

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

[Create Config Rule](#)

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

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

[Experiment On Private Bucket](#)

[Experiment On Public Bucket](#)

Create S3 Bucket With Private Access (Upload a image)

Create Config Rule

The image shows two screenshots of the AWS Config console. The top screenshot displays the 'Rules' page, which lists existing rules and provides options to view details, edit, or add new rules. The bottom screenshot shows the 'Configure rule' wizard, specifically Step 1: Specify rule type. The wizard guides the user through customizing fields for a new rule, including Name, Description, and Managed rule name.

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules: Any status

View details Edit rule Actions Add rule

Step 1: Specify rule type

Configure rule

Customize any of the following fields

Details

Name
A unique name for the rule. 128 characters max. No special characters or spaces.

s3-bucket-level-public-access-prohibited

Description

Checks if Amazon Simple Storage Service (Amazon S3) buckets are publicly accessible. This rule is NON_COMPLIANT if an Amazon S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.

Managed rule name

S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

Keep other settings as defaults and create rule.

AWS Config > Rules

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

Any status ▼

View details Edit rule Actions ▼ Add rule

< 1 > ⚙

| | Name | Remediation action | Type | Compliance |
|-----------------------|--|--------------------|-------------|------------|
| <input type="radio"/> | s3-bucket-level-public-access-prohibited | Not set | AWS managed | - |

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

AWS Config ×

s3-bucket-level-public-access-prohibited

Actions ▼

▼ Rule details

Edit

Description

Checks if Amazon Simple Storage Service (Amazon S3) buckets are publicly accessible. This rule is NON_COMPLIANT if an Amazon S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.

Config rule ARN
arn:aws:config:us-east-1:448513207641:config-rule/config-rule-2mqbk

Trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

S3 Bucket

Last successful evaluation

✓ April 12, 2021 1:08 PM

Parameters

| Key | Type | Value | Description |
|-----------------------|------|-------|--|
| excludedPublicBuckets | CSV | | Comma-separated list of known allowed public Amazon S3 bucket names. |

▼ Resources in scope

View details Remediate ↻

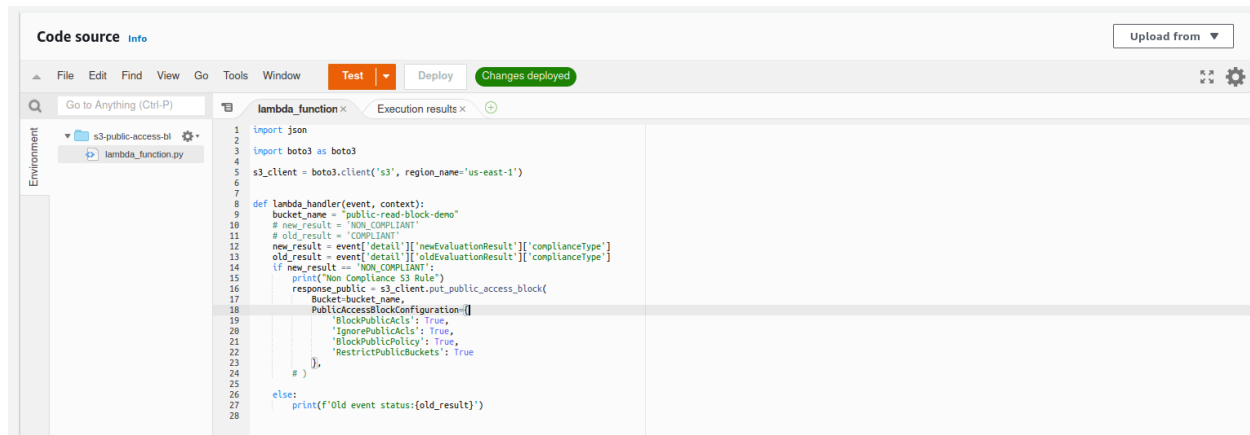
Compliant ▼

< 1 > ⚙

| | ID | Type | Status | Annotation | Compliance |
|-----------------------|--------------------------------------|-----------|--------|------------|-------------|
| <input type="radio"/> | aws-cloudtrail-logs-448513207641-... | S3 Bucket | - | - | ✓ Compliant |
| <input type="radio"/> | public-read-block-demo | S3 Bucket | - | - | ✓ Compliant |

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

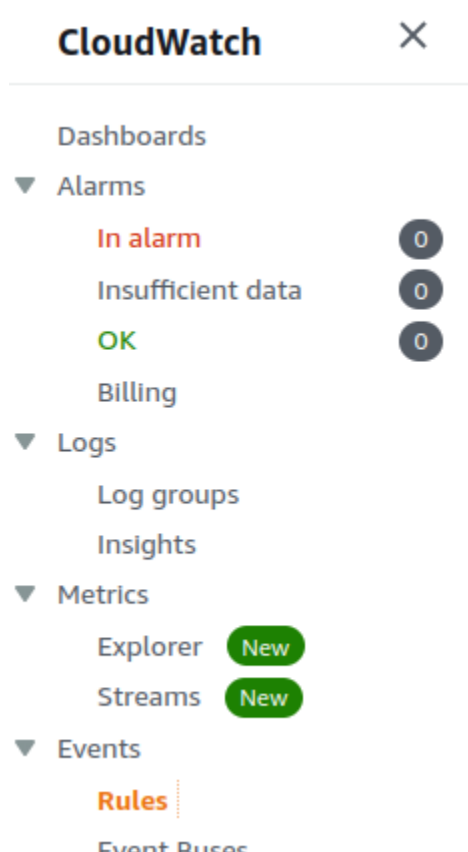


The screenshot shows the AWS Code Editor interface. The top bar includes 'Code source' and 'Info' tabs, along with an 'Upload from' button. Below this is a menu bar with 'File', 'Edit', 'Find', 'View', 'Go', 'Tools', and 'Window'. The main editor area displays a Python script for a lambda function named 'lambda_function'. The script imports 'json' and 'boto3', initializes an S3 client for 'us-east-1', and defines a 'lambda_handler' function. The handler checks the 'complianceType' of a bucket. If it's 'NON_COMPLIANT', it prints a message and calls 's3_client.put_public_access_block' with a 'PublicAccessBlockConfiguration' dictionary. The dictionary includes 'BlockPublicAcls' (True), 'IgnorePublicAcls' (True), 'BlockPublicPolicy' (True), and 'RestrictPublicBuckets' (True). If the bucket is 'COMPLIANT', it prints a message. The script ends with a 'print' statement for the old event status.

```
1 import json
2
3 import boto3 as boto3
4
5 s3_client = boto3.client('s3', region_name='us-east-1')
6
7
8 def lambda_handler(event, context):
9     bucket_name = 'public-read-block-deno'
10    # new_result = 'NON_COMPLIANT'
11    # old_result = 'COMPLIANT'
12    new_result = event['detail']['newEvaluationResult']['complianceType']
13    old_result = event['detail']['oldEvaluationResult']['complianceType']
14    if new_result == 'NON_COMPLIANT':
15        print("Non Compliance S3 Rule")
16        response_public = s3_client.put_public_access_block(
17            Bucket=bucket_name,
18            PublicAccessBlockConfiguration={
19                'BlockPublicAcls': True,
20                'IgnorePublicAcls': True,
21                'BlockPublicPolicy': True,
22                'RestrictPublicBuckets': True
23            },
24            # )
25        )
26    else:
27        print(f'Old event status:{old_result}')
28
```

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

Rules

Rules route events from your AWS resources for processing by selected targets. You can create, edit, and delete rules.

Create rule

Actions

Status

All

Name

«

<

Viewing 1 to 2 of 2 Rules

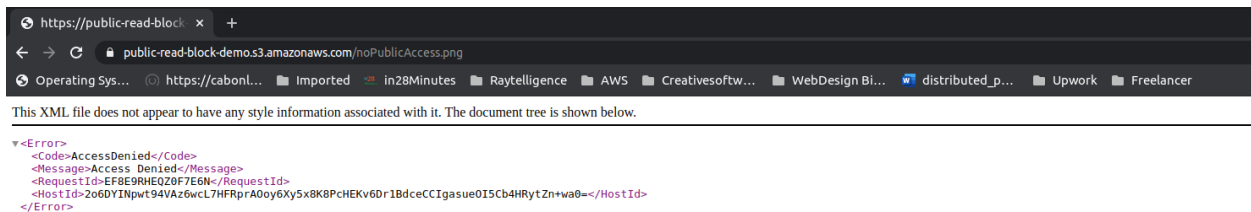
>

»

| Status | Name | Description |
|-----------------------|----------------------------------|------------------------|
| <input type="radio"/> | <input checked="" type="radio"/> | block-s3-public-access |

Experiment On Private Bucket

Experiment : Try to access Bucket objects in publicly without doing any change to policy. It won't allow us.



Experiment On Public Bucket

Change Bucket Policy to Public Access Default Bucket Configs

public-read-block-demo

[Objects](#)[Properties](#)[Permissions](#)[Metrics](#)[Management](#)[Access Points](#)

Permissions overview

Access

Bucket and objects not public

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

[Edit](#)

Block all public access

☒ On

- Block public access to buckets and objects granted through *new* access control lists (ACLs)**
☒ On
- Block public access to buckets and objects granted through *any* access control lists (ACLs)**
☒ On
- Block public access to buckets and objects granted through *new* public bucket or access point policies**
☒ On
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**
☒ On

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](#)

[Edit](#) [Delete](#)

Public access is blocked because Block Public Access settings are turned on for this bucket.

To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

No policy to display.


[Copy](#)

Change Bucket Policy to access public

- Uncheck the checkboxes

Edit Block public access (bucket settings)

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

☐ **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.

Cancel

Save changes

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/*"
    }
  ]
}
```

Edit bucket policy

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::public-read-block-demo

Policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicRead",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": [  
9         "s3:GetObject",  
10        "s3:GetObjectVersion"  
11      ],  
12      "Resource": "arn:aws:s3::public-read-block-demo/*"  
13    }  
14  ]  
15 }
```

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

Amazon S3 > public-read-block-demo


public-read-block-demo

Publicly accessible

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

Permissions overview

Access

 Public

Upload an image and copy object url

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

Amazon S3 > public-read-block-demo > noPublicAccess.png

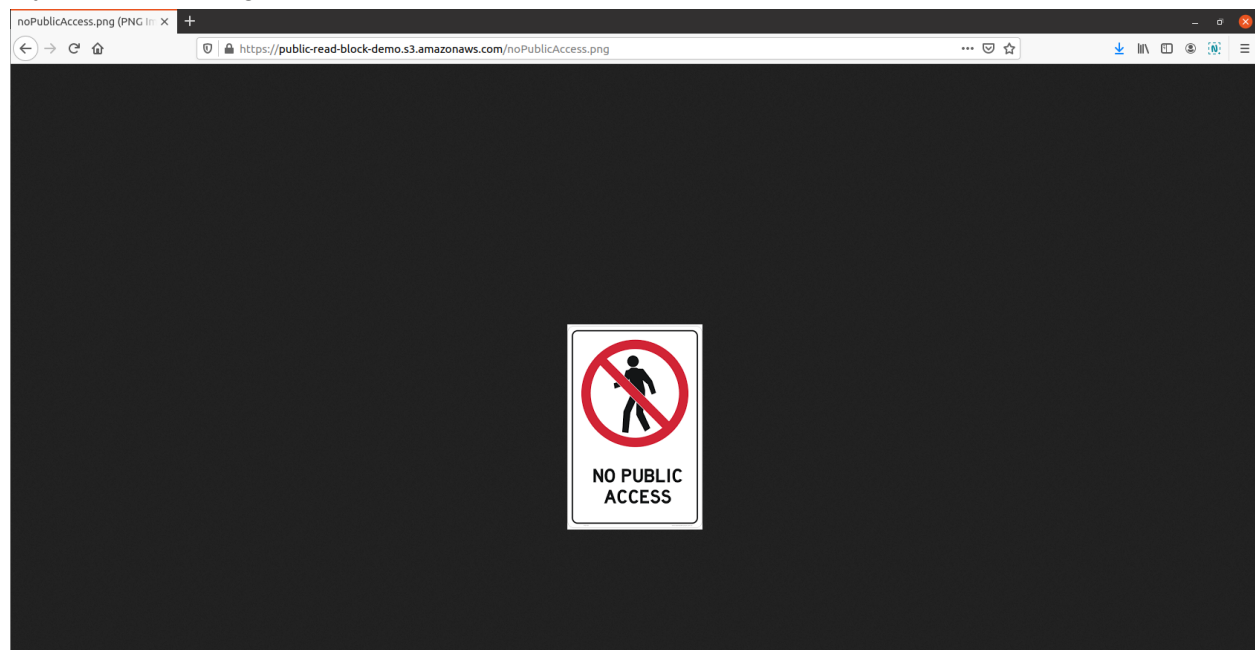
noPublicAccess.png Copy S3 URI Object actions ▼

Properties | Permissions | Versions

Object overview

| | |
|--------------------------------------|--|
| Owner | S3 URI |
| SUJIGOUDAR | s3://public-read-block-demo/noPublicAccess.png |
| AWS Region | Amazon Resource Name (ARN) |
| US East (N. Virginia) us-east-1 | arn:aws:s3:::public-read-block-demo/noPublicAccess.png |
| Last modified | Entity tag (Etag) |
| April 12, 2021, 12:22:25 (UTC+05:30) | c43d494c8c0d03fc53cf1639daa6f59 |
| Size | Object URL |
| 6.0 KB | https://public-read-block-demo.s3.amazonaws.com/noPublicAccess.png |
| Type | |
| png | |
| Key | |
| 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)

s3-bucket-level-public-access-prohibited

Actions ▾

▼ Rule details

Edit

Description

Checks if Amazon Simple Storage Service (Amazon S3) buckets are publicly accessible. This rule is NON_COMPLIANT if an Amazon S3 bucket is not listed in the excludedPublicBuckets parameter and bucket level settings are public.

Config rule ARN

arn:aws:config:us-east-1:448513207641:config-rule/config-rule-2rrqbk

Trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

S3 Bucket

Last successful evaluation

🟢 April 12, 2021 1:21 PM

Parameters

| Key | Type | Value | Description |
|-----------------------|------|-------|--|
| excludedPublicBuckets | CSV | | Comma-separated list of known allowed public Amazon S3 bucket names. |

▼ Resources in scope

View details

Remediate



Noncompliant ▾

< 1 > ⚙

| | ID | Type | Status | Annotation | Compliance |
|-----------------------|--|-----------|--------|------------|----------------|
| <input type="radio"/> | config-bucket-448513207641 | S3 Bucket | - | - | ⚠ Noncompliant |
| <input type="radio"/> | public-read-block-demo | S3 Bucket | - | - | ⚠ Noncompliant |

public-read-block-demo

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

Permissions overview

Access

Only authorized users of this account

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

🟢 On

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

🟢 On

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

🟢 On

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

🟢 On

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

🟢 On

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}')
```