ALIBABA CLOUD

Alibaba Cloud

云原生数据仓库AnalyticDB MySQL版

账号和权限管理

文档版本：20220713

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.账号类型 05
2.权限模型 06
3.数据库账号和权限 08
4.RAM用户和权限 10
5.授权服务账号 13
6.重置高权限账号密码 14

1.账号类型

您可以通过阿里云账号或者RAM子账号创建和管理AnalyticDB for MySQL集群，通过数据库账号连接数据库、创建数据库以及创建表等。

账号类型	作用范围	可进行的操作
阿里云账号	AnalyticDB for MySQL集群	阿里云账号用于创建和管理集群，例如登录阿里云产品控制台、设置白名单、创建数据库账号、申请和释放公网地址、设置可维护时间段、扩容集群、恢复新集群以及删除集群等。
RAM子账号	AnalyticDB for MySQL集群	阿里云账号授予RAM子账号一定的权限后，RAM子账号也可以在权限范围内创建和管理集群。 例如登录阿里云产品控制台、设置白名单、创建数据库账号、申请和释放公网地址、设置可维护时间段、扩容集群、恢复新集群以及删除集群等。 RAM子账号从属于阿里云主账号，并且这些子账号下不能拥有实际的任何资源，所有资源都属于阿里云主账号。
数据库账号	数据库	数据库账号在权限范围内用于对数据库进行操作，例如创建/删除数据库、连接数据库、创建/删除表、创建/删除视图等。 数据库账号包括： • 高权限账号 • 普通账号
服务账号	AnalyticDB for MySQL集群	当您在使用AnalyticDB for MySQL集群过程中需要阿里云技术支持时，如果技术支持过程中需要对您的集群进行操作。您需要授权AnalyticDB for MySQL集群的服务账号，技术支持人员才可以通过服务账号提供技术支持服务。在授权有效期结束后，服务账号的权限会被自动回收。

2.权限模型

AnalyticDB for MySQL支持针对不同的权限粒度授予不同的权限达到权限控制的目的。

权限粒度

AnalyticDB for MySQL集群支持以下四个粒度的权限控制：

- GLOBAL：集群级别。
- DB：数据库级别。
- TABLE：表级别。
- COLUMN：列（字段）级别 。

  如果您希望某个用户只查询某一张表的某一列数据，可以将该列的SELECT权限授予该用户，例如`GRANT select (customer_id) ON customer TO 'test321'` 。

操作和权限关系

操作	需要的权限	权限支持的粒度
SELECT	SELECT	• DB • TABLE • COLUMN
INSERT	INSERT	• DB • TABLE • COLUMN
INSERT...SELECT...FROM...	• INSERT • SELECT	• DB • TABLE • COLUMN
UPDATE	UPDATE	• DB • TABLE • COLUMN
DELETE	DELETE	• DB • TABLE
TRUNCATE TABLE	DROP	• DB • TABLE
ALTER TABLE	• ALTER • INSERT • CREATE	• DB • TABLE

操作	需要的权限	权限支持的粒度
CREATE DATABASE	CREATE	-
CREATE TABLE	CREATE	• DB • TABLE
SHOW CREATE TABLE	SELECT	• DB • TABLE
DROP DATABASE	DROP	DB
DROP TABLE	DROP	• DB • TABLE
CREATE VIEW	• CREATE VIEW 执行 `CREATE VIEW REPLACE` 命令时，除了上述权限，还需要DROP权限。 • SELECT	• DB • TABLE
DROP VIEW	DROP	• DB • TABLE
SHOW CREATE VIEW	• SHOW VIEW • SELECT	• DB • TABLE
CREATE USER/DROP USER/RENAME USER	CREATE_USER	-
SET PASSWORD	SUPER	-
GRANT/REVOKE	GRANT	-

3.数据库账号和权限

云原生数据仓库AnalyticDB MySQL版支持高权限账号和普通账号两种类型的数据库账号，高权限账号可以管理所有普通账号和数据库；使用普通账号进行数据库操作时，需要手动创建普通账号，然后为普通账号授权。

数据库账号类型

AnalyticDB MySQL版支持高权限账号和普通账号这两种数据库账号，两种账号的区别见下表。

数据库账号类型	说明
高权限账号	• 只能通过控制台创建和管理高权限账号。 • 一个集群中只能创建一个高权限账号，高权限账号可以管理所有普通账号和数据库。 • 使用高权限账号可以断开任意普通账号的连接。 • 开放了更多权限，可满足个性化和精细化的权限管理需求，例如可按用户分配不同表的查询权限等。 • AnalyticDB MySQL版中的高权限账号相当于MySQL中的root账号。
普通账号	• 只能通过SQL语句进行创建，创建方式，请参见CREATE USER。 • 一个集群最多可以创建256个普通账号。 • 需要手动为普通账号授予指定数据库的权限，详情请参见GRANT和权限模型。 • 普通账号不能断开其他普通账号的数据库连接。

创建高权限账号

1. 登录云原生数据仓库AnalyticDB MySQL控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4. 根据您的集群类型，选择**数仓版（3.0）**。
5. 单击目标集群ID。
6. 在左侧导航栏单击**账号管理**。
7. 在**账号管理**页面右上角，单击**创建高权限账号**。
8. 在**创建高权限账号**面板，设置相关参数。

参数	说明
数据库账号	高权限账号的账号名称。名称需符合如下要求： ○ 长度为2~16个字符。 ○ 以小写字母开头，小写字母或数字结尾。 ○ 可包含小写字母、数字以及下划线（_）。
账号类型	固定为**高权限账号**，无需配置。

参数	说明
密码	高权限账号的密码，密码需符合如下要求： ○ 长度为8~32个字符。 ○ 至少包含大写字母、小写字母、数字或特殊字符中的任意三种。 ○ 特殊字符为：`!@#$%^&*()_+-=` 。
确认密码	再次输入高权限账号的密码。
备注说明	备注该账号的相关信息，便于后续账号管理。可选。

9. 单击**确定**即可。

创建和授权普通账号

只能通过数据链路的SQL语句创建和管理普通账号：

- 创建子账号，请参见CREATE USER。
- 授权子账号，请参见GRANT。
- 撤销子账号权限，请参见REVOKE。
- 更改子账号名，请参见RENAME USER。
- 删除子账号，请参见DROP USER。

4.RAM用户和权限

访问控制RAM（Resource Access Management）是阿里云提供的权限管理系统。RAM主要的作用是控制账号系统的权限，您可以使用RAM在阿里云账号（主账号）的权限范围内创建RAM用户（子账号），给不同的RAM用户分配不同的权限来允许或拒绝RAM用户对云资源的访问，从而达到授权管理的目的。

背景信息

> 说明
> - RAM用户从属于阿里云账号，并且这些RAM用户下不能拥有实际的任何资源，所有资源都属于阿里云账号。
> - 通过RAM用户创建AnalyticDB MySQL版集群后，只能通过该RAM用户和所属阿里云账号查看或使用集群；其他RAM用户需要授权后才能查看或者使用该集群。

使用场景

通过阿里云账号创建AnalyticDB MySQL版集群后，如果您的组织里有多个用户需要使用AnalyticDB MySQL版集群，这些用户只能共享使用您的云账号AccessKey。这里有两个问题：

- 您的密钥由多人共享，泄露的风险很高。
- 您无法控制特定用户可以对集群进行哪些操作，例如扩容集群、重启集群等。

此时，您可以创建RAM用户，并授予RAM用户对应的权限。之后，让您的用户通过RAM用户访问或管理您的AnalyticDB MySQL版集群。

如何实现

通过RAM用户访问或者管理AnalyticDB MySQL版集群需要以下两个步骤。

1. 创建RAM用户。
2. 为RAM用户授权。

创建RAM用户

1. 登录RAM控制台。
2. 单击左侧导航栏的**身份管理 > 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**。

   > 说明 单击**添加用户**，可一次性创建多个RAM用户。

4. 在**访问方式**区域下，选择**控制台访问**或**OpenAPI调用访问**。
   - **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。
   - **OpenAPI调用访问**：自动为RAM用户创建访问密钥（AccessKey）。RAM用户可以通过其他开发工具访问AnalyticDB MySQL版集群。

   为保障账号安全，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AnalyticDB MySQL版集群。
5. 单击**确认**，创建RAM用户。

为RAM用户授权

1. 登录RAM控制台。
2. 单击左侧导航栏的**身份管理 > 用户** 。
3. 在**用户**页面，单击目标RAM用户右侧的**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。

   权限策略说明：

   - 数仓版（3.0）集群的权限：
     - **AliyunADBReadOnlyAccess**，只读访问数仓版（3.0）集群的权限。
     - **AliyunADBFullAccess**，管理数仓版（3.0）集群的权限。
   - 湖仓版（3.0）集群的权限：
     - **AliyunADBReadOnlyAccess**，只读访问湖仓版（3.0）集群的权限。
     - **AliyunADBFullAccess**，管理湖仓版（3.0）集群的权限。
     - **AliyunADBDeveloperAccess**，湖仓版（3.0）集群的开发者权限。与**AliyunADBFullAccess**策略相比，**AliyunADBDeveloperAccess**不包含集群的创建、变配、删除、RAM用户绑定等操作权限。
5. 单击**确认**，为RAM用户授权。

   为RAM用户授予相应的权限后，您就可以通过RAM用户访问或者管理AnalyticDB MySQL版集群。

创建权限策略

如需对RAM用户进行精细到实例级别的操作授权，这种场景需要在RAM中创建自定义权限策略。

1. 登录RAM控制台。
2. 单击左侧导航栏的**权限管理 > 权限策略** 。
3. 单击**创建权限策略**，本文以创建AnalyticDB MySQL数仓版（3.0）集群的管理权限为例。
4. 配置模式选择**脚本配置**。
5. 输入配置脚本，脚本内容示例如下。

   管理“am-xxx”实例权限：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": ["adb:DescribeDBClusters", "adb:ListTagResources"],
            "Resource": "acs:adb:*:*:dbcluster/*",
            "Effect": "Allow"
        },
        {
            "Action": "adb:*",
            "Resource": ["acs:adb:*:*:dbcluster/am-xxx"],
            "Effect": "Allow"
        }
    ]
}
```

只读“am-xxx”实例权限：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": ["adb:DescribeDBClusters", "adb:ListTagResources"],
            "Resource": "acs:adb:*:*:dbcluster/*",
            "Effect": "Allow"
        },
        {
            "Action": "adb:Describe*",
            "Resource": ["acs:adb:*:*:dbcluster/am-xxx"],
            "Effect": "Allow"
        }
    ]
}
```

若RAM用户需要管理或只读多个集群，在脚本的 `"Resource": ["acs:adb:*:*:dbcluster/am-xxx"]` 中增加相应的集群ID即可，例如 `"Resource": ["acs:adb:*:*:dbcluster/am-xxx", "acs:adb:*:*:dbcluster/am-yyy"]` 。

权限策略创建完成后，将权限策略授权给对应RAM用户即可。

6. 单击**下一步：编辑基本信息**。
7. 输入策略名称，单击**确定**。

相关文档

- 当使用AnalyticDB MySQL湖仓版（3.0）时，可以将数据库普通账号绑定RAM用户，直接在AnalyticDB MySQL控制台的SQL编辑器或Spark编辑器中进行数据库开发，请参见绑定RAM账号与数据库普通账号。
- 当RAM用户不再需要某些权限或离开组织时，您可以将这些权限移除或者删除RAM用户，请参见为RAM用户移除权限以及删除RAM用户。

5.授权服务账号

当您在使用云原生数据仓库AnalyticDB MySQL版集群过程中需要阿里云技术支持时，如果技术支持过程中需要对您的集群进行操作，您需要授权AnalyticDB MySQL集群的服务账号，技术支持人员才可以通过服务账号提供技术支持服务。在授权有效期结束后，服务账号的权限会被自动回收。

操作步骤

1. 登录AnalyticDB 控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4. 在**数仓版（3.0）**页签中，单击目标**集群ID**。
5. 在左侧导航栏，单击**账号管理**，然后单击**服务账号授权**。
6. 根据需要，为服务账号授予相应的权限并设置**授权过期时间**。
   - **配置权限**：查看并修改集群的配置。
   - **数据权限**：查看表结构、索引以及SQL。

6.重置高权限账号密码

在使用云原生数据仓库AnalyticDB MySQL版集群的过程中，如果忘记集群的高权限账号密码，可以通过管理控制台重新设置密码。

注意事项

为了数据安全，建议您定期更换密码。

操作步骤

1. 登录云原生数据仓库AnalyticDB MySQL控制台。
2. 在页面左上角，选择集群所在地域。
3. 在左侧导航栏，单击**集群列表**。
4.
5. 在左侧导航栏，单击**账号管理**。
6. 单击高权限账号右侧的**修改密码**。
7. 在弹出的**修改密码**对话框中，输入新密码并确认后，单击**确定**。

   密码设置规则为：

   - 长度为2~16个字符。
   - 以小写字母开头，小写字母或数字结尾。
   - 可包含小写字母、数字以及下划线（_）。