報道各位

2017 年 7 月 10 日
株式会社インプレスR&D
http://nextpublishing.jp/

オープンソースの BI ツールで簡単データ分析！

『Elastic Stack で作る BI 環境』発行

アクセスログや機器の動作状況をビジュアル豊かにグラフ化しよう！

インプレスグループで電子出版事業を手がける株式会社インプレス R&D は、『Elastic Stack で作る BI 環境』(著者:石井 葵)を発行いたしました。

『Elastic Stackで作るBI環境』
http://nextpublishing.jp/isbn/9784844397809

著者:石井 葵
小売希望価格:電子書籍版 1200 円(税別)／印刷書籍版 1600 円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様:B5 判／モノクロ／本文 104 ページ
ISBN:978-4-8443-9780-9
発行:インプレス R&D

＜＜内容紹介＞＞

サーバーのアクセスログや Twitter のつぶやき、様々な機器の動作状況など各種のログファイルを Excel で分析していませんか?

本書は OSS で提供されている BI 環境「Elastic Stack」をつかってログファイルを集計し、グラフなどでビジュアル豊かに分析するための環境構築チュートリアルです。《本書籍は、技術系同人誌即売会「技術書典２」で頒布されたものを底本に、加筆修正を行ったものです》

（本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。）

Elastic Stack のインストール方法も詳しく紹介

Elasticsearch のインストール

```
$ sudo yum install elasticsearch
```

RPMパッケージをダウンロードしてインストールする場合

wgetコマンドを用いてパッケージをダウンロードし、rpmコマンドでインストールを行います。明示的にバージョンを指定したい場合、rpmパッケージからインストールすると良いでしょう。

rpm パッケージの取得とインストール

```
# パッケージの取得
$ wget https://artifacts.elastic.co/downloads/elasticsearch/
elasticsearch-5.4.0.rpm
sha1sum elasticsearch-5.4.0.rpm

# Elasticsearchのインストール
$ sudo rpm --install elasticsearch-5.4.0.rpm
```

debパッケージを用いたインストール（Elasticsearch）

インストール用PGP Keyの入手

debパッケージもPGPを用いて暗号化されています。使用にはPGP鍵の入手が必要なため、Elastic社が提供する署名済みの鍵または公開されている署名された鍵をダウンロードします。

PGP 鍵の入手

```
$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch
| sudo apt-key add -
```

APTリポジトリからインストールする場合

はじめに、Elasticsearchの動作に必要なapt-transport-httpsパッケージをインストールします。

必要パッケージのインストール

```
$ sudo apt-get install apt-transport-https
```

次にElastic Stackのaptリポジトリを/etc/apt/sources.list.d/に登録し、apt-getコマンドを用いてインストールします。バージョン指定しない場合、最新版がインストールされます。

リポジトリの登録

```
$ echo "deb https://artifacts.elastic.co/packages/5.x/apt
stable main" | sudo tee -a
/etc/apt/sources.list.d/elastic-5.x.list
```

elasticsearch のインストール

```
$ sudo apt-get update && sudo apt-get install elasticsearch
```

debパッケージをダウンロードしてインストールする場合

wgetコマンドを用いてパッケージをダウンロードし、dpkgコマンドでインストールを行います。明示的にバージョン指定したい場合、dpkgパッケージからインストールすると良いでしょう。

dpkg パッケージの取得とインストール

```
# パッケージの取得
$ wget https://artifacts.elastic.co/downloads/elasticsearch/
elasticsearch-5.4.0.deb
sha1sum elasticsearch-5.4.0.deb
# Elasticsearchのインストール
sudo dpkg -i elasticsearch-5.4.0.deb
```

Elasticsearch起動前の設定項目

どのインストール方法をとった場合でも、事前に設定するべき項目とElasticsearchの起動方法は変わりません。

メモリ使用率の変更

ElasticsearchはJavaで動くアプリなのですが、最大ヒープサイズ（Xms）は物理メモリの50%以下である必要があります。メモリが50%以上を超えてしまう場合、Elasticsearchプロセスが立ち上がりません。ヒープサイズはjvm.optionsで設定します。（rpmパッケージかdebパッケージを用いてインストールした場合、/etc/elasticsearch下に配置されています。）

-Xmsは初期ヒープサイズの設定を行い、-Xmxでは最大ヒープサイズの設定を行います。

サーバの物理メモリが4GBであれば、2GBで設定しておくと良いでしょう。メガバイトを指定する場合は「-Xms512m」と設定します。

Kibana を使ったグラフ化もカラーで紹介

Kibanaを使ったデータの閲覧

「やっとデータが取得できたー！早速Kibanaで見てみよう！…と思ったけれど、グラフはすぐ見えないのかな？画面もいくつかあるみたいだけれど、どれを使えばいいのか分からないよ！」

集めたデータを見る前に、Kibanaを起動しているか確認してください。無事、サービス起動できていれば、Webブラウザから KibanaのURLにアクセスします。まずは各画面の役割を把握しましょう。

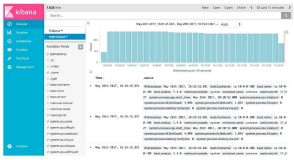
KibanaのUI

Kibana画面は大きく分けて、データを分析する画面とグラフを作って表示する画面で構成されています。後ほど各画面の使用方法を説明しますので、ここでの解説は概要のみに留めています。

Discover：データの詳細を閲覧する

Discoverは、Elasticsearchのindex内に保持されている生データを閲覧できる箇所です。fieldごとに分割されたログの詳細はもちろん、fieldごとのデータのサマリ情報や何時頃そのログが出力されたのか棒グラフを用いて確認することもできます。

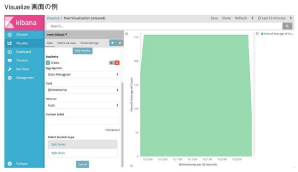
Discover 画面の例



Visualize：データを使ってグラフを作成する

取り込まれたログを使って棒グラフや折れ線グラフを作成できます。グラフは保存できるので、昔作ったグラフを呼び出して参照することが可能です。ちなみに、グラフの設定はElasticsearchの中に保存されます。

Visualize 画面の例



Dashboard:グラフを集めて閲覧する

Visualizeで作成したグラフを一箇所にまとめて参照できます。各グラフの配置・大きさは自由に決定することができます。Googleで「Kibana」を画像検索するとDashboardの画面が多く表示されます。やはりグラフが集まっていると見栄えも良いですよね。

Dashboardに表示されるグラフは、Visualize画面で作成したものを参照します。よってDashboard作成前にグラフを作成しておく必要がありますので注意しましょう。

Dashboard 画面の例

Timelion：関数を定義してグラフを複数描画する

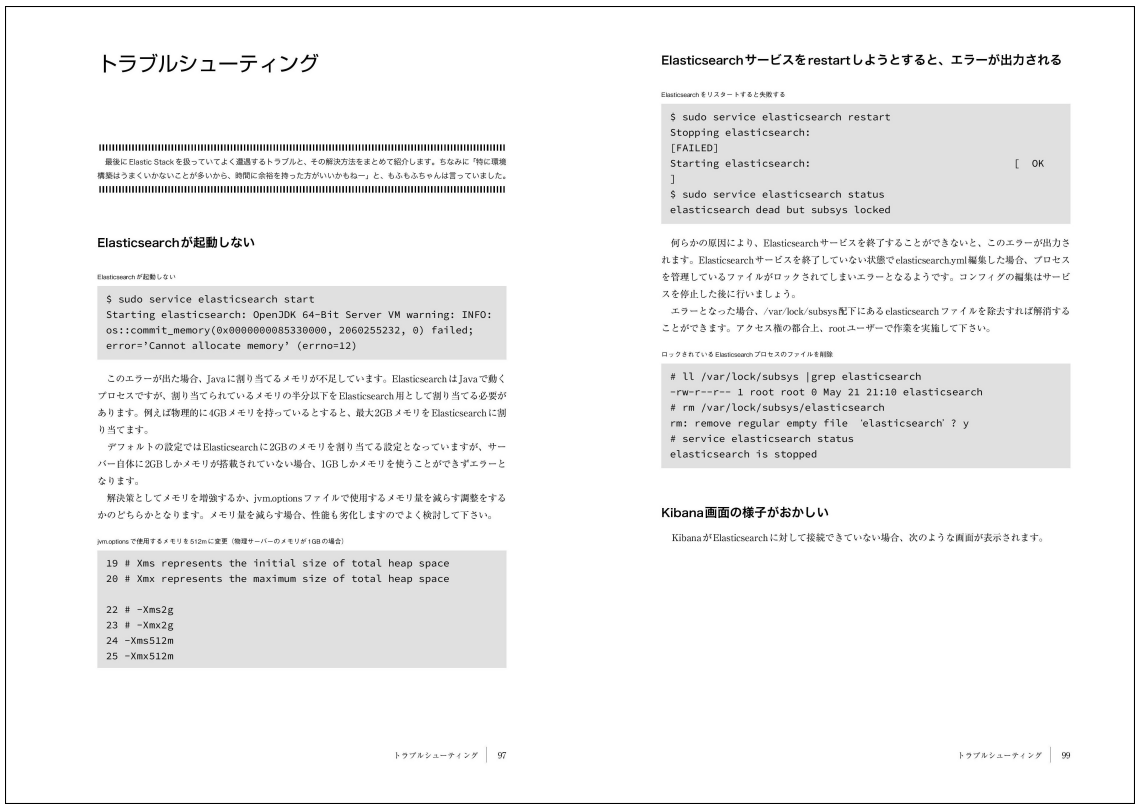
Timelionでは1つのグラフに複数の要素を描画することができます。複数データを比較して分析したい場合、1つの画面で違うデータの種類を閲覧できるTimelionを使用すると便利です。

ただし、設定が難解かつ独自関数を使用しているので、初めて利用する場合はVizualizeの「Visual Builder」グラフを利用して関数の記載方法イメージを掴んでから利用すると良いでしょう。ただし、Visual Builderはバージョン5.4以降からサポートされています。

Dev Tools：Elasticsearch用のクエリをテストする

Dev ToolsのConsoleを使用すると、Kibana画面から直接Elasticsearchに対して検索用クエリ

困った時に役に立つトラブルシューティングも紹介



トラブルシューティング

最後にElastic Stackを扱っていてよく遭遇するトラブルと、その解決方法をまとめて紹介します。ちなみに「特に環境構築はうまくいかないことが多いから、時間に余裕を持った方がいいかもねー」と、もふもふちゃんは言っていました。

Elasticsearchが起動しない

Elasticsearch が起動しない

```
$ sudo service elasticsearch start
Starting elasticsearch: OpenJDK 64-Bit Server VM warning: INFO:
os::commit_memory(0x0000000085330000, 2060255232, 0) failed;
error='Cannot allocate memory' (errno=12)
```

このエラーが出た場合、Javaに割り当てるメモリが不足しています。ElasticsearchはJavaで動くプロセスですが、割り当てられているメモリの半分以下をElasticsearch用として割り当てる必要があります。例えば物理的に4GBメモリを持っているとすると、最大2GBメモリをElasticsearchに割り当てます。

デフォルトの設定ではElasticsearchに2GBのメモリを割り当てる設定となっていますが、サーバー自体に2GBしかメモリが搭載されていない場合、1GBしかメモリを使うことができずエラーとなります。

解決策としてメモリを増強するか、jvm.optionsファイルで使用するメモリ量を減らす調整をするかのどちらかとなります。メモリ量を減らす場合、性能も劣化しますのでよく検討して下さい。

jvm.optionsで使用するメモリを512mに変更（物理サーバーのメモリが1GBの場合）

```
19 # Xms represents the initial size of total heap space
20 # Xmx represents the maximum size of total heap space

22 # -Xms2g
23 # -Xmx2g
24 -Xms512m
25 -Xmx512m
```

トラブルシューティング | 97

Elasticsearchサービスをrestartしようとすると、エラーが出力される

Elasticsearchをリスタートすると失敗する

```
$ sudo service elasticsearch restart
Stopping elasticsearch:
[FAILED]
Starting elasticsearch:                                    [  OK
]
$ sudo service elasticsearch status
elasticsearch dead but subsys locked
```

何らかの原因により、Elasticsearchサービスを終了することができないと、このエラーが出力されます。Elasticsearchサービスを終了していない状態でelasticsearch.yml編集した場合、プロセスを管理しているファイルがロックされてしまいエラーとなるようです。コンフィグの編集はサービスを停止した後に行いましょう。

エラーとなった場合、/var/lock/subsys配下にあるelasticsearchファイルを除去すれば解消することができます。アクセス権の都合上、rootユーザーで作業を実施して下さい。

ロックされているElasticsearchプロセスのファイルを削除

```
# ll /var/lock/subsys |grep elasticsearch
-rw-r--r-- 1 root root 0 May 21 21:10 elasticsearch
# rm /var/lock/subsys/elasticsearch
rm: remove regular empty file `elasticsearch'? y
# service elasticsearch status
elasticsearch is stopped
```

Kibana画面の様子がおかしい

KibanaがElasticsearchに対して接続できていない場合、次のような画面が表示されます。

トラブルシューティング | 99

＜＜目次＞＞

・Elastick Stack って何？
・環境構築
・データを集めて可視化しよう（Twitter のつぶやき履歴編）
・Kibana を使ったデータの閲覧
・データを集めて可視化しよう（Beats を使って情報を集めてみる）・
・Kibana を使ったデータの閲覧
・Visualize 画面でデータを可視化する
・Dashboard 画面を使ってグラフを一覧表示する

＜＜著者紹介＞＞

石井 葵（いしい あおい）
オンプレ環境の方が得意だけど、最近はAWSも勉強中なインフラエンジニア。Elasticsearch,Kibana,Logstashを使用したデータ分析基盤の設計・構築をメインに行なっている。ご飯とお菓子を自分で作って食べるのが最近の趣味。

＜＜販売ストア＞＞

電子書籍:
Amazon Kindle ストア、楽天 kobo イーブックストア、Apple iBookstore、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER
印刷書籍:
Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス
※　各ストアでの販売は準備が整いしだい開始されます。
※　全国の一般書店からもご注文いただけます。

【株式会社インプレス R&D】 http://nextpublishing.jp/

株式会社インプレス R&D（本社：東京都千代田区、代表取締役社長：井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。

※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【インプレスグループ】 http://www.impressholdings.com/

株式会社インプレスホールディングス(本社: 東京都千代田区、代表取締役: 唐島夏生、証券コード: 東証 1 部 9479)を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「モバイルサービス」を主要テーマに専門性の高いコンテンツ＋サービスを提供するメディア事業を展開しています。2017 年 4 月 1 日に創設 25 周年を迎えました。

【お問い合わせ先】

株式会社インプレス R&D NextPublishing センター
〒101-0051　東京都千代田区神田神保町 1-105
TEL 03-6837-4820
電子メール: np-info@impress.co.jp