

## 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 the below command to enable presigned 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)

Amazon S3 > Create bucket

### Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

**General configuration**

Bucket name  
photosnap-cloudtrail-logs

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region  
US West (Oregon) us-west-2

Copy settings from existing bucket - optional  
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

**Block Public Access settings for bucket**

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

Feedback English (US)

© 2009 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Cookie preferences](#)

Cancel [Create bucket](#)

## 2. Configuring Account Logging With AWS CloudTrail

### a. Creating a trail

The screenshot shows the 'Choose trail attributes' page in the AWS CloudTrail console. The page is divided into three steps: Step 1 (Choose trail attributes), Step 2 (Choose log events), and Step 3 (Review and create). The 'General details' section is active. It includes a 'Trail name' field with the value 'photowrap-cloudtrail', a checkbox for 'Enable for all accounts in my organization', a 'Storage location' section with 'Use existing S3 bucket' selected, a 'Trail log bucket name' field with the value 'photowrap-cloudtrail-logs', and a 'Prefix - optional' field with the value 'logs'. Red arrows point to these specific fields and buttons.

- Enable Log Validation

The screenshot shows the 'Additional settings' section of the AWS CloudTrail console. It includes a 'Log file validation' checkbox which is checked, an 'SNS notification delivery' checkbox which is unchecked, and a 'CloudWatch Logs - optional' section. The 'Log file validation' checkbox is highlighted with a red arrow. At the bottom right, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red arrow.

- Configure log type

CloudTrail > Create trail

Step 1  
Choose trail attributes

Step 2  
**Choose log events**

Step 3  
Review and create

## Choose log events

**Events** Info  
Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#)

**Event type**  
Choose the type of events that you want to log.

☒ **Management events**  
Capture management operations performed on your AWS resources.

☐ **Data events**  
Log the resource operations performed on or within a resource.

☐ **Insights events**  
Identify unusual activity, errors, or user behavior in your account.

**Management events** Info  
Management events show information about management operations performed on resources in your AWS account.

**API activity**  
Choose the activities you want to log.

☒ **Read** ☒ **Write**

☐ **Exclude AWS KMS events**

Cancel Previous **Next**

### - Create Trail

CloudTrail

Dashboard  
Event history  
Insights  
Trails

pricing   
 documentation   
 features   
 FAQs

Use the old console

Step 1  
Choose trail attributes

Step 2  
Choose log events

Step 3  
**Review and create**

## Review and create

Step 1: Choose trail attributes

**General details**

Trial name photoapp-cloudtrail	Trial log location photoapp-cloudtrail-logs/Logs/TrailLog/20180827/TrailLog	Log file validation Enabled
Multi-region trail Yes	Log file S3-KMS encryption Disabled	S3S notification delivery Disabled
Apply trail to my organization Not enabled		

**CloudWatch Logs**

No CloudWatch Logs log groups  
CloudWatch Logs is not configured for this trail.

**Tags**

Key	Value
No tags	

No tags associated with this trail.

Step 2: Choose log events

**Management events**

API activity All	Exclude AWS KMS events No
---------------------	------------------------------

**Data events**

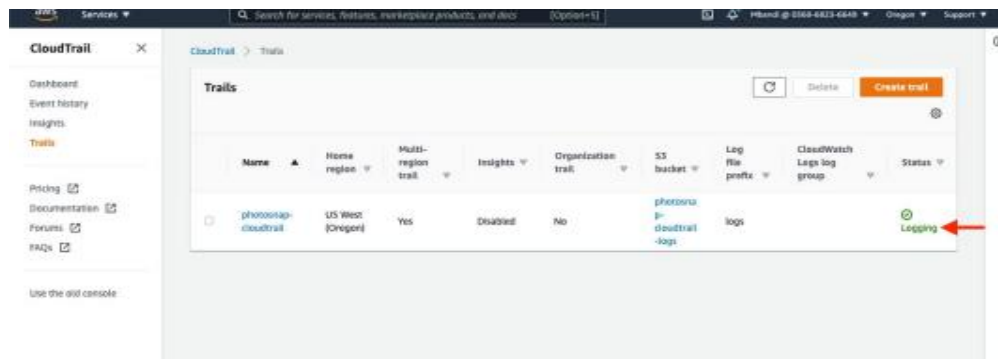
Data event collection is not configured for this trail.

**Insights events**

CloudTrail Insights can only be enabled on trails that log All or Write management events. [Learn more](#)

Cancel Previous **Create trail**

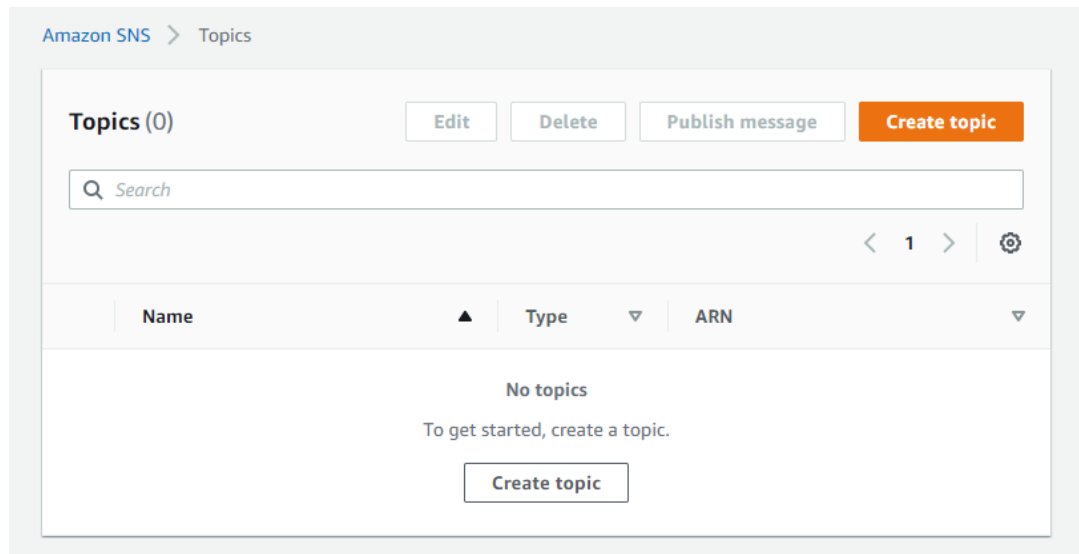
### - Confirm Logging Is Turned On



## Configure Compliance Status Check With AWS Config and Amazon SNS

### 1. SNS Notification SetUp

- Go to the SNS console and click on create topic.



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

Amazon SNS > Topics > Create topic

## Create topic

**Details**

**Type** info  
Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)
 

- Strictly-ordered message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard
 

- Best-effort message ordering
- At least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

**Name**

configtesttopic

Can include alphanumeric characters, hyphens (-) and underscores (\_).

**Display name - optional**  
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. info

My Topic

Maximum 100 characters, including hyphens (-) and underscores (\_).

► **Encryption - optional**  
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic. info

► **Access policy - optional**  
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic. info

► **Delivery retry policy (HTTP/S) - optional**  
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section. info

► **Delivery status logging - optional**  
These settings configure the logging of message delivery status to CloudWatch Logs. info

► **Tags - optional**  
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#)

Cancel **Create topic**

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

configtesttopic
Edit
Delete
Publish message

**Details**

**Name**

configtesttopic

**Display name**

-

**ARN**

arn:aws:sns:us-east-2:708758135370:configtesttopic

**Topic owner**

708758135370

**Type**

Standard

Subscriptions
Access policy
Delivery retry policy (HTTP/S)
Delivery status logging
Encryption
Tags

**Subscriptions (0)**
Edit
Delete
Request confirmation
Confirm subscription
**Create subscription**

ID	Endpoint	Status	Protocol
No subscriptions found			
You don't have any subscriptions to this topic.			
<b>Create subscription</b>			

d. In the details page, select Email or protocol

## Create subscription

**Details**

Topic ARN

arn:aws:sns:us-east-2:708758135370:configtesttopic

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

example@gmail.com

After your subscription is created, you must confirm it.

Subscription filter policy - optional

This policy filters the messages that a subscriber receives.

Redrive policy (dead-letter queue) - optional

Send undeliverable messages to a dead-letter queue.

Cancel

Create subscription

- Go to your email and confirm the subscription.



### Simple Notification Service

#### Subscription confirmed!

You have successfully subscribed.

Your subscription's id is:

arn:aws:sns:us-east-1:708758135370:configtesttopic:1b9ad7df-10c7-49f2-9a7a-7f5b41fdaa17

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

2. Enable AWS config and create a rule to check the compliance status of Amazon S3 and 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

The screenshot shows the 'Settings' page for AWS Config. It is divided into two main sections: 'General settings' and 'Delivery method'. In the 'General settings' section, the 'Resource types to record' is set to 'Record all resources supported in this region', and the 'AWS Config role' is set to 'Create AWS Config service-linked role'. In the 'Delivery method' section, the 'Amazon S3 bucket' is set to 'Create a bucket', and the 'Amazon SNS topic' is set to 'Choose a topic from your account'. The 'S3 bucket name' is 'config-bucket-708758135370' and the 'SNS topic name' is 'configtesttopic'. Red boxes highlight the 'Record all resources supported in this region' option, the 'Create AWS Config service-linked role' option, the 'Create a bucket' option, the 'Choose a topic from your account' option, and the 'configtesttopic' text input field.

**Settings**

**General settings**

Resource types to record

☒ Record all resources supported in this region ☐ Record specific resource types

☐ Include global resources (e.g., AWS IAM resources)  
Supported global resource types are IAM users, groups, roles, and customer managed policies.

AWS Config role

☒ Create AWS Config service-linked role ☐ Choose a role from your account

**Delivery method**

Amazon S3 bucket

☒ Create a bucket ☐ Choose a bucket from your account ☐ Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. [Learn more](#)

S3 bucket name

config-bucket-708758135370  /AWSLogs/708758135370/Config/us-east-1

Amazon SNS topic

☒ Stream configuration changes and notifications to an Amazon SNS topic.  
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. [Learn more](#)

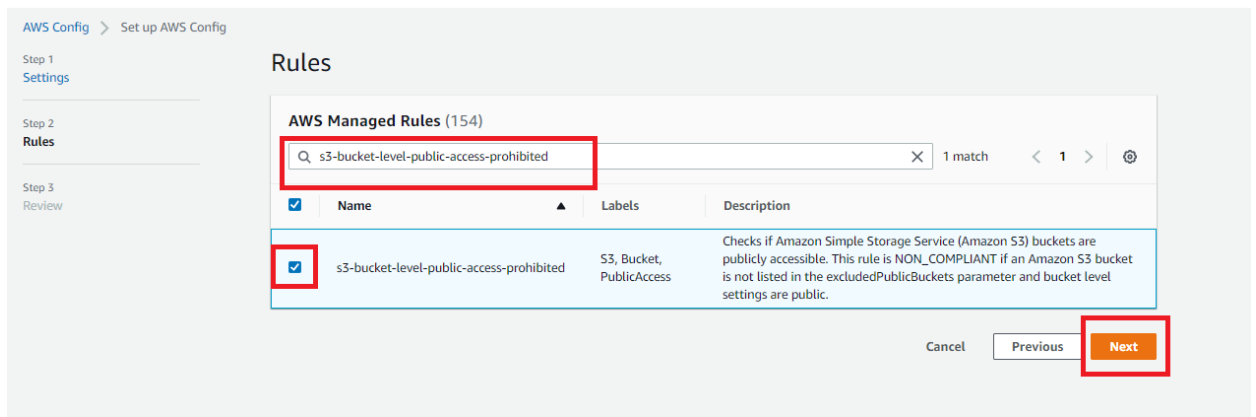
☐ Create a topic ☒ Choose a topic from your account ☐ Choose a topic from another account

Ensure appropriate permissions are available in this SNS topic's policy. [Learn more](#)

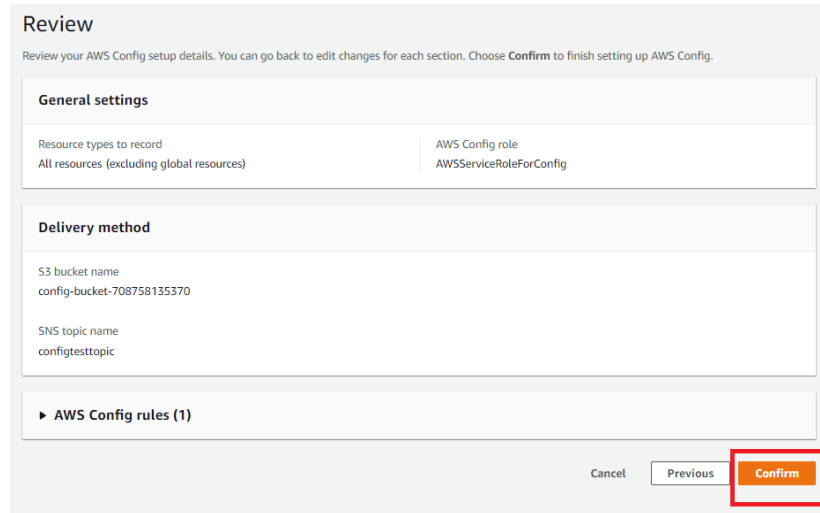
SNS topic name

configtesttopic

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

**Name and description**

Name: S3eventRule

Description - optional: S3eventRule

**Define pattern**

Build or customize an Event Pattern or set a Schedule to invoke Targets.

☒ **Event pattern** [Info](#)  
Build a pattern to match events

☐ **Schedule** [Info](#)  
Invoke your targets on a schedule

**Event matching pattern**  
You can use pre-defined pattern provided by a service or create a custom pattern

☐ Pre-defined pattern by service

☒ **Custom pattern**

**Event pattern**

```

9  "messageType": [
10   "ComplianceChangeNotification"
11 ],
12  "configRuleName": [
13   "s3-bucket-level-public-access-prohibited"
14 ],
15  "resourceType": [
16   "AWS::S3::Bucket"
17 ],
18  "newEvaluationResult": {
19   "complianceType": [
20    "NON_COMPLIANT"
21   ]
22 }
23 }
24 }

```

**Save** **Cancel**

- 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

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule).

SNS topic

Topic

configtesttopic

▼ Configure input

☐ Matched events [Info](#)

☐ Part of the matched event [Info](#)

☐ Constant (JSON text) [Info](#)

☒ Input transformer [Info](#)

`time": "$.detail.newEvaluationResult.resultRecordedTime",  
"resourceType": "$.detail.resourceType"`

"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>"

► Retry policy and dead-letter queue

Add target

Tags - optional

Key

Value

Remove tag

Add tag

Cancel 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.