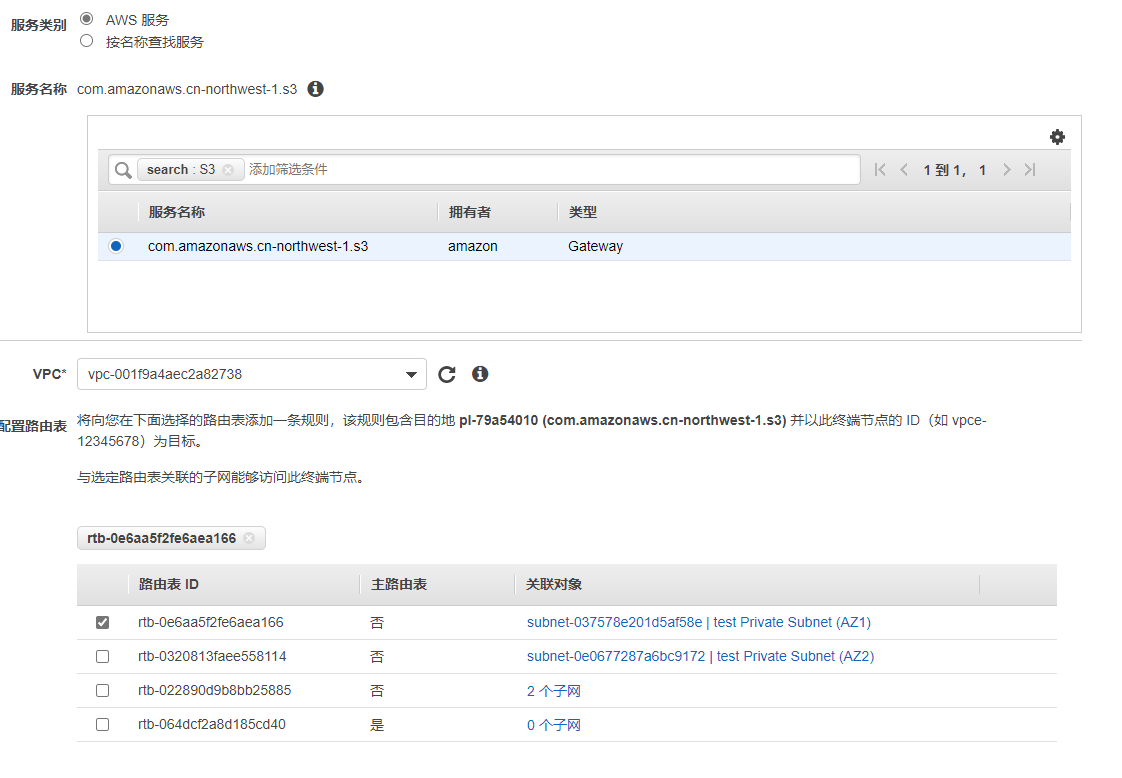
1.创建一个有公有子网和私有子网的VPC和S3桶，S3桶阻止公共访问



2.为私有子网1创建连接S3的终端节点

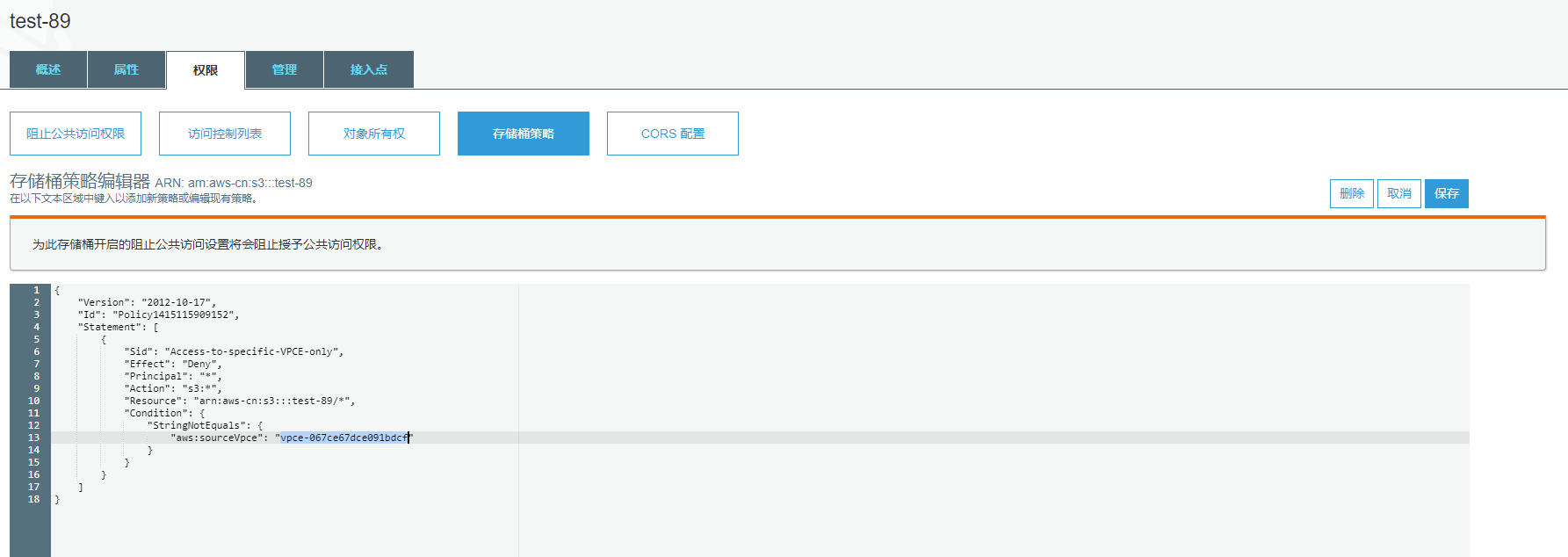


3.编辑终端节点策略，蓝色高亮处填写创建的S3桶的ARN，此举确保权限最小化



策略示例<https://docs.amazonaws.cn/vpc/latest/userguide/vpc-endpoints-s3.html>

4.编辑S3桶策略，使得创建完的终端节点可以访问S3



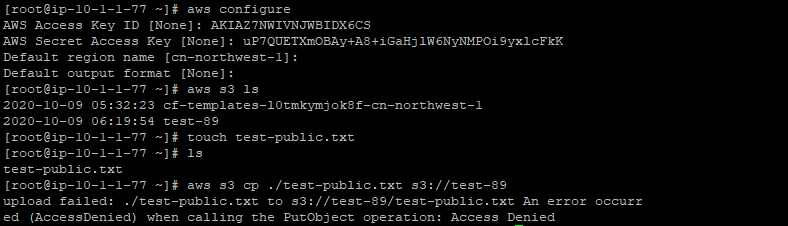
5.验证

创建三台实例，配置aksk，分别放在公有子网1(没有vpc endpoint)，私有子网1（附加了vpc endpoint），私有子网2(没有vpc endpoint),然后创建文件尝试向S3上传

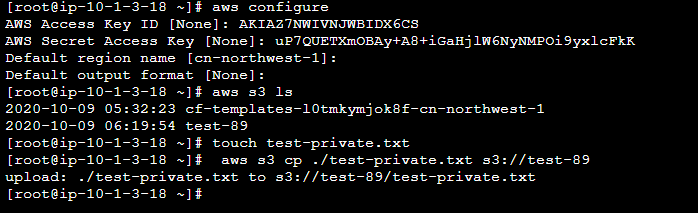


上传结果

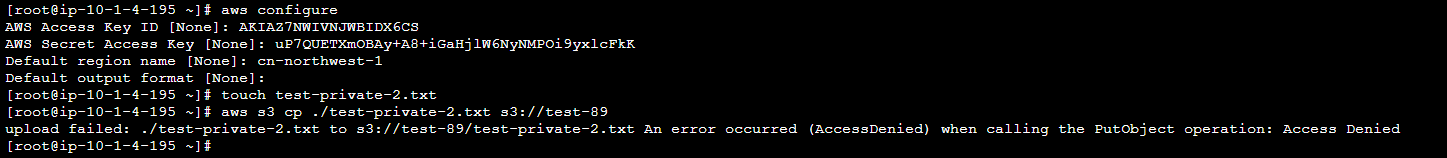
Public Sub1 instance



Private Sub1 instance

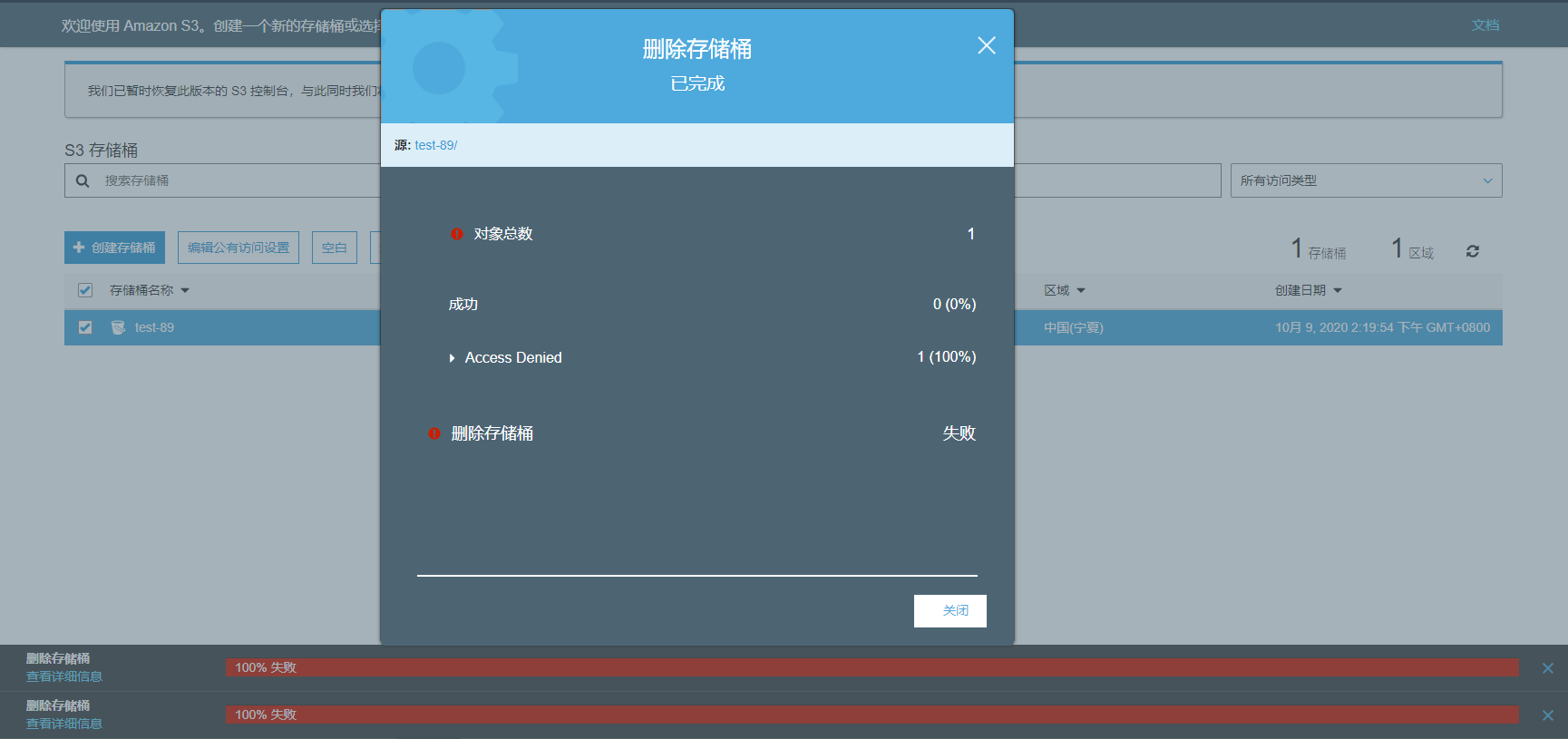


Private Sub2 instance



6.清除资源

直接在控制台清除资源会发生错误



原因是我们设置了存储桶权限，而上传的测试文件我们在控制台没有权限删除

因此需要使用Private Sub1 instance来先删除之前上传的文件



随后可以在控制台删除剩余资源了