

# I tried setting up a collector in Sumo Logic to collect logs from Github

---

 [dev.classmethod.jp/articles/i-tried-setting-up-a-collector-in-sumo-logic-to-collect-logs-from-github](https://dev.classmethod.jp/articles/i-tried-setting-up-a-collector-in-sumo-logic-to-collect-logs-from-github)

HemanthKumar R

August 22, 2023



## 目次

## Introduction

---

Hemanth from the Department of Alliance. I'll demonstrate how to set up a Sumo Logic collector to automatically collect logs from GitHub in this blog article.

## Sumo Logic

---

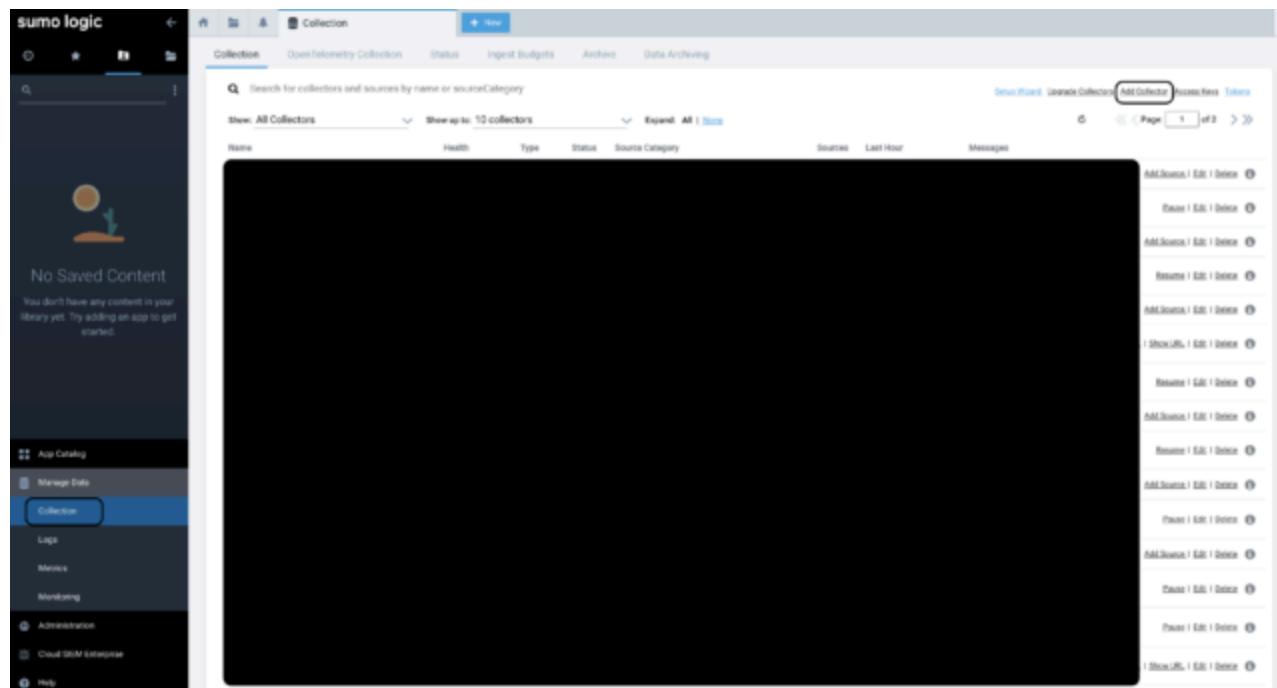
Before going further let's understand what sumo logic is. A cloud-based log management and analytics software called Sumo Logic enables businesses to exploit their machine data for useful insights. Sumo Logic's flexible capabilities make log data analysis simple and offer real-time visibility into operational and security insights.

# Github

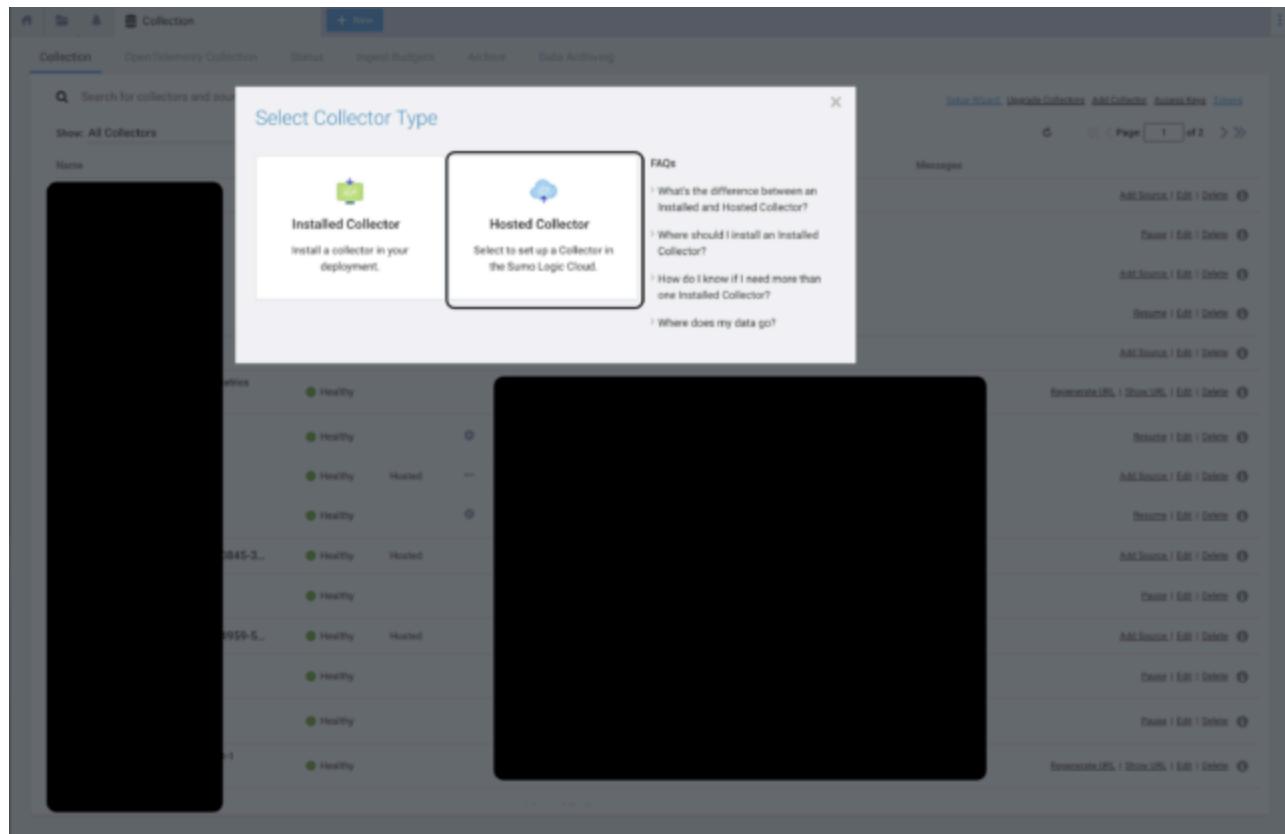
Developers can work together on software projects, manage their code, and participate in open source communities using the GitHub platform. Over 100 million developers utilize GitHub worldwide, and it is the home to many well-known open source projects. This platform promotes creativity and collaboration, allowing people from all over the world to create anything they can imagine.

## Demo

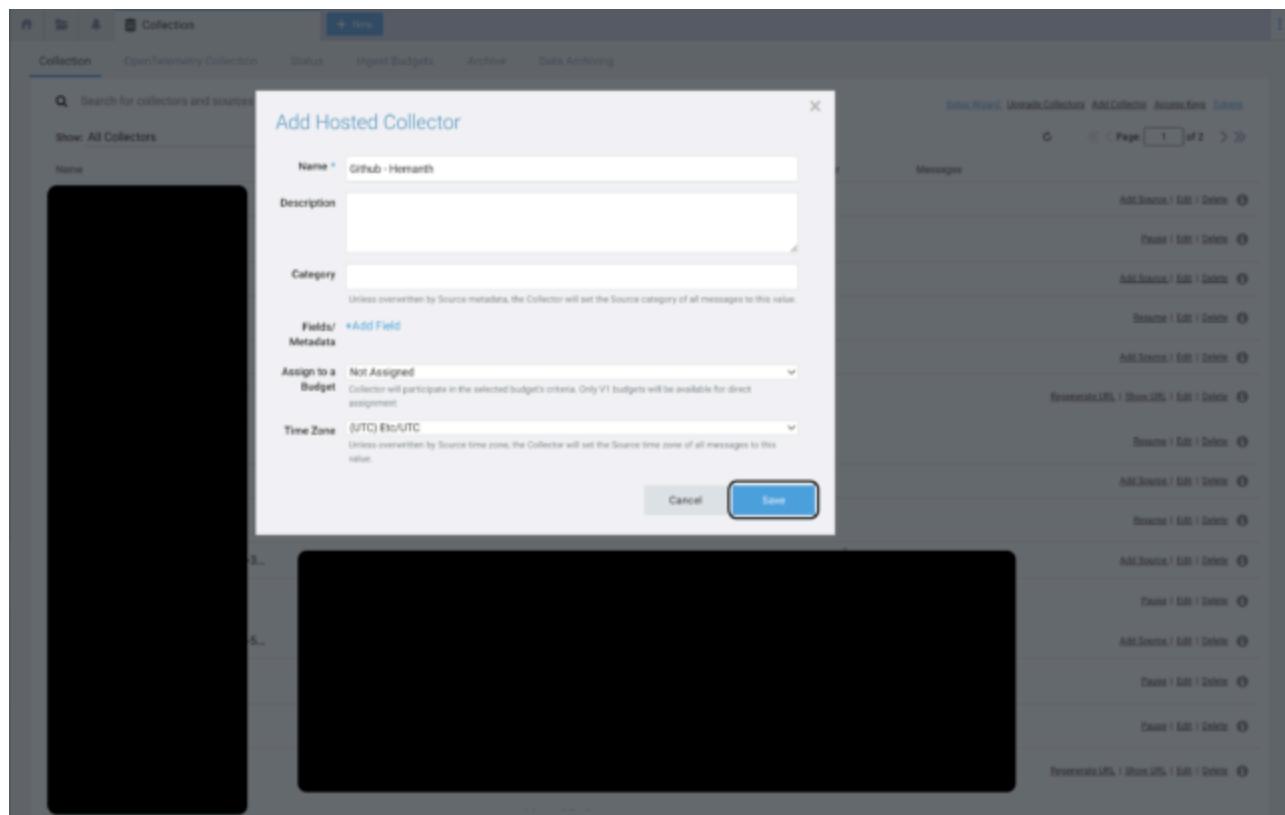
Log into your Sumo logic account, navigate to Manage data, then click on collection and click "Add Collector" button located in the top right



click on hosted collector



Provide a name and description for the hosted collector as required, select your preferred time zone and click save

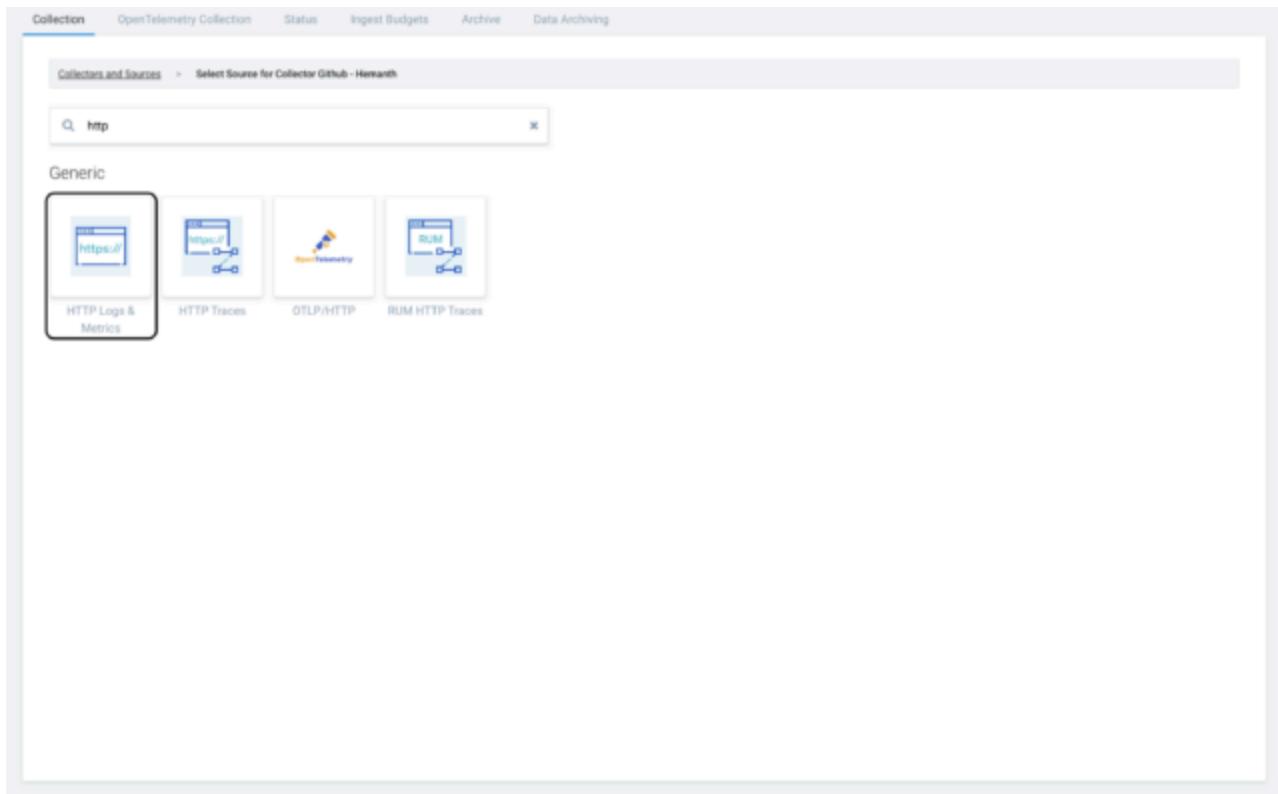


The screenshot shows the Grafana Collector interface. At the top, there are tabs for Collection, OpenTelemetry Collection, Status, Ingest Budgets, Archive, and Data Archiving. Below the tabs, a search bar contains the query 'github'. A dropdown menu shows 'Show: All Collectors' and 'Show up to: 10 collectors'. The main table has columns for Name, Health, Type, Status, Source Category, Sources, Last Hour, and Messages. One row is visible: 'Github - Hemanth' is healthy, hosted, and has no sources or messages. At the bottom right of the table, there are buttons for 'Add Source', 'Edit', and 'Delete'.

Configuring an HTTP Source on to the created hosted collector by clicking on Add Source at right hand side of the created collector

This screenshot is identical to the one above, showing the 'Github - Hemanth' collector. However, a red box highlights the 'Add Source' button located at the bottom right of the collector's row.

Search for HTTP Logs and Metrics and select it



Assign a name and a source category, input key and value. Keep other settings as default before saving

Collection OpenTelemetry Collection Status Ingest Budgets Archive Data Archiving

Collectors and Sources > Select Source for Collector Github - Hernanck > HTTP Logs & Metrics

**HTTP Logs & Metrics**

Name:

Description (optional):

Source Host (optional):

Source Category (optional):

Forward to SIEM

Fields/Metadata:

Key	Value
convertHeadersToFile	True

+ Add

Automatically activate all fields on save.  
You are going to create 1 more field (used 82 / 200).

Advanced Options for Logs (Optional)

Timestamp Parsing

Extract timestamp information from log file entries

Default Time Zone (optional):   
If no time zone is selected, Collector's time zone will be used

FAQs

- How do I upload to an HTTP Source?
- Can I use the URL to upload from more than one data source?
- Is there a way to generate a new URL?
- What file types can be collected from an HTTP Source?
- How do I send metrics to an HTTP Source?
- How do I search for metrics sent to an HTTP Source?
- How do I append custom metadata and dimensions to metrics sent to an HTTP Source?
- How should I configure my timestamp options?
- How do I use "Fields" feature to add metadata to logs and metrics ?

Collection OpenTelemetry Collection Status Ingest Budgets Archive Data Archiving

Collectors and Sources > Select Source for Collector GitHub - Hernan! > HTTP Logs & Metrics

Advanced Options for Logs (Optional)

Timestamp Parsing

Extract timestamp information from log file entries

Default Time Zone (optional)

If no time zone is selected, Collector's time zone will be used

Use time zone from log file. If not detected, use default time zone

Ignore time zone from log file and instead use default time zone

Timestamp Format

Automatically detect  Specify a format

Message Processing

Multiline Processing

Detect messages spanning multiple lines

Infer Message Boundaries

Detect Automatically  Add Boundary Regex

One Message Per Request

Each request will be treated as a single message (ignore line breaks)

Processing Rules (Optional)

Learn More [\[?\]](#)

Cancel Save

Copy the displayed HTTP source Address for later use. After that click ok.

Collection OpenTelemetry Collection Status Ingest Budgets Archive Data Archiving

github

Show: All Collectors Show up to:

Name	Health
Github - Hernan!	Healthy
github-personal	Healthy
HTTP	Healthy

HTTP Source Address

Use the following address to send data to the Collector. [Learn more...](#)

Keep this address private since anyone can use it to send data.

<https://collectors.jx.sumologic.com/receiver/v1/http/ZevW...>

Copy OK

Last Hour Messages None

Add Source | Edit | Delete [\[?\]](#)

Collector URL | Show URL | Edit | Delete [\[?\]](#)

The screenshot shows the CloudWatch Metrics Collection interface. At the top, there are tabs for 'Collection', 'OpenTelemetry Collection', 'Status', 'Ingest Budgets', 'Archive', and 'Data Archiving'. A search bar at the top left contains the query 'github'. Below the search bar, there are dropdown menus for 'Show: All Collectors' and 'Show up to: 10 collectors'. A 'Select Wizard' button is also present. On the right side, there are buttons for 'Upload Collectors', 'Add Collector', 'Access Keys', and 'Metrics'. The main area displays a table of collectors:

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
Github - Hemanth	Healthy	Hosted			1	None	Add Source   Edit   Delete
github-personal	Healthy		github				Regenerate URL   Show URL   Edit   Delete

Configuring Github Webhook, sign in to Github account, Navigate to your organization, in that repository and click on settings

The screenshot shows the GitHub repository settings page for 'codemn / automatingtesting-githubactions'. The 'General' tab is selected. The left sidebar lists various settings categories: General, Access, Collaborators, Code and automation, Branches, Tags, Rules, Actions, Webhooks, Codebases, Pages, Security, Code security and analysis, Deploy keys, Secrets and variables, Integrations, GitHub Apps, and Email notifications. The 'General' section contains the following configuration:

- Repository name:** automatingtesting-githubactions (with a 'Rename' button)
- Template repository:** A checkbox for generating new repositories with the same directory structure and files.
- Require contributors to sign off on web-based commits:** A checkbox for enabling commit signing off through GitHub's web interface.
- Default branch:** The 'main' branch is selected.
- Features:** A section containing three checkboxes:
  - Wiki:** Host documentation for your repository.
  - Upgrade or make this repository public to enable Wikis:** A link to upgrade the repository.
  - Issues:** Integrate lightweight task tracking into your repository.

Click on Webhooks in the left-hand menu and click on add webhook

The screenshot shows the 'General' tab in the GitHub repository settings. On the left, there's a sidebar with various repository management options like Access, Collaborators, Code and automation, Branches, Tags, Rules, Actions, Webhooks (which is highlighted with a red box), Codespaces, Pages, Security, Code security and analysis, Deploy keys, Secrets and variables, Integrations, GitHub Apps, and Email notifications. The main area is titled 'General' and contains sections for 'Repository name' (automatingtesting-githubactions), 'Template repository' (disabled), 'Require contributors to sign off on web-based commits' (disabled), and 'Default branch'. Below these are sections for 'Features' including 'Wiki' (disabled) and 'Issues' (disabled). A button at the bottom right of the features section says 'Get organized with issue templates'.

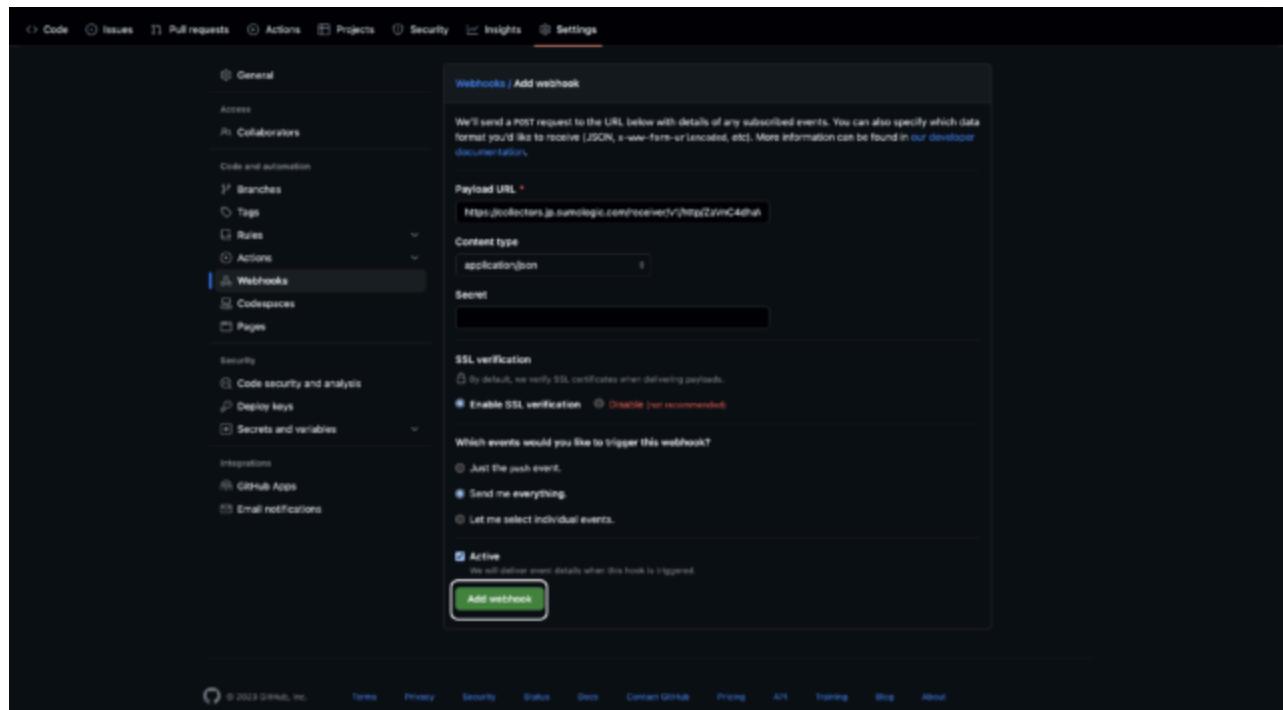
Paste the copied HTTP source address in the payload URL, set the content type as application/json

The screenshot shows the 'Webhooks / Add webhook' configuration page. It's part of the same GitHub interface as the previous screenshot. The sidebar on the left is identical. The main form has fields for 'Payload URL' (https://influxdb.jenkins.xsumologic.com/receivedev?token=HTTP2xvNc4dha), 'Content type' (application/json), and a 'Secret' field. Under 'SSL verification', the 'Enable SSL verification' option is selected. In the 'Which events would you like to trigger this webhook?' section, 'Just the push event.' is selected. There's also an 'Active' checkbox which is checked. At the bottom is a green 'Add webhook' button.

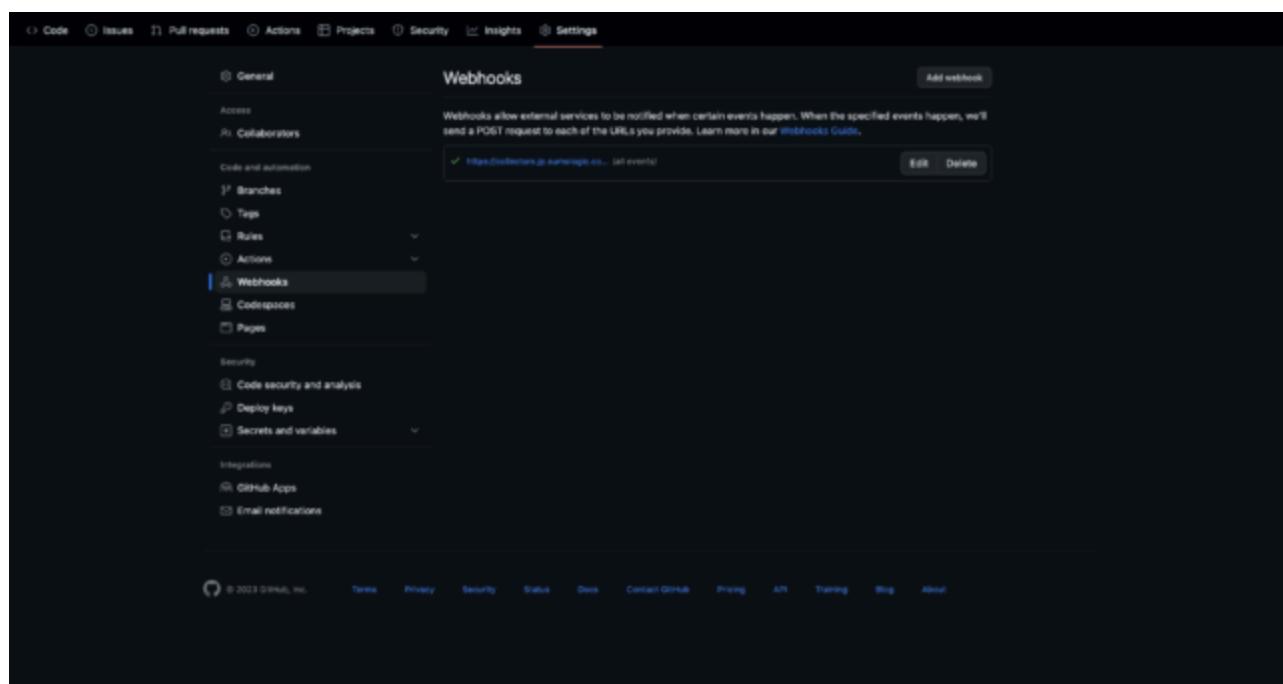
Note - If you have misplaced your URL then you can regenerate as shown below

For events you would like to trigger, you can select any of below only "push events", "send me everything" or "selecting individual events" (there are many options if you have preference select them). I am selecting "send me everything".

Click the active section and click on add webhook



Webhook has been added successfully



To ensure Sumo Logic comprehends incoming events, enable the x-github-event event type. Return to sumo logic and bottom left under collection click on logs

No Saved Content

You don't have any content in your library yet. Try adding an app to get started.

Logs

github

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
Github - Hemanth	Healthy	Hosted			1	None	
github-personal	Healthy	HTTP		github			Add Source   Edit   Delete

click "Add", give the above name it "x-github-event" and click save.

No Saved Content

You don't have any content in your library yet. Try adding an app to get started.

Logs

Logs

Status	Field Name	Data Type	Field Extraction Rules	Role Based Access Control	Partitions	Collectors	Sources
2				0	0	0	0
2				0	0	0	0
2				0	0	0	0
1				0	0	0	0
1				0	0	0	0
2				0	0	0	0
2				0	0	0	0
1				0	0	1	8
2				0	0	0	0
2				0	0	0	0
2				0	0	0	0
2				0	0	0	0
2				0	0	0	0
1				0	0	0	0
2				0	0	0	0
0				0	0	0	0
1				0	0	0	0
1				0	0	0	0
0				0	0	0	0
0				0	0	0	0

No Saved Content

You don't have any content in your library yet. Try adding an app to get started.

Add Catalog

Manage Data

Collection

Logs

Metrics

Monitoring

Administration

Cloud SIEM Enterprise

Help

Fields

Field Extraction Rules

Parsers

Partitions

Scheduled Views

Data Forwarding

Existing - Custom Fields

+ Add

x-github-event

It might take several minutes for a new field to be available.

No Saved Content

You don't have any content in your library yet. Try adding an app to get started.

Add Catalog

Manage Data

Collection

Logs

Metrics

Monitoring

Administration

Cloud SIEM Enterprise

Help

Fields

Field Extraction Rules

Parsers

Partitions

Scheduled Views

Data Forwarding

Existing - Custom Fields

+ Add

x-github-event

String

Fields Capacity: Your account is using 83 (41%) out of the 200 fields available

You can check the collection tab once

The screenshot shows the Sumo Logic interface for managing collectors. At the top, there are tabs for Collection, OpenTelemetry Collection, Status, Ingest Budgets, Archive, and Data Archiving. Below the tabs, a search bar displays 'github'. A dropdown menu shows 'Show: All Collectors' and 'Show up to: 20 collectors'. The main area lists two collectors:

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
▼ Github - Hemant's	Healthy	Hosted			1	1	1
github-personal HTTP	Healthy		github				Add Source   Edit   Delete   Generate URL   Show URL   Edit   Delete

On the right side of the interface, there are buttons for 'Save Wizard', 'Upgrade Collectors', 'Add Collector', 'Access Keys', and 'Tables'. Below these are navigation icons and a page indicator showing '1 of 1'.

## Conclusion

---

After completion of the above steps, your setup is complete. Successfully established a collector in Sumo Logic to gather valuable logs from GitHub.



## クラスメソッドの AWS請求 代行サービスで コスト削減を実現!



[請求代行サービスを見る](#)

まずは資料請求だけでも

**classmethod**

## EVENTS



[【1/29 \(木\)】クラスメソッドの会社説明会を開催します](#)

開催前



[【1/28 \(水\)】クラスメソッドの新卒向け会社説明会を開催します](#)

開催前



[【CMグループ/エンド直案件特集】ITフリーランス向け「CMパートナーズ」説明会 by クラスメソッド](#)

開催前



[【2/5 \(木\) 東京】オペレーターの生産性を50%アップ! 見て、聞いて、納得できるAIコールセンター実演セミナー](#)

開催前



[【2/25 \(水\)】AI駆動開発、実際どうなの?【実践編】～現場でぶつかる課題と乗り越え方～](#)

[開催前](#)



[【1/29 \(木\)】今日から始めるAWSセキュリティ対策 3ステップでわかる実践ガイド](#)

[開催前](#)

[セミナー一覧](#) [会社説明会一覧](#) [勉強会一覧](#)