

# 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.)

The screenshot shows the 'Edit settings' page for AWS Config. Under the 'Recorder' section, 'Enable recording' is checked. In the 'General settings' section, 'Record specific resource types' is selected. A list of resources to record includes: AWS EC2 CustomerGateway, AWS EC2 EIP, AWS EC2 Host, AWS EC2 InternetGateway, AWS EC2 NetworkAcl, AWS EC2 RouteTable, AWS EC2 SecurityGroup, AWS EC2 Subnet, AWS CloudTrail Trail, AWS EC2 VPC, AWS EC2 VPNGateway, AWS IAM Group, AWS IAM Policy, AWS IAM Role, AWS IAM User, AWS ACM Certificate, AWS RDS DBInstance, AWS RDS DBSubnetGroup, AWS RDS DBSecurityGroup, AWS RDS EventSubscription, AWS ElasticLoadBalancingV2 LoadBalancer, and AWS S3 Bucket.

The screenshot shows the 'Amazon S3 bucket' creation dialog. It has three options: 'Create a bucket' (radio button), 'Choose a bucket from your account' (selected radio button), and 'Choose a bucket from another account'. Below this, it says 'Ensure appropriate permissions are available in this S3 bucket's policy.' Under 'S3 bucket name', there is a dropdown menu with 'com.amazonaws.us-east-1.s3' and a 'Prefix (optional)' field. A red arrow points to the 'Amazon SNS topic' section, which contains a checked checkbox for 'Stream configuration changes and notifications to an Amazon SNS topic.' Below this, it says 'If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email.' There are three options for creating an SNS topic: 'Create a topic' (selected radio button), 'Choose a topic from your account', and 'Choose a topic from another account'. A red arrow points to the 'Create a topic' input field, which contains 'ConfigSNSTopic'. Below this, it says 'Ensure appropriate permissions are available in this SNS topic's policy.' At the bottom right are 'Cancel' and 'Save' buttons.

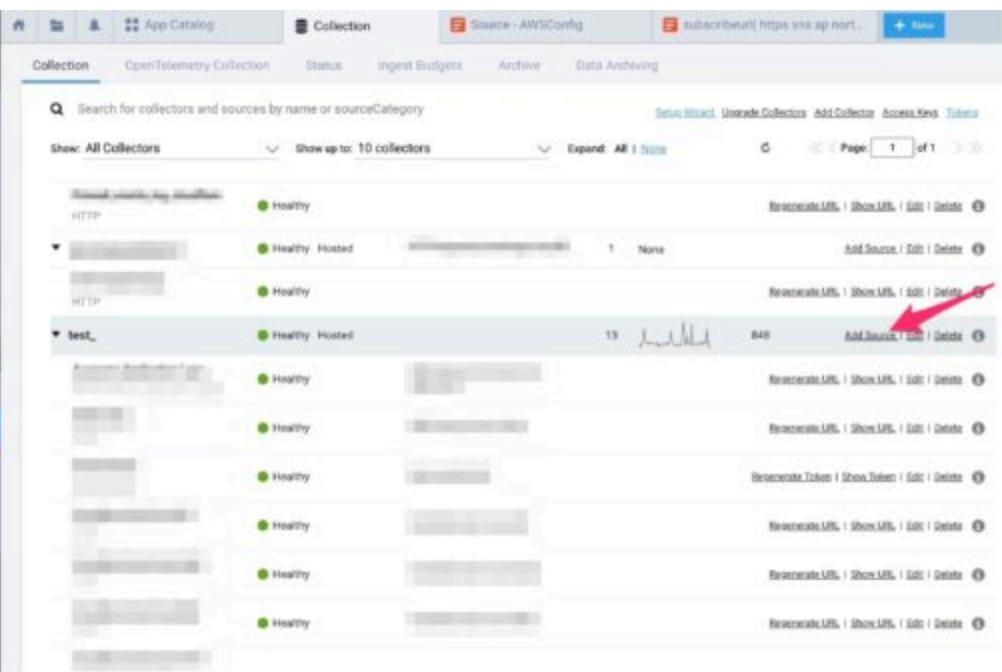
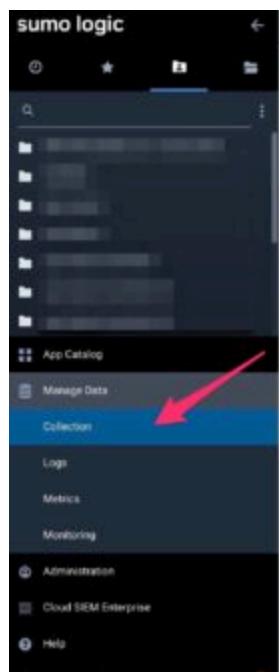
This will create a topic on SNS.

## Configure a Source in Sumo Logic

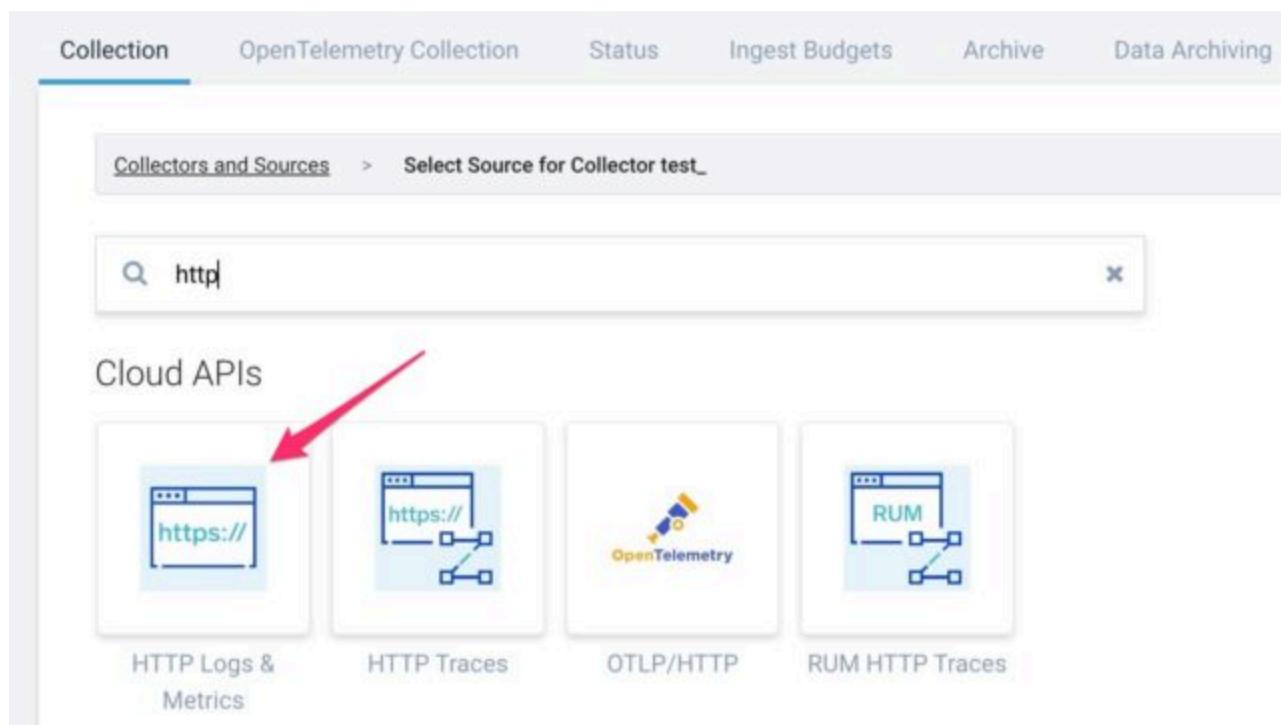
Next, create an HTTP Logs & Metrics Source from the Sumo Logic Management Console to the Hosted Collector, which will be the endpoint for receiving the SNS topic.

Manage Data > Collection

Add Source



The screenshot shows the Sumo Logic Management Console interface. On the left, there's a sidebar with links like 'Manage Data', 'Logs', 'Metrics', 'Monitoring', 'Administration', 'Cloud SEM Enterprise', and 'Help'. A red arrow points to the 'Collection' link under 'Manage Data'. The main area is titled 'Collection' and shows a list of collectors. One collector is expanded, revealing its sources. At the bottom right of this expanded section, another red arrow points to the 'Add Source' button. The browser's address bar at the top shows the URL <https://sumologic-test-123456.sumologic.net>.



The screenshot shows the 'Select Source for Collector test\_>' page. At the top, there's a breadcrumb navigation: 'Collectors and Sources > Select Source for Collector test\_>'. Below that is a search bar with the text 'http'. The main area is titled 'Cloud APIs' and contains four icons: 'HTTP Logs & Metrics' (highlighted with a red arrow), 'HTTP Traces', 'OTLP/HTTP', and 'RUM HTTP Traces'.

Set the source name and source category to any value.

The screenshot shows a user interface for creating a new collection. At the top, there are tabs: 'Collection' (which is selected), 'OpenTelemetry Collection', 'Status', 'Ingest Budgets', and 'Archives'. Below the tabs, a breadcrumb navigation path is shown: 'Collectors and Sources' > 'Select Source for Collector test' > 'HTTP Logs & Metrics'. The main section is titled 'HTTP Logs & Metrics'. It contains fields for 'Name' (set to 'AWSConfig'), 'Description (optional)', 'Source Host (optional)', 'Source Category (optional)' (set to 'AWS/myaccount/config'), and a checkbox for 'Forward to SIEM' which is unchecked. There is also a 'Fields/Metadata' table with a single row labeled '+ Add'. At the bottom of the form, there is a link 'Advanced Options for Logs (Optional)'.

Collection

OpenTelemetry Collection

Status

Ingest Budgets

Archives

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 |
|-------|-------|
| + Add |       |

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.

**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.

The screenshot shows the AWS SNS 'Topics' page with a single topic named 'ConfigSNSTopic'. The 'Subscriptions' tab is selected. At the bottom of the 'Subscriptions' section, there is a prominent orange 'Create subscription' button. A red arrow points from the right side of the image towards this button. The rest of the page displays the topic's details (Name: ConfigSNSTopic, ARN: arn:aws:sns:ap-northeast-1:123456789012:ConfigSNSTopic, Type: Standard) and various policy and delivery settings tabs.

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

The screenshot shows the 'Create subscription' page in the Amazon SNS console. The 'Topic ARN' field contains the URL 'Q\_arn:aws:sns:ap-northeast-1:...ConfigSNSTopic'. The 'Protocol' dropdown is set to 'HTTPS'. The 'Endpoint' input field contains the URL 'https://collectors.jp.sumologic.com/receiver/v1/http/2'. There is a note below the endpoint field stating 'After your subscription is created, you must confirm it.' A section for 'Subscription filter policy - optional' is shown at the bottom.

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

The screenshot shows the Sumo Logic interface with a search results page. The search query is '\_source="AWSConfig" and \_collector="test\_"' and the time range is '-15m'. The results show one log entry. The log details a successful subscription confirmation from AWSConfig to a test collector. The log includes fields like Time, Status, Elapsed Time, Results, Session, and Source. The log message is partially visible, showing 'Type: "Message", Token: TopicArn, Message' and 'Subscri'.

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 AWS SNS 'ConfigSNSTopic' configuration page. At the top, there are buttons for 'Edit', 'Delete', and 'Publish message'. Below that is a 'Details' section with fields for Name (ConfigSNSTopic), Display name (-), ARN (arn:aws:sns:ap-northeast-1:...:ConfigSNSTopic), Topic owner (redacted), and Type (Standard). Below the details is a navigation bar with tabs: Subscriptions (highlighted in blue), Access policy, Data protection policy, Delivery policy (HTTP/S), Delivery status logging, Encryption, and >. Under the Subscriptions tab, there is a sub-header 'Subscriptions (1)'. Below it is a table with columns: ID, Endpoint, Status, and Protocol. One row is shown: Pending confirmation, https://collectors.jp.sumologi..., Pending confirmation, HTTPS. To the right of the table are buttons for 'Edit', 'Delete', 'Request confirmation', 'Confirm subscription' (which has a red arrow pointing to it), and 'Create subscription'. There is also a search bar and pagination controls (< 1 >).

Paste the Subscribe URL and confirm your subscription.

The screenshot shows a 'Confirm subscription' dialog box. At the top left is the title 'Confirm subscription' and at the top right is a close button (X). Below the title is a instruction: 'Enter the subscription confirmation url.' followed by a text input field containing the URL: <https://sns.ap-northeast-1.amazonaws.com/?Action=ConfirmSubscription&TopicArn=>. At the bottom are two buttons: 'Cancel' and 'Confirm subscription' (which is highlighted in orange).

You will then see the status change to Verified.

The screenshot shows the AWS SNS 'ConfigSNSTopic' configuration page. At the top, there are three buttons: 'Edit', 'Delete', and 'Publish message'. Below this is a 'Details' section with fields: Name ('ConfigSNSTopic'), Display name ('-'), ARN ('arn:aws:sns:ap-northeast-1:xxxxxxxxxxxx:ConfigSNSTopic'), Topic owner ('[REDACTED]'), and Type ('Standard'). Below the details is a navigation bar with tabs: 'Subscriptions' (selected), 'Access policy', 'Data protection policy', 'Delivery policy (HTTP/S)', 'Delivery status logging', 'Encryption', and 'Encryption'. Under the 'Subscriptions' tab, there is a table titled 'Subscriptions (1)'. The table has columns: ID, Endpoint, Status, and Protocol. A single row shows an ID starting with '60842cb3-52e5-4ddb-8d97-d...', an Endpoint of 'https://collectors.jp.sumologic...', a Status of 'Confirmed' (with a green checkmark icon), and a Protocol of 'HTTPS'. A red arrow points to the 'Confirmed' status in the table. There are also buttons for 'Edit', 'Delete', 'Request confirmation', 'Confirm subscription', and 'Create subscription'.

## 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.