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.

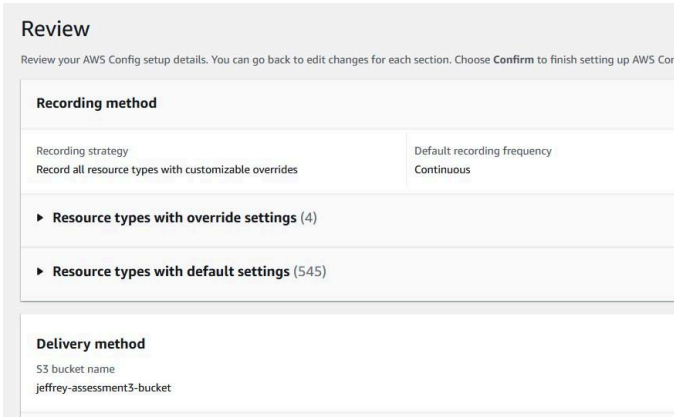
Phase 1: Setting up AWS Config

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

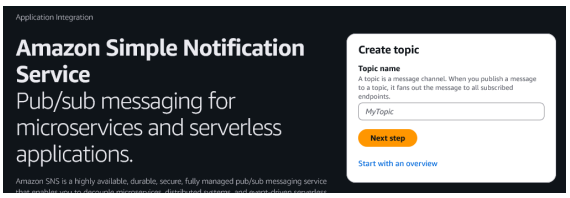
On the **Settings** page, configure the following: • Recording Strategy: **All resource types...** • IAM role for AWS Config: **Create AWS Config** • Delivery channel: **Create a bucket** • S3 Bucket name: **jeffrey-assessment3-bucket** • Click **Next** ➜ **Rules** page ➜ **Next** ➜ **Review** page ➜ **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**.

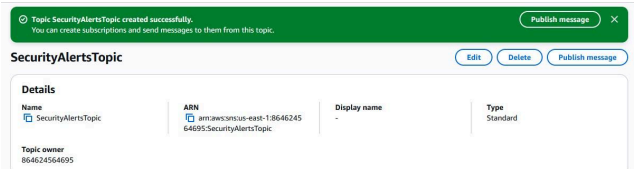


Step 2: Create Topic

AWS SNS ➜ Topics ➜ Create topic • Configure the following:

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

Click **Create topic.**

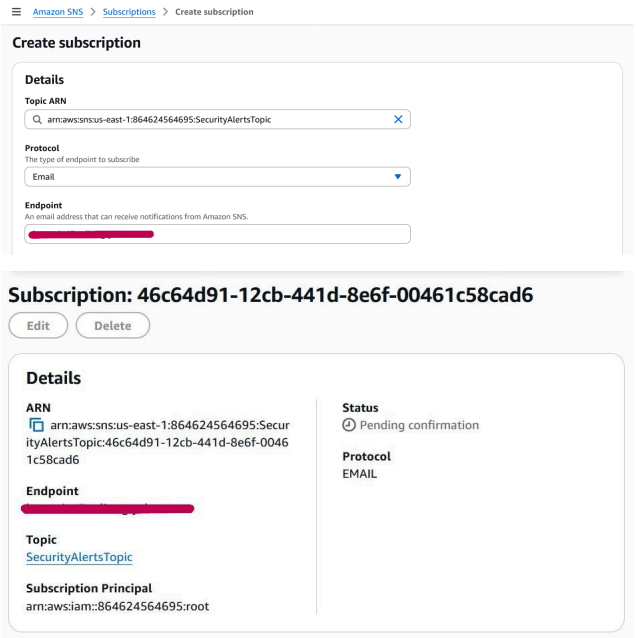


Step 3: Configure Alert Subscription

Subscriptions ➜ Create subscription • Configure the following:

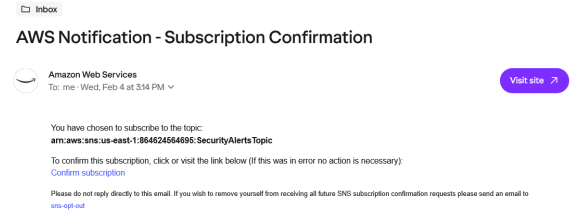
• *Protocol:* ***Email*** • *Endpoint:* ***<emailAddress>*** •

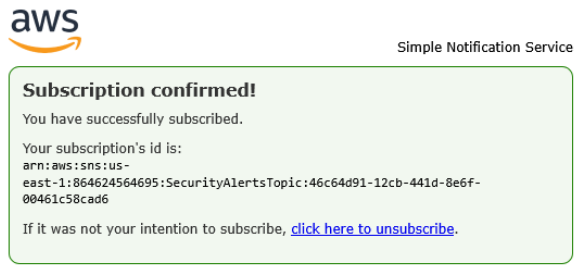
Click **Create subscription** • This opens the new subscription’s page.



Step 4: Confirm Email Alerting

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

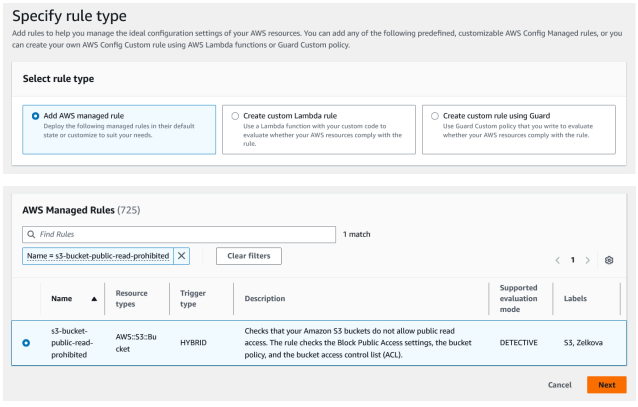




Phase 3: Adding Compliance Rule & Linking SNS

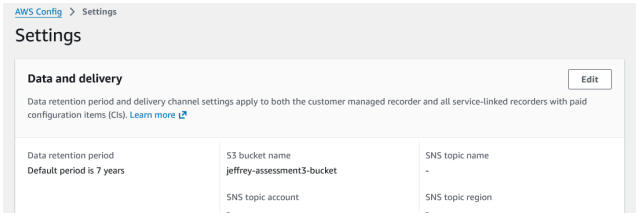
Step 1: Add Rule

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.**



Step 2: Access AWS Config Settings

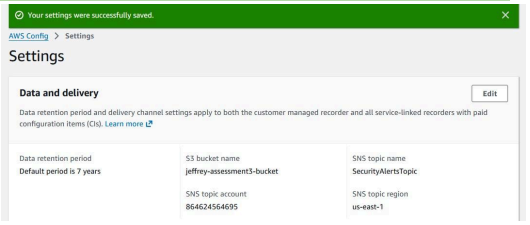
AWS Config ➜ Settings ➜ Data and delivery ➜ Edit.



Step 3: Link Rule Configuration to SNS

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

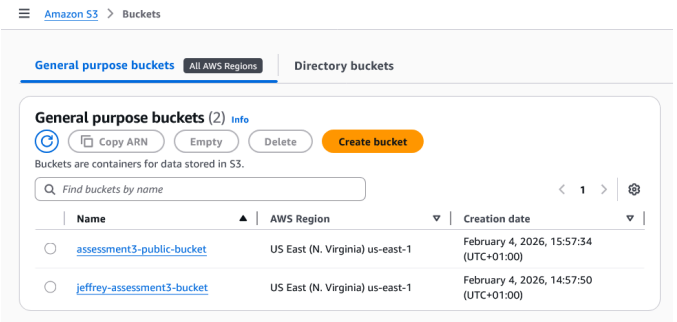
Amazon S3 bucket: **Choose a bucket from your account** • S3 bucket name: **jeffrey-assessment3-bucket** • Amazon S3 bucket: Check the **Stream configuration changes** box • Select **Choose a bucket from your account** • SNS topic name: **SecurityAlertTopic.** Click **Save.**



Phase 4: Testing (The Break & Fix)

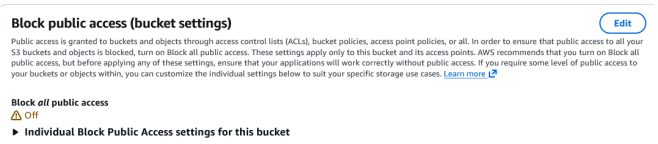
Step 1: Create Test Bucket

Search "S3" • Click the **S3** service • **Amazon S3 ➜ Buckets ➜ Create bucket** • Input bucket name ("assessment3-public-bucket") • Click **Create bucket.**



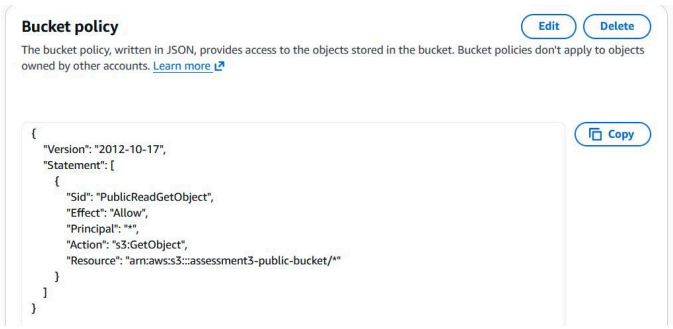
Step 2: Unblock Public Access to Bucket

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



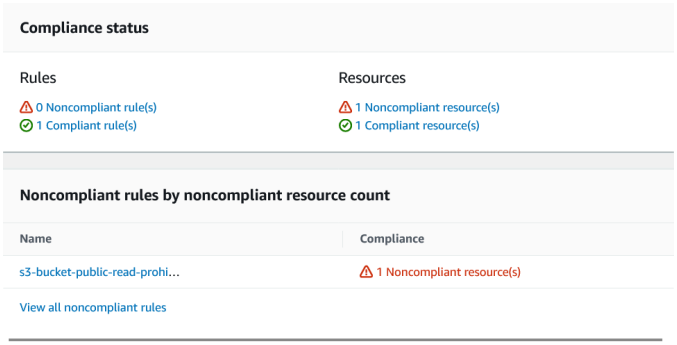
Step 3: Add Public Access Policy to Bucket

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



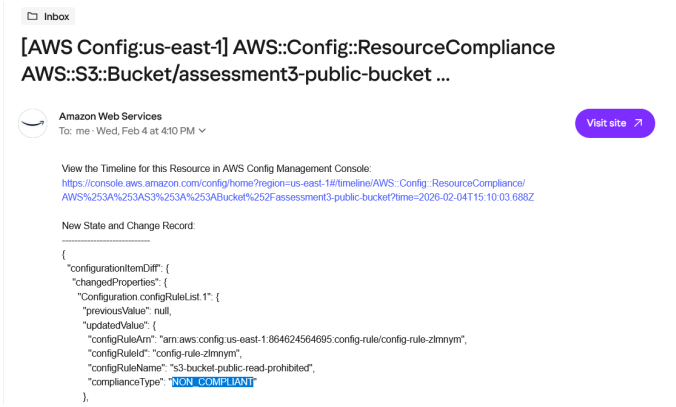
Step 4: Confirm Noncompliance on Dashboard

AWS Config ➜ Dashboard ➜ Compliance status & Noncompliant rules



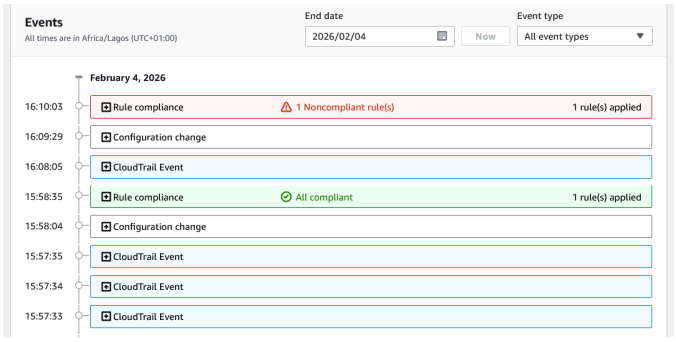
Step 5: Confirm Noncompliance via Email

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



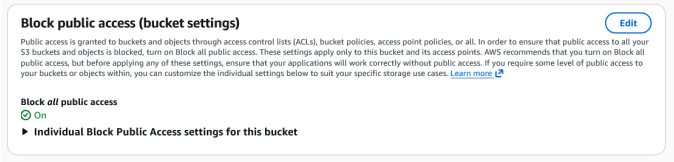
Step 6: View Resource Timeline

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

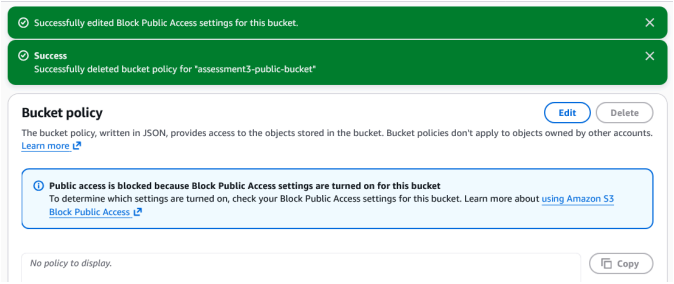


Step 7: Undo Test Bucket Public Access

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

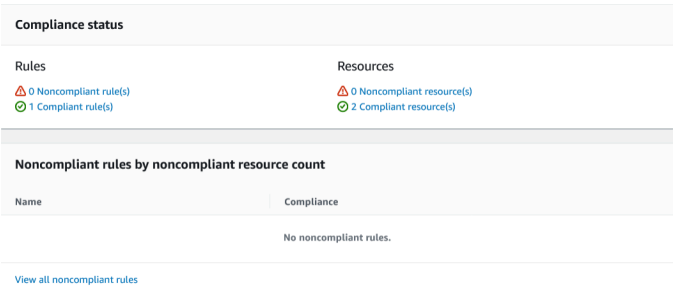


Permissions tab **➜ Bucket policy ➜ Delete**



Step 8: Confirm Compliance on Dashboard

AWS Config ➜ Dashboard ➜ Compliance status & Noncompliant rules



Step 9: Confirm Compliance via Email

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