

# Sending AWS Config logs to Sumo Logic

---

 [dev.classmethod.jp/articles/sumo-logic-aws-config](https://dev.classmethod.jp/articles/sumo-logic-aws-config)

酒井剛

March 28, 2023

# sumo logic

## Give it a try

---

The content of this post is basically verified based on Sumo Logic's official documentation.

## AWS Config settings

---

First, enable AWS Config and configure it to send configuration changes to an SNS topic when they are made.

Log in to the AWS Management Console and enable Config. (It was already enabled in my account, so I will start by creating an SNS Topic in the Config settings.)

**Edit settings**

**Recorder**

☒ Enable recording

**General settings**

Resource types to record

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

If you select this option, when AWS Config adds support for a new type of regional resource, it starts recording resources of that type automatically. [Learn more](#)

Resource category: All resource categories Resource type: Multiple Selected

AWS EC2 CustomerGateway X AWS EC2 EIP X AWS EC2 Host X AWS EC2 InternetGateway X AWS EC2 NetworkAcl X

AWS EC2 RouteTable X AWS EC2 SecurityGroup X AWS EC2 Subnet X AWS CloudTrail Trail X AWS EC2 VPC X

AWS EC2 VPNConnection X AWS EC2 VPNGateway X AWS IAM Group X AWS IAM Policy X AWS IAM Role X

AWS IAM User X AWS ACM Certificate X AWS RDS DBInstance X AWS RDS DBSubnetGroup X

AWS RDS DBSecurityGroup X AWS RDS EventSubscription X AWS ElasticLoadBalancingV2 LoadBalancer X AWS S3 Bucket X

**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**

Prefix (optional)

**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**

ConfigSNSTopic

**Amazon CloudWatch Events rule**

AWS Config sends detailed information about the configuration changes and notifications to Amazon CloudWatch Events. To create rules, visit the [Step 1: Create Rule](#) page in the Amazon CloudWatch Events console.

Cancel Save

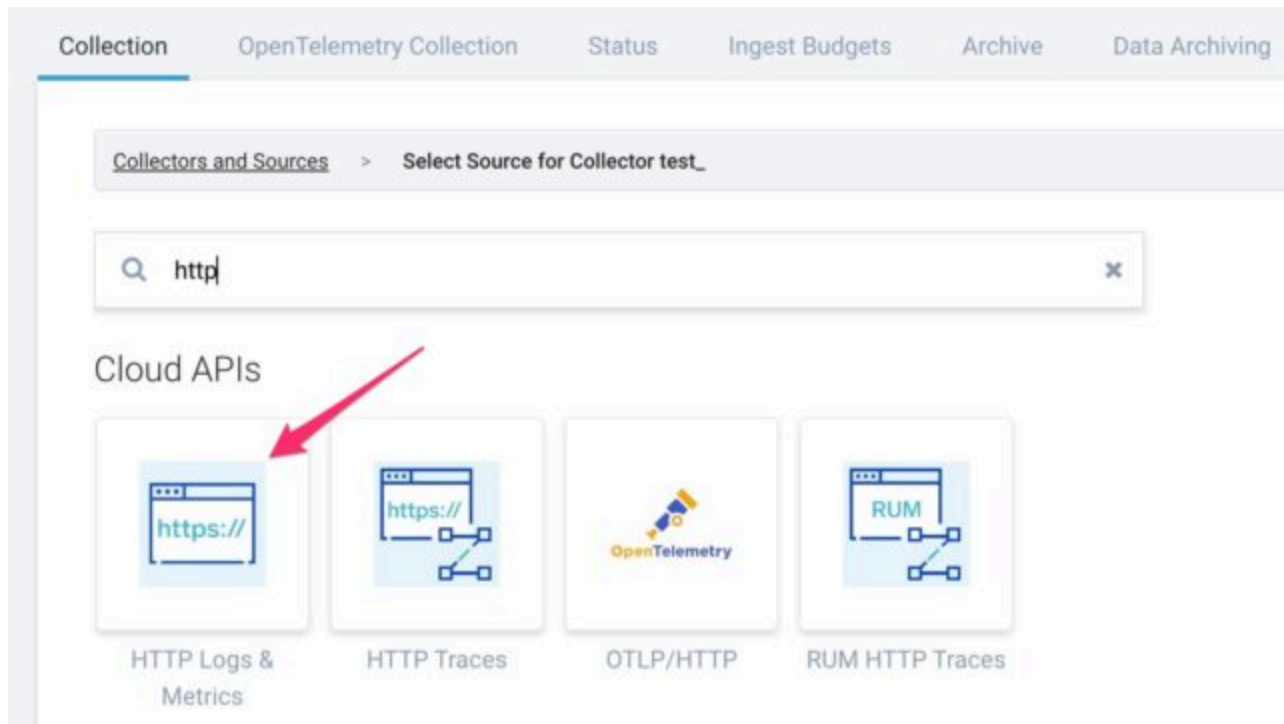
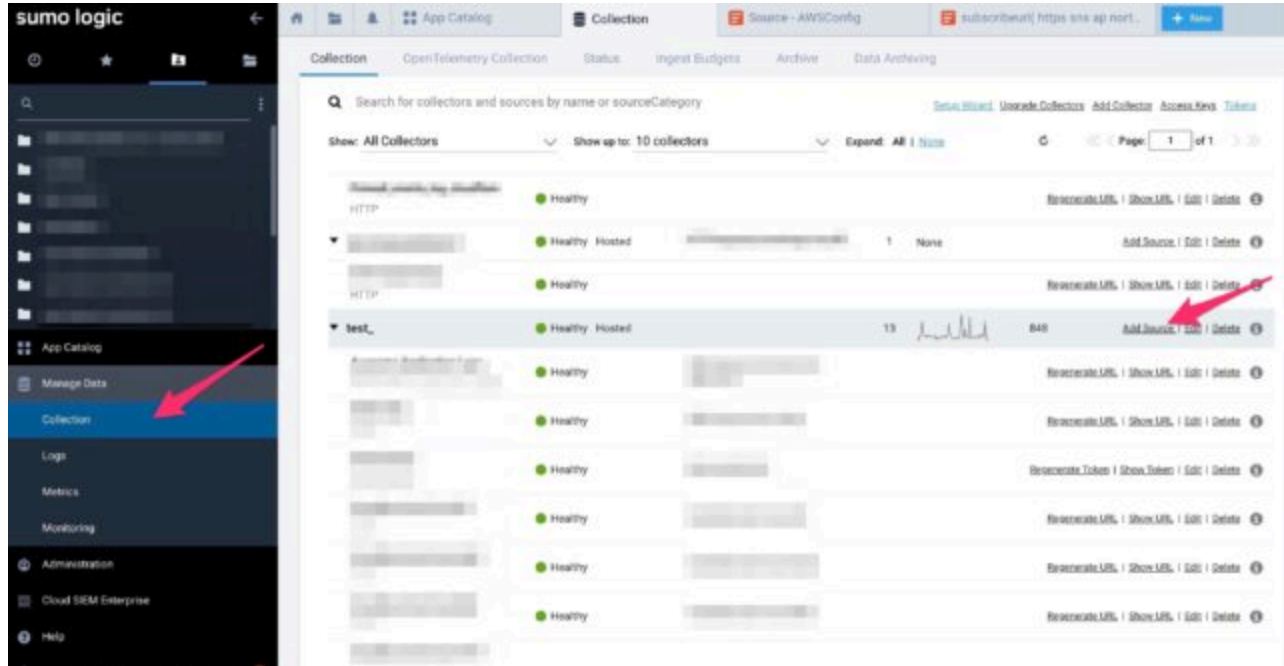
This will create a topic on SNS.

## Configure a Source in Sumo Logic

Next, create an HTTP Logs & Metrics Source from the Sumo Logic Management Console to the Hosted Collector, which will be the endpoint for receiving the SNS topic.

Manage Data > Collection

Add Source



Set the source name and source category to any value.

Collection

OpenTelemetry Collection

Status

Ingest Budgets

Archiv

Collectors and Sources

>

Select Source for Collector test

>

HTTP Logs & Metrics

HTTP Logs & Metrics

Name

AWSConfig

Description (optional)

Source Host (optional)

Source Category (optional)

AWS/myaccount/config

☐ Forward to SIEM

Fields/Metadata

Key	Value
<div>+ Add</div>	

Advanced Options for Logs (Optional)

In the Advanced Options for Logs settings, Multiline Processing under Message Processing is enabled by default, so disable it, check One Message Per Request, and save the settings.

Collection   OpenTelemetry Collection   Status   Ingest Budgets   Archive

Collectors and Sources > Edit Source: AWSConfig

▼ Advanced Options for Logs (Optional)

Timestamp Parsing

☒ Extract timestamp information from log file entries

Default Time Zone (optional)

If no time zone is selected, Collector's time zone will be used

☒ Use time zone from log file. If not detected, use default time zone

☐ Ignore time zone from log file and instead use default time zone

Timestamp Format

☒ Automatically detect the format

☐ Specify a format

Message Processing

☐ Multiline Processing

Detect messages spanning multiple lines

☒ One Message Per Request

Each request will be treated as a single message (ignore line breaks)

After creation, the endpoint URL will be displayed, so copy it.

×

# HTTP Source Address

Use the following address to send data to the Collector. [Learn more...](#)

**Keep this address private since anyone can use it to send data.**

https://collectors.jp.sumologic.com/receiver/v1/http/ZaVnC4

Copy

OK

## Social Media Settings

Return to the AWS Management Console and configure SNS.

Select the newly created topic in the Config settings and configure the subscription.

Amazon SNS > Topics > ConfigSNSTopic

ConfigSNSTopic

EditDeletePublish message

Details

Name

ConfigSNSTopic

ARN

arn:aws:sns:ap-northeast-1:123456789012:ConfigSNSTopic

Type

Standard

Display name

-

Topic owner

123456789012

<SubscriptionsAccess policyData protection policyDelivery policy (HTTP/S)Delivery status loggingEncryption>

Subscriptions (0)

EditDeleteRequest confirmationConfirm subscriptionCreate subscription

Q Search

< 1 > ⓘ

ID▲Endpoint▼Status▼Protocol▼

No subscriptions found

In your subscription settings, change the protocol to HTTPS and paste the value you copied into the endpoint, then save the settings.

After that, wait a few minutes and you will receive a message from Sumo Logic confirming your subscription.

#	Time	Message
1	03/28/2023 8:43:52.422 PM +0900	<pre>{   "Type": "Message",   "Token": "Token",   "TopicAr": "TopicAr",   "Message": "Message",   "Subscri": "Subscri",   "Timesta": "Timesta",   "Signatu": "Signatu",   "Signatu": "Signatu",   "Signing": "Signing" }</pre>

Once you have confirmed this log, copy the SubscribeURL value.



Again, go back to your SNS settings, select Subscriptions, and select Confirm Subscription.

The screenshot shows the Amazon SNS console interface for a topic named 'ConfigSNSTopic'. The breadcrumb navigation at the top reads 'Amazon SNS > Topics > ConfigSNSTopic'. On the right side of the topic header, there are buttons for 'Edit', 'Delete', and 'Publish message'. Below this is a 'Details' section with a table of attributes:

Attribute	Value
Name	ConfigSNSTopic
Display name	-
ARN	arn:aws:sns:ap-northeast-1: ConfigSNSTopic
Type	Standard
Topic owner	

Below the details is a horizontal tab bar with options: 'Subscriptions' (selected), 'Access policy', 'Data protection policy', 'Delivery policy (HTTP/S)', 'Delivery status logging', and 'Encryption'. Under the 'Subscriptions' tab, there is a search bar and a list of subscriptions. The list has columns for ID, Endpoint, Status, and Protocol. One subscription is listed with ID 'Pending confirmation', Endpoint 'https://collectors.jp.sumologi...', Status 'Pending confirmation', and Protocol 'HTTPS'. Above the subscription list, there are buttons: 'Edit', 'Delete', 'Request confirmation', 'Confirm subscription' (highlighted with a red arrow), and 'Create subscription'.

Paste the Subscribe URL and confirm your subscription.

The screenshot shows a 'Confirm subscription' dialog box with a close button (X) in the top right corner. The text inside the dialog says 'Enter the subscription confirmation url.' Below this is a text input field containing the URL 'https://sns.ap-northeast-1.amazonaws.com/?Action=ConfirmSubscription&TopicArn='. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Confirm subscription'.



You will then see the status change to Verified.

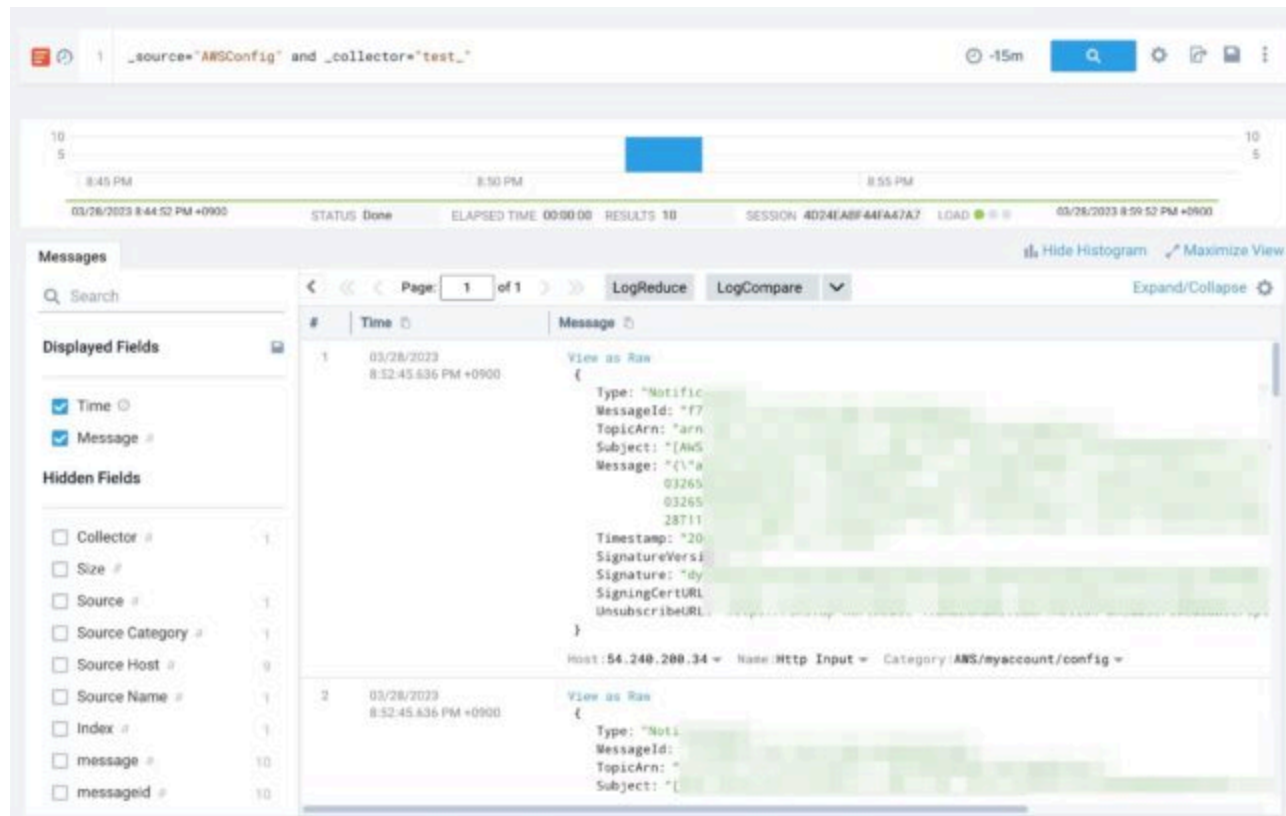
The screenshot shows the AWS SNS console for a topic named 'ConfigSNSTopic'. The 'Details' section shows the topic's name, ARN, and type (Standard). Below this, the 'Subscriptions' tab is active, displaying a table with one subscription. The subscription's status is 'Confirmed', indicated by a green checkmark icon and a red arrow pointing to it. The subscription's endpoint is 'https://collectors.jp.sumologi...' and the protocol is 'HTTPS'.

ID	Endpoint	Status	Protocol
60842cb3-52e5-4ddb-8d97-d...	https://collectors.jp.sumologi...	Confirmed	HTTPS

## Verify that Config is being ingested into Sumo Logic

I created a new VPC in AWS,  
and then checked the source I set up on Sumo Logic.

You can see that the logs are being imported correctly.



This allows you to analyze logs for unexpected configuration changes and deploy Sumo Logic's built-in dashboards.

## summary

This time, I tried to import AWS Config logs into Sumo Logic. I hope this blog will be helpful to someone.