

ALIBABA CLOUD

# Alibaba Cloud

云防火墙  
业务可视

文档版本：20200818

 阿里云

## 法律声明

阿里云提醒您在使用或阅读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  |
|--|------------------------------------|---|
|  危险   | 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。   |  危险<br>重置操作将丢失用户配置数据。          |
|  警告   | 该类警示信息可能会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<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
|  注意   | 用于警示信息、补充说明等，是用户必须了解的内容。           |  注意<br>权重设置为0，该服务器不会再接受新请求。    |
|  说明 | 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<br>您也可以通过按Ctrl+A选中全部文件。  |
| >  | 多级菜单递进。                            | 单击设置> 网络> 设置网络类型。   |
| <b>粗体</b>  | 表示按键、菜单、页面名称等UI元素。                 | 在结果确认页面，单击确定。   |
| <code>Courier</code> 字体  | 命令或代码。                             | 执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。  |
| <i>斜体</i>  | 表示参数、变量。                           | <code>bae log list --instanceid</code><br><i>Instance_ID</i>  |
| [ ] 或者 [a b]   | 表示可选项，至多选择一个。                      | <code>ipconfig [-all -t]</code>   |
| { } 或者 {a b}   | 表示必选项，至多选择一个。                      | <code>switch {active stand}</code>  |

# 目录

|          |    |
|----------|----|
| 1.自定义分组  | 05 |
| 2.应用分组可视 | 11 |

# 1.自定义分组

云防火墙通过业务间的流量可视化，帮助用户了解业务之间的访问关系，以此判断执行什么样的访问控制策略。

## 前提条件

在实现流量可视化之前，用户需先创建业务区、应用组，并将应用添加到业务区和应用组，以建立应用和应用组、业务区之间的关系。

## 背景信息

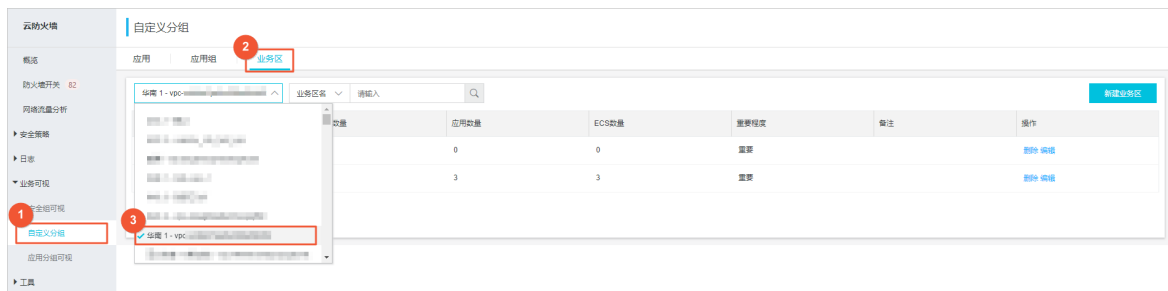
您需要提前了解以下概念：

- **业务区**：业务区是东西向业务可视中，构成用户某个业务的各个应用组的集合，通常是按您实际业务的类型进行分类。例如：门户网站业务区（将包含Web应用组、DB应用组）等。
- **应用组**：应用组是东西向业务可视中，提供的相同或相似服务的应用集合。例如：所有部署了MySQL的ECS可以归属到同一个DB应用组。
- **应用**：应用是东西向业务可视的最小单位。默认情况下，一个应用等于一台ECS上所有开放端口的集合。您可以通过指定端口克隆应用来创建新的应用。

## 步骤一：创建业务区

1. 登录**云防火墙控制台**。
2. 单击导航栏的业务可视 > 自定义分组 > 业务区。
3. 在业务区页签左上角选择您要创建的业务区所属的VPC。

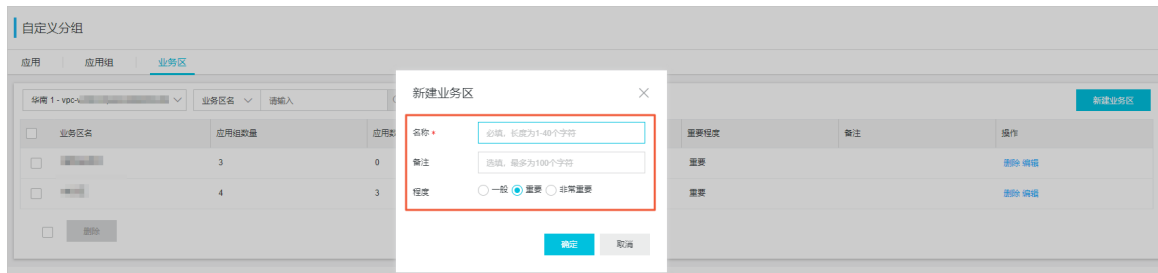
**说明** VPC包括用户已有的VPC网络和ECS经典网络。每个业务区必须并且只能属于一个VPC。



4. 单击右上角**新建业务区**。

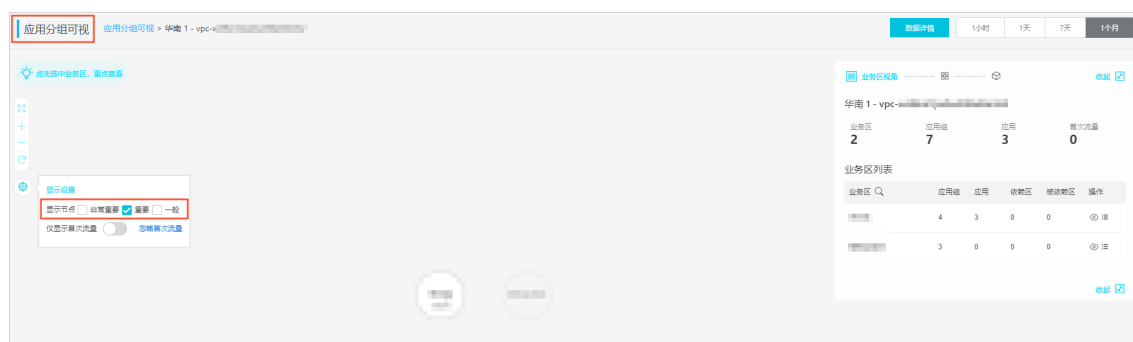


5. 在**新建业务区**对话框中配置业务区信息。



- **名称**：业务区的命名，手动输入。长度范围为1-40个字符。
- **备注**：业务区的备注信息。
- **程度**：业务区的重要程度，帮助您在业务关系可视图清晰区分不同重要程度的业务区。可选择**一般**、**重要**和**非常重要**3个程度。

您可以在应用分组可视页面，通过筛选不同的重要程度等级，查看对应重要级别的业务区。



6. 单击确定，完成业务区的创建。

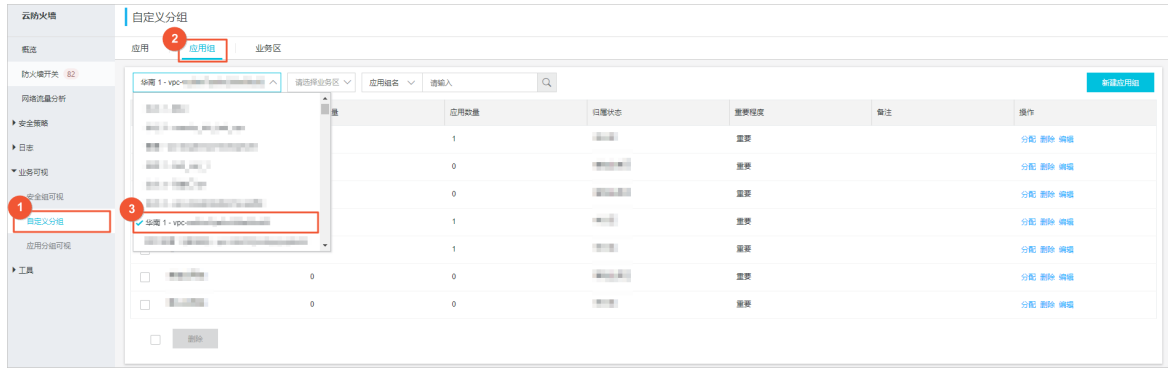
业务区创建完成后，会归属到您之前选择的VPC中。您可在业务区列表中，对业务区基本信息进行编辑或删除业务区。

**说明** 业务区下存在应用组时，不可删除业务区。

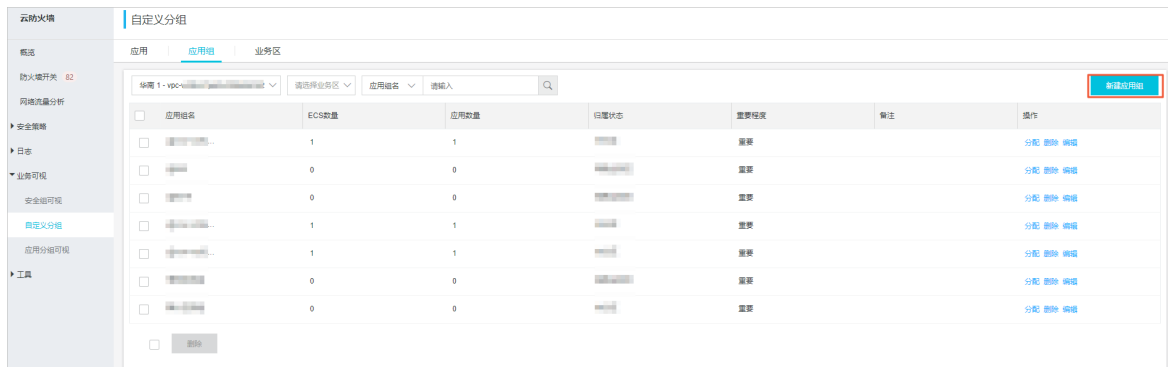


## 步骤二：创建应用组

1. 登录**云防火墙控制台**。
2. 单击导航栏的业务可视 > 自定义分组 > 应用组。
3. 在应用组页签左上角选择您要创建的应用组所属的VPC。



4. 单击右上角新建应用组。

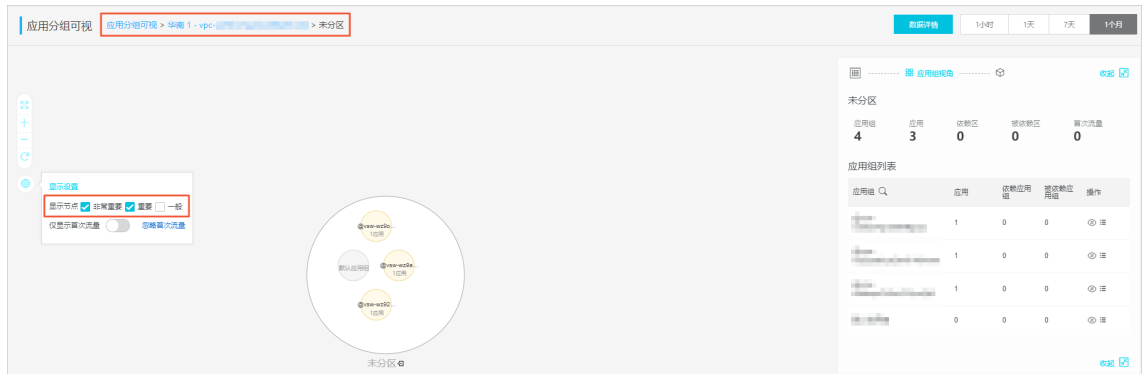


5. 在新建应用组对话框中配置应用组的信息。



- **名称**：应用组的命名，手动输入。长度范围为1-40个字符。
- **备注**：应用组的备注信息。
- **程度**：应用组的重要程度，帮助您在业务关系可视图清晰区分不同重要程度的业务区。可选择**一般**、**重要**和**非常重要**3个程度。

您可以在应用分组可视页面，双击打开某个业务区后，通过筛选不同的重要程度等级，查看对应重要级别的应用组。



- 业务区：可选选择已有业务区和新建业务区。
  - 选择了选择已有业务区选项，则需在下方名称下拉框中选择之前您已创建好的业务区名称。



- 如果选择新建业务区，则需在下方填写新建业务区的名称、备注信息并选择重要程度。

- 单击确定，完成应用组的创建。
- (可选步骤) 单击操作栏的分配，可修改应用组所属的业务区。





完成业务区分配后，业务区页面的应用组数量将会同步更新。

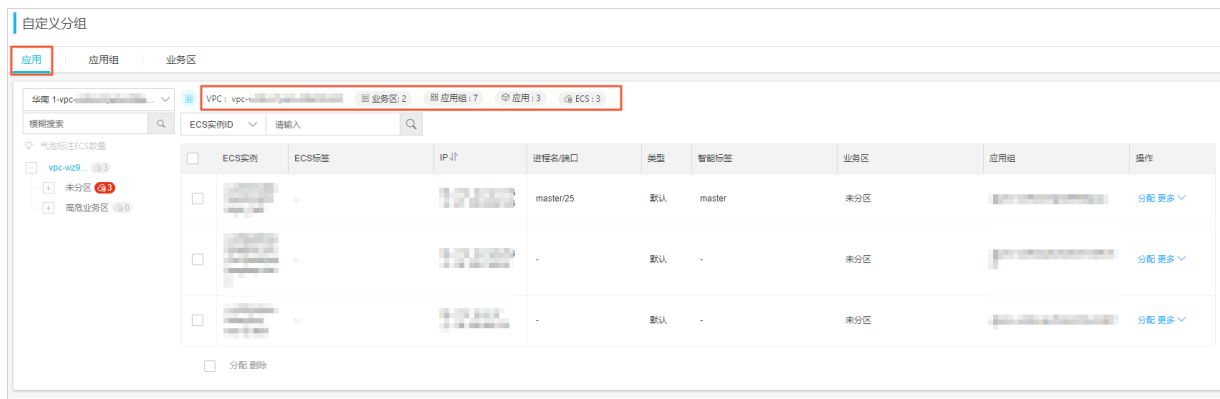


应用组创建完成后，还可在应用组列表中，对应用组的基本信息进行编辑或删除应用组。

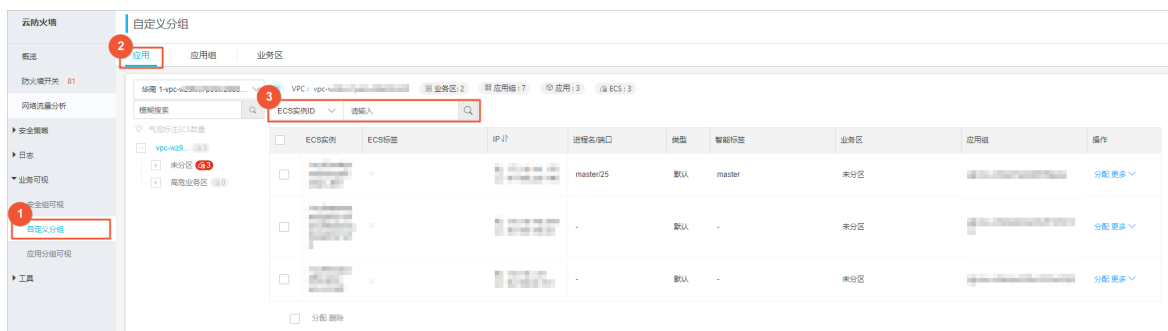
**说明** 应用组下存在应用时，不可删除应用组。

### 步骤三：为应用分配应用组和业务区

您可在应用页面查看云防火墙中已有的业务区、应用组、应用和ECS数量。



1. 登录云防火墙控制台。
2. 单击导航栏的业务可视 > 自定义分组 > 应用。
3. 通过搜索功能定位到需要操作的应用。



4. 单击操作栏的分配，将该应用添加到之前您已创建好的业务区和应用组中。

**说明** 完成应用分配后，业务区页面的业务区数量和应用组数量将会同步更新。



5. (可选步骤) 您也可以在应用列表中，单击右侧操作栏的克隆，复制现有的应用。

云防火墙开通后会对每个ECS创建一个默认的应用，访问ECS的流量会自动映射到该默认应用中。如果ECS中有多个应用属于不同的业务类型，您可以通过克隆操作创建新的应用，并为该应用分配另一个业务区和应用组。克隆应用时，可对应用所属的ECS实例ID、侦听端口和进程名进行修改。

## 后续操作

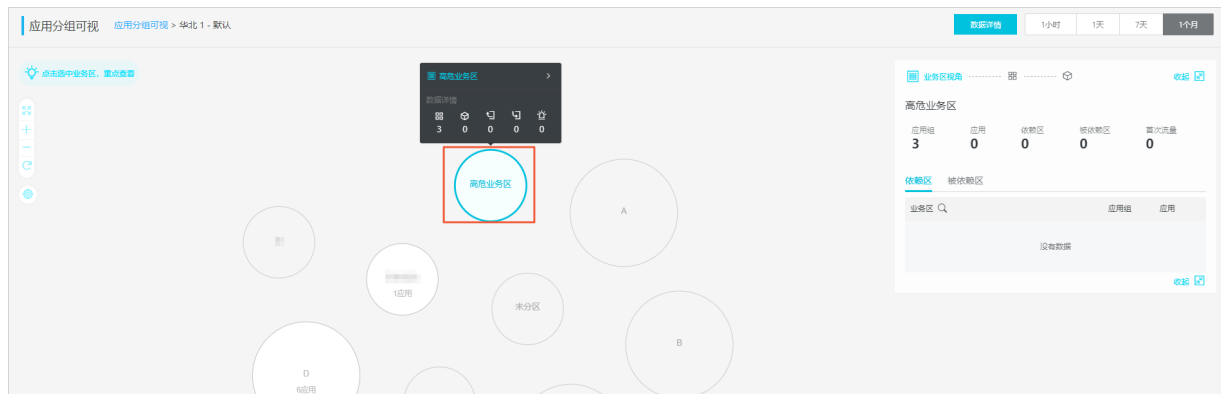
[应用分组可视](#)

## 2.应用分组可视

业务区和应用组创建完成后，您可在应用分组可视页面中查看云防火墙某个区域下存在的业务区、应用组、应用、vSwitch（虚拟交换机）和ECS的数量。

### 背景信息

在应用分组可视页面单击云防火墙的某个区域名称，跳转至该区域下的应用分组可视页面。您可在这个页面中查看当前区域下所有业务区的可视图。单击业务区名称，展示该业务区中含有的应用组、应用、依赖区、被依赖区、首次流量等信息。



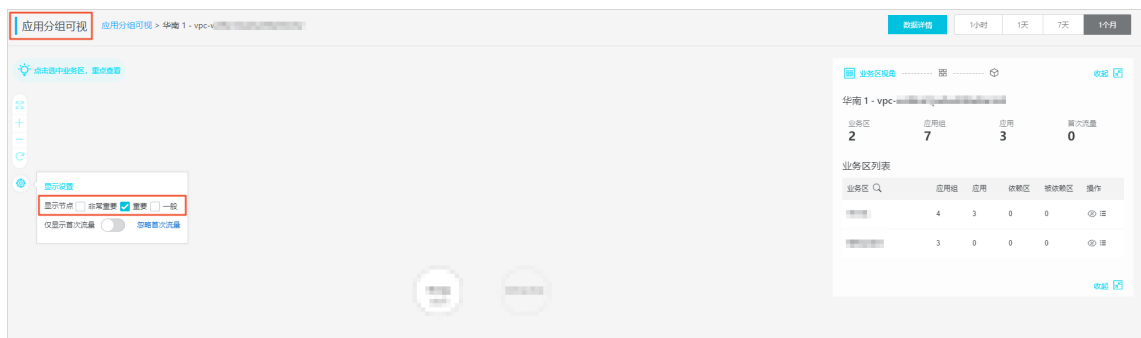
### 操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击业务可视 > 应用分组可视。
3. 在应用分组可视页面，定位到需要查看的VPC网络，单击该VPC模块。



4. 在该VPC网络下的应用分组可视页面，您可以查看业务区内容的访问情况以及选定业务区的依赖和被依赖关系。

- 单击应用分组可视页面左侧的显示设置，设置展示不同重要程度的业务区。



① 说明 在应用分组可视页面中，您可以查看业务的类型。例如：中心标有应用的圆圈表示应用组；中心标有业务区的圆圈表示业务区。圆圈大小代表重要程度的高低，圆圈越大重要程度越高。

在应用分组可视页面右侧展示了该VPC网络下业务区、应用组、应用和首次流量的统计数据，以及该VPC网络下所有业务区的列表信息。



- 单击应用分组可视页面右侧的点击查看数据详情，可打开该业务区的业务关系详情页面。在该页面中您可以查看业务区的业务节点和业务关系。

