

データ収集ツール Fluentdの最新動向 With Splunk

福田大司郎

株式会社クリアコード

2024-09-19

About

me

Fluentd

メンテナー

株式会社クリアコード
の
ソフトウェアエンジニア

株式会社クリアコード



自由ソフトウェアとビジネスを両立！

Fluentdメンテナー3名！！



2021年から

コミュニティの

中心となって開発に参加

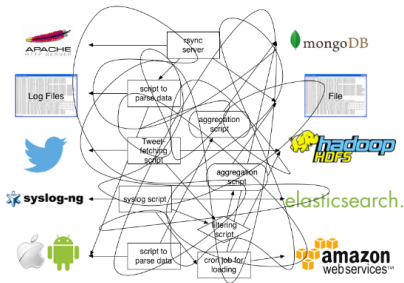
Fluentdとは？

“*Fluentd is an open source data collector that unifies data collection and consumption.*”

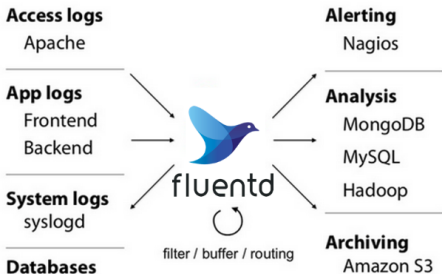


Fluentdの役割

Without Fluentd



With Fluentd



Fluentd

の特徴

自由ソフトウェア
(オープンソース)

1000以上の
プラグイン

自分でプラグイン
を作れる (Ruby)

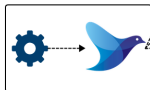
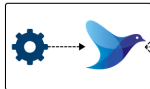
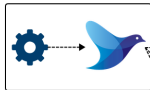
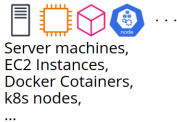
スケール

する

スケーラビリティ

Fluentd as Forwarder

(Collecting, Filtering, ...)



⋮

Fluentd as Aggregator

(Filtering, Formatting for output)



⋮



DB,
S3,
ElasticSearch,
...

大規模

運用可能

クラウドネイ ティブと相性◎

Splunk

x

Fluentd

Splunk用プラグイン

The screenshot shows the GitHub repository page for `fluent / fluent-plugin-splunk`. The repository is public and has 42 unwatchers, 19 forks, and 41 stars. The current branch is `master`, with 6 other branches and 8 tags. A recent commit by `pbthorste` and `Petur.Thorsteinsson` is visible, titled "Discard empty events - Splunk hec gives an error if..." with commit hash `fad2c77` and 159 commits. The repository description is "Fluentd Plugin for Splunk" and it uses the Apache-2.0 license.

fluent / fluent-plugin-splunk

Type to search

<> Code Issues 10 Pull requests 4 Discussions Actions Projects Wiki Security Insights Settings

fluent-plugin-splunk Public

Unwatch 42 Fork 19 Star 41

master 6 Branches 8 Tags

Go to file Add file Code

pbthorste and Petur.Thorsteinsson Discard empty events - Splunk hec gives an error if... fad2c77 · 3 years ago 159 Commits

bin Initial commit 7 years ago

About

Fluentd Plugin for Splunk

Readme

Apache-2.0 license

Splunk用プラグイン(via HEC)

The screenshot shows the GitHub repository page for `splunk / fluent-plugin-splunk-hec`. The repository is public and has 28 watchers, 89 forks, and 83 stars. The current branch is `develop`, with 21 other branches and 21 tags. The repository description states: "This is the Fluentd output plugin for sending events to Splunk via HEC." The repository includes a `Readme` and is licensed under `Apache-2.0 license`. Recent commits by `Vihass Splunk` are listed, including updates to `.github`, `ci_scripts`, and `docker` folders, as well as updates to `ubi`, `cve`, and `ruby` dependencies.

Navigation: <> Code, Issues 17, Pull requests 1, Actions, Projects, Security, Insights

Repository: **fluent-plugin-splunk-hec** (Public)

Interactions: Unwatch 28, Fork 89, Starred 83

Branches: develop (21 Branches), 21 Tags

Search: Go to file

Actions: Add file, Code

About: This is the Fluentd output plugin for sending events to Splunk via HEC.

Tags: plugin, splunk, fluentd, hec

Links: README, Apache-2.0 license

Commit	Message	Time
3fc5ddb	Merge branch 'main' into develop	last year
	fix: update ubi, fix cve, update ruby (#282)	last year
	fix: update ubi, fix cve, update ruby (#282)	last year
	update to 1.3.3 (#283)	last year

Splunk 関連

開発停滞

Splunk OpenTelemetry Collector

Fluentdの課題

フィードバック求

む

Fluentd

最新パッケージ



td-agent

簡単に

インストール

歴史

Year	Package	Fluentd
2011	td-agent v1	v0.9
2014	td-agent v2	v0.10
2017	td-agent v3	v0.14
2020	td-agent v4	v1.11
2023	fluent- package v5	v1.16

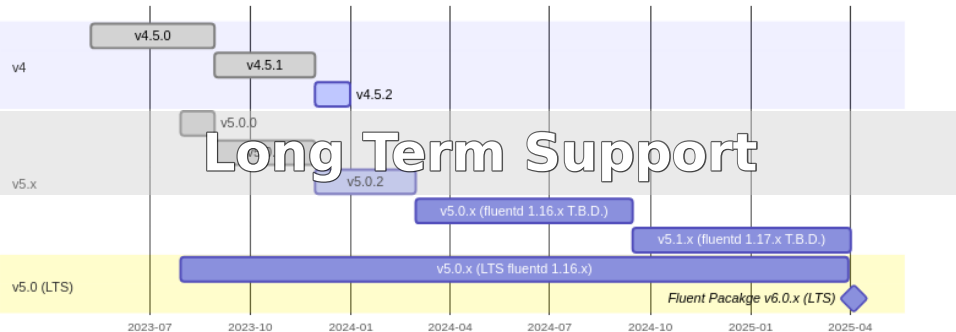


Fluent Package

td-agent

の後継

Scheduled Support lifecycle for Fluent Package



バグFIX

セキュリティ

FIX

アップデート

しやすい！

**長期の
安定運用に
おすすめ**

**td-agentから
アップグレード
可能！**

最後に

**Splunk x
Fluentd**

お困りの人

**ぜひ課題をシェア
してください！**

日本語Discussions

The screenshot shows the GitHub Discussions page for the repository `fluent / fluentd`. The navigation bar includes links for Issues (153), Pull requests (10), Discussions (selected), Actions, Wiki, Security (31), Insights, and Settings. Two discussion cards are visible at the top: "New Release Cycle for td-agent (Fluentd LTS)" by ashie and "Revising Project Hierarchy within the Fluent Organization" by edsiper. Below these, a search bar contains the query `iscopen category:"Q&A (Japanese)"`. The search results are sorted by "Latest activity" and filtered to "Open" discussions. A "New discussion" button is present. Under the "Categories" section, the "Q&A (Japanese)" category is selected, with a description: "日本語用のQ&Aです。困ったことがあったらここでコミュニティに質問してみましょう！". A specific discussion is highlighted: "rotate_age の設定について教えてほしい" by mikankun1003, asked on Jul 5, 2023, and marked as "Answered" with 8 reactions.

<https://github.com/fluent/fluentd/discussions/categories/q-a-japanese>