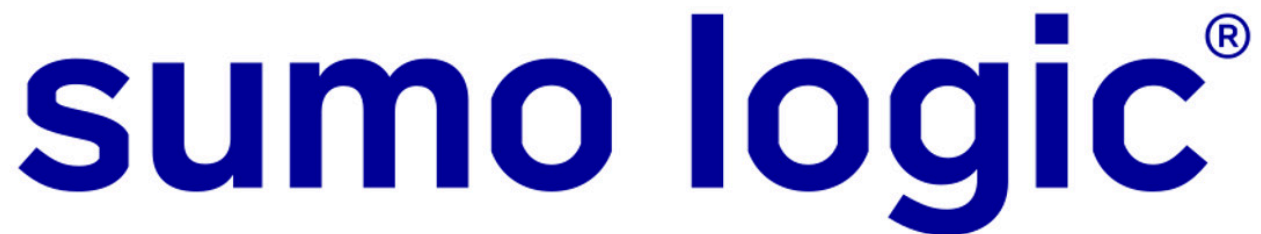


I tried setting up a collector in Sumo Logic to collect logs from Github

 dev.classmethod.jp/articles/i-tried-setting-up-a-collector-in-sumo-logic-to-collect-logs-from-github

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

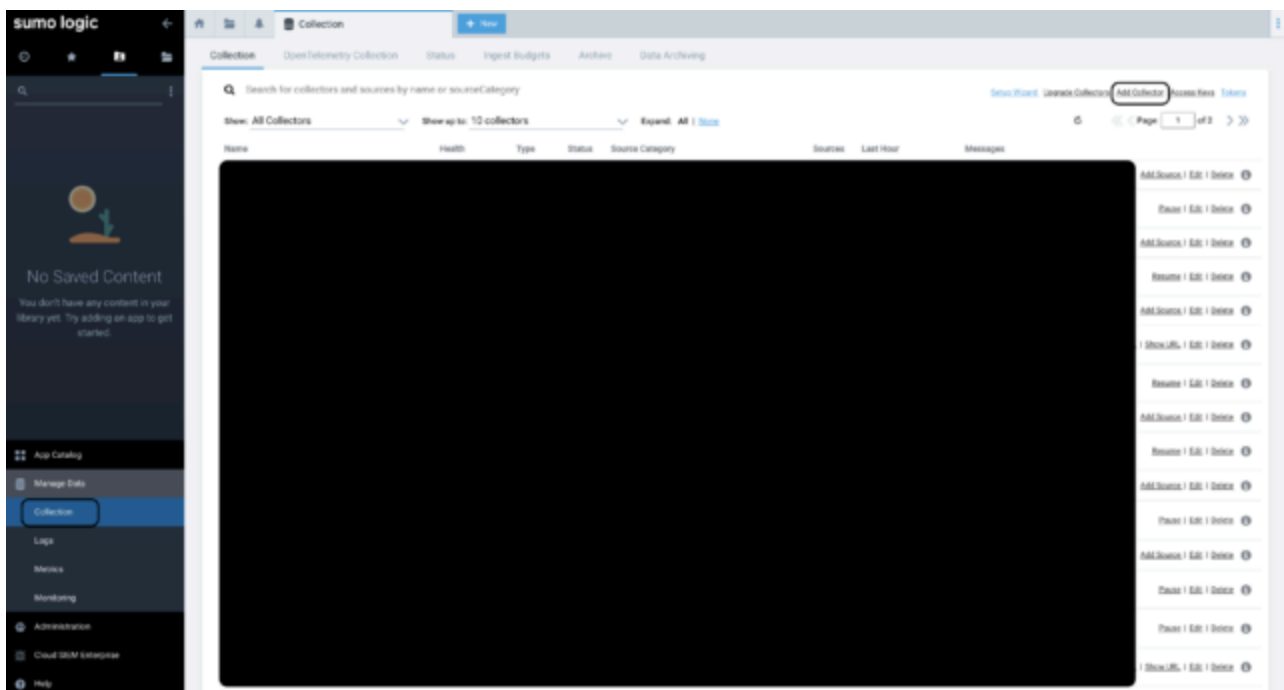
Before going further let's understand what sumo logic is. A cloud-based log management and analytics software called Sumo Logic enables businesses to exploit their machine data for useful insights. Sumo Logic's flexible capabilities make log data analysis simple and offer real-time visibility into operational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

Github

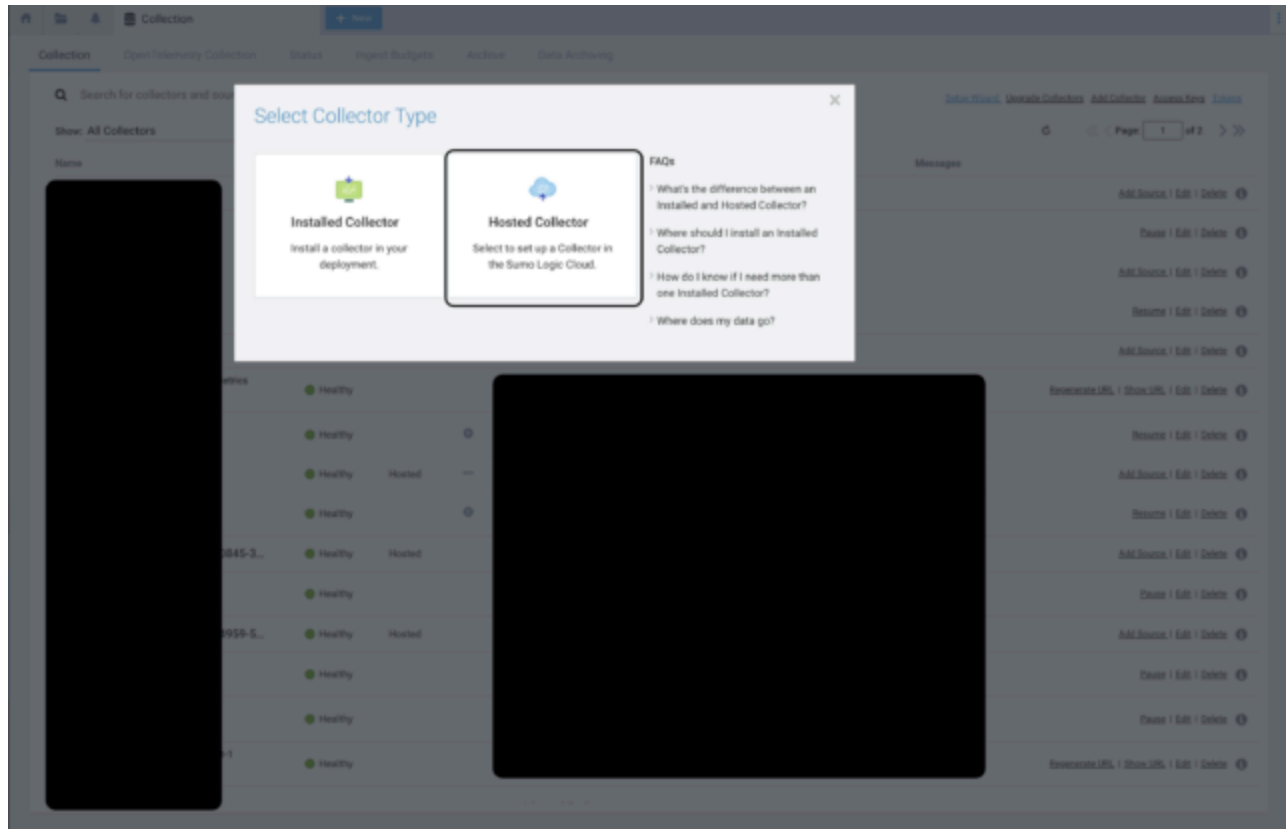
Developers can work together on software projects, manage their code, and participate in open source communities using the GitHub platform. Over 100 million developers utilize GitHub worldwide, and it is the home to many well-known open source projects. This platform promotes creativity and collaboration,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

Demo

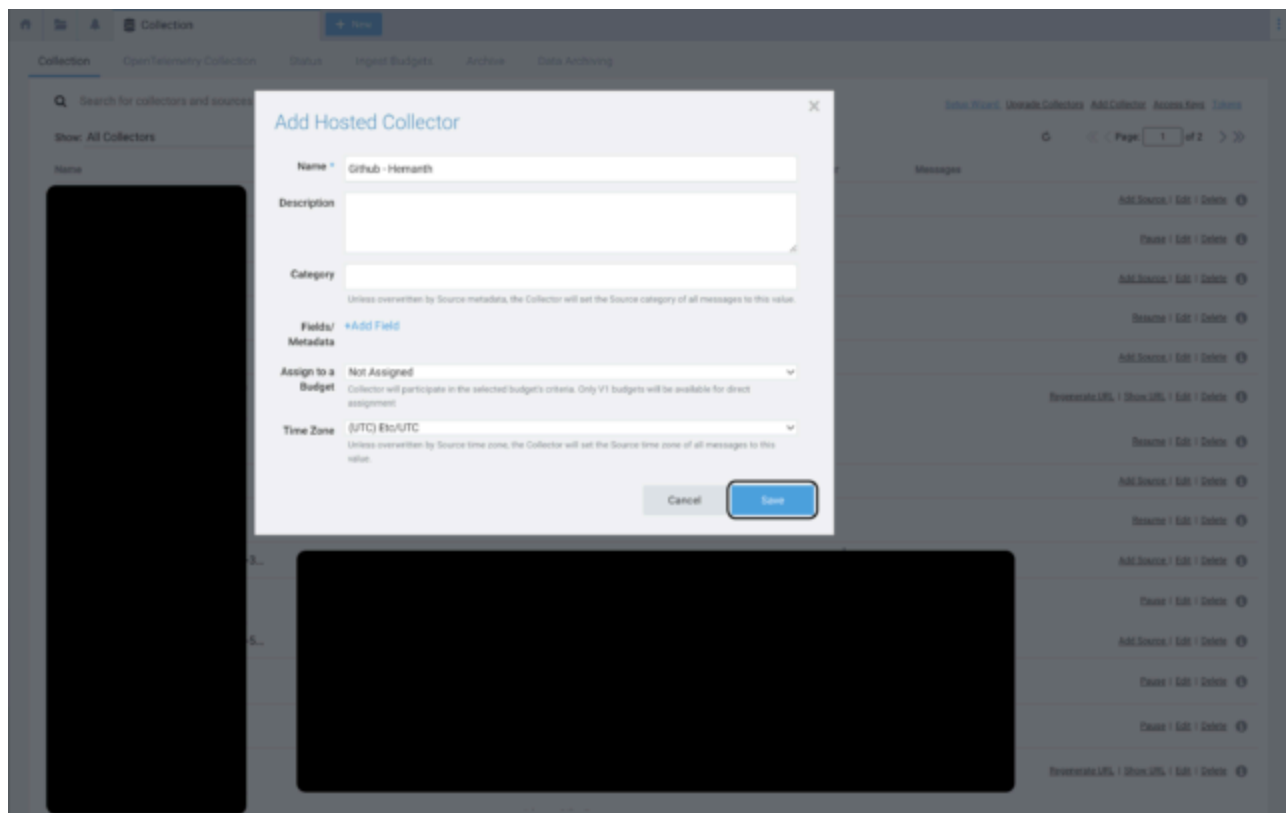
Log into your Sumo logic account, navigate to Manage data, then click on collection and click "Add Collector" button located in the top right

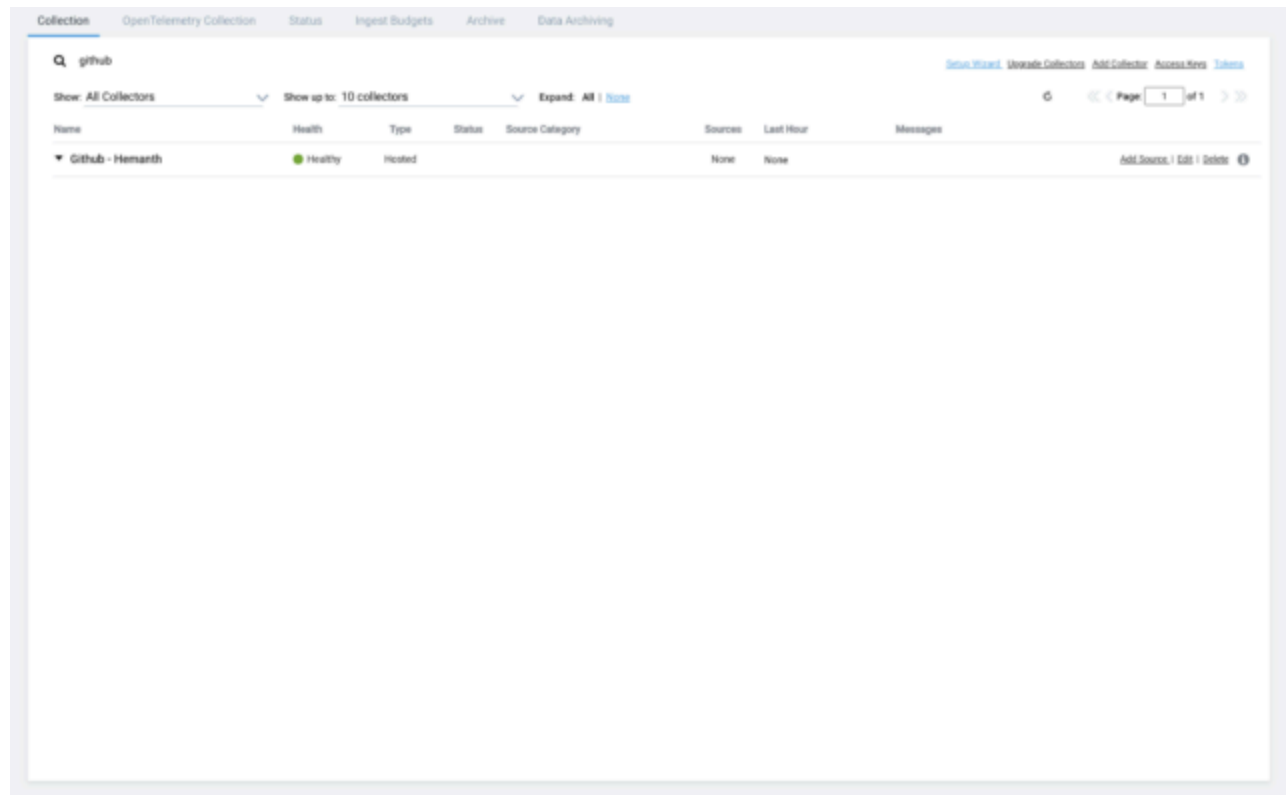


click on hosted collector

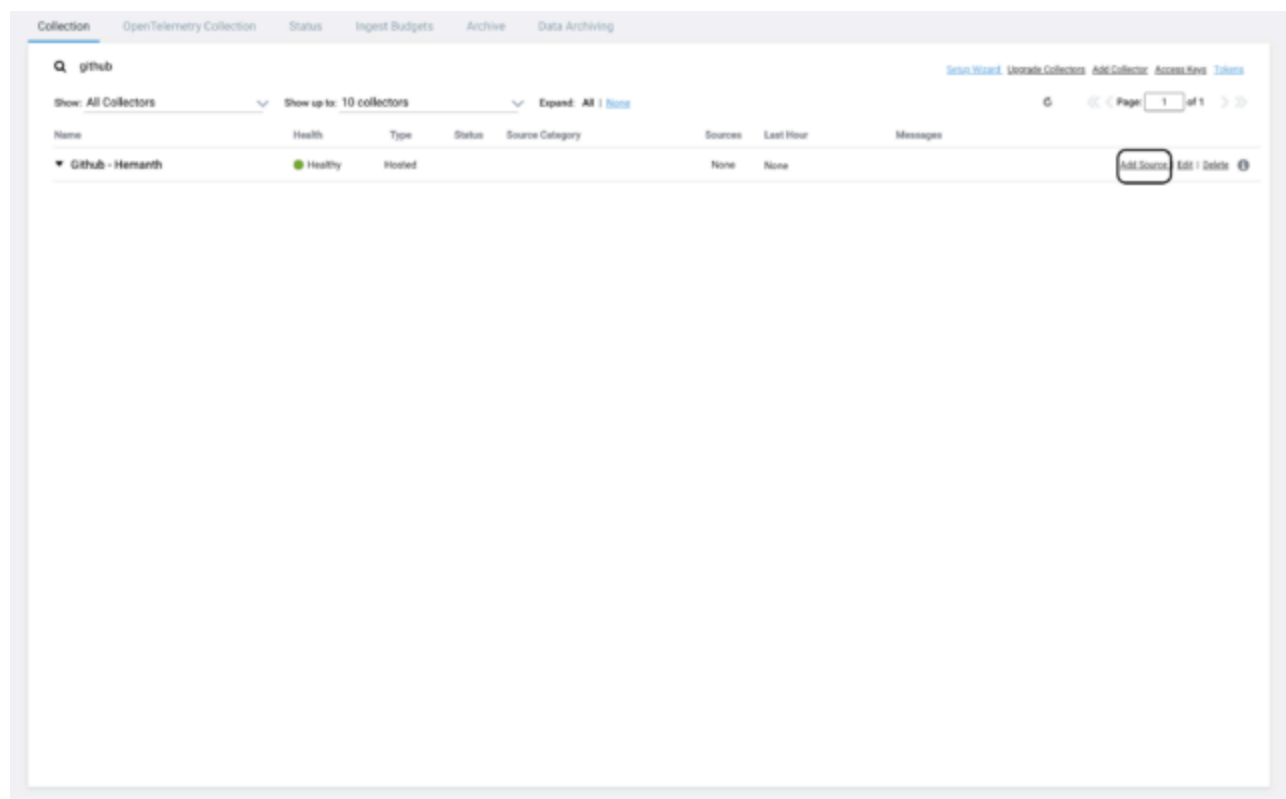


Provide a name and description for the hosted collector as required, select your preferred time zone and click save

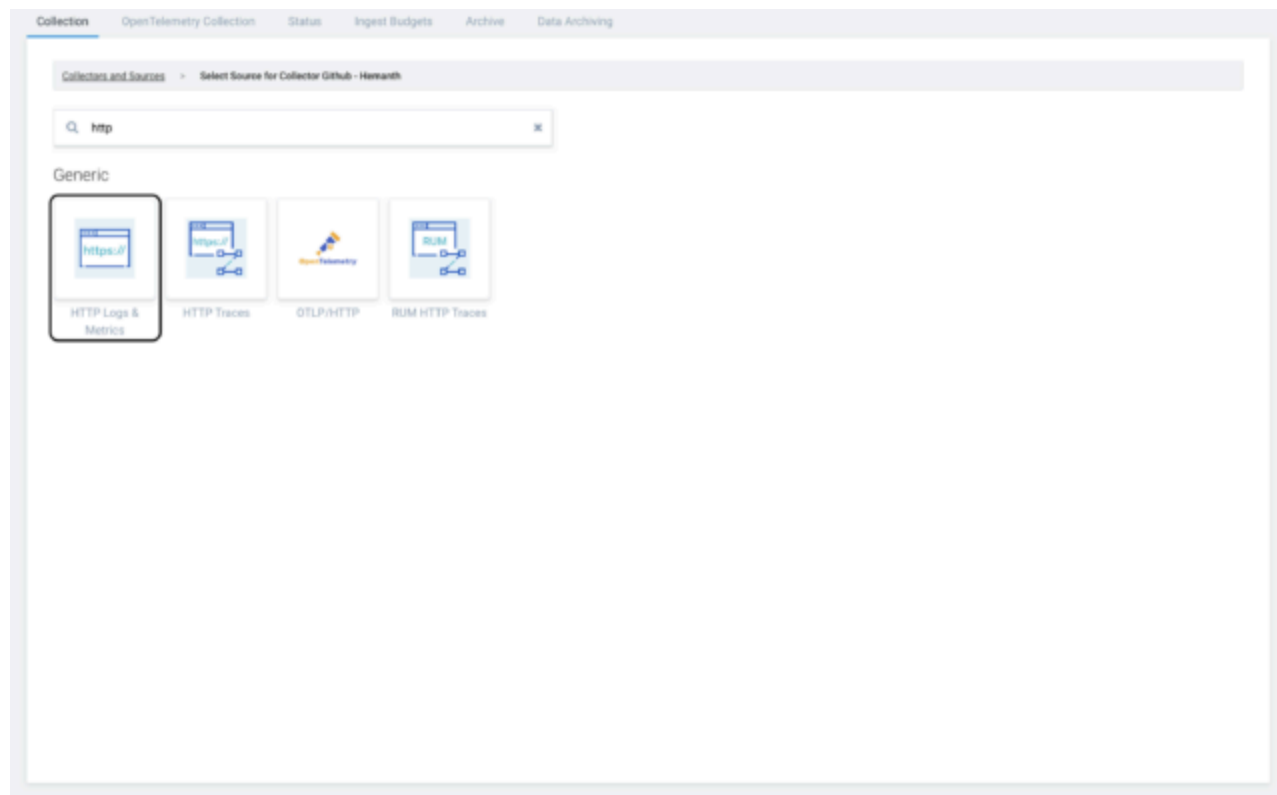




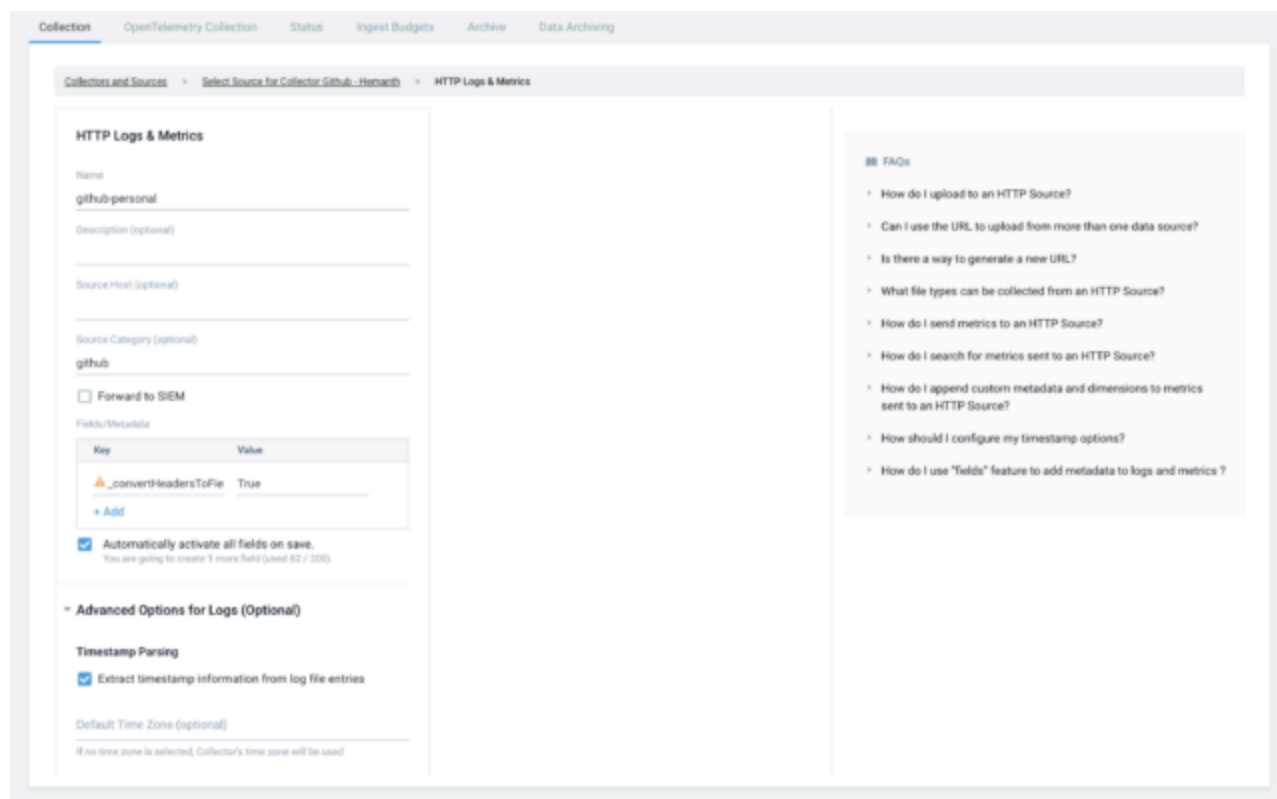
Configuring an HTTP Source on to the created hosted collector by clicking on Add Source at right hand side of the created collector



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:Heremath 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 the format ☐ 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 - Heremath Healthy

github-personal Healthy

HTTP

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.gx.sumologic.com/receiver/v1/http/ZaVnD` Copy

OK

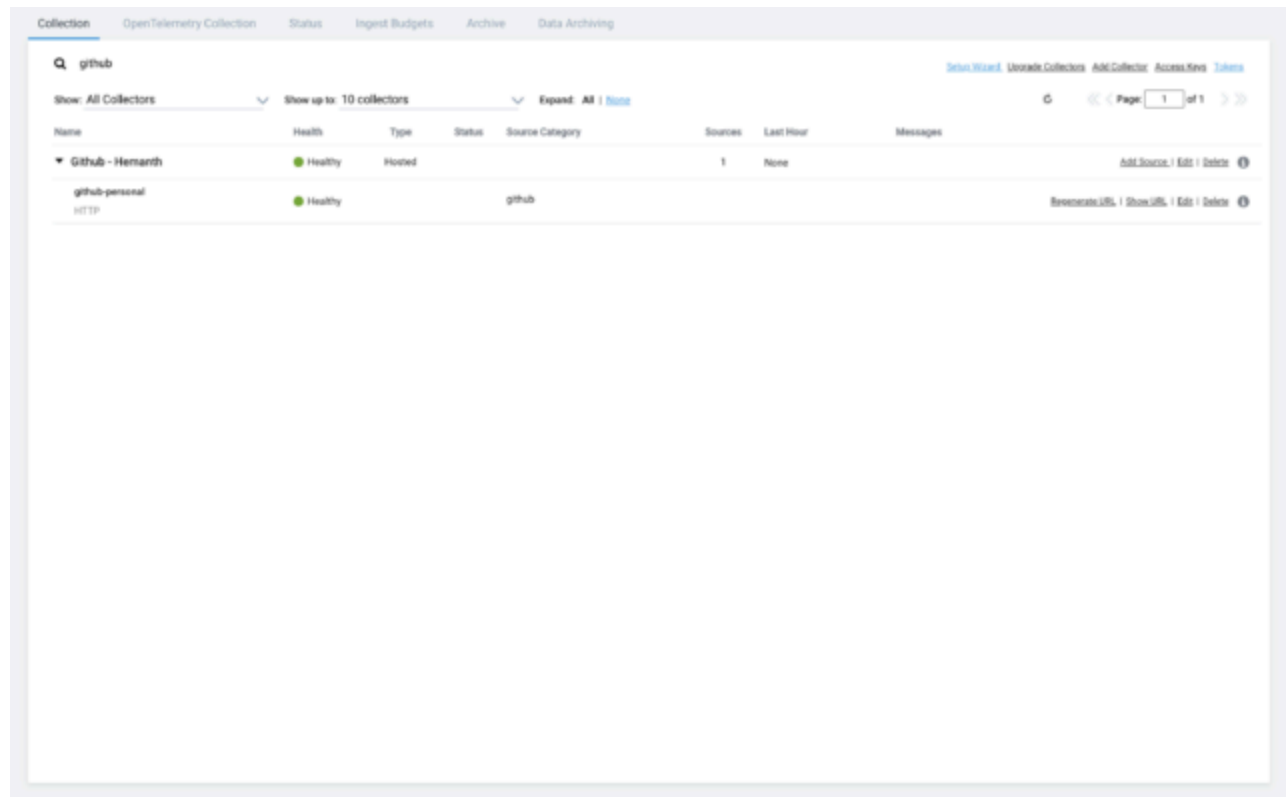
John Housh Upgrade Collectors Add Collector Access Keys Tables

Page 1 of 1

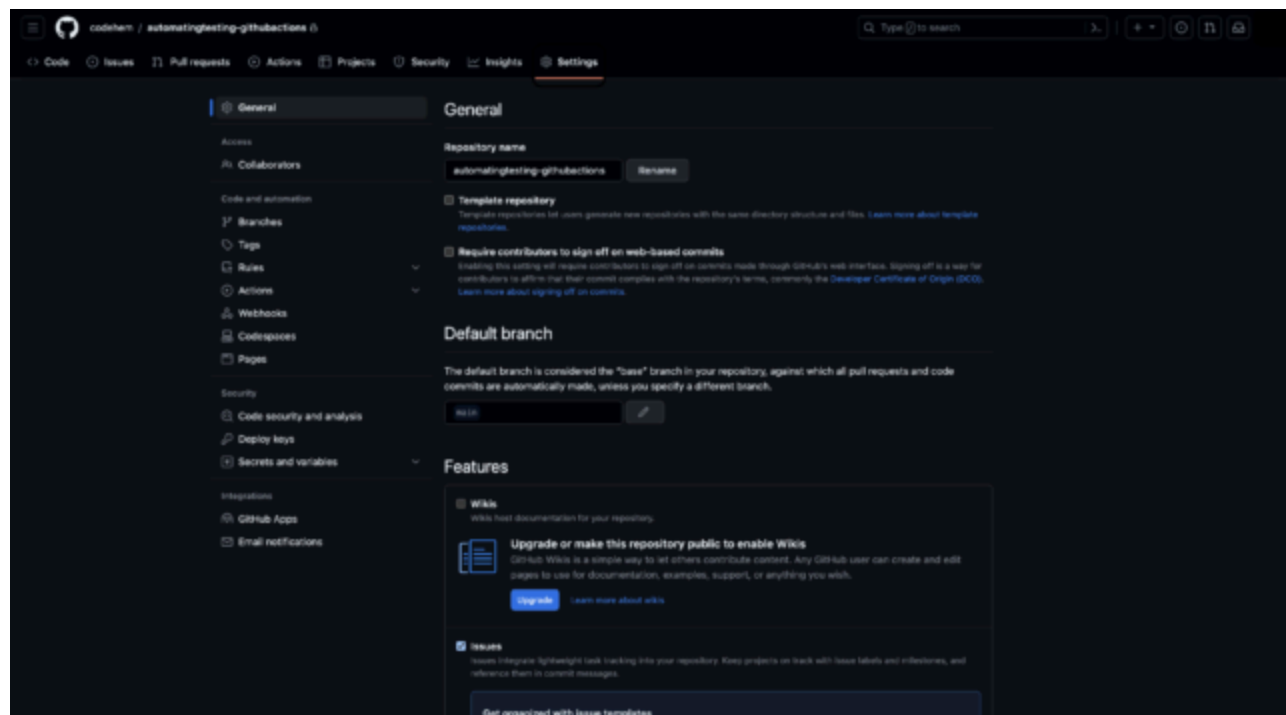
Last Flow Messages

Name Add Source Edit Delete

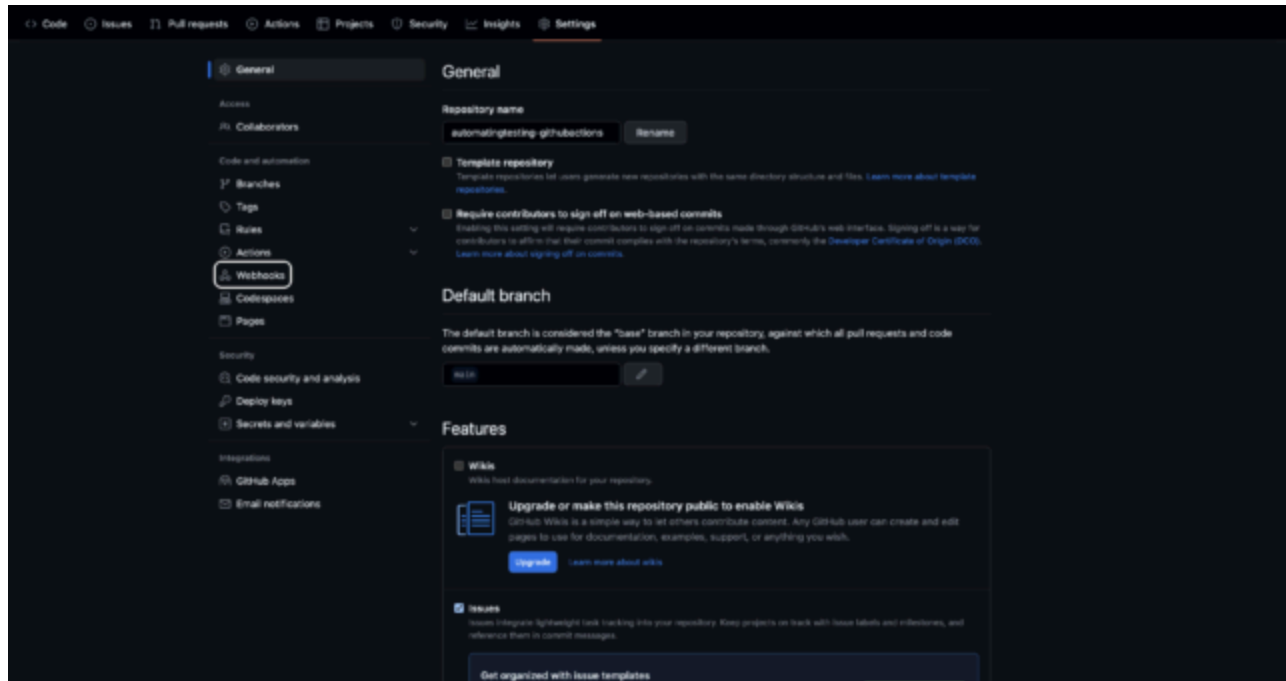
Reconnect 100% Show 100% Edit Delete



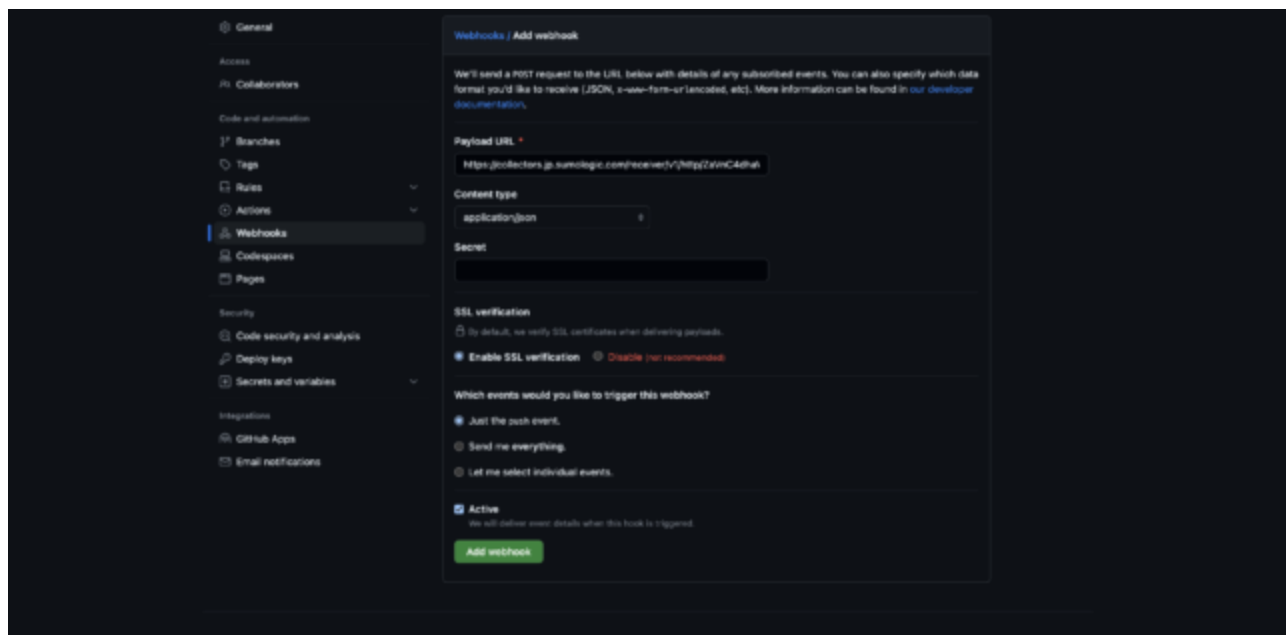
Configuring Github Webhook, sign in to Github account, Navigate to your organization, in that repository and click on settings



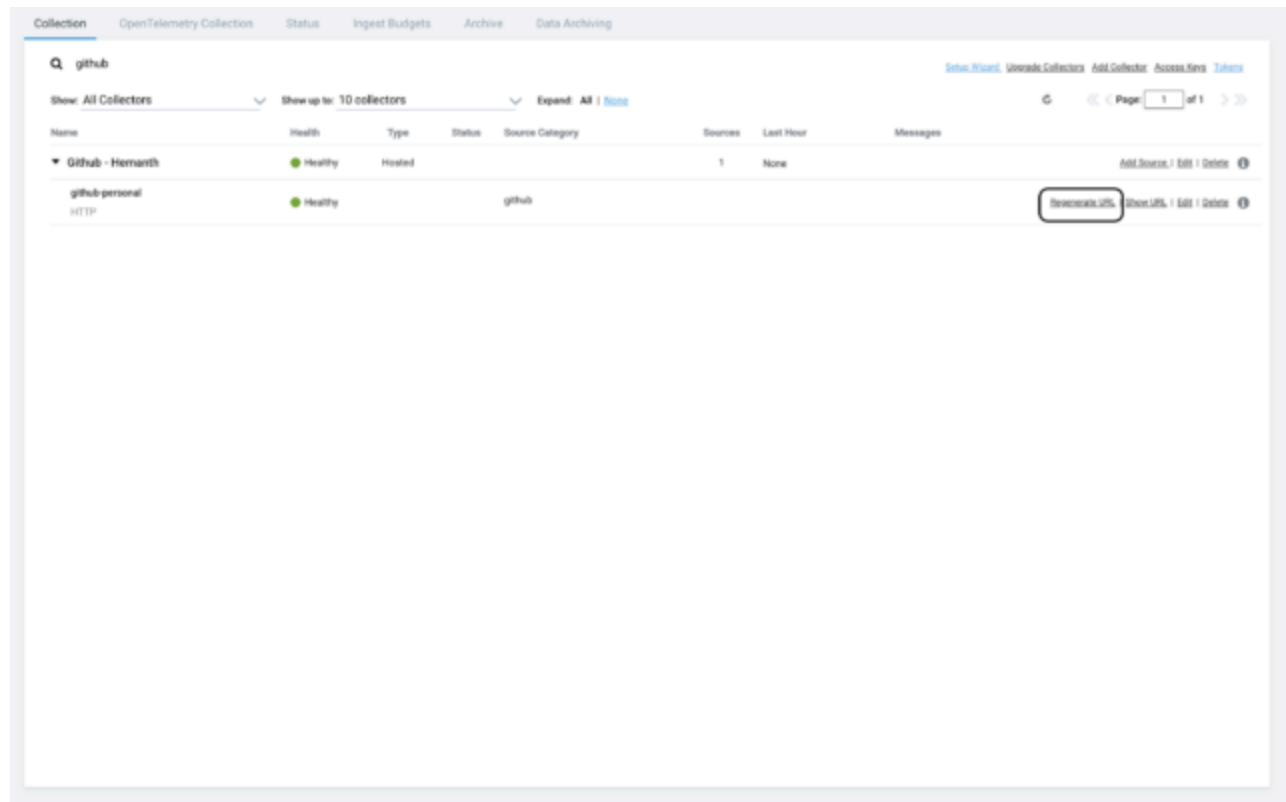
Click on Webhooks in the left-hand menu and click on add webhook



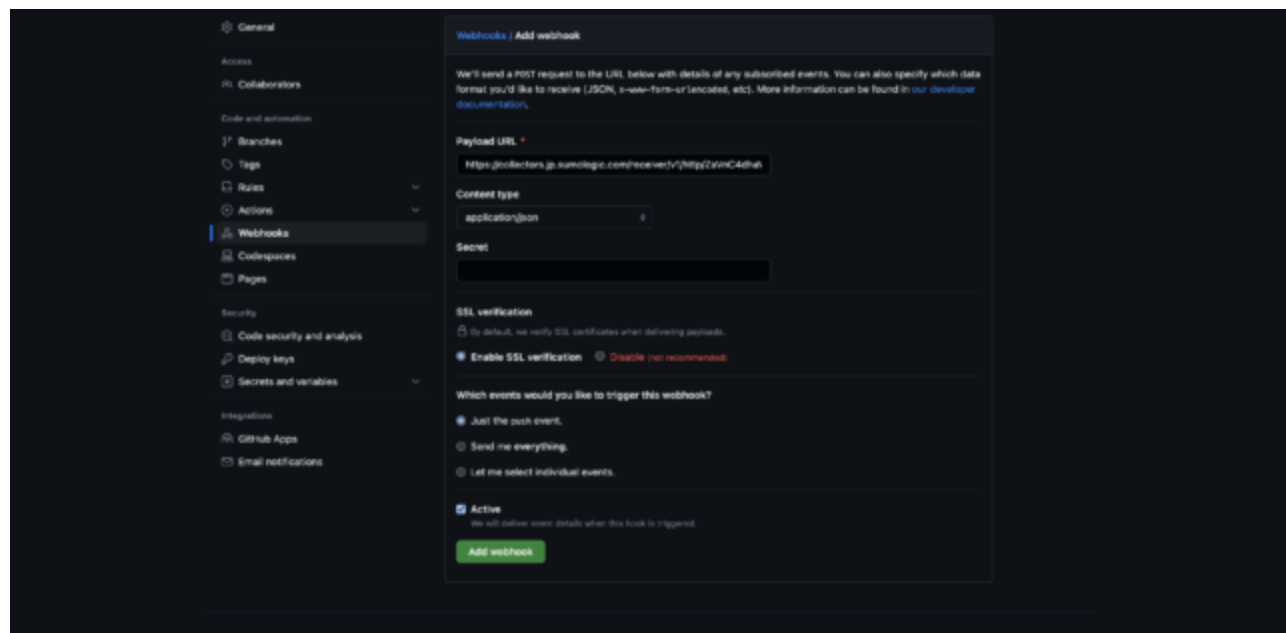
Paste the copied HTTP source address in the payload URL, set the content type as application/json



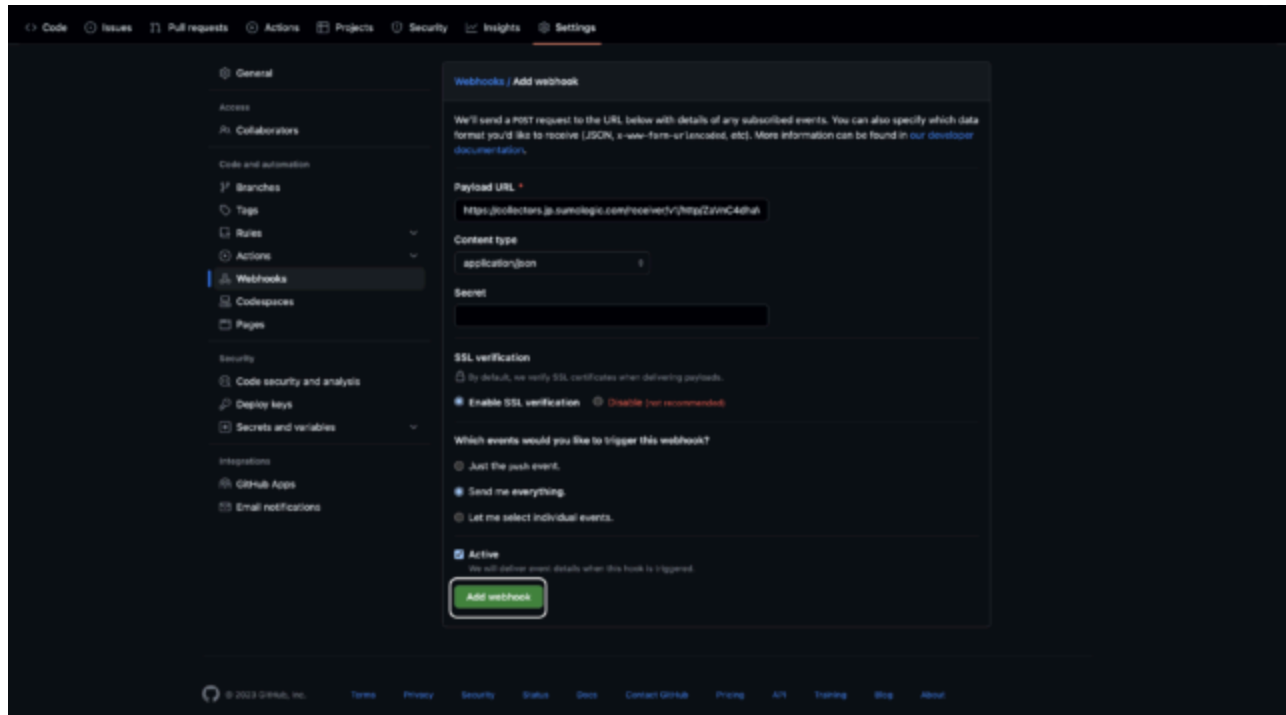
Note - If you have misplaced your URL then you can regenerate as shown below



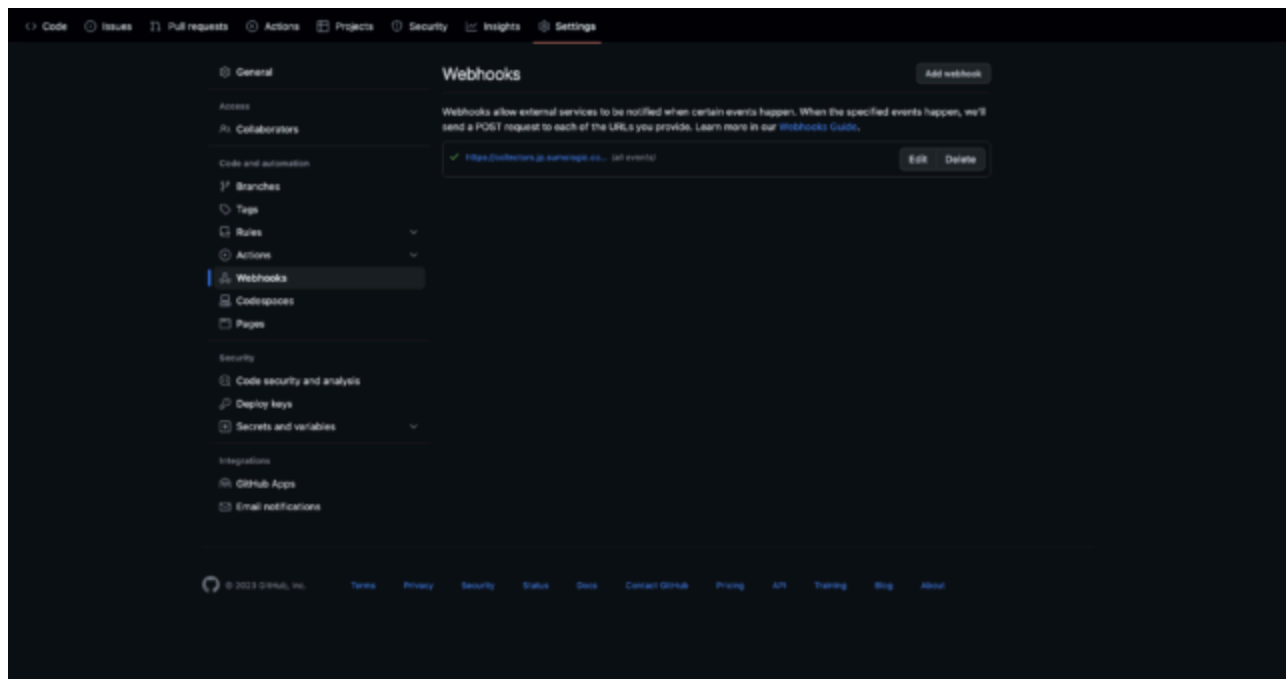
For events you would like to trigger, you can select any of below only "push events", "send me everything" or "selecting individual events" (there are many options if you have preference select them). I am selecting "send me everything".



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

The screenshot shows the Sumo Logic web application. On the left is a dark sidebar with the Sumo Logic logo at the top and a menu containing: App Catalog, Manage Data, Collection, Logs (highlighted), Metrics, Monitoring, Administration, Cloud SIEM Ecosystem, and Help. Below the menu is a section titled "No Saved Content" with a message: "You don't have any content in your library yet. Try adding an app to get started!" and an illustration of a sun and a plant.

The main panel has a top navigation bar with tabs: Fields (selected), Field Extraction Rules, Parsers, Partitions, Scheduled Views, and Data Forwarding. A "+ New" button is on the right. Below the tabs is a search bar with a magnifying glass icon and a close button (X). To the right of the search bar is a dropdown menu labeled "Existing - Custom Fields" and another "+ Add" button.

A table lists the fields for the selected collection:

Status	Field Name	Data Type	Field Extraction Rules	Role Based Access Control	Partitions	Collectors	Sources
OK	a-github-event	String	0	0	0	0	0

At the bottom of the page, there is a footer note: "Fields Capacity: Your account is using 83 (41.5%) out of the 200 fields available."

12/16

Collection							
OpenTelemetry Collection Status Ingest Budgets Archive Data Archiving							
<div> <div>Q github</div> <div> Setup Wizard Upgrade Collectors Add Collector Access Keys Tokens </div> </div>							
<div> <div>Show: All Collectors</div> <div>Show up to: 20 collectors</div> <div>Expand: All None</div> <div> <div>Page: 1 of 1</div> </div> </div>							
Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
▼ Github - Hemantk	Healthy	Hosted			1		1
<div> <div>github-personal</div> <div>HTTP</div> <div>github</div> <div> Refresh Show Logs Edit Delete </div> </div>							

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](#)