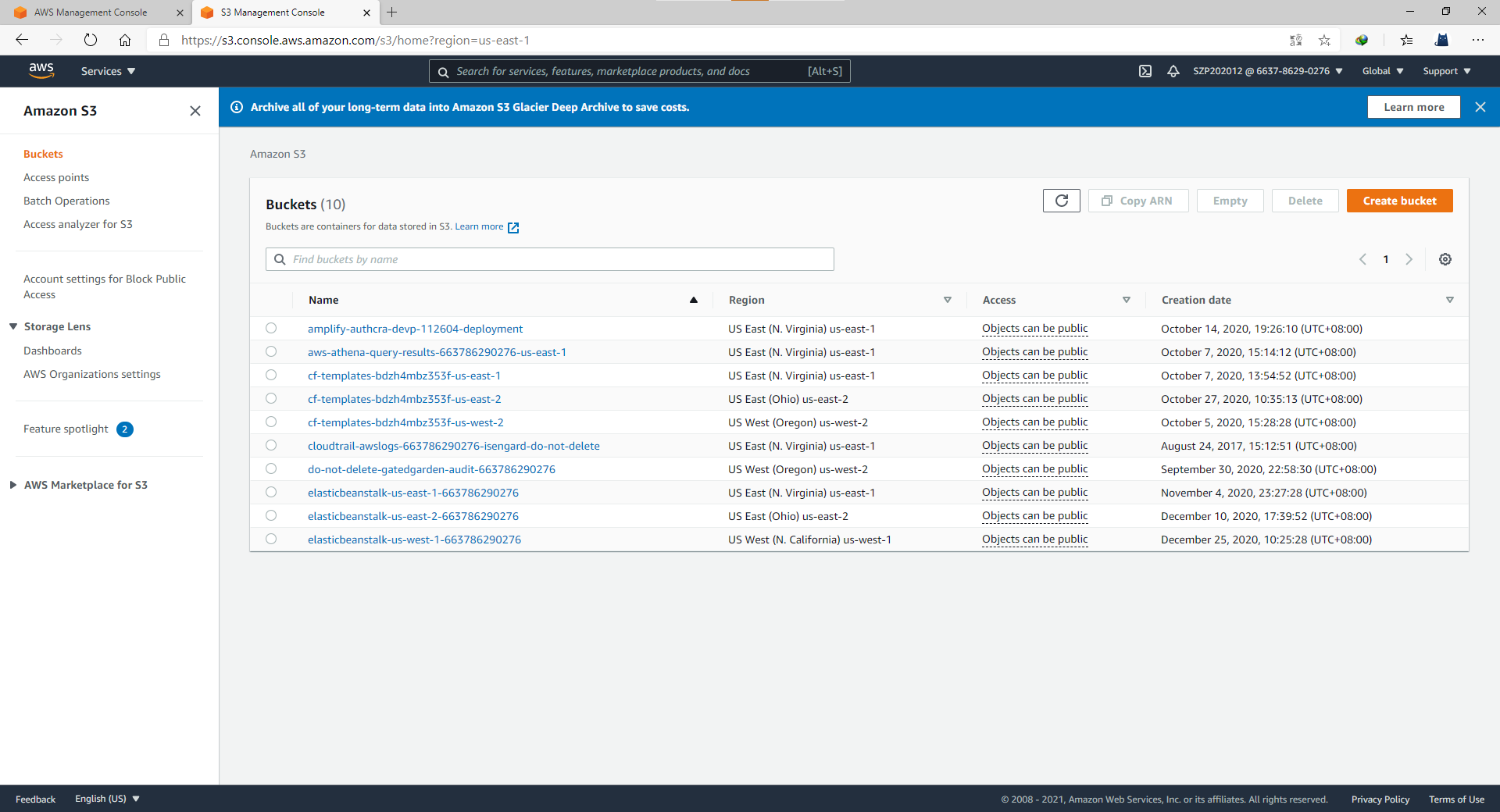
Amazon Simple Storage Service

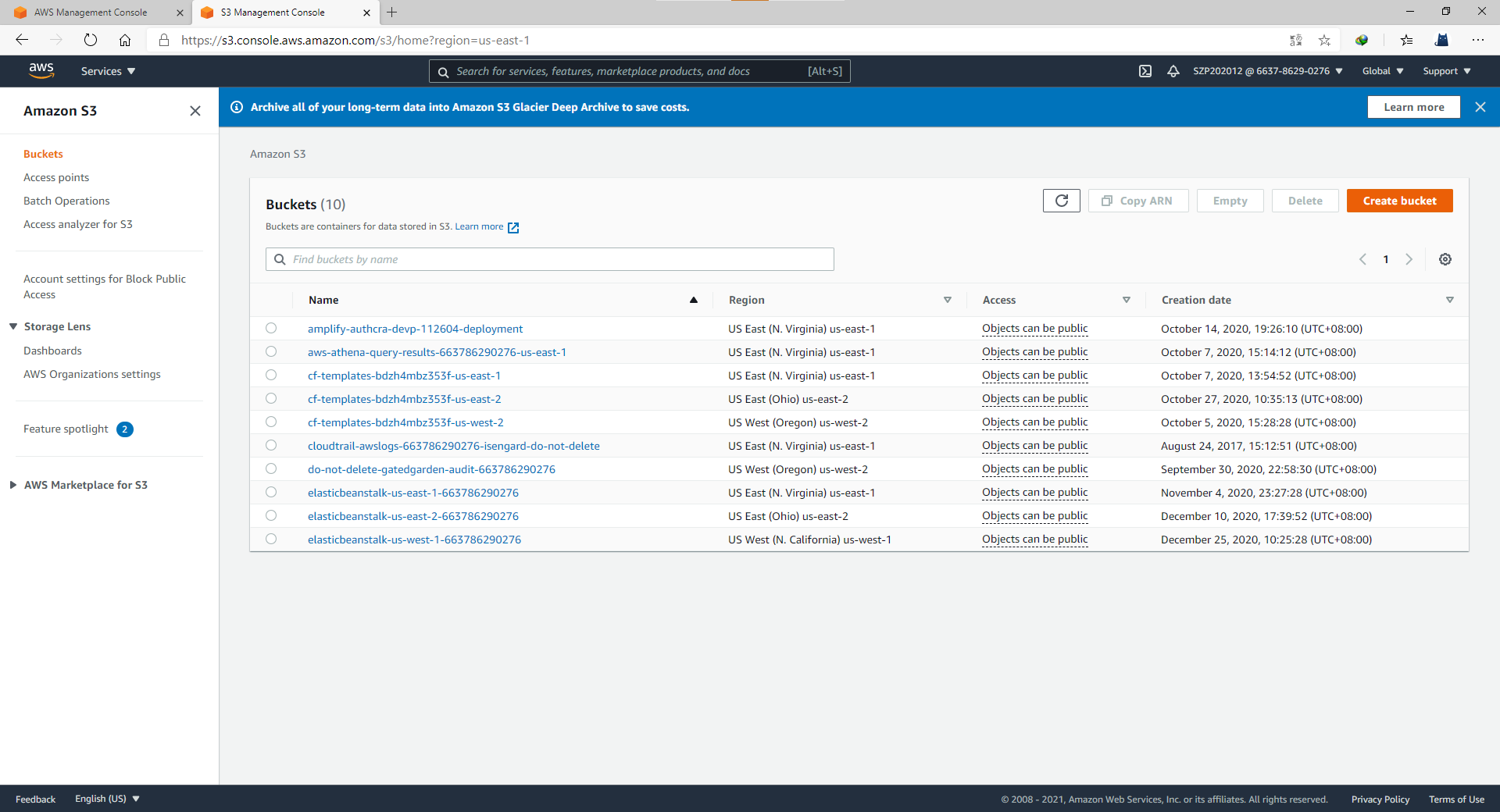
什么是Amazon S3

Amazon Simple Storage Service (Amazon S3) 是一项面向 Internet 的存储服务。您可以通过 Amazon S3 随时在 Web 上的任何位置存储和检索的任意大小的数据。您可以通过 AWS 管理控制台这一简单直观的 Web 界面来完成这些任务。

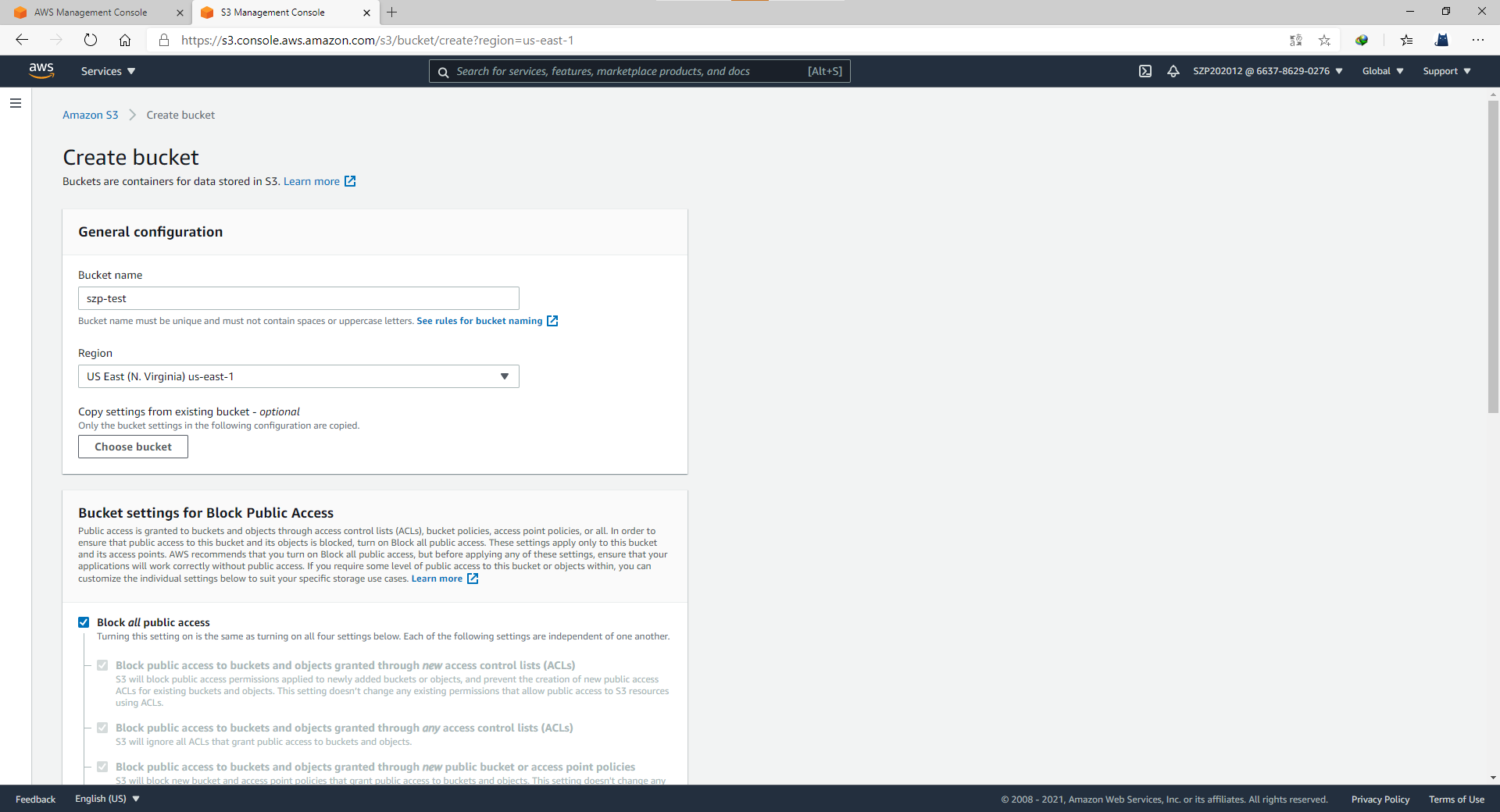


实验：创建一个S3存储桶

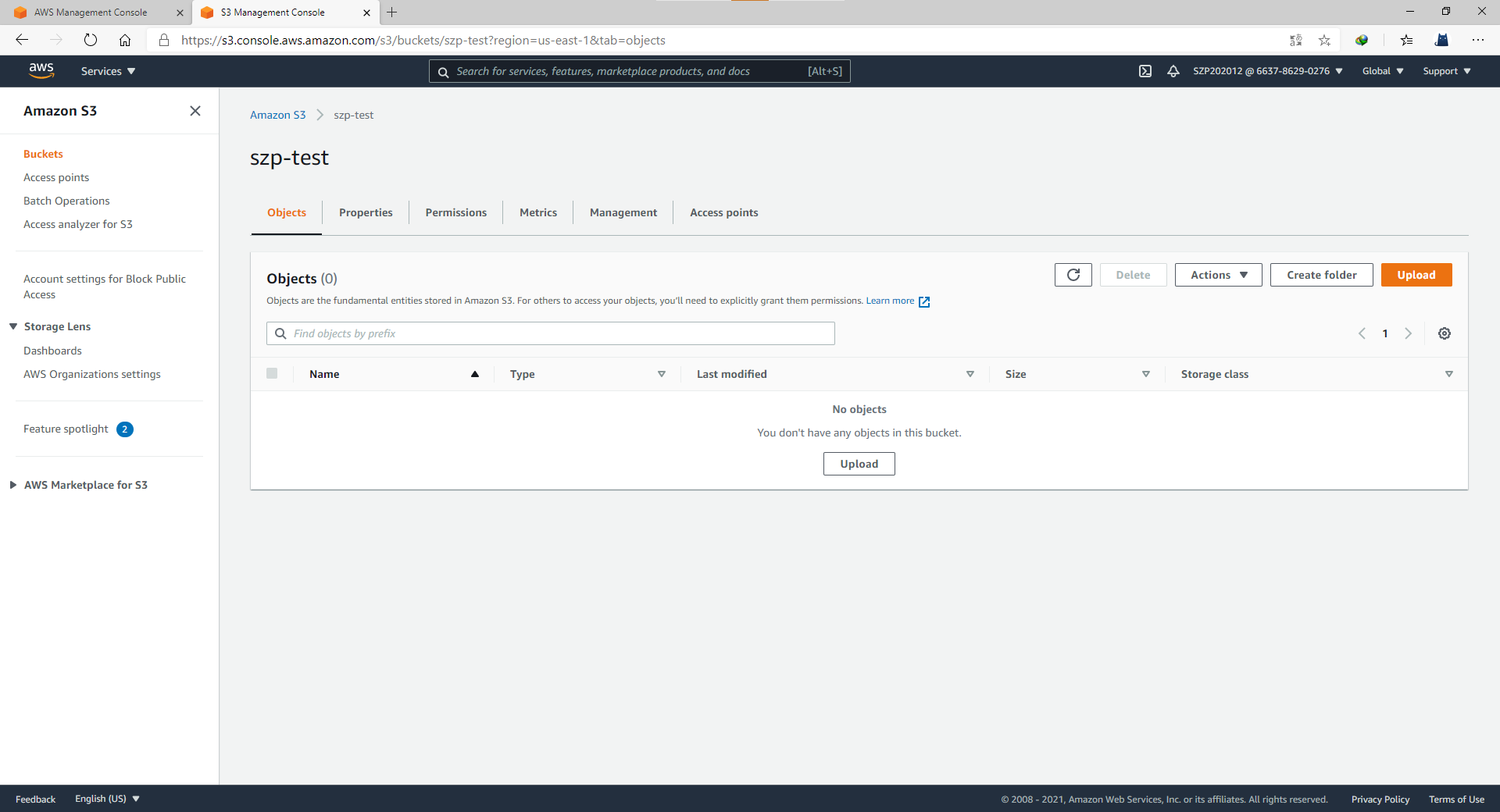
1. 点击Create Bucket



1. 输入存储桶的名字，存储桶的名字必须唯一

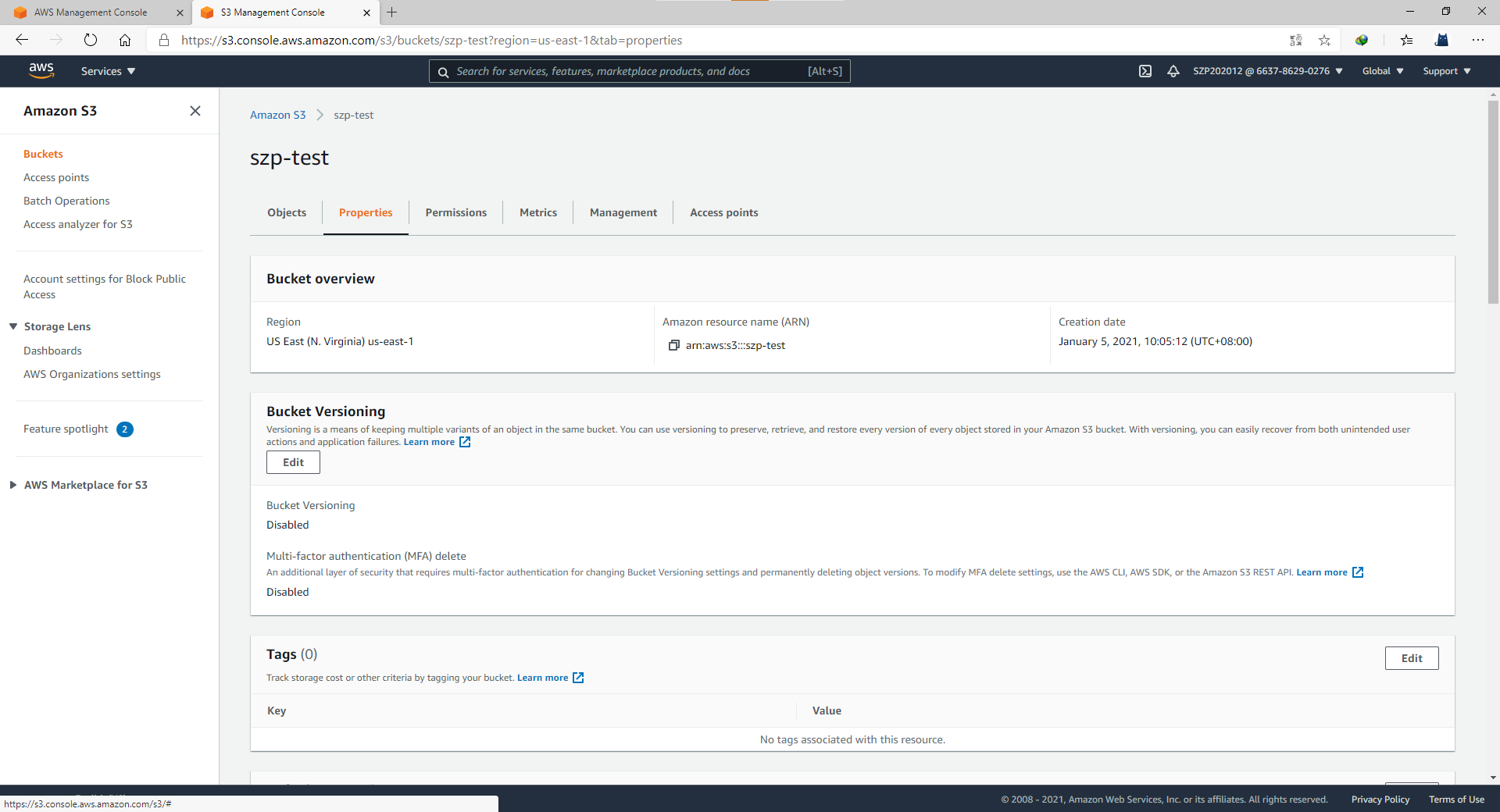


1. 存储桶就算创建成功了，尝试上传一个文件吧

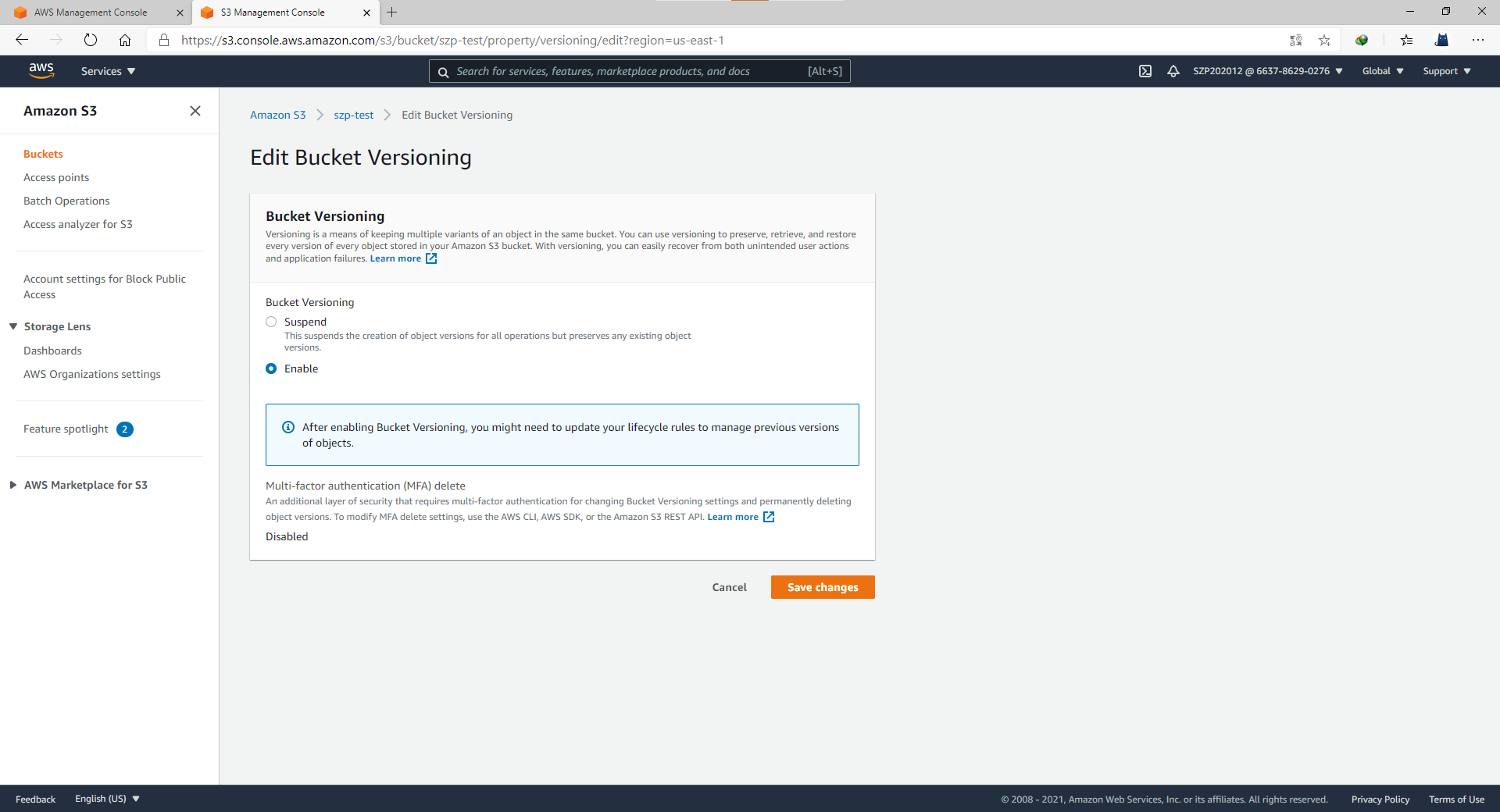


版本控制

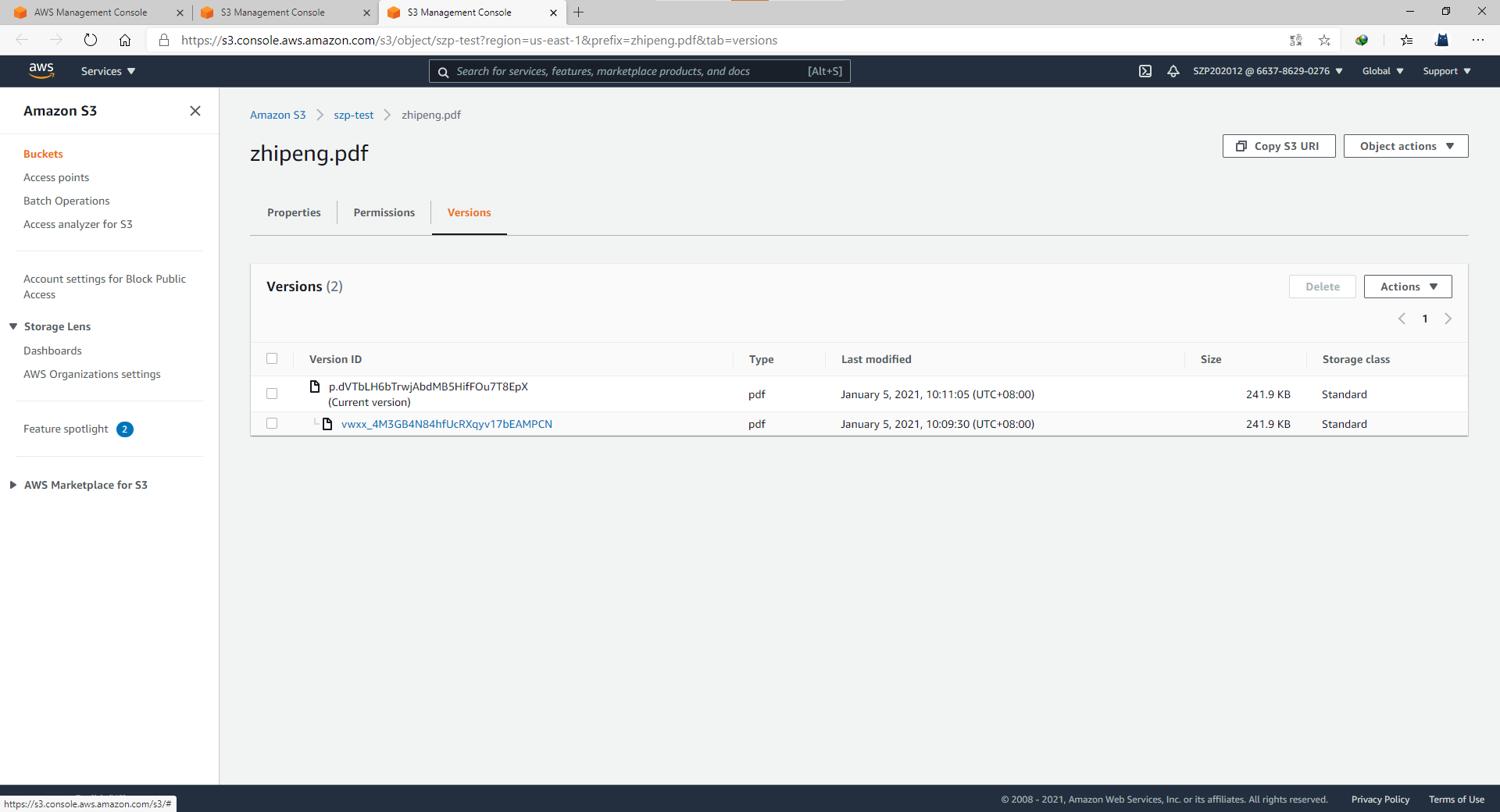
版本控制是在相同的存储桶中保留对象的多个变量的方法。对于 Amazon S3 桶中存储的每个对象，您可以使用版本控制功能来保存、检索和还原它们的各个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。当您为存储桶启用版本控制时，如果 Amazon S3 同时收到针对同一对象的多个写入请求，它会存储所有对象。



打开Bucket Versioning



点击上传的文件详情，有一个Versions选项，就会发现根据上传次数会有不同的版本了



托管静态网站

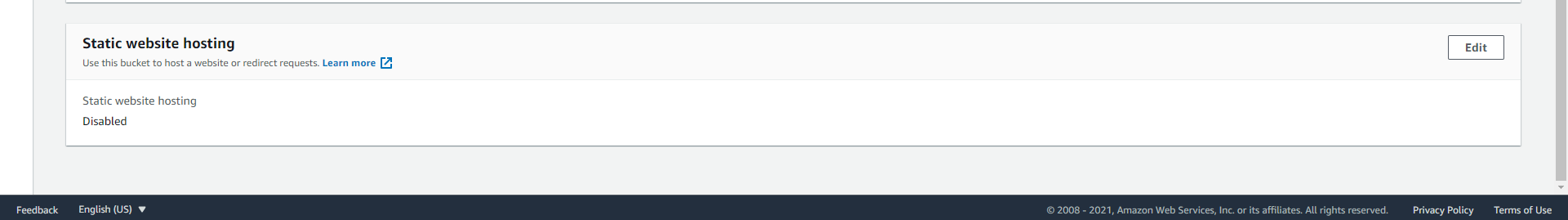
您可以使用 Amazon S3 托管静态网站。在静态网站上，单独的网页包含静态内容。它们也可能包含客户端脚本。

相比之下，动态网站 依赖服务器端处理，包括服务器端脚本（如 PHP、JSP 或 ASP.NET）。Amazon S3 不支持服务器端脚本编写，但 AWS 具有其他用于托管动态网站的资源。要了解有关 AWS 上的网站托管的更多信息，请参阅 Web 托管。

要为静态网站托管配置存储桶，您可以使用 AWS 管理控制台而无需编写任何代码。您还可以使用 AWS 开发工具包，以编程方式创建、更新和删除网站配置。开发工具包围绕 Amazon S3 REST API 提供封装类。如果应用程序需要它，可以直接从应用程序发送 REST API 请求。

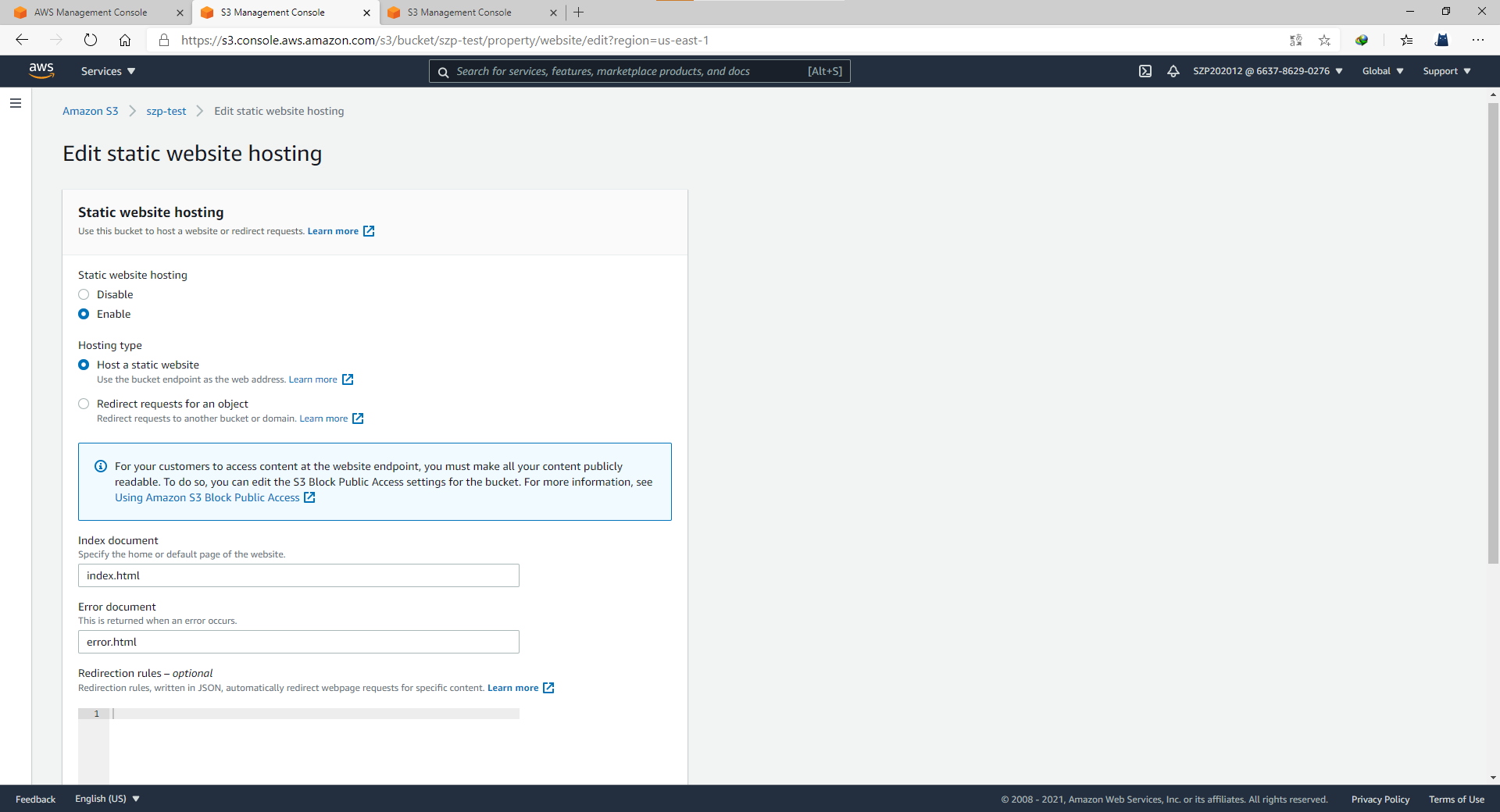
要在 Amazon S3上托管静态网站，您需要为网站托管配置 Amazon S3 存储桶，然后将网站内容上传到存储桶。将存储桶配置为静态网站时，您必须启用静态网站托管、设置权限并创建和添加索引文档。根据您的网站要求，您还可以配置重定向、Web 流量日志记录和自定义错误文档。

将存储桶配置为静态网站后，您可以通过存储桶的 AWS 区域特定的 Amazon S3 网站终端节点访问存储桶。



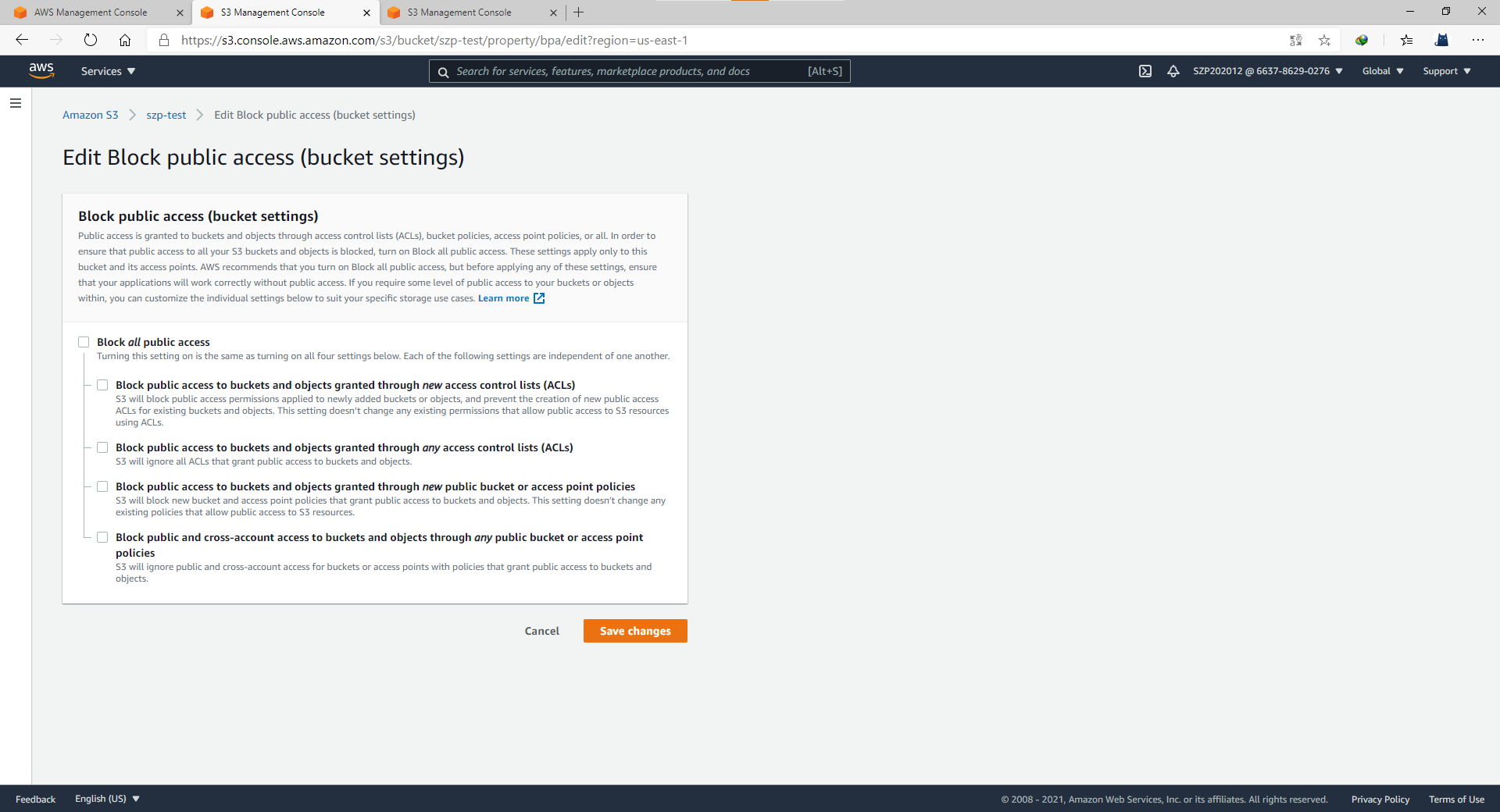
实验：静态网站托管

1. 开启静态网站托管



1. 编辑阻止公有访问设置

点击Permission->Block public access (bucket settings)->Edit，关闭所有Block权限



1. 添加可使您的存储桶内容公开可用的存储桶策略

选择Permission->Bucket policy->Edit

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "PublicReadGetObject",

"Effect": "Allow",

"Principal": "\*",

"Action": [

"s3:GetObject"

],

"Resource": [

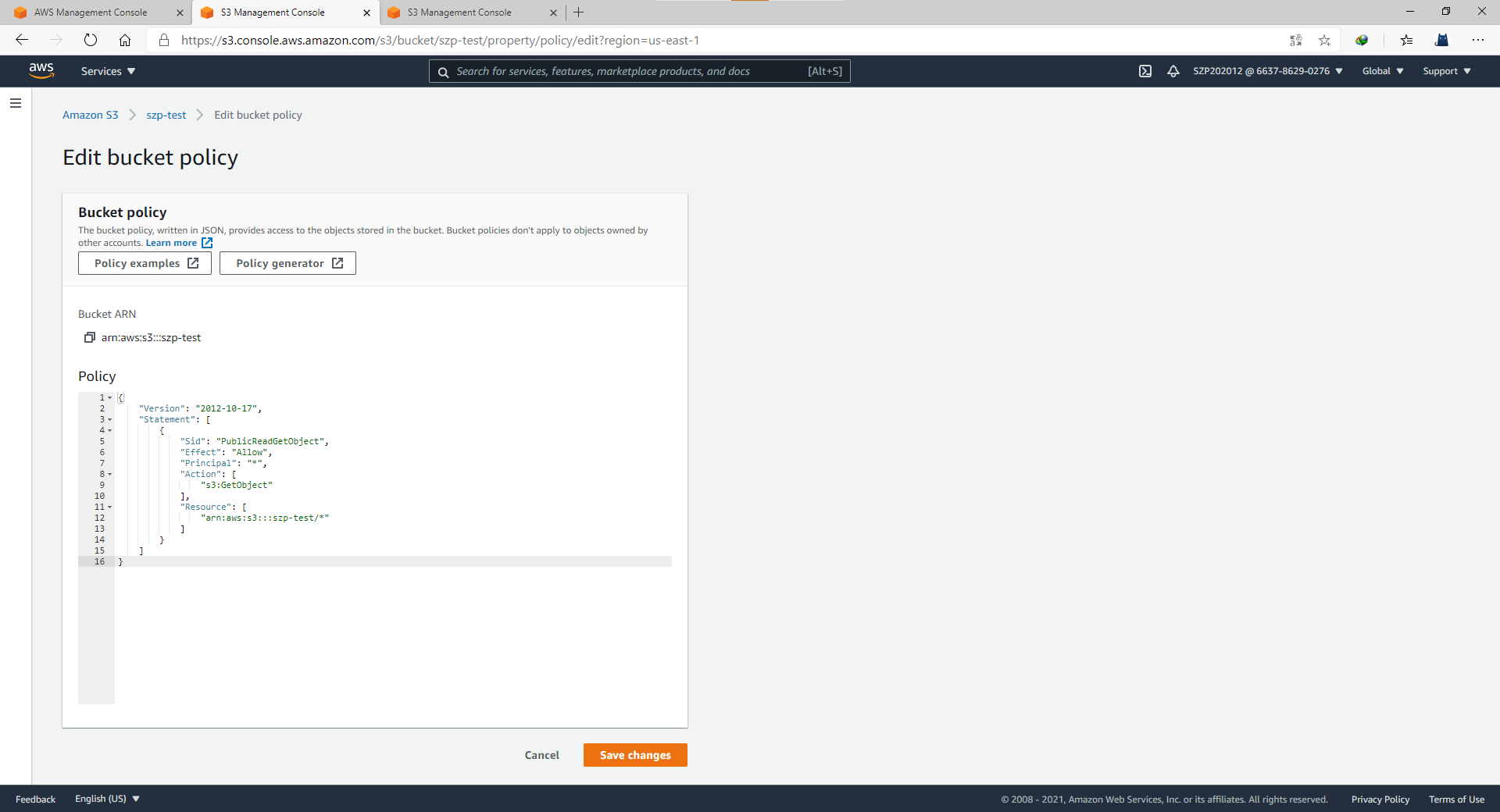
"arn:aws:s3:::<your S3 bucket name>/\*"

]

}

]

}



1. 编写一个index.html文件并上传

<html xmlns="http://www.w3.org/1999/xhtml" >

<head>

<title>My Website Home Page</title>

</head>

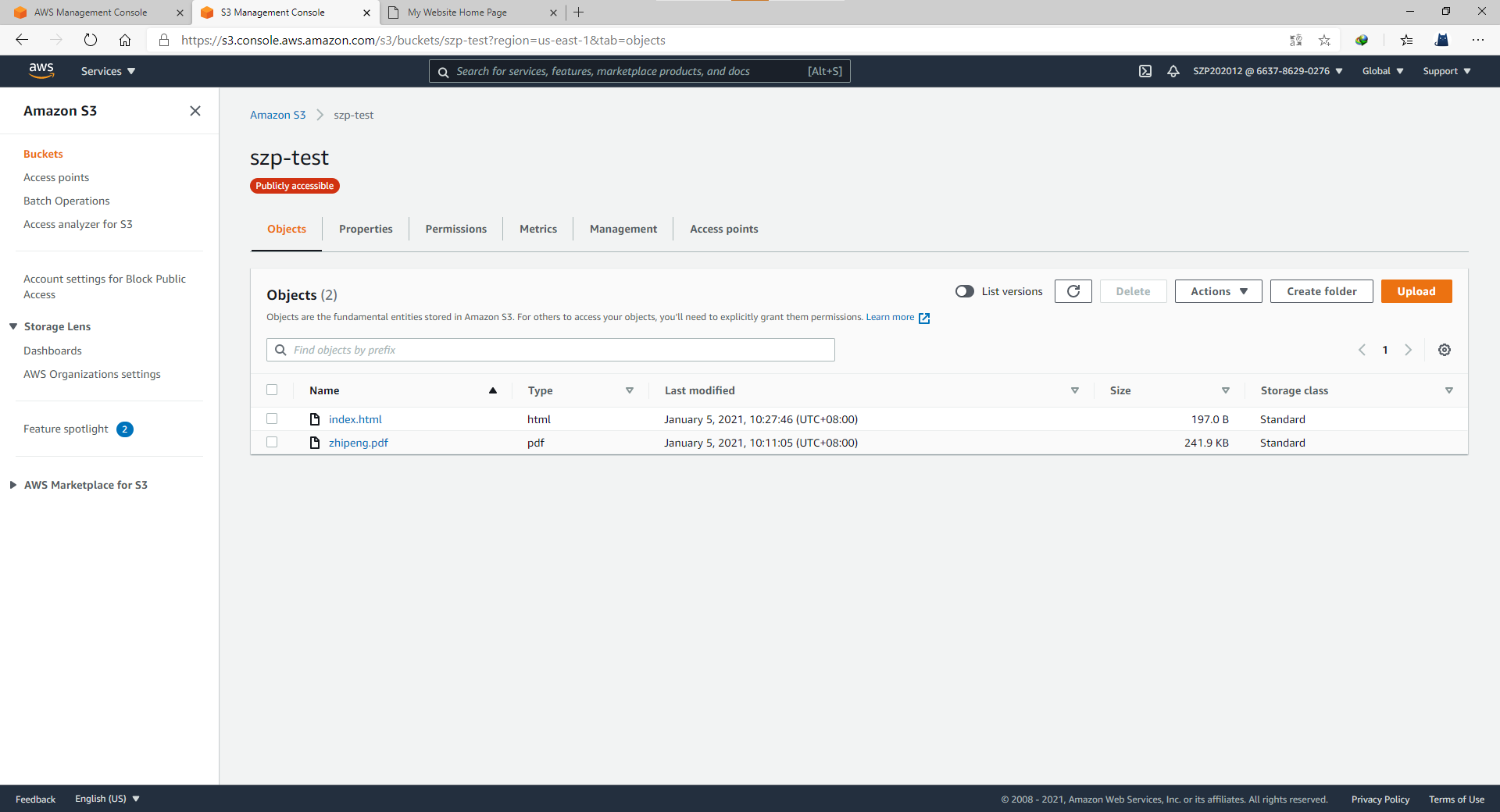
<body>

<h1>Welcome to my website</h1>

<p>Now hosted on Amazon S3!</p>

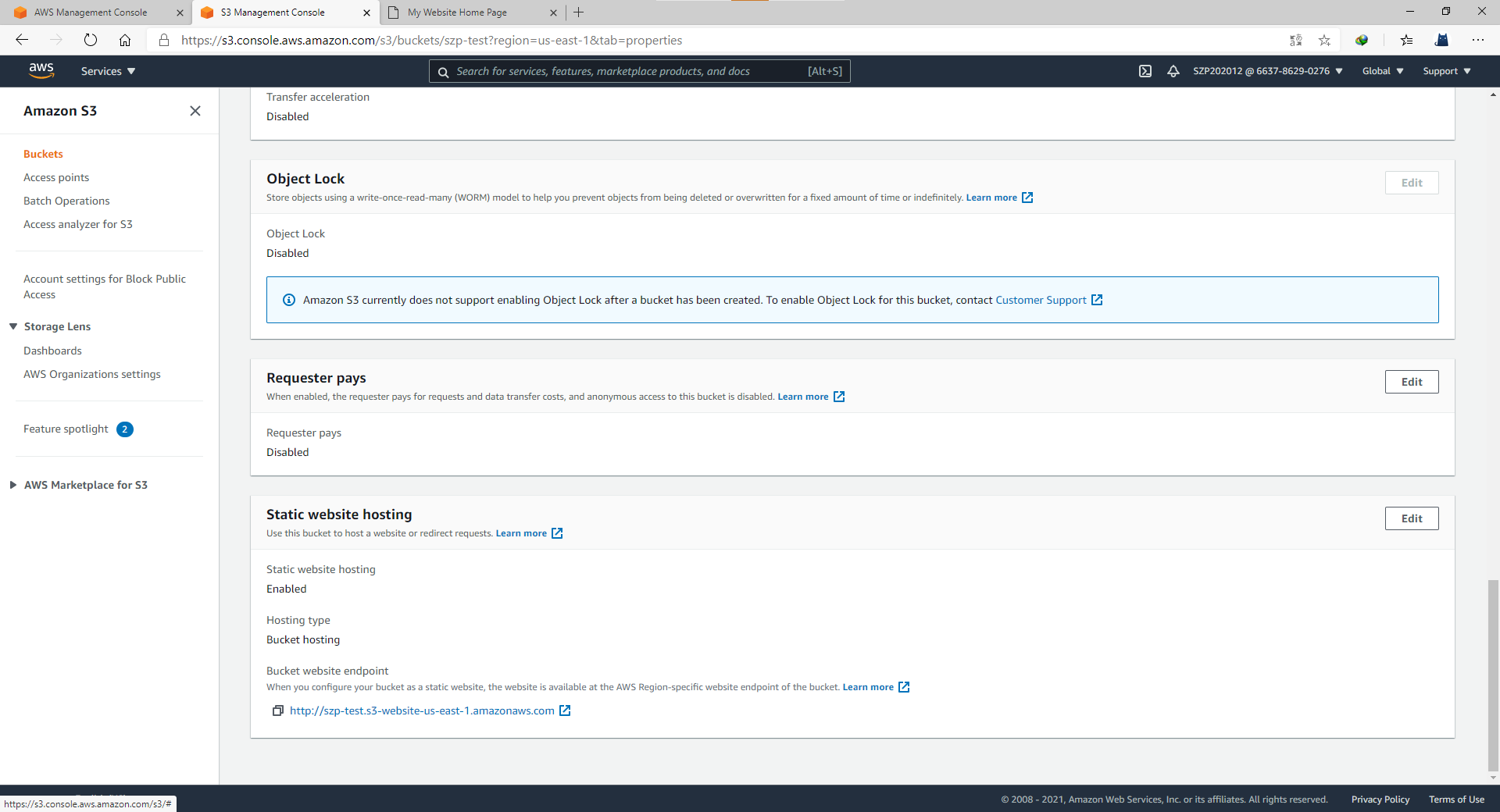
</body>

</html>

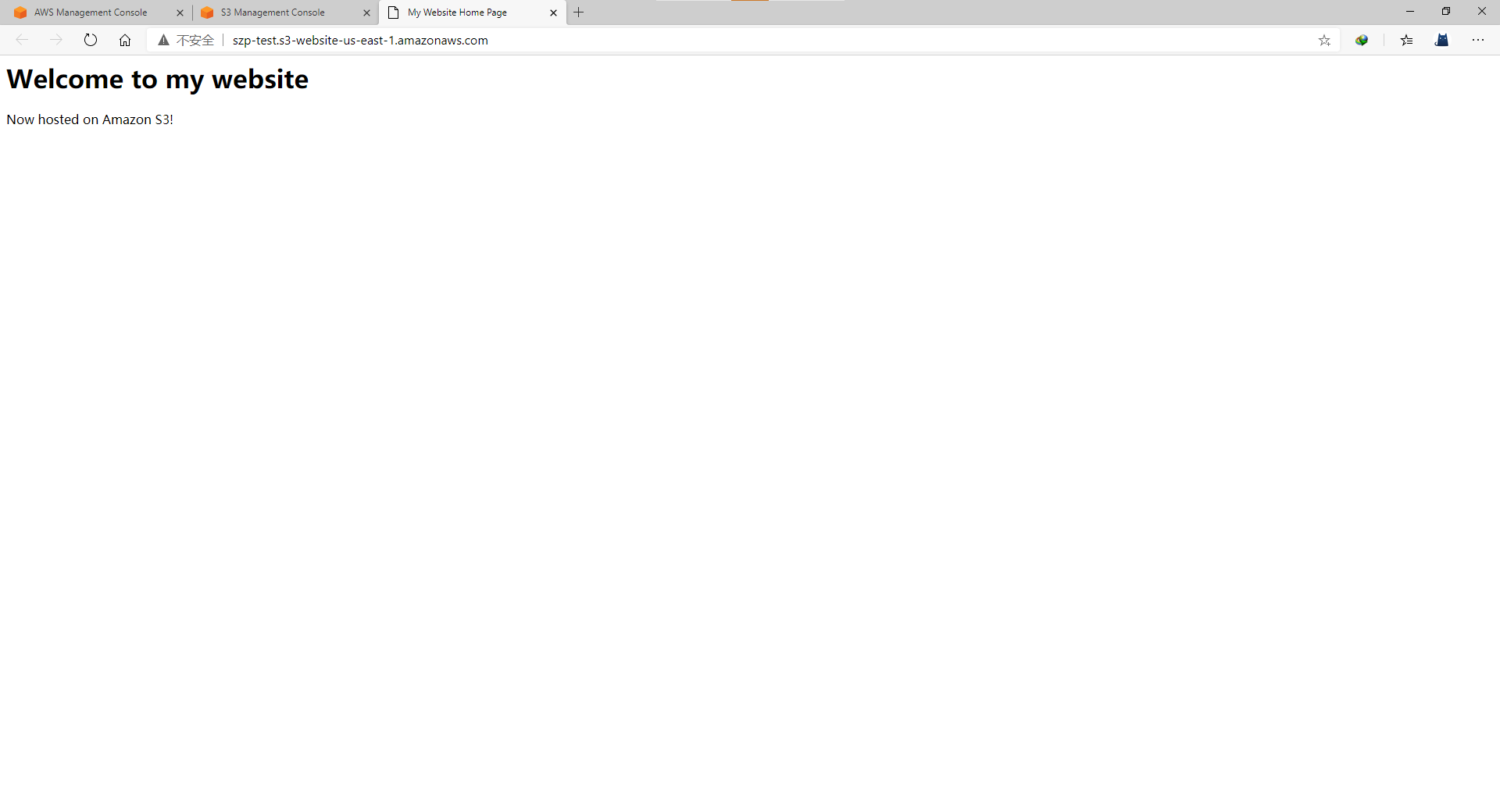


1. 访问终端节点

Static website hosting选项下有个Endpoint，点击即可访问



部署成功，恭喜！（做实验使用了国际版AWS账号和资源，所以访问这个节点时需要翻墙）



S3的权限

存储桶允许公开访问是一件很危险的事，严重违反了安全策略。所以对于S3要尽可能遵循Amazon S3 预防性安全最佳实践

* 确保您的 Amazon S3 存储桶使用正确的策略且不可公有访问。
* 实现最低权限访问
* 对需要 Amazon S3 访问权限的应用程序和 AWS 服务使用 IAM 角色。
* 考虑静态数据加密
* 启用版本控制
* 考虑使用 VPC 终端节点进行 Amazon S3 访问