Amazon-s3 (Simple Storage Service)

2015

Yu-Tsuen Lin

Learning object

1. Create an Amazon S3 bucket and manage properties. (P5-P9)
2. Upload objects and manage object-level permissions.

   Access objects from a web browser. (P10-P11)
3. Create folders and apply bucket-wide security with a bucket policy. (P12-P17)
4. Using API to operate s3.   (P18-P23)

What service to use ?

- Amazon Simple Storage Service (Amazon S3)-

  is a scalable object storage service designed for the Internet.

Pricing

- Storage Pricing

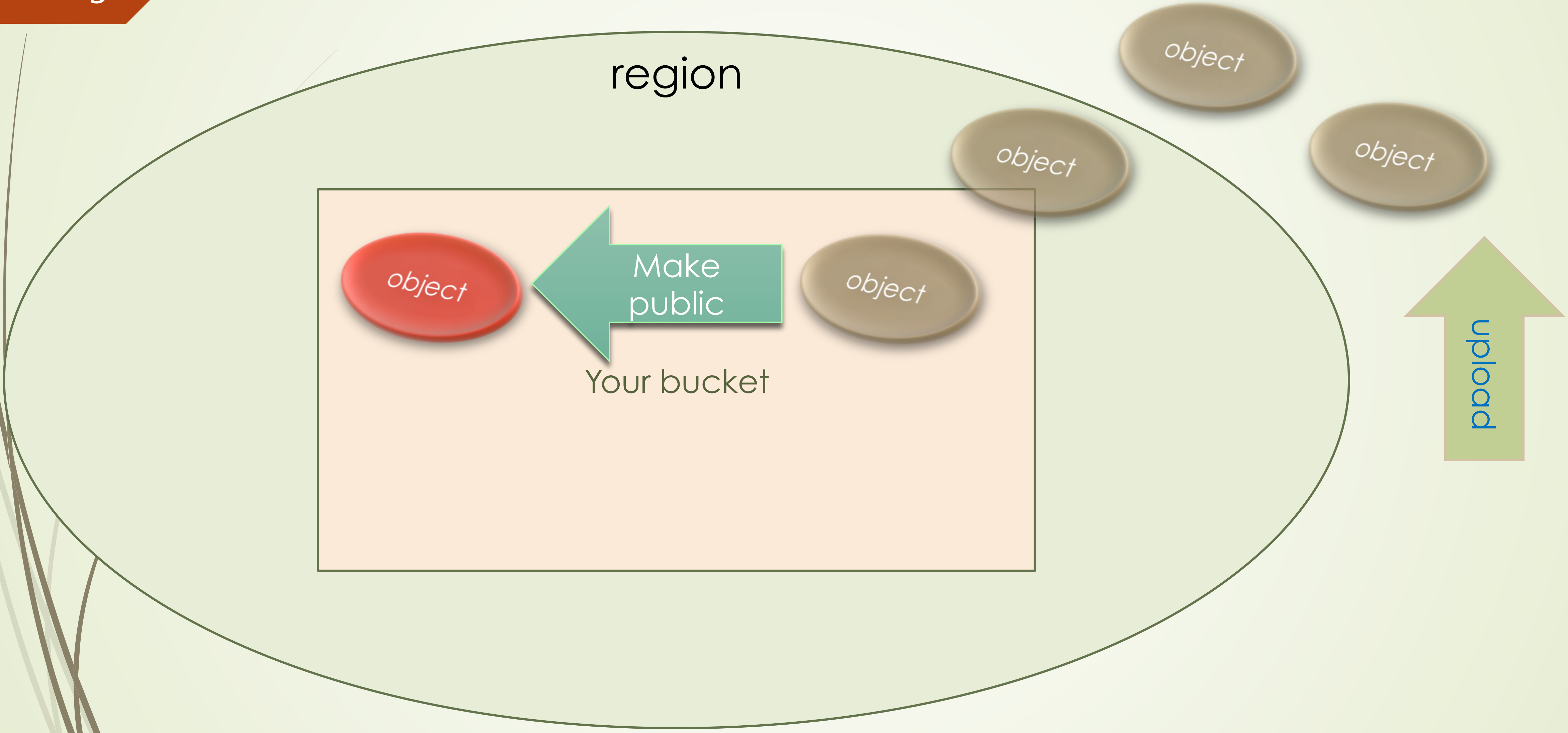
E.g.: $0.0300 per GB

- Request Pricing

E.g.: PUT, COPY, POST, or LIST Requests ,$0.005 per 1,000 requests

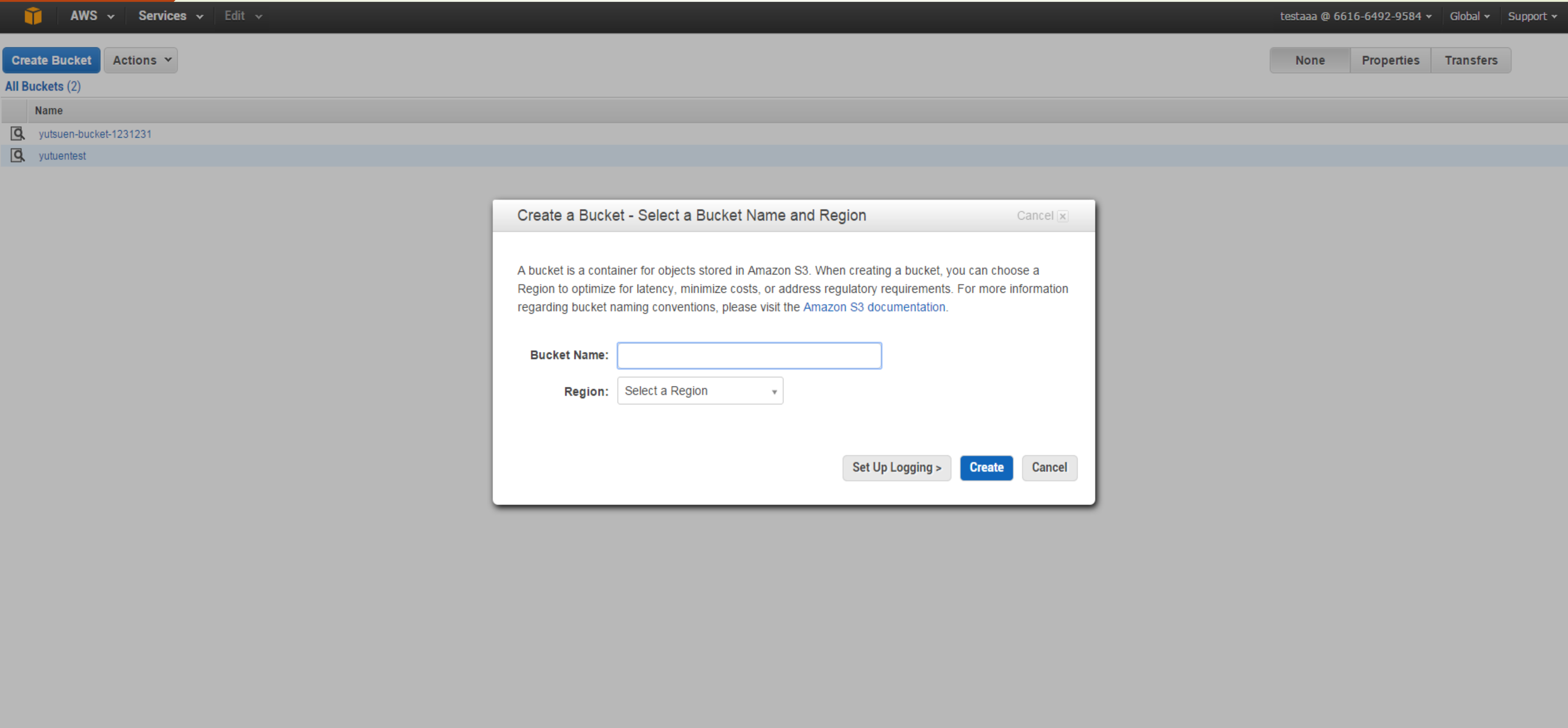
- Data Transfer Pricing

E.g.: Data Transfer OUT From Amazon S3 To Internet , $0.085 per GB


region
object
object
object
object
Make public
object
Your bucket
upload

Amazon S3 Basics

- In the AWS Management Console, on the Services menu, click S3.
- Click Create Bucket to create a new bucket.
- In the Create a Bucket dialog box, type a Bucket Name. This name must be globally unique, Named your bucket with your User Name and student ID to ensure uniqueness. (example:cp01-103065525)
- For Region, choose your closest location(Oregon).



Create a Bucket - Select a Bucket Name and Region

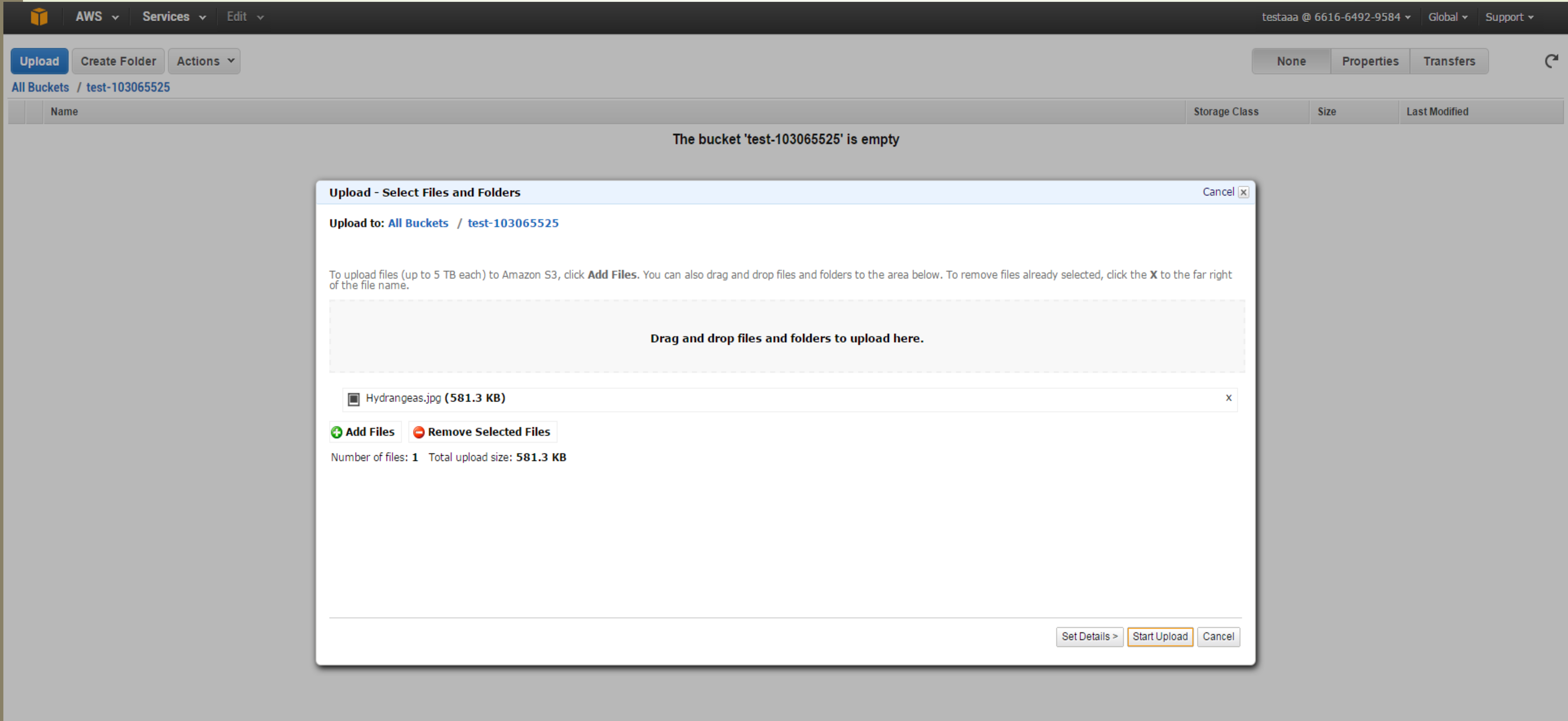
A bucket is a container for objects stored in Amazon S3. When creating a bucket, you can choose a Region to optimize for latency, minimize costs, or address regulatory requirements. For more information regarding bucket naming conventions, please visit the Amazon S3 documentation.

Bucket Name:

Region: Select a Region

Amazon S3 Basics (continued…)

- Click Create.
- To view the contents of this bucket, double-click its name. You will receive a message indicating that the bucket is empty.
- To add a new file object to your bucket, click button Actions, click Upload.
- In the “Upload – Select Files and Folders” dialog box, Add Files.
- Select a file from any location on your local machine to use as an object (for example, from the My Pictures folder).
- Click Start Upload. You will see the upload progress is shown in the Transfers panel.



The bucket 'test-103065525' is empty

Upload - Select Files and Folders

Upload to: All Buckets / test-103065525

To upload files (up to 5 TB each) to Amazon S3, click **Add Files**. You can also drag and drop files and folders to the area below. To remove files already selected, click the **X** to the far right of the file name.

Drag and drop files and folders to upload here.

Hydrangeas.jpg **(581.3 KB)** x

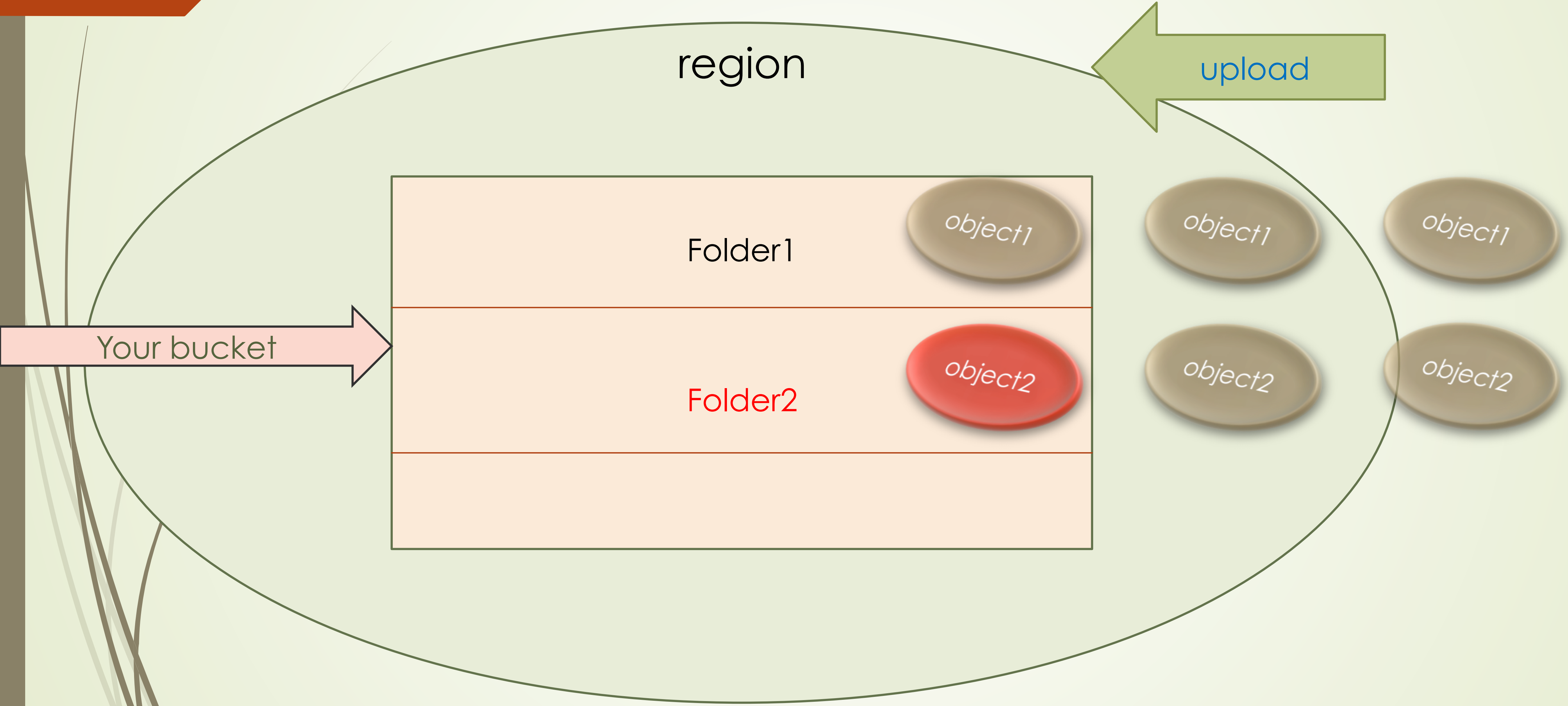
Number of files: **1** Total upload size: **581.3 KB**

Working with Objects

- Click on the name of the object to select it.
- With the object you uploaded still selected, click Properties. The object details panel appears on the right.
- To open the object, click the link. You will notice a lock icon next to it.
- To make your object publically accessible, return to your object details page, right- click the object, click Make Public, and then click OK.
- Click Properties.
- In the properties panel, click the object link again. The object should open without error this time.

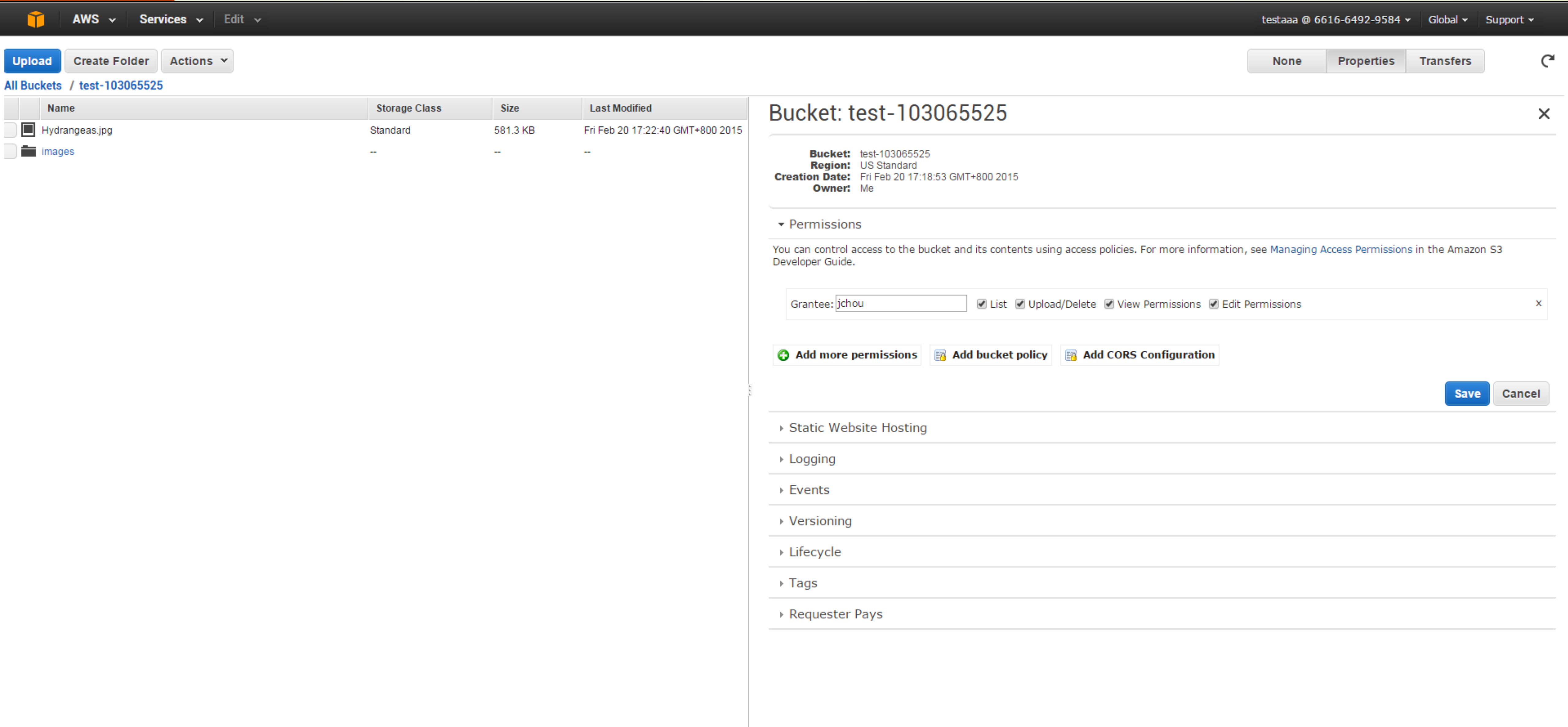
Working with Objects (continued…)

- In the properties panel, expand the Details section.
- For Storage Class, click Reduced Redundancy. The RRS storage class reduces costs by storing noncritical, reproducible data at lower levels of redundancy than the Standard storage class.
- For Server Side Encryption, select the AES-256 check box. Encryption provides added security for the object data stored in your buckets in Amazon S3.
- Click Save. This changes your object’s storage class to Reduced Redundancy (storing it in only two facilities rather than three), and automatically encrypts the object.


region
upload
Folder1
object1
object1
object1
Your bucket
Folder2
object2
object2
object2

Folders and Bucket Policies

- Click Create Folder and create a folder with name: images.
- Select your bucket again by clicking its name in the path.
- Click Properties.
- In the properties panel, view the bucket's properties, and then click Permissions . Bucket policies define the permissions structure for Amazon S3.
- Click Add bucket policy.
- In the Bucket Policy Editor dialog box, click the AWS Policy Generator link.



All Buckets / test-103065525

Name	Storage Class	Size	Last Modified
Hydrangeas.jpg	Standard	581.3 KB	Fri Feb 20 17:22:40 GMT+800 2015
images	--	--	--

Bucket: test-103065525

Bucket: test-103065525
Region: US Standard
Creation Date: Fri Feb 20 17:18:53 GMT+800 2015
Owner: Me

Permissions

You can control access to the bucket and its contents using access policies. For more information, see Managing Access Permissions in the Amazon S3 Developer Guide.

Grantee: jchou ☑ List ☑ Upload/Delete ☑ View Permissions ☑ Edit Permissions

Folders and Bucket Policies (continued...)

- Set the following values in the AWS Policy Generator:

a. Select Type of Policy: S3 Bucket Policy

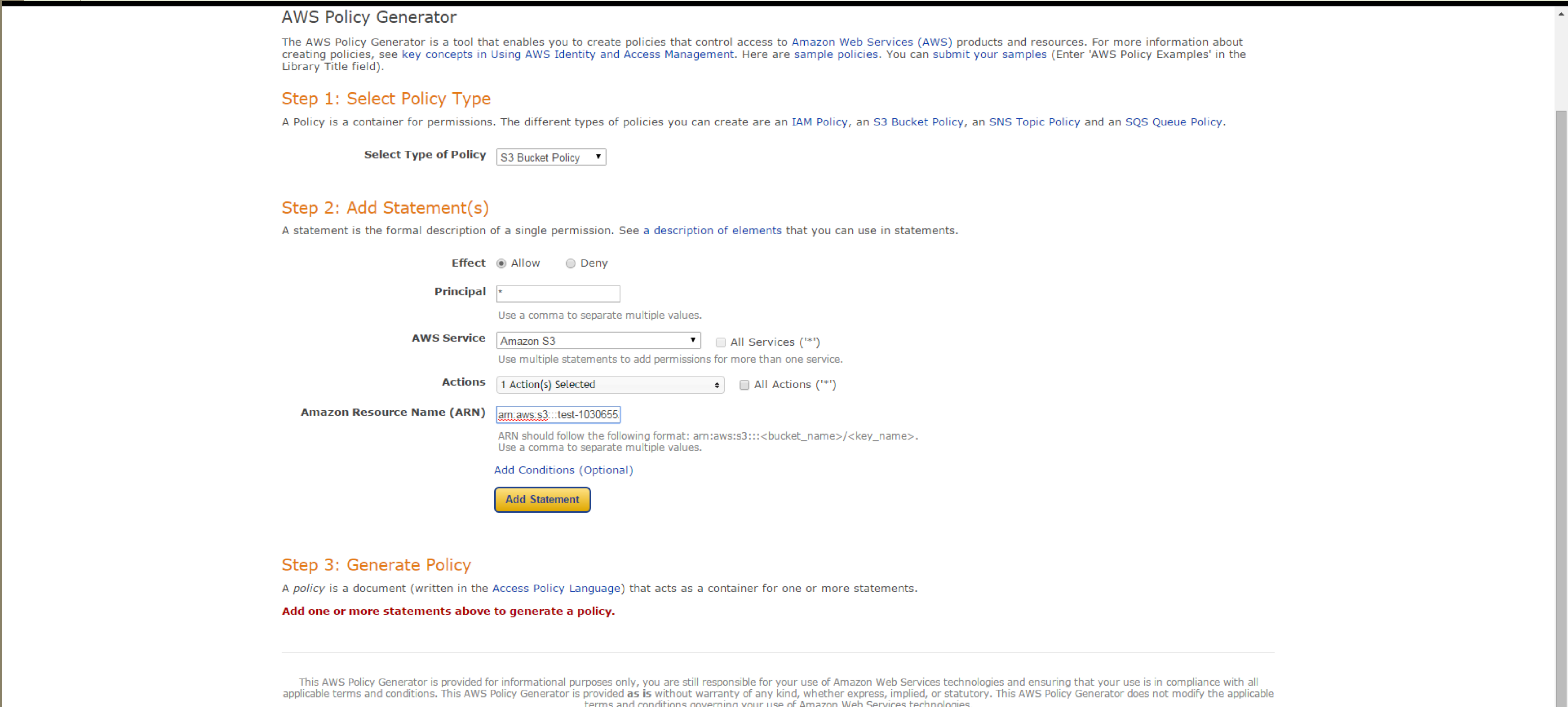
b. Effect:Allow

c. Principal: *

d. AWSService:AmazonS3

e. Actions:GetObject

f. Amazon Resource Name (ARN): arn:aws:s3:::<your-bucket-name>/images/*



AWS Policy Generator

The AWS Policy Generator is a tool that enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see key concepts in Using AWS Identity and Access Management. Here are sample policies. You can submit your samples (Enter 'AWS Policy Examples' in the Library Title field).

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy and an SQS Queue Policy.

Select Type of Policy S3 Bucket Policy ▾

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow ○ Deny

Principal *

Use a comma to separate multiple values.

AWS Service Amazon S3 ▾ □ All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected □ All Actions ('*')

Amazon Resource Name (ARN) arn:aws:s3:::test-1030655

ARN should follow the following format: arn:aws:s3:::<bucket_name>/<key_name>.
Use a comma to separate multiple values.

Step 3: Generate Policy

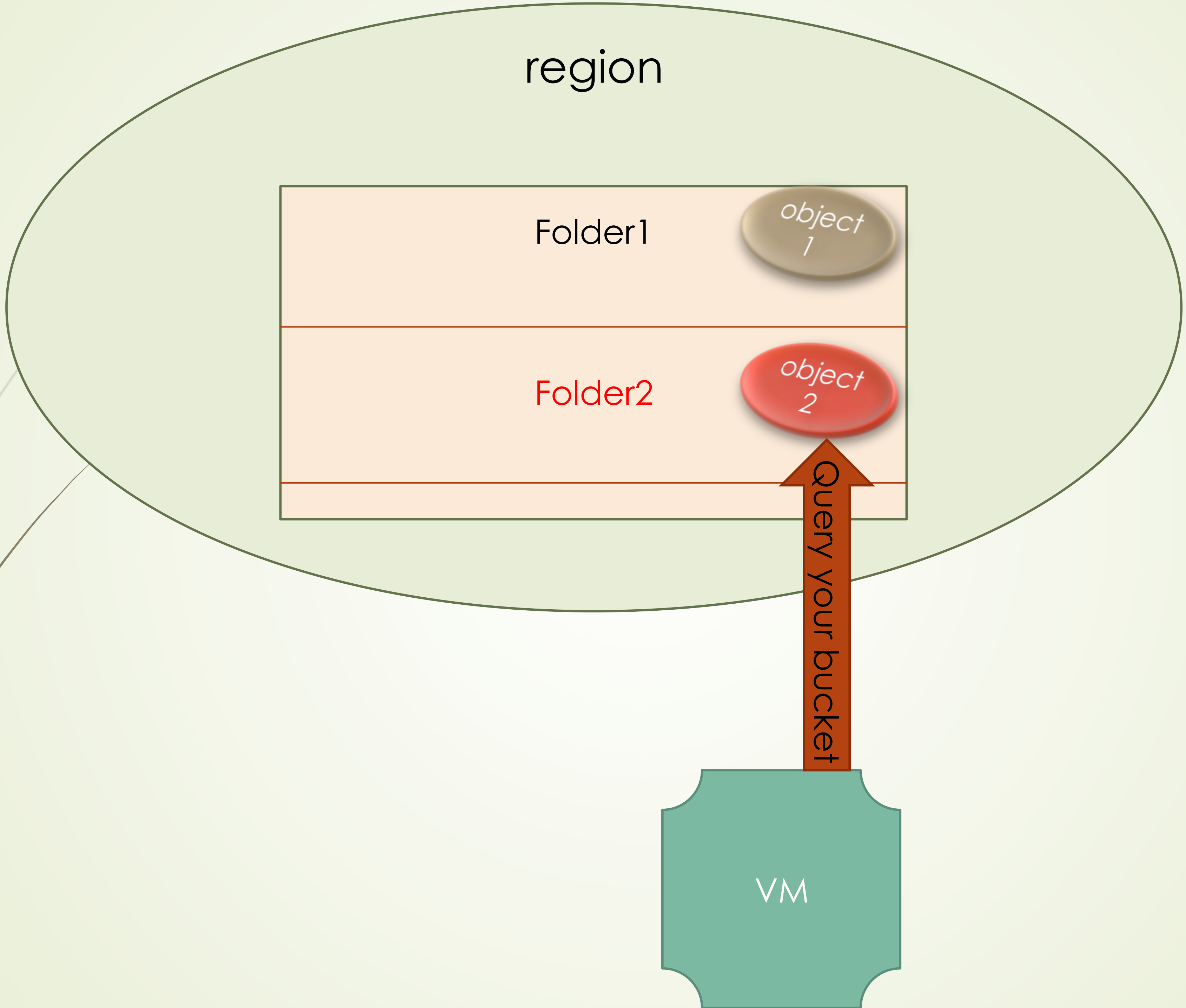
A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided **as is** without warranty of any kind, whether express, implied, or statutory. This AWS Policy Generator does not modify the applicable terms and conditions governing your use of Amazon Web Services technologies.

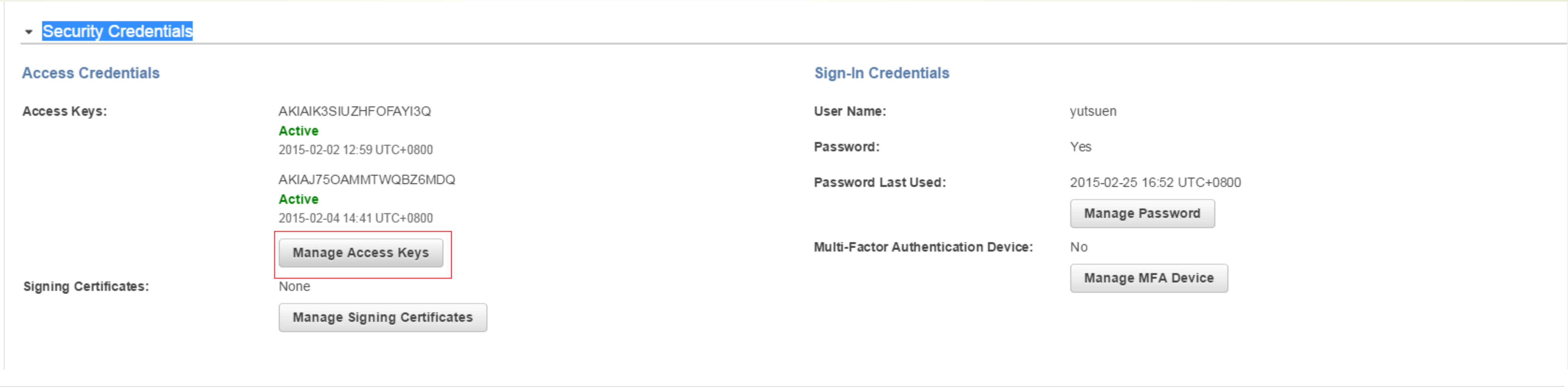
Folders and Bucket Policies (continued…)

- Click Add Statement to apply the new statement to the policy editor.
- Click Generate Policy.
- Copy the policy text to your clipboard.
- In the Policy JSON Document dialog box, click Close.
- Close the AWS Policy Generator dialog box to return to the S3 Management Console.
- Paste the policy text into the Bucket Policy Editor dialog box.
- Click Save.


region
Folder1
object 1
Folder2
object 2
Query your bucket
VM

Create Access Keys

- In the AWS Management Console, on the Services menu, click IAM.
- In the left panel , click Users.
- Select your account and click it.
- In the Security Credentials field , click Manage Access Keys button



Security Credentials

Access Credentials

Access Keys: AKIAIK3SIUZHFOFAYI3Q
Active
2015-02-02 12:59 UTC+0800

AKIAJ75OAMMTWQBZ6MDQ
Active
2015-02-04 14:41 UTC+0800

Signing Certificates: None

Sign-In Credentials

User Name: yutsuen

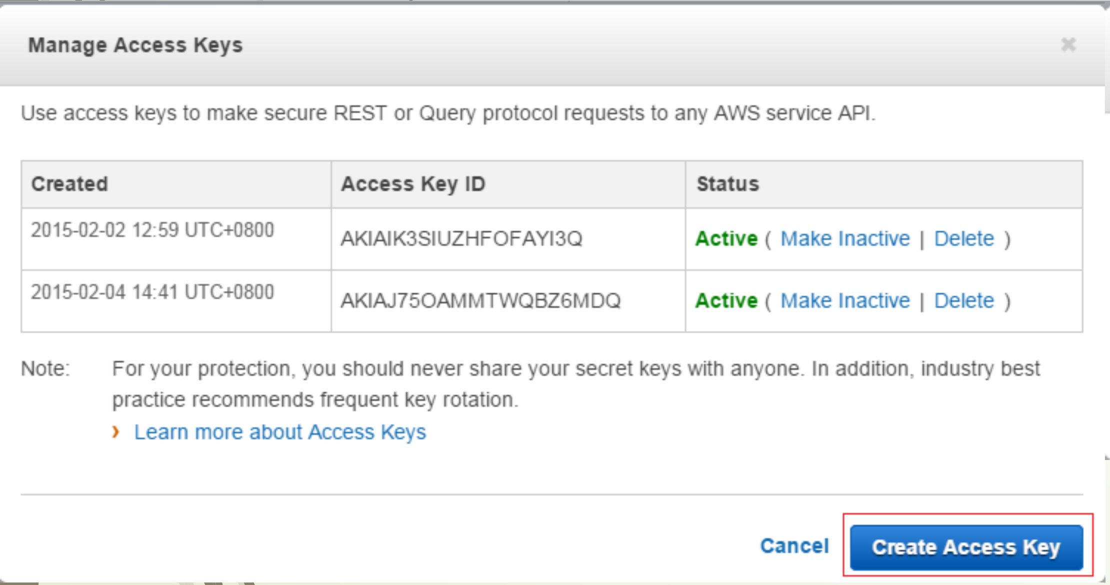
Password: Yes

Password Last Used: 2015-02-25 16:52 UTC+0800

Multi-Factor Authentication Device: No

Create Access Keys (continued…)

- Click Create Access key button
- Click Download Credentails



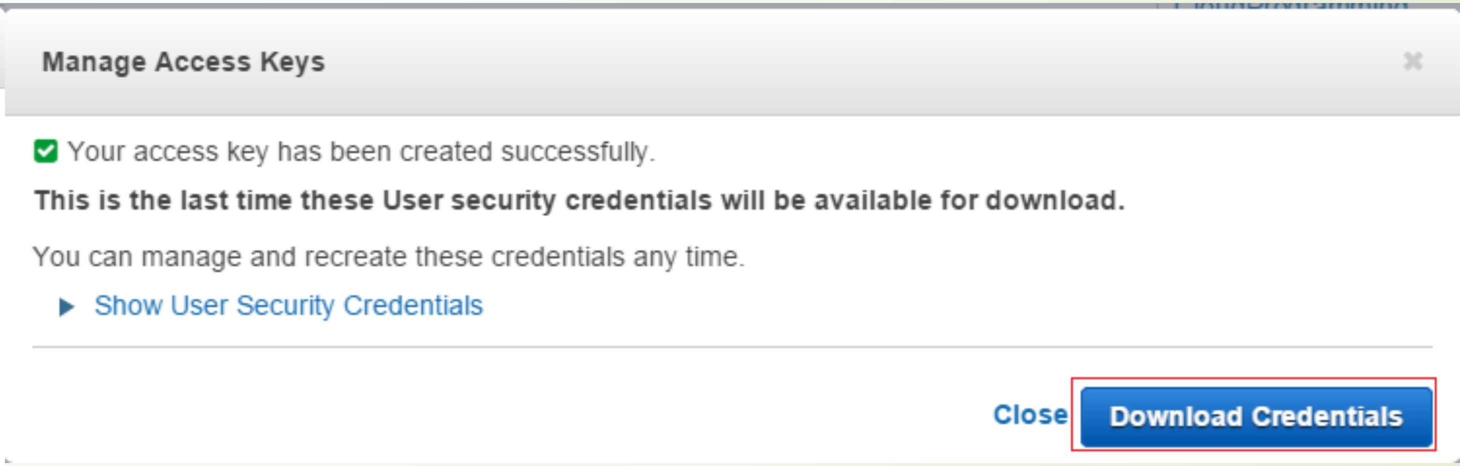
Manage Access Keys

Use access keys to make secure REST or Query protocol requests to any AWS service API.

Created	Access Key ID	Status
2015-02-02 12:59 UTC+0800	AKIAIK3SIUZHFOFAYI3Q	Active (Make Inactive | Delete)
2015-02-04 14:41 UTC+0800	AKIAJ75OAMMTWQBZ6MDQ	Active (Make Inactive | Delete)

Note: For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation.

› Learn more about Access Keys



Manage Access Keys

☑ Your access key has been created successfully.

This is the last time these User security credentials will be available for download.

You can manage and recreate these credentials any time.

▶ Show User Security Credentials

Sample code to initiate a s3client

```
<?php
require 'vendor/autoload.php';
use Aws\S3\S3Client;
$client = S3Client::factory(array(
        'key'    => 'YOUR_AWS_ACCESS_KEY_ID',
         'secret' => 'YOUR_AWS_SECRET_ACCESS_KEY',
));
?>
```

Reference:

php s3 using guide

pup install guide

P.S.: If you want to write in other languages, please google it with AWS .

Lab (3%)

- Please using your code to

   1. Create a bucket. (1%)

   2. upload two images from your machine to your bucket. (1%)

   3. list objects of your bucket on the webpage. (1%)