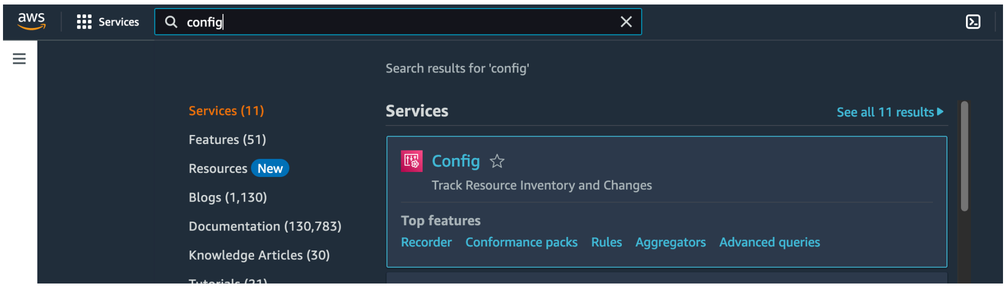
# Use AWS Config Rules to Detect a Public Bucket

AWS Config provides a detailed view of the configuration of AWS resources in your AWS account. With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time.

These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

In this exercise, will show you how to use AWS Config to detect whether a configuration change has made objects within your S3 bucket public.

From the AWS console in the top search bar, search and select `Config` for AWS Config.



Click `Get Started`.

For **Step 1: Settings**, leave the default selections and click `Next`.

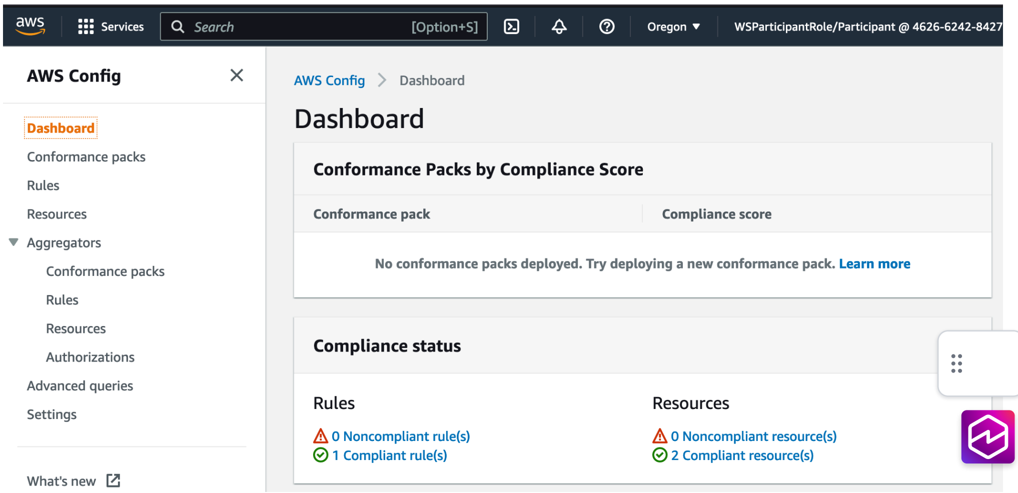
For **Step 2: Rules**, filter the rules by typing `S3` in the search bar. Look for `s3-bucket-public-read-prohibited` and select the rule. Note: If you do not see the rule it is likely on the next page, as the filter only displays 9 rules per page.

Click `Next`.

For **Step 3: Review**, confirm the settings and click `Confirm`.

It may take 2 or 3 minutes for the rule to run. You may need to refresh your page a few times. You should see the **Config Dashboard**. If not, select 'Dashboard' on the left.

Wait until the the Compliant rule(s) is 1



We will configure a bucket policy to allow public read to the `text01` object created in the earlier SSE-KMS encryption lab.

From the AWS console in the top search bar, search and select `S3`.

- Click the bucket name starting with `sid-security-xxxxxxxx`.
- Click on the `Permissions` tab.
- Under `Bucket Policy` click `Edit`

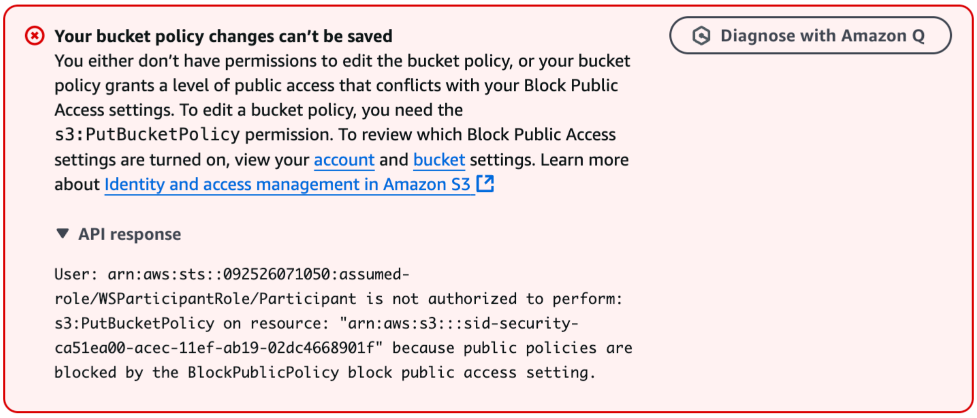
Remove the current policy and replace it with the bucket policy below and paste into the Bucket Policy Editor.

```
{
    "Version": "2012-10-17",
    "Id": "S3-Allow-public-object",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::BUCKET_NAME/text01"
        }
    ]
}
```

ⓘ Ensure your bucket policy keeps the key /text01 after the `BUCKET_NAME`

Replace `BUCKET_NAME` with the bucket name you copied to your text editor and click `Save changes`.

But wait, you should get an error similar to the following:



**Your bucket policy changes can't be saved**

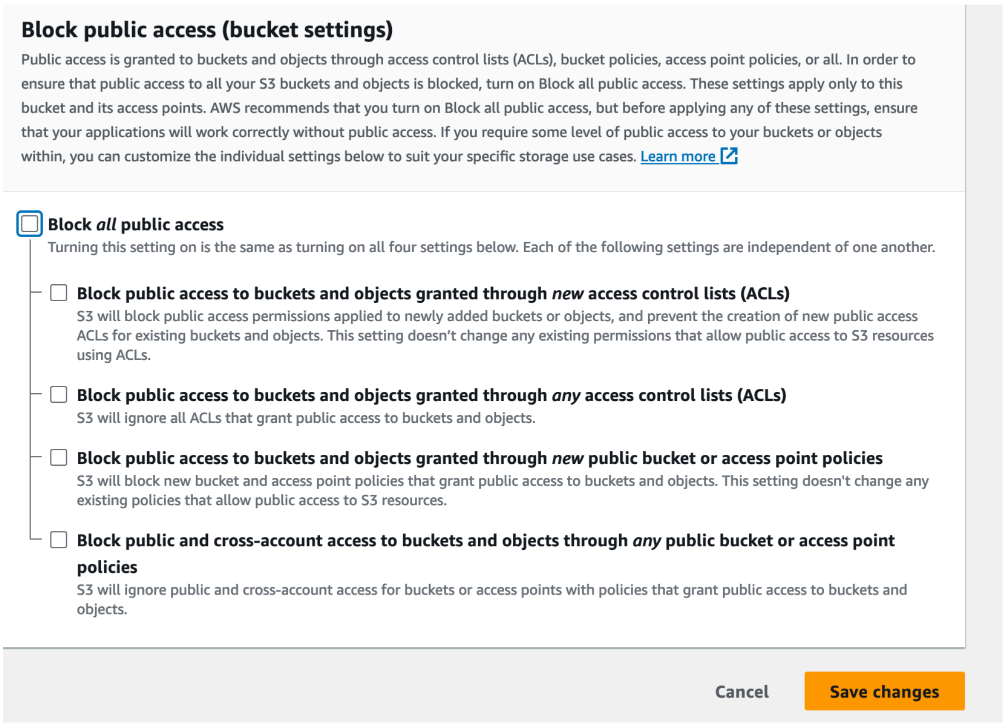
You either don't have permissions to edit the bucket policy, or your bucket policy grants a level of public access that conflicts with your Block Public Access settings. To edit a bucket policy, you need the `s3:PutBucketPolicy` permission. To review which Block Public Access settings are turned on, view your account and bucket settings. Learn more about Identity and access management in Amazon S3

▼ **API response**

```
User: arn:aws:sts::092526071050:assumed-
role/WSParticipantRole/Participant is not authorized to perform:
s3:PutBucketPolicy on resource: "arn:aws:s3:::sid-security-
ca51ea00-acec-11ef-ab19-02dc4668901f" because public policies are
blocked by the BlockPublicPolicy block public access setting.
```

This is because by default `Block public access` is enabled, click `Cancel` and we will disable Block public access for the sake of this lab.

You should be on the `Permissions` tab and click `Edit` under "Block public access (bucket settings)", now uncheck the `Block all public access` checkbox and click `Save changes`. A warning box will pop up and type "confirm" in the text box and click `Confirm`.



### 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.

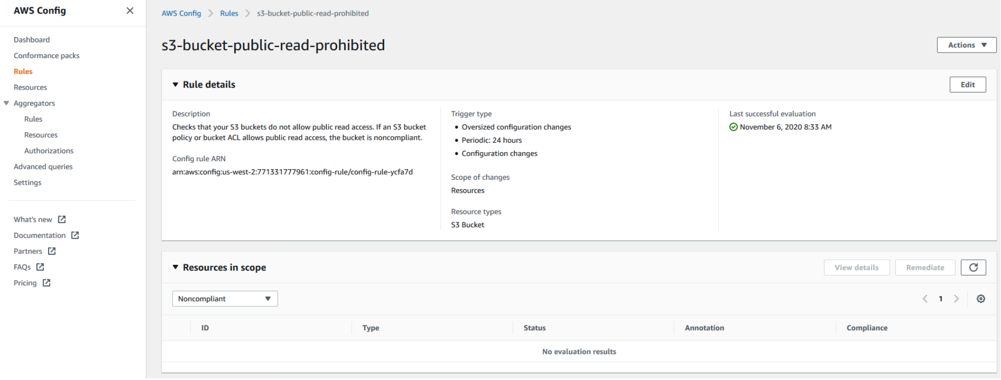
- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any 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.

Scroll back up and copy the bucket policy from before and click `Save changes`. This time the policy will be saved.

From the AWS console, click `Services` and select `Config`.

Click `Rules`.

Click on the `s3-bucket-public-read-prohibited` rule. This should bring you to the following page.



s3-bucket-public-read-prohibited

Rule details

Description
Checks that your S3 buckets do not allow public read access. If an S3 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.

Config rule ARN
arn:aws:config:us-west-2:771331777961:config-rule/config-rule-ycfa7d

Trigger type
- Oversized configuration changes
- Periodic: 24 hours
- Configuration changes

Scope of changes
Resources

Resource types
S3 Bucket

Last successful evaluation
✓ November 6, 2020 8:33 AM

Resources in scope

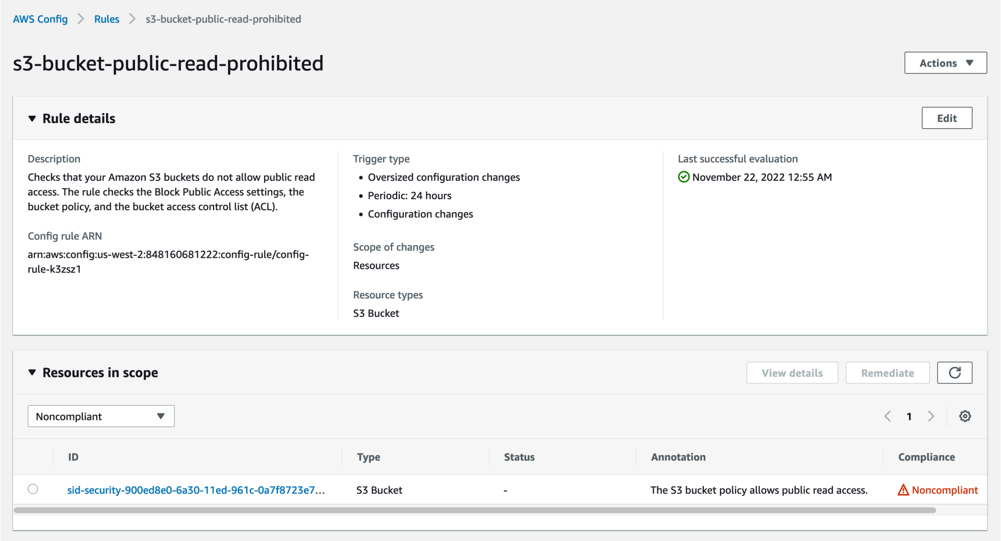
Noncompliant

| ID | Type | Status | Annotation | Compliance |
|---|---|---|---|---|
| No evaluation results | | | | |

Notice there are no non-compliant resources even though you just changed the bucket policy to allow a public object. This is because, this rule runs every 24 hours.

Under the `Actions` tab select `Re-evaluate`. It may take a 2 to 3 minutes for the rule to re-evaluate. If the S3 bucket is not showing up, select `Re-evaluate` again. You may also need to refresh your browser.

Once the rule has successfully run, you will see the non-compliant S3 Bucket because there are objects the bucket policy allows public read.



s3-bucket-public-read-prohibited

▼ Rule details

Description
Checks that your Amazon S3 buckets do not allow public read access. The rule checks the Block Public Access settings, the bucket policy, and the bucket access control list (ACL).

Config rule ARN
arn:aws:config:us-west-2:848160681222:config-rule/config-rule-k3zsz1

Trigger type
- Oversized configuration changes
- Periodic: 24 hours
- Configuration changes

Scope of changes
Resources

Resource types
S3 Bucket

Last successful evaluation
✓ November 22, 2022 12:55 AM

▼ Resources in scope

Noncompliant ▼

| | ID | Type | Status | Annotation | Compliance |
|---|---|---|---|---|---|
| ○ | sid-security-900ed8e0-6a30-11ed-961c-0a7f8723e7... | S3 Bucket | - | The S3 bucket policy allows public read access. | ⚠ Noncompliant |

For more information, see the below link for an example of an AWS Config Rule for S3 following operational best practices. https://docs.aws.amazon.com/config/latest/developerguide/operational-best-practices-for-amazon-s3.html

Previous Next