Sending AWS Config logs to Sumo Logic

dev.classmethod.jp/articles/sumo-logic-aws-config

酒井剛

March 28, 2023

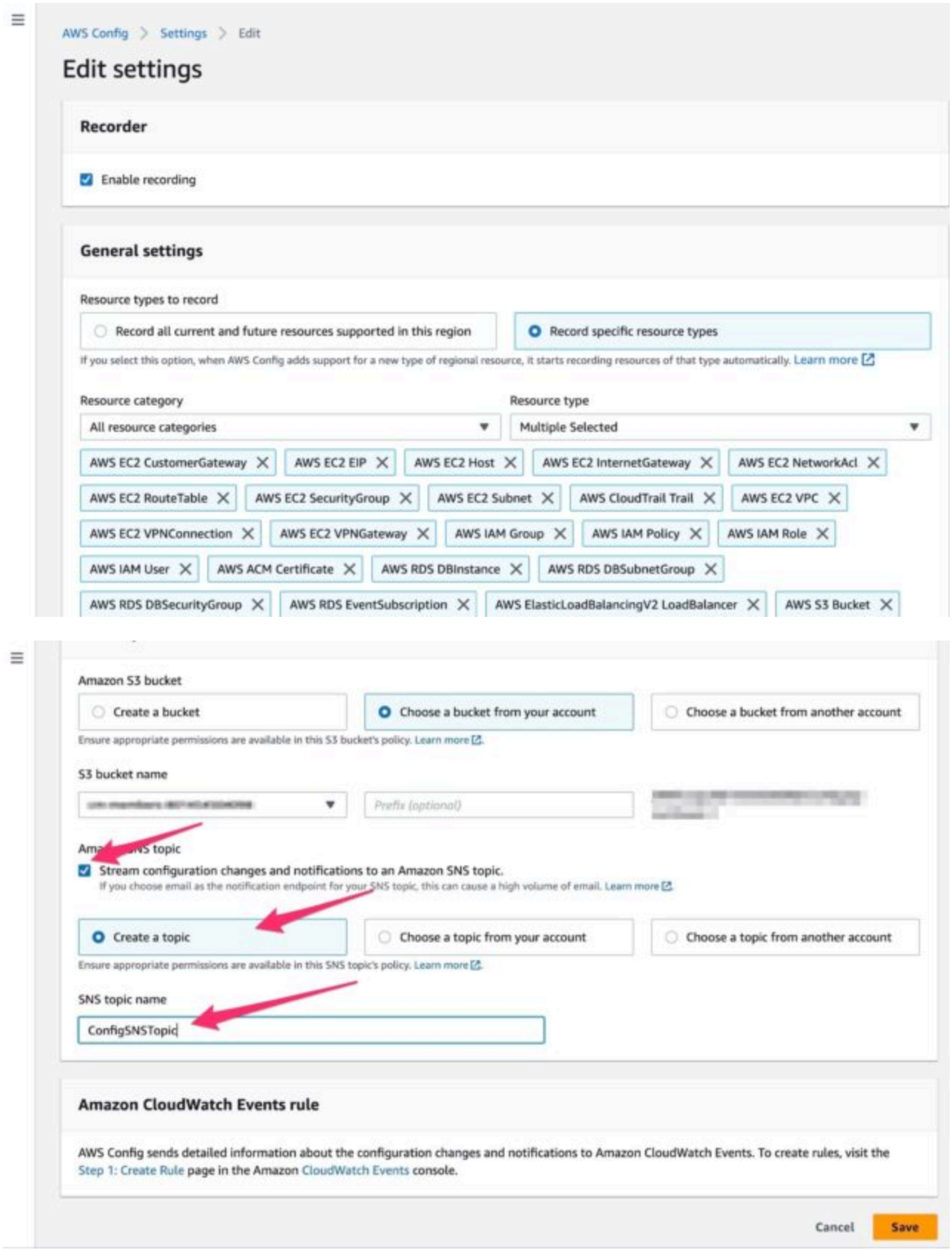
Give it a try

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.)

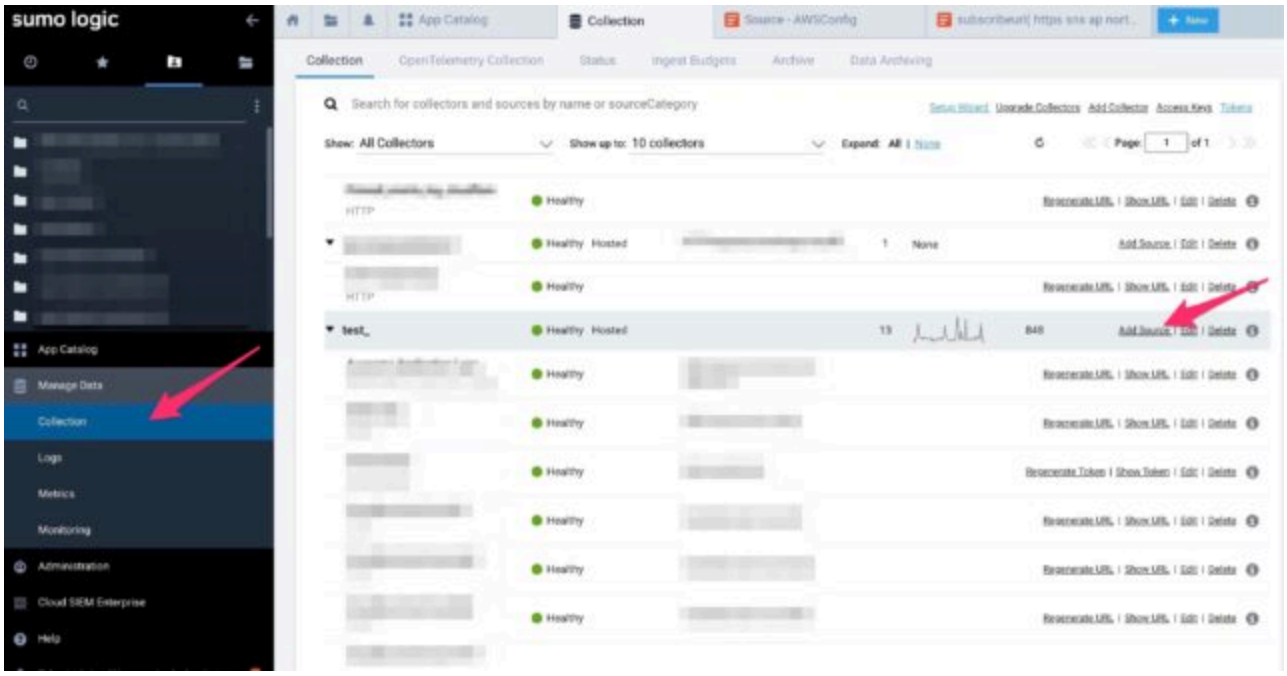


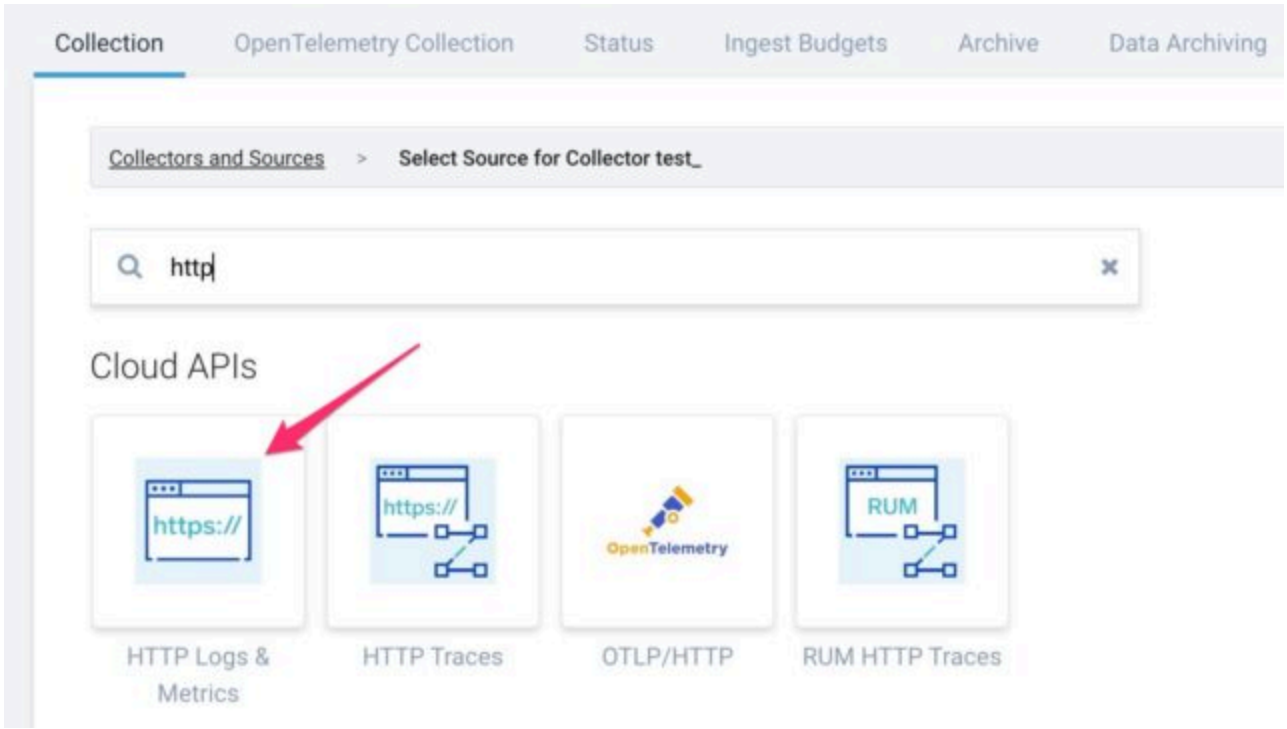
This will create a topic on SNS.

Configure a Source in Sumo Logic

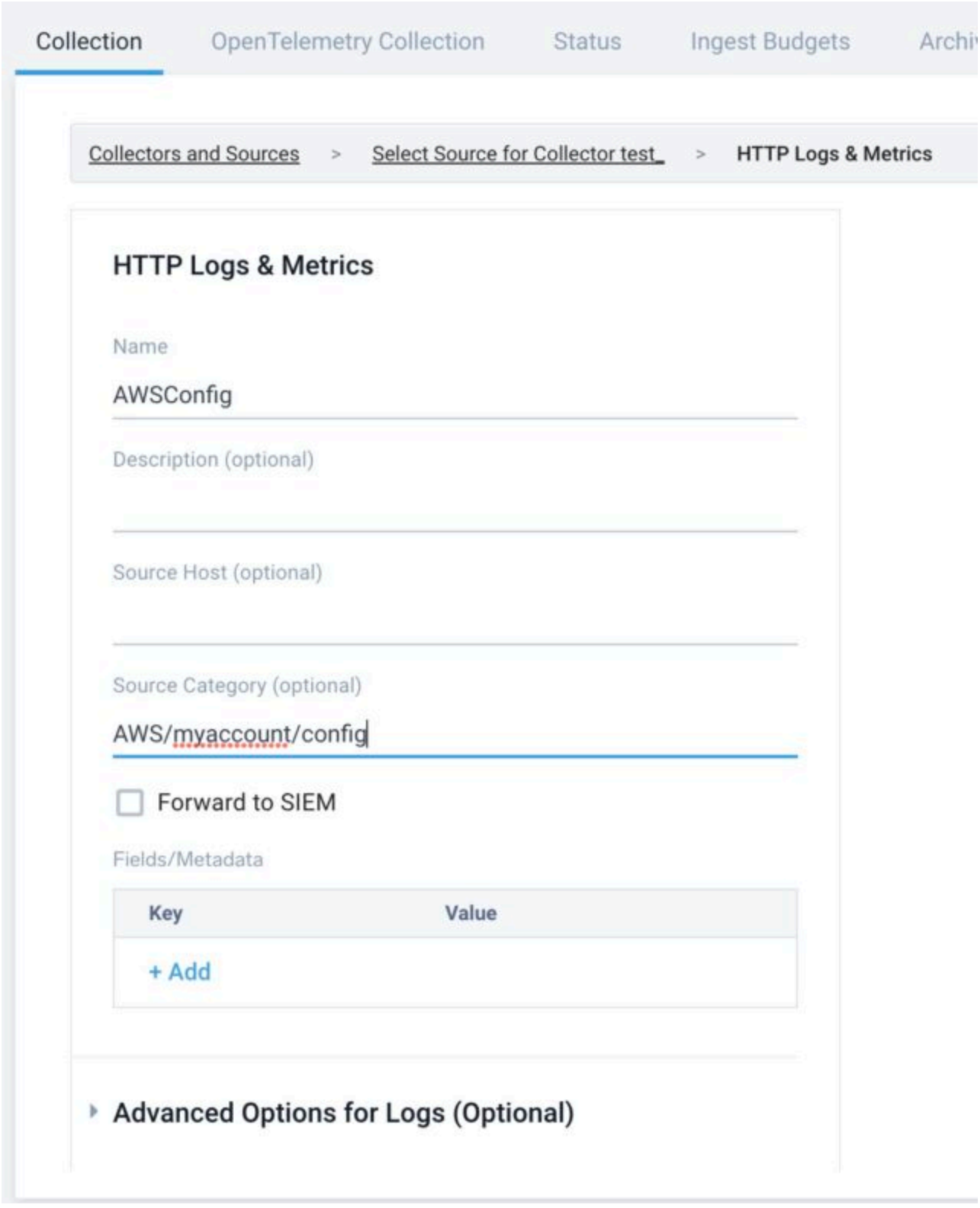
Next, create an HTTP Logs & Metrics Source from the Sumo Logic Management Console to the Hosted Collector, which will be the endpoint for receiving the SNS topic.

Manage Data > Collection
Add Source

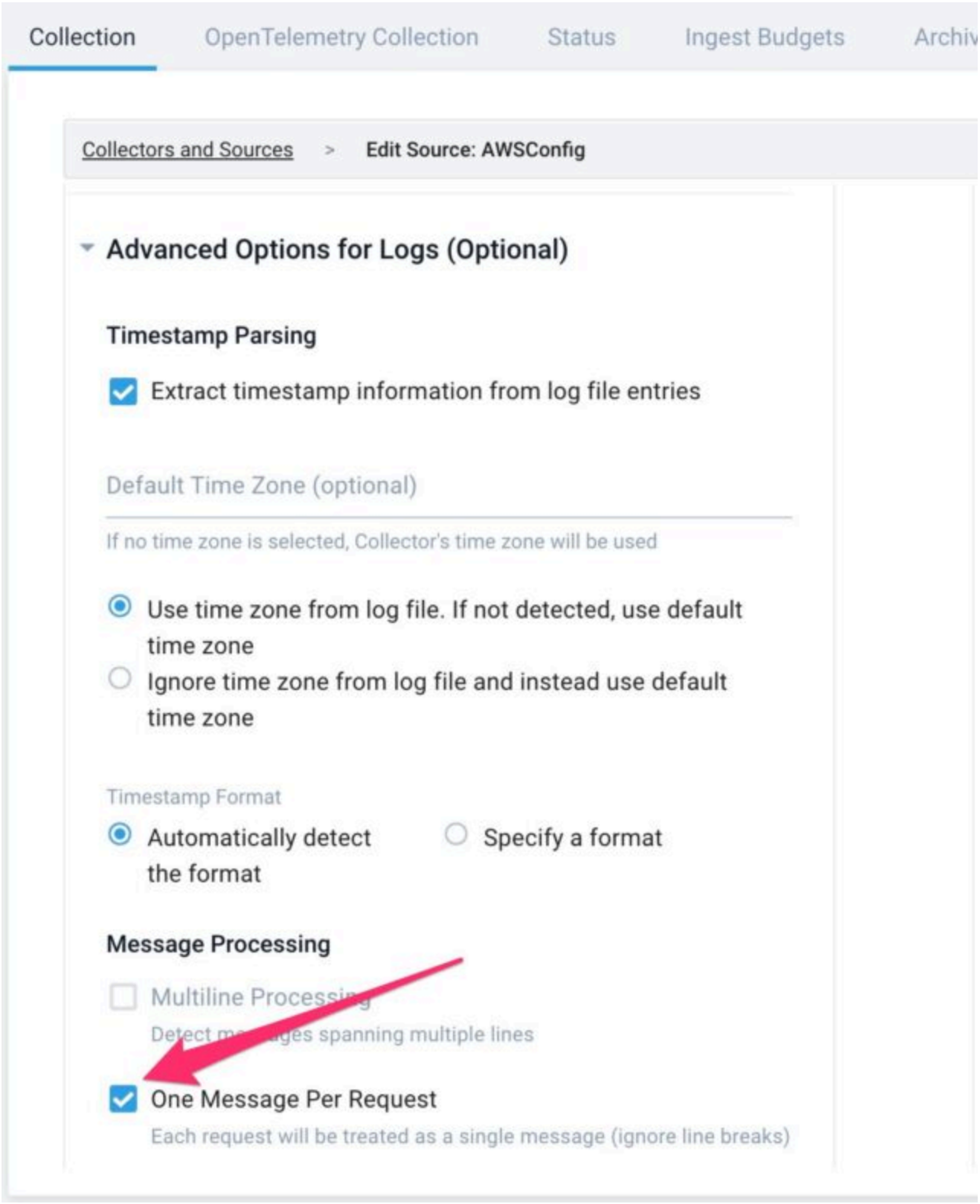




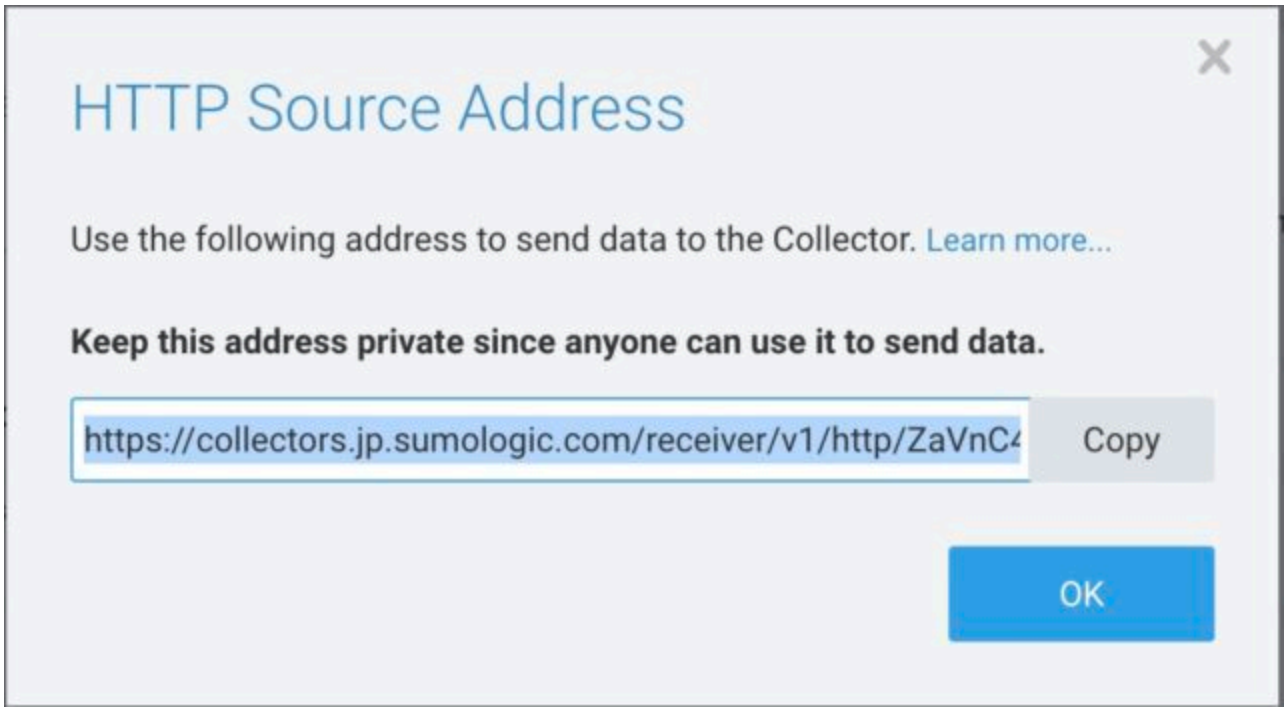
Set the source name and source category to any value.



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.

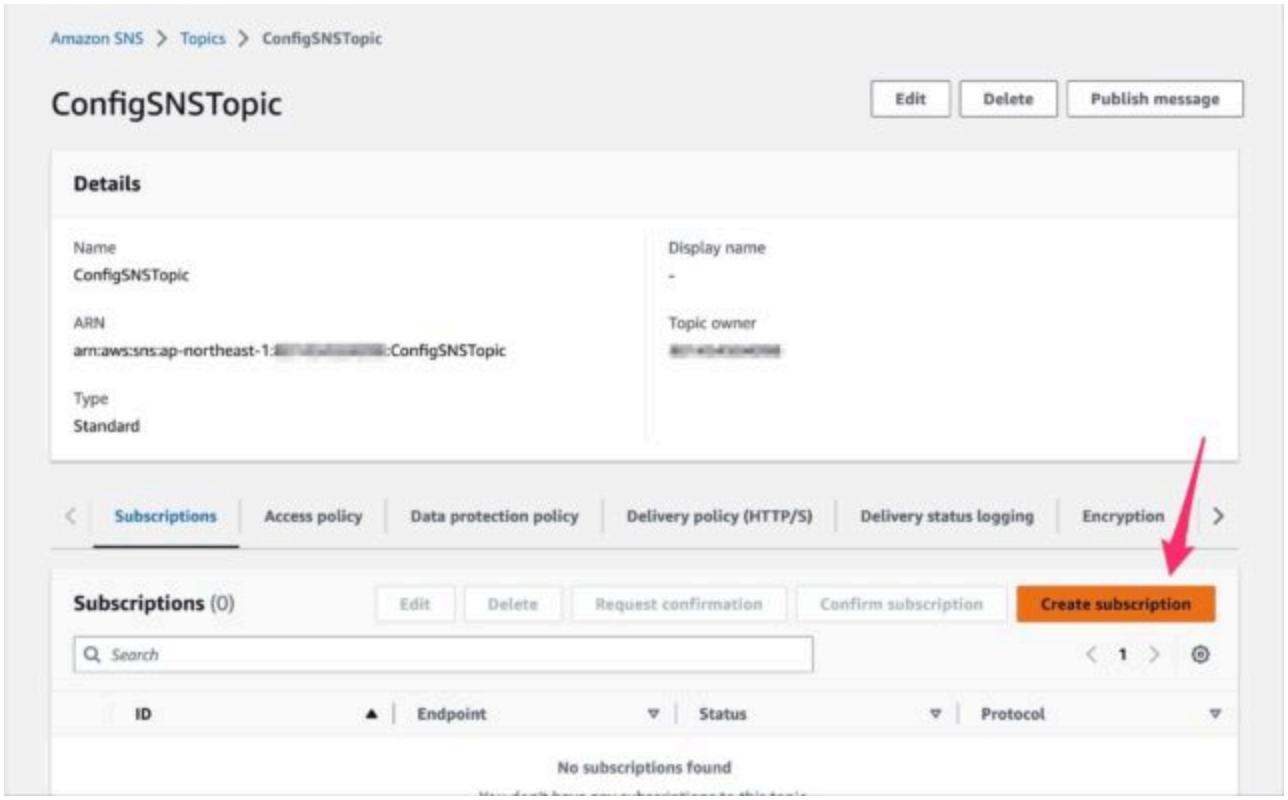


After creation, the endpoint URL will be displayed, so copy it.

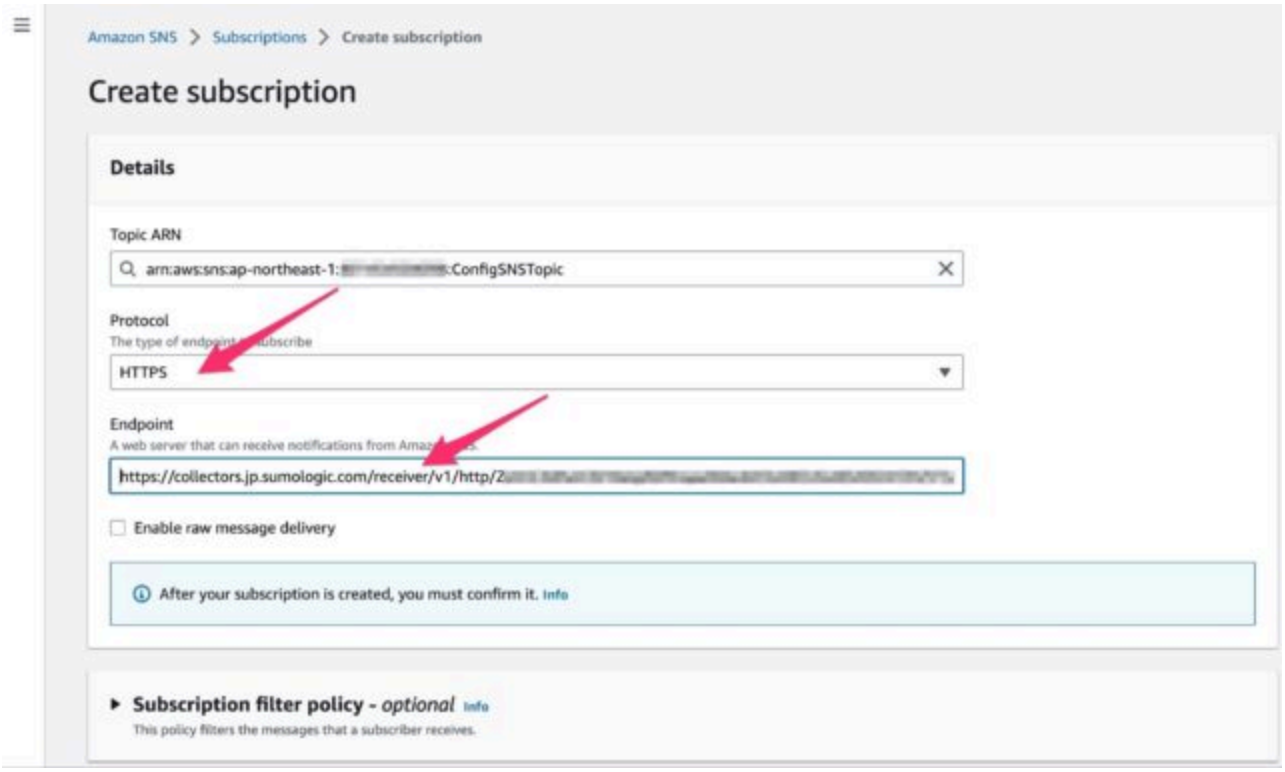


Social Media Settings

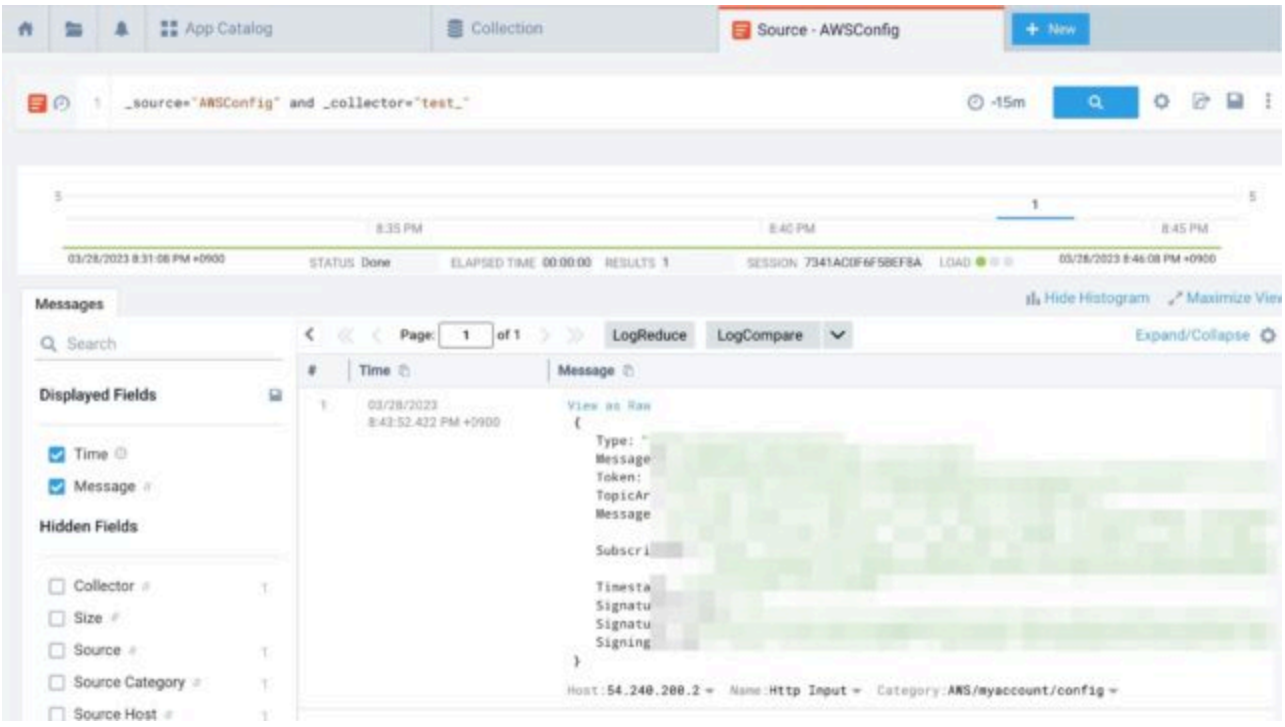
Return to the AWS Management Console and configure SNS.
Select the newly created topic in the Config settings and configure the subscription.



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

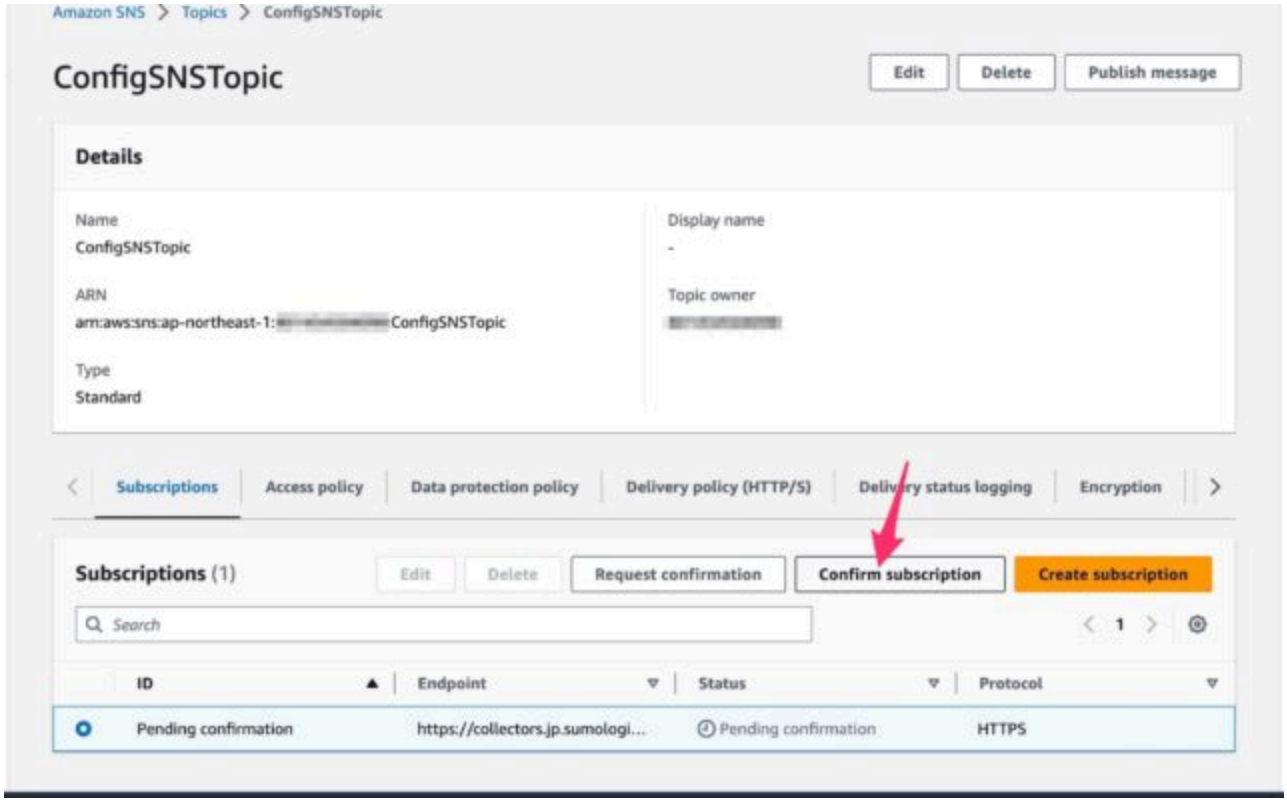


After that, wait a few minutes and you will receive a message from Sumo Logic confirming your subscription.

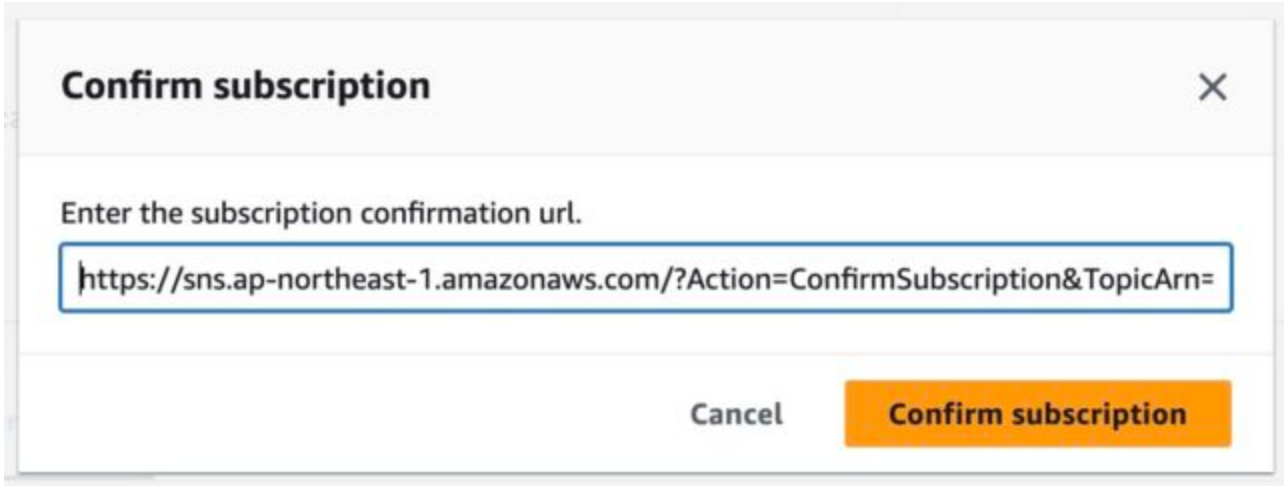


Once you have confirmed this log, copy the SubscribeURL value.

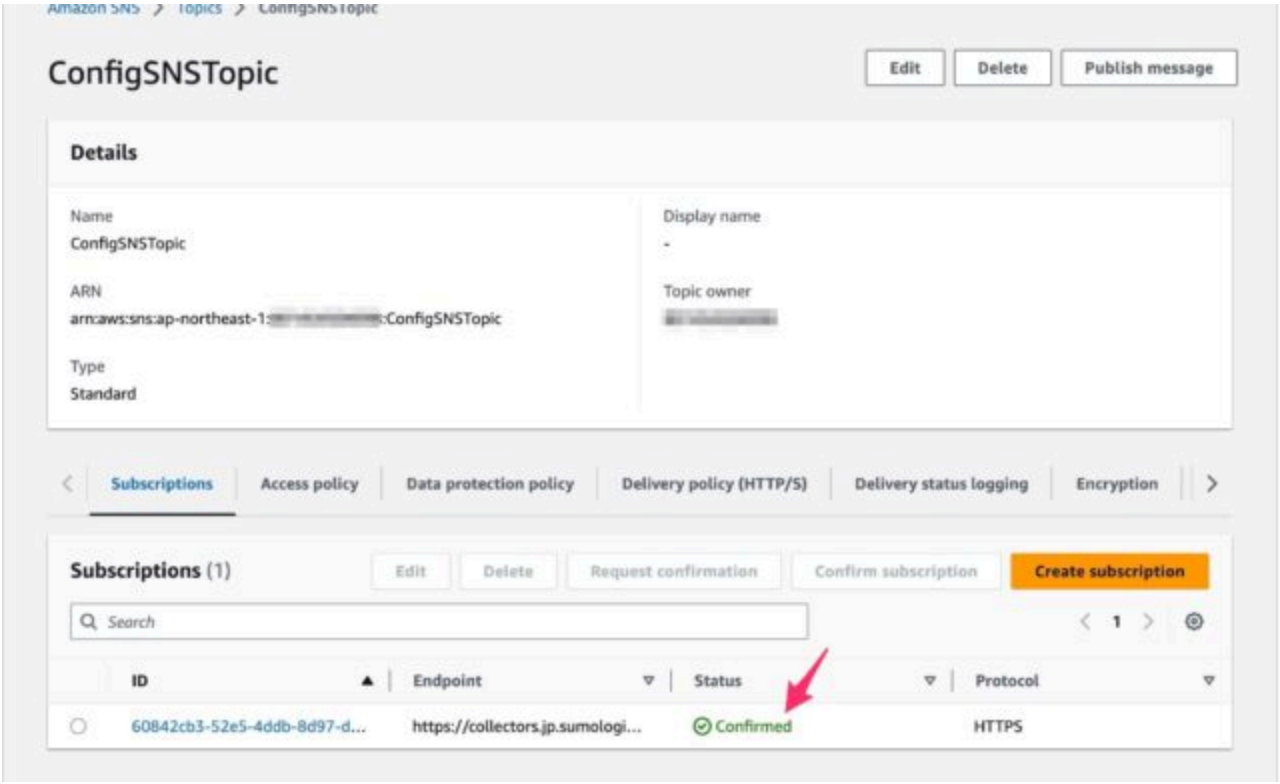
Again, go back to your SNS settings, select Subscriptions, and select Confirm Subscription.



Paste the Subscribe URL and confirm your subscription.



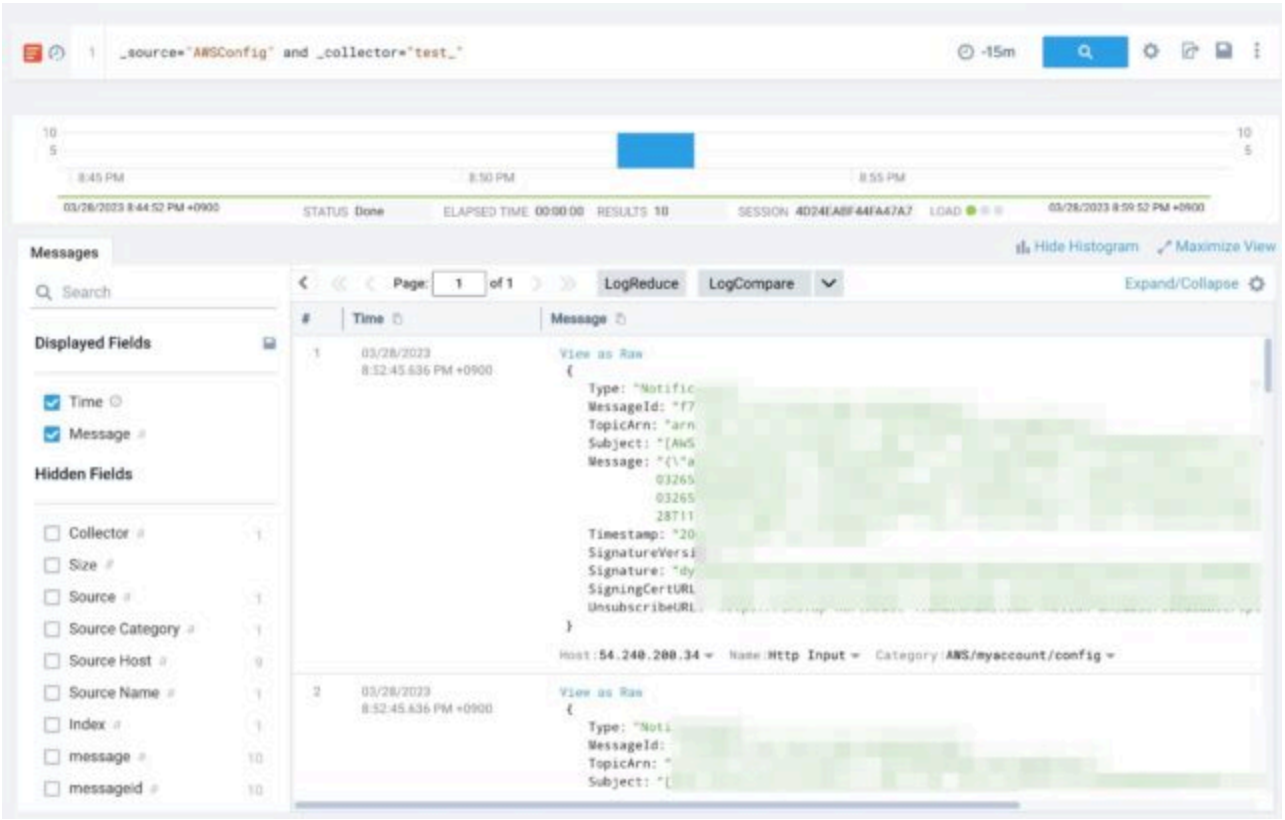
You will then see the status change to Verified.



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.