Fluentd + Zabbix + Grafana で グラフィカルなログ監視・分析システムを構築してみよう！

2016年7月29日

SRA OSS, Inc. 日本支社
マーケティング部 OSS技術グループ

アジェンダ

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

Fluentd について

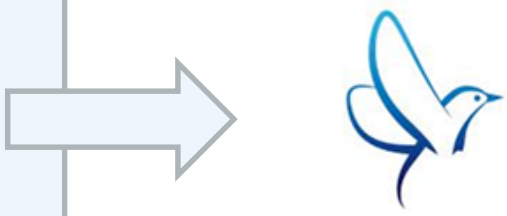
- Fluentd
  - ログを取得して転送してくれるミドルウェア
  - ログの加工や構造化ができる
  - いろんなデータベースにデータを保存できる
- URL

  http://fluentd.org/
- 開発
  - 米国Treasure Data社の開発者
  - コミュニティベース
  - 言語：Ruby + C言語
- ライセンス
  - Apache License Version 2.0

イメージ

データ入力：Input

アプリケーションのログ
Webサーバのログ
データベースのログ
Syslog
http入力
Unixドメインソケット入力
コマンド実行結果



フィルタ・バッファ・ルーティング

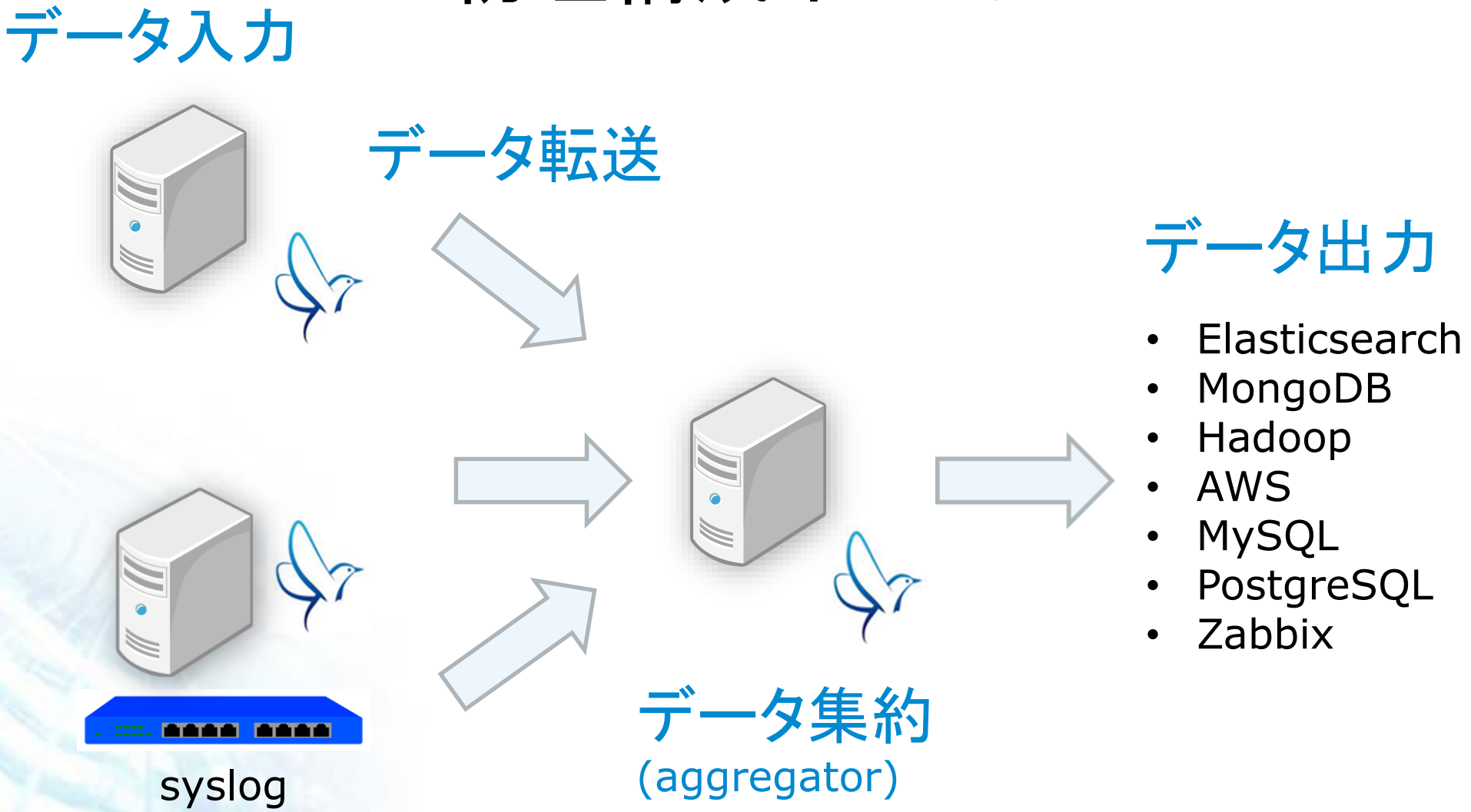
データ出力：Output

DB

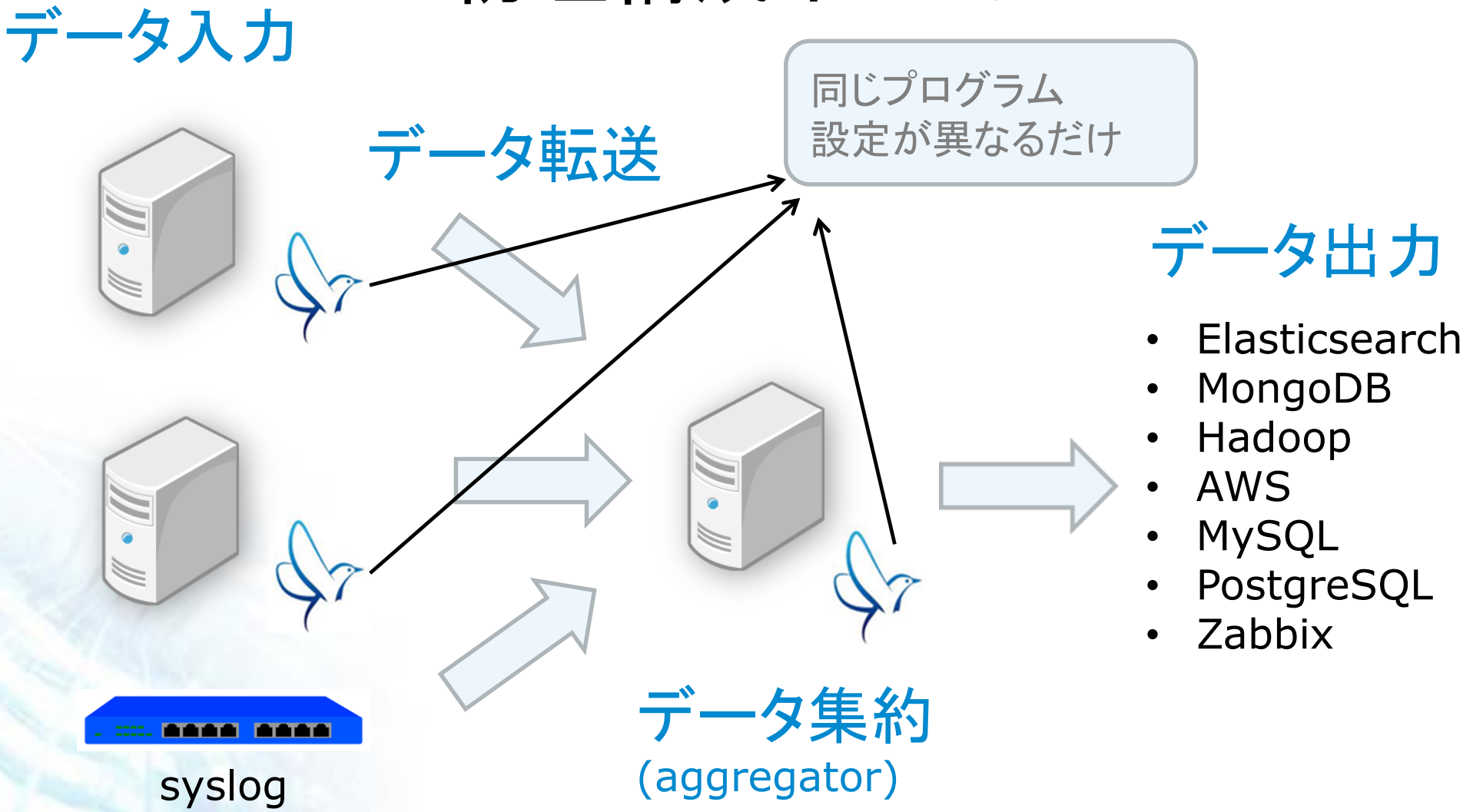
ファイル

コマンド

物理構成イメージ



物理構成イメージ

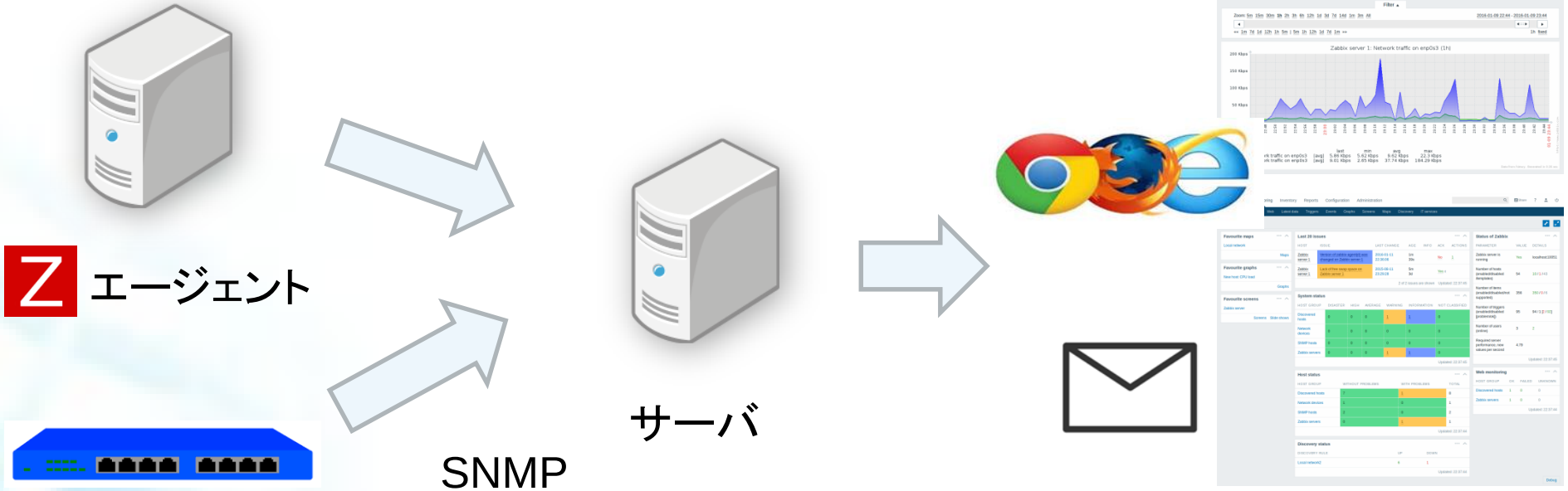


Zabbixについて

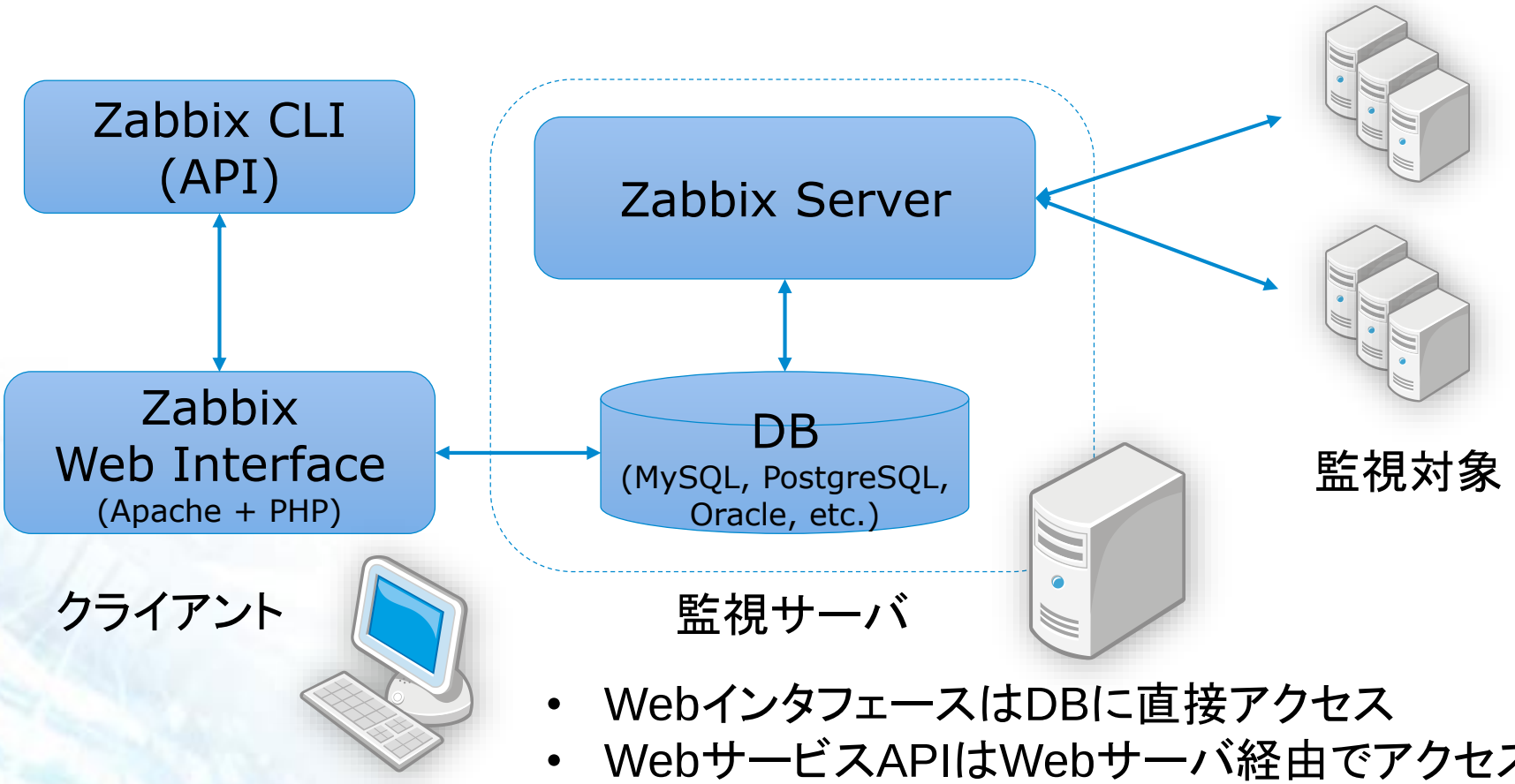
- Zabbix

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

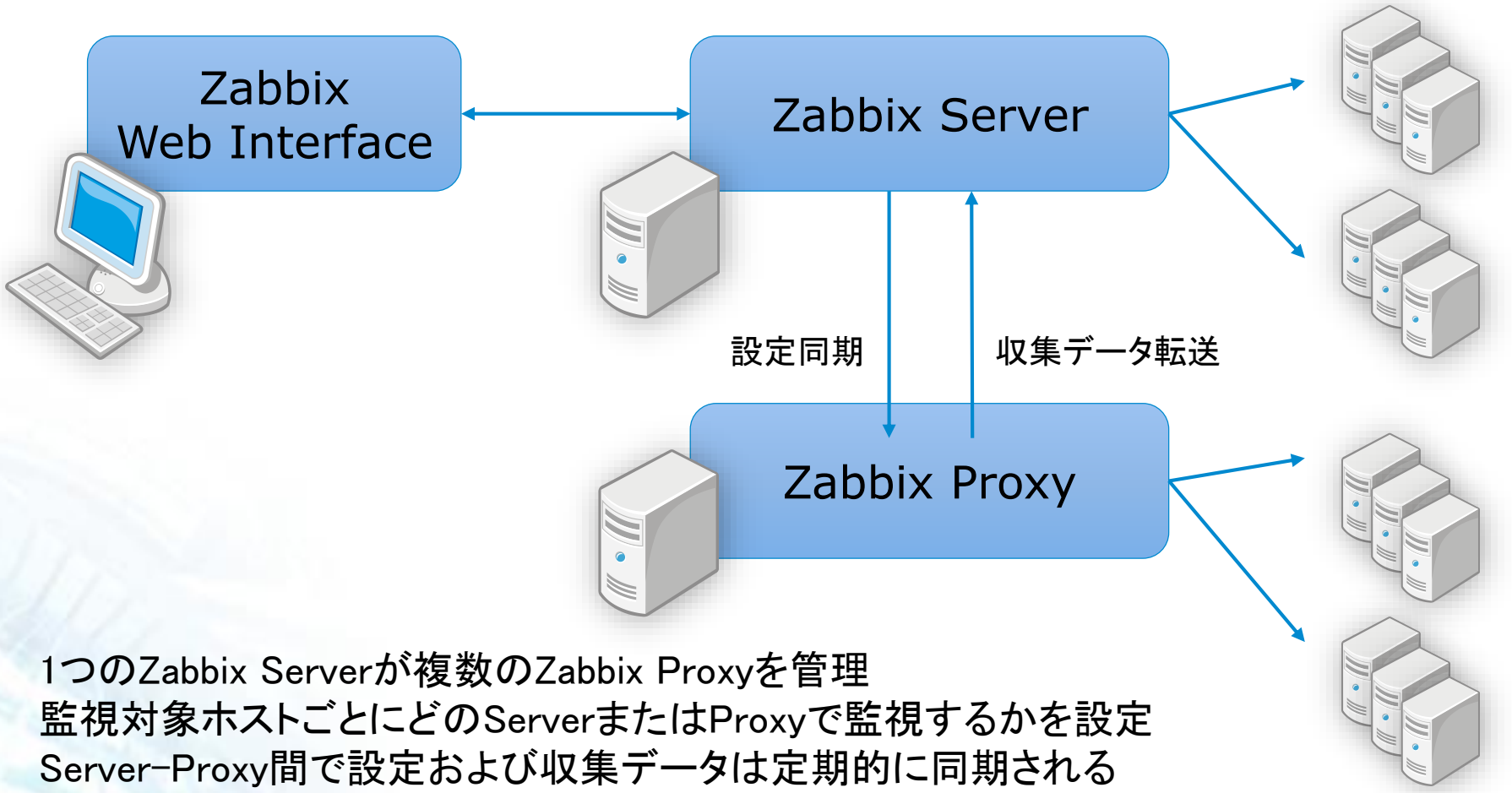


Zabbixのアーキテクチャ



- WebインタフェースはDBに直接アクセス
- WebサービスAPIはWebサーバ経由でアクセス
- インタフェースと監視サーバで処理を分散するアーキテクチャ

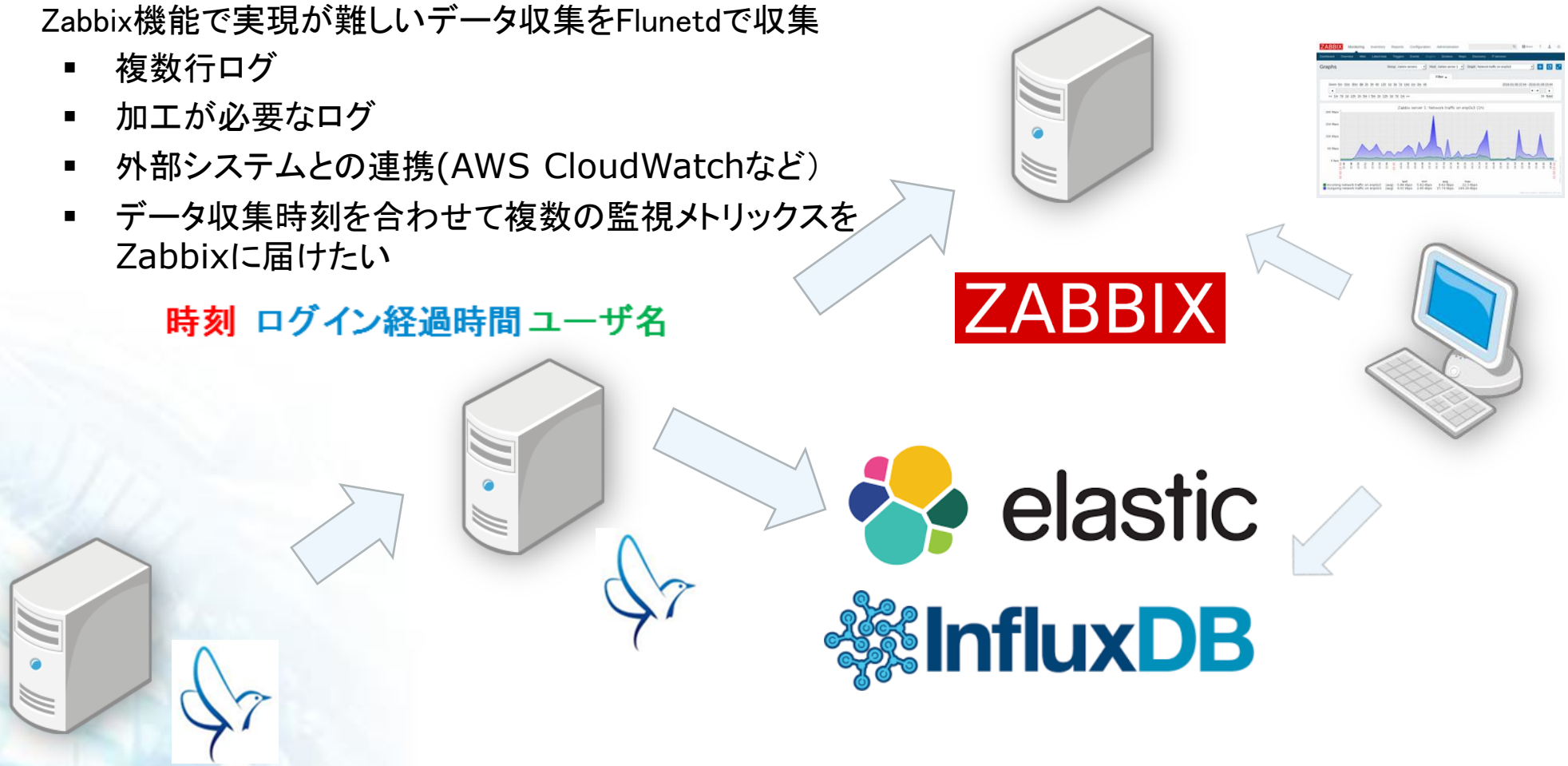
Zabbix 分散監視



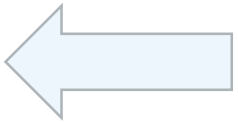
- 1つのZabbix Serverが複数のZabbix Proxyを管理
- 監視対象ホストごとにどのServerまたはProxyで監視するかを設定
- Server-Proxy間で設定および収集データは定期的に同期される
- Zabbix Serverがボトルネックになるケースもあり、Serverを複数台使うケースもある

FluentdとZabbixを一緒に

- Flunetdで収集したデータから問題があればZabbixへ通知
- Zabbix機能で実現が難しいデータ収集をFlunetdで収集
  - 複数行ログ
  - 加工が必要なログ
  - 外部システムとの連携(AWS CloudWatchなど)
  - データ収集時刻を合わせて複数の監視メトリックスをZabbixに届けたい



ツールを使い分ける ？



ZABBIX

elastic

InfluxDB

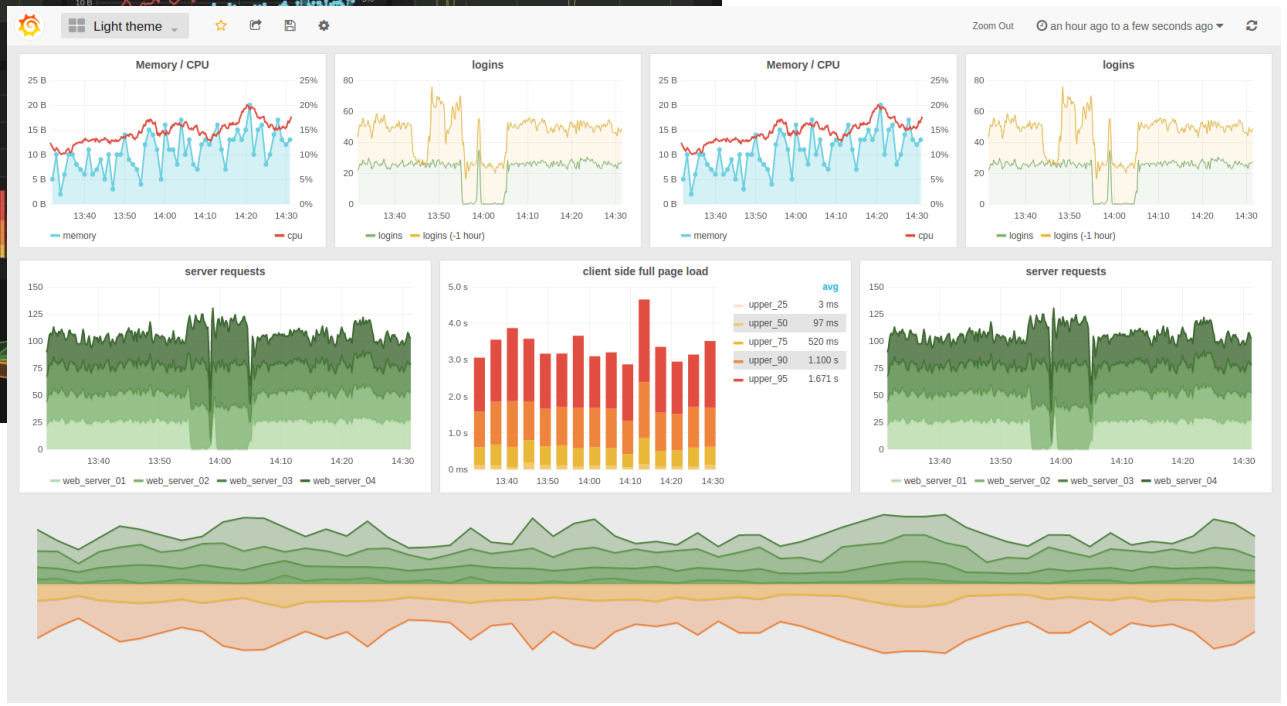
amazon web services CloudWatch

ここで

Grafana

Grafanaとは

- 複数のいろんな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



基本的な特徴　データソース

- 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
- ✓ Elasticsearch
- ✓ Amazon Cloud Watch
- ✓ Bosun
- ✓ Heroic
- ✓ InfluxDB
- ✓ OpenTSDB
- ✓ Zabbix
- ✓ Prometheos
- ✓ 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

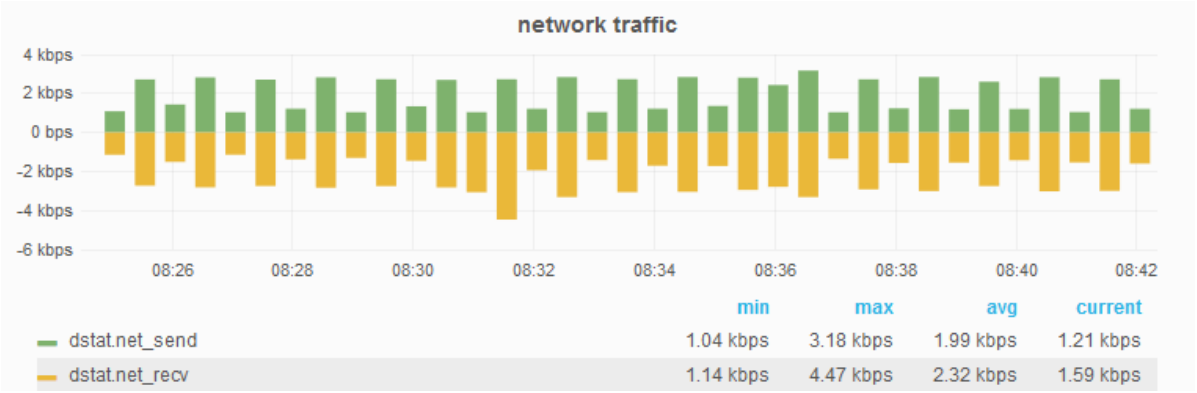
  → SQLite(デフォルト), PostgreSQL MySQL

基本的な特徴　構成

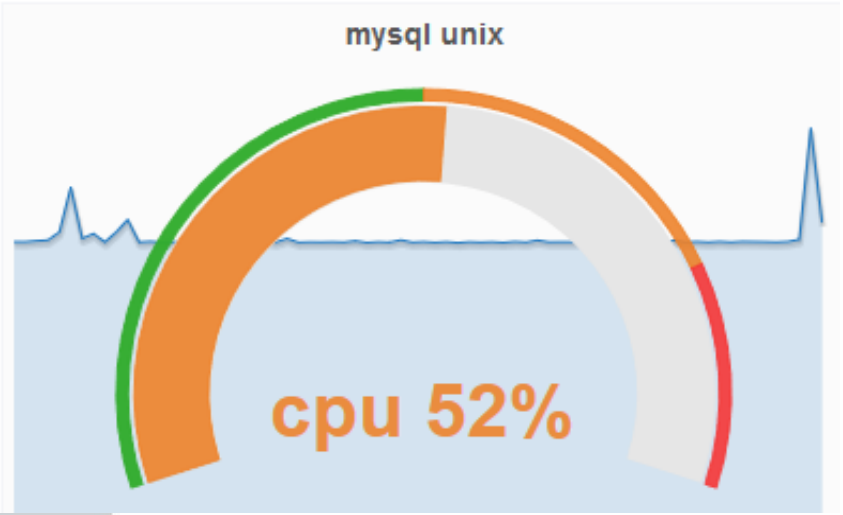
- JavaScriptのフロントエンド(ブラウザ)とGo言語で書かれたバックエンド構成
- ブラウザから直接データソースにアクセスするDirectモードとバックエンド経由でデータソースにアクセスするproxyモードの選択ができる

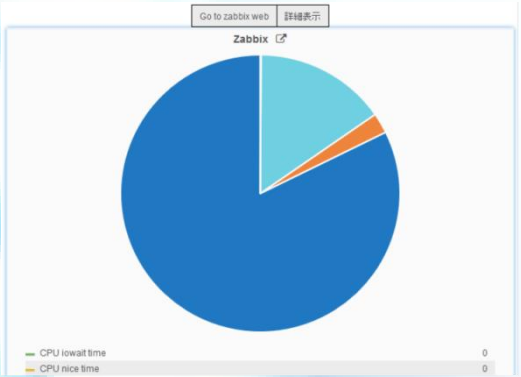
基本的な特徴　描画機能

- 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)

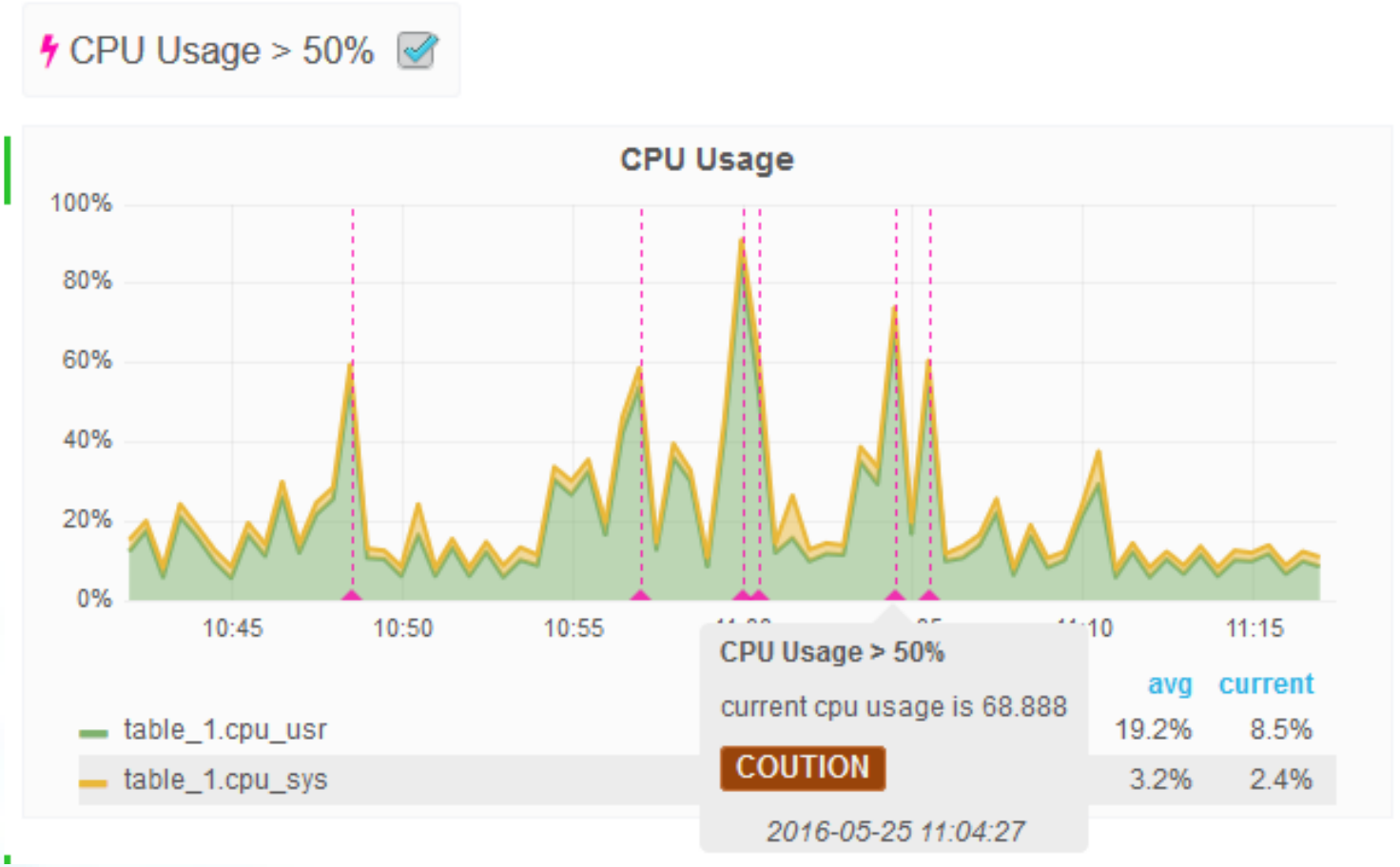


- World map
- Table(表)
- Singlestat
  - +ゲージ表示　+SparkLine表示
- text html markdown
- Pieチャート





基本的な特徴　Annotation機能



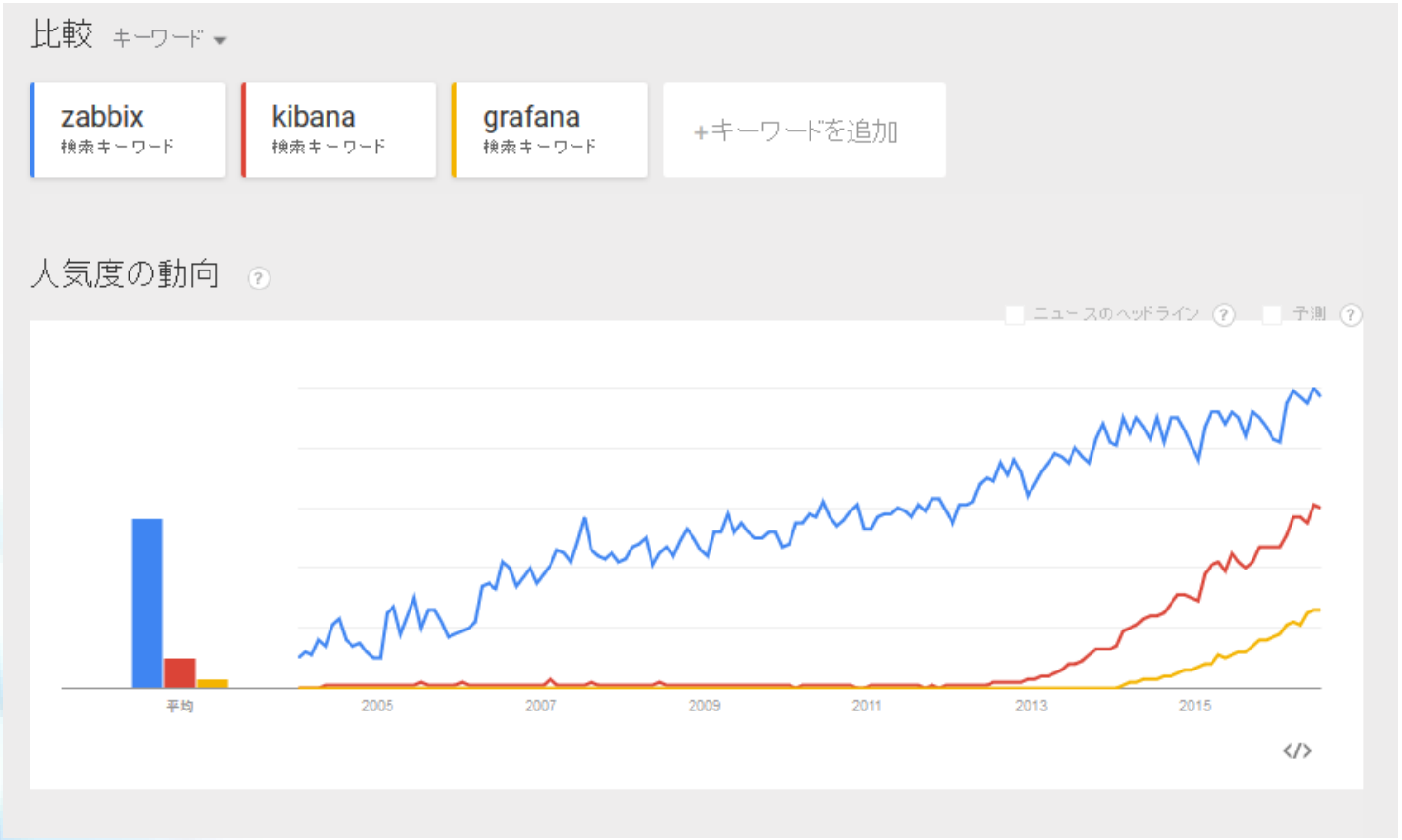
- データストアに入っているイベントを元にダッシュボード内のグラフに注釈として表示する機能

特徴　その他機能

- ✓ 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
- ✓ Repeat Panel
  - テンプレート変数を使って変数を変えたパネル(グラフ)を繰り返し設定
- ✓ 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

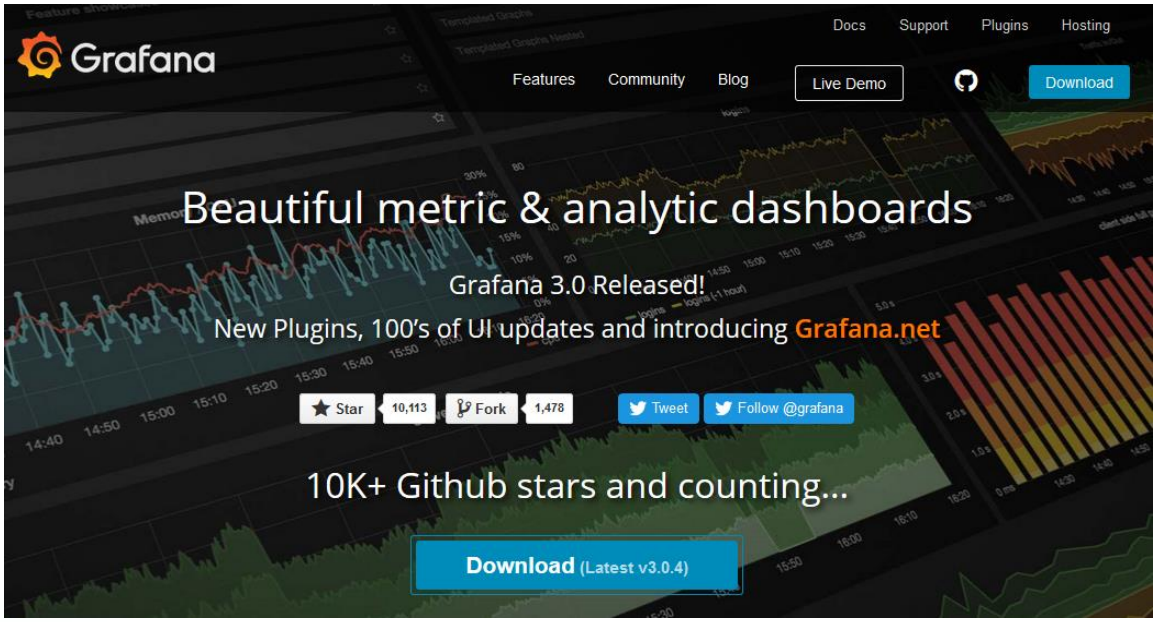
注目度と人気度?

- エンジニアの注目度　Githubから2016/7/26の情報
  Watch数 648 ★Star数 10969　Fork数 1642
  (参考)　kibana　Watch数485　★Star数　5694 Fork数　2095
- Googleトレンドによる人気度



Grafana 3.0 リリース

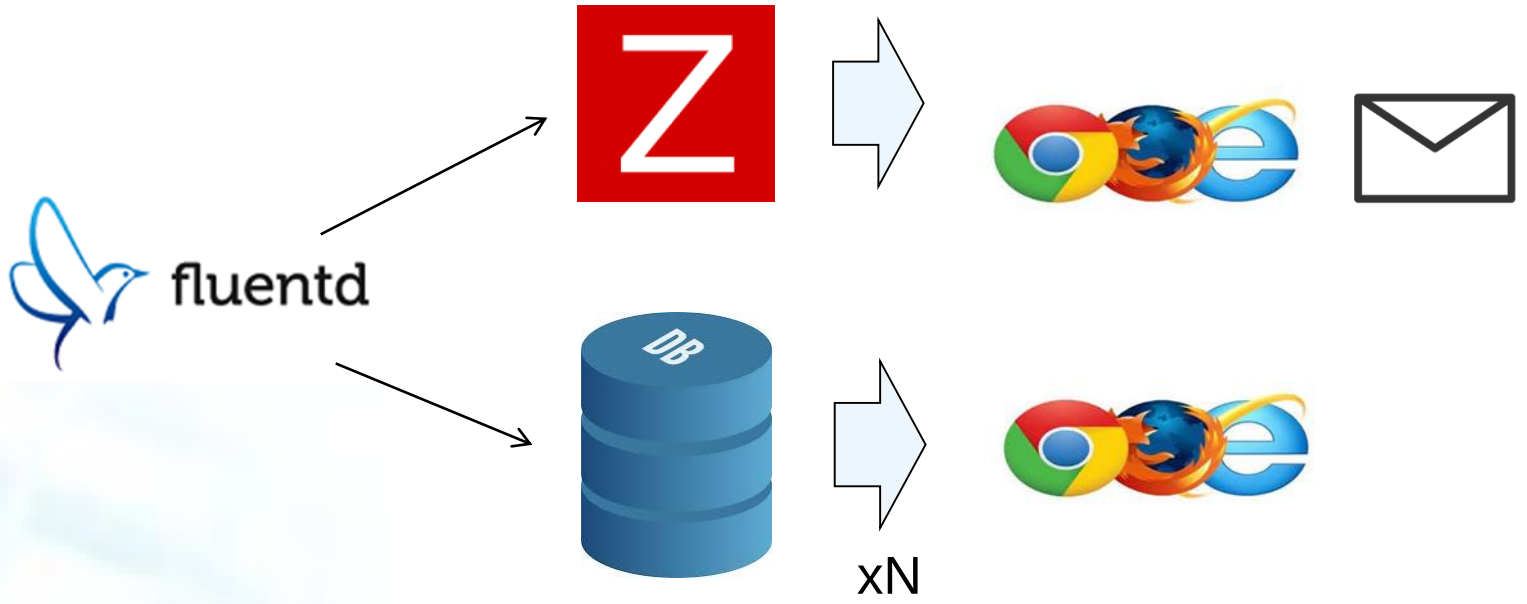
- 最新版のメジャーバージョン3.0が2016/5/11リリース



- 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（4.0で入る予定　10月末ごろ? ）

Fluentd+Zabbix+Grafana 構成の利点

- 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

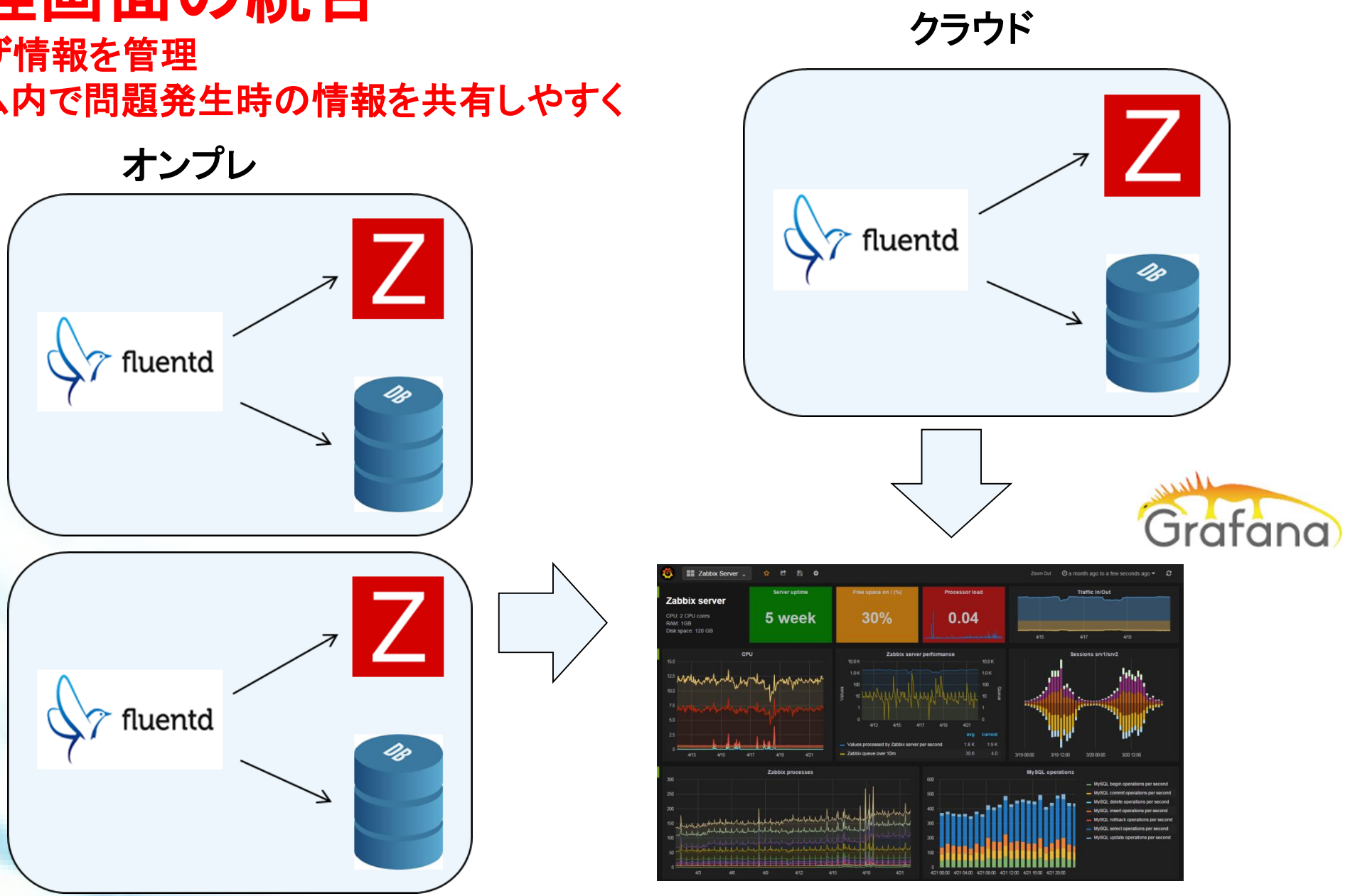


- **利用者は管理画面を切り替えて運用**
- **管理者は管理画面ごとにユーザ設定**

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

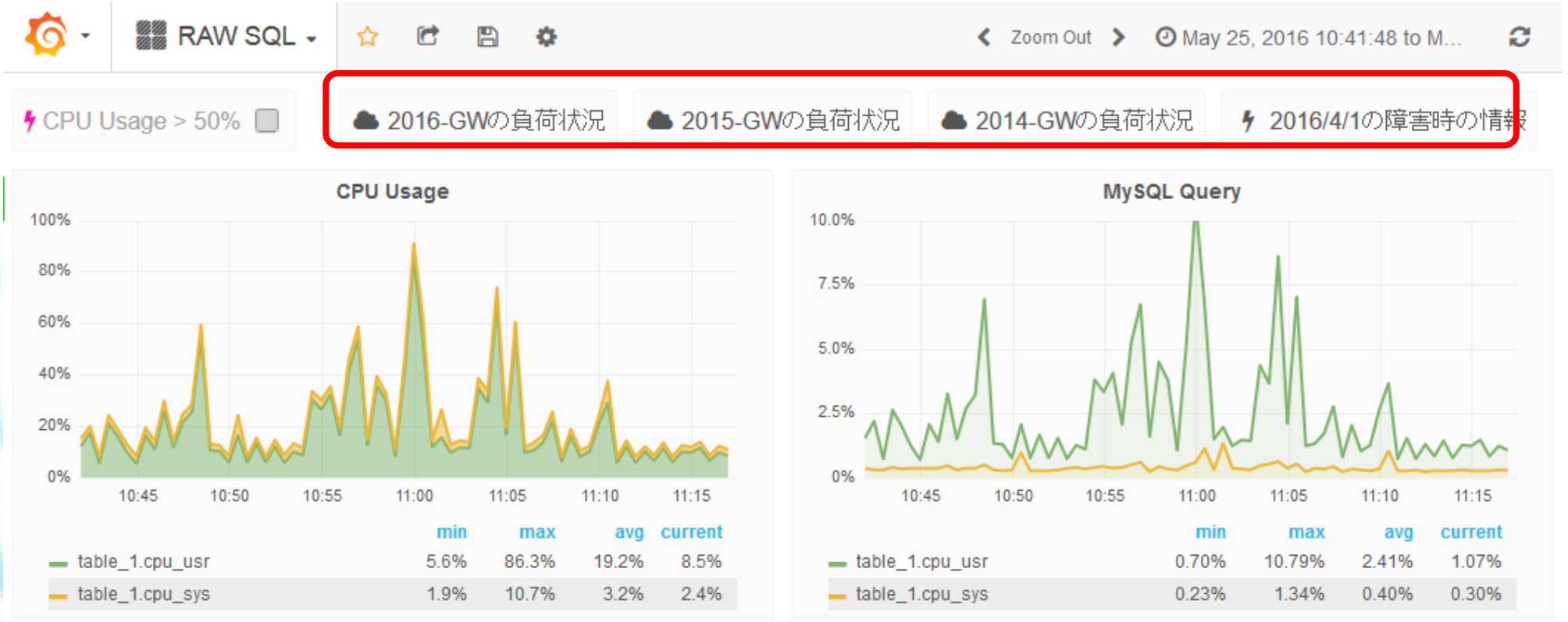
  - FluentdもZabbixもデータの取集が得意
    DBの肥大化が問題

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

Grafana

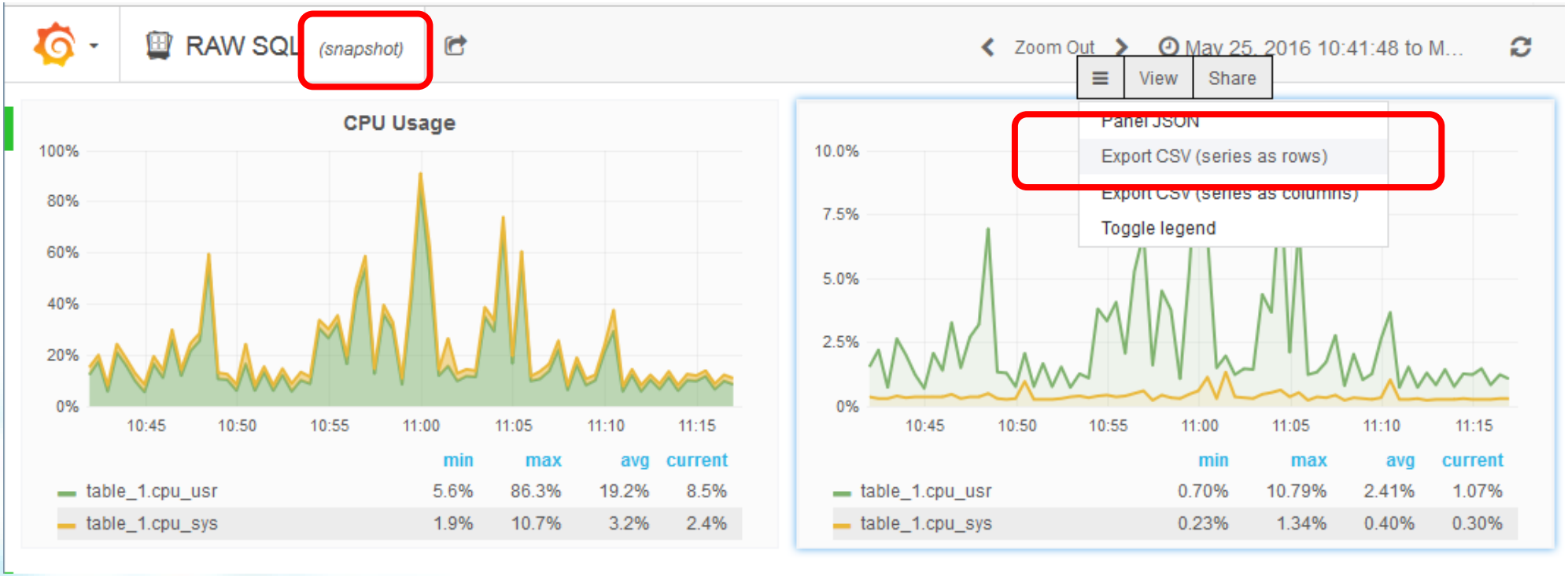
は古いデータをDBから
削除しても大切なデータ
を残すことができる

- 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



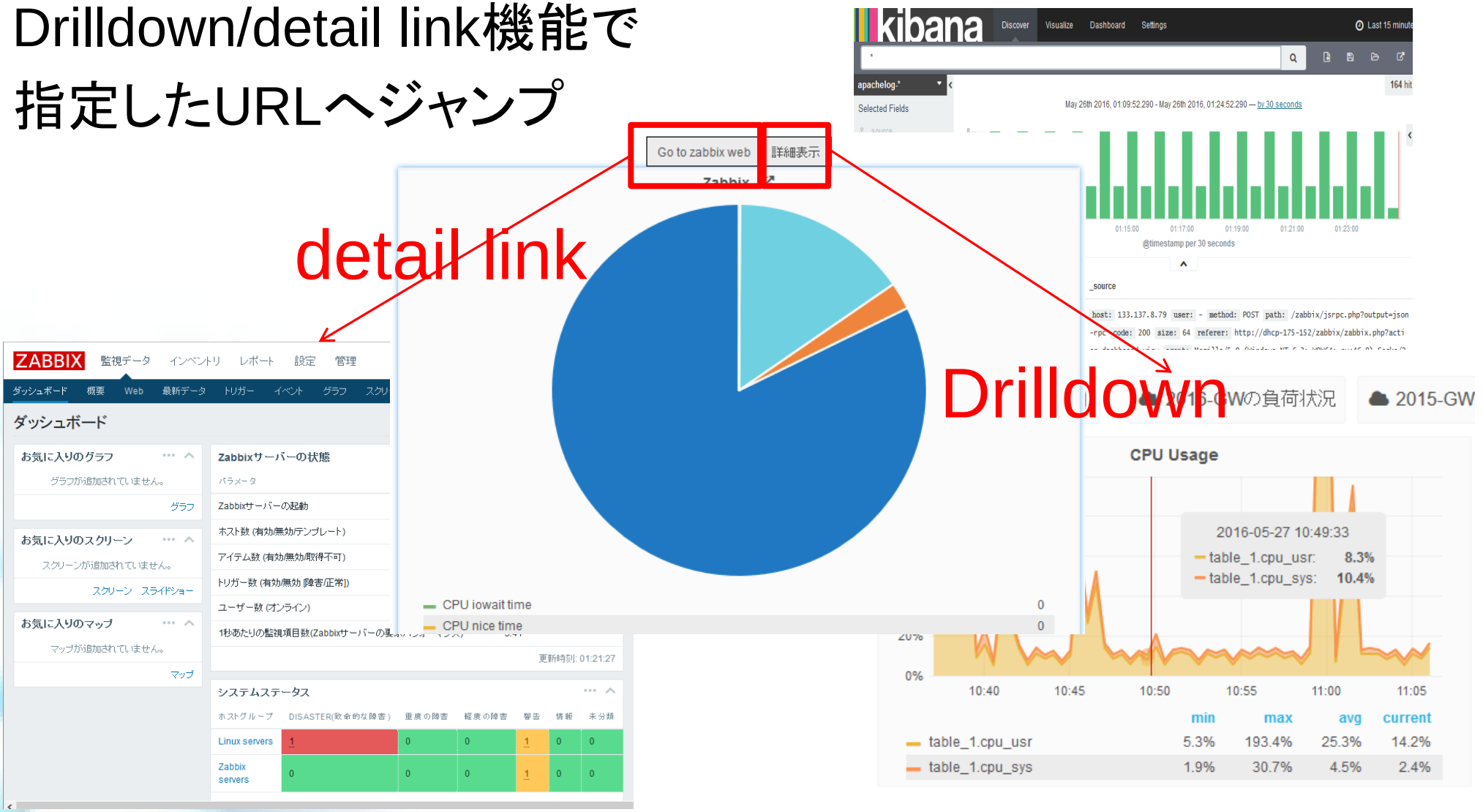
スナップショットからデータの
CSVエクスポートも可能！

- 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

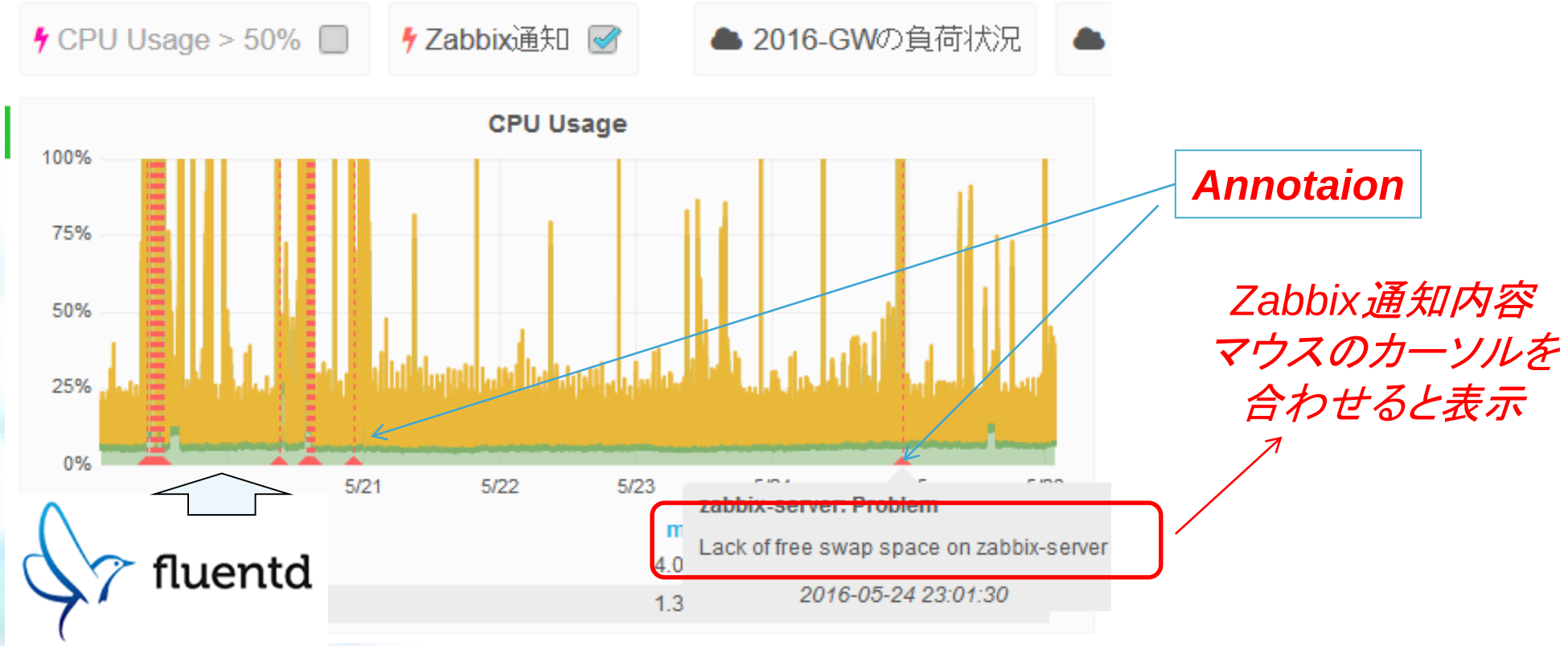
指定したURLへジャンプ



- ケース4

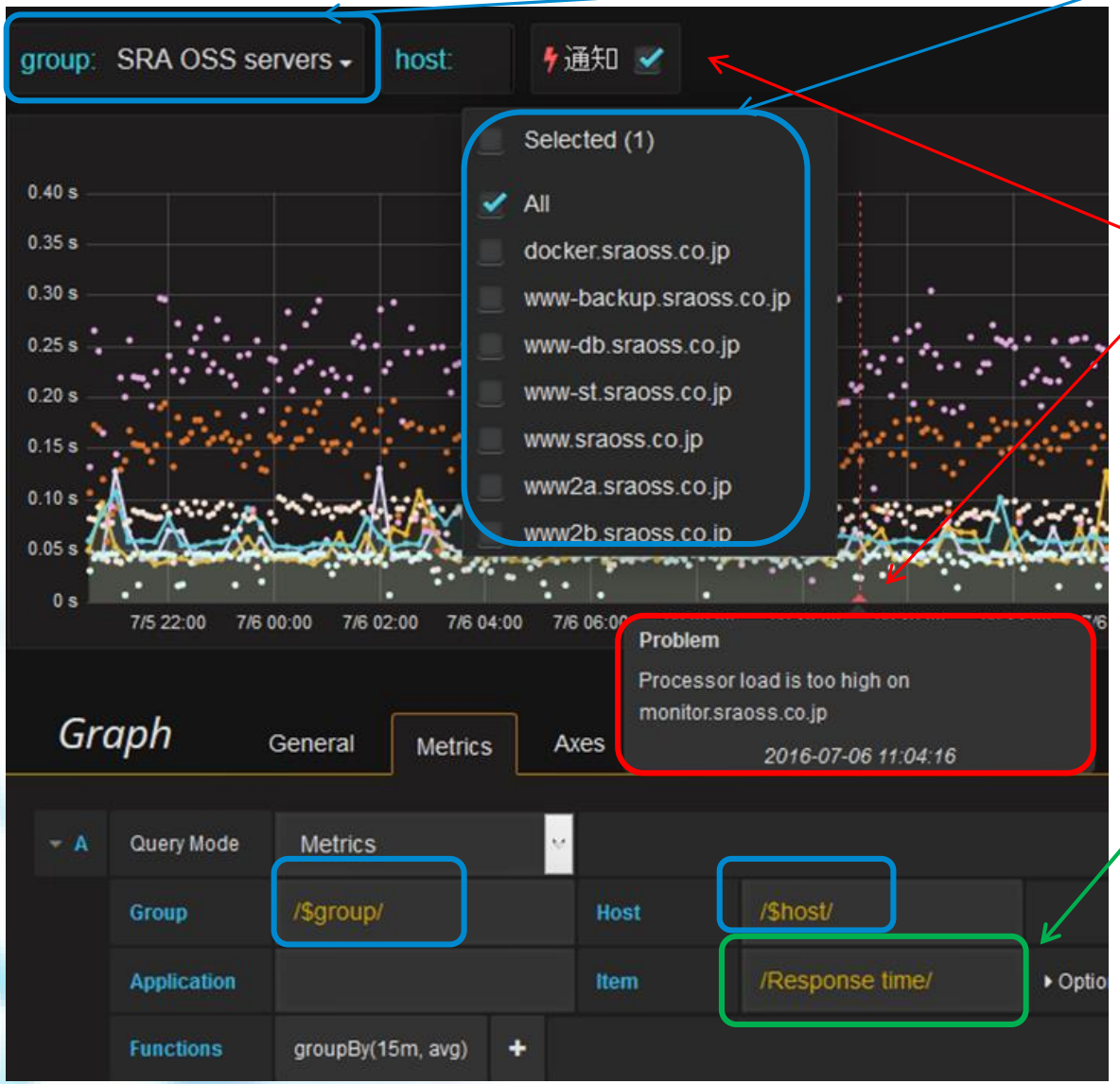
Zabbixが障害を検知したときにFluentdで取得したデータと関連づけさせたい

GrafanaのAnnotaion機能を使って問題の事象確認が迅速に!



おまけ

- Zabbixの利用例



Template機能
グループの取得・表示
ホストの取得・表示

Anotation機能
Zabbixの通知を
グラフに表示

Zabbixデータソース機能
Item名の部分一致で
まとめてデータの取得・表示

データソースとDBについて

- 現在GrafanaとFluentd共通で対応しているDB(データソース)

✓ Graphite
✓ Elasticsearch
✓ Prometheus
✓ 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

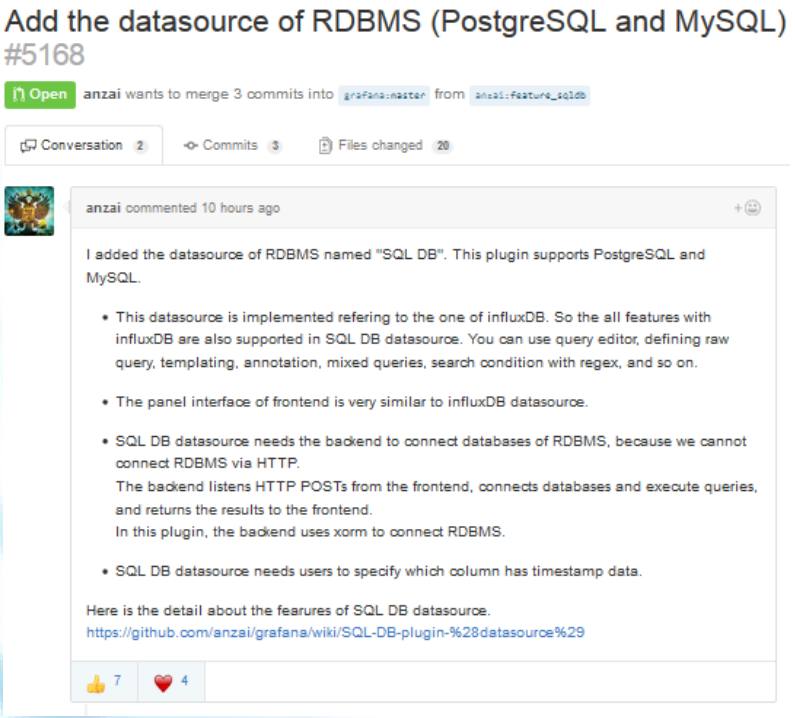
SRA OSSのGrafanaの取り組み

- 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/5364

  https://github.com/sraoss/grafana-sqldb-datasource



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.

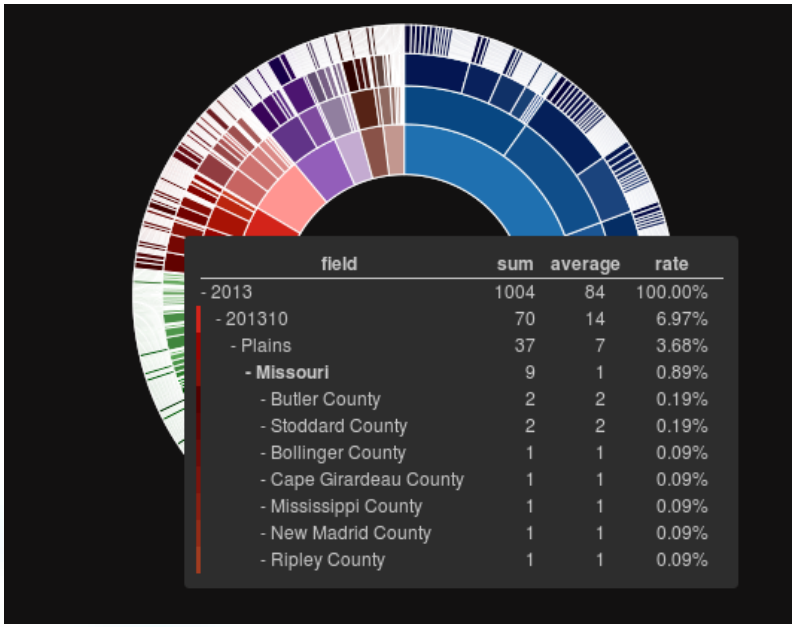
- This datasource is implemented refering to the one of influxDB. So the all features with influxDB are also supported in SQL DB datasource. You can use query editor, defining raw query, templating, annotation, mixed queries, search condition with regex, and so on.
- The panel interface of frontend is 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 fearures of SQL DB datasource.
https://github.com/anzai/grafana/wiki/SQL-DB-plugin-%28datasource%29

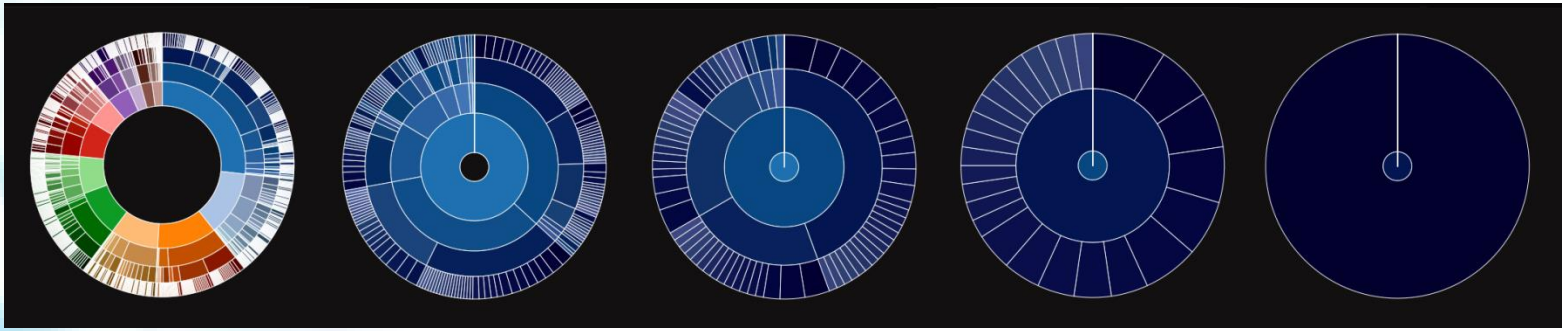
7 4

- Sunburstパネルプラグインを作りました

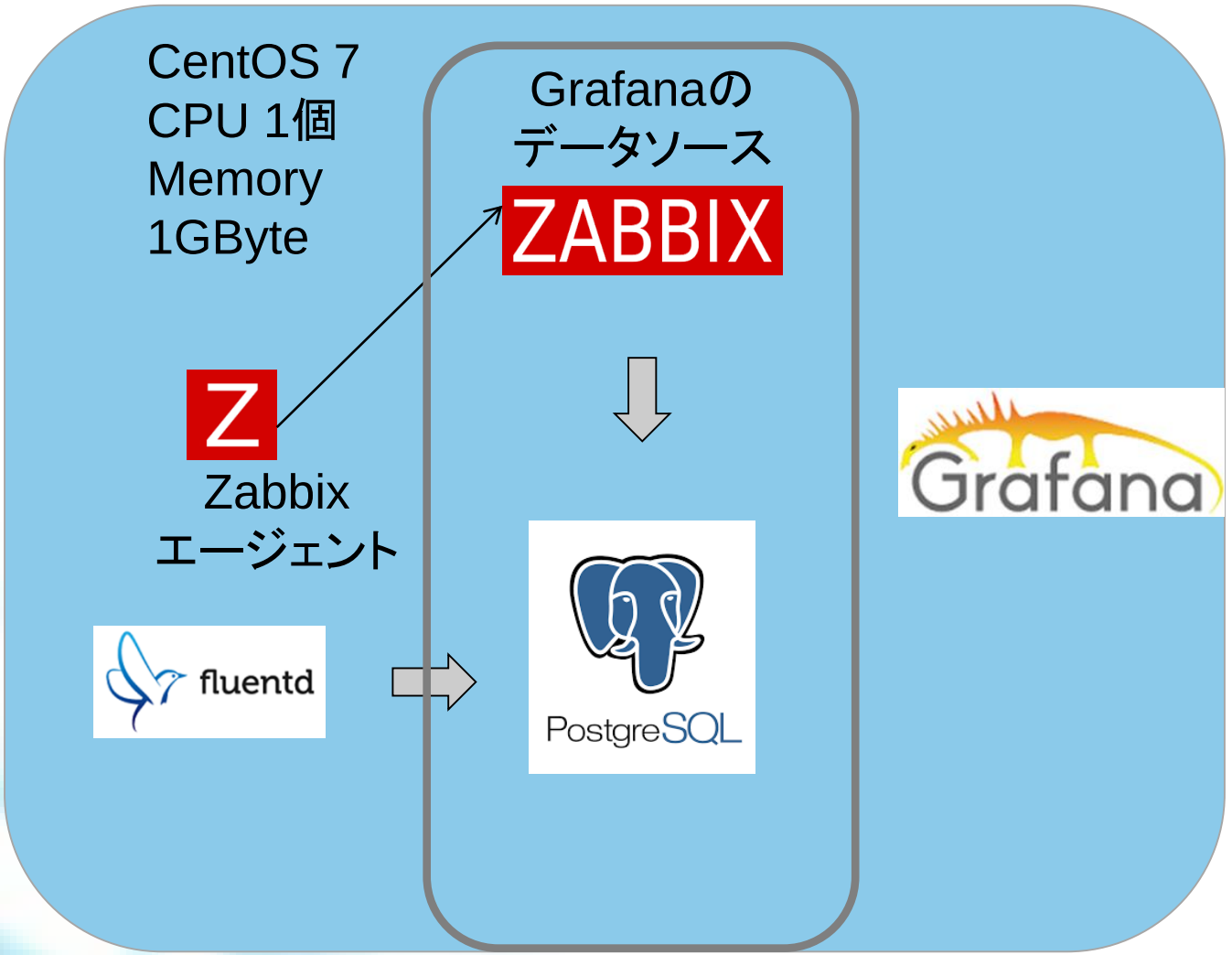
  https://github.com/sraoss/grafana-sunburst-panel



階層が表示可能な円グラフ



デモ



Flunetd
- Apacheアクセスログ
- dstat　性能メトリックス
- PostgerSQLを利用

Zabbix
- 4台の監視ホストを登録
- Linuxテンプレートを適用