How to create a Scheduled View

dev.classmethod.jp/articles/sumologic-scheduled-view-creation-and-notes

佐久間昇吾

December 21, 2022

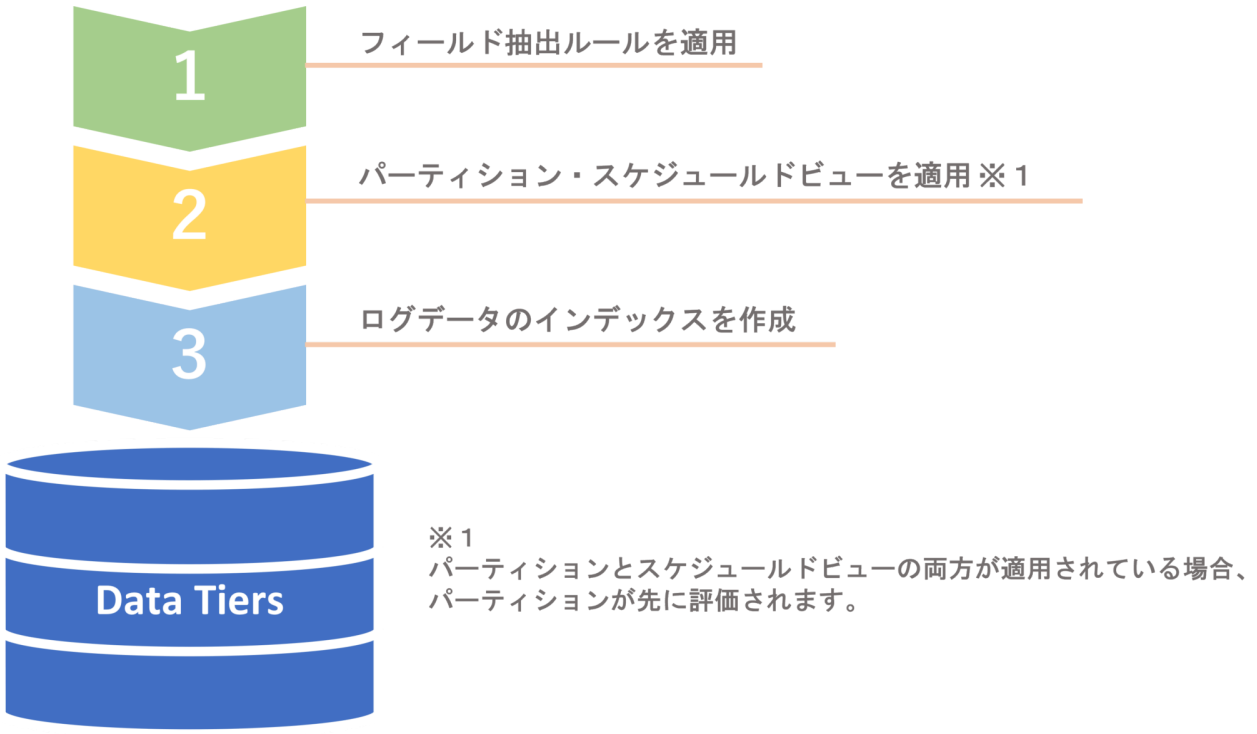
If the content of the article is outdated, please also check the official website.

For more information about Sumo Logic, please see below.

- Sumo Logic official website
- Classmethod - Cloud-native log management and analytics SaaS "Sumo Logic"

First

When Sumo Logic receives message data (logs and metrics), it evaluates the data in the following order:



***This time we will introduce Scheduled View!**

About Scheduled Views

Scheduled Views proactively aggregate log data before it is indexed, calculating and outputting data within a specific time period.

Common use cases include gaining rapid insights into traffic patterns, user activity, and threat trends such as firewalls.

Therefore, the goal is to analyze trends over the medium to long term.

The aggregated data is indexed in a later step, and historical data is indexed to allow data aggregation within a period.

Points to note when creating a Scheduled View

There are some limitations and best practices for creating a Scheduled View:

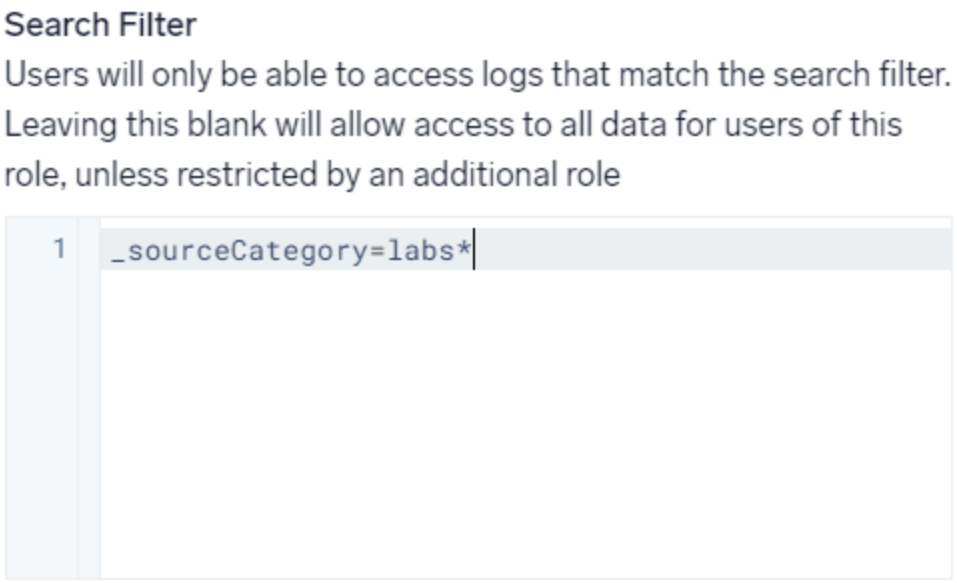
Required roles for creating a Scheduled View

- **Manage Scheduled Views**
  You can view, create, edit, and delete Scheduled Views.

  Account administrators and accounts with the Manage Scheduled Views permission can configure Scheduled Views.
  All other users without this permission can search Scheduled Views. If you do not

want users to be able to search, you can control this by using roles in the search filter to control log data access.

- Tip -
① Administration > ② Users and Roles > ③ Roles > ④ + Add Role
The search filter allows you to display only the data that you are allowed to access according to your role. In the following case, you can only access data in _sourceCategory that starts with labs.



- Source -
Create and Manage Roles
Understanding search filters

Scheduled View Limitations

- **Up to 500 per account**
- **I can't edit/update a Scheduled View I created**
  When editing, you can change only the data retention period and data transfer.
  Also, if you want to shorten the default retention period, you can choose to shorten it after 7 days or immediately.

- **Once a Scheduled View has been created, it cannot be disabled and then enabled.**
  Scheduled views can be paused or resumed.
  Scheduled views that you decide you will not use can be disabled. If disabled, they cannot be resumed.

- **Scheduled View search queries run once every minute.**
- **If raw log messages are included, they will be counted as ingested**

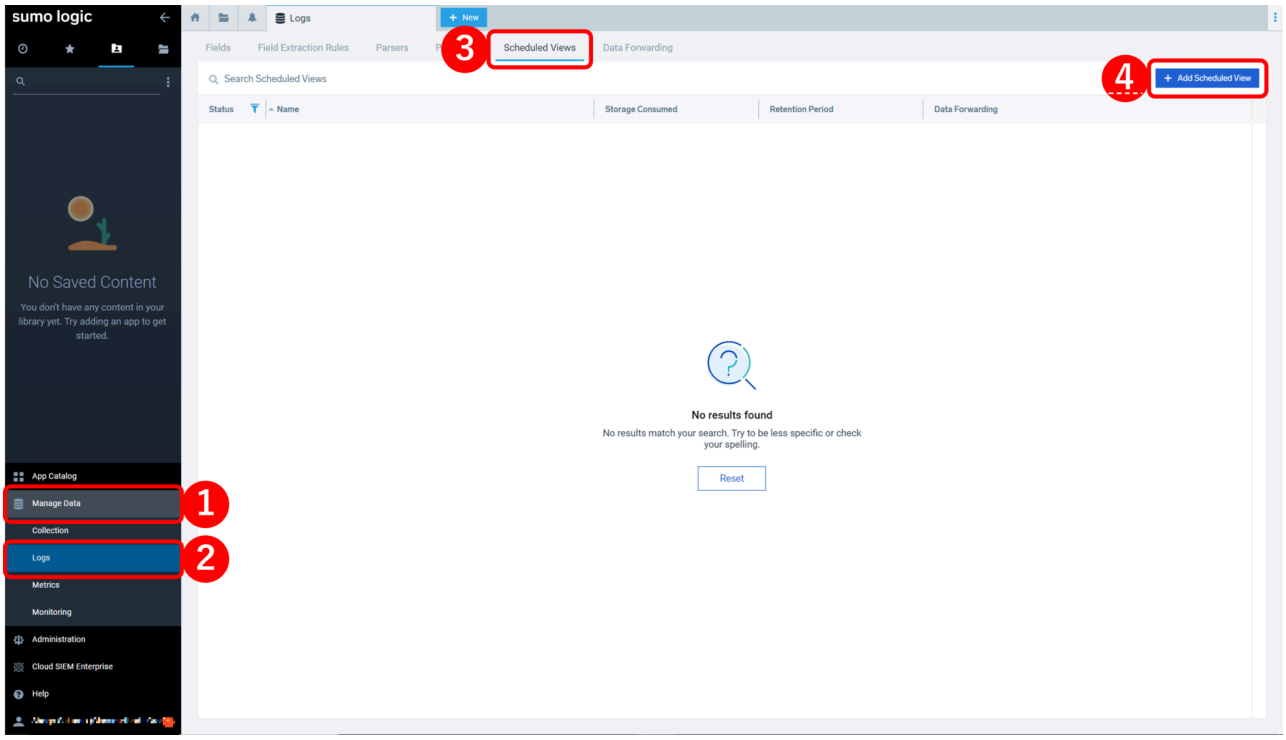
If raw data is included, the collected message data will be counted as the amount of data ingested.

Scheduled View Best Practices

- **Set an appropriate retention period and use it for trend analysis**
  Scheduled Views do not analyze large amounts of log data at once, but instead query data for a set retention period, allowing for ad-hoc searches.

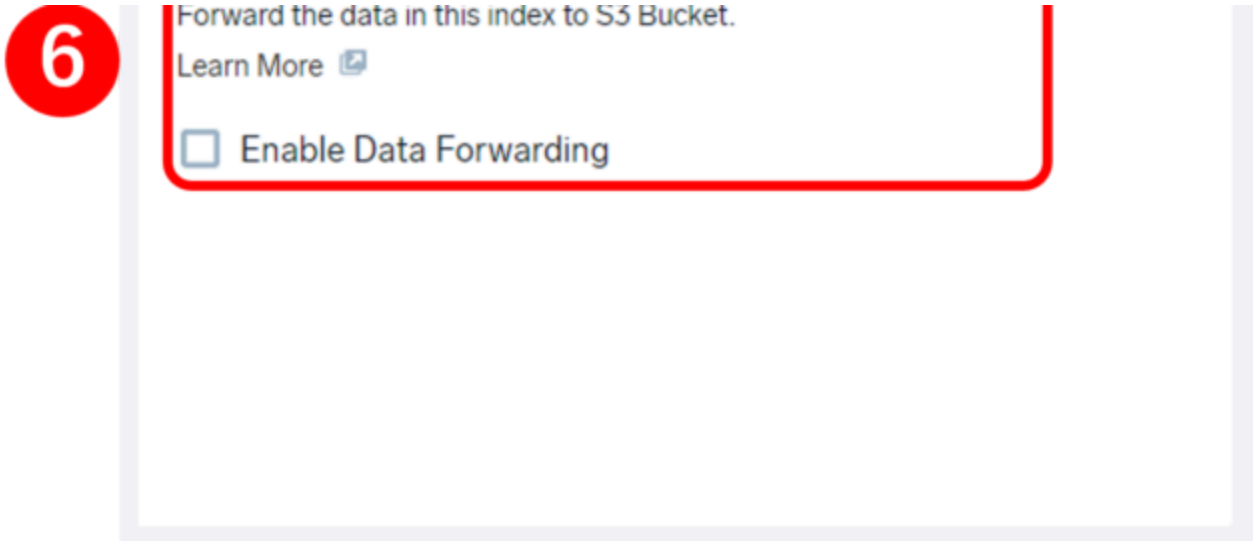
- **Using the schedule view in conjunction with partitions allows for the fastest query search.**
- **Do not create queries that are subject to change**
- **Query expressions can be defined flexibly.**
  Make sure that changes to the metadata do not break the query.
  For example,
  _sourceCategory=*/apache/*

① Manage Data > ② Logs > ③ Scheduled Views > ④ + Add Scheduled View



The following Scheduled View creation menu will then appear on the right.


Create New Scheduled View
Save
1
Scheduled View Name
Query
2
3
Search Mode
Auto Parse Mode
4
Start Date
5
Retention Period (in days)
Apply the retention period of the Default Continuous Partition
Data Forwarding



① Scheduled View name

Enter the name of the Scheduled View you want to create.
Alphanumeric characters (uppercase and lowercase), numbers, and underscores (_) can be used.

② Query

Use Parse Operators and Search Operators to write queries to the indexed data.
For more information about operators, see Scheduled Views Best Practices and Examples .

Tip: We recommend using
the group operator, aggregate operator , or even the timeslice search operator
, as theseallow you to create a Scheduled View for **small amounts of data .**
Both the **group operator and the aggregate operator**
have the feature of compartmentalizing the data to be aggregated.
The **timeslice Search Operator**
allows you to specify the period of data to be aggregated.
If you do not specify a period here, you must specify a period using Receipt Time .

③ Search Mode

Select how to parse the message data.

- **Auto Paarse Mode**
  SumoLoigc will automatically analyze and parse the message data. This is the mode to select when using this function.
- **Manual Mode**

This is the mode to select when you want to manually write and parse a combination of Parse syntax and regular expressions.

④ Start Date

Specify the start date for indexing data. Data from the selected date onwards will be indexed as Scheduled View data.

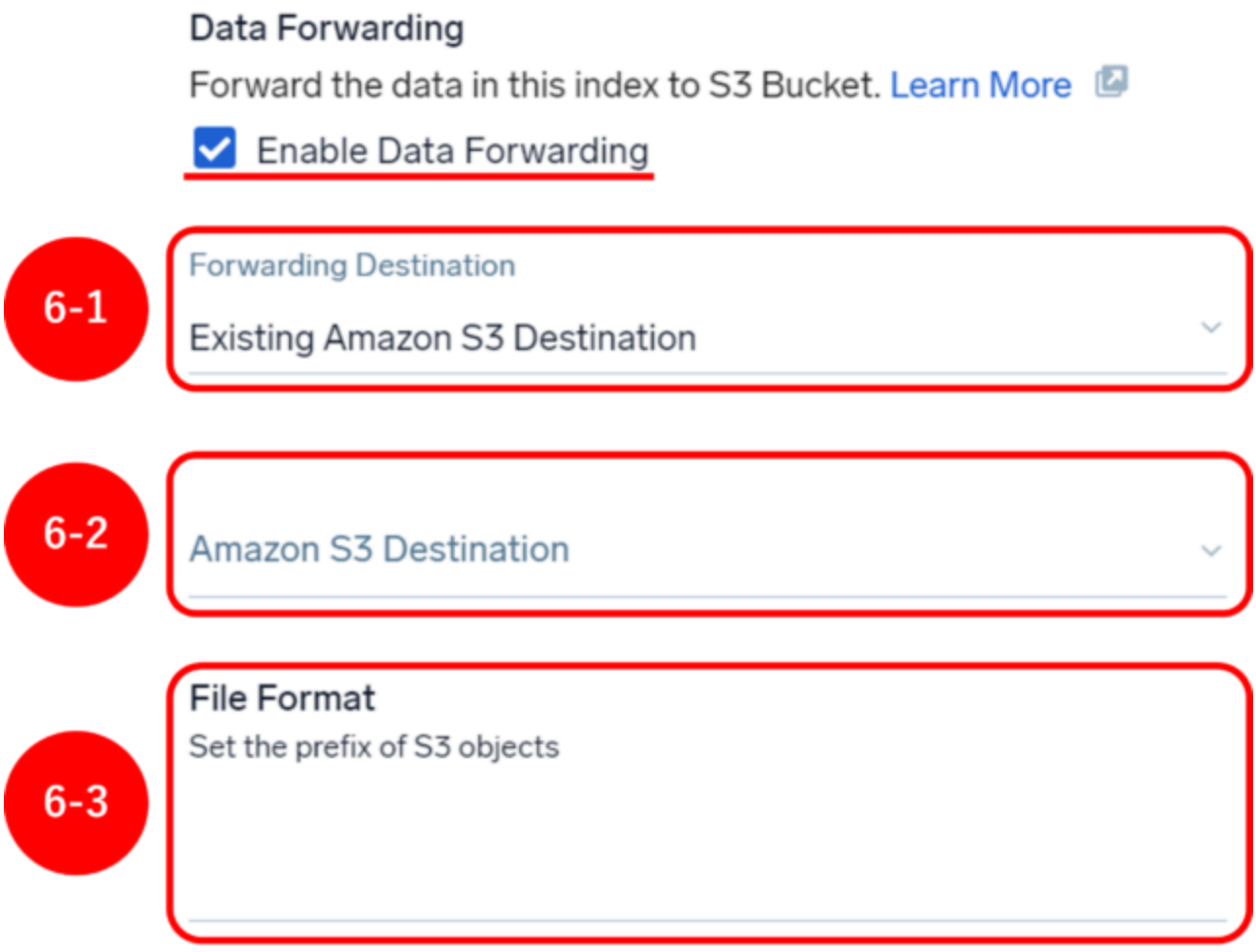
⑤ Retention Period (in days)

Set the retention period for indexed data, between 1 and 5000 days.

- Tip -
Apply the retention period of Default Partition
: Checking this box will set the data retention period to the default of 30 days.

⑥ Data Forwarding

When you enable the Data Forwarding checkbox, the following settings screen will appear.



6-1. Forwarding Destination
: Select either an existing forwarding destination to S3 or create a new forwarding destination. If you select a new forwarding destination, you will need to configure the bucket name, access method, ARN, etc. on the same screen.
6-2. Amazon S3 Destination:
This will only be displayed if you select an existing forwarding destination.
A list of configured forwarding destinations will be displayed, so please select one.

6-3. File Format
Set the path to the directory in the S3 bucket.
For details on the path format, please see Forward data to S3 .

- Note -
If you transfer to another region, you will need a transfer amount.

summary

Scheduled views and partitions are similar features that both speed up query searches. However, they have different purposes. Partitions compartmentalize and index message data from the present onwards. In contrast, scheduled views index data from the past as well, allowing for mid- to long-term query searches. They are
suitable for cases where you want to analyze data to find patterns and trends.

Reference source

- Scheduled Views
- Scheduled Views Best Practices and Examples
- Add a Scheduled View