[Create S3 Bucket With Private Access (Upload a image)](#_4mdqhfbc2mo8)

[Create Config Rule](#_375r828gf9gi)

[Create Lambda Function To Take Remediate Actions:](#_eka1bqlif98v)

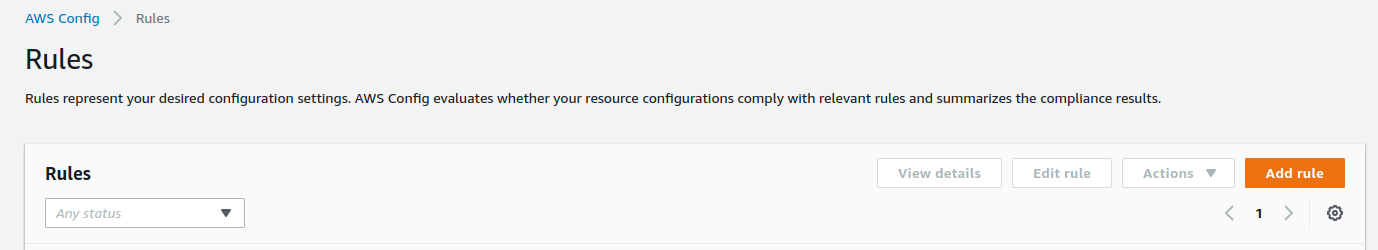
[Configure Cloudwatch Rule To Trigger Remediate Lambda](#_stql0zykwpgu)

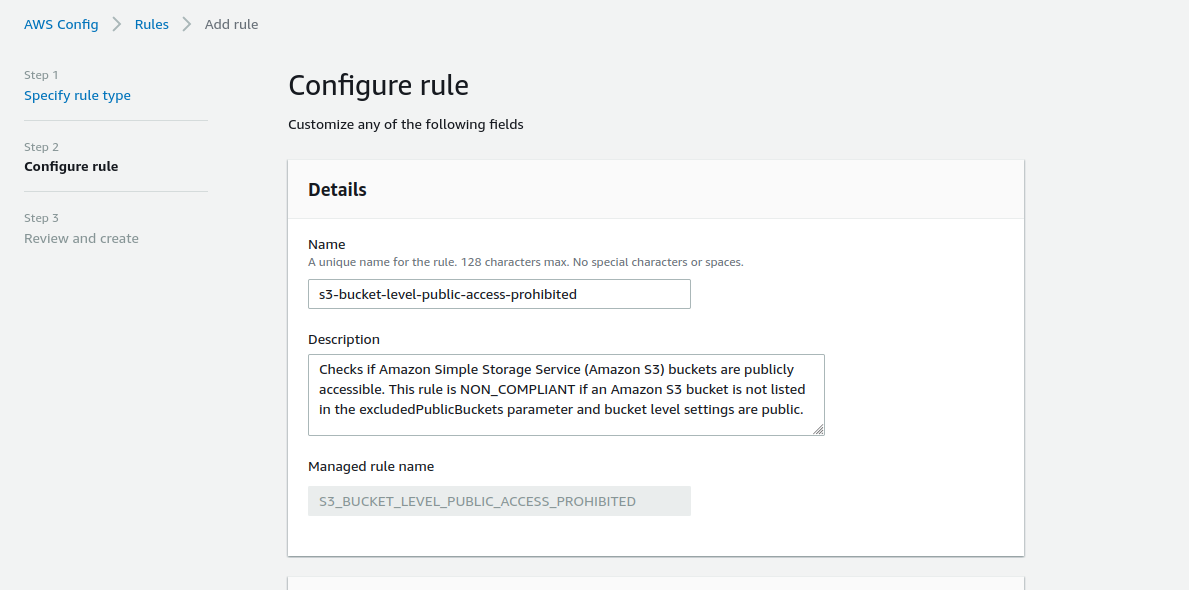
[Experiment On Private Bucket](#_n1j011aamrbx)

[Experiment On Public Bucket](#_18tlepw68it0)

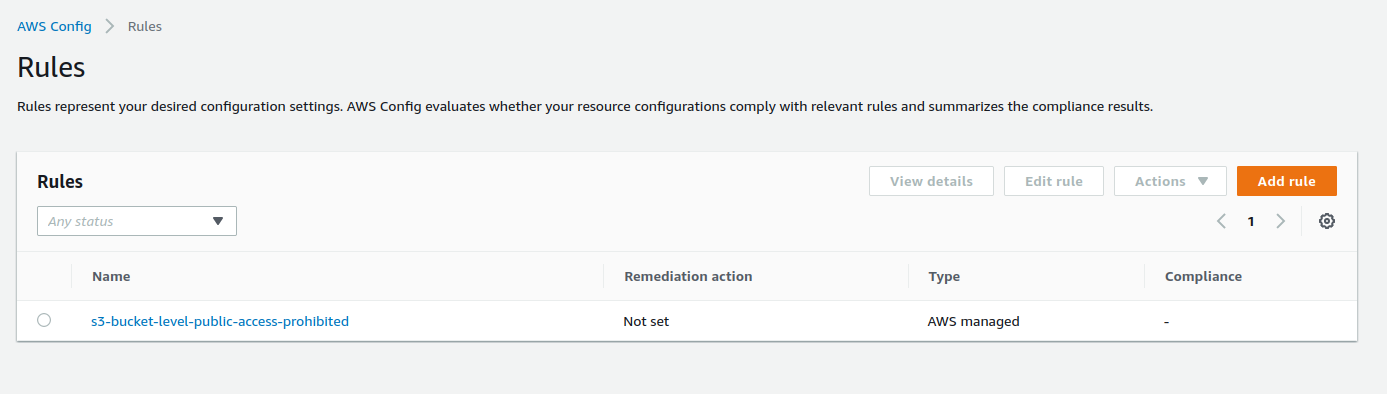
## **Create S3 Bucket With Private Access (Upload a image)**

## Create Config Rule

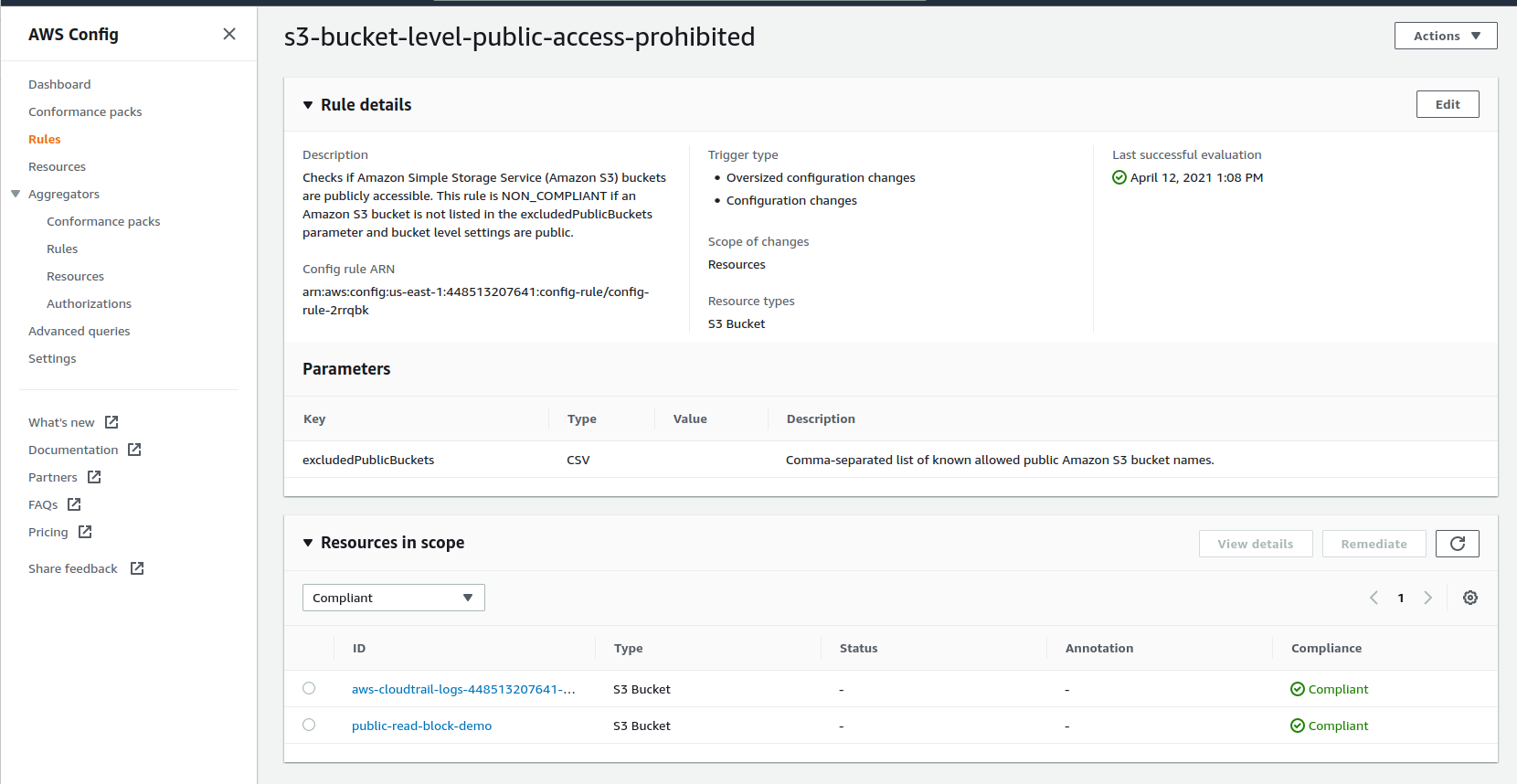




Keep other settings as defaults and create rule.

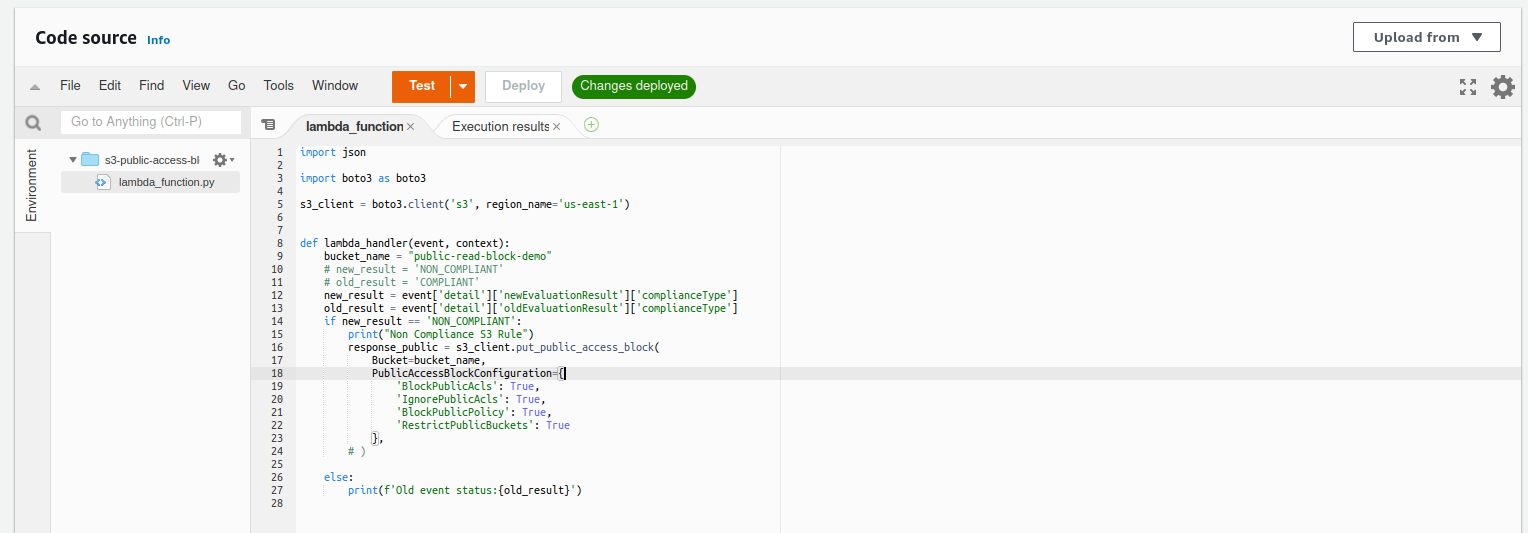


Wen we go inside the rule , we could see our bucket is in compliance list like below:



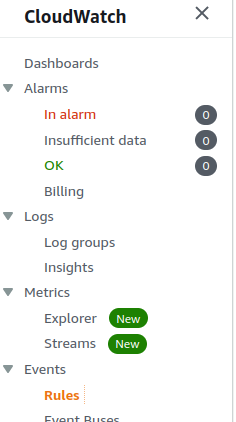
## **Create Lambda Function To Take Remediate Actions:**

* This will change bucket policy to private and send a sms when someone changed the bucket accessibility to public



## **Configure Cloudwatch Rule To Trigger Remediate Lambda**

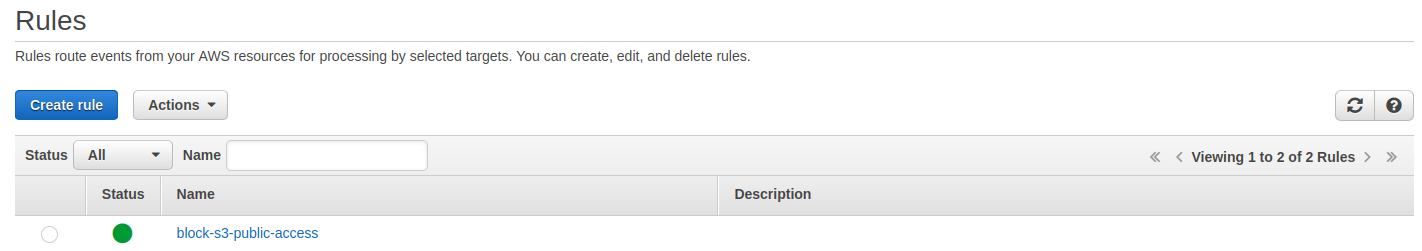
Select Cloudwatch rules



* Select “Create New Rule”
* Add pattern like below

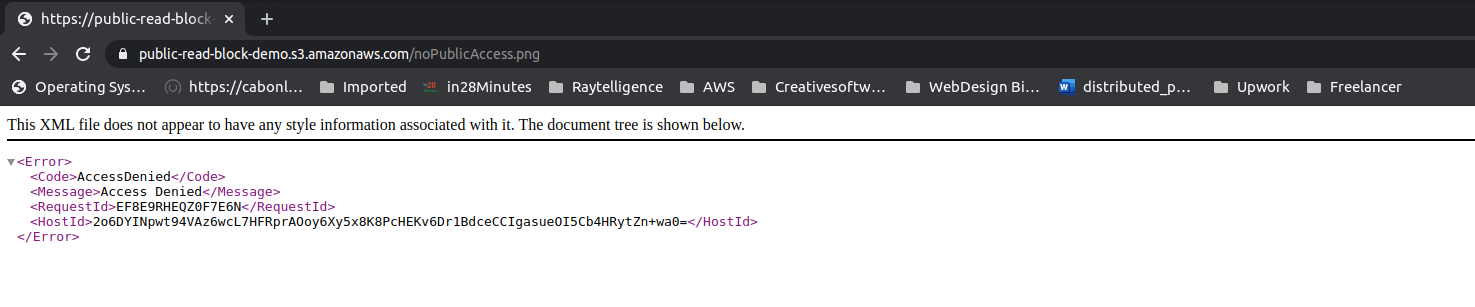
|  |
| --- |
| {  "source": [  "aws.config"  ],  "detail-type": [  "Config Rules Compliance Change"  ],  "detail": {  "messageType": [  "ComplianceChangeNotification"  ],  "resourceType": [  "AWS::S3::Bucket"  ]  }  } |

* Select our lambda as target lambda



## Experiment On Private Bucket

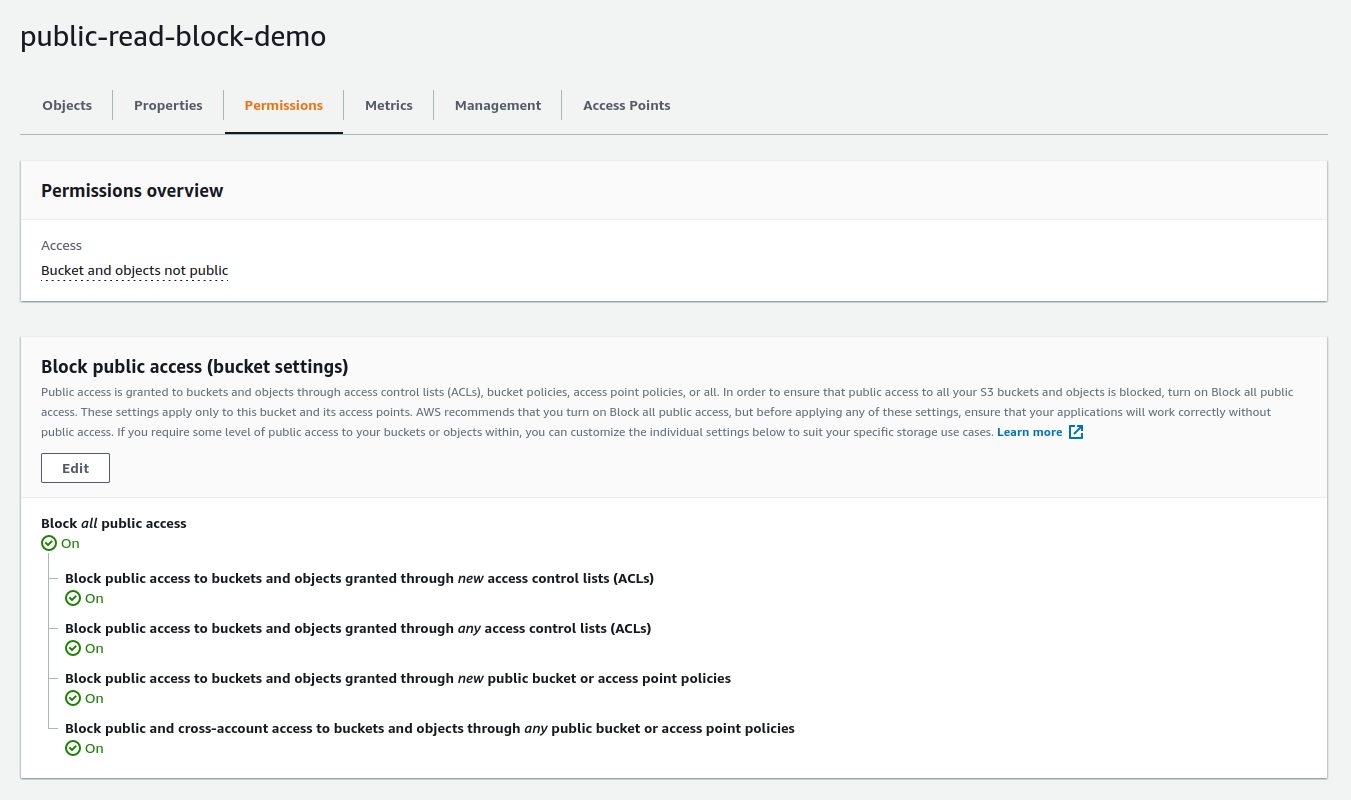
Experiment : Try to access Bucket objects in publicly without doing any change to policy.It wont allow us.

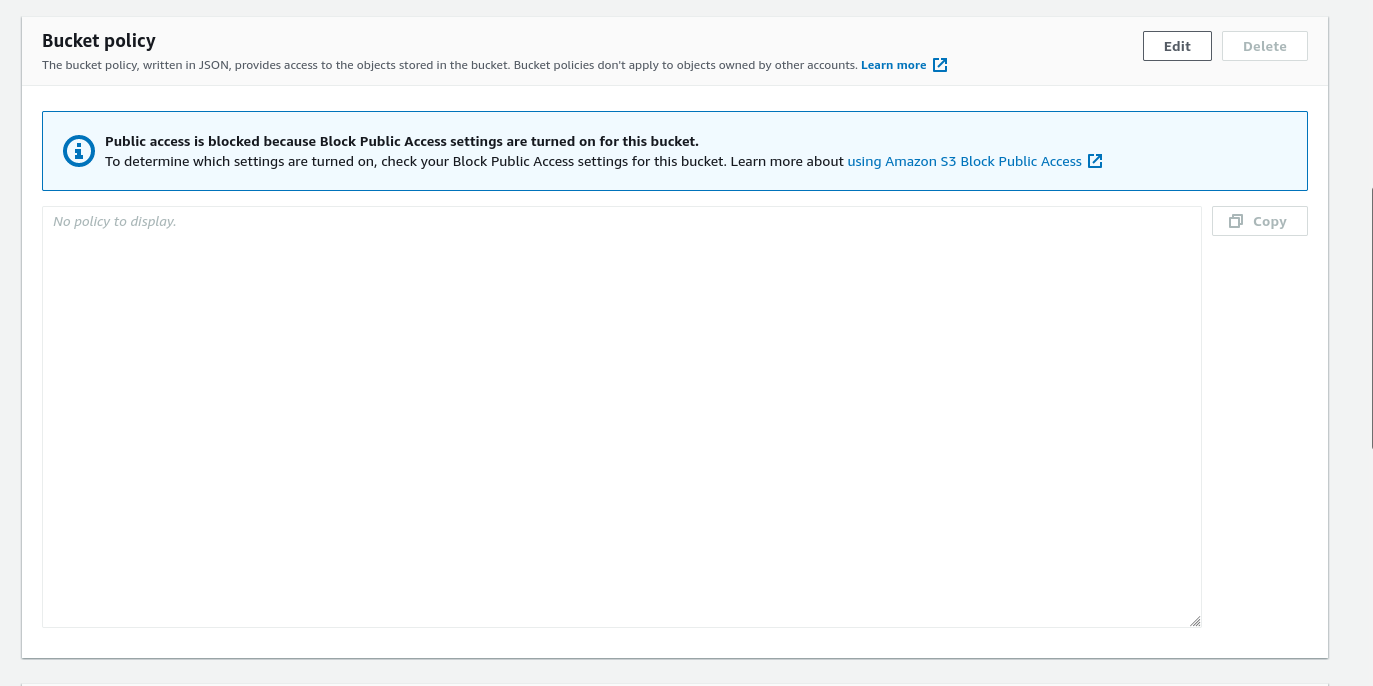


## **Experiment On Public Bucket**

Change Bucket Policy to Public Access

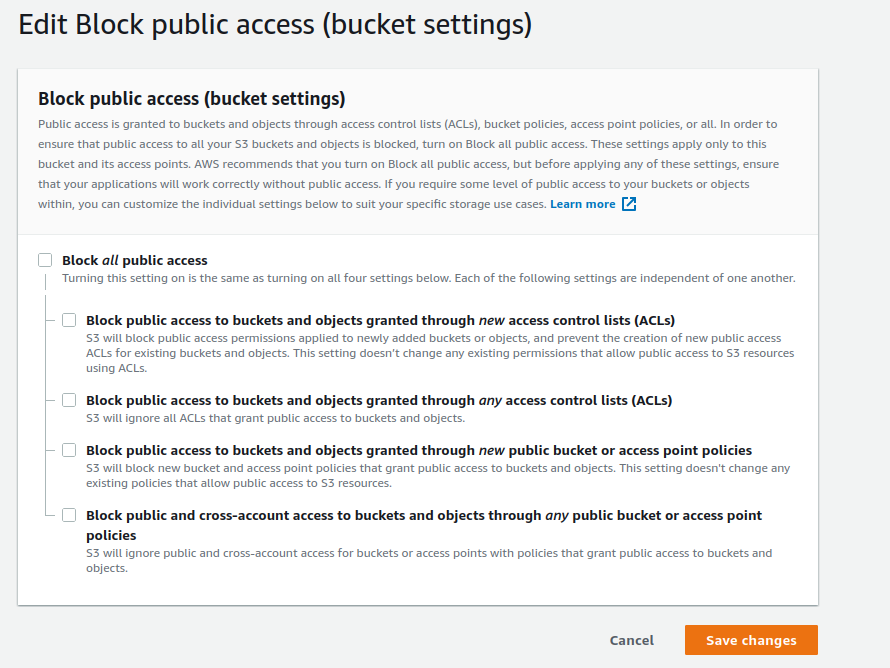
Default Bucket Configs





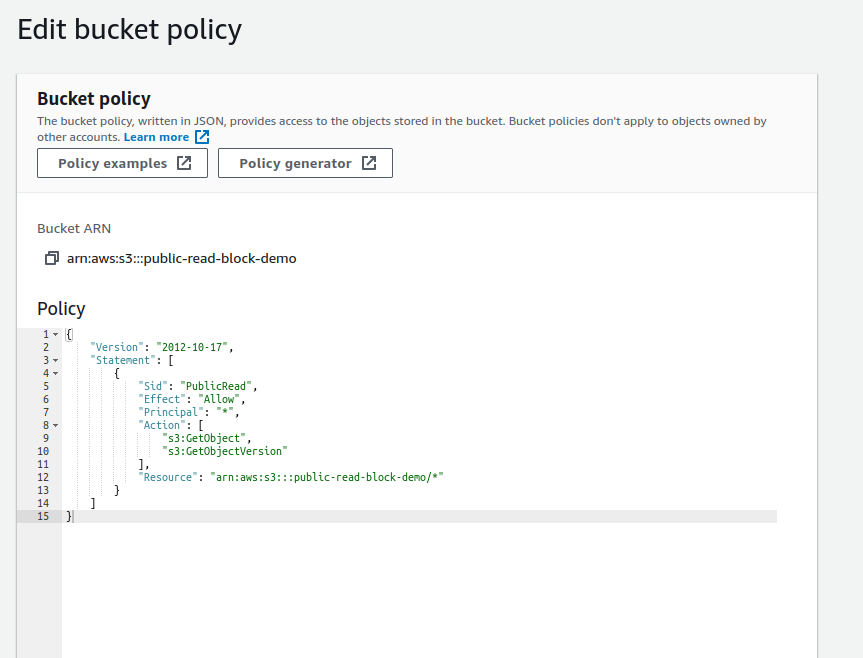
Change Bucket Policy to access public

* Uncheck the checkboxes

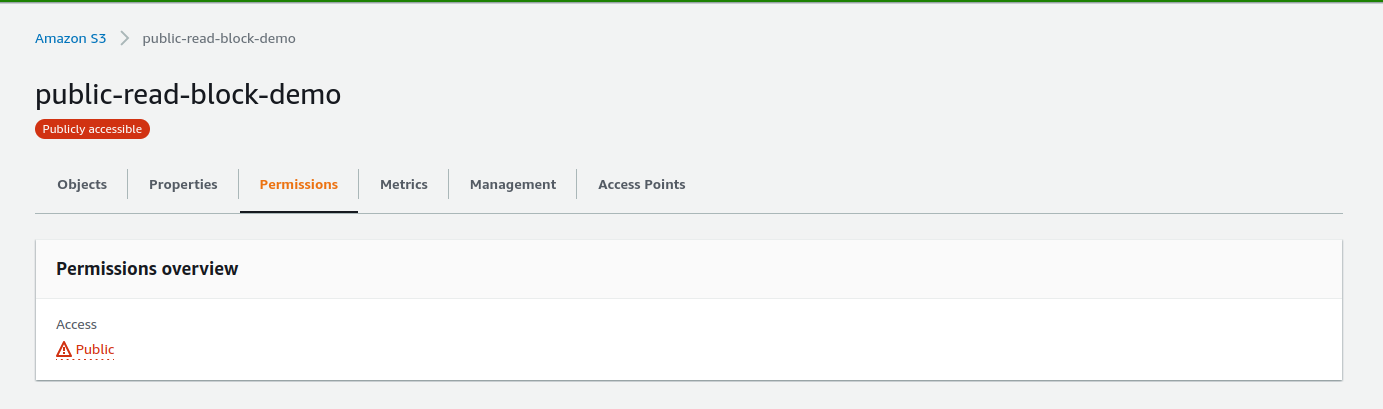


Give below policy

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Sid": "PublicRead",  "Effect": "Allow",  "Principal": "\*",  "Action": [  "s3:GetObject",  "s3:GetObjectVersion"  ],  "Resource": "arn:aws:s3:::public-read-block-demo/\*"  }  ]  } |

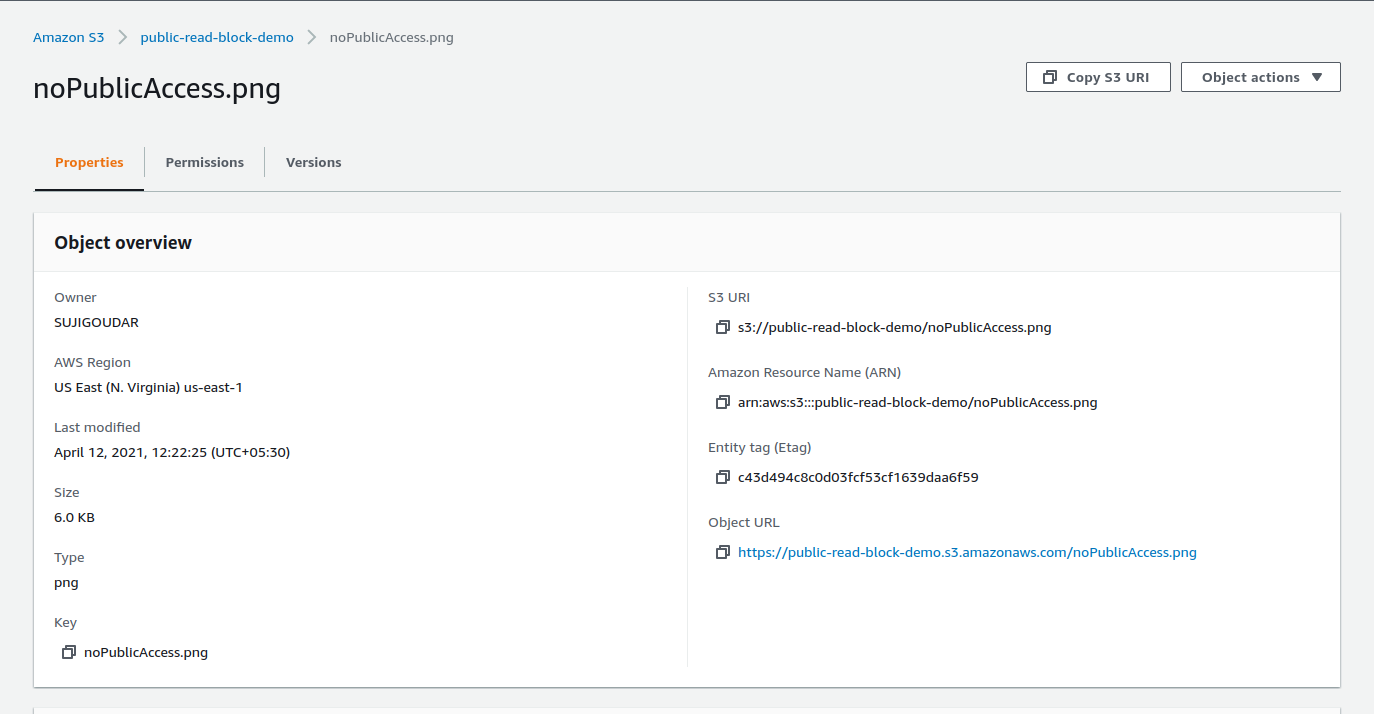


Now we could see this warning(bucket is accessible from internet)

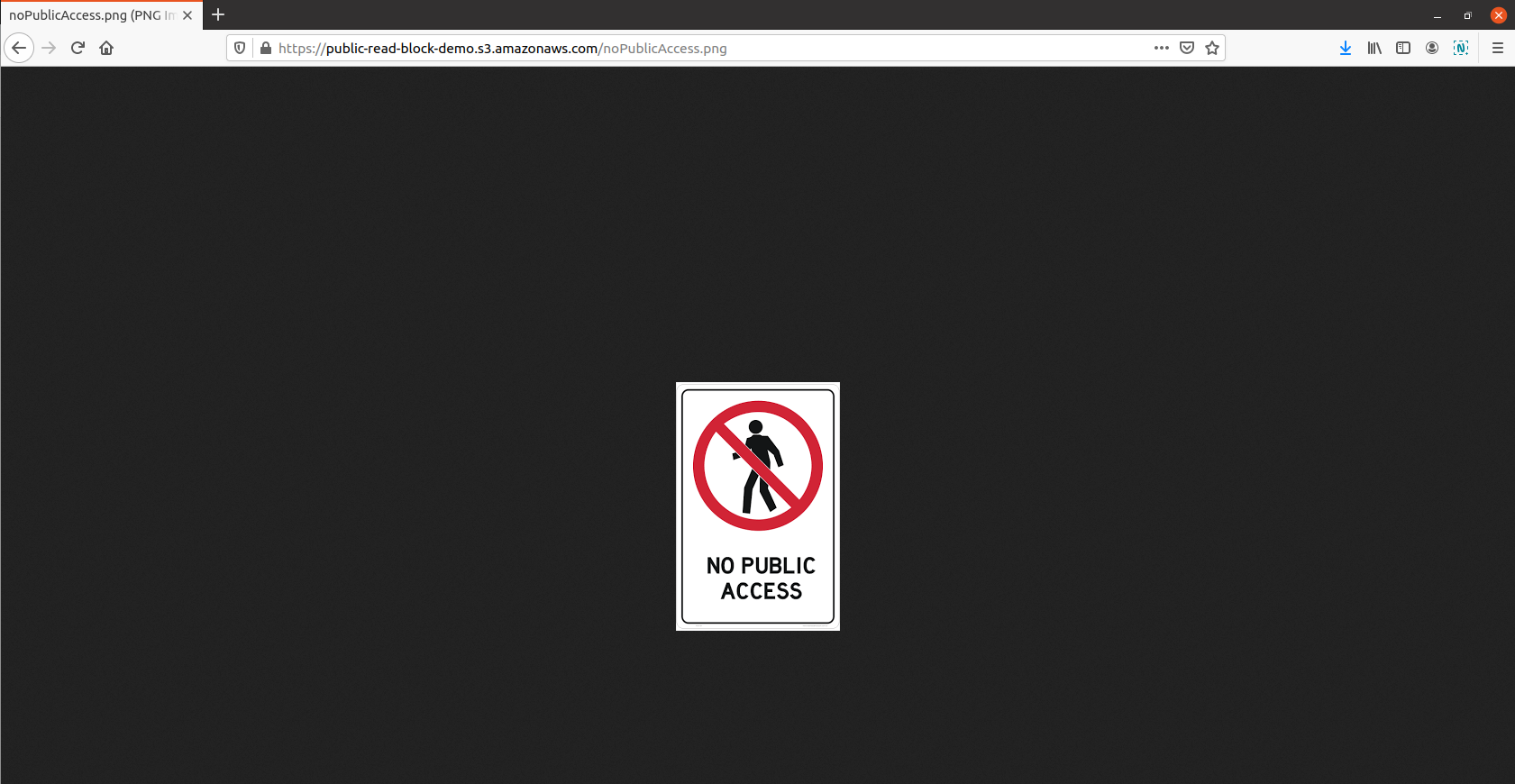


Upload an image and copy object url

<https://public-read-block-demo.s3.amazonaws.com/noPublicAccess.png>

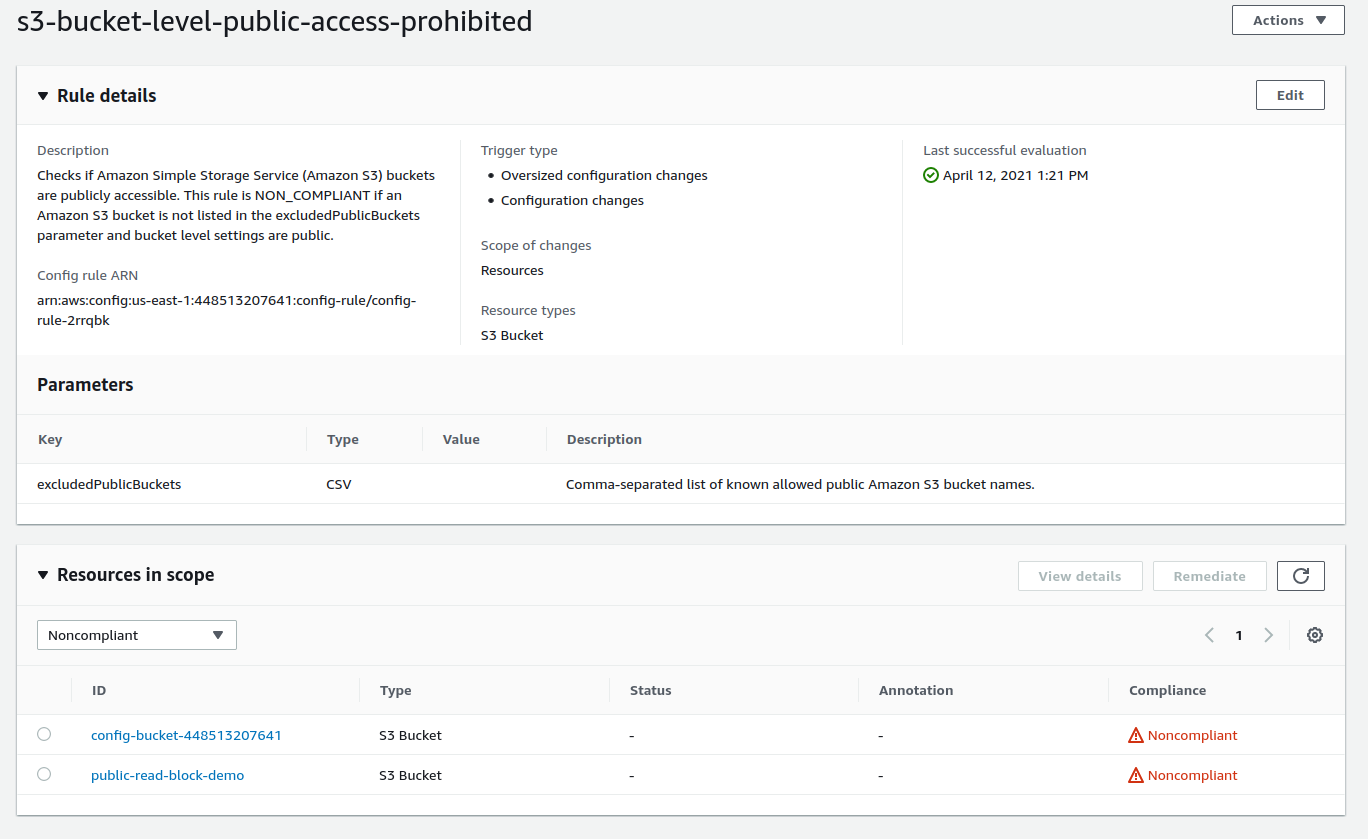


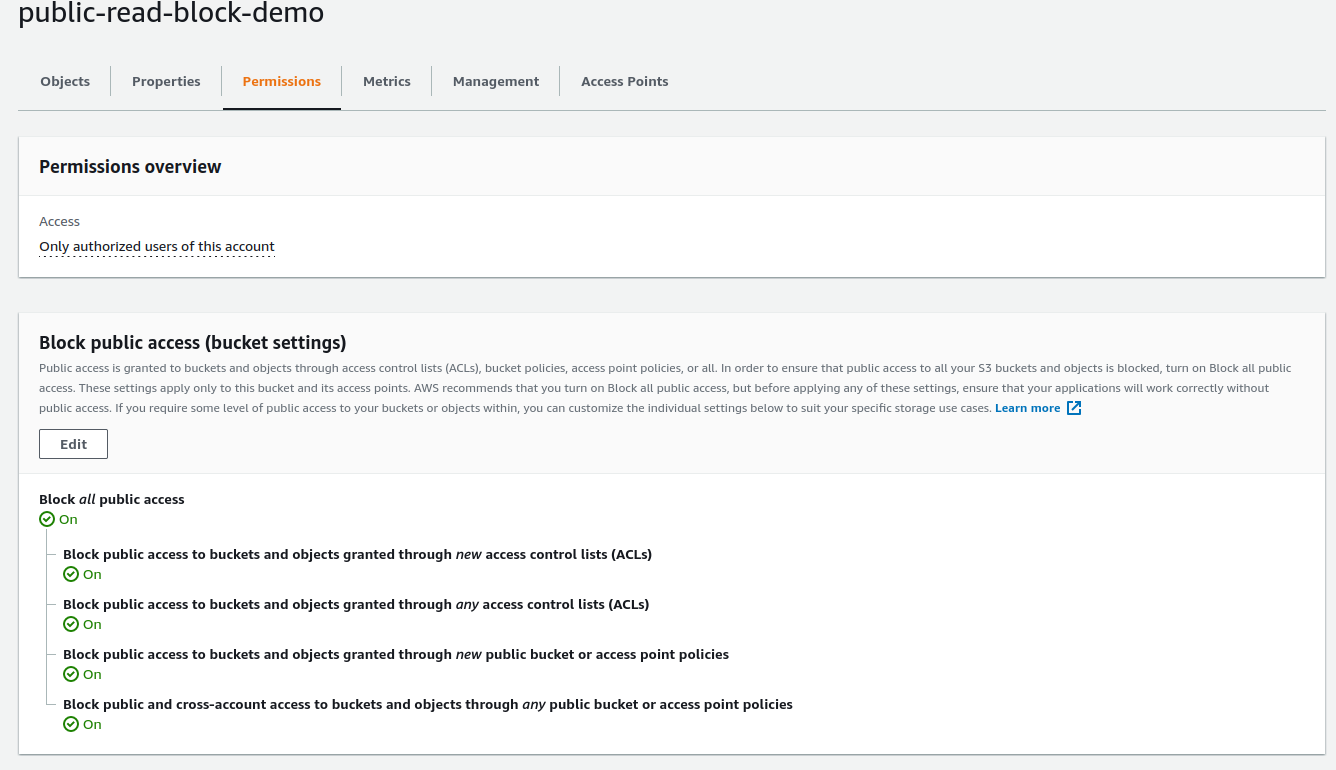
Try to access using private web window



===============================================

After 3-4 minutes , you will receive a sms and when to see the bucket permission , you could see that is changed back to private (automatically)





Supporting Codes:

Lambda

|  |
| --- |
| import json  import boto3 as boto3  s3\_client = boto3.client('s3', region\_name='us-east-1')  sns\_client = boto3.client('sns', region\_name='us-east-1')  def lambda\_handler(event, context):  bucket\_name = "public-read-block-demo"  # new\_result = 'NON\_COMPLIANT'  # old\_result = 'COMPLIANT'  new\_result = event['detail']['newEvaluationResult']['complianceType']  old\_result = event['detail']['oldEvaluationResult']['complianceType']  if new\_result == 'NON\_COMPLIANT':  message = {"BucketInRisk": f'{bucket\_name}'}  response = sns\_client.publish(  TargetArn='arn:aws:sns:us-east-1:448513207641:security-alert-demo',  Message=json.dumps({'default': json.dumps(message)}),  MessageStructure='json'  )  print("Non Compliance S3 Rule")  response\_public = s3\_client.put\_public\_access\_block(  Bucket=bucket\_name,  PublicAccessBlockConfiguration={  'BlockPublicAcls': True,  'IgnorePublicAcls': True,  'BlockPublicPolicy': True,  'RestrictPublicBuckets': True  },  )  else:  print(f'Old event status:{old\_result}') |