操作审计

PHP SDK 文档

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

PHP SDK 文档
- 创建操作审计
- 开启日志采集
- 更新操作审计
- 关闭日志采集
- 拉取 COS 列表
- 拉取操作审计列表
- 获取操作审计信息
- 删除操作审计
- 检索日志

版权所有：腾讯云计算（北京）有限责任公司

PHP SDK 文档
创建操作审计

最近更新时间：2024-02-28 17:32:29

SDK 描述

CreateAudit 用于创建操作审计（CloudAudit），每个用户只能创建 50 个 CloudAudit。

请求参数

参数名称	必选	类型	描述
IsMultiRegionAudit	否	Number	是否开启多地域采集。0：不开启，1：开启
KmsKeyId	否	String	Kms 的 scretId，用于数据加密
Name	是	String	CloudAudit 名称，3-128 字节，只能包含 ASCII 编码字母 `a-z`，`A-Z`，数字 `0-9`，下划线 `_`
CosBucketName	是	String	要投递的 COS Bucket 的名称，命名规范参照 COS 的命名要求
CosKeyPrefix	否	String	COS Bucket 前缀，命名规范参照 COS
CmqTopicName	否	String	CMQ 主题名称，如果开启消息队列请填写，命名规范参照 CMQ 要求

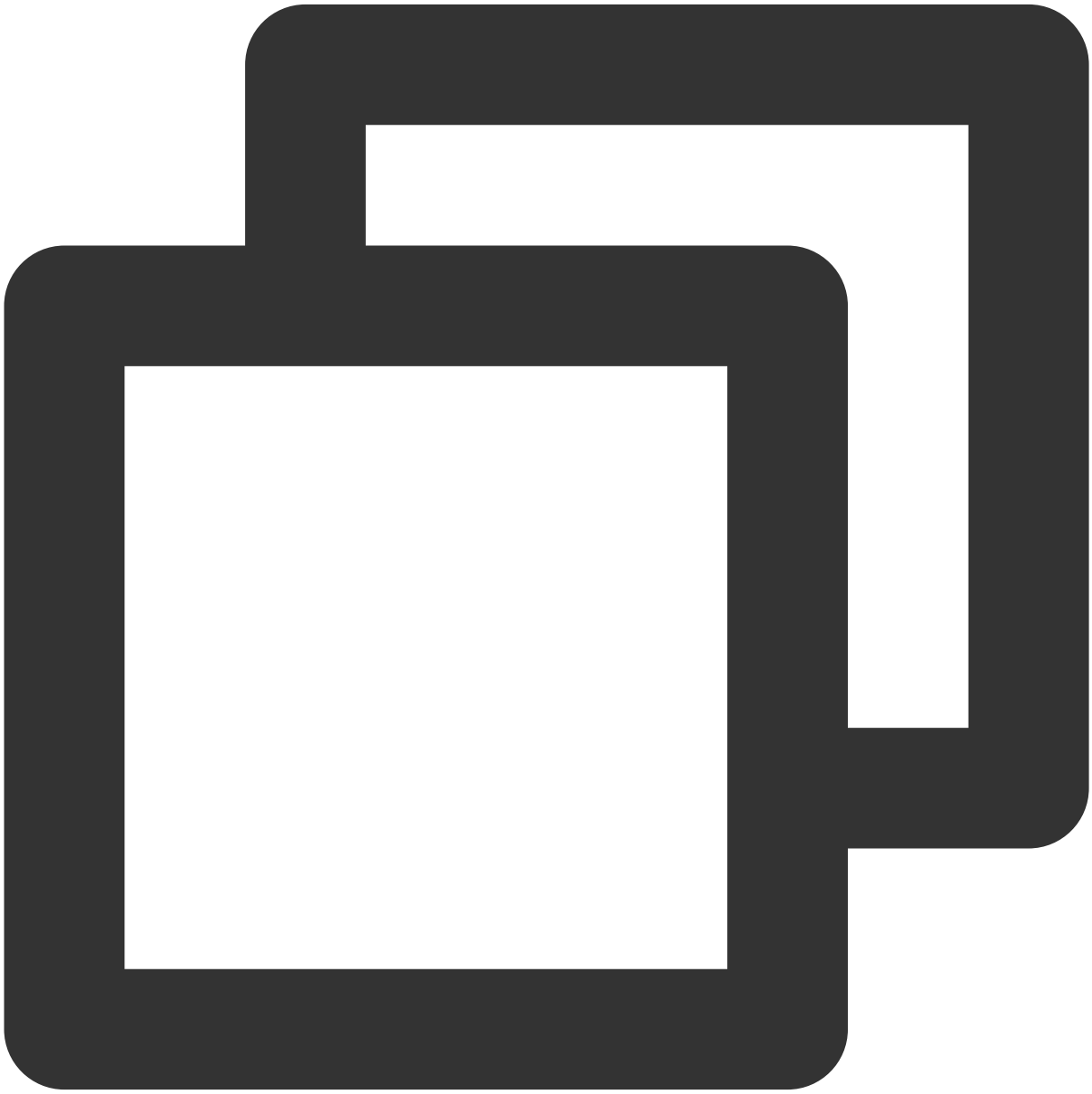
响应参数

参数名称	类型	描述
IsMultiRegionAudit	Number	是否开启多地域采集。1 代表是，0 代表否
KmsKeyId	String	Kms 密钥 ID
Name	String	CloudAudit 名称
CosBucketName	String	COS Bucket 名称

CosKeyPrefix	String	COS Bucket 前缀
CmqTopicName	String	CMQ 主题名称

实际案例

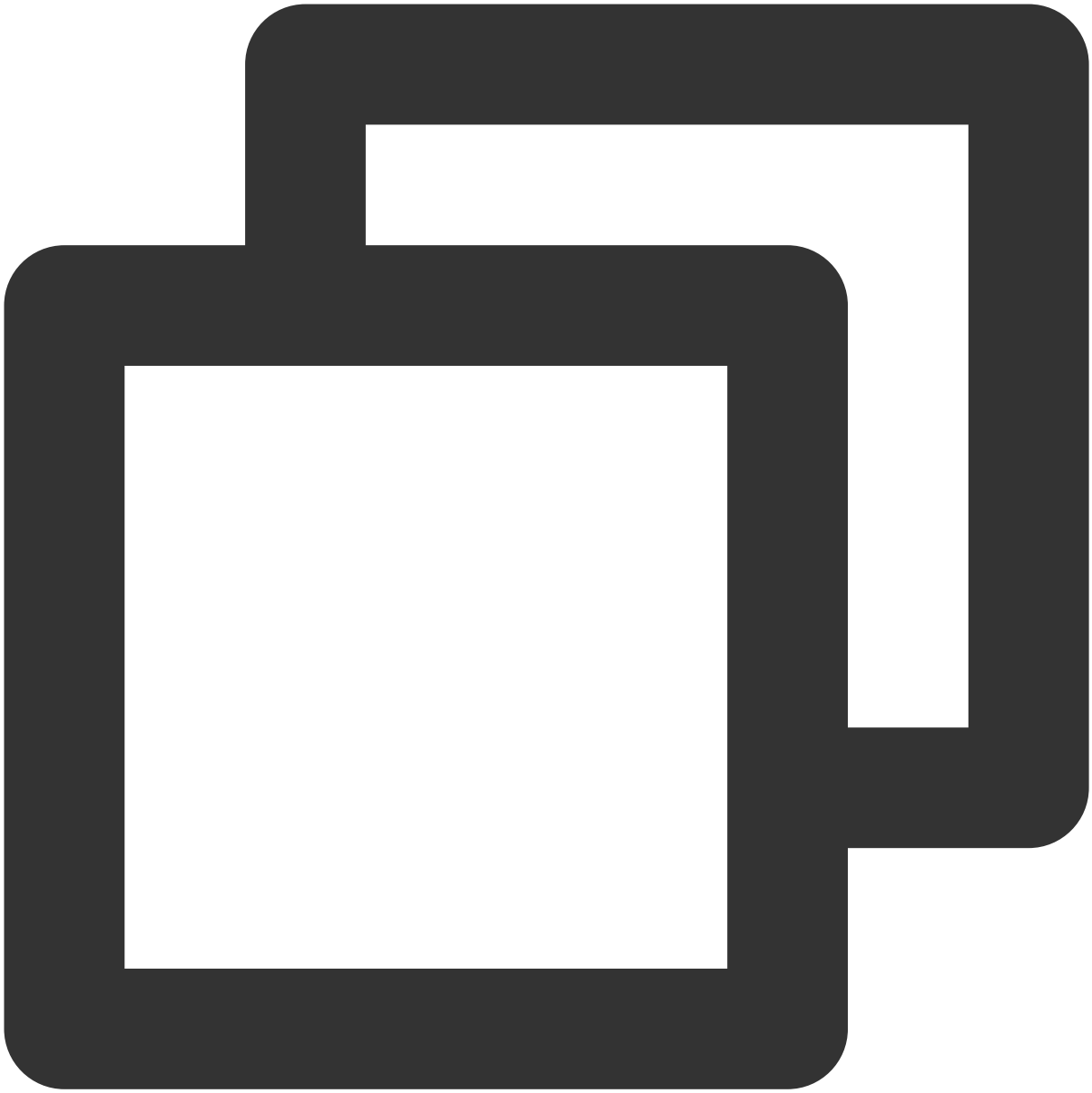
请求示例



```
$config = array('SecretId'       => '你的secretId',
```

```
                'SecretKey'      => '你的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array('IsMultiRegionAudit ' => 1, 'Name' => 'ayisunxxx','CosBucketName'=
$a = $ca->CreateAudit($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
{
    "IsMultiRegionAudit": "1",
    "KmsKeyId": "",
    "Name": "ayisunxxx",
    "CosBucketName": "sundehuixxx",
    "CosKeyPrefix": "91000000009",
    "CmqTopicName": ""
}
```

开启日志采集

最近更新时间：2024-02-28 17:27:24

SDK 描述

StartLogging 用于开启日志采集。

请求参数

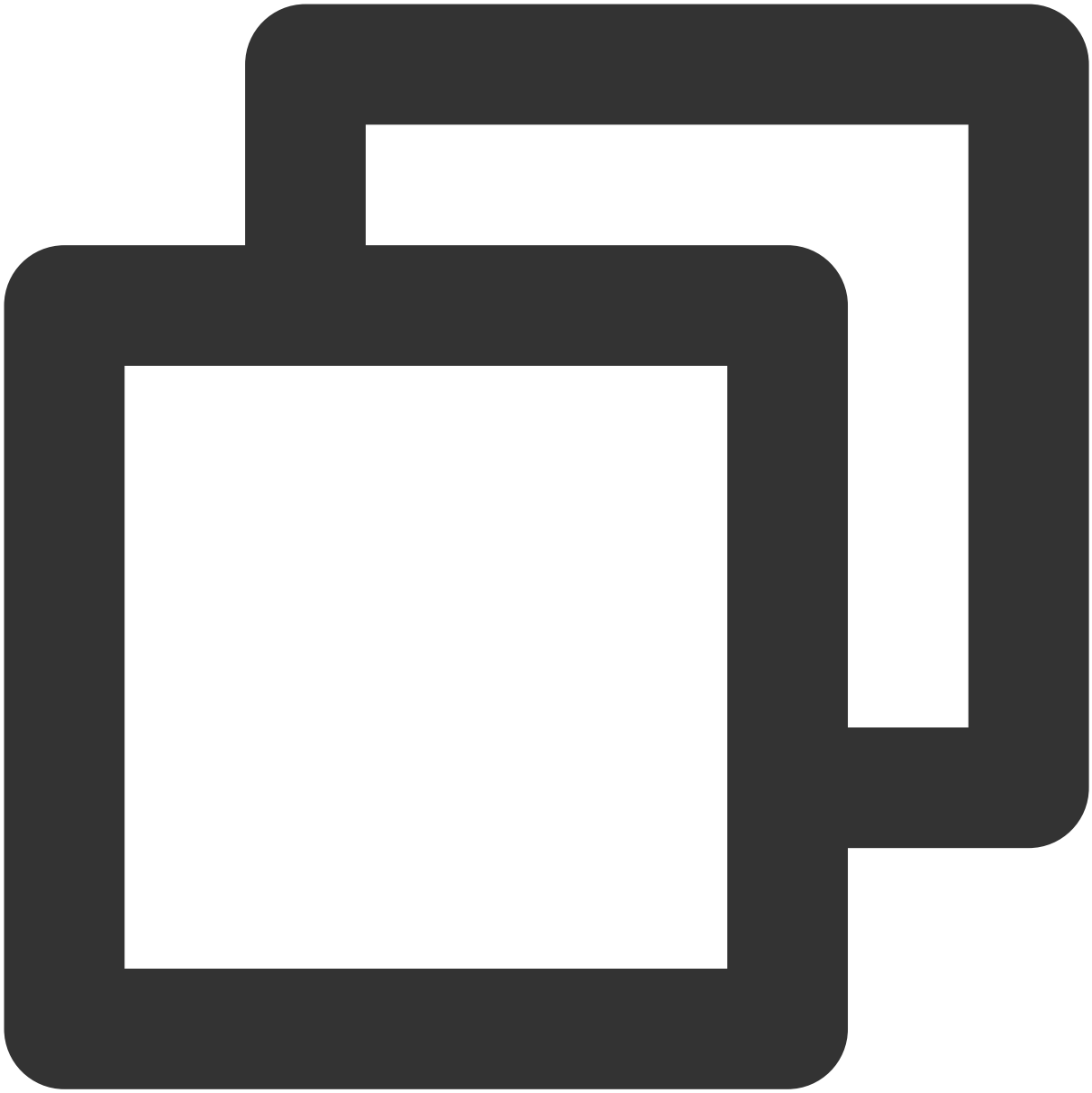
参数名称	必选	类型	描述
Name	是	String	CloudAudit 名称。

响应参数

响应参数为空。

实际案例

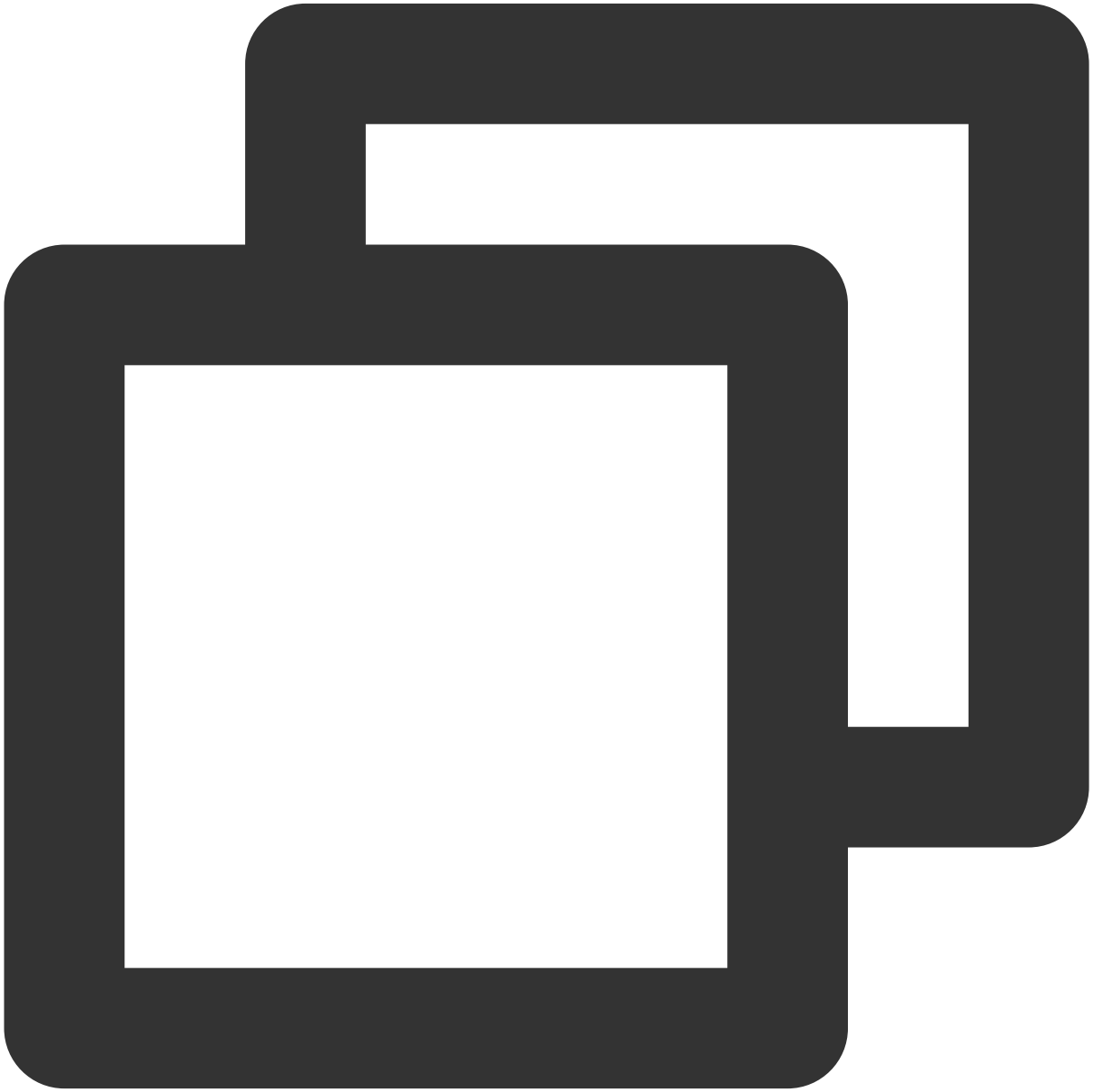
请求示例



```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array('Name'=>'ayisunxxx');
$a = $ca->StartLogging($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
```

```
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
[]
```

版权所有：腾讯云计算（北京）有限责任公司

更新操作审计

最近更新时间：2024-02-28 17:32:50

SDK 描述

UpdateAudit 用于更新操作审计（CloudAudit），其中可用于更新指定日志文件中的一些设置，例如路径，COS Bucket 等设置，请注意 CloudAudit 的名称是不能修改的。对路径的更改，不需要停止 CloudAudit 服务。对 COS Bucket 的更改，如果该 COS Bucket 之前是 CloudAudit 日志文件的目标，则可以更改成功。否则需要手动授权 COS 存储桶，使得 CloudAudit 具有写权限才行。

请求参数

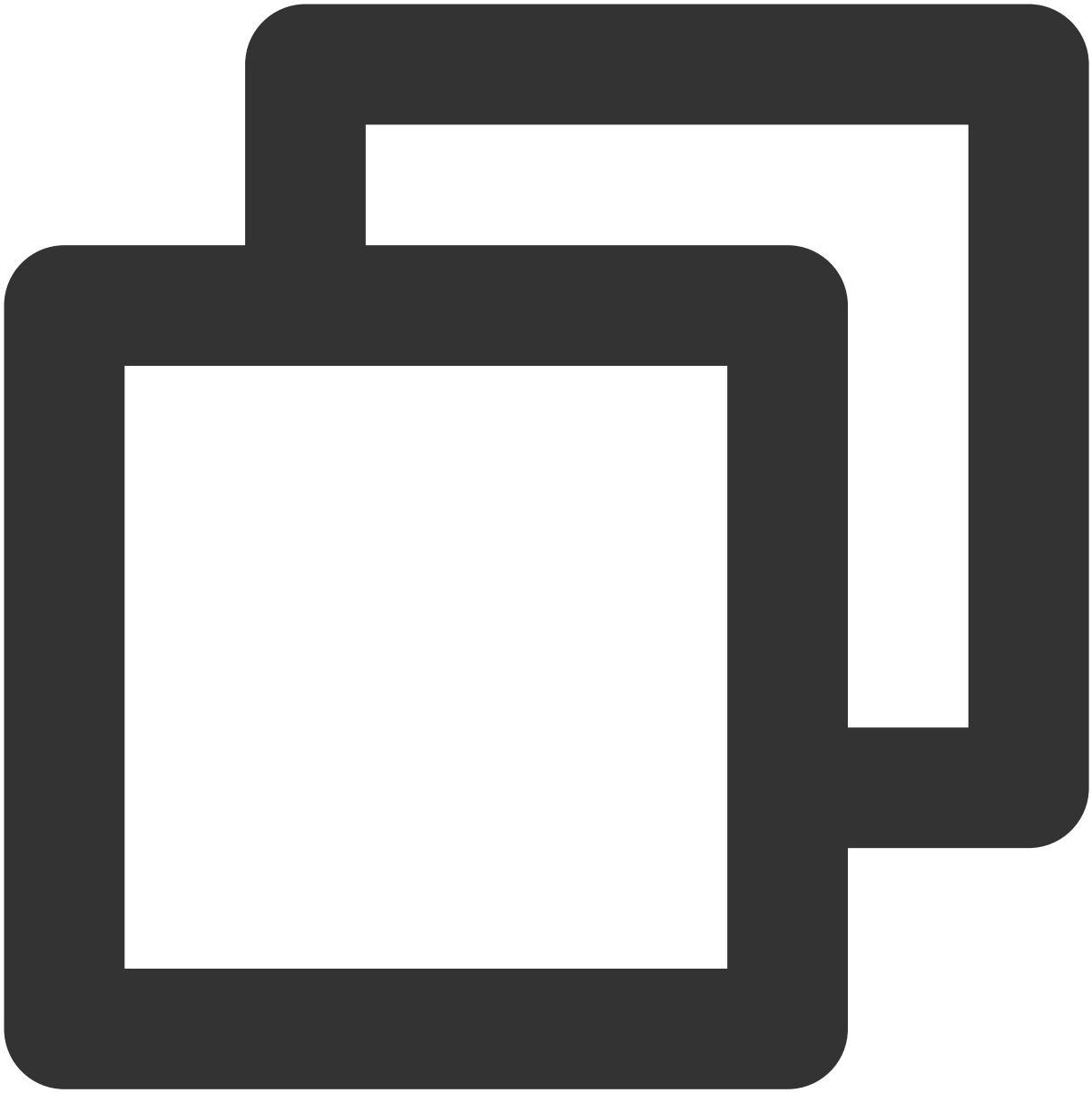
参数名称	必选	类型	描述
IsMultiRegionAudit	否	Number	是否开启多地域采集。0：不开启，1：开启。
KmsKeyId	否	String	Kms 的 scretId，用于数据加密。
Name	是	String	CloudAudit 的名称，3-128 字节，只能包含 ASCII 编码字母 `a-z，A-Z` ，数字 `0-9` ，下划线 `_` 。
CosBucketName	是	String	要投递的 COS Bucket 的名称，命名规范参照 COS 的命名要求。
CosKeyPrefix	否	String	COS Bucket前缀，命名规范参照 COS。
CmqTopicName	否	String	CMQ 主题名称，如果开启消息队列请填写，命名规范参照 CMQ 要求。

响应参数

响应参数为空。

实际案例

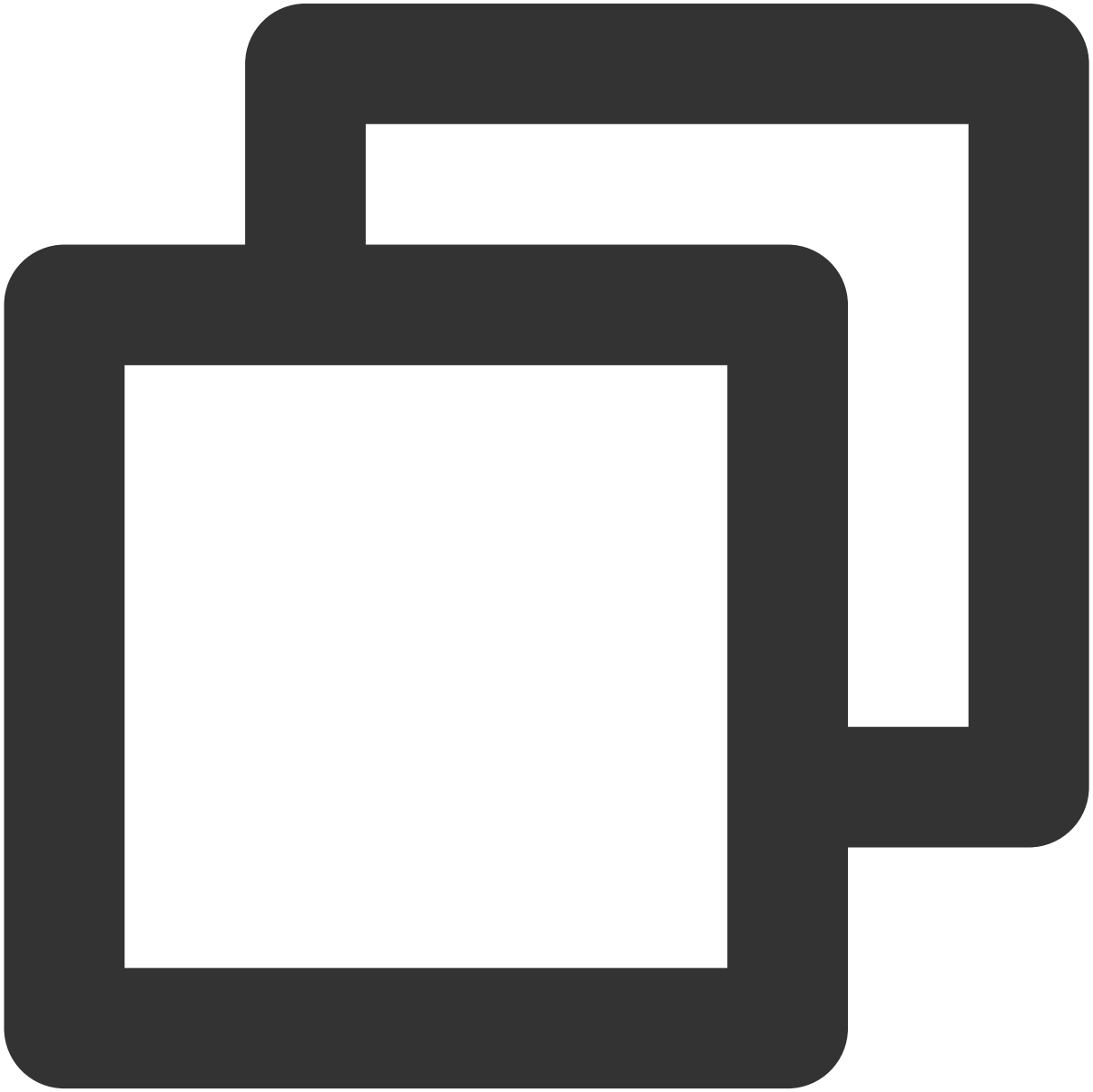
请求示例



```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array('Name'=>'ayisunxxx','CosBucketName'=>'sundehuixxx','CosKeyPrefix'=
$a = $ca->UpdateAudit($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
```

```
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
[]
```

版权所有：腾讯云计算（北京）有限责任公司

关闭日志采集

最近更新时间：2024-02-28 17:27:24

SDK 描述

StopLogging 用于关闭日志采集。

请求参数

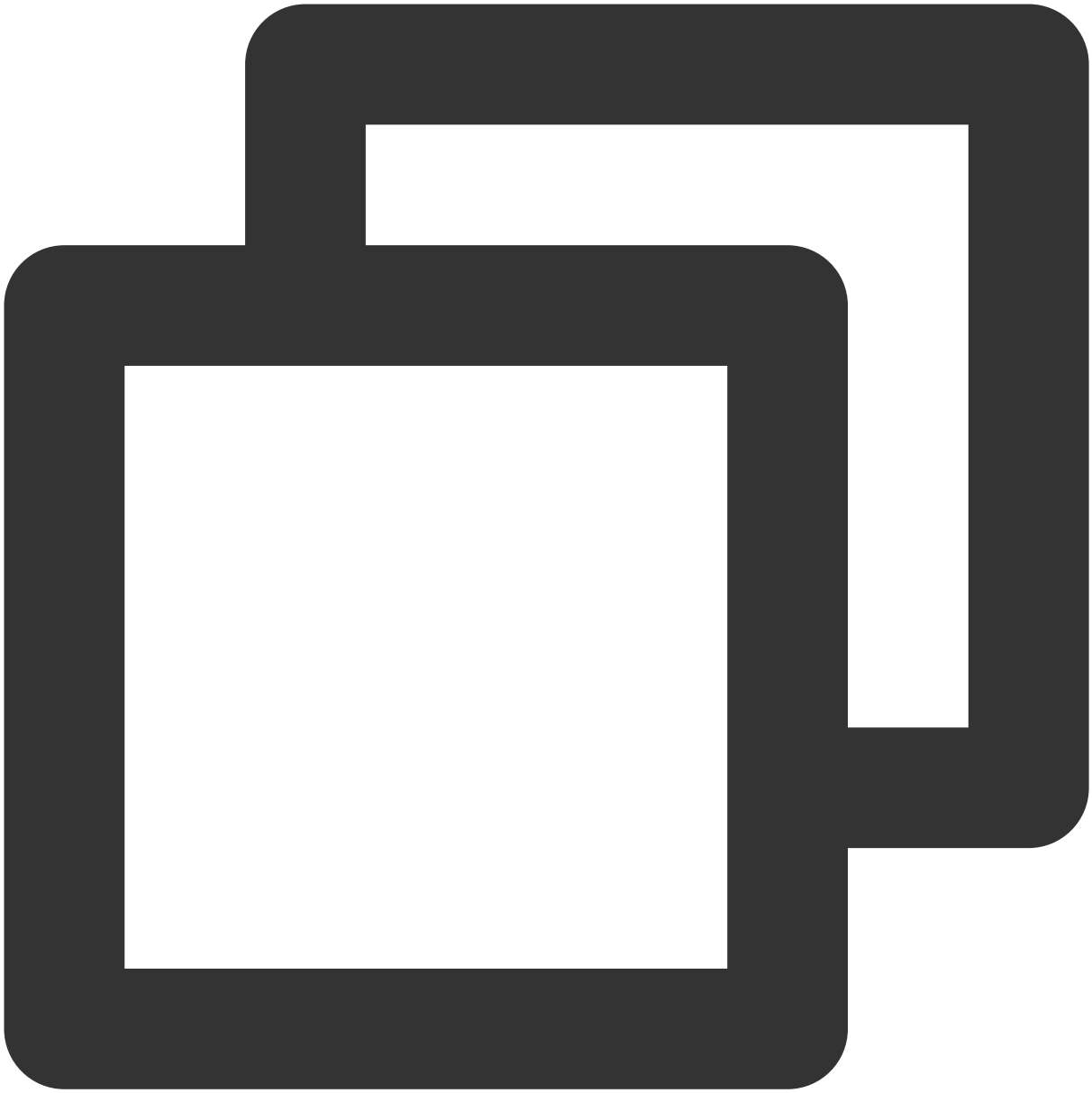
参数名称	必选	类型	描述
Name	是	String	CloudAudit 名称。

响应参数

响应参数为空。

实际案例

请求示例

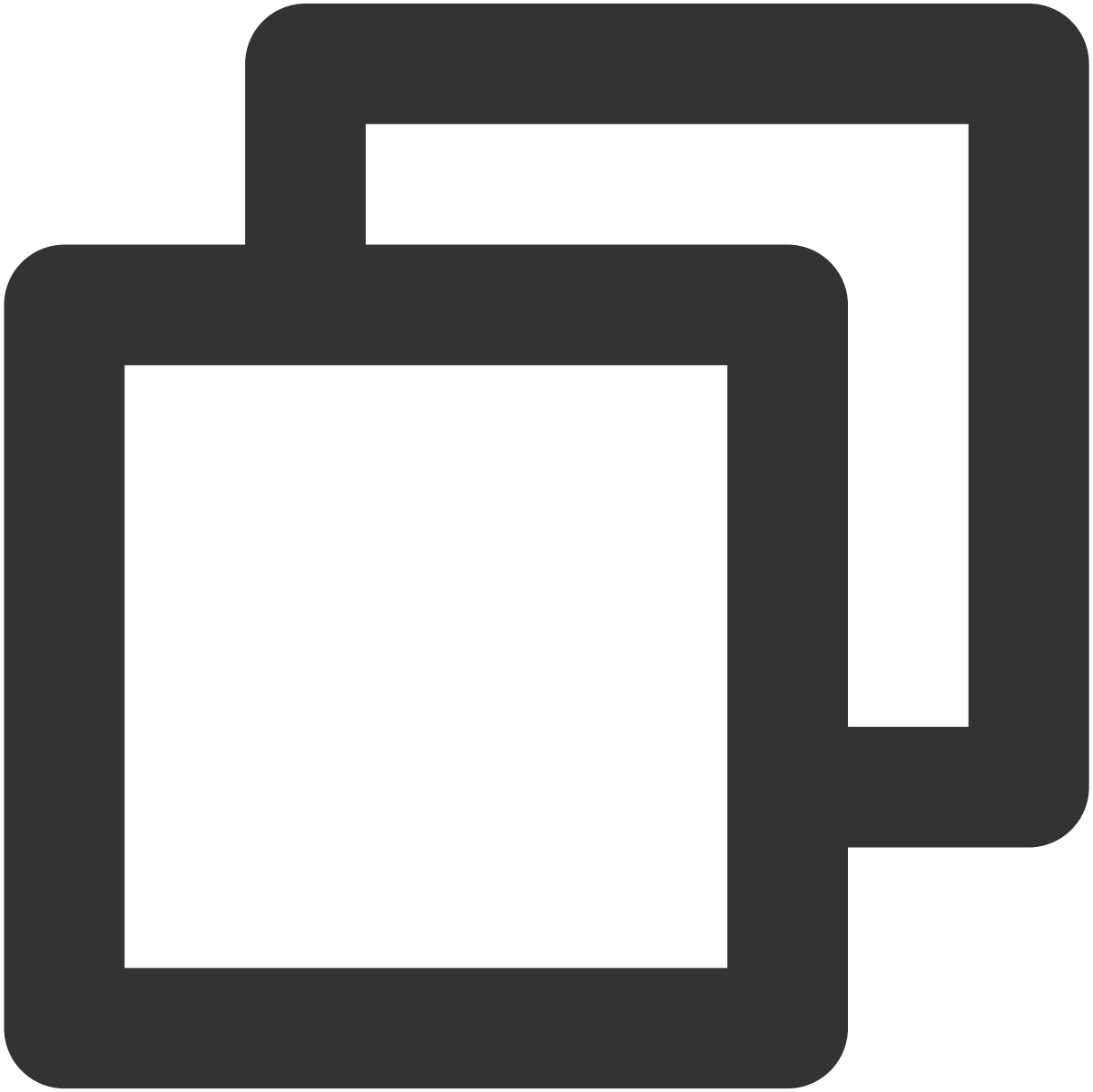


```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array('Name'=>'ayisunxxx');
$a = $ca->StopLogging($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
```

版权所有：腾讯云计算（北京）有限责任公司

```
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
[]
```

版权所有：腾讯云计算（北京）有限责任公司

拉取 COS 列表

最近更新时间：2024-02-28 17:27:24

SDK 描述

ListCosBuckets 用于拉取 COS 的 Bucket 列表。

请求参数

详见公共请求参数页面。

响应参数

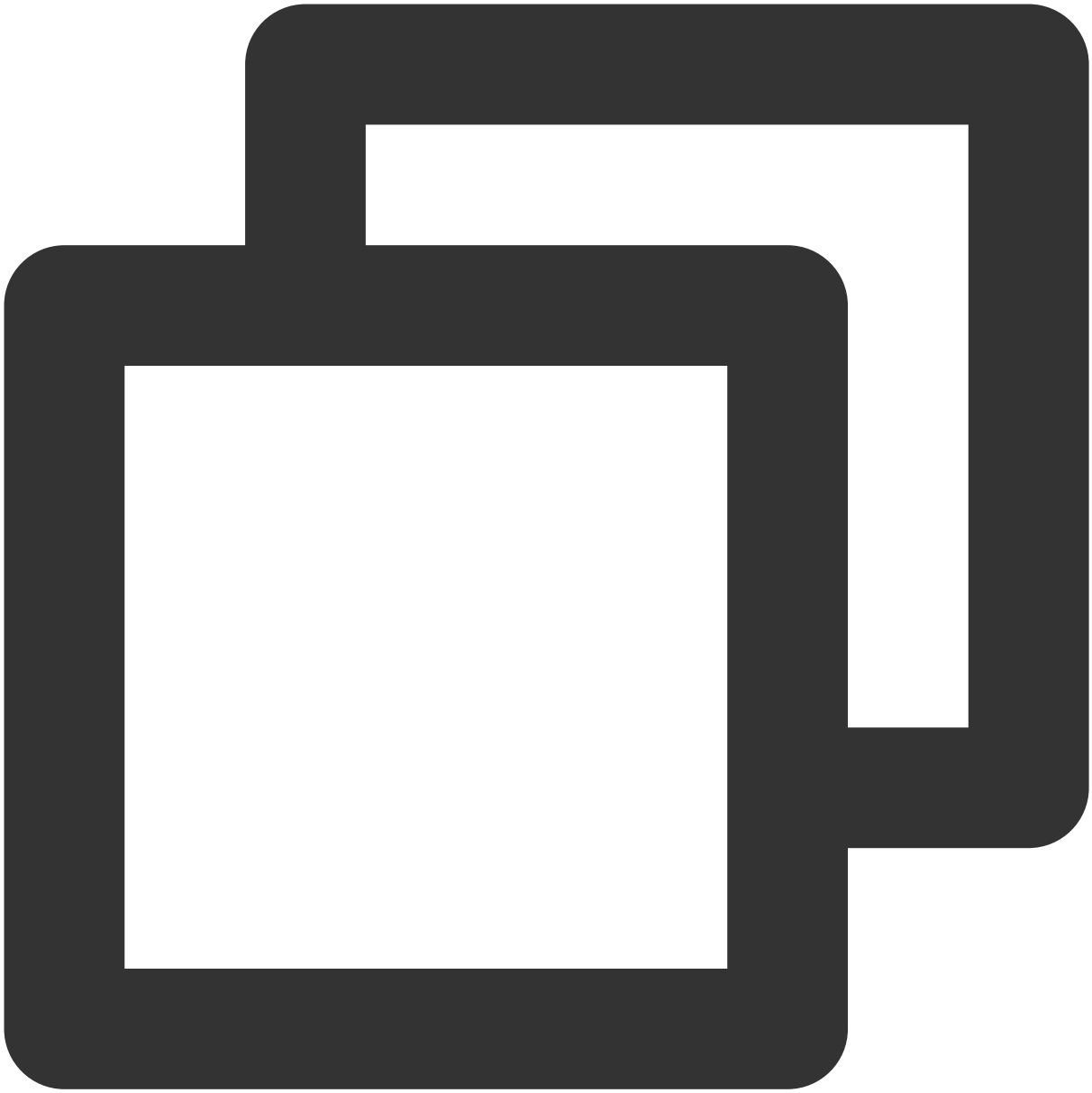
参数名称	类型	描述
cosBucketsList	Array	COS Bucket 列表。

其中 cosBucketsList 的参数如下：

参数名称	类型	描述
name	String	COS Bucket 名称。
region	String	Bucket 所在的地域。
appId	String	账号 APPID 或者项目 APPID 。

实际案例

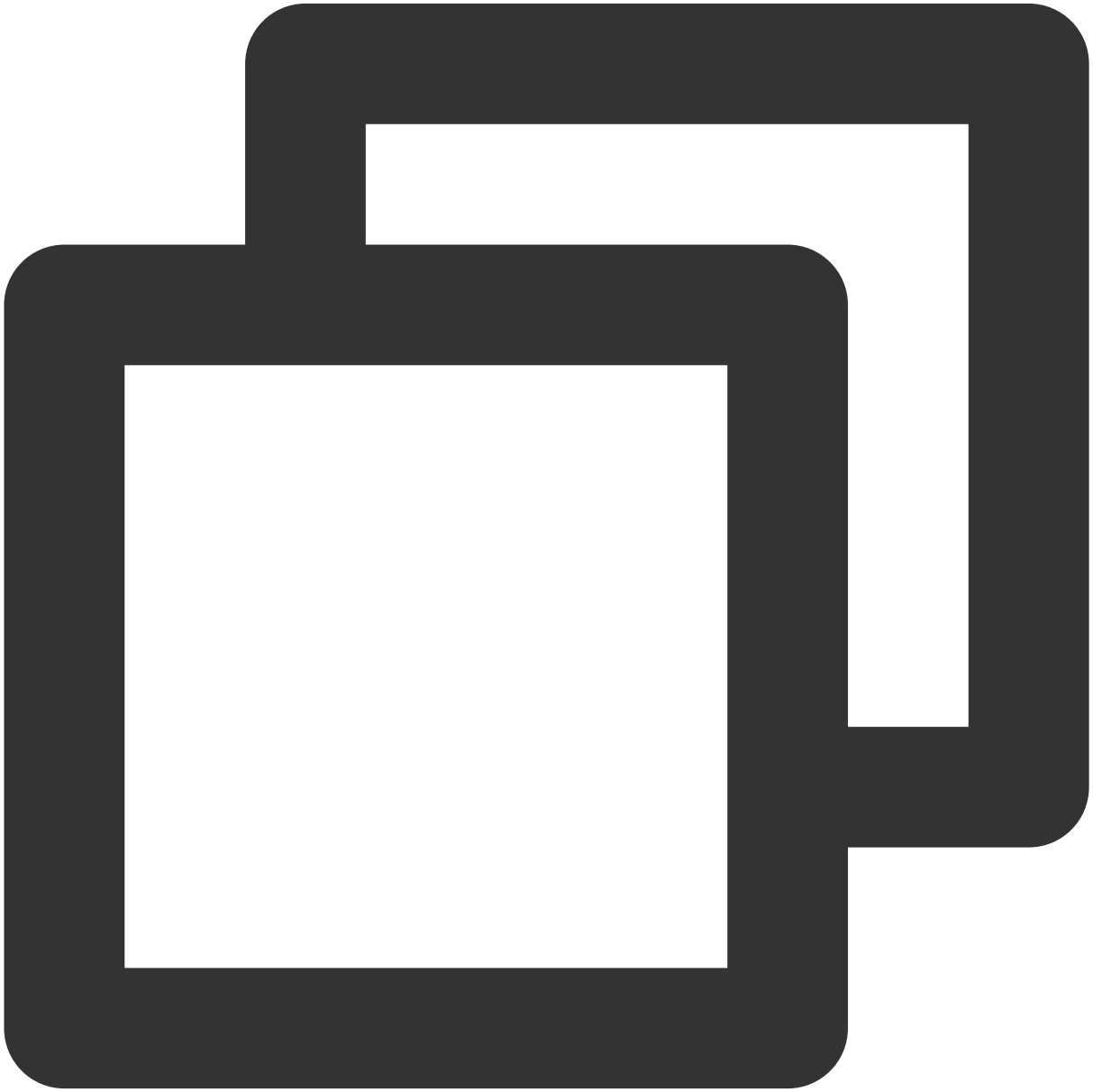
请求示例



```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array();
$a = $ca->ListCosBuckets($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
```

```
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
{
    "cosBucketsList": [
        {
            "name": "cloudaudit",
            "region": "ap-shanghai",
            "appId": "1254962721"
        },
        {
            "name": "cloudtrail",
            "region": "ap-shanghai",
            "appId": "1254962721"
        },
        {
            "name": "sundehuixxx",
            "region": "ap-shanghai",
            "appId": "1254962721"
        }
    ]
}
```

拉取操作审计列表

最近更新时间：2024-02-28 17:33:11

SDK 描述

ListAudits 用于拉取 CloudAudit 列表。

响应参数

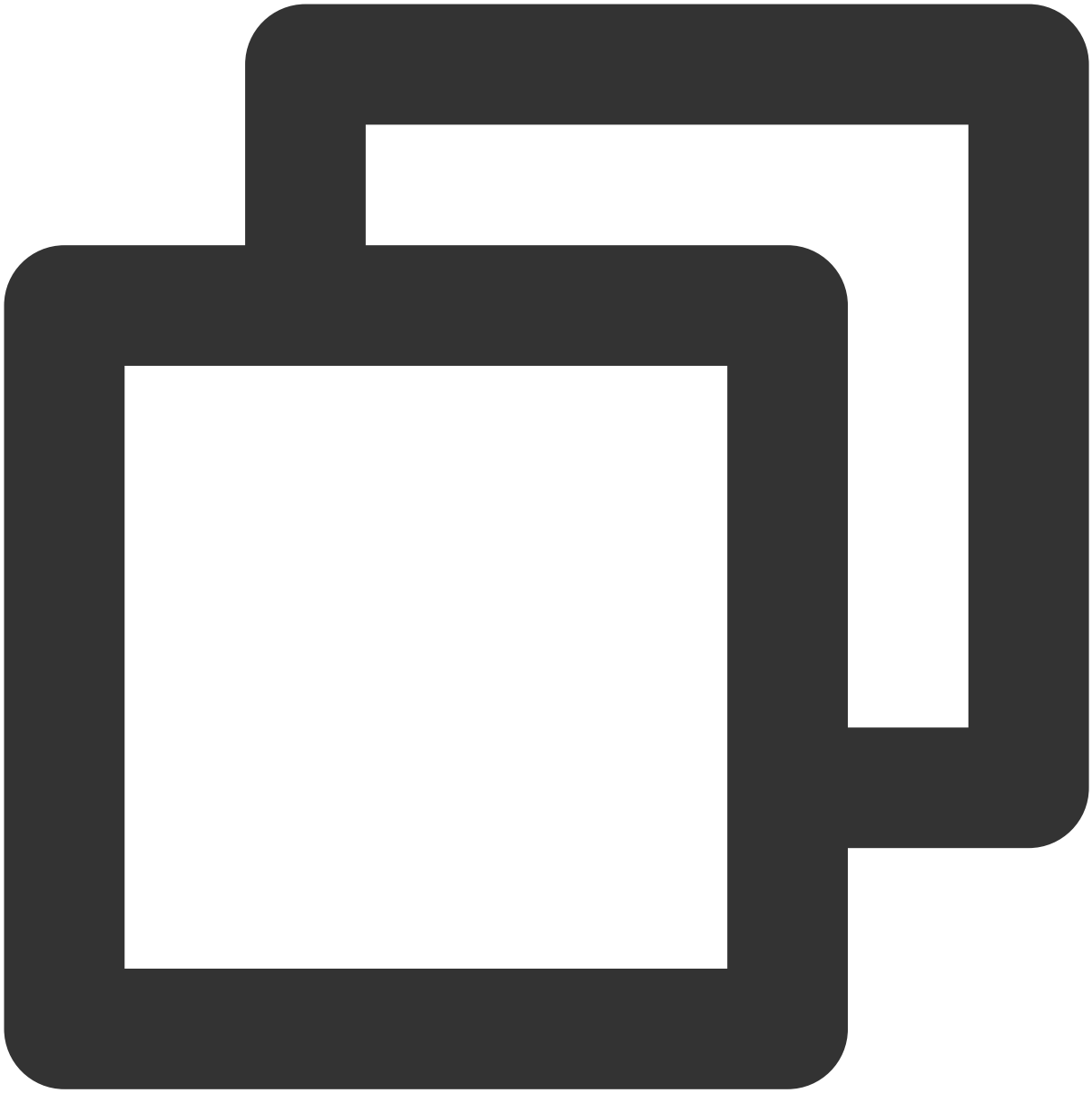
参数名称	类型	描述
auditLists	Array	跟踪集列表。

以下是 auditLists 列表的数据。

参数名称	类型	描述
Name	String	CloudAudit 名称。
bucketName	String	COS Bucket 名称。
prefix	String	日志前缀。
status	Number	Audit 状态，0：代表关闭，1：代表开启。
IsMultiRegionAudit	Number	是否开启多地域采集。0：否，1：是。

实际案例

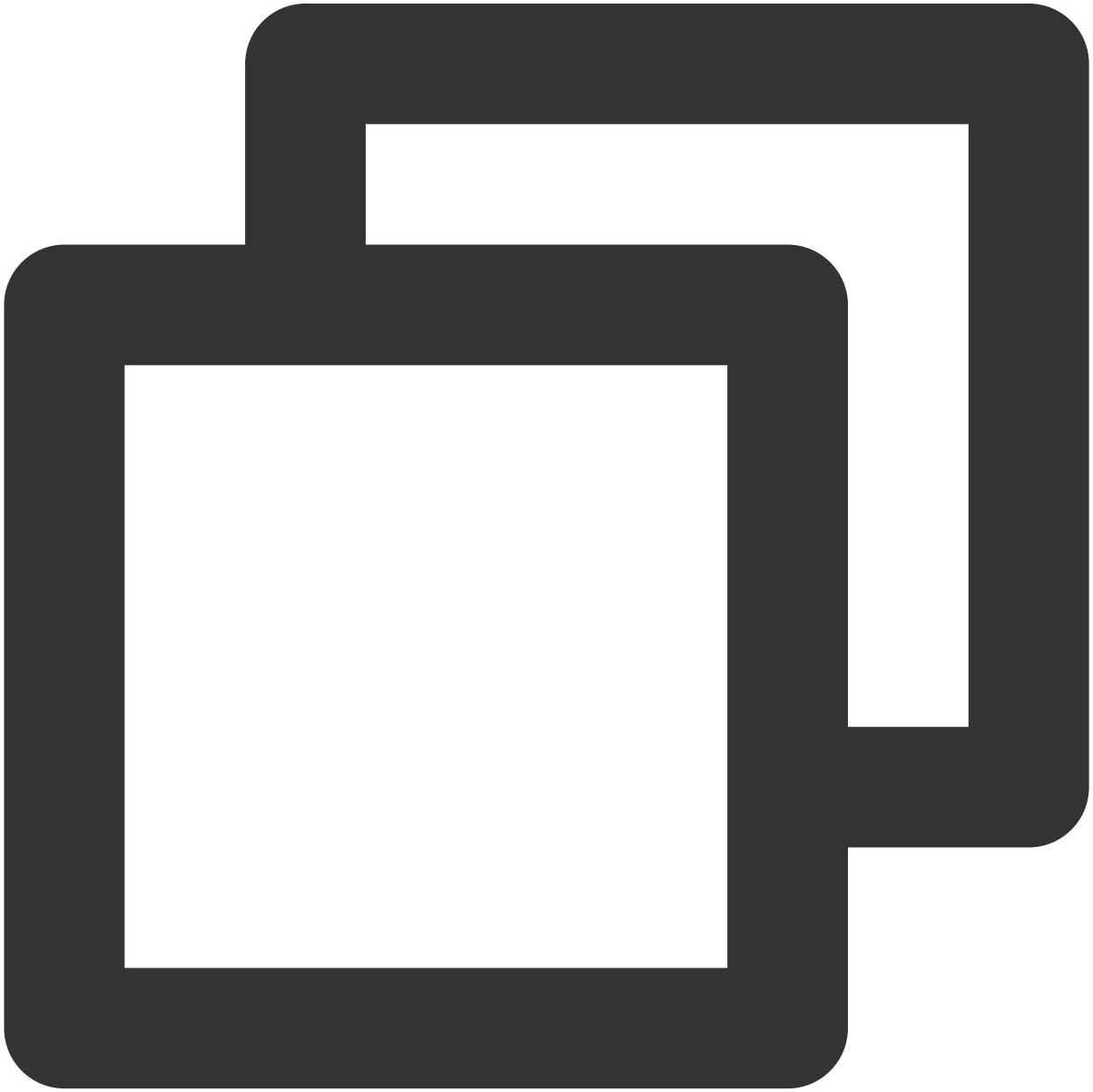
请求示例



```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array();
$a = $ca->ListAudits($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
```

```
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
{
    "auditLists": [
        {
            "name": "ayisunxxx",
            "bucketName": "sundehuixxx",
            "prefix": "91000000009",
            "status": 1,
            "isMultiRegionAudit": 1
        }
    ]
}
```


版权所有：腾讯云计算（北京）有限责任公司

获取操作审计信息

最近更新时间：2024-02-28 17:33:30

SDK 描述

DescribeAudits 用于获取 CloudAudit 信息。

请求参数

参数名称	必选	类型	描述
auditNameList	是	Array	auditName 列表

响应参数

参数名称	类型	描述
auditLists	Array	跟踪集列表

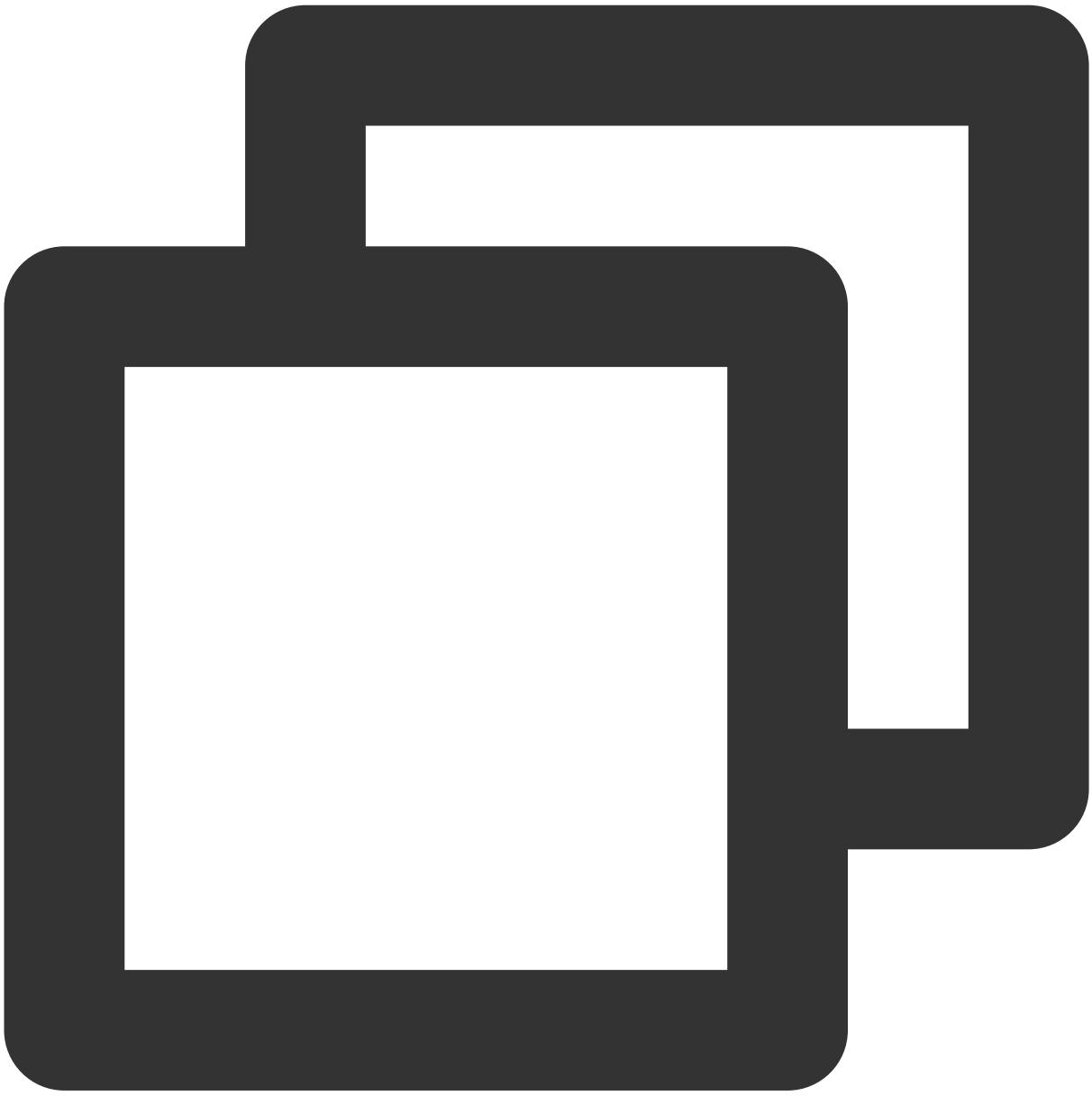
其中 auditList 的参数如下：

参数名称	类型	描述
IsMultiRegionAudit	Number	是否开启多地域查询。0：代表否，1：代表是
KmsKeyId	String	Kms 密钥 ID
Name	String	Audit 名称
CosBucketName	String	COS Bucket 名称
CosKeyPrefix	String	COS Bucket 前缀
CmqTopicName	String	CMQ 主题名称
Status	Number	Audit 状态，0：代表关闭，1：代表开启

版权所有：腾讯云计算（北京）有限责任公司

实际案例

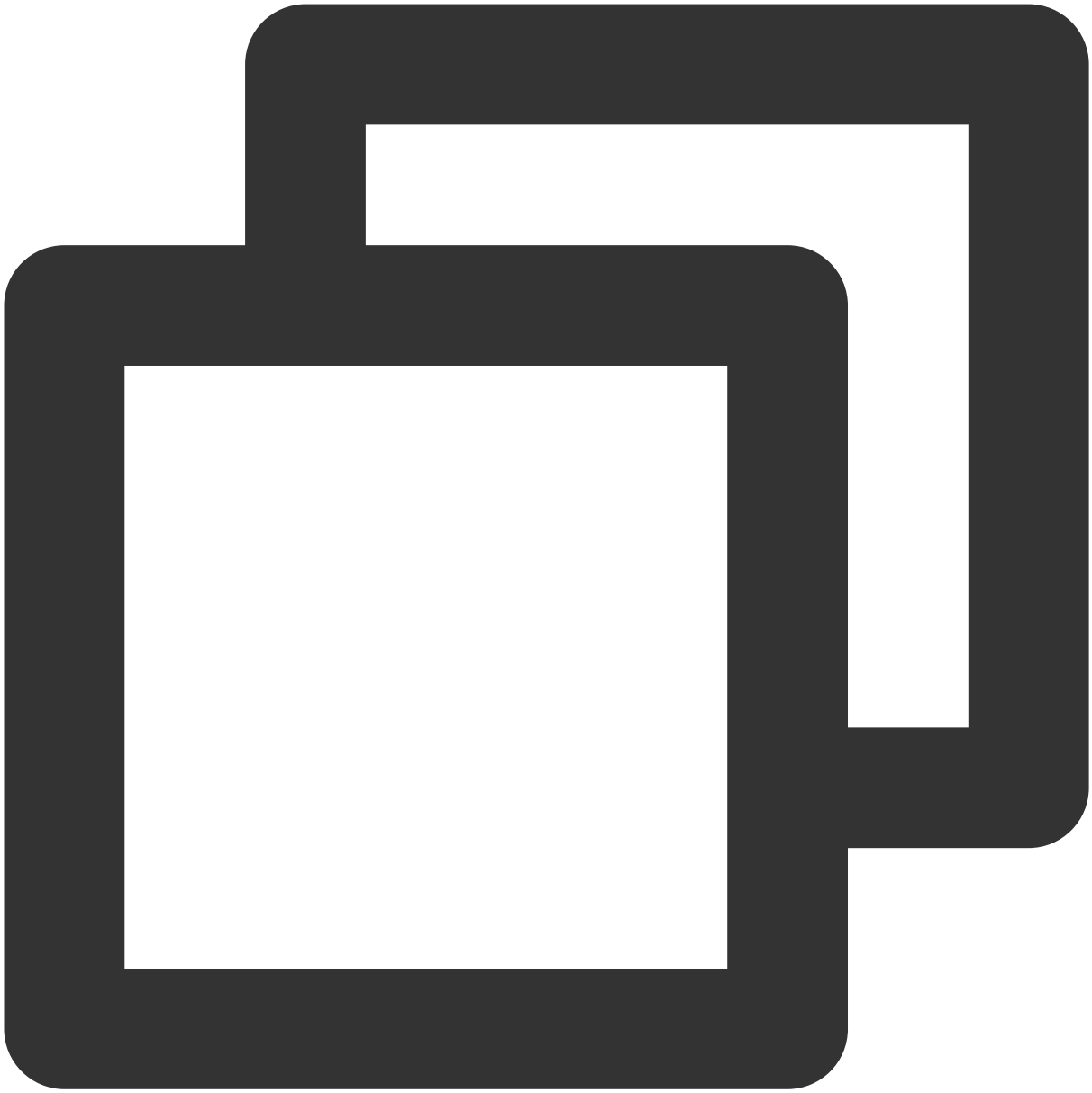
请求示例



```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array('auditNameList'=>'["ayisunxxx"]');
```

```
$a = $ca->DescribeAudits($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
{
    "auditList": [
        {
            "Name": "ayisunxxx",
            "CosBucketName": "sundehuixxx",
            "CosKeyPrefix": "91000000009",
            "Status": 1,
            "IsMultiRegionAudit": 1,
            "CmqTopicName": ""
        }
    ]
```

```
}
```

版权所有：腾讯云计算（北京）有限责任公司

删除操作审计

最近更新时间：2024-02-28 17:51:56

SDK 描述

DeleteAudit 用于删除操作审计（CloudAudit）。

请求参数

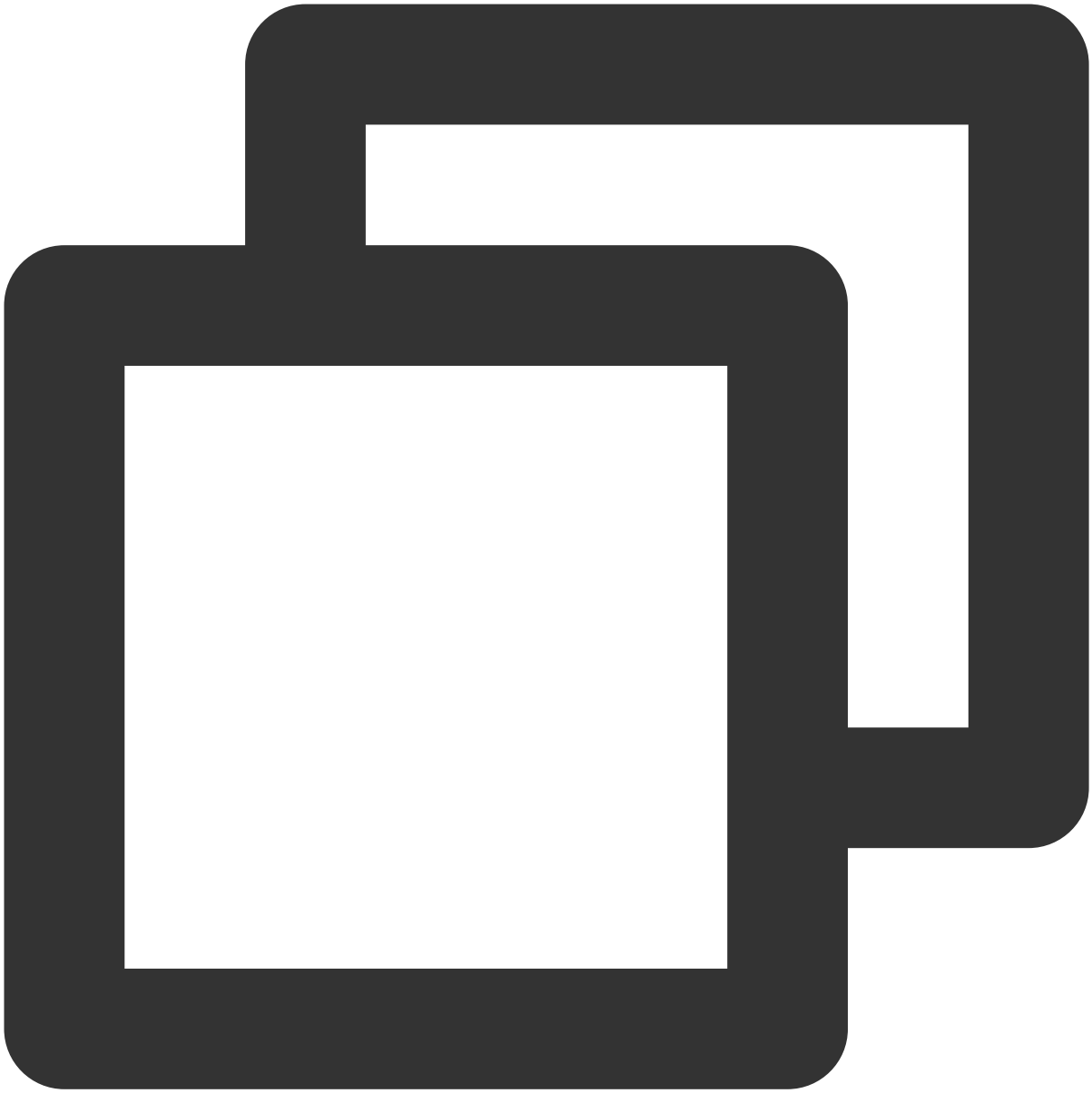
参数名称	必选	类型	描述
Name	是	String	CloudAudit 名称

响应参数

响应参数为空。

实际案例

请求示例

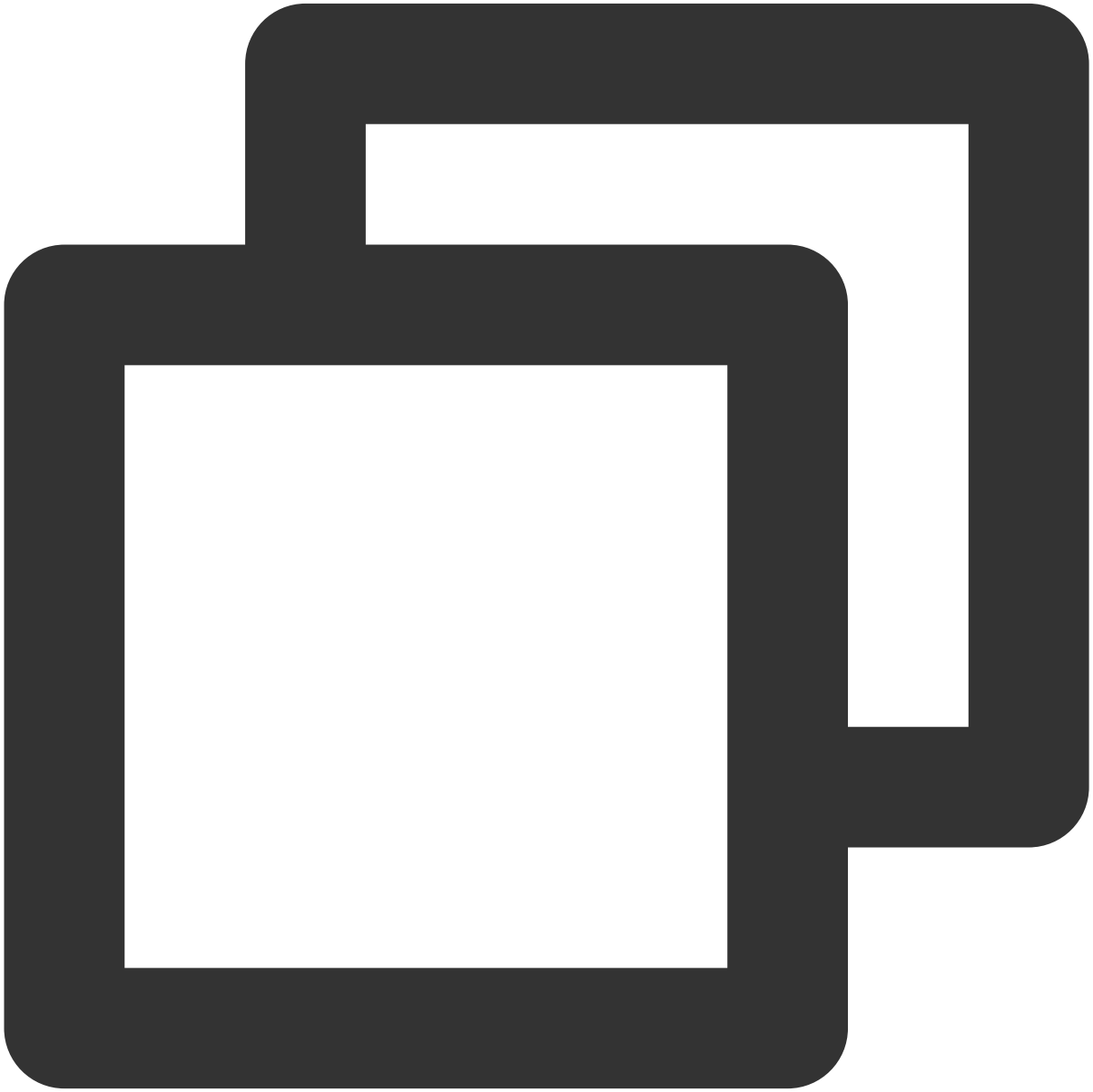


```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$package = array('Name'=>'ayisunxxx');
$a = $ca->DeleteAudit($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
```

版权所有：腾讯云计算（北京）有限责任公司

```
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例



```
[]
```

版权所有：腾讯云计算（北京）有限责任公司

检索日志

最近更新时间：2024-02-28 17:53:49

SDK 描述

LookupEvents 用于对操作日志进行检索，便于用户查询相关的操作信息。

请求参数

参数名称	必选	类型	描述
EndTime	是	DateTime	结束时间。
LookupAttributes	是	Array	属性数组，目前仅支持一个元素，不填默认返回前十条数据。
MaxResults	否	Number	日志返回的条数，不填默认返回 10 条，最多支持 50 条。
NextToken	否	String	加载更多日志的时候使用。
StartTime	是	DateTime	开始时间。

其中 LookupAttributes 的参数如下：

参数名称	必选	类型	描述
AttributeKey	否	String	搜索类型（枚举值），包括 Username：用户名，EventName：事件名称，ResourceType：资源类型，ResourceName：资源名称，EventSource：事件源，EventId：事件 ID。
AttributeValue	否	String	Value 值。

响应参数

参数名称	类型	描述
Events	Array	事件数组。
NextToken	String	加载更多时使用。

版权所有：腾讯云计算（北京）有限责任公司

其中 Events 数组的参数如下：

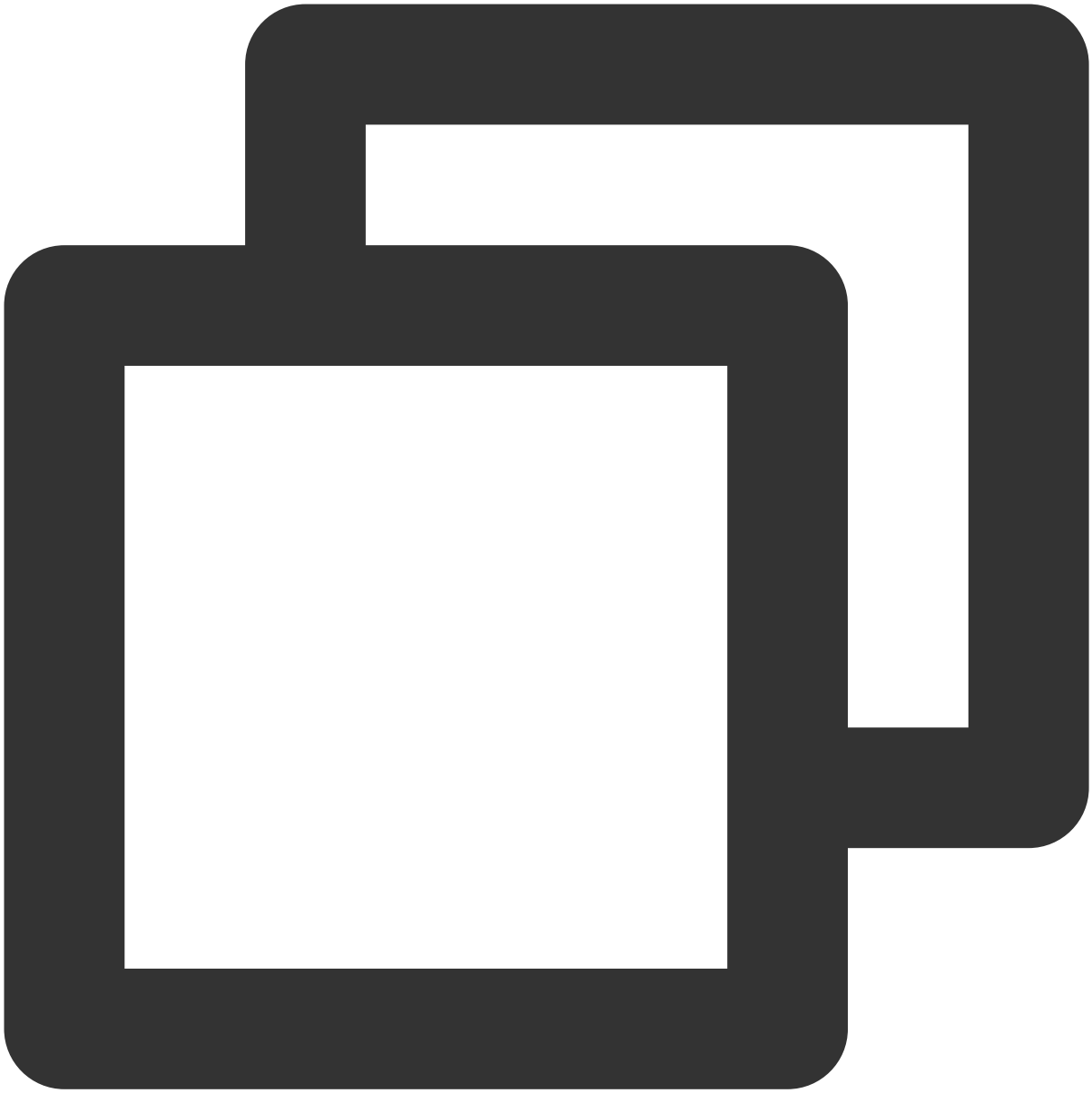
参数名称	类型	描述
CloudAuditEvent	String	事件字符串 。
EventId	String	事件 ID。
EventName	String	事件名称。
EventSource	String	事件源。
EventRegion	String	区域。
EventTime	String	事件时间。
SecretId	String	访问密钥。
EventRegion	String	区域。
ErrorCode	Number	错误码。0 代表正常，其他代表错误。
RequestID	String	请求 ID。
AccountID	String	主账号 ID。
SourceIPAddress	String	源 IP 地址。
Resources	Object	资源。
Username	String	用户名。主账号为：root，子账号为：子账号 ID，角色用户为：roleUser。

其中 Resources 的参数如下：

参数名称	类型	描述
ResourceName	String	资源名称。
ResourceType	String	资源类型。

实际案例

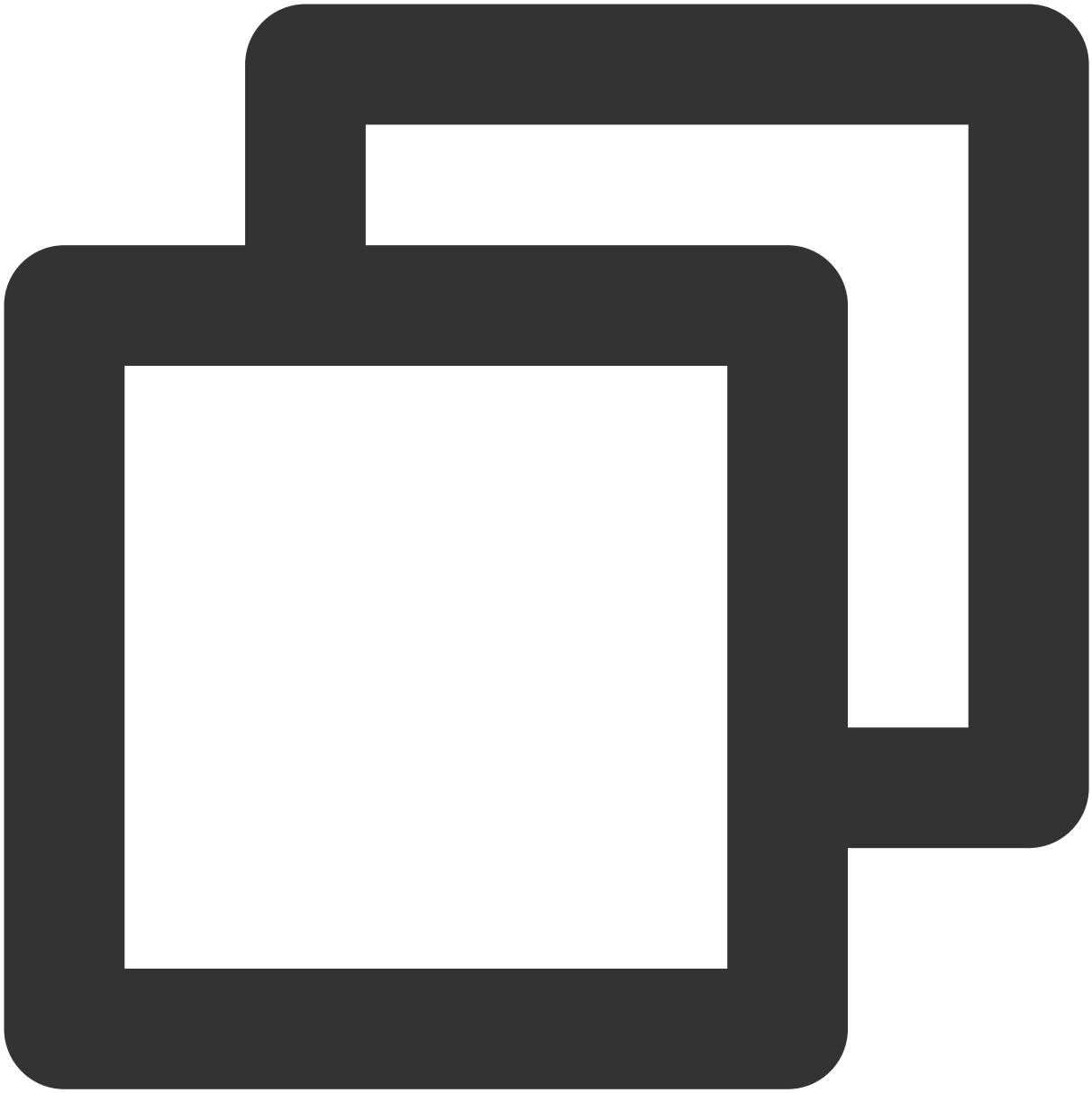
请求示例



```
$config = array('SecretId'       => '您的secretId',
                'SecretKey'      => '您的secretKey',
                'RequestMethod'  => 'GET',
                'DefaultRegion'  => 'gz');
$ca = QcloudApi::load(QcloudApi::MODULE_CLOUDAUDIT, $config);
$nowTime = time();
$startTime = $nowTime-86400;
$package = array(
       'EndTime'=>$nowTime,
       'LookupAttributes'=>'[{"AttributeKey":"string","AttributeValue":"LookupEvent
       'MaxResults'=>10,
```

```
        'StartTime'=>$startTime
);
$a = $ca->LookUpEvents($package);
if ($a === false) {
    $error = $ca->getError();
    echo "Error code:" . $error->getCode() . ".\\n";
    echo "message:" . $error->getMessage() . ".\\n";
    echo "ext:" . var_export($error->getExt(), true) . ".\\n";
} else {
    var_dump($a);
}
echo "\\nRequest :" . $ca->getLastRequest();
echo "\\nResponse :" . $ca->getLastResponse();
echo "\\n";
```

响应示例




```
{
    "Events": [
        {
            "CloudAuditEvent": "{\\"userIdentity\\":{\\"type\\":\\"Root\\",\\"princ
            "EventId": "5e9ec3fae7d93fd346cc28d397d4f1db1",
            "EventName": "LookupEvents",
            "EventTime": "2017-11-02 19:08:14",
            "SecretId": "AKIDVu8FB**********4RcbO2UnvsdDdvxqX",
            "ErrorCode": "0",
            "RequestID": 662138269,
            "AccountID": "91000000009",
```


版权所有：腾讯云计算（北京）有限责任公司

```
            "SourceIPAddress": "10.251.88.12",
            "EventSource": "cloudaudit.api.tencentyun.com/v2/index.php",
            "EventRegion": "ap-guangzhou",
            "Resources": {
                "ResourceName": "*",
                "ResourceType": "cloudaudit"
            },
            "Username": "root"
        },
        {
            "CloudAuditEvent": "{\\"userIdentity\\":{\\"type\\":\\"Root\\",\\"princ
            "EventId": "7f59b78fec0ffe363b8cd30aad159cc31",
            "EventName": "LookupEvents",
            "EventTime": "2017-11-02 15:56:53",
            "SecretId": "AKIDPhn**********EJLCqKbloJhx4yoGhv",
            "ErrorCode": "0",
            "RequestID": 1603560497,
            "AccountID": "91000000009",
            "SourceIPAddress": "14.17.22.36",
            "EventSource": "cloudaudit.api.tencentyun.com/v2/index.php",
            "EventRegion": "gz",
            "Resources": {
                "ResourceName": "*",
                "ResourceType": "cloudaudit"
            },
            "Username": "root"
        },
        {
            "CloudAuditEvent": "{\\"userIdentity\\":{\\"type\\":\\"Root\\",\\"princ
            "EventId": "8311e673d12535f8a1ae66b163554c221",
            "EventName": "LookupEvents",
            "EventTime": "2017-11-02 15:56:47",
            "SecretId": "AKIDPh**********kEJLCqKbloJhx4yoGhv",
            "ErrorCode": "0",
            "RequestID": 1352885274,
            "AccountID": "91000000009",
            "SourceIPAddress": "14.17.22.36",
            "EventSource": "cloudaudit.api.tencentyun.com/v2/index.php",
            "EventRegion": "gz",
            "Resources": {
                "ResourceName": "*",
                "ResourceType": "cloudaudit"
            },
            "Username": "root"
        },
        {
            "CloudAuditEvent": "{\\"userIdentity\\":{\\"type\\":\\"Root\\",\\"princ
```

```
            "EventId": "cc737c139d689b109c265561a7e5bfe61",
            "EventName": "LookupEvents",
            "EventTime": "2017-11-02 15:06:41",
            "SecretId": "AKIDVu8F**********w4RcbO2UnvsdDdvxqX",
            "ErrorCode": "0",
            "RequestID": 803010205,
            "AccountID": "91000000009",
            "SourceIPAddress": "14.17.22.36",
            "EventSource": "cloudaudit.api.cloud.tencent.com/v2/index.php",
            "EventRegion": "gz",
            "Resources": {
                "ResourceName": "*",
                "ResourceType": "cloudaudit"
            },
            "Username": "root"
        }
    ],
    "NextToken": "MjAxNzExMDIxMywyMDE3MTEwMjEyLDIwMTcxMTAyMTEsMjAxNzExMDIxMCwyMDE3M
    "ListOver": false
}
```