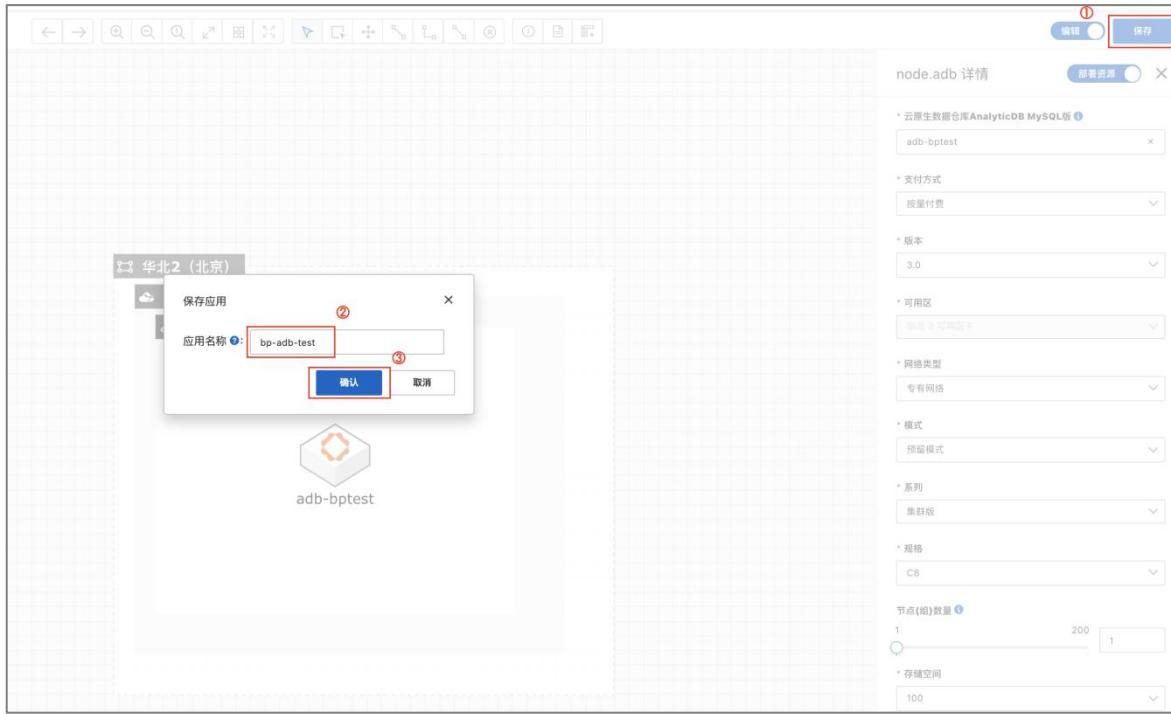
### 4.7.3.配置资源参数

步骤 1 双击 adb 图标，参考下表进行参数配置。

配置项	参数说明
云原生数据仓库 AnalyticDB MySQL 版	adb-bptest
支付方式	按量付费
版本	3.0
网络类型	专有网络
模式	预留模式
系列	集群版
规格	C8
节点(组)数量	1
存储空间	100 (G)

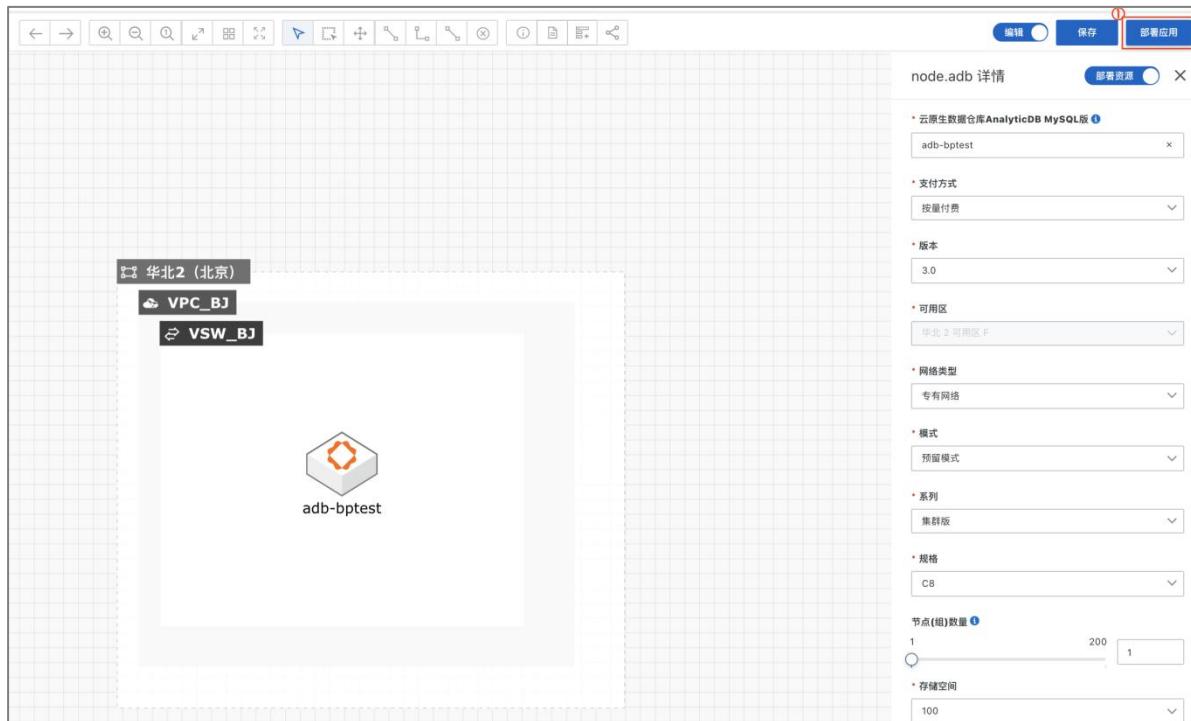


步骤 2 完成以上资源配置后，单击保存，并设置应用名称，最后单击确认。

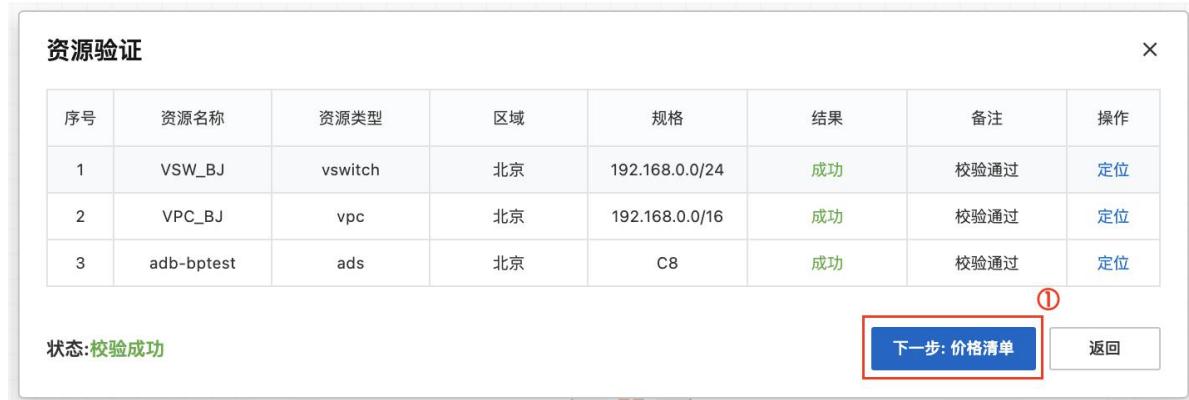


#### 4.7.4.部署应用

步骤 1 用保存完成后，单击右上角的部署应用。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、ADB 是否有库存等，一般需要十几秒左右。



步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息。



步骤 4 可以单击**查看报告**，查看应用的价格信息。



步骤 5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

确认订单

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1 ①	adb-bptest	ads	北京	C8	1	元/时	元/时	新购

《云速搭服务条款》  
部署前，请阅读并勾选服务条款

按量付费：元/时 ②

状态：计价成功

上一步：价格清单

下一步：支付并创建

步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**

1. 部署流程一旦开始后，无法取消。
2. 部署时间预计 **30分钟**左右，请耐心等待。



步骤 7 部署完成后，如下图所示。



步骤 8 单击**查看报告**，可以查看本次的部署报告。

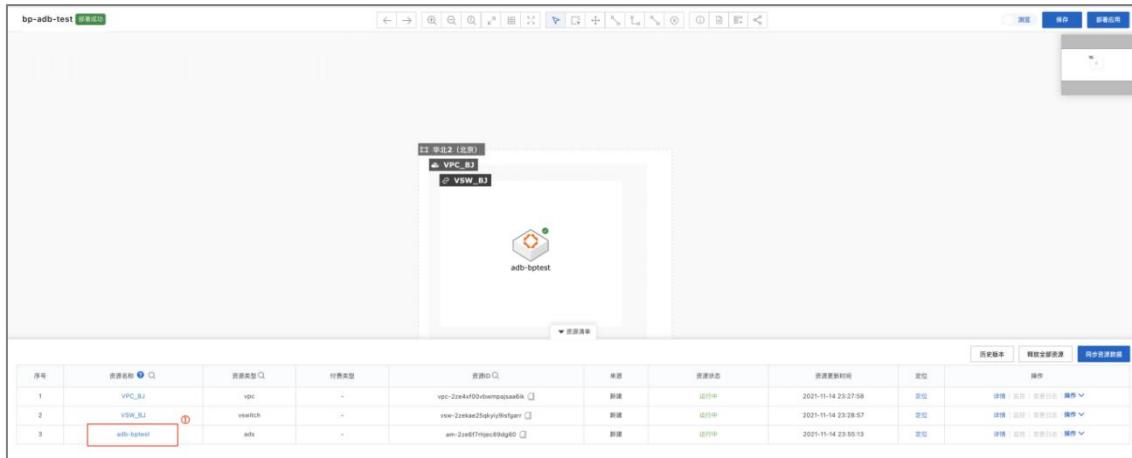


步骤 9 单击返回，然后单击资源清单。

The screenshot shows the Aliyun Resource List interface. At the top, it displays two resources: "VPC\_BJ [192.168.0.0/16]" and "VSW\_BJ [f-192.168.0.0/24]". Below this, there is a search bar and a "资源清单" button highlighted with a red box. The main area lists three resources:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC_BJ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2ze6pbww40v9ovbce	新建	运行中	2021-11-17 17:45:11	定位	详情 监控 变更日志 操作
2	VSW_BJ [f-192.168.0.0/24]	vsswitch (虚拟交换机)	-	vsw-2ze4h5gb3pq53uctxv16g	新建	运行中	2021-11-17 17:45:43	定位	详情 监控 变更日志 操作
3	adb-bptest	ads	-	adb-2ze4h5gb3pq53uctxv16g	新建	运行中	2021-11-17 18:10:06	定位	详情 监控 变更日志 操作

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。



步骤 10 单击资源名称 **adb-bptest**, 可跳转到对应的控制台。



步骤 11 开发配置 ADB

可参考 <https://bp.aliyun.com/detail/100> 中第 3 章的“ADB 数据库配置”。

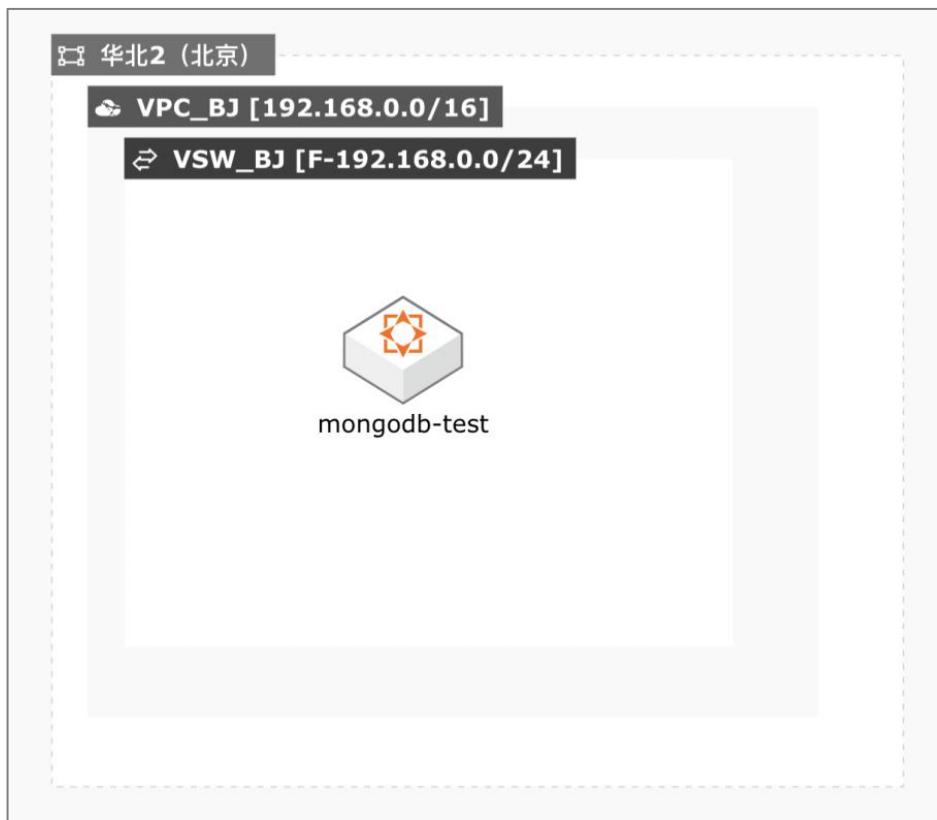
## 4.8.云速搭部署 MongoDB 应用

作者 | 阿里云解决方案架构师 袁影

### 4.8.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现一个云数据库 MongoDB 版的产品实例，其中产品的选型请参考文档：  
[https://help.aliyun.com/document\\_detail/61906.html](https://help.aliyun.com/document_detail/61906.html)。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
MongoDB	VSW

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

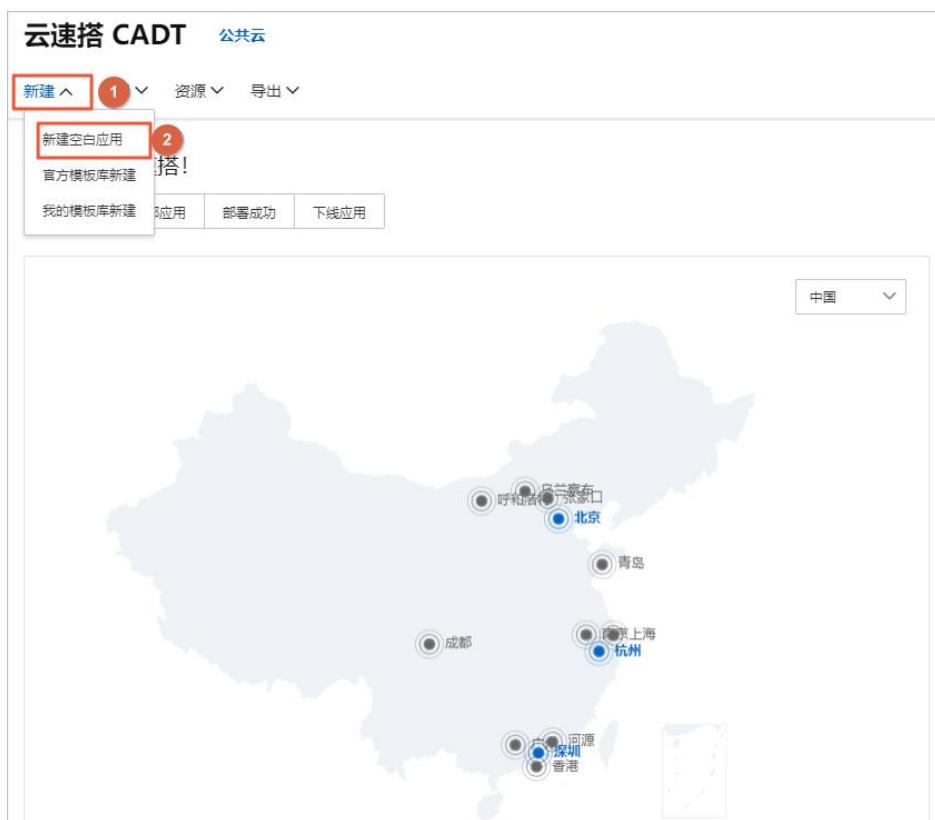
资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC_BJ	192.168.0.0/16
AZ	VSW_BJ	192.168.0.0/24

### 4.8.2.应用架构设计

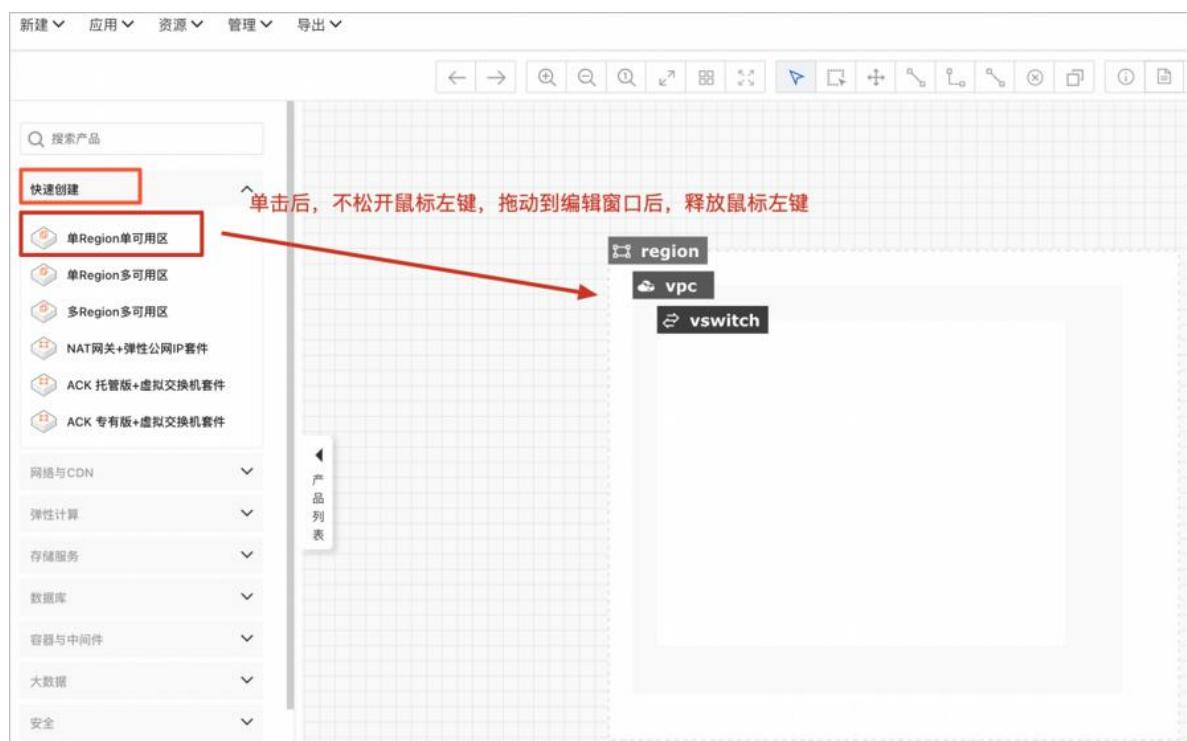
步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录**云速搭 CADT** 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在 CADT 控制台的菜单栏单击**新建 > 新建空白应用**。

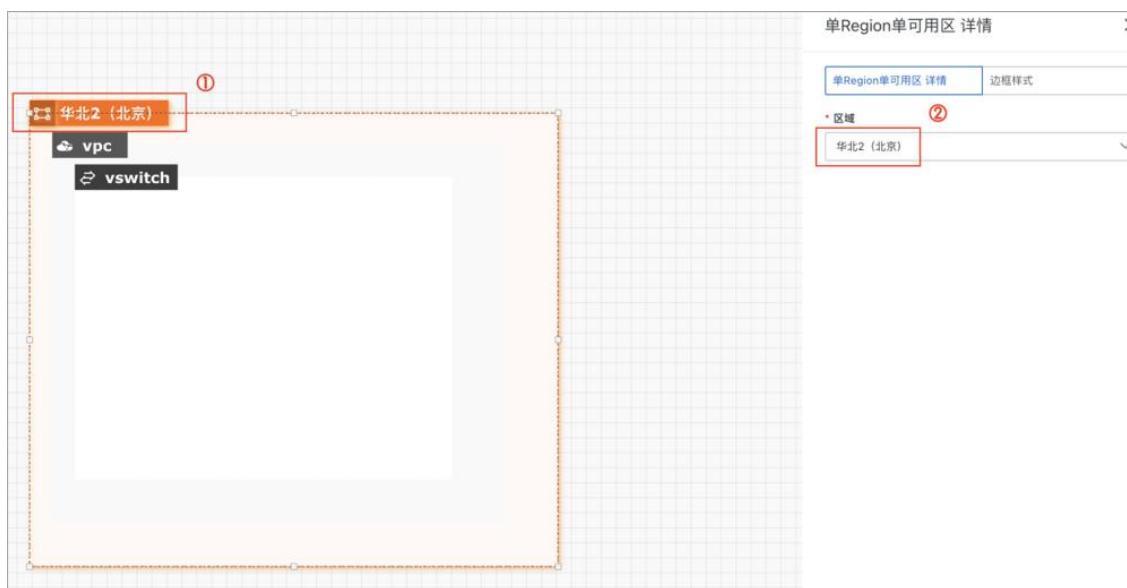


步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。



步骤 4 依次双击 Region、VPC、vswitch 进行配置。

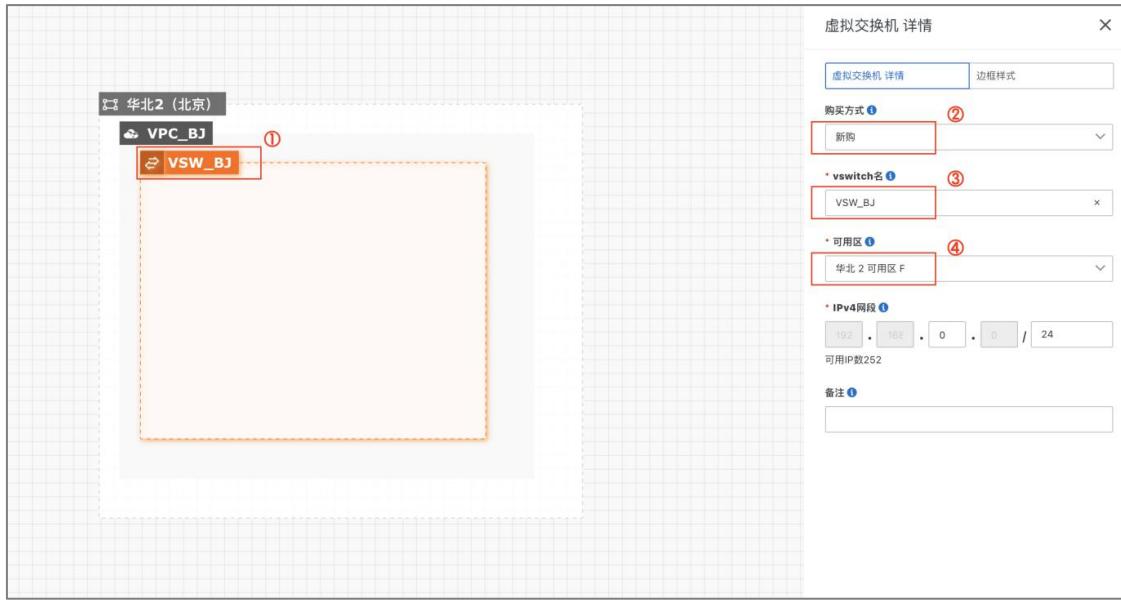
1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



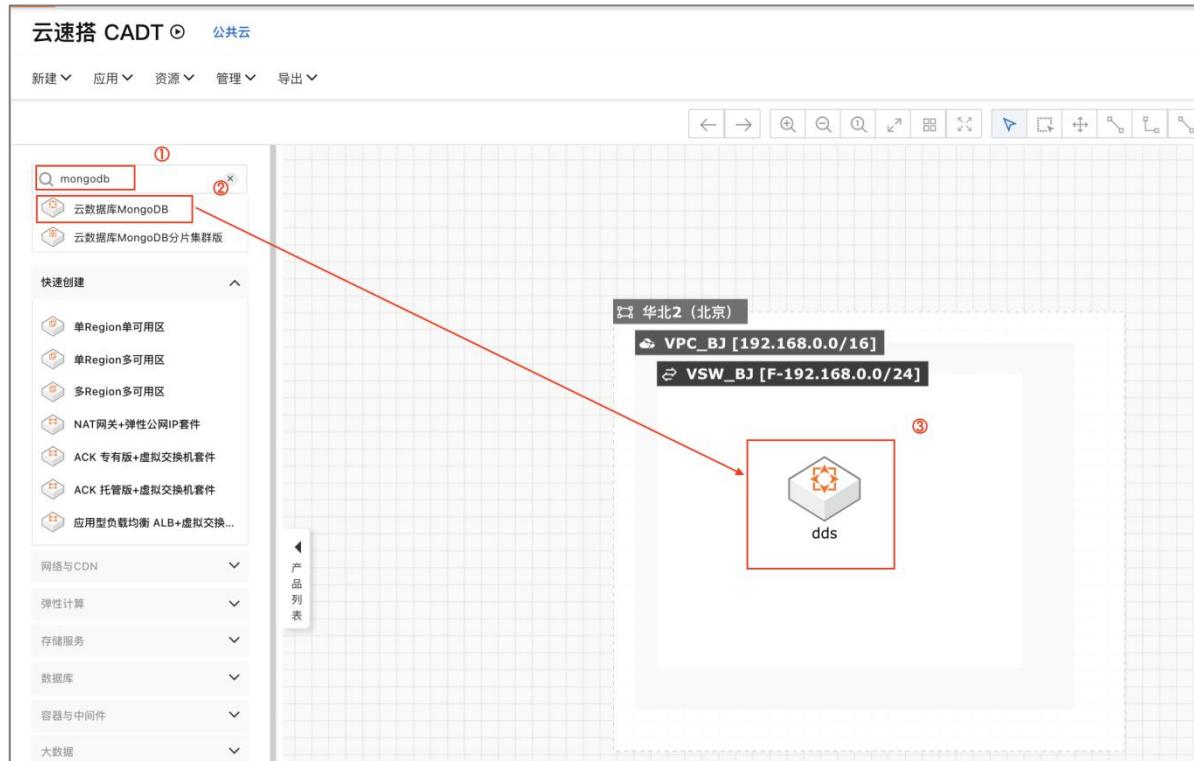
2. 双击 VPC，配置 VPC 参数。



3. 双击 vswitch，配置 vswitch 参数，可用区选择：华北 2 可用区 F。



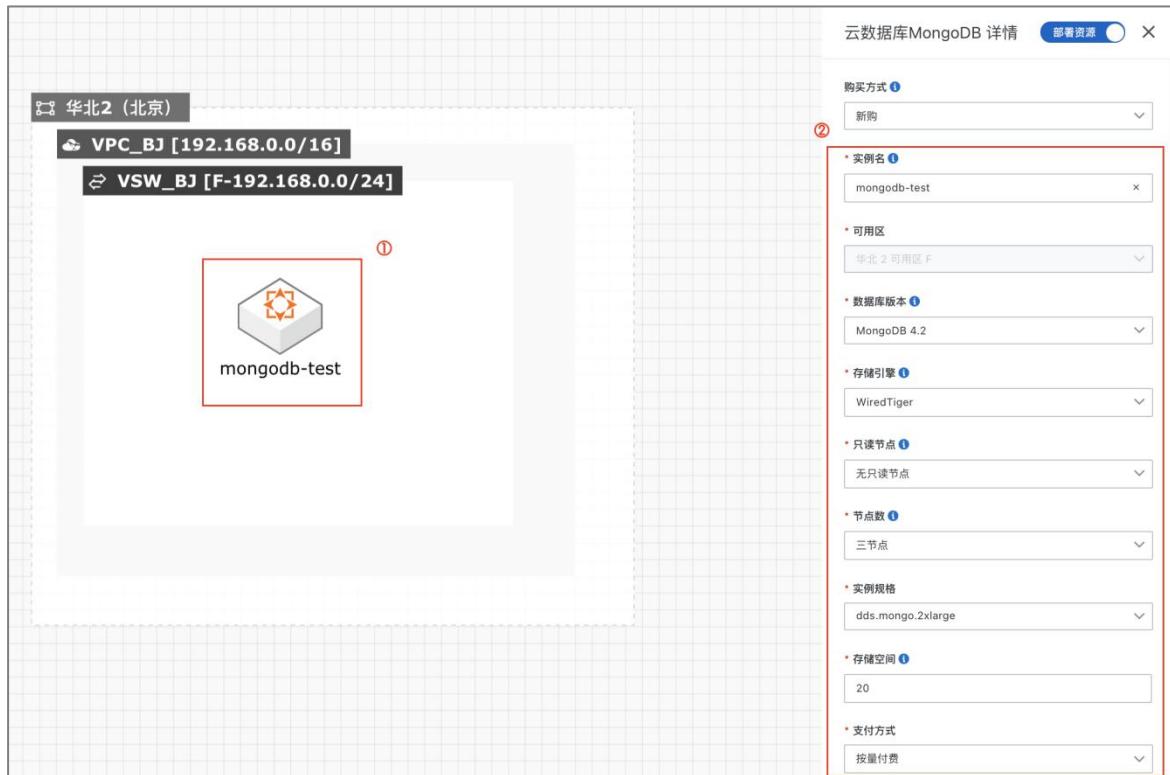
步骤 5 在左侧搜索框中输入 mongodb，选定 MongoDB 图元，拖动到 VSW\_BJ 中。



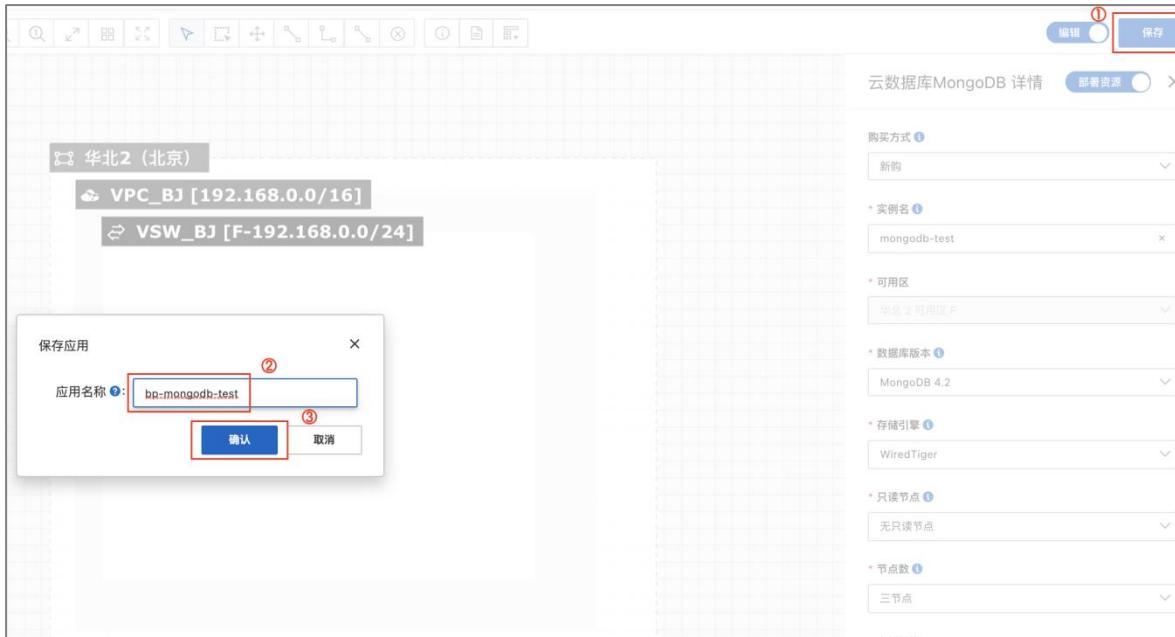
### 4.8.3.配置资源参数

步骤 1 双击 MongoDB 图标，参考下表进行参数配置。

配置项	参数说明
实例名	mongodb-test
支付方式	按量付费
数据库版本	4.2
存储引擎	WiredTiger
只读节点	无只读节点
节点数	三节点
实例规格	dds.mongo.2xlarge
存储空间	20 (G)
支付方式	按量付费
设置密码	(大写、小写、数字、特殊字符占三种，长度为 8–32 位)

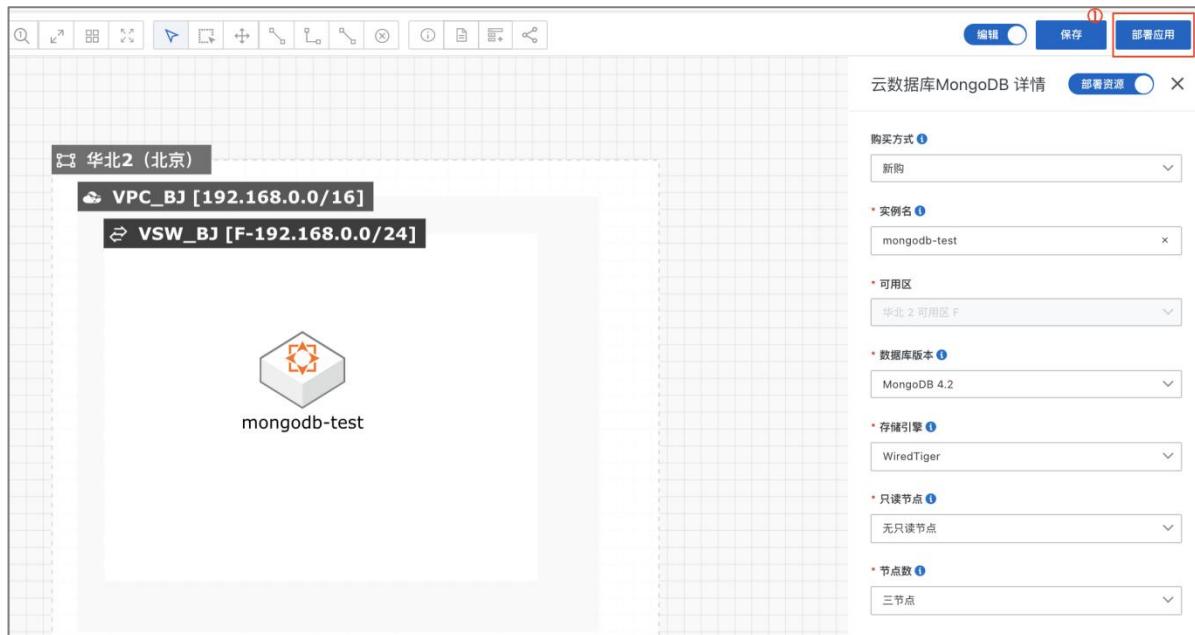


步骤 2 完成以上资源配置后，单击**保存**，并设置**应用名称**，最后单击**确认**。



#### 4.8.4. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、MongoDB 是否有库存等，一般需要十几秒左右。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	VSW_BJ [F-192.1 68.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	<a href="#">定位</a>
2	VPC_BJ [192.16 8.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	<a href="#">定位</a>
3	mongodb-test	dds	北京	4.2	成功	校验通过	<a href="#">定位</a>

状态:校验成功

① [下一步: 价格清单](#) [返回](#)

步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息。

**导出价格清单**

[免费](#) [按量付费](#)

资源成本占比

资源预算  
● 数据库 数据库: 10... 元/时

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	mongodb-test	dds	北京	dds.mongo.2xlarge	1	10元/时	省 10 元/时	10元/时	<a href="#">定位</a>

状态: 计价成功

① [上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

步骤 4 可以单击**查看报告**，查看应用的价格信息。



步骤 5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

确认订单

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	mongodb-test	dds	北京	dds.mongo.2xlarge	1	8.42元/时	8.42元/时	新购

①  《云速搭服务条款》  
部署前，请阅读并勾选服务条款

按量付费： 8.42 元/时 ②

状态：计价成功

上一步：价格清单

下一步：支付并创建

步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

#### 注意：

1. 部署流程一旦开始后，无法取消。
2. 部署时间预计 **10 分钟**左右，请耐心等待。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
 部署中，不要进行任何操作，请耐心等待...							

每页显示 10 共0条 < 上一页 1 下一页 >

**部署概要**

状态：部署中 方案编号：445V24XFR0U1B82K

[返回](#)

步骤 7 部署完成后，如下图所示。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	VPC_BJ [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2ze67nedawcmnob45308g	运行中	2021-12-05 20:44:15	定位
2	VSW_BJ [F-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze70tc42fxmhpk2q1vt7	运行中	2021-12-05 20:44:34	定位
3	mongodb-test	dds (云数据库MongoDB)	按量付费	dds-2ze8d5e2c403ded4	运行中	2021-12-05 20:51:18	定位

每页显示 10 共3条 < 上一页 1 下一页 >

**部署概要**

状态：部署成功 订单编号：211775295880425  
方案编号：445V24XFR0U1B82K

[查看报告](#) [返回](#)

步骤 8 单击**查看报告**，可以查看本次的部署报告。



步骤 9 单击返回，然后单击资源清单。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC_BJ [192.168.0.0/16]	VPC (专有网络(VPC))	-	vpc-2ze67nedacmcmrob4330bg	新建	运行中	2021-12-05 20:44:15	定位	<a href="#">详情</a>   <a href="#">返回</a>   <a href="#">更多动作</a>   <a href="#">操作</a>
2	VSW_BJ [F-192.168.0.0/24]	vnwatch (虚拟交换机)	-	vsw-2ze70c42fkmhp42q1n7	新建	运行中	2021-12-05 20:44:34	定位	<a href="#">详情</a>   <a href="#">返回</a>   <a href="#">更多动作</a>   <a href="#">操作</a>
3	mongodb-test	dds (云数据库MongoDB)	按量付费	dds-2ze8d5e2c4053kd4	新建	运行中	2021-12-05 20:51:18	定位	<a href="#">详情</a>   <a href="#">返回</a>   <a href="#">更多动作</a>   <a href="#">操作</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。

步骤 10 单击资源名称 **mongodb-test**, 可跳转到对应的控制台。

The screenshot shows the Alibaba Cloud MongoDB instance configuration page. The instance ID is `dds-2ze8d5e2c403ded4` and it is currently running. The basic information panel displays the instance ID, location (Beijing, China), network type (Private Network), and storage engine (WiredTiger). The specification information panel shows details like node count (3 nodes), storage code (dds.mongo.2xlarge), and IOPS (14000). The connection information panel provides the connection string URI.

步骤 11 开发配置 ADB

可参考 [https://help.aliyun.com/document\\_detail/26577.html](https://help.aliyun.com/document_detail/26577.html)。

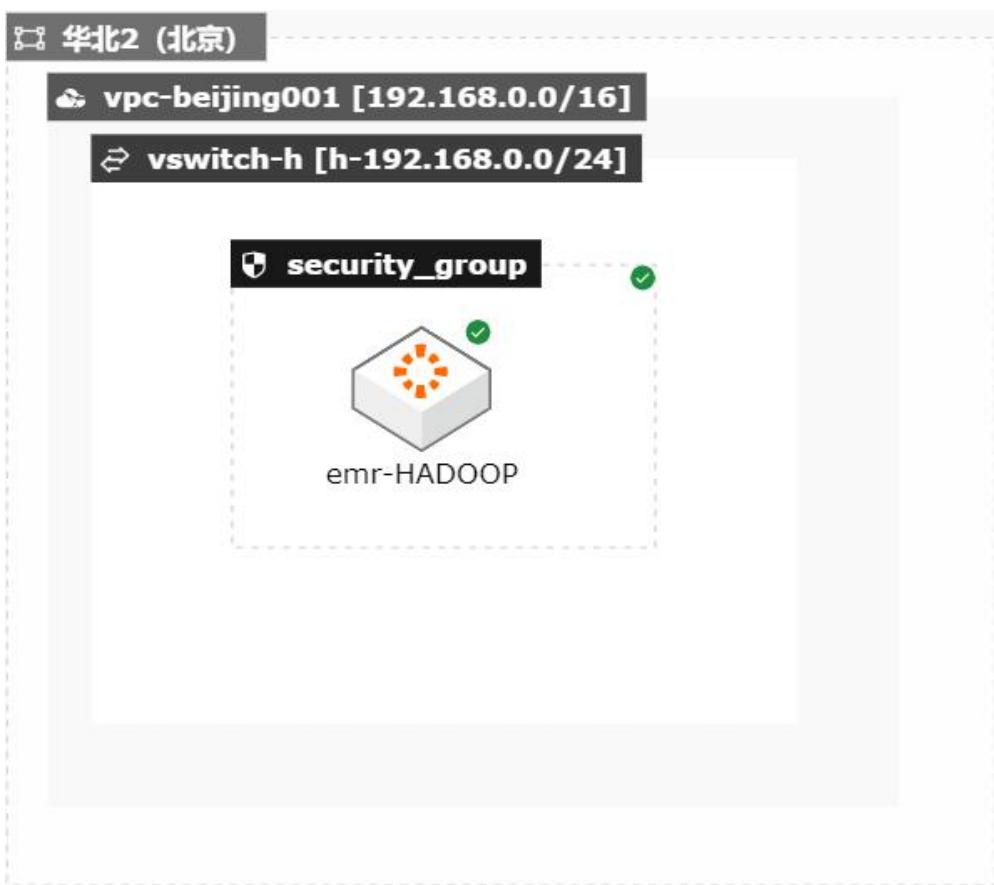
## 4.9.云速搭部署 EMR

作者 | 阿里云解决方案架构师 敬海

### 4.9.1.云速搭架构设计入门

#### 方案架构

通过云速搭实现 EMR 的部署：



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
EMR	vswitch 交换机
ECS	vswitch 交换机

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

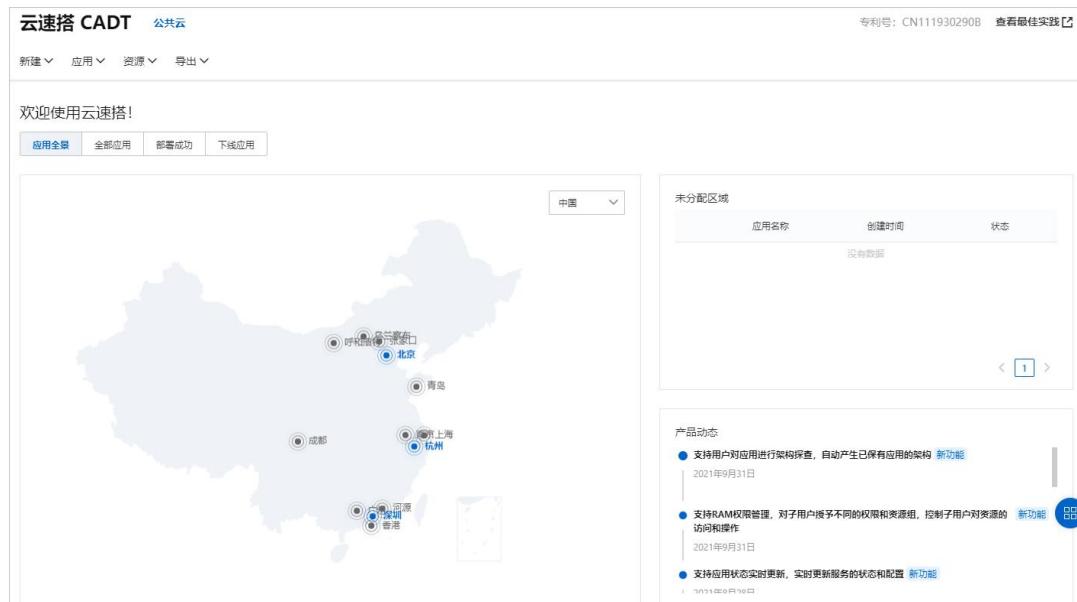
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
安全组	security_group	-

## 4.9.2. 应用架构设计门

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

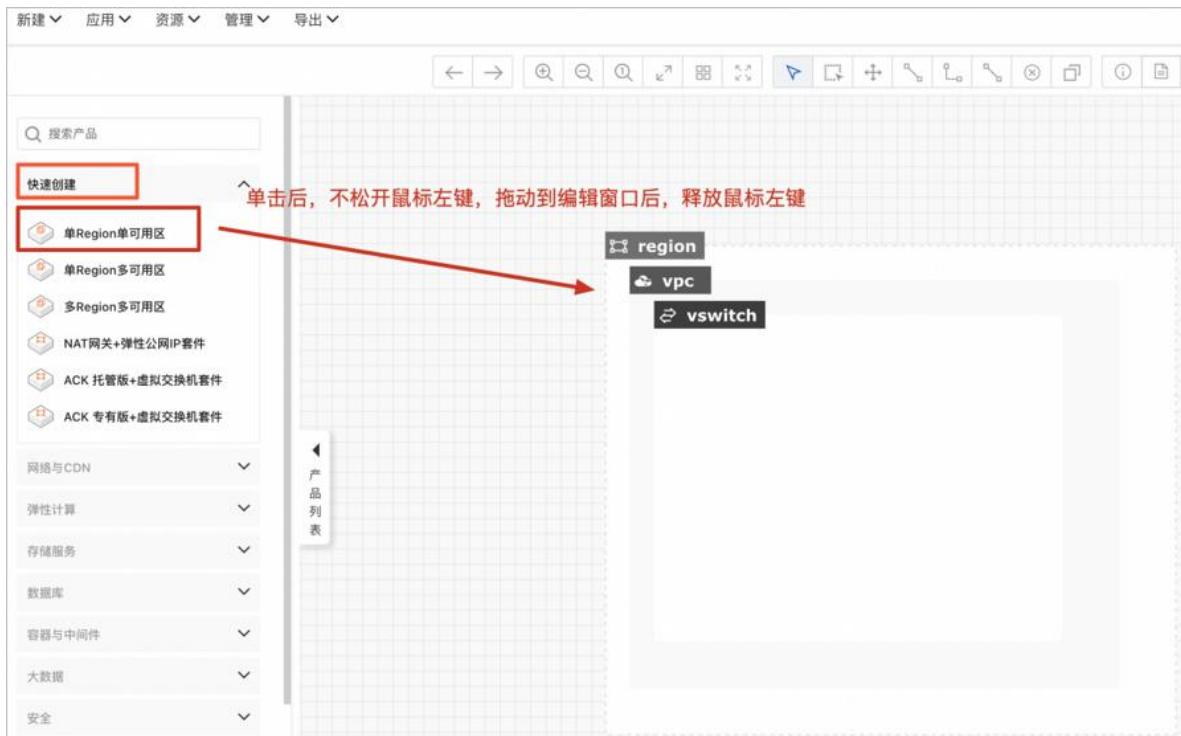
**说明：**如果提示需要开通服务，请根据提示进行开通。



步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

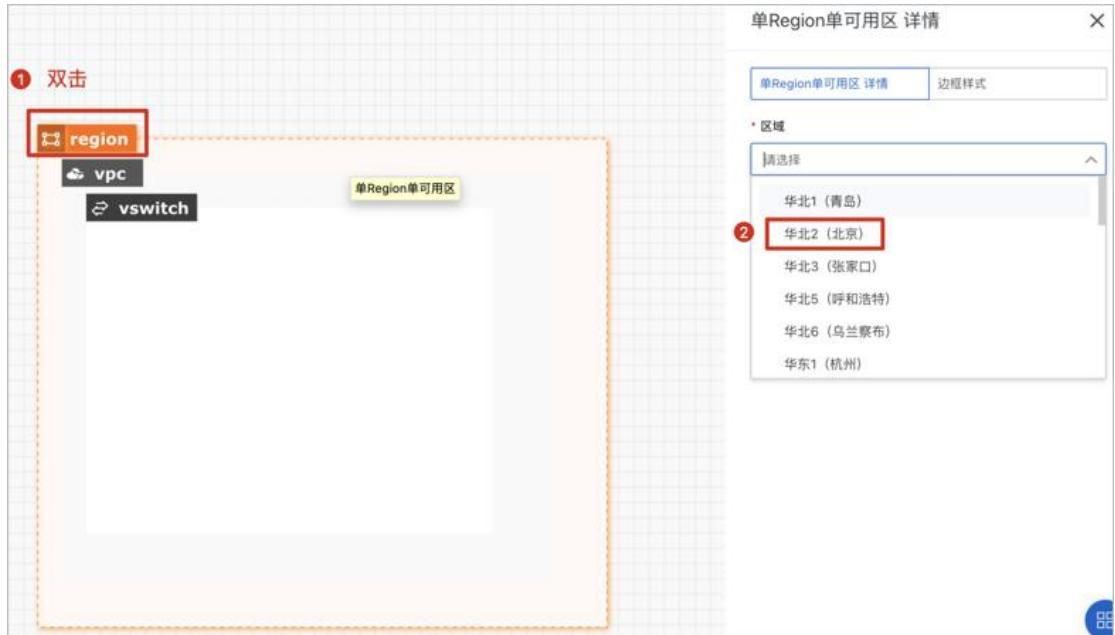


步骤 3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

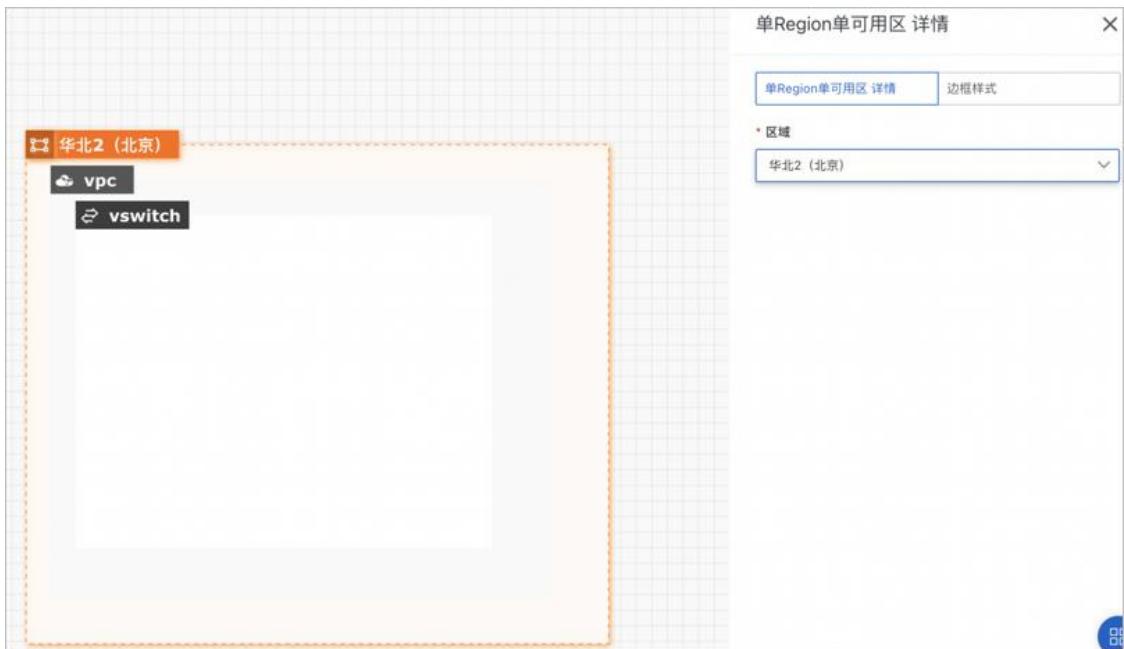


步骤 4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



选择后，如下图所示：



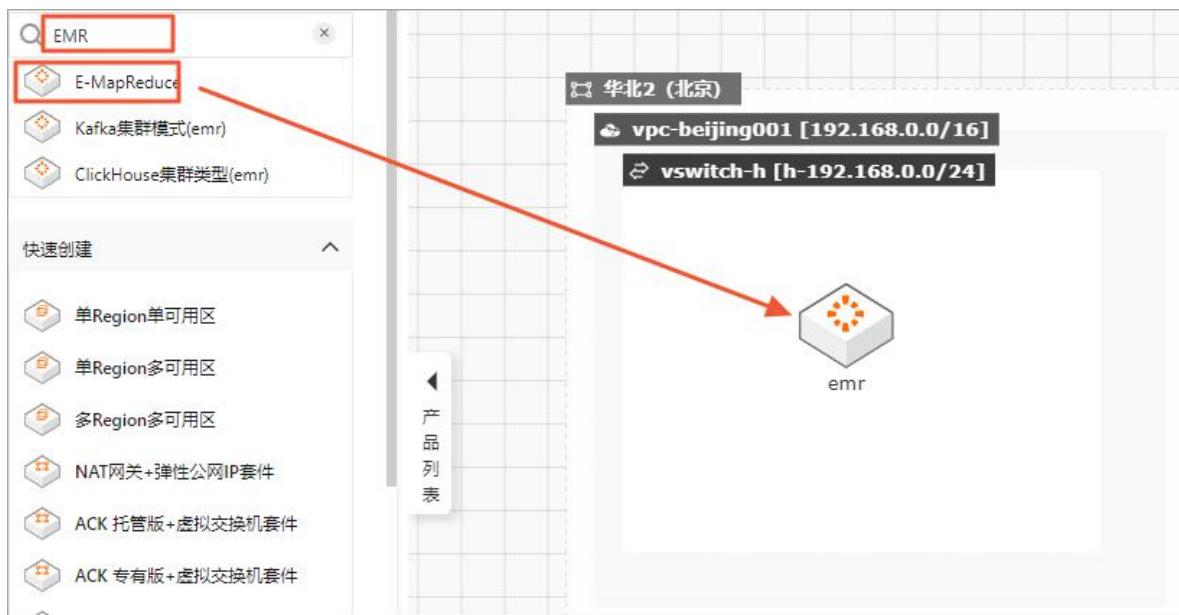
2. 双击 VPC，配置 VPC 参数。



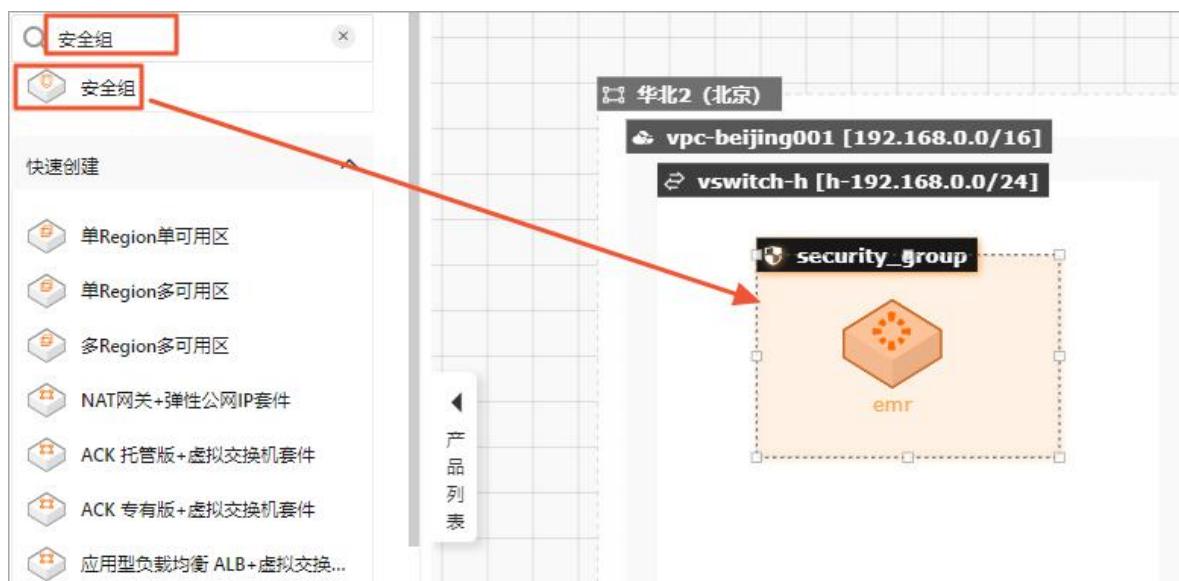
3. 双击 Vswitch，配置 vswitch 参数。



步骤 5 左侧搜索 EMR，拖到 vswitch 中。



步骤 6 搜索安全组，拖动到 EMR 上，框住 EMR。



步骤 7 双击 EMR，配置为如下参数（仅为示例，需要根据自己的实际情况选择）

**购买方式**

新购

**\* 集群名称**

emr

**集群类型**

HADOOP

**\* 产品版本**

EMR-3.23.0

**可选服务**

ZOOKEEPER

**软件自定义配置**

**\* 付费类型**

按量付费

**\* 可用区**

华北 2 可用区 H

**\* 高可用**

**实例选型配置**

host\_group = [

{

**\* 实例组** Master 实例

**\* 实例数量** 1

**\* 当前机型** ecs.c6e.2xlarge(8 vCPU 16 GiB)

**\* 系统盘配置** cloud\_essd

**\* 系统盘大小** 120

**\* 数据盘配置** cloud\_essd

**\* 数据盘大小** 80

**\* 数据磁盘数量** 1

}, ]

{

**\* 实例组** Core 实例

**\* 实例数量** 2

**\* 当前机型** ecs.d1ne.2xlarge(8 vCPU 32 GiB)

**\* 系统盘配置** cloud\_ssd

**\* 系统盘大小** 120

**\* 数据盘配置** local\_disk

**\* 数据盘大小** 80

**\* 数据磁盘数量** 4

}

]

**元数据选择**

集群内置MySQL

**挂载公网**

**远程登录**

**\* 登录密码**

.....

8 - 30 个字符，且必须同时包含大写字母、小写字母、数字和特殊字符!@#\$%^&\*

**\* 确认登录密码**

.....

8 - 30 个字符，且必须同时包含大写字母、小写字母、数字和特殊字符!@#\$%^&\*

**ECS应用角色**

AliyunEmrEcsDefaultRole

**资源标识**

请填写标签键 : 请填写标签值

(1/20)

步骤 8 双击安全组，修改安全组参数。（请根据实际情况配置，作为演示，本示例保持默认。）

购买方式 ①	SSH(22) X
新购	网络类型 ① intranet
* 安全组 ①	* 目标IP地址范围 ① 0.0.0.0/0 X
security_group	跨账户授权安全组 ①
安全组的类型 ①	安全组规则的描述 ①
请选择	}
安全组规则 ①	{
security_group_rule = [	* 规则的类型 ① 入方向
{	授权策略 ① 允许
* 规则的类型 ① 入方向	* 优先级 ① 1
授权策略 ① 允许	* 协议类型 ① 全部ICMP(IPv4)
* 优先级 ① 1	* 端口范围 ① -1/-1 X
* 协议类型 ① 自定义 TCP	网络类型 ① intranet
* 端口范围 ① HTTP(80) X	* 目标IP地址范围 ① 0.0.0.0/0 X
HTTP(80) X	跨账户授权安全组 ①
HTTPS(443) X	安全组规则的描述 ①
RDP(3389) X	

步骤 9 单击右上角的保存，填写应用名称。

保存应用	
应用名称 ②:	CADT-EMR-DEMO
<input type="button" value="确认"/>	<input type="button" value="取消"/>

### 4.9.3. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。

步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、资源是否有库存等，一般需要十几秒左右。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch [h-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	vpc [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
3	security_group	security.group	北京		成功	校验通过	定位
4	emr-HADOOP	emr	北京	HADOOP	成功	校验通过	定位

状态:校验成功

下一步: 价格清单 返回

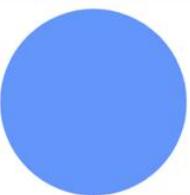
步骤 3 等待校验成功，单击**下一步：价格清单**。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch [h-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	vpc [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
3	security_group	security.group	北京		成功	校验通过	定位
4	emr-HADOOP	emr	北京	HADOOP	成功	校验通过	定位

状态:校验成功

下一步: 价格清单 返回

这里会拉取应用所有配置的价格信息，可以查看计费详情。

导出价格清单																			
免费		按量付费		资源成本占比															
<b>资源成本占比</b>																			
 <span style="margin-left: 100px;">资源预算 ● 大数据 大数据: 10... 元/时</span>																			
<b>价格列表</b>																			
序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作										
1	emr	emr	北京	HADOOP	1	15.76元/时			定位										

状态: 计价成功

上一步: 资源校验 查看报告 下一步: 确认订单

步骤4 可以单击**查看报告**，查看应用的价格信息。



步骤5 单击**下一步：确认订单**。

导出价格清单

免费 按量付费

资源成本占比

资源预算  
● 大数据 大数据: [redacted] 元/时

10...

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	emr	emr	北京	HADOOP	1	15.76元/时	[green bar]	[blue bar]	定位

状态: 计价成功

上一步: 资源校验 查看报告 下一步: 确认订单

A screenshot of a web-based price list export interface. It shows a summary section with a pie chart of resource cost distribution and a detailed table of prices. The table lists an EMR instance with its specifications, quantity, original price, discount, actual payment, and an 'Operate' button. At the bottom, there are navigation buttons for previous steps, viewing reports, and confirming the order.

步骤 6 在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。



步骤 7 单击**下一步：支付并创建**，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。



资源部署状态

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zejy8l3kvyaiobzl1w	运行中	2021-11-22 19:26:11	定位
2	vswitch [h-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze6uw2g2dvcctnmyas3s	运行中	2021-11-22 19:27:10	定位
3	security_group	security.group (安全组)	-	sg-2zegm2ytp5hrp0vw93ds	运行中	2021-11-22 19:26:12	定位
4	emr-HADOOP	emr (E-MapReduce)	按量付费	C-C7459B201E944DB3	运行中	2021-11-22 19:32:03	定位

部署概要

状态：部署成功 方案编号：IQRCSV75Q0ZD5U18

[查看报告](#) [返回](#)

步骤 8 部署完成后，单击[查看报告](#)，可以查看本次的部署报告。



步骤 9 单击返回，然后单击资源清单。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zejy8l3kvyaiobzlr1w	运行中	2021-11-22 19:26:11	定位
2	vswitch [h-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze6uw2g2dvccnrmay3s	运行中	2021-11-22 19:27:10	定位
3	security_group	security.group (安全组)	-	sg-2zegm2ytp5hrp0vw93ds	运行中	2021-11-22 19:26:12	定位
4	emr-HADOOP	emr (E-MapReduce)	按量付费	C-C7459B201E944DB3	运行中	2021-11-22 19:32:03	定位

**部署概要**

状态: 部署成功 方案编号: IQRCVS75Q0ZD5U18

[查看报告](#) [返回](#)

The screenshot shows the 'Resource Deployment Status' page. At the top, it displays the deployment summary: 'Status: Deployment successful' and 'Plan ID: IQRCVS75Q0ZD5U18'. Below this is a 'Deployment Summary' section with a 'View Report' button and a 'Return' button. The main area is a table showing the deployed resources:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	vpc-beijing001 [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zedq6nt7b7hlq3goqwqk	新建	运行中	2021-11-23 10:39:52	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
2	security_group	security.group (安全组)	-	sg-2ze3bxajhjkf7gd8jcm0	新建	运行中	2021-11-23 10:40:33	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 10 找到 EMR，单击后面的**操作**，单击**查看拓扑**，可以看到如下拓扑。

The screenshot shows the RAM console interface. At the top, it displays the VPC configuration for 'vpc-beijing001 [192.168.0.0/16]' and its subnet 'vswitch-h [h-192.168.0.0/24]'. Below this, a security group named 'security\_group' is associated with the subnet. A red box highlights the 'emr-HADOOP' entry in the resource list table, which is identified by a red number '1'. The table includes columns for序号 (Index), 资源名称 (Resource Name), 资源类型 (Resource Type), 付费类型 (Billing Type), 资源ID (Resource ID), 来源 (Source), 资源状态 (Resource Status), 资源更新时间 (Last Update Time), 定位 (Location), 操作 (Operations), and three buttons: 历史版本 (History Version), 释放全部资源 (Release All Resources), and 同步数据 (Sync Data). A red box highlights the '操作' button for the 'emr-HADOOP' entry, with a red number '2' next to it.

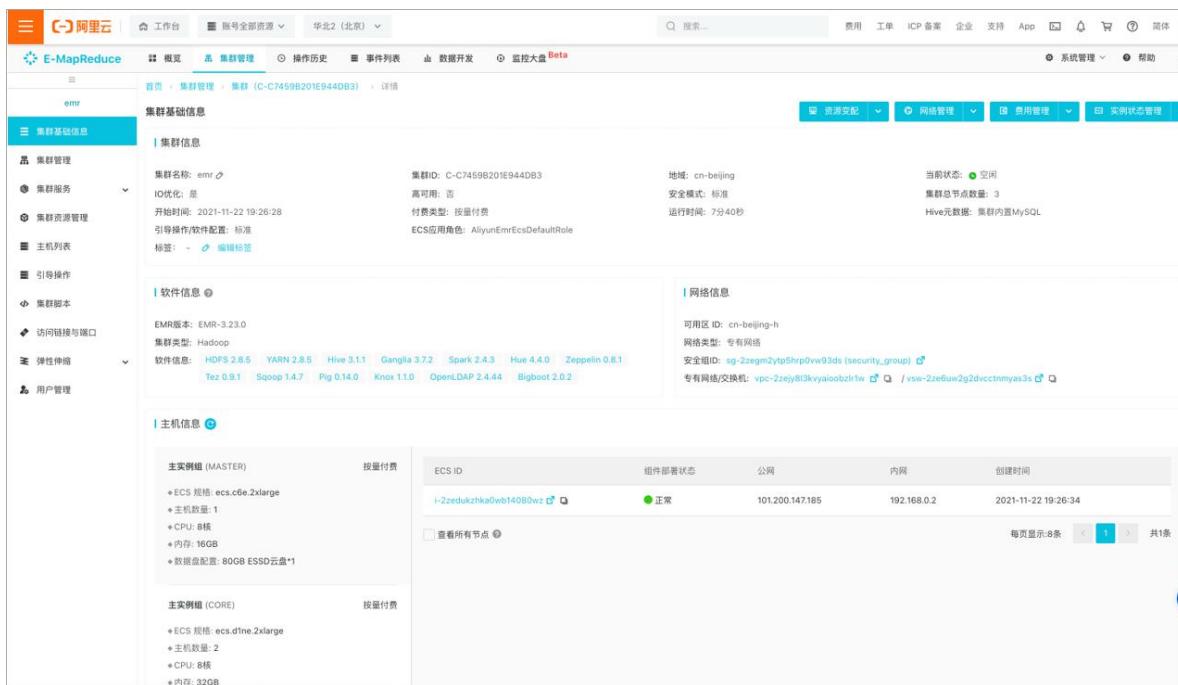
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
3	vswitch-h [h-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze85ocbqmal447yzb69a	新建	运行中	2021-11-23 10:40:33	定位	详情 监控 ① 查看拓扑
4	emr-HADOOP	emr (E-MapReduce)	按量付费	C-3D0B28235F589191	新建	运行中	2021-11-23 10:46:58	定位	详情 监控 变更日志 ② 操作

The screenshot shows the EMR console interface. It displays the cluster topology for 'cn-beijing'. At the top, it shows the VPC configuration 'vpc-2zejy8l3kvyaiobzir1w' and its subnet 'sg-2zegm2ytp5hrp0vw93ds'. Below this, the cluster structure is shown with two main components: 'MASTER' and 'CORE'. The 'MASTER' node is represented by a single ECS icon, and the 'CORE' node is represented by a stack of three ECS icons. A red box highlights the 'emr-HADOOP' entry in the resource list table, with a red number '1'. To the right, detailed information for the 'MASTER' and 'CORE' instances is provided, including ECS specifications, instance counts, CPU and memory configurations, and storage disk details. Buttons at the bottom include '导出图片' (Export Image), '导出CSV' (Export CSV), and '关闭' (Close).

步骤 11 单击 EMR 的名称后，跳转到 EMR 控制台查看。



序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
-		(安全组)				
3	vswitch-h [h-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze85ocbqmal447yzb69a	新建	运行中
4	<b>emr-HADOOP</b>	emr (E-MapReduce)	按量付费	C-3D0B28235F589191	新建	运行中

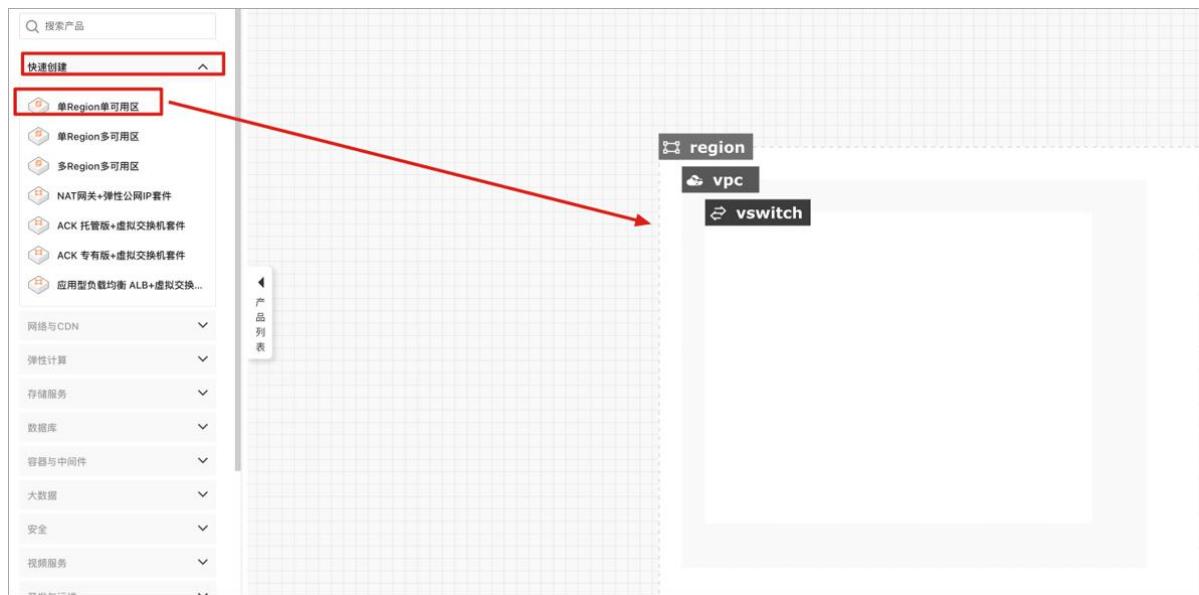
  


#### 4.9.4. 导入已保有 EMR 应用架构

步骤 1 单击新建 > 新建空白应用。



步骤 2 从快速创建下找到单 region 单可用区，拖入到编辑窗口。



步骤 3 双击地域，选择北京。

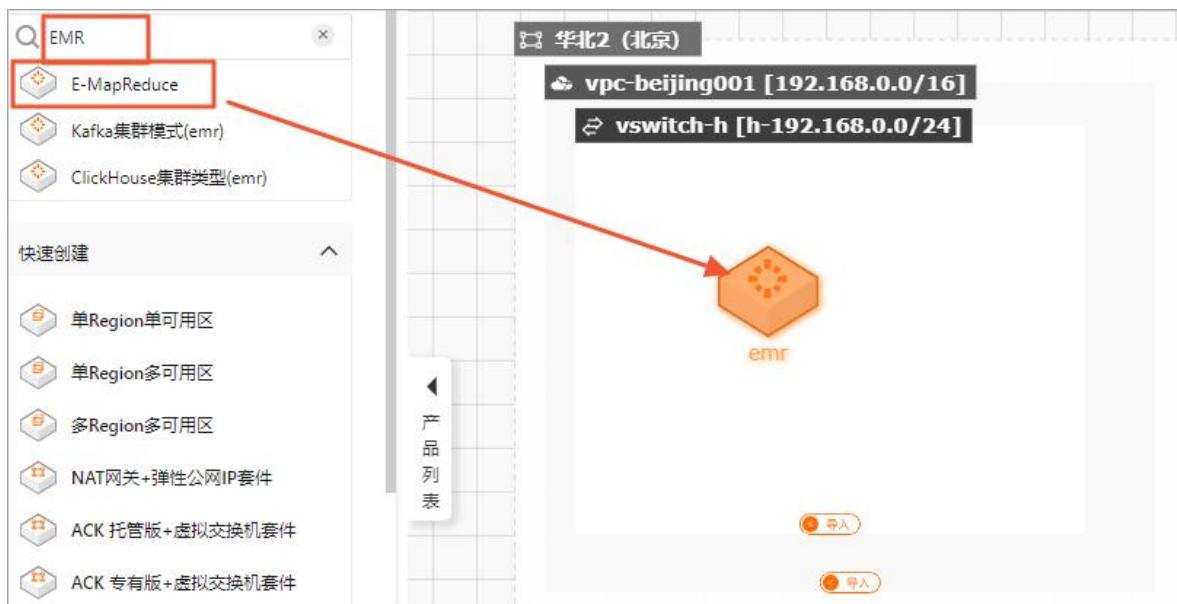
步骤 4 双击 vpc，选择已保有，选择之前创建的 vpc。



步骤 5 双击 vswitch，选择已保有，选择 vswitch。



步骤 6 搜索 EMR，并拖入 vswitch 中。



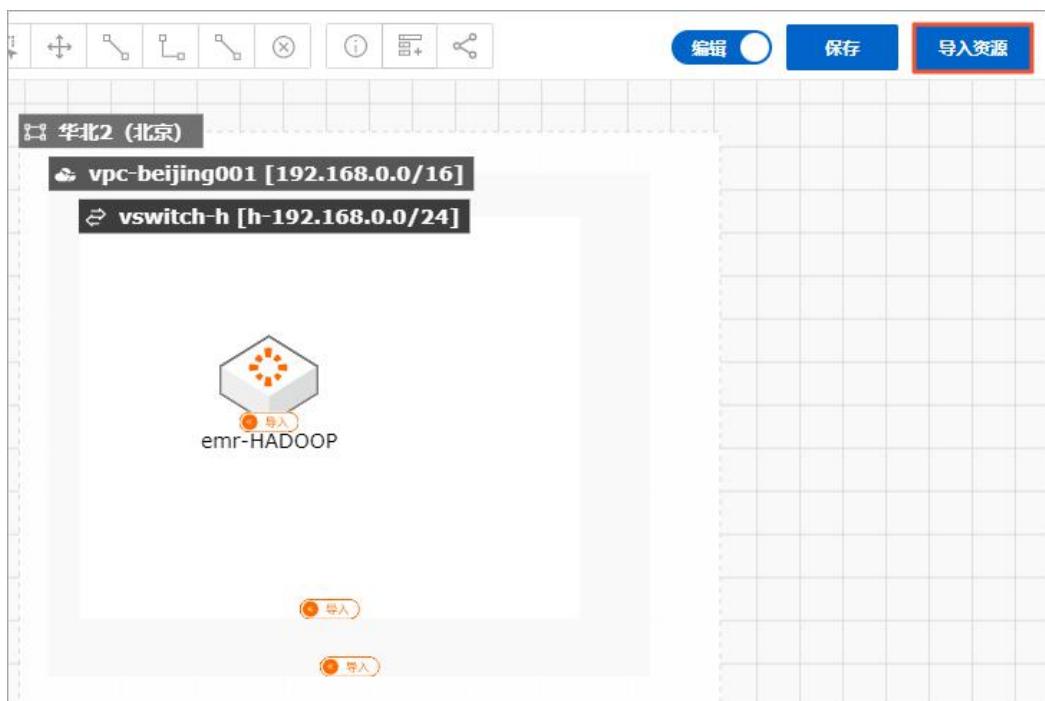
步骤 7 双击 EMR，选择已保有，选择之前创建的 EMR。



步骤 8 单击保存，输入应用名称。



步骤 9 单击导入资源。



步骤 10 单击导入。

Import Resource List						
序号	Resource Name	Resource Type	Payment Type	Resource ID	Resource Status	Location
1	vswitch [h-192.168.0.0/24]	vswitch	Free	vsw-2ze6uw2g2dvcctnmyas3s	Pending Import Structure	Location
2	vpc [192.168.0.0/16]	vpc	Free	vpc-2zejy8l3kvyaioobzlr1w	Pending Import Structure	Location
3	emr-HADOOP	emr	Pay-as-you-go	C-C7459B201E944DB3	Pending Import Structure	Location

**Note:** New purchased resources, after successful import, click "Deploy Application" to create new resources.

**Import**

步骤 11 导入成功后，如下图所示：

**资源导入状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vswitch [h-192.1 68.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze6uw2g2dvcctnmyas3s	运行中	-	定位
2	vpc [192.168.0.0/ 16]	vpc (专有网络VPC)	-	vpc-2zejy8l3kvyaiobzlr1w	运行中	-	定位
3	emr-HADOOP	emr (E-MapReduc e)	按量付费	C-C7459B201E944DB3	运行中	-	定位

**导入概要**

状态：导入成功 方案编号：78U28D3UT93J1UWS

[返回](#)

步骤 12 资源清单也会生成如下：

**EMR-导入 导入成功**

华北2 (北京)

vpc [192.168.0.0/16] vswitch [h-192.168.0.0/24]

▼ 资源清单

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	vswitch [h-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2ze6uw2g2dvcctnmyas3s	已保有	运行中	-	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>
2	vpc [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2zejy8l3kvyaiobzlr1w	已保有	运行中	-	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>
3	emr-HADOOP	emr (E-MapReduce)	按量付费	C-C7459B201E944DB3	已保有	运行中	-	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>

## 4.10.云速搭部署 ACK 集群

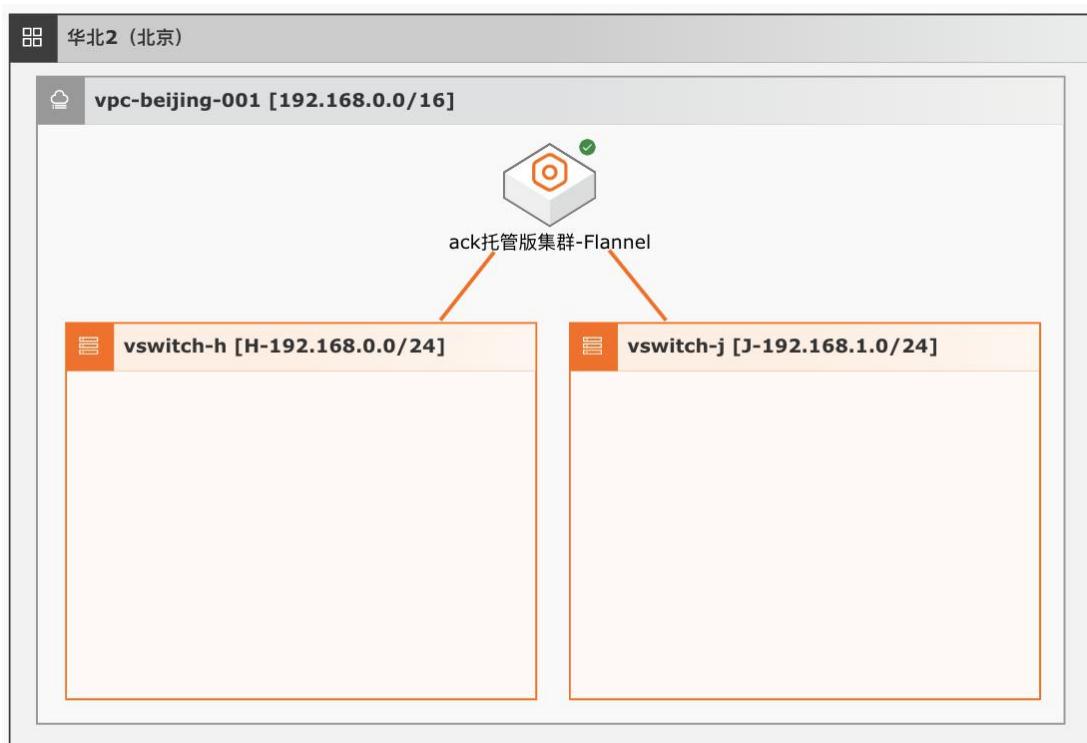
作者 | 阿里云解决方案架构师 七凌

### 4.10.1.云速搭架构设计

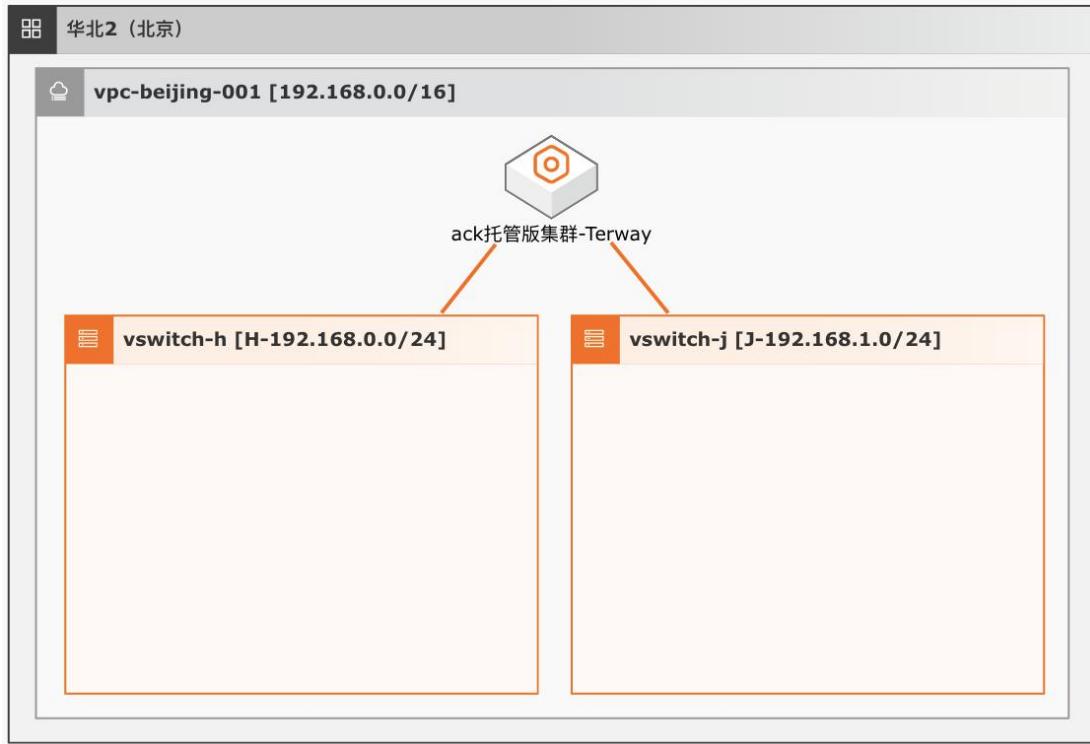
#### 方案架构

通过云速搭实现 ACK 的部署：

- Flannel 网络插件：



- Terway 网络插件：



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
ACK	vswitch 交换机
ECS	vswitch 交换机

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	vpc-beijing-001	192.168.0.0/16
AZ	vswitch-h	192.168.0.0/24
AZ	Vswitch-j	192.168.1.0/24
安全组	security_group	-

## 部署说明

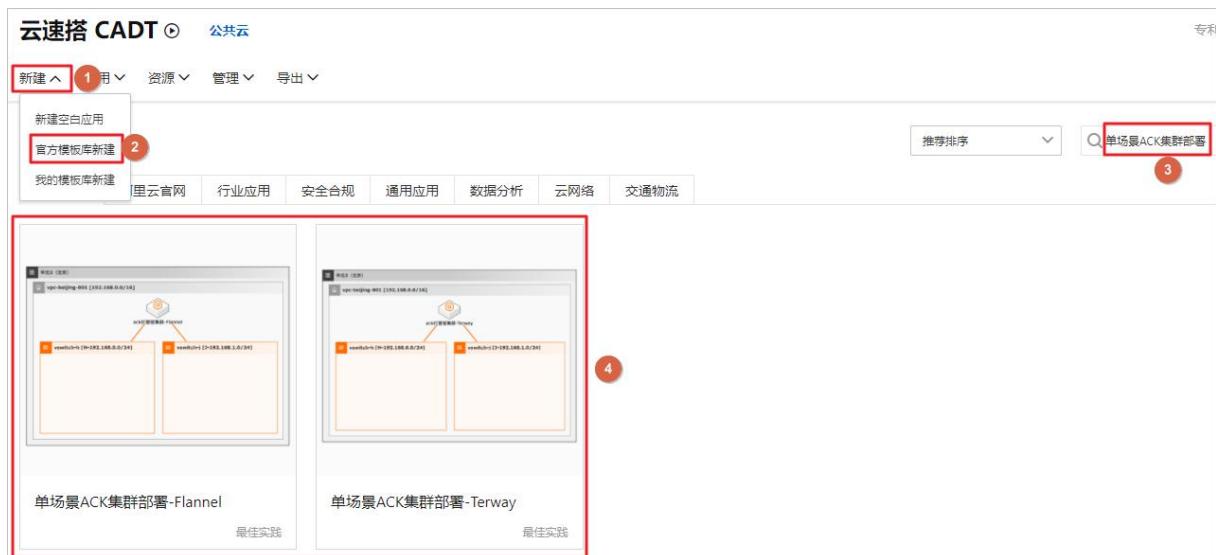
您可以通过 CADT 手动创建自定义应用来分别构建两种网络插件的 ACK 集群，请见 [2.1.1. 手动创建 ACK 集群](#)；另外，CADT 已将两种网络插件版本的 ACK 集群集成为模板供您使用，请见 [2.1.2. 基于官方模板新建 ACK 集群](#)。

- ACK 托管版集群-Flannel：

<https://bpstudio.console.aliyun.com/#/bpStudio/topo?TemplateId=8R11TI5A57Y1XFZB>

- ACK 托管版集群-Terway：

<https://bpstudio.console.aliyun.com/#/bpStudio/topo?TemplateId=7164C34SRRKJWLSG>



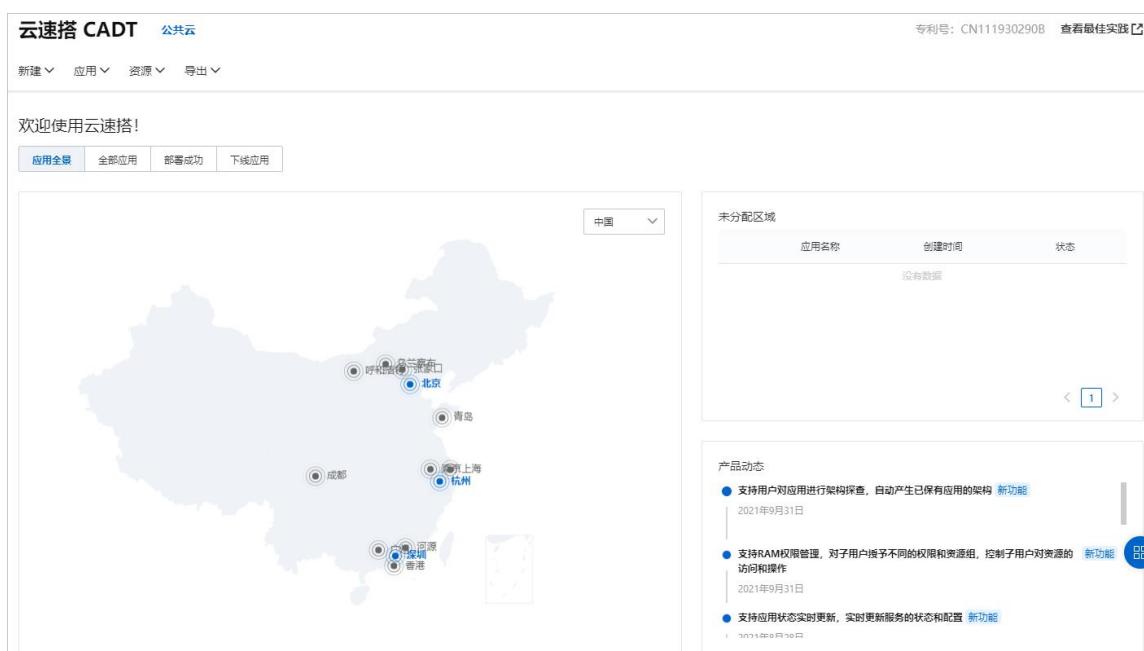
## 4.10.2.通过 CADT 创建 ACK 集群

### 4.10.2.1.手动创建 ACK 集群

本节向您介绍通过 CADT 手动创建 Flannel 网络插件和 Terway 网络插件的 ACK 集群。

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。



欢迎使用云速搭！

未分配区域

应用名称	创建时间	状态
无数据		

产品动态

- 支持用户对应用进行架构探查，自动生成已保有的架构 [新功能](#)
- 支持RAM权限管理，对子用户授予不同的权限和资源组，控制子用户对资源的 [访问和操作](#) [新功能](#)
- 支持应用状态实时更新，实时更新服务的状态和配置 [新功能](#)

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



云速搭 CADT 公共云

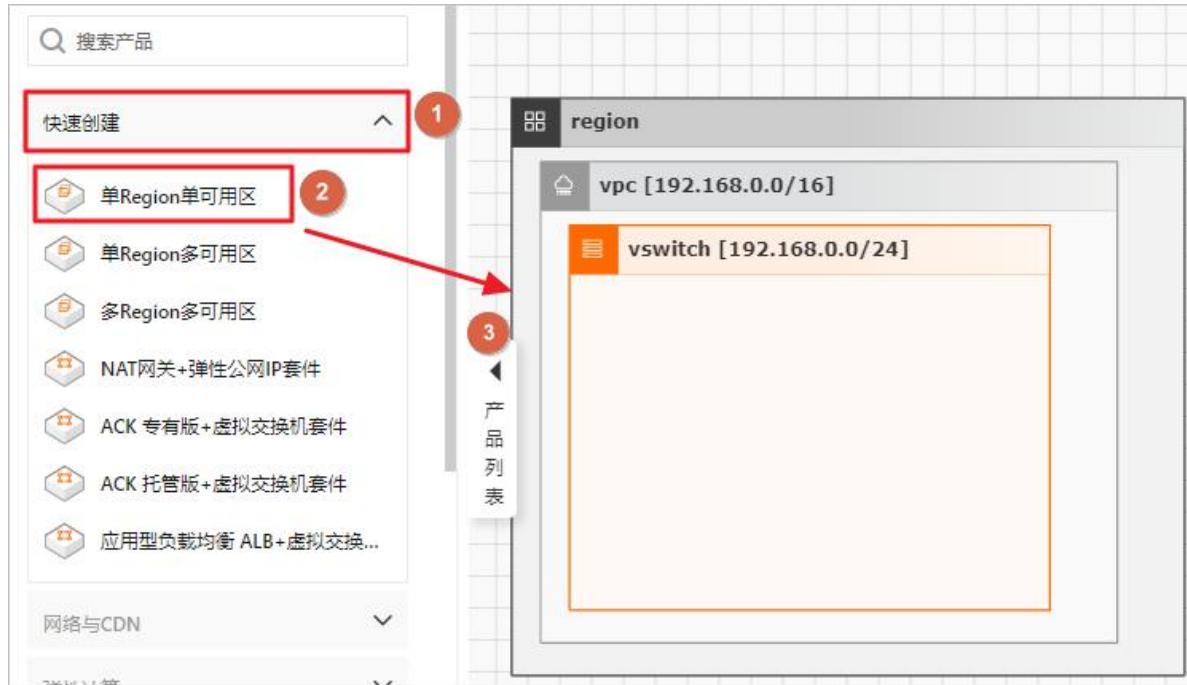
新建 ▾ ① 资源 ▾ 导出 ▾

② 新建空白应用

官方模板库新建  
我的模板库新建

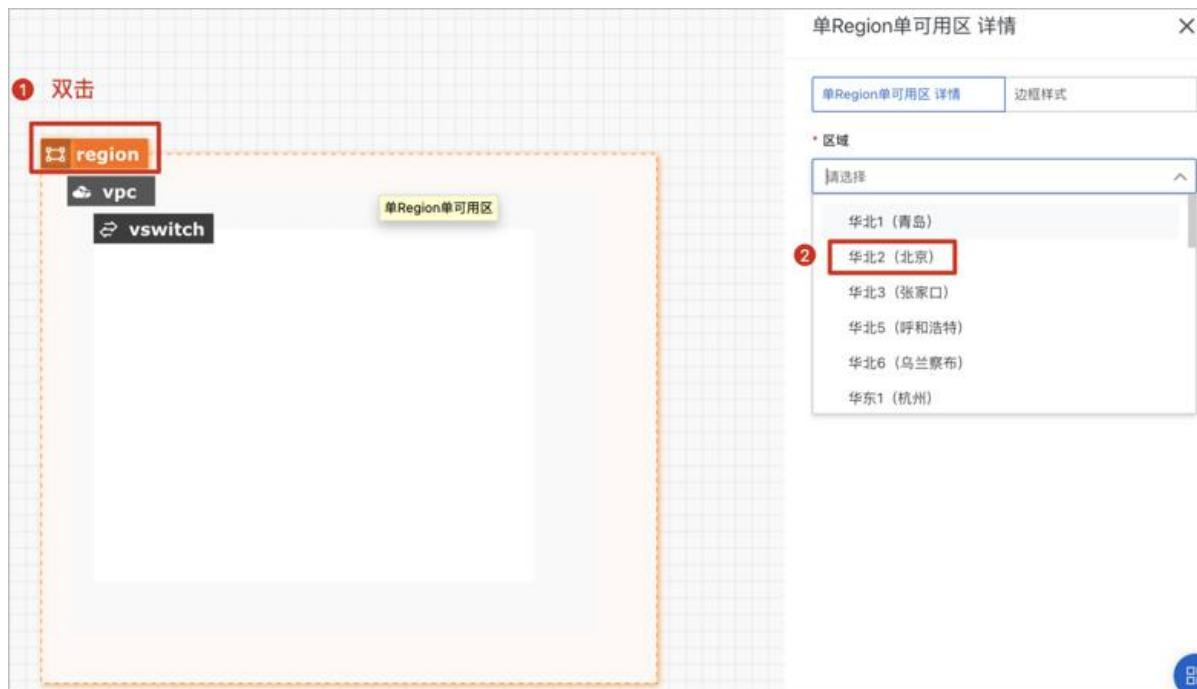
应用 部署成功 下线应用

步骤3 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

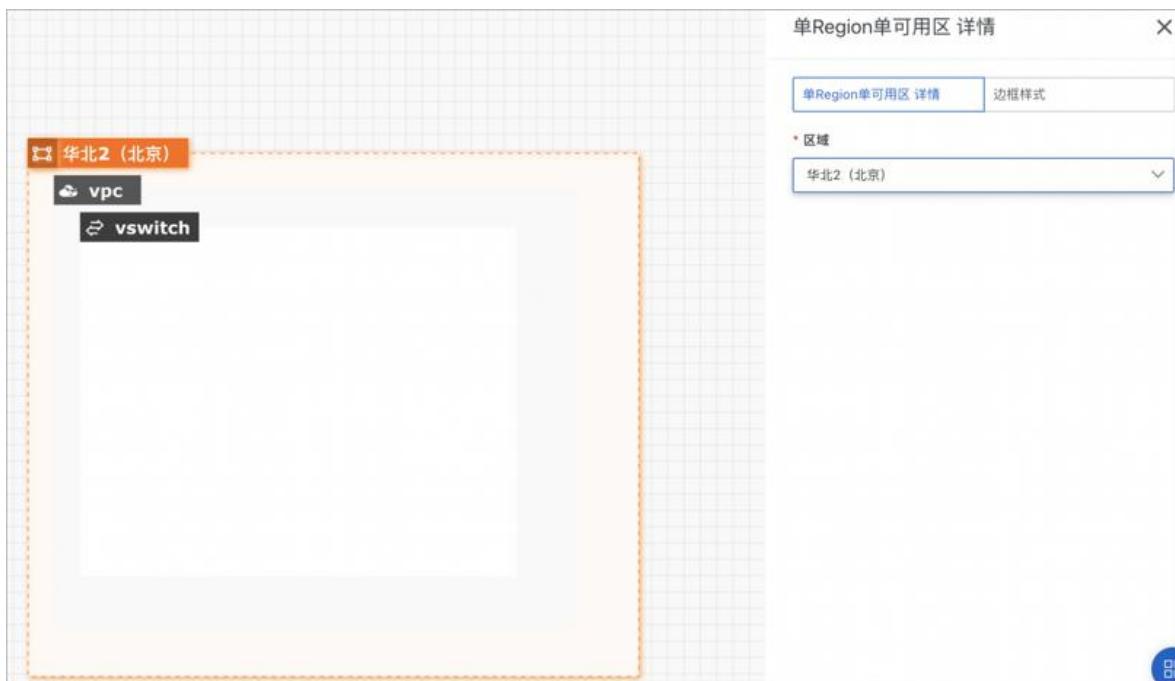


步骤4 依次双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北2（北京）。



选择后，如下图所示：



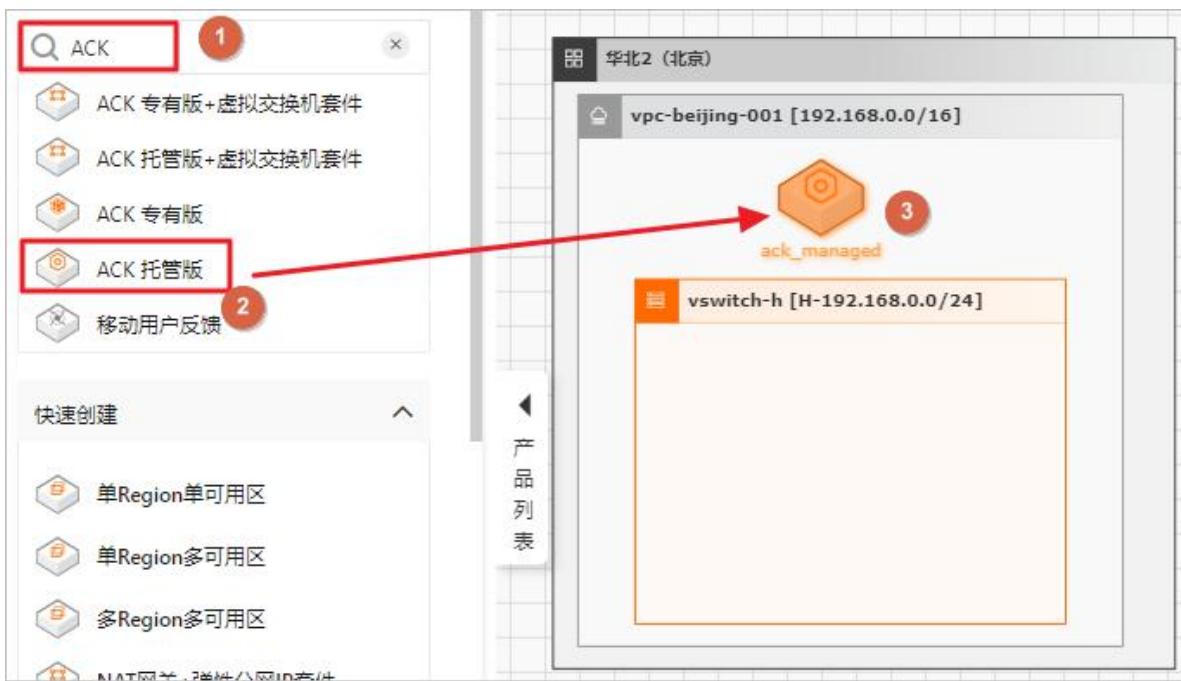
2. 双击 VPC，配置 VPC 参数。



3. 双击 Vswitch，配置 vswitch 参数。



步骤 5 左侧搜索 ACK 找到 ACK 托管版，拖到 vpc 中。



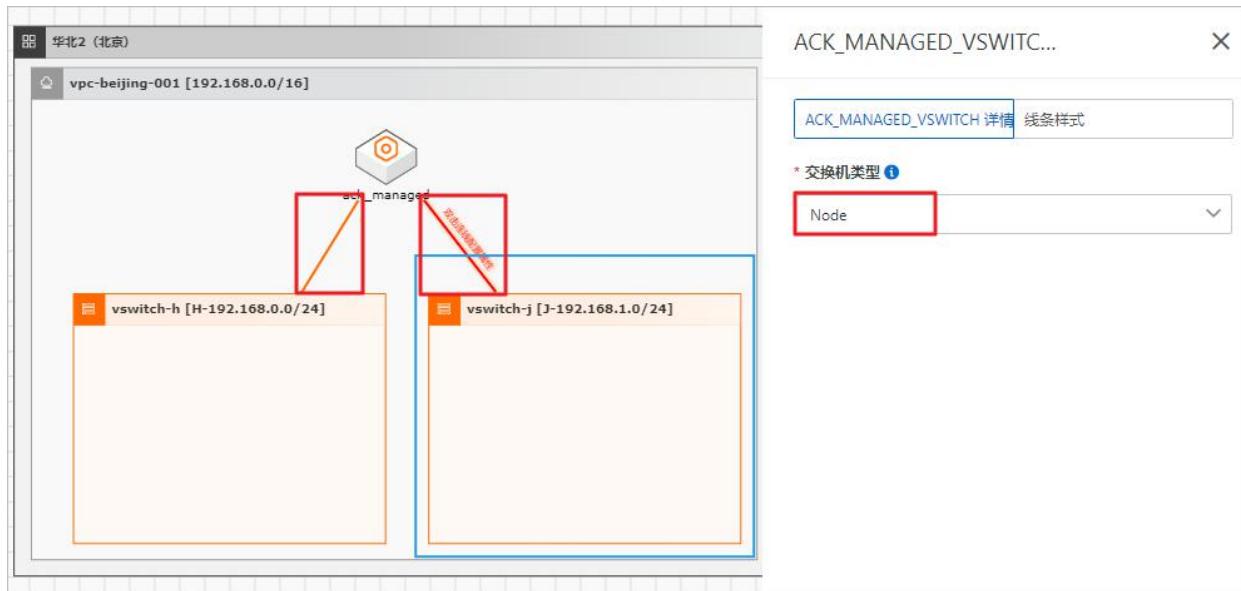
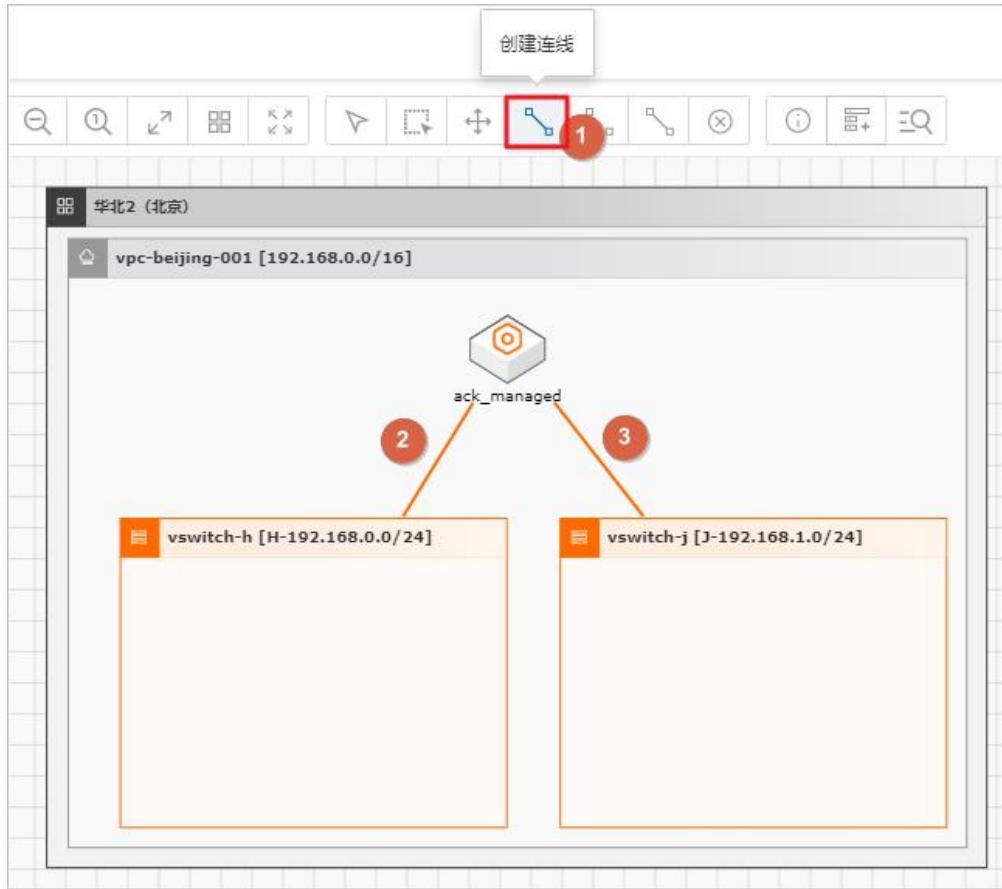
步骤 6 为了做到集群资源的 HA，创建另外一个 vswitch 子网。



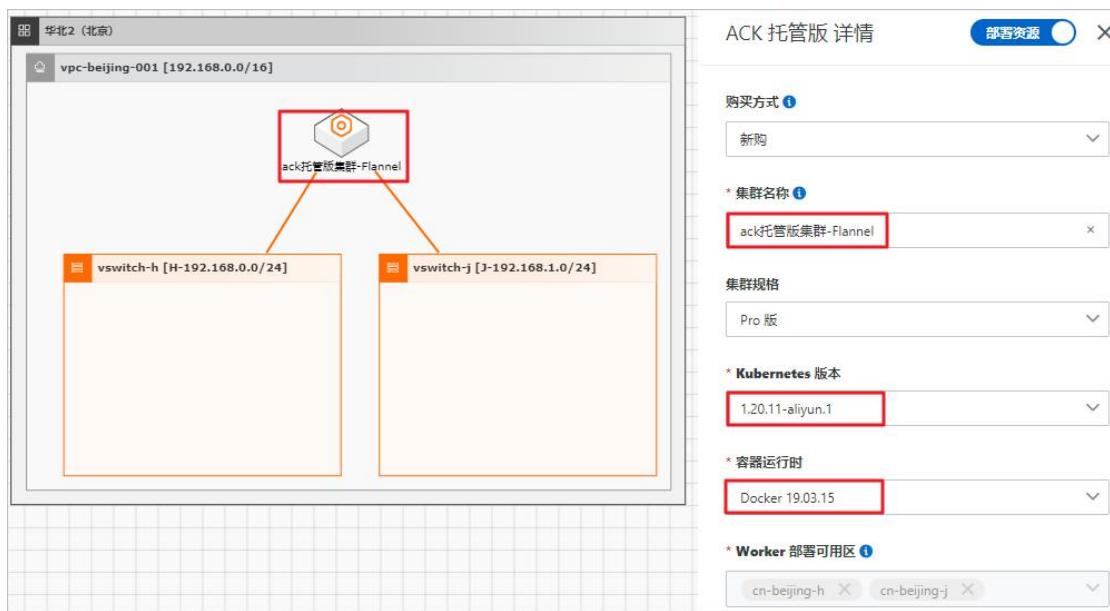
步骤 7 双击 vswitch，配置对应的网段和可用区。



步骤 8 将 ACK 集群和对应的可用区建立关联，并在连线上面选择交换机类型为 Node。



步骤 9 双击 ACK 集群，进行集群的配置，这里网络插件选择 Flannel。



### ACK 托管版 详情

**\* 网络插件** Flannel

**\* Pod 网络 CIDR** 10.30.0.0/16

**\* Service CIDR** 172.16.0.0/16

**\* 节点 IP 数量** 32

**配置 SNAT**  为专有网络配置 SNAT

**公网访问**  使用EIP 暴露 API Server

### ACK 托管版 详情

**\* API Server 访问** 标准型 (slb.s2.small)

**RDS白名单**

**安全组** 自动创建企业级安全组

**\* Worker 付费类型** 按量付费

**\* worker 实例规格** ecs.c6e.8xlarge (32c 64g) | ecs.hfc6.8xlarge (32c 64g)

**\* worker 数量** 4

\* worker 系统盘类型

cloud\_essd

性能级别

PL1 (单盘IOPS性能上限5万)

\* worker 系统盘大小

120

worker 挂载数据盘 i

worker\_data\_disks = [  
]  
+

\* worker 操作系统 i

Alibaba Cloud Linux

worker 登录方式

设置密码

\* 登录密码 i

..... x

\* 确认登录密码 i

..... x

Ingress

Nginx Ingress

服务发现

安装 NodeLocal DNSCache

负载均衡类型

内网

负载均衡类型

内网

\* 负载均衡规格

标准型I (slb.s2.small)

存储插件

CSI

监控插件

在 ECS 节点上安装云监控插件

日志服务

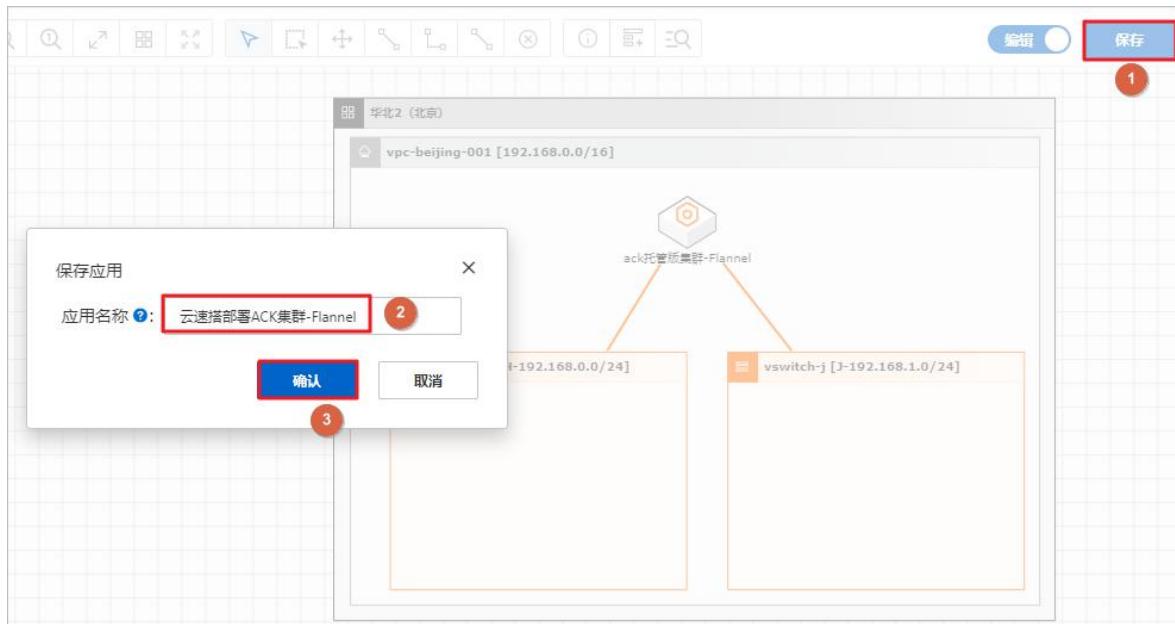
使用日志服务

资源组ID

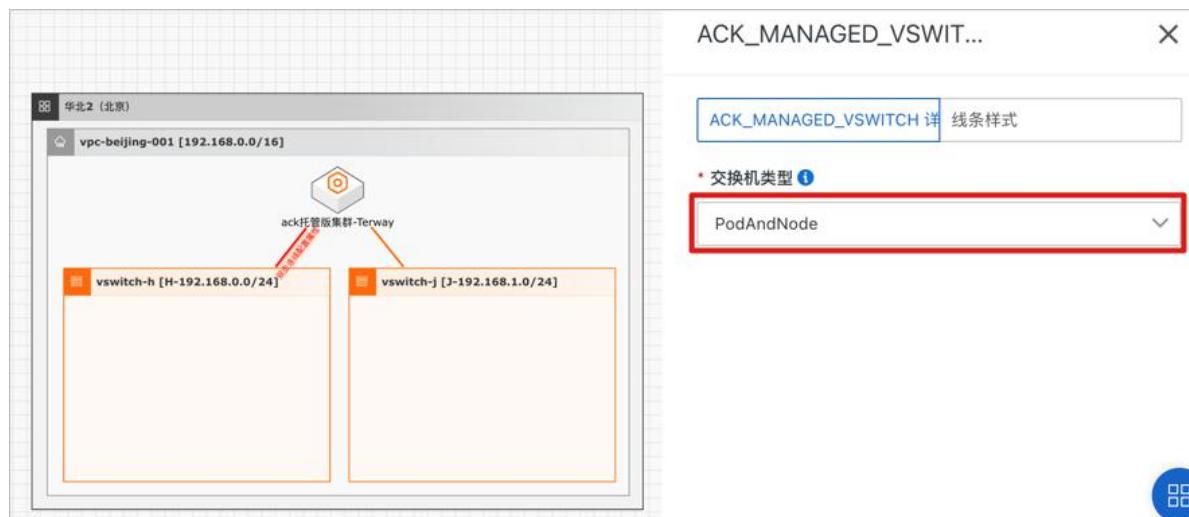
请选择

其他配置，采用默认即可。

步骤 10 配置完成后，单击右上角的保存，并设置应用名称。



步骤 11 关于 Terway 网络插件的集群，在于集群与 vswitch 边关系的不同，Terway 模式下您需要为每一个节点虚拟交换机指定至少一个相同可用区的 Pod 虚拟交换机；



#### 4.10.2.2. 基于官方模板新建 ACK 集群

本节向您介绍通过 CADT 官方模板创建 Flannel 网络插件和 Terway 网络插件的 ACK 集群。

步骤 1 登录云速搭 CADT 管理控制台。(<https://bpstudio.console.aliyun.com/>)

步骤 2 单击新建 > 官方模板库新建。



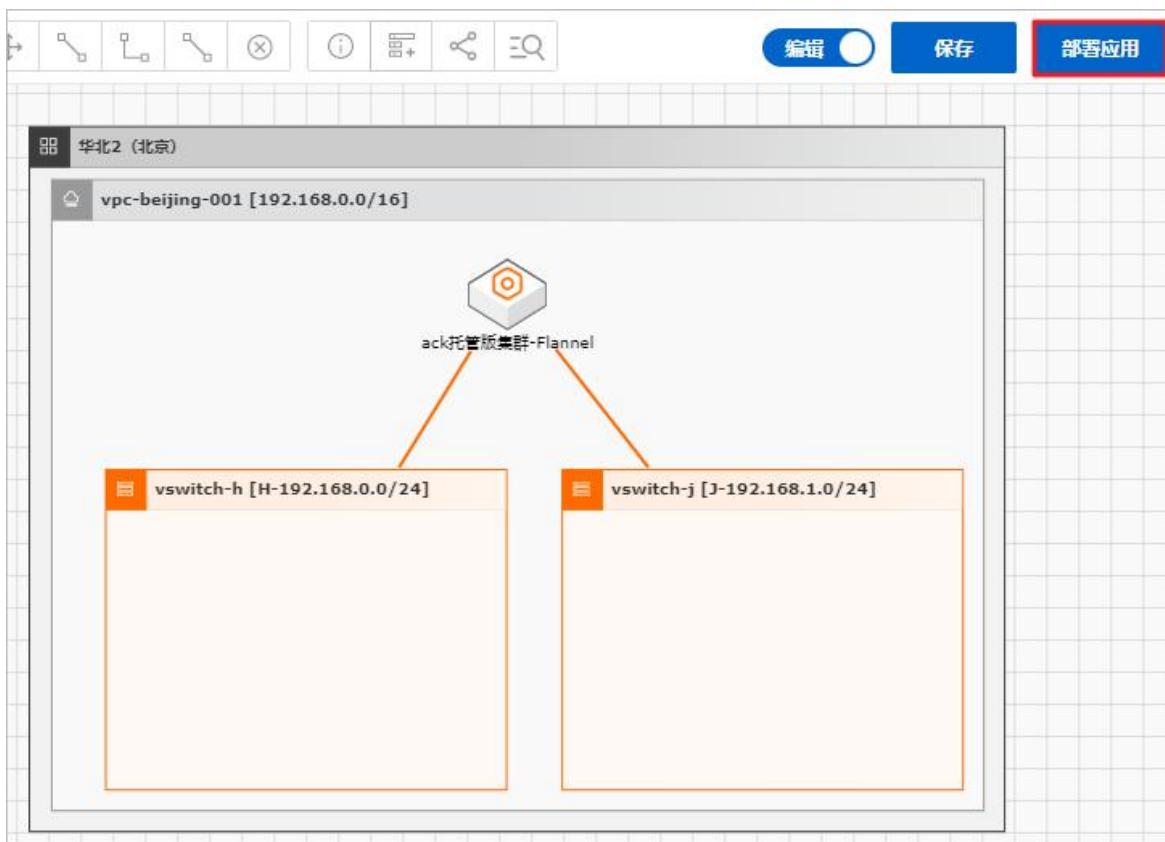
步骤 3 通过搜索关键字找到 ACK 集群部署模板，选择对应的模板，单击基于应用新建。



步骤 4 根据实际需要调整资源参数或直接保存为应用即可。

### 4.10.3. 部署应用

步骤 1 应用保存完成后，单击右上角的部署应用。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、资源是否有库存等，一般需要十几秒左右。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	ack托管版集群-Flannel	ack_managed	北京	1.20.11-aliyun.1	成功	校验通过	定位
2	vpc-beijing-001 [192.168.0.0/16]	vpc	北京	192.168.0.0/16	成功	校验通过	定位
3	vswitch-j [J-192.168.1.0/24]	vswitch	北京	192.168.1.0/24	成功	校验通过	定位
4	vswitch-h [H-192.168.0.0/24]	vswitch	北京	192.168.0.0/24	成功	校验通过	定位

状态:校验成功 下一步: 价格清单 返回

步骤 3 等待校验成功，单击下一步：价格清单。

导出价格清单

免费 按量付费

资源成本占比

暂无成本占比

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	状态	操作
1	ack托管版集群-Flannel	ack_manage_d	北京	1.20.11-aliyun.1	1			计费方式	新购	定位

状态: 计价成功

上一步: 资源校验 查看报告 下一步: 确认订单

步骤 4 可以单击[查看报告](#), 查看应用的价格信息。



**步骤 5 单击下一步：确认订单。**

**注意：**ACK 现在算不出来具体价格，以展示为主，按实际使用量计费，计费规则，请参考：

[https://help.aliyun.com/document\\_detail/86759.html](https://help.aliyun.com/document_detail/86759.html)

**步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。**

**注意：**部署流程一旦开始后，无法取消。

**确认订单**

免费	按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	ack托管版集群-Flannel	ack_managed	北京	1.20.11-aliyun.1	1			新购

《云速搭服务条款》

1 部署前，请阅读并勾选服务条款

2

状态：**计价成功**

上一步：价格清单

下一步：支付并创建

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc (专有网络VPC)	-	vpc-2zeduedefhdit3fys058l	运行中	2022-01-06 11:14:10	定位	
2	vswitch (虚拟交换机)	-	vsw-2zeri8zs7i1wfrusb350	运行中	2022-01-06 11:14:58	定位	
3	vswitch (虚拟交换机)	-	vsw-2zepqqqf2dbyi3qvothjc	运行中	2022-01-06 11:14:58	定位	

每页显示 10 共3条 < 上一页 1 下一页 >

**部署概要**

状态：部署中 应用编号：YMZX1R0E2UKLE1PQ

返回

**步骤 7 部署完成后，单击查看报告，可以查看本次的部署报告。**

资源部署状态

序号	资源名称 <a href="#">?</a> <a href="#">Q</a>	资源类型 <a href="#">Q</a>	付费类型	资源ID <a href="#">Q</a>	资源状态	资源更新时间	定位
1		vpc (专有网络VPC)	-	vpc-2zer1371on4isophblpcv <a href="#">D</a>	运行中	2022-01-10 11:23:32	定位
2		vswitch (虚拟交换机)	-	vsw-2zeo6lexofvgekoqdc62m <a href="#">D</a>	运行中	2022-01-10 11:24:36	定位
3		ack_managed (ACK 托管版)	-	c241b8fb4050b412f8d3bbcd218737f3f <a href="#">D</a>	运行中	2022-01-10 11:32:43	定位
4		vswitch (虚拟交换机)	-	vsw-2zep7qr6peb55iudu0q3m <a href="#">D</a>	运行中	2022-01-10 11:24:36	定位

每页显示  共4条 < 上一页 [1](#) 下一页 >

部署概要

状态: 部署成功 应用编号: LK8RAB7X9V53W08S

[查看报告](#) [返回](#)



步骤 8 单击返回，然后单击资源清单。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	免费	vpc-2zer1371on4isophblpcv	新建	运行中	2022-01-10 11:23:32	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
2	vswitch-h [H-192.168.0.0/24]	vswitch (虚拟交换机)	免费	vsw-2zeo6lexofygekoqdc62m	新建	运行中	2022-01-10 11:24:36	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>

每页显示 10 共4条 < 上一页 1 下一页 >

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

步骤 9 找到 ACK 集群，单击后面的**操作**，单击**查看详情**，可以看到如下拓扑。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
3	ack托管集群-Flannel	ack_managed (ACK 托管版)	按量付费	c241b8fb4050b412f8d3bbcd218737f3f	新建	运行中	2022-01-10 11:32:43	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
4	vswitch-j [J-192.168.1.0/24]	vswitch (虚拟交换机)	免费	vsw-2zeo7qr6peb55iudu0q3m	新建	运行中	2022-01-10 11:24:36	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">查看详情</a>

每页显示 10 共4条 < 上一页 1 下一页 >

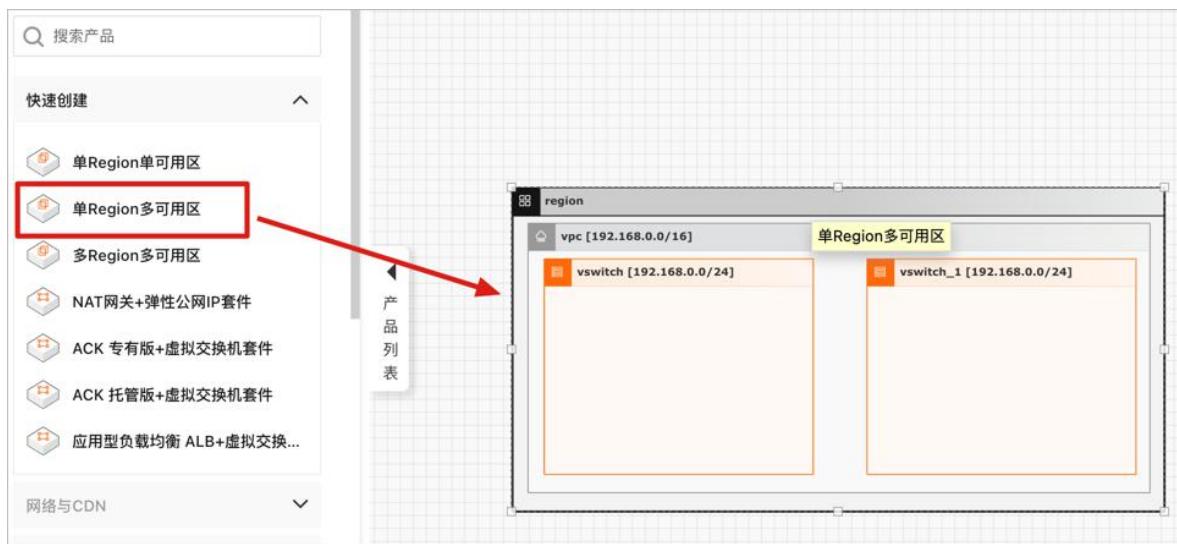


#### 4.10.4.导入已保有 ACK 应用架构

步骤 1 单击新建 > 新建空白应用。



步骤 2 从快速创建下找到单 region 多可用区，拖入到编辑窗口。



步骤 3 双击地域，选择北京。



步骤 4 双击 vpc，选择导入已保有，选择之前创建的 vpc。

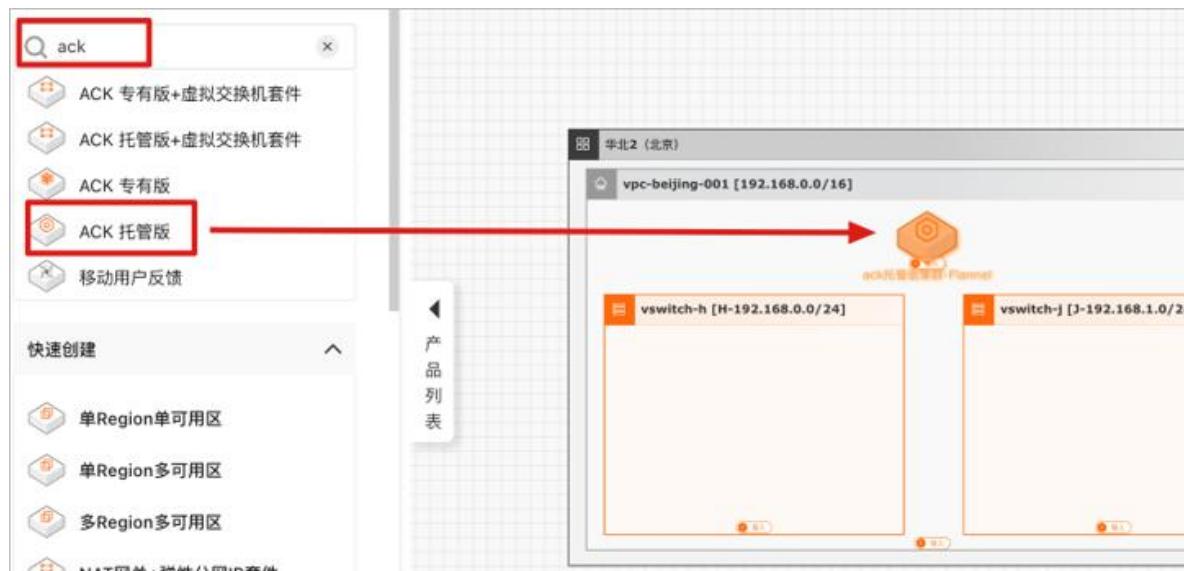


步骤 5 双击 vswitch，选择已保有，选择 vswitch。





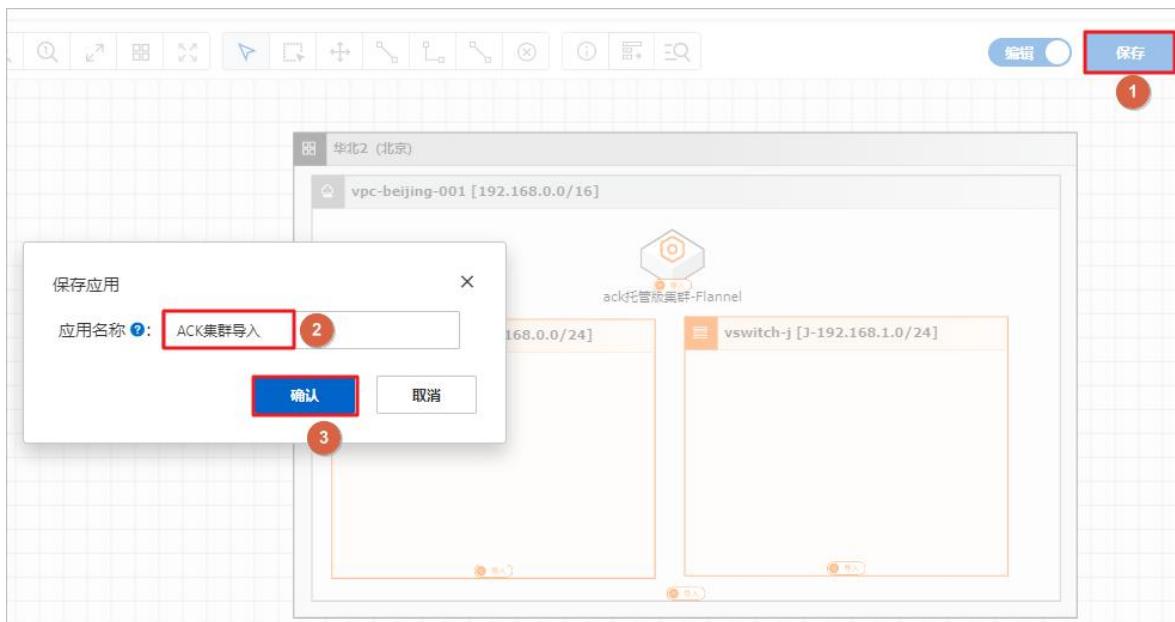
步骤 6 搜索 ACK 找到 ACK 托管版，并拖入 VPC 中。



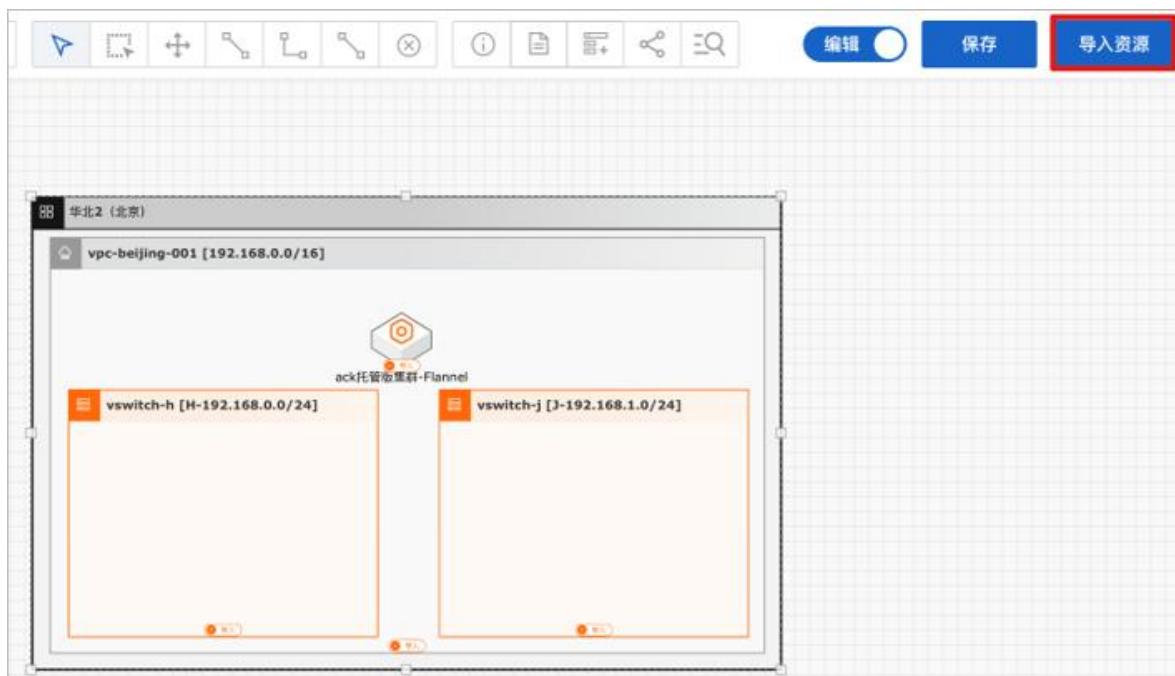
步骤 7 双击 ACK，选择导入已保有，选择之前创建的 ACK。



步骤 8 单击保存，输入应用名称。



步骤 9 单击导入资源。



步骤 10 单击导入。

**导入资源清单**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	定位
1	vpc-beijing-001 [192.168.0.0/16]	vpc	免费	vpc-2ze39vyvqaa51yattabo	待导入架构	定位
2	vswitch-h [H-192.168.0.0/24]	vswitch	免费	vsw-2zeolfbm580z7v4klqo5o	待导入架构	定位
3	vswitch-j [J-192.168.1.0/24]	vswitch	免费	vsw-2zebn9bnflmy1c67k3yo4	待导入架构	定位
4	ack托管版集群-Flannel	ack_managed	按量付费	c4d6b31a8045546b88521223517cbb d92	待导入架构	定位

① 注：新购资源，待导入成功后，再点击“部署应用”创建新的资源。

**导入**

步骤 11 导入成功后，如下图所示：

**资源导入状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-2ze39vyyvqaa51yattabo	运行中	-	定位
2	vswitch-h [H-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-2zeolfbm580z7v4klqo5o	运行中	-	定位
3	vswitch-j [J-192.168.1.0/24]	vswitch (虚拟交换机)	-	vsw-2zebn9bnflmy1c67k3yo4	运行中	-	定位
4	ack托管版集群-Flannel	ack_managed (ACK 托管版)	按量付费	c4d6b31a8045546b88521223517cbbd 92	运行中	-	定位

每页显示 10 共4条 < 上一页 1 下一页 >

**导入概要**

状态: 导入成功 应用编号: U0YFBUUSZ6R22UK8

[返回](#)

步骤 12 资源清单也会生成如下:

**ACK集群**

The screenshot shows the ACK Cluster management interface. At the top, there's a toolbar with various icons for navigation and operations. Below it is a network diagram titled "华北2 (北京)" showing three resources: "vpc-beijing-001 [192.168.0.0/16]", "vswitch-h [H-192.168.0.0/24]", and "vswitch-j [J-192.168.1.0/24]". A callout box points to the "资源清单" (Resource List) button at the bottom right of the diagram area. At the bottom of the screen is a table listing the imported resources.

应用操作	导出资源清单	历史版本	移出全部资源	同步资源数据				
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	操作
1	vpc-beijing-001 [192.168.0.0/16]	vpc (专有网络VPC)	免费	vpc-2ze39vyyvqaa51yattabo	已保有	运行中	-	
2	vswitch-h [H-192.168.0.0/24]	vswitch (虚拟交换机)	免费	vsw-2zeolfbm580z7v4klqo5o	已保有	运行中	-	

## 5.资源组合部署

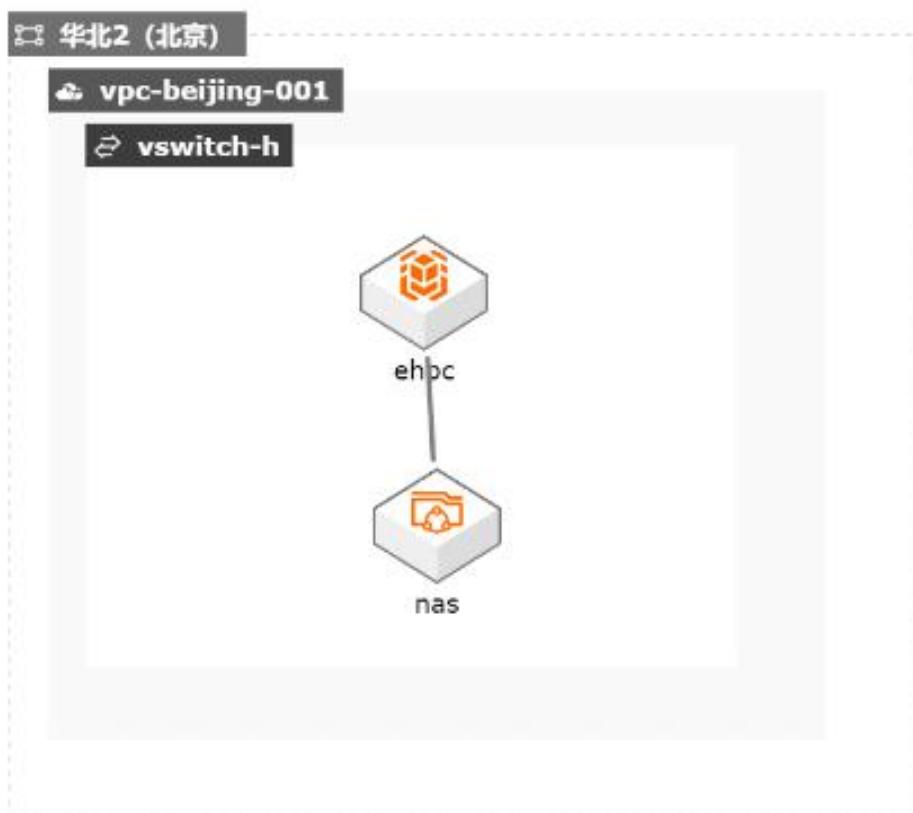
### 5.1.云速搭部署 E-HPC+NAS 应用

作者 | 阿里云解决方案架构师 敬海

#### 5.1.1.云速搭架构设计入门

##### 方案架构

通过云速搭实现最简单架构设计一个 E-HPC+NAS 的架构，构建一个实际可用的弹性高性能计算系统。



云资源	架构级别
VPC	Region 地域
E-HPC	vswitch 交换机
NAS	VPC 私有网络
ECS	vswitch 交换机

## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

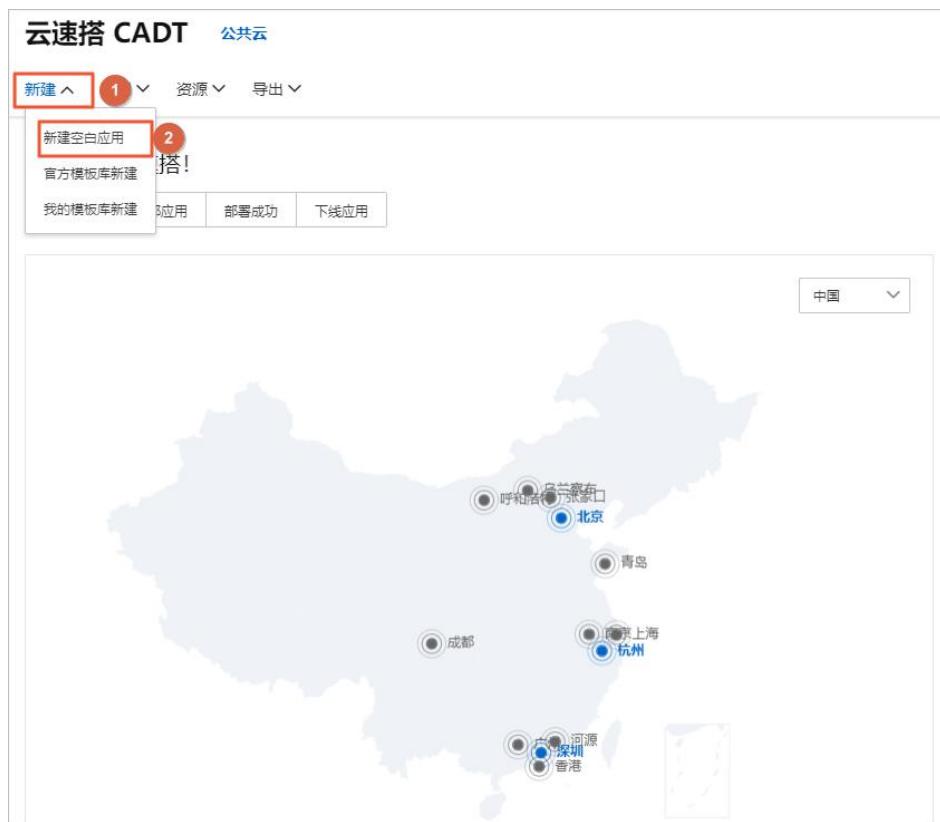
### 5.1.2. 应用架构设计

在进行应用架构设计时，可以提前进行资源规划。

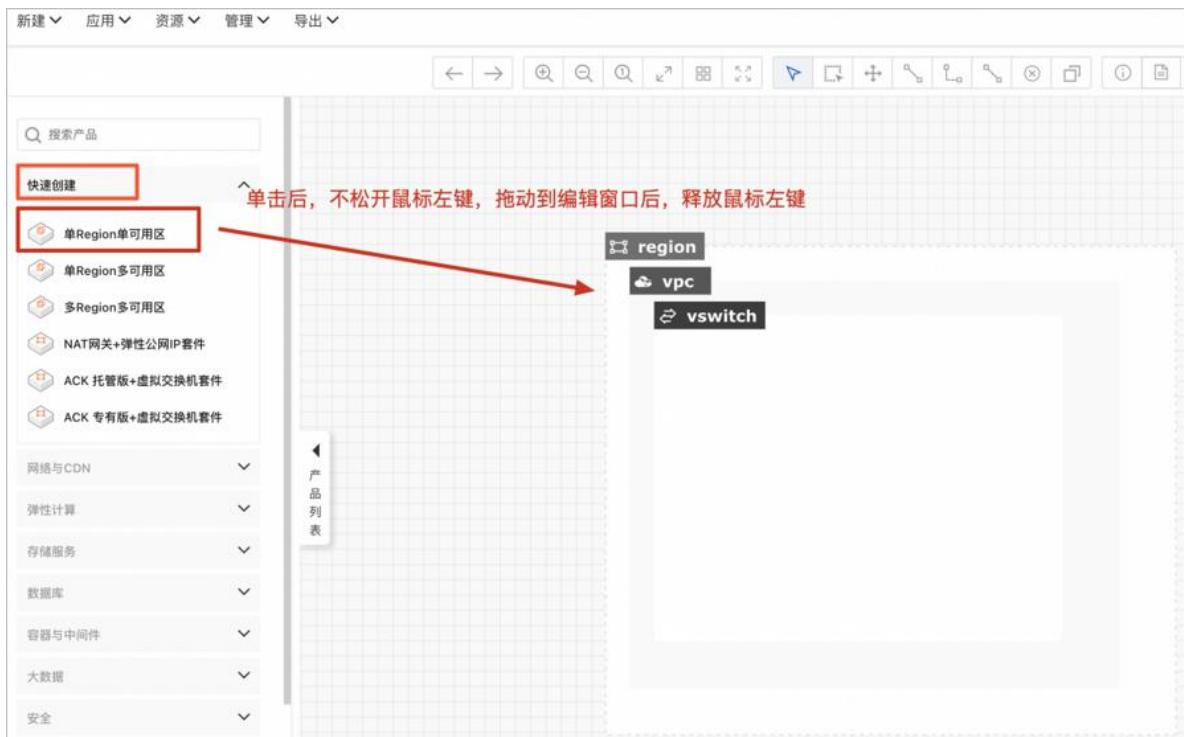
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	北京	-
VPC	VPC-BJ	192.168.0.0/16
AZ	北京 H 可用区	192.168.0.0/24
安全组	SG-BJ-TEST	-

步骤 1 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。

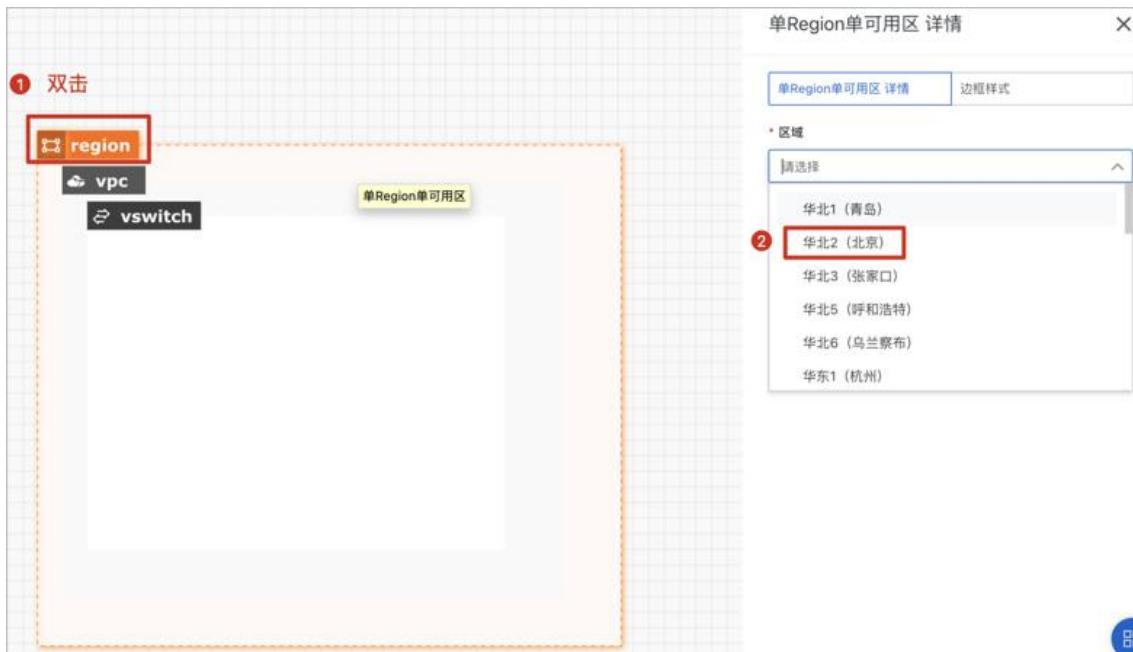


步骤 2 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。

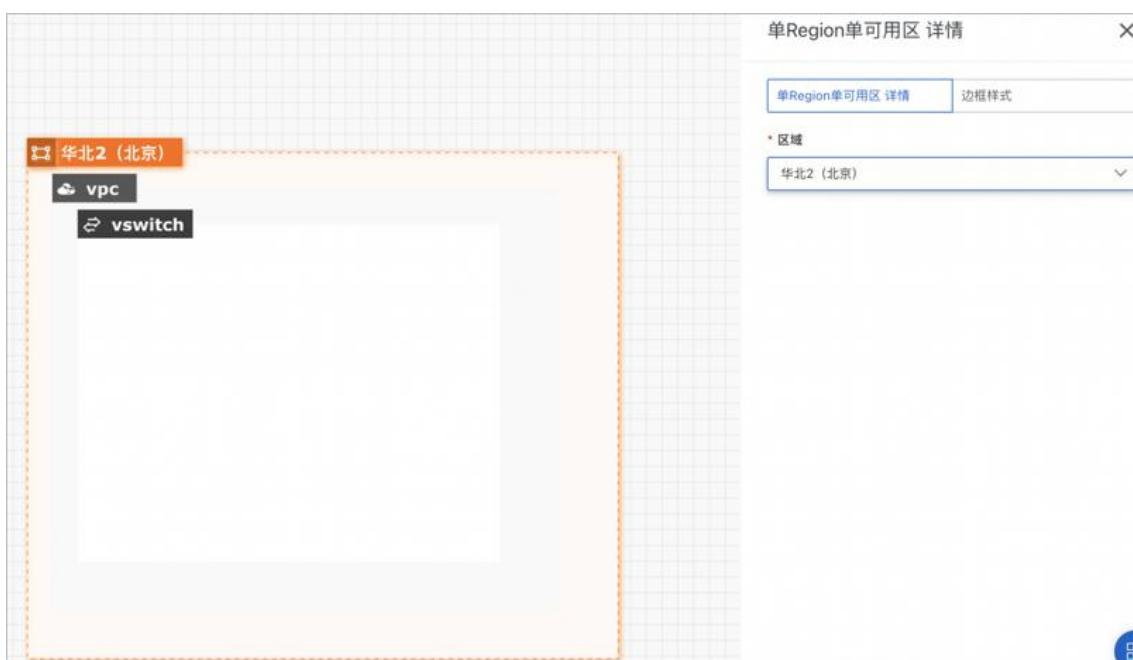


步骤3 依次双击Region、VPC、vswitch进行配置。

1. 双击region，在右侧弹出窗口中，选择华北2（北京）。



选择后，如下图所示：



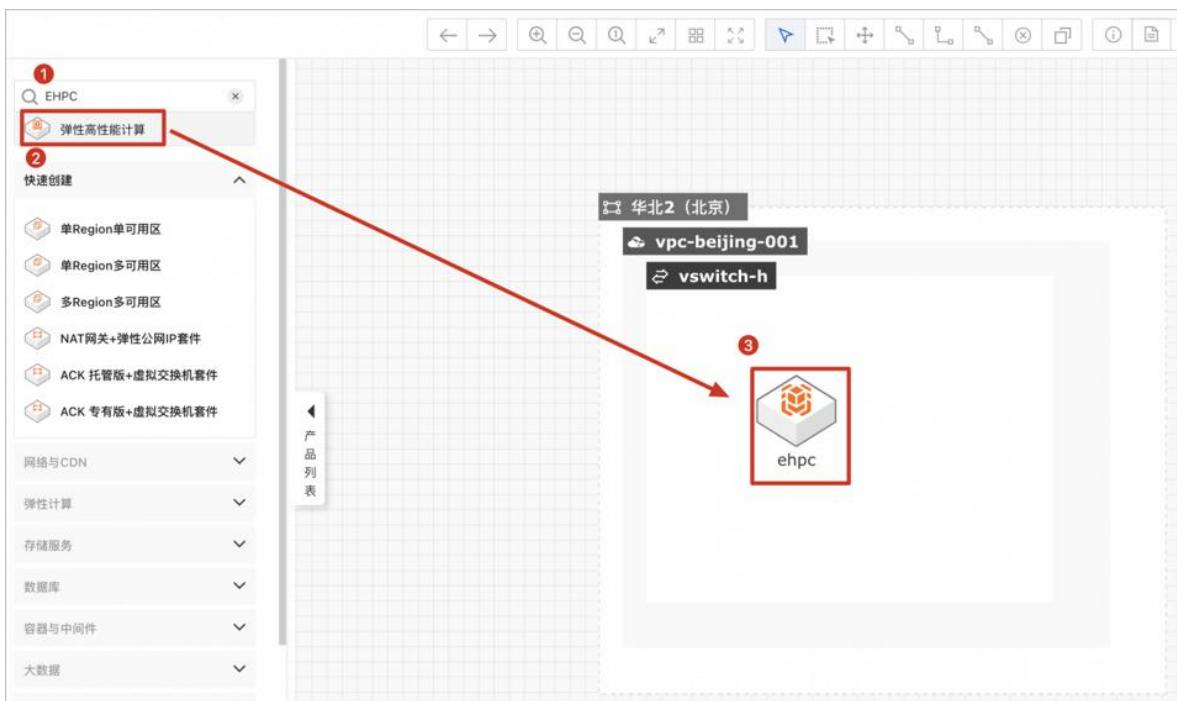
2. 双击VPC，配置VPC参数。



3. 双击 Vswitch，配置 vswitch 参数。



步骤 4 在左侧搜索框中输入 EHPC，选定弹性高性能计算，拖动到 vswitch 中。



步骤 5 双击 ehpc 组件，配置参数，这里输入一些示例配置。

### 弹性高性能计算 详情

部署资源

\* 集群名称 i

\* 支付方式

按量付费

\* 可用区

cn-beijing-h

部署方式 i

标准

\* 计算节点

ecs.n4.large(2c 4g)

\* 计算节点数量

1

\* 管控节点

ecs.n4.large(2c 4g)

\* 管控节点数量 i

2

### 登录节点

ecs.n4.large(2c 4g)

登录节点 i

1

\* 登录密码 i

.....

\* 确认登录密码 i

.....

\* 系统盘

cloud\_efficiency

系统盘容量 i

40 2000 40

\* 弹性公网IP

\* 新建安全组

**安全组名称** sg-ehpc-beijing-001

**镜像类型** 公共镜像

**镜像** CentOS\_7.6\_64

**按文件夹配置**

**文件类型** 通用型nas

**远程目录** /mnt

**调度器** pbs

**是否新建队列** 默认队列

**VNC**

**产品版本** 1.0.0

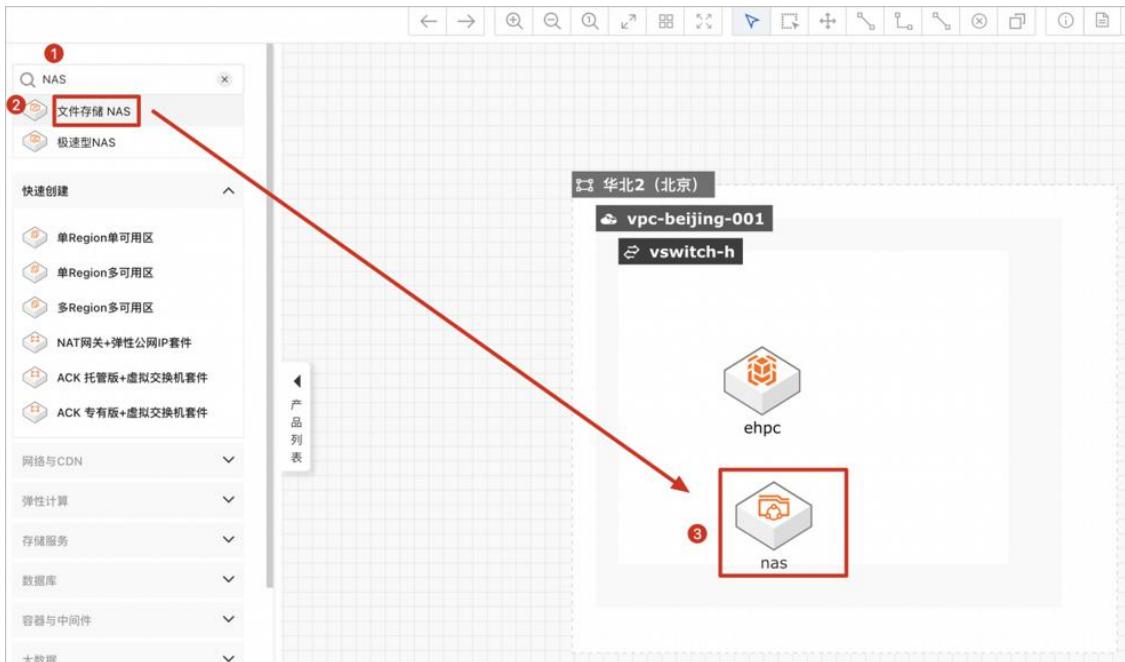
**域账号服务** nis

**其他软件** 无数据原因如下:  
1.当前vswitch所选可用区下无可售资源  
2.以上属性配置组合下无可售资源

**请选择**

**资源组选择** default resource group

步骤 6 在左侧搜索框中输入 NAS，选定文件存储 NAS，拖动到 vswitch 中。



步骤 7 双击 NAS 图标，配置 NAS 参数。

文件存储 NAS 详情

部署资源  X

购买方式

\* NAS名称

\* 支付方式

\* 可用区

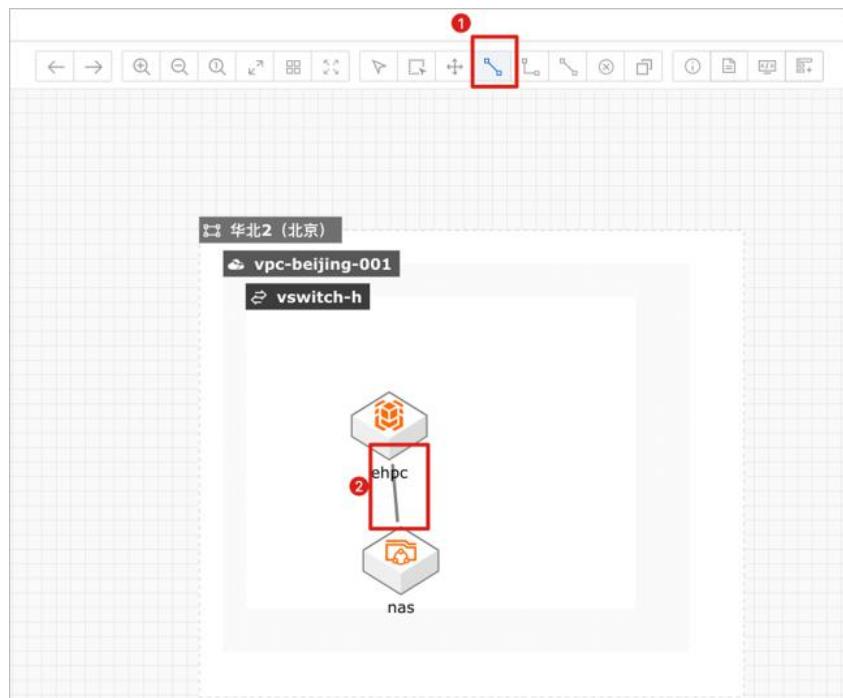
\* 存储规格

\* 协议类型

是否加密

\* 生命管理周期

步骤 8 单击创建连线按钮，切换到连线模式，将 EHPC 和 NAS 连接起来，这条线连接表示将 NAS 挂载到 EHPC 的集群上，所有实例都会挂载这个 NAS 实例。

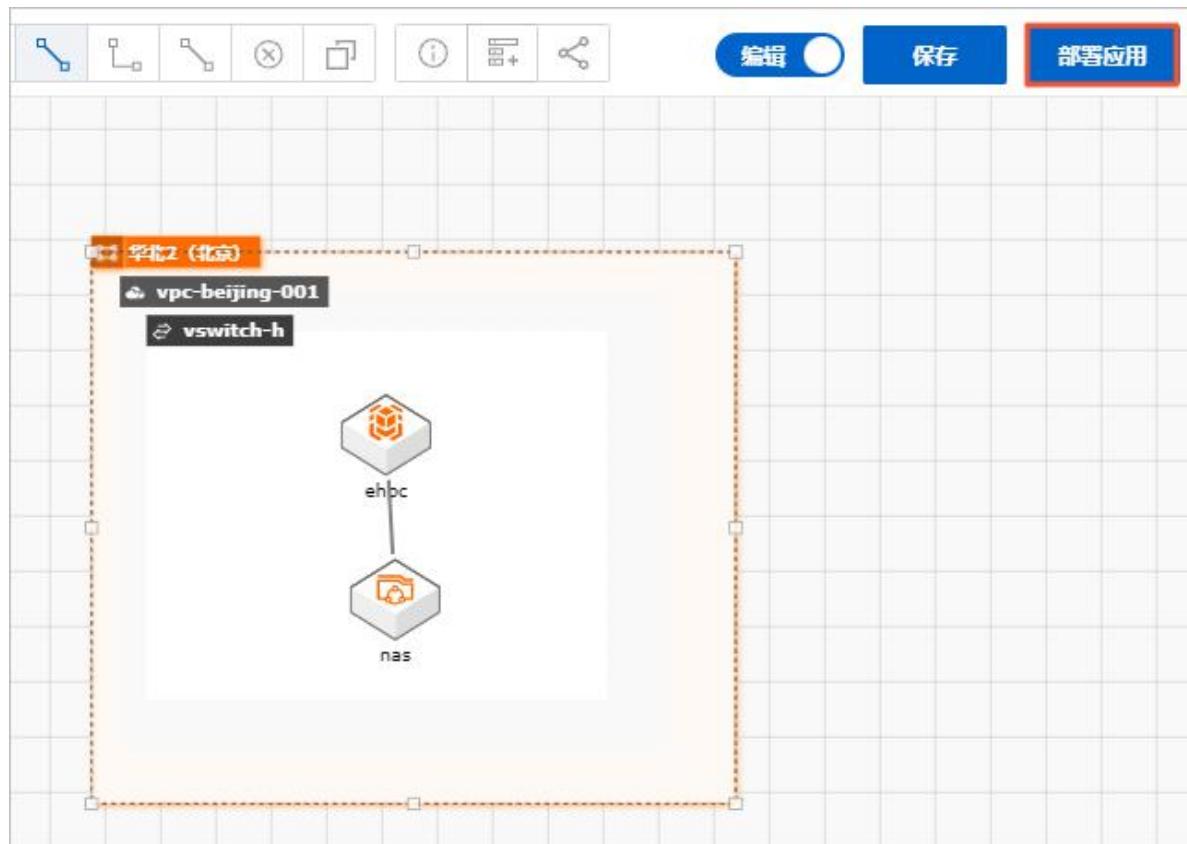


步骤 9 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写应用名称，并单击**确认**。



### 5.1.3. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、ECS 是否有库存等，一般需要几十秒左右。

**资源验证**

资源名称	资源类型	区域	规格	结果	备注	操作
nas	nas	北京	hybrid	成功	校验通过	定位
vswitch-h	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
vpc-beijing-001	vpc	北京	192.168.0.0/16	成功	校验通过	定位
ehpc	ehpc	北京	ecs.n4.small	成功	校验通过	定位

状态:校验成功

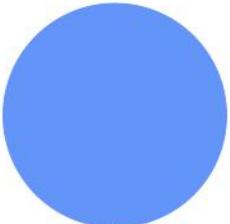
[下一步: 价格清单](#) [返回](#)

步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息，由于 nas 这里选择了按量付费，暂时没有数据存储到 nas，所以价格不会显示。

**导出价格清单**

[免费](#) [按量付费](#)

资源成本占比



资源预算  
● 计算 计算: 元/时

100%

价格列表

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
ehpc	ehpc	北京	ecs.n4.large	1	2.92元/时	元/时	元/时	定位
nas	nas	北京	hybrid	1				定位

状态: 计价成功

[上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

步骤 4 可以单击**查看报告**，查看应用的价格信息。



步骤 5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

**确认订单**

**按量付费**

资源名称	资源类型	区域	规格	数量	原价	实付	状态
nas	nas	北京	hybrid	1			新购
ehpc	ehpc	北京	ecs.n4.large	1	2.92元/时	元/时	新购

《云速搭服务条款》

① 部署前，请阅读并勾选服务条款

按量付费：   元/时

状态：计价成功

② [上一步: 价格清单](#) [下一步: 支付并创建](#)

步骤 6 单击下一步：支付并创建，就会进入部署流程，这里会进行扣费并开始创建资源。

**注意：**部署流程一旦开始后，无法取消。



部署过程大致分为三个阶段：

- 第一阶段：按照依赖顺序创建应用内的资源，比如先创建全局资源，然后是地域级资源，然后是 vpc 级别的资源，然后是 vswitch 级别的资源。这里是先创建 vpc，再创建 vswitch，然后是 e-hpc 和 nas。
- 第二阶段：创建连线代表的配置关系，这里是创建 nas 的挂载点，挂载到 ehpc 集群。
- 第三阶段：生成部署报告和资源清单，其中资源清单列表中还包括了监控，常用操作等。

步骤 7 部署完成后，如下图所示。

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
vpc-beijing-00 1	vpc	-	vpc-2zey7mgagrbmkjucscjz	运行中	2021-10-21 17:44:51	定位
vswitch-h	vswitch	-	vsw-2zevcq4wa9n7gjwPIP93o	运行中	2021-10-21 17:44:51	定位
nas	nas	按量付费	1a6cf49576	运行中	2021-10-21 17:44:51	定位
ehpc	ehpc	-	ehpc-bj-e8ZYtv6YLT	运行中	2021-10-22 09:58:02	定位

**部署概要**

状态: 部署成功 方案编号: HC80P8WFYBEU3C3E

**查看报告** **返回**

步骤 8 单击**查看报告**，可以查看本次的部署报告。



步骤 9 单击返回，然后单击资源清单。

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位	操作
vpc-beijing-001	vpc	-	vpc-2zeey7mgagrbmkjucscjtz	运行中	2021-10-21 17:44:51	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
vswitch-h	vswitch	-	vsw-2zevcq4wa9n7gjwpp93o	运行中	2021-10-21 17:44:51	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a> <a href="#">操作</a>
nas	nas	按量付费	1a6cf49576	运行中	2021-10-21 17:44:51	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a>
ehpc	ehpc	-	ehpc-bj-e8ZYtv6YLT	运行中	2021-10-22 09:58:02	定位	<a href="#">详情</a> <a href="#">监控</a> <a href="#">变更日志</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。单击**监控**，直接跳到对应资源的云监控页面。

## 5.1.4. 部署结果验证

步骤 1 单击 ehpc，跳转到 ehpc 控制台查看。

The screenshot shows the AliCloud Ehpc console interface. On the left, there's a sidebar with '弹性高性能计算' (Elastic High Performance Computing) selected, followed by '集群管理' (Cluster Management). Under '集群管理', there are several options: '节点与队列' (Nodes and Queues), '调度器' (Scheduler), '用户' (Users), '共享存储' (Shared Storage), and '高性能容器应用' (High-performance Container Application). The main area is titled 'ehpc 运行中' (ehpc Running). It displays basic information about the cluster, including its ID ('集群ID: ehpc-bj-e8ZYtv6YLT'), public IP ('公网IP: 123.57.229.47'), and creation time ('创建时间: 2021年10月22日 09:53:23'). To the right, there's a summary section with three circular progress bars: one for '正常计算节点/总计节点' (Normal Calculation Nodes / Total Nodes) showing 1/1, another for '已用内存/总内存(GB)' (Used Memory / Total Memory (GB)) showing 0/4, and a third for '已用存储/总存储(GB)' (Used Storage / Total Storage (GB)) showing 0/2. Below these bars are buttons for '刷新' (Refresh), '创建集群' (Create Cluster), and '更多' (More).

这里可以看到 ehpc 集群已经创建成功。

步骤 2 单击详情，查看 ehpc 详情信息

这里可以看到，nas 实例已经挂载到了集群上：

This screenshot shows the 'ehpc' cluster details page. On the left, there's a sidebar with '返回' (Back) and '集群详情' (Cluster Details). The main content area has tabs for '基本信息' (Basic Information), '节点信息' (Node Information), and '存储信息' (Storage Information). The '基本信息' tab shows the cluster ID ('集群ID: ehpc-bj-e8ZYtv6YLT'), VPC ID ('VPC ID: vpc-2zey7mgagrbmkjucscjz'), and other parameters like status ('状态: 运行中') and exchange machine ID ('交换机ID: vsw-2zevcq4wa9n7gjwplp93o'). The '节点信息' tab provides details about managed nodes ('管控节点数量: 2', '管控节点规格: ecs.n4.large (CPU: 2核 内存: 4GB)'), calculation nodes ('计算节点数量: 1', '计算节点规格: ecs.n4.large (CPU: 2核 内存: 4GB)'), and login nodes ('登录节点数量: 1', '登录节点规格: ecs.n4.large (CPU: 2核 内存: 4GB)'). The '存储信息' tab, which is highlighted with a red box, shows the storage configuration: '存储类型: nas', '存储实例ID: 1a6cf49576', '挂载协议: nfs', '挂载点: 1a6cf49576-pip87.cn-beijing.nas.aliyuncs.com', and '远程挂载目录: /mnt'. The '存储信息' tab also includes a note: '注意: 在使用 NFS 协议挂载时, 请确保挂载点在 Linux 系统中存在且权限正确。' (Note: When using the NFS protocol to mount, please ensure that the mounting point exists in the Linux system and has the correct permissions.)

步骤 3 获取 ehpc 集群的连接地址，使用 ssh 登录。

```
ssh root@${IP}
```

```
jh@MAC ~ $ ssh root@123.***.29.47
The authenticity of host '123.***.29.47 (123.***.29.47)' can't be established.
ECDSA key fingerprint is SHA256:mHckjZaYd80A00jdd6q5YnggahniWp2Ta+jzZ8RyBds.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '123.***.29.47' (ECDSA) to the list of known hosts.
root@123.***.29.47's password:

Welcome to Alibaba Cloud Elastic Compute Service !
```

步骤4 查看挂载情况，之前我们指定了挂载目录 `/mnt`，会将 nas 根目录下的 `/mnt` 挂载到主机的`/ehpcdata` 目录下。

```
[root@login0 ~]# df -h
文件系统                                容量  已用  可用  已用% 挂载点
/dev/vda1                               40G   3.6G  34G   10% /
devtmpfs                                1.9G    0   1.9G   0% /dev
tmpfs                                    1.9G    0   1.9G   0% /dev/shm
tmpfs                                    1.9G  544K  1.9G   1% /run
tmpfs                                    1.9G    0   1.9G   0% /sys/fs/cgroup
tmpfs                                    379M    0  379M   0% /run/user/0
1a6cf49576-pip87.cn-beijing.nas.aliyuncs.com:/mnt          10P   51M  10P   1% /ehpcdata
1a6cf49576-pip87.cn-beijing.nas.aliyuncs.com:/mnt/ehpc-bj-e8ZYtv6YLT/opt  10P   51M  10P   1% /opt
1a6cf49576-pip87.cn-beijing.nas.aliyuncs.com:/mnt/ehpc-bj-e8ZYtv6YLT/home  10P   51M  10P   1% /home
```

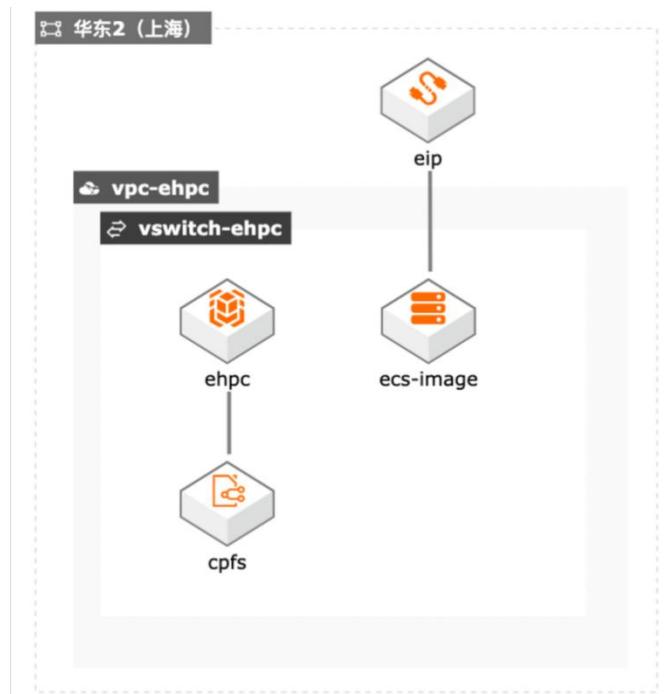
## 5.2.云速搭部署挂载 CPFS 的 E-HPC

作者 | 阿里云解决方案架构师 天裴

### 5.2.1. 云速搭架构设计入门

#### 方案简介

- 本最佳实践讲解如何通过云速搭部署一个挂载 CPFS 的 E-HPC 集群。



- 以 CPFS 为共享存储的 E-HPC 集群，在创建之前必须事先制作好安装了 CPFS 客户端的自定义镜像，再通过该镜像创建 E-HPC 集群。
- CPFS 在 E-HPC 中的使用有如下限制：
  - 一个 CPFS 文件系统只能供一个 E-HPC 集群使用。
  - CPFS 客户端仅支持 CentOS (7.2、7.3、7.4、7.6) 操作系统。
  - 扩容集群时，只能选择创建集群时的自定义镜像对集群进行扩容，否则会出现集群异常。
- 注意事项：**对于现有版本的 CPFS，EHPG 集群必须创建在与 CPFS 相同的虚拟交换机下。在近期的 CPFS 迭代中，将会支持同 VPC 下的不同虚拟交换机。

## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下图，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
弹性公网 IP	Region
云服务器 ECS	Vswitch
文件存储 CPFS	Vswitch
弹性高性能计算	Vswitch

## 资源配置清单

本例中我们按照以下规格部署资源：

资源类别	配置项	配置明细
区域	区域	华东 2 (上海)
专有网络 VPC	状态	新购
	VPC 名	vpc-ehpc
	网段	192.168.0.0/16
虚拟交换机	状态	新购
	vswitch 名	vswitch-ehpc
	可用区	华东 2 可用区 L
	IPv4 网段	192.168.0.0/24
EIP	付费类型	按量付费
	网络类型	公网
	公网带宽	按流量付费
	带宽	5Mbps
ECS	规格	ecs.c6.xlarge (4C/8G)
	实例名	ecs-image
	主机名	ecs-image

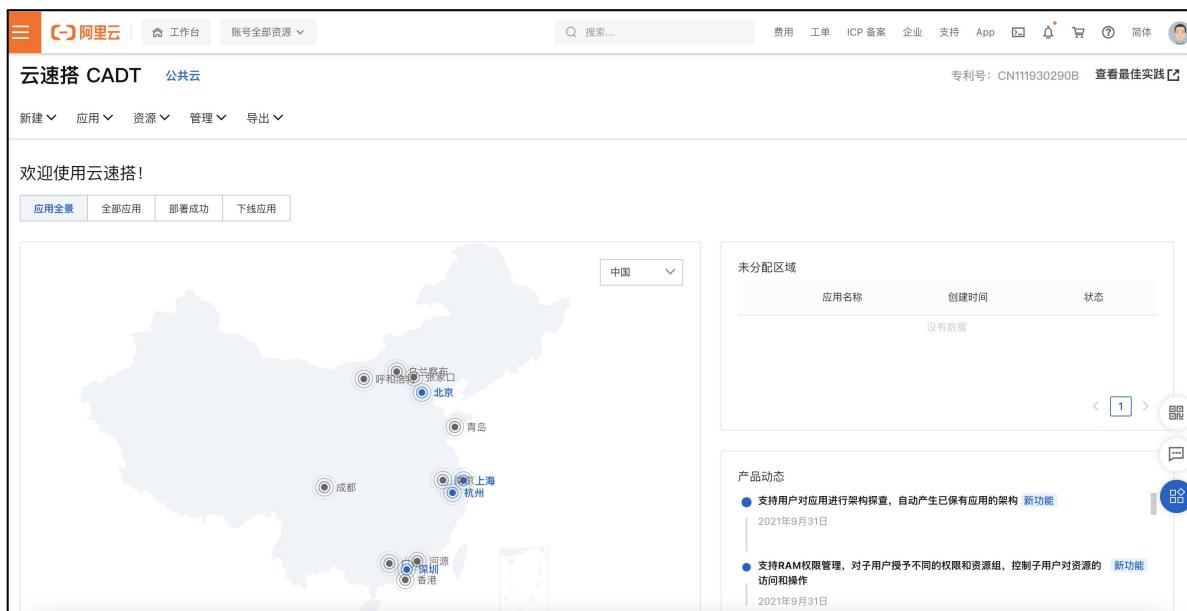
资源类别	配置项	配置明细
ECS	付费类型	按量付费
	镜像及版本	Centos 7.6 64 位
	系统盘及容量	ESSD 40GB
	登录密码	(自定义, 密码将在后续 <a href="#">章节 5.2.3.5</a> 中使用)
CPFS	支付方式	按量付费
	存储类型	100MB/sTiB 基线
	容量	4800GB
E-HPC	支付方式	按量付费
	部署方式	标准
	计算节点	ecs.c6.xlarge
	计算节点数量	1
	管控节点	ecs.c6.xlarge
	管控节点数量	2
	登录节点	ecs.c6.xlarge
	登录节点数量	1
	登录密码	(自定义)
	系统盘	cloud_essd
	系统盘容量	40G
	性能级别	PL0
	弹性公网 IP	(无需启用)
	新建安全组	启用
	安全组名称	sg-ehpc
	镜像类型	自定义镜像
	镜像	(选择在 <a href="#">章节 5.2.3.7</a> 中创建的自定义镜像)
	文件类型	CPFS
	调度器	custom (不安装调度器), E-HPC 提供丰富的调度器, 本例中不安装
	VNC	启用
	产品版本	1.0.0
	域账号服务	nis (E-HPC 提供 nis 和 ldap 两种域账号服务, 本例选择 nis, 也可选择 custom 不安装域账号服务)

## 5.2.2.部署 CPFS 和 ECS

### 5.2.2.1.创建基础网络资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。



The screenshot shows the Cloud Speed Stack (CADT) control console interface. At the top, there's a navigation bar with links for '费用' (Billing), '工单' (Work Orders), 'ICP 备案' (ICP Record Filing), '企业' (Enterprise), '支持' (Support), 'App' (Application), and a search bar. Below the navigation bar is a map of China with several cities marked: Beijing, Shanghai, Hangzhou, Shenzhen, Guangzhou, Chongqing, and others. To the right of the map is a sidebar titled '未分配区域' (Unallocated Regions) which lists '应用名称' (Application Name), '创建时间' (Creation Time), and '状态' (Status). It notes '没有数据' (No data). Below this is a section titled '产品动态' (Product Activity) with two bullet points: '支持用户对应用进行架构探查, 自动产生已保存有应用的架构' (Supports users to probe application architecture, automatically generates saved application architecture) and '支持RAM权限管理, 对于用户授予不同的权限和资源组, 控制子用户对资源的访问和操作' (Supports RAM permission management, grants different permissions and resource groups to users, controls sub-users' access to resources). A date '2021年9月31日' (September 31, 2021) is also mentioned.

步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



The screenshot shows the 'Cloud Speed Stack (CADT)' control console. The top navigation bar includes the '阿里云' logo, '工作台' (Workstation), and '账号全部资源' (All Account Resources). Below the navigation bar is a secondary menu with options: '1 建立' (Create), '应用' (Application), '资源' (Resources), '管理' (Management), and '导出' (Export). A modal dialog box is open, step 2: '新建空白应用' (Create New Blank Application). The dialog contains the text '搭!' (Build!). Below the text are three buttons: '应用' (Application), '部署成功' (Deployment Success), and '下线应用' (Offline Application). The background of the main interface shows a map of China with city markers and a sidebar with regional allocation and product activity information.

步骤3 从左侧**快速创建**列表找到**单 Region 单可用区**，单击拖入到画布区域中，松开鼠标。



步骤4 在 region 的任意位置双击鼠标，开启配置清单，选择**华东2（上海）**。



**说明：**配置完一个对象后，可以直接打开下一个对象，云速搭会自动保存现有配置。

步骤5 在VPC的任意位置双击鼠标，开启配置清单，根据[章节5.2.1资源配置清单](#)配置VPC。

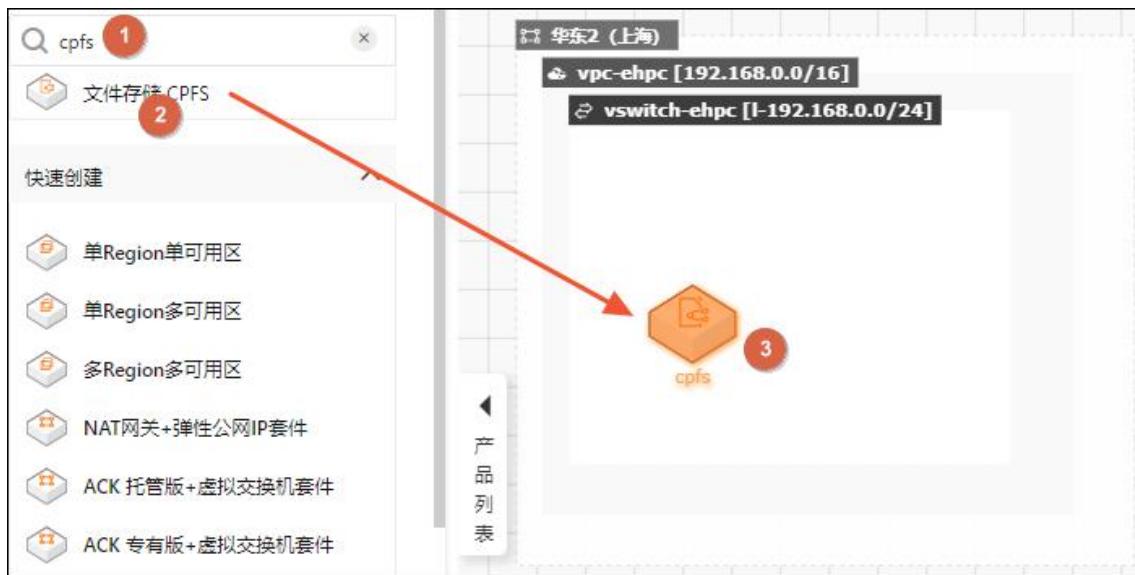


步骤6 在vswitch的任意位置双击鼠标，开启配置清单，根据[章节5.2.1资源配置清单](#)配置vswitch。



### 5.2.2.2.创建 CPFS

步骤 1 在左侧搜索栏中搜索 CPFS，拖拽**文件存储 CPFS** 到虚拟交换机中。



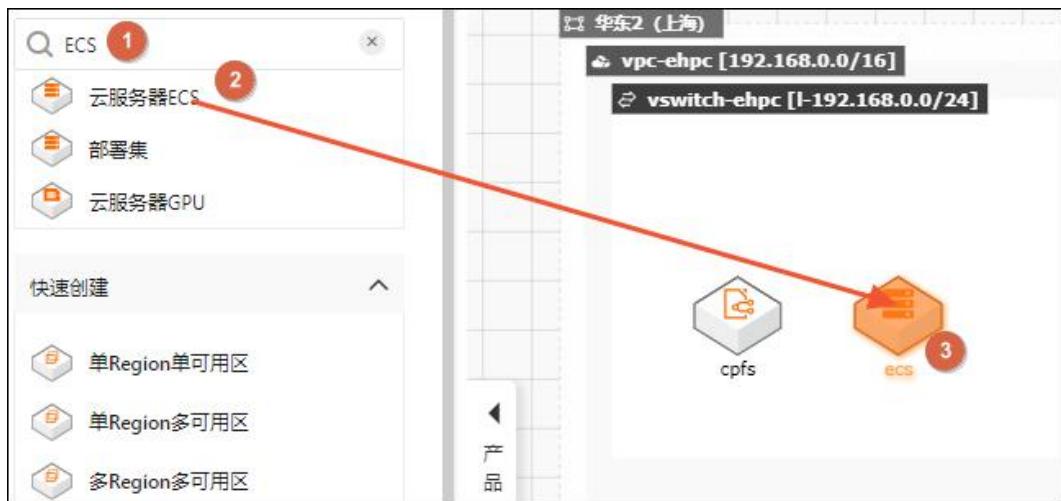
步骤 2 双击 cpfs 打开配置，根据**章节 5.2.1 资源配置清单**配置 cpfs。



### 5.2.2.3. 创建 ECS 并挂载 EIP

**说明：**该 ECS 是用于制作 EHPC 使用的自定义镜像，挂载 EIP 是为了在 ECS 上安装 CPFS 客户端和依赖的包。

步骤 3 在左侧搜索栏中搜索 ECS，拖拽云服务器 ECS 到虚拟交换机中。



步骤 4 双击 ecs 打开配置，根据**章节 5.2.1 资源配置清单**配置 ecs。



**注意：**镜像版本请选择 CentOS 7.6，不同版本会影响后续安装步骤。

**注意：**请记录 ECS 的登录密码，以备在后续**章节 5.2.3.5** 中使用。

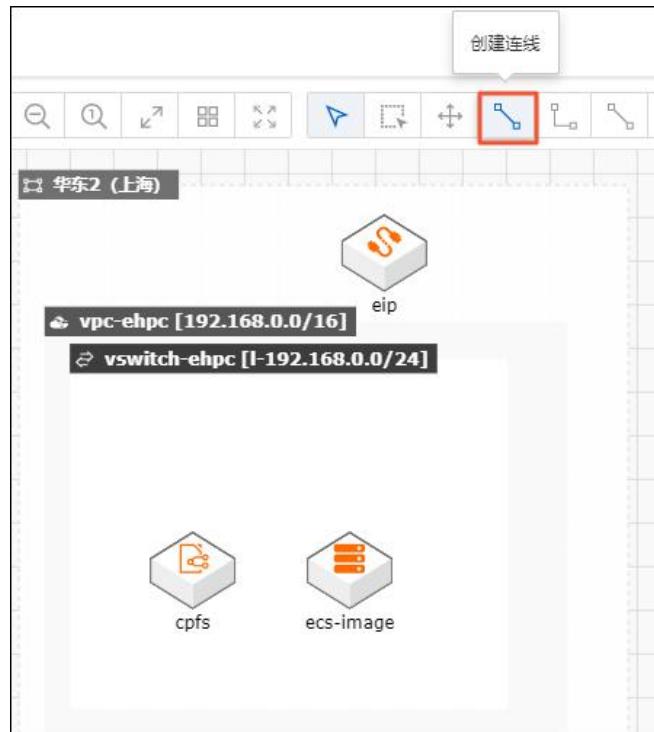
步骤 5 在左侧搜索栏中搜索 EIP，拖拽弹性公网 IP 到区域中。



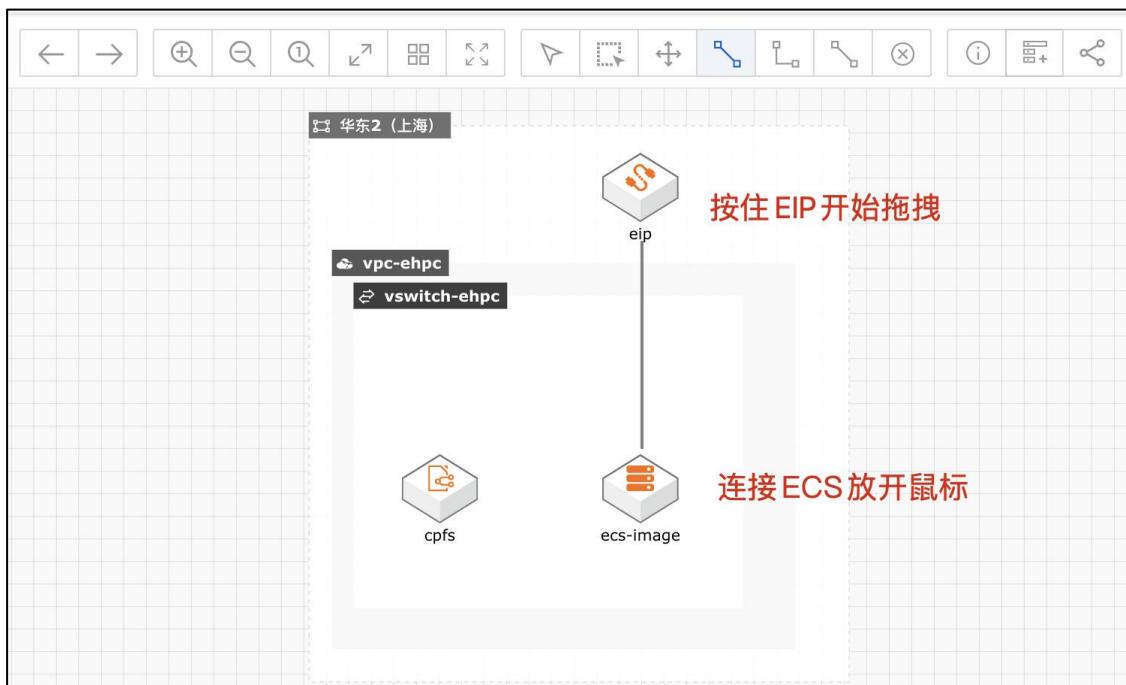
步骤 6 双击 eip 打开配置，根据**章节 5.2.1 资源配置清单**配置 eip。



步骤 7 单击创建连线。



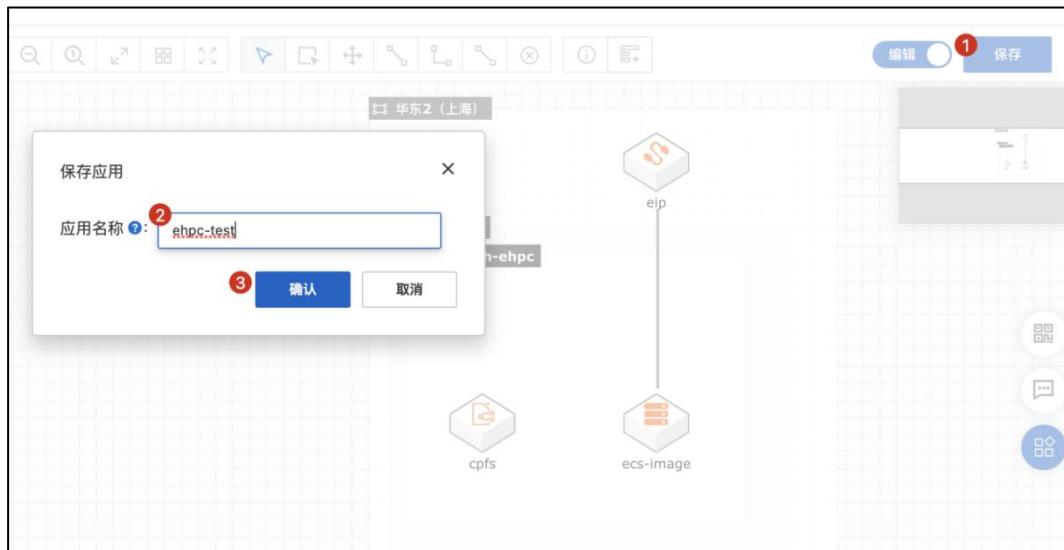
步骤 8 鼠标点击 EIP，按住不动，拖拽连接 ECS。



该连接线将 EIP 挂载到 ECS 上。

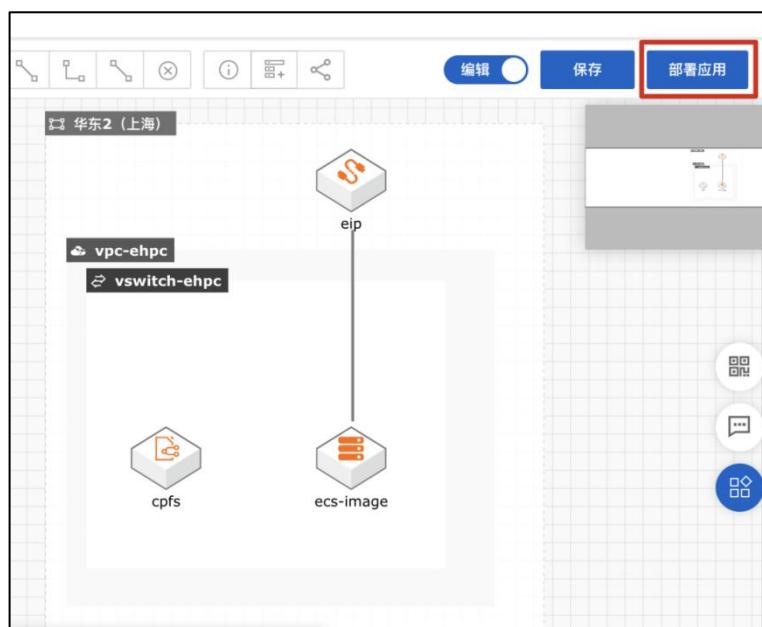
### 5.2.2.4.保存架构图

步骤 1 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写**应用名称**，并单击**确认**。



### 5.2.2.5.执行部署

步骤 1 单击右上角的**部署应用**。



步骤 2 开始进行资源验证，如果有校验错误提示，根据提示进行修改，直至校验成功后单击**下一步：价格清单**。

### 资源验证

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	ecs-image	ecs	上海	ecs.c6.xlarge	成功	校验通过	定位
2	vpc-ehpc	vpc	上海	192.168.0.0/16	成功	校验通过	定位
3	vswitch-ehpc	vswitch	上海	192.168.0.0/24	成功	校验通过	定位
4	eip	eip	上海	public	成功	校验通过	定位
5	默认安全组	security.group	上海		成功	校验通过	定位
6	cpfs	cpfs	上海	advance_100	成功	校验通过	定位

**i** cpfs添加挂载点会在您的账号下自动创建3个客户端管理节点（一般是3台g6.large ECS）用于客户端集群管理。这3个管理节点会产生额外费用，请知悉。

状态: **校验成功** 下一步: 价格清单 返回

步骤 3 待询价成功后，核对方案价格（也可以单击**查看报告**导出 PDF 版的报价清单），单击**下一步：确认订单**。

### 导出价格清单

**按量付费**

资源成本占比

资源预算

- 计算 计算: 111元/时
- 网络 网络: 111元/时
- 存储 存储: 111元/时

价格列表

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
1	eip	eip	上海	public	1	111元/时	111元/时	111元/时	定位
2	cpfs	cpfs	上海	advance_100	1	111元/时	111元/时	111元/时	定位
3	ecs-image	ecs	上海	ecs.c6.xlarge	1	111元/时	111元/时	111元/时	定位

状态: **计价成功** 上一步: 资源校验 查看报告 下一步: 确认订单

步骤4 勾选《云速搭服务条款》，单击 **下一步：支付并创建**。



步骤5 进入部署流程，这里会进行扣费并开始创建资源。



步骤6 等待资源部署完成，单击**返回**。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	vpc-ehpc	vpc	-	vpc-uf6y2sv8xi4sk2tue7bqi	运行中	2021-11-12 19:35:42	定位
2	eip	eip	按量付费	eip-uf6e4kr8mpj92blvofv88	运行中	2021-11-12 19:35:42	定位
3	默认安全组	security.group	-	sg-uf6ifriaweb9z3db64krf	运行中	2021-11-12 19:35:42	定位
4	vswitch-ehpc	vswitch	-	vsw-uf6u74yo4fknjo70upfxb	运行中	2021-11-12 19:36:41	定位
5	ecs-image	ecs	按量付费	i-uf6gu00vbk30znx5smtb	运行中	2021-11-12 19:36:42	定位

**部署概要**

状态: 部署成功 订单编号 : 211498165020497  
方案编号: 00M220STITPWYV10

[查看报告](#) 返回

**注意:** CPFS 文件系统创建时间约 15 分钟, 请耐心等待。

步骤 7 资源部署完成后, 可打开**资源清单**查看所有的资源信息。

**ehpc-test 部署成功**

The diagram illustrates the deployed resources. A VPC interface (vpc-ehpc) is connected to a VSwitch interface (vswitch-ehpc). Both interfaces are connected to a single Elastic IP (eip). The eip is highlighted with a red box.

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	vpc-ehpc [192.168.0.0/16]	vpc	-	vpc-uf6hn9f6q86galhux3ao	新建	运行中	2021-11-15 17:56:33	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>
2	eip	eip	按量付费	eip-uf6tey9czr9z7xot5ztsd	新建	运行中	2021-11-15 17:56:33	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>
3	默认安全组	security.group	-	sg-uf6ifriaweb9z3db64krf	新建	运行中	2021-11-15 17:56:33	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>

### 5.2.2.6.记录用于制作镜像的 ECS 私网 IP

步骤 1 请在资源清单中找到创建的 ECS 实例 **ecs-image**，单击详情。

The screenshot shows the Alibaba Cloud Resource Catalog interface. At the top, there's a network diagram with components labeled 'vpc-ehpc [192.168.0.0/16]', 'vswitch-ehpc [192.168.0.0/24]', and 'eip'. Below the diagram is a table titled '资源清单' (Resource List) with the following data:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	详情
4	vswitch-ehpc	vswitch	-	vsw-uf6gsfb4h00ep3e6nwhi	新建	运行中	2021-11-15 17:57:18	<a href="#">定位</a>	<a href="#">详情</a>
5	<b>ecs-image</b>	ecs	按量付费	i-uf6ec8tbwnldo0ozdbln	新建	运行中	2021-11-15 17:57:18	<a href="#">定位</a>	<a href="#">详情</a>

步骤 2 记录 ECS 的 **private\_ip** 以备后续在 章节 5.2.3.3 中使用，本例为 192.168.0.52。

The screenshot shows the details of the ECS instance 'ecs-image'. The 'private\_ip' field is highlighted with a red box and contains the value '192.168.0.52'.

hostName: ecs-image	memory: 8192
creationTime: 2021-11-12T11:35:46Z	instanceName: ecs-image
internetMaxBandwidthOut: 0	private_ip: 192.168.0.52
instanceId: i-uf6gu00vbk30nx5smtb	requestId: 6851EA9D-97EB-55D4-A773-FB9A24C5C8D7

### 5.2.2.7.确认 CPFS 挂载点状态并记录初始密码

**注意：**CPFS 文件系统通过 CADT 创建成功后，系统还须约 10 分钟来完成**挂载点**的自动创建。

步骤 1 请单击资源列表中的 **cpfs**，跳转到控制台，确认挂载点是否创建完成，若未完成，请耐心等待。

The screenshot shows a network topology diagram for '华东2 (上海)' region. At the top, there is a VPC interface (vpc-ehpc [192.168.0.0/16]) connected to a vswitch-ehpc interface (vswitch-ehpc [l-192.168.0.0/24]). An EIP (弹性公网IP) is attached to the vswitch-ehpc interface. Below the diagram is a table titled '资源清单' (Resource List) with the following data:

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态
4	vswitch-ehpc	vswitch	-	vsw-uf6gsfb4h00ep3e6nwhi	新建	运行中
5	ecs-image	ecs	按量付费	i-uf6ec8tbwnldo0ozdbln	新建	运行中
6	<b>cpfs</b>	cpfs	按量付费	cpfs- <span style="background-color: #f0f0f0;">XXXXXXXXXX</span>	新建	运行中

步骤 2 进入文件系统控制台后，单击左侧的**挂载使用**。

待 CPFS 文件系统挂载点状态可用后，请记录客户端管理节点初始密码，以备后续在**章节 5.2.**

### 3.2 中使用。

The screenshot shows the 'NAS文件系统' (NAS File System) control console for the 'cpfs-0101e78032c00808' file system. On the left sidebar, under '文件系统列表', the '挂载使用' (Mount Usage) tab is selected. In the main area, the '挂载点' (Mount Point) section displays the following information:

挂载点类型	VPC	交换机	挂载点	状态	操作
专有网络	vpc-uf6y2sv8xi4sk2tue7bqj	vsw-uf6u74yo4fknoj70upfbx	0101e78032c00808-000001.ali.net	<span style="border: 2px solid red; padding: 2px;">可用</span>	<span style="border: 1px solid red; padding: 2px;">删除</span>

Below the table, the '客户端管理节点' (Client Management Node) section lists three ECS instances with their private IP addresses:

ECS实例ID	私网IP	初始密码
i-uf6ci3vt7rdc12tnknqt	192.168.0.60	.....
i-uf6ci3vt7rdc12tnknqu	192.168.0.59	.....
i-uf6ci3vt7rdc12tnknqv	192.168.0.58	.....

Key UI elements highlighted with red boxes and numbers:

- Step 1: '可用' (Available) status indicator for the mount point.
- Step 2: '显示初始密码' (Show Initial Password) button for the first client management node.

Annotations at the bottom of the page:

- ① 客户端管理节点只用于CPFS挂载管理，使用CPFS时禁止对客户端管理节点做删除/停机操作，删除挂载点时会释放客户端管理节点。
- ② 删除挂载点时，会自动释放管理节点ECS，请谨慎操作。
- 建议您在首次登录客户端管理节点以后修改登录密码，并妥善保管。

## 5.2.3.制作镜像

### 5.2.3.1.允许远程登录 CPFS 管理节点

步骤 1 登录 ECS 控制台**安全组**页面，找到**CPFS**安全组，单击**配置规则**。

(<https://ecs.console.aliyun.com/securityGroup/region/cn-shanghai> )

步骤 2 手工添加一条入方向的规则，对 workbench 的 IP 地址段 **100.104.0.0/16** 开放 **22** 号端口的访问。

## 5.2.3.2.远程登录 CPFS 客户端管理节点 qr001

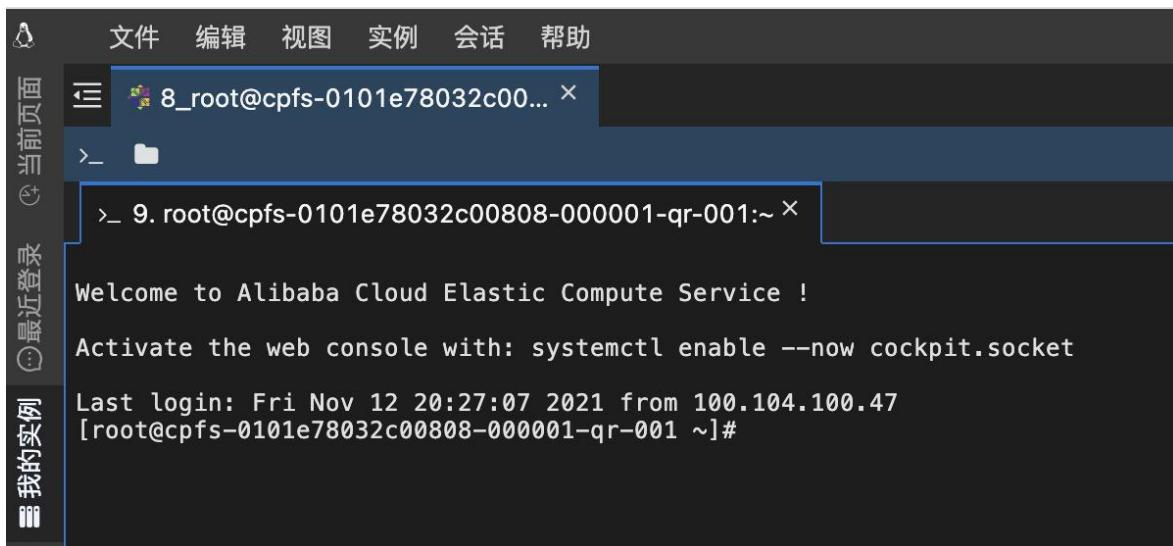
步骤 1 登录 ECS 控制台实例页面，找到 CPFS 管理节点 ECS 实例 qr-001，单击**远程连接**。  
(<https://ecs.console.aliyun.com/server/region/cn-shanghai>)

The screenshot shows the AliCloud ECS console interface. On the left, there's a sidebar with options like '概览', '事件', '标签', '自助问题排查', '发送命令/文件 (云助手)', '我的常用' (with '实例' selected), '安全组', '镜像', '快照', '云盘', and '实例与镜像'. The main area is titled '实例 华东2 (上海)'. It shows a list of instances with columns for '实例 ID / 名称', '状态', '标签', '操作系统', '监控', and '操作'. Three instances are listed: 'qr-001' (status: 运行中), 'qr-002' (status: 运行中), and 'qr-003' (status: 运行中). Each instance row has a '远程连接 | 资源变配' button, which is highlighted with a red circle and a callout bubble containing '2 远程连接 | 资源变配 停止 | :'. The URL in the browser bar is <https://ecs.console.aliyun.com/server/region/cn-shanghai>.

步骤 2 选择 workbench 登录。

The screenshot shows the '远程连接与命令' (Remote Connection and Commands) dialog box. It has three main sections: 'Workbench远程连接' (Workbench Remote Connection), 'VNC远程连接' (VNC Remote Connection), and '发送远程命令 (云助手)' (Send Remote Command (Cloud Assistant)). The 'Workbench远程连接' section contains a large blue button labeled '立即登录' (Log In Immediately), which is highlighted with a red rectangle. Below it, there's a note: '通过网页可以对ECS实例进行远程控制，支持复制粘贴文本，支持多操作系统用户登录同一台实例，支持可视化查看系统文件资源。' (Through the web page, you can perform remote control on the ECS instance, support copy and paste text, support multiple operating system users to log in to the same instance, support visualized viewing of system file resources.). The 'VNC远程连接' section also has a '立即登录' button. The '发送远程命令 (云助手)' section has a '推荐' (Recommended) label and a '发送远程命令' (Send Remote Command) button.

步骤 3 输入在[章节 5.2.2.7](#) 中获取的 CPFS 管理节点的 root 账号密码，单击登录。（如果登录失败请查看是否拷贝了多余的空格）



### 5.2.3.3.配置 CPFS 管理节点对客户端节点的免密钥登录

步骤 1 确认 CPFS 管理节点的 /etc/ssh/sshd\_config 文件中的如下配置。

```
StrictHostKeyChecking=no
```

```

# 
# Uncomment this if you want to use .local domain
# Host *.local
#   CheckHostIP no

Host *
  GSSAPIAuthentication yes
# If this option is set to yes then remote X11 clients will have full access
# to the original X11 display. As virtually no X11 client supports the untrusted
# mode correctly we set this to yes.
  ForwardX11Trusted yes
# Send locale-related environment variables
  SendEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
  SendEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
  SendEnv LC_IDENTIFICATION LC_ALL LANGUAGE
  SendEnv XMODIFIERS
StrictHostKeyChecking no

```

步骤 2 运行以下命令，将公钥信息拷贝至制作自定义镜像的 ECS 实例。

本例中用于制作镜像的 ECS 实例 ecs-image 的私网 IP 已从[章节 5.2.2.6](#) 中获取 -- 192.168.0.52。

```
ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.0.52
```

该步骤实现从 CPFS 管理节点到目标 ECS (ecs-image) 的免密登录。

```

[~ 9. root@cpfs-0101e78032c00808-000001-qr-001:~ ×]
[root@cpfs-0101e78032c00808-000001-qr-001 ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.0.52
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: /root/.ssh/id_rsa.pub
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.0.52's password:
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'root@192.168.0.52'"
and check to make sure that only the key(s) you wanted were added.

[root@cpfs-0101e78032c00808-000001-qr-001 ~]# ■

```

步骤 3 测试免密登录。

```
ssh root@192.168.0.52
```

```

[root@cpfs-0101e78032c00808-000001-qr-001 ~]# ssh root@192.168.0.52 验证免密登录
Welcome to Alibaba Cloud Elastic Compute Service !
[root@ecs-image ~]# exit 验证成功，退出返回CPFS管理节点
logout
Connection to 192.168.0.52 closed.
[root@cpfs-0101e78032c00808-000001-qr-001 ~]# ■

```

验证成功后使用 `exit` 命令返回 CPFS 管理节点。

### 5.2.3.4.记录 CPFS 管理节点的 Quorum 和 Contact 内容

步骤 1 确认登录在 CPFS 管理节点 qr-001 中。

步骤 2 获取/etc/hosts 文件中的相关内容。

复制除 localhost 记录以外的全部其他记录，以备后续在章节 5.2.3.6 中使用。

```
vim /etc/hosts
```

```

8_root@cpfs-0101e78032c00808-000001-qr-001:~ %
9. root@cpfs-0101e78032c00808-000001-qr-001:~ %
192.168.0.55      cpfs-contact-node2          cpfs-contact-node2          #CPFS_192_168_0_55_MAGIC
192.168.0.54      cpfs-contact-node1          cpfs-contact-node1          #CPFS_192_168_0_54_MAGIC
192.168.0.58      cpfs-0101e78032c00808-000001-qr-003  cpfs-0101e78032c00808-000001-qr-003  #CPFS_192_168_0_58_MAGIC
192.168.0.59      cpfs-0101e78032c00808-000001-qr-002  cpfs-0101e78032c00808-000001-qr-002  #CPFS_192_168_0_59_MAGIC
192.168.0.60      cpfs-0101e78032c00808-000001-qr-001  cpfs-0101e78032c00808-000001-qr-001  #CPFS_192_168_0_60_MAGIC
::1   localhost    localhost.localdomain    localhost.localdomain    localhost.localdomain6  localhost6.localdomain6
127.0.0.1          localhost    localhost.localdomain    localhost.localdomain4  localhost4.localdomain4

192.168.10.47    iZbp1dnm3b75i4pe2w9dx9Z iZbp1dnm3b75i4pe2w9dx9Z
192.168.0.60      cpfs-0101e78032c00808-000001-qr-001  cpfs-0101e78032c00808-000001-qr-001
192.168.0.60      cpfs-0101e78032c00808-000001-qr-001  cpfs-0101e78032c00808-000001-qr-001_MAGICTAG
192.168.0.59      cpfs-0101e78032c00808-000001-qr-002  cpfs-0101e78032c00808-000001-qr-002_MAGICTAG
192.168.0.58      cpfs-0101e78032c00808-000001-qr-003  cpfs-0101e78032c00808-000001-qr-003_MAGICTAG

```

### 5.2.3.5.远程登录用于制作镜像的 ECS 实例

步骤 1 登录 ECS 控制台实例页面，单击 ECS 实例 ecs-image 后的远程连接。

(<https://ecs.console.aliyun.com/server/region/cn-shanghai> )

实例 ID / 名称	状态	可用区	配置	IP 地址	操作
i-uf6ci3vt7rdc12tnknqt cpfs-0101e78032c00808-000001-qr-001	运行中	每 可用区L	2 核 8 GiB (I/O 优化) ecs.g6.large 0 Mbps (峰值)	192.168.0.0	<a href="#">远程连接</a>   <a href="#">资源变配</a> <a href="#">停止</a>   <a href="#">更多</a>
i-uf6ci3vt7rdc12tnknqu cpfs-0101e78032c00808-000001-qr-002	运行中	每 可用区L	2 核 8 GiB (I/O 优化) ecs.g6.large 0 Mbps (峰值)	192.168.0.0	<a href="#">远程连接</a>   <a href="#">资源变配</a> <a href="#">停止</a>   <a href="#">更多</a>
i-uf6ci3vt7rdc12tnknqv cpfs-0101e78032c00808-000001-qr-003	运行中	每 可用区L	2 核 8 GiB (I/O 优化) ecs.g6.large 0 Mbps (峰值)	192.168.0.0	<a href="#">远程连接</a>   <a href="#">资源变配</a> <a href="#">停止</a>   <a href="#">更多</a>
i-uf6gu00vbk30znx5smtb ecs-image	运行中	每 可用区L	4 核 8 GiB (I/O 优化) ecs.c6.xlarge 5 Mbps (峰值)	120.55.16.0 192.168.0.0	<a href="#">远程连接</a>   <a href="#">资源变配</a> <a href="#">停止</a>   <a href="#">更多</a>

选择 workbench 登录，**root** 账号密码为在 CADT 中创建 ECS 时（[章节 5.2.2.3](#)）使用的密码。

```
_ 9. root@ecs-image:~ >
Last login: Fri Nov 12 20:56:22 2021 from 47.96.60.215
Welcome to Alibaba Cloud Elastic Compute Service !
[root@ecs-image ~]#
```

### 5.2.3.6. 在用于制作镜像的 ECS 上安装 CPFS 客户端

步骤 1 在/etc/hosts 中添加 CPFS 管理节点的 Quorum 和 Contact 内容。

将在[章节 5.2.3.4](#) 中获取的 CPFS 管理节点的 Quorum 和 Contact 内容复制到 ecs-image 的/etc/hosts 文件。

```
_ 9. root@ecs-image:~ >
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
192.168.0.52 ecs-image ecs-image
192.168.0.55 cpfs-contact-node2 cpfs-contact-node2 #CPFS_192_168_0_55_MAGIC
192.168.0.54 cpfs-contact-node1 cpfs-contact-node1 #CPFS_192_168_0_54_MAGIC
192.168.0.58 cpfs-0101e78032c00808-000001-qr-003 cpfs-0101e78032c00808-000001-qr-003 #CPFS_192_168_0_58_MAGIC
192.168.0.59 cpfs-0101e78032c00808-000001-qr-002 cpfs-0101e78032c00808-000001-qr-002 #CPFS_192_168_0_59_MAGIC
192.168.0.60 cpfs-0101e78032c00808-000001-qr-001 cpfs-0101e78032c00808-000001-qr-001 #CPFS_192_168_0_60_MAGIC
192.168.10.47 iZbp1dnm3b75i4pe2w9dx9Z iZbp1dnm3b75i4pe2w9dx9Z
192.168.0.60 cpfs-0101e78032c00808-000001-qr-001 cpfs-0101e78032c00808-000001-qr-001
192.168.0.60 cpfs-0101e78032c00808-000001-qr-001 cpfs-0101e78032c00808-000001-qr-001_MAGICTAG
192.168.0.59 cpfs-0101e78032c00808-000001-qr-002 cpfs-0101e78032c00808-000001-qr-002_MAGICTAG
192.168.0.58 cpfs-0101e78032c00808-000001-qr-003 cpfs-0101e78032c00808-000001-qr-003_MAGICTAG
```

步骤 2 运行以下命令，下载并解压 RPM 包。

```
mkdir /tmp/rpms
cd /tmp/rpms
wget https://gpfs-rpms.oss-cn-beijing.aliyuncs.com/CPFS2.2-CentOS.tar.gz
tar xvfz CPFS2.2-CentOS.tar.gz
```

```
[root@ecs-image ~]# mkdir /tmp/rpms
[root@ecs-image ~]# cd /tmp/rpms
[root@ecs-image rpms]# wget https://gpfs-rpms.oss-cn-beijing.aliyuncs.com/CPFS2.2-CentOS.tar.gz
--2021-11-12 21:07:09-- https://gpfs-rpms.oss-cn-beijing.aliyuncs.com/CPFS2.2-CentOS.tar.gz
Resolving gpfs-rpms.oss-cn-beijing.aliyuncs.com (gpfs-rpms.oss-cn-beijing.aliyuncs.com)... 59.110.190.38
Connecting to gpfs-rpms.oss-cn-beijing.aliyuncs.com (gpfs-rpms.oss-cn-beijing.aliyuncs.com)|59.110.190.38|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 351553526 (335M) [application/gzip]
Saving to: 'CPFS2.2-CentOS.tar.gz'

15% [=====>]
100%[=====>] 351,553,526 10.4MB/s in 30s

2021-11-12 21:07:39 (11.3 MB/s) - 'CPFS2.2-CentOS.tar.gz' saved [351553526/351553526]

[root@ecs-image rpms]# tar xvfz CPFS2.2-CentOS.tar.gz
CentOS/
CentOS/CentOS7/
CentOS/CentOS7/gpfs.base-5.1.2-0.x86_64.rpm
CentOS/CentOS7/gpfs.gpl-5.1.2-0.noarch.rpm
CentOS/CentOS7/gpfs.msg.en_US-5.1.2-0.noarch.rpm
CentOS/CentOS7/gpfs.gskit-8.0.55-19.x86_64.rpm
CentOS/CentOS7/gpfs.adv-5.1.2-0.x86_64.rpm
CentOS/CentOS7/gpfs.license.dm-5.1.2-0.x86_64.rpm
CentOS/CentOS7/gpfs.crypto-5.1.2-0.x86_64.rpm
CentOS/CentOS7/gpfs.docs-5.1.2-0.noarch.rpm
CentOS/CentOS7/gpfs.java-5.1.2-0.x86_64.rpm
CentOS/CentOS7/gpfs.compression-5.1.2-0.x86_64.rpm
CentOS/CentOS7/gpfs.gui-5.1.2-0.noarch.rpm
CentOS/CentOS7/gpfs.afm.cos-1.0.0-3.x86_64.rpm
CentOS/CentOS7/gpfs.librdkafka-5.1.2-0.el7.x86_64.rpm
CentOS/CentOS7/gpfs.gss.pmsensors-5.1.2-0.el7.x86_64.rpm
CentOS/CentOS7/gpfs.pmcollector-5.1.2-0.el7.x86_64.rpm
CentOS/CentOS8/
CentOS/CentOS8/gpfs.adv-5.1.2-0.x86_64.rpm
CentOS/CentOS8/gpfs.afm.cos-1.0.0-3.x86_64.rpm
CentOS/CentOS8/gpfs.base-5.1.2-0.x86_64.rpm
CentOS/CentOS8/gpfs.compression-5.1.2-0.x86_64.rpm
CentOS/CentOS8/gpfs.crypto-5.1.2-0.x86_64.rpm
CentOS/CentOS8/gpfs.docs-5.1.2-0.noarch.rpm
CentOS/CentOS8/gpfs.gpl-5.1.2-0.noarch.rpm
CentOS/CentOS8/gpfs.gskit-8.0.55-19.x86_64.rpm
CentOS/CentOS8/gpfs.pmcollector-5.1.2-0.el8.x86_64.rpm
CentOS/CentOS8/gpfs.gss.pmsensors-5.1.2-0.el8.x86_64.rpm
CentOS/CentOS8/gpfs.gui-5.1.2-0.noarch.rpm
CentOS/CentOS8/gpfs.java-5.1.2-0.x86_64.rpm
CentOS/CentOS8/gpfs.librdkafka-5.1.2-0.el8.x86_64.rpm
CentOS/CentOS8/gpfs.license.dm-5.1.2-0.x86_64.rpm
CentOS/CentOS8/gpfs.msg.en_US-5.1.2-0.noarch.rpm
[root@ecs-image rpms]# ]]
```

步骤3 运行以下命令，安装CPFS客户端的依赖软件。

```
yum install -y cpp gcc gcc-c++ binutils ksh elfutils elfutils-devel rpm-build
```

```
Installed:
  elfutils.x86_64 0:0.176-5.el7    elfutils-devel.x86_64 0:0.176-5.el7    gcc-c++.x86_64 0:4.8.5-44.el7    ksh.x86_64 0:20120801-142.el7    rpm-build.x86_64 0:4.11.3-46.el7_9
Dependency Installed:
  bzip2.x86_64 0:1.0.6-13.el7          dwz.x86_64 0:0.0.11-3.el7      elfutils-libelf-devel.x86_64 0:0.176-5.el7    gdb.x86_64 0:7.6.1-120.el7
  libgcc.x86_64 0:4.8.5-44.el7        perl-TThread-Queue.noarch 0:3.02-2.el7    perl-SIPM-Macros.noarch 0:1-8.el7    python-5 rpm-macros.noarch 0:3-34.el7
  redhat-rpm-config.noarch 0:9.1.0-88.el7.centos  unzip.x86_64 0:5.6-22.el7_9  xz-devel.x86_64 0:5.2-2.el7      zip.x86_64 0:3.0-11.el7
  zlib-devel.x86_64 0:1.2.7-19.el7_9

Updated:
  binutils.x86_64 0:2.27-44.base.el7_9.1          cpp.x86_64 0:4.8.5-44.el7          gcc.x86_64 0:4.8.5-44.el7
Dependency Updated:
  elfutils-libelf.x86_64 0:0.176-5.el7    elfutils-libs.x86_64 0:0.176-5.el7    libgcc.x86_64 0:4.8.5-44.el7    libgomp.x86_64 0:4.8.5-44.el7    libstdc++.x86_64 0:4.8.5-44.el7
  rpm.x86_64 0:4.11.3-46.el7_9          rpm-build-libs.x86_64 0:4.11.3-46.el7_9  rpm-libs.x86_64 0:4.11.3-46.el7_9  rpm-python.x86_64 0:4.11.3-46.el7_9  zlib.x86_64 0:1.2.7-19.el7_9
Complete!
[root@ecs-image rpms]# ]
```

步骤4 运行以下命令，安装CPFS客户端。

```
cd CentOS/CentOS7/
yum install -y gpfs.adv-*x86_64.rpm    gpfs.base-*x86_64.rpm
gpfs.docs-*noarch.rpm    gpfs.gpl-*noarch.rpm    gpfs.gskit-*x86_64.rpm
gpfs.gss.pmsensors-*x86_64.rpm    gpfs.license.dm-*x86_64.rpm
gpfs.msg.en_US-*noarch.rpm
```

```
Installed:
  gpfs.adv.x86_64 0:5.1.2-0          gpfs.base.x86_64 0:5.1.2-0          gpfs.docs.noarch 0:5.1.2-0          gpfs.gpl.noarch 0:5.1.2-0          gpfs.gskit.x86_64 0:8.0.55-19
  gpfs.gss.pmsensors.x86_64 0:5.1.2-0.el7    gpfs.license.dm.x86_64 0:5.1.2-0          gpfs.msg.en_US.noarch 0:5.1.2-0
Dependency Installed:
  libalo.x86_64 0:0.3.109-13.el7      libtirpc.x86_64 0:0.2.4-0.16.el7     python3.x86_64 0:3.6.8-18.el7    python3-libs.x86_64 0:3.6.8-18.el7   python3-pip.noarch 0:9.0.3-8.el7
  python3-setuptools.noarch 0:39.2.0-10.el7
Complete!
[root@ecs-image CentOS7]#
```

步骤 5 运行以下命令，构建系统。

```
/usr/lpp/mmfs/bin/mmbuildgpl
```

```
>_ 9. root@ecs-image:/tmp/rpms/CentOS/CentOS7 ×
[root@ecs-image CentOS7]# /usr/lpp/mmfs/bin/mmbuildgpl
mmbuildgpl: Building GPL (5.1.2.0) module begins at Fri Nov 12 21:16:14 CST 2021.
-----
Verifying Kernel Header...
  kernel version = 310000957 (310000957021003, 3.10.0-957.21.3.el7.x86_64, 3.10.0-957.21.3)
  module include dir = /lib/modules/3.10.0-957.21.3.el7.x86_64/build/include
  module build dir  = /lib/modules/3.10.0-957.21.3.el7.x86_64/build
  kernel source dir = /usr/src/linux-3.10.0-957.21.3.el7.x86_64/include
  Found valid kernel header file under /usr/src/kernels/3.10.0-957.21.3.el7.x86_64/include
Getting Kernel Cipher mode...
  Will use blkcipher routines
Verifying Compiler...
  make is present at /bin/make
  cpp is present at /bin/cpp
  gcc is present at /bin/gcc
  g++ is present at /bin/g++
  ld is present at /bin/ld
Verifying Additional System Headers...
  Verifying kernel-headers is installed ...
    Command: /bin/rpm -q kernel-headers
    The required package kernel-headers is installed
make World ...
make InstallImages ...
mmbuildgpl: Building GPL module completed successfully [at Fri Nov 12 21:16:31 CST 2021.
-----
[root@ecs-image CentOS7]# []
```

当返回以上红框中的信息时，说明系统已构建。

### 5.2.3.7.制作自定义镜像

步骤 1 回到 ECS 控制台实例页面，为 ecs-image 创建自定义镜像。

The screenshot shows the Alibaba Cloud ECS console interface. On the left, there's a list of existing instances. On the right, there's a sidebar with various configuration options like 'Resource Allocation' and 'Scaling'. At the bottom right of the main area, there's a blue button labeled 'Create Custom Image' with a red circle containing the number '1' over it.

步骤 2 填写自定义镜像名称和自定义镜像描述，单击确认开始创建镜像。

The screenshot shows the 'Create Custom Image' dialog box. It contains several input fields and instructions:

- 创建自定义镜像 ②**
- 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磁盘。该实例的每块磁盘会新增一个快照，可以在快照列表中查询。需要等待每块磁盘的快照创建完成，镜像才能使用，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 ②**: ① ehpc-cfps
- \* 自定义镜像描述 ②**: ② ehpc-cfps
- 镜像族系**: 请输入或选择镜像族系
- 资源组**: 请选择
- 标签**: 请选择或输入完整的标签键 : 请选择或输入完整的标签值
- ③ 确认** (highlighted with a red box) | **取消**

步骤 3 进入 ECS 控制台镜像页面，确认镜像创建完成。

(<https://ecs.console.aliyun.com/image/region/cn-shanghai/imageList> )

创建镜像耗时受镜像大小影响，本例的自定义镜像耗时约 10 分钟左右，请耐心等待。

The screenshot shows the Alibaba Cloud ECS Image Management interface. On the left, there's a sidebar with 'ECS 云服务器' and '镜像' selected. The main area has tabs for '自定义镜像' (Custom Image), '公共镜像' (Public Image), '共享镜像' (Shared Image), and '镜像市场' (Image Market). Below these tabs is a search bar and a '镜像族系' (Image Family) search input. A table lists images, with one entry highlighted: 'm-uf685rpkoqg9dhrz8n4l ehpc-cpfs'. This row includes columns for '镜像ID/名称' (Image ID/Name), '镜像族系' (Image Family), '操作' (Operation), '平台' (Platform), '系统位数' (System Bit Size), '状态(全部)' (Status), and '进度' (Progress). The progress bar for this image is at 100%, indicated by a red box.

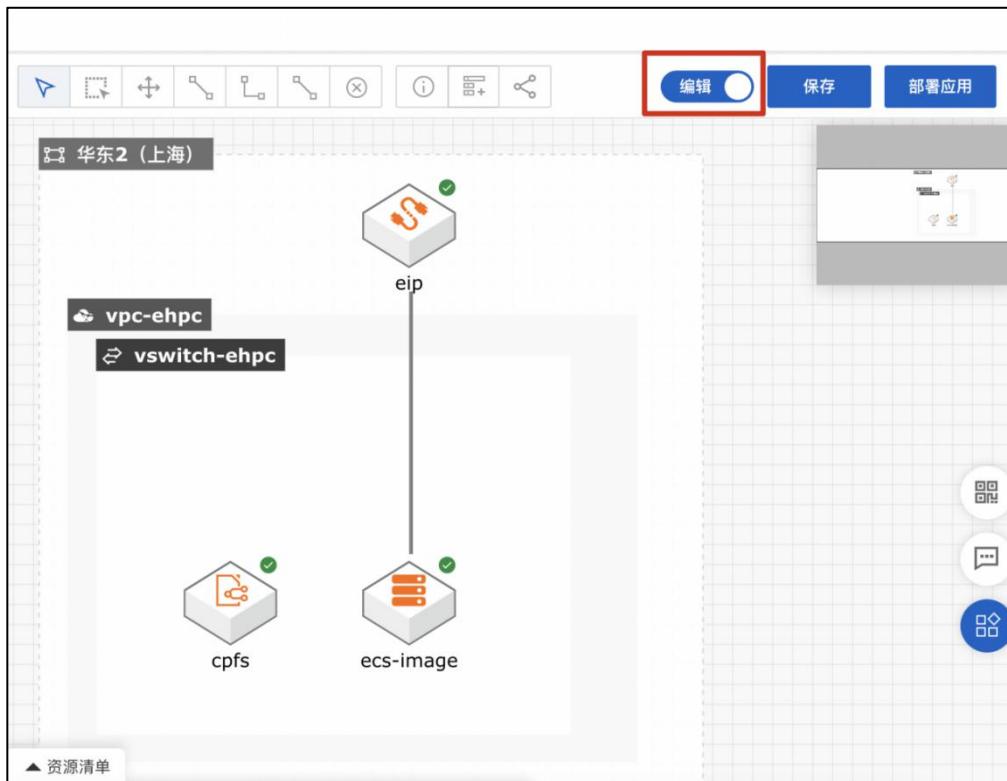
## 5.2.4. 部署 E-HPC

### 5.2.4.1. 创建 E-HPC

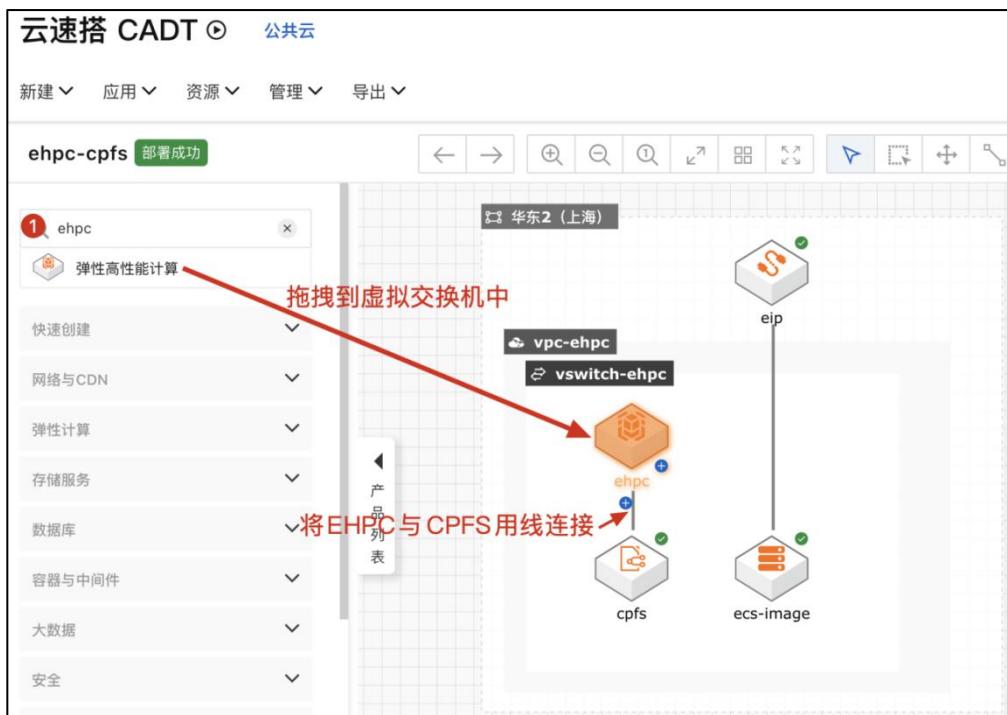
步骤 1 回到 CADT 控制台，找到在[章节 5.2.2.1](#) 中创建的应用，单击编辑架构图。[\(https://bps.tudio.console.aliyun.com/ \)](https://bps.tudio.console.aliyun.com/)

The screenshot shows the Cloud Speed Stack (CADT) control panel. At the top, there are navigation links: 新建 (New), 应用 (Application), 资源 (Resources), 管理 (Management), and 导出 (Export). Below this is a welcome message: '欢迎使用云速搭!' (Welcome to Cloud Speed Stack!). There are two tabs: '全部应用' (All Applications) and '部署成功' (Deployment Success). The '全部应用' tab is selected, showing a diagram of an application architecture. The diagram includes components like 'ehpc-cpfs' and 'ec2-image'. A blue button labeled '2 编辑架构图' (Edit Architecture Diagram) is highlighted with a red circle and number 2. To the right of the diagram, there's a deployment status section with the text '部署成功' (Deployment Success) and a progress bar at 100%.

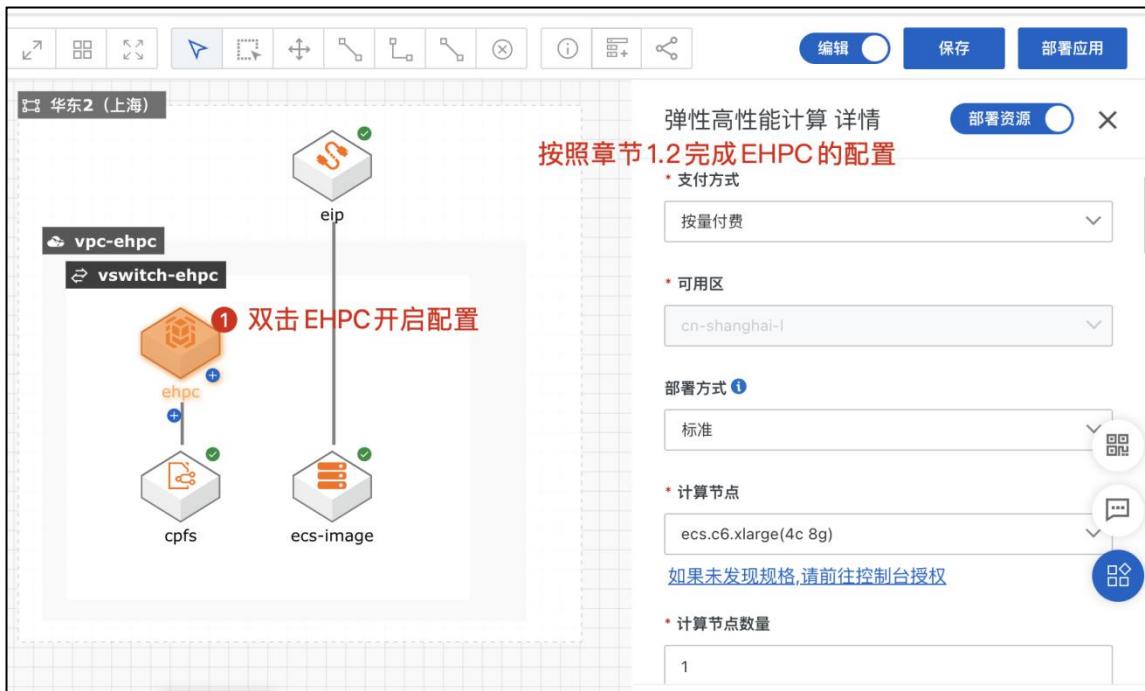
步骤 2 切换到编辑模式。



步骤 3 在左侧搜索栏中搜索 ehpc，拖拽弹性高性能计算到虚拟交换机中，并连接 CPFS。

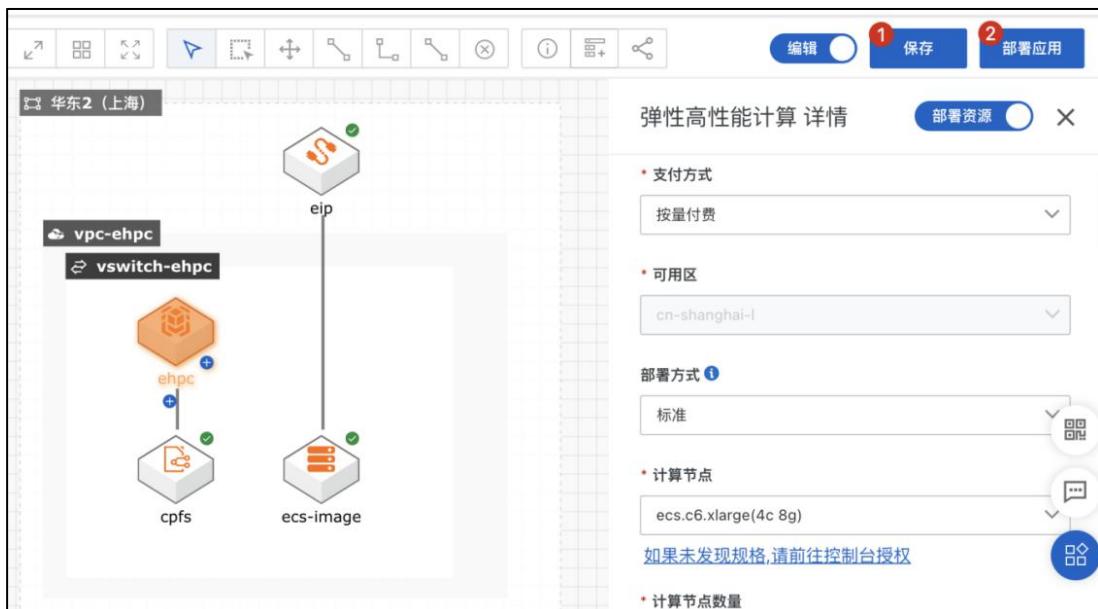


步骤4 双击 ehpc 打开配置，根据**章节 5.2.1 资源配置清单**配置 ehpc。



### 5.2.4.2. 执行部署

步骤1 重新保存后，单击**部署应用**。



**说明：**云速搭支持增量部署，本次部署只创建 EHPC 集群，不会影响到在**章节 5.2.2.1** 中已经部署的资源。

后续步骤与**章节 5.2.2.5** 一致，此处不再赘述。

EHPC 集群的创建耗时约 10 分钟，请耐心等待。

### 5.2.4.3.确认 E-HPC 集群运行正常

步骤 1 CADT 成功部署 E-HPC 后，登录 E-HPC 控制台，确认集群状态为**运行中**。

(<https://ehpc.console.aliyun.com/#/cluster?regionId=cn-shanghai> )



The screenshot shows the AliCloud E-HPC control panel. On the left, there's a sidebar with '弹性高性能计算' (E-HPC) selected, and '集群' (Cluster) is the active tab. A cluster named 'ehpc 运行中' (ehpc Running) is listed. The main area displays basic information about the cluster, including its ID, public IP, and creation time. To the right, there are three performance metrics shown as gauges: '正常计算节点/总算节点' (Normal Compute Nodes / Total Nodes) at 1/1, '已用核数/总核数' (Used Cores / Total Cores) at 0/4, and '已用内存/总内存(GB)' (Used Memory / Total Memory (GB)) at 0/8. The status bar at the bottom indicates the cluster is 'Running'.

## 5.3.云速搭基于资源组部署云资源

作者 | 阿里云解决方案架构师 阿瑟

### 5.3.1.云速搭架构设计入门

#### 背景信息

根据业务需求，针对某个部门或业务，进行权限管理。希望该部门或业务的同学，只需要查看对应的阿里云资源。

#### 资源规划

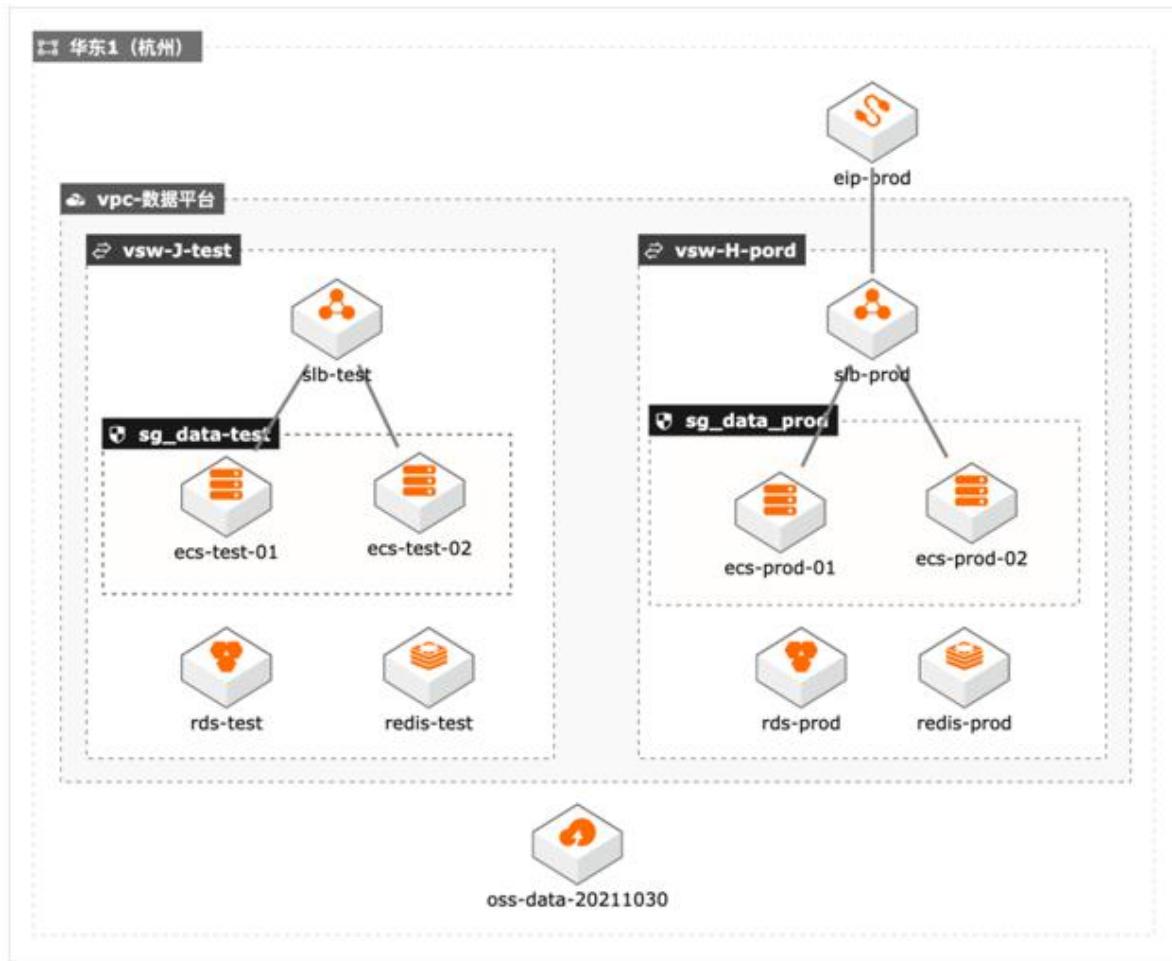
根据业务需要，规划“数据平台”一期在阿里云上资源需求。如下表所示：

环境说明	产品名称	产品描述	所属资源组	自定义名称	规格
-	地域	华东1（杭州）			
	专有网络	VPC	数据平台组	vpc-数据平台	10.0.0.0/8
	oss	标准存储	/	oss-data-20211030	
线上环境	交换机	可用区H， 线上环境	/	vsw-H-pord	10.0.2.0/24
	slb	slb.s1.small	数据平台组	slb-prod	
	rds	mysql.x2. large.2c, mysql5.7	数据平台组	rds-prod	4 vCpu   8GB (独享型) 内存   100.0G cloud_essd 硬盘
	kvstore	社区版 5.0, 标准型	数据平台组	redis-prod	官网标准 1G(QPS:80000 Connections:10000)

环境说明	产品名称	产品描述	所属资源组	自定义名称	规格
测试环境	eip	public	数据平台组	eip-prod	按流量付费, 5Mb
	安全组	普通安全组	数据平台组	sg_data-prod	安全规则自定义
	ecs	ecs.c6.xlarge	数据平台组	ecs-prod-01	4 vCpu   8.0G 内存   40.0G cloud_essd 硬盘 PL0   aliyun_3_x64_20G_alibase_20210910.vhd
	ecs	ecs.c6.xlarge	数据平台组	ecs-prod-02	4 vCpu   8.0G 内存   40.0G cloud_essd 硬盘 PL0   aliyun_3_x64_20G_alibase_20210910.vhd
	交换机	可用区 J , 测试环境	/	vsw-J-test	10.0.1.0/24
	slb	slb.s1.small	数据平台组	slb-test	
	rds	mysql.x2.medium.2c, mysql5.7	数据平台组	rds-test	2 vCpu   4GB (独享型) 内存   100.0G cloud_ssd 硬盘
	kvstore	社区版 5.0, 标准型	数据平台组	redis-test	官网标准 1G(QPS:80000 Connections:10000)
测试环境	安全组	普通安全组	数据平台组	sg_data-test	安全规则自定义
	ecs	ecs.c6.large	数据平台组	ecs-test-01	2 vCpu   4.0G 内存   40.0G cloud_essd 硬盘 PL0   aliyun_3_x64_20G_alibase_20210910.vhd
	ecs	ecs.c6.large	数据平台组	ecs-test-02	2 vCpu   4.0G 内存   40.0G cloud_essd 硬盘 PL0   aliyun_3_x64_20G_alibase_20210910.vhd

## 方案架构

通过云速搭 CADT，利用资源管理，实现资源权限设置、部署和验证的全链路。参考规划的资源，进行云资源架构设计和部署。架构图如下：

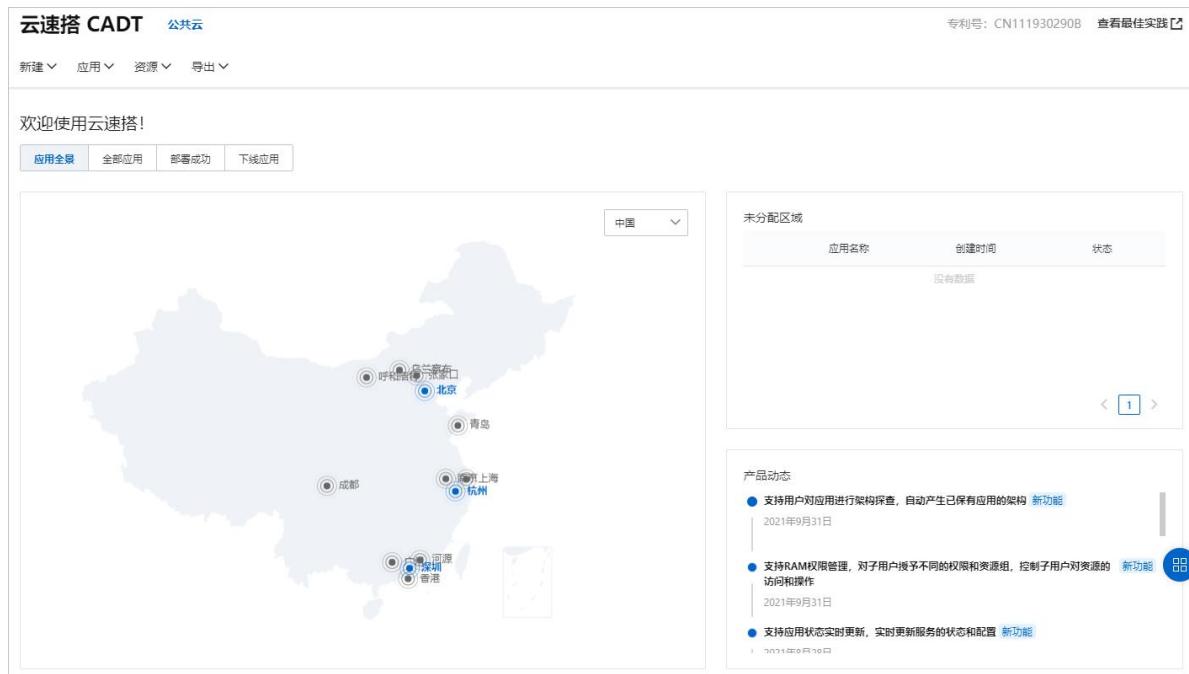


### 5.3.2.权限管理

#### 5.3.2.1. 创建用户和用户组

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。



步骤 2 在 CADT 控制台单击管理 > 权限管理 > 创建用户。



或直接登录 RAM 访问控制台: <https://ram.console.aliyun.com/users>

步骤 3 根据实际需求，创建用户，本示例配置如下表所示：

配置项	示例						
用户账号信息	<table> <tr> <td>登录名称</td> <td>显示名称</td> </tr> <tr> <td>user001</td> <td>user001</td> </tr> <tr> <td>user002</td> <td>user002</td> </tr> </table>	登录名称	显示名称	user001	user001	user002	user002
登录名称	显示名称						
user001	user001						
user002	user002						
访问方式	<p>控制台访问 说明：为提高安全性，控制台访问或 OpenAPI 调用访问，建议只选择一种访问方式。</p>						
控制台密码	自定义密码						
需要重置密码	根据需要选择						
MFA 多因素认证	开启 MFA 认证（本示例未开通）						

用户账号信息

\* 登录名称 ①

user001 @ [REDACTED] onaliyun.com user001

user002 @ [REDACTED] onaliyun.com user001

+ 添加用户

访问方式 ②

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

#### 步骤 4 创建用户组

RAM 访问控制 / 用户组

概览

身份管理

用户

用户组

角色

用户组

通过用户组对职责相同的 RAM 用户进行分类并授权，可以更加高效地管理用户及其权限。  
对一个用户组进行授权后，用户组内的所有用户会自动继承该用户组的权限。  
如果一个用户被加入到多个用户组，那么该用户将会继承多个用户组的权限。

创建用户组

用户组名称:

\* 用户组名称  
data\_team  
最大长度 64 个字符，允许英文字母、数字、\_、- 或 .。

\* 显示名称  
数据平台组  
最大长度 128 个字符或汉字。

备注

最大长度 128 个字符。

**确定** **取消**

## 步骤 5 添加组成员

用户组			
通过用户组对职责相同的 RAM 用户进行分类并授权，可以更加高效地管理用户及其权限。 对一个用户组进行授权后，用户组内的所有用户会自动继承该用户组的权限。 如果一个用户被加入到多个用户组，那么该用户将会继承多个用户组的权限。			
创建用户组	用户组名称	备注	操作
	data_team 数据平台组	2021年11月1日 14:01:25	<b>添加组成员</b> <b>添加权限</b> <b>删除</b>

添加组成员

用户加入到用户组后，将拥有该组所有权限。

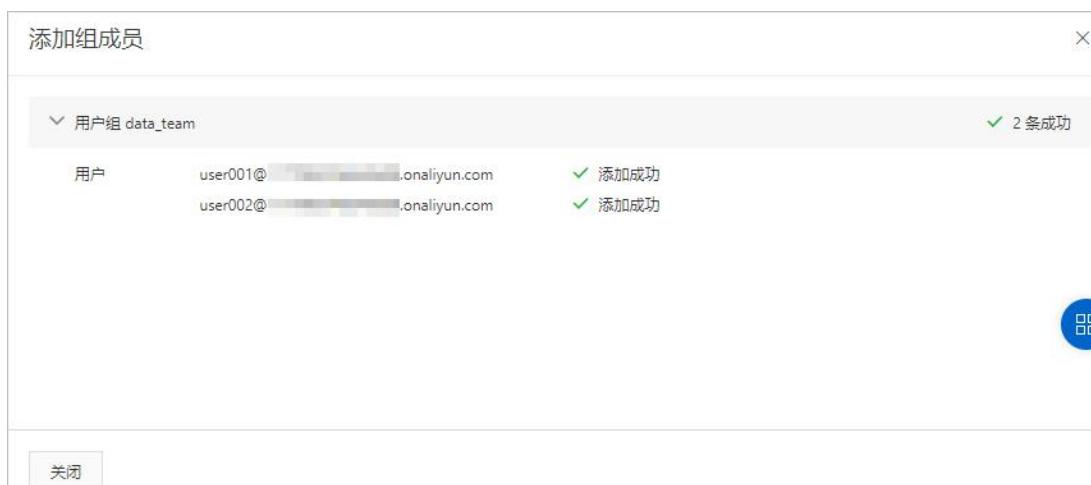
\* 用户组  
data\_team

\* 用户 **+ 新建用户**

请输入	已选择 (2)	清空
user002@...onaliyun.com user002	user002@...onaliyun.com user001@...onaliyun.com	
user001@...onaliyun.com user001		
Alice	开发组	
Bob	test团队人员	
sts		

**确定** **取消**

步骤 6 如果提示需要输入手机验证码，按界面提示操作即可。



### 5.3.2.2.创建资源组

步骤 1 在 CADT 控制台单击管理 > 权限管理 > 创建资源组。



或直接登录资源管理控制台：

<https://resourcemanager.console.aliyun.com/resource-groups>

步骤 2 根据实际需求，创建资源组，填写

- 资源组标示: data
  - 数据组名称: 数据平台组



步骤 3 在 CADT 控制台查看资源组，刷新后，可以看到已创建的资源组。

权限管理						
1	2	3	4	5	6	7
创建用户		创建资源组			用户授权	
操作				更多操作		
资源组名称	资源组Id	资源组唯一标识	状态	创建时间	操作	操作
默认资源组	rg-acfmyrjrfgru2sq	default	可用	2019-10-29 14:49:10	管理资源组	<a href="#">管理资源组</a>
test	rg-aek3bufimh7foq	test	可用	2020-05-12 17:29:05	管理资源组	<a href="#">管理资源组</a>
开发环境	rg-aek22hkgslk4zaa	dev	可用	2020-12-09 16:12:28	管理资源组	<a href="#">管理资源组</a>
生产环境	rg-aekzlmqcmq5zhtq	prod	可用	2020-12-09 16:12:57	管理资源组	<a href="#">管理资源组</a>
测试环境	rg-aek2f7ovisbd2oa	test-	可用	2020-12-09 16:13:15	管理资源组	<a href="#">管理资源组</a>
数据平台组	rg-aek2l2v2g4zoso7a	data	可用	2021-11-01 14:08:07	管理资源组	<a href="#">管理资源组</a>

### 5.3.2.3.资源组授权

步骤 1 添加资源组需要的产品使用权限，在 CADT 控制台单击**资源组授权**。

或直接登录资源组控制台 <https://resourcemanager.console.aliyun.com/resource-groups>



步骤 2 本示例，用户需要管理如下权限：VPC、ECS、RDS、Redis、EIP、SLB、CADT、云监控、安全组、OSS（需自定义权限）

添加如下权限：

**【注意：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】**

AliyunVPCFullAccess、AliyunECSFullAccess、AliyunRDSFullAccess、  
AliyunOSSFullAccess、AliyunKvstoreFullAccess  
AliyunEIPFullAccess、AliyunSLBFullAccess、AliyunCADTFullAccess、  
AliyunCloudMonitorFullAccess



步骤 3 查看已经添加的权限，根据需求，可继续添加或移除授权。

资源管理	新增授权	主体类型:	请选择	被授权主体:	请输入	操作
资源目录	<input type="checkbox"/>	主体类型	被授权主体		权限策略名称	备注
概览	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunOSSFullAccess	管理对象存储服务(OSS)权限
资源共享	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunECSFullAccess	管理云服务器服务(ECS)的权限
我的资源	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunRDSFullAccess	管理云数据库服务(RDS)的权限
资源组	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunSLBFullAccess	管理负载均衡服务(SLB)的权限
标签	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunVPCReadOnlyAccess	只读访问专有网络(VPC)的权限
预置标签	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunEIPFullAccess	管理弹性公网IP(EIP)的权限
标签编辑器	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunKvstoreFullAccess	管理云数据库Redis版(Kvstore)的权限
配额管理	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunCloudMonitorFullAccess	管理云监控(CloudMonitor)的权限
	<input type="checkbox"/>	用户组	data_team@group.1431808278228723.onaliyun.com	data_team	AliyunCADTFullAccess	管理云架构设计工具(CADT)的权限。

步骤 4 查看用户组，权限管理的授权范围，也是“数据平台组”。

授权范围	权限策略名称	权限策略类型	备注
数据平台组 rg-aek2iofz7bvtfty	AliyunOSSFullAccess	系统策略	管理对象存储服务(OSS)的权限
数据平台组 rg-aek2iofz7bvtfty	AliyunECSFullAccess	系统策略	管理云服务器服务(ECS)的权限
数据平台组 rg-aek2iofz7bvtfty	AliyunRDSFullAccess	系统策略	管理云数据库服务(RDS)的权限

### 5.3.2.4.添加授权架构

#### 前提条件

需要授权的架构已在 CADT 控制台创建完成，添加授权架构后，该资源组可以查看该架构。

#### 操作步骤

步骤 1 在 CADT 控制台单击管理 > 权限管理，在对应的资源组，单击添加授权。

资源组名称	资源组ID	资源组唯一标识	状态
测试环境	rg-aek2amhmr3jtai	test	可用
数据平台组	rg-aek2iofz7bvtfty	database	可用

步骤 2 添加需要授权的架构，并授权。



步骤 3 授权确认后，该资源组的用户，登录 CADT 可以查看到该架构。

前提：需要 RAM 用户有 CADT 查看或管理权限（[资源组授权](#)已授权 AliyunCADTFullAccess）。



## 5.3.3.云资源部署

### 5.3.3.1.设计资源架构

参考[云速搭架构设计入门](#)中资源规划涉及的云资源，设计云上架构，或直接使用 CADT 提供的模版进行验证。

登录 CADT 控制台 (<https://bstudio.console.aliyun.com/>)。

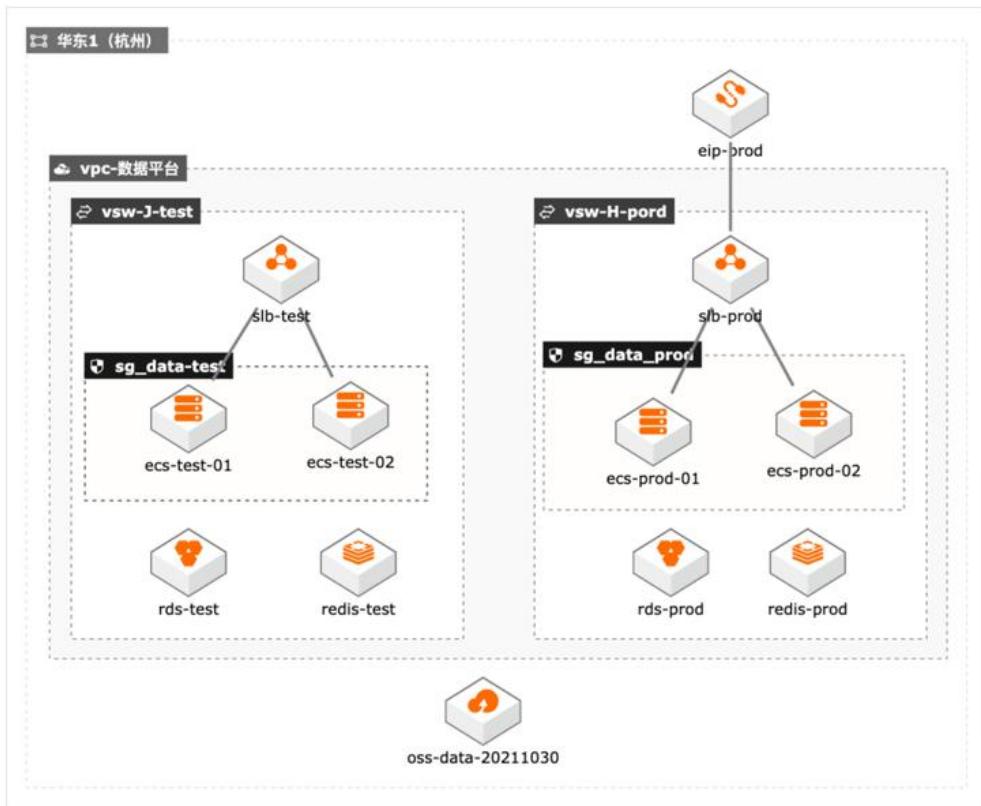
步骤 1 单击新建 > 官方模板库新建。



步骤 2 在搜索框中搜索“资源组场景验证”，找到目标模板，将鼠标移到模板图标上，单击**基于方案新建**。



步骤3 系统基于模板生成应用架构图，双击资源图标进行参数配置。

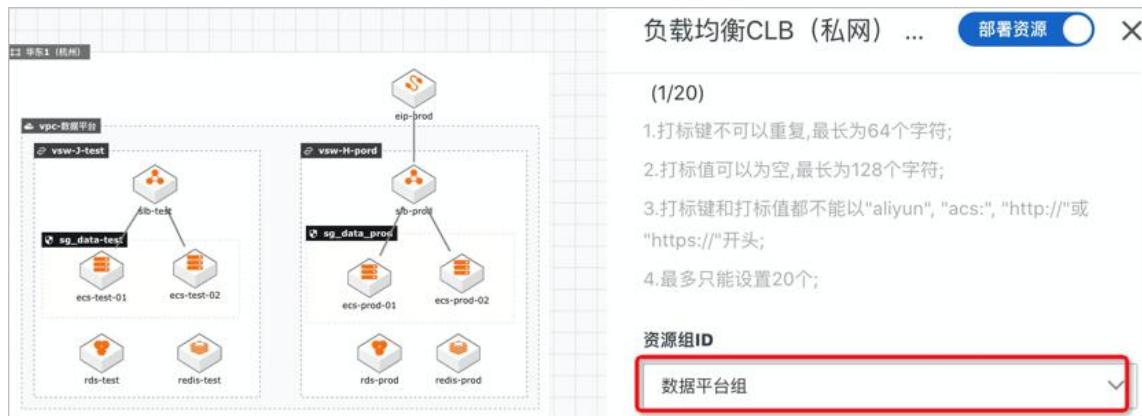


### 操作注意事项：

- 如果存在已保有资源，比如VPC、交换机等，购买方式选择“导入已保有”



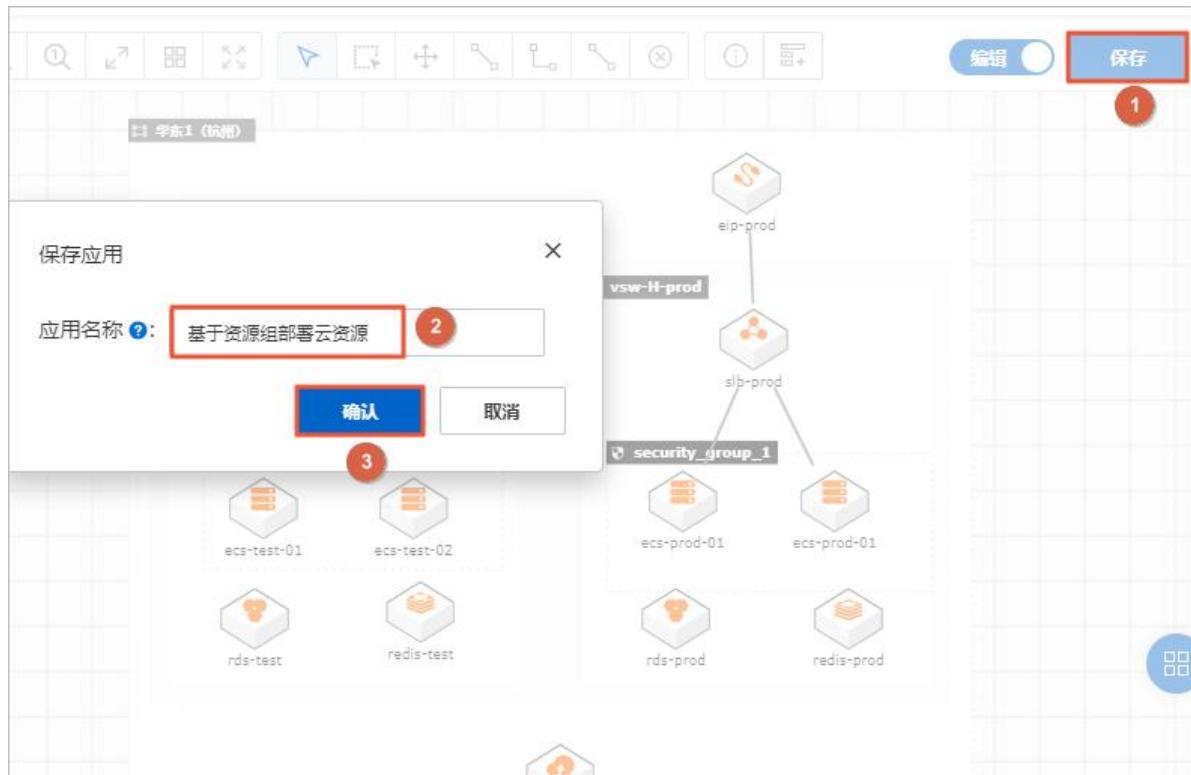
- 根据实际情况调整可用区后，请确认资源在对应可用区是否有库存。
- 模版里各个云资源的资源组都修改为上文中创建的资源组（数据平台组）



- OSS bucket 全局唯一, 请添加适当后缀, 避免重名
- 云服务器 ECS 需要预设登录密码, 或者选择“稍后创建”。

### 5.3.3.2.部署资源

步骤 1 将配置好的架构保存为应用。



步骤 2 保存架构后, 单击**部署应用**。



步骤3 开始进行资源验证，如果有校验错误提示，根据提示进行修改，直至校验成功。

**资源验证**

资源名称	资源类型	区域	规格	结果	备注	操作
rds-prod	rds	杭州	MySQL	成功	校验通过	定位
rds-test	rds	杭州	MySQL	成功	校验通过	定位
vsw-H-pord	vswitch	杭州	10.0.2.0/24	成功	校验通过	定位
vsw-J-test	vswitch	杭州	10.0.1.0/24	成功	校验通过	定位
ecs-prod-01	ecs	杭州	ecs.c6.xlarge	成功	校验通过	定位
ecs-test-01	ecs	杭州	ecs.c6.large	成功	校验通过	定位
ecs-test-02	ecs	杭州	ecs.c6.large	成功	校验通过	定位
ecs-prod-02	ecs	杭州	ecs.c6.xlarge	成功	校验通过	定位

状态: **校验成功**

[下一步: 价格清单](#) [返回](#)

步骤4 核对方案价格，也可以单击[查看报告](#)得到一份报价清单。



步骤 5 勾选《云速搭服务条款》，确认价格后，单击**下一步：支付并创建**。

**确认订单**

免费 包年包月 按量付费 X

资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
oss-data-20211030	oss	杭州	Standard	1	-			新购

《云速搭服务条款》 1  
部署前，请阅读并勾选服务条款

按量付费: /时 2

状态: 计价成功

[上一步: 价格清单](#) 下一步: 支付并创建

步骤 6 等待资源部署完成后，可打开**资源清单**查看所有的资源信息。



## 5.3.4.权限验证

### 5.3.4.1.验证资源组支持的产品权限

步骤 1 在主账号的 RAM 控制台记录登录地址。

The screenshot shows the RAM Access Control console. On the left, the '概览' (Overview) tab is selected under '身份管理' (Identity Management). The main area displays account statistics: 2 users, 1 user group, 1 custom policy, and 36 roles. To the right, the '账号管理' (Account Management) section shows the '主账号' (Primary Account) with the login address 'https://signin.aliyun.com/...onaliyun.com'. A red box highlights this URL.

步骤 2 在浏览器输入登录地址，通过子账号，输入用户名和密码访问阿里云。

The screenshot shows the 'RAM 用户登录' (RAM User Login) page. It has a field for entering the username 'user001@...onaliyun.com'. Below the field, a note says: 'RAM 用户名格式: <用户名>@<默认域名> 或 <用户名>@<企业别名>, 例如: username@company-alias.onaliyun.com 或 username@company-alias.' At the bottom, there's a note about adhering to the '产品协议' (Product Agreement) and a blue '下一步' (Next Step) button.



步骤3 验证资源组，试图修改权限。如图所示，登录资源组“无操作权限”。 【权限正常】  
登录**资源管理**控制台，找到对应的资源组，然后打开**权限管理**页签：

资源组名称	资源组标识	资源组ID	资源数量
数据平台组	data	rg-aekzufj2i6kaabi	1

步骤4 登录VPC控制台，只能看到“数据平台组”下的VPC。【权限正常】

VPC控制台地址：<https://vpc.console.aliyun.com/>

实例ID/名称	标签	网段	IPv6网段	状态	默认专有网络	路由表
vpc-bp1f0vbxmh4shz9lhtg0 vpc-数据库平台		10.0.0.0/8		开通IPv6 可用	未绑定云企业网	否

步骤5 查看交换机，只能看到“数据平台组”下的交换机。【权限正常】

实例ID/名称	专有网络	标签	状态	IPv4网段	可用IP数
vsw-bp1mu91ucmgl7uxxim9n vsw-J-test	vpc-bp1f0vbxmh4shz9lhtg0 vpc-数据库平台		可用	10.0.1.0/24	247
vsw-bp19k2gcc1oyvh5wt6kgo vsw-H-pord	vpc-bp1f0vbxmh4shz9lhtg0 vpc-数据库平台		可用	10.0.2.0/24	247

步骤6 查看弹性公网IP，只能看到“数据平台组”下的弹性公网IP。【权限正常】

实例ID/名称	安全防护	IP地址	监控	带宽	带宽包服务	IP状态
eip-bp1y6iktunicuk41aexjm eip-prod		J22		5 Mbps 按使用流量计费	未加入带宽包服务 加入	已分配

步骤 7 登录 ECS 控制台，只能看到“数据平台组”下的 ECS。【权限正常】

ECS 控制台地址：<https://ecs.console.aliyun.com/home>

The screenshot shows the ECS console interface. The top navigation bar includes the Alibaba Cloud logo, workspace selection, a dropdown for 'Data Platform Group' (which is highlighted with a red box), a search bar, and a 'Fees' button. On the left, a sidebar for 'ECS Cloud Servers' has 'Instance' selected (highlighted with a red box). The main area displays a table of instances in the 'East China 1 (Hangzhou)' region. The table columns include 'Instance ID / Name', 'Status', 'Tags', 'Operating System', 'Monitoring', and 'Region'. Four instances are listed:

- i-bp1fttdhw5lwajpjstfo ecs-prod-01 (Running)
- i-bp1e30op4t0vna48iowq ecs-prod-02 (Running)
- i-bp13dziilg8gdmcnpgy6 ecs-test-02 (Running)
- i-bp17aaabsmos51wgj30o ecs-test-01 (Running)

步骤 8 登录 RDS 控制台，只能看到“数据平台组”下的 RDS。【权限正常】

RDS 控制台地址：<https://rdsnext.console.aliyun.com/rdsList/cn-hangzhou/basic>

The screenshot shows the RDS console interface. The top navigation bar includes the Alibaba Cloud logo, workspace selection, a dropdown for 'Data Platform Group' (highlighted with a red box), a search bar, and a 'Fees' button. On the left, a sidebar for 'Cloud Database RDS' has 'Instance List' selected. The main area displays a table titled 'Instance List' with tabs for 'Basic Information', 'Label Information', and 'High Performance'. The table columns include 'Instance ID/Name', 'Status', 'Creation Time', 'Instance Type', 'Database Type', and 'Billing Type'. Two database instances are listed:

- rm-bp1zsh1m801kydk09 rds-prod (Running, MySQL 5.7, Pay-As-You-Go)
- rm-bp1d6e1cmmt3w38dv1 rds-test (Running, MySQL 5.7, Pay-As-You-Go)

步骤 9 登录 Redis 控制台，只能看到“数据平台组”下的 Redis。【权限正常】

Redis 控制台地址：<https://kvstore.console.aliyun.com/Redis/instance/cn-hangzhou>

实例ID/名称	状态	已用内存及配额	可用区	版本
r-bp1j124y8z4dr8h9oo redis-prod	运行中	3.76% 38.52MB/1.00GB	杭州 可用区H	Redis 5.0 社区版
r-bp1uxuwu314fwk3gb0 redis-test	运行中	3.76% 38.52MB/1.00GB	杭州 可用区J	Redis 5.0 社区版

### 5.3.4.2.自定义策略管理产品

对于支持资源组的云资源，可以通过上述方案，在架构设计时将其加入资源组，然后针对资源组授权。可以直接使用系统策略，操作便捷，学习成本低。

查看已经支持资源组的产品：[https://help.aliyun.com/document\\_detail/94479.htm](https://help.aliyun.com/document_detail/94479.htm)

对于更加精细的授权，或暂时不支持资源组的产品，也可以使用自定义策略。

以 OSS 为例，授权 RAM 用户（或用户组）通过 OSS 控制台列举并读取名为#**更改为 CADT 创建的 bucket#** 存储空间中的资源。

步骤 1 登录 RAM 访问控制，创建自定义权限策略。

(<https://ram.console.aliyun.com/policies/new>)

- 输入自定义名称：控制台访问 OSS 指定 bucket 的资源
- 配置方式：脚本配置
- 策略内容：输入下方策略内容，对应 OSS Bucket 修改为 **CADT 创建的 bucket**

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "oss>ListBuckets",
        "oss>GetBucketStat",
        "oss>GetBucketInfo",
        "oss>GetObject"
      ]
    }
  ]
}
```

```
        "oss:GetBucketTagging",
        "oss:GetBucketLifecycle",
        "oss:GetBucketWorm",
        "oss:GetBucketVersioning",
        "oss:GetBucketAcl"
    ],
    "Resource": "acs:oss:*:*"
},
{
    "Effect": "Allow",
    "Action": [
        "oss>ListObjects",
        "oss:GetBucketAcl"
    ],
    "Resource": "acs:oss:*:*:CADT 创建的 bucket"
},
{
    "Effect": "Allow",
    "Action": [
        "oss:GetObject",
        "oss:GetObjectAcl"
    ],
    "Resource": "acs:oss:*:*: CADT 创建的 bucket/*"
}
]
```

## ← 新建自定义权限策略

\* 策略名称

备注

配置模式  
 可视化配置  
 脚本配置

策略内容  
  

```

22     "oss:GetBucketAcl"
23   ],
24   "Resource": "acs:oss:*:* oss-data-20211030"
25 },
26 {
27   "Effect": "Allow",
28   "Action": [
29     "oss:GetObject",
30     "oss:GetObjectAcl"
31   ],
32   "Resource": "acs:oss:*:* oss-data-20211030/*"
33 }
34 ]
35 }
36

```

步骤 2 登录用户组，新增授权自定义策略。[\(https://ram.console.aliyun.com/groups\)](https://ram.console.aliyun.com/groups)

### 用户组

通过用户组对职责相同的 RAM 用户进行分类并授权，可以更加高效地管理用户及其权限。  
 对一个用户组进行授权后，用户组内的所有用户会自动继承该用户组的权限。  
 如果一个用户被加入到多个用户组，那么该用户将会继承多个用户组的权限。

操作	创建时间	备注	用户组名称/显示名称	用户组名称	创建用户组
<input type="button" value="添加权限"/>	2021年11月1日 14:01:25		data_team 数据平台组	data_team	<input type="button" value="添加用户组"/>

步骤3 完成以下配置，并单击确定。

- 授权范围：整个云账号
- 授权主题：在[创建用户和用户组](#)中创建的用户组
- 选择权限：创建的自定义策略

### 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 1

指定资源组

请选择或输入资源组名称进行搜索

\* 授权主体

2

\* 选择权限

<input type="radio"/> 系统策略	<input type="radio"/> 自定义策略 <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">3</span>	<input type="radio"/> 新建权限策略
请输入权限策略名称进行模糊搜索。		
<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">取消</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">完成</span>		
<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">已选择 (1)</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">清空</span>		
<span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">控制台访问OSS指定bucket的资源</span> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">×</span>		

权限策略名称      备注

cadt-full-access	cadt-full-access
数据平台组的OSS	(已添加)
<input type="checkbox"/> 控制台访问OSS指定bucket的...	4

5 消

### 添加权限

授权范围      整个云账号

data\_team@group.123456.onaliyun.com      ✓ 1条成功

权限策略名称      控制台访问OSS指定bucket的资源      ✓ 授权成功

完成

步骤 4 通过子账号（user001 或 user002）登录 OSS 控制台，可以查看具体的 oss-bucket。如果需要进一步的精细授权，可以增加自定义策略。



#### 5.3.4.3. 查看 CADT 架构

步骤 1 登录 CADT 控制台，只能看到“数据平台组”下的 CADT 架构。【权限正常】

控制台地址: <https://bpstudio.console.aliyun.com/#/bpStudio/template/mine>



**注：**如果需要做精细化管理，可以使用自定义策略。

### 5.3.4.4.查看应用组监控

步骤 1 通过子账号 RAM 登录云监控控制台。

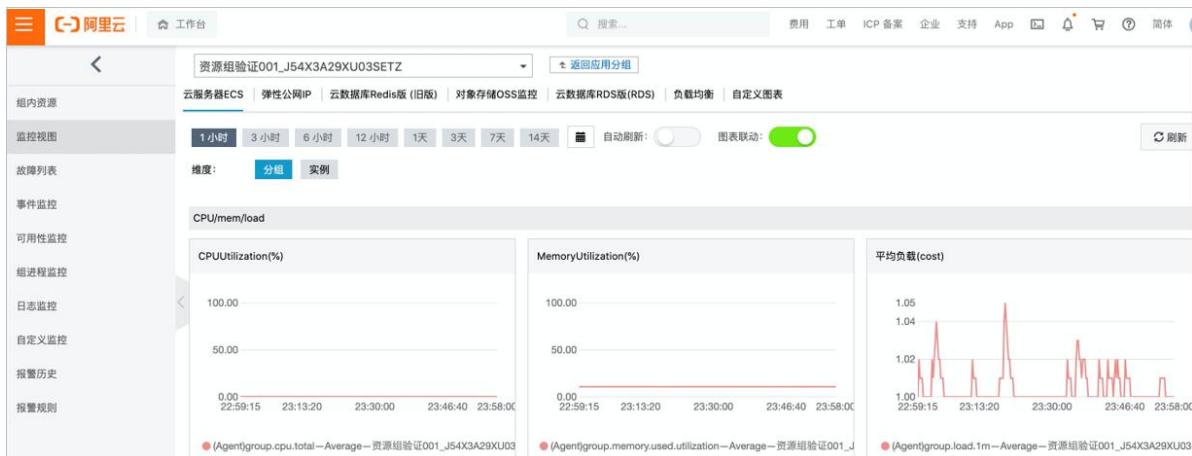
(<https://cloudmonitor.console.aliyun.com/#/home/ecs>)

步骤 2 查看应用分组。

通过 CADT 架构创建的应用，已经自动生成应用分组，如下图所示：

步骤 3 查看所在资源组内的云产品监控信息。

对该资源组下的监控进行统一管理，包括增加阀值告警、添加联系人组、查看监控视图、故障列表等。



### 5.3.4.5.跨资源组转移资源

如果需要将一个资源组内的资源转移到另一个资源组，可以通过如下步骤。

支持通过资源管理控制台或支持资源组的云服务 API。本示例以控制台操作为例：

步骤 1 登录资源管理控制台。

(<https://resourcemanager.console.aliyun.com/resource-groups>)

步骤 2 在左侧导航栏，单击资源组，单击默认资源组的资源管理。

The screenshot shows the Alibaba Cloud Resource Management Control Panel. The left sidebar has a tree structure with '资源管理' (Resource Management) expanded, showing '资源目录', '资源共享', '我的资源', and '资源组' (Resource Group), which is highlighted with a red box. The main content area is titled '资源组' (Resource Groups). It contains a welcome message and information about resource groups. Below this is a table with two rows:

资源组名称	资源组标识	资源组ID	资源数量	授权数量	状态	操作
默认资源组	default	rg-acfmyoj5mg3w54y	141	0	可用	<a href="#">权限管理</a> <a href="#">资源管理</a> <a href="#">监控管理</a>
控制台资源组	app	rg-aekza3c5znhvocq	0	0	可用	<a href="#">权限管理</a> <a href="#">资源管理</a> <a href="#">监控管理</a>

步骤 3 通过筛选，选择需要转出的资源，然后在列表的底部，单击转出资源。

默认资源组

概览 资源管理 权限管理 设置

新购资源 转入资源 产品 云数据库Redis版 资源类型 全部 地域 全部 支持筛选

ID/名称	地域	资源类型	标签
<input checked="" type="checkbox"/> z4dr8h9oo	华东1 (杭州)	云数据库Redis版-实例	-
<input checked="" type="checkbox"/> ffwk3gb0	华东1 (杭州)	云数据库Redis版-实例	-
<input type="checkbox"/> r-uf6zxbub64mupfm14kvstore	华东2 (上海)	云数据库Redis版-实例	-
转出资源 (2)			

步骤 4 在转出资源面板，选择将要转入的目标资源组，并单击**确定**。

转出资源

资源组名称	资源组标识	资源组ID	资源数量	授权数量	状态
控制台资源组	app	rg-aekza3c5zhvocq	0	0	可用
资源组场景验证	cadt-DB-rg-aekzma6ithev4wi-202...	rg-aekzma6ithev4wi	0	0	删除中...
生产环境	prod	rg-aekzk5ecgpvkdndq	0	0	可用
开发环境	dev	rg-aek2umm2gril7li	0	2	可用
测试环境	test	rg-aek2amhmr3jtai	2	0	可用
数据平台组	database	rg-aek2iofz7bvtfty	19	11	可用

确定 取消

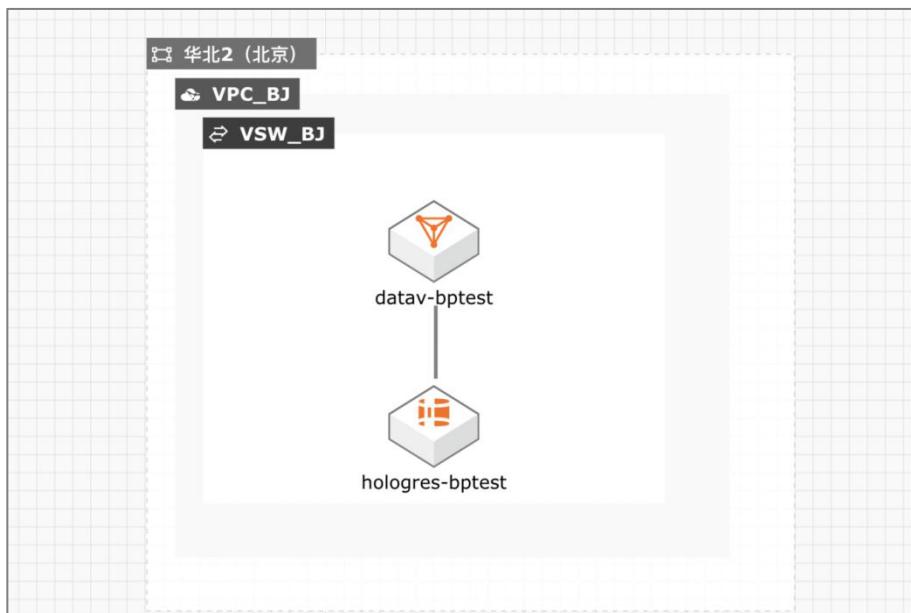
## 5.4.云速搭部署 Hologres 应用

作者 | 阿里云解决方案架构师 袁影

### 5.4.1. 云速搭架构设计

#### 方案架构

通过云速搭实现一个 Hologres+DataV 的可视化大屏开发架构，利用将 Hologres 存储的聚合数据呈现到 DataV 可视化大屏中。



#### 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
Hologres	Region
DataV	全局

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	华北 2 (北京)	-
VPC	VPC_BJ	192.168.0.0/16
AZ	VSW_BJ	192.168.0.0/24

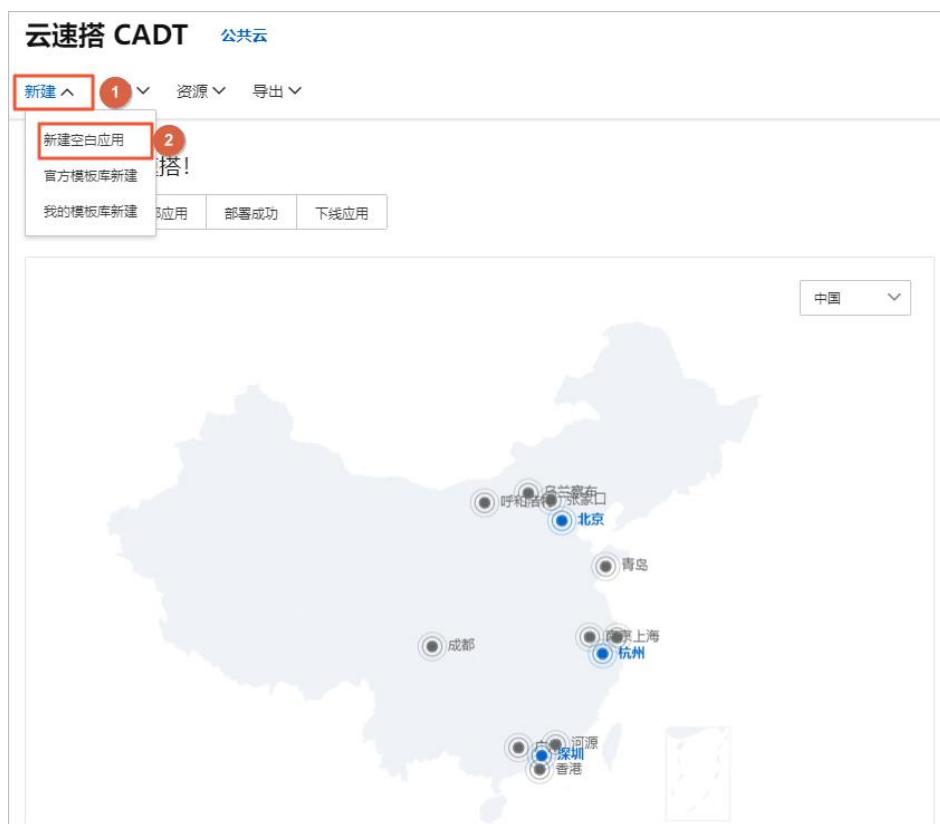
### 5.4.2.应用架构设计

在进行应用架构设计时，可以提前进行资源规划。

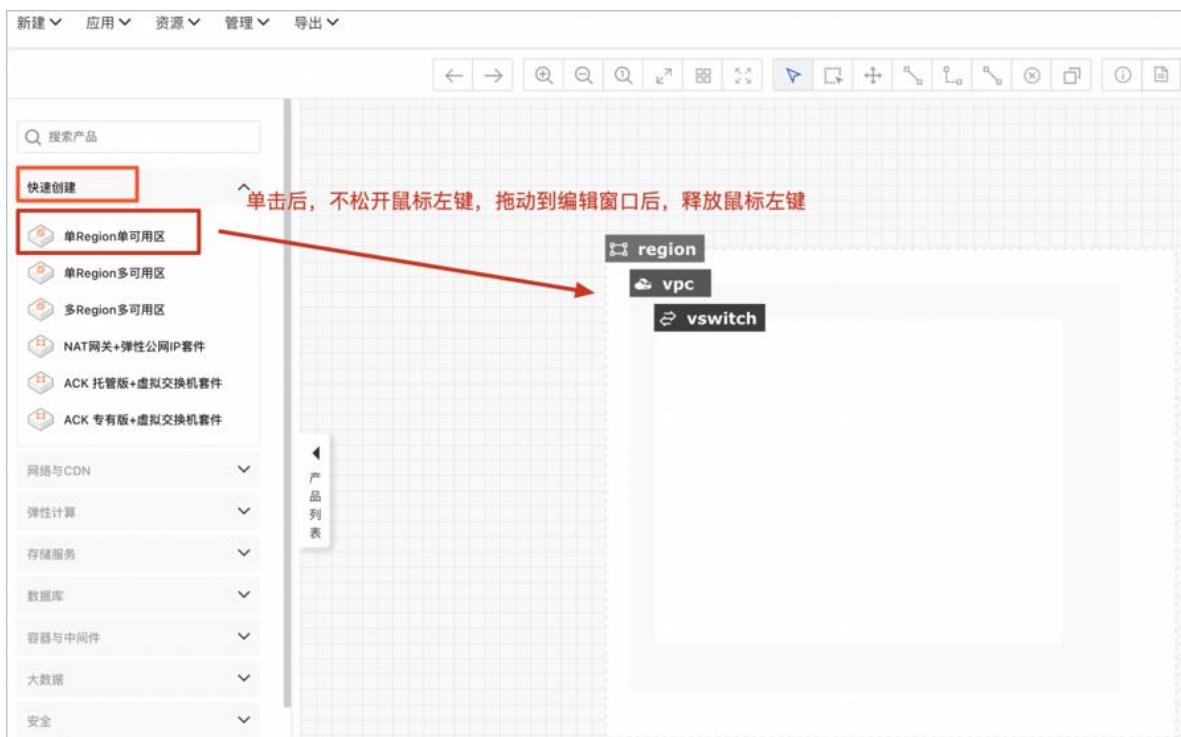
本示例资源规划清单如下表所示。

资源分类	资源名称	网段
Region	深圳	-
VPC	VPC_BJ	192.168.0.0/16
AZ	VSW_BJ	可用区 F 区, 192.168.0.0/24

步骤 1 在 CADT 控制台的菜单栏单击**新建 > 新建空白应用**。

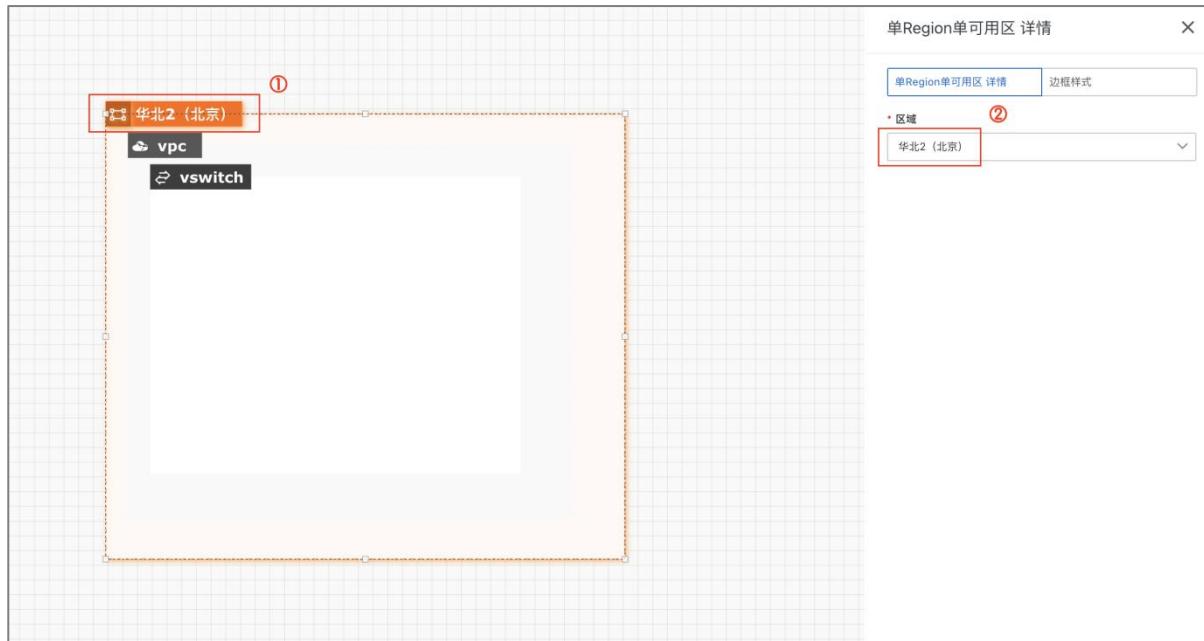


步骤 2 从左侧产品列表的**快速创建**分类下，找到**单 Region 单可用区**，单击后拖入到画布区域中，松开鼠标左键。



依步骤 3 次双击 Region、VPC、vswitch 进行配置。

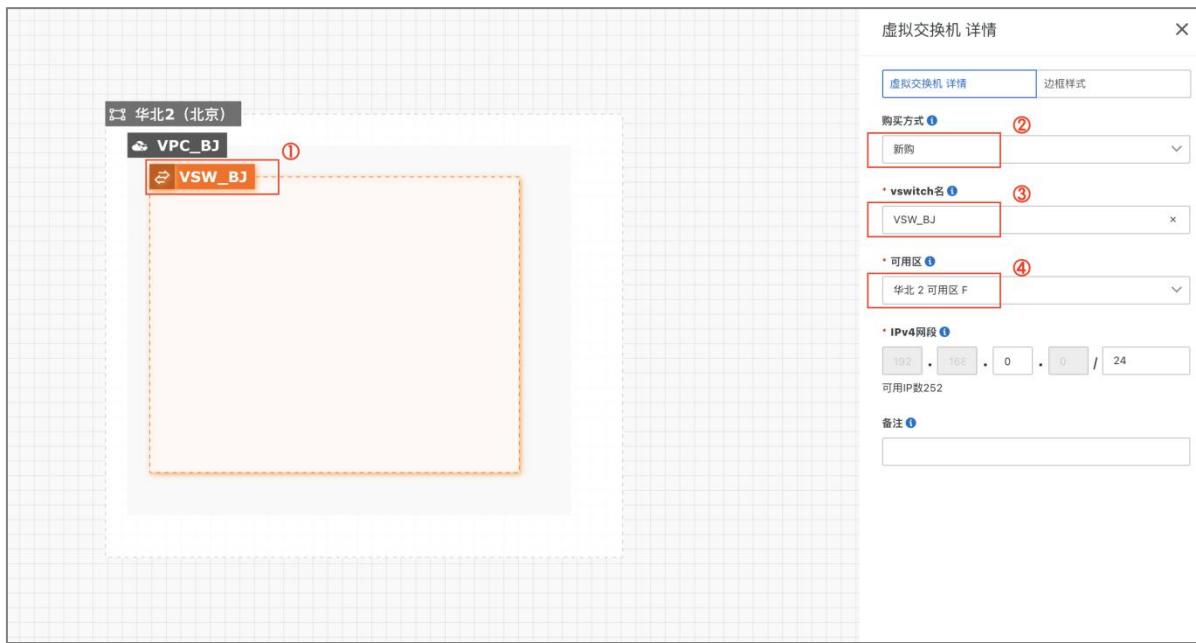
1. 双击 region，在右侧弹出窗口中，选择华北 2（北京）。



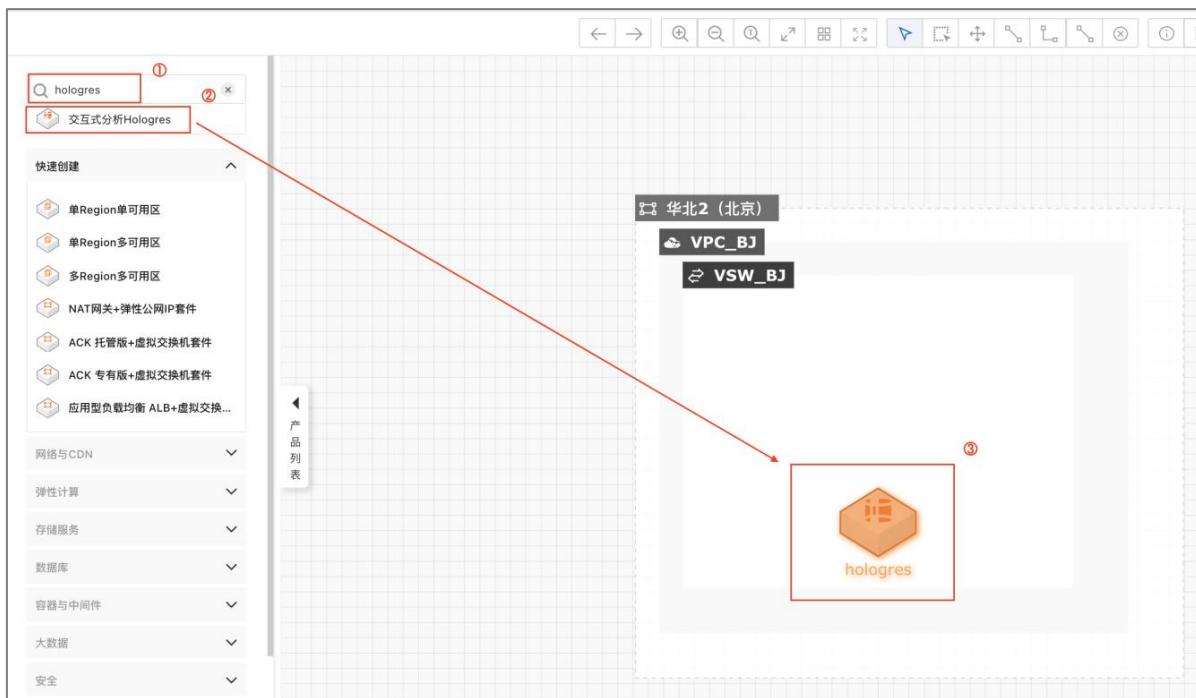
2. 双击 VPC，配置 VPC 参数。



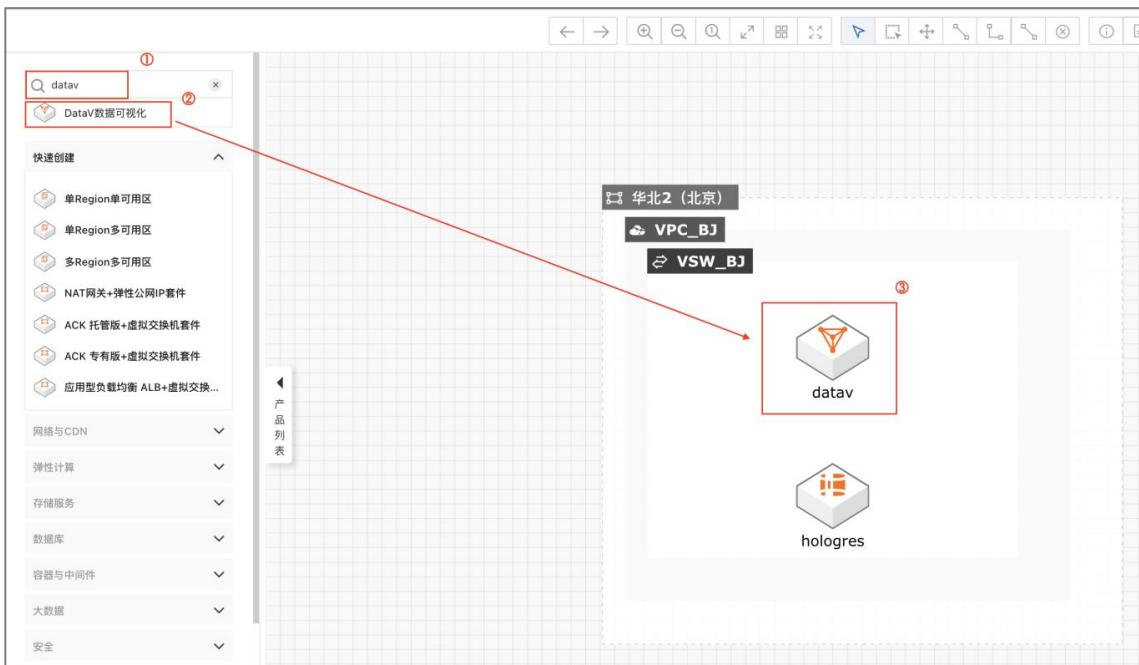
3. 双击 vswitch，配置 vswitch 参数，可用区选择：华北 2 可用区 F。



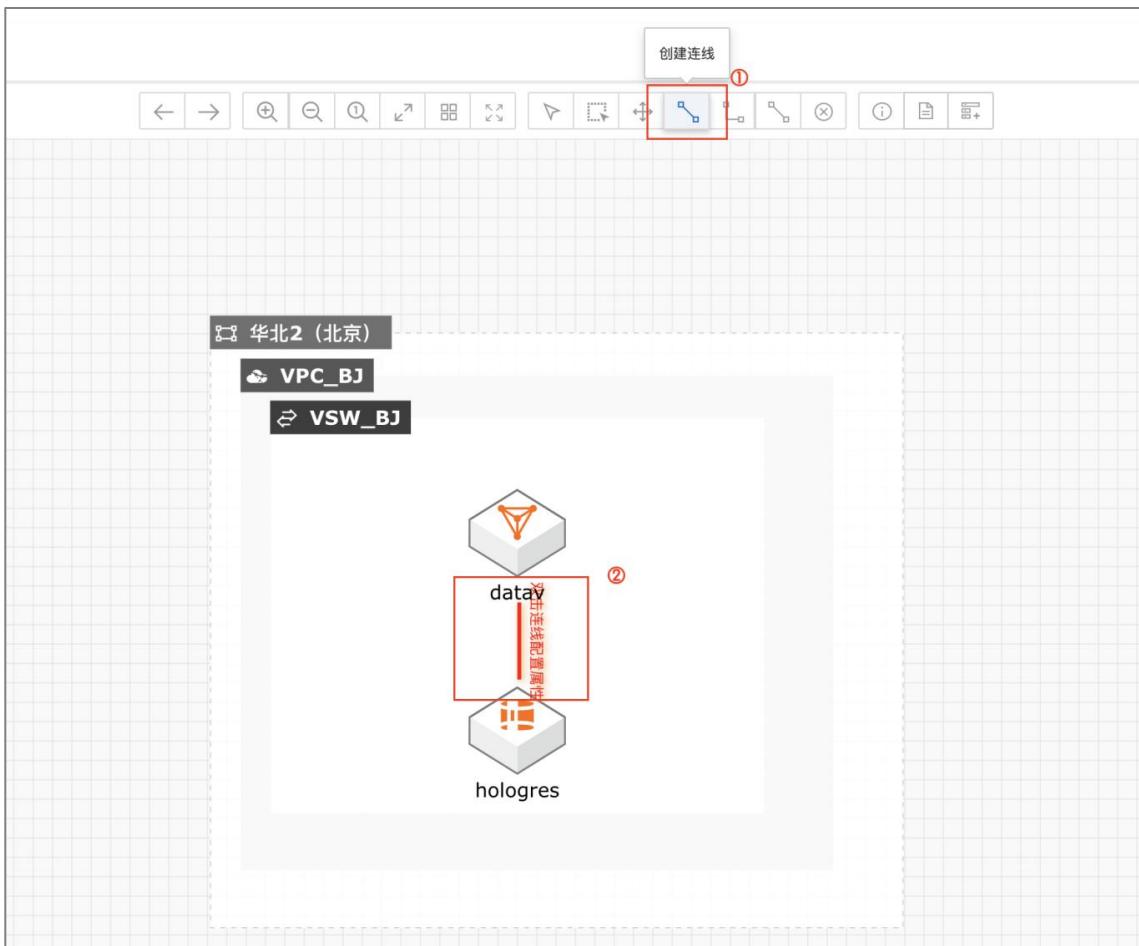
步骤 4 在左侧搜索框中输入 hologres，选定 hologres 图元，拖动到下方。



步骤 5 在左侧搜索框中输入 datav，选定 DataV 数据可视化，拖动到图中。

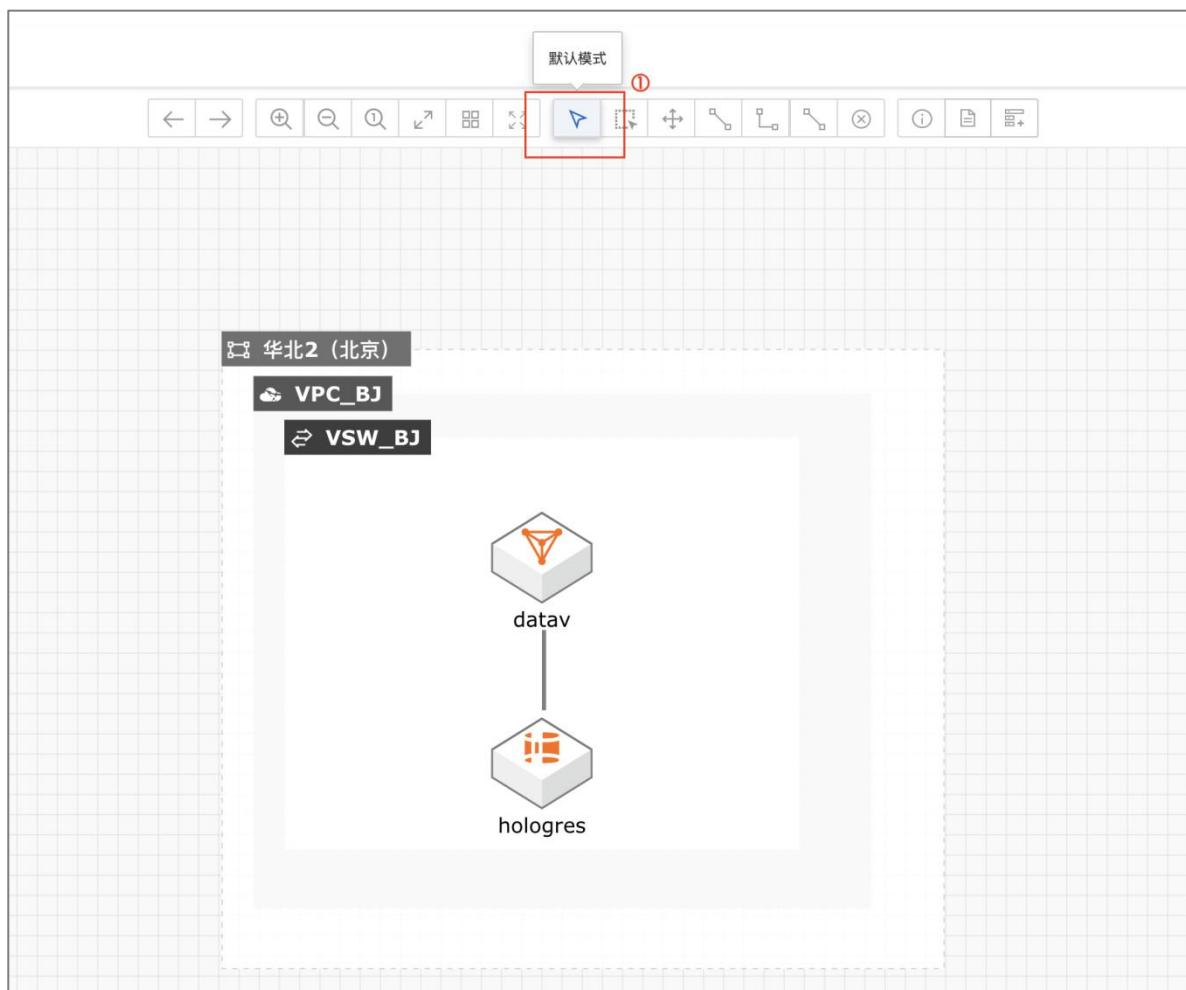


步骤 6 单击**创建连线**按钮，切换到连线模式，依次将 dataV 和 hologres 连接。



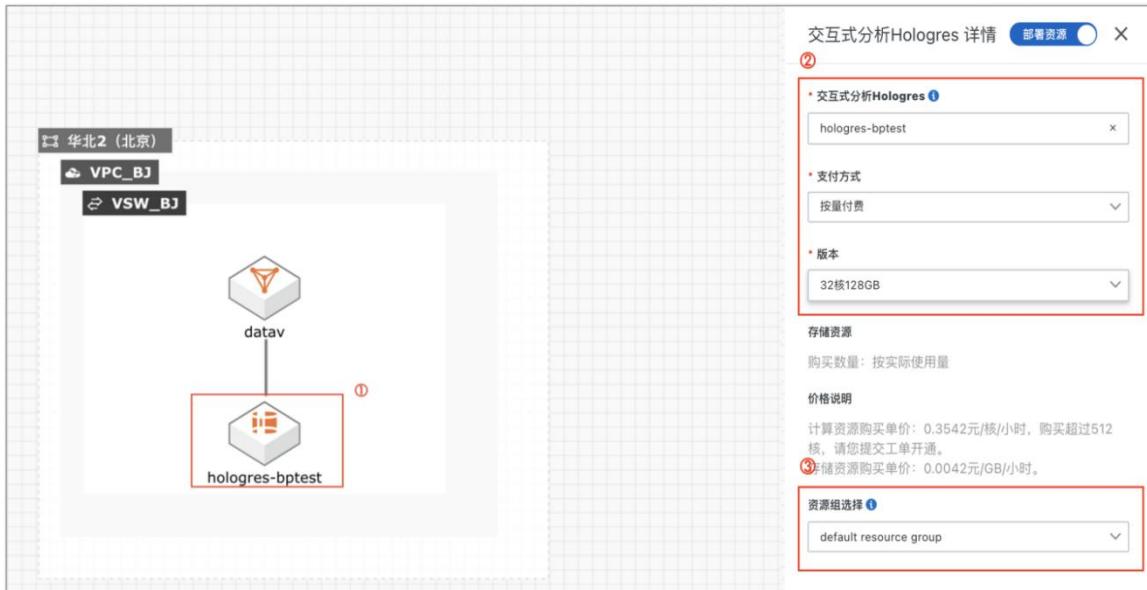
### 5.4.3.配置资源参数

步骤 1 切换回默认模式。



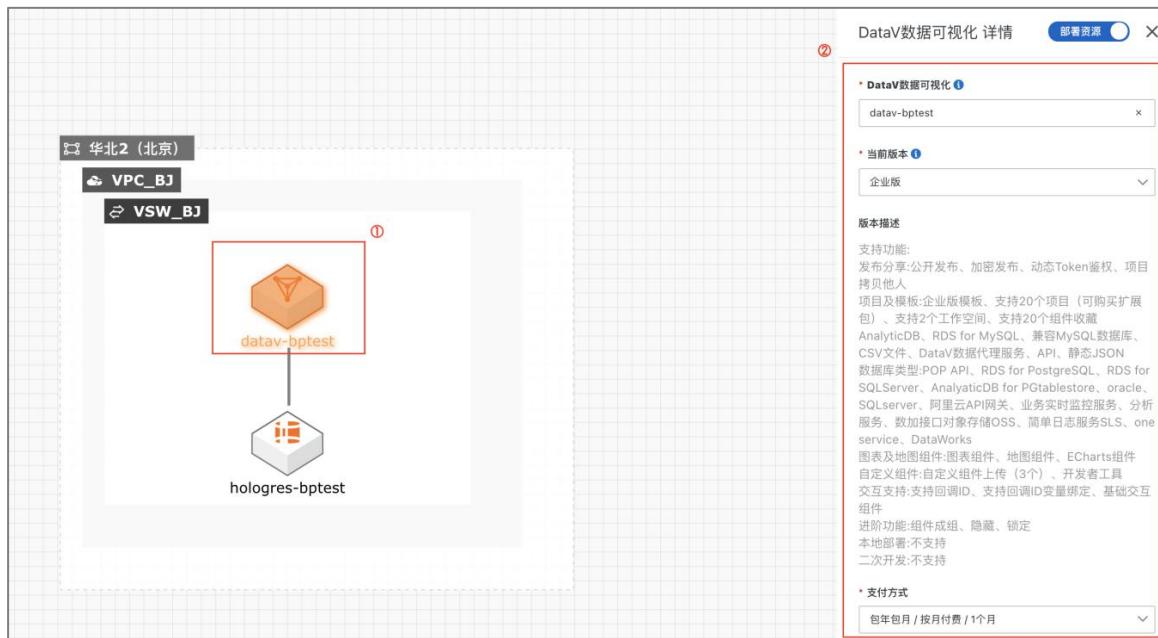
步骤 2 双击 hologres 图标，参考下表进行参数配置。

配置项	参数说明
交互式分析 Hologres	hologres-bptest (确保本账号内不重复)
支付方式	按量付费
版本	32 核 128GB
资源组选择 <b>(必填)</b>	default resource group

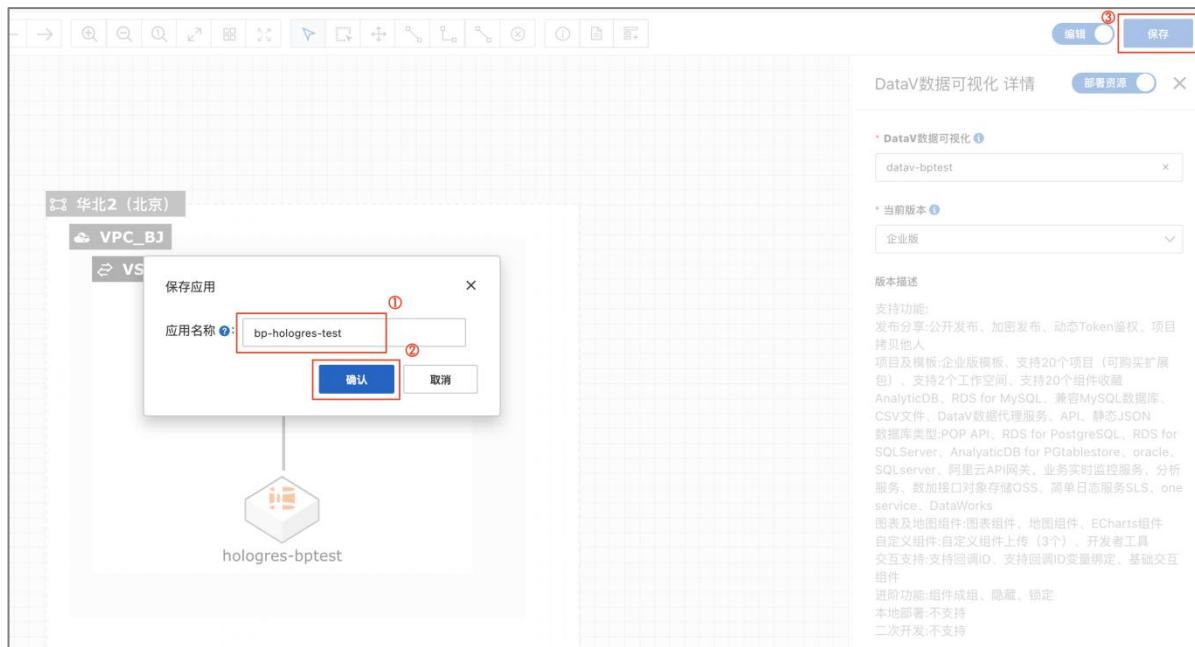


步骤3 双击 dataV 图标，参考下表进行参数配置。

配置项	参数说明
DataV 数据可视化	datav-bptest
当前版本	企业版
支付方式	包年包月/按月付费/1个月

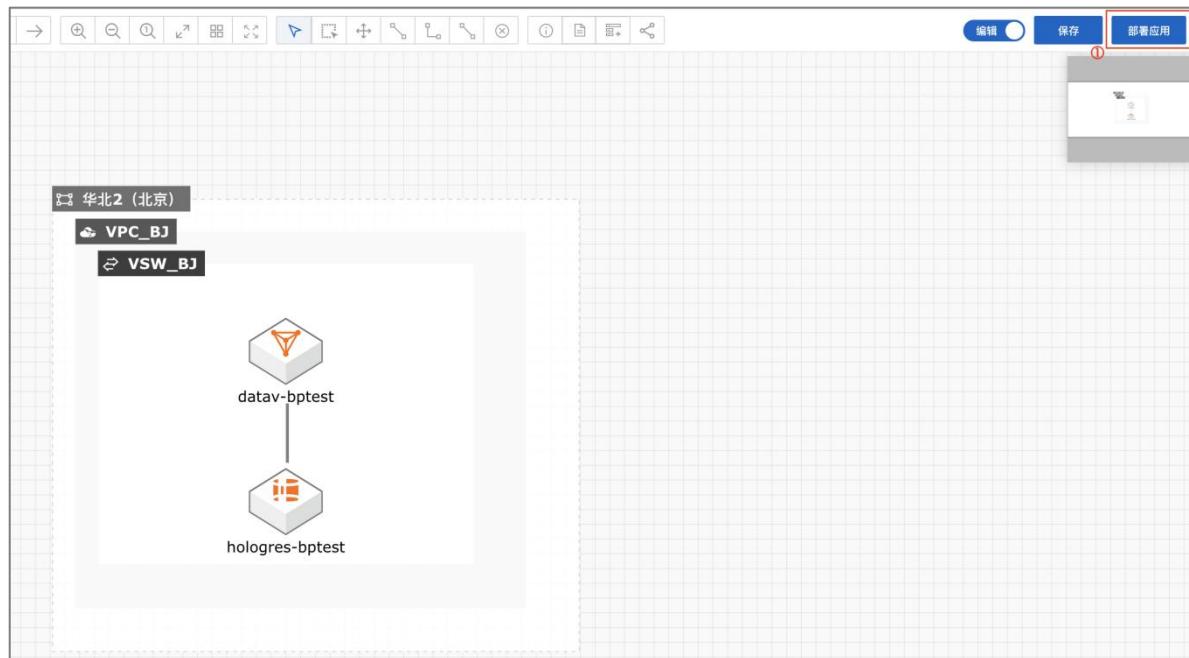


步骤4 完成以上资源配置后，单击**保存**，并设置**应用名称**，最后单击**确认**。



#### 5.4.4. 部署应用

步骤 1 应用保存完成后，单击右上角的**部署应用**。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法、连线配置是否合法、dataV 和 hologres 是否有库存等，一般需要几十秒左右。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	VSW_BJ	vswitch	北京	192.168.0.0/24	成功	校验通过	定位
2	datav-bptest	datav		compVersion	成功	校验通过	定位
3	hologres-bptest	hologres	北京	32	成功	校验通过	定位
4	VPC_BJ	vpc	北京	192.168.0.0/16	成功	校验通过	定位

状态: **校验成功**

① **下一步: 价格清单** **返回**

步骤 3 等待校验成功，单击**下一步：价格清单**。这里会拉取应用所有配置的价格信息。

**导出价格清单**

免费 **包年包月** 按量付费

资源成本占比

资源预算  
● 大数据 大数据: 10... 元

价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
1	datav-bptest	datav	杭州	compVersion	1	1月	500.00元/月	10%	450元/月	定位

状态: **计价成功**

① **上一步: 资源校验** **查看报告** **下一步: 确认订单**

步骤 4 可以单击**查看报告**，查看应用的价格信息。



步骤5 单击下一步：确认订单，在新的窗口中，勾选《云速搭服务条款》，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

确认订单

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	hologres-bpt est	hologres	北京	32	1	11.33元/时	元/时	新购

《云速搭服务条款》  
部署前，请阅读并勾选服务条款

包年包月：  元 按量付费：  元/时

状态：计价成功

[上一步：价格清单](#) [下一步：支付并创建](#)

对于包年包月的资源系统有提示，请单击确认。



步骤 6 单击**下一步: 支付并创建**, 就会进入部署流程, 这里会进行扣费并开始创建资源。

#### 注意:

1. 部署流程一旦开始后, 无法取消。
2. 部署时间预计 3~5 分钟左右, 请耐心等待。



步骤 7 部署完成后, 如下图所示。

**资源部署状态**

序号	资源名称  	资源类型 	付费类型	资源ID 	资源状态	资源更新时间	定位
1	datav-bptest	datav	包年包月	datav-cn-tl32f7kum004 	运行中	2021-11-04 08:57:25	定位
2	VPC_BJ	vpc	-	vpc-2zerwvi1mo1wd6ovcn4vp 	运行中	2021-11-04 08:57:25	定位
3	hologres-bptest	hologres	-	hgpostcn-cn-i7m2f7kup001 	运行中	2021-11-04 08:57:57	定位
4	VSW_BJ	vswitch	-	vsw-2ze08v1qm39fzjiu2du80 	运行中	2021-11-04 08:58:17	定位

**部署概要**

状态: 部署成功 订单编号: 211389255030425211388856280425  
方案编号: VXUOL1T5AIUYYWA4

[查看报告](#) [返回](#)

步骤 8 单击查看报告, 可以查看本次的部署报告。

**资源部署状态**

序号	资源名称  	资源类型 	付费类型	资源ID 	资源状态	资源更新时间	定位
1	datav-bptest	datav	包年包月	datav-cn-tl32f7kum004 	运行中	2021-11-04 08:57:25	定位
2	VPC_BJ	vpc	-	vpc-2zerwvi1mo1wd6ovcn4vp 	运行中	2021-11-04 08:57:25	定位
3	hologres-bptest	hologres	-	hgpostcn-cn-i7m2f7kup001 	运行中	2021-11-04 08:57:57	定位
4	VSW_BJ	vswitch	-	vsw-2ze08v1qm39fzjiu2du80 	运行中	2021-11-04 08:58:17	定位

**部署概要**

状态: 部署成功 订单编号: 211389255030425211388856280425  
方案编号: VXUOL1T5AIUYYWA4

[查看报告](#) [返回](#)



步骤 9 单击返回，然后打开资源清单。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	datav-bptest	datav	包年包月	datav-cn-tl32f7kum004	运行中	2021-11-04 08:57:25	定位
2	VPC_BJ	vpc	-	vpc-2zerwwi1mo1wd6ovcn4vp	运行中	2021-11-04 08:57:25	定位
3	hologres-bptest	hologres	-	hgpostcn-cn-i7m2f7kup001	运行中	2021-11-04 08:57:57	定位
4	VSW_BJ	vswitch	-	vsw-2ze08v1qm39fzjiu2du80	运行中	2021-11-04 08:58:17	定位

**部署概要**

状态：部署成功

订单编号：211389255030425211388856280425

方案编号：VXUOL1T5AIUYYWA4

[查看报告](#) [返回](#)

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC_BJ [192.168.0.0/16]	vpc (专有网络VPC)	免费	vpc-2zepeqavvo5gsfox8btue	新建	运行中	2021-12-14 11:26:12	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>
2	hologres-bptest	hologres (交互式分析Holo)	免费	hgpostcn-cn-i7m2f7kup001	新建	运行中	2021-12-14 11:26:12	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>

这里可以查看资源列表和清单，单击左侧资源名称，直接跳转到对应资源的控制台，单击右侧**详情**，可以查看资源实例的详情。单击**操作**，可以对资源做一些常用的操作。

步骤 10 单击资源名称 **hologres-bptest**，可跳转到对应的控制台。

序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间	定位	操作
1	VPC_BJ [192.168.0.0/16]	vpc (专有网络VPC)	免费	vpc-2zepeqavvo5gsfox8btue	新建	运行中	2021-12-14 11:26:12	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>
2	<b>hologres-bptest</b>	hologres (交互式分析Holo)	免费	hgpostcn-cn-i7m2f7kup001	新建	运行中	2021-12-14 11:26:12	定位	<a href="#">详情</a>   <a href="#">监控</a>   <a href="#">变更日志</a>   <a href="#">操作</a>

网络类型	域名	使用场景	操作
公网	hgpostcn-cn-i7m2f7kup001-cn-beijing.hologres.aliyuncs.com:80	适用于无网络访问限制场景，ETL、BI工具和数据应用直接连接访问	<input checked="" type="checkbox"/>
经典	hgpostcn-cn-i7m2f7kup001-cn-beijing-internal.hologres.aliyuncs.com:80	经典网络内部访问，无公网流量开销	<input checked="" type="checkbox"/>
VPC	hgpostcn-cn-i7m2f7kup001-cn-be-ing-vpc.hologres.aliyuncs.com:80	VPC网络访问	<input checked="" type="checkbox"/>

此外，本实践创建的 dataV，可以将 hologres 中的结果呈现到 dataV 的可视化工具中。

#### 步骤 11 开发配置 hologres

- 可参考 <https://bp.aliyun.com/detail/176> 中第 2 章第 2.3.2 小节 的“创建数据库”对 hologres 数据库进行详细的配置。
- 可参考 <https://bp.aliyun.com/detail/176> 中第 6 章的“可视化工具 DataV 搭建”，学习如何将 hologres 集成到 dataV 中。

## 5.5.云速搭部署 WAF 和 SLB 透明接入应用

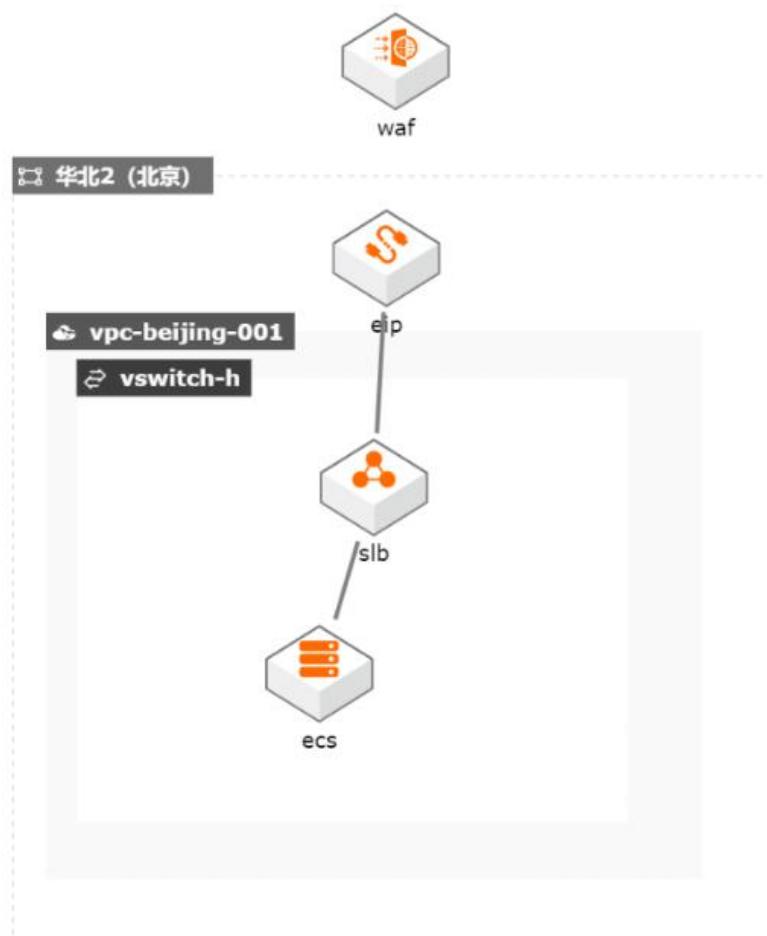
作者 | 阿里云解决方案架构师 敬海

### 5.5.1. 云速搭架构设计入门

#### 方案架构

通过云速搭设计并部署一个 WAF 和 SLB 透明接入的架构。

WAF 和 SLB 透明接入详情请见 [https://help.aliyun.com/document\\_detail/171452.html](https://help.aliyun.com/document_detail/171452.html)



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下图，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
EIP	Region 地域
SLB	Vswitch 交换机
ECS	vswitch 交换机
WAF	全局资源

## 资源规划

在进行应用架构设计时，可以提前进行资源规划。

本示例资源规划清单如下表所示。

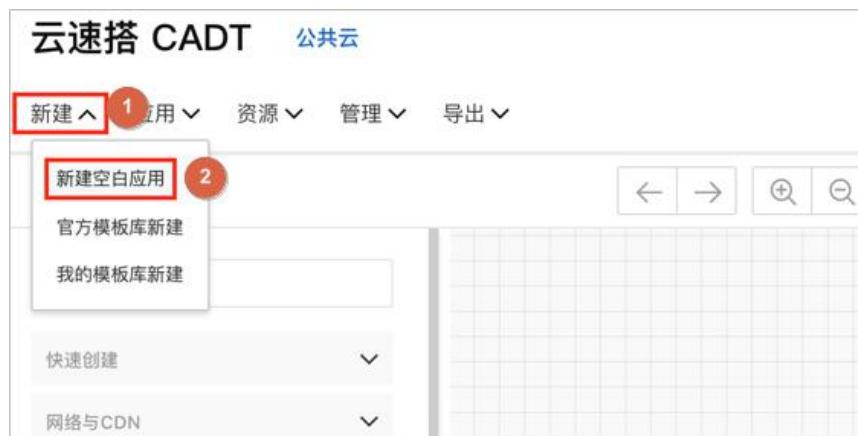
资源分类	资源名称	网段
Region	北京	-
VPC	VPC-BJ	192.168.0.0/16
AZ	北京 H 可用区	192.168.0.0/24

### 5.5.2. 设计 WAF 和 SLB 透明接入架构

步骤 1 登录云速搭 CADT 控制台。（<https://bpstudio.console.aliyun.com/>）

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 在菜单栏单击新建 > 新建空白应用。

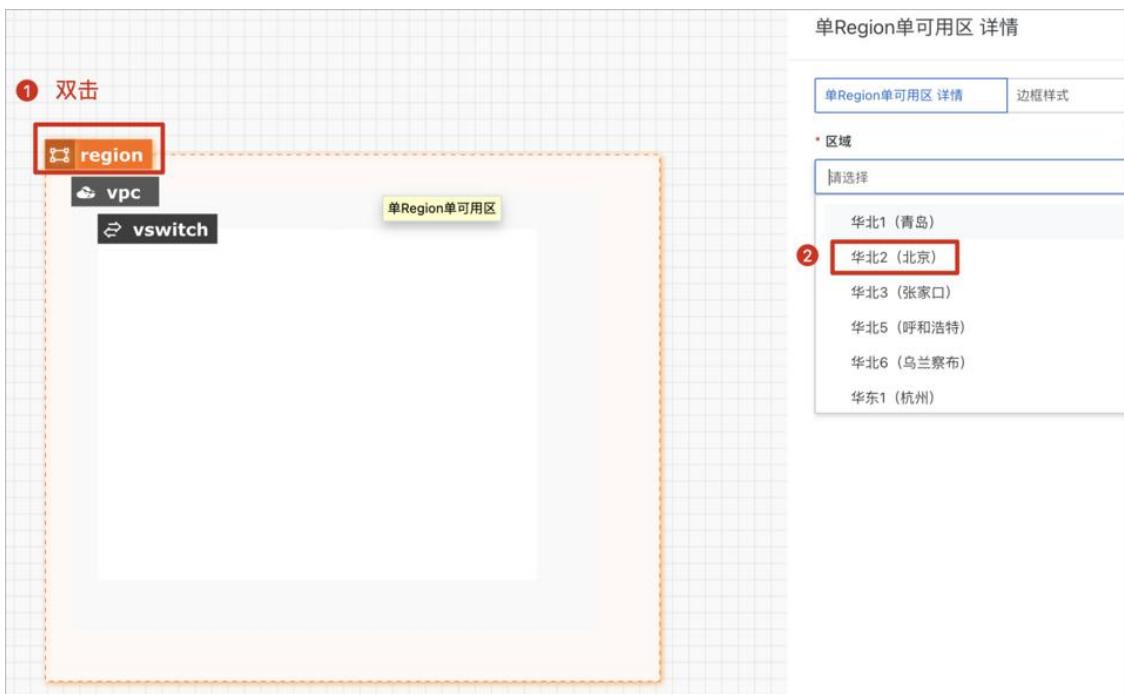


步骤3 从左侧工具栏**快速创建**下选择合适的网络拓扑类型，本场景适用**单 Region 单可用区**，单击选中并拖拽到右侧空白画布中。



步骤4 双击 Region、VPC、vswitch 进行配置。

1. 双击 region，在右侧弹出窗口中，选择华北2（北京）。



2. 双击 VPC，配置 VPC 参数。



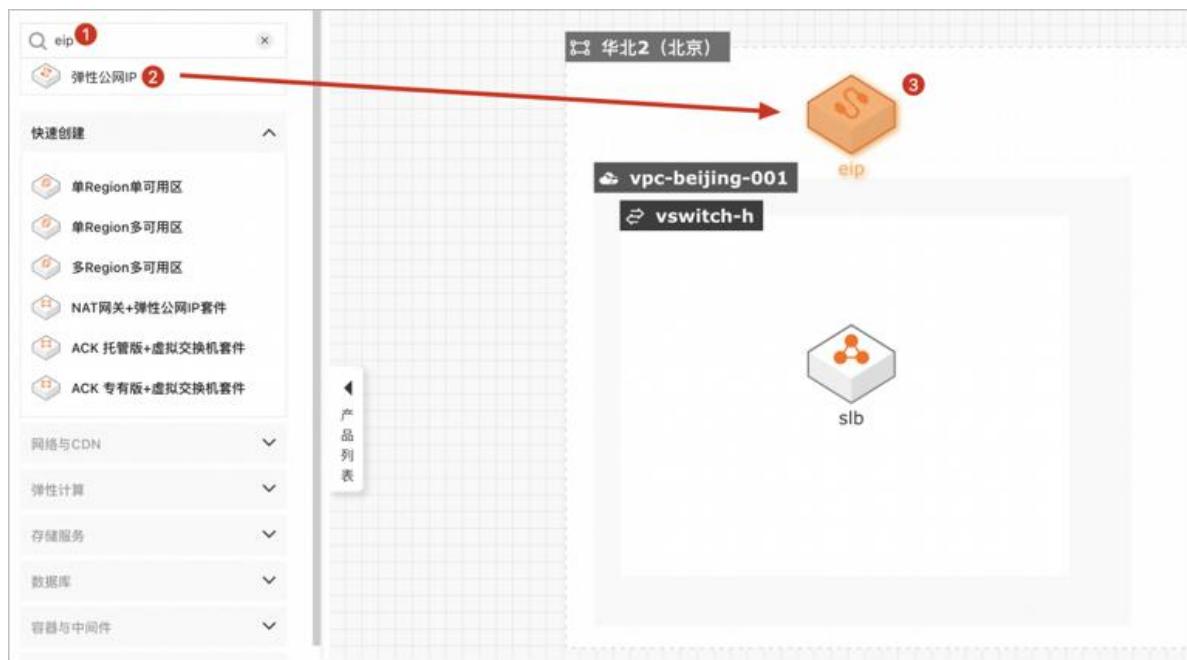
3. 双击 Vswitch，配置 vswitch 参数。



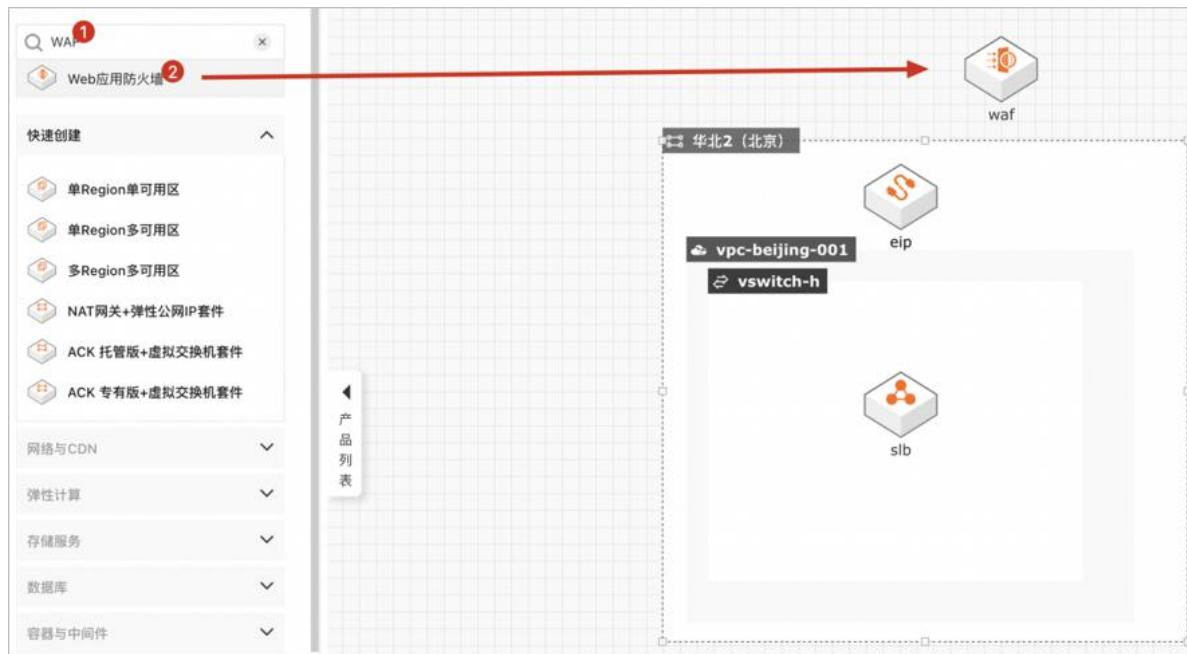
步骤 5 在左侧搜索框中输入 SLB，选定负载均衡 CLB（私网），拖动到 vswitch 中。



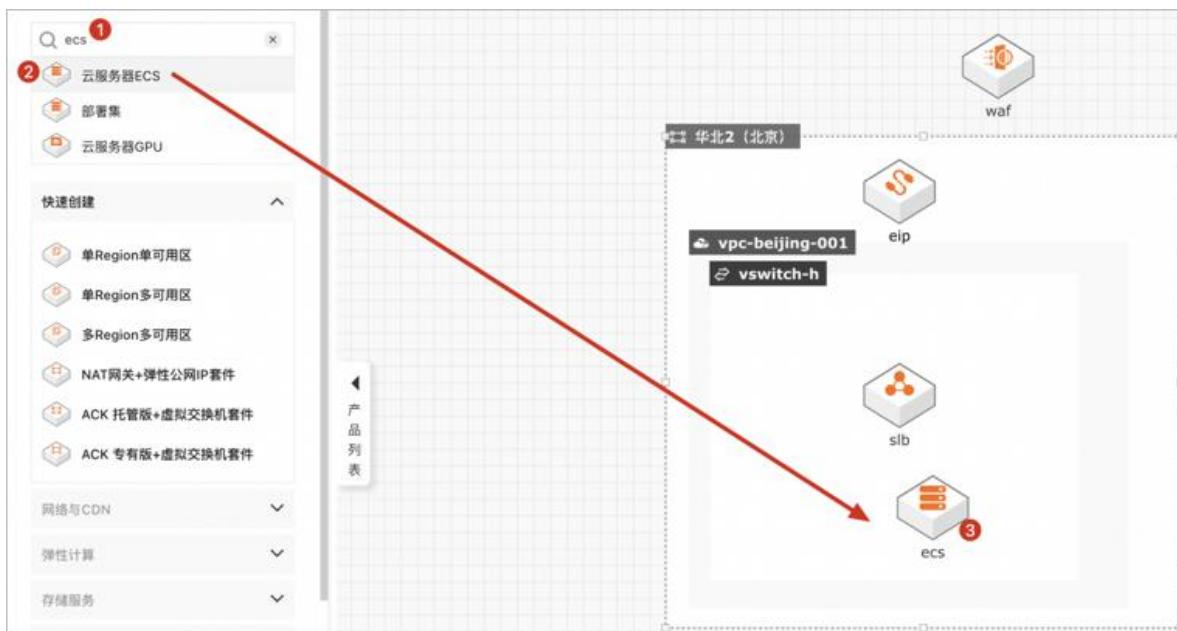
步骤 6 在左侧搜索框中输入 eip，选定弹性公网 IP，拖动到地域中。



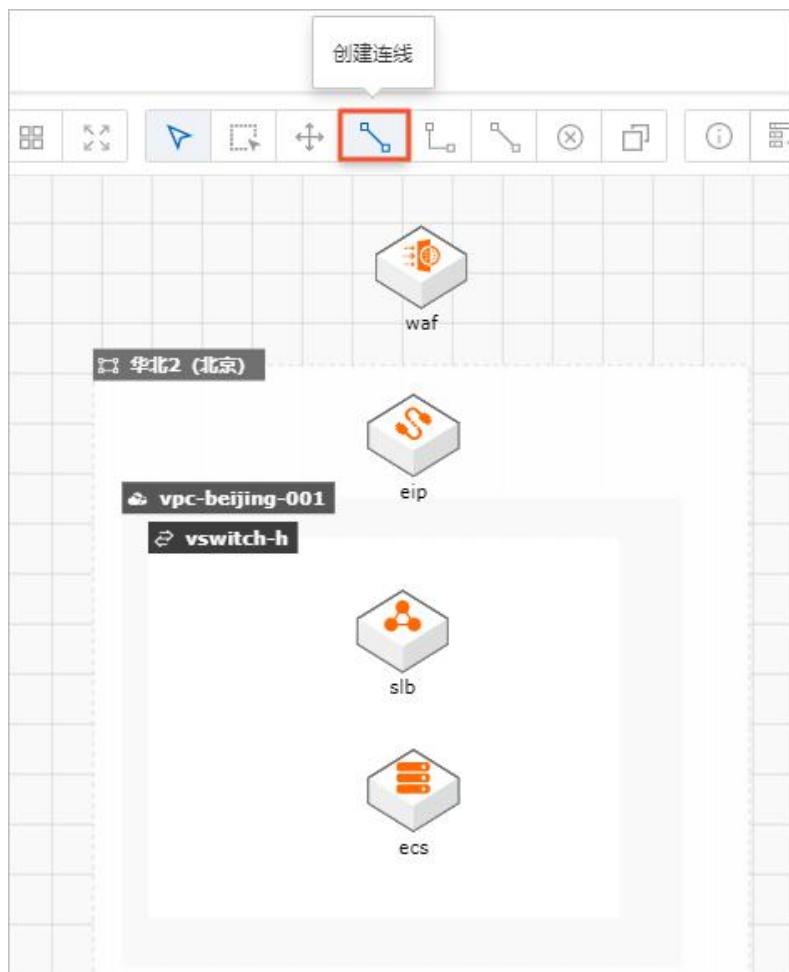
步骤 7 在左侧搜索框中输入 WAF，选定 Web 应用防火墙，拖动到地域之外。



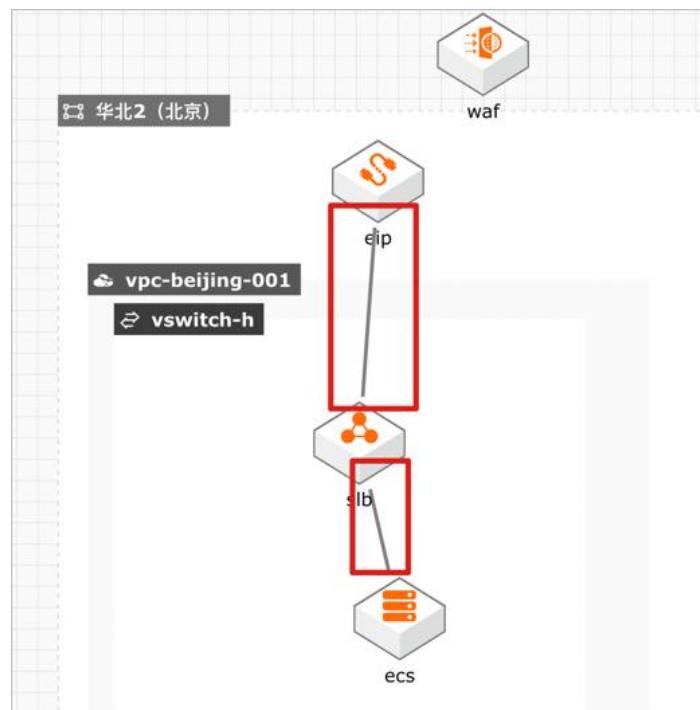
步骤 8 在左侧搜索框中输入 ECS，选定云服务器 ECS，拖动到 vswitch 中。



步骤 9 单击创建连线，切换到连线模式。



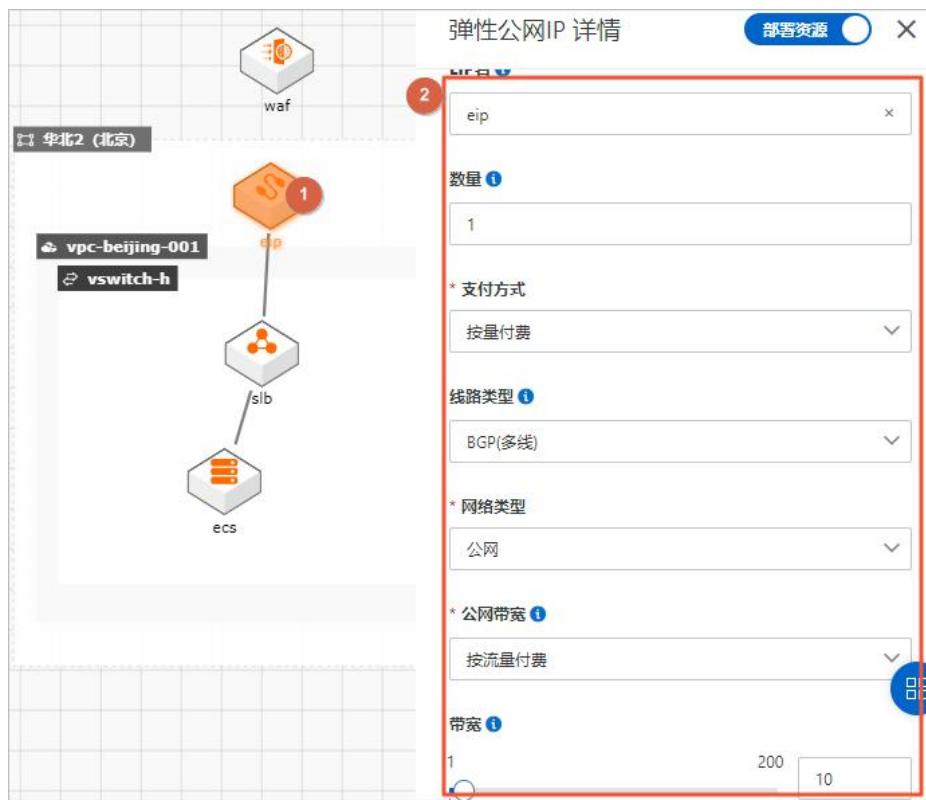
步骤 10 分别链接 eip 和 slb，slb 和 ecs。



步骤 11 双击配置 waf 参数，这里以按量付费模式的 waf 为例。



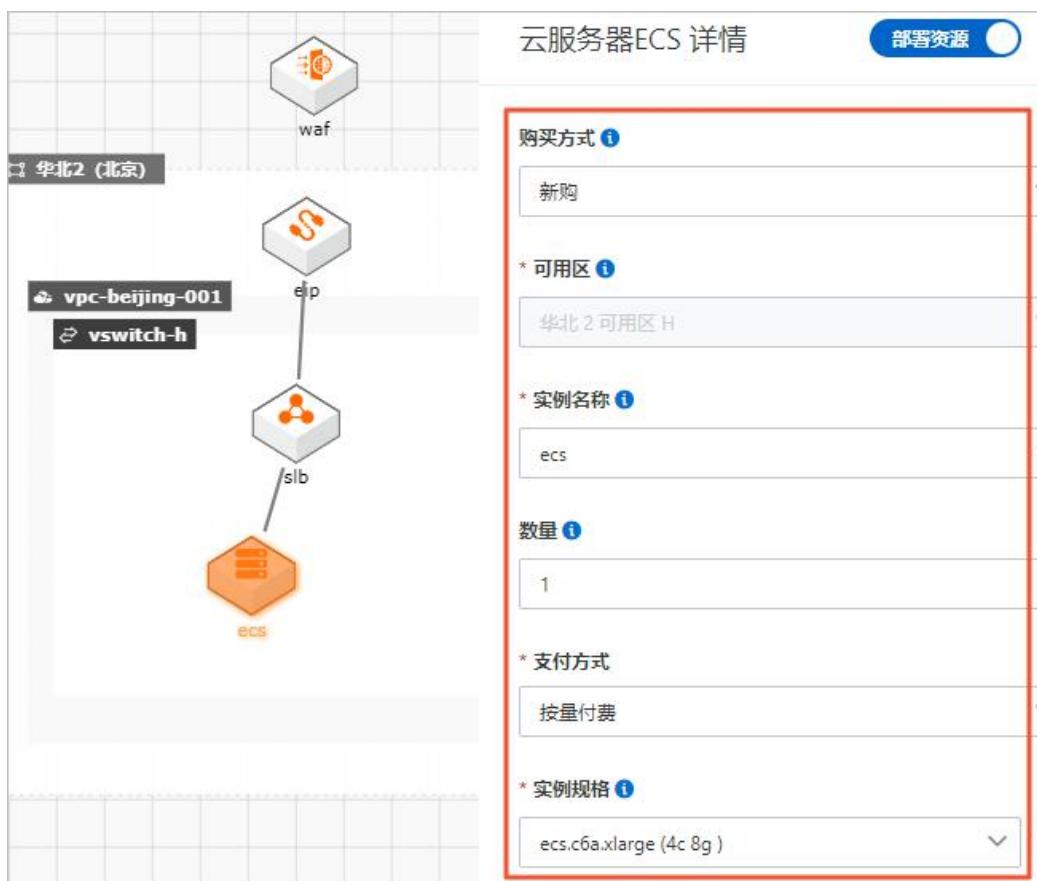
步骤 12 双击配置 eip 参数。



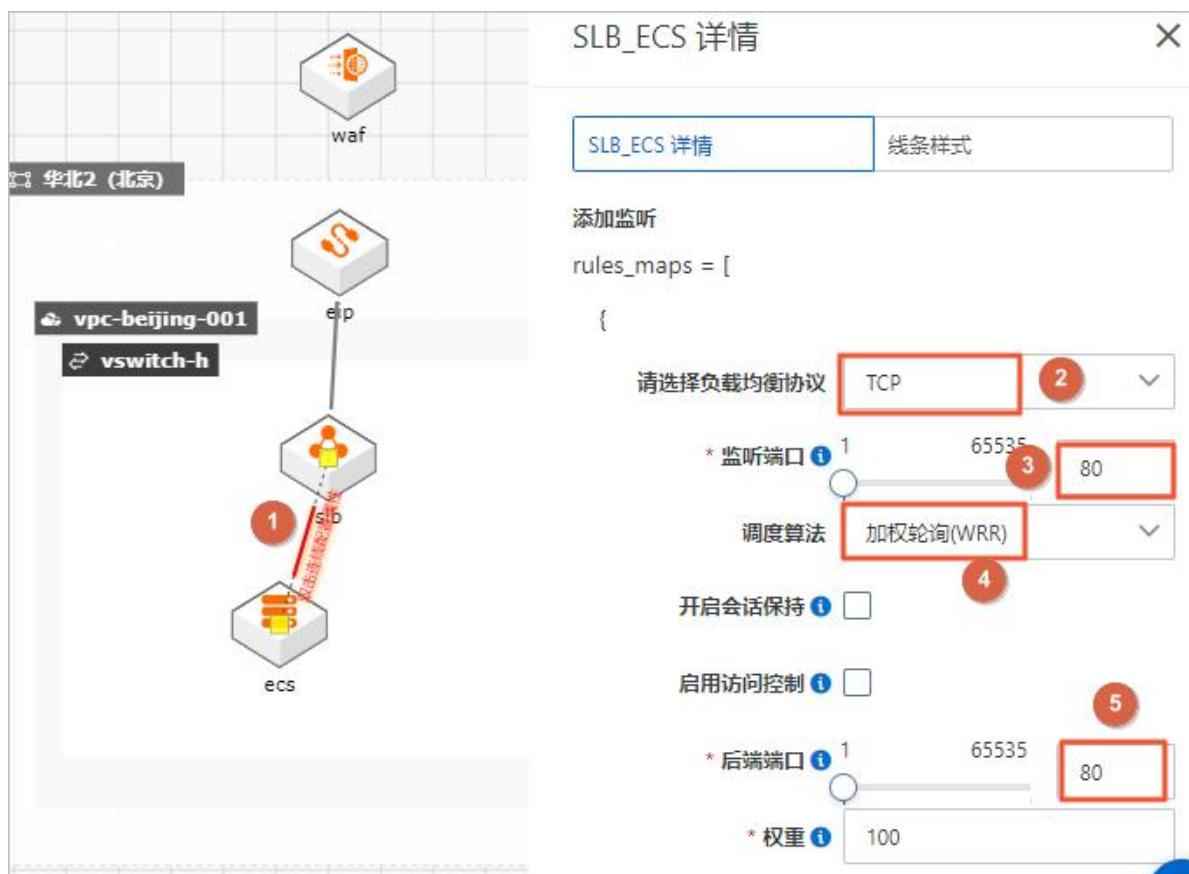
步骤 13 双击配置 slb 参数。

步骤 14 双击配置 ecs 参数。

配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs
支付方式	按量付费
实例规格	ecs.c6a.xlarge(4c 8g)
镜像	CentOS
镜像版本	CentOS 8.4 64 位
系统盘类型	ESSD 云盘
系统盘容量	40
性能级别	PL0
主机名	ecs
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>



步骤 15 双击连线，配置参数。

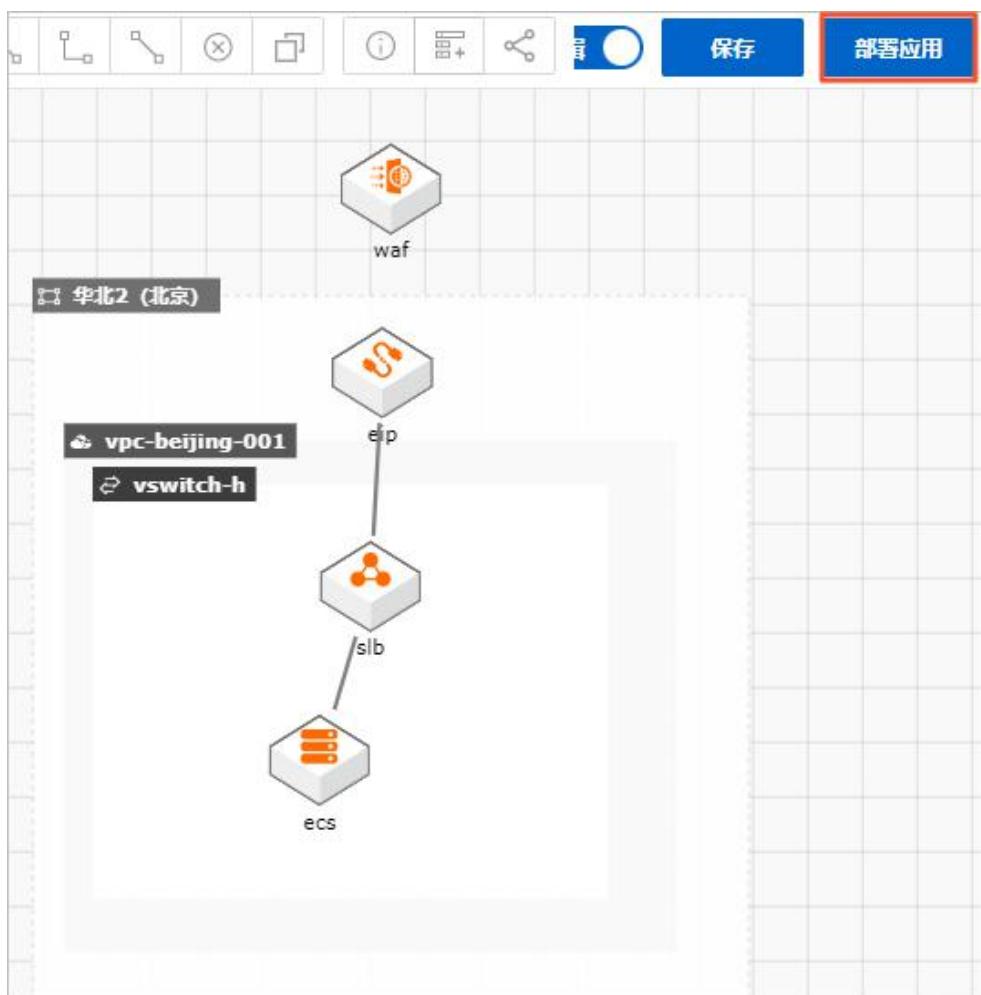


步骤 16 配置完成，单击右上角的保存，并设置应用名称。



### 5.5.3.部署应用

步骤 1 单击部署应用。



步骤 2 弹出如下校验页面，这里会校验参数配置是否合法，连线配置是否合法，ECS 是否有库存等，一般需要几十秒左右。

校验成功，单击**下一步：价格清单**。

**资源验证**

资源名称	资源类型	区域	规格	结果	备注	操作
ecs	ecs	北京	ecs.c6a.xlarge	成功	校验通过	定位
slb	clb	北京	slb.s2.small	成功	校验通过	定位
vpc-beijing-001	vpc	北京	192.168.0.0/16	成功	校验通过	定位
默认安全组	security.group	北京		成功	校验通过	定位
eip	eip	北京	public	成功	校验通过	定位
waf	waf			成功	您在该地域 (Region) 已购买过相关产品，本次不重复购买	定位

状态:校验成功

[下一步: 价格清单](#) [返回](#)

步骤 3 在导出价格清单对话框中，这里会显示价格信息，按量的会按小时扣除，包年包月的会一次性扣除（如有）。

**导出价格清单**

[免费](#) [按量付费](#)

**资源成本占比**

资源预算
计算 计算: [redacted] 元/时
网络 网络: [redacted] 元/时

**价格列表**

资源名称	资源类型	区域	规格	数量	原价	优惠	实付	操作
eip	eip	北京	public	1	0.02元/时	[redacted]	[redacted]	定位
slb	clb	北京	slb.s2.small	1	0.32元/时	[redacted]	[redacted]	定位
ecs	ecs	北京	ecs.c6a.xlarge	1	0.63元/时	[redacted]	[redacted]	定位

状态: 计价成功

[上一步: 资源校验](#) [查看报告](#) [下一步: 确认订单](#)

步骤 4 这里可以单击**查看报告**，查看应用的价格信息。



步骤 5 单击下一步：确认订单。

步骤 6 在新的窗口中，勾选《云速搭服务条款》，单击下一步：支付并创建就会进入部署流程，开始扣费并创建资源，**一旦点击后，无法取消**。

**确认订单**

免费  按量付费

资源名称	资源类型	区域	规格	数量	原价	实付	状态
ecs	ecs	北京	ecs.c6a.xlarge	1	0.63元/时	元/时	新购
slb	clb	北京	slb.s2.small	1	0.32元/时	元/时	新购
eip	eip	北京	public	1	0.02元/时	元/时	新购

《云速搭服务条款》  
部署前，请阅读并勾选服务条款

按量付费：元/时

状态：计价成功

上一步：价格清单 下一步：支付并创建

步骤 7 等待应用部署完成。



部署过程大致分为三个阶段：

- 第一个阶段按照依赖顺序创建应用内的资源，比如先创建全局资源，然后是地域级资源，然后是 vpc 级别的资源，然后是 vswitch 级别的资源。这里是先创建 vpc，再创建 vswitch，然后是 slb 和 ecs。
- 第二阶段是创建连线代表的配置关系，这里是配置 slb 和 ecs 的端口绑定关系等。
- 第三阶段是生成部署报告和资源清单，其中资源清单列表中还包括了监控，常用操作等。

步骤 8 部署完成后，如下图所示。

资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
eip	eip	按量付费	eip-2zetcn8llexkumbvi0owfm	运行中	2021-10-28 20:42:50	定位
vpc-beijing-001	vpc	-	vpc-2zeplmszi8wquw7994yi6	运行中	2021-10-28 20:42:50	定位
默认安全组	security.group	-	sg-2ze8tiyk741atelybgw7	运行中	2021-10-28 20:42:50	定位
vswitch-h	vswitch	-	vsw-2ze8zoo05et62r32mdfen	运行中	2021-10-28 20:42:50	定位
slb	clb	按量付费	lb-2zea24lqkrkyjuiwxkcve	运行中	2021-10-28 20:43:43	定位

**部署概要**

状态: 部署成功  
订单编号 : 211322083000159, 211321685700159  
方案编号: DD4CCQWHARESC79X

查看报告 返回

步骤 9 单击**查看报告**，可以查看本次的部署报告。



步骤 10 单击返回，然后单击应用下方的资源清单。



这里可以查看资源列表和清单，单击左侧资源名称，直接跳到对应资源的控制台；点击右侧详情，可以查看资源实例的详情；单击操作，可以对资源做一些常用的操作。单击监控，直接跳到对应资源的云监控页面。

## 5.5.4.透明接入

waf 和 slb 透明接入详情, 请参考:

[https://help.aliyun.com/document\\_detail/171452.html](https://help.aliyun.com/document_detail/171452.html)

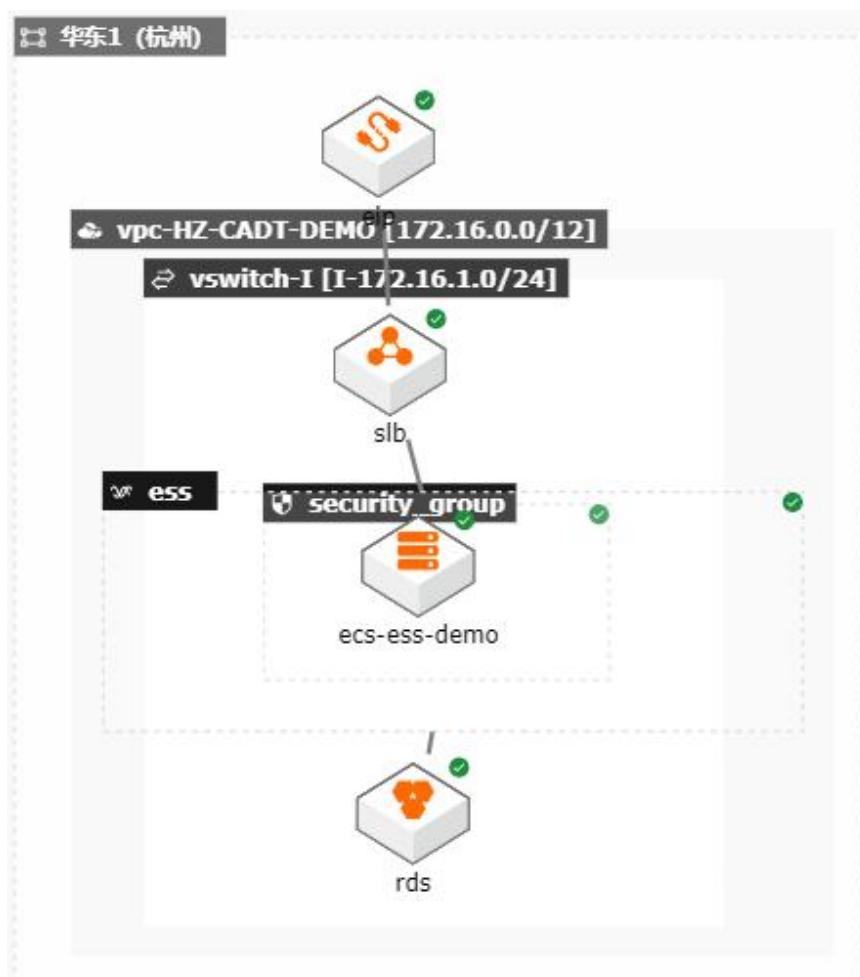
## 5.6.云速搭部署 ESS 实现弹性伸缩

作者 | 阿里云解决方案架构师 洁谦

### 5.6.1.通过云速搭创建 ESS

#### 方案架构

- 通过云速搭部署 SLB+ECS+RDS，创建一个 web 网站。
- 通过云速搭部署 ESS 弹性伸缩组，并将 ECS 加入到 ESS 伸缩组中。模拟弹性伸缩自动扩容 ECS，将扩容的 ECS 挂载到 SLB，并将扩容 ECS IP 加入到 RDS 白名单中。
- 具备一个安全组，通过安全组对 ECS 进行详细的安全策略配置。



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源及其级别如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
ESS	VPC
ECS	VSW
安全组	VPC
SLB	VSW
RDS	VSW

## 资源规划清单

资源类别	配置项	配置明细	说明
区域	区域	华东 1 (杭州)	本最佳实践全部资源部署在杭州（主数据中心）
专有网络 VPC	状态	新购（根据实际情况选择新购或已保有，本最佳实践新购 VPC）	云上选择专有网络（VPC）以保障安全性。 选择离原系统公网 IP 近的云上区域减少网络延迟。
	VPC 名	vpc-HZ-CADT-DEMO	选择资源丰富、离用户近的区域保障项目顺利实施。
	网段	172.10.0.0/16	网络规划留足可用 IP 数即可。
虚拟 交换机	状态	新购（根据实际情况选择新购或已保有，本最佳实践新购交换机）	
	vswitch 名	vswitch-l	
	可用区	华东 1 可用区 I	
	IPv4 网段	172.10.1.0/24	

资源类别	配置项	配置明细	说明
ECS	可用区	默认（华东1 可用区 I）	ECS 创建在 vswitch-1 下，无需选择。
	ECS 名	ecs-ess-demo	
	主机名	ecs-ess-demo	
	支付方式	后付费	按量付费
	实例规格	4 核 CPU, 16GB 内存 (ecs.g6.xlarge)	云上业务系统规格按照原规格购买。
	镜像	CentOS	
	镜像版本	使用自定义镜像	镜像已经安装配置了 nginx 服务
	系统盘	ESSD 云盘	ESSD 云盘
	硬盘容量	120GiB (本实践提供的镜像为 120GiB, 请根据实际情况选择)	
	公网带宽	按流量付费	
安全加固	出网带宽	10	分配公网 IP
	登陆密码	*****	初始 root 用户密码，创建成功后由业务方分别登录修改密码。
	安全加固	Active	

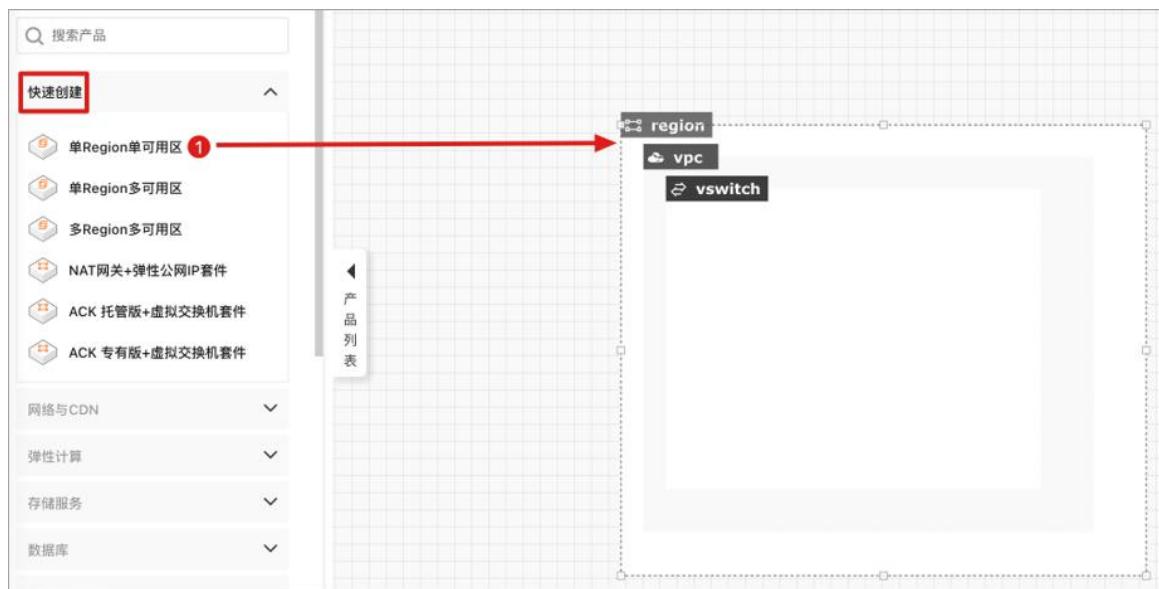
## 5.6.2.通过云速搭 CADT 部署资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录 CADT 控制台，如果提示需要开通服务，请根据提示进行开通。

步骤 2 单击新建 > 新建空白应用



步骤3 拖入单Region单可用区到画布区域。



步骤4 分别双击 region、vpc、vswitch 进行设置

配置 region：



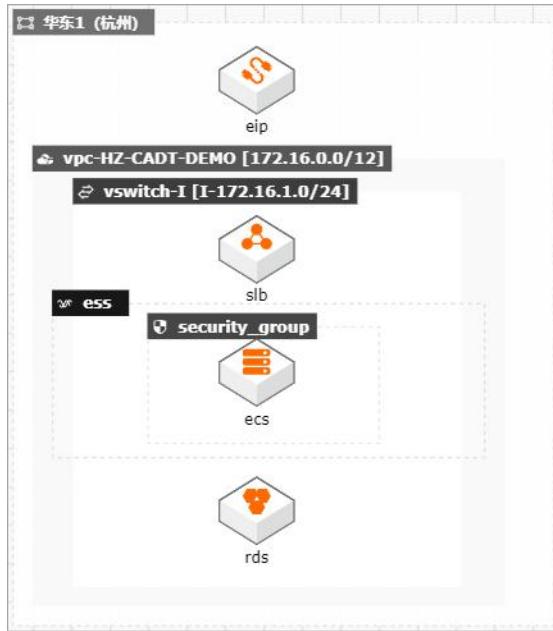
配置 vpc：



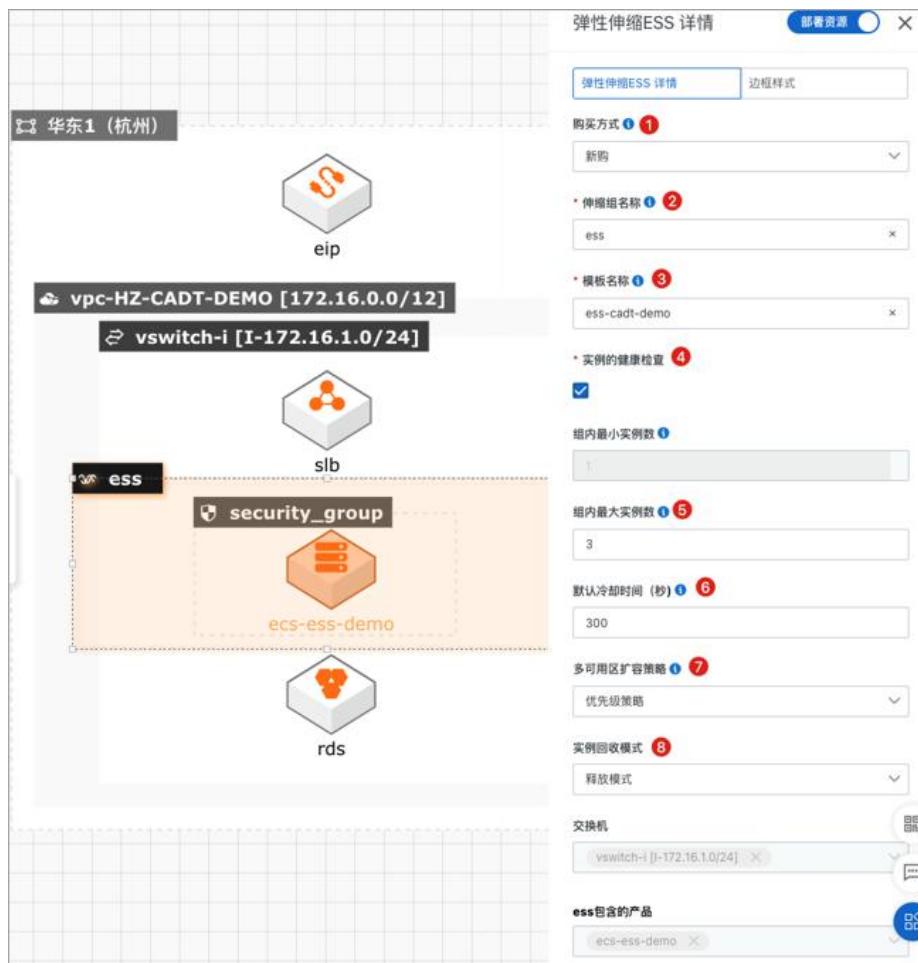
配置 vswitch:



步骤 5 在画布区域调整 region、vpc、vswitch 图层到合适大小后，分别从左侧产品列表中选择安全组、ECS、ESS、SLB 和 RDS 拖入对应区域中（参考 1.1，根据架构资源级别）



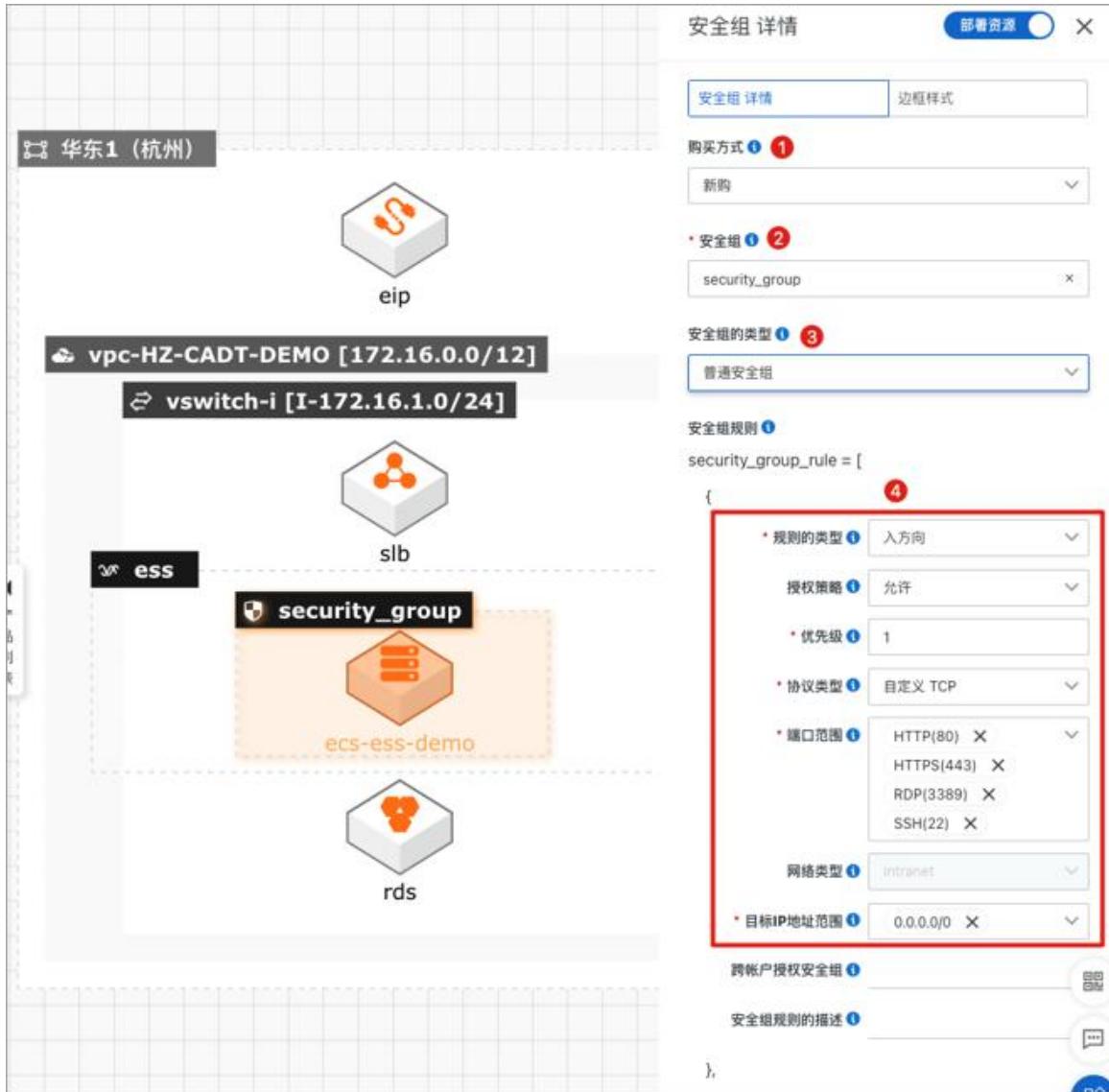
### 步骤 6 双击 ESS 配置弹性伸缩组



步骤 7 双击 ECS 配置实例信息，ECS 实例信息如下：

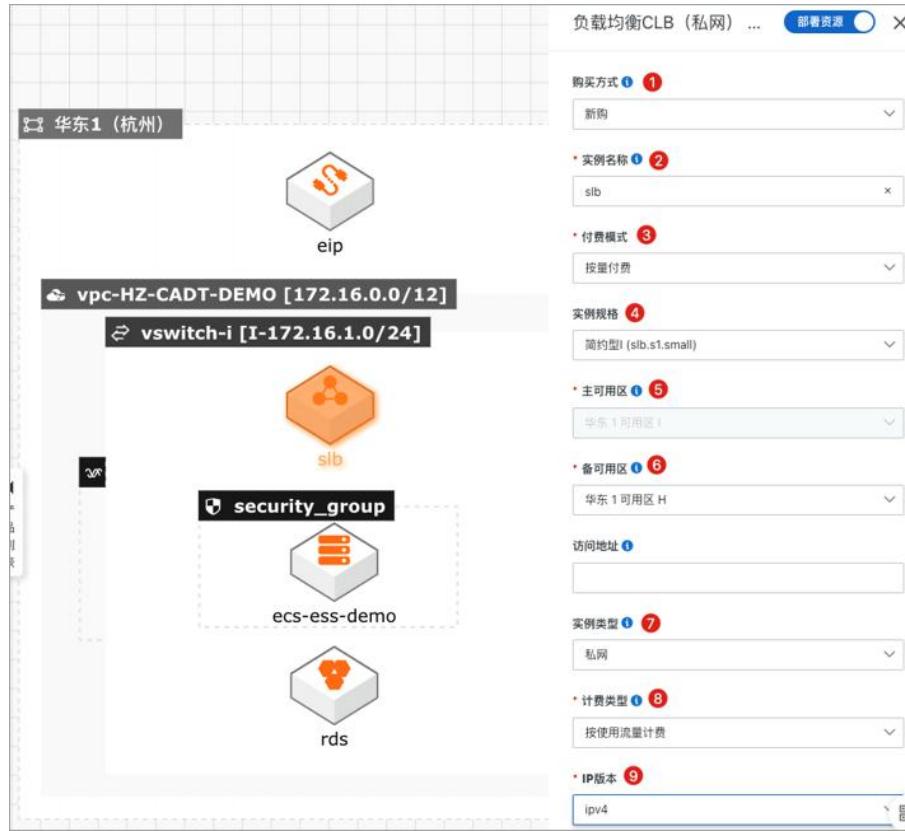
配置项	配置明细
购买方式	新购
可用区	<根据所在 vswitch>
实例名称	ecs-ess-demo
数量	1
支付方式	按量付费
实例规格	ecs.g6.xlarge(4c 16g)
镜像	共享镜像 (获取镜像请联系作者)
系统盘类型	ESSD 云盘
系统盘容量	120
性能级别	PL0
公网 IP	分配公网 IPv4 地址
宽带计费模式	按流量付费
带宽 (峰) 值	10 Mbps
主机名	ecs-ess-demo
登录凭证	自定义密码
登录密码/确认登录密码	<输入自定义密码>

步骤 8 双击安全组，配置安全组策略，放行 22、80、443 端口

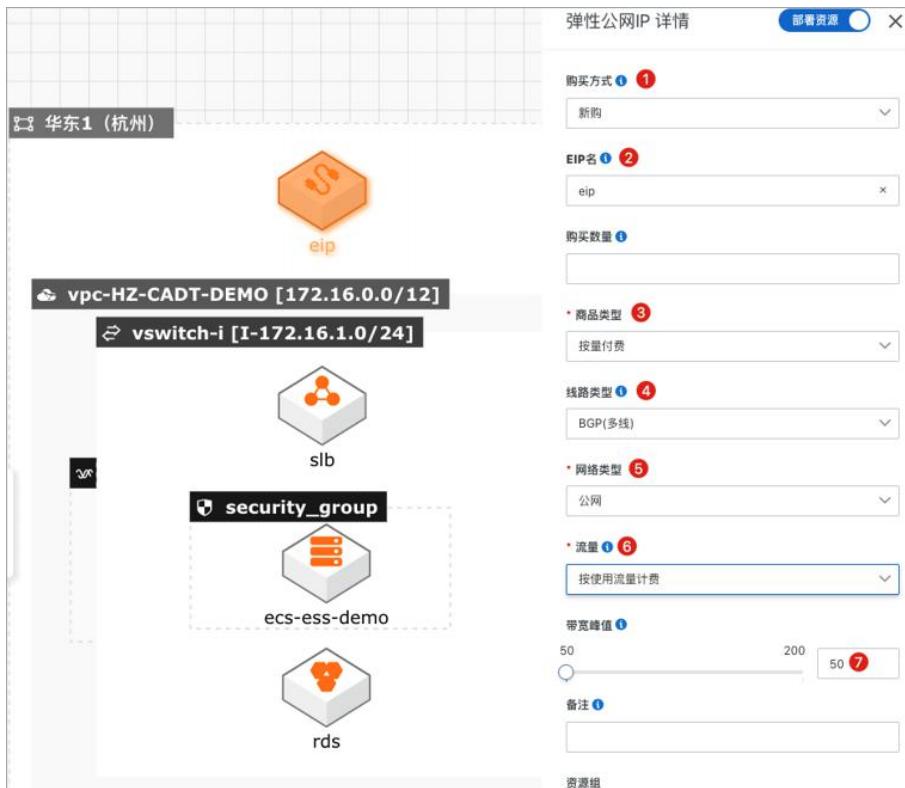


步骤 9 分别双击 SLB、EIP、RDS 完成实例配置。

SLB 配置如下：



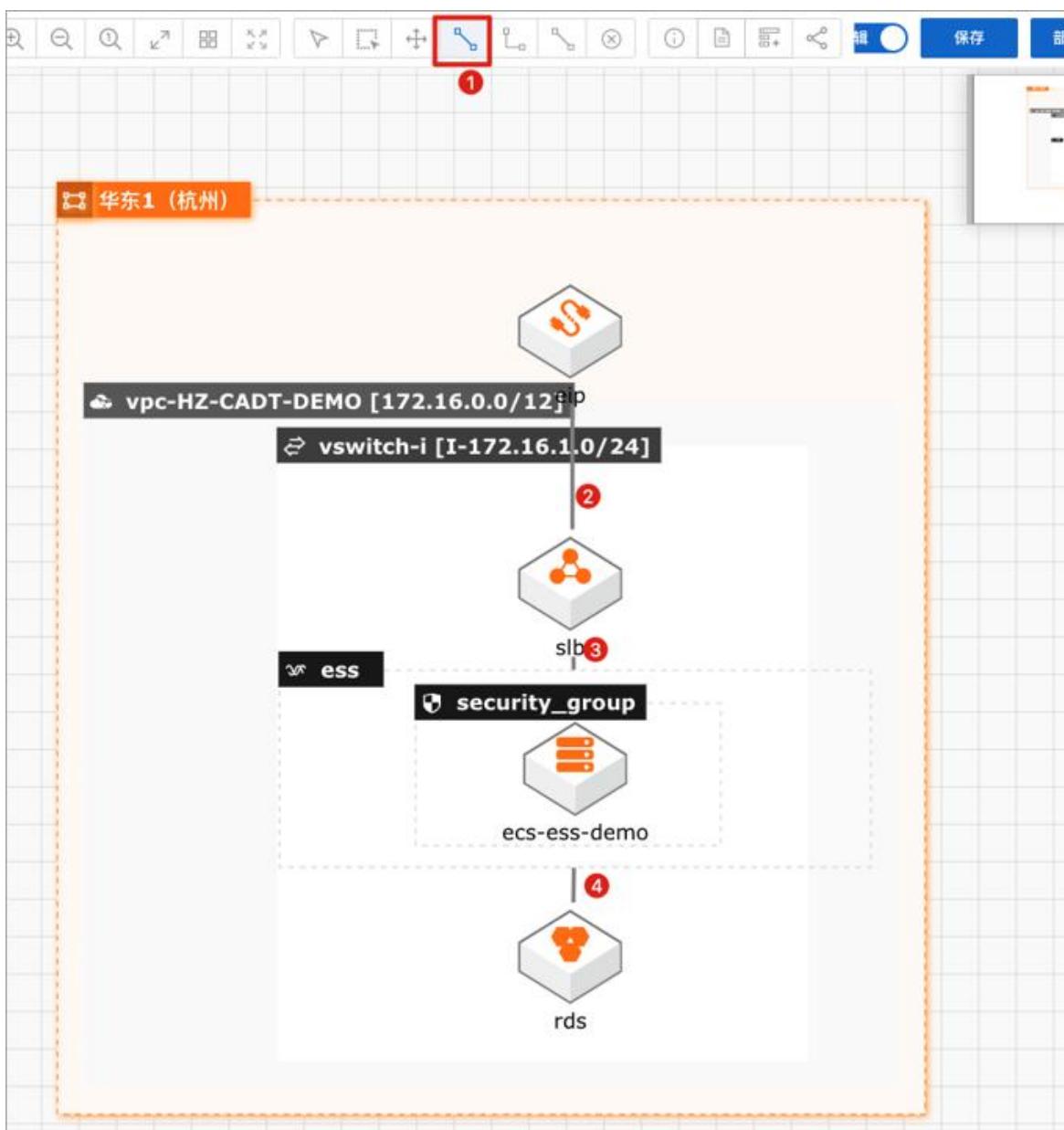
EIP 配置如下：



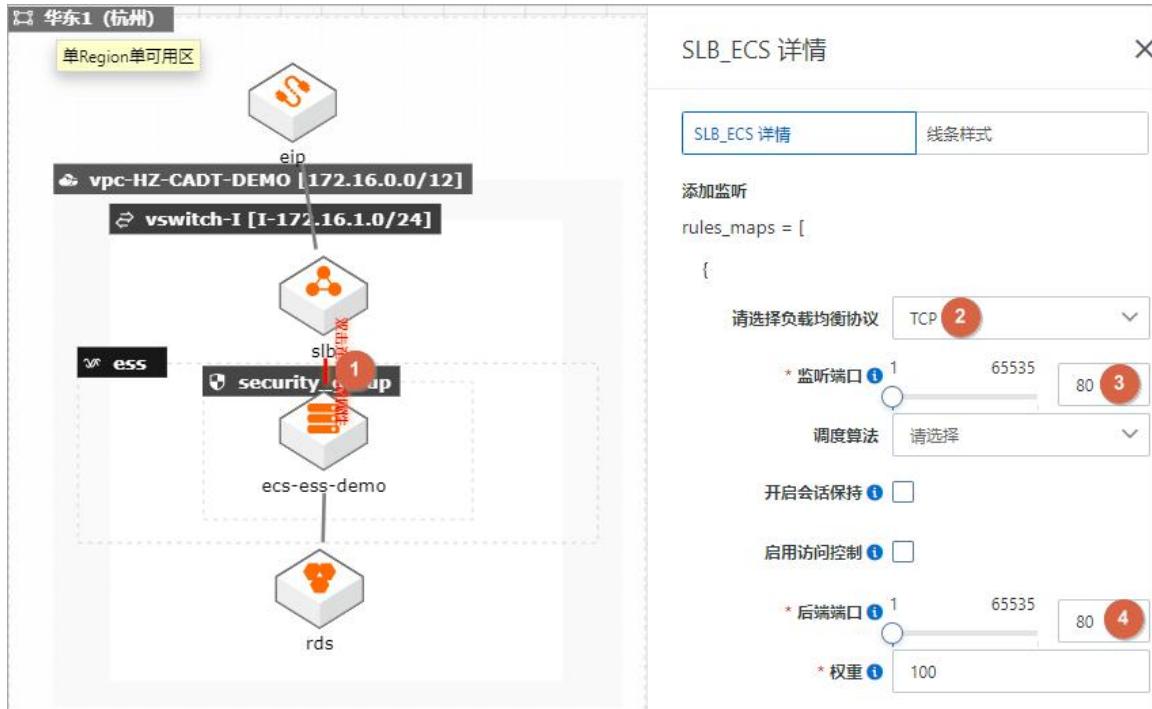
RDS 配置如下：



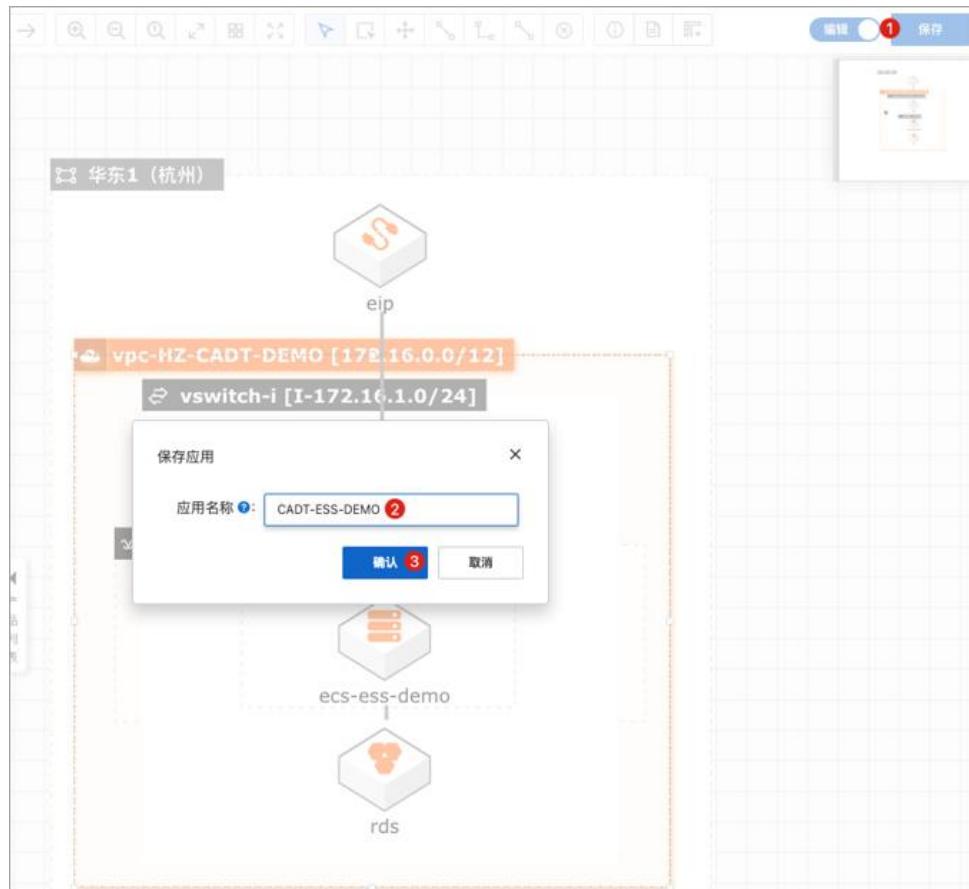
步骤 10 创建连线，将 eip 与 slb，slb 与 ess，rds 与 ess 相连。



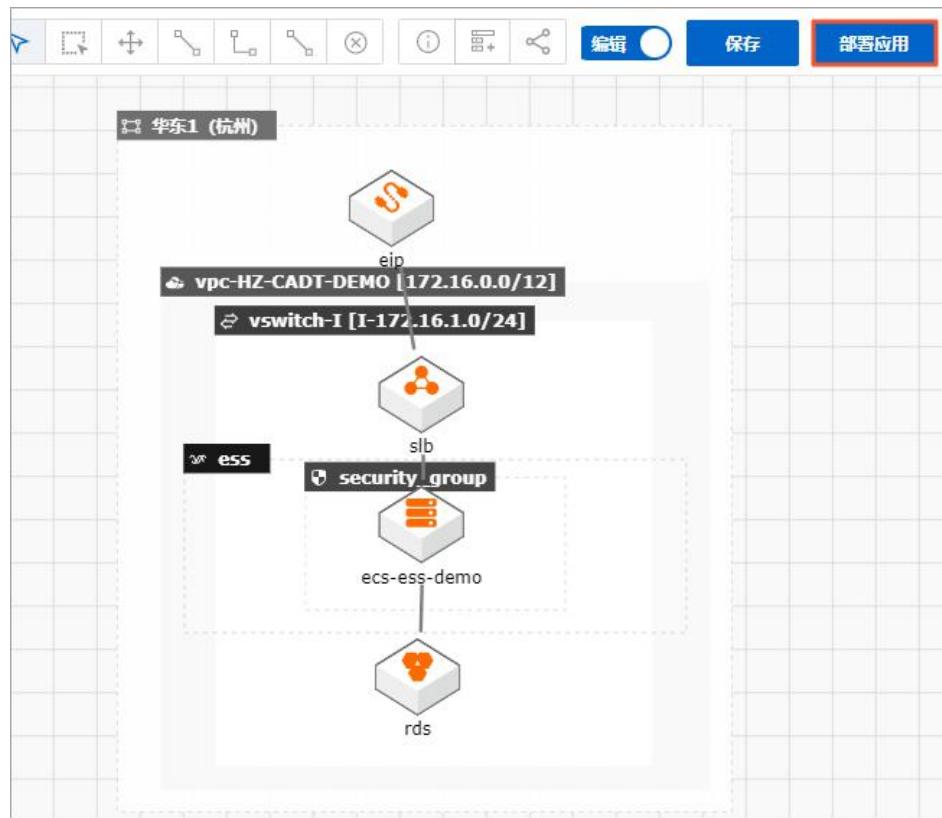
步骤 11 双击 slb 到 ess 连线，配置监听。



步骤 12 配置完成后，单击**保存**，输入应用名称。



步骤 13 单击应用部署。



步骤 14 等待校验成功，单击下一步：价格清单。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vswitch-1 [I-172.16.1.0/24]	vswitch	杭州	172.16.1.0/24	成功	校验通过	定位
2	rds	rds	杭州	MySQL	成功	校验通过	定位
3	ecs-ess-demo	ecs	杭州	ecs.g6.xlarge	成功	校验通过	定位
4	vpc-HZ-CADT-DEMO [172.16.0.0/12]	vpc	杭州	172.16.0.0/12	成功	校验通过	定位
5	默认安全组	security.group	杭州		成功	校验通过	定位
6	eip	eip	杭州	public	成功	校验通过	定位
7	security_group	security.group	杭州	normal	成功	校验通过	定位

状态:校验成功

下一步: 价格清单    返回

步骤 15 查看架构资源成本及占比，单击**下一步：确认订单**。



步骤 16 单击**下一步：支付并创建**。

**确认订单**

**按量付费**

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	rds	rds	杭州	rds.mysql.s2.xlarge	1	0.00 元/时	0.00 元/时	新购
2	ess	ess	杭州		1			新购
3	ecs-ess-demo	ecs	杭州	ecs.g6.xlarge	1	0.00 元/时	0.00 元/时	新购
4	slb	clb	杭州	slb.s1.small	1	0.00 元/时	0.00 元/时	新购
5	eip	eip	杭州	public	1	0.00 元/时	0.00 元/时	新购

**《云速塔服务条款》**

部署前，请阅读并勾选服务条款

按量付费: 0.00 元/时

状态: **计价成功**

**上一步: 价格清单** **下一步: 支付并创建**

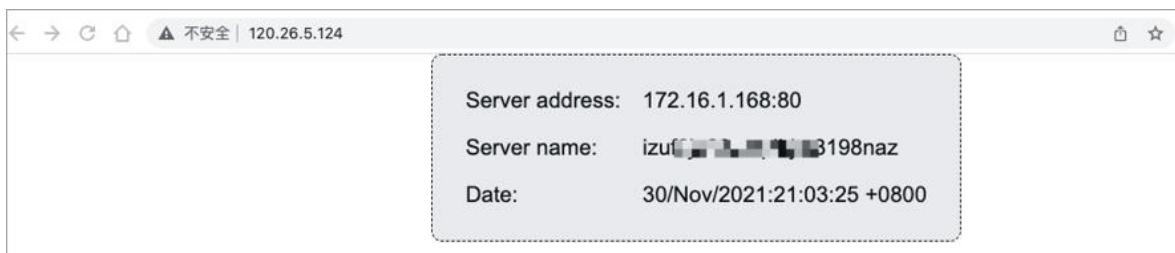
步骤 17 部署完成，单击[查看报告](#)，可以导出应用架构方案部署报告。

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	eip	eip (弹性公网IP)	按量付费	eip- <span style="background-color: #f0f0f0;">XXXXXXXXXX</span>	运行中	2021-11-30 20:57:09	定位
2	vpc-HZ-CADT-D EMO [172.16.0/ 12]	vpc (专有网络VPC)	-	vpc-l- <span style="background-color: #f0f0f0;">XXXXXXXXXX</span>	运行中	2021-11-30 20:57:09	定位
3	ess	ess (弹性伸缩ESS)	-	asg- <span style="background-color: #f0f0f0;">XXXXXXXXXX</span>	运行中	2021-11-30 20:57:26	定位
4	默认安全组	security.group (安全组)	-	sg- <span style="background-color: #f0f0f0;">XXXXXXXXXX</span>	运行中	2021-11-30 20:57:09	定位
	clb						



### 5.6.3.验证 ESS 弹性伸缩能力

步骤 1 浏览器输入 <http://<EIP>>，验证可以打开网页。

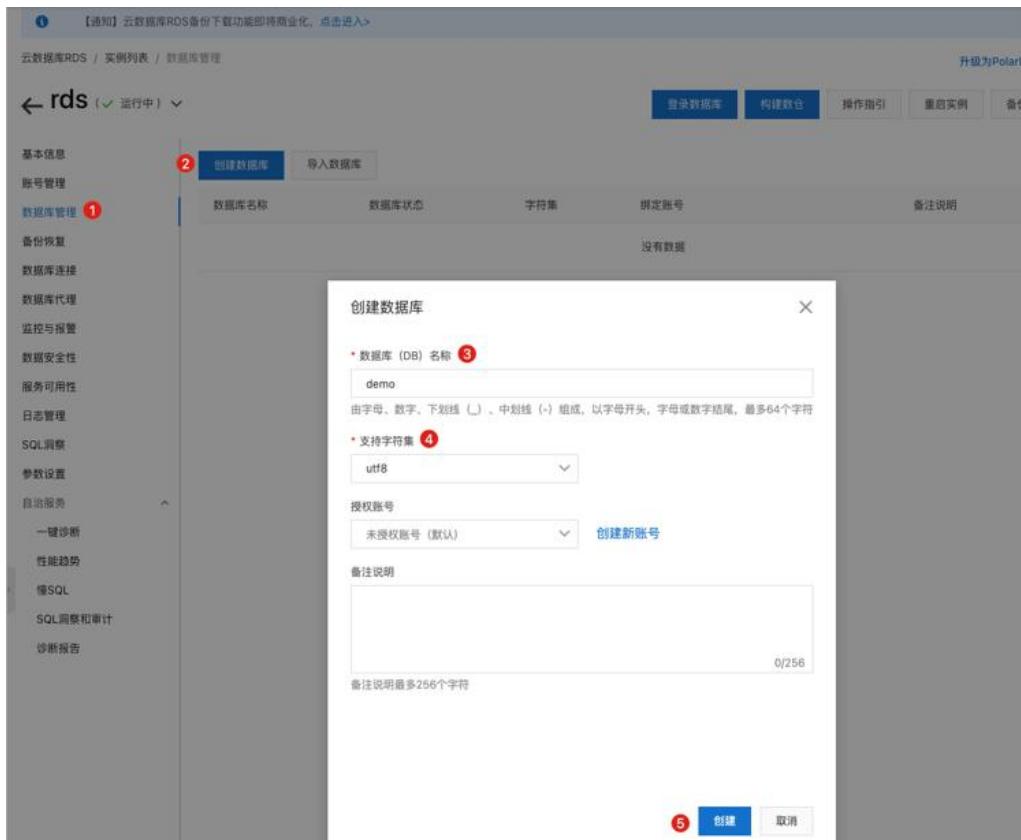


步骤 2 创建数据库：

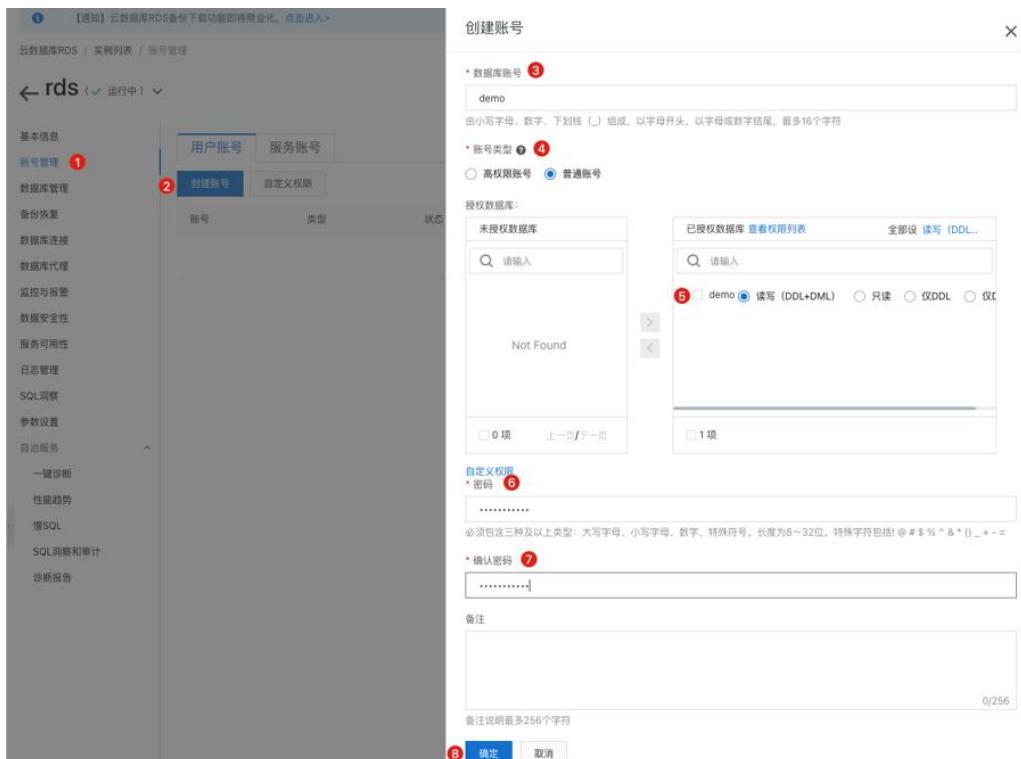
- 在 CADT 单击 RDS 实例名称，前往控制台。

资源部署状态							
序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
6	vpc-HZ-CADT-DEMO [172.16.0.0/12]	vpc (专有网络VPC)	-	vpc-bp12y0uar0cbwwoqy2wed	运行中	2021-12-01 11:59:28	定位
7	vswitch-l [172.16.0.0/24]	vswitch (虚拟交换机)	-	vsw-bp10skjdoj3oof6u314ed	运行中	2021-12-01 11:59:44	定位
8	rds	rds (云数据库RDS)	按量付费	rm-bp1a1sz08034vx160	运行中	2021-12-01 12:01:44	定位
9	security_group	security.group (安全组)	-	sg-bp1fl8ef9wkdf1ft1wnl	运行中	2021-12-01 11:59:29	定位

- 单击数据库管理 > 创建数据库



### 步骤 3 创建账号，单击账号管理 > 创建账号。



步骤 4 修改伸缩组关联 RDS 配置。

进入指定伸缩组，在**基本信息 > 关联 RDS**，单击修改按钮。

The screenshot shows the 'Basic Information' tab of the scaling group configuration page. The 'Associate with RDS' section is highlighted with a red box and a red circle containing the number '1', indicating it's the target for modification. The section displays the current status as 'Not Associated' and provides a 'Modify' button to change the association.

步骤 5 勾选挂载或卸载 RDS 实例时，伸缩组现有的实例添加或移出所选 RDS 实例的白名单(只针对本次挂载或卸载的 RDS 实例)



## 步骤 6 登录 ECS，验证 ECS 可访问 RDS 实例

### 1. 安装 mysql 客户端: `yum install -y mysql`

```
[root@ecs-ess-demo ~]# yum install -y mysql
Loaded plugins: fastestmirror, langpacks, releasever=adapter, update-motd
Loading mirror speeds from cached hostfile
base
epel
extras
plus
updates
Resolving Dependencies
--> Running transaction check
--> Package mariadb.x86_64 1:5.5.68-1.1.al7 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
=====
Package           Arch      Version       Repository      Size
=====
Installing:
mariadb          x86_64   1:5.5.68-1.1.al7   updates        8.9 M
=====
Transaction Summary
Install 1 Package
=====
Total download size: 8.9 M
Installed size: 49 M
Downloading packages:
mariadb-5.5.68-1.1.al7.x86_64.rpm                                         | 8.9 MB  00:00:00
=====
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mariadb-5.5.68-1.1.al7.x86_64                               1/1
    Verifying : 1:mariadb-5.5.68-1.1.al7.x86_64                               1/1
  Installed:
    mariadb.x86_64 1:5.5.68-1.1.al7
  Complete!
[root@ecs-ess-demo ~]#
```

### 2. 连接数据库：

```
[root@ecs-ess-demo ~]# mysql -hrm-b[REDACTED].mysql.rds.aliyuncs.com -P3306 -udemo -pJ[REDACTED] 175
Welcome to the MariaDB monitor  Commands end with ; or \g.
Your MySQL connection id is 1512
Server version: 5.6.16-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| demo |
| mysql |
+-----+
3 rows in set (0.00 sec)

MySQL [(none)]>
```

步骤 7 控制台选择伸缩组管理，单击进入新创建的伸缩组。

The screenshot shows the 'Scaling Group Management' page. On the left sidebar, 'Scaling Group Management' is selected. In the main area, a table lists scaling groups. One row is highlighted with a red box, showing the scaling group ID 'asg-bp126afvicsts634pqja', type 'ECS', status 'Enabled', and configuration details: '启动模板: 始终使用默认版本 lt-bp1eliffkjo5boy684qnc' and '弹性强度差'. The table also includes columns for '实例数/容量' (Instance Count/Capacity), '总实例数: 1', '最小实例数: 1', '最大实例数: 3', and '期望实例数: -'.

可以看到当前伸缩组中的 ECS 实例个数为 1：

This screenshot shows the detailed view of the scaling group 'asg-bp126afvicsts634pqja'. The '基本信息' tab is selected. Key details include: '状态: 启用', '伸缩配置来源: 启动模板: 始终使用默认版本 lt-bp1eliffkjo5boy684qnc (弹性强度差)', '伸缩组名称: asg-bp126afvicsts634pqja', '伸缩组ID: asg-bp126afvicsts634pqja', '伸缩组类型: ECS', '地域: 杭州', '标签: 未设置标签', and '创建时间: 2021年11月30日 20:57'. The '实例伸缩概览' section shows current instance counts: '加入中: 0', '加入挂起中: 0', '总量: 1', '服务中: 1', '备用中: 0', '保护中: 0', '停用中: 0', '移出中: 0', and '移出挂起中: 0'. A red box highlights the '总量: 1' entry. Below this, a box shows the most recent scaling activity: '最近伸缩活动: Add "1" ECS Instance', '伸缩活动ID: asa-bp1...', '状态: 成功', '开始时间: 2021年11月30日 21:00', and '停止时间: 2021年11月30日 21:00'.

步骤 8 选择伸缩规则与伸缩活动 Tab 页，再选择定时/报警任务，单击创建定时任务。

This screenshot shows the 'Scaling Group Management' page with the scaling group 'asg-bp126afvicsts634pqja' selected. The '伸缩规则与伸缩活动' tab is active. Under this tab, the '定时任务' sub-tab is selected. A red box highlights the '定时任务' tab. Below it, there is a button labeled '③ 创建定时任务' and a search bar for '定时任务ID' and '请输入定时任务ID'. The table below lists scheduled tasks with columns: '定时任务名称/ID', '描述', '状态', and '执行的操作'.

## 步骤 9 配置定时任务

### 创建定时任务

\* 任务名称  ①  
名称为2-64个字符，以大小写字母、数字或中文开头，可包含(.)、下划线(\_)或中划线(-)

描述  ②  
描述为2~200个字符

\* 执行时间  ③  
④

\* 伸缩组

\* 伸缩方式  伸缩组内实例数量设置 ⑤ ⑥

最大实例数 (台)  ⑦ ⑧  
当前值为 3

最小实例数 (台)  ⑨  
当前值为 1

重试过期时间 (秒)  ⑩  
⑪ ⑫

重复周期  不设置 ⑬ ⑭ ⑮ ⑯ ⑰

确认 取消

步骤 10 到了定时任务时间后，在实例列表可以看到自动创建 2 台 ECS 加入中。

弹性伸缩 / 伸缩组管理 / asg-bp126afvicsts634pqja

新手引导 产品动态 帮助文档

← asg-bp126afvicsts634pqja

停用 克隆 删除 用户分析 C

基本信息	实例配置来源	实例列表	伸缩组监控	伸缩规则与伸缩活动	生命周期挂钩	消息通知	滚动升级
------	--------	------	-------	-----------	--------	------	------

加入中	2
加入挂起中	0

总数量 3 服务中 1 备用中 0 保护中 0 停用中 0

移出中	0
移出挂起中	0

自动创建 手动创建滚动升级 修改组内实例来源

再均衡分布云服务器ID请输入内容搜索

<input type="checkbox"/>	云服务器ID/名称	配置来源	状态 (全部)	可用区	预热状态	操作
<input type="checkbox"/>	i-bp...yycx	启动模板: 始终使用默认版本 lt-bp...yycx	<input type="radio"/> 加入中	-	不需要预热	<a href="#">删除实例</a>   <a href="#">移出伸缩组</a>
<input type="checkbox"/>	i-bp...yycx	启动模板: 始终使用默认版本 lt-bp...yycx	<input type="radio"/> 加入中	-	不需要预热	<a href="#">删除实例</a>   <a href="#">移出伸缩组</a>

步骤 11 加入完成后，可以看到实例数量已经自动扩展到 3 台。

总数量	服务中	备用中
3	3	0
保护中	停用中	
0	0	

步骤 12 验证 SLB 自动挂载和 RDS 自动添加白名单。

浏览器访问 <http://<EIP>>，并反复刷新页面，可以看到流量已经负载分担到 3 台 ECS。

Server address: 172.16.1.169:80  
 Server name: izuf6je68veqdbjm3198naz  
 Date: 30/Nov/2021:22:03:14 +0800

Server address: 172.16.1.170:80  
 Server name: izuf6je68veqdbjm3198naz  
 Date: 30/Nov/2021:22:04:15 +0800

步骤 13 登录任一新扩容的 ECS，访问数据库正常，RDS 白名单已自动添加。

```
[root@ecs-ess-demo ~]# mysql -hrm-bp1.1902.mysql.rds.aliyuncs.com -P3306 -udemo -p123456 -c 175
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 2129
Server version: 5.6.16-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| demo          |
| mysql         |
+-----+
3 rows in set (0.00 sec)

MySQL [(none)]> 
```

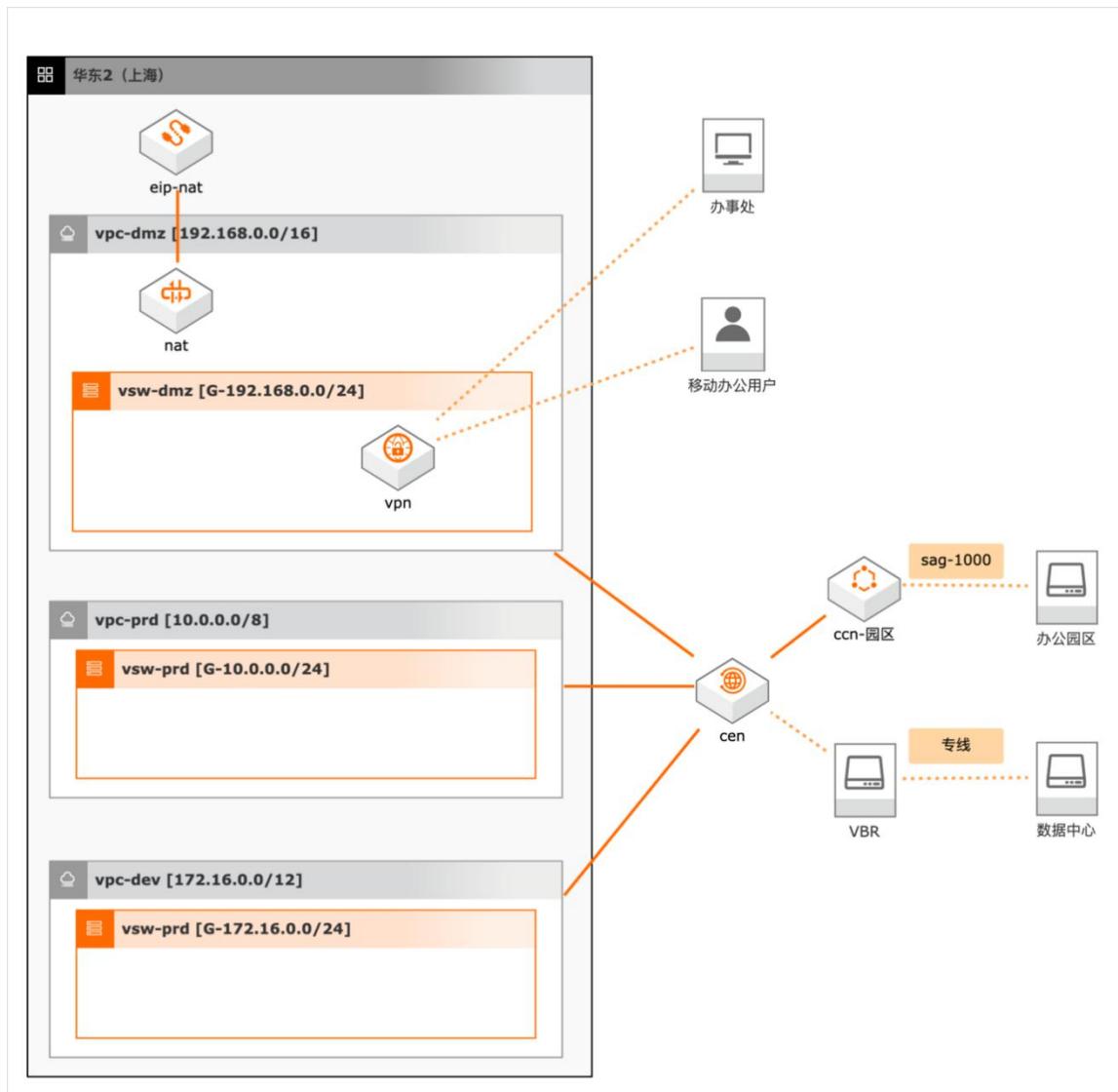
## 5.7.云速搭部署云上网络组网

作者 | 阿里云解决方案架构师 天裴

### 5.7.1.组网设计

本最佳实践讲解如何通过云速搭搭建云上网络环境。

#### 方案架构



## 方案场景

- 某公司将自建数据中心中的部分业务系统迁移到阿里云。
- 数据中心通过专线与阿里云上网络环境打通；办公园区使用 SAG-1000 与阿里云上网络打通；各地办事处和移动办公人员使用 VPN 接入云上网络。
- 阿里云上主机通过 DMZ 区的 NAT 网关访问公网。
- 阿里云上的资源部署在上海可用区 G，通过 VPC 隔离出 DMZ、生产（prd）和开发（dev）三个环境。
- 机房专线、园区 SAG、阿里云上三个 VPC 全部通过 CEN 打通。可以通过调整 CEN 的路由自动学习来控制不同网络之间的访问。

## 其他说明

- 在复杂组网的大型架构中，为了保证架构图的可读性，建议先单独规划和部署网络资源。需要部署应用的计算等资源时，创建新的小型架构图，并导入已有的网络资源。

## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下图所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
云企业网 CEN	全局
云连接网 CCN	全局
弹性公网 IP	Region
NAT 网关	VPC
VPN 网关	Vswitch

## 网络资源配置规划

基础网络资源

资源类别	配置项	配置明细
区域	区域	华东 2 (上海)
专有网络 VPC	状态	新购
	VPC 名	vpc-dmz
	网段	192.168.0.0/16
虚拟交换机	状态	新购
	vswitch 名	vsw-dmz
	可用区	华东 2 可用区 G
	IPv4 网段	192.168.0.0/24
专有网络 VPC	状态	新购
	VPC 名	vpc-prd
	网段	10.0.0.0/8
虚拟交换机	状态	新购
	vswitch 名	vsw-prd
	可用区	华东 2 可用区 G
	IPv4 网段	192.168.0.0/24
专有网络 VPC	状态	新购
	VPC 名	vpc-dev
	网段	172.16.0.0/12
虚拟交换机	状态	新购
	vswitch 名	vsw-dev
	可用区	华东 2 可用区 G
	IPv4 网段	172.16.0.0/24
EIP	购买方式	新购
	EIP 名	eip-nat
	商品类型	按量付费
	网络类型	公网
	流量	按使用流量付费
	带宽	10Mbps

## 网关资源

资源类别	配置项	配置明细
NAT 网关	购买方式	新购
	NAT 网关名	nat
	支付方式	按量付费
	网关类型	增强型
	计费类型	按使用量计费
	所属 vswitch	(与 DMZ 的 vsw 保持一致)
VPN 网关	vpn 名	vpn
	带宽规格	5Mbps
	支付方式	包年包月/1 个月
	是否开启 IP-secVPN	enable
	是否开启 SSL-VPN	disable

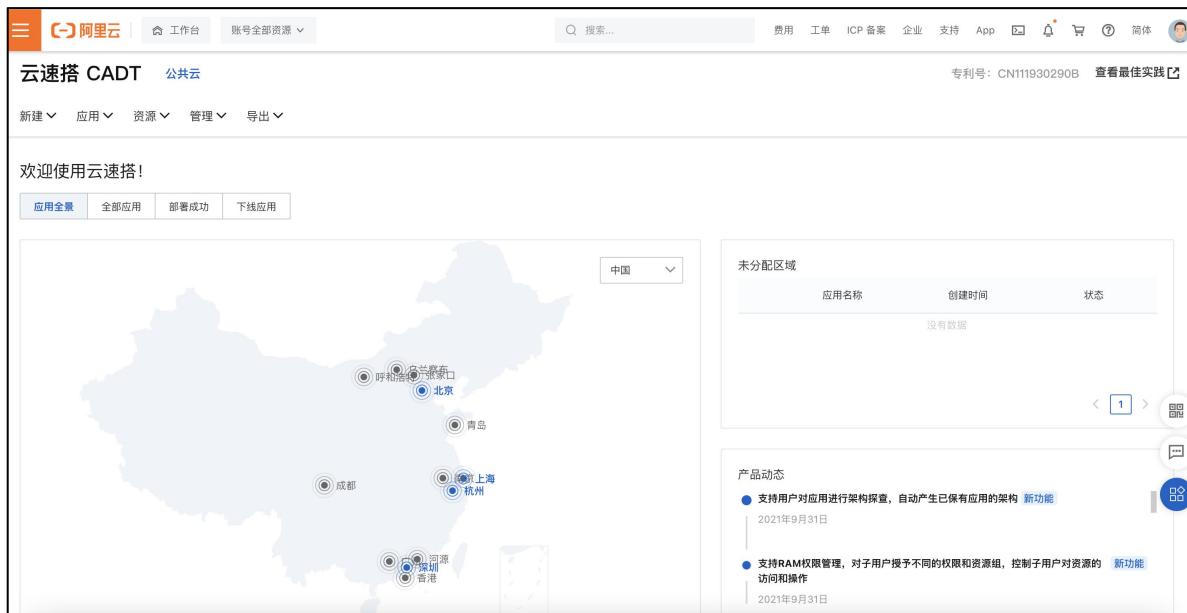
## 云企业网

资源类别	配置项	配置明细
CEN	购买方式	新购
	云企业网	cen
	带宽包	同地域组网无需购买带宽包
CCN	云链接网	ccn-园区
	区域	中国内陆
	私网网段	192.168.100.0/24
	是否创建	true

## 5.7.2. 绘制基础网络资源

步骤 1 访问 <https://bpstudio.console.aliyun.com/> 登录 CADT 控制台。

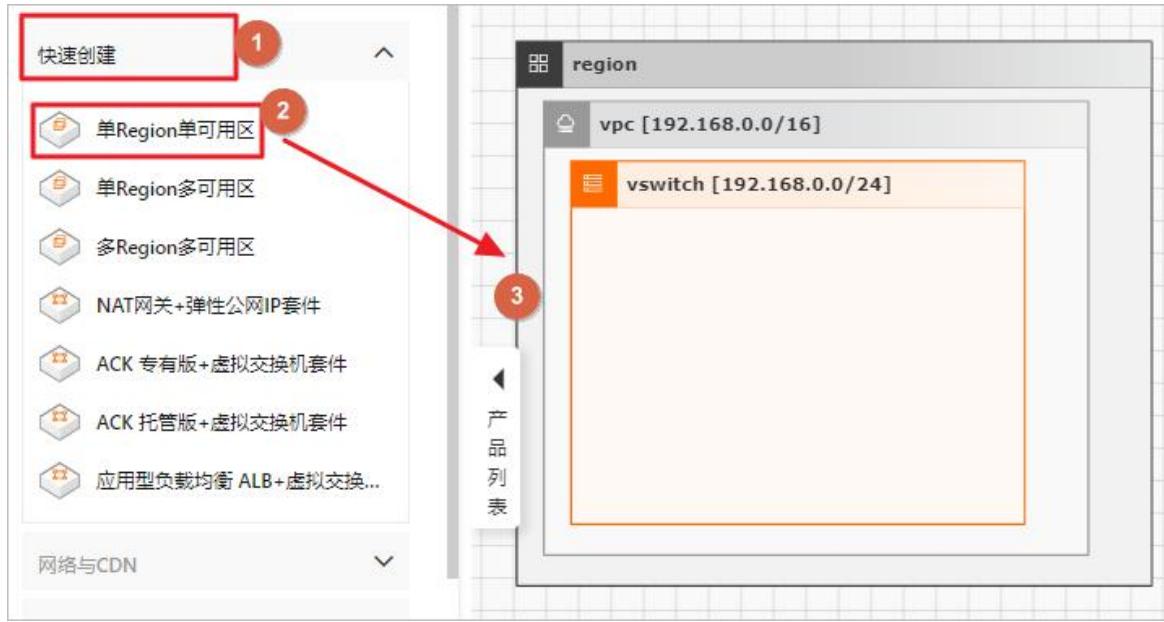
**说明：**如果提示需要开通服务，请根据提示进行开通。



步骤 2 在 CADT 控制台的菜单栏单击新建 > 新建空白应用。



步骤 3 从左侧快速创建列表找到单 Region 单可用区，单击拖入到画布区域中，松开鼠标。



步骤 4 在 region 的任意位置双击鼠标，开启配置清单，选择 华东 2（上海）。

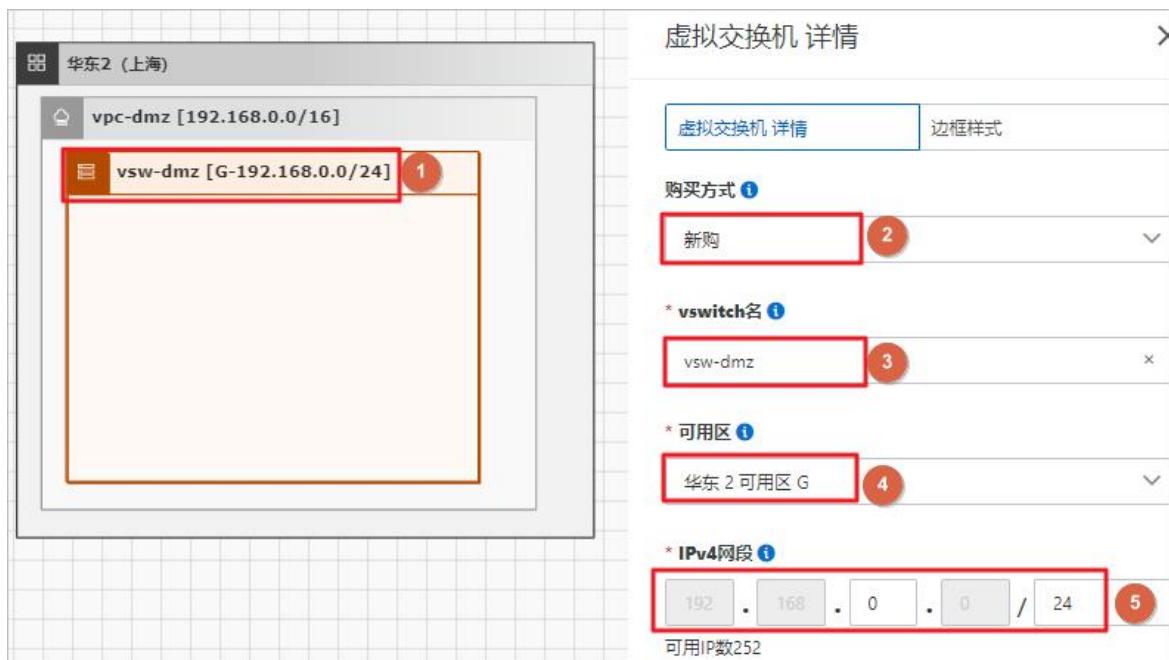


**说明：**配置完一个对象后，可以直接打开下一个对象，云速搭会自动保存现有配置。

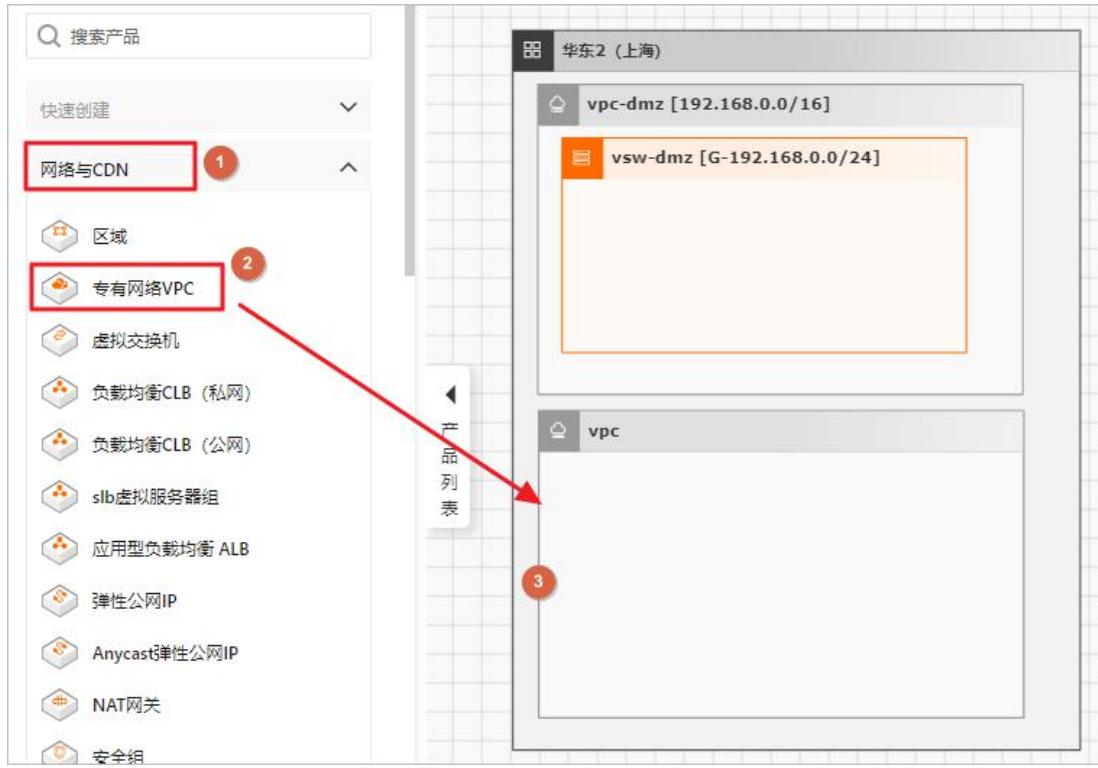
步骤 5 在 VPC 的任意位置双击鼠标，开启配置清单，根据[章节 1.2.1 基础网络资源配置](#)配置 VPC。



步骤 6 在 vswitch 的任意位置双击鼠标，开启配置清单，根据[章节 1.2.1 基础网络资源配置](#) vsw-dmz。



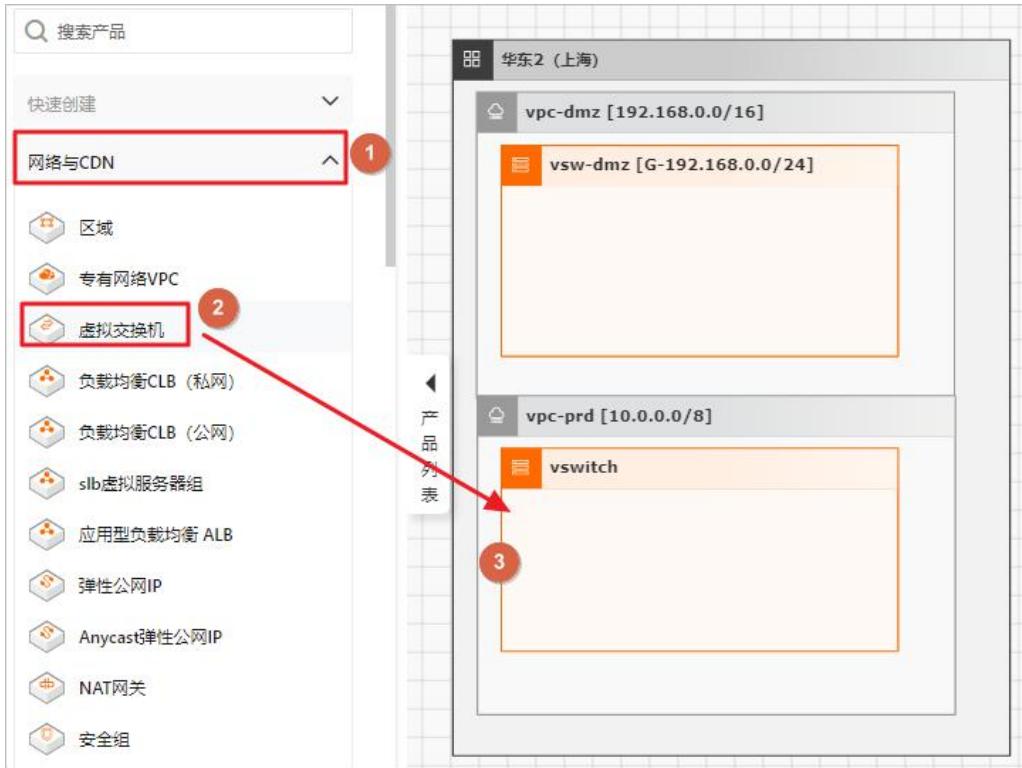
步骤 7 从左侧产品列表中找到 vpc，拖入上海区域。



双击 VPC 开启配置，根据[章节 1.2.1 基础网络资源配置](#)配置 vpc-prd。



步骤 8 从左侧产品列表中找到 虚拟交换机，拖入 vpc-prd。



双击 vswitch 开启配置，根据[章节 1.2.1 基础网络资源配置](#)配置 vsw-prd。

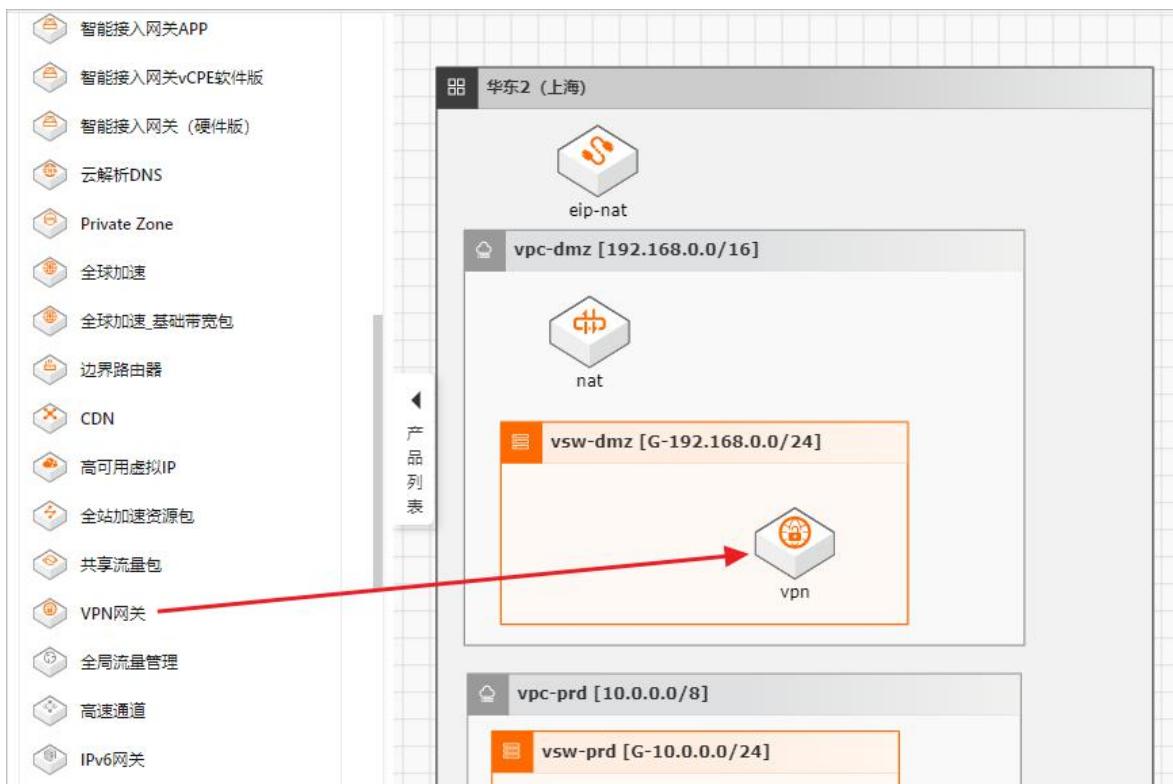
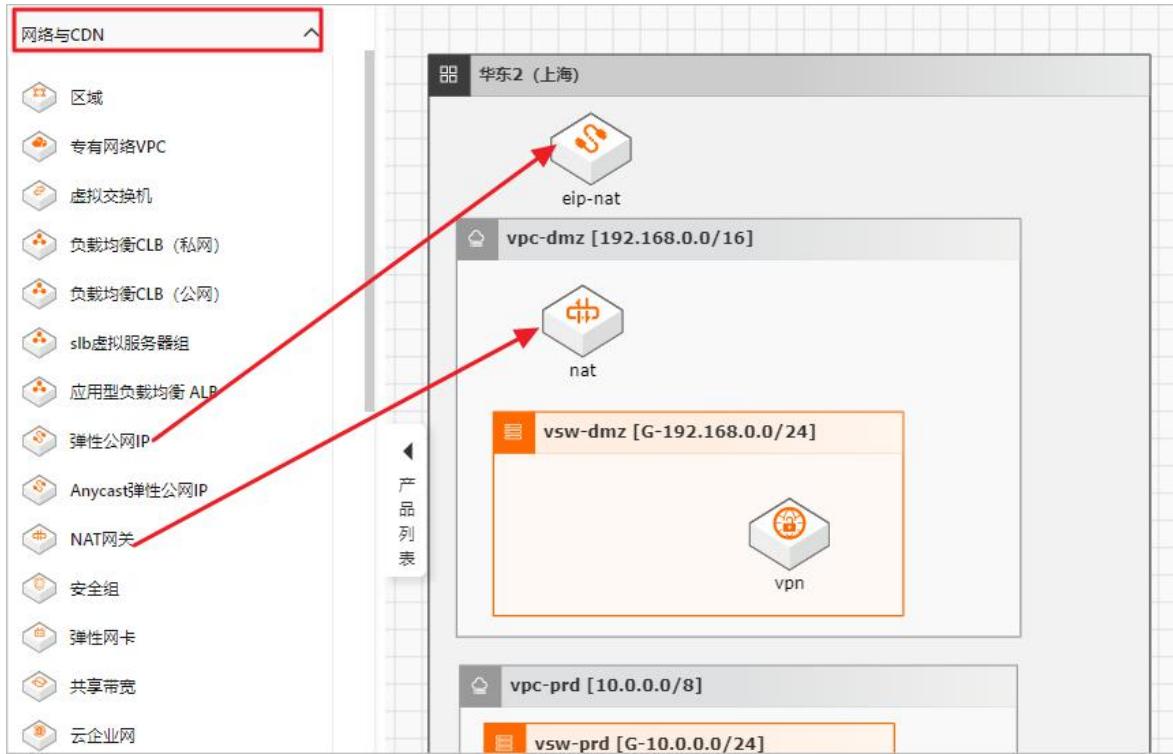


步骤 9 重复步骤 6 ~ 步骤 7，根据[章节 1.2.1 基础网络资源配置](#)配置 vpc-dev 和 vsw-dev。  
调整图上对象的位置和大小，优化可读性：

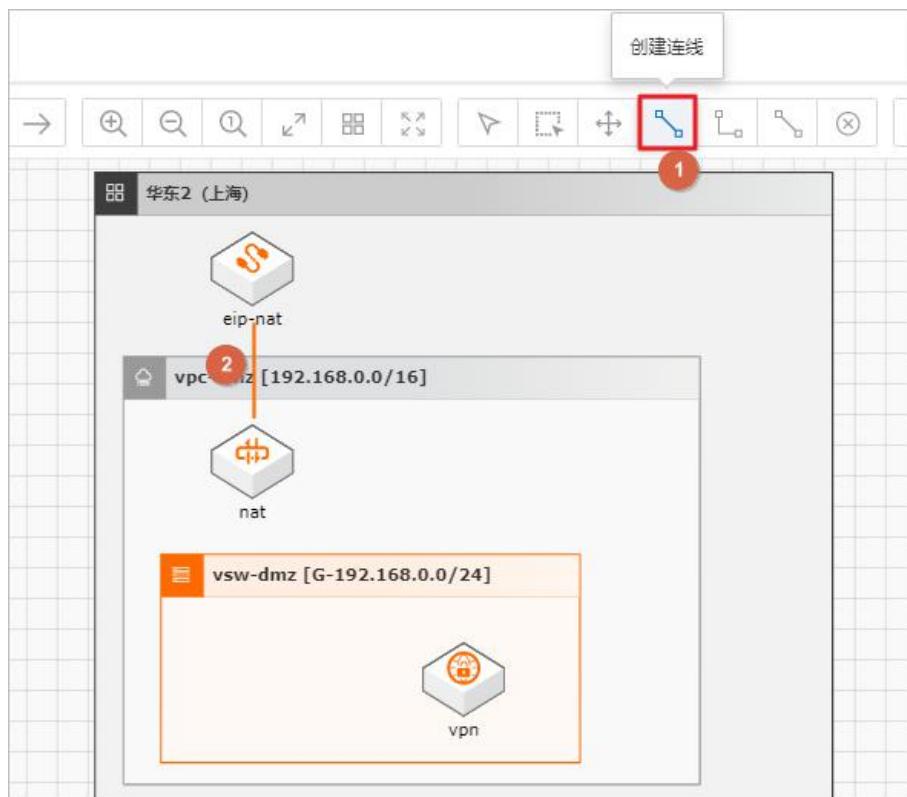


### 5.7.3.绘制网关资源

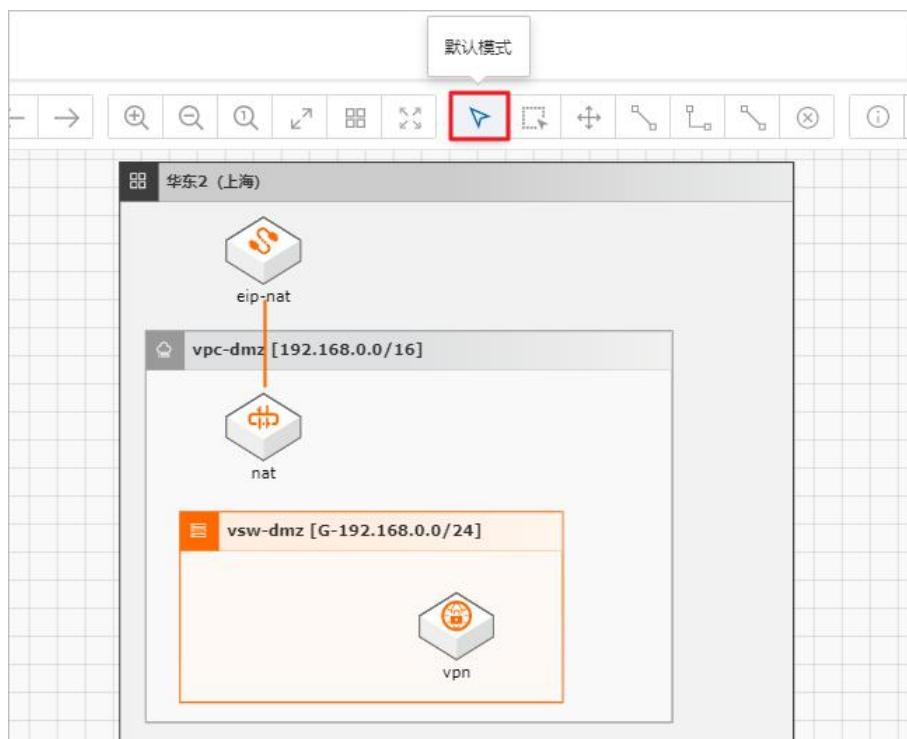
步骤 1 在左侧产品列表搜索 nat 和 vpn，拖拽到 vpc-dmz 和 vsw-dmz 中。搜索 eip，拖拽到上海区域中。根据 [章节 1.2.2 网关资源](#) 配置 nat 网关，vpn 网关，eip\_nat 和 eip\_vpn。



步骤 2 使用连接线给 nat 网关绑定 eip，部署后 eip 将自动挂载到对应的实例上。

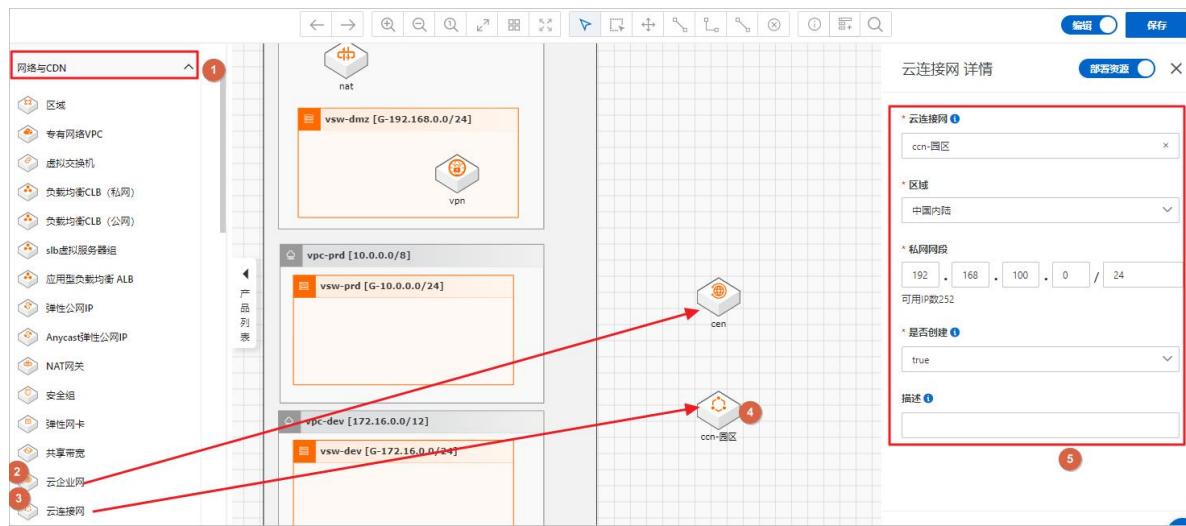


完成连线后切换回默认模式。



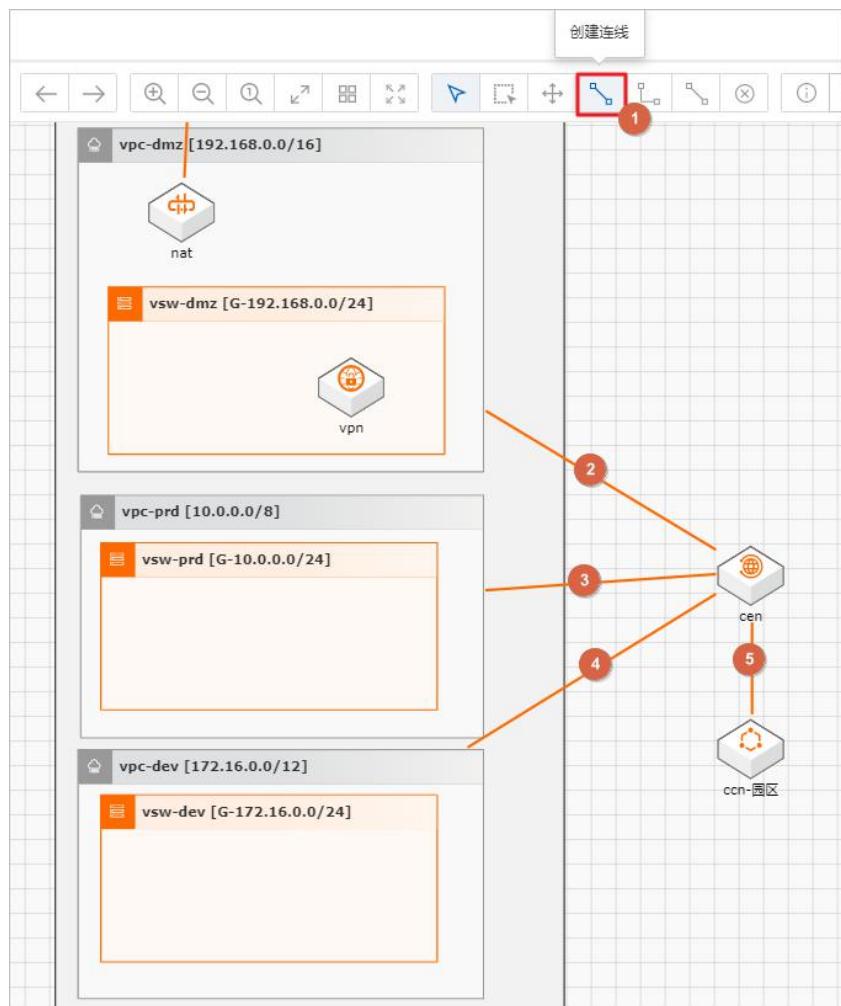
## 5.7.4.绘制云企业网

步骤 1 在左侧产品列表搜索 cen 和 ccn，拖拽到画布中。根据 章节 1.2.3 云企业网 配置 cen 和 ccn-园区。

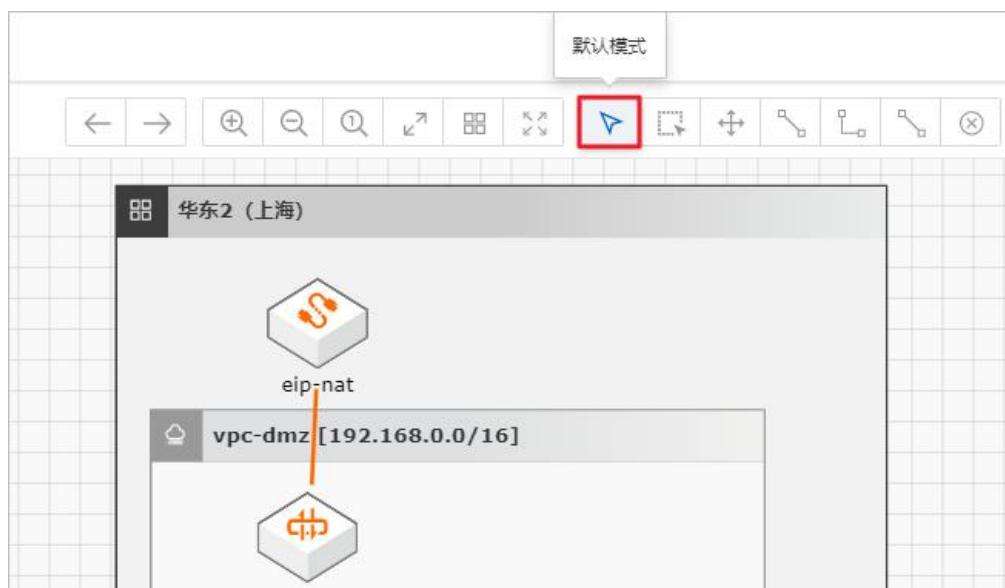


**说明：**CEN 和 CCN 是全局资源，所以他们不属于任何地域。

步骤 2 使用连接线将分别将 3 个 VPC 和 1 个 CCN 连接到 CEN 上，代表将其挂载到 CEN 实例上。



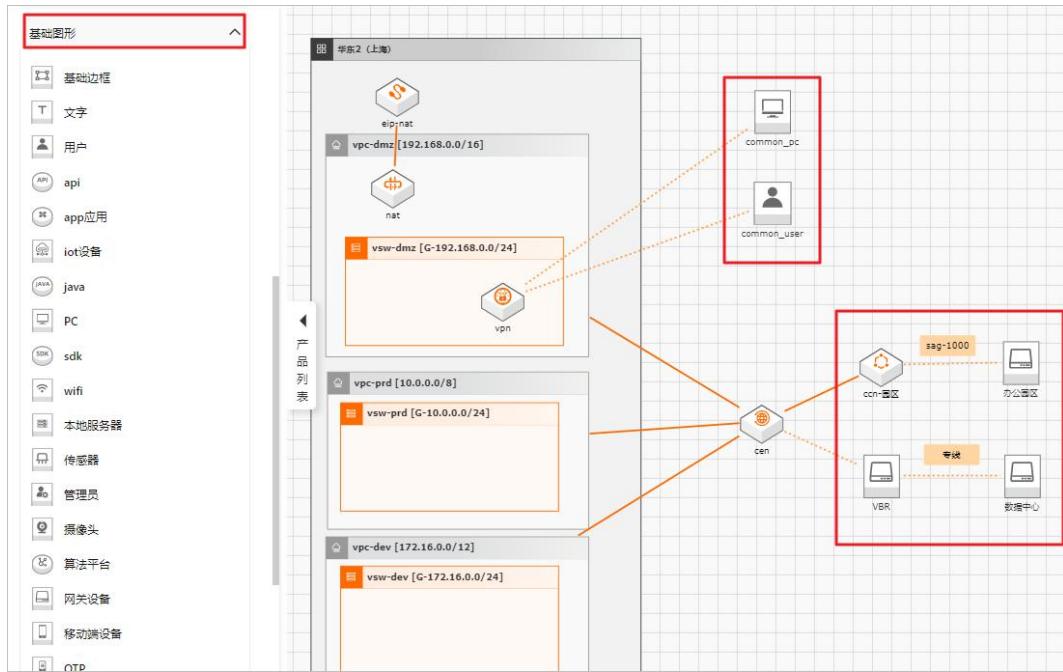
完成连线后切换回默认模式。



## 5.7.5.绘制说明类图标

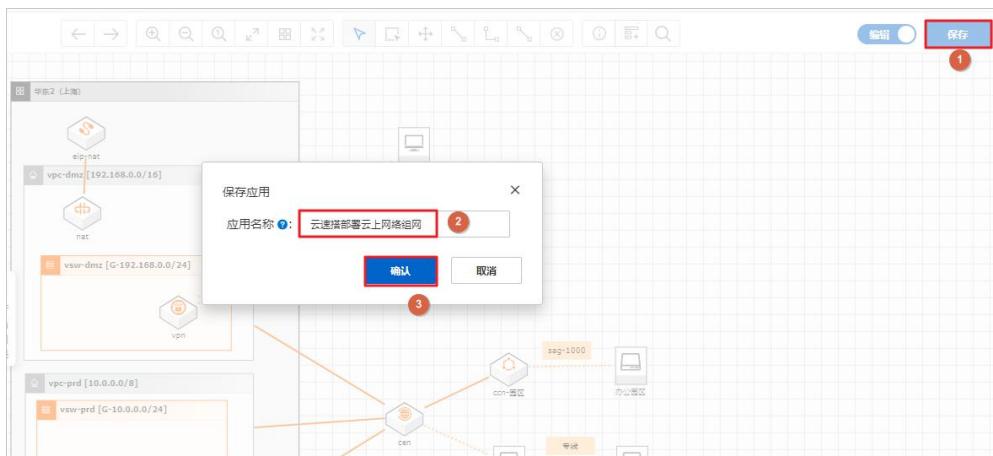
步骤 1 为了表达更丰富的组网信息，可以在图中添加说明性的图标。

**注意：**说明性的图标仅做展示说明，没有任何的资源部署和配置关系。



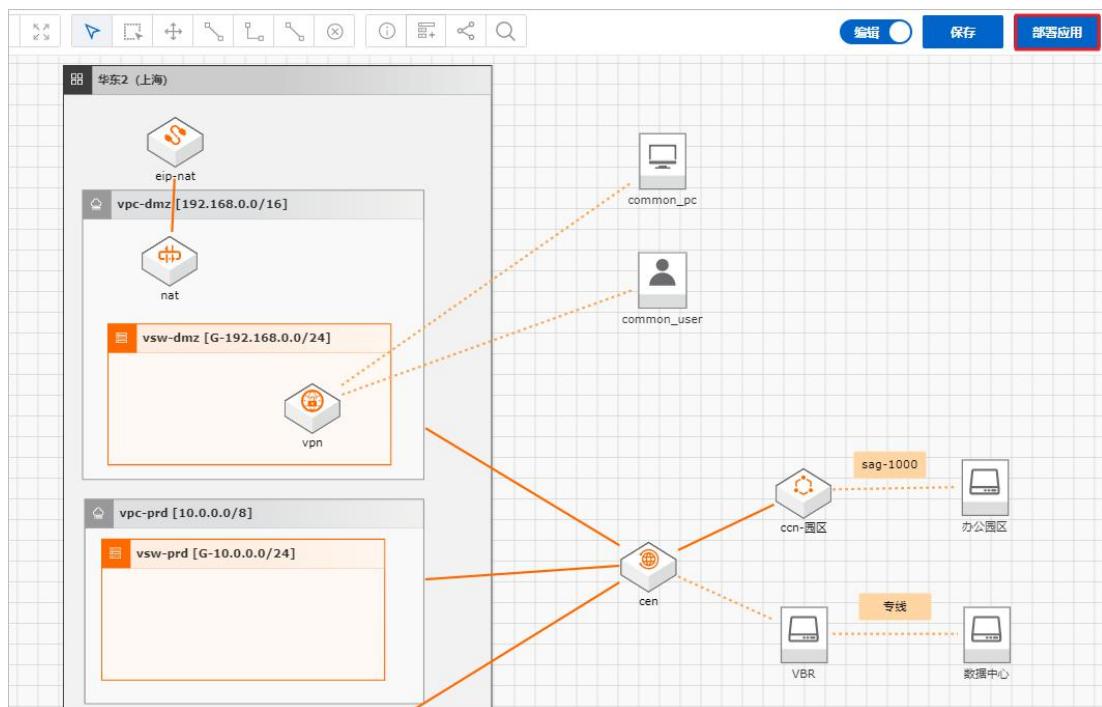
## 5.7.6.保存架构图

步骤 1 将设计好的架构保存为应用，单击右上角的**保存**，在弹出的窗口中，填写**应用名称**，并单击**确认**。



## 5.7.7.执行部署

步骤 1 单击右上角的部署应用。



步骤 2 开始进行资源验证，如果有校验错误提示，根据提示进行修改，直至校验成功后单击下一步：价格清单。

资源验证							
序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vpc-dmz [192.168.0.0/16]	vpc	上海	192.168.0.0/16	成功	校验通过	定位
2	vsw-prd [G-172.16.0.0/24]	vswitch	上海	172.16.0.0/24	成功	校验通过	定位
3	vpn	vpn	上海	5	成功	校验通过	定位
4	ccn-园区	ccn			成功	校验通过	定位
5	eip-nat	eip	上海	public	成功	校验通过	定位
6	vpc-prd [10.0.0.0/8]	vpc	上海	10.0.0.0/8	成功	校验通过	定位

状态: **校验成功**
下一步: 价格清单
返回

步骤3 待询价成功后，核对方案价格（也可以单击**查看报告**导出PDF版的报价清单），单击**下一步：确认订单**。

### 导出价格清单

免费 **包年包月** 按量付费

资源成本占比



资源预算  
● 网络 网络: 100 元

100%

价格列表

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	优惠	实付	操作
1	cen	cen			1	-				<a href="#">定位</a>
2	vpn	vpn	上海	5	1	1月	100元	100元	100元	<a href="#">定位</a>

状态：**计价成功**

上一步：资源校验 **查看报告** **下一步：确认订单**

步骤4 勾选《云速搭服务条款》，单击**下一步：支付并创建**。

### 确认订单

免费 **包年包月** 按量付费

序号	资源名称	资源类型	区域	规格	数量	购买时长	原价	实付	状态
1	vpn	vpn	上海	5	1	1月	100元	100元	新购
2	cen	cen			1	-			新购

**《云速搭服务条款》**

部署前，请阅读并勾选服务条款

包年包月：**100元** 按量付费：**100元/时**

状态：**计价成功**

上一步：价格清单 **下一步：支付并创建**

步骤 5 进入部署流程，这里会进行扣费并开始创建资源。



步骤 6 等待资源部署完成，点击返回。

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	eip-vpn	eip (弹性公网IP)	按量付费	eip-uf6rkq0zhedihsuzzjlqx	运行中	2021-12-05 23:06:16	定位
2	eip-nat	eip (弹性公网IP)	按量付费	eip-uf67up7la3o2scrkafw7a	运行中	2021-12-05 23:06:16	定位
3	cen	cen (云企业网)	-	cen-g6belxwz6coez39hbk	运行中	2021-12-05 23:06:16	定位
4	ccn-园区	ccn (云连接网)	-	ccn-myaysmd09man7dxttqq	运行中	2021-12-05 23:06:16	定位
5	vpc-dmz [192.16 8.0.0/16]	vpc (专有网络VPC)	-	vpc-uf6tbf2xatfghelm91knz	运行中	2021-12-05 23:06:46	定位

每页显示 10 共12条 < 上一页 1 2 下一页 >

**部署概要**

状态: 部署成功

订单编号 : 211778471990497, 211778274160497, 211778816990497,  
211777877120497

方案编号: PMRL986JA6GH6QUL

查看报告 返回

## 5.7.8.检查 CEN 网络资源挂载情况

步骤 1 双击架构图中的 CEN 实例，打开资源详情页，单击前往控制台。



步骤 2 可以看到 3 个 VPC 和一个 CCN 都已经挂载到 CEN 上。

ID: cen-g6belxwz6coez39hbk	状态: 可用																																			
名称: cen 编辑	重叠路由功能: 已开启																																			
描述: - 编辑																																				
<a href="#">网络实例管理</a> <a href="#">带宽包管理</a> <a href="#">跨地域互通带宽管理</a> <a href="#">路由信息</a> <a href="#">云服务</a> <a href="#">Private Zone</a> <a href="#">路由策略</a>																																				
<a href="#">加载网络实例</a> <a href="#">刷新</a> <table border="1" data-bbox="198 1078 1379 1464"> <thead> <tr> <th>实例ID/名称</th><th>所属地域</th><th>实例类型</th><th>所属账号</th><th>加载时间</th><th>状态</th><th>操作</th></tr> </thead> <tbody> <tr> <td>ccn-myaysmd09man7dxtqq ccn-园区</td><td>中国内地云连接网</td><td>云连接网 (CCN)</td><td>1186102223270461</td><td>2021年12月5日 23:08:00</td><td>● 已加载</td><td>卸载</td></tr> <tr> <td>vpc-uf6tbf2xatfghelm91knz vpc-dmz</td><td>华东2 (上海)</td><td>专有网络 (VPC)</td><td>1186102223270461</td><td>2021年12月5日 23:07:00</td><td>● 已加载</td><td>卸载</td></tr> <tr> <td>vpc-uf6wo2ex99z612oicp5yu vpc-prd</td><td>华东2 (上海)</td><td>专有网络 (VPC)</td><td>1186102223270461</td><td>2021年12月5日 23:08:00</td><td>● 已加载</td><td>卸载</td></tr> <tr> <td>vpc-uf69ls0f3whts20czu4ng vpc-dev</td><td>华东2 (上海)</td><td>专有网络 (VPC)</td><td>1186102223270461</td><td>2021年12月5日 23:08:00</td><td>● 已加载</td><td>卸载</td></tr> </tbody> </table>		实例ID/名称	所属地域	实例类型	所属账号	加载时间	状态	操作	ccn-myaysmd09man7dxtqq ccn-园区	中国内地云连接网	云连接网 (CCN)	1186102223270461	2021年12月5日 23:08:00	● 已加载	卸载	vpc-uf6tbf2xatfghelm91knz vpc-dmz	华东2 (上海)	专有网络 (VPC)	1186102223270461	2021年12月5日 23:07:00	● 已加载	卸载	vpc-uf6wo2ex99z612oicp5yu vpc-prd	华东2 (上海)	专有网络 (VPC)	1186102223270461	2021年12月5日 23:08:00	● 已加载	卸载	vpc-uf69ls0f3whts20czu4ng vpc-dev	华东2 (上海)	专有网络 (VPC)	1186102223270461	2021年12月5日 23:08:00	● 已加载	卸载
实例ID/名称	所属地域	实例类型	所属账号	加载时间	状态	操作																														
ccn-myaysmd09man7dxtqq ccn-园区	中国内地云连接网	云连接网 (CCN)	1186102223270461	2021年12月5日 23:08:00	● 已加载	卸载																														
vpc-uf6tbf2xatfghelm91knz vpc-dmz	华东2 (上海)	专有网络 (VPC)	1186102223270461	2021年12月5日 23:07:00	● 已加载	卸载																														
vpc-uf6wo2ex99z612oicp5yu vpc-prd	华东2 (上海)	专有网络 (VPC)	1186102223270461	2021年12月5日 23:08:00	● 已加载	卸载																														
vpc-uf69ls0f3whts20czu4ng vpc-dev	华东2 (上海)	专有网络 (VPC)	1186102223270461	2021年12月5日 23:08:00	● 已加载	卸载																														

## 5.8.云速搭部署高可用虚拟 IP HaVIP

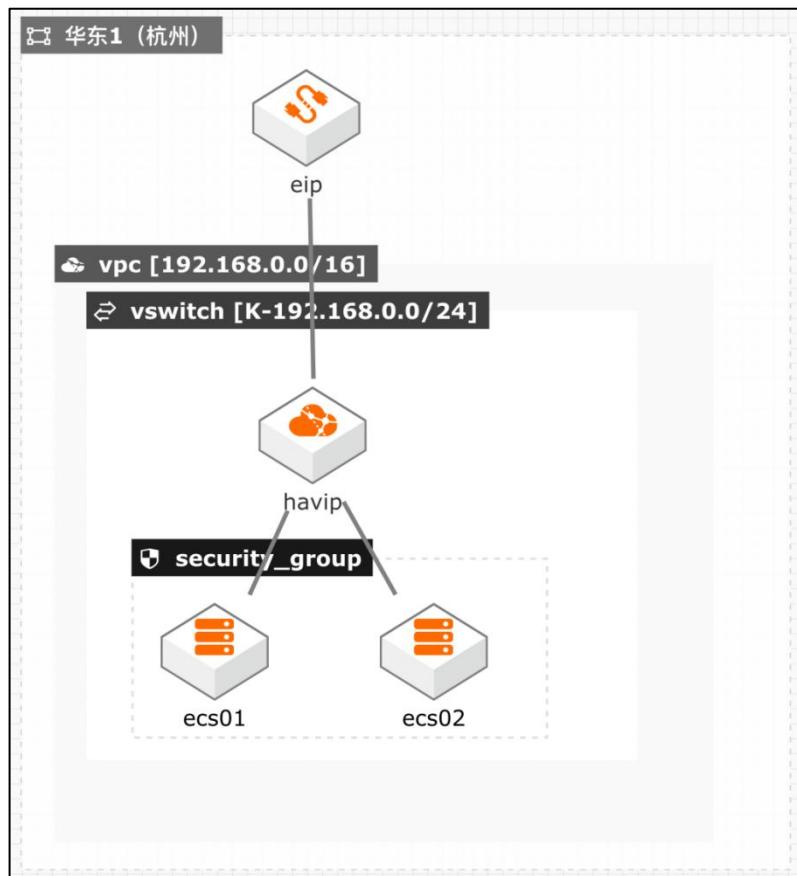
作者 | 阿里云解决方案架构师 厉博

### 5.8.1.云速搭架构设计入门

#### 方案架构

由于 HaVip 功能正在公测，在通过云速搭部署 HaVIP 之前您需要使用阿里云账号（主账号）[提交公测申请](#)。通过了申请后，可以进行资源部署。

通过云速搭部署一个高可用虚拟 IP，并挂载到两个 ECS 实例节点上，大致架构如下图所示。模板部署后，HAVIP 将自动与两个 ECS 关联，并接受通过 ARP 协议宣告来绑定某个 ECS 的网卡。



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

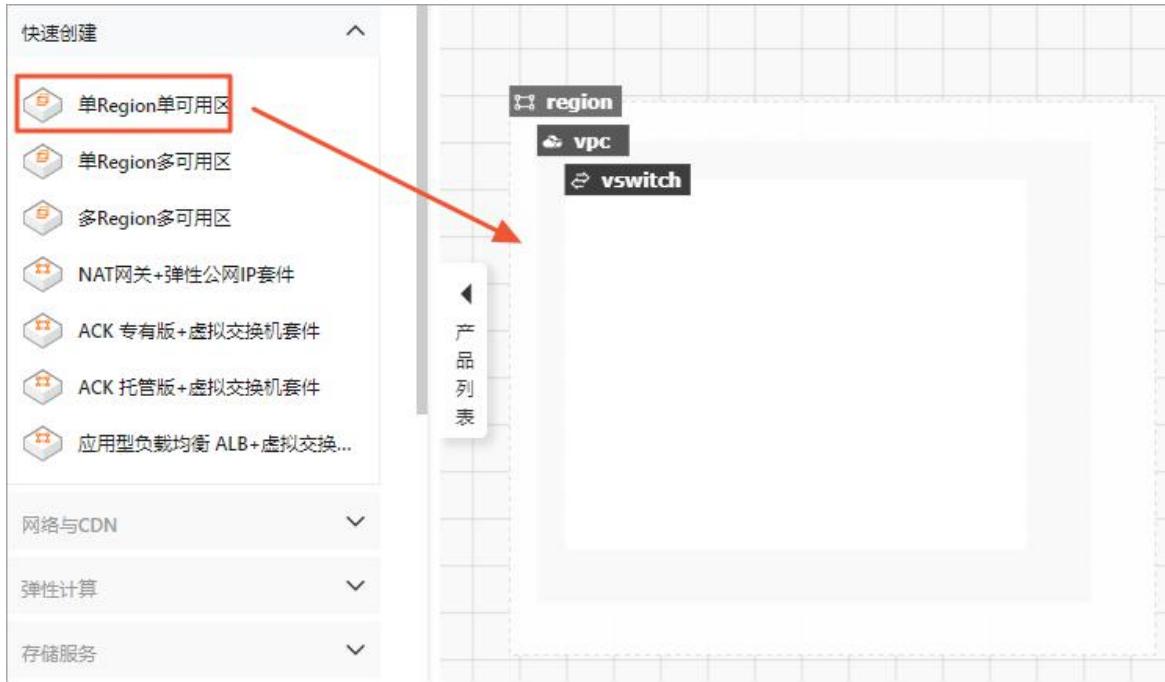
云资源	架构级别
VPC	Region 地域
ECS	vswitch 交换机
HaVIP	vswitch 交换机
EIP	Region 地域

### 5.8.2.设计过程

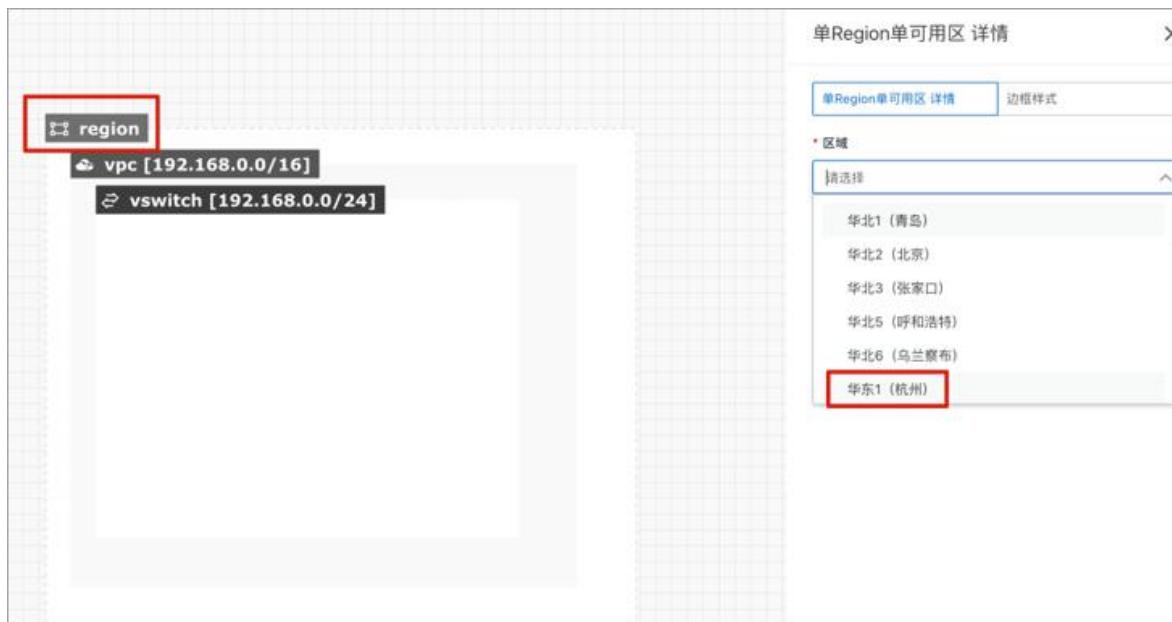
步骤 1 单击新建 > 新建空白应用。



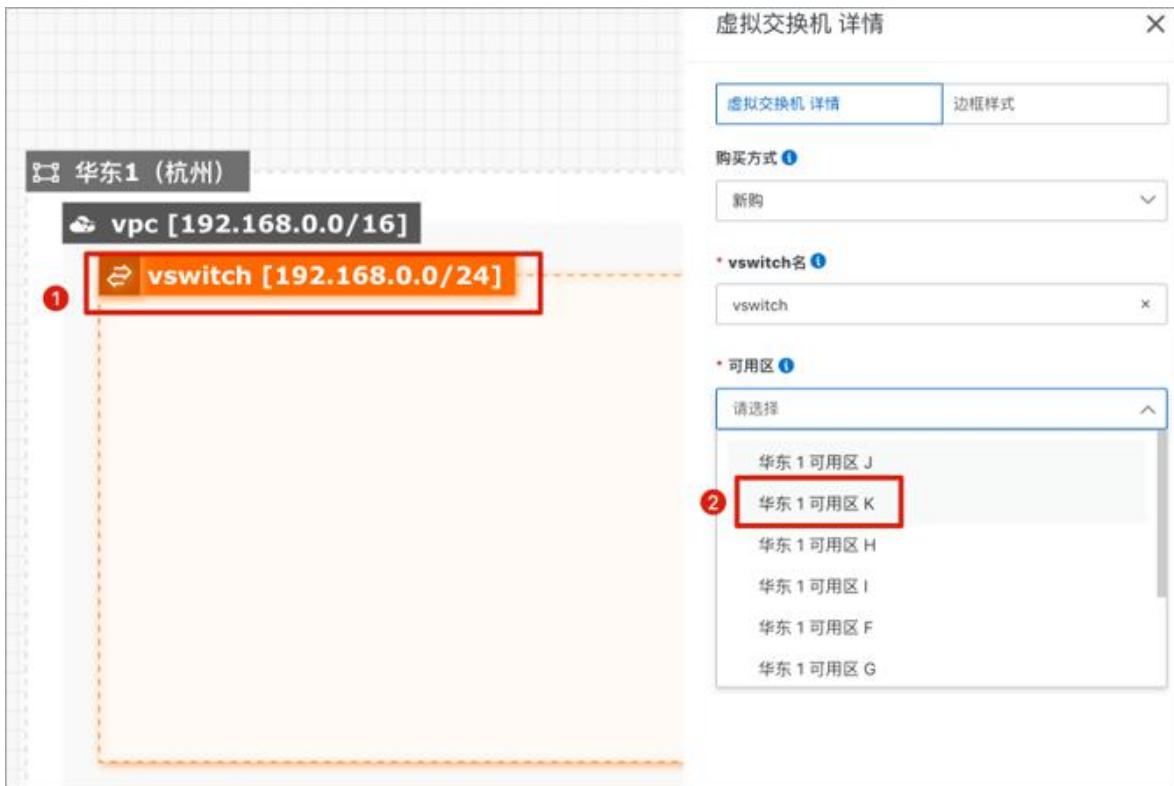
步骤 2 添加一个“单 Region 单可用区”模板到右侧画板中。



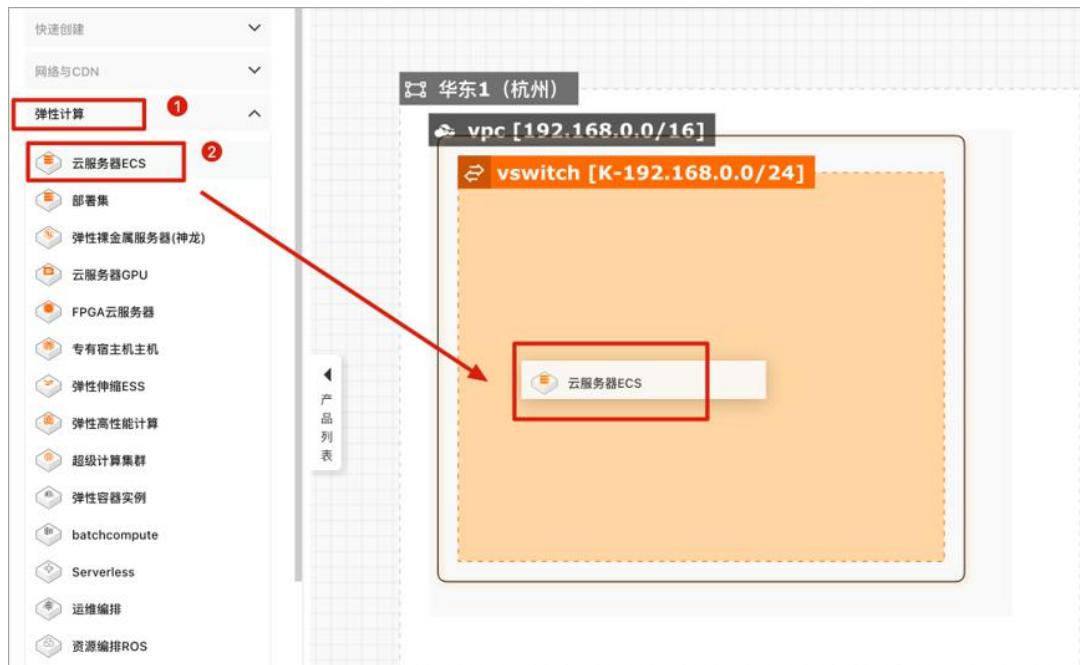
步骤 3 双击区域，选择华东 1（杭州）。(实际部署根据业务需求进行选择)



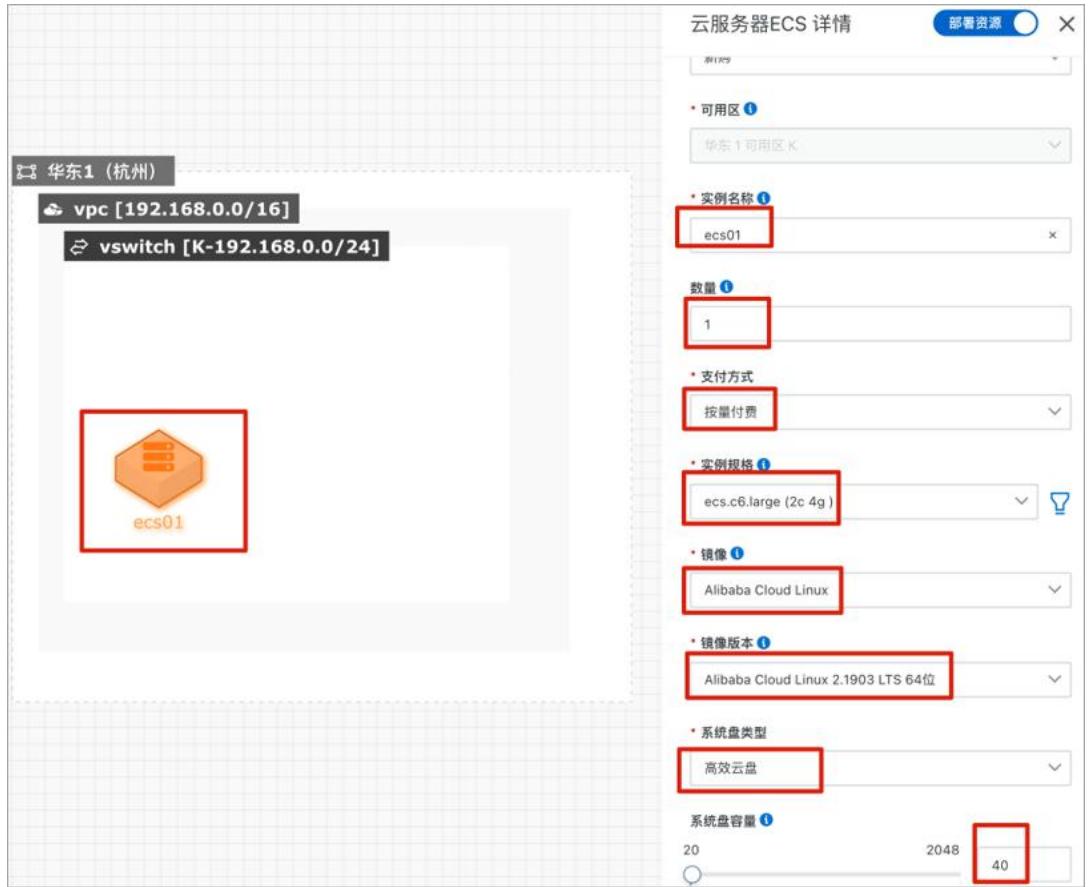
步骤 4 双击 vswitch，选择一个可用区，此处示例为 华东 1 可用区 K



步骤 5 从左侧**弹性计算**分类下拖拽一个云服务器 ECS 到右侧高亮处。



步骤 6 双击 ECS，按下图调整 ECS 的配置。





步骤 7 选中 ECS，右键复制同等配置的 ECS。

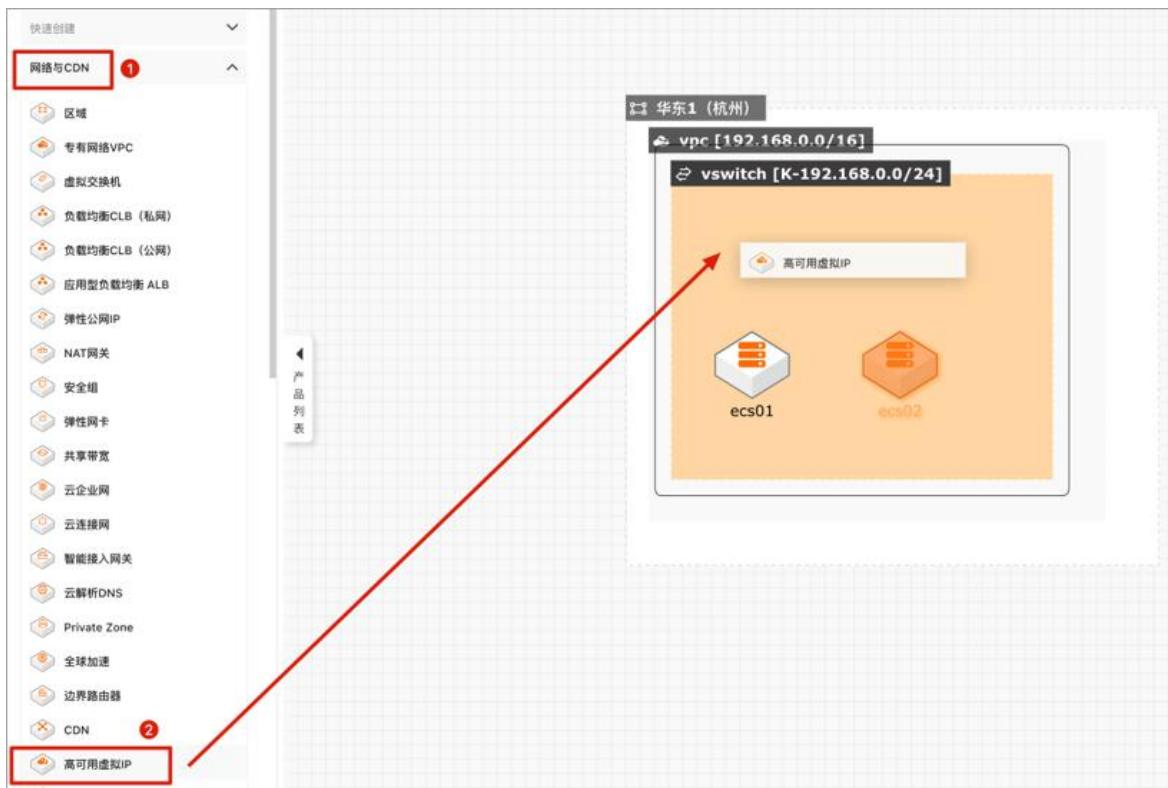


步骤 8 修改实例名称、主机名和私网 IP 地址。

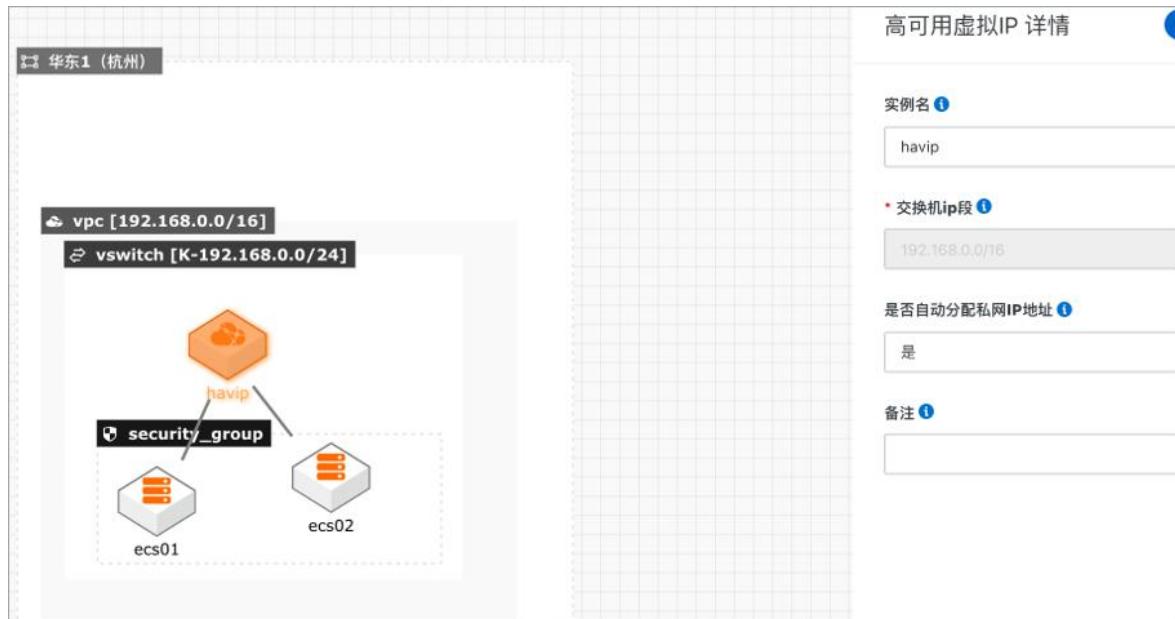




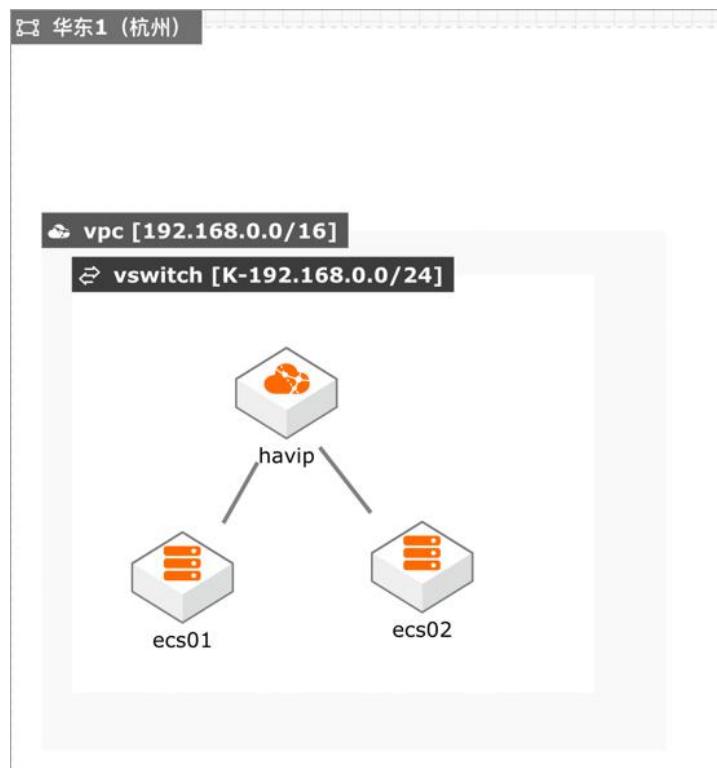
步骤 9 从左侧拖一个高可用虚拟 IP 到右侧高亮处。



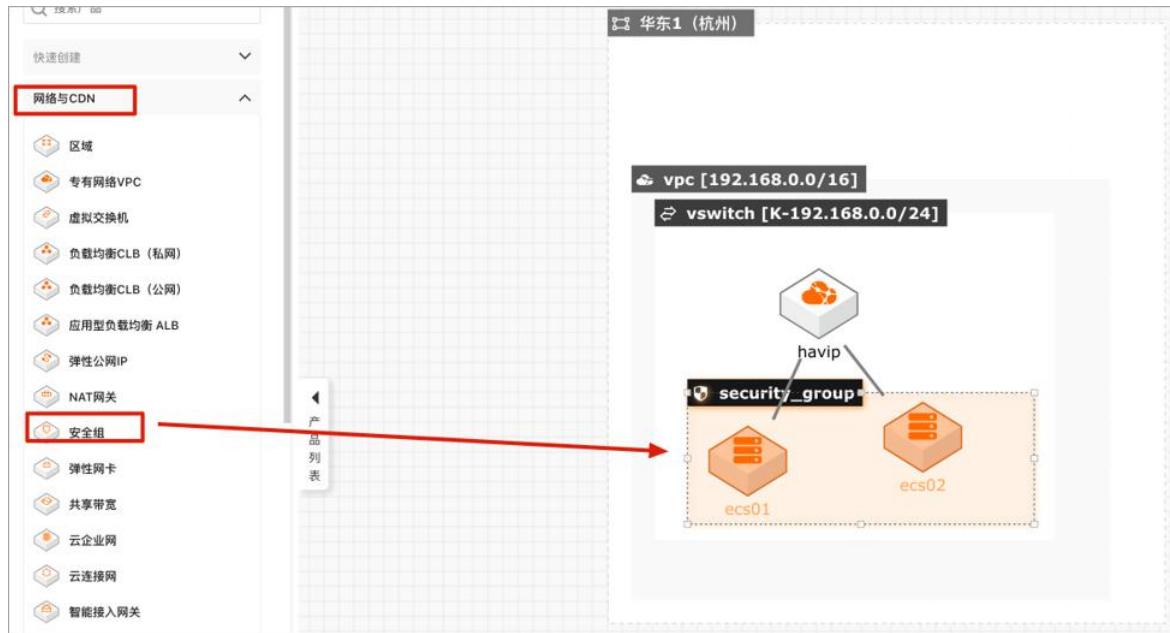
步骤 10 按业务需求决定是否需要指定 HaVIP 的私网地址。



步骤 11 创建连线。在 havip 和两个 ECS 均连线。连线表示资源部署后将自动把 Havip 挂载到两个 ECS 上。但实际 HaVIP 绑定在哪个 ECS 需要 ECS 内部的应用软件通过 ARP 协议宣告来决定。目前 HaVIP 仅支持挂载到两个 ECS 上。



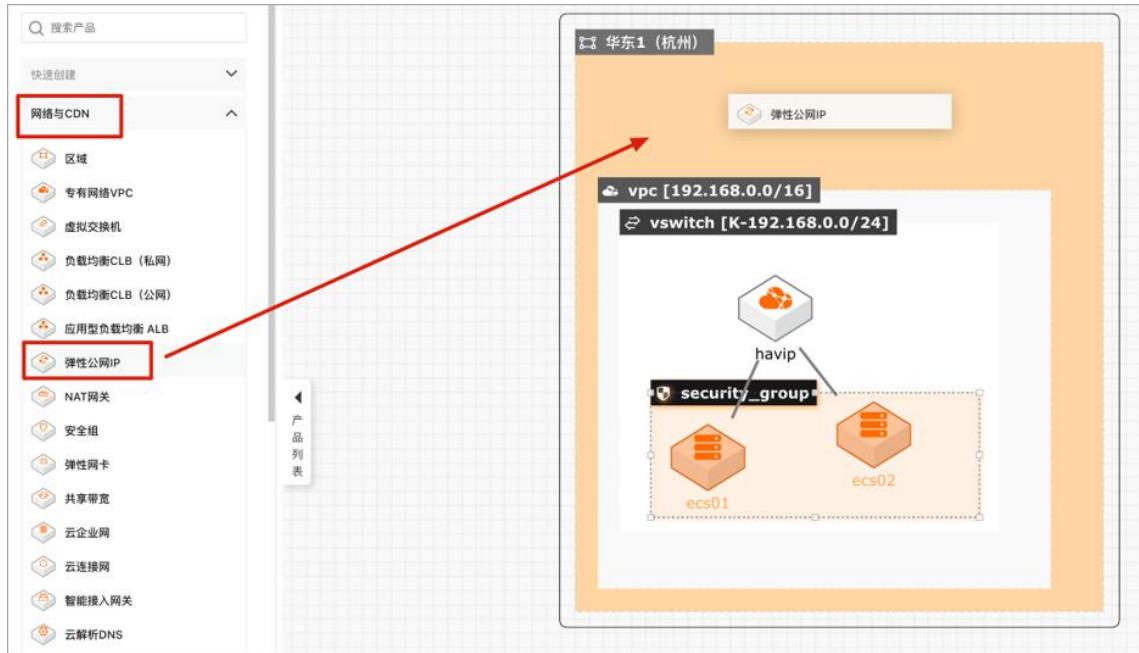
步骤 12 从左侧拖入安全组到两个 ECS 上。双击 ECS 可以按业务需求调整开放的端口。



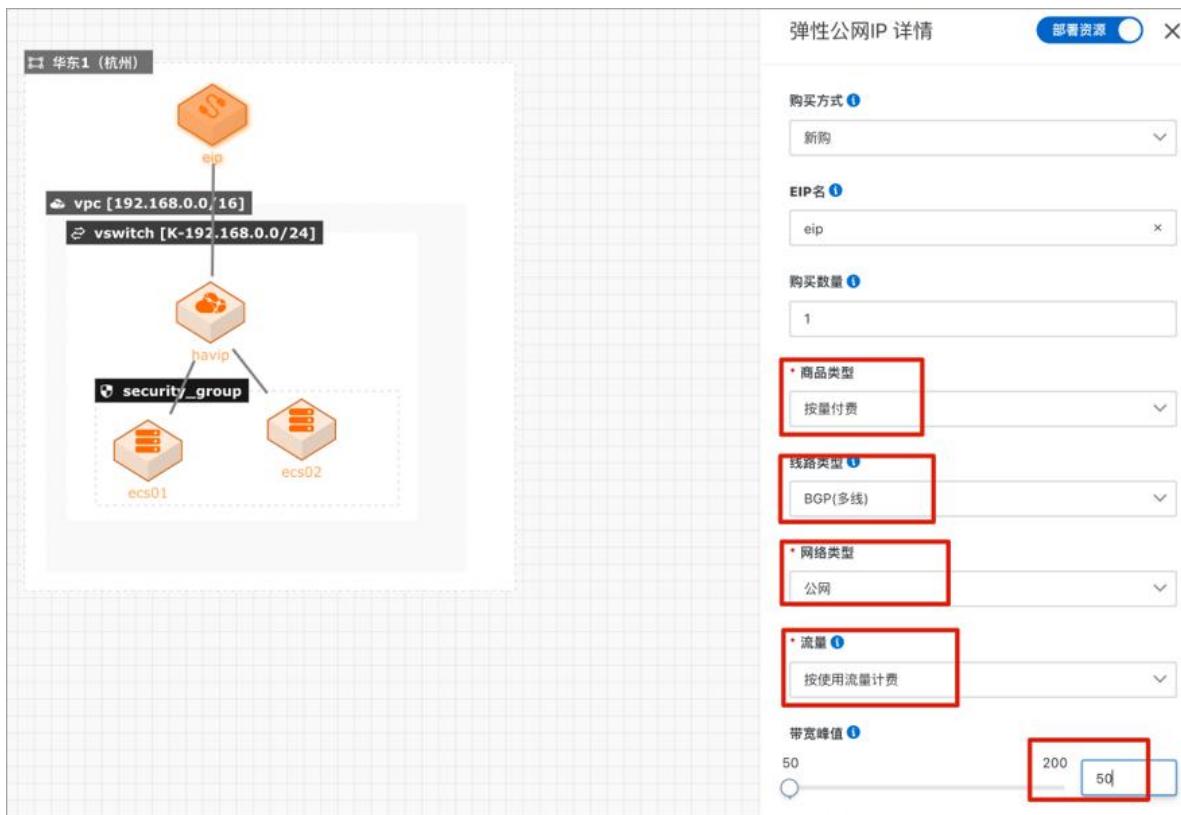
调步骤 13 整安全组规则



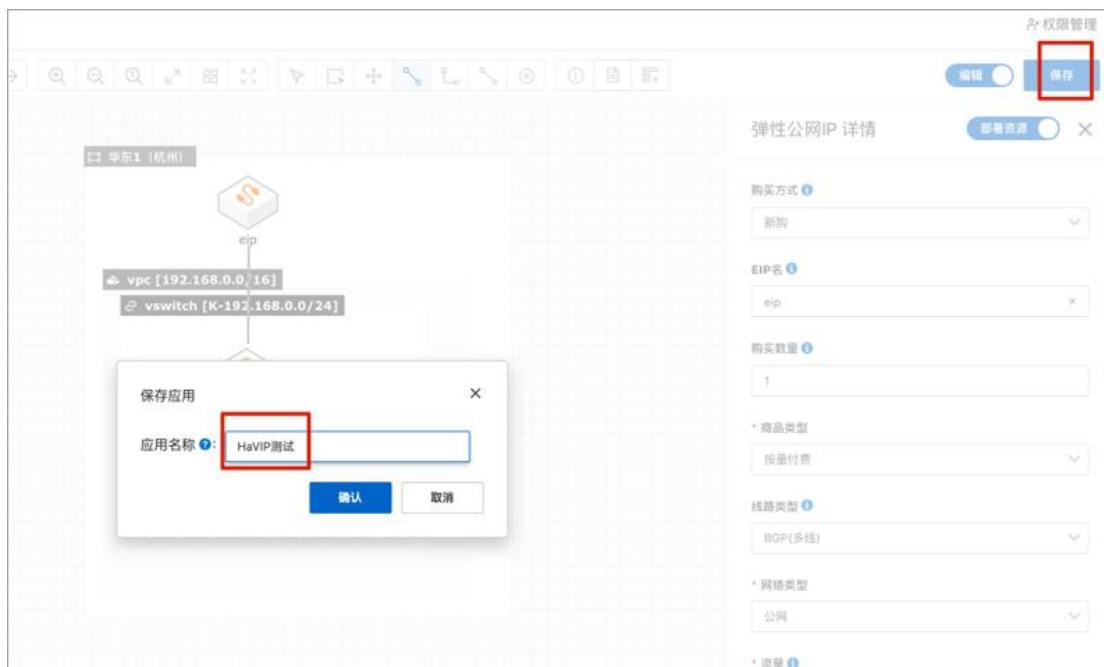
步骤 14 新增一个弹性公网 IP 到右侧区域中。



步骤 15 将 eip 和 HaVIP 连线。部署后 EIP 将和 HaVIP 关联。双击 EIP，按下图进行配置调整。

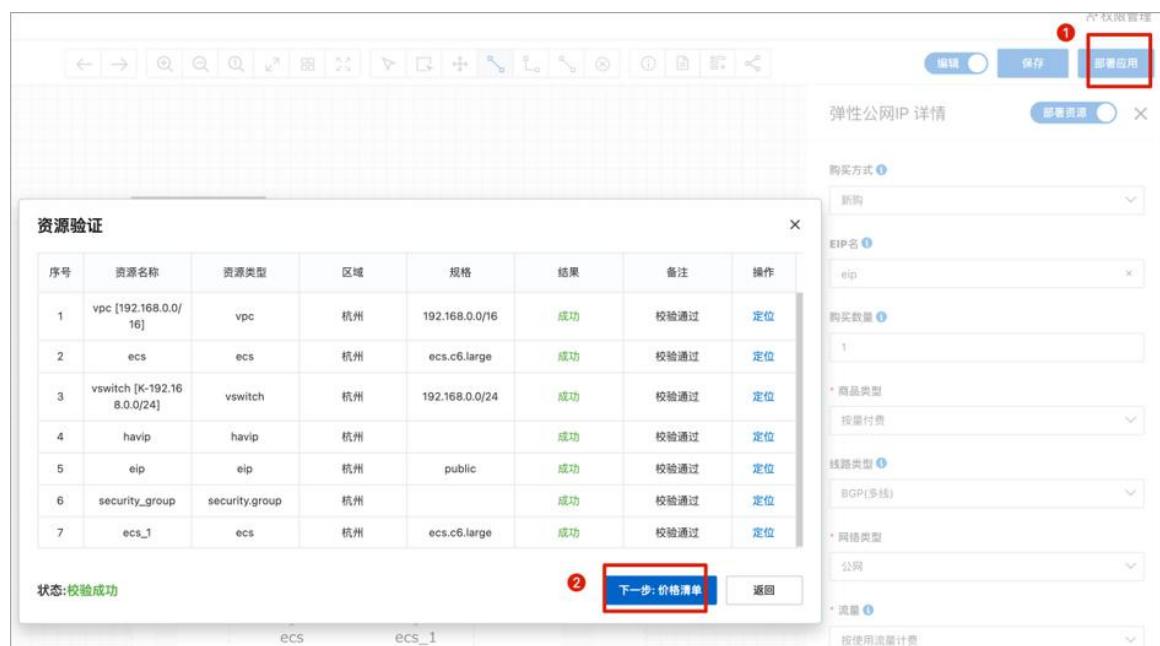


步骤 16 保存架构。



### 5.8.3. 部署过程

步骤 1 保存后单击部署应用，系统将对资源配置进行校验。若校验成功，单击**下一步：价格清单**。



步骤2 确认价格无误后，单击**确认订单**。可以单击查看报告得到一份报价清单。



步骤3 勾选“《云速搭服务条款》”，确认价格后，单击**下一步：支付并创建**。

**确认订单**

免费 按量付费

序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	ecs	ecs	杭州	ecs.c6.large	1	0.41元/时	0.41元/时	新购
2	ecs_1	ecs	杭州	ecs.c6.large	1	0.41元/时	0.41元/时	新购
3	eip	eip	杭州	public	1	0.02元/时	0.02元/时	新购

**《云速搭服务条款》**

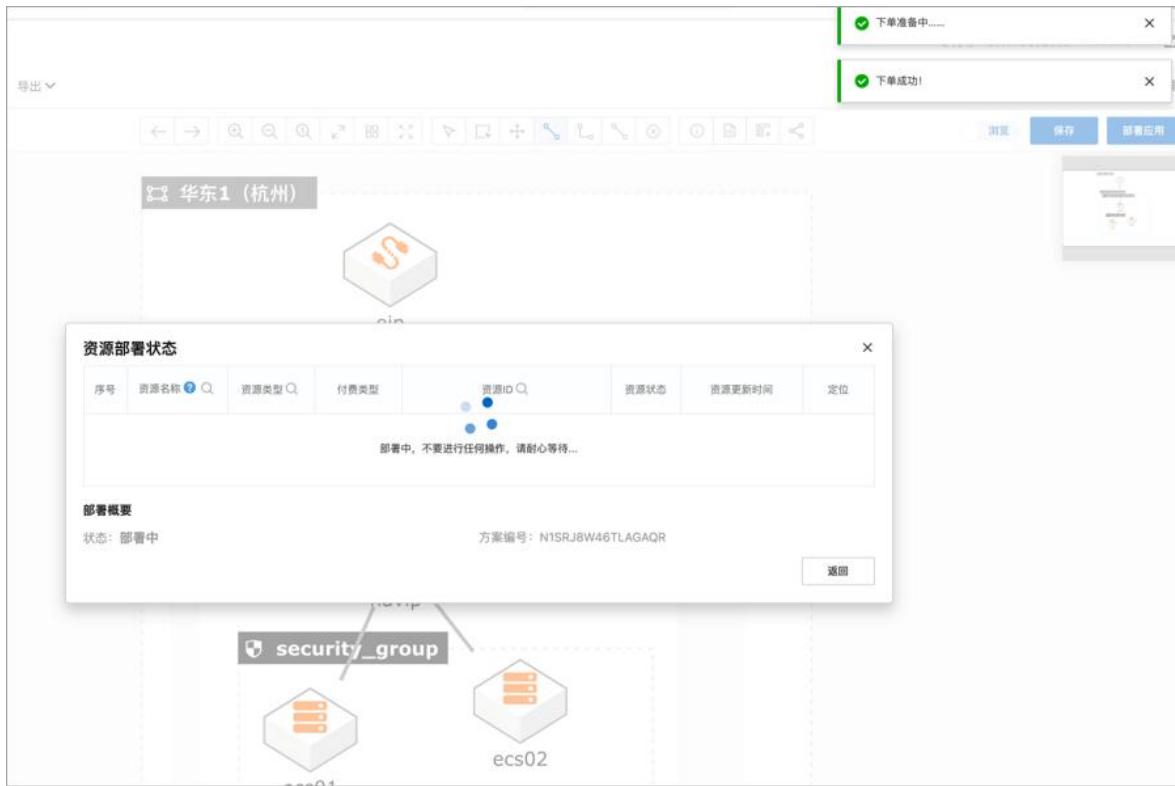
部署前，请阅读并勾选服务条款

**按量付费: 0.03元/时**

状态: **计价成功**

上一步: 价格清单 **下一步: 支付并创建**

步骤4 等待资源部署完成，部署过程为后台调用进程。



步骤5 部署成功。

资源部署状态							
序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
3	vswitch [K-192.1 68.0.0/24]	vswitch (虚拟交换机)	-	vsw-bp1amzrwy01o7qpgovttt	运行中	2021-11-30 17:13:51	定位
4	security_group	security.group (安全组)	-	sg-bp14qiobeqajnxaimvco	运行中	2021-11-30 17:13:51	定位
5	ecs02	ecs (云服务器ECS)	按量付费	i-bp1a124nivpthp18u08m	运行中	2021-11-30 17:14:09	定位
6	ecs01	ecs (云服务器ECS)	按量付费	i-bp10hi7xsurnyz3k93cw	运行中	2021-11-30 17:14:09	定位
7	havip	havip (高可用虚拟IP)	按量付费	havip-bp1f7m53c08xil5yy061c	运行中	2021-11-30 17:13:52	定位

**部署概要**

状态: 部署成功 订单编号: 211714115070125  
方案编号: N1SRJ8W46TLAGAQR

[查看报告](#) [返回](#)

## 5.8.4.验证过程

本验证过程将在 ECS01 上部署 Apache 和 keepalived 服务，在 ECS02 上部署 nginx 和 keepalived 服务，模拟 HaVIP 切换场景，当 ECS01 出现故障，通过 HaVIP 访问到的服务为 Nginx，同样当 ECS02 出现故障，通过 HaVIP 访问到的服务为 Apache。

步骤 1 打开架构图中的**资源清单**，单击 havip，跳转到 havip 控制台。



步骤 2 资源创建成功，并关联两个 ECS。此时两个 ECS 都处于“备”状态。

**基本信息**

ID	havip-bp1f7m53c08xil5yy061c <a href="#">复制</a>	状态	<span style="color: green;">✓ 已分配</span>
地域	华东1 (杭州)	私网IP	192.168.0.220 <a href="#">复制</a>
专有网络ID	vpc-bp1g2g8bxqbydx3gu1ip <a href="#">复制</a>	创建时间	2021年11月30日17:13:47
交换机	vsw-bp1amzrwy01o7qpgovttt <a href="#">复制</a>	描述	<a href="#">编辑</a>

**绑定资源**

```

graph TD
    EP1[弹性公网IP  
116.62.125.183] --- HAVIP[havip-bp1f7m53c08xil5yy061c]
    EP2[高可用虚拟IP  
192.168.0.220 (私网)] --- HAVIP
    HAVIP --- ECS1[ECS实例 (备)  
i-bp1ohi7xsumyz3k93cw  
运行中]
    HAVIP --- ECS2[ECS实例 (备)  
i-bp1a124nivpthp18u08m  
运行中]
  
```

步骤 3 单击其中一个 ECS，进入 ECS 控制台。单击远程连接。

**ECS 云服务器**

**概览**

**事件** 1

**标签**

**自助问题排查**

**发送命令/文件 (云助手)**

**应用管理** NEW

**我的常用**

- 实例** (1)
- 安全组
- 镜像
- 快照
- 云盘

**云服务器 ECS / 实例 / 实例详情**

**ecs01**

**基本信息**

实例ID	i-bp1ohi7xsumyz3k93cw	地域
资源组:	-	所在可用区
公网IP	-	绑定弹性IP
安全组	sg-bp14qiobeqajnxaimvco	主机名
标签	-	加入安全组
描述	-	创建时间
		<a href="#">修改实例描述</a>

**操作**

- 远程连接** (1)
- 监控
- 安全组
- 云盘
- 实例快照
- 快照
- 弹性网卡
- 远程命令

步骤 4 单击 VNC 远程连接：立即登录



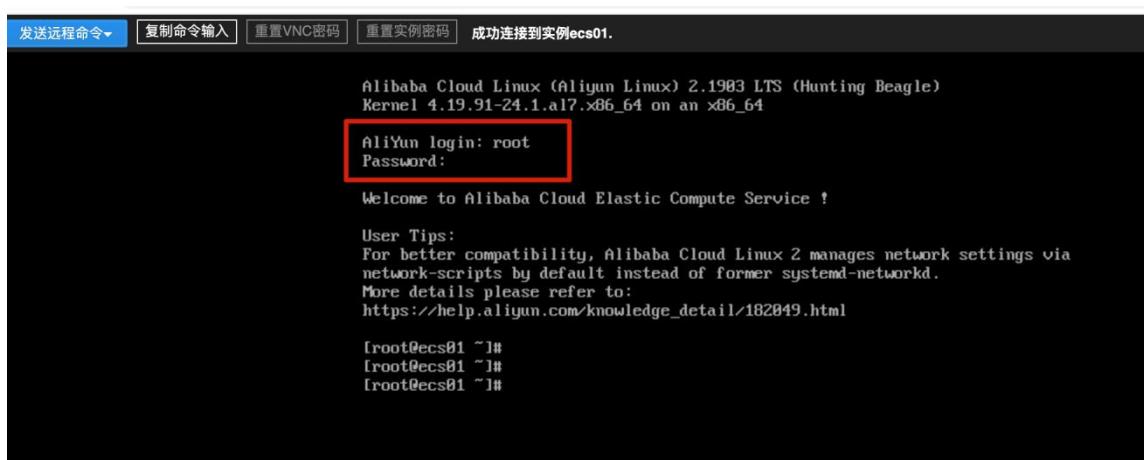
步骤 5 重置 VNC 密码。



## 步骤 6 重置后登录 VNC



## 步骤 7 在 VNC 中用 root 用户密码登录 OS



## 步骤 8 安装 apache 服务，keepalived 服务。

```
yum install -y httpd  
yum install -y keepalived
```

```
[root@ecs01 ~]#  
[root@ecs01 ~]# yum install -y httpd_  
  
[root@ecs01 ~]#  
[root@ecs01 ~]#  
[root@ecs01 ~]# yum install -y keepalived
```

步骤 9 配置 /etc/keepalived/keepalived.conf 文件，配置后如下图所示：

```
[root@ecs01 ~]# cat /etc/keepalived/keepalived.conf
! Configuration File for keepalived

global_defs {
    notification_email {
        acassen@firewall.loc
        failover@firewall.loc
        sysadmin@firewall.loc
    }
    notification_email_from Alexandre.Cassen@firewall.loc
    smtp_server 192.168.200.1
    smtp_connect_timeout 30
    router_id LVS_DEVEL
    vrrp_skip_check_adv_addr
    # vrrp_strict
    vrrp_garp_interval 0
    vrrp_gna_interval 0
}

vrrp_instance VI_1 {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    virtual_ipaddress {
        192.168.0.220
    }
    unicast_src_ip 192.168.0.11
    unicast_peer {
        192.168.0.12
    }
    track_interface {
        eth0
    }
}
[root@ecs01 ~]#
```

步骤 10 启动 apache 和 keepalived 服务

```
systemctl start httpd
systemctl start keepalived
```

```
[root@ecs01 ~]#
[root@ecs01 ~]#
[root@ecs01 ~]#
[root@ecs01 ~]# systemctl start httpd
[root@ecs01 ~]# systemctl start keepalived
[root@ecs01 ~]#
```

步骤 11 同样方式通过 VNC 登录 ECS02，安装 nginx，keepalived 服务。

```
yum install -y nginx  
yum install -y keepalived
```

```
[root@ecs02 ~]#  
[root@ecs02 ~]#  
[root@ecs02 ~]# yum install -y nginx  
  
[root@ecs02 ~]#  
[root@ecs02 ~]#  
[root@ecs02 ~]# yum install -y keepalived _
```

步骤 12 配置 /etc/keepalived/keepalived.conf 文件，配置后如下

```
[root@ecs02 ~]#  
[root@ecs02 ~]# cat /etc/keepalived/keepalived.conf  
! Configuration File for keepalived  
  
global_defs {  
    notification_email {  
        cassen@firewall.loc  
        failover@firewall.loc  
        sysadmin@firewall.loc  
    }  
    notification_email_from Alexandre.Cassen@firewall.loc  
    smtp_server 192.168.200.1  
    smtp_connect_timeout 30  
    router_id LVS_DEVEL  
    vrrp_skip_check_adv_addr  
    # vrrp_strict  
    vrrp_garp_interval 0  
    vrrp_gna_interval 0  
}  
  
vrrp_instance VI_1 {  
    state MASTER  
    interface eth0  
    virtual_router_id 51  
    priority 100  
    advert_int 1  
    authentication {  
        auth_type PASS  
        auth_pass 1111  
    }  
    virtual_ipaddress {  
        192.168.0.220  
    }  
    unicast_src_ip 192.168.0.12  
    unicast_peer {  
        192.168.0.11  
    }  
    track_interface {  
        eth0  
    }  
}  
  
[root@ecs02 ~]# _
```

步骤 13 启动 nginx 和 keepalived 服务

```
systemctl start nginx  
systemctl start keepalived
```

```
[root@ecs02 ~]#  
[root@ecs02 ~]# systemctl start nginx  
[root@ecs02 ~]# systemctl start keepalived  
[root@ecs02 ~]#
```

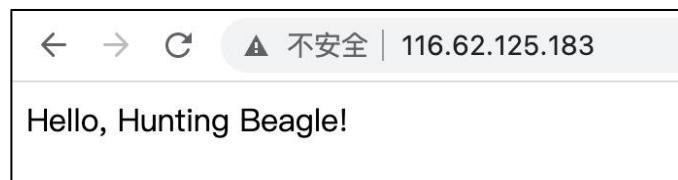
步骤 14 在 ECS01/02 中，通过 curl 命令查看服务状态

```
curl <havip>
```

```
[root@ecs01 ~]#  
[root@ecs01 ~]# curl 192.168.0.220  
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
<html>  
<head>  
<title>Welcome to Aliyun Linux</title>  
</head>  
<body>  
<p>Hello, Hunting Beagle!</p>  
</body>  
</html>  
[root@ecs01 ~]#  
[root@ecs02 ~]# curl 192.168.0.220  
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">  
<html>  
<head>  
<title>Welcome to Aliyun Linux</title>  
</head>  
<body>  
<p>Hello, Hunting Beagle!</p>  
</body>  
</html>  
[root@ecs02 ~]# _
```

两个节点看到的都是 ECS02 上的 Nginx 服务页面。

步骤 16 通过浏览器访问 EIP



步骤 16 在 ECS02 中停掉 keepalived，在通过 curl 查看服务状态。此时服务切换到了 ECS01 上的 apache 服务页面。

```
[root@ecs02 ~]# 
[root@ecs02 ~]# systemctl stop keepalived
[root@ecs02 ~]# 
[root@ecs02 ~]# curl 192.168.0.220
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml11.dtd"><html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <title>Apache HTTP Server Test Page powered by Aliyun Linux</title>
<body>
<p>Hello Apache</p>
</body></html>
[root@ecs02 ~]# 
[root@ecs01 ~]# curl 192.168.0.220
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml11.dtd"><html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
    <title>Apache HTTP Server Test Page powered by Aliyun Linux</title>
<body>
<p>Hello Apache</p>
</body></html>
[root@ecs01 ~]#
[root@ecs01 ~]#
```

步骤 17 通过浏览器访问 EIP



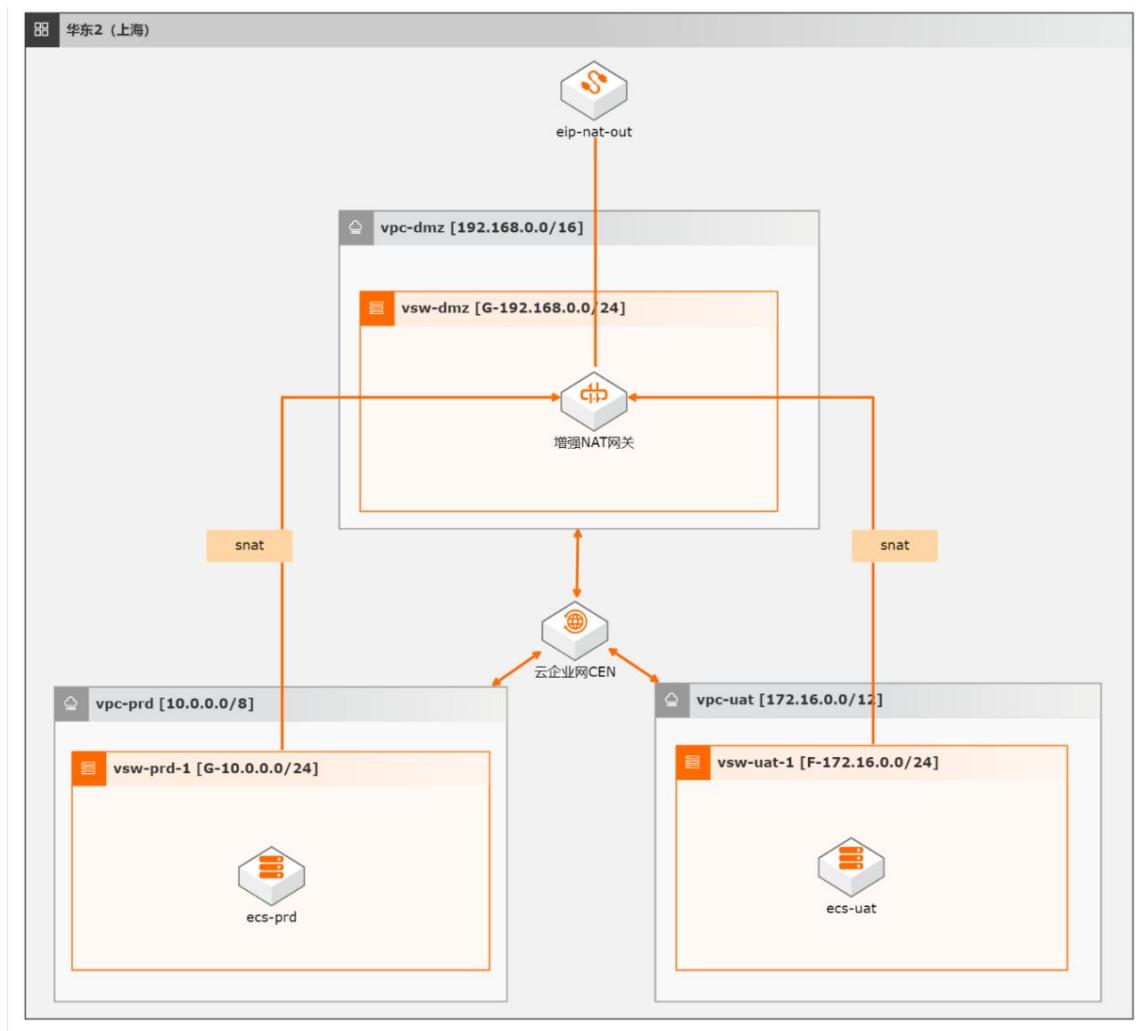
## 5.9.单账号跨 VPC 共享 NAT 网关

作者 | 阿里云解决方案架构师 七凌

### 5.9.1. 云速搭 CADT 架构设计

#### 方案架构

通过云速搭 CADT 设计同账号不同 VPC 共享 NAT 网关的组网架构，大致实现的架构如下图所示：通过云企业网 CEN 连接不同 VPC，然后通过配置 SNAT，让多个 VPC 可以共享同一个增强型 NAT 网关，统一通过 NAT 做流量出口。



## 理解资源级别

每个阿里云资源都有资源级别，本架构中使用的资源如下表所示，这些架构级别在进行架构设计时需要用到。

云资源	架构级别
VPC	Region 地域
CEN	全局资源
ECS	vswitch 交换机
NAT	VPC 专有网络
EIP	Region 地域

## 5.9.2.CADT 部署单账户跨 VPC 共享 NAT 网关

### 设计过程

步骤 1 访问 <https://bpstudio.console.aliyun.com/>，登录云速搭 CADT 控制台。

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 2 目前 CADT 已将“单账户跨 VPC 共享 NAT 网关”定制成官方模板，您可以直接使用。在 CADT 控制台单击新建 > 官方模板库新建。



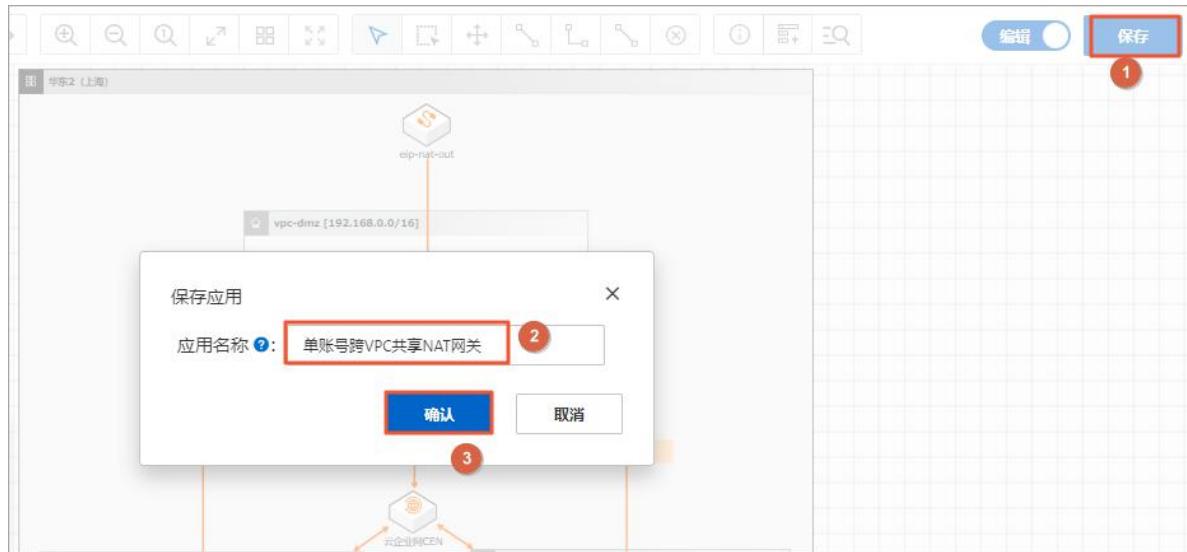
步骤 3 通过搜索关键字找到“同账号跨 VPC 共享 NAT 网关”模板，单击**基于应用新建**。



步骤 4 需要设置模板中 ECS 资源的登录密码，其他资源参数您可以根据实际需求配置。本示例作为演示，使用模板默认参数。



步骤 5 设置 ECS 登录密码后，单击右上角的保存，并设置应用名称。



## 部署过程

步骤 1 保存后单击部署应用，系统将对资源配置进行校验。根据提示修改错误信息，若校验成功，单击下一步：价格清单。

**资源验证**

序号	资源名称	资源类型	区域	规格	结果	备注	操作
1	vsw-dmz [G-192.168.0.0/24]	vswitch	上海	192.168.0.0/24	成功	校验通过	定位
2	vpc-uat [172.16.0.0/12]	vpc	上海	172.16.0.0/12	成功	校验通过	定位
3	ecs-prd	ecs	上海	ecs.c6.large	成功	校验通过	定位
4	vsw-uat-1 [F-172.16.0.0/24]	vswitch	上海	172.16.0.0/24	成功	校验通过	定位
5	vpc-dmz [192.168.0.0/16]	vpc	上海	192.168.0.0/16	成功	校验通过	定位
6	ecs-uat	ecs	上海	ecs.c6t.large	成功	校验通过	定位

状态: **校验成功**

**下一步: 价格清单** **返回**

步骤 2 在导出价格清单对话框中，可以单击**查看报告**得到一份报价清单；单击**下一步：确认订单**。

**导出价格清单**

**免费** **按量付费**

**资源成本占比**

资源预算

- 计算 计算: ... 元/时
- 网络 网络: ... 元/时

**价格列表**

序号	资源名称	资源类型	区域	规格	数量	原价	优惠	实付	状态	操作
1	云企业网CEN	cen			1				新购	定位
2	eip-nat-out	eip	上海	BGP	1	... 元/时	省 ... 元/时	... 元/时	新购	定位
3	ecs-uat	ecs	上海	ecs.c6t.large	1	... 元/时	省 ... 元/时	... 元/时	新购	定位
4	ecs-prd	ecs	上海	ecs.c6t.large	1	... 元/时	省 ... 元/时	... 元/时	新购	定位

状态: **计价成功**

**上一步: 资源校验** **查看报告** **下一步: 确认订单**

步骤 3 勾选《云速搭服务条款》，确认价格后，单击**下一步：支付并创建**。

**确认订单**

免费	按量付费							
序号	资源名称	资源类型	区域	规格	数量	原价	实付	状态
1	增强NAT网关	nat	上海		1	元/时	元/时	新购
2	ecs-prd	ecs	上海	ecs.c6.large	1	元/时	元/时	新购
3	ecs-uat	ecs	上海	ecs.c6t.large	1	元/时	元/时	新购
4	eip-nat-out	eip	上海	BGP	1	元/时	元/时	新购
5	云企业网CEN	cen			1			新购

《云速搭服务条款》  
部署前, 请阅读并勾选服务条款

按量付费: **元/时**

状态: **计价成功**

[上一步: 价格清单](#) [下一步: 支付并创建](#)

步骤 4 等待资源部署完成, 部署过程为后台调用进程。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
 部署中, 不要进行任何操作, 请耐心等待...							

每页显示  共0条 < 上一页  下一页 >

**部署概要**

状态: 部署中 应用编号: W5CW0MY7OTCR10G8

[返回](#)

步骤 5 部署成功。

**资源部署状态**

序号	资源名称	资源类型	付费类型	资源ID	资源状态	资源更新时间	定位
1	默认安全组	security.group (安全组)	-	sg-uf6infwmwzaj1d9mqbei	运行中	2022-01-12 17:07:34	定位
2	ecs-prd	ecs (云服务器ECS)	按量付费	i-uf66ddu4v4ykndmqyeza	运行中	2022-01-12 17:08:00	定位
3	vpc-dmz [192.168.0.0/16]	vpc (专有网络VPC)	-	vpc-uf6nzwsysao3g8uoztglm	运行中	2022-01-12 17:07:33	定位
4	vsw-dmz [G-192.168.0.0/24]	vswitch (虚拟交换机)	-	vsw-uf6bfy8jvg5osnlly0um	运行中	2022-01-12 17:07:34	定位
5	vpc-prd [10.0.0.0/16]	vpc	-	vpc-uf6nukkkkn02o3he0vh45a	运行中	2022-01-12 17:07:33	定位

每页显示 10 共13条 < 上一页 1 2 下一页 >

**部署概要**

状态: 部署成功 订单编号 : 212524375630833, 212525664470833  
应用编号: W5CW0MY7OTCRI0G8

查看报告 返回

### 5.9.3.验证过程

步骤 1 展开应用下的**资源清单**, 单击 CEN 实例 “云企业网 CEN”, 跳转到 CEN 控制台。

The screenshot shows the network topology for the CEN instance "云企业网 CEN". It includes three VPCs: vpc-dmz [192.168.0.0/16], vsw-dmz [G-192.168.0.0/24], and vpc-prd [10.0.0.0/16]. A NAT gateway is connected to the vpc-dmz VPC. Two SNAT rules are applied to the interface connecting the vpc-dmz VPC to the NAT gateway. A red circle labeled "1" points to the "资源清单" (Resource List) button at the bottom of the interface. Another red circle labeled "2" highlights the CEN instance name "云企业网 CEN".

应用操作	导出资源清单						
序号	资源名称	资源类型	付费类型	资源ID	来源	资源状态	资源更新时间
9	云企业网CEN	cen (云企业网)	按量付费	cen-oz6jcb3ifktg0rn2x	新建	运行中	2022-01-12 17:06:54
10	vpc-uat [172.16.0.0/12]	vpc (专有网络VPC)	免费	vpc-uf6j0d4lg027911yetj1w	新建	运行中	2022-01-12 17:07:33

步骤 2 可以看到, CEN 实例加载了 3 个 VPC。

**← cen-oz6jcb3ifiktg0rn2x**

基本信息	资源拓扑	监控图表			
转发路由器 1	带宽包总量 0Mbps	已分配带宽 0Mbps	VPC 3个	VBR 0个	CCN 0个
<b>基本信息</b>					
ID cen-oz6jcb3ifiktg0rn2x 复制	名称 云企业网CEN				
描述 	状态 可用				
标签 	重叠路由功能 已开启				
<a href="#">转发路由器</a> <a href="#">带宽包管理</a>					
<a href="#">创建转发路由器</a> <input type="text" value="请输入名称、实例ID进行模糊搜索"/>					
实例ID/名称 tr-uf621mutmbee17gxa8q04	地域 华东2 (上海)	版本 基础版  立即升级	状态 可用	连接数量 3	路由表 1
创建时间 2022年1月12日 17:08:00	描述 	操作 <a href="#">创建网络实例连接</a>			

**← cen-oz6jcb3ifiktg0rn2x**

基本信息	资源拓扑	监控图表			
转发路由器 1	带宽包总量 0Mbps	已分配带宽 0Mbps	VPC 3个	VBR 0个	CCN 0个
<b>基本信息</b>					
ID cen-oz6jcb3ifiktg0rn2x 复制	名称 云企业网CEN				
描述 	状态 可用				
标签 	重叠路由功能 已开启				
<a href="#">转发路由器</a> <a href="#">带宽包管理</a>					
<a href="#">创建转发路由器</a> <input type="text" value="请输入名称、实例ID进行模糊搜索"/>					
实例ID/名称 tr-uf621mutmbee17gxa8q04	地域 华东2 (上海)	版本 基础版  立即升级	状态 可用	连接数量 3	路由表 1
创建时间 2022年1月12日 17:08:00	描述 	操作 <a href="#">创建网络实例连接</a>			

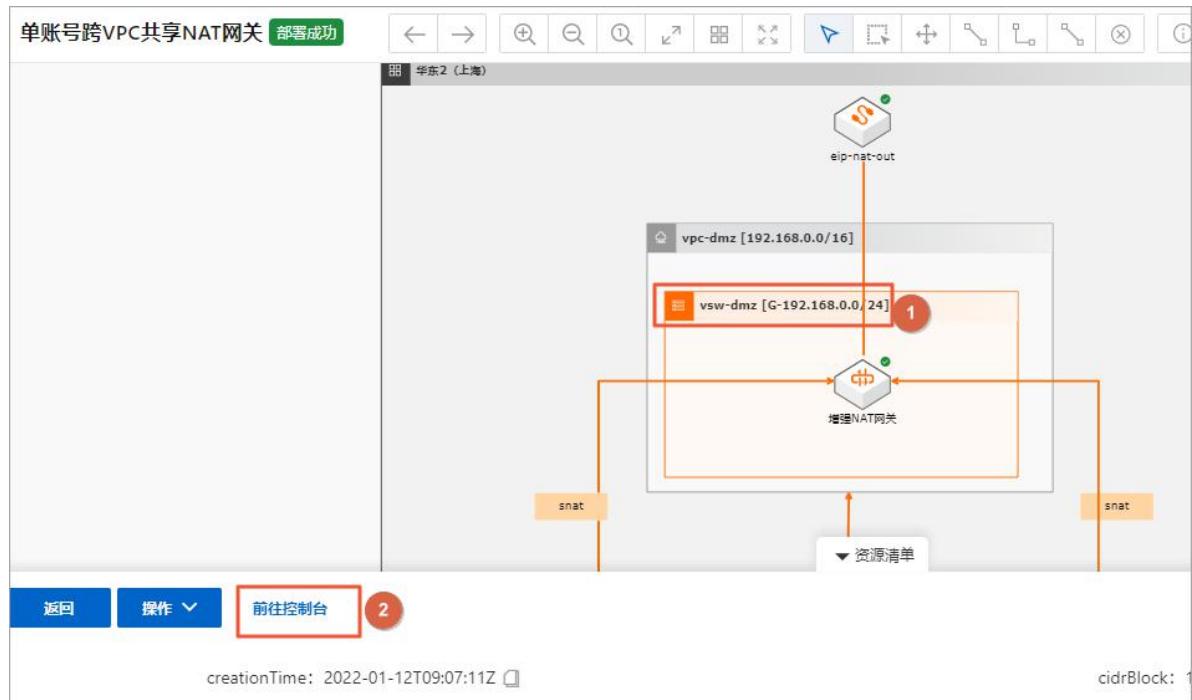
**← tr-uf621mutmbee17gxa8q04(华东2 (上海))** [查看其他实例](#)

基本信息	地域内连接管理	跨地域连接管理	转发路由器路由表	网络实例路由信息	Private Zone
<a href="#">创建网络实例连接</a>					
实例ID/名称 vpc-uf6nzwsyao3g8uoztglmt vpc-dmz	所属地域 华东2 (上海)	实例类型 专有网络 (VPC)	所属账号		
vpc-uf6unkkkpg2o3he0xb45a vpc-prd	华东2 (上海)	专有网络 (VPC)			
vpc-uf6j0d4lg027911yetj1w vpc-uat	华东2 (上海)	专有网络 (VPC)			

步骤3 查看路由信息，此时并没有指向增强型 NAT 网关的路由条目。

← tr-uf621mutmbee17gxa8q04(华东2 (上海)) <a href="#">查看其他实例</a>						
基本信息	地域内连接管理	跨地域连接管理	转发路由器路由表	网络实例路由信息	Private Zone	访问云服务
路由条目	路由策略					
请输入目标网段	<input type="button" value=""/>	TR路由数量/上限: 3/100 <a href="#">申请更多路由上限</a>				
目标网段	下一跳	类型	路由类型	状态	匹配策略	路由属性
10.0.0.0/24	vpc-uf6unkkkpg2o3he0xb45a	VPC	云企业网	可用	-	<a href="#">查看详情</a>
172.16.0.0/24	vpc-uf6j0d4lg027911yetj1w	VPC	云企业网	可用	-	<a href="#">查看详情</a>
192.168.0.0/24	vpc-uf6nzwsyao3g8uoztglmt	VPC	云企业网	可用	-	<a href="#">查看详情</a>

步骤4 回到 cadt 架构图界面，双击 vsw-dmz，然后单击前往控制台。



步骤5 将指向增强型 NAT 网关的路由发布到云企业网 CEN。

**← vsw-uf6bfy8vvg5osnly0um**

**交换机基本信息**

交换机ID	vsw-uf6bfy8vvg5osnly0um 复制	专有网络ID	vpc-uf6nzwsysao3g8uoztglmt 复制
名称	vsw-dmz 编辑	可用IP数	251
IPv4网段	192.168.0.0/24	默认交换机	否
标签	无	IPv6网段	开通IPv6
状态	✓ 可用	创建时间	2022年1月12日 17:07:11
可用区	上海 可用区G	描述	- 编辑
网络ACL	绑定	拥有者	当前账户

云资源管理 路由管理 ①

已绑定路由表:  
vtb-uf69htt3u0wo3h96xw1z / vsw-dmz (系统) 绑定

系统 动态 自定义 ②

添加自定义路由条目

目标网段	状态	下一跳	类型	描述	CEN中状态
0.0.0.0/0	✓ 可用	ngw-uf6918daukmkrhnu4ru62 ③ 删除	自定义	Created with NAT gateway(ngw-uf6918daukmkrhnu4ru62) by system.	未发布 ④ 发布

❓ 发布路由  
你确定要发布路由: 0.0.0.0/0到云企业网:cen-oz6jcb3ifiktg0rn2x中吗?  
说明: 路由一旦发布, 云企业网中的其他网络实例便可学习到该路由并进行访问

确定 取消

步骤 6 几秒钟后, 刷新页面, 确保路由已经发布到 CEN。

**← vsw-uf6bfy8vvg5osnly0um**

**交换机基本信息**

交换机ID	vsw-uf6bfy8vvg5osnly0um 复制	专有网络ID	vpc-uf6nzwsysao3g8uoztglmt 复制
名称	vsw-dmz 编辑	可用IP数	251
IPv4网段	192.168.0.0/24	默认交换机	否
标签	无	IPv6网段	开通IPv6
状态	✓ 可用	创建时间	2022年1月12日 17:07:11
可用区	上海 可用区G	描述	- 编辑
网络ACL	绑定	拥有者	当前账户

云资源管理 路由管理

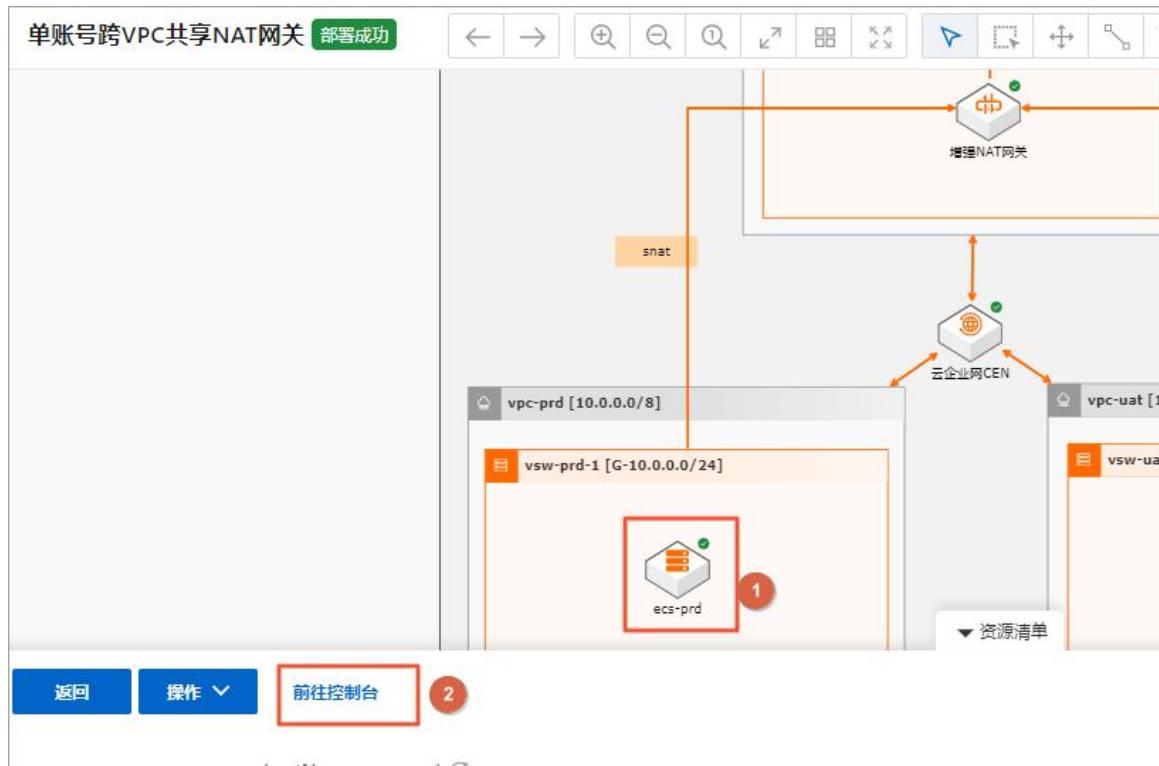
已绑定路由表:  
vtb-uf69htt3u0wo3h96xw1z / vsw-dmz (系统) 绑定

系统 动态 自定义

添加自定义路由条目

目标网段	状态	下一跳	类型	描述	CEN中状态	操作
0.0.0.0/0	✓ 可用	ngw-uf6918daukmkrhnu4ru62 ③ 删除	自定义	Created with NAT gateway(ngw-uf6918daukmkrhnu4ru62) by system.	已发布 ④ 编辑	删除

步骤 7 进入其中一台 ECS 控制台，单击远程连接。



The screenshot shows the "ecs-prd" instance details page. The top navigation bar includes tabs for 实例详情, 监控, 安全组, 云盘, 快照一致性组, 快照, 弹性网卡, 远程命令/文件, 操作记录, and 健康诊断. The "实例详情" tab is active. The main content area displays basic information about the instance, including:

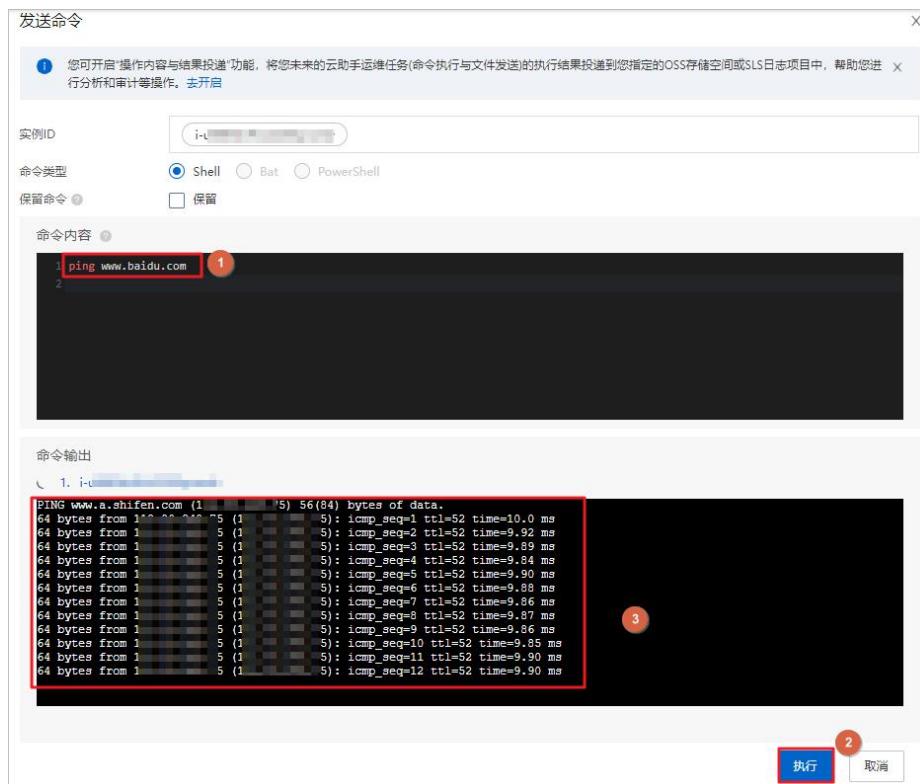
- 状态: 运行中
- 实例ID: i-uf66ddu4v4ykndmquyeza
- 资源组: -
- 公网IP: -
- 安全组: sg-uf6infgmwzaj1d9mqbei
- 描述: -
- 地域: 华东2 (上海)

On the right side, there are three buttons: 绑定弹性IP, 加入安全组, and 修改实例描述. A prominent blue button labeled "远程连接" (Remote Connection) is highlighted with a red box.

步骤 8 测试位于 vpc-prd 的 ecs，能否通过位于 vpc-dmz 的增强型 NAT 网关访问外网。



如下图所示，位于 vpc-prd 的 ecs，可以通过位于 vpc-dmz 的增强型 NAT 网关访问外网：



步骤 9 按同样方式，测试另一台 ECS 能否通过增强型 NAT 网关访问外网。

# 6.云速搭权限管理及场景设计

作者 | 阿里云解决方案架构师 天襄

## 6.1.前置条件

执行本文操作之前，请完成以下准备工作：

- 注册阿里云账号，并完成实名认证。您可以登录阿里云控制台，并前往实名认证页面（<https://account.console.aliyun.com/v2/#/authc/home>）查看是否完成实名认证。
- 如果有购买按量付费资源，阿里云账户余额需要大于 100 元。您可以登录阿里云控制台，并前往账户总览页面（<https://expense.console.aliyun.com/#/account/home>）查看账户余额。
- 已开通 VPC、ECS、CADT、RAM 和资源管理等服务。
- 最佳实践中使用的自定义权限脚本，请从以下链接下载使用：  
<https://code.aliyun.com/best-practice/253.git>

## 6.2. 云速搭权限管理概述

### 实践概述

在大型企业中，由于组织架构、技术架构和项目管理等方面的复杂性，通常需要对云上资源的使用权限做精细化管理。本实践以一个真实的业务需求为背景，来介绍如何对 CADT 上的应用和模板进行权限管控。

### 解决问题

- 企业 IT 治理安全合规要求严密的权限管控策略
- 通过权限的隔离来降低资源风险
- 方便运维人员精确定位职责范围内的资源，简化操作，提升云上体验。

### 方案优势

- CADT 原生支持阿里云 RAM 权限管控体系，无需额外学习成本。
- 预定义的角色分工明确，配置便捷。
- 支持自定义权限策略，适配丰富业务场景。

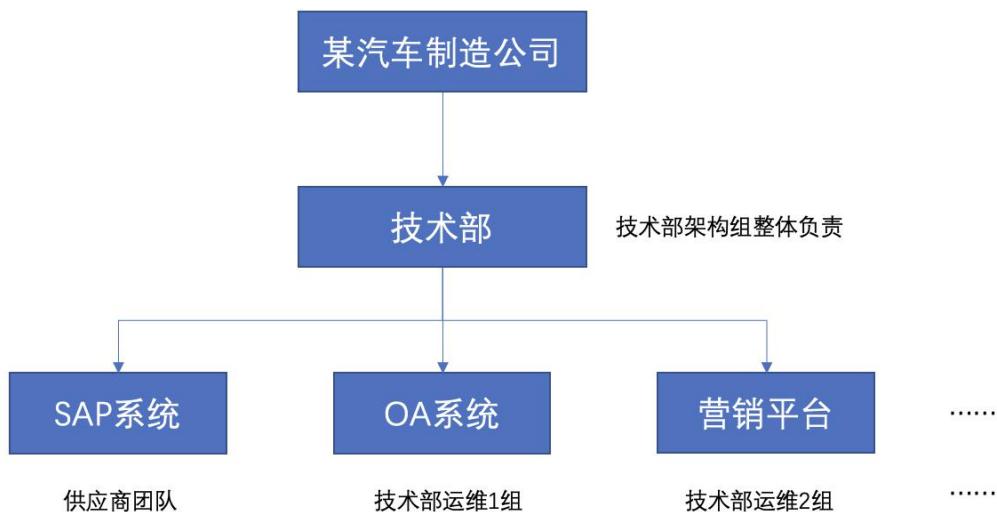
## 6.3.权限管理场景设计

本章节通过一个企业 IT 管理场景，来介绍如何针对性地设计 CADT 的权限管控策略。

### 6.3.1.企业 IT 管理场景

某汽车制造公司的 IT 部门，负责运维 SAP 系统、OA 系统等多个项目。

- 技术部架构组对公司整体技术方案和基础资源负责，规划、管理全部 IT 资源；
- OA 系统由技术部运维 1 组负责；
- 营销平台由技术部运维 2 组负责；
- SAP 系统由外部供应商团队负责运维；  
(其他项目在此不一一举例)



### 6.3.2.设计权限管控策略

使用 CADT 管理云上资源，需要考虑两个方面的权限管控：

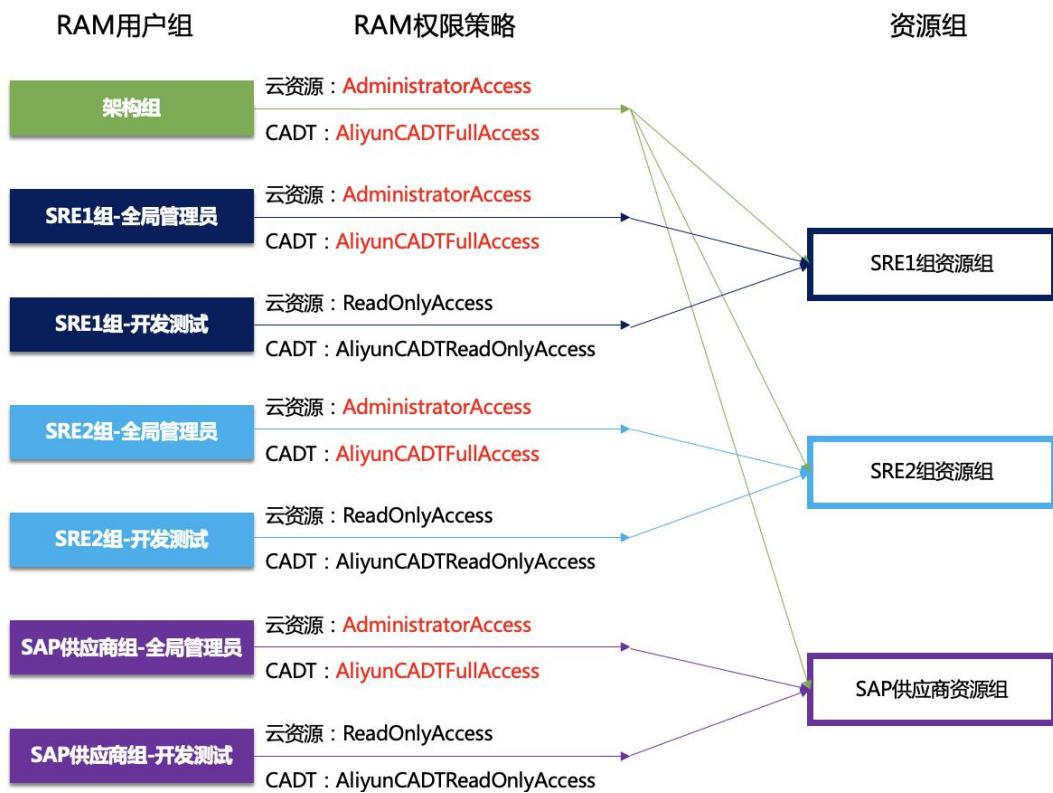
- **对 CADT 产品的使用权限：**授权用户使用 CADT 产品，并限制用户具有哪些 CADT 应用和模板的权限。  
但仅有 CADT 应用和模板的权限还不能操作资源，用户还需要云上资源的操作权限。

- 云上资源的权限：**要查看、创建或修改某一类资源，用户需要具备该资源对应的 RAM 权限。  
(RAM 的使用请参考 [RAM 账号权限管理最佳实践](#))
- 根据[企业 IT 管理场景](#)中的项目架构，我们设计角色权限如下：
- 技术部架构组拥有全局管理员权限，对阿里云上全部资源、CADT 应用和模板具有管理权限。
- 其他各组成员根据所属的组，仅能访问归属于本组的 CADT 应用和云上资源，做到资源和权限隔离。各组内角色分工如下：
  - 全局管理员：拥有组内最高管理权限。
  - 管理员：为防止误操作，进一步降低资源风险，不可使用一键释放功能。但为满足日常运维需求，可以在架构图中逐个删除资源。**(该能力开发中，未来计划支持资源变更审批，本例暂不涉及管理员角色的配置)**
  - 研发和测试：对 CADT 应用和阿里云上应用仅有查看权限，查看 ECS IP 地址，主机名，RDS 数据库地址等信息，用做日常开发测试工作。

组	角色	阿里云资源		CADT应用/模板				
		增/删/改	查看	创建应用/ 模板	删除应用/ 模板	查看应用/ 模板	变更（新增/删除）应用内资源/ 编辑模板	一键释放
架构组	全局管理员	Y	Y	Y	Y	Y	Y	Y
运维1组	全局管理员	Y	Y	Y	Y	Y	Y	Y
	管理员（暂未支持）	Y	Y	Y	Y	Y	Y	
	研发和测试		Y			Y		
运维2组	全局管理员	Y	Y	Y	Y	Y	Y	Y
	管理员（暂未支持）	Y	Y	Y	Y	Y	Y	
	研发和测试		Y			Y		
SAP供应商组	全局管理员	Y	Y	Y	Y	Y	Y	Y
	管理员（暂未支持）	Y	Y	Y	Y	Y	Y	
	研发和测试		Y			Y		

### 6.3.3. 权限管控策略实现

为实现上一章节中的权限管控策略，我们主要需要使用两个阿里云的产品能力：[访问控制\(RAM\)](#) 和 [资源组](#)。RAM 的详细使用指导请参考《[RAM 账号权限管理最佳实践](#)》，资源组的详细使用指导请参考《[资源管理最佳实践](#)》。



## 资源组

用于对云上资源进行分组管理，在对用户授权中，可依据资源组划定权限的边界。

- **资源分组：**根据权限策略，我们将云上资源划分为三个资源组
  - 运维 1 组资源组
  - 运维 2 组资源组
  - SAP 供应商资源组
 架构组有云上全部资源的权限，所以没有单独划分资源组。
- **通过资源组管理 CADT 应用和模板：** CADT 的应用和模板也是一种资源，也可以通过加入资源组的方式，来完成对特定用户组的授权。

## 访问控制（RAM）

RAM 是阿里云提供的管理用户身份与资源访问权限的服务。

- **用户分组：**我们根据用户角色创建六个 RAM 用户组

- 运维 1 组-全局管理员
- 运维 1 组-开发测试
- 运维 2 组-全局管理员
- 运维 2 组-开发测试
- SAP 供应商组-全局管理员
- SAP 供应商组-开发测试

用户根据身份加入各组，再根据权限策略，对各个组授权。通过资源组和用户组的方式管理权限，将大大降低管理难度。

- **CADT 工具的访问权限：**目前 CADT 支持管理（AliyunCADTFullAccess），和只读（AliyunCADTReadOnlyAccess）两个系统权限策略。只读权限可以查看，创建架构图，但不能保存架构图和部署资源。在本例中，我们为全局管理员组授予 CADT 的管理权限，为开发测试组授予只读权限。
- **云上资源的访问权限：**本例中为了演示方便，为全局管理员组赋予云上所有资源类型的管理权限（AdministratorAccess），为开发测试组授予云上所有资源的只读权限（ReadOnlyAccess）。**实际生产中，可以根据管控需要，使用自定义权限策略实现细粒度的权限管控。**

## AdministratorAccess 和 AliyunCADTFullAccess 的补充说明

- 系统权限策略 AdministratorAccess 已经包含了 AliyunCADTFullAccess – 若 RAM 用户有 AdministratorAccess 权限，则不再需要单独授予 AliyunCADTFullAccess。
- 本文为保持前后逻辑简单一致，所以对于管理员角色，同时授予了 AdministratorAccess 和 AliyunCADTFullAccess，不会发生冲突。
- 另外若对管理员删除 AdministratorAccess 权限策略，使用自定义权限策略做更细粒度的权限管控，则需要 AliyunCADTFullAccess 保证对 CADT 的访问权限。

**注意：**ReadOnlyAccess 并没有包含 AliyunCADTReadOnlyAccess。

## 6.4.权限管理策略配置

本章节演示如何在阿里云上操作配置章节 1 中的权限管控策略。

### 6.4.1.创建资源组

步骤 1 登录资源管理控制台，打开资源组页面，单击创建资源组。

(<https://resourcemanager.console.aliyun.com/resource-groups> )



The screenshot shows the AliCloud Resource Management Control Panel. On the left, there's a sidebar with 'Resource Management' and several sub-options: 'Resource Catalog', 'Overview', 'Resource Sharing', 'My Resources', 'Resource Groups' (which is highlighted with a red box and has a red number 1), and 'Tags'. In the main content area, the title 'Resource Groups' is displayed above a message box. The message box contains a welcome note and information about resource groups. Below the message box is a search bar with the placeholder 'Please enter'. At the bottom of the main area, there's a 'Create Resource Group' button, which is also highlighted with a red box and has a red number 2.

步骤 2 为运维 1 组创建资源组。



The screenshot shows a 'Create Resource Group' dialog box. It has two input fields: 'Resource Group Identifier' containing 'sre1' and 'Resource Group Name' containing '运维1组'. Both fields have a red border and a red number 1 or 2 indicating they are required. At the bottom of the dialog box are two buttons: 'Confirm' (highlighted with a red box and red number 3) and 'Cancel'.

步骤3 重复步骤2，为运维2组和SAP供应商组创建资源组。



## 6.4.2. 创建 RAM 用户组

步骤1 登录 RAM 控制台**用户组**页面，单击**创建用户组**。

(<https://ram.console.aliyun.com/groups>)



步骤 2 为架构组创建用户组。

RAM 访问控制 / 创建用户组

## ← 创建用户组

\* 用户组名称  
1 Architect  
最大长度 64 个字符，允许英文字母、数字、.、\_ 或 -。

\* 显示名称  
2 架构组  
最大长度 128 个字符或汉字。

备注  
3 确定 取消

最大长度 128 个字符。



步骤 3 重复步骤 2，为运维 1 组，运维 2 组，SAP 供应商组的管理员和测试开发角色创建对应的 RAM 用户组：

- 运维 1 组-全局管理员
- 运维 1 组-开发测试
- 运维 2 组-全局管理员
- 运维 2 组-开发测试
- SAP 供应商组-全局管理员
- SAP 供应商组-开发测试

<input type="checkbox"/>	用户组名称/显示名称	备注
<input type="checkbox"/>	Architect 架构组	
<input type="checkbox"/>	SAP-Dev SAP供应商组-开发测试	
<input type="checkbox"/>	SAP-GlobalAdmin SAP供应商组-全局管理员	
<input type="checkbox"/>	SRE1-Dev 运维1组-开发测试	
<input type="checkbox"/>	SRE1-GlobalAdmin 运维1组-全局管理员	
<input type="checkbox"/>	SRE2-Dev 运维2组-开发测试	
<input type="checkbox"/>	SRE2-GlobalAdmin 运维2组-全局管理员	

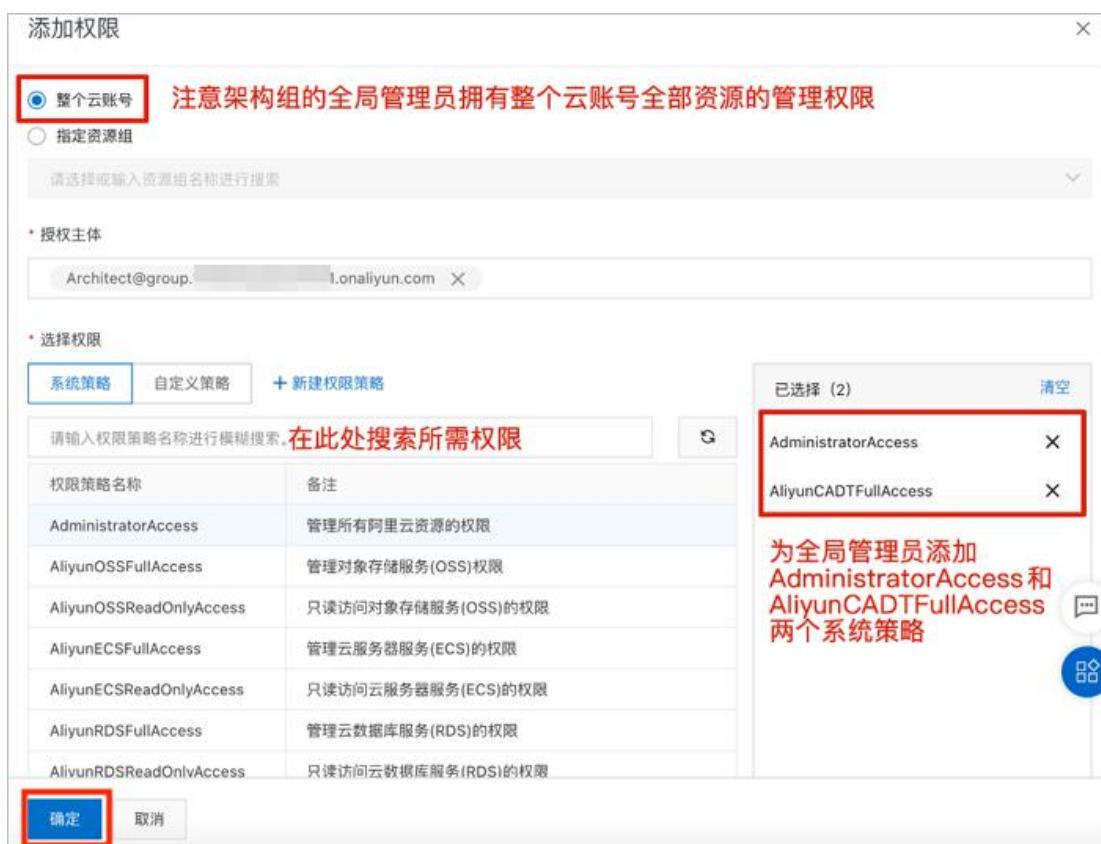
### 6.4.3.为 RAM 用户组授权

首先我们为架构组授权：

步骤 1 在用户组列表中找到架构组，单击添加权限。

用户组			
<p>① 通过用户组对职责相同的 RAM 用户进行分类并授权，可以更加高效地管理用户及其权限。 对一个用户组进行授权后，用户组内的所有用户会自动继承该用户组的权限。 如果一个用户被加入到多个用户组，那么该用户将会继承多个用户组的权限。</p>			
<input type="checkbox"/>	用户组名称/显示名称	备注	创建时间
<input type="checkbox"/>	Architect 架构组	2021年10月25日 10:04: 55	<input type="button" value="添加成员"/> <input style="border: 2px solid red;" type="button" value="添加权限"/> <input type="button" value="删除"/>

步骤 2 为架构组管理员添加 AdministratorAccess 和 AliyunCADCFullAccess 两个系统策略，单击确定。

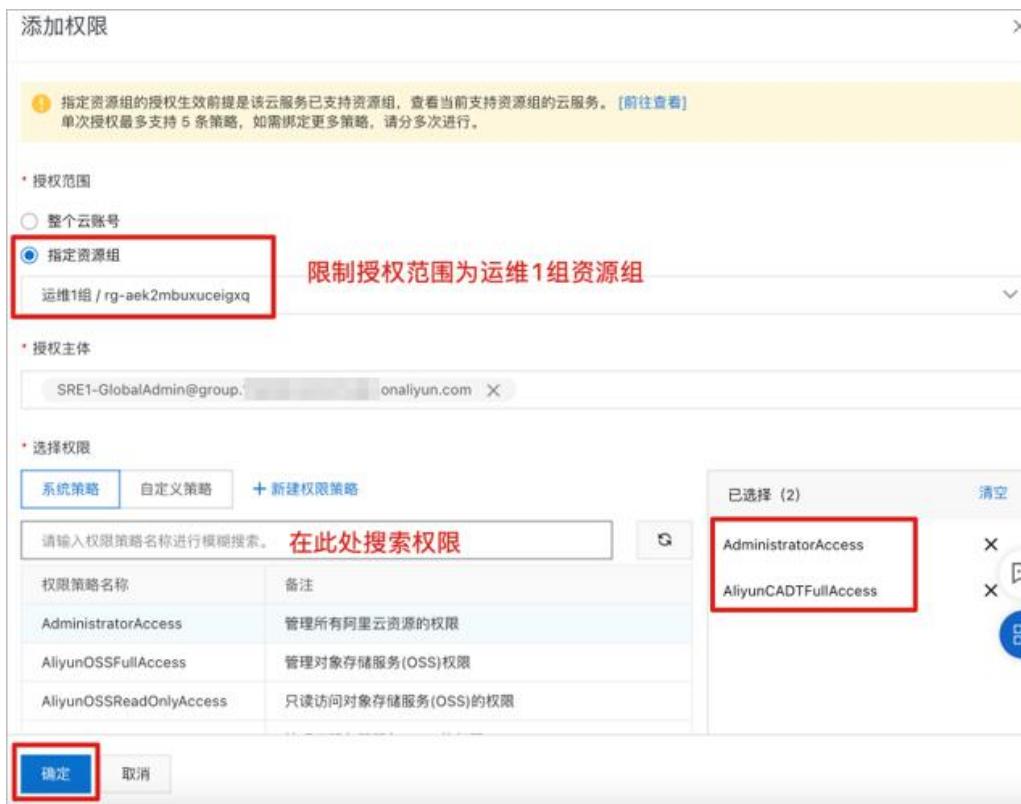


下面我们为运维 1 组全局管理员和开发测试组授权：

步骤 3 在用户组列表中找到运维 1 组-全局管理员，单击后面的添加权限。

Create User Group		Group Name	Search	
	User Group Name / Display Name	Remarks	Creation Time	Action
<input type="checkbox"/>	Architect Architecture		2021-10-25 10:04: 55	Add Member Add Permission Delete
<input type="checkbox"/>	SAP-Dev SAP Supplier Group - Development Test		2021-10-25 10:04: 30	Add Member Add Permission Delete
<input type="checkbox"/>	SAP-GlobalAdmin SAP Supplier Group - Global Administrator		2021-10-25 10:04: 18	Add Member Add Permission Delete
<input type="checkbox"/>	SRE1-Dev SRE1 Group - Development Test		2021-10-25 10:03: 27	Add Member Add Permission Delete
<input type="checkbox"/>	SRE1-GlobalAdmin SRE1 Group - Global Administrator		2021-10-25 10:02: 43	Add Member Add Permission Delete

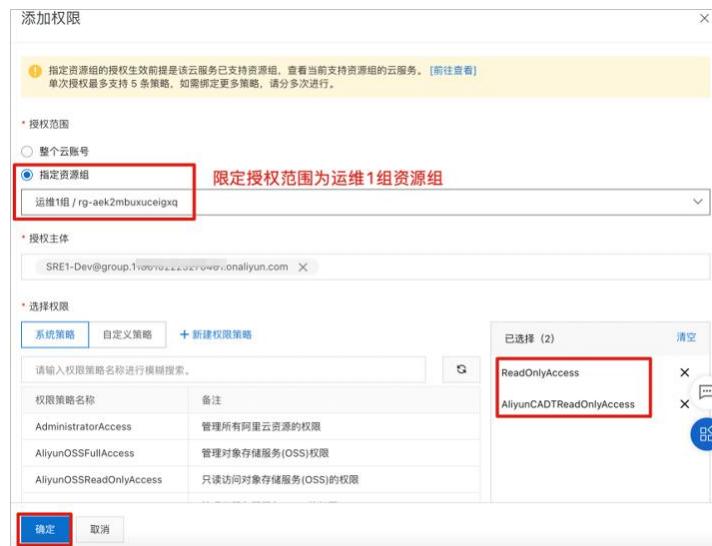
步骤 4 为运维 1 组-全局管理员指定授权范围为运维 1 组资源组，然后添加 AdministratorAccess 和 AliyunCADTFullAccess 两个系统策略，单击确定。



步骤 5 在用户组列表中找到**运维 1 组-开发测试**，单击后面的**添加权限**。

User Groups				
<p>通过用户组对职责相同的 RAM 用户进行分类并授权，可以更加高效地管理用户及其权限。 对一个用户组进行授权后，用户组内的所有用户会自动继承该用户组的权限。 如果一个用户被加入到多个用户组，那么该用户将会继承多个用户组的权限。</p>				
<input type="button" value="Create User Group"/> <input type="text" value="User Group Name"/> <input type="button" value="Search"/>				
User Group Name	Description	Created Time	Operations	
Architect	Architecture Group	2021-10-25 10:04:55	Add Members Add Permissions Delete	<input type="button" value="Add Permissions"/>
SAP-Dev	SAP Supplier Group - Development	2021-10-25 10:04:30	Add Members Add Permissions Delete	<input type="button" value="Add Permissions"/>
SAP-GlobalAdmin	SAP Supplier Group - Global Administrator	2021-10-25 10:04:18	Add Members Add Permissions Delete	<input type="button" value="Add Permissions"/>
SRE1-Dev	运维1组-Development	2021-10-25 10:03:27	Add Members Add Permissions Delete	<input type="button" value="Add Permissions"/>
SRE1-GlobalAdmin	运维1组-Global Administrator	2021-10-25 10:02:43	Add Members Add Permissions Delete	<input type="button" value="Add Permissions"/>

步骤 6 为运维 1 组-开发测试**指定授权范围为运维 1 组资源组**，然后添加 ReadOnlyAccess 和 AliyunCADTReadOnlyAccess 两个系统策略，单击**确定**。



步骤 7 重复步骤 1~4，为剩余的 4 个组授予相应权限。

- 运维 2 组-全局管理员
- 运维 2 组-开发测试
- SAP 供应商组-全局管理员
- SAP 供应商组-开发测试

#### 6.4.4. 创建 RAM 用户并加入用户组

步骤 1 登录 RAM 控制台[用户页面](https://ram.console.aliyun.com/users)，单击[创建用户](#)。（<https://ram.console.aliyun.com/users>）



步骤 2 创建以下 RAM 用户：

**注意：**本例中为了区分方便，直接使用角色名做为 RAM 用户的用户名。实际生产中，请避免此类用法，**应以实际用户的姓名命名 RAM 用户。**

## 用户

RAM 用户是一个身份实体，它通常代表您的组织中需要访问云资源的人员或应用程序。通常的操作步骤如下：

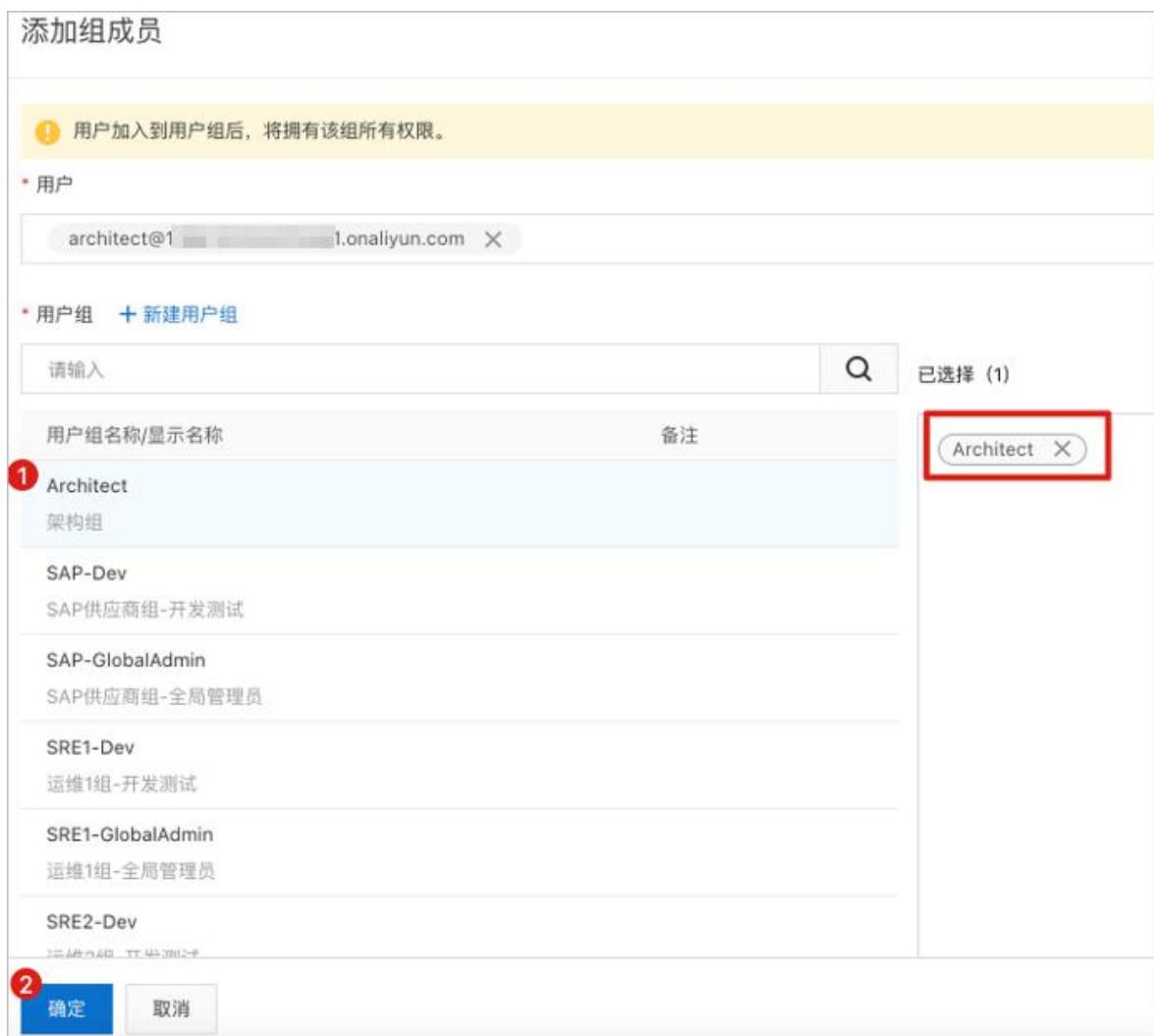
1. 创建用户，并为用户设置登录密码（用户登录控制台场景）或创建 AccessKey（云产品 API 场景）。
2. 添加用户到用户组（需要先创建用户组并完成对用户组的授权）。

创建用户		输入登录名、显示名、用户 ID 或 AccessKey ID
<input type="checkbox"/>	用户登录名称/显示名称	备注
<input type="checkbox"/>	sap-dev@1.1.1.1.onaliyun.com	SAP供应商开发测试
<input type="checkbox"/>	sap-globaladmin@1.1.1.1.onaliyun.com	SAP供应商全局管理员
<input type="checkbox"/>	sre2-dev@1.1.1.1.onaliyun.com	运维2组开发测试
<input type="checkbox"/>	sre2-globaladmin@1.1.1.1.onaliyun.com	运维2组全局管理员
<input type="checkbox"/>	architect@1.1.1.1.onaliyun.com	架构组全局管理员
<input type="checkbox"/>	sre1-globaladmin@1.1.1.1.onaliyun.com	运维1组全局管理员
<input type="checkbox"/>	sre1-dev@1.1.1.1.onaliyun.com	运维1组开发测试

步骤 3 将用户依次加入对应用户组。

这里以架构组全局管理员为例。

<input type="checkbox"/>	sre2-globaladmin@1.1.1.1.onaliyun.com 运维2组全局管理员	添加到用户组 添加权限 删除
<input type="checkbox"/>	architect@1.1.1.1.onaliyun.com 架构组全局管理员	添加到用户组 <b>添加权限</b> 删除
<input type="checkbox"/>	sre1-globaladmin@1.1.1.1.onaliyun.com 运维1组全局管理员	添加到用户组 添加权限 删除



请重复本步骤，将全部 RAM 用户加入到对应用户组。

步骤 4 至此，我们通过 RAM 和资源组，将云上资源的权限授予了用户。

#### 6.4.5.CADT 应用加入资源组

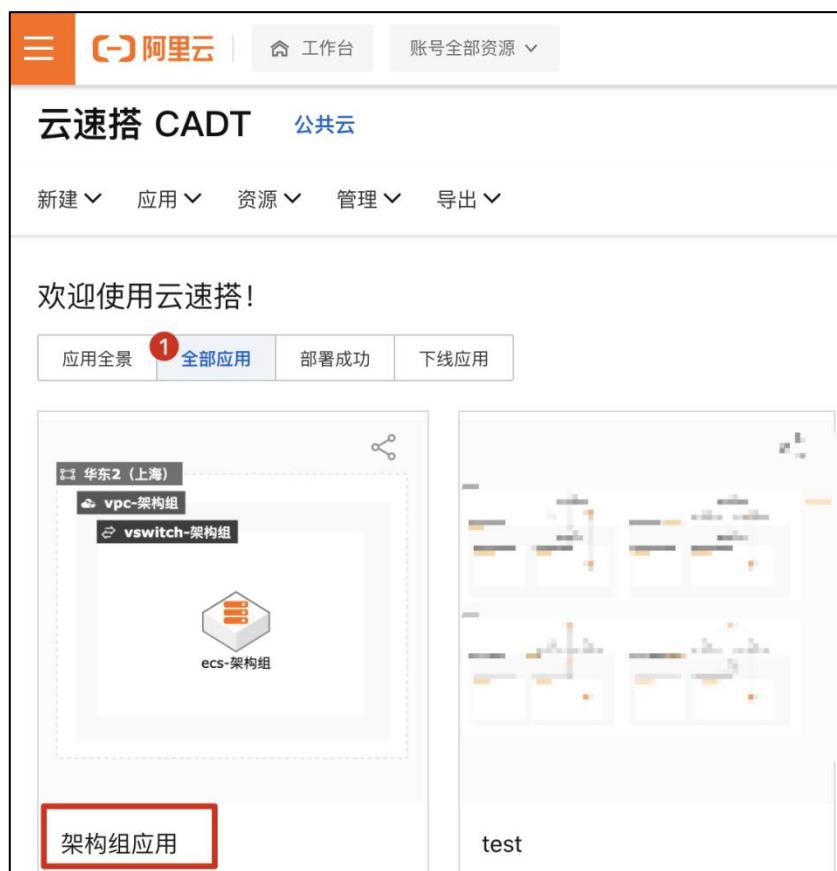
**注意：**只有云账号（主账号）可以使用 CADT 权限管理功能，RAM 账号（子账号）登录 CADT 无法看到权限管控入口。

使用云账号（主账号）登录 CADT 控制台。（<https://bpstudio.console.aliyun.com/>）

**说明：**如果提示需要开通服务，请根据提示进行开通。

步骤 1 在 CADT 主页面单击**全部应用**，本例中架构组已创建了一个 CADT 应用，读者可以用架构组 RAM 用户创建任意 CADT 应用，用于验证授权。

下面我们将该应用授权给运维 1 组。



步骤 2 单击右上角的**权限管理**。（注意只有使用主账号登录才可以看到该功能入口）



步骤 3 定位到运维 1 组资源组，展开授权列表，单击添加授权。

权限管理

1 创建用户 2 创建资源组 3 用户授权 4 资源组授权

资源组名称	资源组Id	资源组唯一标识	状态	创建时间	操作
默认资源组	rg-acfmwwwofpolxepl	default	可用	2020-10-09 17:06:26	<a href="#">管理资源组</a>
运维1组	rg-aek2mbuxuceigxq	sre1	可用	2021-10-24 21:18:41	<a href="#">管理资源组</a>

② 添加授权

步骤 4 找到目标应用“架构组应用”，单击[授权](#)。

添加授权

我的应用

请输入架构名称

批量添加权限

架构Id	架构名称	操作
0Z4FCEDHLLHU9X9	架构组应用	<a href="#">授权</a>

授权成功后，退出授权页面。

步骤 5 在运维 1 组资源组的授权列表中，可以看到完成授权的应用。

权限管理

1 创建用户 2 创建资源组 3 用户授权 4 资源组授权

资源组名称	资源组Id	资源组唯一标识	状态	创建时间	操作
默认资源组	rg-acfmwwwofpolxepl	default	可用	2020-10-09 17:06:26	<a href="#">管理资源组</a>
运维1组	rg-aek2mbuxuceigxq	sre1	可用	2021-10-24 21:18:41	<a href="#">管理资源组</a>

添加授权

资源Id	资源名称	资源类型	授权时间	操作
0Z4FCEDHLLHU9X9	架构组应用	应用	2021-10-31 17:49:59	<a href="#">取消授权</a>

补充说明：CADT 模板的权限管理与应用的权限管理方法一致。



## 6.5.权限场景验证

### 6.5.1.角色权限验证

在本章节中，我们使用 4 个 RAM 用户 -- 架构组全局管理员、运维 1 组全局管理员、运维 1 组开发测试、运维 2 组全局管理员 - 分别登录 CADT，测试对 CADT 应用“架构组应用”（章节 2.5 中提到）的访问权限。

#### 验证架构组全局管理员权限

步骤 1 使用 RAM 账号 - 架构组全局管理员 - 登录 CADT，单击全部应用。

(<https://bpstudio.console.aliyun.com/>)

在页面上方的资源组菜单中，可以看到架构组全局管理员对账号全部资源具有管理权限。



步骤 2 可以验证架构组全局管理员拥有 CADT 的全部权限（如新建，编辑，删除架构图），和资源的全部操作权限（如部署 CADT 应用，释放资源等）。

## 验证运维 1 组全局管理员权限

步骤 1 使用 RAM 账号 – 运维 1 组全局管理员 – 登录 CADT。

(<https://bpstudio.console.aliyun.com/>)

使用运维 1 组全局管理员首次登录 CADT 时，由于资源组默认是账号全部资源，所以报错“4001:您没有权限使用此功能”。



步骤 2 在页面上方的资源组列表中，由于权限策略仅能看到资源组“运维 1 组”，切换资源组为运维 1 组，单击全部应用。

在 CADT 应用列表中，仅能看到在章节 2.5 中授权给运维 1 组的应用“架构组应用”。



可以验证运维 1 组全局管理员在资源组的范围内拥有 CADT 的全部权限（如新建，编辑，删除架构图），和资源的全部操作权限（如部署 CADT 应用，释放资源等）

## 验证运维 1 组开发测试权限

步骤 1 使用 RAM 账号 – 运维 1 组开发测试 – 登录 CADT。

(<https://bpstudio.console.aliyun.com/>)

步骤 2 与运维 1 组全局管理员相同，在页面上方的资源组列表中，由于权限策略仅能看到资源组“运维 1 组”，切换资源组为运维 1 组，单击全部应用。

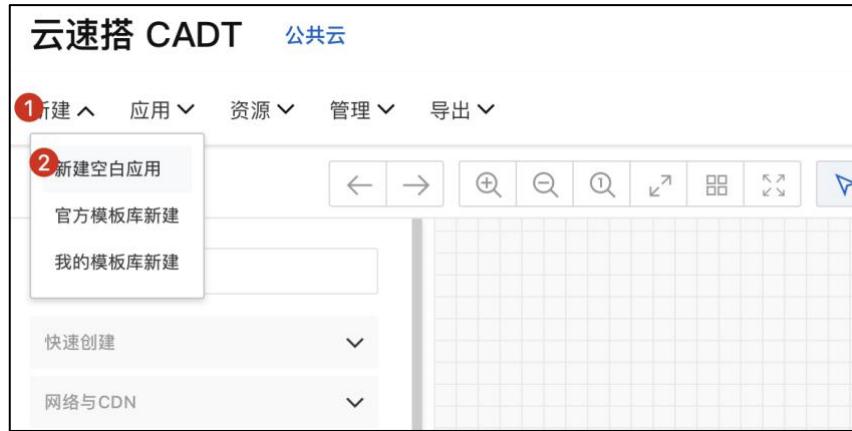
在 CADT 应用列表中，仅能看到在章节 2.5 中授权给运维 1 组的应用“架构组应用”。



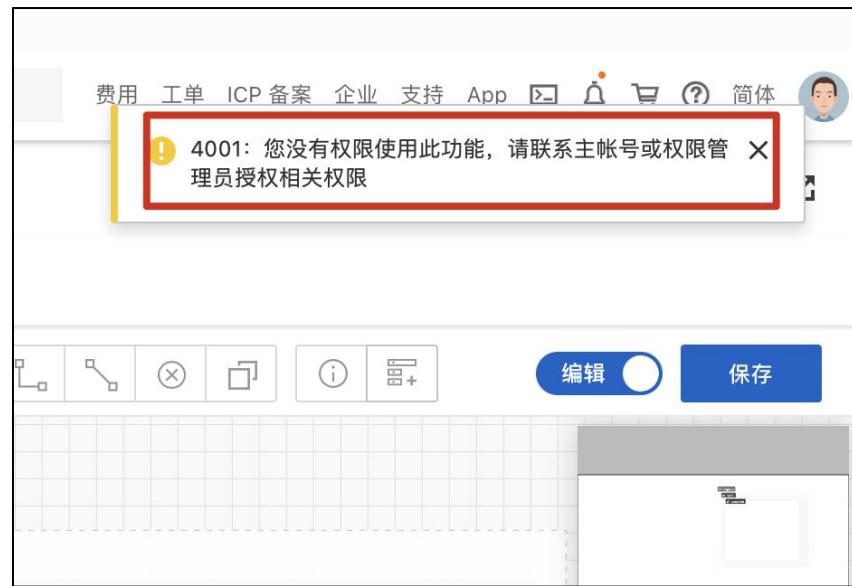
步骤 3 测试权限 – 增、删、改、查：

- 增：

- 单击新建 > 新建空白应用



- 验证结果：可以制作架构图，但由于没有权限无法保存。（符合预期）



- **删：**

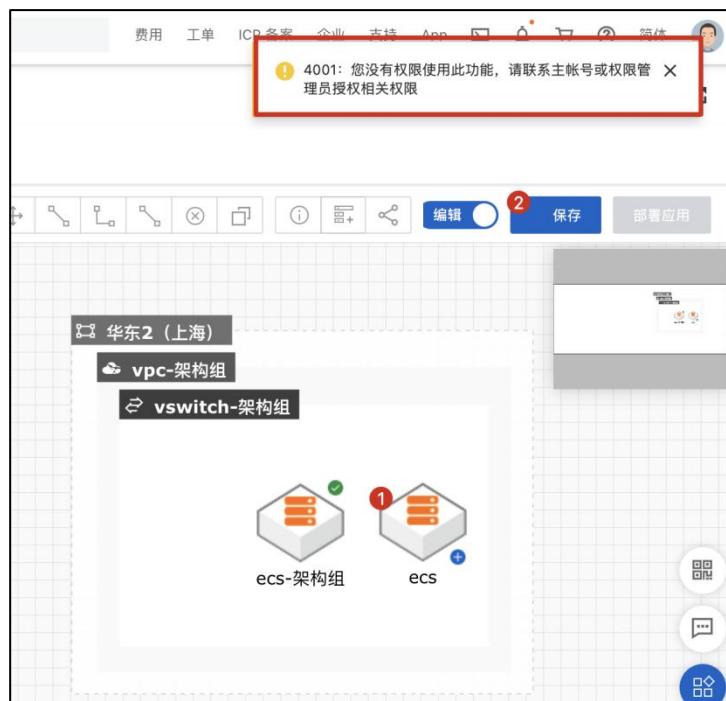
在应用列表中，鼠标移到 CADT 应用上，不能看到删除按钮，无法删除应用。（符合预期）



- 改：

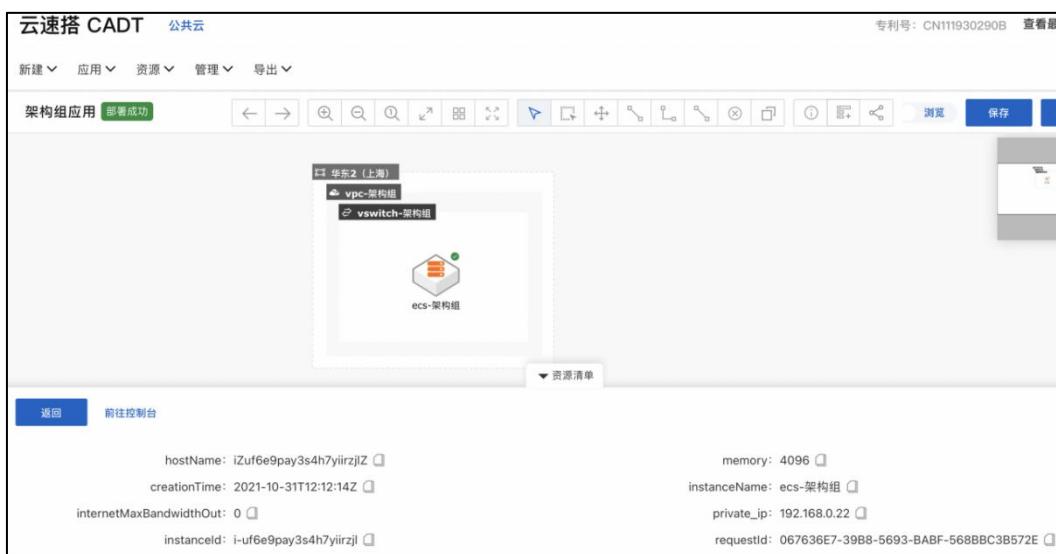
单击编辑架构图，可以成功打开架构图，可以修改架构图，但无法保存。（符合预期）





- **查：**

在架构图编辑页面，可以查看图，也可以查看架构图内资源详情。（符合预期）



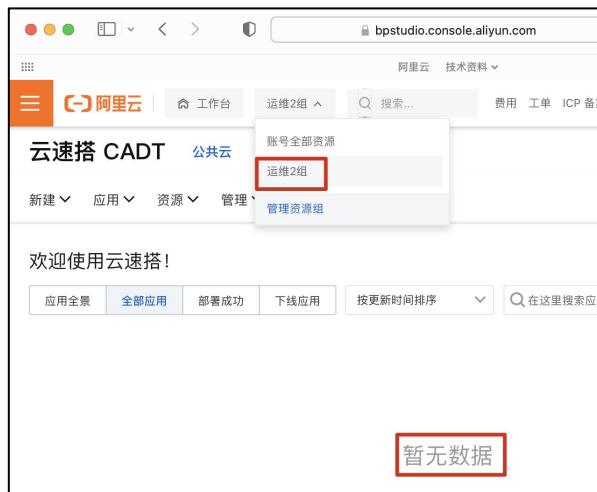
## 验证运维 2 组全局管理员权限

步骤 1 使用 RAM 账号 - 运维 2 组全局管理员 - 登录 CADT。

(<https://bpstudio.console.aliyun.com/>)

步骤 2 在页面上方的**资源组**列表中，由于权限策略仅能看到资源组“运维 2 组”，切换资源组为**运维 2 组**，单击**全部应用**。

在 CADT 应用列表中，授权给运维 1 组的“架构组应用”不可见 - 符合预期。



## 6.5.2. 资源组归属验证

本章节验证由运维 1 组全局管理员创建的 CADT 应用的资源组归属。

步骤 1 使用 RAM 账号 - **运维 1 组全局管理员** - 登录 CADT。

(<https://bpstudio.console.aliyun.com/>)

步骤 2 切换资源组为**运维 1 组**，单击**新建 > 新建空白应用**。



步骤3 制作架构图并保存为“权限测试”。

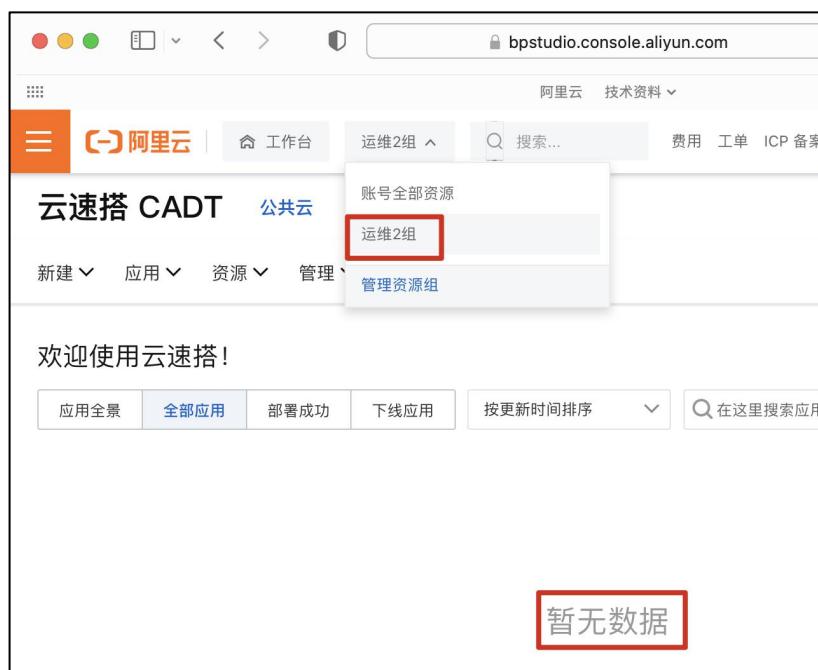


步骤4 使用 RAM 账号 - 运维 2 组全局管理员 - 登录 CADT。

(<https://bpstudio.console.aliyun.com/>)

1.切换资源组为运维 2 组。

2.在应用列表中，看不到由运维 1 组全局管理员创建的 CADT 应用。



步骤 5 使用云账号登录 CADT 控制台。[\(https://bpstudio.console.aliyun.com/ \)](https://bpstudio.console.aliyun.com/) 进入权限管理页面。



可以看到，由运维 1 组全局管理员创建的应用“权限测试”，被自动授权给了运维 1 组资源组，其他资源组没有授权。

This screenshot shows the 'Permissions Management' page. It features two main sections: 'Create User' (1) and 'Create Resource Group' (2). Below these are two buttons: 'Create User' and 'Create Resource Group'. The 'Create Resource Group' button is highlighted with a red box. The main table lists resource groups with columns: 'Resource Group Name', 'Resource Group ID', 'Resource Group Unique Identifier', and 'Status'. One row is highlighted with a red box, showing '运维1组' (Operation 1 Group) as the resource group name, 'rg-ae...gq' as the ID, 'sre1' as the unique identifier, and '可用' (Available) as the status. Below the table is a 'Add Authorization' button, followed by another table with columns: 'Resource ID', 'Resource Name', and 'Resource Type'. Two rows are highlighted with red boxes: the first row shows '0Z4FC...9X9' as the ID, '架构组应用' (Architecture Group Application) as the name, and '应用' (Application) as the type; the second row shows '25LXCQY...W29' as the ID, '权限测试' (Permission Test) as the name, and '应用' (Application) as the type.

步骤 6 架构组全局管理员的权限为全部资源，不受资源组限制，所以架构组全局管理员也拥有该应用的管理权限。

## 6.6.自定义权限（可选）

除系统权限策略外，我们还可以通过自定义权限策略，来更精细地管理权限。

步骤 1 本章节将创建 2 个自定义权限 -- `cadt-full-access` 和 `cadt-read-only`，将云产品和 CADT 的权限整合在一起。

区别于章节 1.3 提到的云资源权限（AdministratorAccess、ReadOnlyAccess）和 CADT 权限（AliyunCADTFullAccess、AliyunCADTReadOnlyAccess），当需要授权时，自定义权限支持根据需要调整权限策略的脚本，再授予对应用户组：

权限策略	属性	云资源权限	CADT权限
AdministratorAccess	系统策略	读/写	包含
ReadOnlyAccess	系统策略	读	无
AliyunCADTFullAccess	系统策略	无	读/写
AliyunCADTReadOnlyAccess	系统策略	无	读
<code>cadt-full-access</code>	自定义策略	包含（自定义）	包含（自定义）
<code>cadt-read-only</code>	自定义策略	包含（自定义）	包含（自定义）

### 6.6.1. 创建自定义权限策略 `cadt-full-access`

步骤 1 登录 RAM 控制台权限策略页面，单击创建权限策略。

(<https://ram.console.aliyun.com/policies>)

**权限策略**

① 权限策略 (Policy) 相当于传统的教科书式角色，它用于描述一组权限集。阿里云使用一种简单的 [权限策略](#)。RAM 支持两种类型的权限策略：由阿里云管理的系统策略和由客户管理的自定义策略。

- 系统策略，统一由阿里云创建，您只能使用而不能修改，系统策略的版本更新由阿里云维护；
- 自定义策略，您可以自主创建、更新和删除，自定义策略的版本更新由您自己维护。

权限策略名称	备注
AdministratorAccess	管理所有阿里云资源的权限
AliyunOSSFullAccess	管理对象存储服务(OSS)的权限
AliyunOSSReadOnlyAccess	只读访问对象存储服务(OSS)的权限
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
AliyunRDSFullAccess	管理云数据库服务(RDS)的权限

步骤 2 填写策略名称为 **cadt-full-access**，单击**脚本配置**。

**← 新建自定义权限策略**

① 策略名称  
cadt-full-access

② 配置模式  
 可视化配置  
 脚本配置

③ 策略内容

```

146      "smartag>DeleteSmartAccessGatewayClientUser",
147      "smartag>:UnbindSmartAccessGateway",
148      "vpc:AddCommonBandwidthPackageIp",
149      "vpc:AssociateEipAddress",
150      "vpc>Create",
151      "vpc>Delete",
152      "vpc:ReleaseEipAddress",
153      "vpc:RemoveCommonBandwidthPackageIp",
154      "vpc:UnassociateEipAddress",
155      "xtrace:GetToken",
156      "yundun-waf>DeleteInstance"
157      ],
158      "Resource": [
159          "*"
160      ],

```

④ 确定 返回

步骤 3 拷贝以下内容到编辑框里。

**注意：**以下策略包含了 CADT 支持的**所有云产品的权限**，请根据实际需要裁剪使用。

为防止从 PDF 中拷贝导致的格式错误，建议从本最佳实践提供的 democode 中拷贝使用 (<https://code.aliyun.com/best-practice/253.git>)。

```
    "ram:CreateServiceLinkedRole",
    "mq:ConsoleMqtInstanceList",
    "rds:PreCheckCreateOrder",
    "mq:OnsRegionList",
    "mq:OnsInstanceBaseInfo",
    "mq:OnsInstanceInServiceList"
],
"Resource": "*",
"Effect": "Allow"
},
{
    "Effect": "Allow",
    "Action": [
        "adb>DeleteDBCluster",
        "adb:ModifyDBClusterAccessWhiteList",
        "alb:GetLoadBalancerAttribute",
        "alikafka:Delete*",
        "alikafka:ForceDeleteInstance",
        "alikafka:StartInstance",
        "apigateway:DeleteInstance",
        "bss:GetOrderDetail",
        "cbn:AttachCenChildInstance",
        "cbn:DetachCenChildInstance",
        "cbn:UnassociateCenBandwidthPackage",
        "cddc>CreateDedicatedHostGroup",
        "cdn:AddCdnDomain",
        "cdn:DeleteCdnDomain",
        "cdn:DescribeUserDomains",
        "cdn:ModifyCdnDomain",
        "cdn:SetDomainServerCertificate",
        "cen>CreateCen",
        "cen>DeleteCen",
        "clickhouse>DeleteDBCluster",
        "clickhouse:ModifyDBClusterAccessWhiteList",
        "clickhouse:ModifyDBClusterAccessWhiteList"
    ]
}
```

```
"cs>CreateCluster",
"cs>DeleteCluster",
"ddi>CreateClusterV2",
"ddi:ReleaseCluster",
"dds>CreateDBInstance",
"dds>CreateShardingDBInstance",
"dds>DeleteDBInstance",
"dds:Modify*",
"dds:TagResources",
"dg>CreateGateway",
"dg>DeleteGateway",
"dts>DeleteSubscriptionInstance",
"dts>DeleteSynchronizationJob",
"ecs>AllocateDedicatedHosts",
"ecs>AttachDisk",
"ecs>AuthorizeSecurityGroup",
"ecs>AuthorizeSecurityGroupEgress",
"ecs>Create*",
"ecs>Delete*",
"ecs>DetachDisk",
"ecs>JoinSecurityGroup",
"ecs>LeaveSecurityGroup",
"ecs>ModifyDiskAttribute",
"ecs>ReleaseDedicatedHost",
"ecs>RunInstances",
"ehpc>CreateCluster",
"emr>CreateClusterV2",
"emr:ReleaseCluster",
"ess:/*",
"ess>CreateScalingGroup",
"ess>DeleteScalingGroup",
"ess>DetachDBInstances",
"ess>DetachInstances",
"ess>DetachLoadBalancers",
```

```
"ess:ModifyScalingGroup",
"gdb:DeleteDBInstance",
"gdb:ModifyDBInstanceAccessWhiteList",
"hbase:DeleteInstance",
"hbase:ModifyClusterDeletionProtection",
"hologram:DeleteInstance",
"kvstore:DeleteInstance",
"kvstore:ModifySecurityIps",
"mq:ConsoleMqttInstanceDelete",
"mq:ConsoleMqttInstanceList",
"mq:ConsoleMqttInstanceUpdate",
"mq>CreateMqttMessageFromRule",
"mq>CreateMqttMessageToRule",
"mq>CreateTopic",
"mq>DeleteMqttMessageFromRule",
"mq>DeleteMqttMessageToRule",
"mq>DeleteTopic",
"mse:DeleteCluster",
"nas>CreateAccessGroup",
"nas>CreateAccessRule",
"nas>CreateMountTarget",
"nas>DeleteFileSystem",
"nas>DeleteMountTarget",
"ons:OnsInstanceBaseInfo",
"ons:OnsInstanceCreate",
"ons:OnsTopicList",
"ots:DeleteInstance",
"ots:InsertInstance",
"polardb>CreateAccount",
"polardb>DeleteDBCluster",
"polardb:ModifyDBClusterAccessWhitelist",
"pvtz>AddZone",
"pvtz>AddZoneRecord",
"pvtz:DeleteZone",
```

```
"rds>Create*",
"rds>DeleteAccount",
"rds>DeleteDBInstance",
"rds>ModifySecurityGroupConfiguration",
"rds>ModifySecurityIps",
"slb>AddBackendServers",
"slb>Create*",
"slb>DeleteLoadBalancer",
"slb>RemoveBackendServers",
"slb>StartLoadBalancerListener",
"smartag>BindSmartAccessGateway",
"smartag>CreateCloudConnectNetwork",
"smartag>CreateSmartAccessGatewayClientUser",
"smartag>DeleteCloudConnectNetwork",
"smartag>DeleteSmartAccessGatewayClientUser",
"smartag>UnbindSmartAccessGateway",
"vpc>AddCommonBandwidthPackagelp",
"vpc>AssociateEipAddress",
"vpc>Create*",
"vpc>Delete*",
"vpc>ReleaseEipAddress",
"vpc>RemoveCommonBandwidthPackagelp",
"vpc>UnassociateEipAddress",
"xtrace:GetToken",
"yundun-waf>DeleteInstance",
"config>GetDiscoveredResourceCounts",
"config>ListDiscoveredResources",
"config>DescribeDiscoveredResourceBatch",
"config>ListDiscoveredResourceRelationsBatch",
"config>DescribeDiscoveredResource"
],
"Resource": [
    "*"
],
```

```
        "Condition": {}  
    }  
],  
"Version": "1"  
}
```

步骤 3 单击确定保存自定义策略。

### 6.6.2. 创建自定义权限策略 cadt-read-only

步骤 1 使用章节 4.1 同样的方法，创建权限策略 cadt-read-only，使用以下脚本。

**注意：**以下策略包含了 CADT 支持的**所有云产品的权限**，请根据实际需要裁剪使用。

为防止从 PDF 中拷贝导致的格式错误，建议从本最佳实践提供的 democode 中拷贝使用 (<https://code.aliyun.com/best-practice/253.git>)。

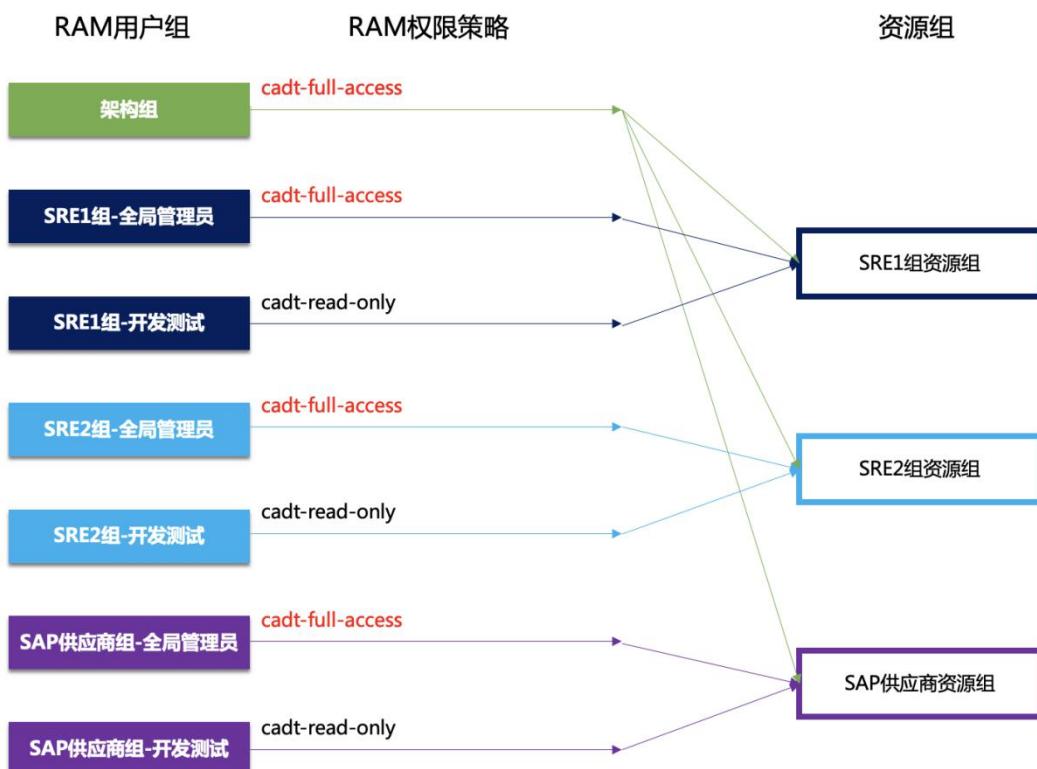
```

        "*:BatchGet",
        "*:Query",
        "*:BatchQuery",
        "actiontrail:LookupEvents",
        "actiontrail:Check",
        "dm:Desc",
        "dm:SenderStatistics"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
],
"Version": "1"
}

```

### 6.6.3. 使用自定义策略

使用自定义策略，通过合理的脚本控制，可以实现更精细化的权限管控；章节 1.3 的权限策略实现可以简化成下图所示：



## 7.最佳实践及官方模板

### 7.1.企业上云等保三级合规最佳实践

作者 | 阿里云解决方案架构师 敬海

#### 7.1.1.场景描述

信息安全等级保护（简称等保），是指国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

《中华人民共和国网络安全法》中要求，“国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改”。

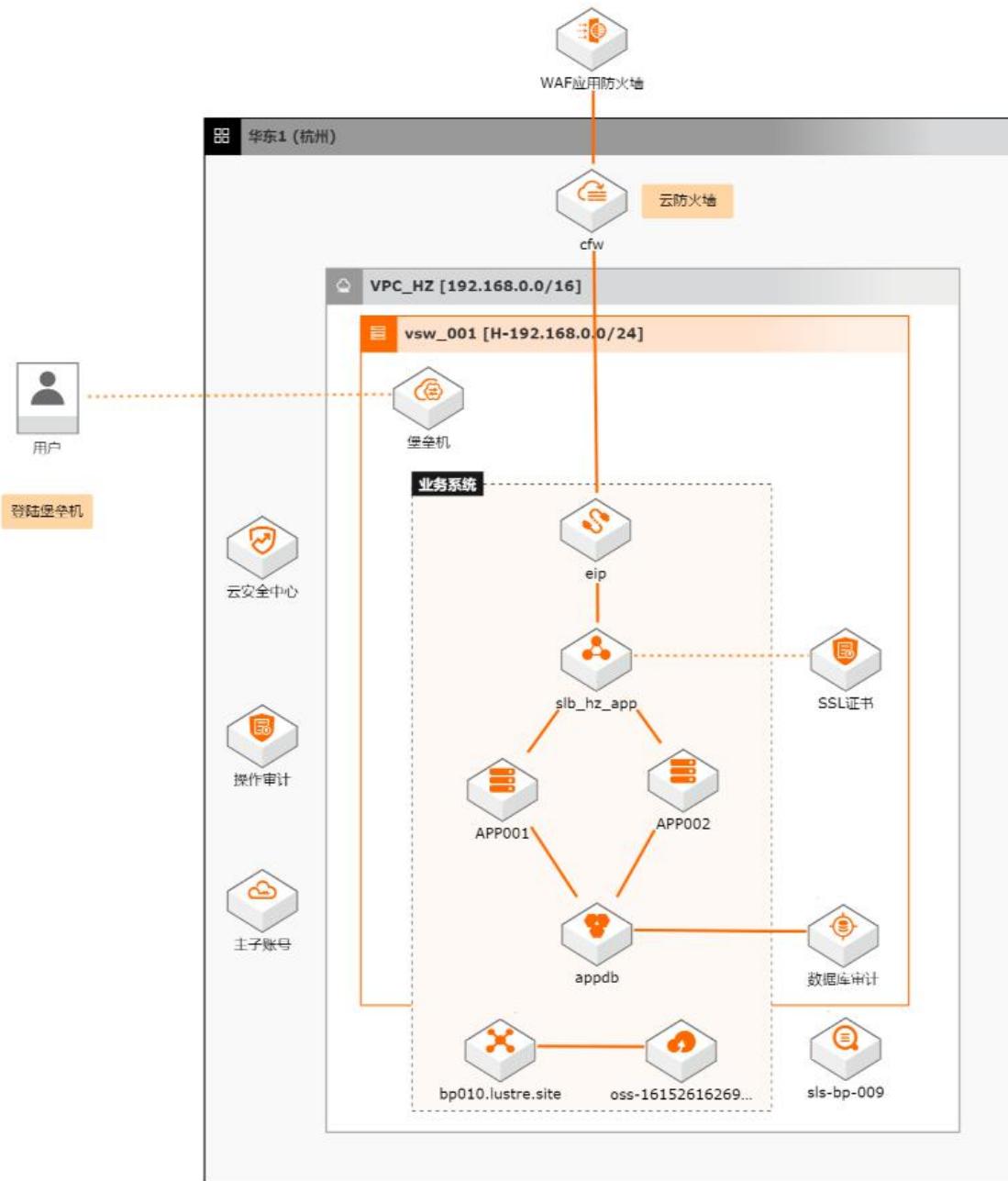
等级保护根据被保护业务系统的重要程度划分一到四个等级。第三级是指比较重要系统，具体指信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

本实践重点解决企业办公、生产等 IT 系统迁移到阿里云后，在做网络安全等级保护三级测评的时候，需要开通的相关产品、如何配置及安全防护效果的说明。

#### 7.1.2.应用范围

- 所有需要过网络安全等级保护三级的单位或企业。
- 从其他云厂商或自建 IDC 搬迁到阿里云，或者原生在阿里云平台。

#### 7.1.3.架构设计



- 查看实践：<https://bp.aliyun.com/detail/39>
- CADT 架构部署：  
<https://bpstudio.console.aliyun.com/#/bpStudio/topo?TemplateId=A5N5UYXXOEWA010G>

## 7.2.云服务器基准性能测试

作者 | 阿里云解决方案架构师 敬海

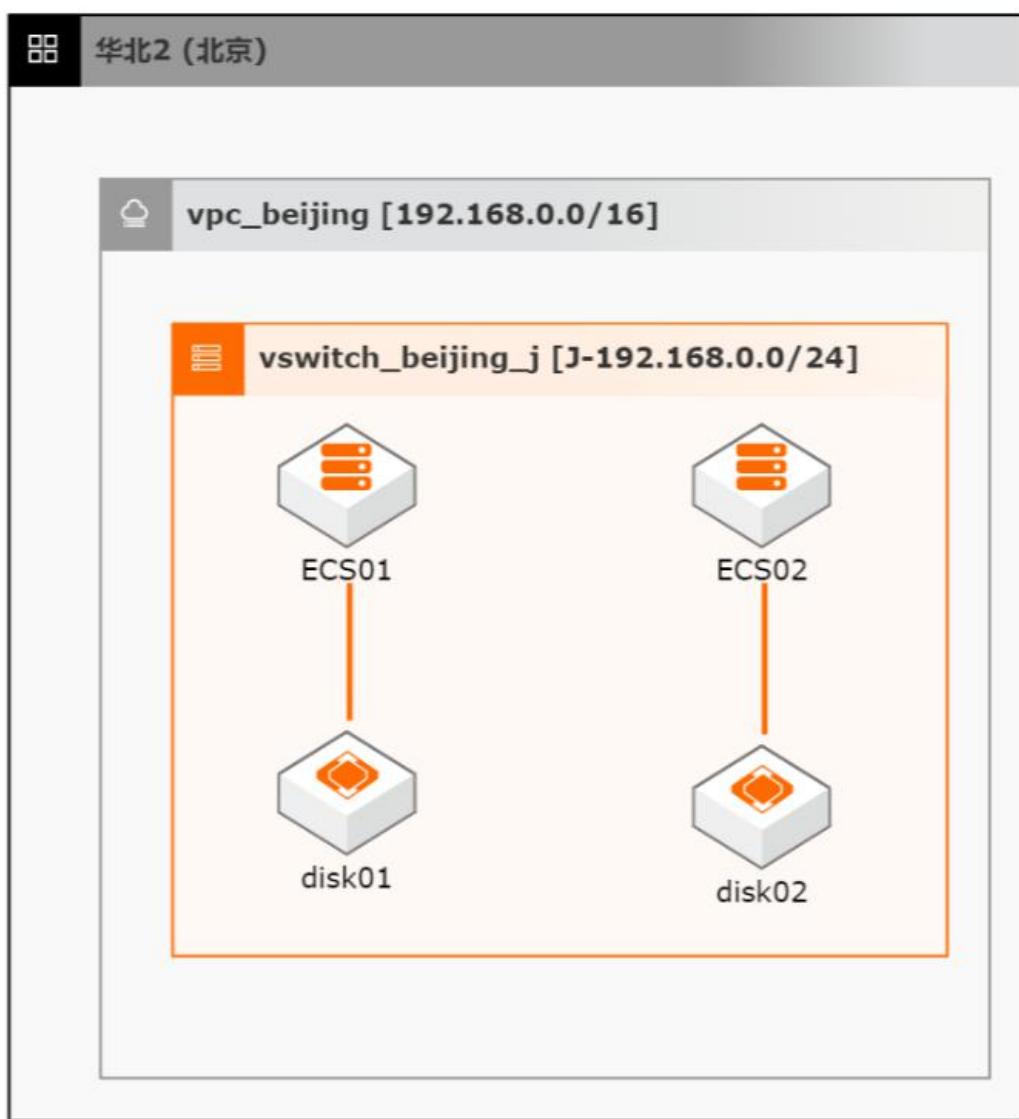
### 7.2.1.场景描述

本最佳实践适合利用标准的 benchmark 工具对云服务器的 CPU、内存、网络和磁盘性能进行测试的场景。

### 7.2.2.解决问题

对云服务器的基准性能进行测试，包括 CPU、内存、网络和磁盘。

### 7.2.3.架构设计



- 查看实践：<https://bp.aliyun.com/detail/189>
- CADT 架构部署：  
<https://bpstudio.console.aliyun.com/#/bpStudio/topo?TemplateId=DHJ5R14A8551LHYF>

## 7.3.PAI 平台搭建企业级个性化推荐系统

作者 | 阿里云解决方案架构师 敬海

### 7.3.1.场景描述

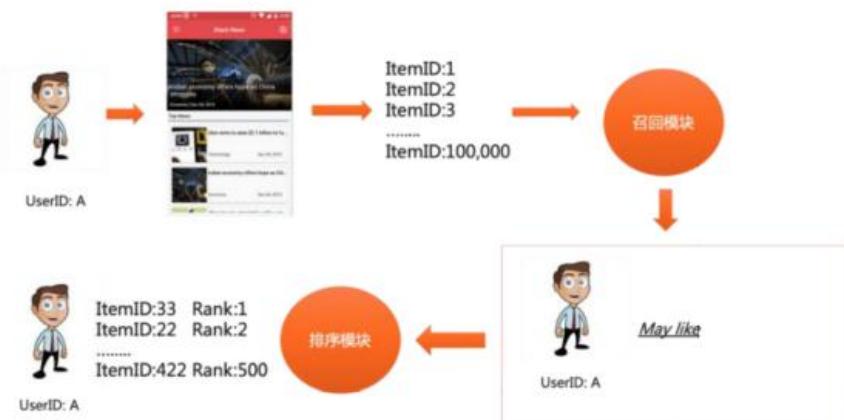
PAI 是阿里云推出的人工智能平台，提供一站式的机器学习解决方案。本最佳实践利用 PAI 平台结合阿里云 RDS for MySQL 版、对象存储 OSS 和云数据库 Redis 版等产品构建一个高效的离线训练+在线推理的推荐业务系统。

### 7.3.2.适用客户

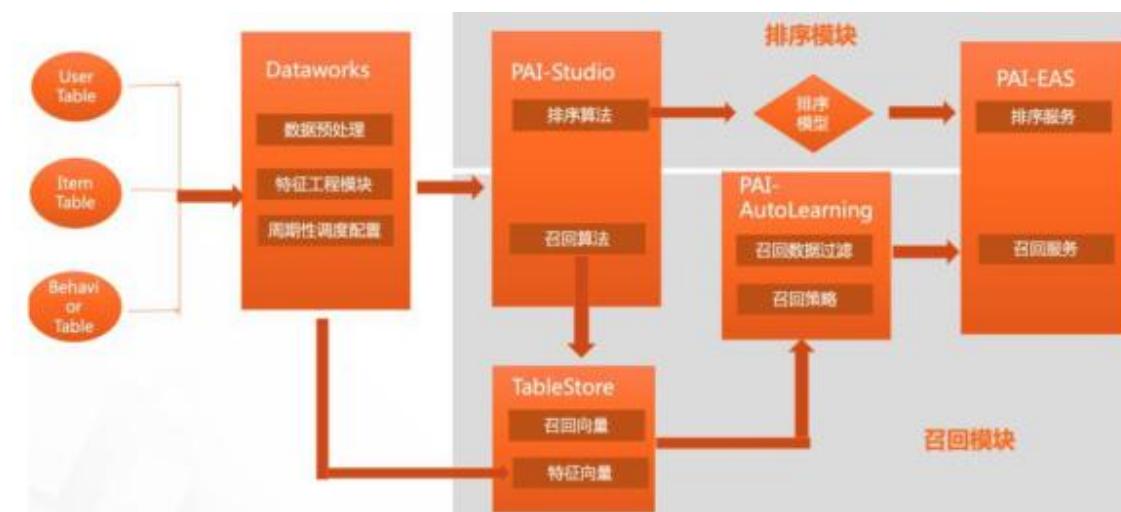
- 1.互联网行业客户，MAU 80 万-1500 万。
- 2.业务为信息流、广告推荐等经典推荐场景。
- 3.数据已经使用了 MaxCompute 或准备使用。
- 4.具备 1-5 名有算法背景的工程人员。
- 5.原有服务基于开源算法自建体系，但是受限现有人员和成本无法进一步提升。

### 7.3.3.架构设计

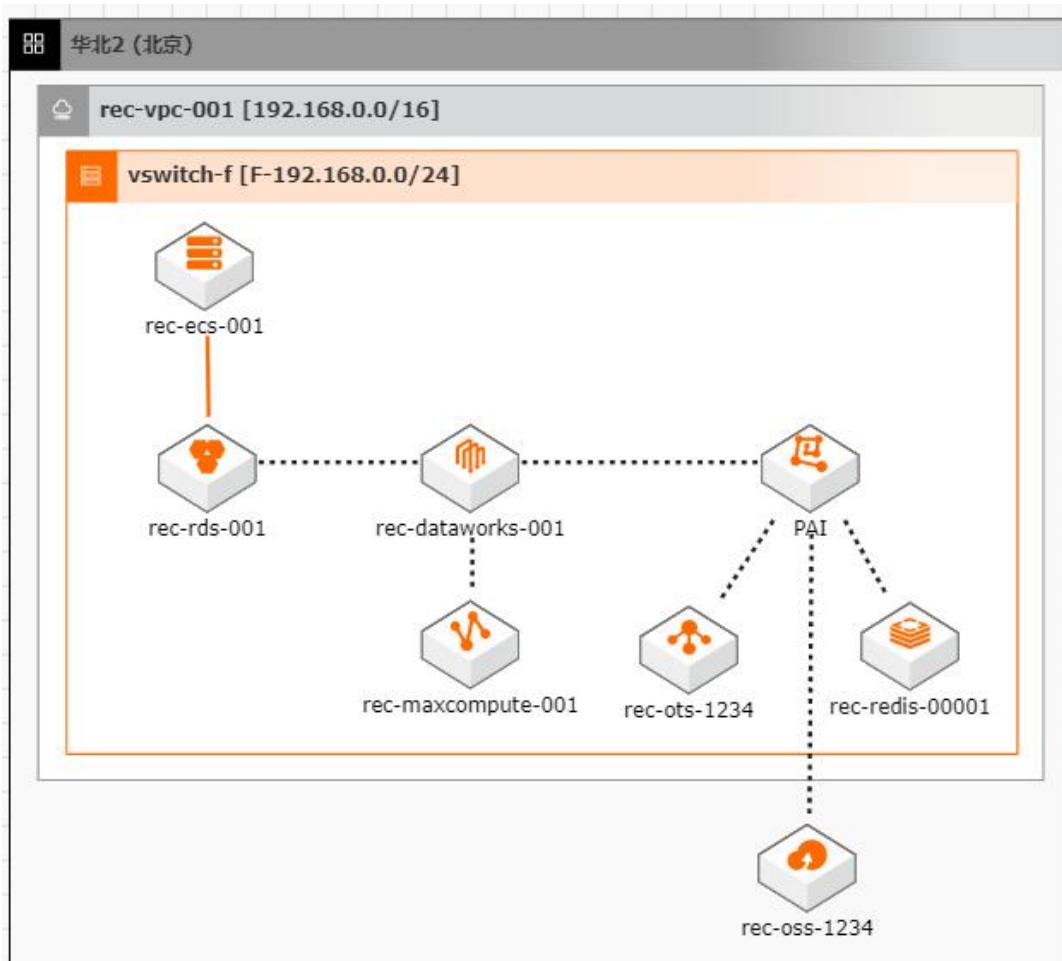
#### 业务流程



## 推荐业务架构



## CADT 架构



- 查看实践：<https://bp.aliyun.com/detail/140>
- CADT 架构部署：  
<https://bpstudio.console.aliyun.com/#/bpStudio/topo?TemplateId=U9VRQ75A7R8N1JE>

## 7.4.基于 ECI 的 ACK 集群高弹性架构

作者 | 阿里云最佳实践

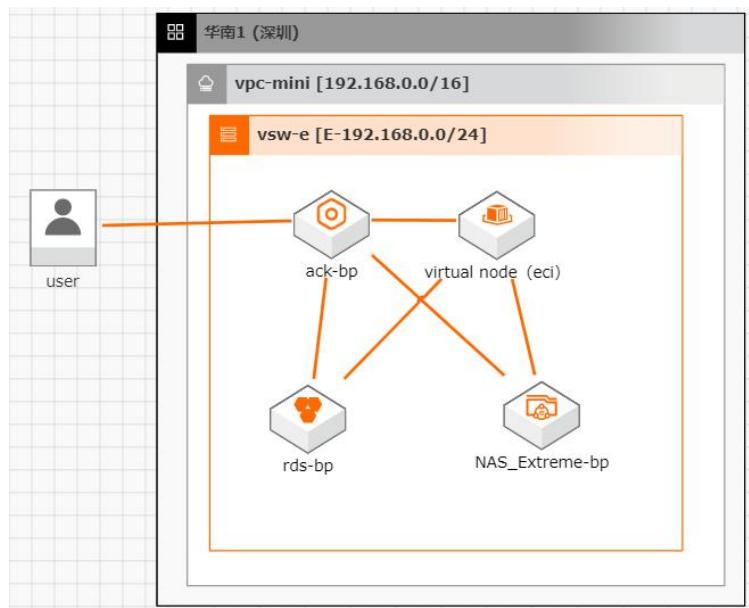
### 7.4.1.场景描述

用户原有的业务部署在阿里云 ACK 集群上，在 ACK 集群上运行常规业务，当业务突发波动（如秒杀活动）时，让突增的业务运行在 ECI 实例上，随着业务波动动态创建/释放 ECI 实例，达到成本的最优控制。同时，业务方无需管理节点和容量规划，全自动实现容器“无限”弹性扩容。

### 7.4.2.解决问题

- 1.Long-Run 类业务，例如：业务生产系统；
- 2.明显的业务弹性诉求，例如：爬虫、秒杀；
- 3.离线任务。

### 7.4.3.架构设计



- 查看实践：<https://bp.aliyun.com/detail/46>
- CADT 架构部署：  
<https://bpstudio.console.aliyun.com/#/bpStudio/topo?spm=a2cls.b92374736.0.0.16881271iEYGFn&TemplateId=MNEPO56PA8H45F3D>

## 7.5.阿里云最佳实践频道

<https://bp.aliyun.com/>

## 7.6. 云速搭 CADT 官方模板计

<https://bpstudio.console.aliyun.com/#/bpStudio/template/all>

## 8.客户成功

### 8.1.最佳实践助力正元智慧上云提效

#### 8.1.1.客户简介

浙江正元智慧科技股份有限公司创建于1994年，是国家火炬计划重点高新技术企业。公司拥有自主研发生产的百余项软件著作权、专利及多系列核心硬件产品。产品通过公安部、人民银行认证，先后获得“武警部队科技进步一等奖”、“国家金卡工程金蚂蚁奖”、“中国国际软件博览会金奖”。公司在原有一卡通的基础上，运用新一代AIoT（人工智能+大数据+区块链+云计算+物联网技术），着力构建物联中台、业务中台、数据中台、算法中台，推出一体化智能化的协同融合服务平台，打造多技术融合、多主体协同、多场景应用的智慧园区全面解决方案。核心业务覆盖校园、企事业、社区等，成为智慧园区解决方案引领者。



#### 8.1.2.客户需求

- 1、业务上云
- 2、基于阿里云产品构建稳定、高可用的基础服务



### 8.1.3.客户价值

- 1、系统架构方面，参照《云上网站经典架构》，让我们熟悉云上的架构实践，可以将我们规划的资源，快速在云上转化为产品架构图和实施部署，借助云速搭 CADT，通过这个工具可以看到资源的可视化、报价清单、架构演进跟踪等，通过一键部署，大大提升了运维效率。
- 2、业务安全方面，参照《企业上云等保三级合规》、《企业上云数据安全》、《AK 防泄漏》、《云上持续审计合规最佳实践》等一系列的安全&合规相关实践，了解云上如何过等保，并基于提供的 CADT 架构模式，快速的部署了云上等保环境，为业务安全获取国家权威认证。
- 3、业务扩展方面，参照《基于 ECI 的 ACK 集群高弹性架构》，为我们二期业务发展，引入了新的发展思路，充分利用云上托管版服务，更好的帮我们支撑业务的发展。



## 8.1.4.客户之声

我是浙江正元智慧科技股份有限公司运营事业部总经理翁金阳。

浙江正元智慧科技股份有限公司创建于1994年，是国家火炬计划重点高新技术企业。公司拥有自主研发生产的百余项软件著作权、专利及多系列核心硬件产品。产品通过公安部、人民银行认证，先后获得“武警部队科技进步一等奖”、“国家金卡工程金蚂蚁奖”、“中国国际软件博览会金奖”。公司在原有一卡通的基础上，运用新一代AIoT（人工智能+大数据+区块链+云计算+物联网技术），着力构建物联中台、业务中台、数据中台、算法中台，推出一体化智能化的协同融合服务平台，打造多技术融合、多主体协同、多场景应用的智慧园区全面解决方案。核心业务覆盖校园、企事业、社区等，成为智慧园区解决方案引领者。

随着云原生时代的到来，为了更好的服务我们的客户，正元智慧从公司战略层面全面拥抱云计算。将我们的业务搬到云端，形成定制化、标准化、简易化等三种不同类别的服务路线。正元智慧将采用“公有云服务+SaaS化软件平台+智能硬件”的模式，积极开拓新行业、新用户，深入布局K12、中小企业领域。针对中小学客户，公司将构建教学、教研、管理、后勤、家校协同等一体化解决方案，提高中小学管理智能化、数字化水平；对于中小企业客户，公司将结合门禁考勤、行政办公、就餐消费、后勤服务等应用场景提供云解决方案。公司在保持原有高校客户长久粘性的基础上，积极谋求多行业、多领域、跨场景的业务扩张，不断提升公司盈利水平，服务好我们的客户和我们的股东。

在业务上云阶段，我们与多家云厂商进行了接触，充分了解、沟通，阿里云的产品齐全、性能优越、质量稳定、服务响应及时，能给我们带来很大帮助。具体有以下方面：

1、系统架构方面，参照《云上网站经典架构》，让我们熟悉云上的架构实践，可以将我们规划的资源，快速在云上转化为产品架构图和实施部署，借助云速搭CADT，通过这个工具可以看到资源的可视化、报价清单、架构演进跟踪等，通过一键部署，大大提升了运维效率。

2、业务安全方面，参照《企业上云等保三级合规》、《企业上云数据安全》、《AK防泄漏》、《云上持续审计合规最佳实践》等一系列的安全&合规相关实践，了解云上如何过等保，并基于提供的CADT架构模式，快速的部署了云上等保环境，为业务安全获取国家权威认证。

3、业务扩展方面，参照《基于 ECI 的 ACK 集群高弹性架构》，为我们二期业务发展，引入了新的发展思路，充分利用云上托管版服务，更好的帮我们支撑业务的发展。

接下来我们将会将更多的应用部署到阿里云上，同时也会帮助我们的客户将云端的业务部署到阿里云上，借助阿里云产品的成熟方案，服务好我们的客户。期待与阿里云更紧密的合作。

——正元智慧运营事业部总经理 翁金阳



### 8.1.5.查看详情

<https://bp.aliyun.com/bpcaseDetail/62>



## 相关最佳实践

- 企业上云等保三级合规：<https://bp.aliyun.com/detail/39>
- 云上网站经典架构：<https://bp.aliyun.com/detail/10>
- 企业上云数据安全：<https://bp.aliyun.com/detail/92>
- AK 防泄漏：<https://bp.aliyun.com/detail/142>
- 云上持续审计合规最佳实践：<https://bp.aliyun.com/detail/114>
- 基于 ECI 的 ACK 集群高弹性架构：<https://bp.aliyun.com/detail/46>

## 8.2.最佳实践助力复星星选项目极速上线成功

### 8.2.1.客户简介

复星星选是面向中高端市场的精准流量分发平台，将复星全产业的 C 端流量实现“汇、粘、通”。用户在各种场景“汇”聚到星选，平台通过数据对用户进行分析，多维度地构建完整用户画像系统；同时，对复星旗下品牌资源加以整合，构成平台的优质权益内容和用户产生“粘”性；借助“数据+AI”的核心能力，将权益在复星全生态内进行精准匹配，实现跨产业间的流量互联，实现会员的横向融“通”，实现乘数效应。通过微信小程序搜索“复星星选”即可方便快捷的获得产品体验。



### 8.2.2.客户需求

为了加速推进复星集团 C 端置顶战略，我们需要构建全新的星选平台，平台由多个子系统构成，团队要在很短的时间内从 0 到 1，完成资源部署；我们看重平台的安全性和稳定性、以及扩展性和弹性。于是，有几个具体任务摆在技术团队面前：

- 1、要搭建一个兼容容器化和非容器化的混合系统架构，需要统一的流量网关，进行全局流量监控和控制；
- 2、对日志统计、入侵防护等等也有相应的要求；
- 3、灵活便捷的资源部署方式，配合和支撑平台的敏捷的开发与发布。

### 8.2.3.客户价值

- 1、云产品即开即用，既满足功能需求，又满足项目实效性需求；
- 2、ALB 作为统一流量入口，降低了系统复杂度和维护成本；
- 3、最佳实践丰富的方案文档，降低沟通和学习成本；

4、云速搭 CADT 实现架构可视化的一键部署，基础设施一键上云。

## 8.2.4.客户之声

团队利用阿里云的几个产品开箱即用的产品，包括：阿里云容器服务（ACK），开源大数据平台（EMR），以及负载均衡（SLB）等产品，进行快速配置满足功能需要；另外，团队使用了云速搭（CADT）产品，这款产品提供了可视化操作界面，通过视图可以实时掌握资源部署情况和项目进度，加上架构模板云速搭可实现资源的一键部署，这对资源种类多样，系统架构复杂的项目，能大大提升开发效率和体验。

期间，我们参考了阿里云最佳实践提供的几篇文章，包括：《基于 K8S 多集群隔离环境下的 DevOps 实现》、《云效+ACK 构建容器云 DevOps 平台》，帮助我们快速熟悉阿里云的产品方案，降低沟通成本，辅助决策，有效缩短项目周期。

也非常有幸，能在此次与阿里云团队的合作中，沉淀并形成了一个新的最佳实践的案例——《基于 ALB 统一流量调度和监控最佳实践》，作为一个利用应用型负载均衡作为复杂系统流量统一入口的一次成功案例，希望能给有关企业和技术团队提供参考和帮助。

在阿里云优秀技术产品的基础上，在和云速搭工具的配合下，复星星选在 2021 年 9 月已成功问世，平台在云上快速落地，与最佳实践方案分不开，也感谢阿里云产品和技术团队，期待在未来与阿里云有更广泛和深入的合作。

—— CTO 兼技术研发部总经理 沈荣华



## 8.2.5.查看详情

<https://bp.aliyun.com/bpcaseDetail/66>



### 相关最佳实践

基于 K8S 多集群隔离环境下的 DevOps 实现：<https://bp.aliyun.com/detail/165>

基于 ALB 统一流量调度和监控：<https://bp.aliyun.com/detail/228>

云效+ACK 构建容器云 DevOps 平台最佳实践：<https://bp.aliyun.com/detail/52>

## 8.3.云速搭助力青莲实现极速项目交付

### 8.3.1.客户简介

广州青莲网络科技有限公司成立于 2009 年 5 月 8 日，坚持以技术创新及品质服务为基础，专注于为企业客户提供企业全流程的 IT 解决方案及技术服务。

作为技术创新驱动的全流程企业服务专家，青莲围绕云、安全、数据、智能四大方向，在公有云、云安全、数据服务、IoT 边缘计算、SAP 上云咨询、自动化运维等领域均有建树，已经成为全国上百家大型上市企业的指定 IT 技术及服务供应商。



### 8.3.2.客户需求

青莲网络在全国范围内为大量的阿里云客户提供了本地化的 MSP 技术服务支持，我们的技术团队在日常很大一部分时间耗在为客户提供标准化的网络、安全环境，以及支撑客户开通和部署云资源等工作中，每个相同类型的项目都需要投入人力重复标准化作业，技术团队内部无法快速横向的进行能力复制。此外，青莲自研的 CRM、ERP 等业务系统也运行在阿里云上，云资源申请缺少标准化的流程。

### 8.3.3.客户价值

为应对这些挑战，青莲以阿里云最佳实践作为实践指导，通过云速搭（CADT）设计了标准化的基础架构环境。在云速搭的帮助下，只需要简单调整模板中资源的配置参数，就可以复用到多个项目中。资源交付从 1-2 天缩短到 1-2 小时，大大提升了资源的交付效率，避免了重复工作。同类型的项目经验通过模板化的方式，也实现了在技术团队中快速的能力复制。

例如，我们在某客户的项目中，参考了《容器跨可用区高可用》这篇最佳实践。通过预先制作的云速搭模板，实现了分钟级的资源交付。在这个项目中，阿里云最佳实践架构师远程指导了云速搭模板的制作，并协助验证了模板准确可用。相比过去单纯通过文档，或人力现场支持的方式，云速搭模板做为知识和经验的交互载体，大大提高了沟通效率，降低了项目交付成本。

在另一家客户的 SAP 上云项目中，我们联合阿里云最佳实践团队共同开发出了《SAP（HANA+S/4）上云基础环境部署最佳实践》，并将基础资源部署的模板发布在了云速搭官方模板库，让广大阿里云的用户共同受益。SAP 产品的常用部署架构高度标准化，非常适合做成模板。但 SAP 要求其产品必须部署在 SAP 官方认证的 ECS 机型上。另外具有 SAP 专业技能的技术人员较少，经验沉淀和复制更加困难。通过云速搭制作的 SAP 基础资源部署模板，很好的解决了这一问题：模板中的机型均为 SAP 认证机型，基础资源的架构经过了项目实战检验。这样，云速搭承担了重复性的基础资源部署工作，使我们可以专注于价值更高的 SAP 软件环境的安装和调试。

以上两个例子中，青莲除了成功交付了项目，还将无形的项目经验沉淀成了有形的云速搭模板，作为公司的知识资产，在未来同类项目中大量复制。此外，借助云速搭，青莲内部自研系统的交付流程，也得到了标准化。

———广州青莲网络科技有限公司技术总监 江峰

### 8.3.4. 查看详情

<https://bp.aliyun.com/bpcaseDetail/58>



### 相关最佳实践

- 容器跨可用区高可用最佳实践：<https://bp.aliyun.com/detail/34>
- SAP S/4HANA 上云基础环境部署最佳实践：<https://bp.aliyun.com/detail/217>

## 8.4.北京乘云至达使用云速搭 CADT 工具快速交付项目

### 8.4.1.客户简介

北京乘云至达科技有限公司是一家提供云计算、云服务 IT 战略咨询于一体的高新技术企业。公司规模约 1000 余人，其中邢台有专业级电销营销中心。乘云至达 2016 年成为阿里云的合作伙伴以及金牌服务商，2020 年完成销售额 1.3 亿（前三强），2021 年成为阿里云旗舰级合作伙伴。



### 8.4.2.客户需求

乘云至达作为阿里云的旗舰级服务商，经常需要帮助客户交付和落地最终的解决方案，主要是在公共云环境下，进行交付。在交付的过程中，希望能够压缩交付周期，批量复制快速交付。

以往在出具架构方案之后，客户整套系统所有资源都从控制台来开，不方便交付，效率较低。并且在架构方案快速交付时，报价，开通资源时间成本一直是个问题点。同一个应用的多种实例资源创建后，又分散在不同的控制台，难以组织和管理，不能从项目的整体角度来统一管理。在后期运维中，会遇到系统架构模糊不清，尤其项目较多的时候，无法快速定位项目资源。

### 8.4.3.客户价值

经过和阿里云架构师交流，引入了使用阿里云的云速搭 CADT 产品，CADT 产品提供了零代码建架构，通过图形化的拖拽生成可部署的架构，并提供了一键部署的功能，还能够自动生成报价清单和部署报告，同时还提供了一些公开的常用的云上最佳实践的架构模板供参考。

一方面，我们利用图形化的界面，基于云上的公共模板，结合用户的实际情况进行简单修改，并通过一键分享功能，交付用户，不需要再一个个通过控制台创建，提升了我们的交付效率，降低了很多沟通成本。另一方面，有了架构图之后，可以从架构角度来管理和组织资源，简化运维工作，提高运维效率。最后，我们还可以，在保留系统架构的基础上，生成资源费用清单，添加已保有资源到架构图中，保存各个历史版本。使用云速搭产品对客户未来架构升级演变过程有不可或缺的优势。

另外，我们将最佳实践和云速搭工具结合起来使用，可以更好的服务客户和帮助客户落地公共云资源交付。

#### 8.4.4.客户之声

我是北京乘云至达科技有限公司的技术经理高丽德，北京乘云至达科技有限公司是一家提供云计算、云服务 IT 战略咨询于一体的高新技术企业。公司规模约 1000 余人，其中邢台有专业级电销营销中心。乘云至达 2016 年成为阿里云的合作伙伴以及金牌服务商，2020 年完成销售额 1.3 亿（前三强），2021 年成为阿里云旗舰级合作伙伴。

我们作为阿里云的金牌服务商，在给客户交付的落地的解决方案的过程中，希望能够压缩交付周期，批量复制快速交付。以往在出具架构方案之后，客户整套系统所有资源都从控制台来开，不方便交付，效率较低。并且在架构方案快速交付时，报价，开通资源时间成本一直是个问题点。同一个应用的多种实例资源创建后，又分散在不同的控制台，难以组织和管理，不能从项目的整体角度来统一管理。在后期运维中，会遇到系统架构模糊不清，尤其项目较多的时候，无法快速定位项目资源。

经过和阿里云架构师交流，引入了使用阿里云的云速搭 CADT 产品，CADT 产品提供了零代码建架构，通过图形化的拖拽生成可部署的架构，并提供了一键部署的功能，还能够自动生成报价清单和部署报告，同时还提供了一些公开的常用的云上最佳实践的架构模板供参考。

一方面，我们利用图形化的界面，基于云上的公共模板，结合用户的实际情况进行简单修改，并通过一键分享功能，交付用户，不需要再一个个通过控制台创建，提升了我们的交付效率，降低了很多沟通成本。另一方面，有了架构图之后，可以从架构角度来管理和组织资源，简化运维工作，提高运维效率。最后，我们还可以，在保留系统架构的基础上，生成资源费用清单，添加已保有资源到架构图中，保存各个历史版本。使用云速搭产品对客户未来架构升级演变过

程有不可或缺的优势。

另外，我们将最佳实践和云速搭工具结合起来使用，可以更好的服务客户和帮助客户落地公共云资源交付。

——北京乘云直达科技有限公司技术经理 高丽德

#### 8.4.5.查看详情

<https://bp.aliyun.com/bpcaseDetail/59>



#### 相关最佳实践

- SAE 无缝对接 CICD 工具实现 DevOps 最佳实践：<https://bp.aliyun.com/detail/138>
- 应用 IPv6 改造最佳实践：<https://bp.aliyun.com/detail/18>
- 云上网站经典架构最佳实践：<https://bp.aliyun.com/detail/10>
- 在线教育视频直播最佳实践：<https://bp.aliyun.com/detail/139>

## 9.相关资源

- 阿里云最佳实践：<https://bp.aliyun.com/>
- 云速搭 CADT 产品详情：<https://www.aliyun.com/product/developperservices/cadt>
- 云速搭 CADT 帮助文档：<https://help.aliyun.com/product/182827.html>
- 云速搭 CADT 产品支持钉钉群：

