

ALIBABA CLOUD

Alibaba Cloud

DataWorks

准备工作

文档版本：20220627

 阿里云

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
 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。
粗体	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 。
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. 开通并登录DataWorks	05
1.1. 开通DataWorks	05
1.2. 准备RAM用户	06
1.3. RAM用户登录并使用DataWorks	09
1.4. (进阶) RAM角色登录并使用DataWorks	11
2. 创建工作空间	18
3. 添加工作空间成员和角色	26
4. 空间管理员职责	30

1. 开通并登录DataWorks

1.1. 开通DataWorks

大数据开发治理平台 DataWorks为您提供专业高效、安全可靠的一站式大数据开发与治理平台，使用前您需要准备好阿里云账号开通DataWorks，开通后可授予RAM子账号登录使用DataWorks。本文为您介绍如何开通DataWorks。

背景信息

DataWorks的账号登录体系与阿里云保持一致，统一采用阿里云主账号或RAM账号登录的方式。

- 阿里云账号（即主账号）是阿里云资源的归属及使用计量计费的基本主体，负责生成本企业组织下的子账号，并对子账号进行管理、授权等操作。
- 子账号由主账号在RAM系统中创建并进行管理，其本身不拥有资源，也没有独立的计量计费，子账号由所属主账号统一控制和付费。

因此，使用DataWorks前，您需要准备一个阿里云账号，并通过RAM管理子账号。

步骤1：注册阿里云账号

仅阿里云主账号，或拥有 `AliyunBSSOrderAccess` 或者 `AliyunDataWorksFullAccess` 权限的RAM用户可以开通DataWorks服务，下面以从未注册过阿里云账号为例，为您介绍如何注册一个阿里云账号并完成账号的实名认证等安全配置，为开通并使用DataWorks做好准备。

如果您已有符合要求的阿里云账号，即可跳过此步骤，直接进行后续操作。

- 注册阿里云账号的操作请参见[创建阿里云账号](#)。
- 账号的实名认证操作请参见[实名登记常见问题](#)。

说明

- 为保证后续操作顺利进行，请务必完成实名认证操作。对于企业级用户，建议进行企业级认证，以获取更多的便利，同时建议您同步完成上述参考文档中其他各项安全配置，以保障账号的安全性。
- 账号创建成功后，作为阿里云系统识别的资源消费账号，会拥有非常高的权限。请您确保账号和密码的安全，切勿借给他人使用，并定期更新密码。

步骤2：开通DataWorks

1. 使用阿里云账号（主账号）登录[阿里云官网](#)后，进入[DataWorks产品首页](#)，单击[立即购买](#)，进入开通配置页面。

DataWorks为您提供了基础版、标准版、专业版、企业版旗舰版这几种不同的版本规格，不同版本规格支持的产品功能和价格不同，您可前往[DataWorks各版本详解](#)页面查看各个版本的详情后，选择开通合适的版本。

2. 选择开通地域。

当前DataWorks已在多个地域部署上线，您可以根据实际需要选择开通哪个地域。

3. 了解各按量付费项和计费详情。

页面为您展示DataWorks各功能模块的按量计费的标准详情，您可单击对应的详情链接了解详情。

4. 单击[立即购买](#)。

5. 根据界面提示确认参数信息，勾选同意服务协议后，单击**立即开通**，完成付费后即完成DataWorks的开通。

步骤3：登录并使用DataWorks

完成DataWorks开通后，您即可开始使用DataWorks进行数据开发、数据集成、数据治理等功能。通常，大数据的开发治理是由不同角色协同完成，例如，开发人员会进行数据开发、数据集成等操作，数据治理人员会进行数据治理操作，管理员会进行权限管控、管理配置等操作。

- 登录DataWorks。

- 使用RAM用户登录DataWorks。

为满足此类协同使用的场景，并同时满足账号安全、权限隔离等要求，您可以在开通的阿里云账号下新建不同的RAM账号，将RAM账号分配给不同人员，并给这些RAM账号授予不同的使用权限，后续不同人员角色使用各自的RAM账号来使用DataWorks。用阿里云RAM账号使用DataWorks的操作注意事项和主要流程请参见[RAM用户登录并使用DataWorks](#)。

- 创建或加入DataWorks工作空间。

工作空间是DataWorks管理任务、成员，分配角色和权限的基本单元。工作空间管理员可以加入成员至工作空间，并赋予工作空间管理员、开发、运维、部署、安全管理员或访客角色，以实现多角色协同工作，因此在使用DataWorks的数据开发等各个功能前，您需要先创建一个工作空间，或由某个工作空间的管理员为您授权，加入某个工作空间。

DataWorks为您提供多样的工作空间模式和完善的权限模型。

- 您可以根据需要选择开发生产环境隔离的**标准模式**工作空间，或不区分开发生产环境的**简单模式**工作空间，两种模式的对比介绍详情请参见[简单模式和标准模式的区别](#)。
- 您可以通过DataWorks的权限模型为不同角色授予不同的操作权限，以实现权限管控。DataWorks的权限模型详情请参见[DataWorks权限管控概述](#)。

创建工作空间及添加成员的操作详情请参见[创建工作空间](#)、[添加工作空间成员和角色](#)。

- 使用DataWorks功能。

DataWorks为您提供数据集成、数据开发、数据运维、数据分析、数据建模、数据治理等功能模块，为您提供一站式开发管理的界面，各工作模块请参见DataWorks帮助文档中功能模块的操作指导。

1.2. 准备RAM用户

本文为您介绍如何创建RAM子账号、子账号的访问密钥，以及如何给予账号授权并将其交付给其它用户使用。

背景信息

- 如果您只需要本人使用DataWorks，请根据[开通DataWorks](#)的操作准备好您的账号，并跳过此章节进行后续操作。
- 如果您计划邀请其它用户协作使用DataWorks，请您根据本文的操作准备RAM子账号。

创建RAM用户

主账号需要先在阿里云RAM控制台创建RAM用户。

1. 使用阿里云账号登录[RAM控制台](#)。
2. 在左侧导航栏，选择**身份管理 > 用户**。
3. 在用户页面，单击**创建用户**。

- 在创建用户页面的用户账号信息区域，输入登录名称和显示名称。

 说明 单击添加用户，可一次性创建多个RAM用户。

- 在访问方式区域，选择访问方式。

- 控制台访问：设置控制台登录密码、重置密码策略和多因素认证策略。

 说明 自定义登录密码时，密码必须满足密码复杂度规则。关于如何设置密码复杂度规则，请参见[设置RAM用户密码强度](#)。

- OpenAPI调用访问：自动为RAM用户生成访问密钥（AccessKey），支持通过API或其他开发工具访问阿里云。

 说明 为了保障账号安全，建议仅为RAM用户选择一种登录方式，避免RAM用户离开组织后仍可以通过访问密钥访问阿里云资源。

- 单击确定。

 注意 RAM用户创建完成后，务必保存用户名和登录密码，并将其告知子账号。

（可选）创建RAM子账号的访问密钥

DataWorks层面任务执行已经不需要绑定AK，如果您有特殊需要，可以在RAM访问控制页，为具体的子账号创建可用的AK。

如果云账号允许RAM用户自主管理AccessKey，RAM用户也可以自行创建AccessKey。

为子账号创建AccessKey的操作如下所示。

- 使用阿里云账号登录[RAM控制台](#)。
- 在左侧导航栏，选择身份管理 > 用户。
- 在用户页面，单击目标RAM用户名称。
- 在用户AccessKey区域，单击创建AccessKey。
- 在创建AccessKey对话框，查看AccessKey ID和AccessKey Secret。

您可以单击下载CSV文件，下载AccessKey信息。或者单击复制，复制AccessKey信息。

- 单击关闭。

 说明

- AccessKey Secret只在创建时显示，不支持查询，请妥善保管。
- 若AccessKey泄露或丢失，则需要创建新的AccessKey，最多可以创建2个AccessKey。

给RAM子账号授权DataWorks相关管理权限

DataWorks上对子账号（RAM用户）有外部权限控制，如果您需要RAM子账号有相关权限，您需要为其在[RAM控制台](#)RAM访问授予对应的RAM权限。

您可以参考以下步骤，为子账号授予相应的RAM权限。

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择身份管理 > 用户。
3. 在用户页面，单击目标RAM用户操作列的添加权限。
4. 在添加权限面板，为RAM用户添加权限。

i. 选择授权应用范围。

- 整个云账号：权限在当前阿里云账号内生效。
- 指定资源组：权限在指定的资源组内生效。

 说明 指定资源组授权生效的前提是该云服务已支持资源组。更多信息，请参见[支持资源组的云服务](#)。

ii. 输入授权主体。

授权主体即需要授权的RAM用户，系统会自动填入当前的RAM用户，您也可以添加其他RAM用户。

iii. 选择权限策略。

 说明 每次最多绑定5条策略，如需绑定更多策略，请分次操作。

5. 单击确定。
6. 单击完成。

将子账号交付其它用户使用

如果您需要子账号进行协同开发，除了准备RAM用户外，您需要为其提供RAM子账号的登录地址，如果子账号需要有ak的场景下，您需要将激活状态的ak信息提供给子账号的使用用户。

 说明

- 子账号归属于主账号，本身不拥有资源，也没有独立的计量计费。
- 子账号在阿里云各产品中操作产生的费用，将由创建这些子账号的主账号统一付费。
- 主账号需要查看RAM用户登录链接和自己的默认域名或域别名，并告知子账号。

交付子账号给其它用户使用，需要提供如下信息：

- RAM用户登录链接。

主账号进入RAM访问控制 > 概览页面，复制用户登录地址提供给RAM子用户。关于子账号登录详情可参考RAM用户登录阿里云控制台。



- 所属主账号的企业别名或默认域名。

主账号进入RAM访问控制 > 设置页面，单击高级设置，即可查看默认域名和域别名。

- 该子账号的用户名和登录密码。
- 该子账号的Access Key ID和Access Key Secret。

同时，您需要确认：

- 已经允许子账号启用控制台登录。
- 已经允许子账号自主管理AccessKey，详情请参见设置RAM用户安全策略。

后续步骤

准备好RAM用户后，请创建工作空间进行数据开发等操作，详情请参见创建工作空间。

1.3. RAM用户登录并使用DataWorks

本文为您介绍RAM用户如何登录DataWorks更新个人信息，并创建工作空间。

前提条件

如果您是第一次使用RAM用户登录数加平台和使用DataWorks，请确认以下信息：

- 该RAM用户所属主账号的企业别名。
- 该RAM用户的用户名和密码。
- DataWorks已不需要强制使用ak，如果您有场景需要使用AK，主账号可为RAM用户创建AccessKey ID和AccessKey Secret。
- 确认主账号已经允许RAM用户启用控制台登录。

如果上述信息无法确认，请首先保证所属主账号满足以下条件：

- 已经根据开通DataWorks和准备RAM用户的操作，准备好RAM用户所需的全部配置和信息。
- 已经根据创建工作空间和添加工作空间成员和角色的操作，成功创建工作空间，并为RAM用户配置合适的成员角色。

登录DataWorks

1. 根据主账号提供的RAM用户登录链接，登录阿里云控制台首页。

主账号可以登录RAM访问控制，复制RAM用户登录链接提供给RAM子用户。关于子账号登录详情可参考：[RAM用户登录控制台RAM用户登录阿里云控制台](#)。



2. 在阿里云控制台首页中搜索Dat aWorks，进入Dat aWorks控制台。

3. 在左侧导航栏，单击工作空间列表。

说明 RAM子账号只能在Dat aWorks控制台，工作空间列表看到自己已经加入的工作空间。

如果工作空间列表为空，您需要找到需要加入的工作空间管理员，让其在工作空间配置页面，成员管理处，将您加入到某个工作空间。详情可参考文档：[角色及成员管理：空间级](#)

如果您需要有创建工作空间的权限，需要主账号为您添加AliyunDat aWorksFullAccess权限。详情可参考文档：[如何授权子账号创建Dat aWorks工作空间的权限？](#)

4. 单击相应工作空间后的进入数据开发。

更新个人信息

您可以通过[报警联系人](#)页面，将RAM子账号个人信息配置在Dat aWorks上，此处配置好的个人信息，将在后续Dat aWorks开发运维过程中的报警接收中生效，在配置任务出错报警规则后，Dat aWorks会将任务运行出错时产生的报警发送至对应联系人，方便您及时发现并处理异常任务，本文为您介绍如何查看并设置报警联系人个人信息。

1. 进入Dat aWorks控制台页面。
2. 在左侧导航栏，单击报警配置。选择报警联系人。报警联系人信息配置详情可参考文档：[查看和设置报警联系人](#)。

创建工作空间

主账号需要给RAM用户授权AliyunDat aWorksFullAccess权限后，RAM用户才可以创建工作空间。详情请参见[为RAM用户授权](#)和[创建工作空间](#)。

后续步骤

当您了解以上内容后，您可以基于Dat aWorks教程，进一步了解Dat aWorks使用。详情可参考文档：[Workshop介绍](#)。

1.4.（进阶）RAM角色登录并使用DataWorks

本文为您介绍如何使用角色SSO的方式登录DataWorks。

背景信息

通常企业用户通过常规登录方式登录阿里云，管理、使用云资源。即在阿里云控制台输入账号、密码后登录。随着企业安全监管要求的日益严格，部分企业更愿意通过角色登录（Role Base_SSO）的方式登录阿里云。详情请参见[SAML角色SSO概览](#)。

说明

阿里云角色登录模式下，任务执行需要使用独享调度资源组，独享调度资源组使用详情，请参见：[新增和使用独享调度资源组](#)。

目前仅MaxCompute计算引擎支持Role Base_SSO方式访问。

DataWorks支持的登录方式

DataWorks支持云账号登录和角色登录：

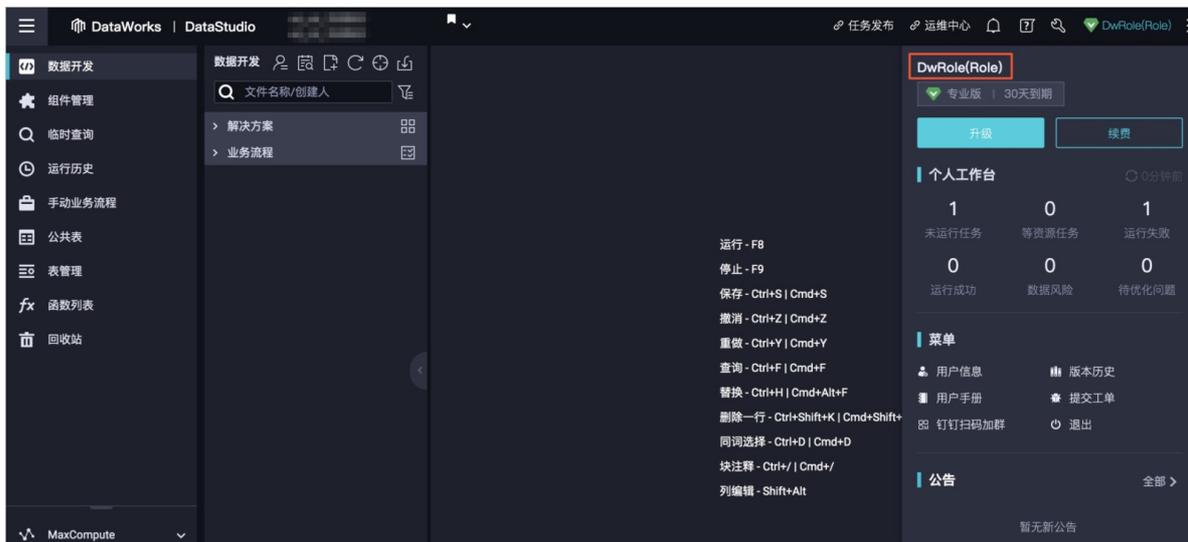
- 通过主账号或RAM用户登录DataWorks。

您可以通过输入账号、密码的方式登录阿里云控制台，并以当前登录账号的身份使用DataWorks。

此时，云账号将成为DataWorks某个工作空间的成员，拥有DataWorks产品的使用权限。

- 通过角色SSO的方式登录DataWorks。

您也可以通过角色SSO的方式登录阿里云，并使用DataWorks。角色SSO详情请参见[SAML角色SSO概览](#)。



此时，阿里云访问控制角色（RAM Role）将成为DataWorks某个工作空间的成员，扮演该RAM Role的使用者将拥有和云账号类成员同样的产品使用权限。详情请参见[RAM角色概览](#)。

角色登录指南

1. 创建待扮演角色。

说明 本步骤如果需要RAM用户或角色完成，请为RAM用户或角色授权AliyunRAMFullAccess策略。

为规范使用方式，建议您分别创建以下两个角色：

o 创建作为MaxCompute访问身份的角色。

- a. 云账号管理者以常规方式（账号和密码）登录阿里云主账号，进入RAM控制台创建待扮演的角色。



- 如果需要通过阿里云控制台切换身份方式扮演该角色，选择阿里云账号类型的角色。详情请参见[创建可信实体为阿里云账号的RAM角色](#)。
- 如果需要通过本地IDP身份提供商账号登录至阿里云扮演该角色，选择身份提供商类型的角色。详情请参见[创建可信实体为身份提供商的RAM角色](#)。

- b. 在配置角色页面，输入角色名称并选择云账号，单击完成。

- c. 在RAM角色管理页面，单击角色名称，修改信任策略管理为如下内容。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "dataworks.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

o 创建作为使用者所扮演的角色。

- 通过RAM用户来扮演的角色。

如果需要通过RAM用户来扮演RAM角色，请进入**RAM角色管理 > 创建RAM角色**，选择可信实体类型为**阿里云账号**，创建一个新的角色，并设置该角色的信任策略为以下内容。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "RAM": [
          "acs:ram::UID:root"
        ]
      }
    },
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "dataworks.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

 **说明** 请替换上述策略中的UID为阿里云主账号的UID。

- 通过IDP身份提供商账号来扮演的角色。

如果需要通过IDP身份提供商账号来扮演RAM角色，请进入**RAM角色管理 > 创建RAM角色**，选择可信实体类型为**身份提供商**，创建一个新的角色，并设置该角色的信任策略为以下内容。

```

{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "saml:recipient": "https://signin.aliyun.com/saml-role/sso"
        }
      },
      "Effect": "Allow",
      "Principal": {
        "Federated": [
          "acs:ram::UID:saml-provider/IDP"
        ]
      }
    },
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "dataworks.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}

```

说明 请替换上述策略中的UID为阿里云主账号的UID，替换IDP为您选择的身份提供商的名称。

假设目前已创建一个通过RAM用户来扮演的角色，即user-role角色。

RAM 访问控制

- 概览
- 人员管理
- 用户组
- 用户
- 设置
- SSO 管理
- 权限管理
- 授权
- 权限策略管理
- RAM 角色管理**
- OAuth 应用管理 (公测中)

什么是 RAM 角色?

RAM 角色机制是向您信任的实体 (例如: RAM 用户、某个应用或阿里云服务) 进行授权的一种安全方法。根据不同应用场景, 受信任的实体可能有如下一些例子:

- 您云账户下的一个 RAM 用户 (可能是代表一个移动 App 的后端服务);
- 其他云账户中的 RAM 用户 (需要进行跨账户的资源访问);
- ECS 实例上运行的应用程序代码 (需要对云资源执行操作);
- 某些阿里云服务 (需要对您账户中的资源进行操作才能提供服务);
- 企业的身份提供商 IDP, 可以用于角色 SSO。

RAM 角色颁发短时有效的访问令牌 (STS 令牌), 使其成为一种更安全的授予访问权限的方法。

特别说明:

RAM 角色不同于传统的教科书式角色 (其含义是指一组权限集)。如果您需要使用教科书式角色的功能, 请参考 RAM 权限策略 (Policy)。

创建 RAM 角色

RAM角色名称	备注	创建时间	操作
AliyunDataWorksAccessingENIRole	DataWorks默认使用此角色来访问您在其他云产品中的资源。	2020年10月29日 11:01:43	添加权限 精确授权 删除
AliyunMaxComputeEncryptionDefaultRole	MaxCompute(ODPS)使用此角色来访问您在KMS产品中的资源。	2020年10月28日 21:04:07	添加权限 精确授权 删除
AliyunServiceRoleForOdpsUserMgmt (服务关联角色)	用于ODPS用户管理 (ODPS user management) 的服务关联角色。ODPS user management使用此角色来访问您在其他云产品中的资源。	2020年10月28日 21:06:06	删除
DwRole		2020年10月28日 16:11:27	添加权限 精确授权 删除
user-role	user-role	2020年11月13日 15:32:36	添加权限 精确授权 删除

2. 创建DataWorks工作空间。

14

> 文档版本: 20220627

 **说明** 本步骤如果需要RAM用户或角色完成，请为RAM用户或角色授权AliyunDataWorksFullAccess策略。

- i. 登录DataWorks控制台。
- ii. 在左侧导航栏，单击工作空间列表，并切换至相应的地域后，单击创建工作空间。
- iii. 在创建工作空间对话框，配置各项参数，单击下一步。

分类	参数	描述
基本信息	工作空间名称	工作空间名称的长度需要在3~23个字符，以字母开头，且只能包含字母、下划线（_）和数字。
	显示名	显示名不能超过23个字符，只能字母、中文开头，仅包含中文、字母、下划线（_）和数字。
	模式	<p>工作空间模式是DataWorks新版推出的新功能，分为简单模式和标准模式：</p> <ul style="list-style-type: none"> ■ 简单模式：指一个DataWorks工作空间对应一个MaxCompute项目，无法设置开发和生产环境，只能进行简单的数据开发，无法对数据开发流程以及表权限进行强控制。 ■ 标准模式：指一个DataWorks工作空间对应两个MaxCompute项目，可以设置开发和生产两种环境，提升代码开发规范，并能够对表权限进行严格控制，禁止随意操作生产环境的表，保证生产表的数据安全。 <p>详情请参见简单模式和标准模式的区别。</p>
	描述	对创建的工作空间进行简单描述。
高级设置	能下载select结果	控制数据开发中查询的数据结果是否能够下载，如果关闭无法下载select的数据查询结果。此参数在工作空间创建完成后可以在工作空间配置页面进行修改，详情可参考文档： 安全设置 。

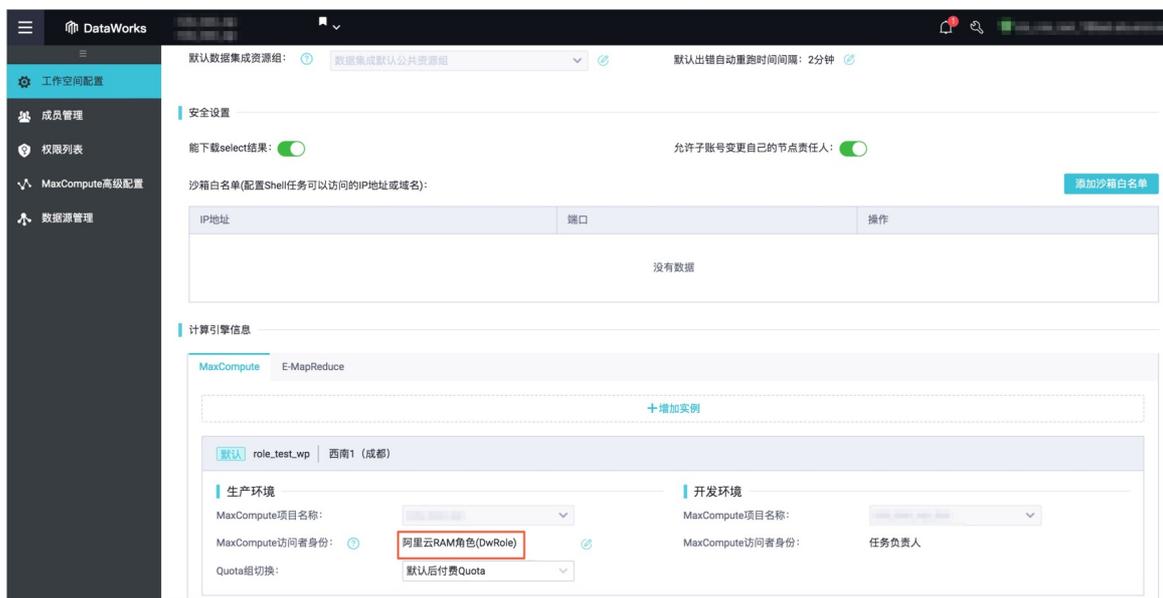
- iv. 在选择引擎页面，选择计算引擎服务为MaxCompute，单击下一步。

v. 在引擎详情页面，配置各项参数。

参数	描述
实例显示名称	实例显示名称需要以字母开头，只能包含字母、数字和下划线（_）。
Quota组切换	Quota用于实现计算资源和磁盘配额。
MaxCompute数据类型	该选项设置后将在5分钟内生效，数据类型模式的详情请参见 数据类型版本说明 。如果您不清楚模式的选择，建议与工作空间管理员确认后再进行选择。
MaxCompute项目名称	开发环境的默认名称为DataWorks工作空间的名称_dev，生产环境的默认名称与DataWorks工作空间名称一致。
MaxCompute访问身份	开发环境的MaxCompute访问身份默认为任务负责人，不可以修改。 生产环境的MaxCompute访问身份请选择阿里云RAM角色。
RAM角色选择	选择DwRole。

vi. 单击创建工作空间。

创建成功后，您可以进入工作空间配置页面，查看当前工作空间的MaxCompute访问身份（即调度任务访问身份）为之前创建成功的RAM Role。

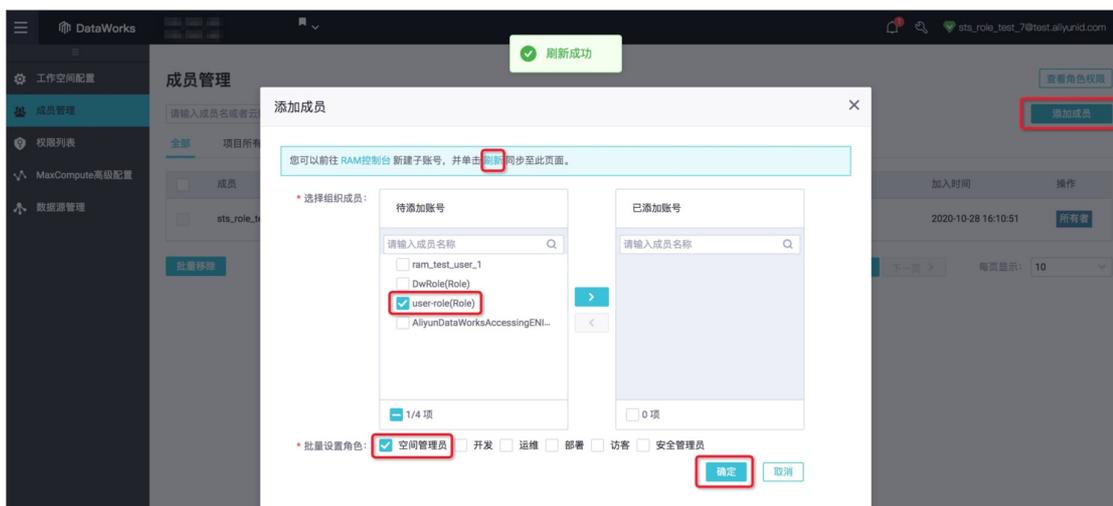


说明 该MaxCompute访问身份对应的RAM角色将用于运行生产调度任务，请勿用于其它地方。仅支持独享调度资源组执行任务。

3. 添加其它角色至DataWorks工作空间。

说明 本步骤如果需要RAM用户或角色完成，请设置RAM用户或角色为该DataWorks工作空间的空间管理员。

- i. 在数据开发页面，单击右上方的图标，进入工作空间配置页面。
- ii. 在左侧导航栏，单击成员管理。
- iii. 在成员管理页面，单击右上方的添加成员。
- iv. 在添加成员对话框中，单击刷新，即可展示已创建的RAM角色。
- v. 在待添加账号处勾选需要添加的账号user-role，单击>，将其移动至已添加的账号中。
- vi. 选中需要授予的角色，单击确定。



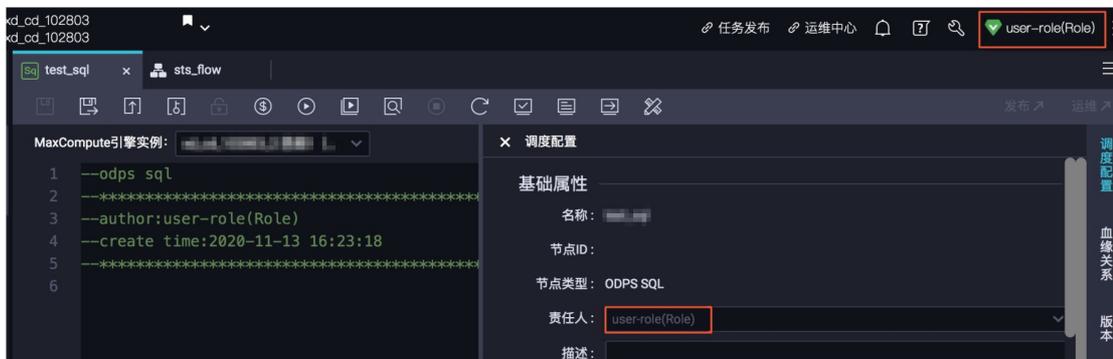
4. (可选) 为使用者授权AliyunSTSAssumeRoleAccess。

如果您即将使用RAM用户而非IDP账号来扮演RAM Role，请先为RAM用户授予AliyunSTSAssumeRoleAccess。

5. 使用者登录Dat aWorks。

本步骤为您展示使用者如何扮演user-role角色登录并使用Dat aWorks。

- i. 登录阿里云。
使用者可以使用角色SSO，扮演RAM角色user-role，并登录至阿里云控制台。角色SSO详情请参见[SAML角色SSO概览](#)。
- ii. 进入DataWorks控制台的工作空间列表页面，单击在上一步已加入的工作空间后的进入数据开发。
- iii. 创建节点，详情请参见[创建ODPS SQL节点](#)。即可查看任务责任人为当前所扮演的角色user-role。



2. 创建工作空间

DataWorks的工作空间即MaxCompute中项目的概念，本文为您介绍如何创建工作空间。

前提条件

请根据[开通DataWorks](#)中的步骤检查账号是否已可用。如果验证无误，请根据下文操作创建工作空间。

说明

子账号如果需要代主账号进行相关操作，需要拥有对应的权限。

主账号为子账号授权相应的权限可参考：[主账号如何给子账号添加Aliyundatavworksfullaccess权限？](#)，[如何为子账号授权购买相关服务的权限？](#)。

操作步骤

1. 使用主账号登录[DataWorks控制台](#)。
2. 在概览页面，单击右侧的创建工作空间。
您也可以单击左侧导航栏中的工作空间列表，切换至相应的区域后，单击创建工作空间。
3. 在创建工作空间对话框，配置各项参数，单击下一步。

分类	参数	描述
基本信息	工作空间名称	工作空间名称的长度需要在3~23个字符，以字母开头，且只能包含字母、下划线（_）和数字。
	显示名	显示名不能超过23个字符，只能字母、中文开头，仅包含中文、字母、下划线（_）和数字。
	模式	<p>工作空间模式是DataWorks新版推出的新功能，分为简单模式和标准模式：</p> <ul style="list-style-type: none"> 简单模式：指一个DataWorks工作空间对应一个MaxCompute项目，无法设置开发和生产环境，只能进行简单的数据开发，无法对数据开发流程以及表权限进行强控制。 标准模式：指一个DataWorks工作空间对应两个MaxCompute项目，可以设置开发和生产两种环境，提升代码开发规范，并能够对表权限进行严格控制，禁止随意操作生产环境的表，保证生产表的数据安全。 <p>详情请参见简单模式和标准模式的区别。</p>
	描述	对创建的工作空间进行简单描述。
高级设置	能下载select结果	控制数据开发中查询的数据结果是否能够下载，如果关闭无法下载select的数据查询结果。此参数在工作空间创建完成后可以在工作空间配置页面进行修改，详情可参考文档： 安全设置 。

4. 进入选择引擎界面，选择相应引擎后，单击下一步。

说明

- 如果您需要绑定实时计算、E-MapReduce、交互式分析Hologres、Graph Compute、AnalyticDB for MySQL或AnalyticDB for PostgreSQL计算引擎，请首先开通相应的服务，才能进行选择。
- 如果创建工作空间时，未选择正确的计算引擎，可能导致无法在数据开发页面进行创建表和基于引擎节点进行数据清洗等操作。

DataWorks已正式商用，如果该地域没有开通，需要首先开通正式商用服务。

选项	参数	描述
选择DataWorks服务 说明 默认选中该模块。	数据集成	数据集成是稳定高效、弹性伸缩的数据同步平台。致力于提供复杂网络环境下、丰富的异构数据源之间数据高速稳定的数据移动及同步能力。详情请参见 数据集成 模块。
	数据开发	该页面是您根据业务需求，设计数据计算流程，并实现为多个相互依赖的任务，供调度系统自动执行的主要操作页面。详情请参见 数据开发 模块。
	运维中心	该页面可对任务和实例进行展示和操作，您可以在这里查看所有任务的实例。详情请参见 运维中心 模块。
	数据质量	DataWorks数据质量依托DataWorks平台，为您提供全链路的数据质量方案，包括数据探查、数据对比、数据质量监控、SQLScan和智能报警等功能。详情请参见 数据质量 模块。
选择计算引擎服务	MaxCompute	MaxCompute是一种快速、完全托管的TB或PB级数据仓库解决方案，能够更快速为您解决海量数据计算问题，有效降低企业成本，并保障数据安全。详情请参见 MaxCompute 。 说明 完成创建DataWorks工作空间后，需要关联MaxCompute项目，否则现执行命令会报 <code>project not found</code> 的错误。
	实时计算	开通后，您可以在DataWorks中进行流式计算任务开发。
	E-MapReduce	开通后，您可以在DataWorks中使用E-MapReduce，进行大数据处理任务的开发。详情请参见 E-MapReduce 。 注意 DataWorks已暂停绑定E-MapReduce计算引擎，如您有相关需求，请 提交工单 申请。
	交互式分析Hologres	开通后，您可以在DataWorks中使用Hologres进行交互式分析的表管理、外部表管理和SQL任务的开发。

选项	参数	描述
	Graph Compute	开通后，您可以在DataWorks中使用Graph Studio进行图计算开发。
	AnalyticDB for PostgreSQL	开通后，您可以在DataWorks中进行分析型数据库AnalyticDB for PostgreSQL任务的开发，AnalyticDB for PostgreSQL的详情请参见 产品概述 。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 您需要购买DataWorks标准版及以上版本，才可以开通AnalyticDB for PostgreSQL服务。 </div>
	AnalyticDB for MySQL	开通后，您可以在DataWorks中进行分析型数据库AnalyticDB for MySQL任务的开发，AnalyticDB for MySQL的详情请参见 产品概述 。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 您需要购买DataWorks标准版及以上版本，才可以开通AnalyticDB for MySQL服务。 </div>
选择机器学习服务	机器学习PAI	机器学习是指机器通过统计学算法，对大量的历史数据进行学习从而生成经验模型，利用经验模型指导业务。

5. 进入引擎详情页面，配置选购引擎的参数。

- 绑定MaxCompute计算引擎

参数	描述
新增方式	您可以创建MaxCompute项目或者绑定已有MaxCompute项目。
实例显示名称	实例名称长度需要控制在3~28个字符，仅支持字母开头，仅包含字母、下划线（_）和数字。
地域	默认当前工作空间所在的地域。
付费模式	包括按量付费、包年包月和开发者版本。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin-top: 5px;"> ? 说明 标准模式下不支持添加开发者版本的实例。 </div>
Quota组	Quota用来实现计算资源和磁盘配额。
MaxCompute数据类型	包括2.0数据类型（推荐）、1.0数据类型（面向已有使用1.0数据类型用户）和Hive兼容类型（面向Hive迁移用户），详情请参见： 数据类型版本说明 。
是否加密	根据实际情况选择是否需要加密当前实例。

参数	描述
生产环境	<p>生产环境下的配置项包括MaxCompute项目名称和访问身份：</p> <ul style="list-style-type: none"> ■ MaxCompute项目名称：当前DataWorks工作空间底层使用的MaxCompute生产环境的项目名称。 ■ 访问身份：支持您通过阿里云主账号、阿里云子账号或阿里云RAM角色角色访问MaxCompute。
开发环境	<p>开发环境下的配置项包括MaxCompute项目名称和访问身份：</p> <ul style="list-style-type: none"> ■ MaxCompute项目名称：当前DataWorks工作空间底层使用的MaxCompute开发环境的项目名称。 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px; margin: 5px 0;"> <p> 说明 该MaxCompute项目是计算和存储资源。</p> </div> <ul style="list-style-type: none"> ■ 访问身份：默认是任务执行者，不可以修改。

○ 绑定E-MapReduce计算引擎

参数	描述
实例显示名称	自定义实例的名称。
地域	默认当前工作空间所在的地域。
访问模式	<ul style="list-style-type: none"> ■ 当EMR计算引擎的绑定模式为快捷模式时，阿里云主账号或RAM用户在DataWorks运行代码或自动调度任务，都只是下发代码至EMR集群，实际运行的身份为集群内的Hadoop用户。 ■ 当EMR计算引擎的绑定模式为安全模式时，阿里云主账号或RAM用户在下发代码的同时，EMR集群内会匹配对应的同名用户来运行任务。管理者可以使用EMR集群内的Ranger组件对每个用户进行权限管控，最终实现不同阿里云主账号、任务责任人或阿里云子账号在DataWorks上运行EMR任务时，拥有对应不同数据权限的目的，进行更安全的数据权限隔离。

参数	描述
调度访问身份	<ul style="list-style-type: none"> 如果访问模式选择快捷模式，当提交任务至调度系统后，DataWorks调度系统自动运行任务时，您可以选择阿里云主账号或阿里云子账号提交代码至EMR集群。 如果访问模式选择安全模式，当任务被提交、发布至生产环境后，DataWorks调度系统自动运行任务时，您可以选择任务责任人、阿里云主账号或阿里云子账号提交代码至EMR集群，同时该身份对应的Hadoop用户将实际运行代码。 <p>说明</p> <ul style="list-style-type: none"> 仅生产环境涉及配置该参数。 为保证工作空间成员可以在DataStudio内正常运行EMR类的任务，请确保开发、管理员等相关角色拥有AliyunEMRDevelopAccess权限策略。 <ul style="list-style-type: none"> 如果您使用阿里云主账号运行任务，该账号天然拥有AliyunEMRDevelopAccess权限策略。 如果您使用RAM用户运行任务，则需要授予该用户AliyunEMRDevelopAccess权限策略，详情请参见RAM用户授权。
访问身份	<p>在开发环境运行任务时，提交代码至EMR引擎所使用的身份。此处默认为任务执行者。</p> <p>说明</p> <ul style="list-style-type: none"> 仅DataWorks标准模式的工作空间会显示该参数，并且仅开发环境涉及配置该参数。 任务执行者可以为阿里云主账号或RAM用户。 <p>为保证工作空间成员可以在DataStudio内正常运行EMR类的任务，请确保开发、管理员等相关角色拥有AliyunEMRDevelopAccess权限策略。</p> <ul style="list-style-type: none"> 如果您使用阿里云主账号运行任务，该账号天然拥有AliyunEMRDevelopAccess权限策略。 如果您使用RAM用户运行任务，则需要授予该用户AliyunEMRDevelopAccess权限策略。
集群ID	<p>从下拉列表中选择调度访问身份账户所在的EMR集群，作为任务的运行环境。</p>
项目ID	<p>从下拉列表中选择调度访问身份账户所在的EMR项目，作为任务的运行环境。</p> <p>说明 如果EMR项目开启访问模式为安全模式，则无法被选择。</p>

参数	描述
YARN资源队列	当前集群下的队列名称。如果无特殊需求，请输入 <i>default</i> 。
覆盖DataStudio任务队列映射	<ul style="list-style-type: none"> 勾选覆盖DataStudio任务队列时：所有任务将按照当前指定的队列运行。 未勾选覆盖DataStudio任务队列时： <ul style="list-style-type: none"> 如果节点高级配置中配置了queue，则按照节点的queue配置运行。 如果节点高级配置中没有配置queue（自己删除了该配置），任务将按照当前界面指定的队列运行。 <p> 说明 如果您看不到覆盖DataStudio任务队列功能，可以提交工单联系我们进行升级。</p>
Endpoint	EMR的Endpoint，不可以修改。
选择资源组	<p>选择已与当前DataWorks工作空间配置网络连通性的独享调度资源组。如果您没有可用的独享调度资源组则需要新建。新建独享调度资源组并配置网络连通性，详情请参见新增和使用独享调度资源组。</p> <p>选择后，单击测试连通性进行测试，以验证独享调度资源组和E-MapReduce实例的网络连通性。验证后会对资源组进行初始化。</p> <p> 说明 当EMR集群配置变更时，需要对资源组重新进行初始化。</p>

○ 绑定Hologres计算引擎

参数	描述
实例显示名称	实例的显示名称。
访问身份	<ul style="list-style-type: none"> DataWorks任务提交调度后，作为在Hologres引擎内执行代码的账号。包括阿里云主账号和阿里云子账号。 <p> 说明 仅生产环境涉及配置该参数。</p> <ul style="list-style-type: none"> 在开发环境运行任务时，此处默认为任务执行者。
Hologres实例名称	选择需要绑定的Hologres实例。
数据库名称	输入在SQL Console中新建的数据库的名称。例如，testdb。

○ 绑定GraphCompute计算引擎

○ 绑定AnalyticDB for PostgreSQL计算引擎

参数	描述
实例显示名称	实例的显示名称，请注意名称需要保持唯一性。
实例名称	选择需要在工作空间中使用的AnalyticDB for PostgreSQL实例。
数据库名称	AnalyticDB for PostgreSQL实例下需要绑定使用的数据库的名称。
用户名	拥有数据库操作权限的Username。，详情请参见 创建数据库账号 ，进入AnalyticDB for PostgreSQL的 账号管理 页面获取。
密码	拥有数据库操作权限的Password。，详情请参见 创建数据库账号 ，进入AnalyticDB for PostgreSQL的 账号管理 页面获取。
连通性测试	AnalyticDB for PostgreSQL任务实例需要运行在独享调度资源组上，请在此处选择需要使用的独享调度资源组，详情请参见 独享资源组模式 。 选择后，单击 测试连通性 进行测试，以验证独享调度资源组和AnalyticDB for PostgreSQL实例的网络连通性。如果您没有可用的独享调度资源组，请单击 新建独享资源组 创建。

○ 绑定AnalyticDB for MySQL计算引擎

参数	描述
实例显示名称	实例的显示名称，请注意名称必须唯一。
实例名称	选择需要在工作空间中使用的AnalyticDB for MySQL实例。
数据库名称	AnalyticDB for MySQL实例下绑定的需要使用的数据库名称。
用户名	拥有数据库操作权限的Username。，详情请参见 数据库账号和权限 ，进入AnalyticDB for MySQL的 账号管理 页面获取。
密码	拥有数据库操作权限的Password。，详情请参见 数据库账号和权限 ，进入AnalyticDB for MySQL的 账号管理 页面获取。
连通性测试	AnalyticDB for MySQL任务实例需要运行在独享调度资源组上，请在此处选择需要使用的独享调度资源组，详情请参见 独享资源组模式 。 选择后，单击 测试连通性 进行连通性测试，以验证独享调度资源组和AnalyticDB for MySQL实例的网络连通性。如果您没有可用的独享调度资源组，请单击 新建独享资源组 创建。

6. 配置完成后，单击[创建工作空间](#)。

工作空间创建成功后，即可在[工作空间列表](#)页面查看相应内容。

② 说明

- 如果您成为工作空间所有者，代表该工作空间内的所有东西都属于您。在给别人赋权之前，任何人无权限访问您的空间。如果您使用的是子账号创建的工作空间，则该工作空间会同时属于子账号和对应的主账号。
- 子账号无需创建工作空间，只需要被加入到某个工作空间，即可使用MaxCompute。

后续步骤

现在，您已经学习了如何创建工作空间，您可以选择继续[添加工作空间成员和角色](#)或直接开始[快速入门](#)的操作。您可以通过学习快速入门模块，快速完成一个完整的数据开发和运维操作。

3. 添加工作空间成员和角色

本文为您介绍如何添加工作空间成员和角色，以及各角色拥有的权限和区别。

前提条件

如果您需要邀请其它用户协同使用DataWorks，请先根据[准备RAM用户](#)的操作准备必要的RAM用户，并[创建工作空间](#)后，再进行本文的操作。

背景信息

说明 如果您计划仅使用主账号，可以跳过本文的操作，直接创建表并上传数据，详情请参见[建表并上传数据](#)。

阿里云数加产品的账号登录体系与阿里云保持一致，统一采用RAM主账号或RAM用户登录的方式。

RAM用户计费的说明如下：

- 阿里云账号（即主账号）是阿里云资源的归属及使用计量计费的基本主体，负责生成本企业组织下的RAM用户，并对RAM用户进行管理、授权等操作。
- RAM用户由主账号在RAM系统中创建并管理，本身不拥有资源，也没有独立的计量计费，这些账号由所属主账号统一控制和付费。

操作步骤

1. 进入工作空间配置页面。
 - i. 登录[DataWorks控制台](#)。
 - ii. 在左侧导航栏，单击工作空间列表。
 - iii. 单击相应工作空间后的工作空间配置。
 - iv. 在工作空间配置对话框，单击更多设置，进入工作空间配置页面。

您也可以进入数据开发页面，单击右上角的图标，进入工作空间配置页面。
2. 在左侧导航栏，单击成员管理。
3. 在成员管理页面，单击右上角的添加成员。
4. 在添加成员对话框，单击刷新，同步当前阿里云账号下的RAM用户至待选列表中。

添加成员

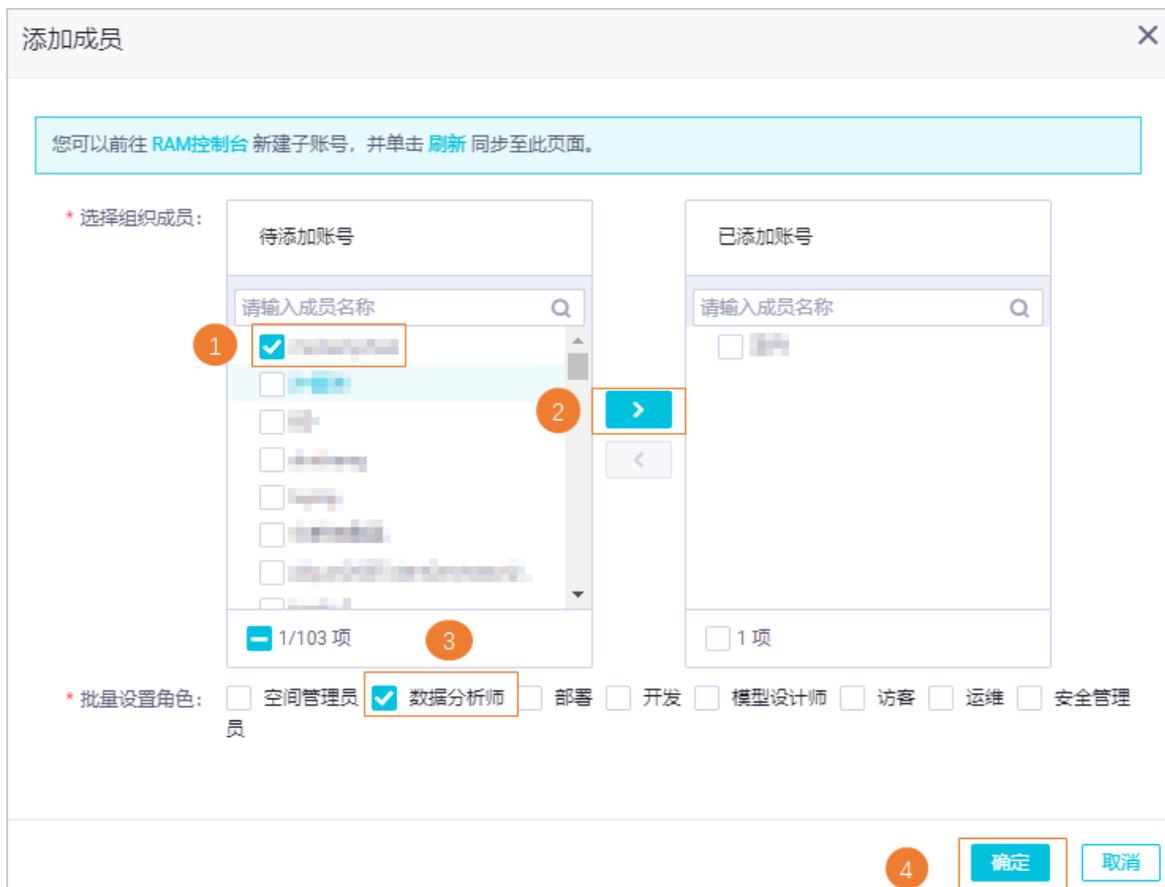
您可以前往 [RAM控制台](#) 新建子账号，并单击 **刷新** 同步至此页面。

* 选择组织成员：

待添加账号	已添加账号
<input type="text" value="请输入成员名称"/>	<input type="text" value="请输入成员名称"/>

说明 如果您需要添加新的RAM用户，请单击上图中的RAM控制台，打开阿里云访问控制页面。添加RAM用户并交付使用的具体操作请参见[准备RAM用户](#)。

- 在待添加账号处勾选需要添加的成员账号，单击>，将需要添加的RAM用户移动至已添加的账号中。
- 勾选需要授予的角色，单击确定。



注意 需要将RAM用户移动至已添加的账号列表下，才可以进行授权。

- 添加完成后，您可以在工作空间中列表中查看或修改已有的成员和对应角色，也可以从工作空间中删除非项目所有者角色的RAM用户。

工作空间成员包括项目所有者、空间管理员、数据分析师、开发、运维、部署、访客和安全管理员等角色，工作空间创建者默认为管理员角色。

角色	描述
项目所有者	项目所有者拥有工作空间的所有权限。
空间管理员	除拥有开发角色和运维角色的全部权限外，还可以进行添加/移出工作空间成员并授予角色，创建自定义资源组等操作。
数据分析师	当前默认只有数据分析模块操作权限。
开发	负责数据开发页面的设计和维护工作。
运维	负责在运维中心页面管理全部任务的运行情况并进行相应处理。
部署	仅在多工作空间模式时审核任务代码并决定是否提交运维。

角色	描述
访客	仅有只读权限，可以查看数据开发页面的业务流程设计和代码内容。
安全管理员	仅有数据保护伞模块的操作权限，无其它模块权限。详情请参见 数据保护伞 。

DataWorks预设角色与MaxCompute项目存在角色映射关系，其中MaxCompute开发项目角色默认拥有一定的项目操作权限。但MaxCompute生产项目默认无权限，需要在[安全中心](#)申请。

MaxCompute角色	开发项目数据权限	DataWorks成员角色	DataWorks平台权限特征
Project Owner	MaxCompute项目空间的所有者，拥有该项目空间的所有权限。	无	无
Super_Administrator	MaxCompute项目空间的超级管理员，拥有项目空间的管理类权限以及项目空间内所有类型资源的全部权限。	无	无
Admin	<p>每一个项目空间在创建时，会自动创建一个Admin角色，并且为该角色授予确定的权限。即可以访问项目空间内的所有对象、对用户或角色进行管理、对用户或角色进行授权。</p> <p>与项目空间的所有者相比，Admin角色不能将Admin权限指派给用户，不能设定项目空间的安全配置，不能修改项目空间的鉴权模型，Admin角色所对应的权限不能被修改。</p> <p>项目空间的所有者可以将Admin角色赋权给一个用户，让该用户代理安全管理。</p>	无	无
Role_Project_Data_Analyst	默认在开发环境和生产环境中没有访问MaxCompute引擎的权限，请您前往 安全中心 申请权限。	数据分析师	数据分析师角色的用户默认只有数据分析模块的操作权限。

MaxCompute角色	开发项目数据权限	DataWorks成员角色	DataWorks平台权限特征
Role_Project_Admin	当前项目空间下 project/table/fuction/resource/instance/job/package的所有权限。	项目管理员	指项目空间的管理者。可以对该项目空间的基本属性、数据源、当前项目空间计算引擎配置和项目成员等进行管理，并为项目成员赋予项目管理员、开发、运维、部署、访客角色。
Role_Project_Dev	当前项目空间下 project/fuction/resource/instance/job/package/table的所有权限。	开发	开发角色的用户能够创建 workflow、脚本文件、资源和UDF以及新建和删除表，同时可以创建发布包，但不能执行发布操作。
Role_Project_Pe	当前项目空间下 project/fuction/resource/instance/job的所有权限，拥有 package的read权限和table的read/describe权限。	运维	运维角色的用户由项目管理员分配运维权限，拥有发布及线上运维的操作权限，没有数据开发的操作权限。
Role_Project_Deploy	默认无权限。	部署	部署角色与运维角色相似，但是它没有线上运维的操作权限。
Role_Project_Guest	默认无权限。	访客	访客角色的用户只具备查看权限，没有权限进行编辑 workflow和代码等操作。
Role_Project_Security	默认无权限。	安全管理员	安全管理员仅在数据保护伞模块中使用，用于敏感规则配置、数据风险审计等。

详情请参见[用户、角色与权限概述](#)。

4. 空间管理员职责

本文为您介绍项目管理员的权限和职责。默认创建工作空间的阿里云账号是工作空间所有者，拥有最高权限。

如果工作空间创建完成后，项目所有者不想自行管理，可以指定其子账号为项目管理员角色。

创建工作空间

工作空间创建完成后，工作空间责任人为阿里云主账号（子账号代主账号创建的工作空间，其责任人也为阿里云主账号），创建工作空间的操作请参见[创建工作空间](#)。

② 说明

- 子账号需要有AliyunDataWorksFullAccess权限时，才可以代主账号创建工作空间。详情可参考文档：[给RAM子账号授权DataWorks相关管理权限](#)。
- 空间管理员需要保证工作空间生产环境的稳定、控制工作空间成员中的角色权限（权限最小化，够用即可），并控制表的权限。

添加工作空间成员

空间管理员有权限添加RAM子账号为工作空间成员，并在相应的工作空间为子账号授权相应的角色。每个角色对应的权限点，请参见[附录：预设角色权限列表（空间级）](#)。

② 说明 建议不要同时授予一个子账号开发角色和运维角色。

控制相关权限

DataWorks角色分为预设角色与DataWorks空间级别自定义角色，每个角色拥有的权限不同。您可以在添加子账号进入工作空间时，为子账号授予具体对应的角色，授权后，该用户将有该角色拥有的权限，详情可参考：[角色及成员管理：空间级](#)。每个角色拥有的界面操作权限不同，您可以参考[附录：预设角色权限列表（空间级）](#)了解详情。

当您使用MaxCompute引擎时，DataWorks预设角色MaxCompute开发引擎（开发项目）存在一定的权限映射，即授权预设角色后，该用户拥有对应的引擎开发项目的资源操作权限。详情可参考文档：[用户、角色与权限概述](#)。

为保证生产环境的稳定性和安全性，不允许个人账号拥有生产表的删除、修改等权限，且不允许成员随意提交任务。

功能权限要求：

- 数据集成：添加数据源、批量上云等功能，仅空间所有者和空间管理员角色可以操作。
- 计算资源（MaxCompute管家）：空间管理员设置DataWorks的资源组分配后，运维人员即可通过MaxCompute管家查看系统状态、资源组分配和任务监控。
- 运维中心：仅运维角色和空间管理员角色有运维中心更高的操作权限。
- 数据开发：仅开发角色和空间管理员角色可以在数据开发进行具体的开发工作。

在设置工作空间的级别时，您需要首先选择设置调度引擎执行任务时，使用阿里云主账号还是阿里云子账号执行任务。如果设置有误，权限体系会被破坏。

- 阿里云主账号：执行SQL使用的是主账号的AccessKey，可以操作当前区域下所有工作空间的表，请谨慎设置。

- **阿里云子账号**：执行SQL使用的是子账号的AccessKey，权限会受到严格控制，无法直接操作生产表。

② 说明

为保证数据安全，请保持最小粒度为角色授权，够用即可。