ALIBABA CLOUD

阿里云

数据管理

安全管理

文档版本：20210811

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.数据安全防护

1.1. 开启数据安全防护

数据安全防护为应用程序调用企业数据库带来更全面的安全管控、访问控制、数据脱敏以及操作审计等安全保障。应用程序可以使用标准的MySQL/HTTPS协议，直连数据安全防护为数据库实例生成的代理地址，轻松实现安全的数据库访问。管理员、DBA、实例owner可以为实例开启数据安全防护。本文介绍如何开启实例的数据安全防护。

前提条件

- 实例的数据库类型为MySQL与MariaDB，包括阿里云RDS MySQL、PolarDB MySQL引擎、PolarDB-X、AnalyticDB MySQL，也支持自建MySQL与MariaDB库、第三方云MySQL与MariaDB库。

  > **说明** 您可以在左侧导航栏，将鼠标放在目标实例上，查看实例的数据库类型。

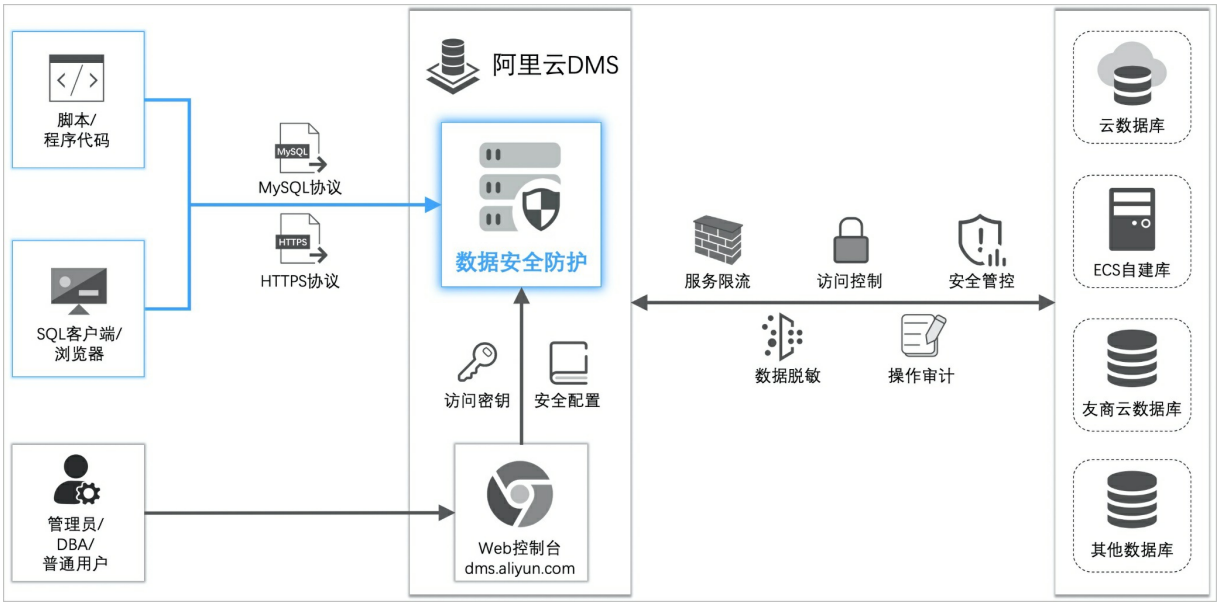
- 数据库实例所在地区为华东1（杭州）、华北2（北京）。

  > **说明** 您可以在左侧导航栏，将鼠标放置在目标实例上，查看实例所在地区。
  > 如您有新地区的需求，请提交工单或联系阿里云售后进行反馈。

- 用户是管理员角色或DBA角色，或者是目标实例owner。

背景信息

DMS一直致力于为人员通过DMS界面访问数据库时，提供高安全等级的保障服务。现在通过数据安全防护，可以为应用程序访问数据库提供同等的安全保障能力。数据安全防护完全复用了DMS产品内已有的安全规则、数据权限、敏感列配置等功能，为企业数据库提供更全面的安全管控、访问控制、数据脱敏以及操作审计等安全能力。您的应用可以使用标准的MySQL/HTTPS协议，直连数据安全防护为数据库实例生成的代理地址，轻松实现安全的数据库访问。



开启数据安全防护

1. 登录数据管理DMS 5.0。

> **说明** 如果您需要切换到旧版数据管理DMS，单击页面右下角，进入**数据管理DMS**平台。具体操作，请参见数据管理DMS 5.0切换至旧版。

2. 在顶部菜单栏中，选择**数据资产 > 实例管理**。

> **说明** 如果您使用的是旧版数据管理DMS，在顶部菜单栏中，选择**全部功能 > 系统管理 > 实例管理**。

3. 单击**实例列表**页签，从操作列中选择**更多 > 数据安全防护**。
4. 在**数据安全防护**页面，单击**开启数据安全防护**。
5. 在**开启数据安全防护**对话框中，输入数据库账号和密码。
该实例的数据安全防护功能开启。

相关操作

实例开启了数据安全防护功能后，管理员、DBA、实例owner、责任人可以进行以下相关操作：

- 开启公网地址：当应用程序与实例不在同一VPC内，或需要从本地应用程序调用目标实例时，可单击**开启**，获取公网地址。
- 编辑责任人：实例的数据安全防护责任人有以下操作的权限：授权、回收权限、编辑数据库账号、开启/关闭公网地址、关闭实例的数据安全防护。单击责任人右侧的编辑图标，将当前实例的责任人权限转移给其他用户。
- 编辑数据库账号：单击数据库账号右侧的编辑图标，修改连接数据库实例的账号。

后续步骤

您需要为用户授权，被授权的用户才可以使用数据安全防护的服务来调用目标实例。用户授权的具体操作，请参见授权通过数据安全防护地址调用数据库实例。

1.2. 授权通过数据安全防护地址调用数据库实例

在数据安全防护开启后，被授权的用户可以在数据安全防护的机制下调用数据库实例。管理员角色、DBA角色、实例的数据安全防护责任人可以为用户授权。本文介绍如何进行用户授权。

前提条件

- 实例已开启数据安全防护。开启方法，请参见开启数据安全防护。

  > **说明** 只有管理员角色、DBA角色、实例owner可以开启实例的数据安全防护。

- 您是以下其中一种角色：管理员角色、DBA角色、当前实例的数据安全防护责任人。

  > **说明** 数据安全防护责任人为开启数据安全防护的用户。您可以在**数据安全防护**页面查看责任人。

- 您还没有权限通过数据安全防护生成的地址去调用目标实例。

为用户授权

1. 在DMS左侧的实例列表中，右键单击目标实例，从弹出的列表中选择**数据安全防护**。

   > **说明** 更多进入方式：
   > - 在**工作台 > 资源列表 > 实例列表**中，选择目标实例，单击**更多 > 数据安全防护**。
   > - 在**全部功能 > 系统管理 > 实例管理 > 实例列表**中，选择目标实例，单击**更多 > 数据安全防护**。

2. 在**数据安全防护**页面，单击**授权**。

   > **说明** 管理员角色、DBA角色、当前实例的数据安全防护责任人有权限进行授权操作。

3. 在**数据安全防护-授权**对话框，选择要授权的目标用户。
4. 单击**确定**，完成授权设置。
   目标用户出现在被授权人列表。被授权人可以使用自己的认证信息调用目标实例。

   > **说明** 管理员、DBA可以看到所有被授权人，普通用户角色只能看到自己的授权信息。

> **说明** 您也可以通过审批工单为申请开通数据安全防护的用户进行授权。审批授权的具体操作，请参见审批工单。

相关操作

为用户授权后，您还可以进行以下相关操作：

- 开启公网地址：当应用程序与实例不在同一VPC内，或需要从本地应用程序调用目标实例时，可单击**开启**，获取公网地址。
- 编辑责任人：实例的数据安全防护责任人有以下操作的权限：授权、回收权限、编辑数据库账号、开启/关闭公网地址、关闭实例的数据安全防护。单击责任人右侧的编辑图标，将当前实例的责任人权限转移给其他用户。
- 编辑数据库账号：单击数据库账号右侧的编辑图标，修改连接数据库实例的账号。
- 查看AccessSecret：AccessSecret用于连接数据安全防护为实例数据库生成的代理地址，默认加密。单击**查看**，查看自己的AccessSecret。
- 更新AccessSecret：单击**更新**，得到新的AccessSecret，更新后应用程序无法继续使用变更前的AccessSecret调用实例。
- 释放自己的权限：无需通过数据安全防护地址去调用实例时，可以单击**释放**，放弃自己的权限。
- 回收权限：当被授权人无需通过数据安全防护地址去调用实例时，单击**回收**，回收被授权人的权限。

> **说明** 如果您是普通用户角色的责任人，则无法更新其他被授权人的AccessSecret，也无法回收其他被授权人的权限。

1.3. 申请通过数据安全防护地址调用数据库实例

如果用户没有权限通过数据安全防护生成的代理地址去调用数据库实例，可以主动申请权限。申请通过后，用户将得到一个认证信息，该认证信息可以用来连接数据库实例的代理地址从而去调用数据库。

前提条件

- 实例已开启数据安全防护。开启方法，请参见开启数据安全防护。
- 用户尚未得到授权。

> **说明** 通过以下方法查看自己的权限：
>
> - 在**我的权限**页面，单击**数据安全防护**，查看具有哪些实例的数据安全防护权限。进入**我的权限**页面，请参见查看我的权限。
> - 在**数据安全防护**页面中查看自己是否属于被授权人。进入该页面的方法，请参见进入数据安全防护页面。

- 用户不是管理员、DBA，也不是当前实例的责任人。

申请开通服务权限

1. 在DMS左侧的实例列表中，右键单击目标实例，从弹出的列表中选择**数据安全防护**。

> 说明 更多进入方式：
> - 在**工作台 > 资源列表 > 实例列表**中，选择目标实例，单击**更多 > 数据安全防护**。
> - 在**全部功能 > 系统管理 > 实例管理 > 实例列表**中，选择目标实例，单击**更多 > 数据安全防护**。

2. 在**数据安全防护**页面，单击**一键申请开通**。

申请后，生成**数据安全防护工单**。

审批通过后，用户可以在数据安全防护页面看到自己的认证信息。

相关操作

用户在申请得到权限后，管理自己的认证信息与权限：

- 查看AccessSecret：AccessSecret默认加密。用户可单击**查看**，看到AccessSecret明文。
- 更新AccessSecret：单击**更新**，得到新的AccessSecret，更新后应用程序无法继续通过变更前的AccessSecret调用目标实例。

- 释放自己的权限：当被授权人无需再调用实例时，被授权人可以单击**释放**，放弃自己的权限。

后续步骤

用户取得权限后，可以通过MySQL协议和HTTPS协议去连接数据安全防护为数据库实例生成的代理地址从而调用数据库实例：

- 通过MySQL协议调用目标实例
- 通过HTTPS协议调用目标实例

1.4. 通过MySQL协议调用目标实例

本文介绍应用程序如何通过MySQL协议调用已开启数据安全防护的目标实例。

前提条件

- 已开启数据安全防护。具体的开启方法，请参见设置数据安全防护中开启数据安全防护的内容。
- 准备好数据安全防护的认证信息和连接地址。可在**数据安全防护**页面查看自己的认证信息和连接地址。

调用示例

您可以通过命令行、数据库管理工具、程序代码来调用已开启数据安全防护的目标实例。

- 使用MySQL命令行调用的示例
  需遵循以下格式：
  ```
  mysql -h<host> -P<port> -u<user_name> -p<password> <database> -e '<sql_statements>'
  ```
  其中：
  - host：目标实例的连接地址。在**数据安全防护**页面中查看内网连接或公网连接的MySQL协议地址，该地址即为目标实例的连接地址。
  - port：目标实例的端口号，例如3306。在**数据安全防护**页面的内网连接或公网连接的MySQL协议地址中可以看到端口号。
  - user_name：经授权后，DMS为您分配的AccessID。在**数据安全防护**页面的被授权人列表可以查看自己的AccessID。
  - password：经授权后，DMS为您分配的AccessSecret。在**数据安全防护**页面的被授权人列表可以查看自己的AccessSecret。
  - database：目标实例中的数据库的名称。
  - sql_statements：您要执行的SQL命令。例如：SHOW DATABASES。

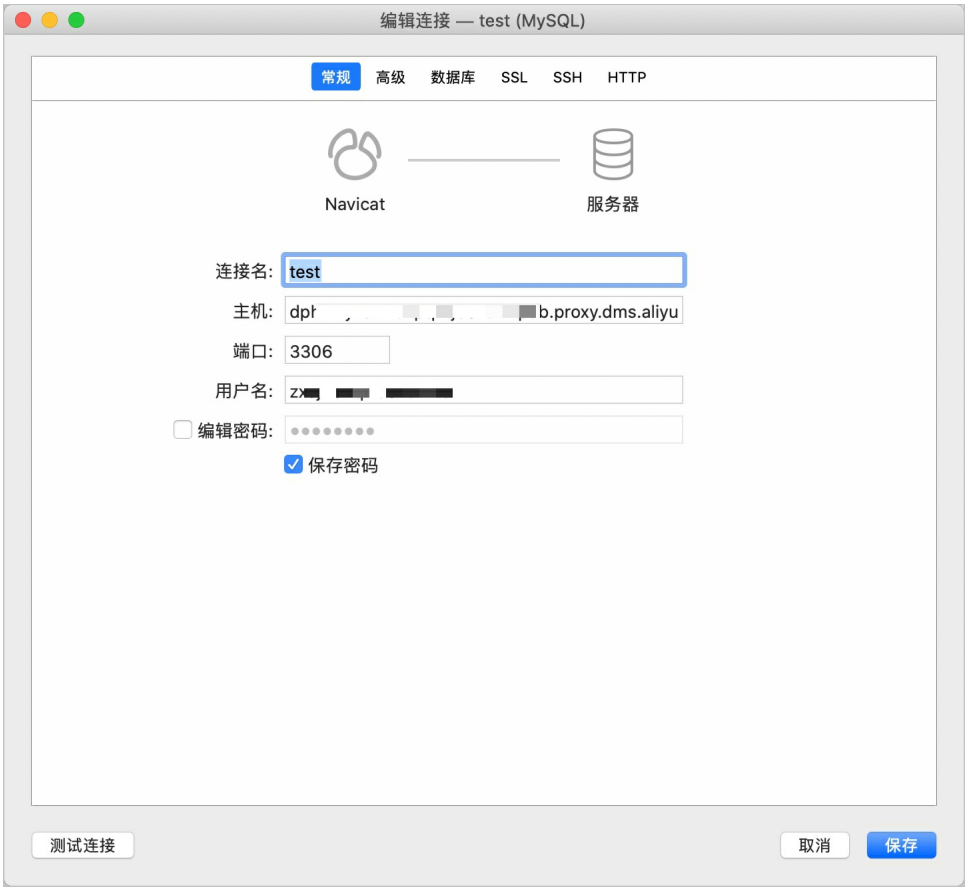
  命令行示例：
  ```
  mysql -hdpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com -P3306 -uAccessID -pAccessSecret Schema -e 'SHOW DATABASES'
  ```
- 程序调用的示例

  Java | Python | Node.js
- 使用数据库管理工具的示例

```
//dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com:3306是目标实例的连接地址与端口号。可在数据安全防护页面的MySQL协议地址获取连接地址与端口号。
//schema是目标实例的数据库名称。
String url = "jdbc:mysql://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com:3306/schema";
Properties properties = new Properties();
//AccessID是您的AccessID。可在数据安全防护页面的被授权人列表中查看。
properties.setProperty("user", "AccessID");
//AccessSecret是您的AccessSecret。可在数据安全防护页面的被授权人列表中查看。
properties.setProperty("password", "AccessSecret");
try (Connection connection = DriverManager.getConnection(url, properties)) {
    try (Statement statement = connection.createStatement()) {
        //使用execute方法执行SQL语句。本示例以SHOW DATABASES为例，您也可以换成其它SQL语句。
        statement.execute("SHOW DATABASES");
        ResultSet resultSet = statement.getResultSet();
        while (resultSet.next()) {
            System.out.println(resultSet.getString(1));
        }
    }
} catch (Exception e) {
    e.printStackTrace();
}
```

以Navicat客户端为例，配置以下信息：

- 主机：目标实例的连接地址。
- 端口号：目标实例的端口号。
- 用户名：AccessID。
- 密码：AccessSecret。



1.5. 通过HTTPS协议调用目标实例

本文介绍如何通过HTTPS协议调用已开启数据安全防护的目标实例。

前提条件

- 已开启数据安全防护。具体的开启方法，请参见设置数据安全防护中开启数据安全防护的内容。
- 准备好数据安全防护的认证信息和连接地址。可在**数据安全防护**页面查看自己的认证信息和连接地址。

请求参数说明

参数名	含义	是否必须	传递方式
accessId	AccessID	是	accessId支持以下传值方式： • Query参数 例如：?accessId=AccessID • Header参数 例如：accessId:AccessID
accessSecret	AccessSecret	是	accessSecret支持以下传值方式： • Query参数 例如：?accessSecret=AccessSecret • Header参数 例如：accessSecret:AccessSecret

参数名	含义	是否必须	传递方式
schema	数据库名称	否	schema支持以下传值方式： • URL路径参数 例如：/server/[您的数据库名] • Body参数 例如：{ "schema": "[您的数据库名]" }
sql	SQL语句	是	sql支持以下传值方式： • URL参数 • Body参数 例如：纯文本格式：[您的SQL语句] JSON格式：{ "sql": "[您的SQL语句]" }

返回值说明

通过HTTPS协议调用，以JSON格式返回数据

JSON对象格式如下：

字段名	类型	描述
columnMetas	Array	字段元信息列表
columnName	String	字段名
columnLabel	String	字段标签，对应SQL语句中as后的别名，没有别名时，则与columnName一致
columnTypeName	String	字段类型，例如VARCHAR，BIGINT等
precision	Integer	精度，部分字段类型包含精度定义，例如VARCHAR(32)的精度为32
scale	Integer	范围，浮点型的字段类型包含范围定义，表示小数位数，例如DECIMAL(10,2)的范围为2
nullable	Boolean	能否为空，true表示值可以为空，false表示值不可为空
autoIncrement	Boolean	是否自增，true表示自增，false表示非自增
tableName	String	字段所在的表名
msg	String	执行出错时，返回错误信息
updateCount	Integer	执行DML时，影响的记录数
requestId	String	请求ID，遇到问题时用于帮助排查
rowCount	Integer	查询操作时，返回的记录数
rows	Array	查询操作时，返回的记录列表，数组中每个元素表示一行数据，与List Map结构相同

字段名	类型	描述
success	Boolean	执行是否成功，true表示成功，false表示失败

返回值示例如下：

- 成功查询到数据


```
{
 "columnMetas": [
  {
   "columnName":"column1",
   "columnLabel":"column1",
   "columnTypeName":"varchar",
   "precision":10,
   "scale":2,
   "nullable":true,
   "autoIncrement":true,
   "tableName":"table1"
  },
  {
   "columnName":"column2",
   "columnLabel":"column2",
   "columnTypeName":"varchar",
   "precision":10,
   "scale":2,
   "nullable":true,
   "autoIncrement":true,
   "tableName":"table1"
  }
 ],
 "updateCount": 0,
 "requestId": "xhqej0xgcytbhc8scjopgqsywcaibi",
 "rowCount": 1,
 "rows": [
  {
   "col1": 1,
   "col2": "xxxx"
  }
 ],
 "success": true
}
```


- 成功更新数据


```
{
 "updateCount": 0,
 "requestId": "xhqej0xgcytbhc8scjopgqsywcaibi",
 "success": true
}
```


- 调用失败

```
{
 "message": 'AccessID is required.',
 "requestId": "xhqej0xgcytbhc8scjopgqsywcaibi",
 "success": false
}
```

调用示例

您可以通过命令行、数据库管理工具、程序代码来调用已开启数据安全防护的目标实例。

假设连接地址为dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com，数据库名称为database，accessId为user，accessSecret为pwd，sql命令为show database。

- 使用CURL命令行调用的示例

```
# GET请求
curl 'https://[您的连接地址]/server/[您的数据库名]?accessId=[您的AccessID]&accessSecret=[您的AccessSecret]&sql=[SQL语句]'
```

```
# GET请求示例
#curl 'https://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com/server/database?accessId=user&accessSecret=pwd&sql=SHOW%20DATABASES'
```

```
# POST请求
curl 'https://[您的连接地址]/server/[您的数据库名]' -H 'accessId:[您的AccessID]' -H 'accessSecret:[您的AccessSecret] -H 'Content-Type:text/plain' -d '[SQL语句]'
```

```
# POST请求示例
curl 'https://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com/server/database' -H 'accessId:user' -H 'accessSecret:pwd -H 'Content-Type:text/plain' -d 'SHOW DATABASES'
```

- Python程序调用的示例
  GET请求

```
import requests
url = "https://[连接地址]/server/[您的数据库名]?accessId=[您的AccessID]&accessSecret=[您的AccessSecret]&sql=[sql语句]"
print requests.get(url).text
```

GET请求示例：

```
import requests
url = "https://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com/server/database?accessId=user&accessSecret=pwd&sql=SHOW DATABASES"
print requests.get(url).text
```

POST请求：

```
import requests
url = "https://[连接地址]/server/[您的数据库名]"
headers = {
  "Content-Type": "text/plain;charset=utf-8",
  "accessId": "[您的AccessID]",
  "accessSecret": "[您的AccessSecret]"
}
print requests.post(url, headers=headers, data='[sql语句]').text
```

POST请求示例：

```
import requests
url = "https://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com/server/database"
headers = {
  "Content-Type": "text/plain;charset=utf-8",
  "accessId": "user",
  "accessSecret": "pwd"
}
print requests.post(url, headers=headers, data='SHOW DATABASES').text
```

- Node.js程序调用的示例
  GET请求：

```
const https = require("https");
https.get("https://[连接地址]/server/[您的数据库名]?accessId=[您的AccessID]&accessSecret=[您的AccessSecret]&sql=SHOW DATABASES", resp => {
  resp.on("data", data => {
    console.log(JSON.parse(data));
  });
});
```

GET请求示例：

```
const https = require("https");
https.get("https://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com/server/database?accessId=user&accessSecret=pwd&sql=SHOW DATABASES", resp => {
  resp.on("data", data => {
    console.log(JSON.parse(data));
  });
});
```

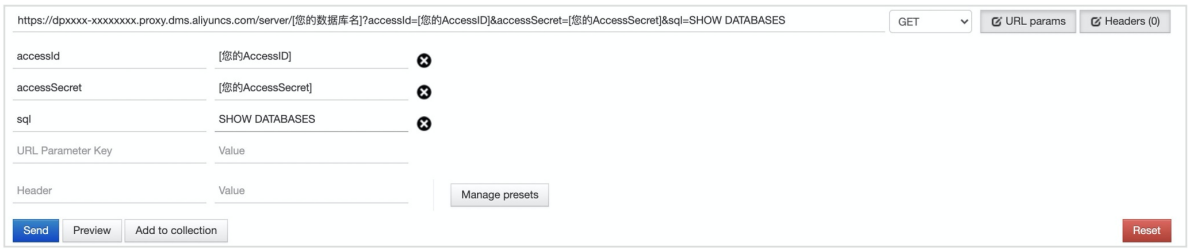
POST请求：

```
const https = require("https");
var req = https.request({
  hostname: '[连接地址]',
  port: 443,
  path: '/server/[您的数据库名]',
  method: 'POST',
  headers: {
    'Content-Type': 'text/plain; charset=UTF-8',
    accessId: '[您的AccessID]',
    accessSecret: '[您的AccessSecret]'
  }
}, resp => {
  resp.on("data", data => {
    console.log(JSON.parse(data));
  });
});
req.write("[sql语句]");
req.end();
```

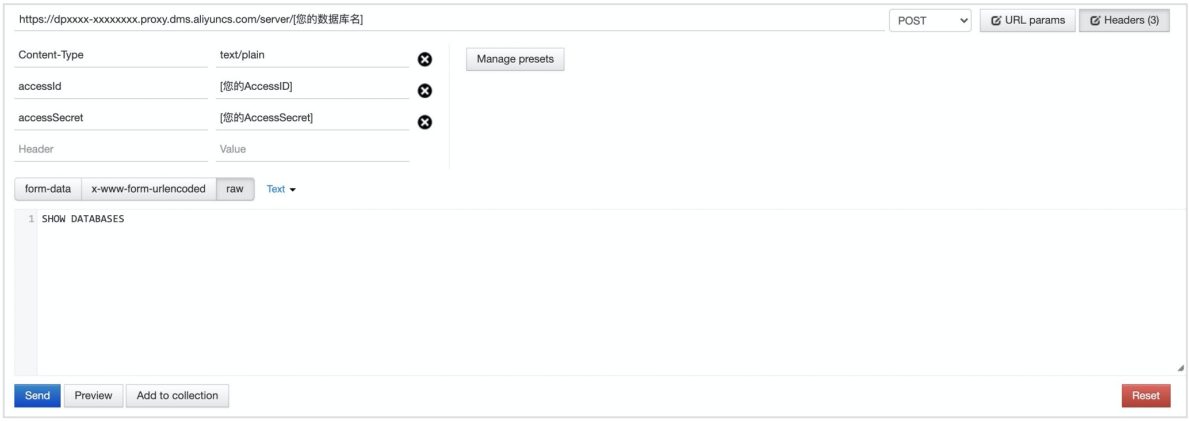
POST请求示例：

```
const https = require("https");
var req = https.request({
  hostname: 'dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com',
  port: 443,
  path: '/server/database',
  method: 'POST',
  headers: {
    'Content-Type': 'text/plain; charset=UTF-8',
    accessId: 'user',
    accessSecret: 'pwd'
  }
}, resp => {
  resp.on("data", data => {
    console.log(JSON.parse(data));
  });
});
req.write("SHOW DATABASES");
req.end();
```

- Postman客户端调用的示例
  GET请求：



POST请求：


https://dpxxxx-xxxxxxxx.proxy.dms.aliyuncs.com/server/[您的数据库名]
POST
URL params
Headers (3)
Content-Type
text/plain
Manage presets
accessId
[您的AccessID]
accessSecret
[您的AccessSecret]
Header
Value
form-data
x-www-form-urlencoded
raw
Text
1 SHOW DATABASES
Send
Preview
Add to collection
Reset

2.操作审计

为了方便快速定位、排查数据库问题以及提供审计用途，数据管理DMS在原来操作日志的基础功能上，重磅推出了操作审计功能，包含SQL窗口产生的SQL语句列表、工单列表、登录列表、操作日志。

功能说明

数据管理DMS的操作审计功能包含了操作日志与操作审计：

功能	说明	内容项
操作日志	用户通过DMS系统发起所有操作的流水账式日志。	包含纯管理、配置类的操作行为，也包含SQL窗口产生的SQL语句列表、工单列表、登录列表。
操作审计	仅包含用户在DMS系统中对数据库进行直接操作的所有行为。 **说明** 为操作审计工作提供统一视图入口，方便您快速定位、排查数据库问题。	SQL窗口产生的SQL语句列表、工单列表、登录列表。 **说明** 仅管理员、DBA、工单的发起者和工单相关人允许查看工单详情。

日志数据将在DMS中永久保留，您可随时访问与查看管控模式为**稳定变更**、**安全协同**的实例日志数据。

说明 您仅能查看管控模式为**自由操作**的实例7天内的日志数据，可通过升级实例的管控模式查看所有日志数据，具体操作，请参见产品升级管理。

操作入口与支持的用户角色

DMS支持多种角色用户、多入口按需进行操作审计：

审计维度	限制	操作审计入口	支持的用户角色
数据库	仅限查看当前数据库的操作审计。	• 在目标数据库的SQL Console页，单击左上角的图标，单击**操作审计**。 • 在DMS对象列表中，展开目标实例，右键单击目标数据库，选择**操作审计**。	管理员、安全管理员、DBA、实例Owner、普通用户。 **说明** 普通用户仅限查看当前数据库中当前用户的操作审计。
实例	仅限查看当前实例的操作审计。	在DMS对象列表中，右键单击目标实例，在弹出的列表中，选择**操作审计**。	管理员、安全管理员、DBA、实例Owner、普通用户。 **说明** 普通用户仅限查看当前实例中当前用户的操作审计。

审计维度	限制	操作审计入口	支持的用户角色
全局	查看全局的操作审计。	在顶部菜单栏中，选择**安全与规范 > 操作审计**。 **说明** 如果您使用的是旧版数据管理DMS，在顶部菜单栏中，选择**全部功能 > 系统管理 > 安全 > 操作审计**。	管理员、安全管理员、DBA。

下载操作审计

本示例将介绍如何下载全局近1个月的SQL窗口产生的SQL语句列表。

1. 登录数据管理DMS 5.0。

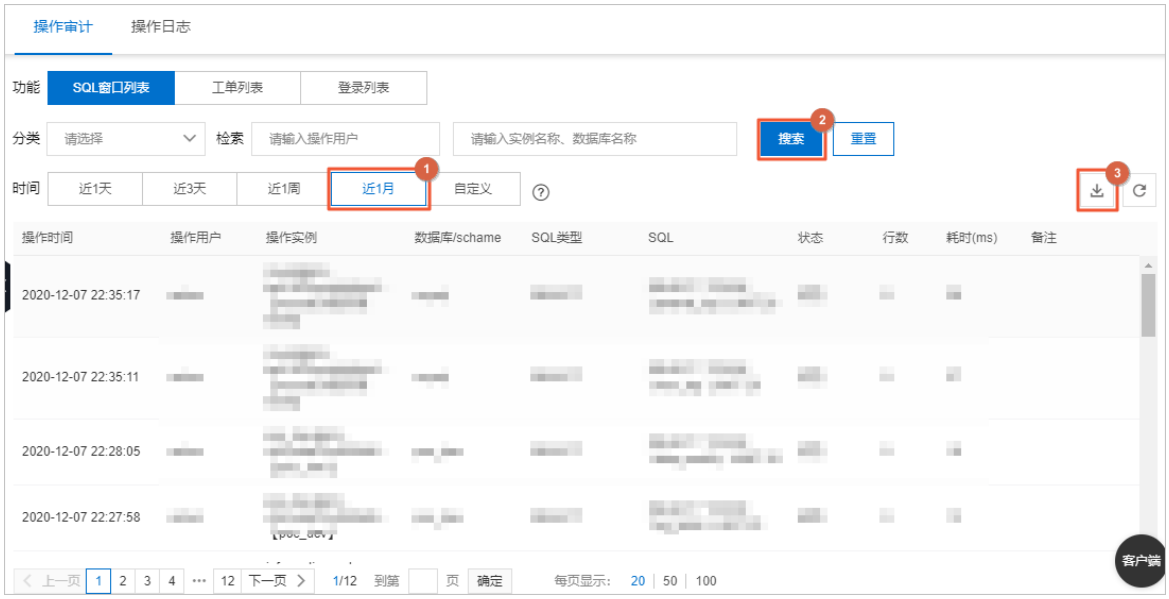
   说明 如果您需要切换到旧版数据管理DMS，单击页面右下角，进入**数据管理DMS**平台。具体操作，请参见数据管理DMS 5.0切换至旧版。

2. 在顶部菜单栏中，选择**安全与规范 > 操作审计**。

   说明 如果您使用的是旧版数据管理DMS，在顶部菜单栏中，选择**全部功能 > 系统管理 > 安全 > 操作审计**。

3. 单击**SQL窗口列表**。
4. 在**时间**区域选择**近1月**，并单击**搜索**。
   系统将返回搜索结果。
5. 单击 图标即可下载。

   系统将以XLSX文件的格式导出当前搜索页的结果。



> 说明 为预览与导出更多结果，您可以将**每页显示**参数设置为**100**。

下载操作日志

当前仅支持通过GetOpLog接口下载操作日志，更多信息，请参见GetOpLog。