ALIBABA CLOUD

Alibaba Cloud

数据湖分析

账号和权限管理

文档版本：20210126

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 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	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。	`switch {active|stand}`

目录

1.账号概览

您在使用DLA服务的过程中会涉及多种类型的账号，包括阿里云账号、RAM账号、DLA账号（Root账号、子账号、服务账号）。本文档主要针对这几种账号类型进行一个简单的概括说明。

账号类型	权限说明	使用说明
阿里云账号	默认拥有所有的OpenAPI调用权限和控制台操作权限。主要针对DLA服务进行全量管理。	阿里云账号用于开通和管理DLA服务。例如登录DLA控制台、创建虚拟集群等。
RAM账号	RAM账号的权限由阿里云账号进行授予。在授权的范围内，对DLA服务进行管理。	阿里云账号授予RAM账号一定的权限后，RAM账号也可以在权限范围内管理DLA服务。例如可以授权RAM账号登录DLA控制台、提交DLA Spark作业、调用DLA Meta。 **说明** RAM账号从属于阿里云账号，RAM账号不能拥有任何实际的资源，所有资源都属于阿里云账号。
DLA账号（Root账号、子账号、服务账号）	DLA账号用于对DLA数据库进行操作，例如创建和删除Schema、创建和删除表等、执行DLA SQL(Presto) 引擎的SQL等。DLA账号的权限范围按照Region进行隔离，不同Region有不同的DLA账号，只在Region内有效。	DLA账号分为以下三种类型： • **Root账号**：开通DLA服务后，DLA系统会自动为您创建DLA Root账号，即Root账号。Root账号既能执行SQL，也能够提交DLA Spark作业。 **说明** DLA Root账号会跟RAM主账号默认绑定，且不能解绑。 • **子账号**：开通DLA服务后，可以在DLA控制台上创建子账号，子账号主要用于企业内部不同的用户使用。子账号创建成功后，可以通过Root账号为子账号进行授权、查看、撤销权限等操作。具体操作请参考GRANT、SHOW GRANTS、REVOKE。 **说明** 子账号可以与RAM账号进行绑定，绑定成功后RAM账号就可以通过DLA SQL访问到Spark里面的库表，同样也可以通过Spark访问到DLA SQL里面的库表。 • **服务账号**：被集成服务使用。包括以下两种类型： ○ DLA 服务帐号：用户在DLA控制台上执行创建数据源、创建表以及执行SQL时所使用的默认数据库帐号。用户在操作控制台时遇到需要该帐号的时会自行提示用户进行开通。 ○ DBS服务账号：为DBS产品创建的一个专属DLA数据库帐号。该帐号通常只具备建库建表权限，并允许DBS使用这个帐号在DLA中进行相关操作。此帐号的开通需要由DBS控制台发起。

2.管理DLA账号

本文介绍了如何在DLA中创建、删除子账号和重置数据库密码，以及如何授权子账号、撤销子账号权限。

创建数据库子账号

1. 登录Data Lake Analytics管理控制台。
2. 单击左侧导航栏的**账号管理**。
3. 在**账号管理**页面单击**创建子账号**。

4. 在**创建数据库子账号**页面，设置账号名称和账号密码。

DLA提供两种设置子账号密码的方式：

- **系统随机密码**：DLA系统随机生成子账号密码。选中**使用系统随机密码**，单击**确定**，系统自动生成密码。
- **手动设置密码**：输入子账号密码，单击**确定**。

删除数据库子账号

1. 登录Data Lake Analytics管理控制台。
2. 单击左侧导航栏的**账号管理**。
3. 在**账号管理**页面定位到要删除的子账号，单击**操作**列的**删除**。
4. 在**确认删除**对话框中，单击**确定**，系统将验证码发送至绑定的手机，输入正确的验证码后，单击**确定**删除子账号。

重置数据库密码

在使用DLA过程中，如果忘记数据库账号的密码，您可以通过DLA控制台重置密码。

> **说明** 为了您的数据安全，建议您定期更换账号密码。

1. 登录Data Lake Analytics管理控制台。
2. 单击左侧导航栏**账号管理**。
3. 在**账号管理**页面定位到要重置密码的账号，单击**操作**列的**重置密码**。
4. 在**重置密码**页面，为账号设置新密码。

   DLA提供两种设置子账号密码的方式：

   - **系统随机密码**：DLA系统随机生成子账号密码。选中**使用系统随机密码**，单击**确定**，系统自动生成密码。
   - **手动设置密码**：输入子账号密码，单击**确定**。
5. 在**手机验证**框中，输入验证码，然后单击**确定**。

当您修改的是Root账号密码，DLA还会给您发送一封站内信，提醒您正在进行密码变更操作。如果后续您忘记Root账号密码，可以通过站内信找回。

授权数据库子账号

您必须通过Root账号为子账号进行授权。您可以通过以下两种方式对子账号进行授权：

- 登录Data Lake Analytics管理控制台，在**Serverless SQL > SQL执行**页面，使用Root账号通过GRANT为子账号授权。
- 在应用中以Root权限通过程序代码、MySQL命令行工具或者MySQL客户端连接DLA，然后通过GRANT为子账号授权。

撤销数据库子账号权限

您必须通过Root账号撤销子账号权限。关于如何撤销子账号权限，请参见REVOKE。

3.管理RAM账号

通过阿里云账号开通DLA服务后，如果您的组织里有多个用户需要使用DLA服务，这些用户只能共享使用您的阿里云账号AccessKey。您的AccessKey存在泄漏的风险，且您无法控制用户的操作权限。此时您可以创建RAM账号，并授予RAM账号对应的操作权限，让您的用户通过RAM账号来访问或管理DLA服务。

创建RAM账号

1. 登录RAM控制台。
2. 单击左侧导航栏的**人员管理 > 用户**。
3. 在**用户**页面，单击**创建用户**，输入**登录名称**和**显示名称**。
4. 在**访问方式**区域下，选择**控制台访问**或**编程访问**。

- **控制台访问**：可以完成对登录安全的基本设置，包括自动生成或自定义登录密码、是否要求下次登录时重置密码以及是否要求开启多因素认证。
- **编程访问**：自动为RAM账号创建访问密钥（AccessKey）。RAM账号可以通过其他开发工具访问DLA服务。

> **说明** 为保障账号安全，建议仅为RAM账号选择一种访问方式。避免RAM账号离开组织后仍可以通过访问密钥访问DLA服务。

5. 单击**确认**，创建RAM子账号。

为RAM账号授权

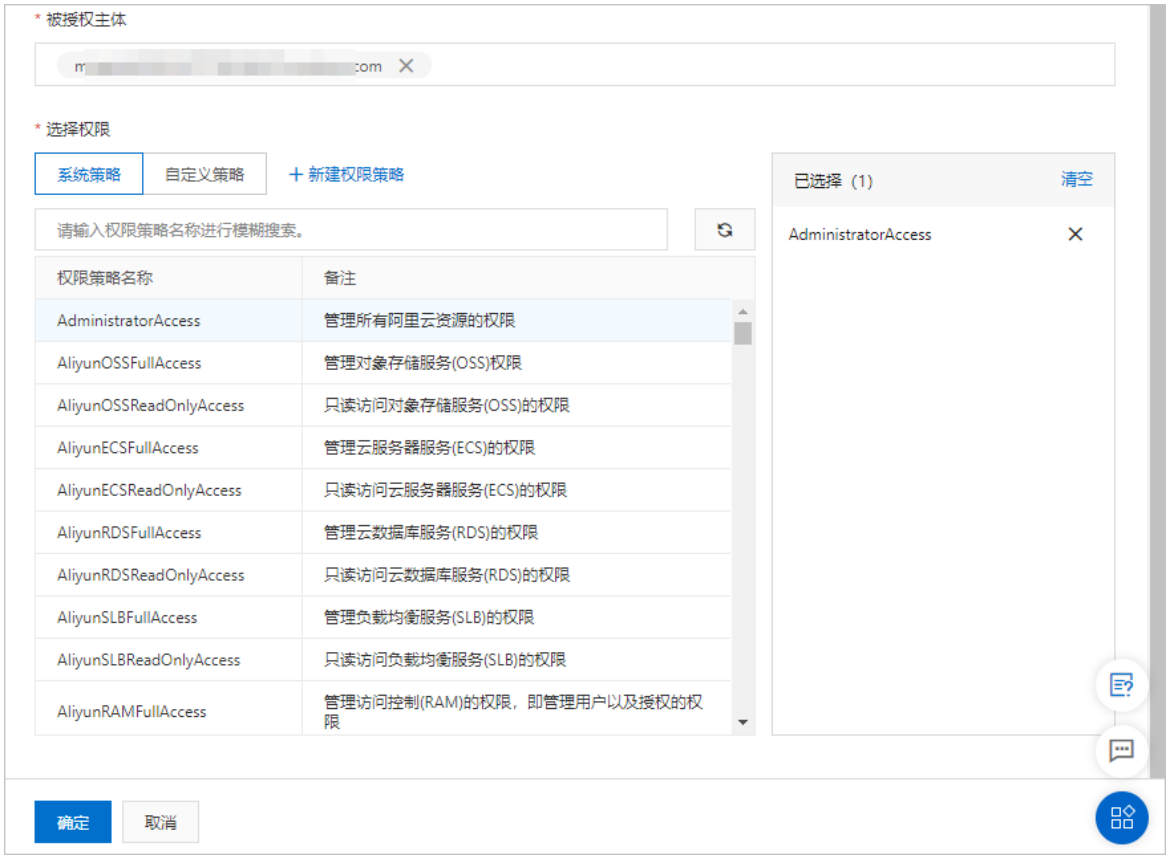
RAM中提供两种DLA系统策略：

- `AliyunDLAFullAccess`：授予RAM账号`AliyunDLAFullAccess`系统策略后，RAM账号将在DLA中继承阿里云账号的所有权限，即在DLA服务中，RAM账号拥有的权限与阿里云账号完全相同，请慎重使用。
- `AliyunDLAReadOnlyAccess`：授予RAM账号`AliyunDLAReadOnlyAccess`权限策略后，RAM账号只能只读访问DLA服务。

> **说明** 系统策略统一由阿里云创建，您只能使用而不能修改，策略的版本更新由阿里云维护。

1. 登录RAM控制台。
2. 单击左侧导航栏的**人员管理 > 用户**。
3. 在**用户**页面，单击目标RAM账号**操作**列的**添加权限**。

4. 在**添加权限**页面，权限类型选择**系统策略**，输入策略名称找到对应的权限策略，单击将其添加到**已选择**框中。



5. 单击**确认**，为RAM账号授权。

   为RAM账号授予相应的权限后，您就可以通过RAM账号访问或者管理DLA服务。

4.DLA子账号绑定RAM账号

本文主要介绍如何将DLA子账号绑定到RAM账号。

背景信息

目前DLA的SQL功能都是通过DLA账号运行的，但是Spark功能是通过RAM账号来运行的。为了打通DLA产品的SQL和Spark两个引擎的元数据互访互通，需要将RAM账号和DLA子账号进行绑定，这样您就可以通过DLA SQL访问到Spark引擎的库表，同样也可以通过Spark访问到DLA SQL引擎的库表。

操作步骤

- 如果您还没有创建DLA子账号，请参考以下步骤绑定RAM账号。
  i. 登录Data Lake Analytics管理控制台
  ii. 在左侧导航栏，单击**账号管理**。
  iii. 在**账号管理**页面，单击**创建子账号**。

  iv. 在**创建数据库子账号**页面的**绑定RAM账号**选项，选择需要绑定的RAM账号，然后单击**确定**。
- 如果您已经创建了DLA子账号，请参考以下步骤绑定RAM账号。
  i. 登录Data Lake Analytics管理控制台。
  ii. 在左侧导航栏，单击**账号管理**。
  iii. 在**账号管理**页面，定位到需要绑定的DLA子账号，在**操作**列单击**绑定RAM账号**。然后选择需要绑定的RAM账号，单击**确定**完成绑定。

> **说明**
> - 如果**绑定RAM账号**下拉选择里面没有您所需要的RAM账号，您可以新建RAM账号，具体请参见创建RAM账号。
> - 一个RAM账号只能绑定到一个DLA子账号。
> - 如果DLA子账号已经绑定了RAM账号，不支持解绑再绑定。您可以通过删除DLA子账号，然后再重新绑定。
> - DLA的Root账号对应的RAM账号为当前阿里云账号的UID，在DLA自动创建Root账号时会进行自动绑定。

5.授予RAM账号细粒度访问DLA的权限

本文主要介绍在RAM访问控制中，如何通过阿里云账号配置RAM账号对DLA的访问权限。

DLA的API操作说明

在DLA中一个基本的概念是虚拟集群，阿里云账号可以在自定义策略中通过API定义一系列的操作和组合来限制RAM账号的权限。API定义如下表所示：

API	说明
openanalytics:ConsolePermission	允许被授权的RAM账户可以访问DLA控制台，如果RAM账户没有此权限则只能通过阿里云OpenAPI通过API的方式来使用DLA。
openanalytics:CreateVirtualCluster	允许被授权的RAM账户在DLA服务中新建一个虚拟集群。
openanalytics:GetVirtualCluster	允许被授权的RAM账户在DLA服务中获取一个虚拟集群的状态和配置。
openanalytics:ListVirtualClusters	允许被授权的RAM账户查询虚拟集群列表。
openanalytics:UpdateVirtualCluster	允许被授权的RAM账户修改虚拟集群的状态和配置，表示该用户可以修改虚拟集群的CPU、Memory配置，以及开启、停止虚拟集群。
openanalytics:DeleteVirtualCluster	允许被授权的RAM账户删除虚拟集群。
openanalytics:ExecuteOnVirtualCluster	允许被授权的RAM账户在虚拟集群中提交作业。

当您希望用户可以获取虚拟集群的状态，同时可以在虚拟集群中提交作业。您可以在RAM控制台中新建一个自定义权限策略，具体操作请参见创建自定义策略，并配置如下脚本：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "openanalytics:ConsolePermission",
        "openanalytics:ListVirtualCluster",
        "openanalytics:GetVirtualCluster",
        "openanalytics:ExecuteOnVirtualCluster"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

通过上述操作被授予了自定义权限策略的RAM账号就拥有了DLA控制台的访问权限，并可以在DLA控制台中查找虚拟集群，向虚拟集群提交作业。

配置RAM账号只能访问某个特定的虚拟集群

当您希望RAM账号只能访问某几个特定的虚拟集群时，就需要修改自定义权限策略中的 `Resource` 来更细粒度的控制RAM账号访问权限。 `Resource` 取值示例和说明如下：

```
acs:openanalytics:${RegionId}:${OwnerId}:virtualcluster/${VirtualClusteName}
```

参数	说明
RegionId	区域。映射关系如下： • 杭州：cn-hangzhou • 北京：cn-beijing • 上海：cn-shanghai • 深圳：cn-shenzhen • 张家口：cn-zhangjiakou • 中国香港：cn-hongkong • 新加坡：ap-southeast-1 • 雅加达：ap-southeast-5 • 以上所有区域：*
OwnerId	为资源所在的阿里云账户的账户ID。您可以在阿里云账号的**安全设置**中看到自己的账号ID。
VirtualClusterName	虚拟集群的名称。

参考上述说明您可以组装出一个虚拟集群对应的唯一一个 `ResourceId` ，并将这个 `ResourceId` 配置到RAM控制台的自定义策略中，您就可以更细粒度的控制RAM账号的行为，配置示例如下：

```
//该示例让RAM用户只能操作杭州区域的daily-test集群，其它的集群则无法进行操作。
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "openanalytics:ConsolePermission",
        "openanalytics:ListVirtualCluster",
        "openanalytics:GetVirtualCluster",
        "openanalytics:ExecuteOnVirtualCluster"
      ],
      "Resource": "acs:openanalytics:cn-hangzhou:123456:virtualcluster/daily-test"
      "Effect": "Allow"
    }
  ]
}
```