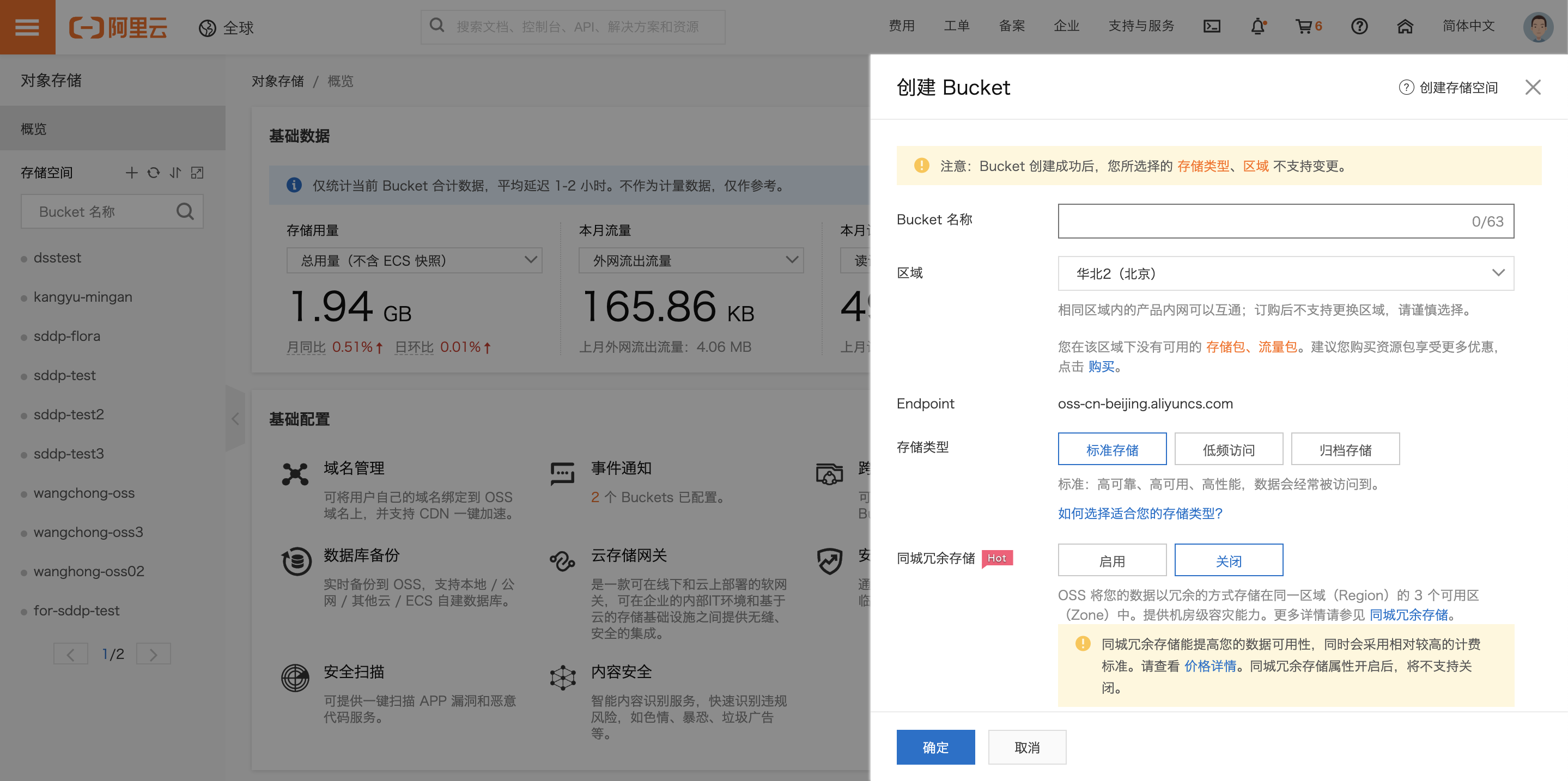
SDDP测试用手册

**测试场景一**：OSS敏感数据识别

**目标**：识别OSS存储桶空间的敏感数据

**步骤**：

1）创建一个测试用OSS存储空间：选择对象存储OSS，创建一个测试用OSS Bucket。注意记录下存储Bucket名称。



2）上传测试用文件夹：选择创建的OSS Bucket，选择文件管理，点击“上传文件”。将附件里的OSS Sample文件夹拖拽到这个存储桶里。



3）打开授权链接：[https://yundunnext.console.aliyun.com/?p=sddp#/config/authorize/list](https://yundunnext.console.aliyun.com/?p=sddp" \l "/config/authorize/list)，将刚刚创建的测试用OSS Bucket选中后，点击右移符号并点击确定完成授权。



4）等待10分钟后，就能在首页看到识别结果。

**测试场景二**：RDS敏感数据识别

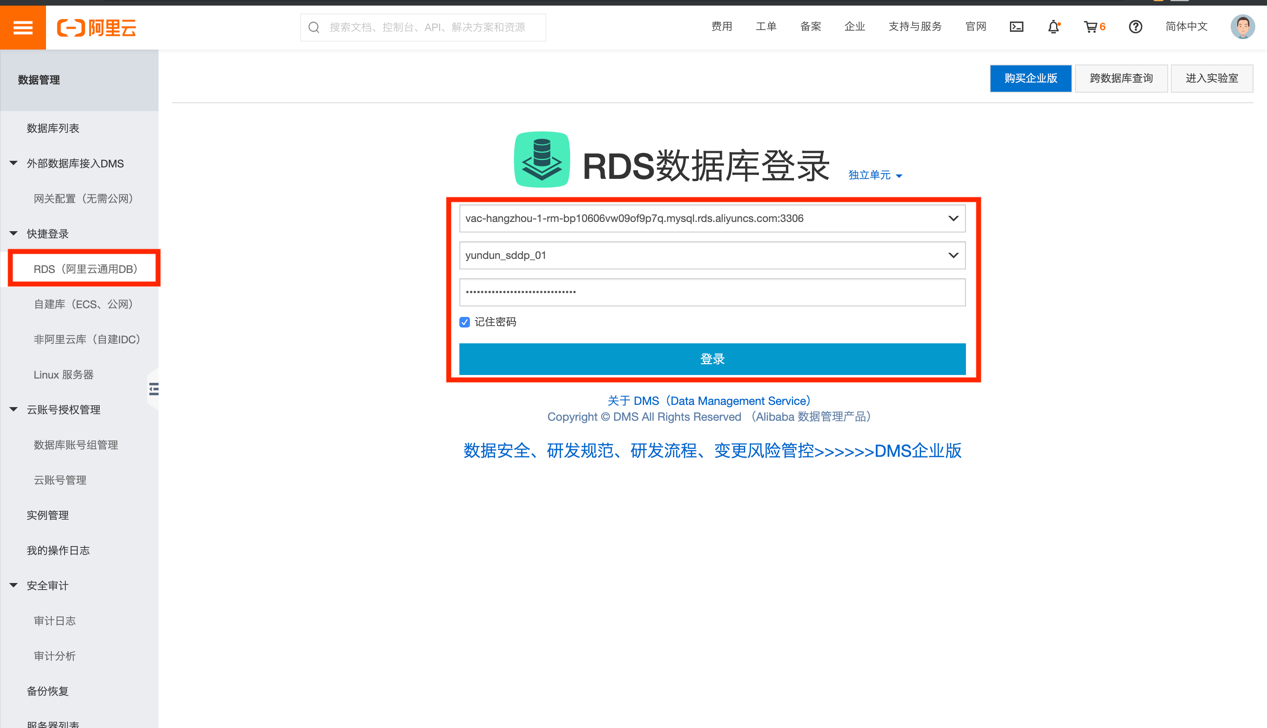
**目标**：识别RDS表里的敏感数据

**步骤**：

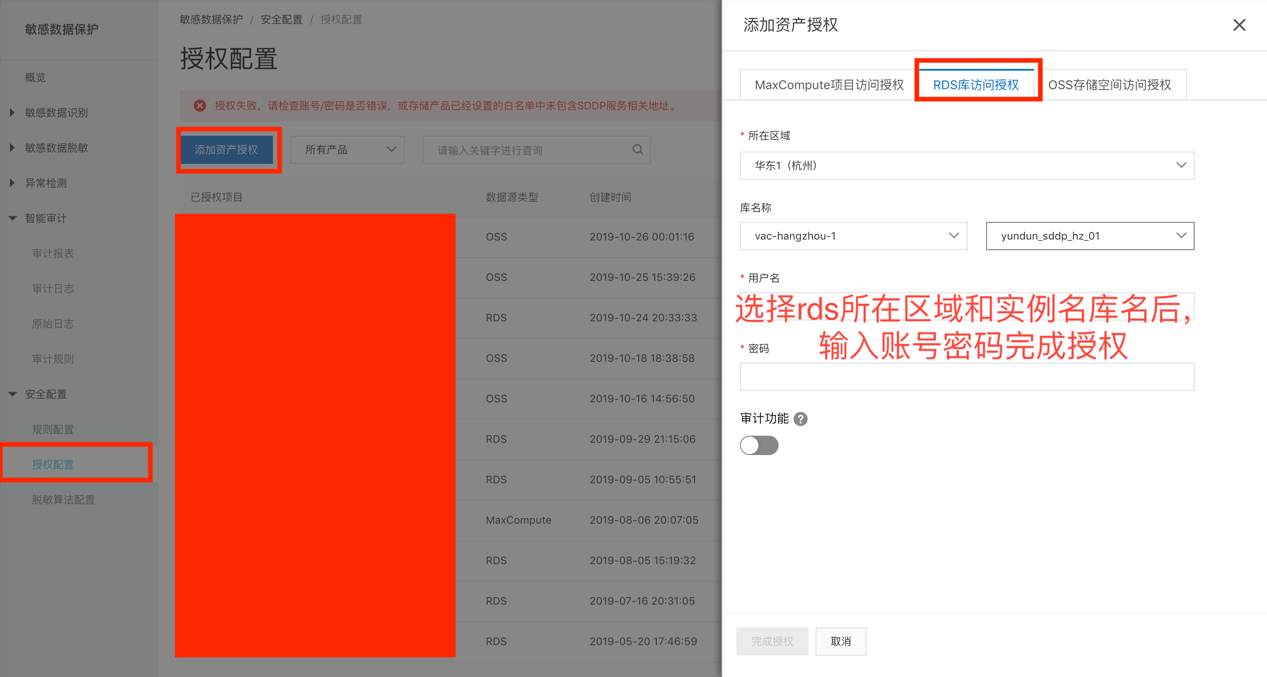
1. 创建一个测试用RDS数据库，如果已有测试用RDS数据库，可直接使用。具体RDS数据库创建方法参考RDS指南：<https://help.aliyun.com/document_detail/26117.html>
2. 登录RDS控制台，选中基本信息，然后点击右侧登录数据库。



1. 输入创建时的账号密码点击登录。



1. 点击SQL操作中的SQL窗口
2. 
3. 拷贝samples目录test.sql文件中的语句，将{{table}}替换成创建的表名后拷贝到SQL窗口执行。
4. 点击连接授权，添加资产授权，RDS库访问授权，选择区域库名后输入账号密码完成授权。



1. 等待10分钟后，就能在首页看到识别结果。

**测试场景三**：MaxCompute敏感数据识别

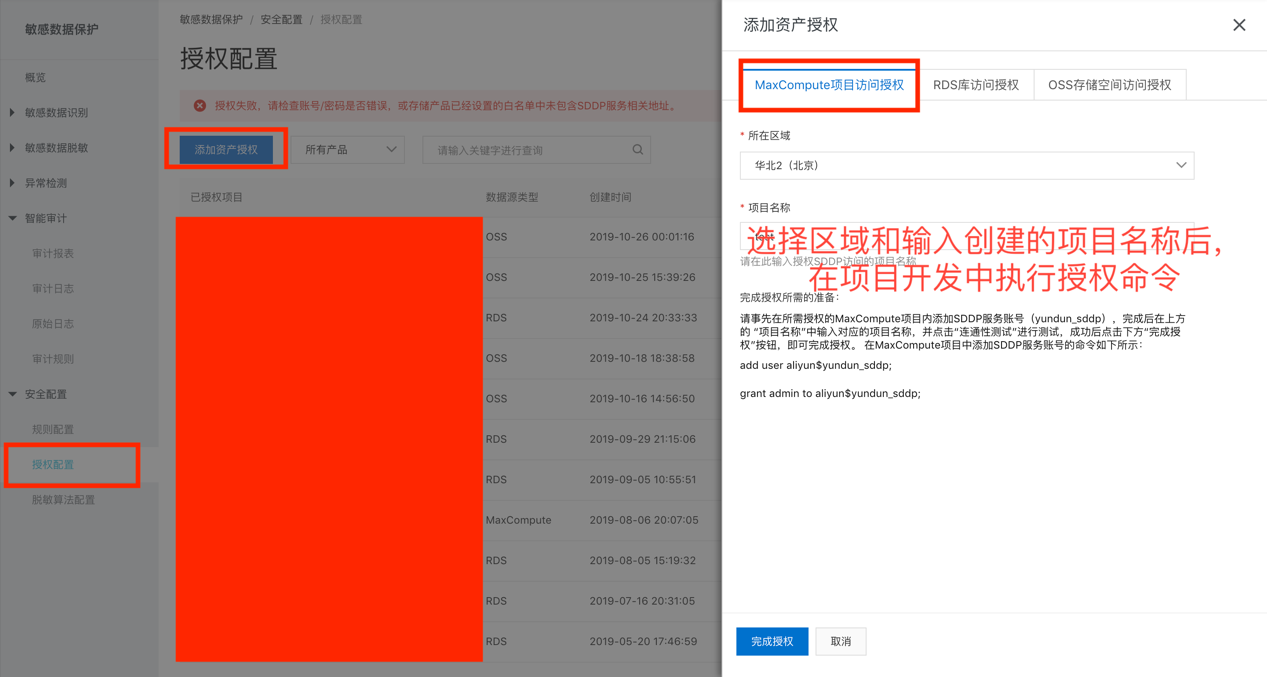
**目标**：识别MaxCompute表里的敏感数据

**步骤**：

创建一个测试用MaxCompute项目表，如果已有MaxCompute项目表，可直接使用。具体MaxCompute项目创建方法参考MaxCompute指南：https://help.aliyun.com/document\_detail/74293.html

1. 在控制台选择新建的MaxCompute项目，点击进入开发。
2. 拷贝samples目录test.odps文件中的语句，将{{table}}替换成创建的表名后拷贝到开发界面执行。
3. 点击连接授权，添加资产授权，MaxCompute项目访问授权，选择区域输入项目名称后，在项目开发中执行授权命令:

*add user aliyun$yundun\_sddp;grant admin to aliyun$yundun\_sddp;*



1. 等待10分钟后，就能在首页看到识别结果。

附录

SDDP-Tester使用说明

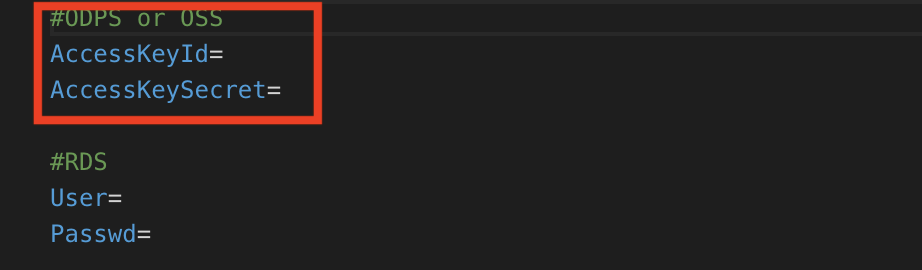
1. OSS篇

Step1.

打开链接

<https://usercenter.console.aliyun.com/#/manage/ak>

页面上如果已有AK则将AccessKeyId、AccessKeySecret拷贝到config.ini进行保存，没有AK则点击创建AK新建一个。

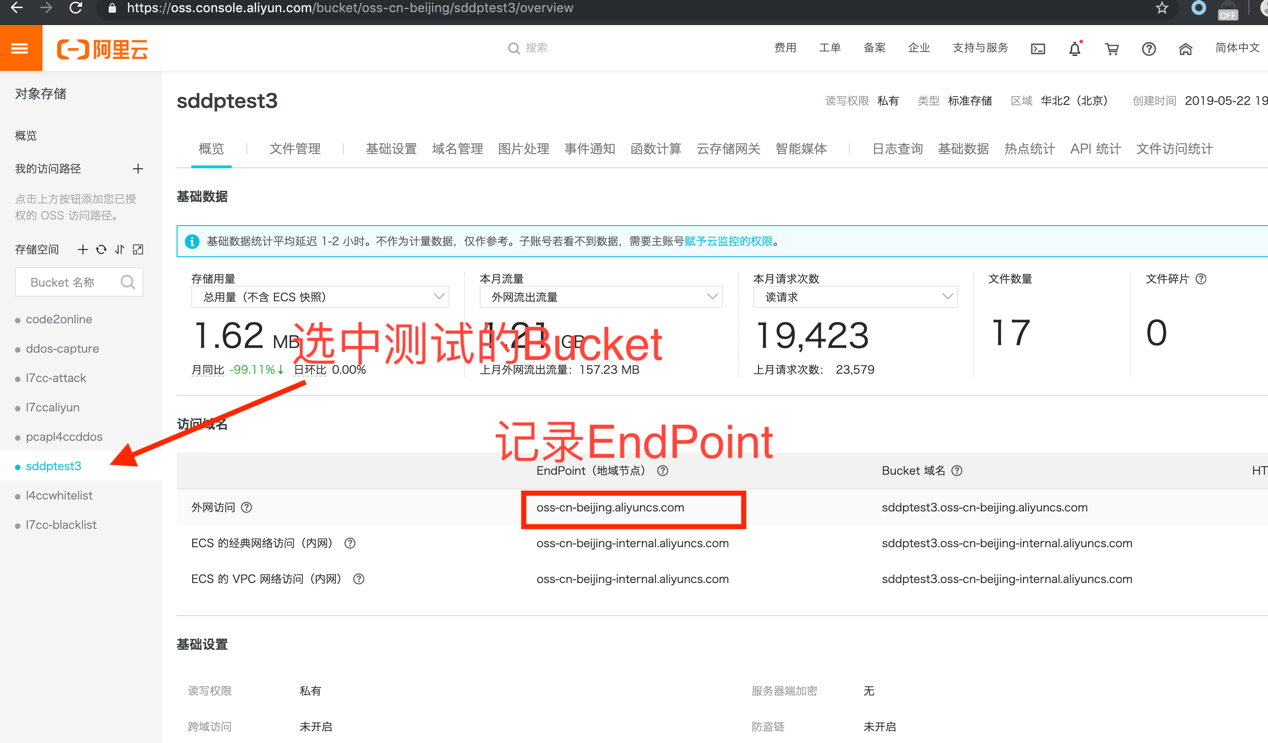


Step2.

打开链接

<https://oss.console.aliyun.com/overview>

选中测试的Bucket，记录下外网访问的EndPoint



Step3.

打开命令行界面cd到项目目录

Step4.

输入*./sddp\_tester scan* *-p oss --ossendpoint <oss的endpoint> --bucketname <测试的bucket>*

即可进行敏感文件自动上传，上传完毕后几分钟内SDDP产品会自动扫描上传文件中的敏感数据，可以点击下面的链接在官网查看

<https://yundunnext.console.aliyun.com/?p=sddp#/asset/oss>

输入*./sddp\_tester abnormal -p oss --ossendpoint <oss的endpoint> --bucketname <测试的bucket> --sensitiveobject <test/1.jpg> --proxyip <http://1.1.1.1:8888>*

会自动模拟一些常见的黑客攻击，后台会自动审计日志并在官网产出攻击告警

<https://yundunnext.console.aliyun.com/?p=sddp#/event/workspace>

1. RDS篇

Step1.

打开链接[https://yundunnext.console.aliyun.com/?p=sddp#/config/authorize/list](https://yundunnext.console.aliyun.com/?p=sddp" \l "/config/authorize/list)



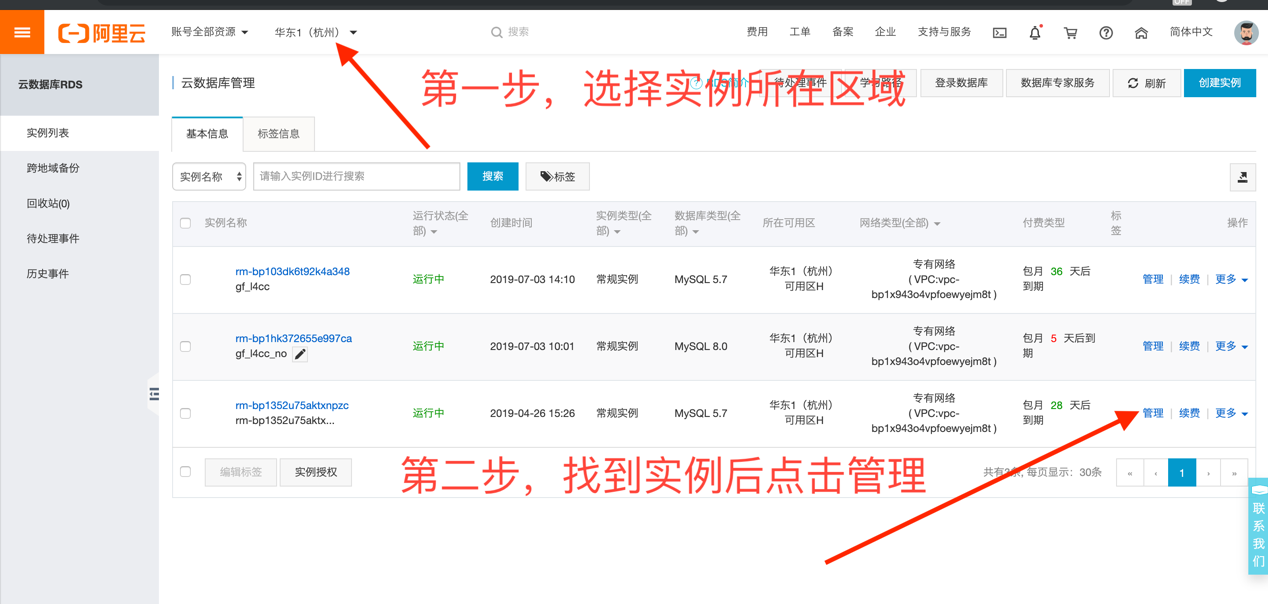
依次根据引导选择进行测试的数据库和对应的用户名密码进行授权。

Step2.

打开链接

<https://rdsnext.console.aliyun.com/#/rdsList>

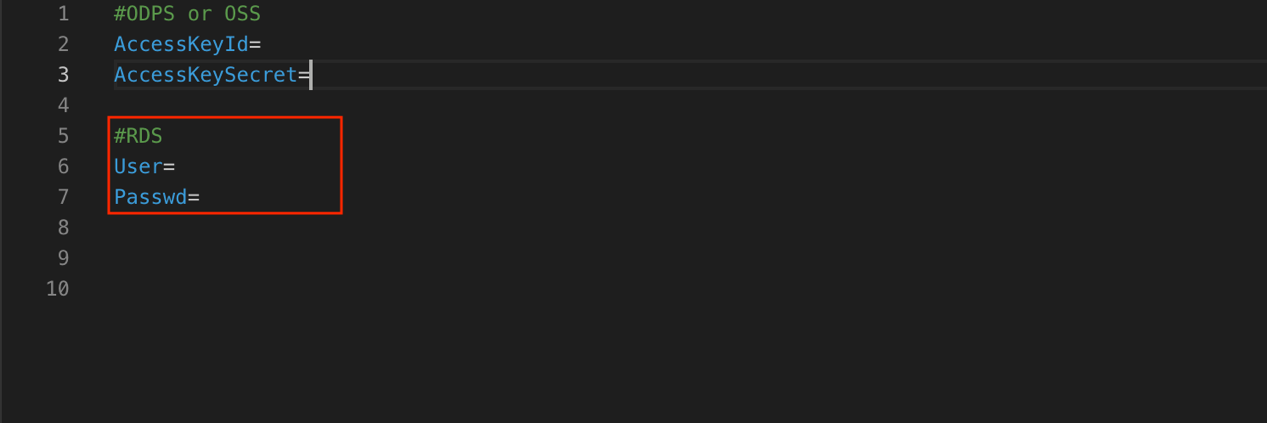
找到刚刚授权测试的RDS实例,点击管理进入管理页面



检查本机IP是否在实例白名单中，不存在则需要添加。



Step3.

打开SDDP-Tester目录中的config.ini输入User和Passwd，与之前授权管理键入的一致。

Step4.

打开命令行界面cd到项目目录

Step5.

输入

*./sddp\_tester scan -p rds -t <rds类型(mysql/mssql)> -d <测试数据库名称> -P <数据库端口> -H <数据库域名>*

可以进行敏感表的创建，创建完毕后几分钟内SDDP产品会自动扫描创建的表中各个字段的类型，可以点击下面的链接在官网查看

<https://yundunnext.console.aliyun.com/?p=sddp#/asset/rds>

输入

*./sddp\_tester abnormal -p rds -t <rds类型(mysql/mssql)> -d <测试数据库名称> -P <数据库端口> -H <数据库域名> --table <敏感表名> --proxy <http://1.1.1.1:8888>*

会自动模拟一些常见的黑客攻击，后台会自动审计日志并在官网产出攻击告警

<https://yundunnext.console.aliyun.com/?p=sddp#/event/workspace>

1. ODPS篇

Step1.

打开链接

<https://yundunnext.console.aliyun.com/?p=sddp#/config/authorize/list>



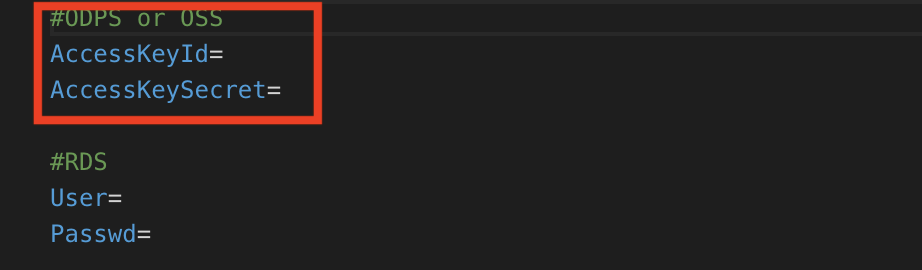
依次根据引导选择进行测试的项目区域和项目名称完成授权。

Step2.

打开链接

<https://usercenter.console.aliyun.com/#/manage/ak>

页面上如果已有AK则将AccessKeyId、AccessKeySecret拷贝到config.ini进行保存，没有AK则点击创建AK新建一个。



Step3.

打开命令行界面cd到项目目录

Step4.

输入

*./sddp\_tester scan -p odps --odpsendpoint http://service.cn.maxcompute.aliyun.com/api --project <测试的project>*

可以进行敏感表的创建，创建完毕后几分钟内SDDP产品会自动扫描创建的表中各个字段的类型，可以点击下面的链接在官网查看

<https://yundunnext.console.aliyun.com/?p=sddp#/asset/maxcompute>

输入

*./sddp\_tester abnormal -p odps --odpsendpoint http://service.cn.maxcompute.aliyun.com/api --project <测试的project> --table <敏感表名> --proxy <http://1.1.1.1:8888>*

会自动模拟一些常见的黑客攻击，后台会自动审计日志并在官网产出攻击告警

<https://yundunnext.console.aliyun.com/?p=sddp#/event/workspace>

1. 清理篇

Step1.

打开命令行界面cd到项目目录

Step2.

输入

*./sddp\_tester clean*

将会删除RDS新建的表和OSS中上传的文件。