阿里云
轻量级分布式应用服务

最佳实践

文档版本：20190906

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
`courier 字体`	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 应用访问公网

1.1 应用如何访问公网

应用业务通常需要获取公网资源或者跨 VPC 访问，本文介绍应用如何从 VPC 内网环境访问公网。

背景信息

当在实际场景中有如下几种场景需要访问公网。

- 容器在运行时需要建立公网上的依赖。
- 与第三方有合作，例如使用微信小程序需要上公网。
- 应用需要跨 VPC 或 Region 访问数据库。

实施方案

- 方案一：为应用实例绑定弹性公网 IP（简称 EIP）。

  如果 VPC 内存在多个应用需要公网，每个应用中至少有 1 个实例绑定 EIP。
- 方案二：为应用实例配置 NAT 网关代理并绑定 EIP。

  通过 SNAT 的功能，为 VPC 内所有无公网 IP 的应用实例配置访问互联网代理。

  单个 VPC 内存在多个应用访问互联网，配置代理后仅需绑定 1 个 EIP。

当前 SAE 应用绑定 EIP 的功能正在开发中，将于近期上线。您的应用如有访问公网的需求，建议暂时采用 NAT 网关和 EIP 组合的方案来访问公网。

创建 NAT 网关

1. 登录 VPC 控制台，在左侧导航栏单击 NAT 网关。
2. 在 NAT 网关页面单击组合购买 EIP。
3. 在组合购买（NAT 网关+弹性公网 IP）页面，计费设置完成后单击立即购买。
   a. 选择 SAE 应用所在的地区和 VPCID。
   b. 参照NAT 网关的计费说明选择规格、EIP 和计费周期。

      选择已有 EIP，您只需为 NAT 网关的购买费用付费。

      选择新购 EIP，您还需设置弹性公网 IP的参数，并为 NAT 网关和 EIP 付费。

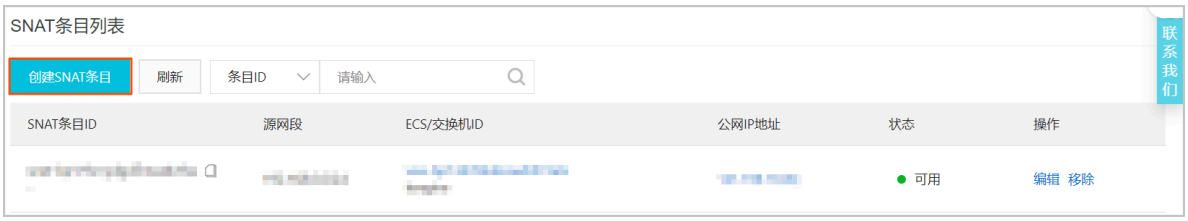
4. 购买完成之后，NAT 网关创建成功，在 NAT 网关页面的 NAT 网关列表内可以查看到实例的弹性公网 IP。

创建 SNAT 条目

创建 SNAT 条目，为专有网络中没有公网 IP 的应用实例，提供访问公网代理服务。

1. 在目标 NAT 网关的操作列单击设置 SNAT。

2. 在 SNAT 表页面单击创建 SNAT 条目。



3. 在创建 SNAT 条目页面配置 SNAT 条目信息。

- 交换机：选择 VPC 中的交换机。该交换机下所有的应用实例均可通过 SNAT 功能进行公网访问。

  > 说明:
  > 如果持有公网 IP 的应用实例（例如已经绑定了EIP）发起互联网访问，系统会优先使用其持有的公网 IP，而不会使用 NAT 网关的 SNAT 功能。

- 交换机网段：显示该交换机的网段。
- 公网 IP 地址：选择用来提供互联网访问的公网 IP。

  > 说明:
  > 用户创建 DNAT 条目的公网 IP 地址不能再用来创建 SNAT 条目。

1.2 常见访问公网场景示例

本文通过具体示例演示应用访问公网。

背景信息

某企业需要在 SAE 北京 Region 创建应用，并在该应用上部署 WordPress 服务，同时使用杭州 Region 的 RDS 作为数据库。

前提条件

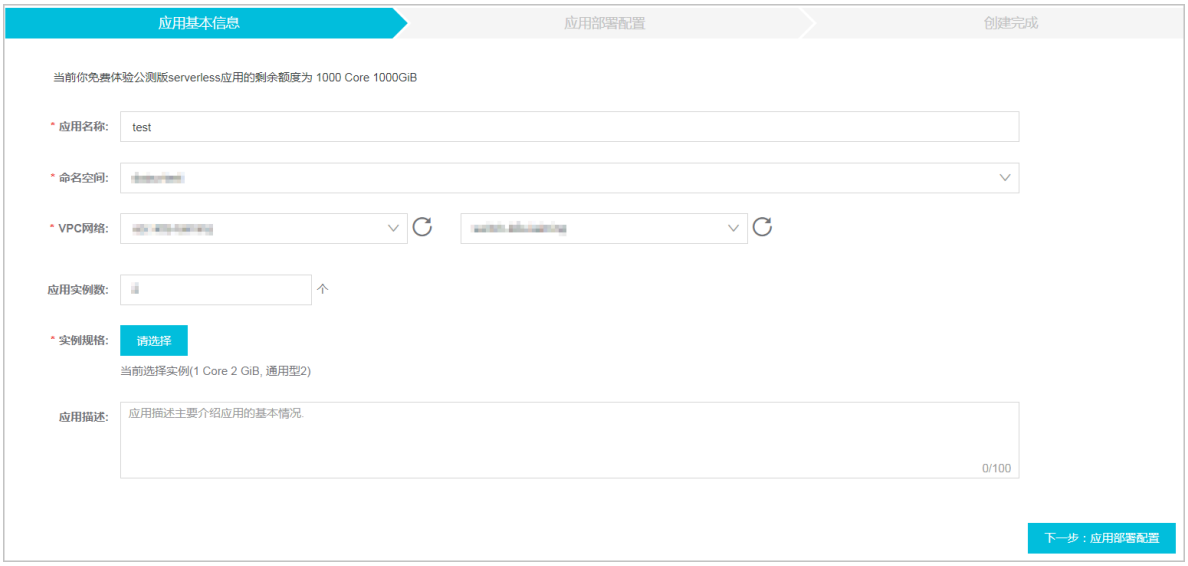
- 开通 SAE 服务。
- 创建专有网络 VPC。
- #unique_6/unique_6_Connect_42_section_cu5_k9p_xuf。

创建并部署 WordPress 应用

> 注意:
> 目前 SAE 现已开放了华北 2（北京）、华东 1（杭州）、华东 2（上海）和华南 1（深圳）地域，您需选择地域为华北 2（北京）、华东 1（杭州）、华东 2（上海）和华南 1（深圳），才能登录 SAE 控制台。

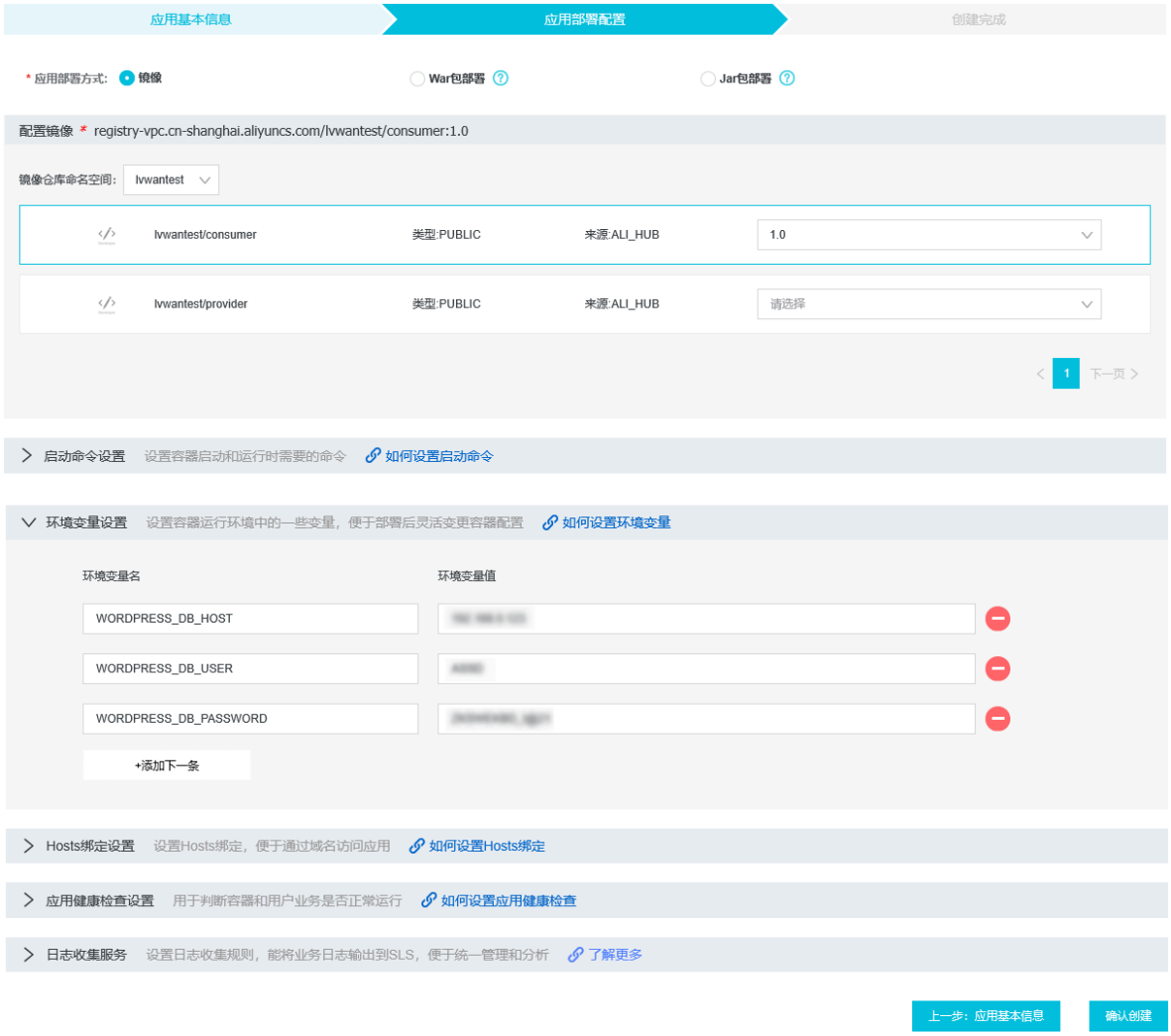
1. 登录 SAE 控制台。
2. 在左侧导航树选择Serverless 应用引擎 > 应用列表，并在 应用列表页面单击右上角 创建应用。

3. 在创建应用页面的应用基本信息页签内，设置应用相关信息，并单击下一步：应用部署配置。



- 应用名称：输入应用名称。允许数字，字母，下划线以及中划线组合，仅允许字母开头，最大长度 36 个字符。
- 命名空间：在下拉菜单中选择创建好的命名空间。
- VPC 网络：在下拉菜单中选择VPC 和 vswitch 。
- 应用实例数：选择要创建的实例个数。
- 实例规格：单击请选择，在选择实例规格页面内选择实例的 CPU 和 Memory 规格。
- 应用描述：填写应用的基本情况，输入的描述信息不超过100个字符。

4. 在应用部署配置页面，选择 镜像，依据页面指示进行配置。完成设置后单击确认创建。

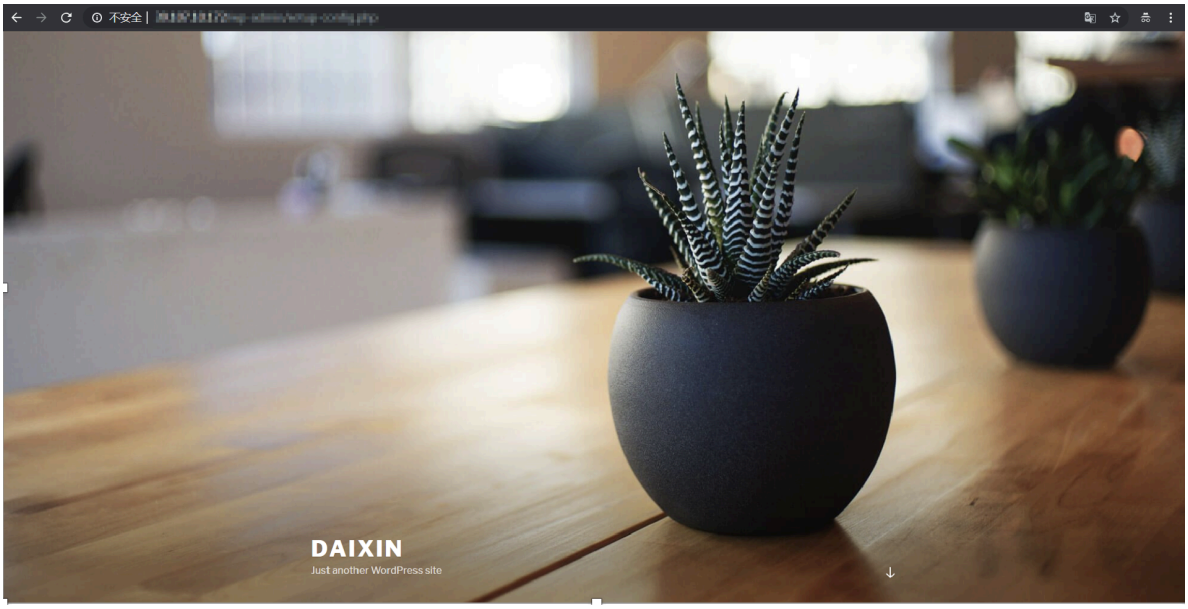


- 配置镜像：在镜像列表的下拉框内选择您所创建的镜像，镜像选中后会在配置镜像后面显示您所选择的镜像。
- 启动命令设置（可选）：请参见#unique_7配置。
- 环境变量设置（可选）：请参见如何设置环境变量配置。
- Hosts 绑定设置（可选）：请参见如何设置 Hosts 绑定配置。
- 应用健康检查（可选）：请参见如何设置应用健康检查配置。
- 日志收集设置（可选）：请参见如何设置日志收集配置。

5. 进入应用详情页，查看应用的基本信息和实例部署信息。当实例部署信息页面显示实例的运行状态为 Running 时，表示应用成功发布。

6. 进入应用详情的基本信息页面，在应用访问设置区域，单击添加公网 SLB 访问，进入添加公网 SLB 访问页面。在对话框中设置 SLB 的监听规则，SLB 服务监听规定了如何将请求转发给后端服务器。一个 SLB 实例至少添加一条监听规则。设置完监听参数后单击确定。

7. 通过设置的公网 SLB 来访问 Wordpress 应用。



为 Wordpress 应用添加公网访问权限

参考 #unique_8，为 Wordpress 应用添加公网访问权限。

为 Wordpress 应用设置跨区域的 RDS 数据库

1. 开通 RDS 服务，在购买 RDS 实例时，需选择地域为华东1（杭州），设置可用区为华东 1 可用区 F，选择网络类型为专有网络。

2. 进入 RDS 管理控制台，在左侧导航栏单击实例列表。选择您刚刚所创建的 RDS 实例，单击实例名称进入 RDS 实例管理页面。
3. 单击申请外网地址。在申请外网地址对话框中单击确定完成申请。

4. 申请后申请外网地址右边的按钮会变成设置白名单。单击设置白名单进入数据安全性页面，在该页面的白名单设置页签内，单击切换高安全白名单模式（推荐），并在弹出的确认框中单击确认切换。

5. 在白名单设置页签内，单击添加白名单分组。

6. 在添加白名单分组页面内，设置分组名称和组内白名单。此处设置组内白名单为 0.0.0.0/0，即允许所有的外网都可访问。设置完毕后单击确定。

7. 返回 RDS 实例管理页面的申请外网地址的外网地址。

8. 在 RDS 实例左侧导航栏单击账号管理，在用户账号页签内单击创建账号。然后按照页面提示设置账号信息。设置完成后单击确定。

9. 本地测试是否可以通过外网访问 RDS 应用。

```
vagrant@dev:~$ mysql -h rm-[redacted].rds.aliyuncs.com -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 535
Server version: 5.7.18-log Source distribution

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

2 应用访问阿里云数据库

2.1 如何设置 RDS 白名单

创建 SAE 应用之后，如果你需要访问 RDS 数据库，需要设置 RDS 白名单。

背景信息

不同场景下，白名单设置的内容不同。本文我们将从以下两个场景来分别说明白名单设置的相关操作。

- 场景一：应用访问本 VPC 内的 RDS 数据库
- 场景二：应用跨 VPC 或跨 Region 访问 RDS 数据库

场景一：应用访问本 VPC 内的 RDS 数据库

1. 登录 RDS 管理控制台。
2. 在控制台页面左上角，选择实例所在地域。

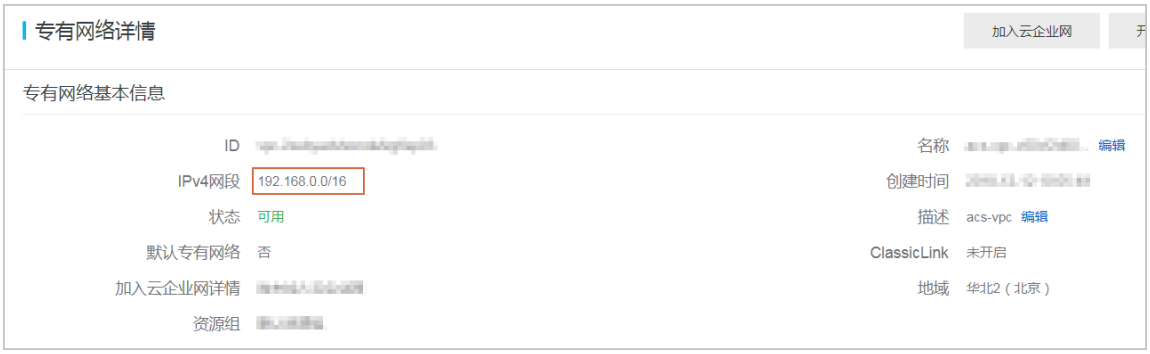
> **注意:**
> 目前 SAE 现已开放了华北 2（北京）、华东 1（杭州）、华东 2（上海）和华南 1（深圳）地域。

3. 在左侧导航栏单击实例列表，然后在云数据管理的基本信息页签单击具体实例名称。
4. 在实例基本信息页面左侧导航栏中单击数据安全性。
5. 在数据安全性页面的白名单设置页签中，单击 default 区域右侧的修改按钮。

6. 在弹出的对话框中，将 SAE 应用所在的 VPC 网络的网段地址配置在白名单输入框中。

   a. 登录 VPC 控制台，在专有网络列表中找到应用所在的 VPC，单击该 VPC 的名称进入专有网络详情页面。

   b. 复制应用所在的 VPC 的 IPv4 网段。



   c. 在组内白名单设置框中粘贴该 VPC 的 IPv4 网段地址，然后单击确定。

7. 在完成以上设置后，您的 SAE 应用就能访问本 VPC 内的 RDS 数据库了。

场景二：应用跨 VPC 或跨 Region 访问 RDS 数据库

不同 VPC 和不同 Region 之间逻辑上完全隔离，故常规情况下不能跨 VPC 和跨 Region 访问 RDS 数据库。若您的应用想跨 VPC 或跨 Region 访问 RDS 数据库，请按照下面步骤进行相关配置。

1. 前提准备

   参考 SAE 应用如何访问公网购买 NAT 网关和弹性公网 IP 组合包并保证 SAE 应用可以访问公网。

2. 设置白名单

a. 参考场景一：应用访问本 VPC 内的 RDS 数据库步骤 1~5 进入修改白名单分组对话框。

b. 在修改白名单分组对话框中，将 SAE 应用购买的弹性公网 IP 配置在白名单输入框中。

A. 登录 VPC 控制台，在左侧导航栏单击 NAT 网关，复制应用实例所配置的弹性公网 IP。

B. 在组内白名单设置框中粘贴该 VPC 的 弹性公网 IP地址，然后单击确定。

c. 在完成以上设置后，您的 SAE 应用就能跨 VPC、跨 Region 访问 RDS 数据库了。

2.2 如何设置 Redis 白名单

创建 SAE 应用之后，如果你需要访问 Redis 数据库，需要设置 Redis 白名单。

背景信息

不同场景下，白名单设置的内容不同。本文我们将从以下两个场景来分别说明白名单设置的相关操作。

- 场景一：应用访问本 VPC 内的 Redis 数据库
- 场景二：应用跨 VPC 或跨 Region 访问 Redis 数据库

场景一：应用访问本 VPC 内的 Redis 数据库

1. 登录 Redis 管理控制台。
2. 在控制台页面左上角，选择实例所在地域。

> **注意:**
> 目前 SAE 仅开放了华北 2（北京）和华东 1（杭州）地域，故请选择华北 2（北京）或华东 1（杭州）地域。

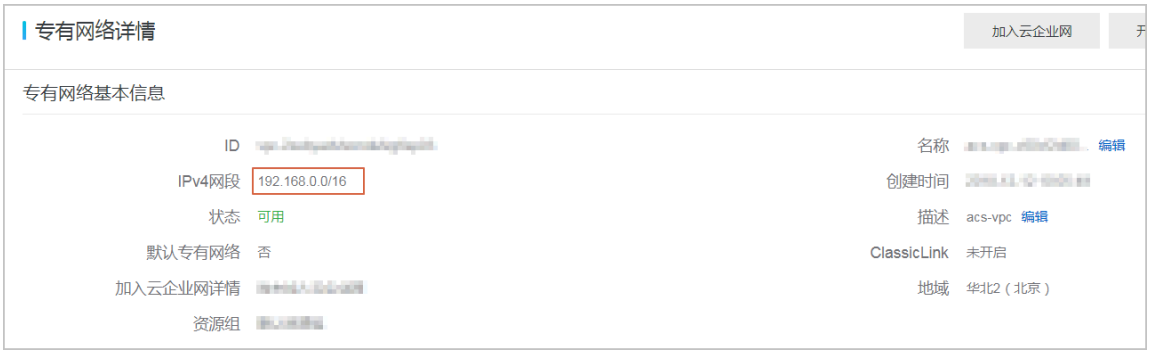
> **注意:**
> 目前 SAE 现已开放了华北 2（北京）、华东 1（杭州）、华东 2（上海）和华南 1（深圳）地域。

3. 在左侧导航栏单击实例列表，然后单击具体实例名称。
4. 在实例信息页面左侧的导航栏中单击白名单设置。
5. 单击 default 区域框右侧的修改。

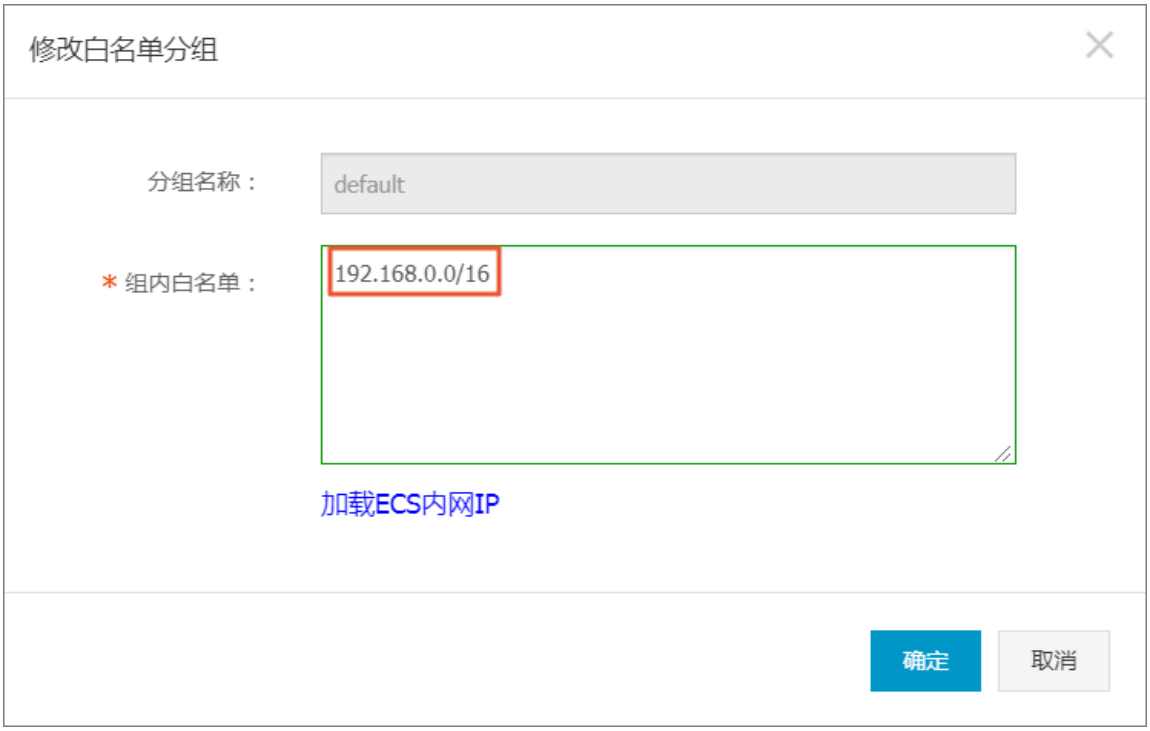
6. 在弹出的对话框中，将 SAE 应用所在的 VPC 网络的网段地址配置在白名单输入框中。

   a. 登录 VPC 控制台，在专有网络列表中找到应用所在的 VPC，单击该 VPC 的名称进入专有网络详情页面。

   b. 复制应用所在的 VPC 的 IPv4 网段。



   c. 在组内白名单设置框中粘贴该 VPC 的 IPv4 网段地址，然后单击确定。



7. 在完成以上设置后，您的 SAE 应用就能访问本 VPC 内的 Redis 数据库了。

场景二：应用跨 VPC 或跨 Region 访问 Redis 数据库

不同 VPC 和不同 Region 之间逻辑上完全隔离，故常规情况下不能跨 VPC 和跨 Region 访问 Redis 数据库。若您的应用想跨 VPC 或跨 Region 访问 Redis 数据库，请按照下面步骤进行相关配置。

1. 前提准备

   参考#unique_8 购买 NAT 网关和弹性公网 IP 组合包并保证 SAE 应用可以访问公网。

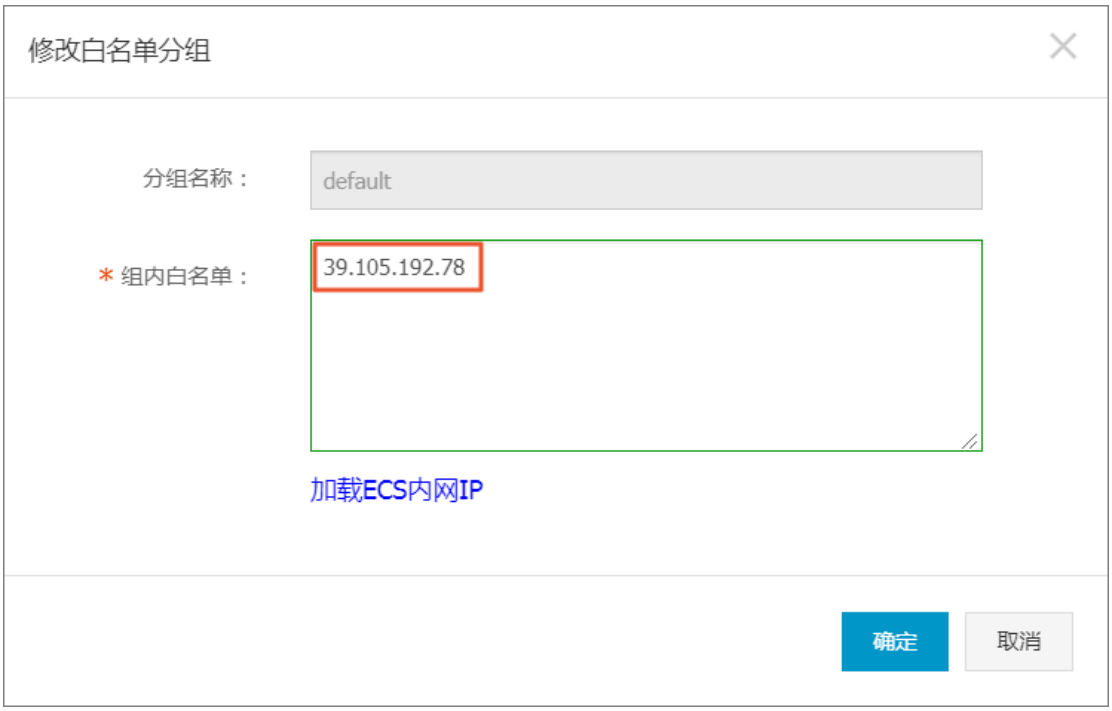
2. 设置白名单

a. 参考场景一：应用访问本 VPC 内的 Redis 数据库步骤 1~5 进入修改白名单分组对话框。

b. 在修改白名单分组对话框中，将 SAE 应用购买的弹性公网 IP 配置在白名单输入框中。

A. 登录 VPC 控制台，在左侧导航栏单击 NAT 网关，复制应用实例所配置的弹性公网 IP。

B. 在组内白名单设置框中粘贴该 VPC 的 弹性公网 IP地址，然后单击确定。



c. 在完成以上设置后，您的 SAE 应用就能跨 VPC、跨 Region 访问 Redis 数据库了。

2.3 如何设置 MangoDB 白名单

创建 SAE 应用之后，如果你需要访问 MangoDB 数据库，需要设置 MangoDB 白名单。

背景信息

不同场景下，白名单设置的内容不同。本文我们将从以下两个场景来分别说明白名单设置的相关操作。

- 场景一：应用访问本 VPC 内的 MangoDB 数据库

- 场景二：应用跨 VPC 或跨 Region 访问 MangoDB 数据库

场景一：应用访问本 VPC 内的 MangoDB 数据库

1. 登录 MangoDB 管理控制台。
2. 在控制台页面左上角，选择实例所在地域。

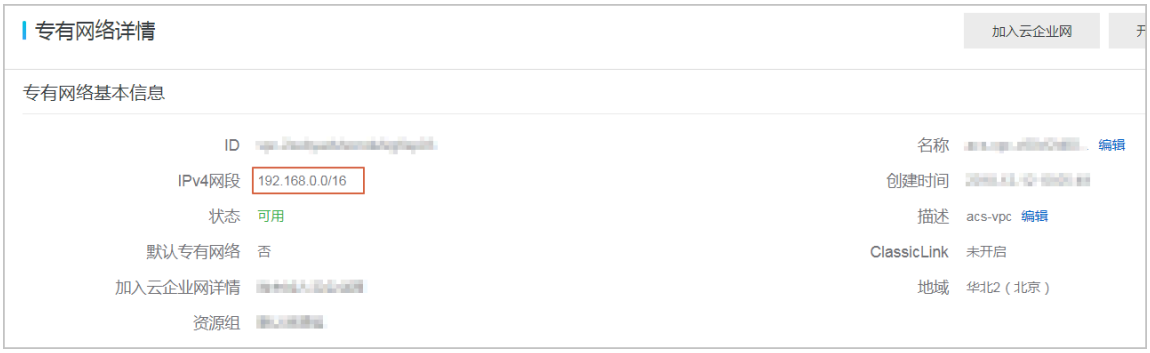
> **注意:**
> 目前 SAE 现已开放了华北 2（北京）、华东 1（杭州）、华东 2（上海）和华南 1（深圳）地域。

3. 在左侧导航栏单击副本集实例列表或分片集群实例列表，找到目标实例，单击实例名称。
4. 在实例基本信息页面的左侧导航栏中，选择数据安全性 > 白名单设置
5. 在 default 分组右侧的操作列选择手动修改。

6. 在弹出的对话框中，将 SAE 应用所在的 VPC 网络的网段地址配置在白名单输入框中。

   a) 登录 VPC 控制台，在专有网络列表中找到应用所在的 VPC，单击该 VPC 的名称进入专有网络详情页面。

   b) 复制应用所在的 VPC 的 IPv4 网段。



   c) 在允许访问IP名单设置框中粘贴该 VPC 的 IPv4 网段地址，然后单击确定。

7. 在完成以上设置后，您的 SAE 应用就能访问本 VPC 内的 MangoDB 数据库了。

场景二：应用跨 VPC 或跨 Region 访问 MangoDB 数据库

不同 VPC 和不同 Region 之间逻辑上完全隔离，故常规情况下不能跨 VPC 和跨 Region 访问 MangoDB 数据库。若您的应用想跨 VPC 或跨 Region 访问 MangoDB 数据库，请按照下面步骤进行相关配置。

前提准备

参考 SAE 应用如何访问公网购买 NAT 网关和弹性公网 IP 组合包并保证 SAE 应用可以访问公网。

设置白名单

1. 参考场景一：应用访问本 VPC 内的 MangoDB 数据库步骤 1~5 进入修改白名单分组对话框。
2. 在修改白名单分组对话框中，将 SAE 应用购买的弹性公网 IP 配置在白名单输入框中。

   a) 登录 VPC 控制台，在左侧导航栏单击 NAT 网关，复制应用实例所配置的弹性公网 IP。

   b) 在允许访问IP名单设置框中粘贴该 VPC 的 弹性公网 IP 地址，然后单击确定。

3. 在完成以上设置后，您的 SAE 应用就能跨 VPC、跨 Region 访问 MangoDB 数据库了。