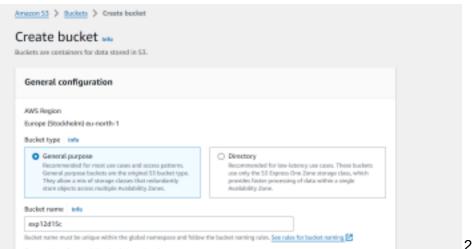
DIMPLE DALWANI D15C 8

Aim: To create a Lambda function which will log "An Image has been added" once you add an object to a specific bucket in S3

STEPS:

1. Create a S3 bucket and give it a bucket name



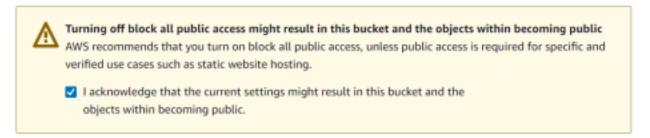
2. Allow public access

to the bucket as we are going to add this bucket as a trigger for our lamda function

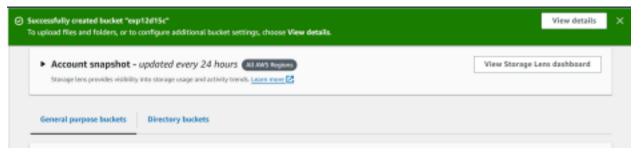
Block Public Access settings for this bucket Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings 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 **These settings apply only to this bucket or objects within, you can
□ 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) 53 will block public access permissions applied to newly added buckets or objects, and present 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 53 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 55 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 53 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies 53 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

3. Give

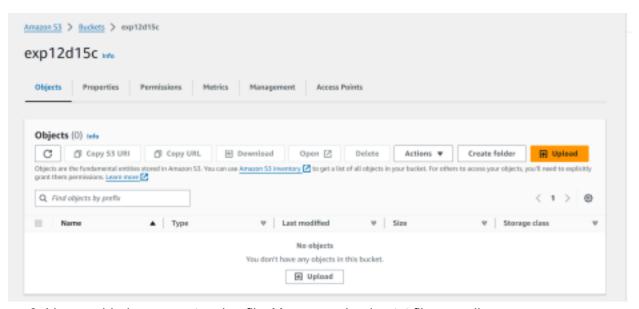
confirmation that you want to allow full public access and create the bucket



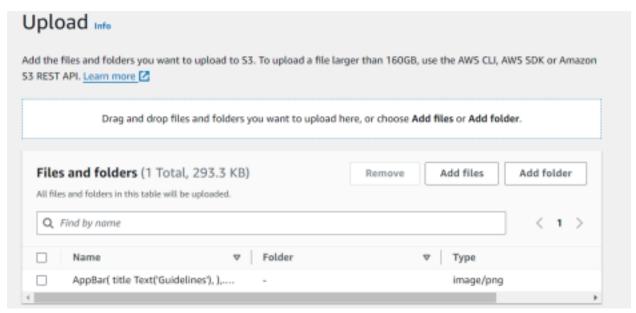
4. You will see the confirmation that the bucket is created successfully



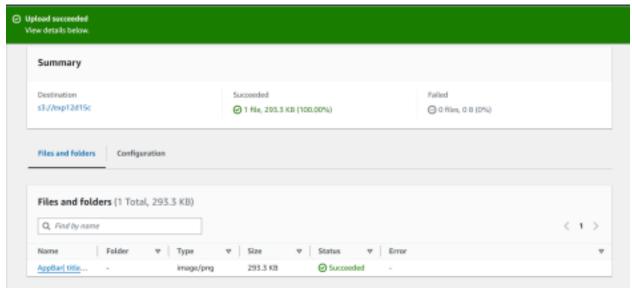
5. Now we need to upload something in the bucket so click on the upload button and add a file



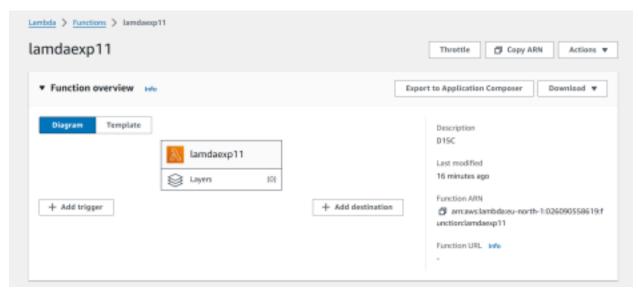
6. I have added a .png extension file; You can upload a .txt file as well



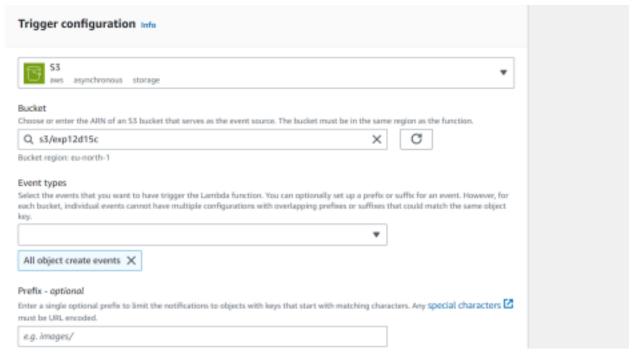
7. Here you can see the confirmation that the upload was a success



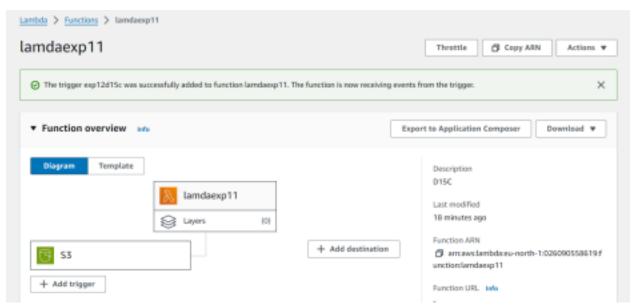
- 8. Now go back to the aws dashboard and search for lamda function service, Open the function we created in experiment 10. We are going to add this bucket as a trigger to this function
- 9. On the function overview section of the dashboard you can see the "Add trigger" button. Click on that



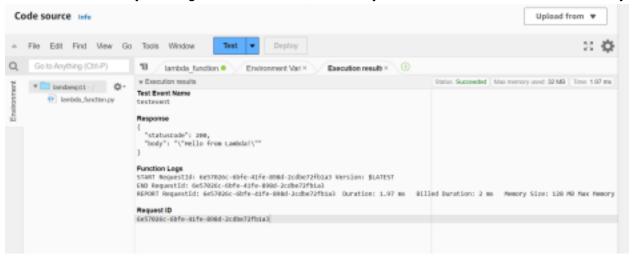
10. It will lead you to the trigger configuration tab; Where you have to select the service and the bucket you created. Add the required configuration information and then save.



11. Here you can see we have the confirmation message as well the the s3 bucket added to our triggers



12. Test the code by clicking on the Test tab; Here as you can see our code ran successfully



Conclusion: In conclusion, the experiment successfully demonstrated the integration of an S3 bucket with an AWS Lambda function as a trigger. By creating the S3 bucket and configuring it to invoke the Lambda function upon object uploads, we established a seamless workflow for automated processing.