

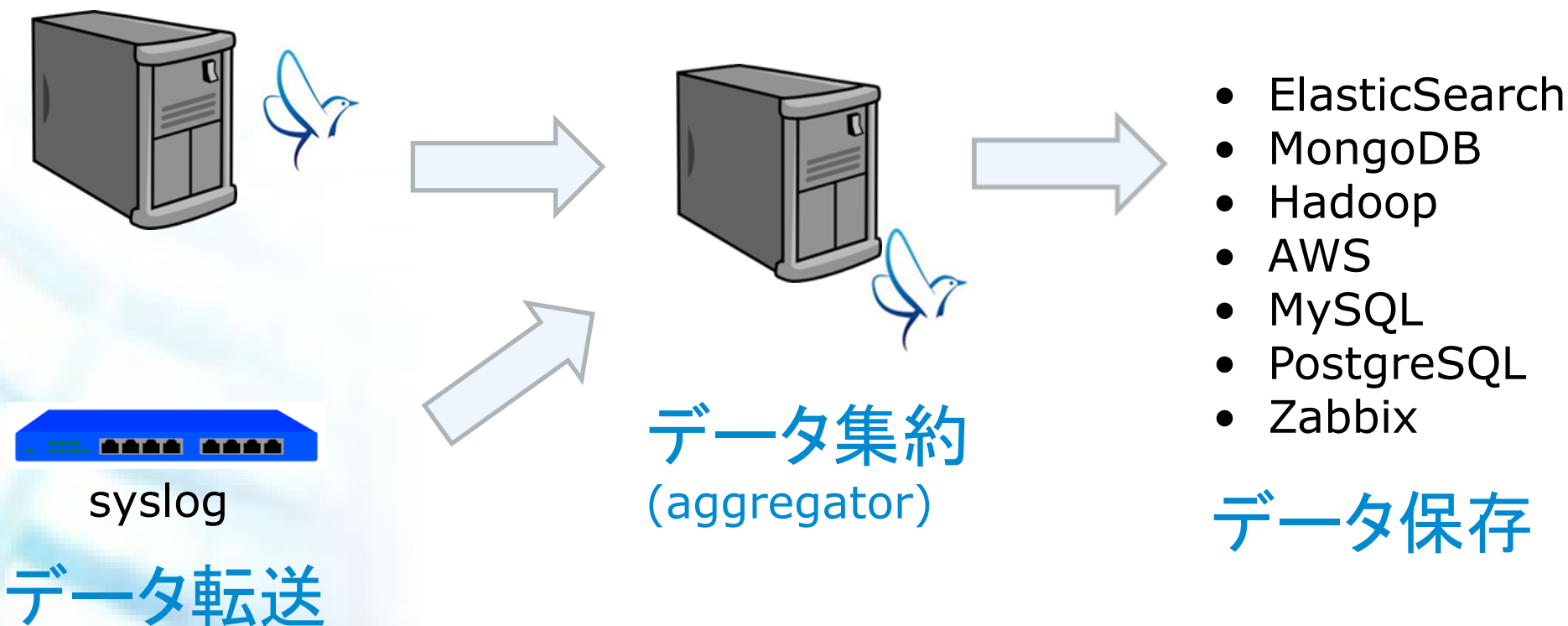
# Fluentd + Zabbix + Grafana で構築する グラフィカルなログ監視・分析システムのご紹介

2016年5月30日

SRA OSS, Inc. 日本支社  
マーケティング部 OSS技術グループ

- FluentdとZabbixについて
- Grafanaとは
- Fluentd + Zabbix + Grafana 構成の利点
- デモ

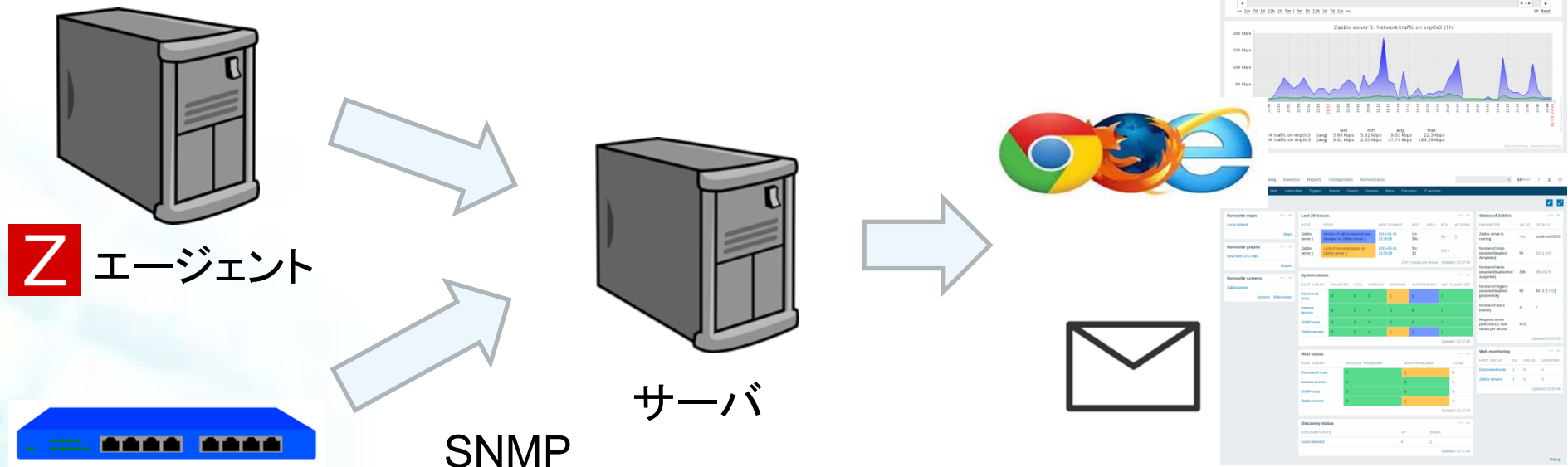
- Fluentd
  - ログを取得して転送してくれるミドルウェア
  - ログの加工や構造化ができる
  - いろんなデータベースにデータを保存できる



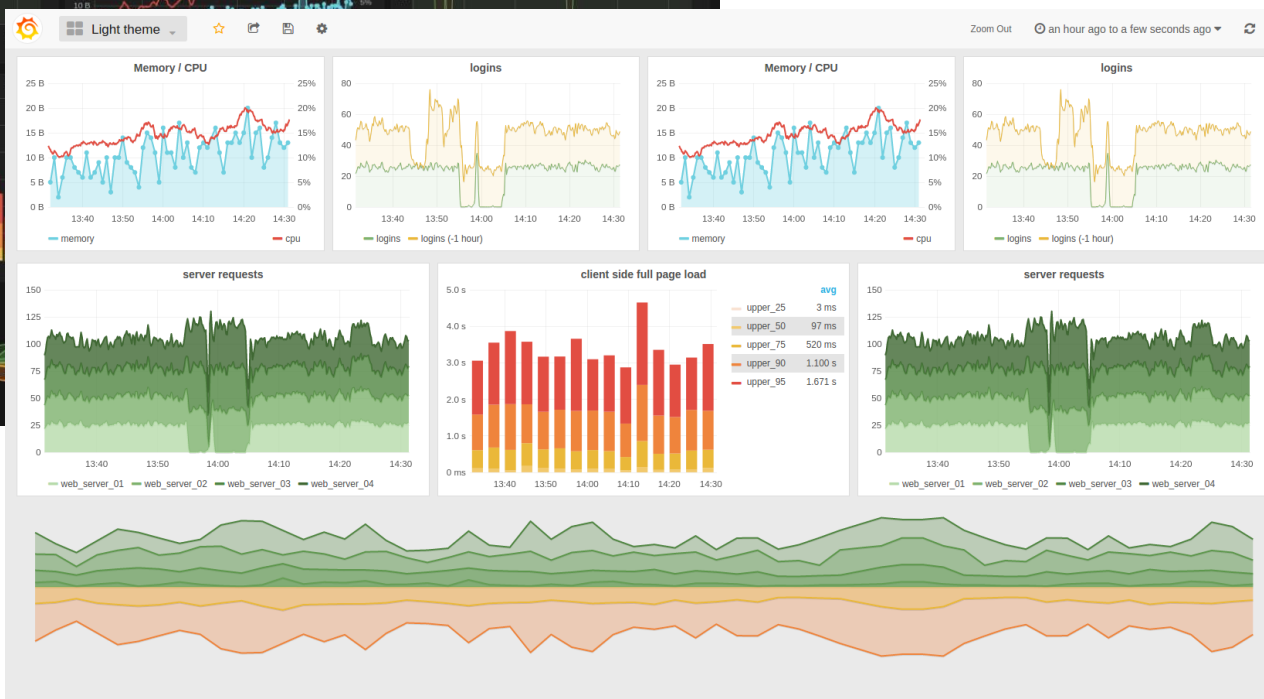
- Zabbix

# ZABBIX

- システムの異常を検知し通知を行う統合監視システム
- ネットワーク機器、OS、プロセス、性能、ログ監視ができる
- 監視結果の確認は専用のWEB画面から



- 複数のいろいろなDBからデータを取得してデータの可視化ができるOSSダッシュボード
- ライセンス Apache License V2



- グラフ描画に必要なデータは、複数の外部データベースからデータを取得することができる  
→ データソースと呼ばれる



## 対応データソース

- |                      |               |
|----------------------|---------------|
| ✓ Graphite           | ✓ InfluxDB    |
| ✓ ElasticSearch      | ✓ Zabbix      |
| ✓ Amazon Cloud Watch | ✓ OpenTSDB    |
| ✓ Bosun              | ✓ Prometheus  |
| ✓ Heroic             | ✓ KariosDB など |



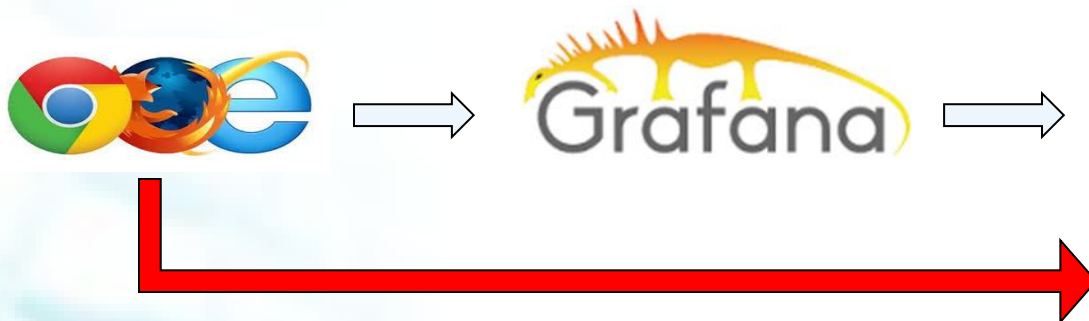
ユーザ/設定DBとデータDBを分離させ、一つのGrafanaから複数のデータソースに接続できるためデータを分散化させやすい

- Grafanaはユーザ管理、設定データ保存などのデータを保存するためのRDBが必要  
→ SQLite(デフォルト), PostgreSQL MySQL

- JavaScriptのフロントエンド(ブラウザ)とGo言語で書かれたバックエンド構成
- ブラウザから直接データソースにアクセスするDirectモードとバックエンド経由でデータソースにアクセスするproxyモードの選択ができる

## proxyモード

Grafanaサーバ経由でデータ取得  
オンプレ環境へアクセス



## Directモード

ブラウザから直接データソースへアクセス  
クラウドなどへアクセス

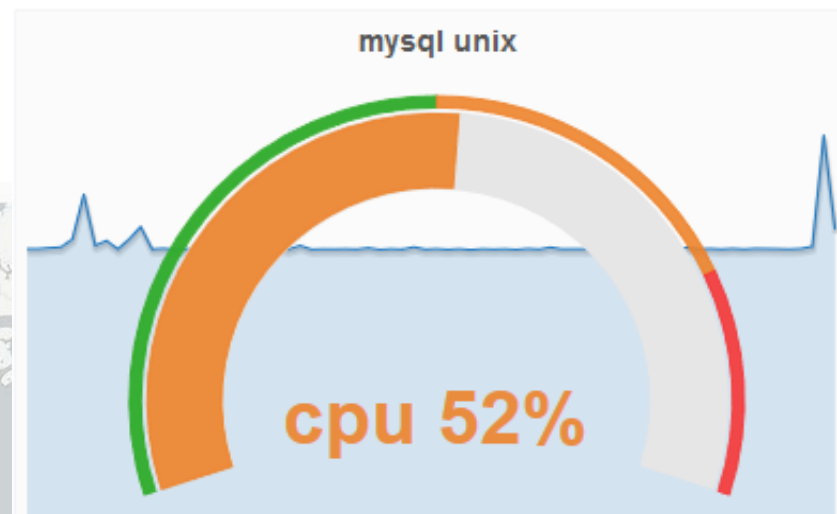
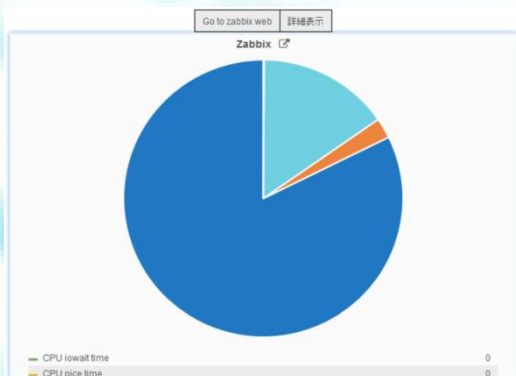
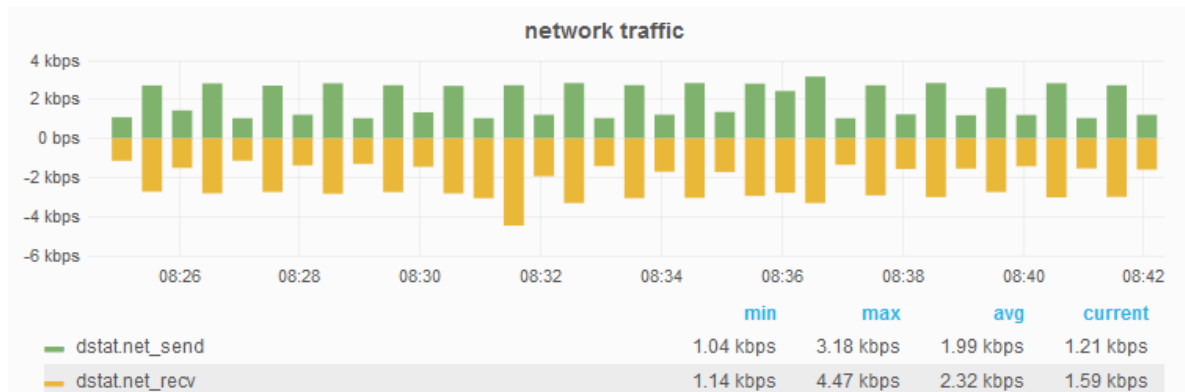


- 線グラフ、棒グラフ、積み上げグラフ
  - y左, y右軸サポート、negative-Y軸、単位(センサー系も豊富)

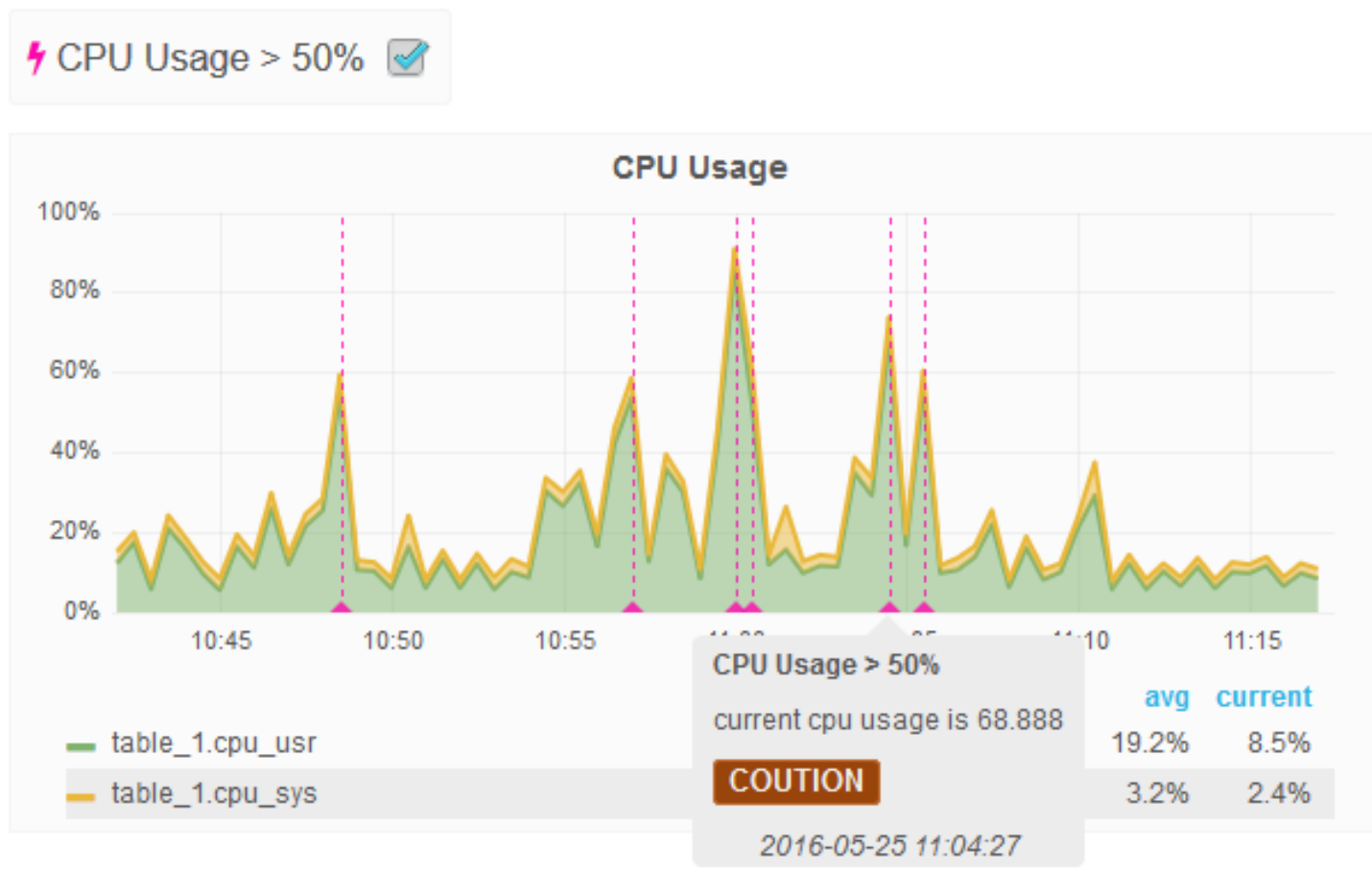
- World map
- Table(表)
- Singlestat

- +ゲージ表示 +SparkLine表示

- text html markdown
- Pieチャート



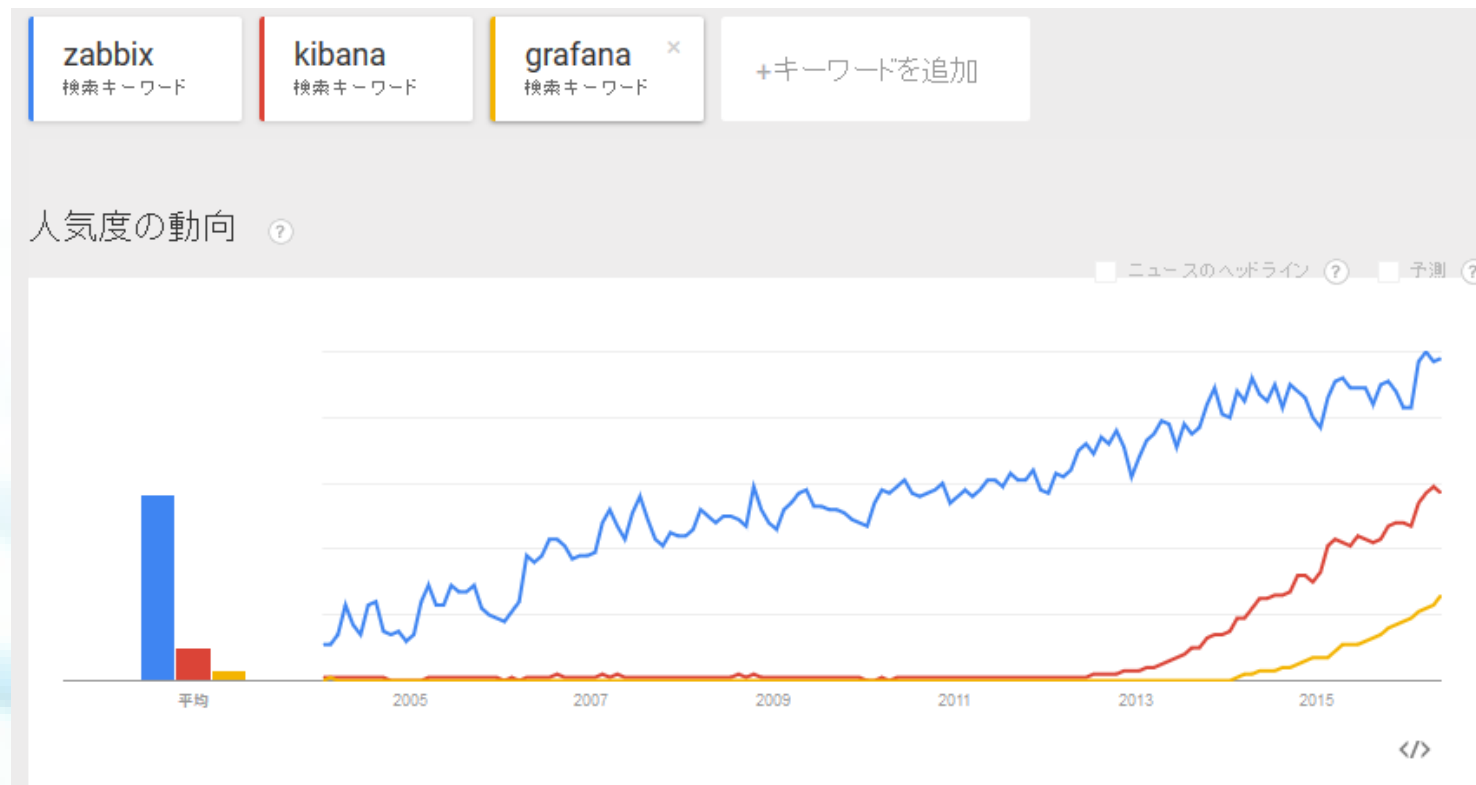




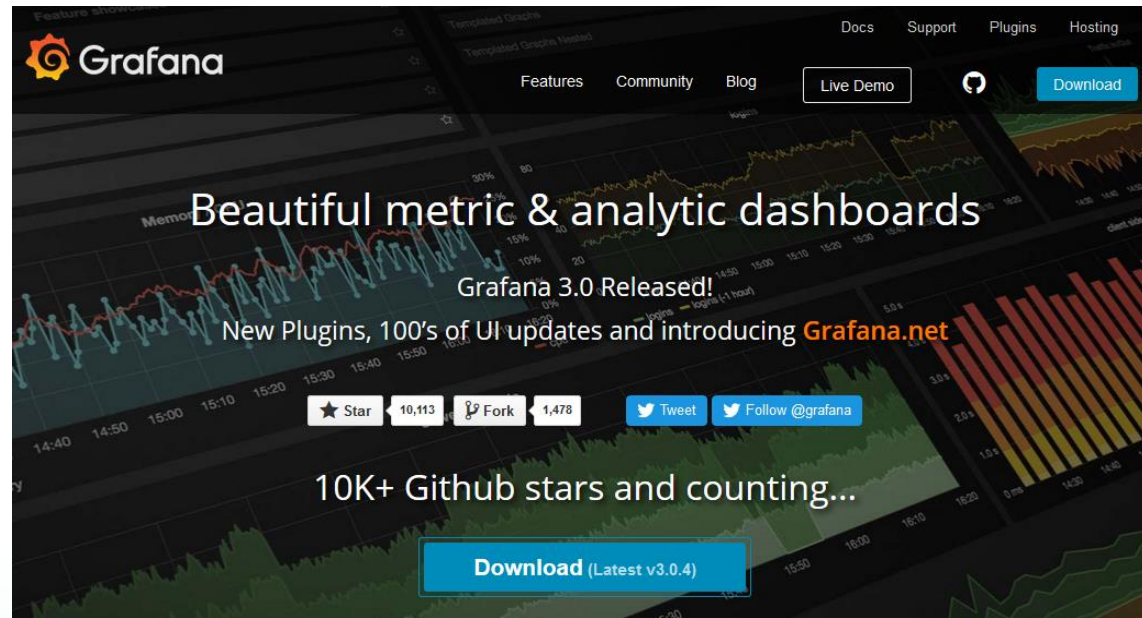
- データストアに入っているイベントを元にダッシュボード内のグラフに注釈として表示する機能

- ✓ テンプレート機能
  - 例) ホスト名だけを変更してダッシュボードの再利用
- ✓ mix データソース
  - 複数のデータソースから取得したデータを1枚のグラフへ描画
- ✓ 表示時間のスライドがキーボード(← →)で可能
  - 時間をスライドさせつつグラフの確認が容易
- ✓ シェア機能とスナップショット機能
  - チーム内で、同じ画面のシェア (URLで連絡)
  - 問題があったときのスナップショットの保管
- ✓ 組み込み機能
  - Grafanaで作成したグラフをHTMLから呼び出してグラフの再利用
- ✓ マルチテナント対応
  - 組織別ユーザ管理が可能

- エンジニアの注目度 Githubから2016/5/24の情報  
Watch数 604 ★Star数 10065 Fork数 1472  
(参考) kibana Watch数470 ★Star数 5356 Fork数 1997
- Googleトレンドによる人気度

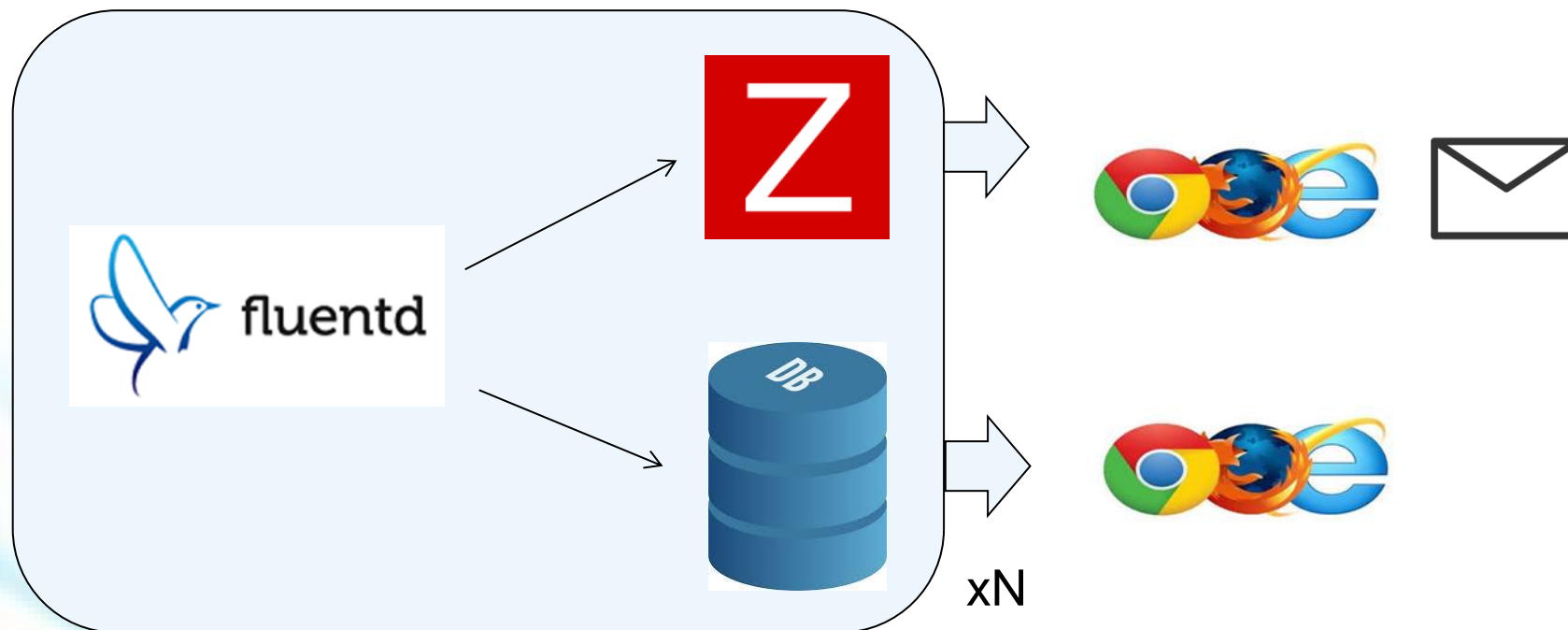


- 最新版のメジャーバージョン3.0が2016/5/11リリース



- 3.0からプラグイン仕様の整備とGrafana.netで誰でもプラグインを開発・公開できるようになった
  - 今後プラグイン開発が盛んになりそう...
- 3.0で入らなかった大きな機能
  - 通知機能

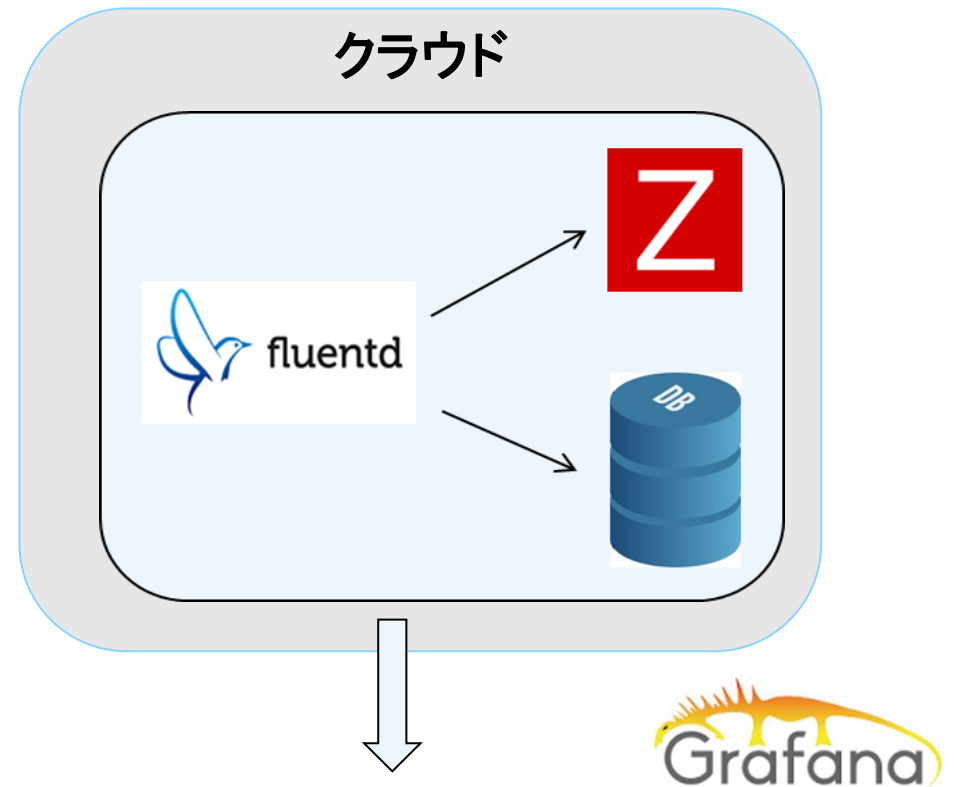
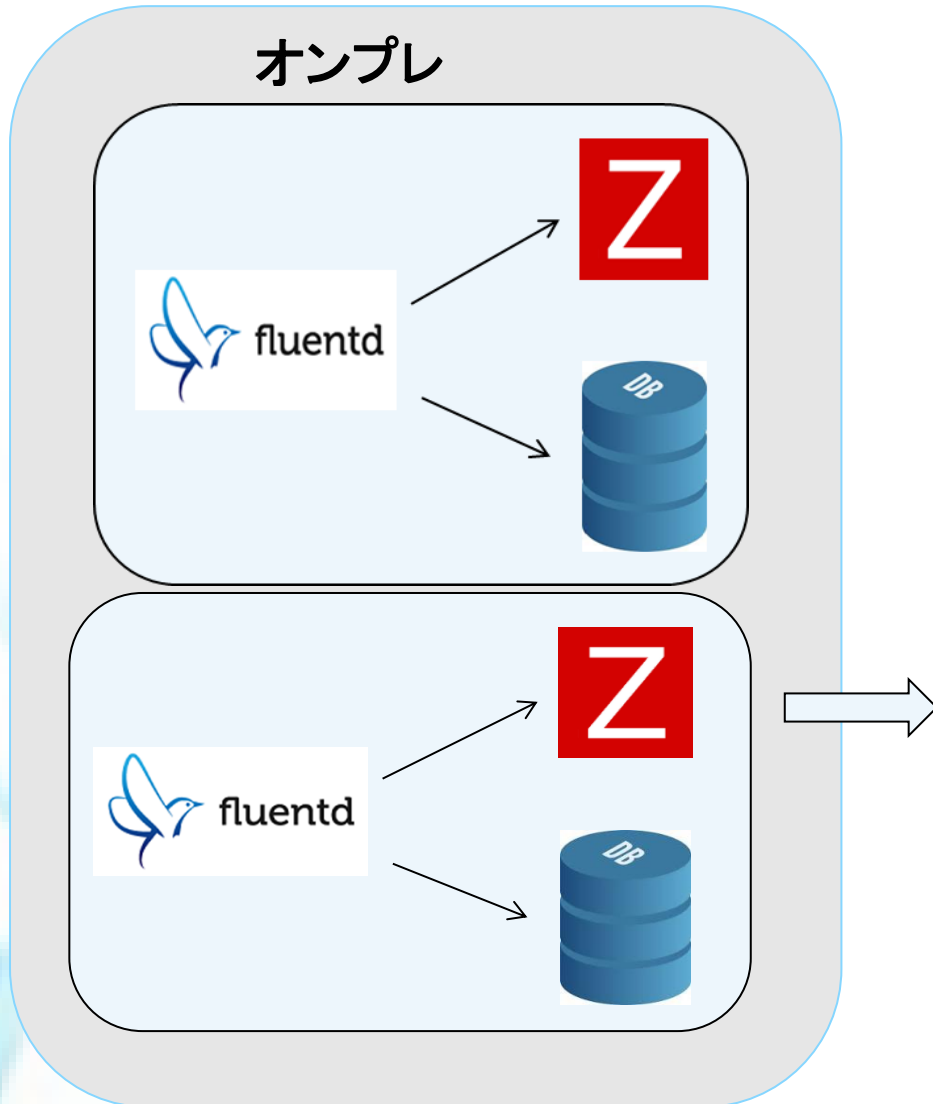
- ケース1
  - Fluentdを使ってログ収集
  - 問題があるログはZabbixに届けてZabbixから通知
  - 生ログはデータベースに格納して解析



- **利用者は管理画面を切り替えて運用**
- **管理者は管理画面ごとにユーザ設定**

# 管理画面の統合

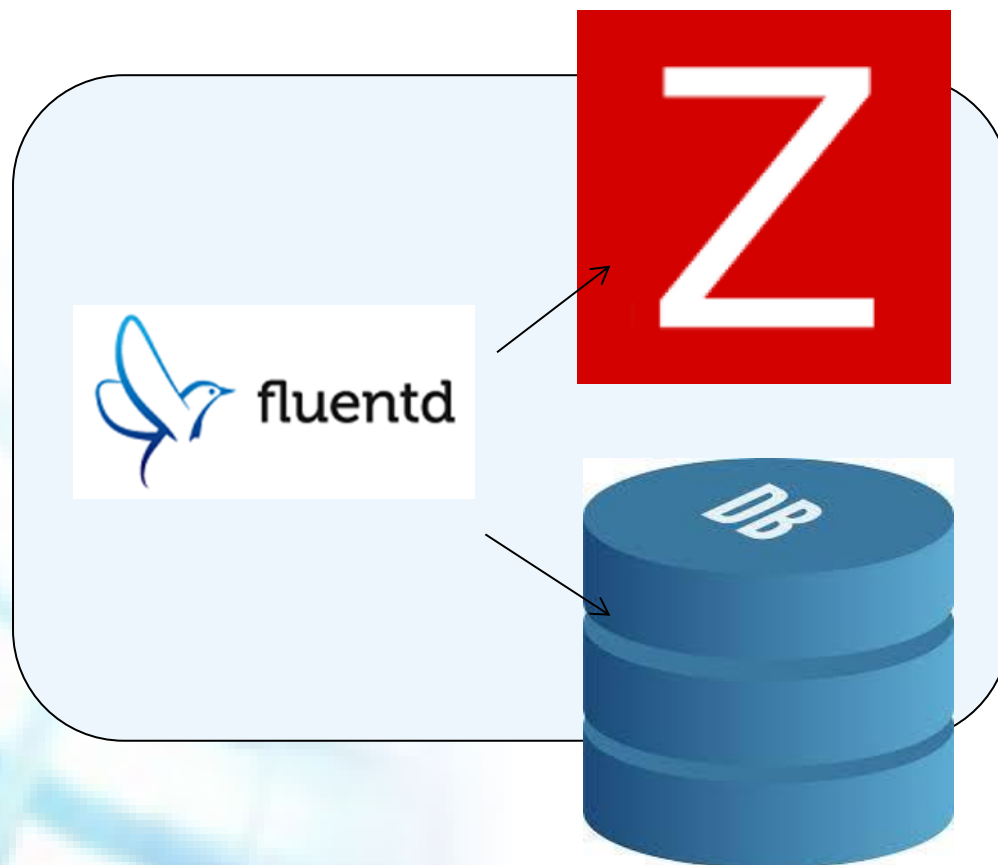
ユーザ情報を管理  
チーム内で問題発生時の情報を共有しやすく



## • ケース2

### 長期間運用すると

- FluentdもZabbixもデータの収集が得意  
DBの肥大化が問題

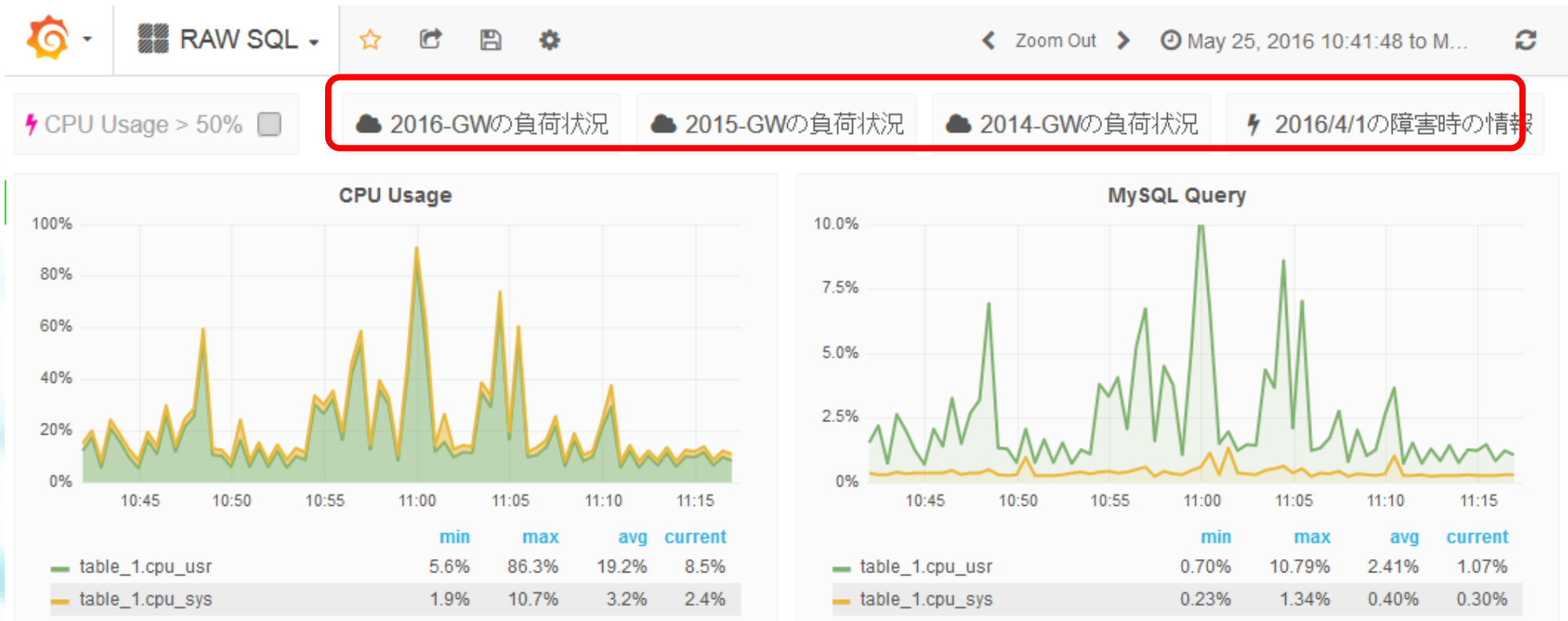


データは捨てたいけど  
重要なイベントのデータは  
残したい



は古いデータをDBから  
削除しても大切なデータ  
を残すことができる

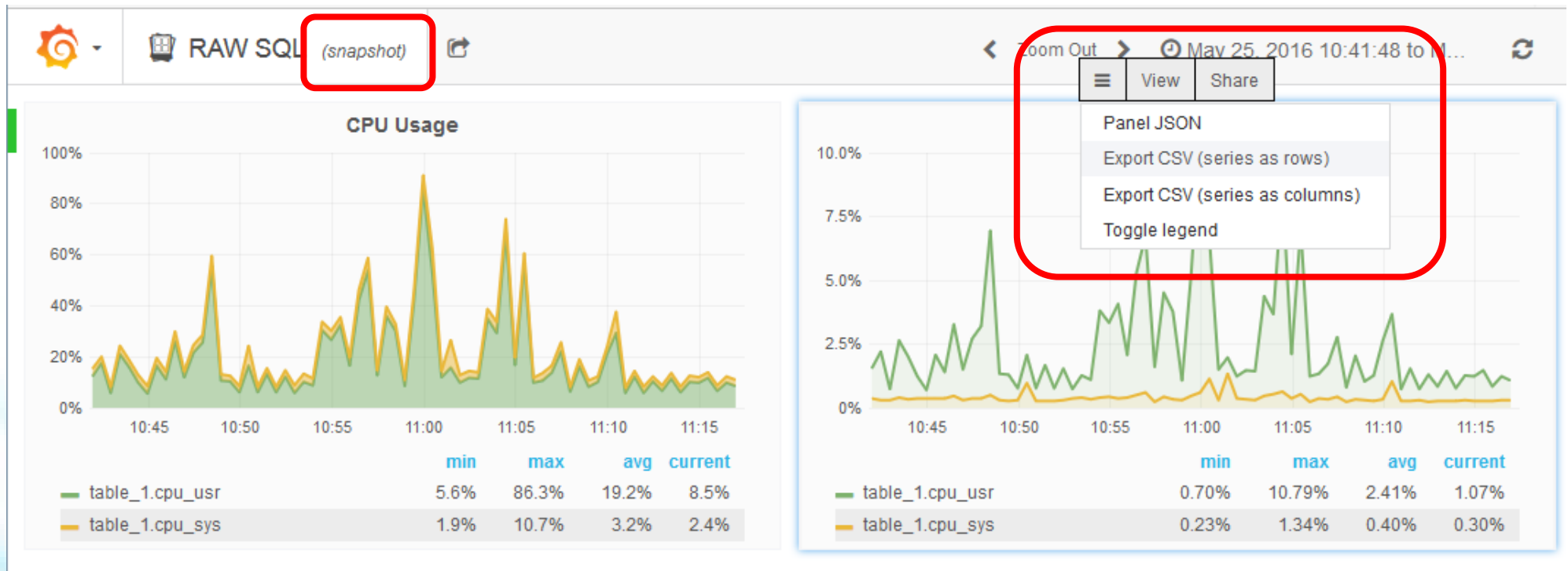
- スナップショット機能
  - ✓ 重要なイベントのダッシュボードをスナップショットとして Grafana の内部DBに保存できる
  - ✓ 保存したスナップショットをダッシュボードへリンク





- スナップショットから過去イベントを確認

↓ スナップショット

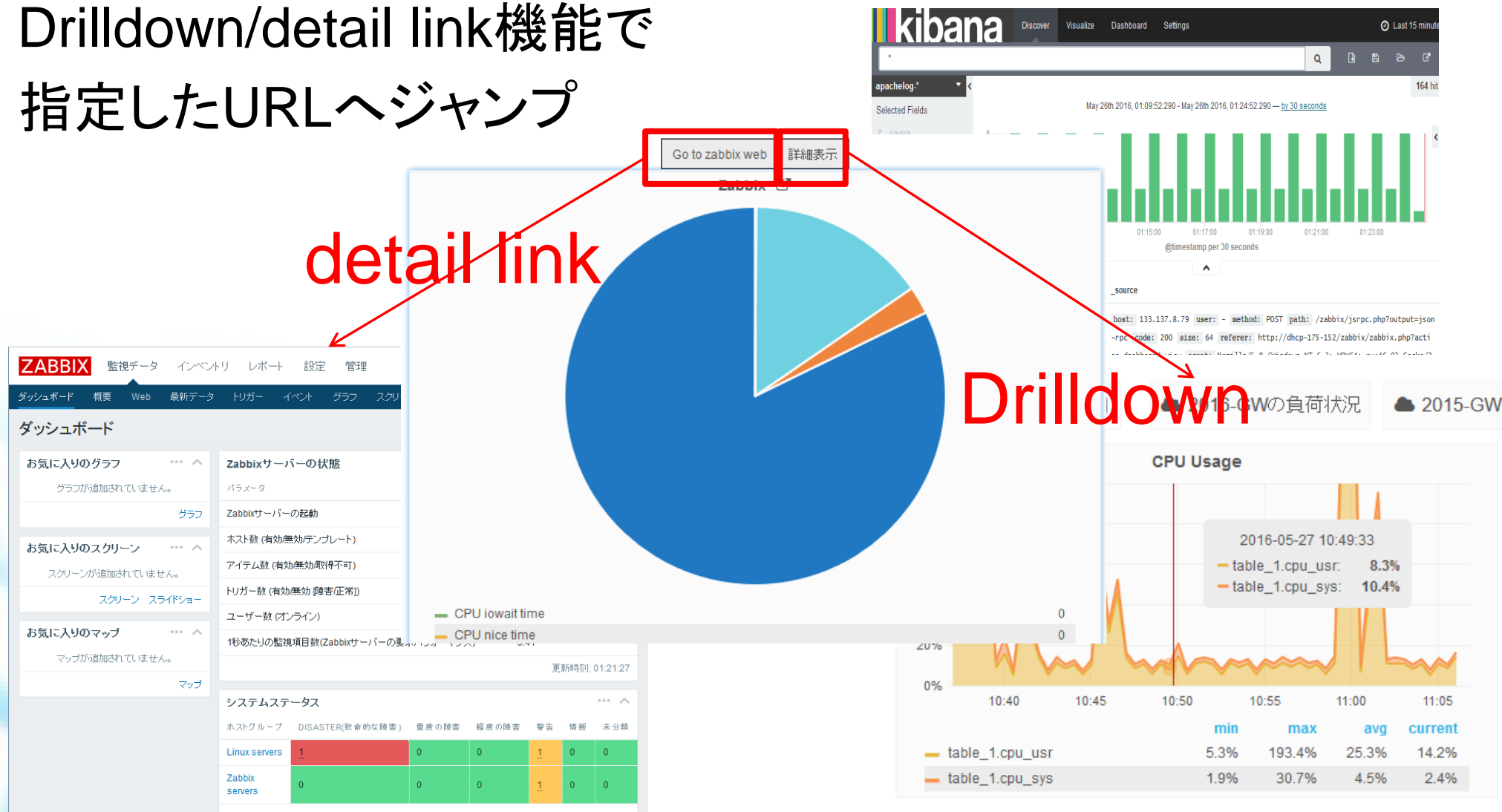


スナップショットからデータの  
CSVエクスポートも可能！

# ケース 3

専用のツール(例えばkibanaやZabbix)で深掘りしたいとき

Drilldown/detail link機能で  
指定したURLへジャンプ



**detail link**

**Drilldown**

Go to zabbix web 詳細表示

Zabbix

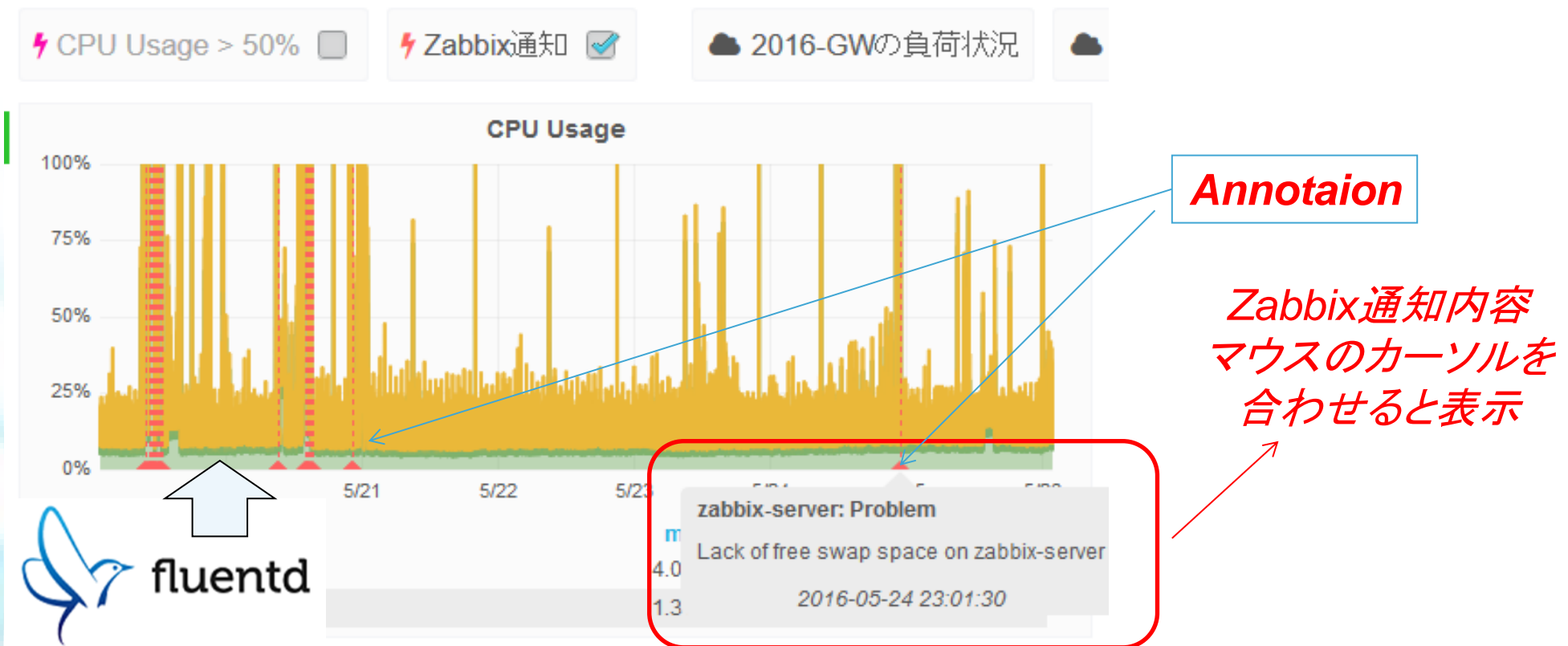
2016-05-27 10:49:33

	min	max	avg	current
table_1.cpu_usr	5.3%	193.4%	25.3%	14.2%
table_1.cpu_sys	1.9%	30.7%	4.5%	2.4%

## ケース4

Zabbixが障害を検知したときにFluentdで取得したデータと関連づけさせたい

GrafanaのAnnotation機能を使って問題の事象確認が迅速に!



- 現在GrafanaとFluentd共通で対応しているDB(データソース)
  - ✓ Graphite
  - ✓ ElasticSearch
  - ✓ InfluxDB
  - ✓ Zabbix
- RDBMSは?
  - アプリケーションや社内システムで利用しているDBはRDBMSなんだけど解析にGrafanaは使えないの？
  - MySQLやPostgreSQLなら知っているけど、新しいDBの導入・運用の敷居は高い・・・
- GrafanaコミュニティでもRDBMS対応の要望が多い

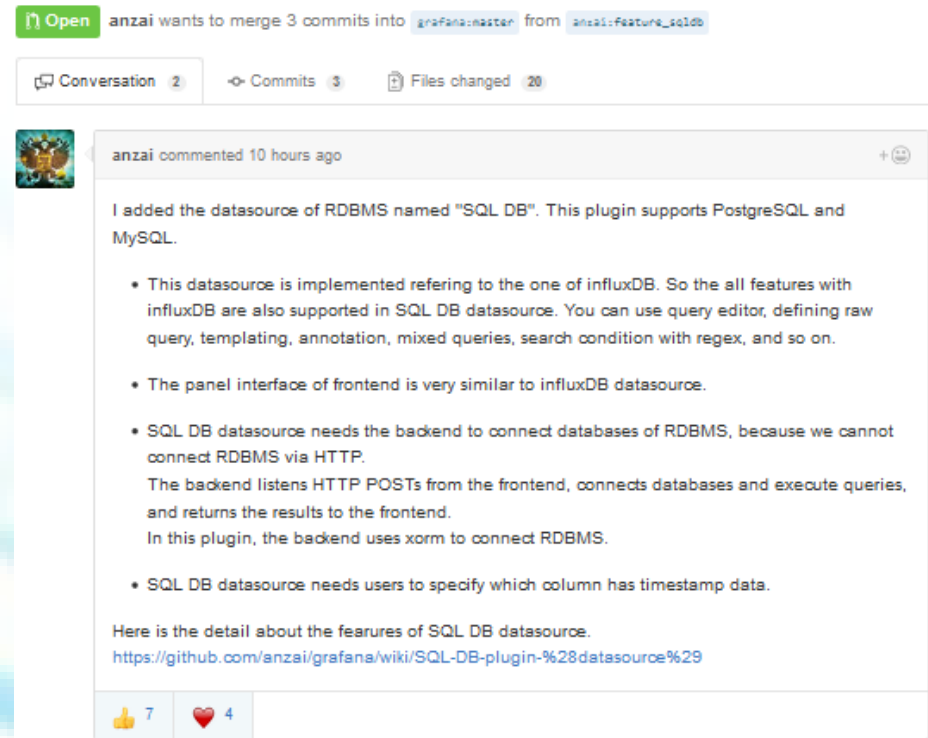
ということで

- MySQLとPostgreSQL対応プラグインを作ってみました
- 状況

githubにpullリクエストを出したところ(2016/5/25)

<https://github.com/grafana/grafana/pull/5168>

Add the datasource of RDBMS (PostgreSQL and MySQL)  
#5168



Open anzai wants to merge 3 commits into grafana:master from anzai:feature\_sqlDB

Conversation 2 Commits 3 Files changed 20

anzai commented 10 hours ago

I added the datasource of RDBMS named "SQL DB". This plugin supports PostgreSQL and MySQL.

- This datasource is implemented referring to the one of influxDB. So the all features with influxDB are also supported in SQL DB datasource. You can use query editor, defining raw query, templating, annotation, mixed queries, search condition with regex, and so on.
- The panel interface of frontend is very similar to influxDB datasource.
- SQL DB datasource needs the backend to connect databases of RDBMS, because we cannot connect RDBMS via HTTP. The backend listens HTTP POSTs from the frontend, connects databases and execute queries, and returns the results to the frontend. In this plugin, the backend uses xorm to connect RDBMS.
- SQL DB datasource needs users to specify which column has timestamp data.

Here is the detail about the features of SQL DB datasource.  
<https://github.com/anzai/grafana/wiki/SQL-DB-plugin-%28datasource%29>

7 4



