

I. Create a bucket for assets of the web app hosted on EC2. Put an image into the bucket.

- Create an inline IAM policy in the LabRole that allows the instance to get objects from the bucket.
- Download the image in the EC2. Copy from S3 to EC2.
- Update the index.html and read the image from the /var/www/html folder

➔ Go to IAM

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar with sections like 'Access management' and 'Access reports'. The main content area is titled 'Summary' and 'Permissions'. The 'Permissions' tab is active, showing a list of permissions policies attached to the role. The list includes three custom policies (VocLabPolicy1, VocLabPolicy2, VocLabPolicy3) and several AWS managed policies (AmazonEKSClusterPolicy, AmazonEKSWorkerNodePolicy, AmazonEC2ContainerRegistryReadOnly, AmazonSSMManagedInstanceCore). The 'Add permissions' button is visible at the top right of the permissions list.

Policy name	Type	Description
c68758a135359032056451w364616735719-VocLabPolicy1-1AEB2G7RJ0APL	Customer managed	
c68758a135359032056451w364616735719-VocLabPolicy2-ANGBA6WG1WSI	Customer managed	
c68758a135359032056451w364616735719-VocLabPolicy3-18XEVEK3RL4F	Customer managed	
AmazonEKSClusterPolicy	AWS managed	This policy provides Kuber
AmazonEKSWorkerNodePolicy	AWS managed	This policy allows Amazon
AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access
AmazonSSMManagedInstanceCore	AWS managed	The policy for Amazon EC2

- ➔ Add permissions
- ➔ Create inline policy

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor **JSON** [Import managed policy](#)

[Expand all](#) [Collapse all](#)

▼ Select a service [Clone](#) [Remove](#)

► Service [Choose a service](#)

► Actions Choose a service before defining actions

► Resources Choose actions before applying resources

► Request conditions Choose actions before specifying conditions

[Add additional permissions](#)

Character count: 39 of 10,240.
The current character count includes character for all inline policies in the role: LabRole.

[Cancel](#) [Review policy](#)

- ➔ Choose Server S3 > Action select get object
- ➔ Specified bucket object with ARN
- ➔ Last add condition

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor **JSON** [Import managed policy](#)

[Expand all](#) [Collapse all](#)

▼ S3 (1 action) [Clone](#) [Remove](#)

► Service S3

► Actions Read
GetObject

▼ Resources ☒ Specific [close](#) ☐ All resources

object [EDIT](#) [Add ARN to restrict access](#) ☐ Any

► Request conditions [Specify request conditions \(optional\)](#)

[Add additional permissions](#)

Character count: 168 of 10,240.
The current character count includes character for all inline policies in the role: LabRole.

[Cancel](#) [Review policy](#)

- ➔ Bucket policy added here because we don't have permission to add policy in IAM with academy account

BWS

Services

Search

[Option+S]

Global

vorlabs/user2293723~changprosth @ 3646-1675-5719

Amazon S3

X

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

► AWS Marketplace for S3

Individual Block Public Access settings for this bucket

Bucket policy

EditDelete

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](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Principal": {
        "Service": "ec2.amazonaws.com"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::second-assignment-bucket-prosth/**",
      "Condition": {
        "ArnLikeIfExists": {
          "aws:PrincipalArn": "arn: aws: ec2:us-east-id-364616735719:instance/i-0a504d1250310aca9"
        }
      }
    }
  ]
}
```

Copy

Object Ownership

Info

Edit

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Object Ownership

Bucket owner enforced

ACLs are disabled. All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

Access control list (ACL)

Edit

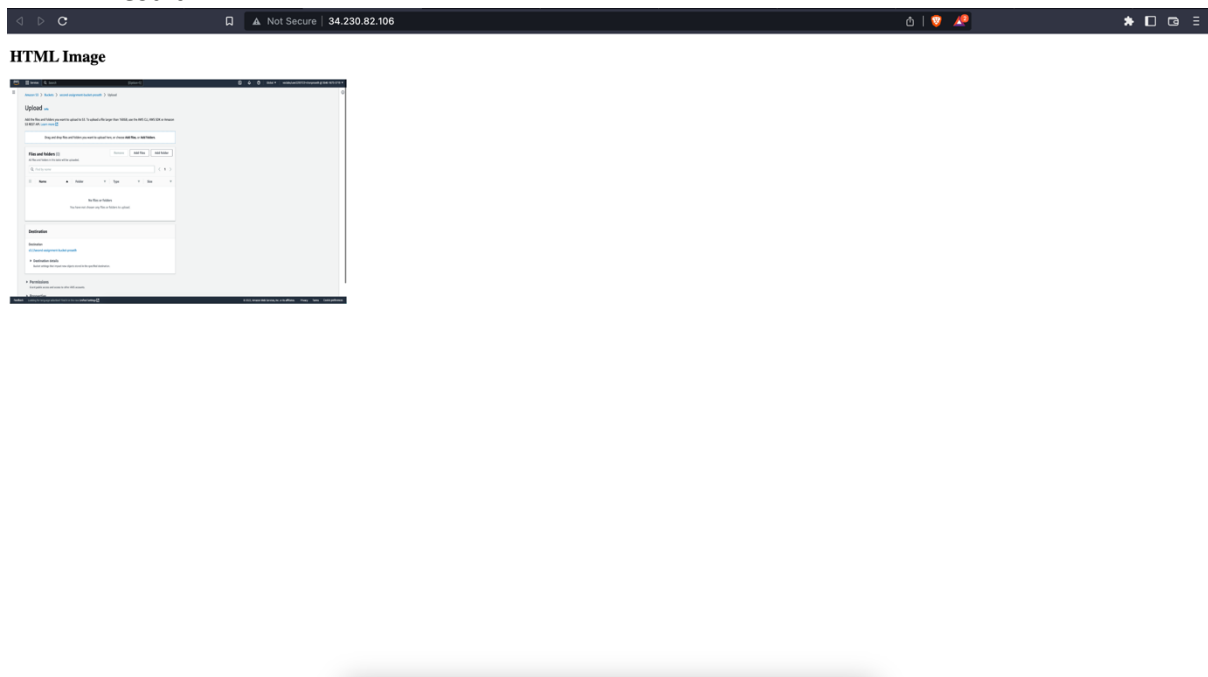
© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms

Cookie preferences

- ➔ Connect EC2 Session Manager
- ➔ Use command to copy image from the bucket
- ➔ We can see it successfully copied

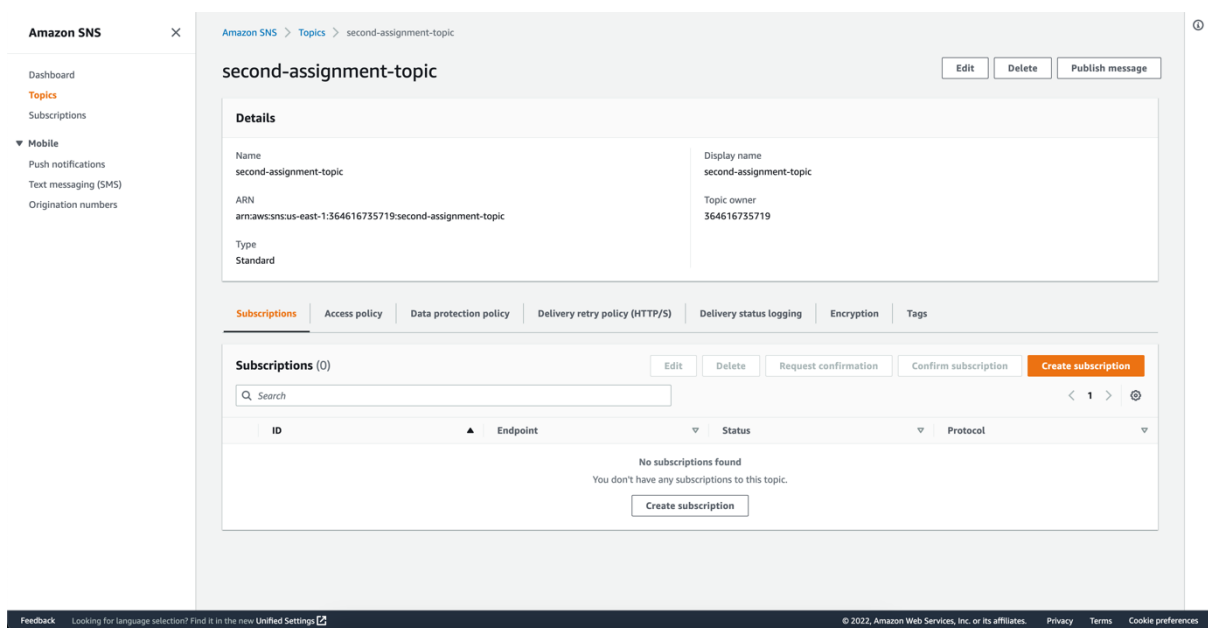
[illegible]

- ➔ Create index.html and read the image to display in the website
- ➔ Result



2. Send an email to yourself when the object is created in the bucket.
 - a) You need to create an SNS topic. Modify the default SNS policy while creating the SNS.
 - b) Subscribe it with your email.

- ➔ Create SNS Topic



➔ Add Policy for S3 to access publish email from event that trigger in the s3 bucket

Display name - optional
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. [Info](#)
second-assignment-topic
Maximum 100 characters.

Encryption - optional
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic. [Info](#)

Access policy - optional
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. [Info](#)

JSON editor

```
27 },  
28 {  
29   "Sid": "_console_pub_2",  
30   "Effect": "Allow",  
31   "Principal": {  
32     "Service": "s3.amazonaws.com"  
33   },  
34   "Action": "SNS:Publish",  
35   "Resource": "arn:aws:sns:us-east-1:364616735719:second-assignment-topic",  
36   "Condition": {  
37     "StringEquals": {  
38       "aws:SourceAccount": "364616735719"  
39     },  
40     "ArnLike": {  
41       "aws:SourceArn": "arn:aws:s3:::second-assignment-bucket-proseth"  
42     }  
43   }  
44 }
```

Data protection policy - optional [Info](#)
This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

Feedback Looking for language selection? Find it in the new Unified Settings [🔗](#) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

➔ Create subscription to my email

Amazon SNS [×](#) **Important changes for sending text messages (SMS) to US destinations**
US mobile carriers have recently changed their regulations, and will require that all toll-free numbers (TFNs) complete a registration process with a regulatory body before September 30, 2022. If you currently have a toll-free number you must register your toll-free number by September 30, 2022 or you will no longer be able to use the toll-free number. [Learn more](#) [🔗](#) [View origination numbers](#)

Amazon SNS > Topics > second-assignment-topic > Subscription: 51c08b01-34c4-434b-b28e-190ad2da0f84

Subscription: 51c08b01-34c4-434b-b28e-190ad2da0f84 [Edit](#) [Delete](#)

Details

ARN arn:aws:sns:us-east-1:364616735719:second-assignment-topic:51c08b01-34c4-434b-b28e-190ad2da0f84	Status Confirmed
Endpoint kchanproseth@gmail.com	Protocol EMAIL
Topic second-assignment-topic	
Subscription Principal arn:aws:iam::364616735719:role/voclabs	

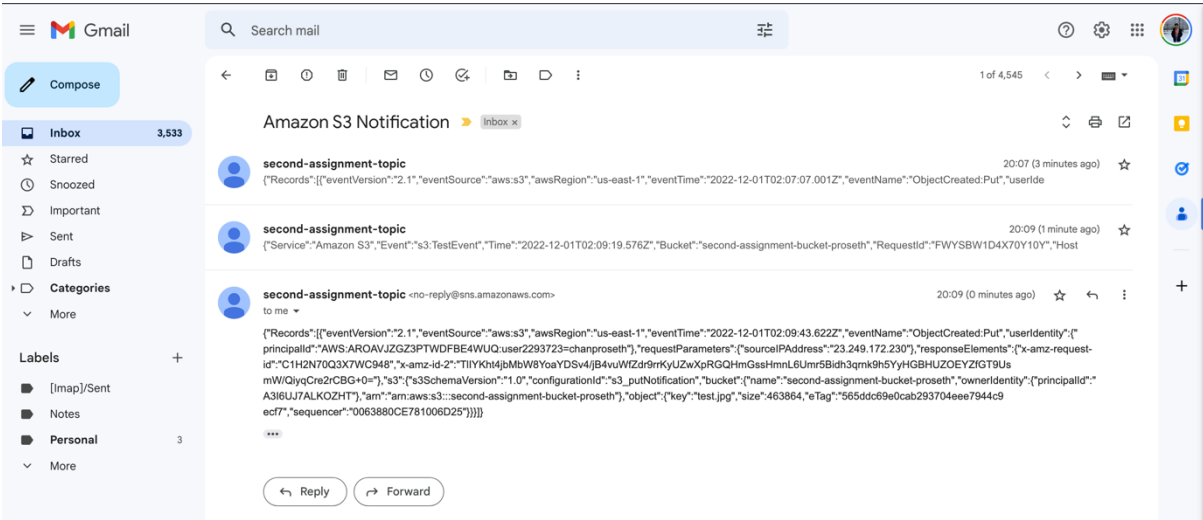
Subscription filter policy [info](#) [Redrive policy \(dead-letter queue\)](#)

Subscription filter policy [info](#)
This policy filters the messages that a subscriber receives.

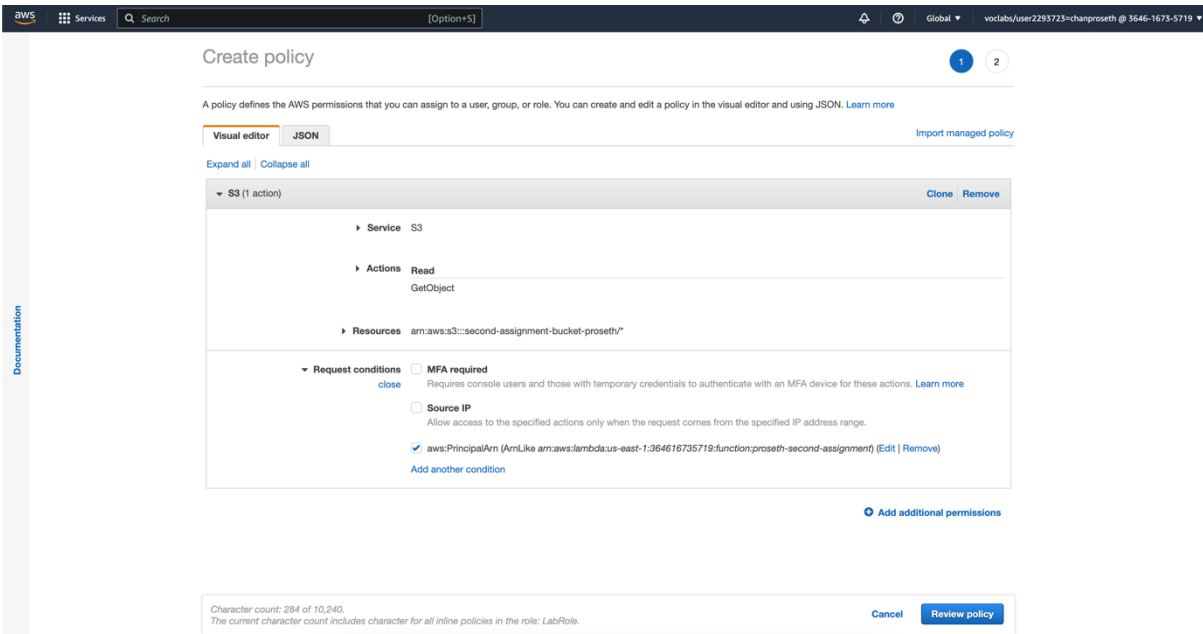
No filter policy configured for this subscription.
To apply a filter policy, edit this subscription. [Edit](#)

Feedback Looking for language selection? Find it in the new Unified Settings [🔗](#) © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

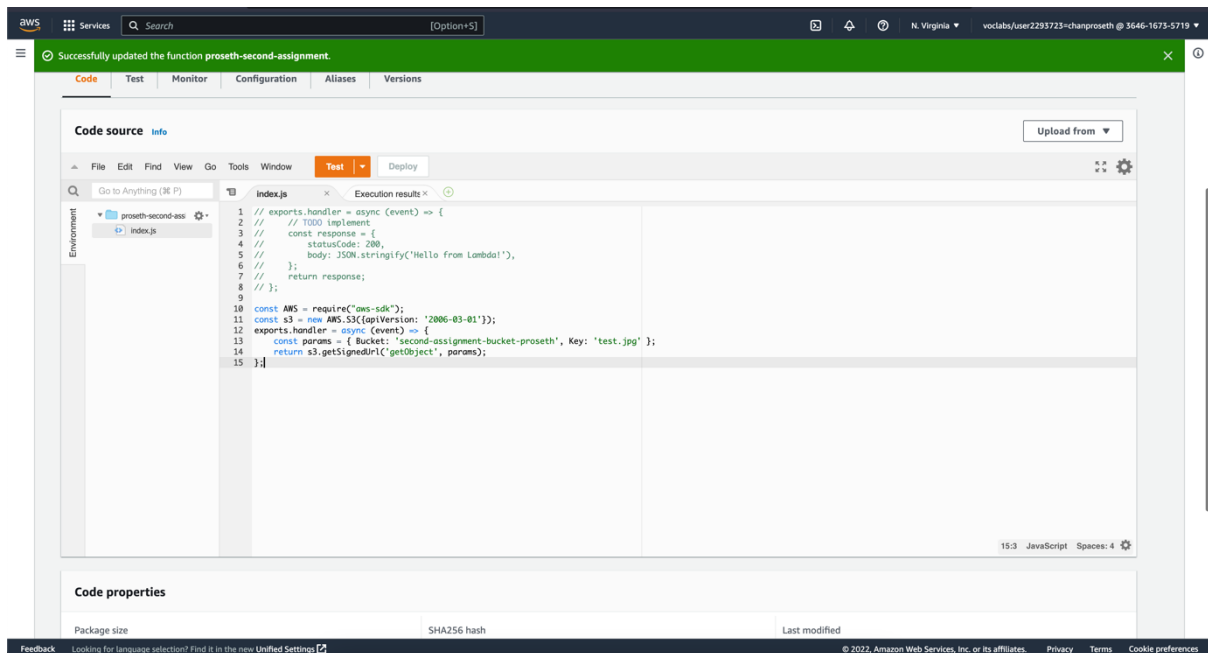
➔ Received email after upload or update new image



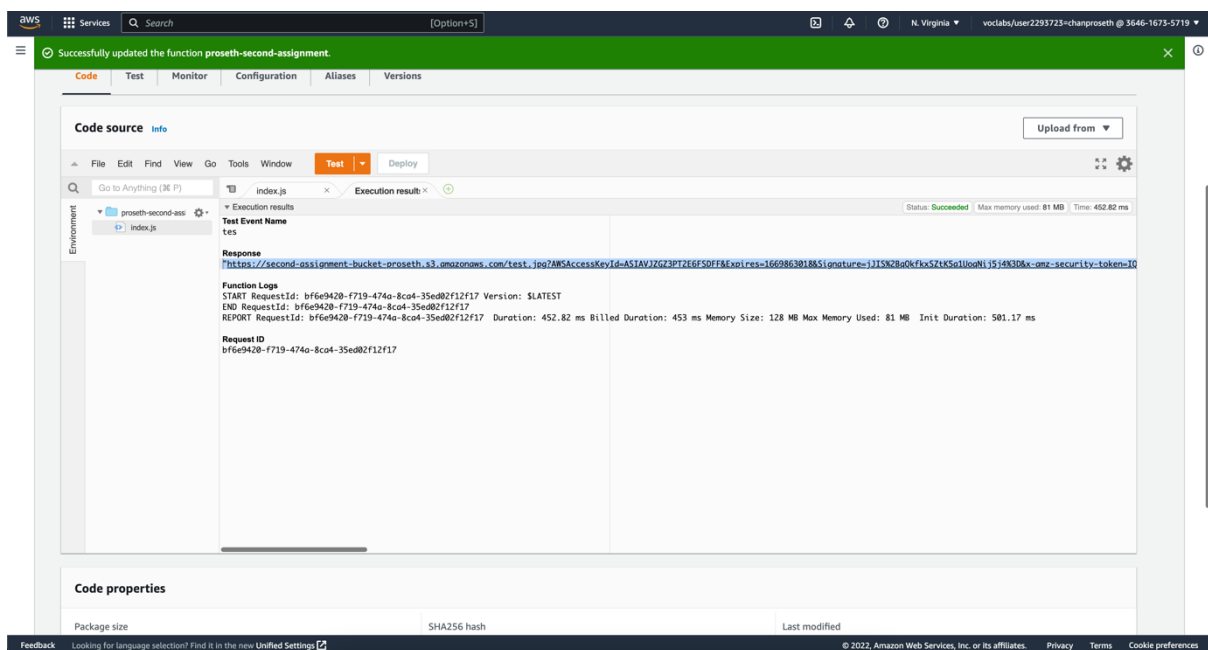
3. Write a lambda that returns a Signed URL of the object. Make sure the LabRole has an inline policy that allows getting objects from the bucket.



➔ Add code snippet to run call aws sdk and get image from bucket then get the signed url



➔ Test result success



second-assignment-bucket-proseith.s3.amazonaws.com/test.jpg?AWSAccessKeyId=ASIAVJZGZ3PTZE6FSDF&Expires=1669863018&Sign...

ServicesSearch[Option+5]

Globalvoclabs/user2293723~chanproseith @ 3646-1673-5719

Amazon S3> Buckets> second-assignment-bucket-proseith> Upload

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 (0)

RemoveAdd FilesAdd folder

All files and folders in this table will be uploaded.

Find by name

< 1 >

NameFolderTypeSize

No files or folders

You have not chosen any files or folders to upload.

Destination

Destination

s3://second-assignment-bucket-proseith

Destination details

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

Permissions

Grant public access and access to other AWS accounts.

Proseith

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)