解决方案实践

通过 Nginx 反向代理访问 OBS 最佳实践

文档版本 1.0.0

发布日期 2023-08-22

华为技术有限公司

版权所有 © 华为技术有限公司 2024。 保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

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

版权所有 © 华为技术有限公司

目 录

版权所有 © 华为技术有限公司

1 方案概述

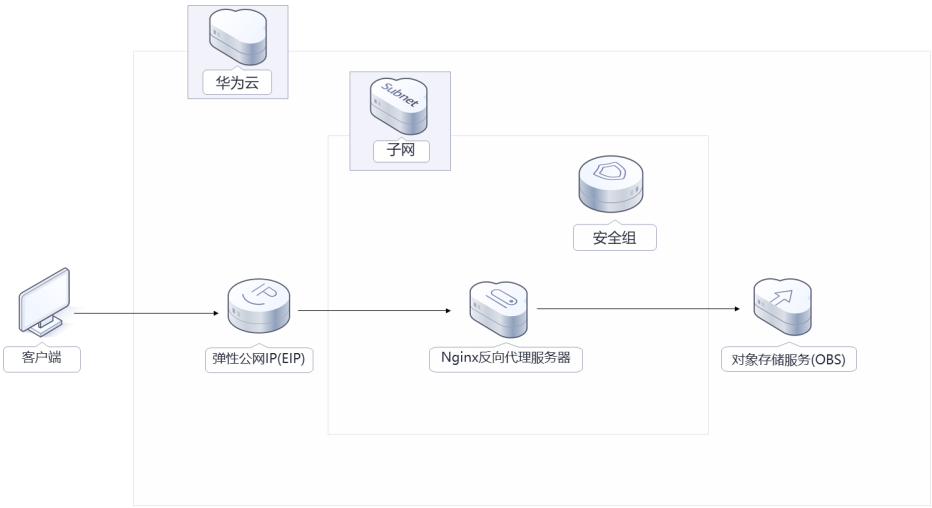
应用场景

该方案通过在弹性云服务器 ECS上部署Nginx反向代理服务器，帮助用户实现固定IP地址访问对象存储服务 OBS桶内的资源。仅暴露代理服务器的IP地址，隐藏对象存储服务 OBS真实域名，有效增强数据的安全性。

方案架构

该解决方案部署架构如下图所示：

图 1-1 方案架构



该解决方案会部署如下资源：

- 创建一台弹性云服务器 ECS，用于搭建Nginx反向代理服务器。
- 创建一个弹性公网IP EIP，并绑定到弹性云服务器 ECS，用于下载Nginx安装包，同时对外提供访问入口。

版权所有 © 华为技术有限公司

- 创建安全组，通过配置安全组访问规则保证Nginx反向代理服务器的安全。

方案优势

- 安全可靠

  通过Nginx反向代理，仅暴露代理服务器的IP地址，隐藏OBS真实域名，保证OBS数据的安全性。

- 开源和定制化

  该解决方案是开源的，用户可以免费用于商业用途，并且还可以在源码基础上进行定制化开发。

- 一键部署

  一键轻松部署，即可搭建Nginx反向代理服务器。

约束与限制

- 在开始解决方案部署之前，请确认您已经拥有一个可以访问该区域的华为账号且已开通华为云。如果选择计费模式选择“包年包月”，请确保账户余额充足以便一键部署资源的时候可以自动支付；或者在一键部署的过程进入费用中心，找到“待支付订单”手动完成支付。
- 已明确被代理的对象存储服务 OBS桶所在区域和桶的名称。

版权所有 © 华为技术有限公司

2 资源和成本规划

该解决方案主要部署如下资源，不同产品的花费仅供参考，具体请参考华为云**官网价格**，实际以收费账单为准：

表 2-1 资源和成本规划（按需计费）

华为云服务	配置示例	每月预估花费
弹性云服务器 ECS	• 区域：亚太-新加坡 • 计费模式：按需计费 • 规格：X86计算 | ECS | s6.medium.2 | 1vCPUs | 2GiB • 镜像：CentOS 7.6 64bit • 系统盘：高IO | 100GB • 购买量：1	$0.04 USD*24*30= $28.8 USD
弹性公网IP EIP	• 按需计费（按带宽计费）：$0.03 USD/5M/小时 • 区域：亚太-新加坡 • 计费方式：按带宽计费 • 线路：动态BGP • 带宽大小：5Mbit/s • 购买量：1	$0.13 USD*24*30= $93.6 USD
合计	-	$122.4 USD

版权所有 © 华为技术有限公司

表 2-2 资源和成本规划（包年包月）

华为云服务	配置示例	每月预估花费
弹性云服务器 ECS	● 区域：亚太-新加坡 ● 计费模式：包年包月 ● 规格：X86计算 | ECS | s6.medium.2 | 1vCPUs | 2GiB ● 镜像：CentOS 7.6 64bit ● 系统盘：高IO | 100GB ● 购买量：1	$25.26 USD
弹性公网IP EIP	● 区域：亚太-新加坡 ● 计费模式：包年包月 ● 线路：动态BGP ● 计费模式：按带宽计费 ● 带宽大小：5Mbit/s ● 购买时长：1个月 ● 购买量：1	$57.00 USD
合计	-	$82.26 USD

版权所有 © 华为技术有限公司

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

版权所有 © 华为技术有限公司

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”

版权所有 © 华为技术有限公司

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

版权所有 © 华为技术有限公司

图 3-7 委托列表

----结束

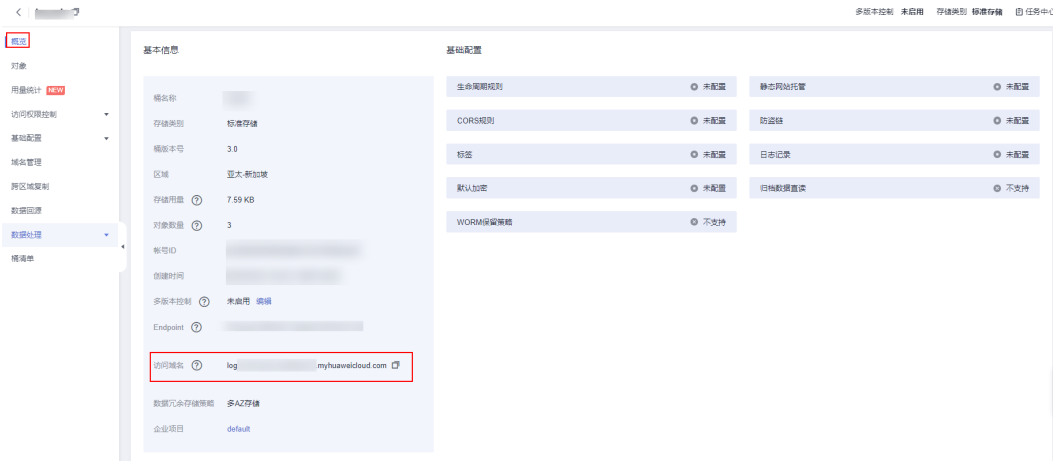
获取 OBS 桶的访问域名

步骤1 登录**对象存储服务 OBS控制台**，单击需要被反向代理的OBS桶名称。

图 3-8 对象存储服务 OBS 控制台

步骤2 选择左侧栏中的“概览”，即可获取访问域名。

图 3-9 获取访问域名



----结束

3.2 快速部署

本章节主要帮助用户快速部署该解决方案。

版权所有 © 华为技术有限公司

表 3-1 参数填写说明

参数名称	类型	是否必填	参数解释	默认值
vpc_name	String	必填	虚拟私有云名称，该模板新建VPC，不允许重名。取值范围：1-55个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	accessing-obs-through-nginx-demo
secgroup_name	Number	必填	安全组名称，该模板新建安全组，如果修改，请参考**安全组规则修改（可选）**。取值范围：1-64个字符，支持数字、字母、中文、_(下划线)、-（中划线）、.（点）。	accessing-obs-through-nginx-demo
ecs_name	String	必填	弹性云服务器名称，命名方式为{ecs_name}_ecs不允许重名。取值范围：1-60个字符，支持字母、数字、中文、下划线（_）、中划线（-）、英文句号（.）。	accessing-obs-through-nginx-demo
ecs_flavor	String	必填	弹性云服务器规格，具体请参考官网**弹性云服务器规格清单**选择。	s6.medium.2
ecs_password	String	必填	弹性云服务器初始密码，创建完成后，请参考**重置ECS实例密码**进行密码修改。取值范围：长度为8-26位，密码至少必须包含大写字母、小写字母、数字和特殊字符（!@$%^-_=+[{}]:,./?）中的三种，密码不能包含用户名或用户名的逆序。管理员账户为root。	空
charging_mode	String	必填	计费模式，默认自动扣费，取值为prePaid（包年包月）或postPaid（按需计费）。	postPaid
charging_unit	String	必填	包年包月。有效值为“year”或“month”。当charging_mode（计费模式）为prePaid时，此选项为必填项。	month
charging_period	String	必填	包年包月时长，当charging_unit取值为“year”，取值范围为1～3;取值为“month”,取值范围为1～9。当charging_mode（计费模式）为prePaid时，此选项为必填项。	1

版权所有 © 华为技术有限公司

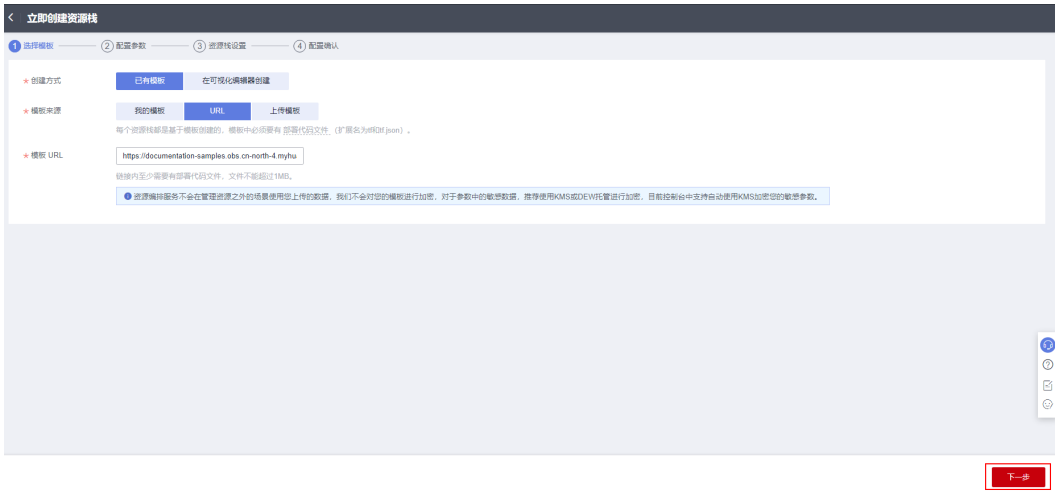
参数名称	类型	是否必填	参数解释	默认值
bandwidth_size	String	必填	弹性公网带宽大小，该模板计费方式为按带宽计费。取值范围：1-2,000Mbit/s。	5
access_domain_name	String	String	被代理的对象存储服务 OBS桶的访问域名，可参考**获取OBS桶的访问域名**获取。	空

步骤1 登录**华为云解决方案实践**，选择“通过Nginx反向代理访问OBS最佳实践”解决方案，数据中心下拉菜单可以选择需要部署的区域，单击“一键部署”，跳转至解决方案创建堆栈界面。

图 3-10 解决方案实施库

步骤2 在选择模板界面中，单击“下一步”。

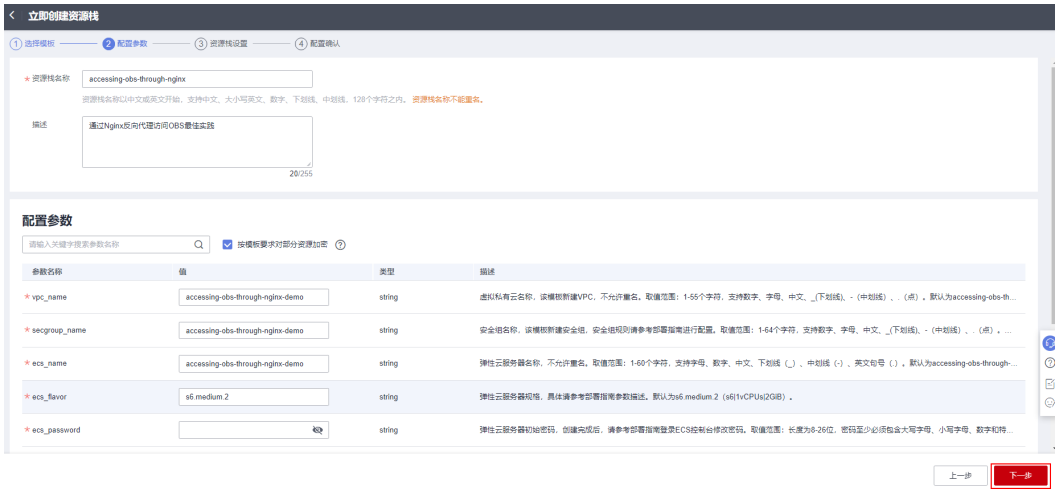
图 3-11 选择模板



版权所有 © 华为技术有限公司

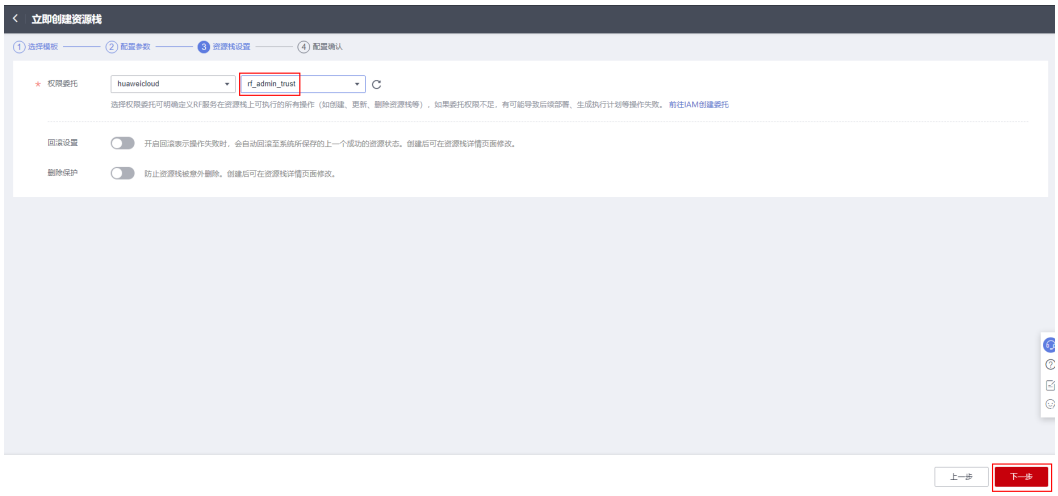
步骤3 在配置参数界面中，自定义填写堆栈名称，根据表3-1填写配置参数信息，单击“下一步”。

图 3-12 配置参数



步骤4 在资源栈设置页面中，权限委托选择“rf_admin_trust"（可选）,单击“下一步”。

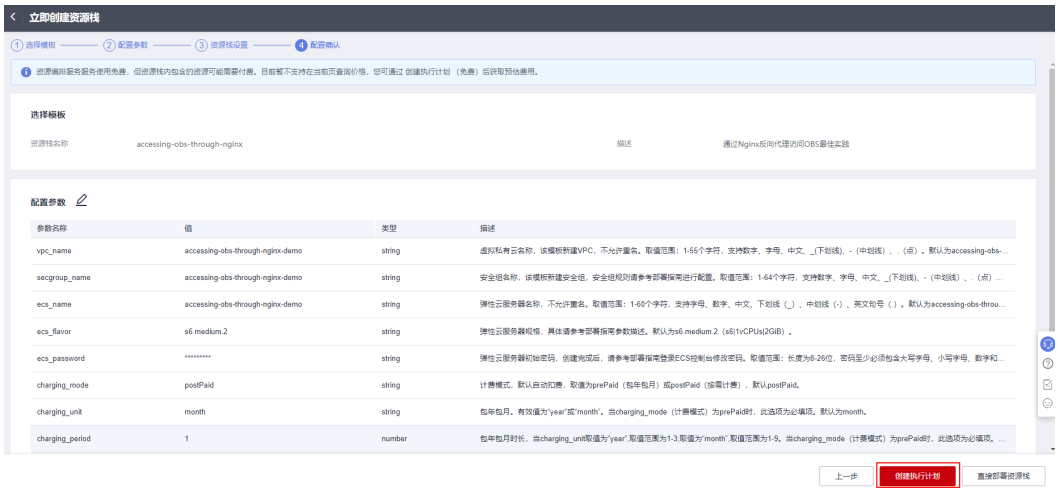
图 3-13 高级配置



步骤5 在配置确认页面中，单击“创建执行计划”。

版权所有 © 华为技术有限公司

图 3-14 配置确认

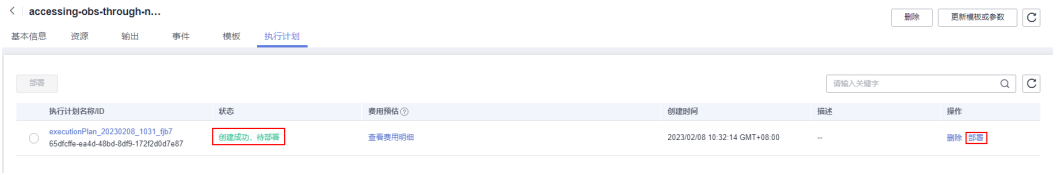


步骤6 在弹出的创建执行计划框中，自定义填写执行计划名称，单击“确定”。

图 3-15 创建执行计划

版权所有 © 华为技术有限公司

图 3-16 执行计划创建成功



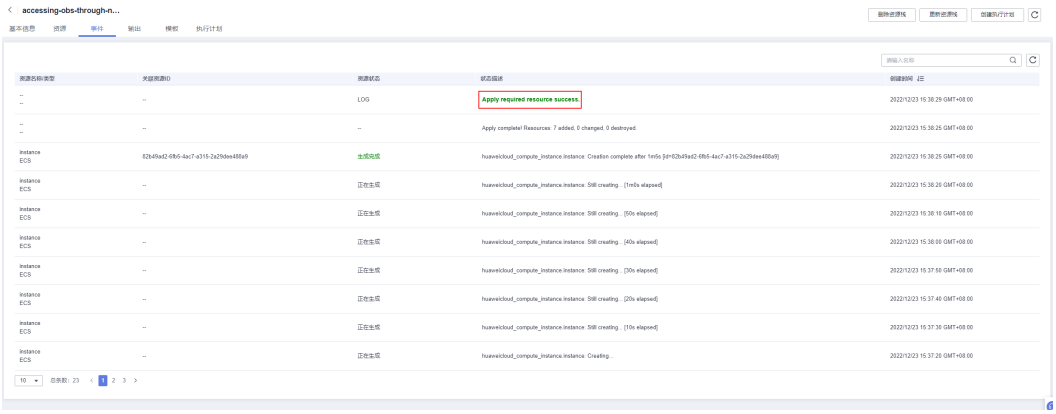
步骤7 单击“部署”，弹出执行计划提示信息，单击“执行”确认执行。

图 3-17 执行计划确认

步骤8 （可选）如果计费模式选择“包年包月”，在余额不充足的情况下（所需总费用请参考**表2-2**）请及时登录**费用中心**，手动完成待支付订单的费用支付。

步骤9 等待解决方案自动部署。部署成功后，单击“事件”，回显结果如下:

图 3-18 资源创建成功



----结束

版权所有 © 华为技术有限公司

3.3 开始使用

安全组规则修改（可选）

安全组实际是网络流量访问策略，包括网络流量入方向规则和出方向规则，通过这些规则为安全组内具有相同保护需求并且相互信任的云服务器、云容器等实例提供安全保护。

如果您的实例关联的安全组策略无法满足使用需求，比如需要添加、修改、删除某个TCP端口，请参考以下内容进行修改。

- 添加安全组规则：根据业务使用需求需要开放某个TCP端口，请参考**添加安全组规则**添加入方向规则，打开指定的TCP端口。
- 修改安全组规则：安全组规则设置不当会造成严重的安全隐患。您可以参考**修改安全组规则**，来修改安全组中不合理的规则，保证云服务器等实例的网络安全。
- 删除安全组规则：当安全组规则入方向、出方向源地址/目的地址有变化时，或者不需要开放某个端口时，您可以参考**删除安全组规则**进行安全组规则删除。

配置 OBS 桶策略（可选）

说明

如果您的OBS桶为公共读，或者访问私有桶内对象时在**URL中携带签名**，则可跳过此步骤。

如果您的OBS桶为私有桶，且不希望使用携带签名的URL访问桶内资源，则建议配置以下桶策略：仅允许Nginx代理服务器的IP地址访问OBS桶。

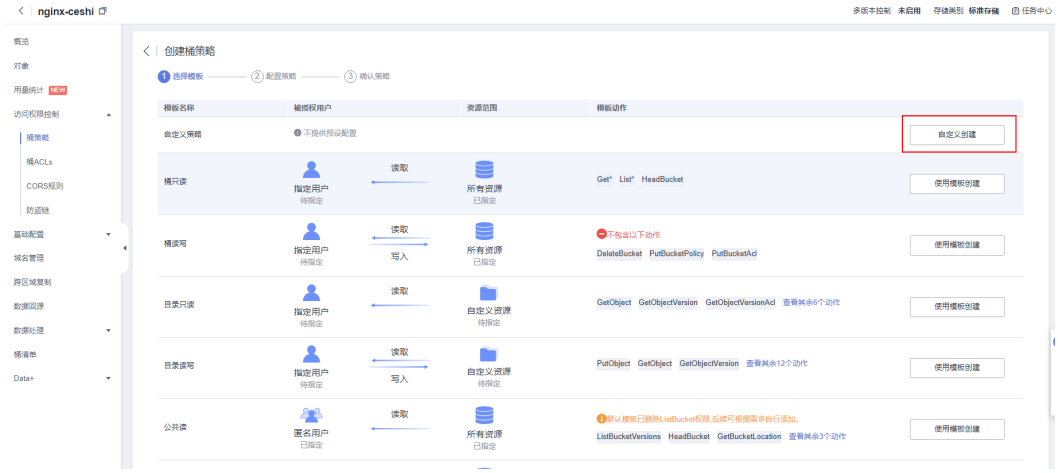
步骤1 登录**对象存储服务 OBS控制台**，在桶列表单击待操作的桶，进入概览页面，单击访问权限控制，选择桶策略。

图 3-19 选择桶策略

步骤2 单击创建，在桶策略模板的第一行，单击右侧的自定义创建。

版权所有 © 华为技术有限公司

图 3-20 自定义创建



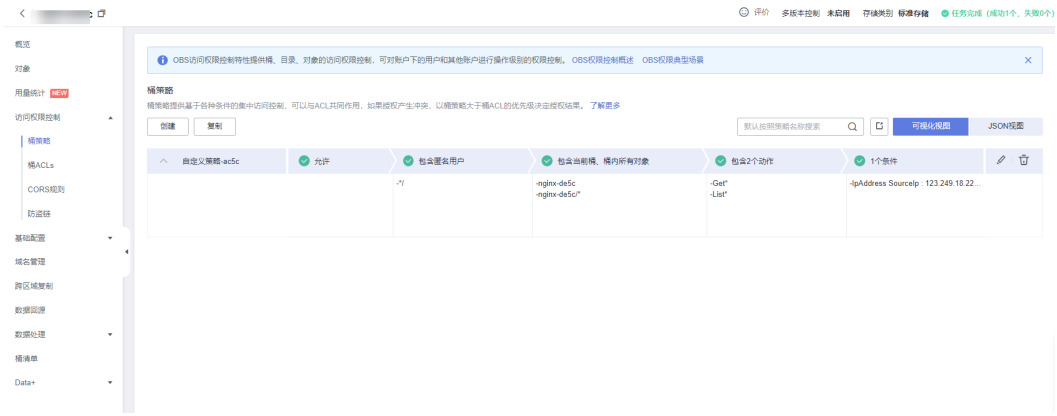
步骤3 配置如下参数，单击右下角配置确认>>创建，完成桶策略创建。如果被代理的桶和ECS实例在同一region下，则配置策略内容中的“条件”取值为100.64.0.0/10,214.0.0.0/7,ECS的私有IP地址。如果被代理的桶和ECS实例不在同一region下，则配置策略内容中的“条件”取值为ECS的弹性公网IP地址。

图 3-21 桶策略参数

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	效果	允许
	被授权用户	• 被授权用户：匿名用户 • 用户策略：包含以上用户
	资源	• 资源范围：同时选择当前桶和桶内对象 • 资源策略：包含以上资源
	动作	• 选择动作：Get*和List* • 操作策略：包含以上动作
	条件	• 条件运算符：IpAddress • 键：SourceIp • 值： ◦ 如果ECS使用公网DNS，取值为：***ECS的弹性公网IP地址*** ◦ 如果ECS使用华为云内网DNS，取值为：**100.64.0.0/10,214.0.0.0/7,*ECS的私有IP地址*** **说明：** 取值需要同时配置三个IP地址（IP地址段），之间用英文逗号（,）隔开。 其中，100网段和214网段为ECS内网访问OBS的网段。

版权所有 © 华为技术有限公司

图 3-22 策略创建成功

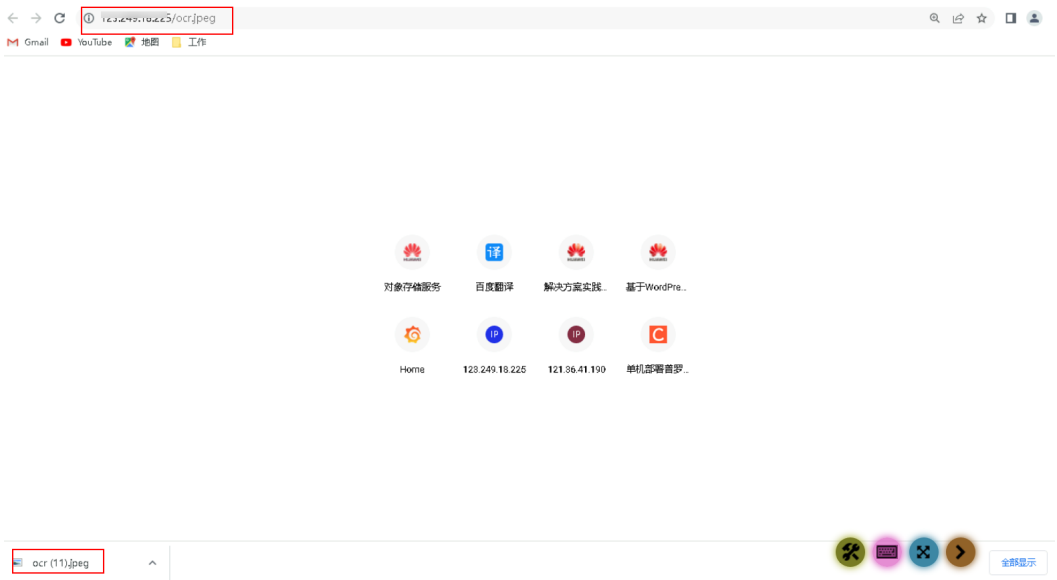


----结束

验证反向代理配置

步骤1 在浏览器使用ECS+对象存储服务 OBS对象名访问资源，即可下载访问的资源。例如http://ECS弹性公网IP地址/对象名。

图 3-23 使用固定 IP 地址访问 OBS 资源



----结束

3.4 快速卸载

步骤1 解决方案部署成功后，单击该方案堆栈后的“删除”。

图 3-24 一键卸载

版权所有 © 华为技术有限公司

步骤2 在弹出的删除堆栈确认框中，输入Delete，单击“确定”，即可卸载解决方案。

图 3-25 删除堆栈确认

----结束

版权所有 © 华为技术有限公司

4 附录

名词解释

基本概念、云服务简介、专有名词解释

- 弹性公网IP EIP：提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟VIP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。
- 虚拟私有云 VPC：是用户在云上申请的隔离的、私密的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性IP搭建业务系统。
- 安全组：安全组是一个逻辑上的分组，为同一个VPC内具有相同安全保护需求并相互信任的弹性云服务器提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当弹性云服务器加入该安全组后，即受到这些访问规则的保护。
- 弹性云服务器 ECS ： 是一种云上可随时自助获取、可弹性伸缩的计算服务，可帮助您打造安全、可靠、灵活、高效的应用环境。

版权所有 © 华为技术有限公司

5 修订记录

发布日期	修订记录
2022-12-30	第一次正式发布。
2023-02-28	修订实施步骤。

版权所有 © 华为技术有限公司