

阿里云 专有网络VPC

通用配置

文档版本：20190916

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 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
##	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[]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>swich {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 管理配额.....	1
2 使用RAM对VPC进行权限管理.....	2

1 管理配额

您可以通过专有网络VPC控制台查询当前资源配额使用情况。如果某个资源的剩余配额不满足业务需求，您可以直接申请增加配额。

操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击配额管理。
3. 在配额管理页面，选择专有网络VPC页签，可以查看当前账号下专有网络VPC的资源使用情况。
4. 如果需要提升配额，可以单击操作列的申请，提交提升配额申请。
 - 申请数量：需要的资源配额数量，申请数量必须为数字且大于当前配额。专有网络VPC的资源默认使用限制，请参见[#unique_4](#)。
 - 申请原因：请详细描述申请配额的原因、业务场景和必要性。
 - 手机/固话：申请配额的用户电话号码。
 - 电子邮箱：申请配额的用户电子邮箱。
5. 单击确定。

系统会自动审批配额申请是否合理：

- 如果不合理，申请状态为拒绝。
- 如果合理，申请状态为通过，配额立即自动提升为申请的数量。

在申请历史列单击申请历史，可以查看配额申请历史。

2 使用RAM对VPC进行权限管理

本文介绍了通过RAM的权限管理功能，创建相应的权限策略，从而对专有网络（VPC）进行权限管理，以满足RAM用户操作VPC的多种需求。

前提条件

请确保您已经注册了阿里云账号。如还未注册，请先完成账号注册。详细信息，请参见[账号注册](#)。

基本信息

使用RAM对VPC进行权限管理前，请先了解几个常用的权限策略。

权限策略	描述
AliyunVPCFullAccess	为RAM用户授予VPC的完全管理权限。
AliyunVPCReadOnlyAccess	为RAM用户授予VPC的只读访问权限。



说明：

VPC的权限定义，请参见[#unique_6](#)。

将自定义权限策略授权给RAM用户

1. 创建自定义权限策略。

详细信息，请参见[#unique_7](#)和[VPC授权样例](#)。

2. 在权限策略管理页面，找到目标权限策略，单击其权限策略名称。

3. 单击引用目录页签，然后单击新增授权。

4. 在添加权限页面，被授权主体处输入需要授权的用户名称或ID，然后单击确定。



说明：

您也可以直接对用户或用户组授予创建好的权限策略，详情信息，请参见[#unique_8](#)和[#unique_9](#)。

VPC授权样例

· 示例1：对VPC的管理权限

假设您的账号为1234567，授权管理该账号下的所有VPC，使某个RAM用户具有操作所有VPC的权限。

```
{
  "Version": "1",
  "Statement": [
    {
```

```

        "Effect": "Allow",
        "Action": [
            "vpc:*"
        ],
        "Resource": [
            "acs:vpc:*:1234567:*/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ecs:*Describe*"
        ],
        "Resource": [
            "*"
        ]
    }
]
}

```

· 示例2：对VPC中VSwitch的管理授权

假设您只想授权青岛Region下的VSwitch的管理权限，使某个RAM用户可以对青岛Region下的VSwitch进行创建/删除/绑定子网路由/解绑子网路由的操作，对于其它地域的VSwitch只有查看权限。

```

{
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:*Describe*",
                "vpc:*VSwitch*",
                "vpc:*RouteTable*"
            ],
            "Resource": [
                "acs:vpc:cn-qingdao:*:*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:*Describe*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}

```

· 示例3：只允许操作特定地域下的路由表以及路由表中的路由条目

假设您的账号为11111111，在多个地域创建了VPC，该权限只授予某个RAM用户对杭州地域VPC的操作权限，且操作权限仅限于：允许新增/删除路由条目，允许创建子网路由并绑定VSwitch，对于其它地域的云产品只有查看权限。

```

{

```

```

    "Version": "1",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "ecs:*Describe*"
        ],
        "Resource": [
          "*"
        ],
        "Condition": {}
      },
      {
        "Effect": "Allow",
        "Action": [
          "slb:*Describe*"
        ],
        "Resource": [
          "*"
        ],
        "Condition": {}
      },
      {
        "Effect": "Allow",
        "Action": [
          "rds:*Describe*"
        ],
        "Resource": [
          "*"
        ],
        "Condition": {}
      },
      {
        "Effect": "Allow",
        "Action": [
          "vpc:*Describe*",
          "vpc:*RouteEntry*",
          "vpc:*RouteTable*"
        ],
        "Resource": [
          "acs:vpc:cn-hangzhou:11111111:*/*"
        ],
        "Condition": {}
      }
    ]
  }

```

- 示例4：只允许修改特定路由表中的路由条目

假设您只希望RAM用户新增/删除特定路由表中的路由条目。

```

{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*RouteEntry*"
      ],
      "Resource": [
        "acs:vpc:cn-qingdao:*:routetable/vtb-m5e64ujkb7
xn5zlq0xxxx"
      ]
    }
  ]
}

```



```
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:*Describe*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```