目录

创建应用并获取授权

操作场景

- 使用APP认证的API，需要在API网关中创建一个应用，以生成应用ID和密钥对（AppKey、AppSecret）。将创建的应用绑定API后，才可以使用APP认证调用API。在API调用过程中，把密钥对替换SDK中的密钥对，API网关服务根据密钥对进行身份核对，完成鉴权。
- 使用无认证/IAM认证的API，无需创建应用。

创建应用

1. 单击“调用API > 应用管理”，进入到应用管理信息页面。

2. 单击“新建应用”，弹出“创建应用”对话框。填写应用名称和描述信息。

3. 单击“确定”，创建应用。创建应用成功后，在“应用管理”页面的列表中显示新创建的应用和应用ID。

4. 单击应用名称，进入应用详情页面，查看AppKey和AppSecret。

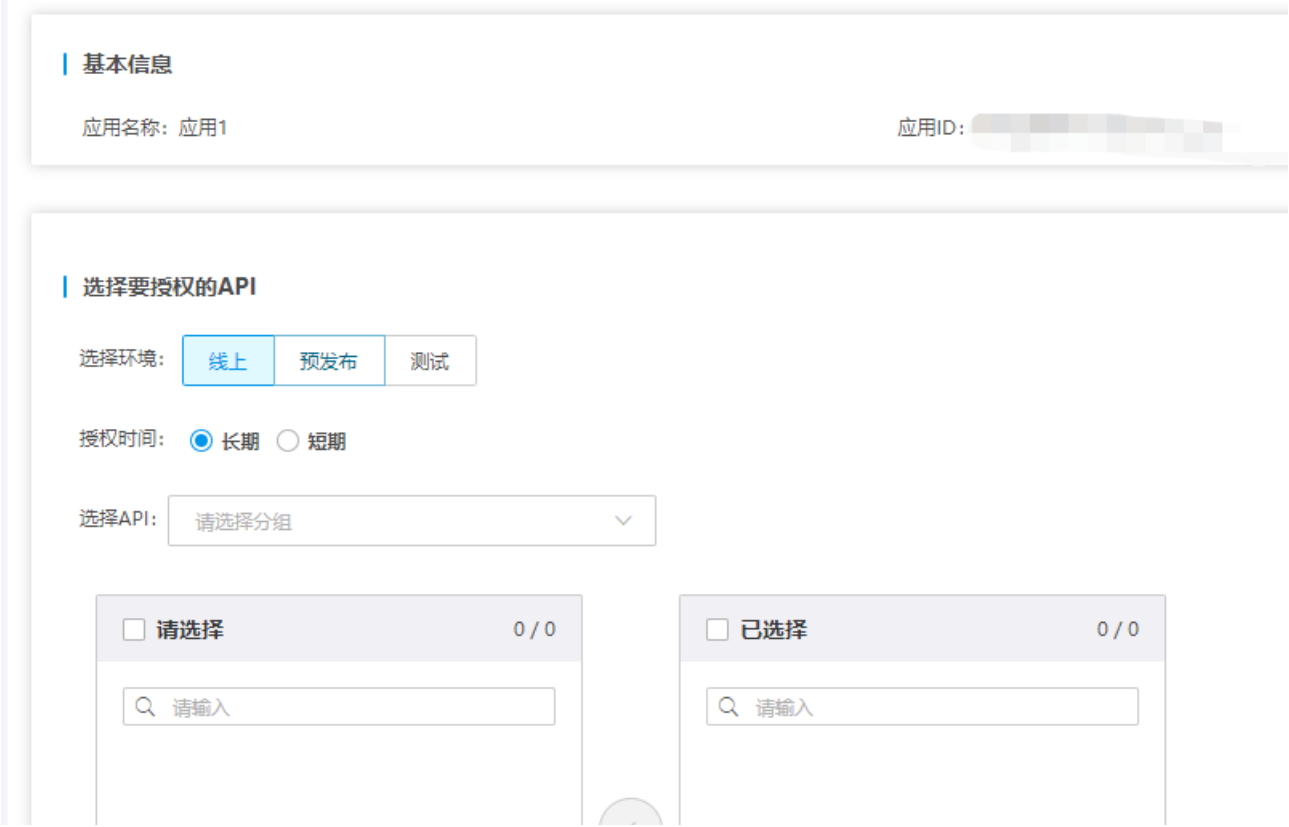
绑定API

1. 单击“调用API > 应用管理”，进入到应用管理信息页面。

2. 通过以下任意一种方法，进入“绑定API”页面。

- 在待绑定API的应用所在行，单击“绑定API”，进入“绑定API”界面。单击“绑定API”。
- 单击待绑定API的应用名称，进入应用详情页面。单击“绑定API”。

3. 选择授权环境和授权时间，勾选API，单击“绑定”，完成API绑定策略。



4.绑定成功后，可以在应用详情页面查看已绑定的API。

IAM认证调用API

域名

使用系统分配的域名调用api，域名形如：**.kscloudapi.com

公共Header参数

名称	描述	是否参与计算签名
x-kscapigw-apigwak	ak 用户在iam控制台建立的AccessKey 例如AKLTgUnjis*****	是
x-kscapigw-nonce	请求调用者生成的uuid，为了避免重放	是
x-kscapigw-timestamp	时间，UTC格式，例如：2020-03-13T17:18:36Z	是
x-kscapigw-signatureversion	签名版本号，固定值：1.0	是
x-kscapigw-signaturemethod	签名算法，固定值：HMAC-SHA256	是
x-kscapigw-signed-headers	参与计算签名的header，多个header使用英文逗号分隔	否
x-kscapigw-signature	签名	否

签名算法

1）根据请求参数(公共header参数和api参数，不包含公共header参数 x-kscapigw-signature)构造规范化请求字符串：CanonicalizedQueryString api参数包含：所有query,path,body,header(x-kscapigw-signed-headers标识参与计算签名的header)参数

第一步：请求参数排序。排序规则以参数名按照字典排序

第二步：请求参数编码。使用UTF-8字符集对每个请求参数的名称和参数取值进行URLEncode，一般在URLEncode后需对三种字符替换：加号（+）替换成 %20、星号（*）替换成 %2A、 %7E 替换回波浪号（~）

第三步：每对URLEncode后的参数名称和参数值，用=进行连接。每对之间使用&进行连接。得到规范化请求字符串CanonicalizedQueryString。

2）计算签名。 sign = hash_hmac('sha256', CanonicalizedQueryString, sk)

sign值为签名算法返回的16进制格式小写字符串

签名样例：
88b203541ce8c757d7d554af2a25de036d3d9a636d91fb44d01bf82dc67a6941

计算签名时使用的sk为AccessKeyID对应的密钥，使用的哈希算法是：HMAC-SHA256。

传递签名

将计算的签名结果放到请求的header中，Key为：X-KSCAPIGW-SIGNATURE。

APP认证调用API

域名

使用系统分配的域名调用api，域名形如：**.kscloudapi.com

- 如果从市场购买的api,请从api文档获取域名信息
- 如果开放者授权调用api,请联系api开放者获取域名信息

公共Header参数

名称	描述	是否参与计算签名
x-kscapigw-apigwak	ak 用户在控制台建立的应用Appkey	是
x-kscapigw-nonce	请求调用者生成的uuid，为了避免重放	是
x-kscapigw-timestamp	时间，UTC格式，例如：2020-03-13T17:18:36Z	是
x-kscapigw-signatureversion	签名版本号，固定值：1.0	是
x-kscapigw-signaturemethod	签名算法，固定值：HMAC-SHA256	是
x-kscapigw-signed-headers	参与计算签名的header，多个header使用英文逗号分隔	否
x-kscapigw-signature	签名	否

签名算法

1）根据请求参数(公共header参数和api参数，不包含公共header参数 x-kscapigw-signature)构造规范化请求字符串：CanonicalizedQueryString api参数包含：所有query,path,body,header(x-kscapigw-signed-headers 标识参与计算签名的header)参数

第一步：请求参数排序。排序规则以参数名按照字典排序

第二步：请求参数编码。使用UTF-8字符集对每个请求参数的名称和参数取值进行URLEncode，一般在URLEncode后需对三种字符替换：加号（+）替换成 %20、星号（*）替换成 %2A、 %7E 替换回波浪号（~）

第三步：每对URLEncode后的参数名称和参数值，用=进行连接。每对之间使用&进行连接。得到规范化请求字符串CanonicalizedQueryString。

2）计算签名。 sign = hash_hmac('sha256', CanonicalizedQueryString, sk)

sign值为签名算法返回的16进制格式小写字符串

签名样例：
88b203541ce8c757d7d554af2a25de036d3d9a636d91fb44d01bf82dc67a6941

计算签名时使用的sk为Appkey对应的秘钥(Secret)，使用的哈希算法是：HMAC-SHA256。

传递签名

将计算的签名结果放到请求的header中，Key为：X-KSCAPIGW-SIGNATURE。