基于CentOS的ECS实例实现OSS反向代理

更新时间：2020-09-21 10:35:48

[**本页目录**](javascript:void(0))

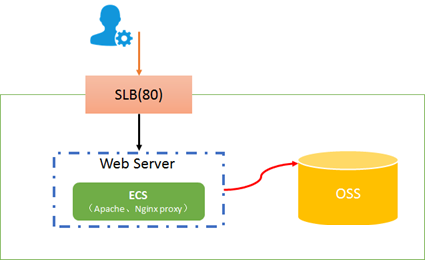
* [背景信息](https://help.aliyun.com/document_detail/107034.html?spm=a2c4g.11186623.2.25.69997148jYtht7#h2-url-1)
* [配置步骤](https://help.aliyun.com/document_detail/107034.html?spm=a2c4g.11186623.2.25.69997148jYtht7#title-nrk-nbq-n2b)
* [更多参考](https://help.aliyun.com/document_detail/107034.html?spm=a2c4g.11186623.2.25.69997148jYtht7#title-zqr-5x6-xp9)

阿里云OSS的存储空间（Bucket）访问地址会随机变换，您可以通过在ECS实例上配置OSS的反向代理，实现通过固定IP地址访问OSS的存储空间。

**背景信息**

阿里云OSS通过Restful API方式对外提供服务。最终用户通过OSS默认域名或者绑定的自定义域名方式访问，但是在某些场景下，用户需要通过固定的IP地址访问OSS：

* 某些企业由于安全机制，需要在出口防火墙配置策略，以限制内部员工和业务系统只能访问指定的公网IP，但是OSS的Bucket访问IP会随机变换，导致需要经常修改防火墙策略。
* 金融云环境下，因金融云网络架构限制，金融云内网类型的Bucket只能在金融云内部访问，不支持在互联网上直接访问金融云内网类型Bucket。

以上问题可以通过在ECS实例上搭建反向代理的方式访问OSS。[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/1554449951/p38572.png)

**配置步骤**

1. 创建一个和对应Bucket相同地域的CentOS系统的ECS实例。

本文演示系统为CentOS 7.6 64位系统。创建过程请参见[创建ECS实例](https://help.aliyun.com/document_detail/25424.html#task-zjx-p1f-5db)。

1. 使用root用户登录ECS实例并安装Nginx。

root@**test**:~# yum install -y nginx

**说明** Nginx默认安装位置：

/usr/sbin/nginx 主程序

/etc/nginx 存放配置文件

/usr/**share**/nginx 存放静态文件

/var/**log**/nginx 存放日志

1. 打开Nginx配置文件。

root@**test**:~# vi /etc/nginx/nginx.conf

1. 在config文件中的http模块中，修改配置如下。
2. **server** {
3. **listen** 80 default\_server;
4. **listen** [::]:80 default\_server;
5. server\_name 47.\*\*.\*\*.43;
6. root /usr/**share**/nginx/html;
7. # **Load** **configuration** files **for** the **default** **server** block.
8. **include** /etc/nginx/**default**.d/\*.conf;
9. location / {
10. proxy\_pass https://bucketname.oss-cn-beijing-internal.aliyuncs.com;
11. proxy\_set\_header Host $host;

}

* + **server\_name**：对外提供反向代理服务的IP，即ECS实例的外网地址。
  + **proxy\_pass**：填写跳转的域名。
    - 当ECS实例与Bucket在同一地域时，填写目标Bucket的内网访问域名。访问域名介绍请参见[OSS访问域名使用规则](https://help.aliyun.com/document_detail/31834.html#concept-hh2-4tv-tdb)。
    - 当ECS实例与Bucket不在同一地域时，填写目标Bucket的外网访问域名。
    - 因OSS的安全设置，当使用默认域名通过浏览器访问OSS中的图片或网页文件时，会直接下载。所以，若您的用户需通过浏览器预览Bucket中的图片或网页文件，需为Bucket绑定自定义域名，并在此项中添加已绑定的域名。绑定自定义域名操作请参见[绑定自定义域名](https://help.aliyun.com/document_detail/31902.html#concept-ozw-m2r-5fb)。
  + **proxy\_set\_header Host $host**：添加此项时，Nginx会在向OSS请求的时候，将host替换为ECS的访问地址。遇到以下情况时，您需要添加此项。
    - 遇到签名错误问题。
    - 如果您的域名已解析到ECS实例的外网上，且您的用户需要通过浏览器预览Bucket中的图片或网页文件。您可以将您的域名绑定到ECS实例代理的Bucket上，不配置CNAME。这种情况下，**proxy\_pass**项可直接配置Bucket的内网或外网访问地址。绑定自定义域名操作请参见[绑定自定义域名](https://help.aliyun.com/document_detail/31902.html#concept-ozw-m2r-5fb)。

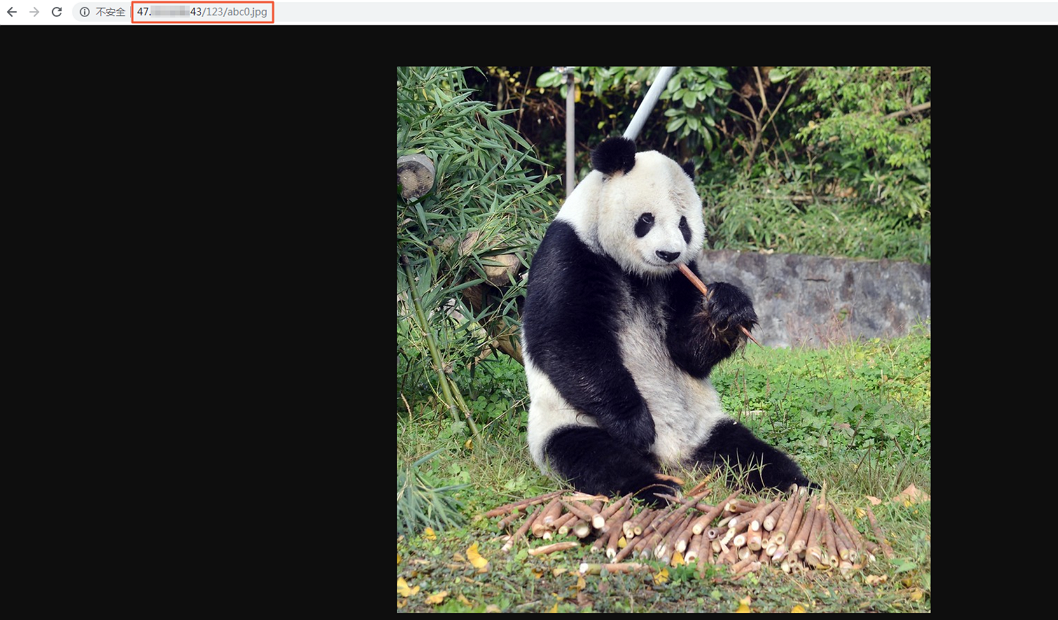
**说明** 本文为演示环境，实际环境中，为了您的数据安全，建议配置https模块，配置方法请参见[反向代理配置](https://help.aliyun.com/knowledge_detail/39544.html)。

1. 进入Nginx主程序文件夹，启动Nginx。
2. root@**test**:~# cd /usr/sbin/

root@**test**:~# ./nginx

1. 开放ECS实例的TCP 80端口。

Nginx默认使用80端口，需在ECS的安全组配置中，允许用户访问TCP 80端口。配置方式请参见[添加安全组规则](https://help.aliyun.com/document_detail/25471.html#concept-sm5-2wz-xdb)。

1. 测试使用ECS外网地址加文件访问路径访问OSS资源。[](http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/zh-CN/1554449951/p38588.png)