

数据管理服务

# 最佳实践

文档版本 01  
发布日期 2023-10-30



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://e.huawei.com>

# 安全声明

## 产品生命周期政策

华为公司对产品生命周期的规定以“产品生命周期终止政策”为准，该政策的详细内容请参见如下网址：  
<https://support.huawei.com/ecolumnsweb/zh/warranty-policy>

## 漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：  
<https://www.huawei.com/cn/psirt/vul-response-process>  
如企业客户须获取漏洞信息，请参见如下网址：  
<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

## 华为预置证书权责说明

华为公司对随设备出厂的预置数字证书，发布了“华为设备预置数字证书权责说明”，该说明的详细内容请参见如下网址：  
<https://support.huawei.com/enterprise/zh/bulletins-service/ENEWS2000015766>

## 华为企业业务最终用户许可协议(EULA)

本最终用户许可协议是最终用户（个人、公司或其他任何实体）与华为公司就华为软件的使用所缔结的协议。最终用户对华为软件的使用受本协议约束，该协议的详细内容请参见如下网址：  
<https://e.huawei.com/cn/about/eula>

## 产品资料生命周期策略

华为公司针对随产品版本发布的售后客户资料（产品资料），发布了“产品资料生命周期策略”，该策略的详细内容请参见如下网址：  
<https://support.huawei.com/enterprise/zh/bulletins-website/ENEWS2000017760>

---

# 目 录

---

1 如何通过 DAS 实现只读账号登录数据库..... 1

2 如何通过 TOP SQL 检查并进行表优化..... 6

# 1 如何通过 DAS 实现只读账号登录数据库

DAS服务的系统权限策略中本身不支持只读账号，但是可以通过在IAM里创建用户自定义策略，搭配数据库自身的只读账号功能来实现。

## IAM 权限和数据库权限的区别

DAS作为管理面服务，不会直接对客户的数据库实例资源进行增删改操作。在DAS页面执行的只有增删改数据库连接（即数据库登录信息）的操作。

IAM权限控制对DAS的应用范围仅在登录数据库连接前，登录数据库连接后，权限校验就由数据库账号自身的权限来接管了。

您可以通过IAM[自定义权限策略](#)来控制子账号是否能增删改数据连接、能否登录数据库连接，但是进入数据库后，IAM无法再干涉用户执行SQL命令，此时只有数据库账号权限可以发挥作用。

## 操作步骤

**步骤1** 使用主账号登录统一身份认证服务IAM控制台。

**步骤2** 创建自定义权限策略。

1. 在左侧导航栏中选择“权限管理 > 权限”，单击“创建自定义策略”。
2. 配置相关参数。

图 1-1 配置自定义权限策略

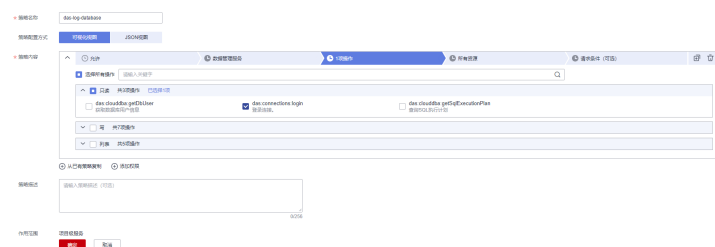
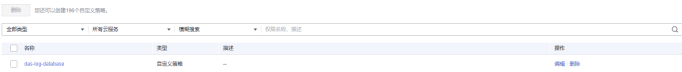


表 1-1 参数说明

| 参数名称   | 说明   | 示例                    |
|--------|--|-----------------------|
| 策略名称   | 自定义名称。   | das-log-database      |
| 策略配置方式 | 支持可视化视图和JSON视图。  | 可视化视图                 |
| 策略内容   | 选择数据管理服务，根据需要添加相应的只读权限。<br>此处以“das:connections:login”为例，添加了此权限的用户或用户组仅具有通过DAS服务登录数据库连接的功能。 | das:connections:login |

3. 单击确定，返回权限页面，可以查看到刚创建好的自定义权限策略。

图 1-2 查看自定义权限策略



**步骤3** 创建用户组并授权**步骤2**中的自定义权限策略。

1. 在左侧导航栏选择用户组，单击“创建用户组”，填写用户组名称，完成用户组创建。
2. 单击用户组操作列的“授权”，选择**步骤2**中创建好的自定义策略。

图 1-3 授权



3. 单击“下一步”，授权范围默认“所有资源”，继续单击“确定”。

**步骤4** 创建用户并添加到用户组。

1. 在左侧导航栏选择用户，单击“创建用户”，配置用户基本信息。

图 1-4 配置用户基本信息



2. 单击下一步，将当前用户添加到步骤3中创建的用户组中。

图 1-5 添加用户到用户组



3. 单击创建用户，即可创建新用户（即IAM子账号）。此时该用户只有DAS登录数据库连接的权限。

步骤5 创建数据库只读账号。此处以RDS for MySQL为例。

1. 登录云数据库RDS控制台。
2. 在实例管理页面，单击目标实例名称，进入基本信息页面。
3. 在左侧导航栏中选择“账号管理”，单击“创建账号”，创建一个只读权限的数据库账号。

图 1-6 创建数据库只读账号



说明

您也可以登录RDS for MySQL数据库通过命令行来创建只读账号，具体可参考如下命令：

```
CREATE USER 'db_read_only'@'%' IDENTIFIED BY '*****';
GRANT SELECT ON *.* TO 'db_read_only'@'%';
FLUSH PRIVILEGES;
```

**步骤6** 主账号通过DAS共享只读数据库功能给IAM子账号。

- 1. 使用主账号登录数据管理服务控制台。
- 2. 使用只读数据库账号新增一条登录信息。

在左侧导航栏选择“开发工具”，在“由我创建的数据库实例登录”页面，单击“新增数据库实例登录”。

新增数据库实例登录

\* 数据库引擎

MySQL

\* 数据库来源

RDS

ECS

数据库实例

数据库引擎版本

实例类型

状态

rds-cc63

MySQL 5.7

Ha

正常

5

总数: 1

<

1

>

\* 登录用户名

rds-test

\* 密码

\*\*\*\*\*

测试连接

连接成功。

☐ 记住密码

同意DAS使用加密方式记住密码

描述

定时采集

☐

若不开启，DAS只能实时的从数据库获取结构定义数据，将会影响数据库实时性能。

SQL执行记录

☐

确定

取消

此处登录用户名使用步骤5中创建好的数据库只读账号。

- 3. 共享只读账号的数据库实例登录信息给IAM子账号。  
单击数据库实例登录信息列表中“共享用户数”列对应的数字。

图 1-7 共享用户

| 数据库实例 | 数据库引擎版本      | 数据库来源 | 登录用户名    | 记住密码                                | 描述 | 创建时间                     | 共享用户数 | 操作         |
|-------|--------------|-------|----------|-------------------------------------|----|--------------------------|-------|------------|
| rds   | MySQL 5.7.41 | RDS   | rds-test | <input checked="" type="checkbox"/> |    | 2023/11/10 11:36:37 C... | 1     | 删除 修改 删除记录 |

选择共享截止时间，添加方式选择同步子账号，在待选用户中选择步骤4中创建的IAM子账号，单击“确定”。



图 1-8 添加共享用户

添加共享用户

共享截止日期2023/11/30

系统将于共享截止日期00:00:00自动取消共享此各数据库实例登录，可能存在因系统繁忙导致的延迟。

添加方式手动录入同步子账号同步EPS用户

主账号hwstaff\_pub\_CBUInfo\_DB

待选用户

请输入用户ID/用户名

| 用户ID  | 用户名    |
|-------|--------|
| 6dae8 | 51dc90 |
| 6dae8 | 51dc90 |
| 6dae8 | 51dc90 |

已选用户

| 用户ID  | 用户名    |
|-------|--------|
| 6dae8 | 51dc90 |
| 6dae8 | 51dc90 |

确定取消

步骤7 使用步骤4中创建好的IAM子账号登录数据管理服务，验证只读权限。

图 1-9 验证只读权限

由我创建的数据库实例登录

他人共享给我的数据库实例登录

查看我的用户ID

全部数据库实例

全部数据库实例

请输入数据库实例ID/实例名称

| 共享人 | 数据库实例   | 数据库引擎版本      | 数据库类型 | 登录用户名   | 记住密码 | 备注 | 创建时间                     | 共享截止日期 | 操作 |
|-----|---------|--------------|-------|---------|------|----|--------------------------|--------|----|
|     | mb-ccc3 | MySQL 5.7.41 | RDS   | ro-test | 否    |    | 2023/11/10 14:26:43 G... |        | 登录 |

10 总页数: 1

使用IAM子账号登录到DAS服务后，选择“开发工具”，可以在他人共享给我的数据库实例登录页面，查看到由主账号共享给IAM子账号的数据库登录信息。在操作列可以看到只有登录数据库连接的权限。

----结束

# 2 如何通过 TOP SQL 检查并进行表优化

## 问题举例

用户在导出的日志记录中发现某一时间段select语句查询test表信息的耗时超过2s，锁等待时间长。

## 建议措施

- 增加索引。
- 优化表。

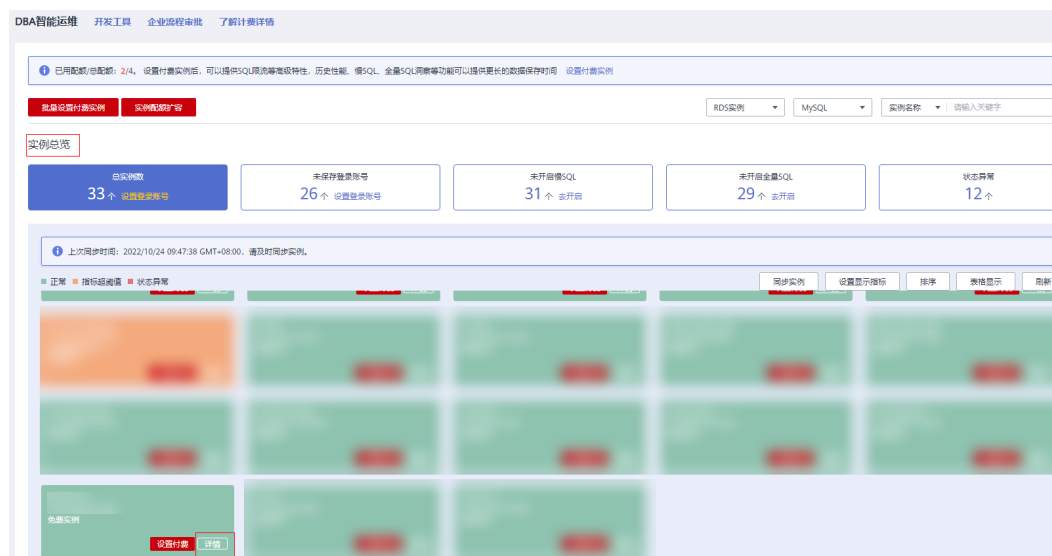
## 操作步骤

**步骤1** 登录华为云console，输入华为账户和密码登录数据管理服务（DAS）。

**步骤2** 在数据管理控制台选择DBA智能运维页签，进入监控实例总览页面。

**步骤3** 在实例总览页面选择所需诊断的实例名称，单击“详情。”

图 2-1 DBA 智能运维实例总览页面



**步骤4** 在所选实例的DBA智能运维总览页面选择“SQL”>“全量SQL洞察”。

步骤5 在“全量SQL洞察”下选择“TOP SQL”。

图 2-2 TOP SQL



步骤6 在“TOP SQL”页签下单击“详情”查看select的SQL模板信息。

步骤7 在SQL详情页查看下方的“SQL列表”，找出在此时间段内select模板执行耗时大于2s的数据库db\_test。

图 2-3 SQL 列表



步骤8 登录当前实例，选择数据管理控制台的“库管理”页签。并选择步骤7中的数据库名称。单击“查看表详情”。检查表格中索引数量、数据容量等信息。

图 2-4 查看表详情



**步骤9** （举例）确认是索引问题后，单击“修改表”，增加索引。返回表管理页签，单击SQL查询进行重试即可。

图 2-5 SQL 查询



----结束