解决方案实践

使用预签名 URL 直传 OBS

文档版本	1.0.0
发布日期	2023-06-06

华为技术有限公司

商标声明


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。

安全声明

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

目 录

1 方案概述

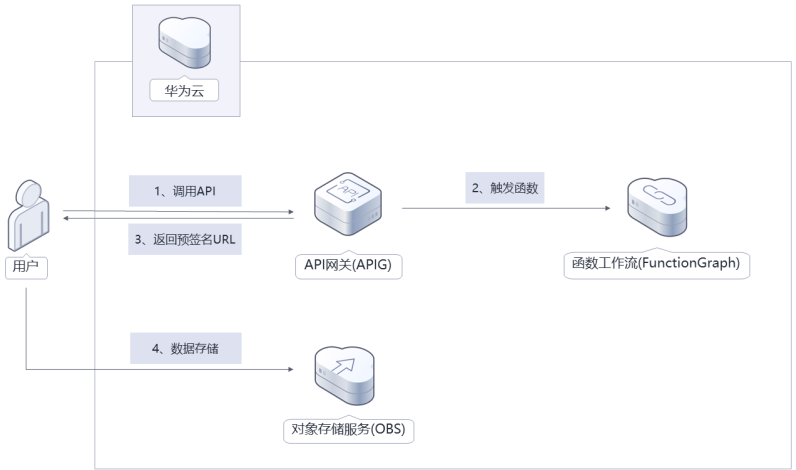
应用场景

该解决方案通过**函数工作流 FunctionGraph**调用后台接口获取文件预签名URL，帮助用户实现无服务器使用文件预签名URL上传文件到对象存储服务OBS桶。适用于在不提供给其他人SK的情况下，让其他人能用自身提供的APIG封装的API接口实现预签名URL上传文件到指定的OBS桶指定目录。

方案架构

该解决方案基于华为云**函数工作流 FunctionGraph**、**API网关 APIG**，帮用户实现预签名URL上传文件到**OBS**桶。解决方案架构图如下：

图 1-1 方案架构图



该解决方案将会部署如下资源：

- 函数工作流 FunctionGraph，用于部署前端及调用后端服务

- API网关 APIG，将函数工作流 FunctionGraph 提供的服务能力封装为API供服务调用
- 对象存储服务 OBS桶，将文件使用文件预签名URL上传到OBS桶指定目录

方案优势

- 无服务器架构

  无服务器化方案，用户无需关注资源运维，只需关注业务运行状态。
- 前端直传OBS

  不需要后台服务器做文件上传OBS的操作。
- 安全可靠

  该方案生成的预签名URL具有有效期，且不会暴露SK信息。

约束与限制

- 部署该解决方案前，您需注册华为账号并开通华为云，完成实名认证，且账号不能处于欠费或冻结状态。
- 服务部署完成之后，需手动开启 函数工作流->设置->高级设置->请求头传入密钥的开关，以保证后台成功获取用户的临时AK、SK信息生成文件预签名URL。

2 资源和成本规划

该解决方案主要部署如下资源，以下费用仅供参考，具体请参考华为云官网**价格详情**，实际收费以账单为准。

表 2-1 成本预估（仅供参考）

华为云服务	计费说明	每月花费（调用100万次）
函数工作流 FunctionGraph	• 区域：华北-北京四 • 产品：函数 • 请求次数： 0-100万次： 0元/100万次 100万次以上： 1.33元/100万次 • 计量时间： 0-400,000 GB/秒： 0元/GB-秒 400,000 GB/秒以上：0.00011108元/GB-秒	0元
API网关（共享版）	• 区域：华北-北京四 • 计费项：API调用次数 • 月累计超过次数：0~1000万次（含） • 价格：0.06 元/万次 • 计费项：流量（公网流出流量） • 价格：0.8 元/GB	API调用次数：0.06元 预计每月新增1GB数据量，花费0.8元，详细请参考每月账单。

华为云服务	计费说明	每月花费（调用100万次）
对象存储服务 OBS	• 区域：华北-北京四 • 存储空间：数据存储（多AZ存储） • 默认存储类别：标准存储 • 桶策略：私有 • 请求费用：0.0100元/万次 • 存储空间：0.0990元/GB/月 • 流量费用： • 公网流出流量 / 00:00-08:00（闲时）0.2500元/G • 公网流出流量 / 08:00-24:00（忙时）0.5000元/GB 费用包括存储空间、请求费用、流量费用两部分，具体请参考**OBS计费详情**。	费用包括存储空间、请求费用、流量费用两部分，详细请参考每月账单。
合计	-	约0.86元

3 实施步骤

3.1 准备工作

创建 rf_admin_trust 委托

步骤1 进入华为云官网，打开**控制台管理**界面，鼠标移动至个人账号处，打开“统一身份认证”菜单

图 3-1 控制台管理界面

图 3-2 统一身份认证菜单

步骤2 进入“委托”菜单，搜索“rf_admin_trust”委托

图 3-3 委托列表

- 如果委托存在，则不用执行接下来的创建委托的步骤
- 如果委托不存在时执行接下来的步骤创建委托

步骤3 单击步骤2界面中的“创建委托”按钮，在委托名称中输入“rf_admin_trust”，委托类型选择“云服务”，输入“RFS”，单击“下一步”

图 3-4 创建委托

步骤4 在搜索框中输入”Tenant Administrator”权限，并勾选搜索结果

图 3-5 选择策略

步骤5 选择“所有资源”，并单击下一步完成配置

图 3-6 设置授权范围

步骤6 “委托”列表中出现“rf_admin_trust”委托则创建成功

图 3-7 委托列表

----结束

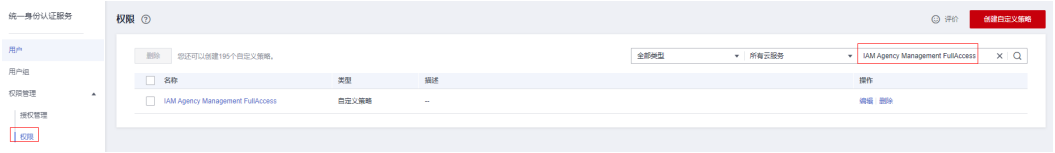
创建 IAM Agency Management FullAcces 策略

步骤1 打开“统一身份认证”菜单

图 3-8 统一身份认证菜单

步骤2 进入“权限管理”-> “权限”菜单，在搜索框输入“IAM Agency Management FullAcces”当前账号是否存在IAM委托管理权限

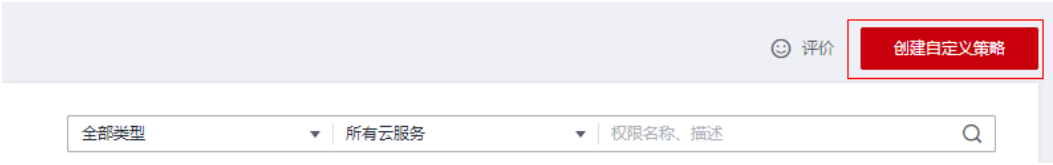
图 3-9 权限列表



- 如果搜索结果不为空，则当前账号已经存在IAM委托管理权限，不需要重复创建
- 如果过搜索结果为空，则继续创建“IAM Agency Management FullAcces”权限

步骤3 单击“创建自定义策略”按钮

图 3-10 创建自定义策略



步骤4 输入策略名称为“IAM Agency Management FullAcces”，选择“JSON视图”，在策略内容中输入如下JSON代码，单击确认按钮

图 3-11 创建自定义策略


```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "iam:agencies:createAgency",
        "iam:agencies:listAgencies",
        "iam:agencies:getAgency",
        "iam:agencies:deleteAgency",
        "iam:agencies:updateAgency",
        "iam:permissions:revokeRoleFromAgencyOnProject",
        "iam:permissions:revokeRoleFromAgencyOnDomain",
        "iam:permissions:revokeRoleFromAgency",
        "iam:permissions:grantRoleToAgencyOnDomain",
        "iam:permissions:grantRoleToAgencyOnProject",
        "iam:permissions:grantRoleToAgency",
```

```
            "iam:permissions:listRolesForAgencyOnDomain",
            "iam:permissions:listRolesForAgencyOnProject",
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:listRolesForAgency",
            "iam:permissions:checkRoleForAgency",
            "iam:roles:listRoles"
        ],
        "Effect": "Allow"
    }
  ]
}
```

步骤5 界面无报错，则成功创建IAM Agency Management FullAcces权限

----结束

给 rf_admin_trust 委托添加 IAM Agency Management FullAcces 策略

步骤1 打开“统一身份认证”菜单

图 3-12 统一身份认证菜单

步骤2 进入“委托”菜单，选择rf_admin_trust委托

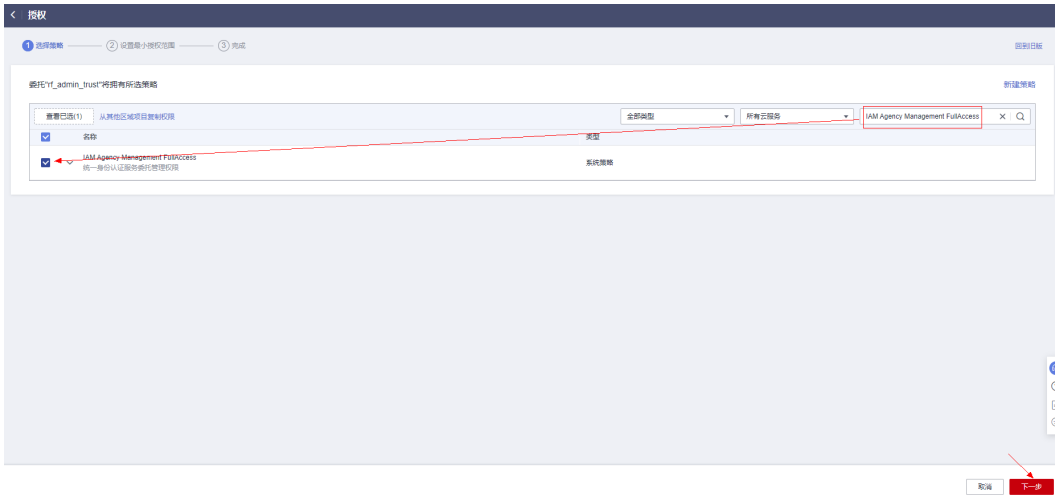
图 3-13 委托列表

步骤3 进入“授权记录”菜单，单击“授权”按钮

图 3-14 授权记录

步骤4 在搜索框输入IAM Agency Management FullAcces，勾选过滤出来的记录，单击下一步，并确认完成权限的配置

图 3-15 配置 IAM Agency Management FullAcces 策略



步骤5 配置好后的情况：rf_admin_trust委托拥有Tenant Administrator和IAM Agency Management FullAccess权限

图 3-16 授权记录列表

----结束

3.2 快速部署

本章节主要帮助用户快速部署“使用预签名URL直传OBS”解决方案。

表 3-1 参数说明

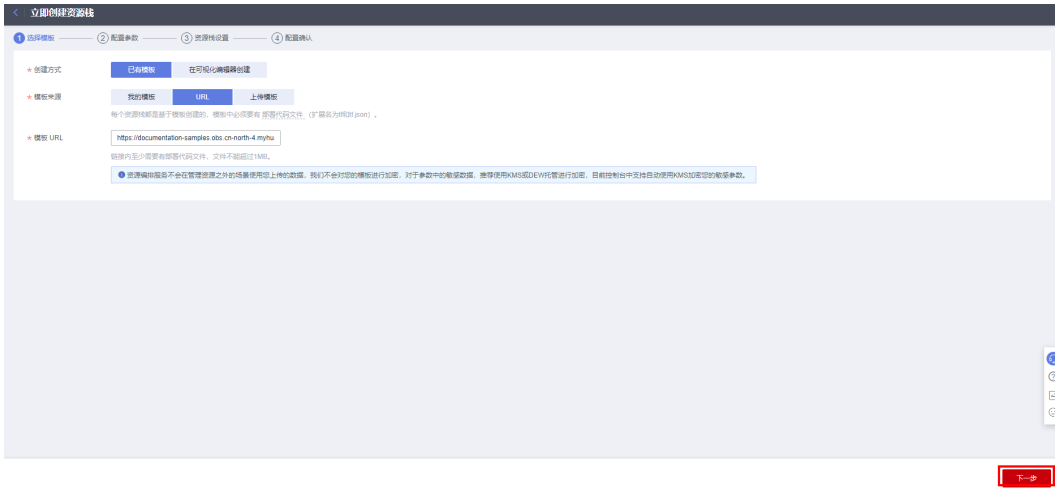
参数名称	类型	是否可选	参数解释	默认值
function_name	string	必填	函数名称，用于定义创建函数及其他资源前缀，不支持重名。取值范围：1-56个字符，可包含字母、数字、下划线和中划线，以大/小写字母开头。	presigned-url-to-obs-demo
obs_bucket_name	string	必填	OBS桶名称，全局唯一，用于上传文件数据。取值范围：3-63个字符，支持小写字母、数字、中划线（-）、英文句号（.）。	空

步骤1 登录**华为云解决方案实践**，选择“使用预签名URL直传OBS”，单击“一键部署”，跳转至解决方案创建资源栈界面。

图 3-17 解决方案实施库

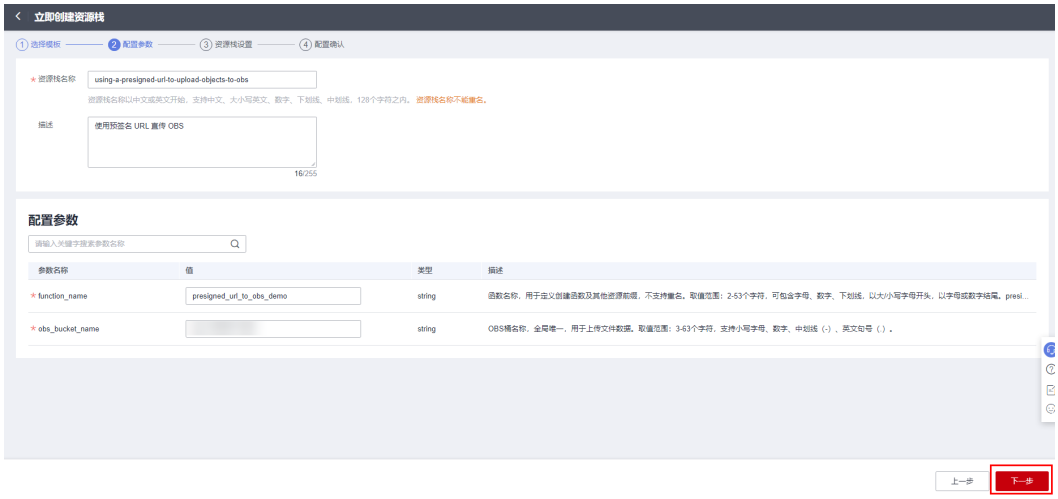
步骤2 在选择模板界面中，单击“下一步”。

图 3-18 选择模板



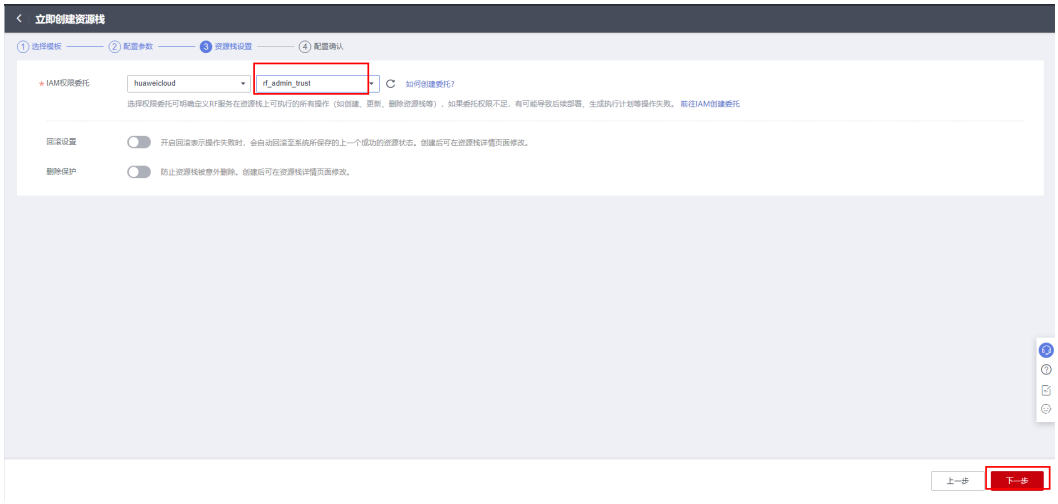
步骤3 在配置参数界面中，参考**表3-1**完成自定义参数填写，单击“下一步”。

图 3-19 配置参数



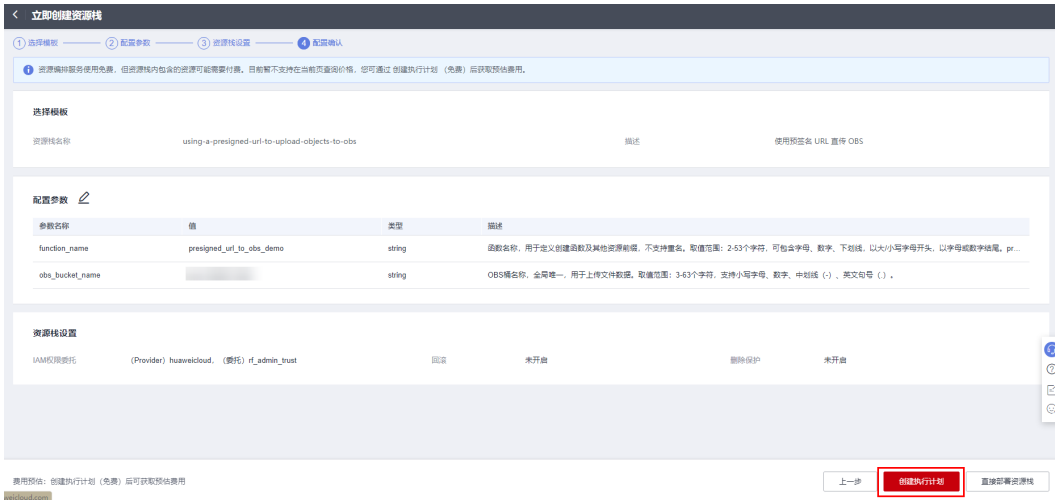
步骤4 在资源设置界面中，在权限委托下拉框中选择“rf_admin_trust”委托，单击“下一步”。

图 3-20 资源栈设置



步骤5 在配置确认界面中，单击“创建执行计划”。

图 3-21 配置确认



步骤6 在弹出的创建执行计划框中，自定义填写执行计划名称，单击“确定”。

图 3-22 创建执行计划

步骤7 单击“部署”，并且在弹出的执行计划确认框中单击“执行”。

图 3-23 执行计划

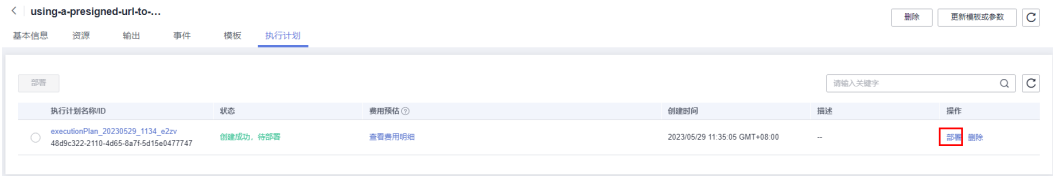
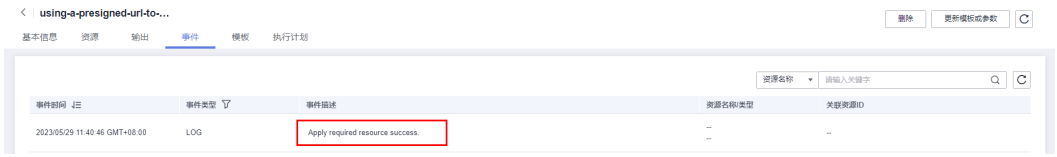


图 3-24 执行计划确认

步骤8 待“事件”中出现“Apply required resource success”，表示该解决方案已经部署完成。

图 3-25 部署完成

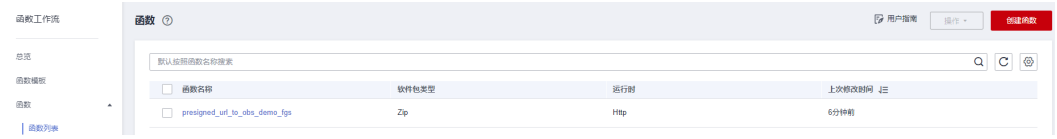


----结束

3.3 开始使用

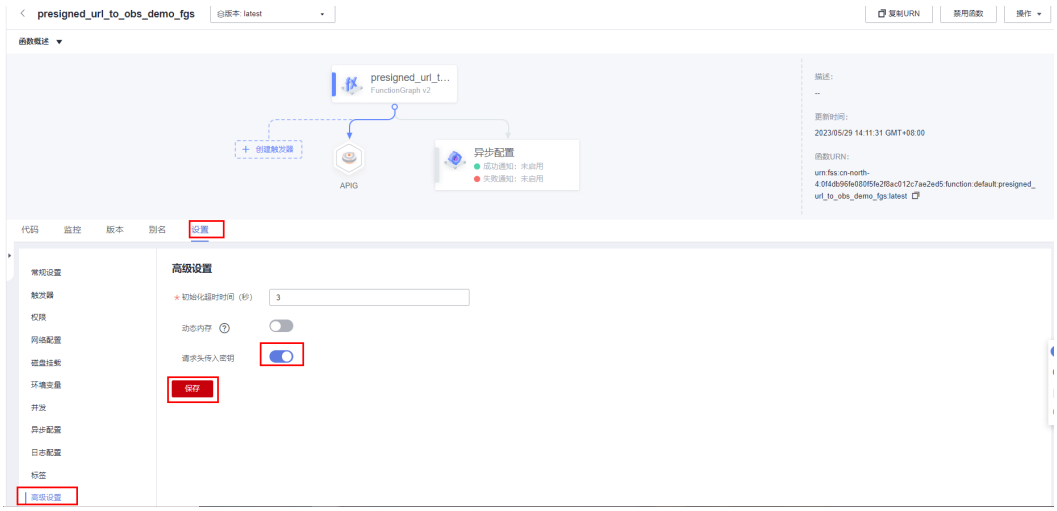
步骤1 登录华为云进入**函数工作流FunctionGraph控制台**，在函数列表中查看该方案创建的函数。

图 3-26 创建的函数



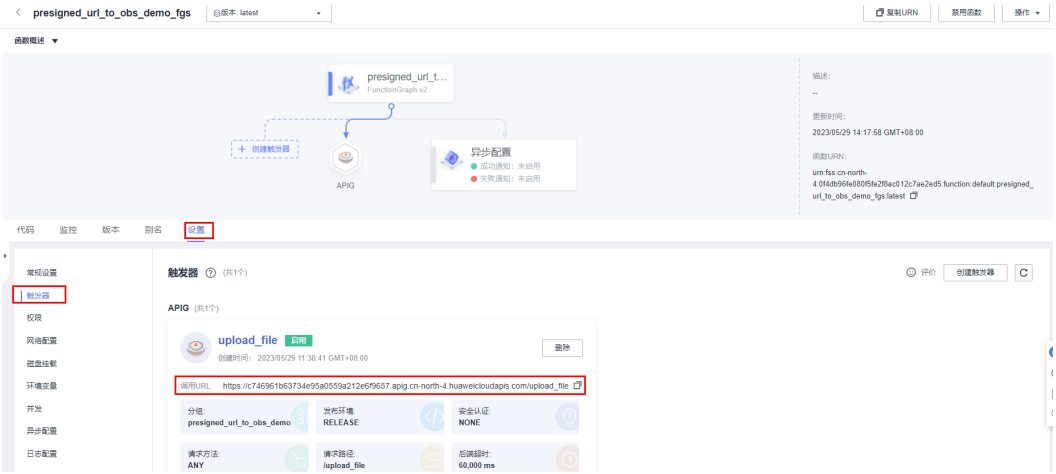
步骤2 进入相应函数中，单击“设置”->“高级设置”->“请求头传入密钥”开关，然后单击“保存”，以保证后台成功获取用户的临时AK、SK信息生成文件预签名URL。

图 3-27 打开请求头传入密钥开关



步骤3 进入相应函数中，单击“设置”->“触发器”查看该方案创建的APIG触发器中的 调用URL。

图 3-28 APIG 触发器调用 URL



步骤4 通过浏览器访问该APIG触发器中的调用URL，即可访问预签名URL直传OBS的前端界面，进行上传操作（详细操作规则参考前端页面规则设置）。

图 3-29 上传文件到 OBS 页面

步骤5 到OBS对象存储服务页面查找创建的桶，打开并查看上传过的文件。

图 3-30 在对应 OBS 桶查看上传过的文件

----结束

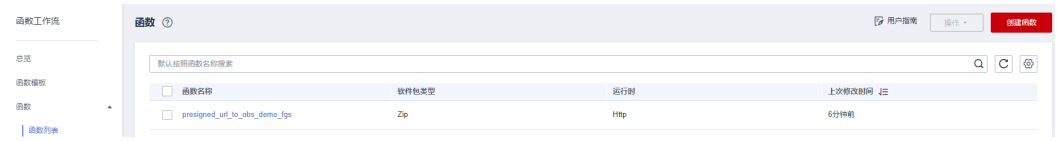
3.4 快速卸载

须知

快速卸载前请确认OBS桶中无文件，否则会导致删除失败。

步骤1 解决方案部署成功后，登录华为云进入**函数工作流FunctionGraph控制台**，在函数列表中查看该方案创建的函数。

图 3-31 创建的函数，



步骤2 进入相应函数中，单击“设置”->“触发器”，然后单击“删除”，删除APIG触发器。

图 3-32 删除 APIG 触发器

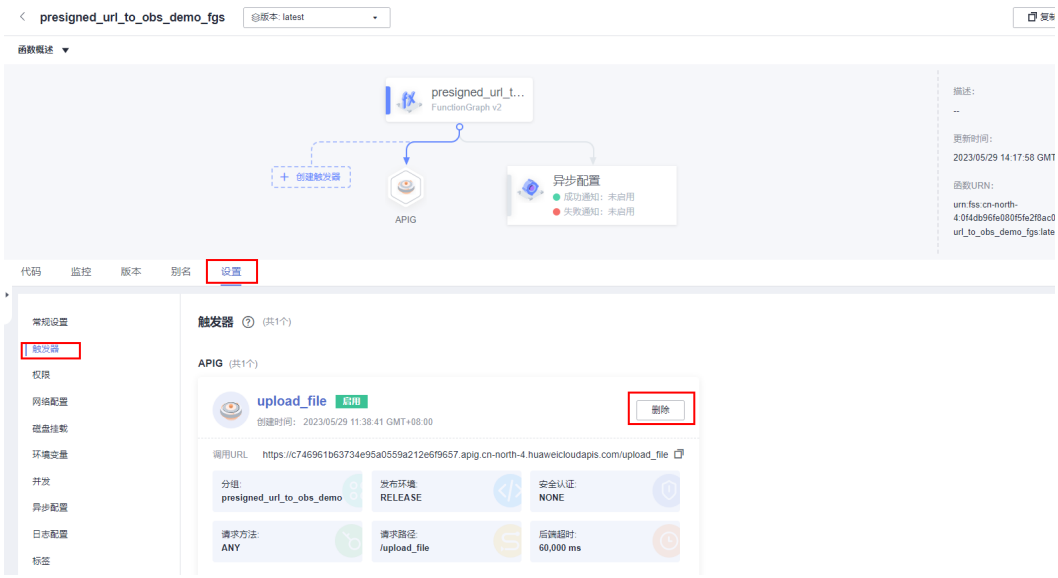


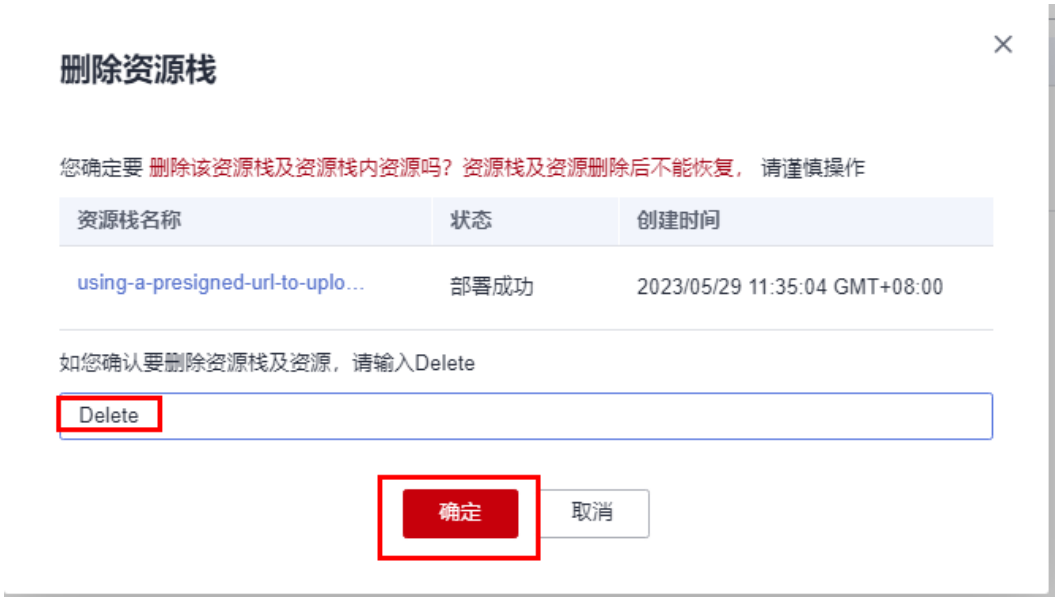
图 3-33 确认执行删除 APIG 触发器操作

步骤3 在资源栈单击该方案堆栈后的“删除”。

图 3-34 一键卸载

步骤4 在弹出的删除堆栈确定框中，输入“Delete”，单击“确定”，即可卸载解决方案。

图 3-35 删除堆栈确定



----结束

4 附录

名词解释

- 函数工作流：**FunctionGraph**是一项基于事件驱动的函数托管计算服务。使用FunctionGraph函数，只需编写业务函数代码并设置运行的条件，无需配置和管理服务器等基础设施，函数以弹性、免运维、高可靠的方式运行。此外，按函数实际执行资源计费，不执行不产生费用。
- API网关：**APIG**（Application Programming Interface，应用程序编程接口）是一些预先定义的函数，应用将自身的服务能力封装成API，并通过API网关开放给用户调用。API包括基本信息、前后端的请求路径和参数以及请求相关协议。
- 对象存储服务(**OBS**)：一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。

5 修订记录

表 5-1 参数说明

发布日期	修订记录
2023-05-30	第一次正式发布。