

# 阿里云

## 实时计算（流计算） 准备工作

文档版本：20220120

## 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 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 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 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 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 <b>确定</b> 。
Courier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。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <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.RAM用户授权	05
2.开通服务和创建项目	07
3.角色授权	12
3.1. 独享模式角色授权	12
3.2. 共享模式角色授权	13

# 1.RAM用户授权

您可以使用阿里云账号购买和创建实时计算项目。同时，阿里云账号也可以授权RAM用户使用阿里云账号创建的实时计算项目。本文为您介绍如何为RAM用户授权。

## 什么是RAM用户

RAM用户是RAM的一种实体身份类型，有确定的身份ID和身份凭证，它通常与某个确定的人或应用程序一一对应。RAM用户具备以下特点：

- RAM用户由阿里云账号（主账号）或具有管理员权限的其他RAM用户、RAM角色创建，创建成功后，归属于该阿里云账号，它不是独立的阿里云账号。
- RAM用户不拥有资源，不能独立计量计费，由所属的阿里云账号统一付费。
- RAM用户必须在获得授权后，才能登录控制台或使用API访问阿里云账号下的资源。
- RAM用户拥有独立的登录密码或访问密钥。
- 一个阿里云账号下可以创建多个RAM用户，对应企业内的员工、系统或应用程序。

您可以创建RAM用户并为其授权，实现不同RAM用户拥有不同资源访问权限的目的。当您的企业存在多用户协同访问资源的场景时，使用RAM可以按需为用户分配最小权限，避免多用户共享阿里云账号密码或访问密钥，从而降低企业的安全风险。

## 授权操作

### 1. 创建RAM用户

创建RAM用户具体步骤请参见[创建RAM用户](#)。

#### ② 说明

- 第一次使用RAM需要进行初始化工作，具体步骤请参见[设置RAM用户密码强度](#)和[设置RAM用户安全策略](#)。
- 为了保证账号安全，实时计算设置了账号验证的功能。如果长时间没有对作业进行操作，系统将会发送短信和邮件进行身份信息验证。

### 2. 创建自定义权限策略

在RAM用户中添加自定义权限策略的具体步骤请参见[创建自定义权限策略](#)。实时计算授权策略代码如下。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "stream:*",
      "Resource": "acs:stream:*:*:*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:PassRole",
      "Resource": "acs:ram:*:*:*",
      "Effect": "Allow"
    }
  ]
}
```

② 说明 实时计算授权策略支持授权至项目粒度，即可以为不同的RAM用户分别授权不同的项目。如果需要为RAM用户授权单个项目，请将以上代码中的Resource修改为"Resource": "acs:stream:\*:\*:projectname"，其中projectname为需要授权的项目名称。

### 3. 授权用户或用户组

将上述权限策略授权添加至指定用户或者用户组，具体步骤请参见[为RAM用户授权](#)和[为用户组授权](#)。

### 4. 使用RAM用户登录实时计算控制台

在[RAM控制台](#)概览页面中，[账号管理](#)区域查看RAM用户登录地址。

## 2. 开通服务和创建项目

本文为您介绍如何开通实时计算Flink版共享模式和独享模式服务，以及如何创建共享模式的项目、独享模式的集群和项目。

### 独享模式开通流程

#### ② 说明

- 独享模式已于2021年4月28日暂停新购，目前仅支持原有项目的扩缩容和续费操作。如果您有新购需求，推荐使用实时计算Flink全托管。如果您有其他问题，请[提交工单](#)。
- 独享模式集群仅能访问相同专有网络VPC、相同Region和相同安全组下的存储资源。如果需要访问其它VPC下的资源，请通过[高速通道](#)等方式连通网络。

独享模式在购买订单后，需要先创建集群，再创建项目。您可以参见[实时计算购买流程](#)。

#### 1. 开通服务

##### i. 登录[实时计算产品首页](#)

② 说明 请使用阿里云账号（不能使用阿里云RAM用户）开通服务和创建项目。如果您还没有阿里云账号，请先完成注册，注册步骤请参见。

- ii. 单击[管理控制台](#)。
- iii. 单击Blink独享集群下的[购买产品](#)，进入购买页面。
- iv. 单击[实时计算独享模式（包年包月）](#)或[实时计算独享模式（按量付费）](#)。
- v. 填写配置信息。根据需求选择地域、master型号、master数量、slave型号、slave数量和计费周期。

② 说明 关于集群配置，请参见[规格选择](#)。

- vi. 单击[立即购买](#)。
- vii. 选中服务协议。例如，[实时计算独享模式（包年包月）服务协议](#)。
- viii. 单击[去支付](#)。

#### 2. 创建集群

##### o 准备工作

- 实时计算Flink版独享模式开通时，实时计算Flink版会在您的VPC内创建安全组并申请弹性网卡，详情请参见[弹性网卡概述](#)。

 **说明** 请勿删除此安全组和弹性网卡，否则会造成集群无法创建成功。

- 如果已有专有网络VPC，请选择实时计算Flink版需要访问的VPC。
- 如果没有VPC，请开通阿里云VPC服务。如何开通专有网络VPC请参见[网络规划](#)。

 **说明** 搭建专有网络时，请确保以下两点：

- VPC内的ECS充足。如果ECS不足，请您[提交工单](#)。
- vSwitch内可用IP个数，要大于等于实时计算Flink版集群节点个数。详情请参见[查看实时计算集群节点信息](#)和[使用交换机](#)。

- 为了保护您的数据安全，独享集群中您上传的UDF包，都会保存到您的OSS存储空间中，请选择已有OSS存储空间。如果没有OSS存储空间，请先创建OSS存储空间。OSS存储空间创建方法，请参见[创建存储空间](#)。
- 完成[独享模式角色授权](#)。

o 创建集群步骤

- a. 订单支付成功后，单击[管理控制台](#)。
- b. 在[集群列表](#)页面，单击[创建集群](#)。

 **说明** 新购订单后，[集群管理](#) > [集群列表](#) > [新建集群](#)上，显示红色数字，表明存在未创建项目的订单。

- c. 在[选择订单](#)页面，[订单号](#)列表选择您的订单号。
- d. 在[基本信息](#)页面，填写[集群名称](#)和[集群备注](#)。
- e. 在[集群配置](#)页面填写配置信息。

 **说明** 您购买的上下游存储必须和实时计算Flink版所选集群存在于相同的Region、相同的VPC和相同的安全组。

### ■ OSS Bucket

选择保存您UDF的OSS存储空间。如果您没有OSS存储空间，请先[创建存储空间](#)。在创建存储空间（Bucket）时，**存储类型**请务必选择**标准存储**，此外，**读写权限**推荐选择**私有**，不能选择**公共读**。

**新建 Bucket** 创建存储空间 ×

**注意：** Bucket 创建成功后，您所选择的**存储类型、区域**不支持变更。

Bucket 名称  0/63

Bucket 命名规范：

- 只能包含小写字母，数字和短横线
- 必须以小写字母和数字开头和结尾
- 长度限制在 3-63 之间

区域

相同区域内的产品内网可以互通；订购后不支持更换区域，请谨慎选择

Endpoint oss-cn-beijing.aliyuncs.com

存储类型  标准存储  低频访问  归档存储

标准：高可靠、高可用、高性能，数据会经常被访问到。  
[如何选择适合您的存储类型？](#)

读写权限  私有  公共读  公共读写

私有：对文件的所有访问操作需要进行身份验证。

### ■ VPC

针对需要连接的VPC，编辑自定义名称，并选择需要连接的VPC。



**说明** 实时计算只能识别自定义编辑后的VPC名称。

### ■ Zone

VPC参数正确选择后，可选用的Zone参数会自动显示。

 说明 以下两种原因可能导致无可选Zone或者vSwitch:

- 所选Zone（可用区）内，ECS库存不足。创建ECS的操作步骤，请参见[使用向导创建实例](#)。
- 所选vSwitch内可用IP个数，小于实时计算Flink版集群节点个数。详情请参见[查看实时计算集群节点信息](#)和[使用交换机](#)。

### ■ Blink网段

可用的Blink网段会自动显示。

f. 在**确认信息**页面，单击**创建**。

 说明 集群创建过程，即集群状态从启动中变化为运行中，大概需要半个小时，如果长时间没有完成集群创建，请您[提交工单](#)。

## 3. 新建项目

- 在**集群管理 > 集群列表**，单击目标集群操作列下的**创建项目**。
- 在**新建项目**页面，填写项目名称和项目备注，在指定CU右侧，滑动指针，选择目标CU。
- 单击**创建**。

## 共享模式开通流程

 说明 实时计算Flink版共享模式已于2019年12月24日正式下线，不再支持共享模式新项目的购买，仅支持原有项目的扩缩容、续费操作。如果您有新购需求，推荐使用实时计算Flink版独享模式或Flink半托管/ACK模式。

### 1. 开通服务

- 登录[实时计算产品首页](#)

 说明 请使用阿里云账号（不能使用阿里云RAM用户）开通服务和创建项目。如果您还没有阿里云账号，请先完成注册，注册步骤请参见。

- 单击**管理控制台**。
- 单击**共享模式（包年包月）下的购买**。
- 根据需求选择**区域、计算资源和购买时长**。
- 单击**立即购买**。
- 选中**服务协议**。
- 单击**去支付**。

### 2. 创建项目

 说明 在创建项目或第一次进入项目时，如果出现类似授权错误或提醒，请参见[共享模式角色授权完成角色授权](#)，详情请参见[共享模式角色授权](#)。

- i. 支付完成后，在支付 > 支付完成页面，单击实时计算控制台。
- ii. 在页面顶部菜单栏上，鼠标悬停在用户头像上，单击项目管理。
- iii. 在项目管理 > 项目列表页面，单击右上角新建项目

 说明 订单支付成功后，如果新建项目上显示红色数字标志，表明存在未创建项目的订单。

- iv. 在创建项目页面，选择订单号、填写项目名称和项目备注信息。
- v. 单击创建。

 说明 项目创建完成后，可在项目管理 > 项目列表查看目标项目。

## 3.角色授权

### 3.1. 独享模式角色授权

本文为您介绍如何完成独享模式角色授权。

#### 创建角色

在创建集群过程中需要您创建角色AliyunStreamDefaultRole，具体操作流程请参见[自动化角色授予流程](#)。

 **说明** 如果AliyunStreamDefaultRole角色已存在，则不必重复创建。

#### 添加授权策略

完成RAM角色创建后，您可以将指定的授权策略添加至RAM角色中。

1. 登录RAM控制台。
  - 云账号登录[RAM控制台](#)。
  - RAM用户登录[RAM控制台](#)。
2. 在左侧导航栏，单击[权限管理](#) > [权限策略管理](#)。
3. 单击[创建权限策略](#)。
4. 填写策略名称（本文以AliyunStreamDefaultRolePolicy为例）和备注。
5. 配置模式中，选择[可视化配置](#)或[脚本配置](#)。
  - **可视化配置**：单击[添加授权语句](#)，根据界面提示，配置权限效力、操作名称和资源等。
  - **脚本配置**：请参见[语法结构](#)编辑策略内容。
6. 在策略内容区域代码框中，输入以下代码，单击[确认](#)。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVpcs",
        "vpc:DescribeVSwitches"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateSecurityGroup",
        "ecs:AuthorizeSecurityGroup",
        "ecs:CreateNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:AttachNetworkInterface",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:CreateNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

 说明 以上授权策略中，以下两个权限可以在创建集群后删除：

- o ecs:CreateSecurityGroup
- o ecs:AuthorizeSecurityGroup

7. 在RAM角色管理页面底部的RAM角色名称列中，单击AliyunStreamDefaultRole操作列下的添加权限。
8. 在选择权限 > 自定义策略下方搜索栏中，输入AliyunOSSFullAccess。
9. 单击权限策略名称中的AliyunOSSFullAccess。
10. 在选择权限区域，单击系统权限策略 > 自定义策略。
11. 在选择权限 > 系统策略下方搜索栏中，输入AliyunStreamDefaultRolePolicy。
12. 单击权限策略名称中的AliyunStreamDefaultRolePolicy。
13. 单击确定。

## 3.2. 共享模式角色授权

本文为您介绍实时计算的角色授权操作，包括自动化角色授予流程、重新初始化流程和常见问题。

您开通实时计算服务时，需要先为实时计算的服务账号，授予系统默认角色AliyunStreamDefaultRole。

说明

- 仅当AliyunStreamDefaultRole被正确授予后，实时计算才能正常地调用相关服务（例如RDS）。
- 实时计算共享模式已于2019年12月24日正式下线，将不再支持共享模式新项目的购买，仅支持原有项目的扩缩容、续费操作。若有新购需求，推荐使用实时计算独享模式或Flink云原生模式。

### 自动化角色授予流程

1. 单击前往授权，进行角色授权。



说明

- 请先完成实时计算产品购买，产品购买步骤请参见[开通服务和创建项目](#)。
- 以上角色授权提示，仅在您没有正确授予实时计算服务账号默认角色时出现。

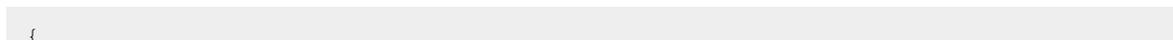
2. 单击AliyunStreamDefaultRole > 同意授权，完成角色授权。



说明 当完成以上授权步骤后，刷新实时计算的控制台，即可以进行业务操作。

### 当前角色授权信息查看

1. 登录RAM角色管理
2. 在RAM角色管理页面底部的RAM角色名称列中单击AliyunStreamDefaultRole。
3. 在AliyunStreamDefaultRole页面中单击权限管理 > AliyunStreamRolePolicy。
4. 在策略内容页签内查看实时计算当前策略信息，如下所示。



```
"Version": "1",
"Statement": [
  {
    "Action": [
      "ots:List*",
      "ots:DescribeTable",
      "ots:Get*",
      "ots:*Row"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "dhs:Create*",
      "dhs:List*",
      "dhs:Get*",
      "dhs:PutRecords",
      "dhs>DeleteTopic"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "log:List*",
      "log:Get*",
      "log:Post*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "mns:List*",
      "mns:Get*",
      "mns:Send*",
      "mns:Publish*",
      "mns:Subscribe"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "drds:DescribeDrdsInstance",
      "drds:ModifyDrdsIpWhiteList"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "rds:Describe*",
```

```

        "rds:ModifySecurityIps*"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "vpc:DescribeVpcs",
      "vpc:DescribeVSwitches"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "ecs:CreateSecurityGroup",
      "ecs:AuthorizeSecurityGroup",
      "ecs:CreateNetworkInterface",
      "ecs:DescribeNetworkInterfaces",
      "ecs:AttachNetworkInterface",
      "ecs:DescribeNetworkInterfacePermissions",
      "ecs:CreateNetworkInterfacePermission"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": "oss:*",
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

## 重新初始化

### 注意

- 删除AliyunStreamDefaultRole角色后，可能导致实时计算正在运行的作业瞬间无法读写上下游外部存储，直到后续重新初始化AliyunStreamDefaultRole角色后才能恢复正常。请务必确认这项操作对于线上实时计算业务造成的影响。
- RAM删除角色和流计算重新初始化操作均需要当前用户的阿里云账号或者经阿里云账号授权的RAM用户操作。

当您删除或修改AliyunStreamRolePolicy授权策略导致无法恢复时，您可以在RAM中删除AliyunStreamDefaultRole，并重新进入实时计算控制台，让实时计算重新启动[自动化角色授予流程](#)。

重新初始化步骤：

1. 登录[RAM角色管理](#)
2. 在RAM角色管理页面底部的RAM角色名称列中单击AliyunStreamDefaultRole。
3. 在AliyunStreamDefaultRole页面的权限管理页签中，单击AliyunStreamRolePolicy操作列下的移

除权限。

 说明 如果AliyunStreamRolePolicy已经删除，可跳过此步骤。

4. 单击AliyunStreamDefaultRole页面底部的RAM角色管理，返回RAM角色管理页面。
5. 在RAM角色管理页面底部，单击AliyunStreamDefaultRole的操作列下的删除。
6. 登录[实时计算控制台](#)。
7. 单击前往授权。
8. 单击同意授权。
9. 通过手机短信等验证方式，完成角色授权。

 说明 实时计算和RAM对于授权均有不同程度的缓存，有可能在删除角色或者授权角色后，实时计算仍然提示需要授权角色。此时系统已经完成授权任务，单击授权完毕即可。

## 常见问题

Q: RAM用户在操作数据存储的时候如果出现错误信息 **操作错误：RAM用户没有passRole权限，请到RAM对该RAM用户赋权。错误详情为：922019**。

A: 请先完成角色授权。详情请参见 [授权操作](#)。