ALIBABA CLOUD

阿里云

数据管理

实例管理

文档版本：20201123

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.数据库账号权限管理

1.1. MySQL数据库账号权限管理

DMS支持细粒度（库、表、列、视图等）级别的MySQL数据库账号权限管控。本文向您介绍如何在DMS中管理MySQL数据库账号权限。

前提条件

- 数据库引擎为RDS MySQL、PolarDB MySQL或自建MySQL。
- 不同管控模式下的角色要求：

管控模式	角色要求
安全协同	管理员、DBA或对应的实例Owner。
稳定变更	无。
自由操作	无。

功能介绍

您可以在RDS MySQL、PolarDB MySQL控制台上对数据库大分类组合权限（例如只读、读写、仅DML、仅DDL）进行便捷地管理与维护，但对于自定义各种权限类型组合或授予某些表级别权限等场景，您可以通过DMS推出的数据库账号权限管理功能进行灵活管控。例如：

- 给A用户授予全局 `SELECT` 和 `UPDATE` 权限。

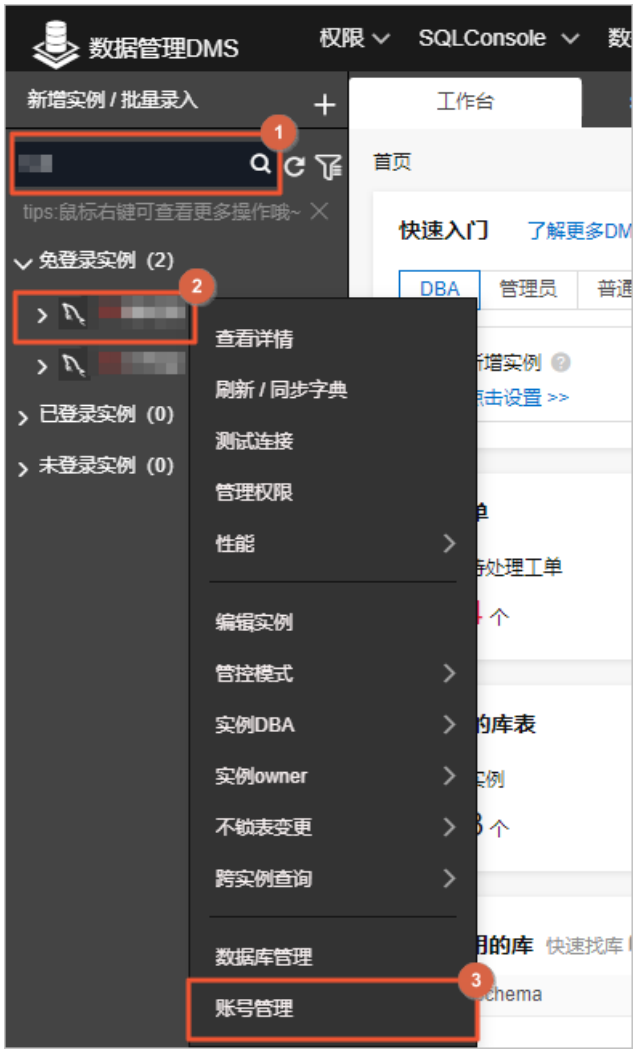
  > **说明** 全局权限作用于整个数据库实例级别，关于更多的全局权限类型介绍请参见MySQL全局权限。

- 给B用户授予单张表的 `SELECT` 权限或某一列的 `UPDATE` 权限。

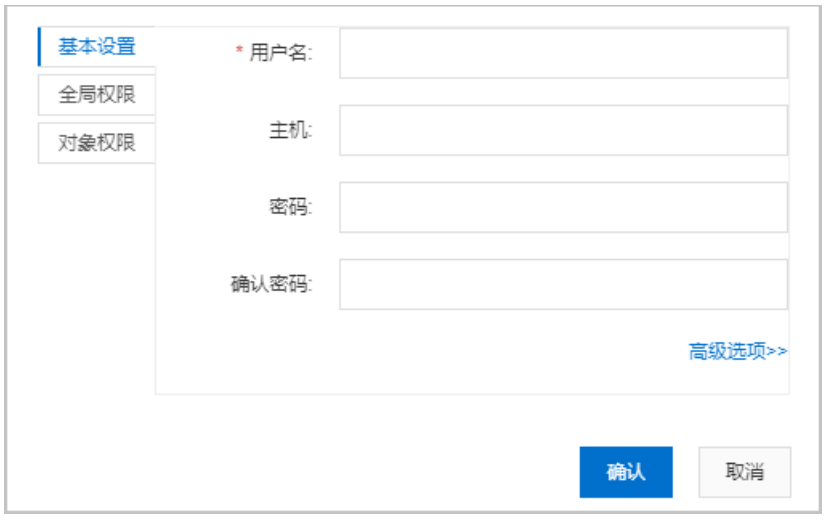
  > **说明** 对象权限作用范围可以是所有数据库对象，也可以指定单个或多个数据库对象，关于更多的对象权限类型介绍请参见MySQL对象权限。

创建用户

1. 登录DMS控制台。
2. 在左上角的导航栏搜索框中输入目标数据库名称，在搜索栏下方的DMS对象列表中找到目标实例。
3. 右键单击目标实例，在弹出的列表中选择**账号管理**。



4. 在**账号管理**页面，单击左上角的**创建用户**按钮。
5. 在弹出的窗口中，设置以下配置项。
   i. 单击**基本设置**页签，配置参数。



配置项	说明
用户名	请输入账号用户名。
主机	请输入用户连接MySQL时所在主机的名字，默认为 `%` 。
密码	请输入登录口令。
确认密码	请再次输入登录口令。

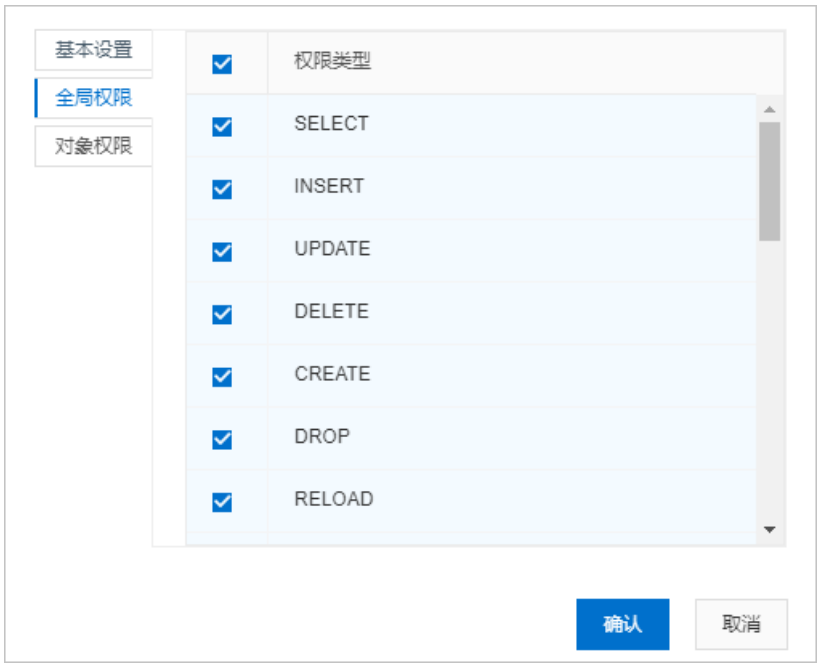
> **说明** 上述配置项的SQL语句格式为 `CREATE USER `用户名`@`主机名` IDENTIFIED BY `登录口令`;` 。

如果您需要配置**高级选项**，请单击**高级选项**按钮，并进行配置。

例如按照下图进行配置的SQL示例为：

```
GRANT USAGE ON *.* TO '用户名'@'主机名' WITH MAX_QUERIES_PER_HOUR 100 MAX_UPDATES_PER_HOUR 200 MAX_CONNECTIONS_PER_HOUR 300 MAX_USER_CONNECTIONS 400;
```

ii. 单击**全局权限**页签，勾选目标权限。



iii. 单击**对象权限**页签，配置参数。例如按照下图进行配置的SQL示例为：

```
GRANT SELECT,INSERT ON `rds_db`.* TO '用户名'@'主机名';
GRANT DELETE ON `rds_db`.`rds_table` TO '用户名'@'主机名';
```

6. 单击**确认**。
7. 在**预览SQL**窗口，单击**确认**。

> **说明** 管控模式为安全协同的数据库实例会受安全规则限制，如无法执行请根据界面提示信息进行操作，或联系DBA、管理员进行确认。

编辑用户

1. 登录DMS控制台。
2. 在左上角的导航栏搜索框中输入目标数据库名称，在搜索栏下方的DMS对象列表中找到目标实例。
3. 右键单击目标实例，在弹出的列表中选择**账号管理**。
4. 单击目标用户右侧**操作**列下的**编辑**即可进行编辑。

删除用户

1. 登录DMS控制台。
2. 在左上角的导航栏搜索框中输入目标数据库名称，在搜索栏下方的DMS对象列表中找到目标实例。
3. 右键单击目标实例，在弹出的列表中选择**账号管理**。
4. 单击目标用户右侧**操作**列下的**删除**。
5. 在新弹窗中，单击**确认**即可删除用户。

MySQL全局权限

权限	权限对象	权限说明
CREATE	数据库、表或索引	创建数据库、表或索引权限。
DROP	数据库、表或视图	删除数据库或表权限。
GRANT OPTION	数据库、表或保存的程序	赋予权限选项。
REFERENCES	数据库、表或列	外键权限。
LOCK TABLES	数据库	锁表权限。
EVENT	数据库	查询、创建、修改、删除MySQL事件的权限。
ALTER	表、视图	更改表，比如添加字段、索引、修改字段等。
DELETE	表	删除数据权限。
INDEX	表	索引权限。
INSERT	表、列	插入权限。
SELECT	表、列	查询权限。
UPDATE	表、列	更新权限。
CREATE VIEW	视图	创建视图权限。
SHOW VIEW	视图	查看视图权限。

权限	权限对象	权限说明
TRIGGER	触发器	创建、删除、执行、显示触发器的权限。
ALTER ROUTINE	存储过程	更改存储过程权限。
CREATE ROUTINE	存储过程	创建存储过程权限。
EXECUTE	存储过程	执行存储过程权限。
FILE	服务器主机上的文件访问	文件访问权限。
CREATE TEMPORARY TABLES	服务器管理	创建临时表权限。
CREATE USER	服务器管理	创建用户权限。
PROCCESS	服务器管理	查看进程权限。
RELOAD	服务器管理	执行 FLUSH-HOSTS 、 FLUSH-LOGS 、 FLUSH-PRIVILEGES 、 FLUSH-STATUS 、 FLUSH-TABLES 、 FLUSH-THREADS 、 REFRESH 、 RELOAD 等命令的权限。
REPLICATION CLIENT	服务器管理	复制权限。
REPLICATION SLAVE	服务器管理	复制权限。
SHOW DATABASES	服务器管理	查看数据库权限。
SHUTDOWN	服务器管理	关闭数据库权限。
SUPER	服务器管理	执行kill线程权限。

MySQL对象权限

权限	权限对象	权限说明
CREATE	数据库、表或索引	创建数据库、表或索引权限。
DROP	数据库、表或视图	删除数据库或表权限。
GRANT OPTION	数据库、表或保存的程序	赋予权限选项。
REFERENCES	数据库、表或列	外键权限。
LOCK TABLES	数据库	锁表权限。

权限	权限对象	权限说明
EVENT	数据库	查询、创建、修改、删除MySQL事件的权限。
ALTER	表、视图	更改表，比如添加字段、索引、修改字段等。
DELETE	表	删除数据权限。
INDEX	表	索引权限。
INSERT	表、列	插入权限。
SELECT	表、列	查询权限。
UPDATE	表、列	更新权限。
CREATE VIEW	视图	创建视图权限。
SHOW VIEW	视图	查看视图权限。
TRIGGER	触发器	创建、删除、执行、显示触发器的权限。

1.2. MongoDB数据库账号权限管理

您可以在DMS中非常便捷地管控MongoDB数据库账号及其对应的**普通操作角色**、**管理员操作角色**、**实例级别操作角色**、**集群管理员角色**、**备份与恢复操作角色**等权限。

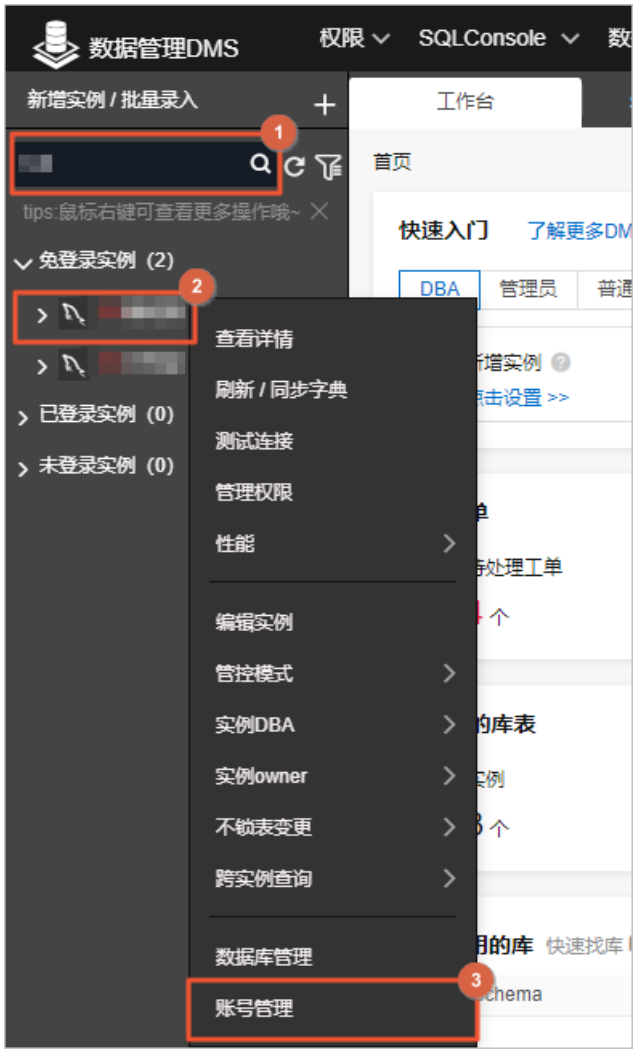
前提条件

- 数据库引擎为MongoDB。
- 不同管控模式下的角色要求：

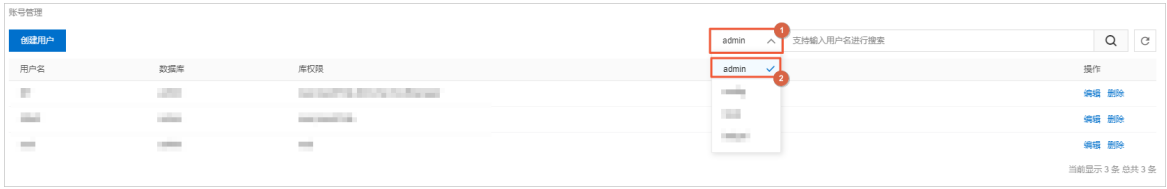
管控模式	角色要求
安全协同	管理员、DBA或对应的实例Owner。
稳定变更	无。
自由操作	无。

创建用户

1. 登录DMS控制台。
2. 在左上角的导航栏搜索框中输入目标数据库名称，在搜索栏下方的DMS对象列表中找到目标实例。
3. 右键单击目标实例，在弹出的列表中选择**账号管理**。



4. 在**账号管理**页面，单击数据库列表，选择目标数据库。



5. 单击页面左上角的**创建用户**按钮。
6. 在**创建用户**页面，设置以下配置项。


创建用户
1
* 目标库:
admin
* 用户名:
* 密码:
* 确认密码:
2
当前库权限
其他库权限
普通操作角色
read 查询本库的权限
readWrite 增删改查本库的权限
管理员操作角色
dbAdmin 数据库对象的管理操作，但没有数据库的读写权限
确认
取消

i. 设置用户信息。

配置项目	说明
目标库	下拉选择该用户保存的目标数据库。 **说明** ■ 目标库选择为非admin库时，创建的用户为普通用户。 ■ 目标库选择为**admin**库时，创建的用户为高权限用户。
用户名	设置用户的名称。 ■ 不支持中文。 ■ 支持英文、数字和特殊字符。 ■ 特殊字符包括： !#$%^&*()_+-=
密码	设置用户的密码。 为保障数据安全性，建议设置的密码由大写字母、小写字母、数字、特殊字符中的至少三种组成，长度为8-32位。 特殊字符包括： !#$%^&*()_+-=
确认密码	再次输入密码。

ii. 设置用户的权限信息。

说明

■ 当目标库选择为admin库时：

在**当前库权限**页签，可以设置**普通操作角色**、**管理员操作角色**、**实例级别操作角色**、**集群管理员角色**、**备份与恢复操作角色**、**超级角色**等权限，角色权限详情请参见MongoDB角色权限说明。

也可以选择**其他库权限**页签，并添加数据库名及设置对应数据库的角色权限。

■ 当目标库选择为非admin库时：

在**当前库权限**页签，只能设置当前库**普通操作角色**和**管理员操作角色**，角色权限详情请参见MongoDB角色权限说明。

无**其他库权限**页签的设置权限。

7. 单击**确认**。

说明 管控模式为安全协同的数据库实例会受安全规则限制，如无法执行请根据界面提示信息进行操作，或联系DBA、管理员进行确认。

编辑用户

1. 登录DMS控制台。
2. 在左上角的导航栏搜索框中输入目标数据库名称，在搜索栏下方的DMS对象列表中找到目标实例。
3. 右键单击目标实例，在弹出的列表中选择**账号管理**。
4. 在**账号管理**页面，单击数据库列表，选择目标数据库。
5. 单击目标用户右侧**操作**列下的**编辑**即可进行编辑。

删除用户

1. 登录DMS控制台。
2. 在左上角的导航栏搜索框中输入目标数据库名称，在搜索栏下方的DMS对象列表中找到目标实例。
3. 右键单击目标实例，在弹出的列表中选择**账号管理**。
4. 在**账号管理**页面，单击数据库列表，选择目标数据库。
5. 单击目标用户右侧**操作**列下的**删除**。
6. 在新弹窗中，单击**确认**即可删除用户。

MongoDB角色权限说明

角色权限的详情说明请参见MongoDB官网介绍。

角色类型	权限	权限说明
普通操作角色	read	查询本库的权限。
	readWrite	增删改查本库的权限。
管理员操作角色	dbAdmin	数据库对象的管理操作，但没有数据库的读写权限。
	userAdmin	在本库下创建用户的权限。
	dbOwner	本库所有操作的权限。
实例级别操作角色	readAnyDatabase	查询本实例所有库的权限。
	readWriteAnyDatabase	增删改查本例所有库的权限。
	userAdminAnyDatabase	在本实例所有库下创建用户的权限。
	dbAdminAnyDatabase	本实例所有库的dbAdmin权限。
	hostManager	数据库对象的管理操作，但没有数据库的读写权限。

角色类型	权限	权限说明
集群管理员角色	clusterMonitor	查询集群和复制集的权限。
	clusterManager	管理和监控集群和复制集的权限。
	clusterAdmin	集群所有操作的权限。
备份与恢复操作角色	backup	查询本实例所有库的权限。
	restore	增删改查本例所有库的权限。
超级角色	Root	超级用户权限。

2.设置管控模式

您可以在录入实例时设置实例的**管控模式**，在录入实例后，您也可以根据您的需求随时在**实例管理**页面下或在控制台首页左侧实例列表中调整目标实例的**管控模式**。

前提条件

您的用户角色为DBA或管理员。

背景信息

数据管理DMS提供**自由操作**、**稳定变更**、**安全协同**三种管控模式，有关各管控模式的功能说明，请参见管控模式简介。

在录入实例时设置管控模式

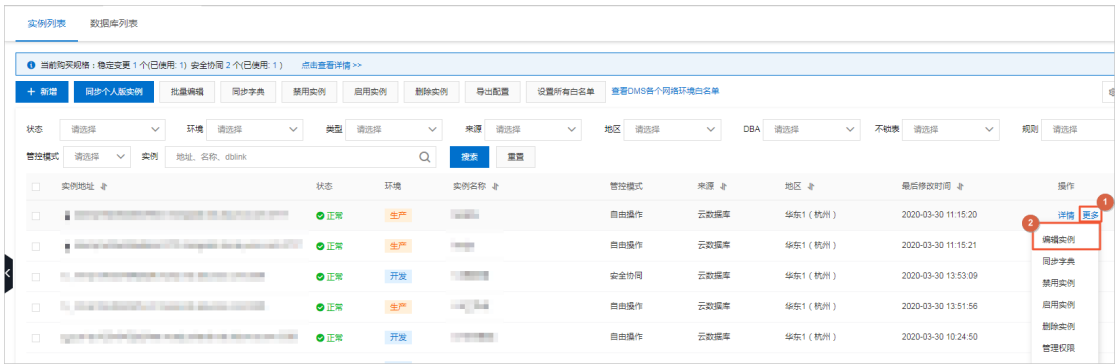
具体操作方法请参见云数据库录入。

在实例管理页面设置管控模式

目前在DMS中有两种进入方式进入**实例管理**。

1. 登录DMS控制台。通过顶部菜单栏进入
   i. 在顶部菜单栏，单击**系统管理 > 实例管理**。

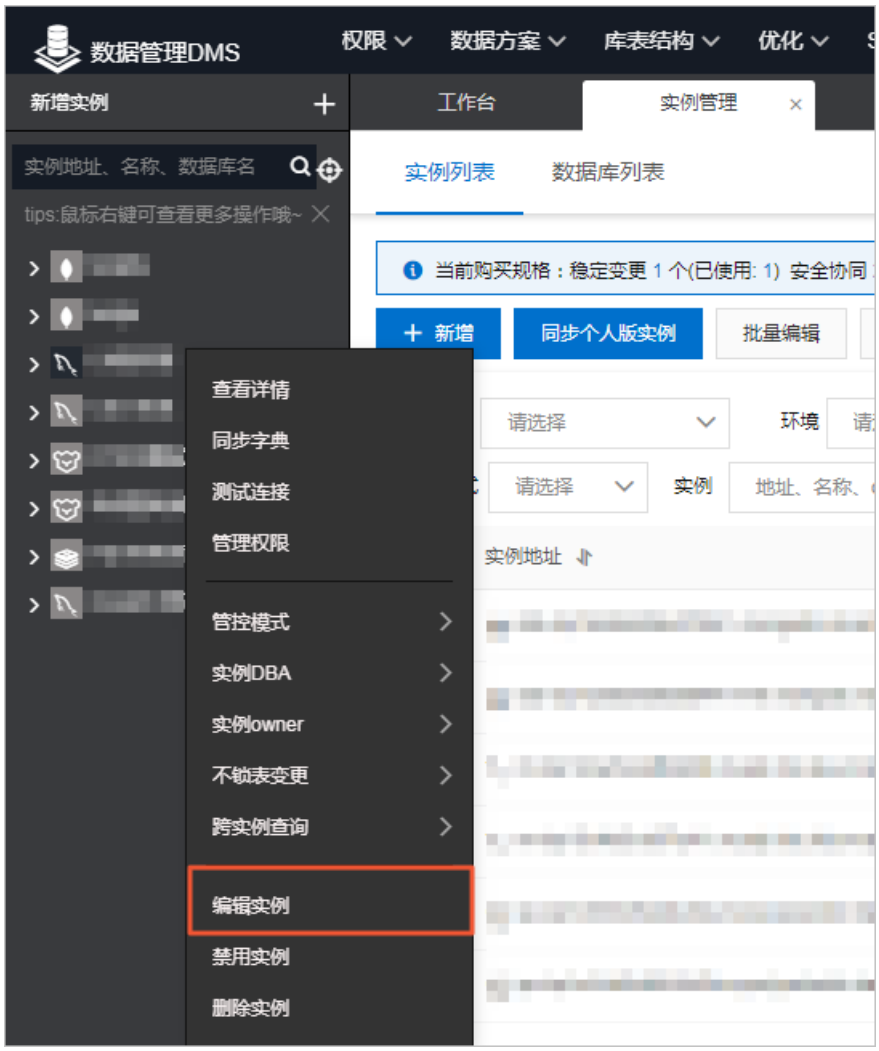
   ii. 在**实例列表**标签页中，单击目标实例**操作**列下面的**更多 > 编辑实例**。



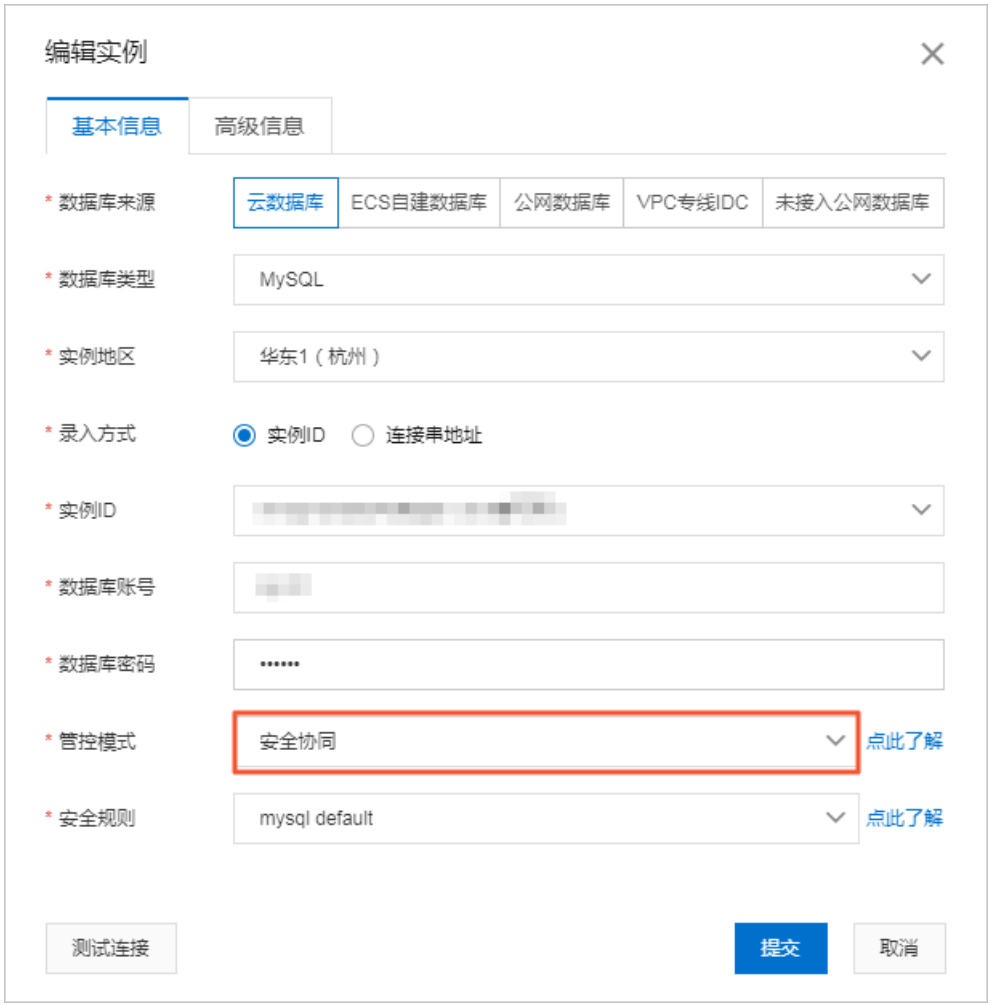
通过控制台首页左侧实例列表进入

   i. 在控制台首页左侧实例列表区域中，右键单击目标实例。

ii. 单击右键菜单中的**编辑实例**。



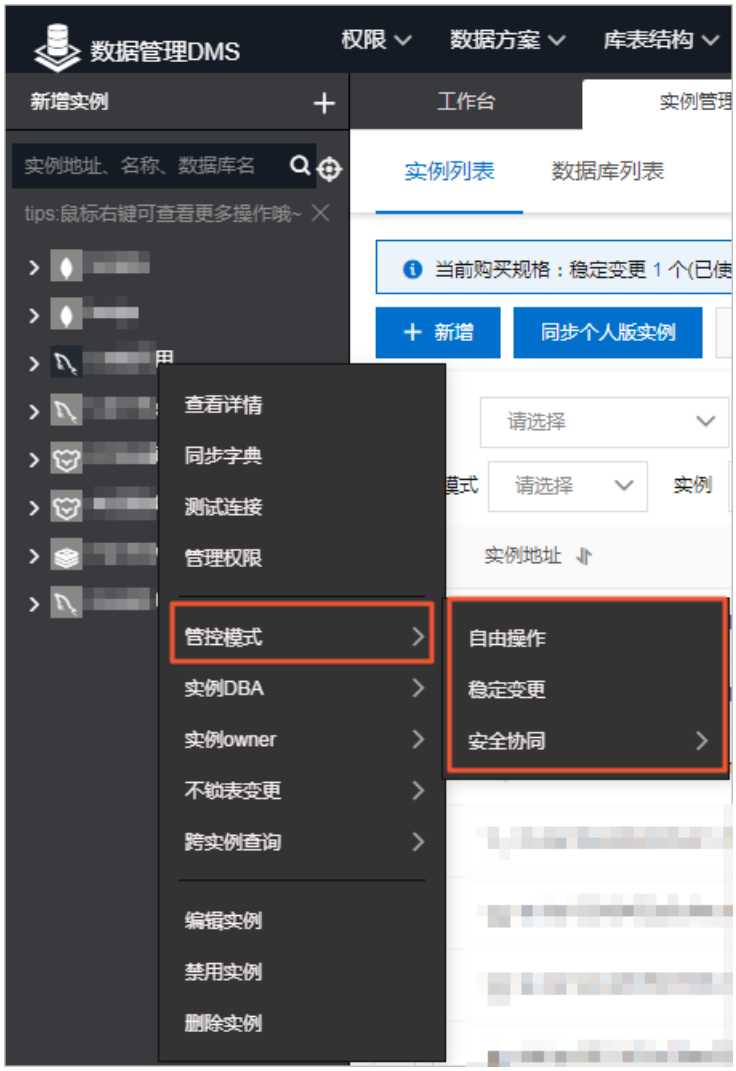
2. 在弹出的**编辑实例**对话框中，根据实际业务需求选择**管控模式**。



> **说明** 如果您选择的**管控模式**为**安全协同**，您还需要选择**安全规则**。具体请参见管控模式简介。

在控制台首页左侧实例列表中快速设置管控模式

1. 登录DMS控制台。
2. 在控制台首页左侧实例列表区域中，右键单击目标实例。
3. 在右键菜单的**管控模式**子菜单中，根据实际业务需求选择**管控模式**。



> **说明** 如果您选择的**管控模式**为**安全协同**，您还需要选择**安全规则**。具体请参见管控模式简介。

3.设置IP白名单

DMS支持批量设置白名单，您可以通过该功能将对应地域的DMS白名单添加至已录入的所有云数据库中。

前提条件

您的用户角色为DBA或管理员。

注意事项

如果您的数据库来源为ECS自建数据库、公网数据库、VPC专线IDC、未接入公网数据库，您需单击**查看DMS各个网络环境白名单**，手动添加对应地域的DMS白名单，详情请参见DMS白名单列表。

操作步骤

1. 登录DMS控制台。
2. 在顶部菜单栏，单击**系统管理 > 实例管理**。

3. 选中目标数据库实例，单击实例列表上方的**设置白名单**。

> **说明** 该操作会将对应地域的DMS白名单添加至目标数据库实例中。

4. 在弹出对话框中，单击**确认**。

DMS白名单列表

当数据订阅的源数据库为**有公网IP的自建数据库**或**通过专线/VPN网关/智能网关接入的自建数据库**时，通过下表定位到源数据库所在区域，获取对应的IP地址段并将其加入到源数据库的安全设置中。

> **说明**
> - 如果**公网数据库**对应的地域没有DMS白名单，您可以选择就近地域的DMS白名单。
> - 下表同时为您列出了经典网络和专有网络的阿里云数据库，当您在维护云数据库的白名单时避免误删除。

地域	经典网络（ECS自建库或阿里云数据库）	专业网络（ECS自建库或阿里云数据库或VPC专线IDC）	公网数据库

地域	经典网络（ECS自建库或阿里云数据库）	专业网络（ECS自建库或阿里云数据库或VPC专线IDC）	公网数据库
华东1（杭州）	11.193.54.0/24 10.143.32.0/24 10.143.34.0/24	100.104.175.0/24	101.37.74.0/24 112.124.140.0/24 121.43.18.66 121.43.18.68
华东2（上海）	10.152.163.0/24	100.104.5.0/24	139.224.4.0/24
华北1（青岛）	10.151.203.0/24	100.104.188.0/24	114.215.161.0/24
华北2（北京）	11.192.101.0/24	100.104.72.0/24	60.205.89.0/24
华北3（张家口）	11.192.243.0/24	100.104.205.0/24	无
华北5（呼和浩特）	11.193.183.0/24	100.104.205.0/24	39.104.29.35/24
西南1（成都）	11.195.52.68/24	100.104.5.0/26	无
华南1（深圳）	10.152.27.0/24	100.104.5.0/24	120.76.91.0/24
华南2（河源）	11.118.24.0/24	100.104.96.64/26	无
中国（香港）	10.152.161.0/24	100.104.205.0/24	47.89.61.0/24
亚太东南 1（新加坡）	10.152.166.0/24	100.104.205.0/24	47.88.147.0/24
亚太东南 2（悉尼）	11.192.100.0/24	100.104.5.0/24	47.91.49.0/24
亚太东南 3（吉隆坡）	11.193.189.0/24	100.104.175.0/24	47.254.212.25/24
亚太东南 5（雅加达）	11.194.48.0/22	100.104.5.0/24	149.129.228.88/24
亚太南部 1（孟买）	11.194.10.0/24	100.104.205.0/24	149.129.164.77/24
亚太东北 1（东京）	11.192.147.0/24 11.192.148.0/24 11.192.149.0/24	100.104.205.0/24	47.91.9.0/24 47.91.12.0/24 47.91.13.0/24
美国西部 1（硅谷）	10.152.31.0/24	100.104.205.0/24	47.89.224.0/24
美国东部 1（弗吉尼亚）	10.152.235.0/24	100.104.205.0/24	47.89.170.0/24
欧洲中部 1（法兰克福）	11.192.169.0/24,11.192.170.0/24	100.104.233.0/24	47.91.83.0/24, 47.91.84.0/24
英国（伦敦）	11.199.93.0/24	100.104.5.0/24	无

地域	经典网络（ECS自建库或阿里云数据库）	专业网络（ECS自建库或阿里云数据库或VPC专线IDC）	公网数据库
中东东部 1（迪拜）	11.192.189.0/24 11.192.190.0/24 11.192.191.0/24	100.104.5.0/24	47.91.102.0/24 47.91.103.0/24 47.91.112.0/24
金融云杭州	无	100.104.175.0/24	无
金融云上海	无	100.104.72.0/24	无
金融云深圳	无	100.104.205.0/24	无

4.设置访问控制

数据管理DMS新推出的元数据访问控制功能，是指在DMS中对数据库、实例的查看与访问权限进行控制的功能。本文将介绍如何在DMS中开启实例访问控制与数据库访问控制。

背景信息

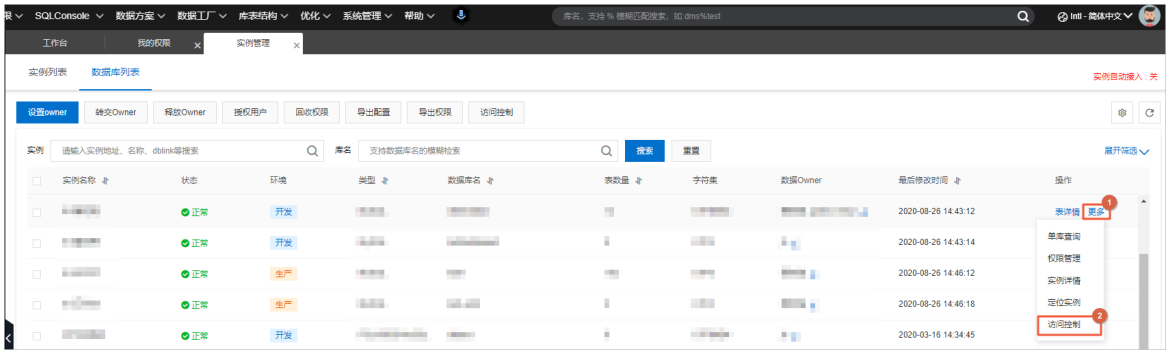
DMS作为企业内数据库统一管理入口，已为不同用户提供了访问不同数据的管控权限。DMS新推出的元数据访问控制功能将进一步加强企业的数据安全管控，该功能开启后可实现指定数据库仅允许被已授权的用户查看和访问。

> **说明** 在DMS中，数据库级别的权限有**查询**、**导出**、**变更**，若某用户有其中任意一种权限即被视为已授权该数据库，可在DMS中获取到如下信息：
>
> - 查看到该数据库（包括实例左侧导航栏、顶部搜索栏、权限申请搜索栏等），能否查询该库的数据取决于是否拥有**查询**权限。
> - 查看到该库所在的实例信息，但不能看到该实例下的其他数据库，能否查看到其他数据库取决于是否拥有其他数据库的权限。

开启数据库访问控制

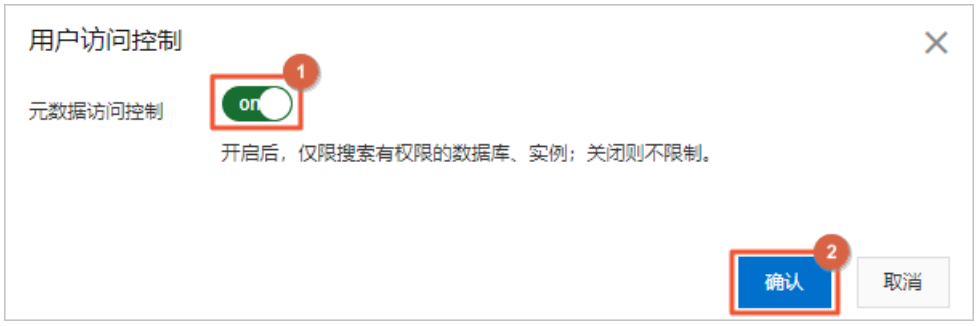
1. 登录DMS控制台。
2. 在顶部菜单栏，单击**系统管理 > 实例管理**。

3. 单击**数据库列表**页签。
4. 在**数据库列表**页签中，找到目标数据库，单击右侧**操作**列下的**更多 > 访问控制**按钮。



> **说明** 您也可以批量选中多个数据库并单击页面上方的**访问控制**按钮，批量开启多个数据库的访问控制开关。

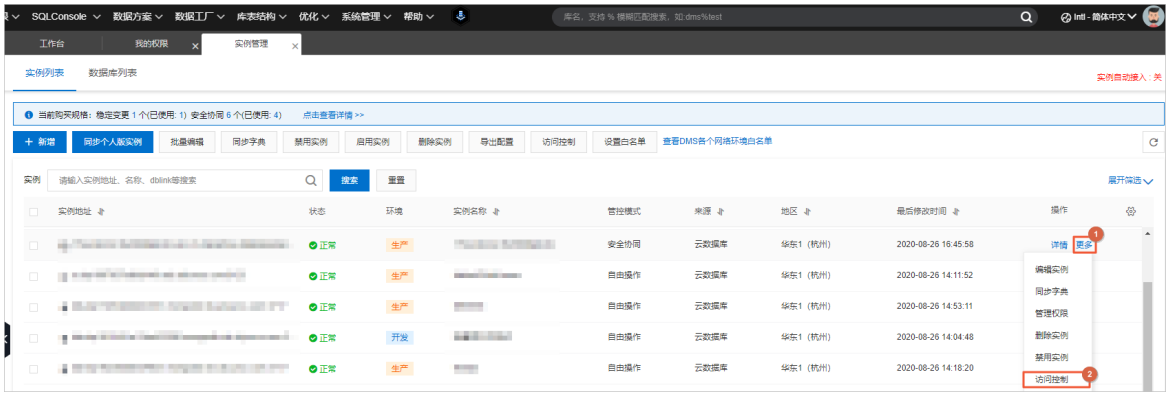
5. 在新弹窗中，打开**元数据访问控制**开关，并单击**确认**即可。



开启实例访问控制

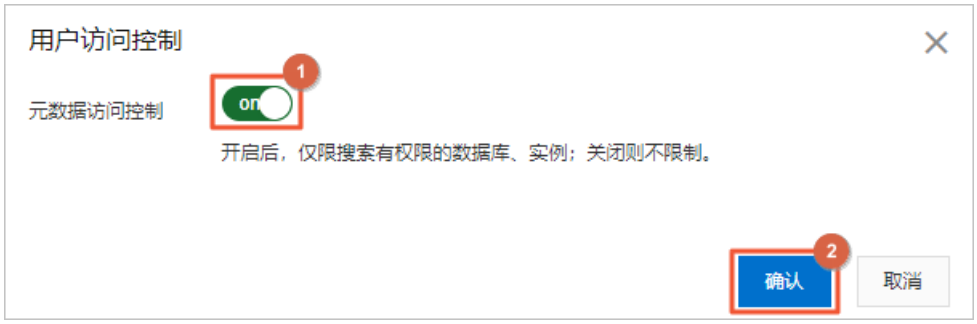
1. 登录DMS控制台。
2. 在顶部菜单栏，单击**系统管理 > 实例管理**。

3. 在**实例列表**页签中，找到目标实例，单击右侧**操作**列下的**更多 > 访问控制**按钮。



> **说明** 您也可以批量选中多个实例并单击页面上方的**访问控制**按钮，批量开启多个实例的访问控制开关。

4. 在新弹窗中，打开**元数据访问控制**开关，并单击**确认**即可。


用户访问控制
元数据访问控制
on
1
开启后，仅限搜索有权限的数据库、实例；关闭则不限制。
2
确认
取消