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

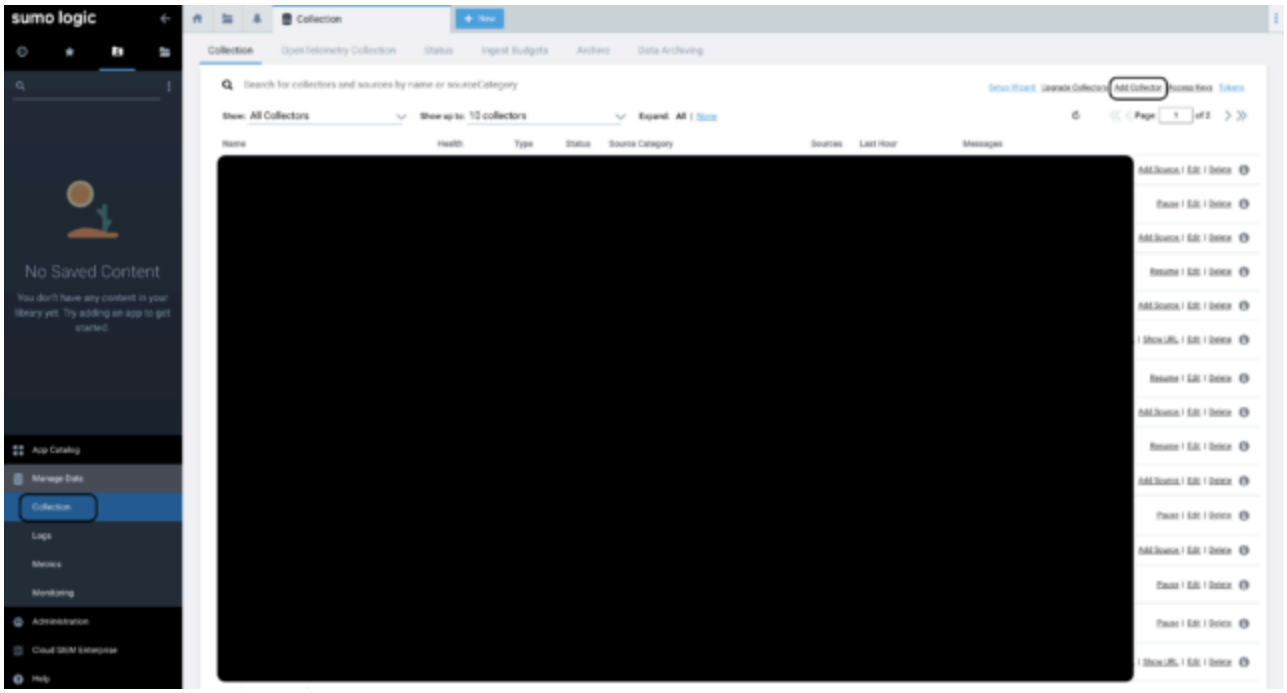
Before going further let's understand what sumo logic is. A cloud-based log management and analytics software called Sumo Logic enables businesses to exploit their machine data for useful insights. Sumo Logic's flexible capabilities make log data analysis simple and offer real-time visibility into operational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

Github

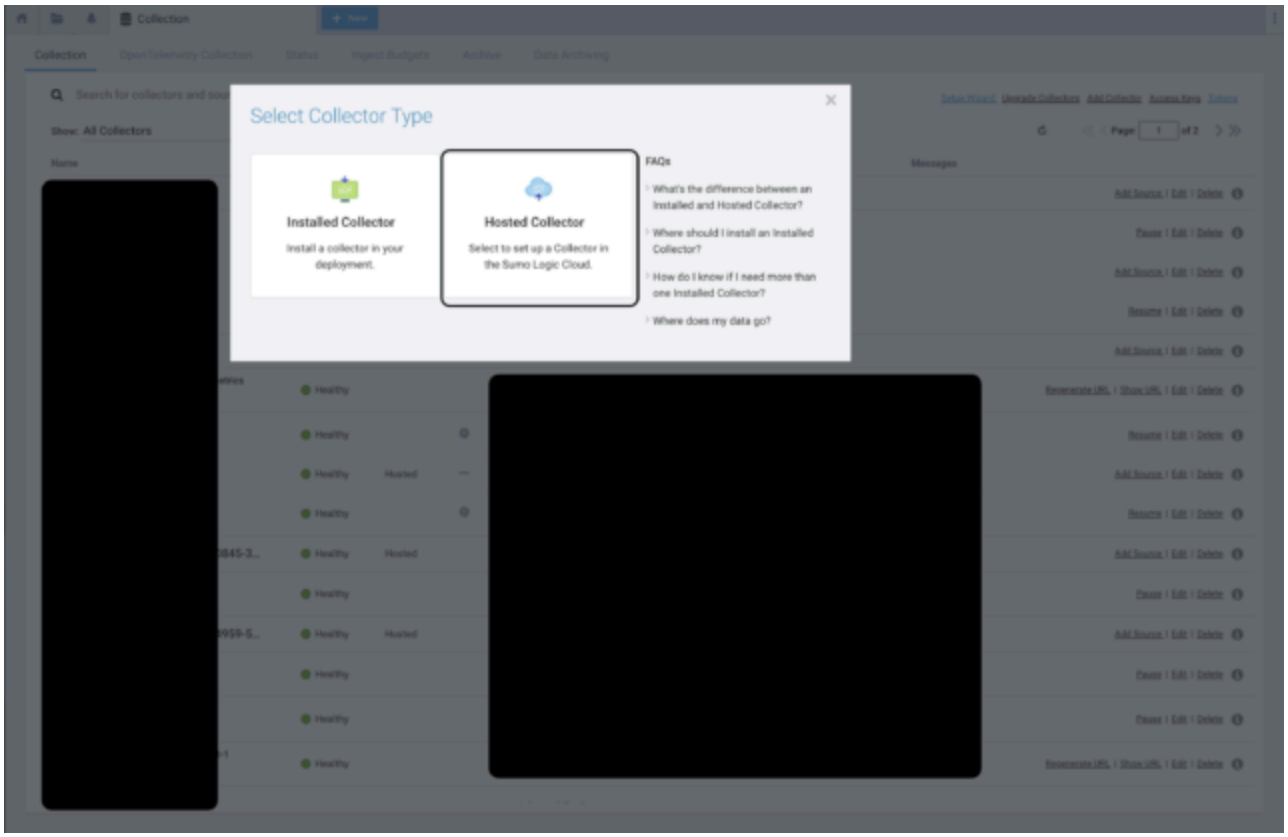
Developers can work together on software projects, manage their code, and participate in open source communities using the GitHub platform. Over 100 million developers utilize GitHub worldwide, and it is the home to many well-known open source projects. This platform promotes creativity and collaboration,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

Demo

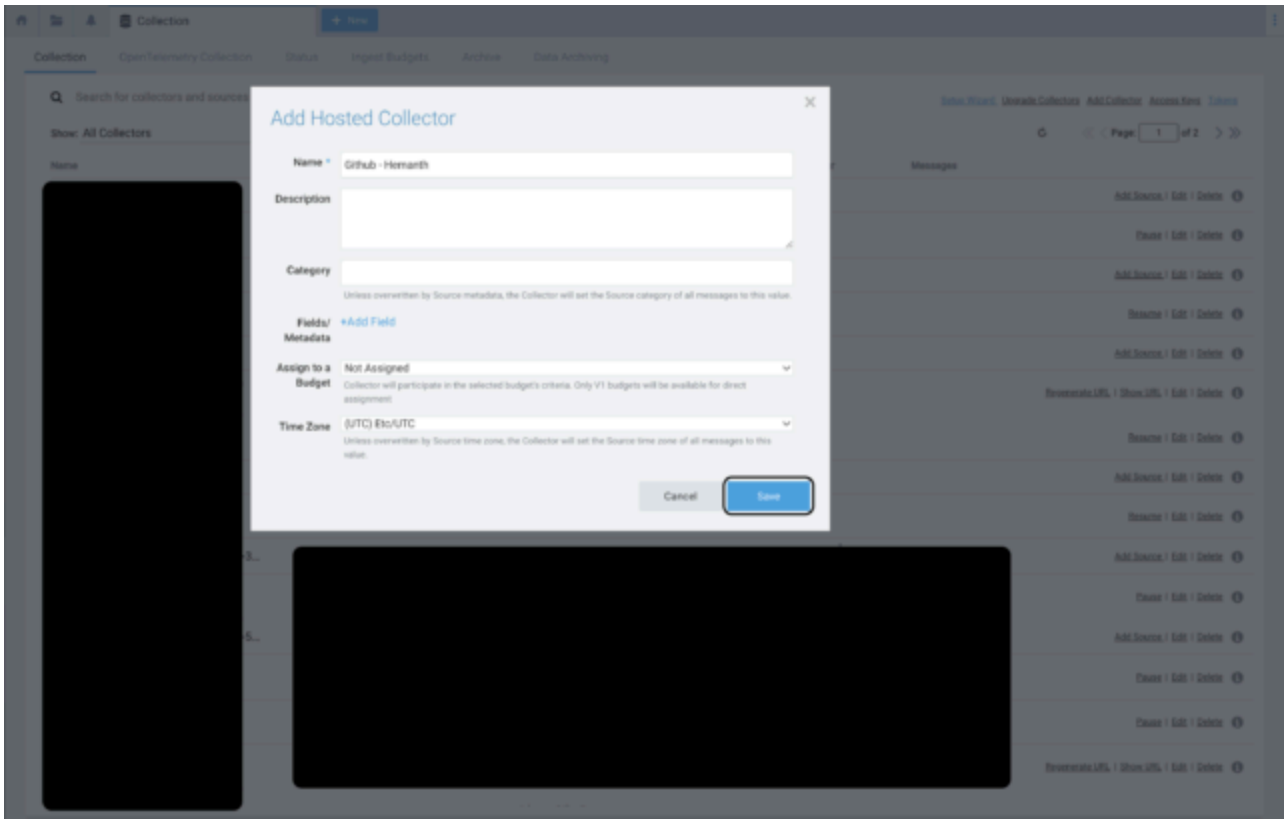
Log into your Sumo logic account, navigate to Manage data, then click on collection and click "Add Collector" button located in the top right

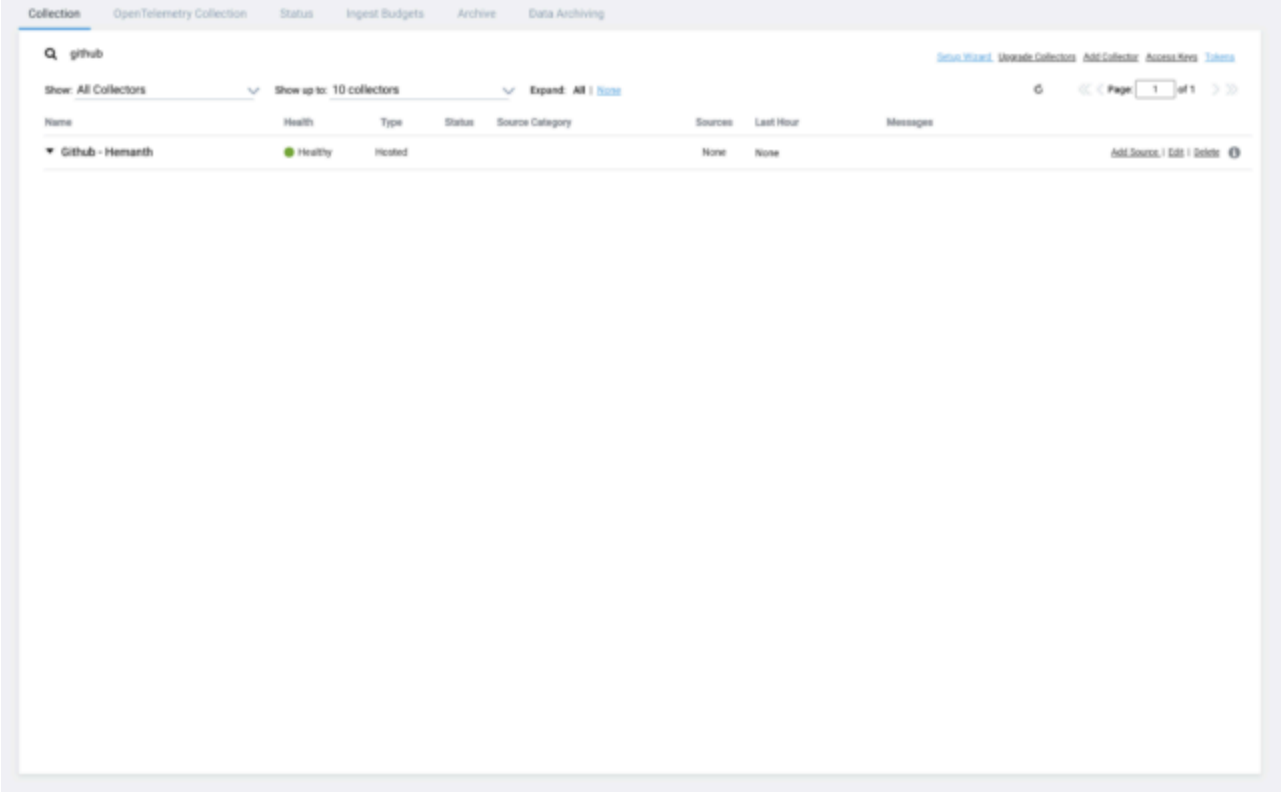


click on hosted collector

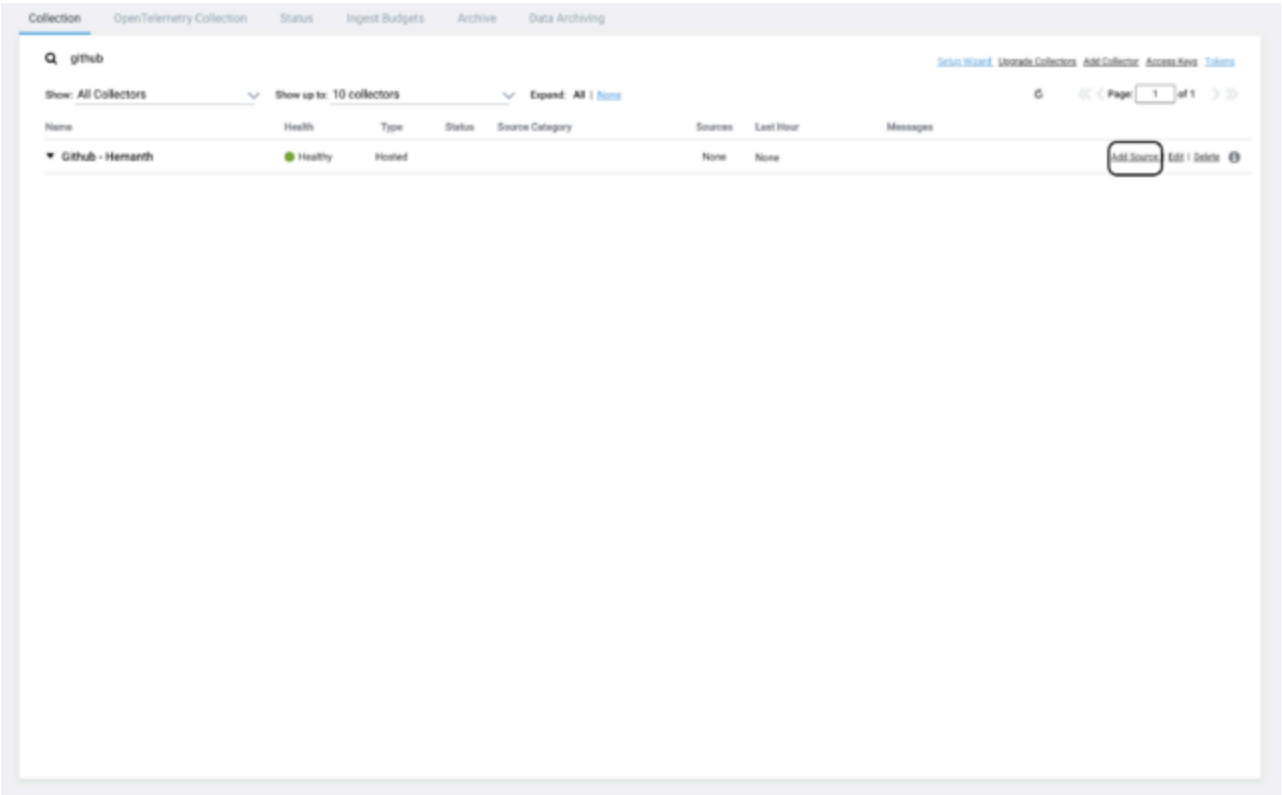


Provide a name and description for the hosted collector as required, select your preferred time zone and click save

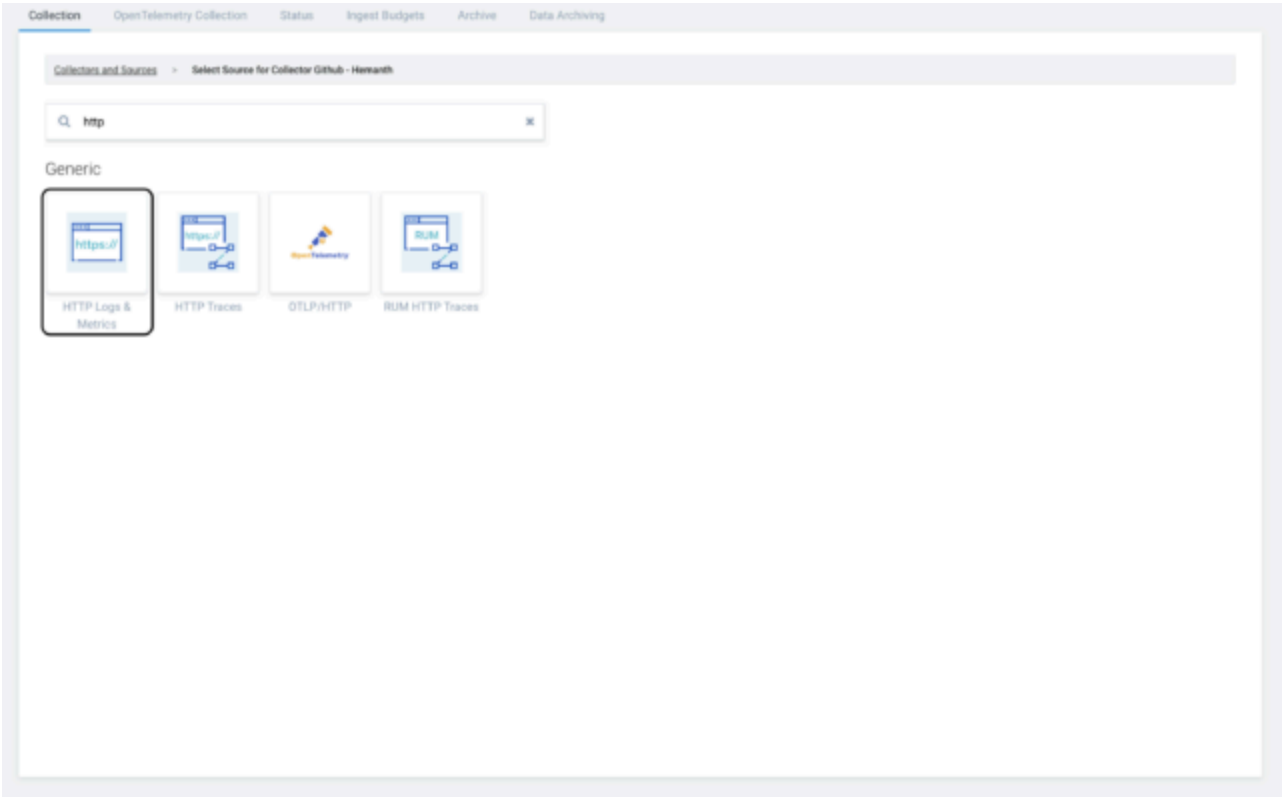




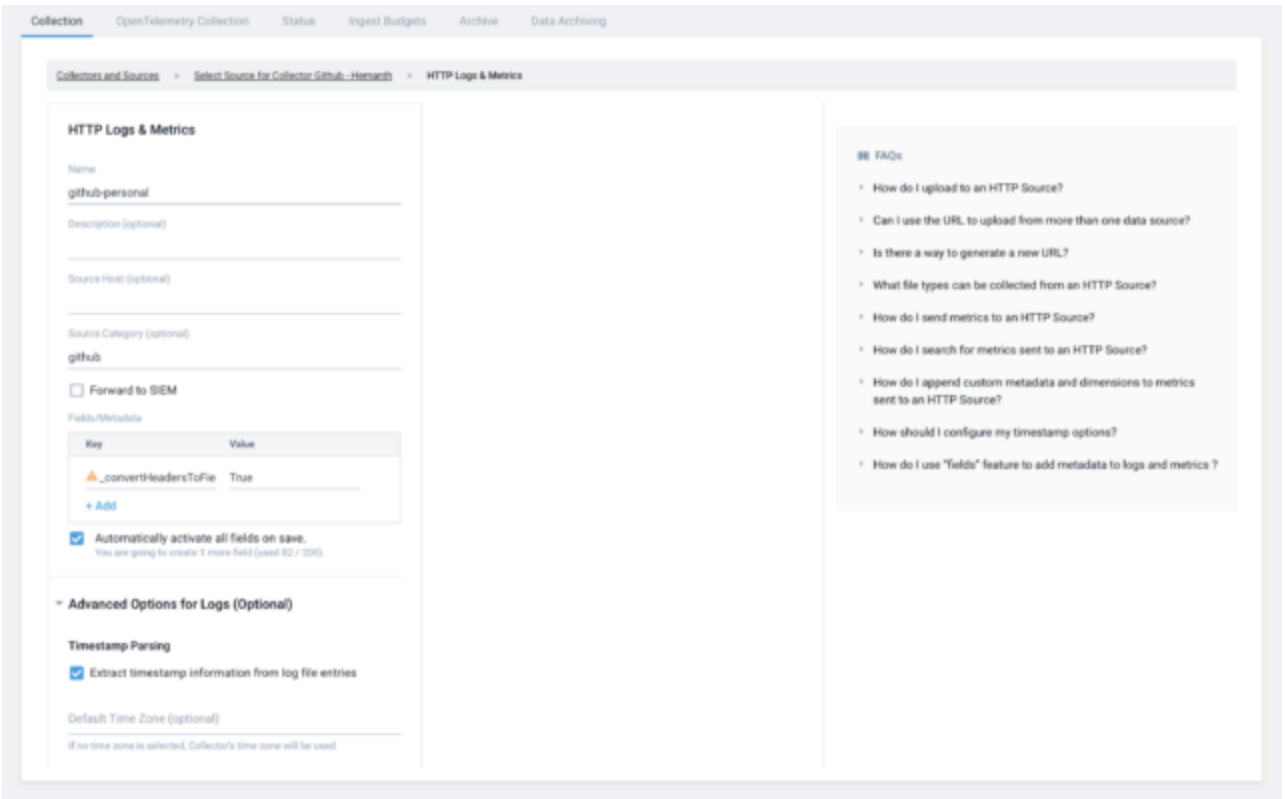
Configuring an HTTP Source on to the created hosted collector by clicking on Add Source at right hand side of the created collector

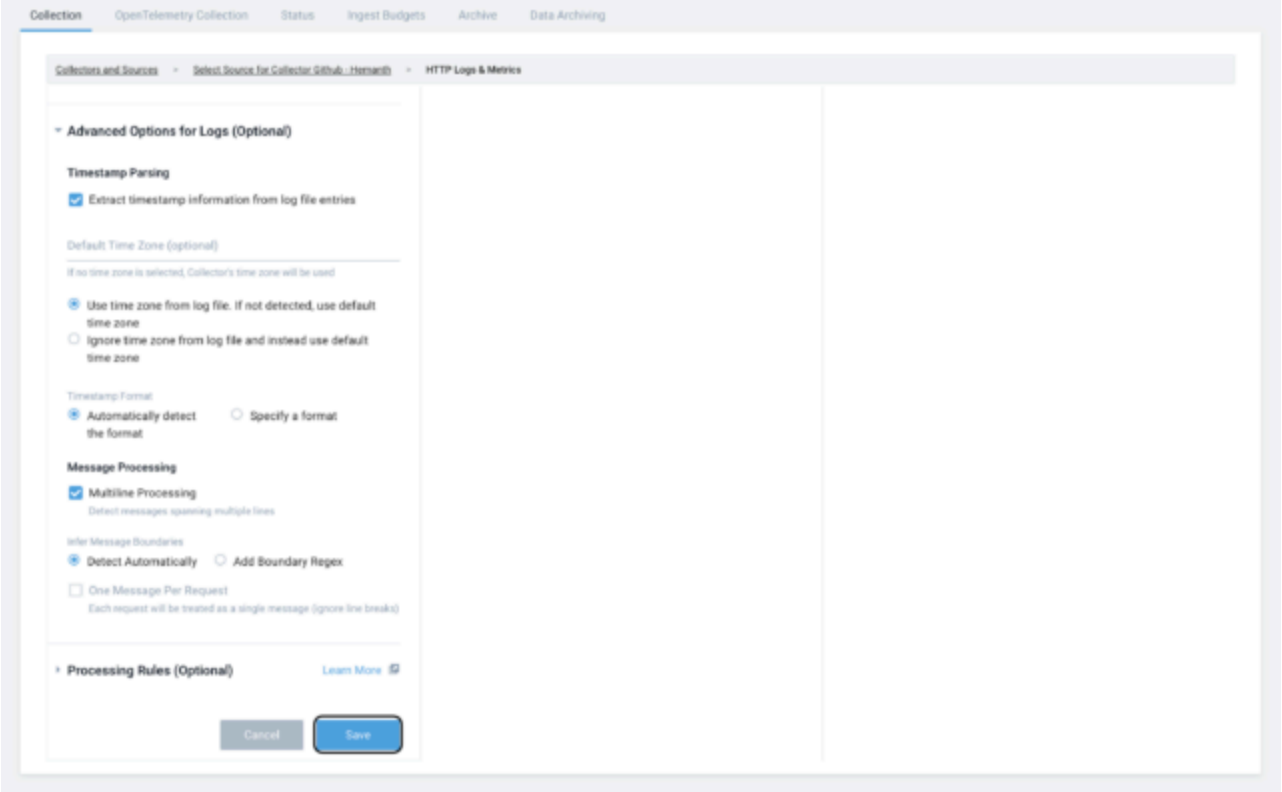


Search for HTTP Logs and Metrics and select it

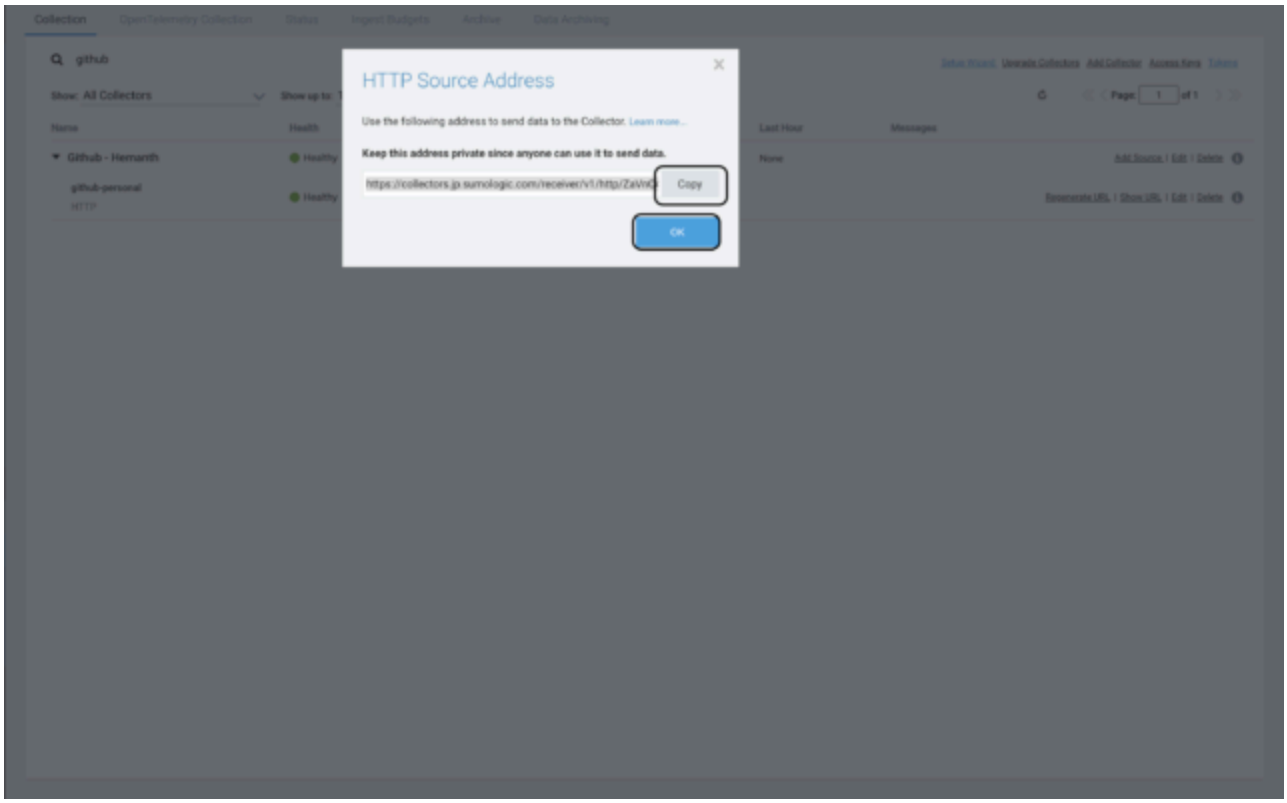


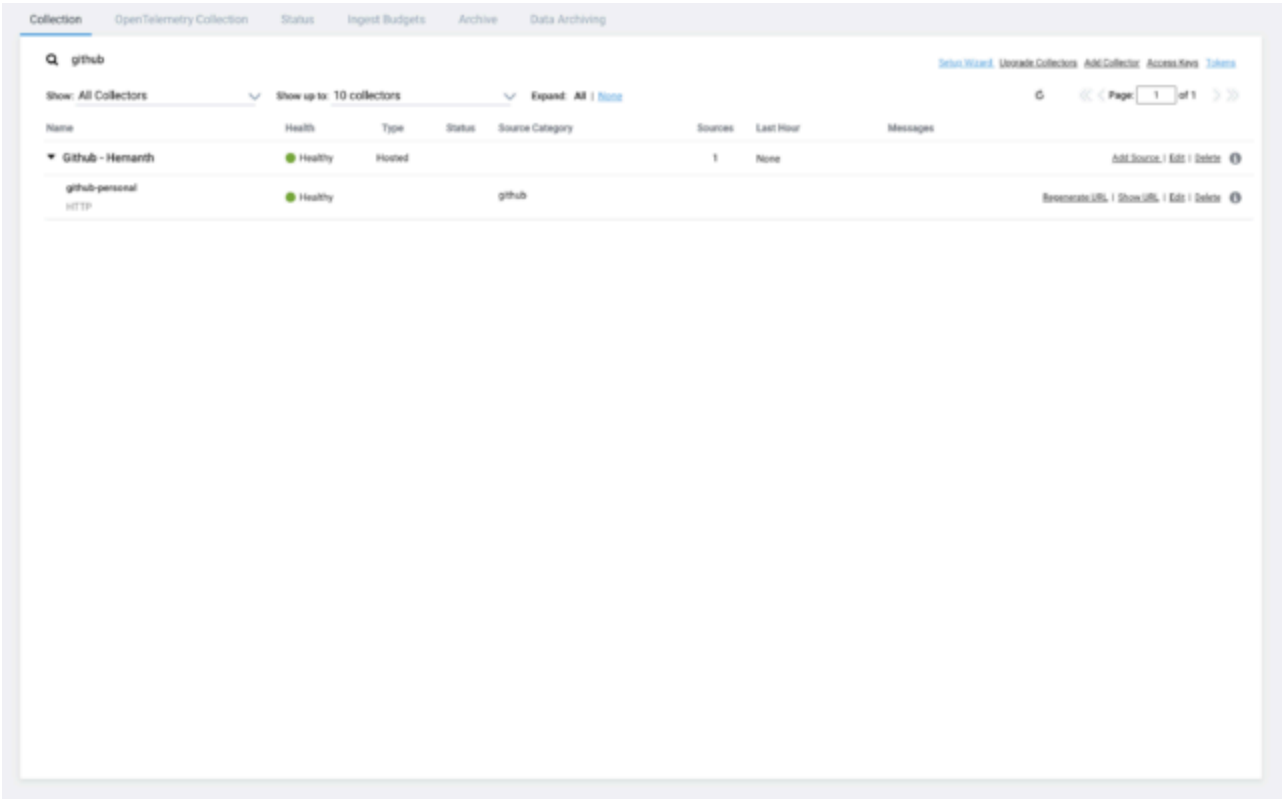
Assign a name and a source category, input key and value. Keep other settings as default before saving



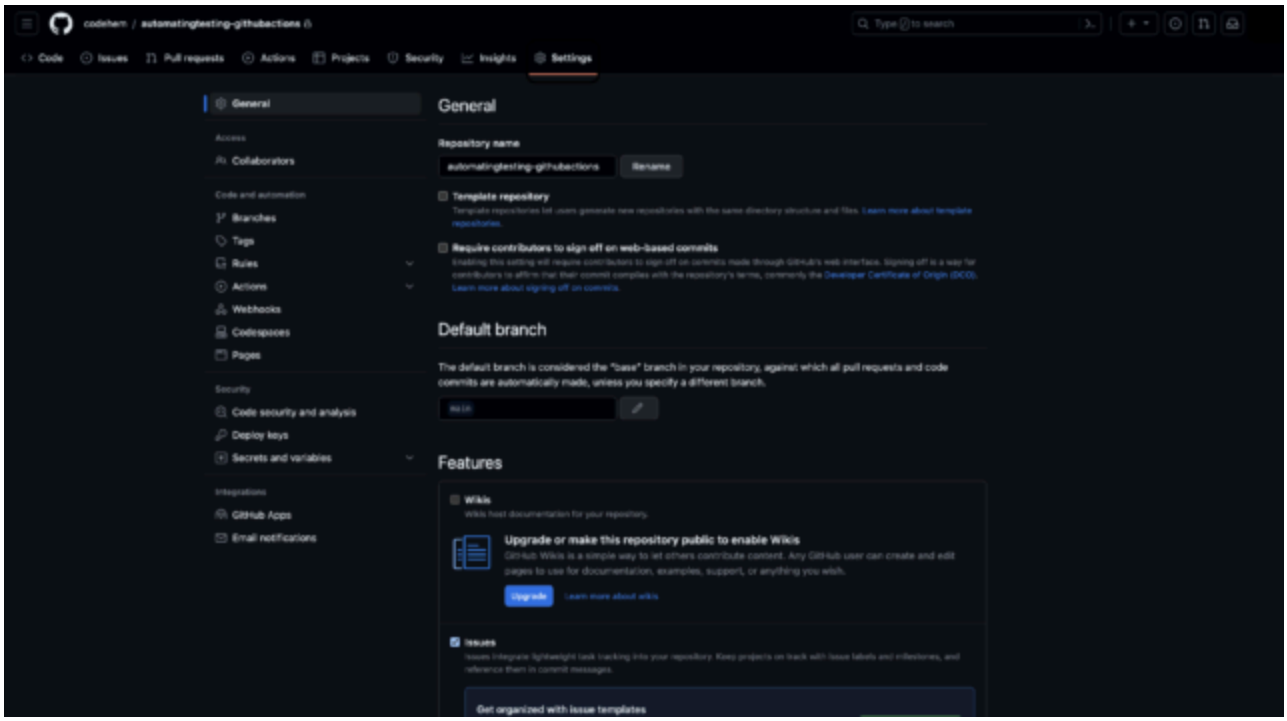


Copy the displayed HTTP source Address for later use. After that click ok.

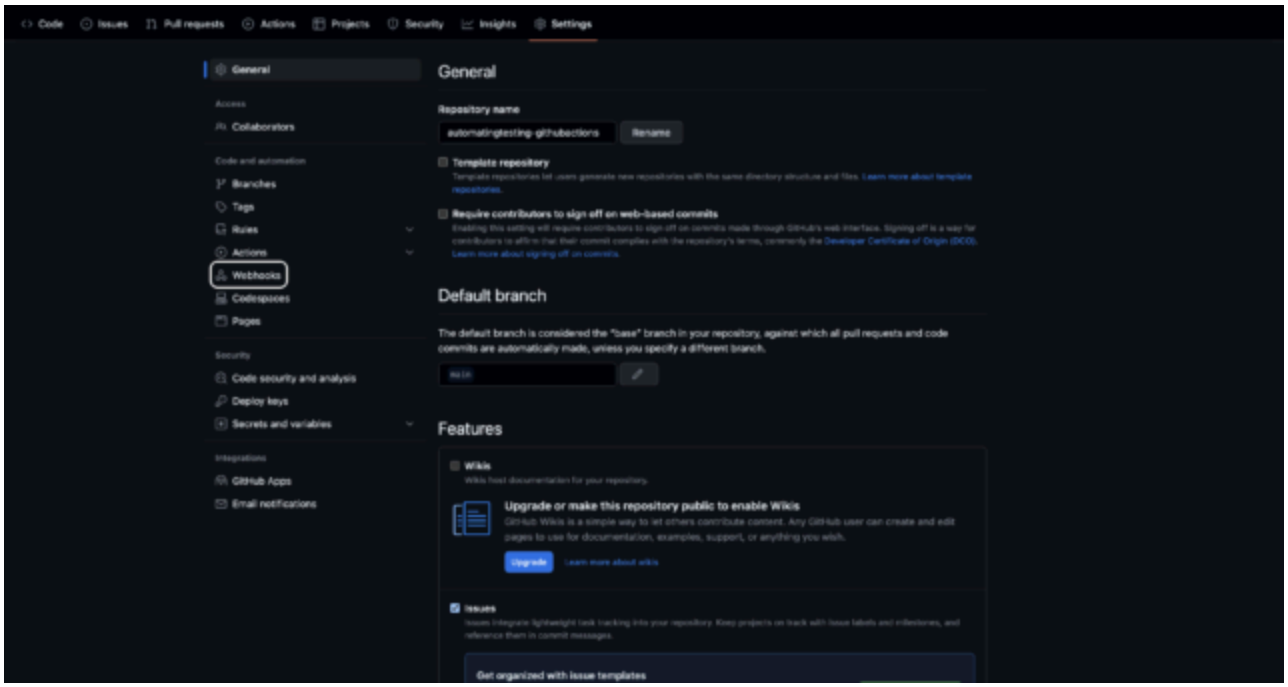




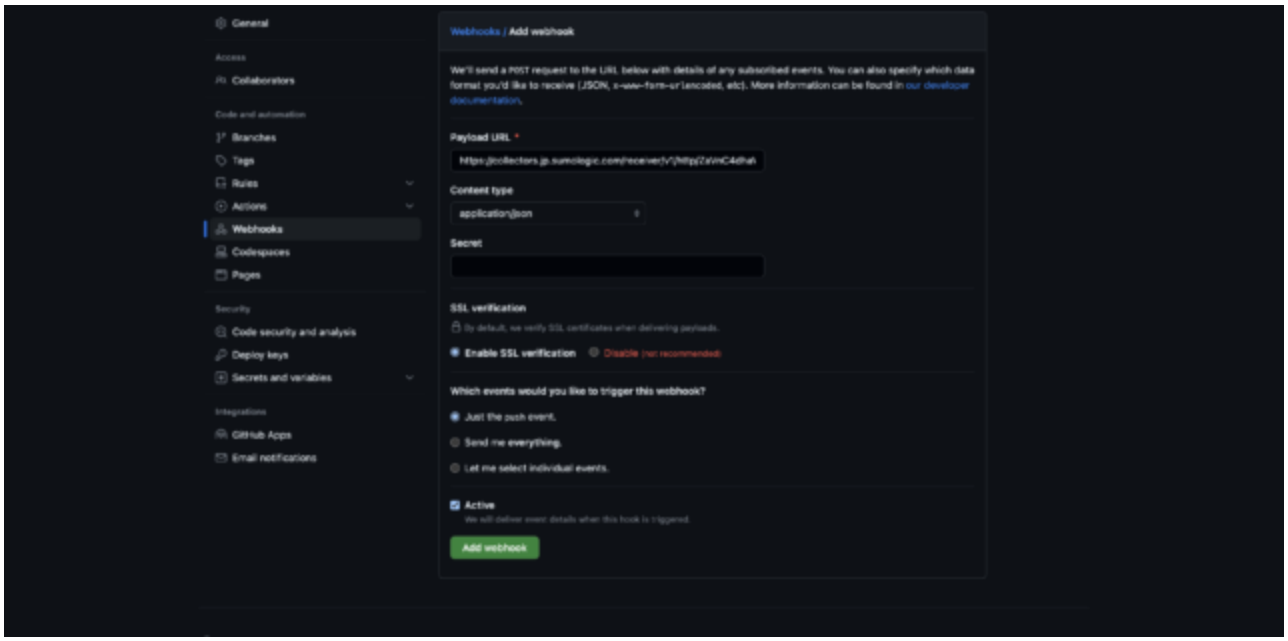
Configuring Github Webhook, sign in to Github account, Navigate to your organization, in that repository and click on settings



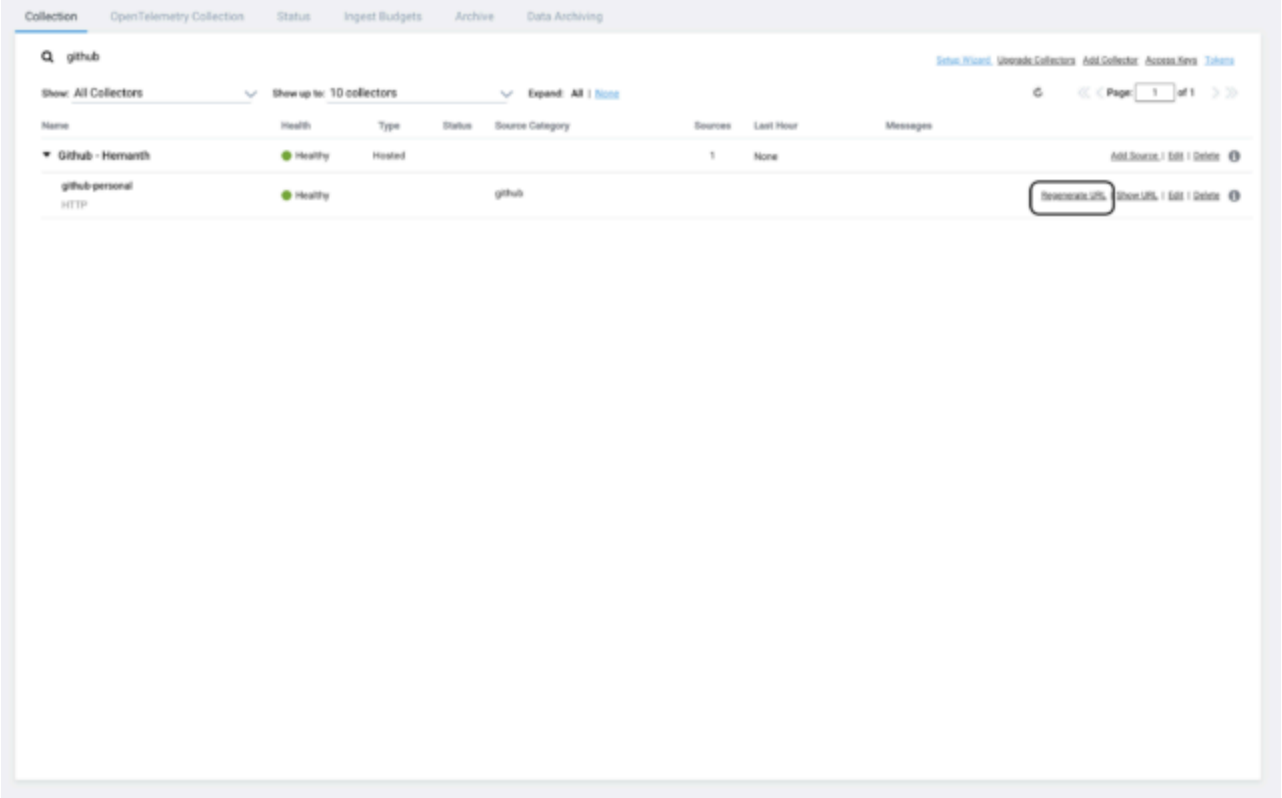
Click on Webhooks in the left-hand menu and click on add webhook



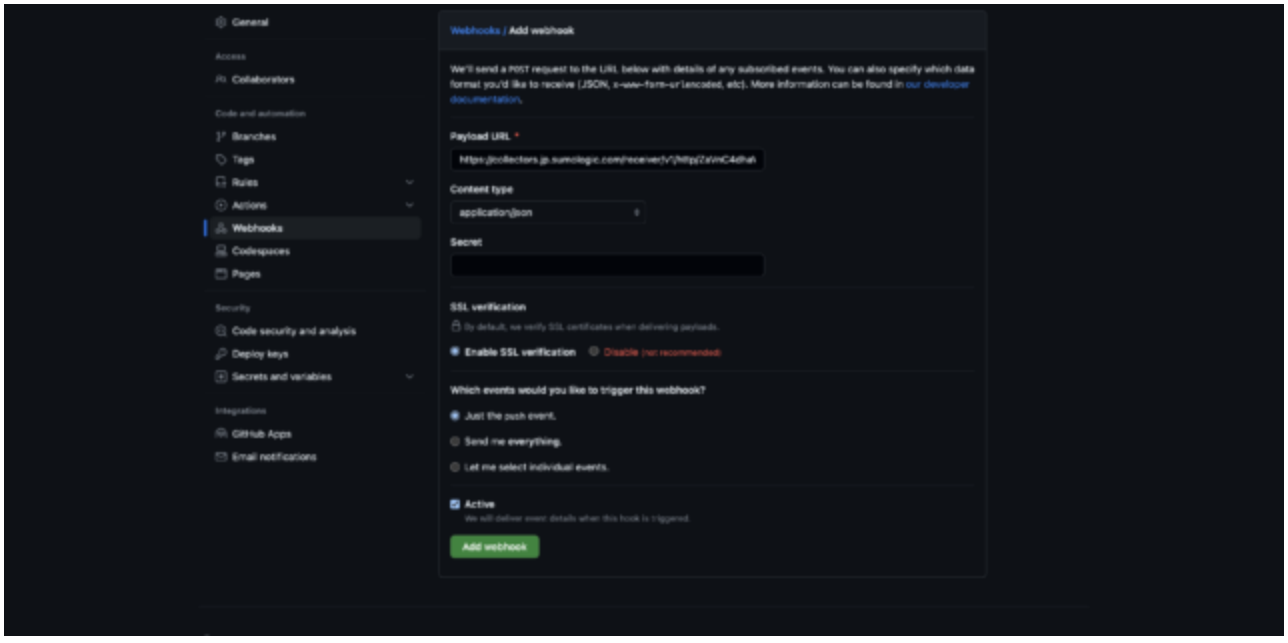
Paste the copied HTTP source address in the payload URL, set the content type as application/json



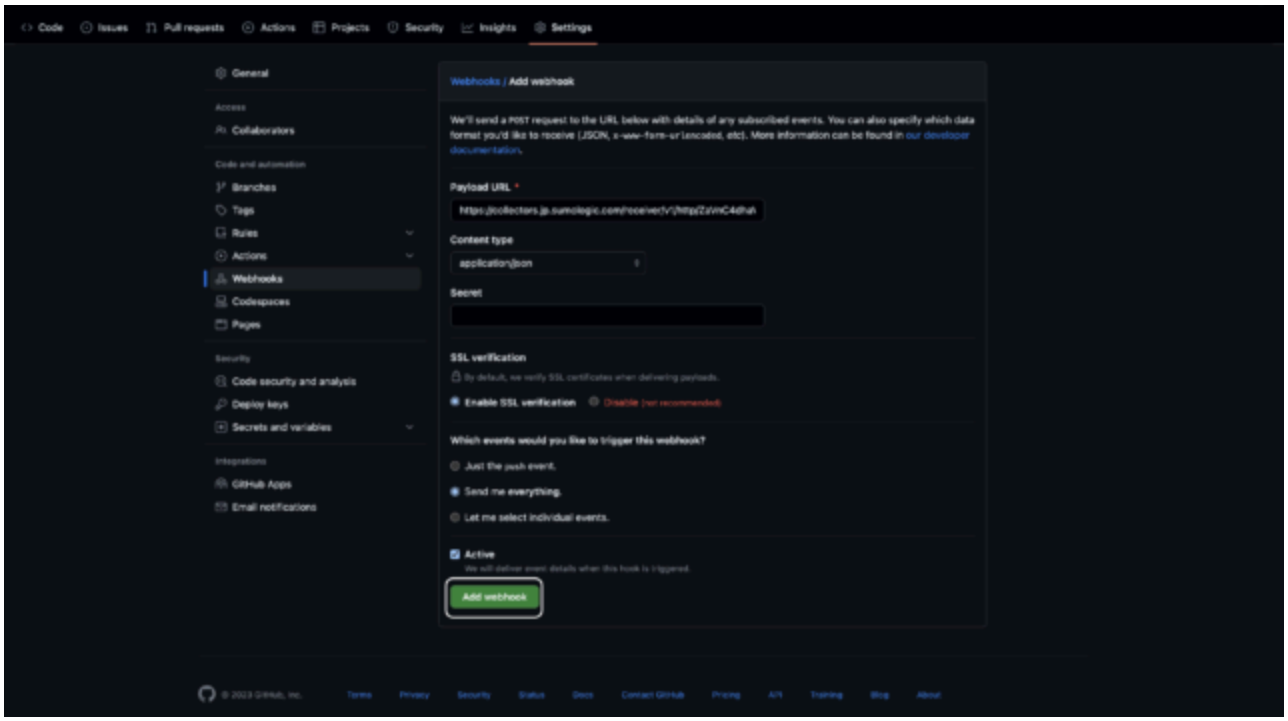
Note - If you have misplaced your URL then you can regenerate as shown below



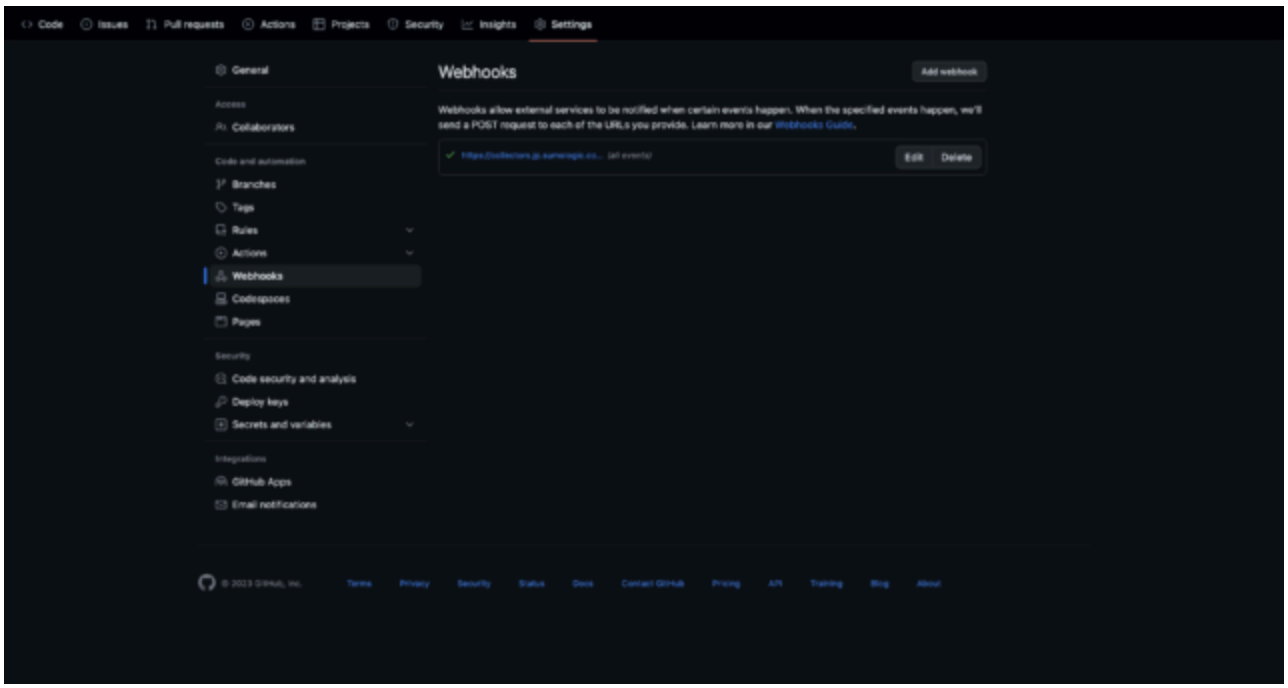
For events you would like to trigger, you can select any of below only "push events", "send me everything" or "selecting individual events" (there are many options if you have preference select them). I am selecting "send me everything".



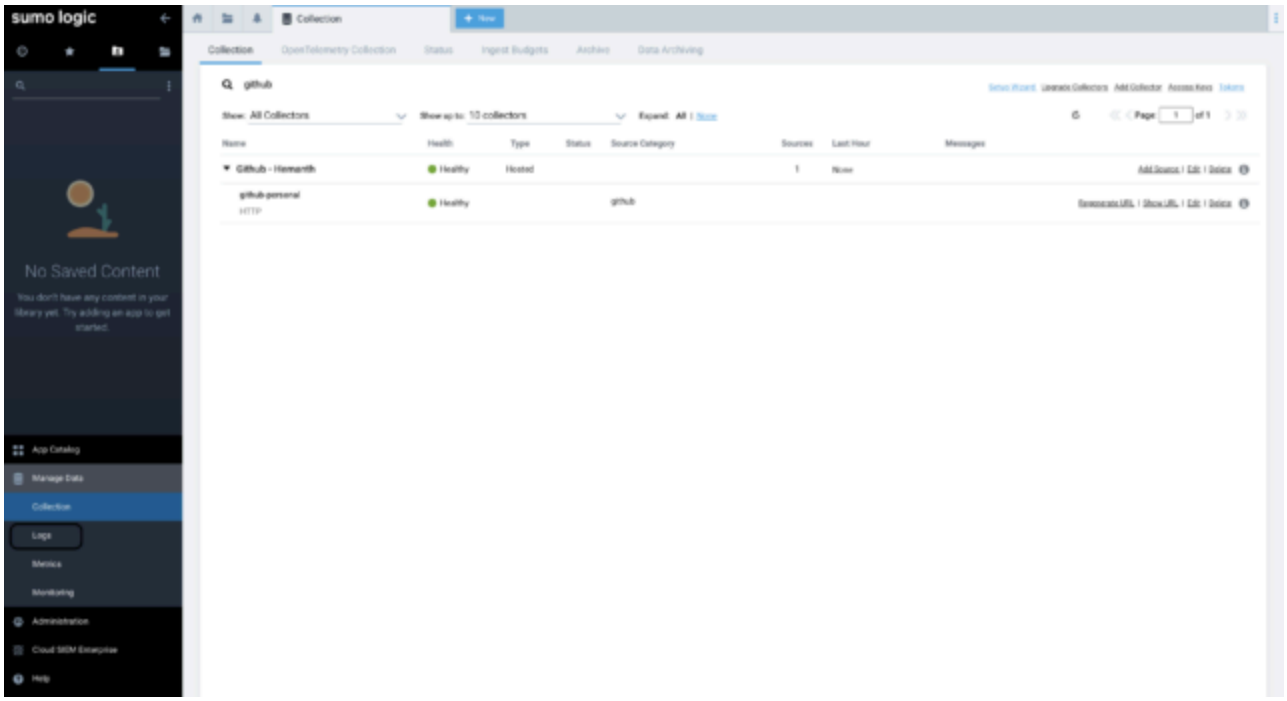
Click the active section and click on add webhook



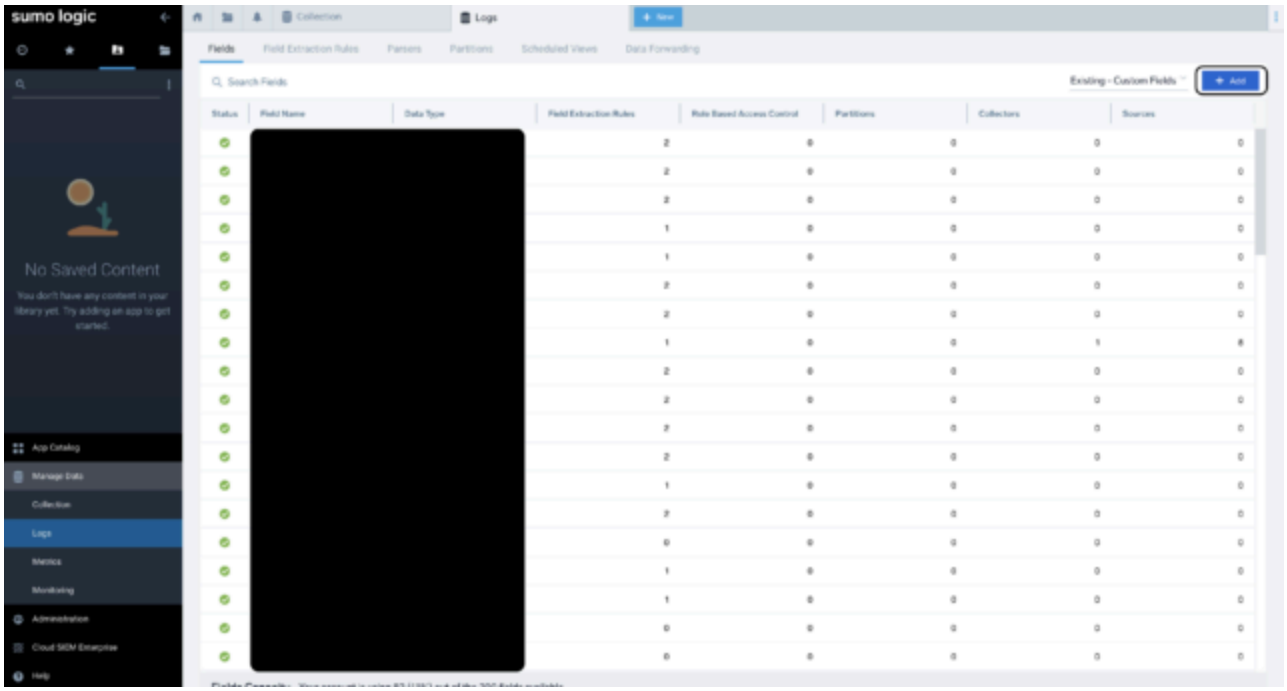
Webhook has been added successfully

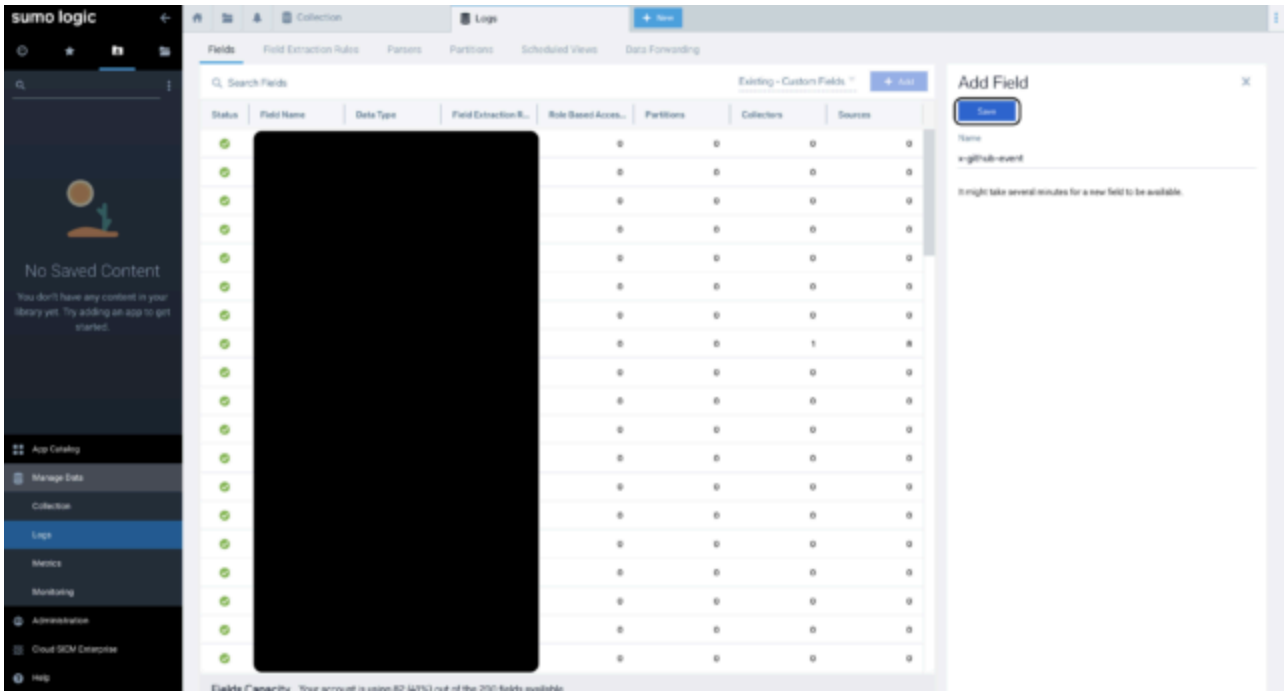


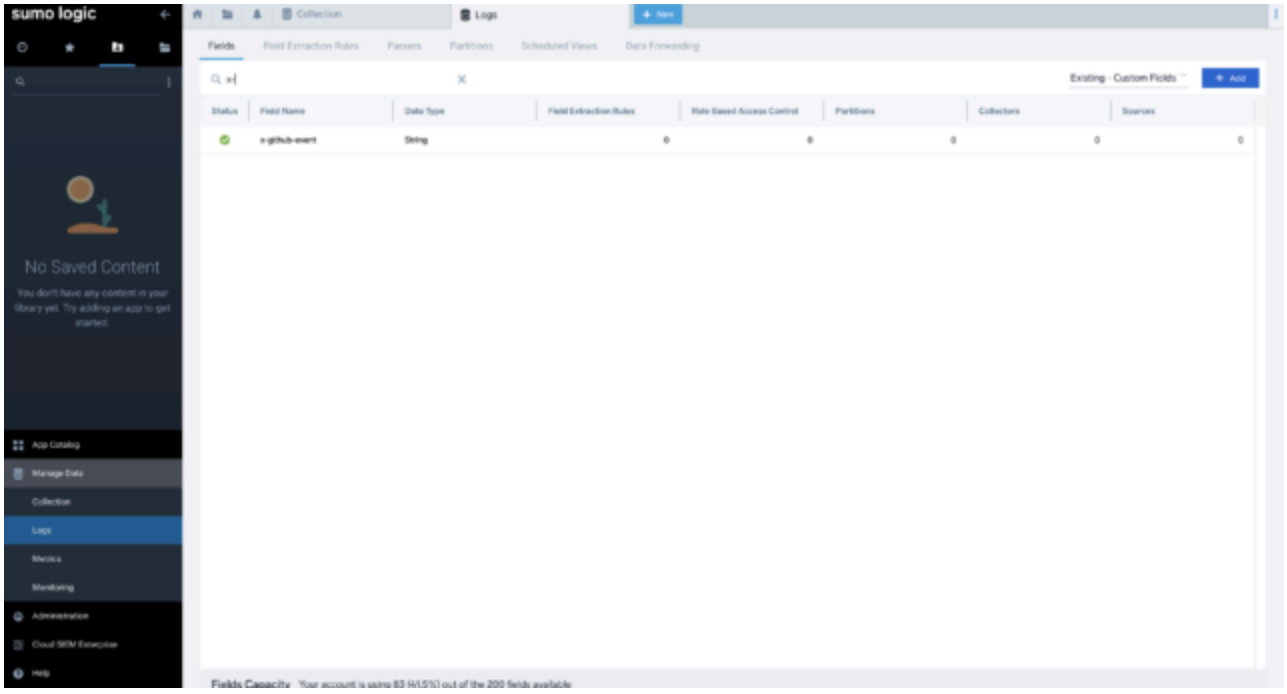
To ensure Sumo Logic comprehends incoming events, enable the x-github-event event type. Return to sumo logic and bottom left under collection click on logs



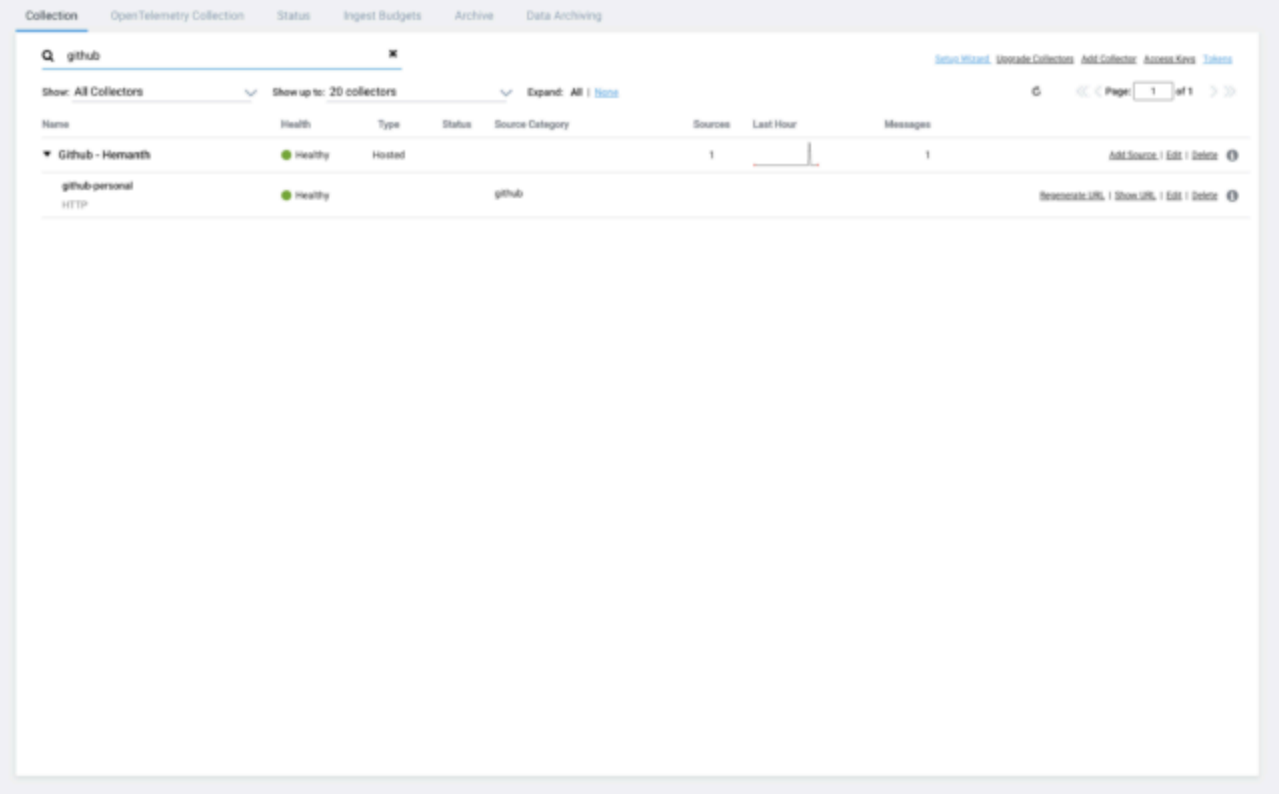
click "Add", give the above name it "x-github-event" and click save.







You can check the collection tab once



Conclusion

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

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