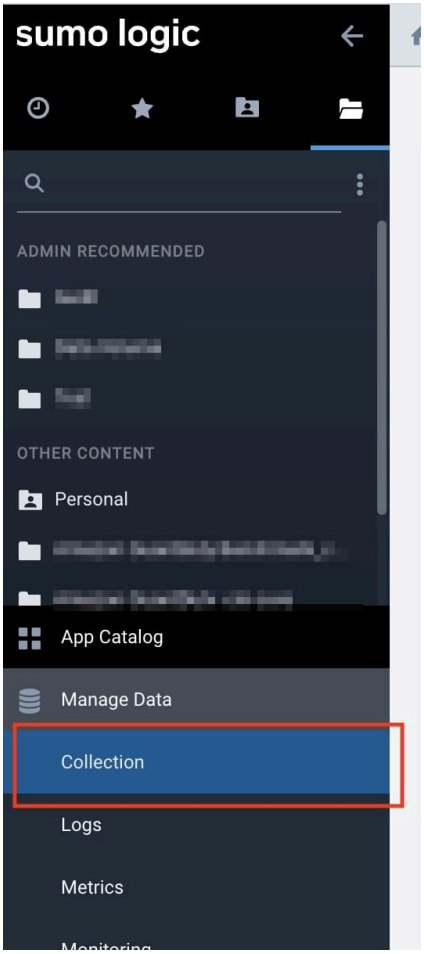
How to ingest logs from S3 into Sumo Logic

dev.classmethod.jp/articles/sumo-logic-aws-s3

酒井剛 June 3, 2022



When trying to aggregate and store AWS logs within AWS, it is very common to store the data in S3. In this article, we will introduce the most basic method of importing logs from AWS, which is from S3.
Let's take a look.

Introduction

There are two ways to import logs into Sumo Logic. In Sumo Logic, the function responsible for data collection is called **a collector . There is an agent-type (Installed Collector) that is installed on a host or instance, and an agentless type (Hosted Collector)** for services like S3 (Cloud Watch in an AWS environment, Microsoft 365 audit logs, etc.) that we will introduce here. Next, you define **a source**
for each type of log you want to import , and link that source to a collector to begin log

collection. Depending on the type of log, the source is a setting that defines various settings such as the log location, credentials for accessing the logs, polling and log acquisition conditions, etc.

procedure

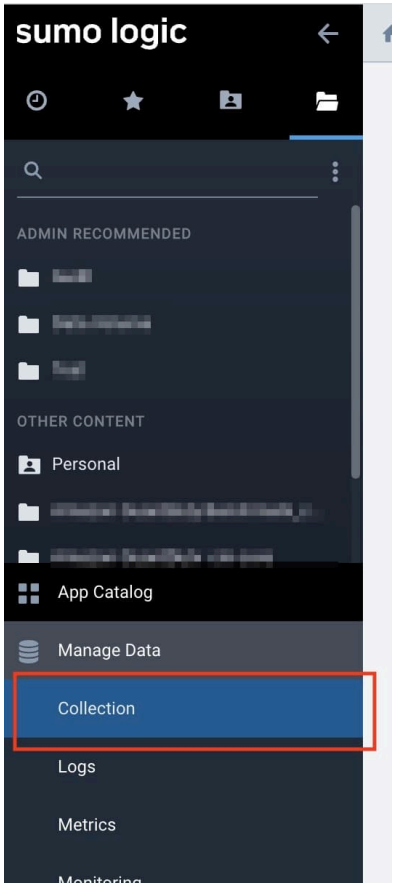
The import settings are generally set up in the following steps:

1. Create a Hosted Collector in Sumo Logic
2. In Sumo Logic, add a source to the collector you created.
    Set permissions (IAM role) in the AWS console during source configuration

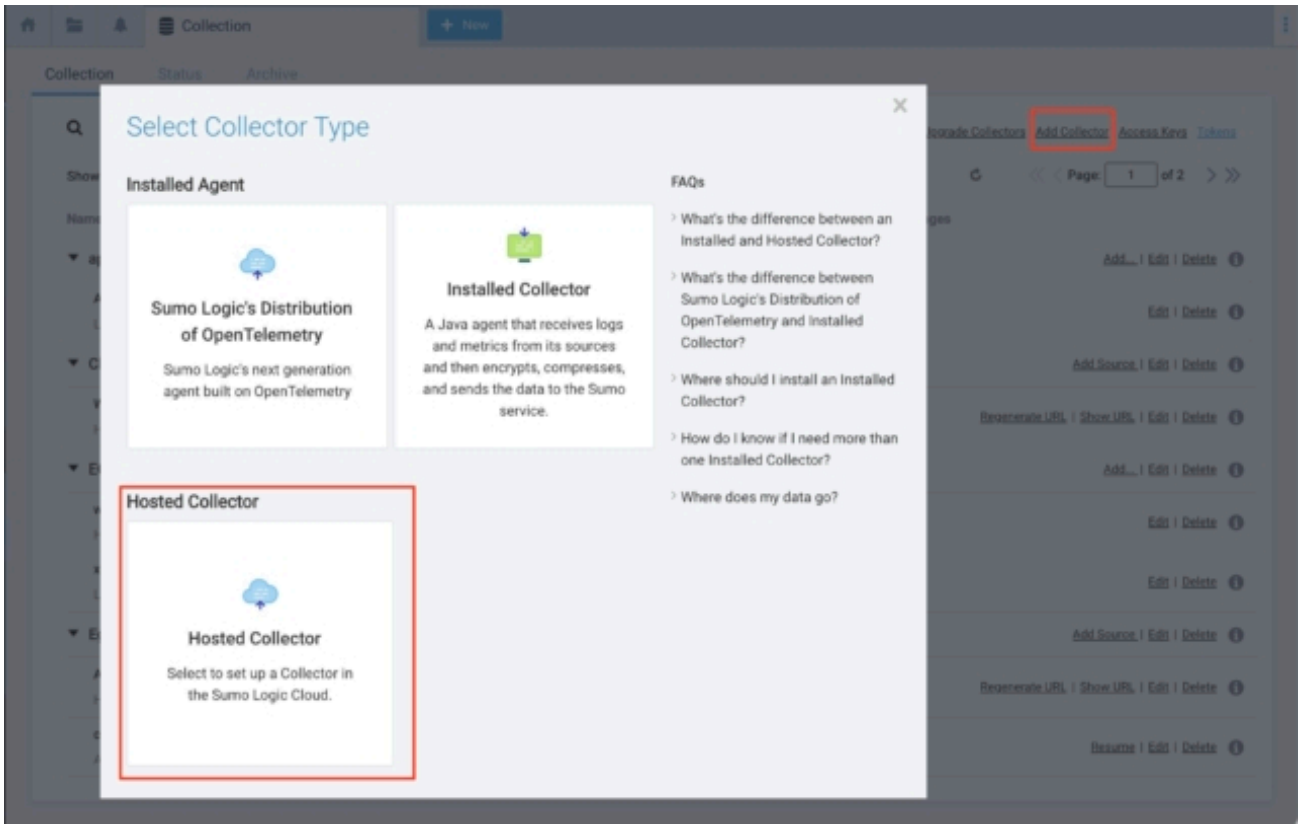
Sumo Logic has designed its setup process to be simple, minimizing the burden on users. Log integration is possible in just a few steps.

1. Create a Hosted Collector in Sumo Logic

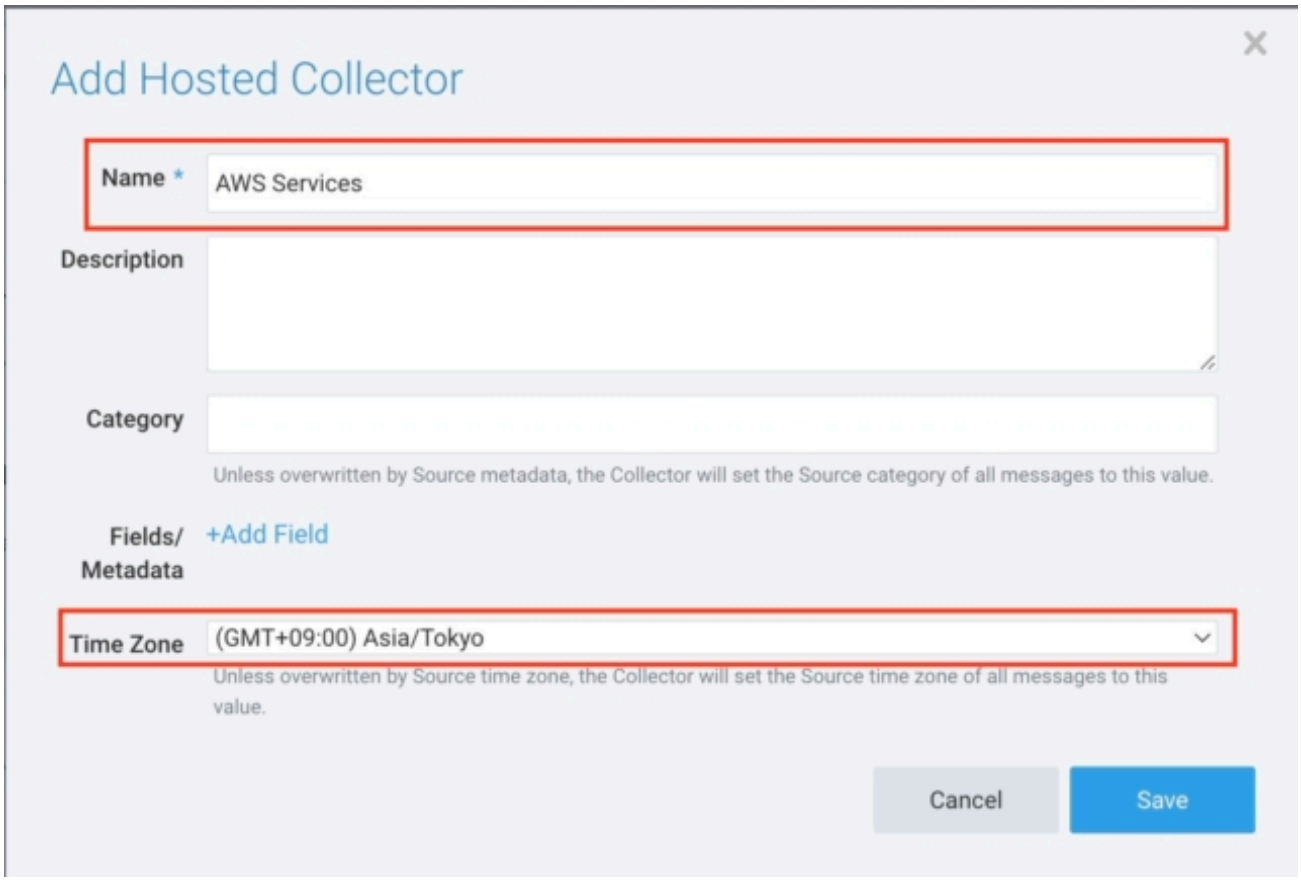
Click Collection under Manage Data on the sidebar



Select Add Collector -> Hosted Collector



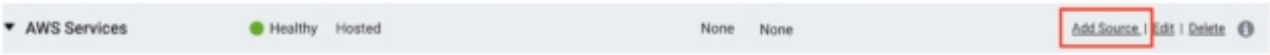
Set up a collector with a name of your choice and a time zone.



2. In Sumo Logic, add a source to the collector you created.

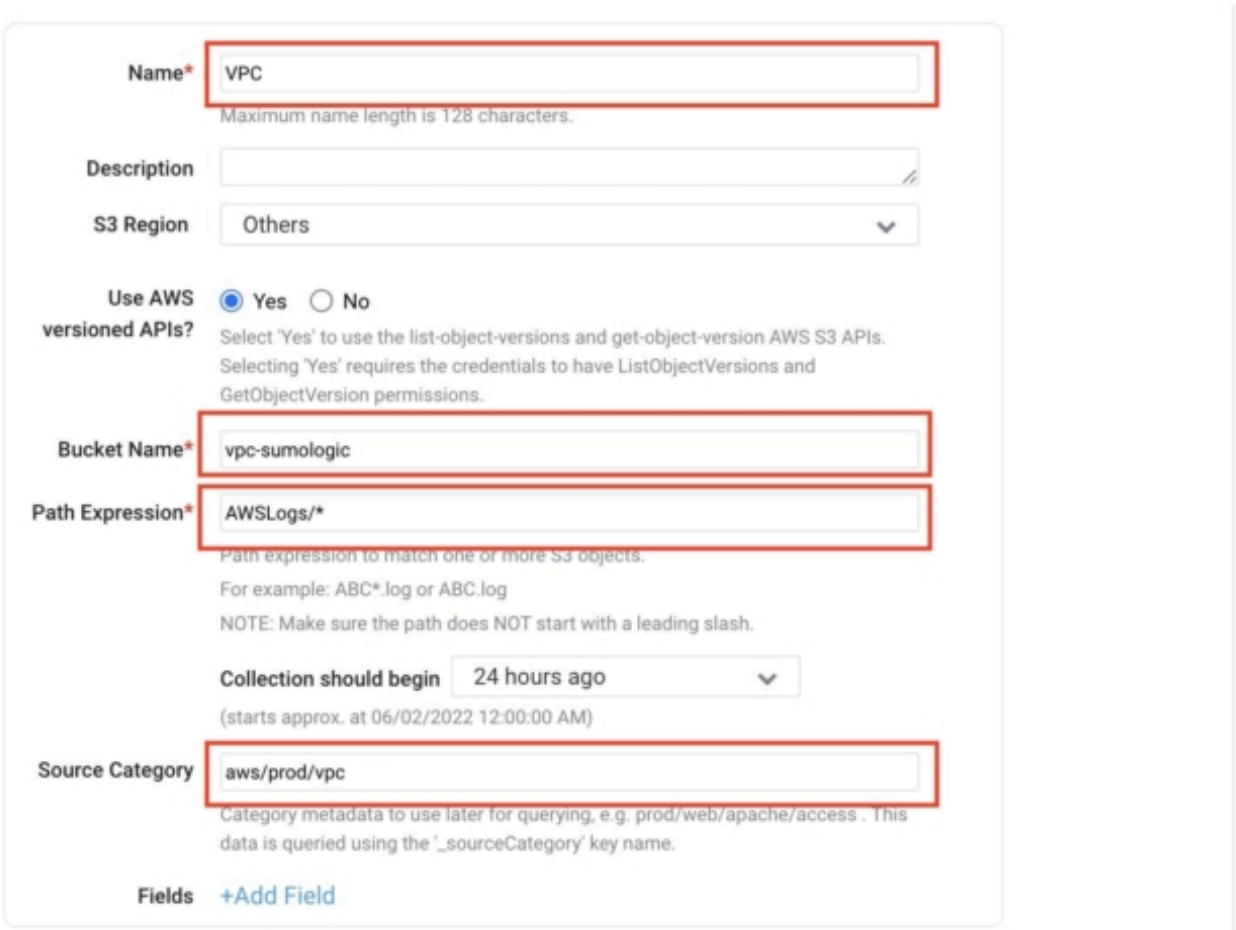
Sumo Logic Console

If you are creating a new collector, simply select Add Source or click "Add Source" for the collector you just created.



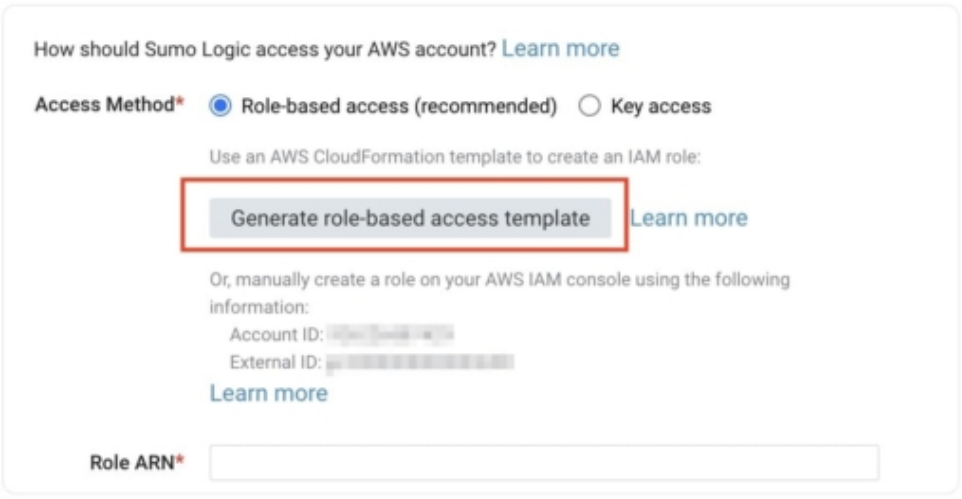
Select "Amazon S3" or "AWS CloudTrail" if you are storing your CloudTrail in S3.

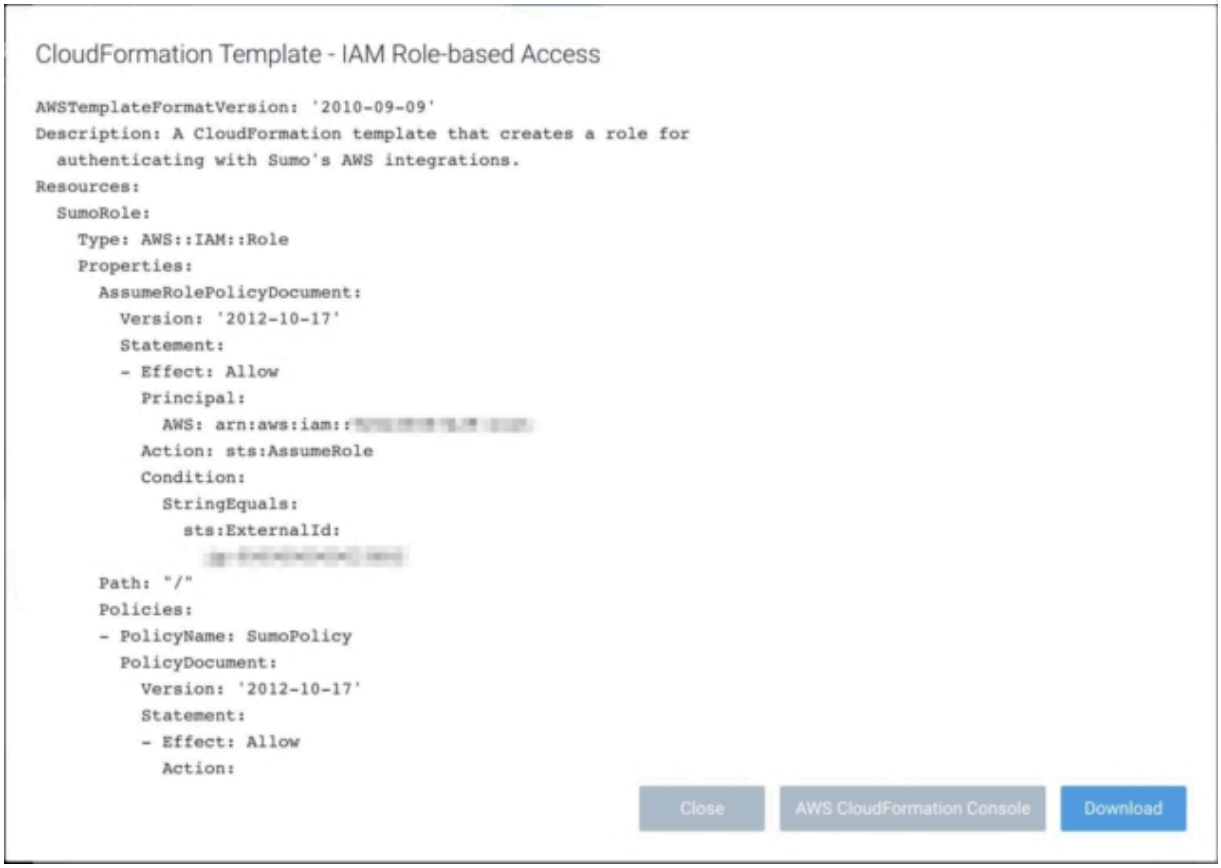
On the source settings screen, first fill in the following fields:



- Name: Any name you like is OK
- Bucket Name: Specify the bucket where the acquired logs are saved.
- Path Expression: Specify the path within the bucket to retrieve. (You can use an asterisk. The asterisk can only appear once in the path, so you can write it like this: path/*.log.)
- Source Category: Add any value to the metadata to identify logs when searching logs. It is recommended to use a hierarchical definition such as "aws/prod/vpc". We recommend using this naming scheme before using Sumo in production. For more information, please refer to the blog below.

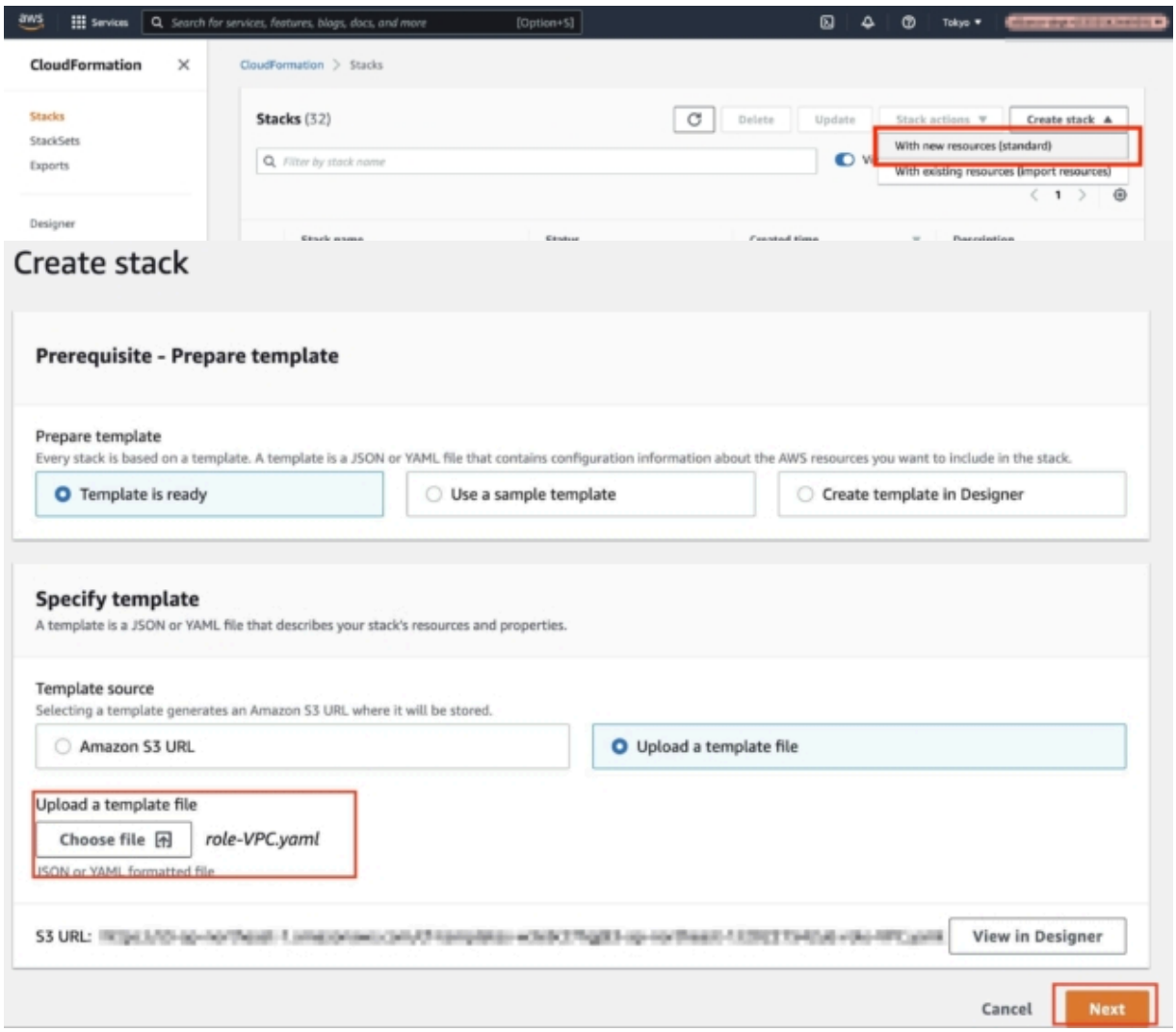
Under Access Method, click "Generate role-based access template." This will download a CloudFormation YAML template, which you can use to access the AWS management console and configure an IAM role that will allow Sumo to access the S3 logs in your AWS environment.



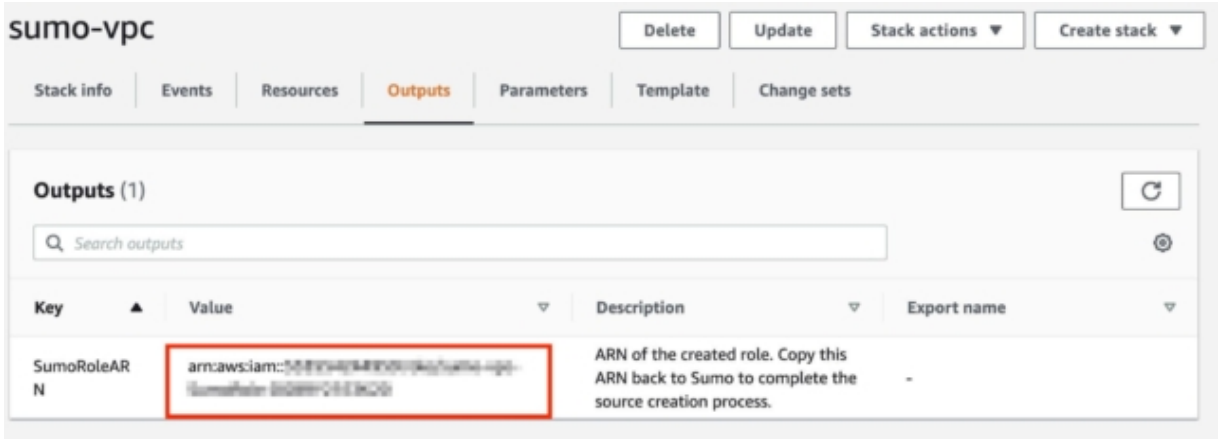


AWS Console

- Using the YAML file downloaded from CloudFormation in the AWS console, create an IAM role that will allow Sumo Logic to call the Get API for the bucket you specified earlier.

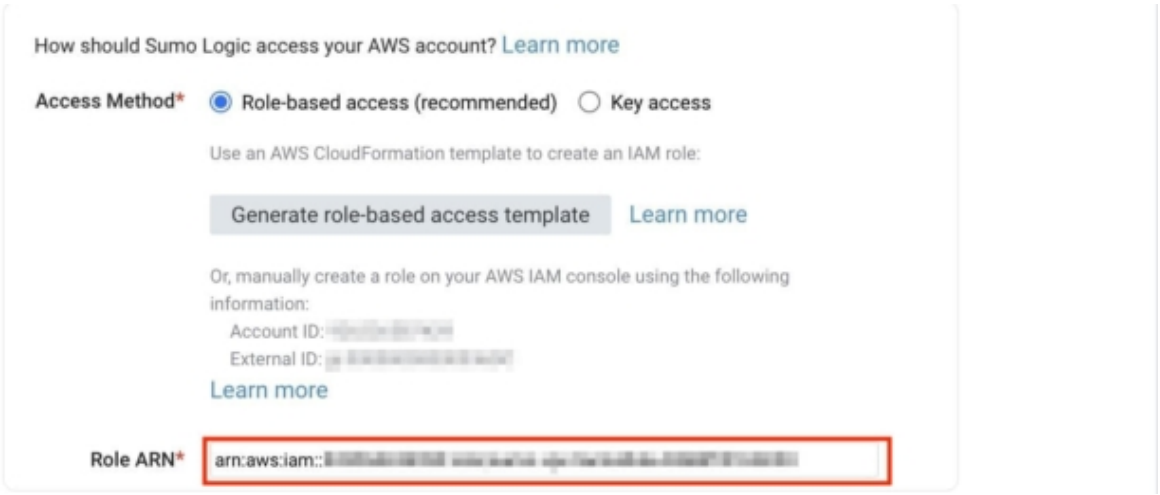


- Once CloudFormation is complete, check the ARN of the created IAM role from the output of the created stack.

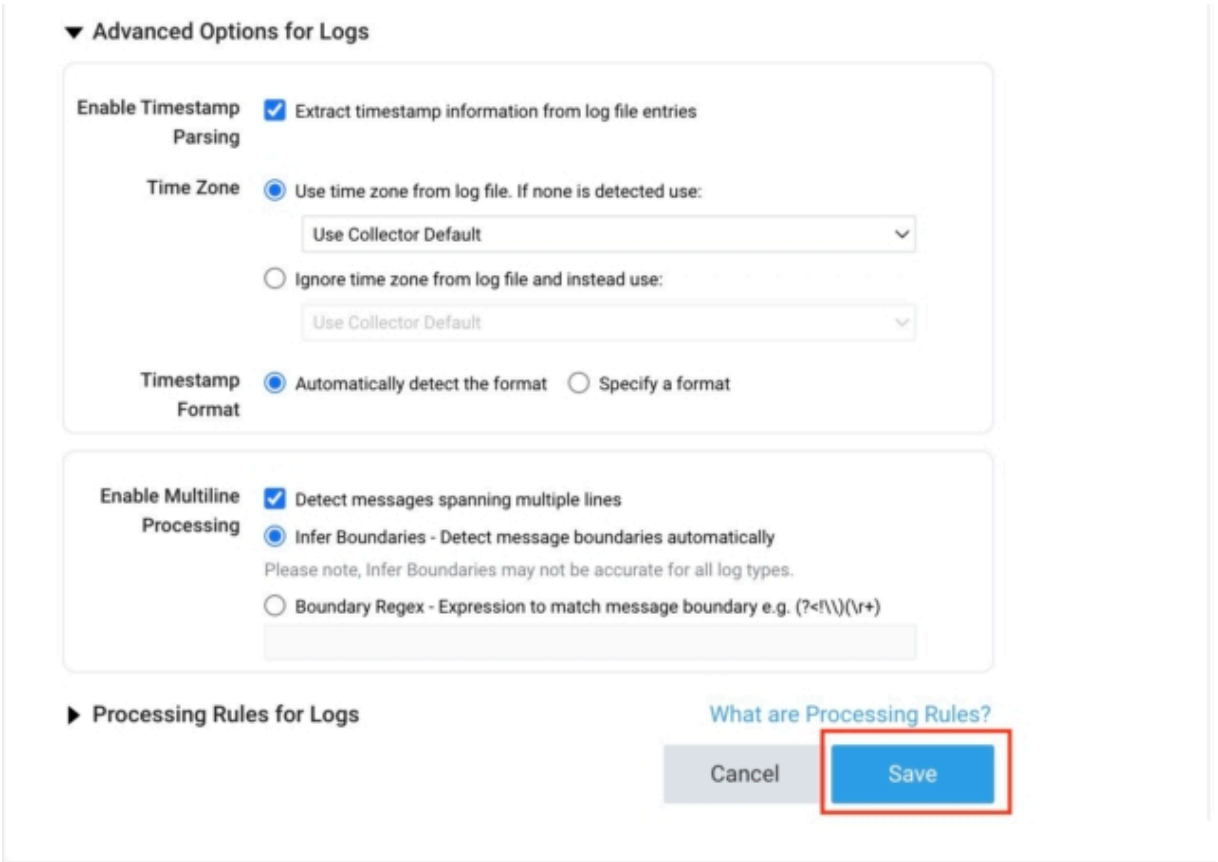


Sumo Logic Console

- Once you have completed the above steps, return to the Sumo Logic console and enter the ARN of the role you just created.

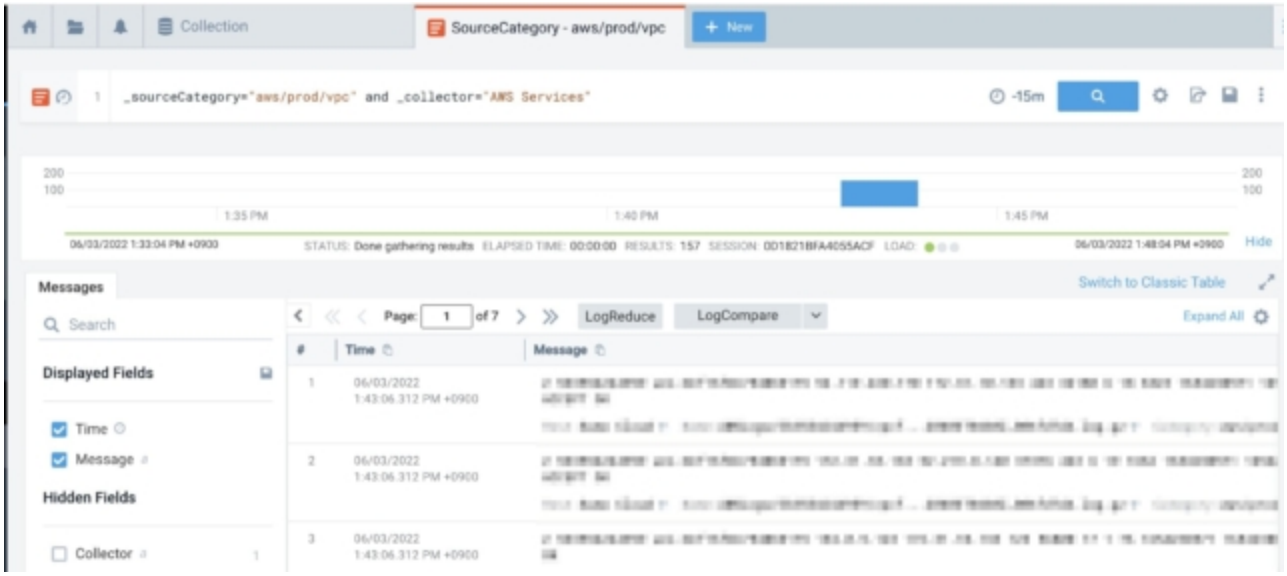


- If no other detailed settings are required, you can leave the remaining settings blank. Once you save the settings, log collection will begin. (Note: If an error message appears and you cannot confirm the settings when saving them, there is an error. Return to the previous item and check the settings.)



Verify that logs are being captured

Check that the logs are being imported by going to the Collection source or by opening a new Log Search screen. If they are not being imported, wait a while and try again.



summary

This time, we introduced the most basic method of ingesting logs from AWS: ingesting logs from S3. We hope this article will be useful for those who are considering trying out Sumo Logic.