

Assignment 6 – S3

Today's tasks:

1. Host a static website on S3
2. Set an event notification with SNS

Play with:

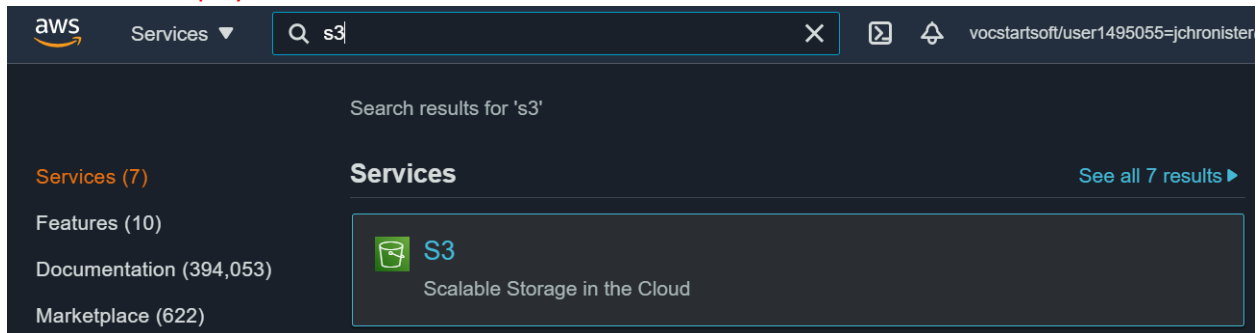
- S3 lifecycle policy
- Versioning

Submit items below in one pdf file:

1. URL of the static app.
2. Screenshots of SNS emails.
 - a. Confirmation
 - b. Object put email.

Instruction 1. Host a static website on S3

Go to the S3 Display



Create Bucket

Account snapshot

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)**Buckets (0)** [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

[Copy ARN](#)

Empty

Delete

Create bucket

< 1 >



Name ▲

AWS Region ▼

Access ▼

Creation date ▼

No buckets

You don't have any buckets.

[Create bucket](#)

1) Click on the S3 Queue

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

2) Name Bucket

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)


AWS Region

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

3) Uncheck Block Public Access

☐ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

4) Check to Acknowledge

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☒ Disable

☐ Enable

Tags (0) - optional

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.

Add tag

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)


Server-side encryption

☒ Disable

☐ Enable

► Advanced settings

5) Click Create Bucket

 After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

Enable Static Web Hosting for Bucket

my-data-fp [Info](#)

Objects

Properties

Permissions

Metrics

Management

Access Points

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#) [↗](#)

Edit

Static website hosting
Disabled

1) Click Create Bucket

Edit static website hosting [Info](#)

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#) [↗](#)

Static website hosting

☐ Disable

☒ Enable

2) Enable Hosting

Hosting type

☒ Host a static website

Use the bucket endpoint as the web address. [Learn more](#) [↗](#)

☐ Redirect requests for an object

Redirect requests to another bucket or domain. [Learn more](#) [↗](#)

Index document

Specify the home or default page of the website.

index.html

3) Specify Home Page

Error document - *optional*

This is returned when an error occurs.

error.html

Redirection rules – *optional*

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#) [↗](#)

1

4) Click on Save Changes

Cancel

Save changes

...

Static website hosting

Edit

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting



Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)







 <http://my-data-fp.s3-website-us-east-1.amazonaws.com>  Web Site Link

Upload Files in Bucket

Objects | Properties | Permissions | Metrics | Management | Access Points


Objects (0)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)


  Copy S3 URI  Copy URL  Download  Open  Delete



Actions ▼

Create folder

 Upload 1) Click Upload

☐ Show versions

< 1 > 

	Name ▲	Type ▼	Last modified ▼	Size ▼	Storage class ▼
No objects					
You don't have any objects in this bucket.					
<div> Upload</div>					

...

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 746.0 B)

All files and folders in this table will be uploaded.

Remove

Add files

Add folder

Find by name

2) Add Files or Folders

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	index.html	-	text/html	746.0 B

Destination

Destination

s3://my-data-fp

Destination details

Bucket settings that impact new objects stored in the specified destination.

Permissions

Grant public access and access to other AWS accounts.

Properties

Specify storage class, encryption settings, tags, and more.

3) Click Upload

Cancel

Upload

Add Public Permissions to S3 Bucket Objects - Edit Bucket Policy Under Permissions Tab

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Policy examples](#)

[Policy generator](#)

Bucket ARN

arn:aws:s3:::my-data-fp

Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicReadGetObject",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3:::my-data-fp/*"  
10    }  
11  ]  
12 }
```

1) Paste in Permission

2) Click Save

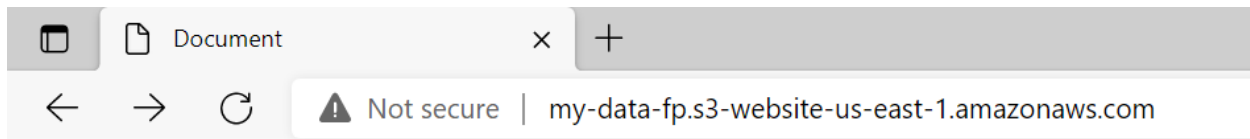
Cancel

Save changes

Permission for Public Access to S3 Bucket and All your Objects in the Bucket

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::<Your Bucket Name>/*"  
    }  
  ]  
}
```

Test Static Website



Hello From my S3 Static Web Site

Instruction 2. Create an event notification when an object got created in the bucket

1. Create SNS. When creating the SNS, give custom resource-based policy to allow the S3 bucket.
2. Create event on S3 and select the SNS topic.

Create SNS Topic & Add Permission for S3 to Publish Message. Subscribe to the SNS Topic

```
{
  "Sid": "__console_pub_0",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": "SNS:Publish",
  "Resource": "<Your SNS ARN>",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": "<Your AWS Account Number>"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:s3:*:*:<Your Bucket Name>"
    }
  }
}
```

Create S3 Event Notification for Your Bucket Under Properties Tab Event Notification

Event notifications (0) Edit Delete Create event notification


Send a notification when specific events occur in your bucket. [Learn more](#)

1) Click Create Event Notification

	Name	Event types	Filters	Destination type	Destination
No event notifications					
Choose Create event notification to be notified when a specific event occurs.					
Create event notification					

...

Create event notification [Info](#)

The notification configuration identifies the events you want Amazon S3 to publish and the destinations where you want Amazon S3 to send the notifications. [Learn more](#) 

General configuration

Event name

S3_Put_Notification

2) Name Event

Event name can contain up to 255 characters.

Prefix - *optional*

Limit the notifications to objects with key starting with specified characters.

images/

Suffix - *optional*

Limit the notifications to objects with key ending with specified characters.

.jpg

Event types

Specify at least one type of event for which you want to receive notifications. [Learn more](#) 

☐ All object create events

s3:ObjectCreated:*

☒ Put

s3:ObjectCreated:Put

3) Select Your Criteria

☐ Post

s3:ObjectCreated:Post

☐ Copy

s3:ObjectCreated:Copy

☐ Multipart upload completed


s3:ObjectCreated:CompleteMultipartUpload

☐ All object delete events


s3:ObjectRemoved:*

☐ Permanently deleted

s3:ObjectRemoved:Delete

Destination
Choose a destination to publish the event. [Learn more](#) 

☐ **Lambda function**
Run a Lambda function script based on S3 events.

☒ **SNS topic** 
Send notifications to email, SMS, or an HTTP endpoint.


☐ **SQS queue**
Send notifications to an SQS queue to be read by a server.


Specify SNS topic

☒ **Choose from your SNS topics**

☐ **Enter SNS topic ARN**

SNS topic

myRequestSNS 



Cancel **Save changes**

Test by Uploading a File to Your S3 Bucket

Instruction 3. Create a lifecycle policy

Create S3 Life Cycle Rule under Management Tab


my-data-fp

Publicly accessible

Objects | Properties | Permissions | Metrics | **Management** | Access Points

Lifecycle rules (0)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

 [View details](#) [Edit](#) [Delete](#) [Actions](#) [Create lifecycle rule](#)

Lifecycle rule name	Status	Scope	Current version actions	Previous version actions	Expired object delete markers	Incomplete multipart uploads
There are no lifecycle rules for this bucket.						
Create lifecycle rule						

1) Click Create Lifecycle Rule

2) Name Rule & Configure Settings based on What You Want to Accomplish...

1) Click Create Rule

[Cancel](#) [Create rule](#)