

Continuous Compliance & Change Management in AWS

Jeffrey Obi
February 2026

Objective

To set up **AWS Config** and **AWS Simple Notification Service (SNS)** to enable automatic real-time alerting via email when an S3 bucket is made public, unsecure and non-compliant.

Phase 1: Setting up AWS Config

Step 1: Open the AWS Config Service Page

Type "AWS Config" in the search bar & click the **AWS Config** icon • Click **Get Started**.

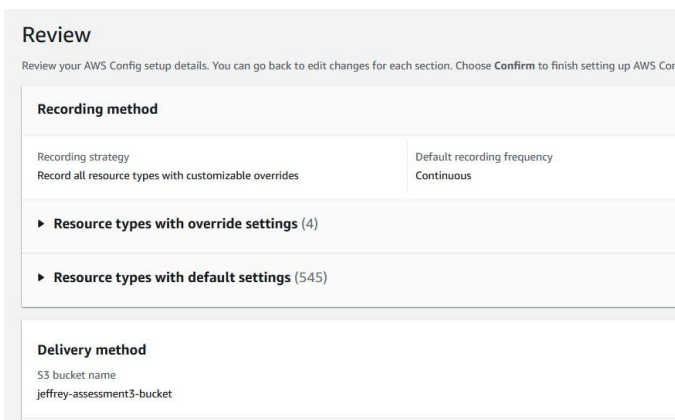


Step 2: Configure Settings

On the **Settings** page, configure the following:

- Recording Strategy: **All resource types...** • IAM role for AWS Config: **Create AWS Config** • Delivery channel: **Create a bucket** • S3 Bucket name: **jeffrey-assessment3-bucket** •

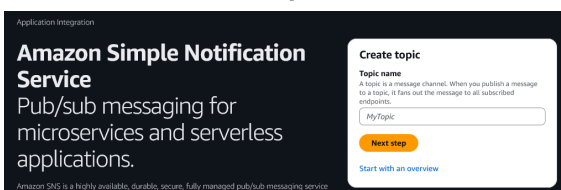
Click **Next** → **Rules** page → **Next** → **Review** page → **Confirm**.



Phase 2: Setting up AWS SNS

Step 1: Open the AWS SNS Page

Search "AWS Simple Notification Service" in the search bar & click **Simple Notification Service**.

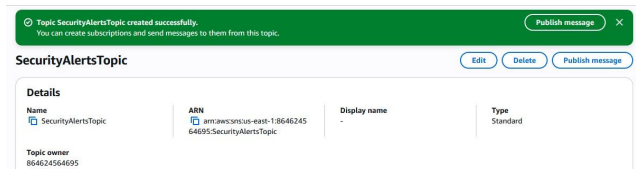


Step 2: Create Topic

AWS SNS → **Topics** → **Create topic** • Configure the following:

- **Type: Standard** • **Name: SecurityAlertsTopic**

Click **Create topic**.



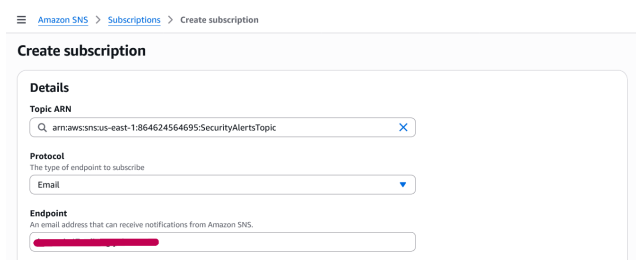
Step 3: Configure Alert Subscription

Subscriptions → **Create subscription** •

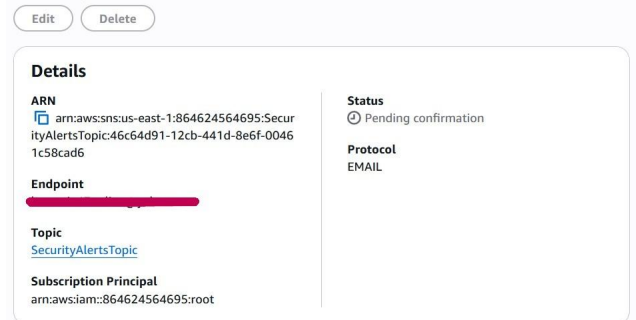
Configure the following:

- **Protocol: Email** • **Endpoint: <emailAddress>** •

Click **Create subscription** • This opens the new subscription's page.

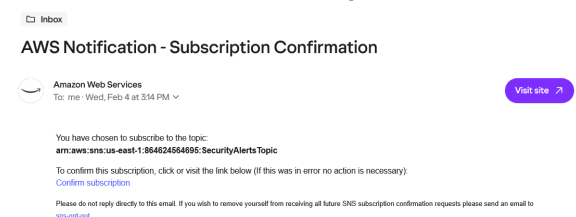


Subscription: 46c64d91-12cb-441d-8e6f-00461c58cad6



Step 4: Confirm Email Alerting

Email inbox → **Subscription Confirmation** email • Click the **Confirm subscription** link.





Simple Notification Service

Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-east-1:864624564695:SecurityAlertsTopic:46c64d91-12cb-441d-8e6f-00461c58cad6

If it was not your intention to subscribe, [click here to unsubscribe](#).

Phase 3: Adding Compliance Rule & Linking SNS

Step 1: Add Rule

AWS Config → Rules → Add Rule • Under **Select rule type**, select **Add AWS Managed Rule** • Under **AWS Managed Rules**, search “s3-bucket-public-read-prohibited” • Check the rule checkbox • Click **Next** → **Configure rule page** → **Next** → **Review and create page** → **Save**.

Specify rule type

Add rules to help you manage the ideal configuration settings of your AWS resources. You can add any of the following predefined, customizable AWS Config Managed Rules, or you can create your own AWS Config Custom rule using AWS Lambda functions or Guard Custom policy.

Select rule type**Add AWS managed rule**

Select the following managed rules in their default state or customize to suit your needs.

Create custom Lambda rule

Use a Lambda function with your custom code to evaluate whether your AWS resources comply with the rule.

Create custom rule using Guard

Use Guard Custom policy that you write to evaluate whether your AWS resources comply with the rule.

AWS Managed Rules (725)

Find Rules

Name = s3-bucket-public-read-prohibited 1 match

Name	Resource types	Trigger type	Description	Supported evaluation mode	Labels
s3-bucket-public-read-prohibited	AWS::S3::Bucket	HYBRID	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).	DETECTIVE	S3, Zekova

Cancel Next

Step 2: Access AWS Config Settings

AWS Config → Settings → Data and delivery → **Edit**.

AWS Config > Settings

Settings**Data and delivery**Data retention period and delivery channel settings apply to both the customer managed recorder and all service-linked recorders with paid configuration items (CIs). [Learn more](#)

Data retention period Default period is 7 years	S3 bucket name jeffrey-assessment3-bucket	SNS topic name -
	SNS topic account -	SNS topic region us-east-1

Step 3: Link Rule Configuration to SNS

On the **Edit data and delivery channel settings** page, Configure the following:

Amazon S3 bucket: Choose a bucket from your account • S3 bucket name:

jeffrey-assessment3-bucket • Amazon S3 bucket: Check the **Stream configuration changes**

box • Select **Choose a bucket from your account** • SNS topic name: **SecurityAlertsTopic**. Click **Save**.

Your settings were successfully saved.

AWS Config > Settings

Settings

Data and delivery Edit

Data retention period and delivery channel settings apply to both the customer managed recorder and all service-linked recorders with paid configuration items (CIs). [Learn more](#)

Data retention period Default period is 7 years	S3 bucket name jeffrey-assessment3-bucket	SNS topic name SecurityAlertsTopic
	SNS topic account 864624564695	SNS topic region us-east-1

Phase 4: Testing (The Break & Fix)

Step 1: Create Test Bucket

Search “S3” • Click the **S3** service • **Amazon S3** → **Buckets** → **Create bucket** • Input bucket name (“assessment3-public-bucket”) • Click **Create bucket**.

Amazon S3 > Buckets

General purpose buckets**Directory buckets****General purpose buckets (2)**

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
assessment3-public-bucket	US East (N. Virginia) us-east-1	February 4, 2026, 15:57:34 (UTC+01:00)
jeffrey-assessment3-bucket	US East (N. Virginia) us-east-1	February 4, 2026, 14:57:50 (UTC+01:00)

Step 2: Unblock Public Access to Bucket

Buckets → **assessment3-public-bucket** → **Permissions tab** → **Block all public access** → **Edit** • Uncheck **Block all public access** • Check I acknowledge that...

Block public access (bucket settings)

Edit

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**

OFF

Individual Block Public Access settings for this bucket

Step 3: Add Public Access Policy to Bucket

Bucket policy → **Edit** • Paste public access policy string in the **Policy CLI** & click **Create policy**

Bucket policy

Edit

Delete

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": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::assessment3-public-bucket/*"
    }
  ]
}
```

Copy

Step 4: Confirm Noncompliance on Dashboard

AWS Config → Dashboard → Compliance status & Noncompliant rules

Compliance status

Rules

0 Noncompliant rule(s)
1 Compliant rule(s)

Resources

1 Noncompliant resource(s)
1 Compliant resource(s)

Noncompliant rules by noncompliant resource count

Name	Compliance
s3-bucket-public-read-prohi...	1 Noncompliant resource(s)

[View all noncompliant rules](#)

Step 5: Confirm Noncompliance via Email

Find the “Noncompliant” notification mail from the email inbox.

Inbox

[AWS Config:us-east-1] AWS::Config::ResourceCompliance AWS::S3::Bucket/assessment3-public-bucket ...

**Amazon Web Services**
To: me - Wed, Feb 4 at 4:10 PM

[Visit site](#)

View the Timeline for this Resource in AWS Config Management Console:
<https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::Config::ResourceCompliance/AWS%253A%253AS3%253A%253ABucket%252Fassessment3-public-bucket?time=2026-02-04T15:10:03.688Z>

New State and Change Record:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration configRuleList.1": {
        "previousValue": null,
        "updatedValue": {
          "configRuleArn": "arn:aws:config:us-east-1:864624564695:config-rule:config-rule-zlmnym",
          "configRuleId": "config-rule-zlmnym",
          "configRuleName": "s3-bucket-public-read-prohibited",
          "complianceType": "NONCOMPLIANT"
        }
      }
    }
  }
}
```

Step 6: View Resource Timeline

AWS Config → Resources → Compliance (Noncompliant) → Apply → assessment-public-bucket → Timeline

Events
All times are in Africa/Lagos (UTC+01:00)

End date: 2026/02/04
Event type: All event types

February 4, 2026

16:10:03

Rule compliance

1 Noncompliant rule(s)

1 rule(s) applied

16:09:29

Configuration change

16:08:05

CloudTrail Event

15:58:35

Rule compliance

All compliant

1 rule(s) applied

15:58:04

Configuration change

15:57:35

CloudTrail Event

15:57:34

CloudTrail Event

15:57:33

CloudTrail Event

Step 7: Undo Test Bucket Public Access

Amazon S3 → Buckets → assessment3-public-bucket → Permissions tab → Block public access → Edit → Block all public access

Block public access (bucket settings) [Edit](#)

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
On
Individual Block Public Access settings for this bucket

Permissions tab → Bucket policy → Delete

Successfully edited Block Public Access settings for this bucket.

Success
Successfully deleted bucket policy for "assessment3-public-bucket"

Bucket policy [Edit](#) [Delete](#)

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](#)

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](#)

Step 8: Confirm Compliance on Dashboard

AWS Config → Dashboard → Compliance status & Noncompliant rules

Compliance status

Rules

0 Noncompliant rule(s)
1 Compliant rule(s)

Resources

0 Noncompliant resource(s)
2 Compliant resource(s)

Noncompliant rules by noncompliant resource count

Name	Compliance
------	------------

[View all noncompliant rules](#)

Step 9: Confirm Compliance via Email

Find the “Compliant” notification mail from the email inbox.

Inbox

[AWS Config:us-east-1] AWS::Config::ResourceCompliance AWS::S3::Bucket/assessment3-public-bucket ...

**Amazon Web Services**
To: me - Wed, Feb 4 at 4:26 PM

[Visit site](#)

View the Timeline for this Resource in AWS Config Management Console:
<https://console.aws.amazon.com/config/home?region=us-east-1#/timeline/AWS::Config::ResourceCompliance/AWS%253A%253AS3%253A%253ABucket%252Fassessment3-public-bucket?time=2026-02-04T15:26:24.903Z>

New State and Change Record:

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration configRuleList.1": {
        "previousValue": null,
        "updatedValue": {
          "configRuleArn": "arn:aws:config:us-east-1:864624564695:config-rule:config-rule-zlmnym",
          "configRuleId": "config-rule-zlmnym",
          "configRuleName": "s3-bucket-public-read-prohibited",
          "complianceType": "COMPLIANT"
        }
      }
    }
  },
  "changeType": "CREATE"
}
```