# How to create a partition

dev.classmethod.jp/articles/202212-sumologic-partitions-creation-and-notes

佐久間昇吾

December 20, 2022

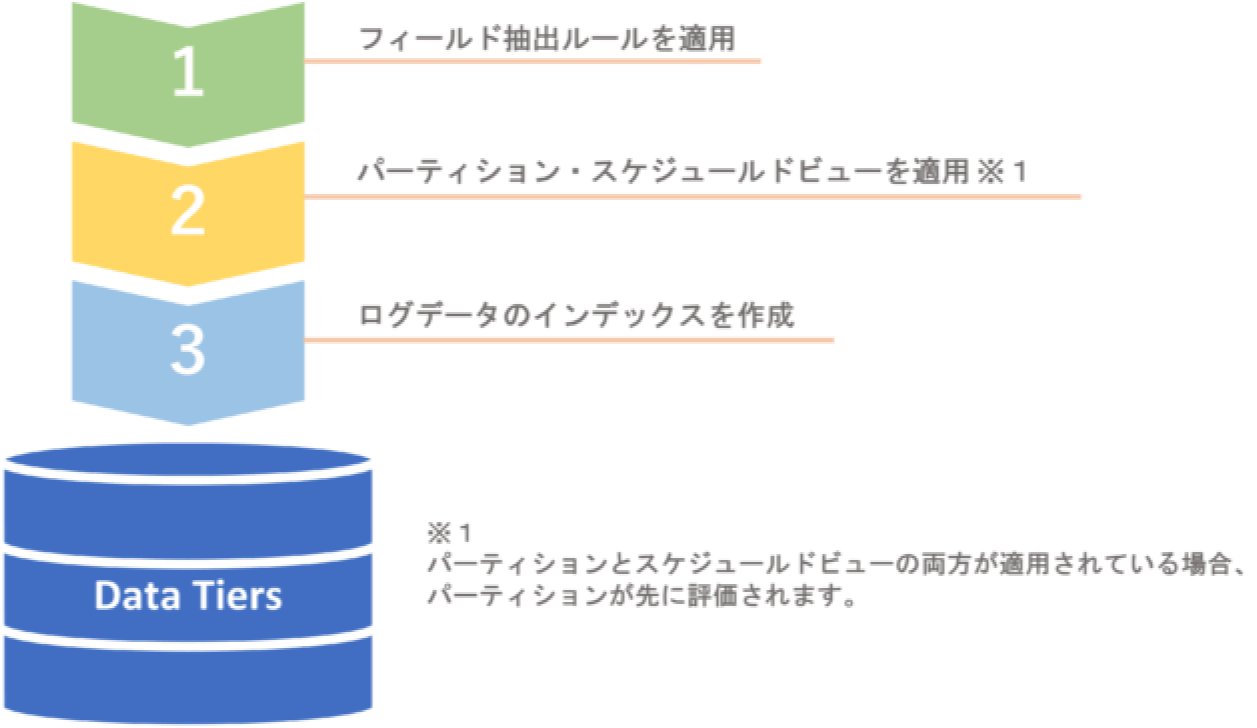
If the content of the article is outdated, please also check the official website.

For more information about Sumo Logic, please see below.

- SumoLogic 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:


1
フィールド抽出ルールを適用
2
パーティション・スケジュールドビューを適用※１
3
ログデータのインデックスを作成
Data Tiers

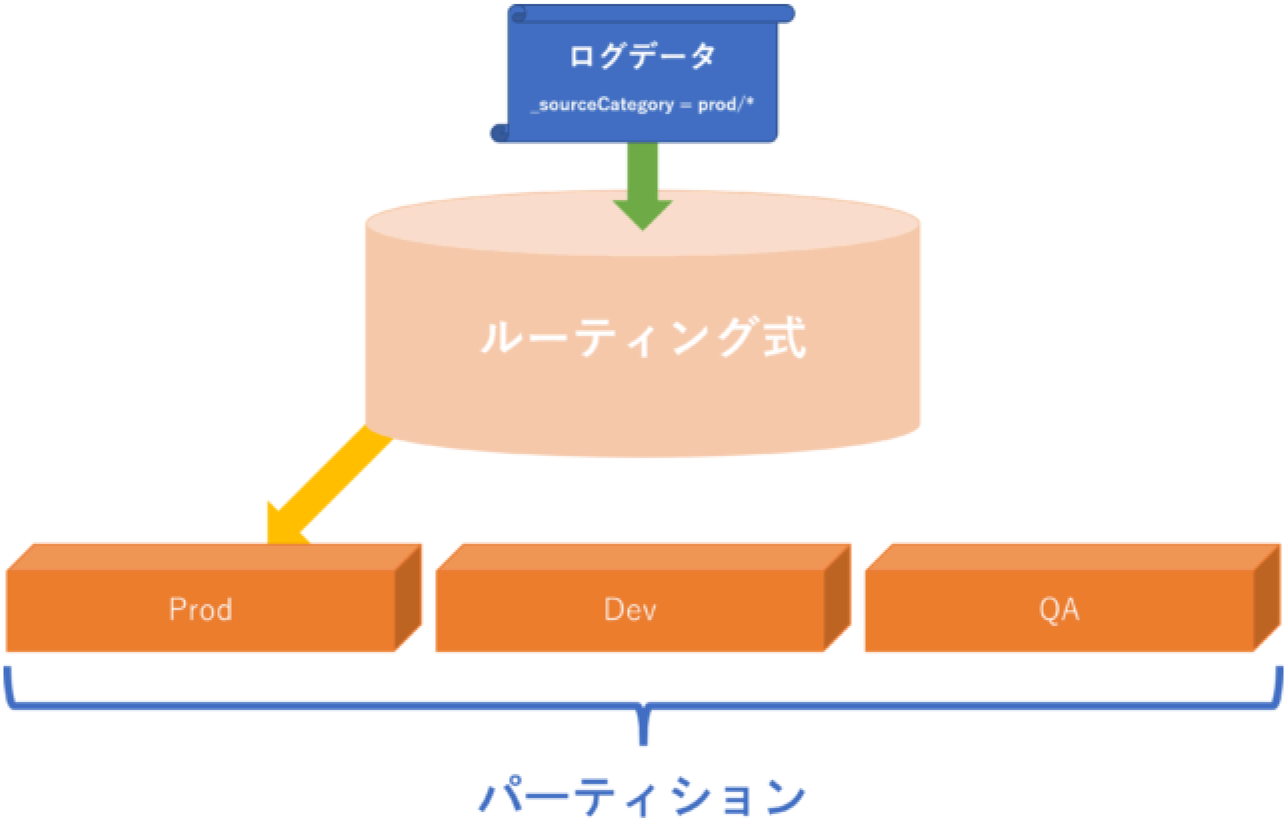
※１
パーティションとスケジュールドビューの両方が適用されている場合、
パーティションが先に評価されます。

***This time we will introduce the Partition function!**

## About Partitions

In Sumo Logic, a partition means "separating a set of message data into smaller subsets."

For example, you can place message data delivered by environment, such as _sourceCategory=prod/*, =dev/*, =qa/*, into partitions such as Prod, Dev, and QA.



Partitioning allows you to query specific pieces of data, which can be beneficial for gaining insights quickly and clearly.

**Partition Application Timing**
: Partitions are applied to message data from the time of creation onward.
They do not backfill aggregated data.

## Points to note when creating partitions

### Roles required for partition creation

- **Manage Partitions**
  You can view, create, edit, and delete partitions. Accounts with this permission also have the ability to manage partitions and manage data transfer to S3.

### Partition Limits

- **Number of partitions that can be created**
  You can create up to 50 per account.

- **Data retention period**
  Select from 1 to 5000 days.

## Notes on editing partitions

There are some items that cannot be changed after creating a partition.
Please take the following editing precautions into consideration when creating a partition.

- **The partition name cannot be changed.**
- **Partition names cannot be reused.**
  Even if you disable an existing partition, you cannot create one with the same name.

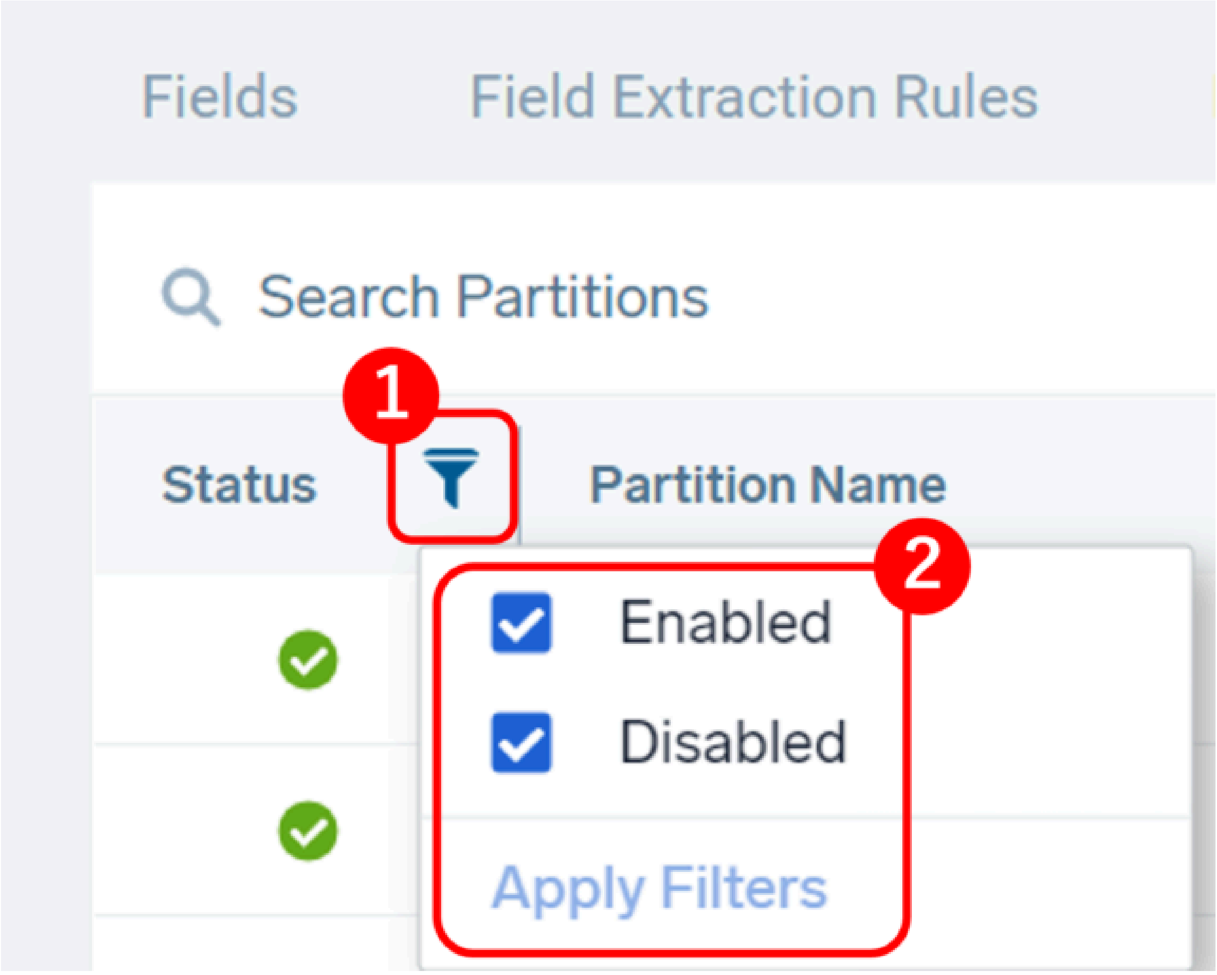
- **The data layer where the partition exists cannot be changed.**
  If you want to change the data layer that imports log data, you must stop the partition that is using the existing layer and create a new partition that uses the new data layer.

- **Partitions cannot be deleted, instead they can be discontinued.**
  Deprecated partitions will still contain data within their retention period
  and will not count against your account's limit of 50.

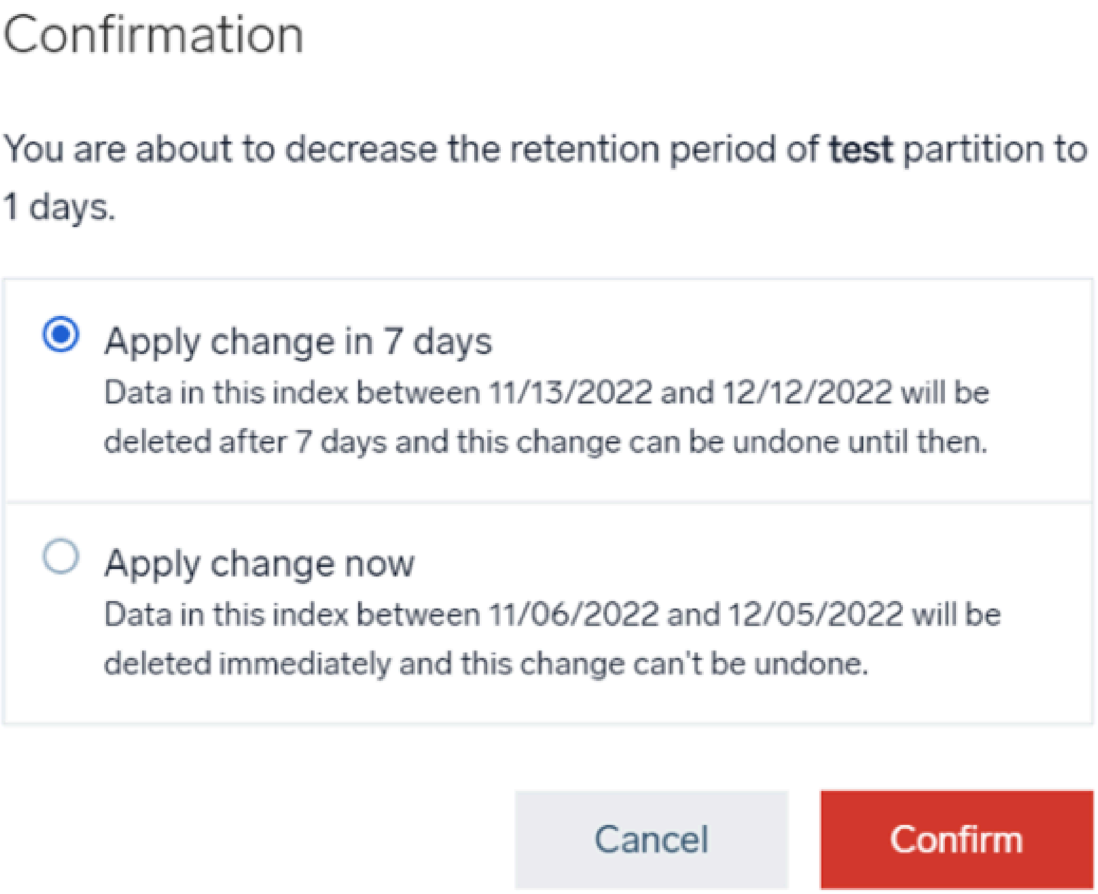
  **- Note -**
  A partition that has been deleted cannot be re-enabled.

  **- Tip -**
  You can view decommissioned partitions by clicking Apply Filters in the Status

section.



- **You can set the data retention period for existing partitions to be shorter than the default period.**
  **- Tip -**
  If you shorten the retention period and save it, the following alert screen will appear.can choose to



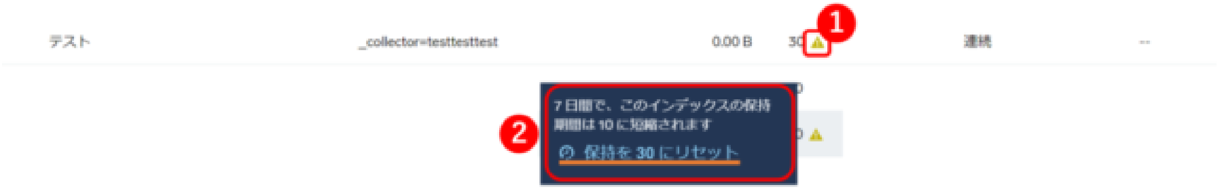
Confirmation

You are about to decrease the retention period of **test** partition to 1 days.

● Apply change in 7 days
Data in this index between 11/13/2022 and 12/12/2022 will be deleted after 7 days and this change can be undone until then.

○ Apply change now
Data in this index between 11/06/2022 and 12/05/2022 will be deleted immediately and this change can't be undone.

**either Apply change in 7 days (shorten the retention period after 7 days and delete data outside the retention period)** or **Apply change now (delete immediately) .**
You can also restore the retention period to its original value after shortening it.



テスト _collector=testtesttest 0.00 B 30 連続 --

7 日間で、このインデックスの保持期間は 10 に短縮されます

保持を 30 にリセット

## Partitioning Best Practices

- **Do not create routing expressions that are subject to change**
  You can edit a routing expression after you create it. However, changing the routing expression also changes the data that goes into that partition. Use partitions to organize your message data long-term.

- **Routing expressions can be defined as specific or flexible depending on the application.**

Routing expressions define which data should be delivered to which partition. Message data that matches the contents of a routing expression is added to the partition.

**Partitions with specific routing expressions allow you to extract specific data** .
For example,
_sourceCategory=/dev/apache/access/*
_sourceCategory=/stg/apache/error/*

**Partitions with flexible routing expressions have the advantage of being able to adjust metadata,**
e.g. ,
_sourceCategory=*/apache/*
_sourceCategory=*/nginx/*

- **The most frequently used data is grouped**
  It is categorized as web data, security data, error data, etc.

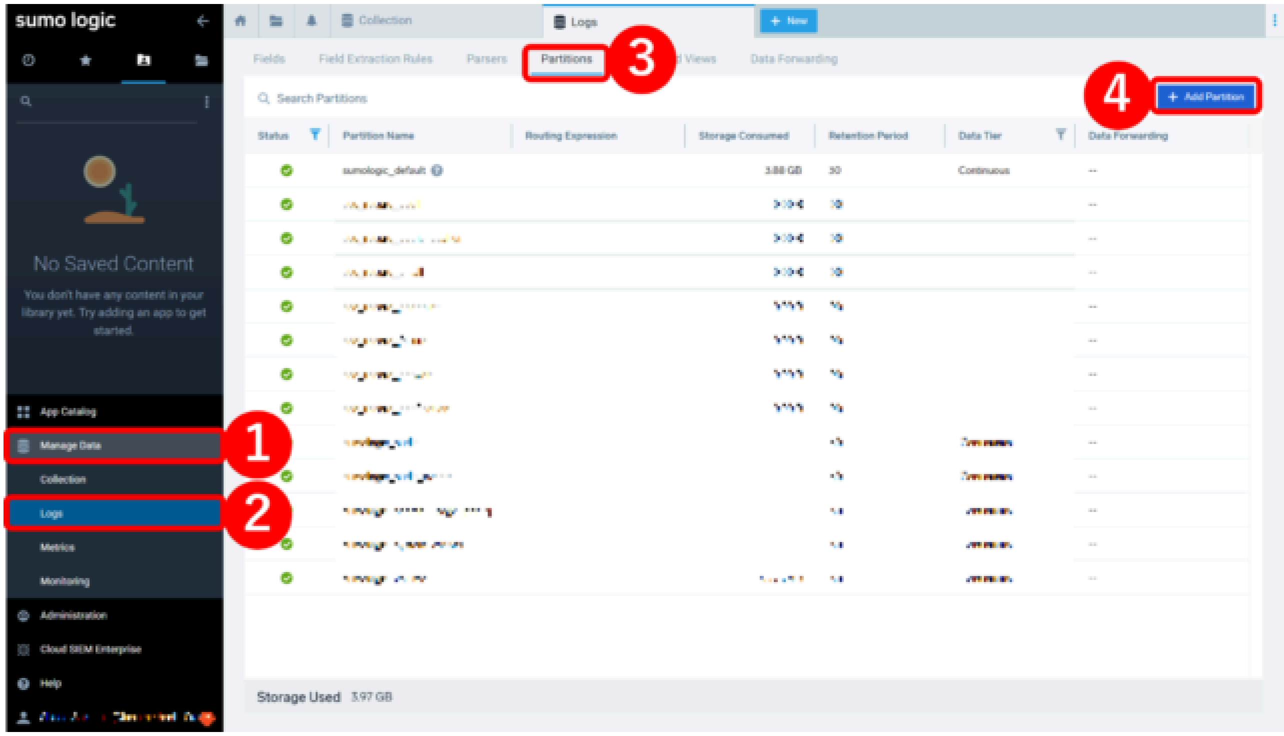
- **Grouping data for use by organization (team, department)**
  Group by roles, teams, or other departments within your organization.

- **Adjust the amount of data contained in a partition**
  Partitions should only distribute 2-20% of your data,
  as there is no point in having a large amount of data in a partition. Partitions should be created to compartmentalize and index data for frequently used data or complex nested data to improve query response times.

- **Don't create duplicate queries**
  Sumo Logic will not return duplicate results, but the process of de-duplication takes extra time.

Follow the steps below to go to the partition creation page.

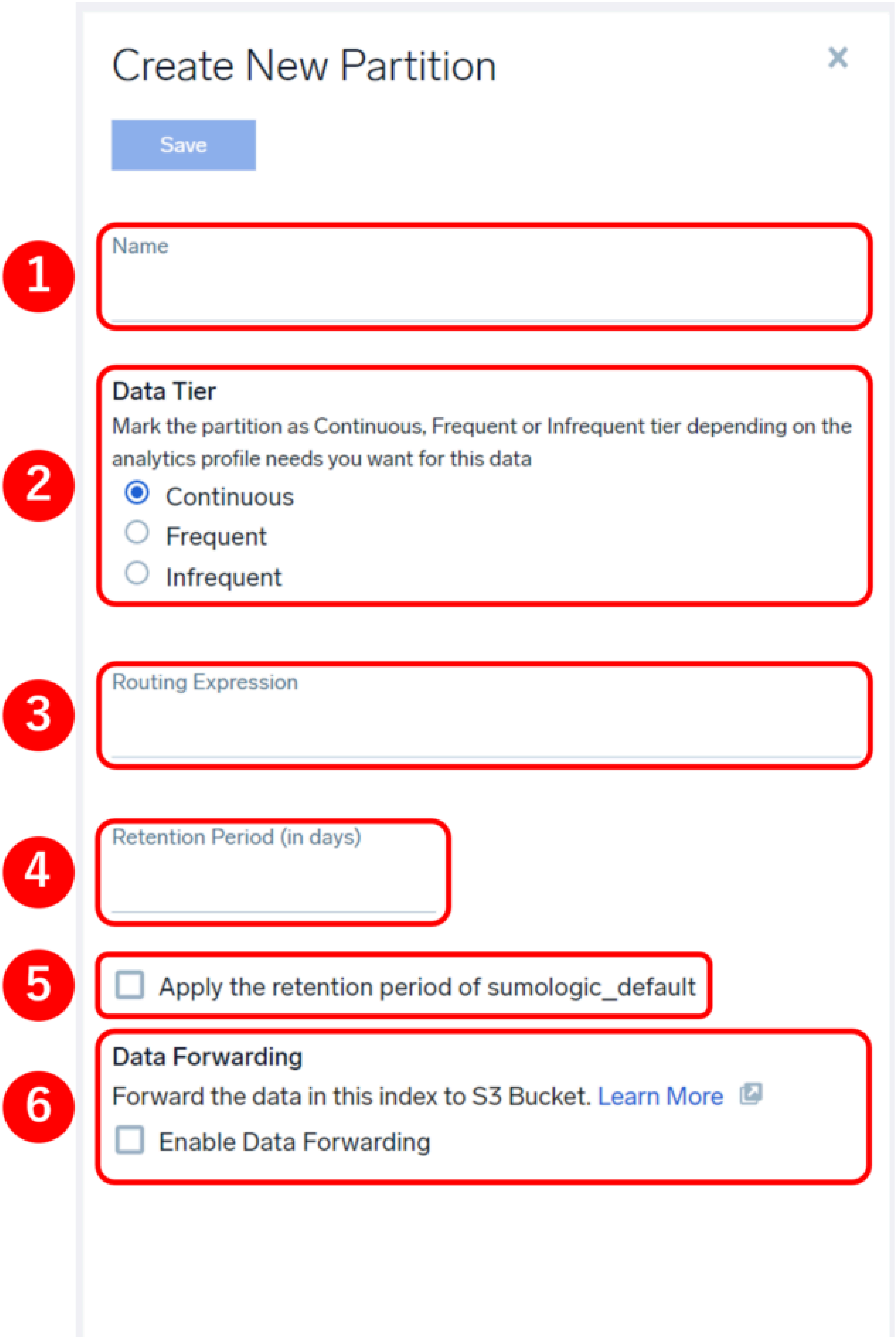
## ① Manage Data > ② Logs > ③ Partitions > ④ + Add Partition



| Status | Partition Name | Routing Expression | Storage Consumed | Retention Period | Data Tier | Data Forwarding |
|---|---|---|---|---|---|---|
| ✓ | sumologic_default | | 3.88 GB | 30 | Continuous | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | | -- |
| | [illegible] | | | [illegible] | [illegible] | -- |
| ✓ | [illegible] | | | [illegible] | [illegible] | -- |
| | [illegible] | | | [illegible] | [illegible] | -- |
| ✓ | [illegible] | | | [illegible] | [illegible] | -- |
| ✓ | [illegible] | | [illegible] | [illegible] | [illegible] | -- |

Storage Used 3.97 GB

The following partition creation menu will then appear on the right.



Create New Partition

Name

**Data Tier**

Mark the partition as Continuous, Frequent or Infrequent tier depending on the analytics profile needs you want for this data

● Continuous
○ Frequent
○ Infrequent

Routing Expression

Retention Period (in days)

□ Apply the retention period of sumologic_default

**Data Forwarding**

Forward the data in this index to S3 Bucket. Learn More

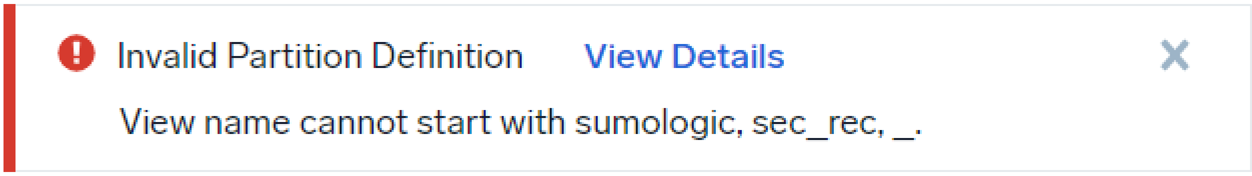
□ Enable Data Forwarding

## ① Name

Enter the partition name using alphanumeric characters.

Unusable characters
and special characters

**- Note -**
Partition names cannot start with "sumologic_", "sec_rec", or "_".
This is because there are partitions provided by Sumo Logic (sumologic_*) and partitions dedicated to the CloudSIEM function (sec_rec*).



Invalid Partition Definition

View name cannot start with sumologic, sec_rec, _.

## ② Data Tier

Only Enterprise Suite accounts can select Frequent or Infrequent.

**- Continuous:**
A data layer that stores general log streams.
**- Frequent**
: A data layer for frequent access.
**- Infrequent:**
A data layer for infrequent access.

For information about data tiers, see Data Tiers .

## ③ Routing Expression

Use keyword search expressions to specify built-in or custom metadata fields
. The specified metadata values will be indexed as partitions.

## ④ Retention Period (in days)

Enter the data retention period between 1 and 5000 days.

## ⑤ Apply the retention period of sumologic_default

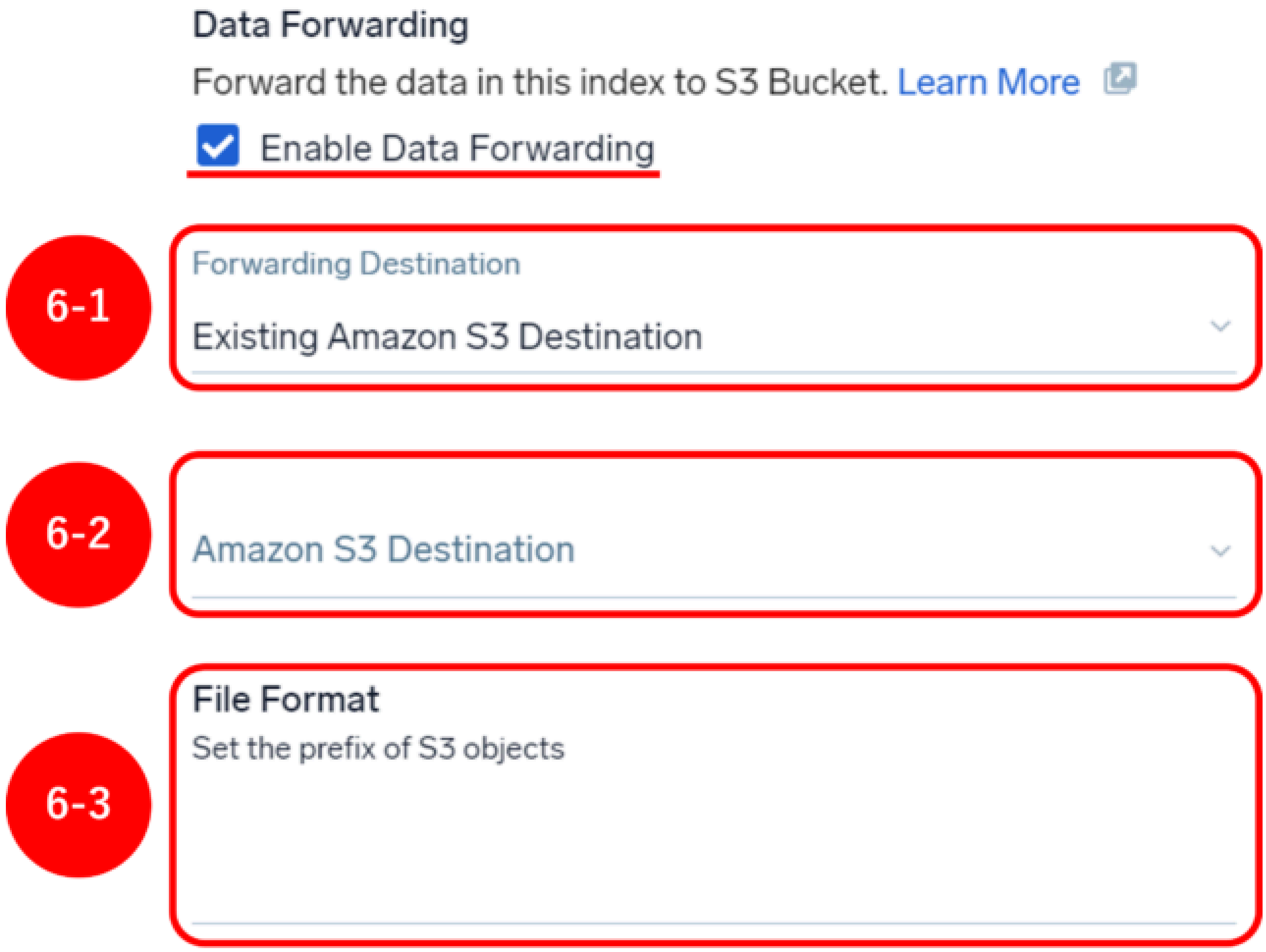
Enabling the Apply **the retention period of sumologic_default**
checkbox will set the data retention period to the same as the sumologic_default partition , which has a retention period of 30 days and a data tier of Continuous.

**Tip:**
A partition called sumologic_default is created by default to hold data that does not belong to any other partition.

## ⑥ Data Forwarding

To transfer data in the partition to the cloud environment, enable this checkbox. The cloud transfer feature transfers log data to an AWS S3 bucket owned by the user.

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



Data Forwarding

Forward the data in this index to S3 Bucket. Learn More

☑ Enable Data Forwarding

Forwarding Destination

Existing Amazon S3 Destination

Amazon S3 Destination

File Format

Set the prefix of S3 objects

**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

When there is a large amount of data, the presence or absence of partitions can make a big difference in the speed of query searches. You can make query searches more comfortable by adjusting the amount of partitions depending on the type of data, such as data that only needs a short expiration date or important and frequently used message data.

Also, if you want to go back in time, you have the option to collect historical data using the Schedule View.

## Reference source

- Sumo Logic - Partitions and Data Tiers
- Sumo Logic - Role Capabilities
- Sumo Logic - Create and Edit a Partition
- Sumo Logic - Optimize Your Search with Partitions