S3 PreSigned URLs

A Presigned url is a url that you can provide to your users to grant temporary access to specific S3 objects. It contains 3 main parameters to limit the access to the user;

.

1. Create an S3 bucket and make sure Block public access is enabled. Also make sure static website hosting is not active on the bucket
2. Upload an object to the bucket
3. Copy the object url to a web browser and you will notice that you have access denied.
4. Run be below command to enable presign url on that object

   $ aws s3 presign <objecturi> --expires-in <timeinseconds> --region <bucketregion>

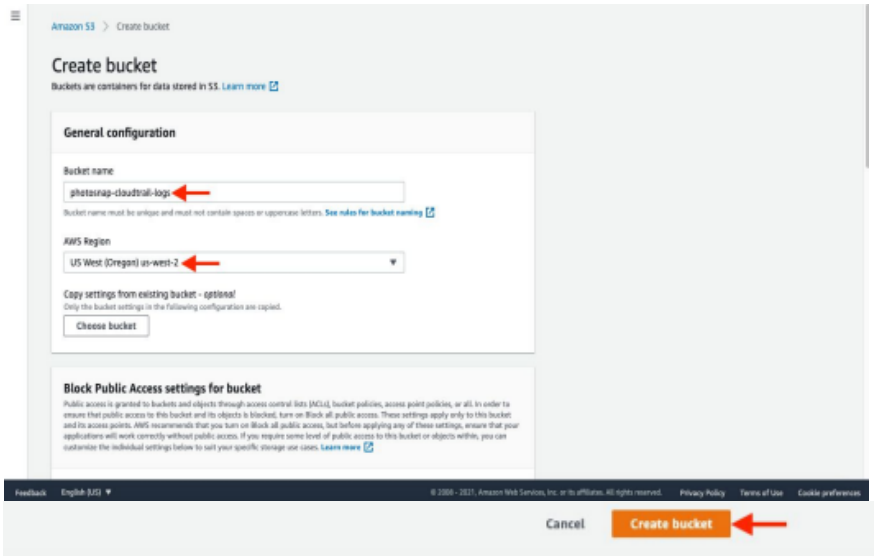
   Ex aws s3 presign s3://susannemith/01.jpg --expires-in 300 —region us-west-2

5. Copy the url created by the command and paste in a browser and you should be able to access the object

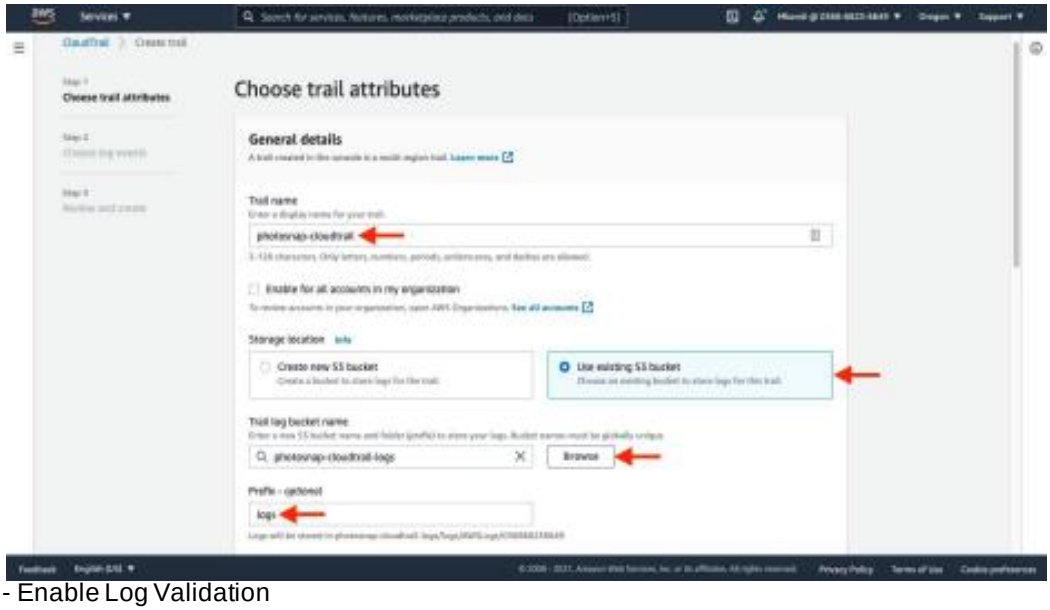
CONFIGURING ACCOUNT LOGGING WITH AWS CLOUDTRAIL

Cloudtrail is a governance service service that enables compliance and risk auditing in AWS accounts.

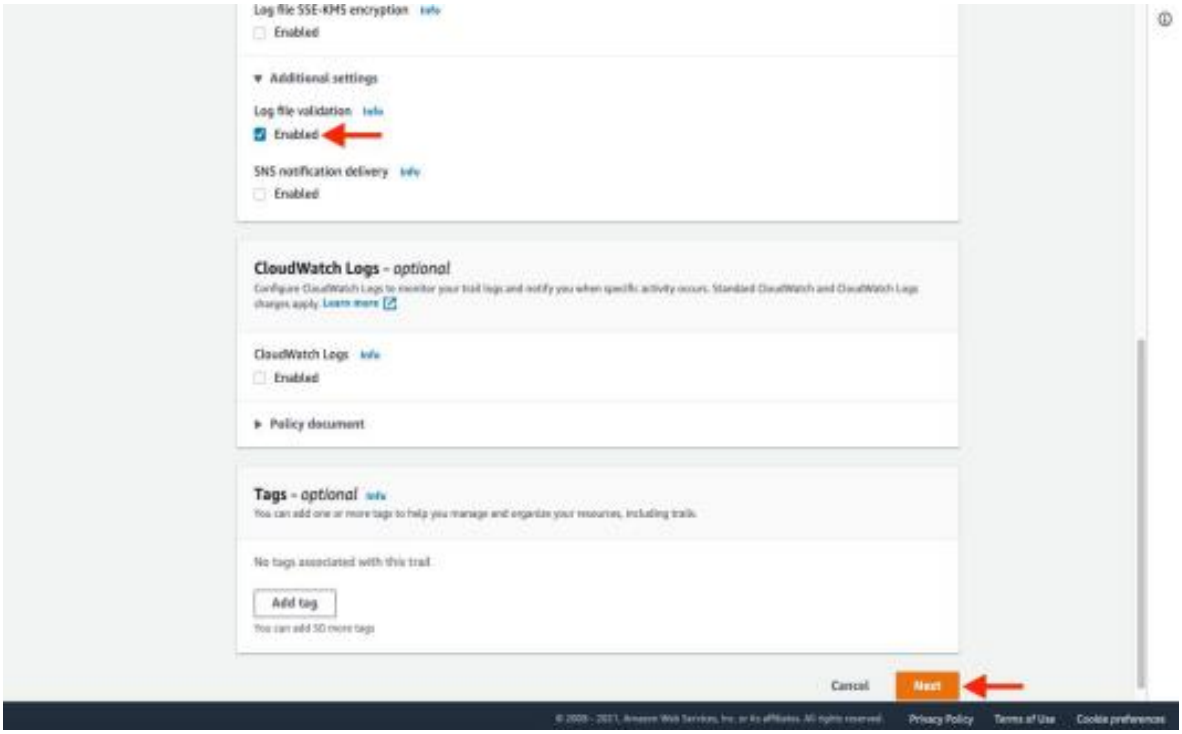
1. Create an S3 bucket and give it a name of your choice. Remember bucket names are globally unique and all lower case.
   a. Upload an object to the bucket (optional)



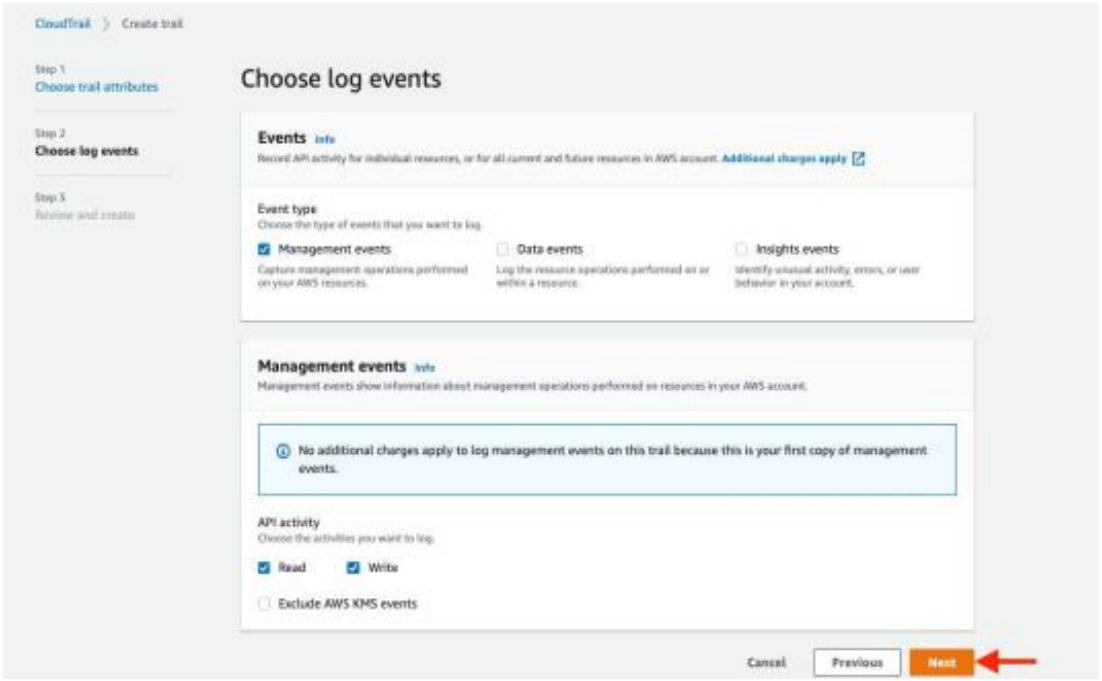
2. Configuring Account Logging With AWS CloudTrail
    a. Creating a trail



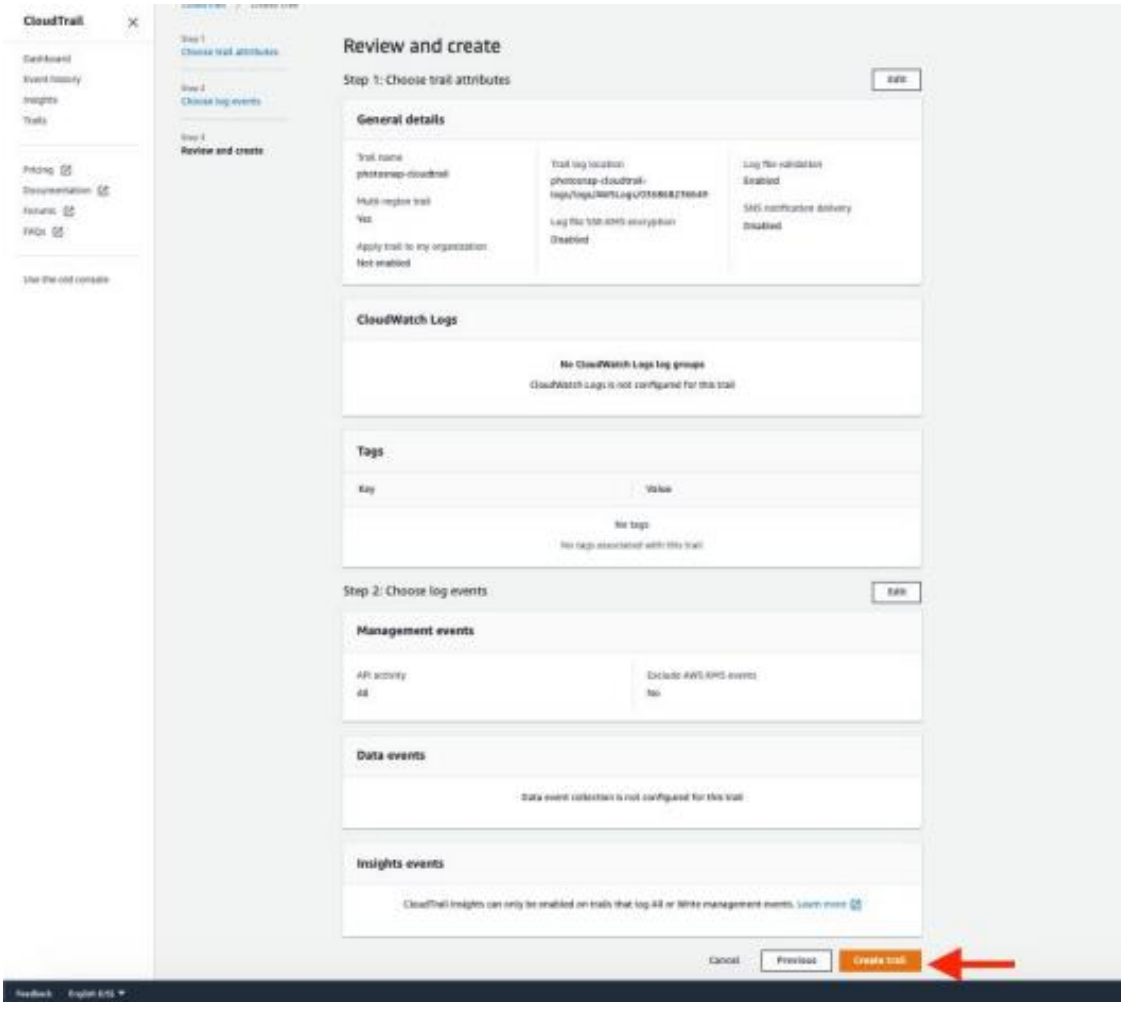
- Enable Log Validation



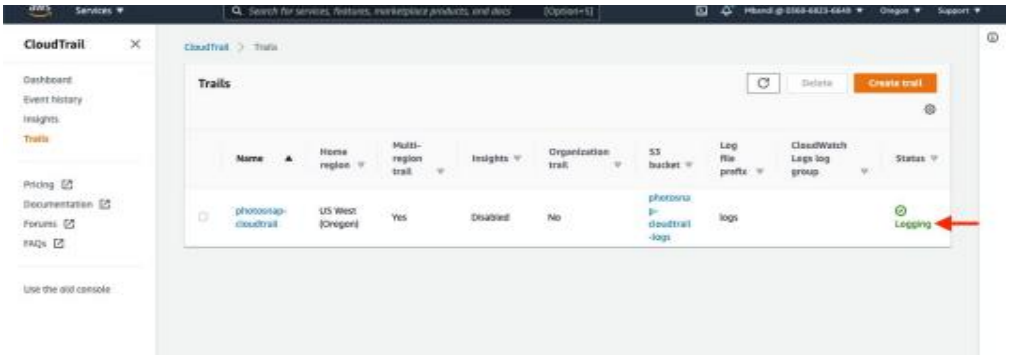
- Configure log type



- Create Trail

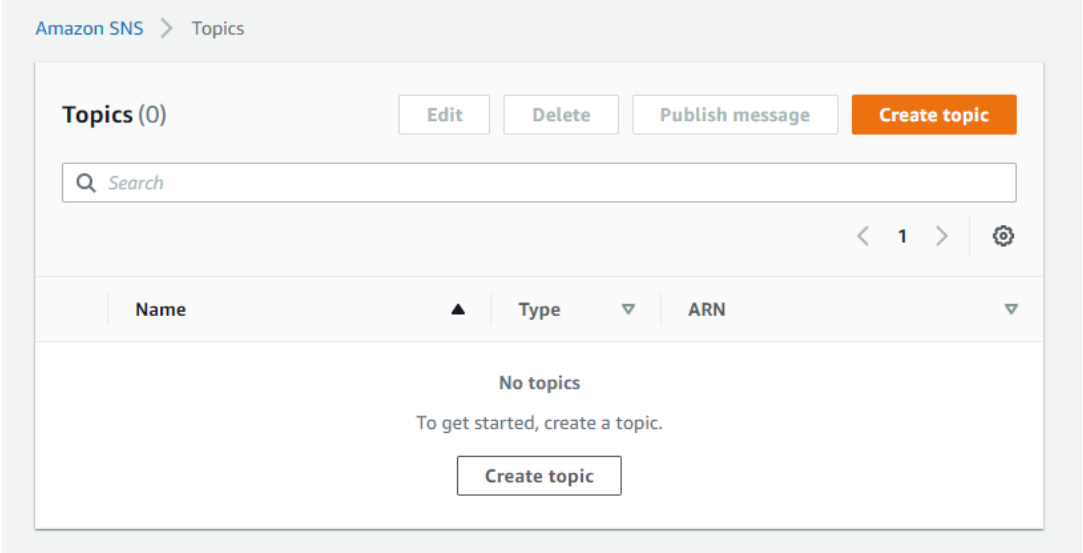


- Confirm Logging Is Turned On

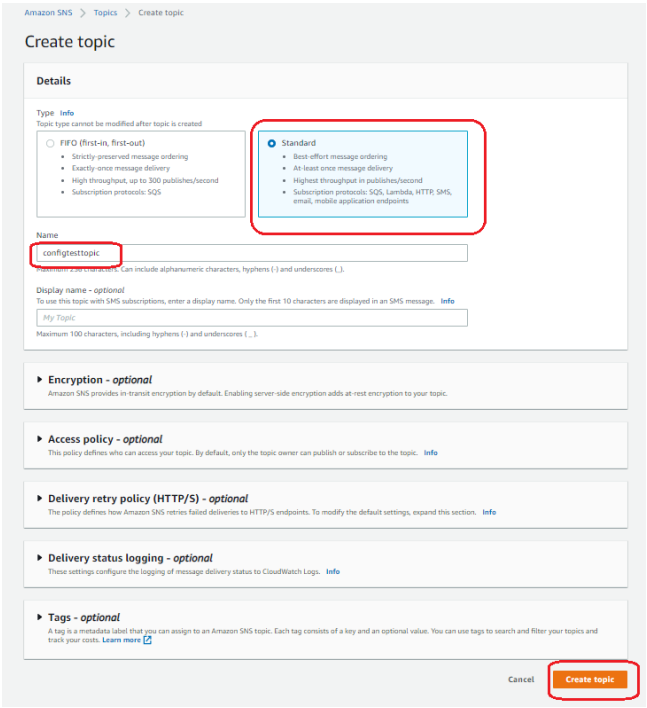


Configure Compliance Status Check With AWS Config and Amazon SNS

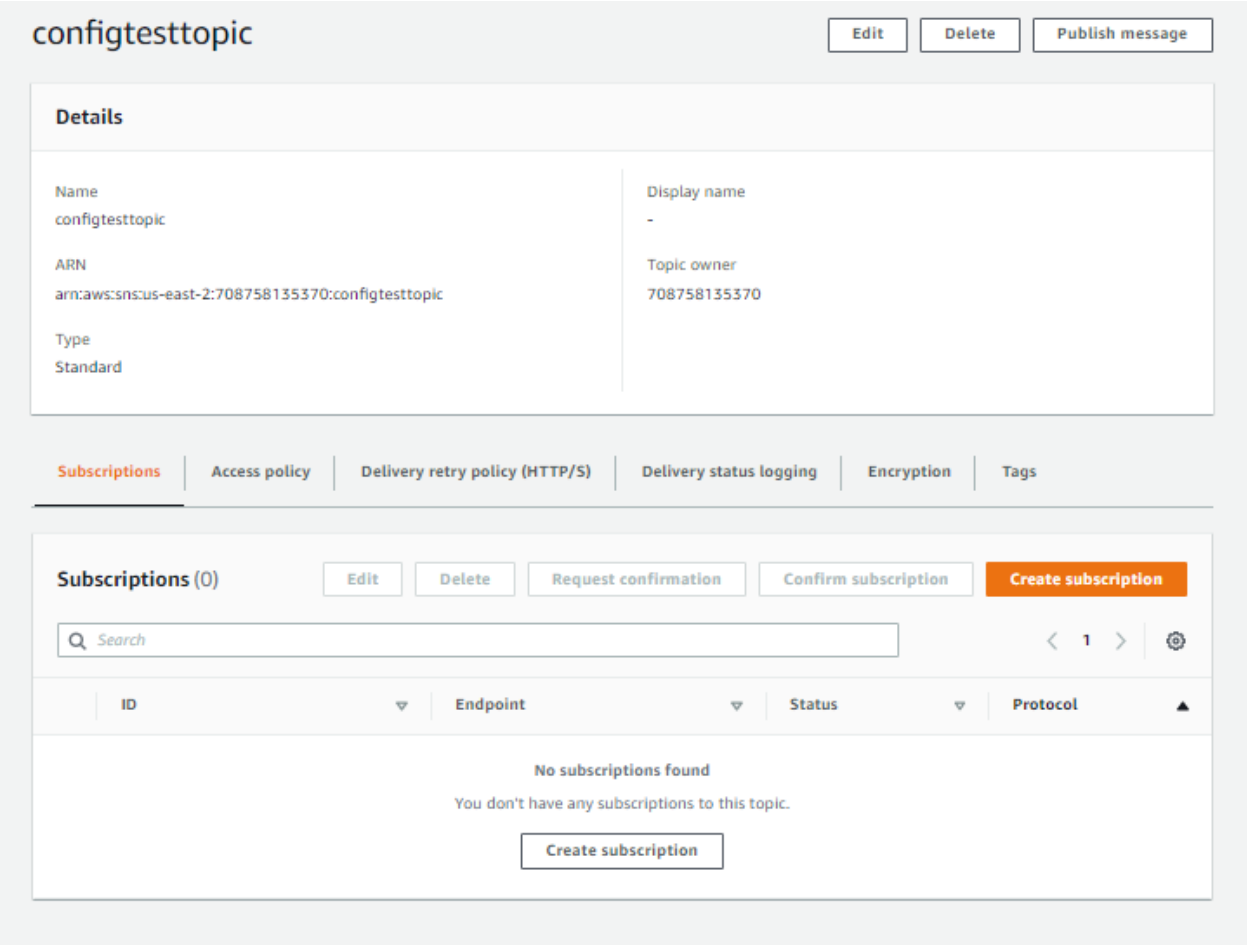
1. **SNS Notification SetUp**
   a. Go to the SNS console and click on create topic.



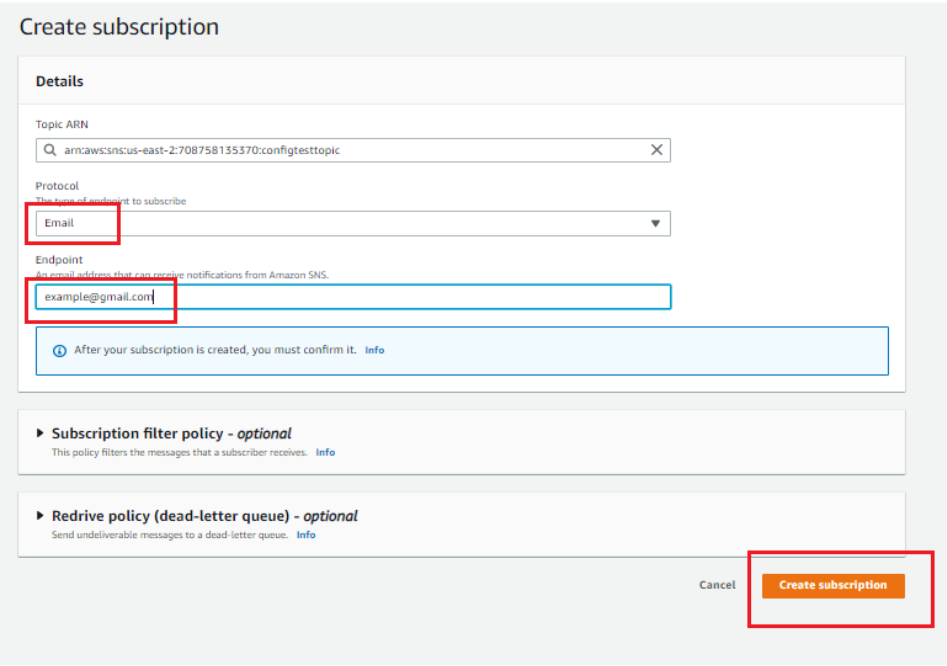
   b. Select the standard type, give your topic a name and click on create topic.



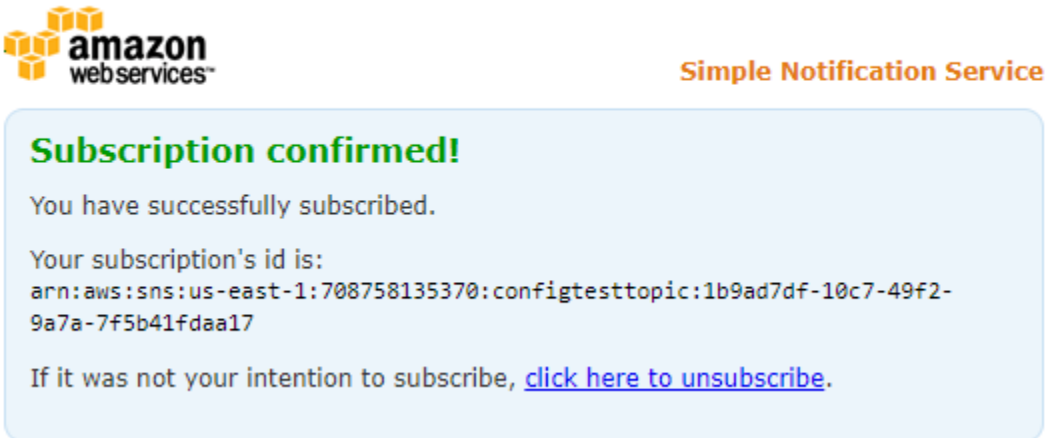
c. Once topic is created click on create subscription to subscribe to that topic.



d. In the details page, select Email or protocol



- Go to your email and confirm the subscription.

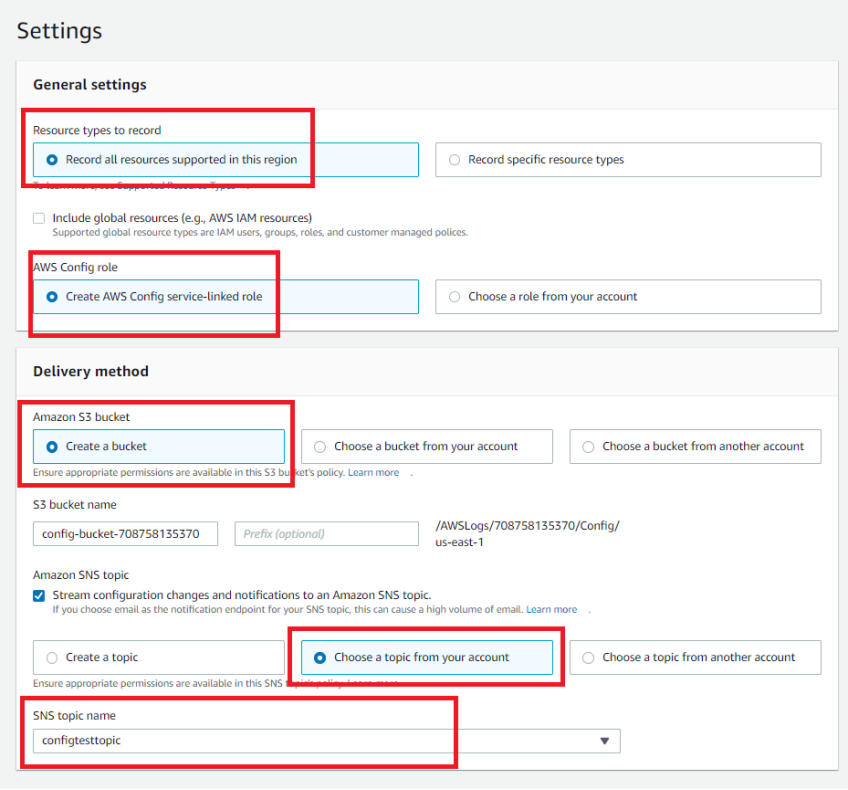


2. **Enable AWS config and create a rule to check the compliance status of Amazon S3 ane integrate with SNS notification if buckets are made public.**

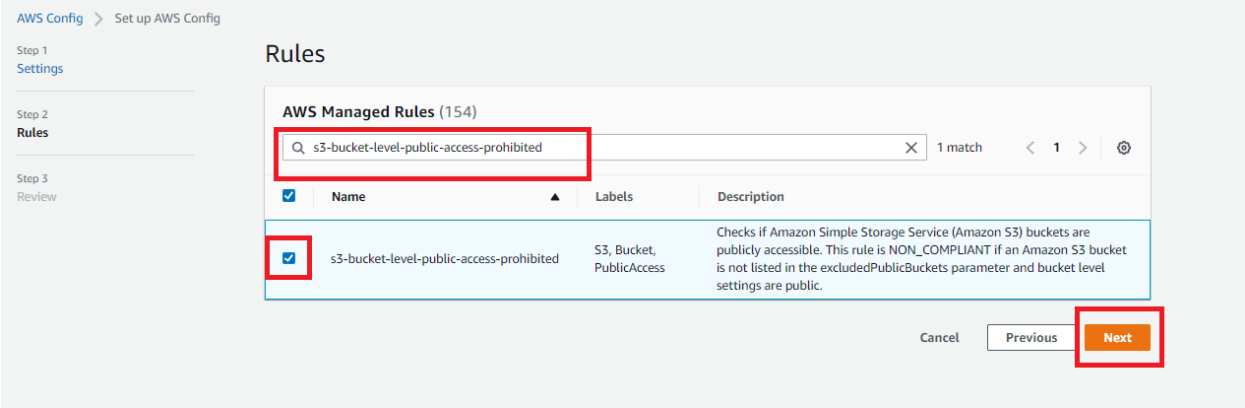
    a. Go to AWS Config console in the same region as your SNS topic and click on Get started

b. In the settings page enter the below details

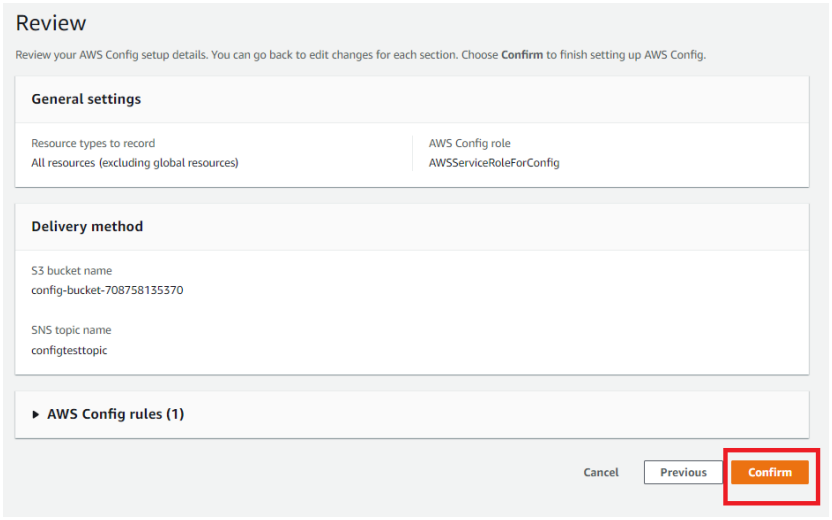
   i. General settings:
      1. Record all resources supported in this region
      2. Create AWS Config service linked role
   ii. Delivery method:
      1. Create a bucket. Leave the bucket name created by AWS
      2. Choose a topic from your account. When prompted select the topic created above.
   iii. Click on Next



c. In the Rules page search the rule **"s3-bucket-level-public-access-prohibited"** Select the rule and click on Next.



d. In the Review page, review to make sure all configurations are correct. Click confirm



Once config is set up, go to the dashboard to make sure that you can see that No resources or rules are compliant.

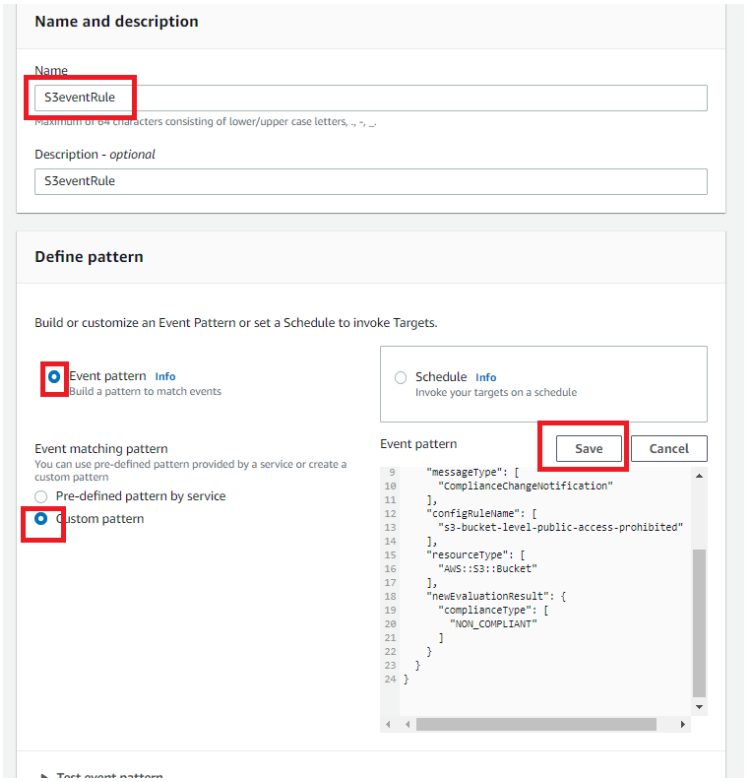
3. Create Event Bridge rule with a custom event pattern which will route NON COMPLIANT configuration changes to the Amazon Simple Notification Service (Amazon SNS) topic.

a. Open the EventBridge console and click on create rule
b. In Name, enter a name for your rule.
c. In Define Pattern, choose Event pattern.
d. In Event Matching pattern, choose Custom pattern.
e. In the Event pattern preview pane, copy and paste the following example event pattern:

```
{
  "source": [
    "aws.config"
  ],
```

```
    "detail-type": [
        "Config Rules Compliance Change"
    ],
    "detail": {
        "messageType": [
            "ComplianceChangeNotification"
        ],
        "configRuleName": [
            "s3-bucket-level-public-access-prohibited"
        ],
        "resourceType": [
            "AWS::S3::Bucket"
        ],
        "newEvaluationResult": {
            "complianceType": [
                "NON_COMPLIANT"
            ]
        }
    }
}
```

f. Choose Save



g. In Select targets, choose SNS topic.
h. In Topic, choose your SNS topic.
i. Expand Configure input, and then choose Input transformer.

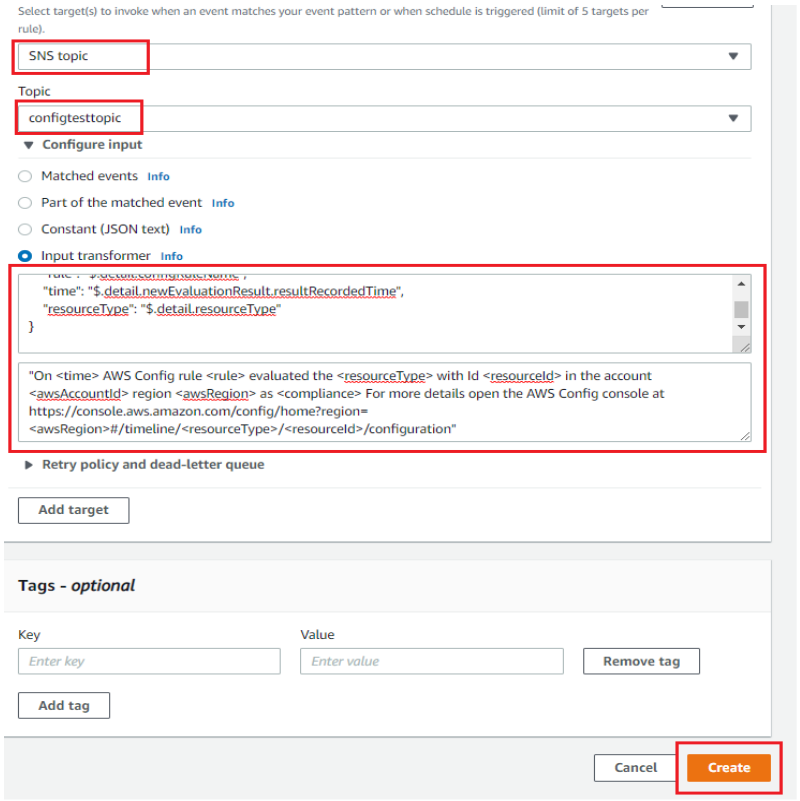
j. In the Input Path text box, copy and paste the following example path:

```
{
    "awsRegion": "$.detail.awsRegion",
    "resourceId": "$.detail.resourceId",
    "awsAccountId": "$.detail.awsAccountId",
    "compliance":
"$.detail.newEvaluationResult.complianceType",
    "rule": "$.detail.configRuleName",
    "time": "$.detail.newEvaluationResult.resultRecordedTime",
    "resourceType": "$.detail.resourceType"
}
```

k. In the Input Template text box, copy and paste the following template:

"On <time> AWS Config rule <rule> evaluated the <resourceType> with Id <resourceId> in the account <awsAccountId> region <awsRegion> as <compliance> For more details open the AWS Config console at https://console.aws.amazon.com/config/home?region=<awsRegion>#/timeline/<resourceType>/<resourceId>/configuration"

j. Choose create



To Test this solution change the configuration setting in an S3 bucket in your account to enable BPA. This will create an event which aligns with the one created above and a notification will be sent out for a Non Compliance.