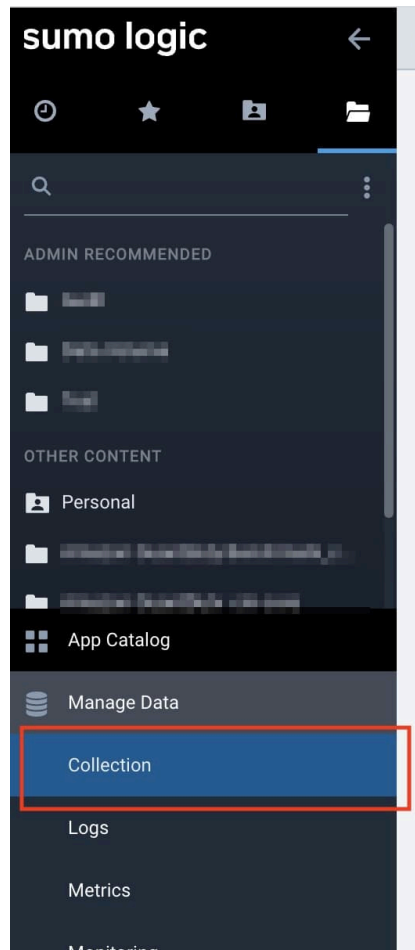


How to ingest logs from S3 into Sumo Logic

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

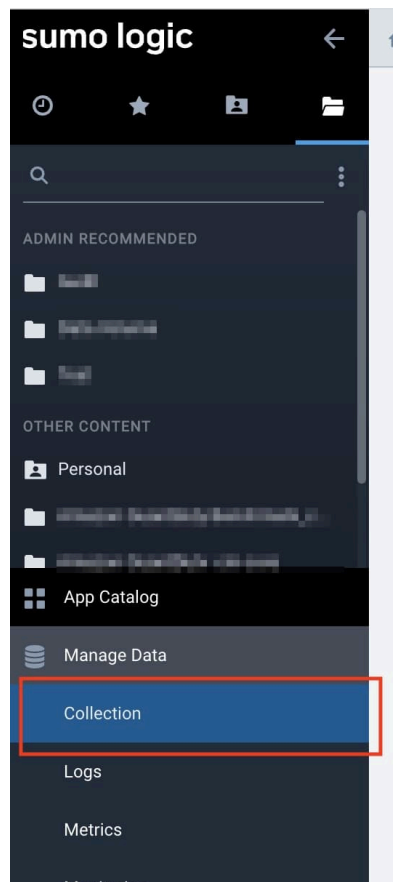
The import settings are generally set up in the following steps:

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

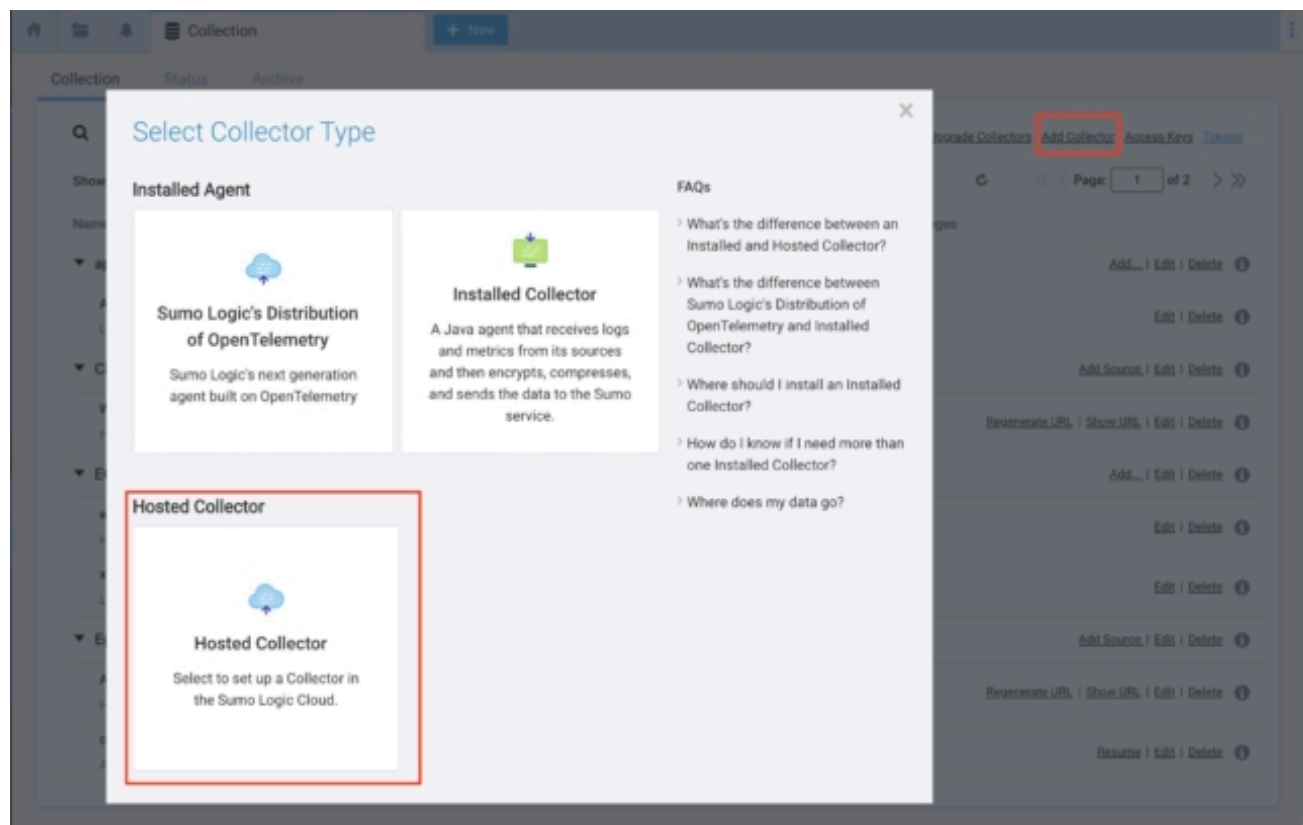
Sumo Logic has designed its setup process to be simple, minimizing the burden on users. Log integration is possible in just a few steps.

1. Create a Hosted Collector in Sumo Logic

Click Collection under Manage Data on the sidebar



Select Add Collector -> Hosted Collector



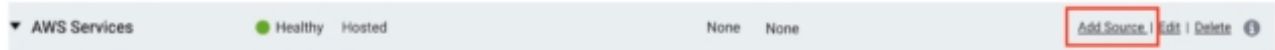
Set up a collector with a name of your choice and a time zone.

A screenshot of the "Add Hosted Collector" form in the Sumo Logic interface. The form has several input fields: "Name" (containing "AWS Services"), "Description" (empty), "Category" (empty), and "Time Zone" (a dropdown menu set to "(GMT+09:00) Asia/Tokyo"). The "Name" and "Time Zone" fields are highlighted with red rectangular boxes. Below the "Time Zone" field is a note: "Unless overwritten by Source time zone, the Collector will set the Source time zone of all messages to this value." At the bottom right of the form are "Cancel" and "Save" buttons.

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:

A screenshot of the Sumo Logic source settings form. The form contains several fields, some of which are highlighted with red rectangular boxes: 'Name' (containing 'VPC'), 'Bucket Name' (containing 'vpc-sumologic'), 'Path Expression' (containing 'AWSLogs/*'), and 'Source Category' (containing 'aws/prod/vpc'). Other visible fields include 'Description', 'S3 Region' (set to 'Others'), 'Use AWS versioned APIs?' (set to 'Yes'), 'Collection should begin' (set to '24 hours ago'), and a 'Fields' section with a '+Add Field' button. The form also includes helpful text and a note about path expressions.

- 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.

How should Sumo Logic access your AWS account? [Learn more](#)

Access Method* ☒ Role-based access (recommended) ☐ Key access

Use an AWS CloudFormation template to create an IAM role:

Generate role-based access template [Learn more](#)

Or, manually create a role on your AWS IAM console using the following information:

Account ID:

External ID:

[Learn more](#)

Role ARN*

CloudFormation Template - IAM Role-based Access

```
AWSTemplateFormatVersion: '2010-09-09'
Description: A CloudFormation template that creates a role for
  authenticating with Sumo's AWS integrations.
Resources:
  SumoRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              AWS: arn:aws:iam::[Account ID]:[External ID]
            Action: sts:AssumeRole
            Condition:
              StringEquals:
                sts:ExternalId: [External ID]
      Path: "/"
      Policies:
        - PolicyName: SumoPolicy
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
```

[Close](#) [AWS CloudFormation Console](#) [Download](#)

AWS Console

- CloudFormation

Stacks

StackSets

Exports

Designer

CloudFormation > Stacks

Stacks (3/2)

Create Delete Update Stack actions Create stack

Filter by stack name

With new resources (standard)
With existing resources (import resources)

< 1 >

Stack name	Status	Created time	Parameter
------------	--------	--------------	-----------

Create stack

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready

☐ Use a sample template

☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

☒ Upload a template file

Upload a template file

Choose file role-VPC.yaml
JSON or YAML formatted file

S3 URL: [https://s3-us-west-2.amazonaws.com/elasticbeanstalk-us-west-2-924460549404/role-VPC.yaml](#)

View in Designer

Cancel Next

- sumo-vpc

Delete

Update

Stack actions ▾

Create stack ▾

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Outputs (1)

🔄

🔍 Search outputs

⚙️

Key	Value	Description	Export name
SumoRoleARN	arn:aws:iam::555541111111:role/sumo-vpc-SumoRole-6122PVA8K0G	ARN of the created role. Copy this ARN back to Sumo to complete the source creation process.	-

6/8

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

How should Sumo Logic access your AWS account? [Learn more](#)

Access Method* ☒ Role-based access (recommended) ☐ Key access

Use an AWS CloudFormation template to create an IAM role:

[Generate role-based access template](#) [Learn more](#)

Or, manually create a role on your AWS IAM console using the following information:

Account ID:

External ID:

[Learn more](#)

Role ARN*

- 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.)

▼ **Advanced Options for Logs**

Enable Timestamp Parsing ☒ Extract timestamp information from log file entries

Time Zone ☒ Use time zone from log file. If none is detected use:

☐ Ignore time zone from log file and instead use:

Timestamp Format ☒ Automatically detect the format ☐ Specify a format

Enable Multiline Processing ☒ Detect messages spanning multiple lines

☒ Infer Boundaries - Detect message boundaries automatically

Please note, Infer Boundaries may not be accurate for all log types.

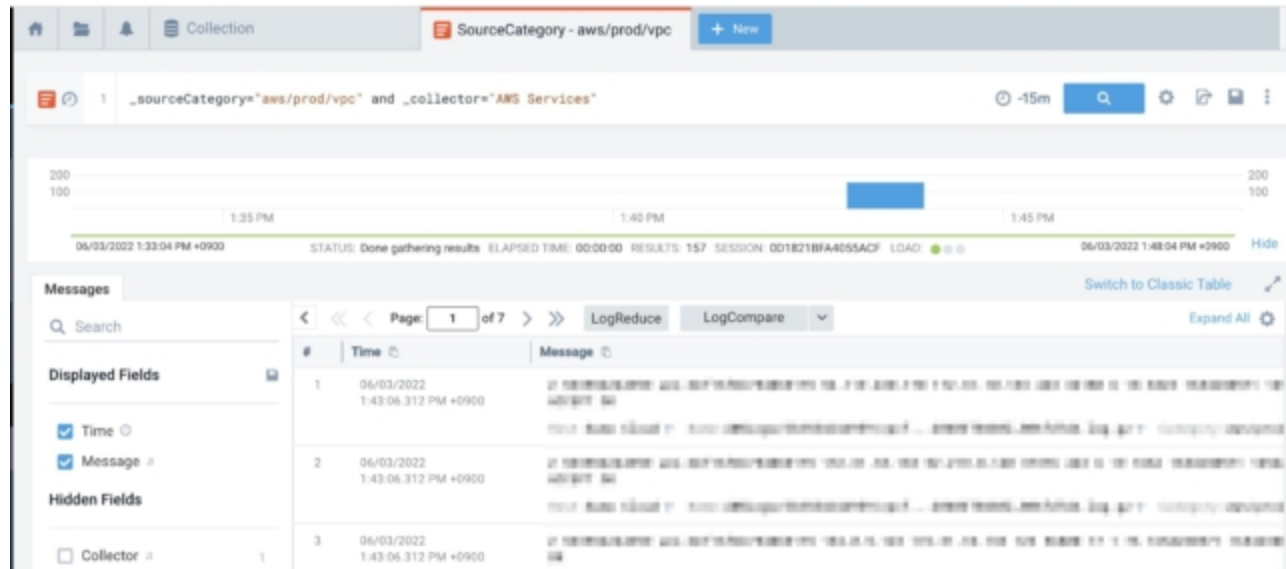
☐ Boundary Regex - Expression to match message boundary e.g. (?<\\)(r+)

► **Processing Rules for Logs**

[What are Processing Rules?](#)

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.