報道各位

2018年6月11日
株式会社インプレスR&D
https://nextpublishing.jp/

最新バージョン6に対応した解説書！

『Introduction of Elastic Stack 6 これからはじめるデータ収集＆分析』発行

技術書典シリーズ最新刊！ 技術書典4からの書籍化第一弾

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、『Introduction of Elastic Stack 6 これからはじめるデータ収集&分析』(著者:石井 葵、前原 応光、須田 桂伍)を発行いたします。

『Introduction of Elastic Stack 6 これからはじめるデータ収集＆分析』
https://nextpublishing.jp/isbn/9784844398295

著者:石井 葵,前原 応光,須田 桂伍
小売希望価格:電子書籍版 1800円(税別)／印刷書籍版 2200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／カラー／本文172ページ
ISBN:978-4- 8443-9829-5
発行:インプレスR&D

＜＜発行主旨・内容紹介＞＞

【Elastic Stack 最新バージョン対応ガイドブック！】

本書はBIツールとしての活用が進むElastic Stackの最新バージョンであるElastic Stack 6の概要と、周辺ツールの紹介を行い実務に活かすためのチュートリアルです。

ユースケースを交えながら各プロダクトの機能解説を行います。

(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。)

AWS での Logstash 活用を詳しく解説

第3章　AWSでLogstashを使ってみる

AWSを利用してWebサイトを運営しているとき、ELBのアクセスログを用いてアクセス元の国やUserAgentを知りたくなることがあるかもしれません。しかし、これらの情報の中にはCloudWatchではモニタリングできないものがあります。

でも大丈夫です！ELBはログを出力しているので、そのログを何らかの形で取得し可視化すればよいのです！ちなみに、今回はALB（Application loadbalancer）からデータを取得します。

この章で目指すことは次の2点です。

・ALB（AWSのアプリケーションロードバランサ）のログをLogstashからElasticsearchに保存する
・Elasticsearchに保存したログをKibanaでビジュアライズできるようになる

3.1　実行環境を準備する

Logstashの使い方を知る前に、実行環境を整える必要があります。サーバーはAWSのEC2を利用し、OSはAmazonLinuxで構築していきます。インスタンスタイプは、稼働に最低限必要なリソースのものを選択しています。OSによって発行するコマンドが変わってくるので、詳しくは公式HPを確認してください。

・Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-97785bed
・t2.medium(vCPU: 2,Mem: 4)

今回導入するミドルウェアのバージョンは次のとおりです。

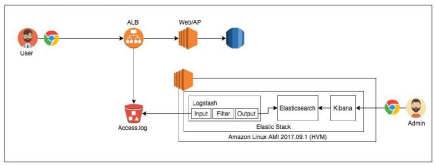
・Elasticsearch 6.2.2
・Logstash 6.2.2
・Kibana 6.2.2
・Metricbeat 6.2.2
・Auditbeat 6.2.2
・Packetbeat 6.2.2

各プロダクトはこちらのリンク（https://www.elastic.co/jp/products）からダウンロードすることが可能です。

3.1.1　想定される環境

ユーザーがWebサイトにアクセスした際に、ALBで出力したアクセスログをS3に保存します。S3に保存されたアクセスログを、Logstashが定期的に取得する構成です。

図3.1: 本章で想定している環境構成



3.1.2　ALBのログを準備する

ALBのログを出力するために、ALB自体のロギングの設定を有効化する必要があります。これにより、ALBのログをS3のバケットに出力できます。

ALB自体のロギング設定・S3バケットの設定方法については本文では解説しません。AWSの公式ドキュメントなどを参考に設定してください。

3.2　ミドルウェアのインストール

次の順番で必要なミドルウェアをインストールします。

1．Java（バージョン8）
2．Elasticsearch
3．Logstash
4．Kibana

3.2.1　Java 8のインストール

Elasticsearch、Logstashの動作にはJava（バージョン8）が必要です。まずは、Javaがインストールされているかを確認します。またインストールされている場合は、Javaのバージョンを確認します。

リスト3.1: Javaのバージョンを確認する

```
java -version
```

AmazonLinuxの場合、Javaが最初からインストールされています。ただしバージョンが7のため、Java 8を新しくインストールする必要があります。

Kibana を使ったデータの可視化について画面遷移を交えて紹介

8.4　Kibanaを使ってGitのコミット状況を閲覧する

では、早速Gitのコミットログ（以降git logとします）をグラフにしていきましょう。まずはKibana（http://localhost:5601）にアクセスします。`kibana.yml`でURLを変更していた場合、自分で設定したURLへアクセスしてください。

アクセスすると、図8.1が見えていますね。まずは画面左端にある歯車アイコンを押して`Management`画面を開きましょう。

8.4.1　利用するindexの設定を行う

Elasticsearchは`index`にデータを保存しています。Kibanaでグラフを作るときに、どの`index`を参照すればよいかはじめに設定する必要があります。

図8.2: Kibanaが参照するindexを設定する

画面下側にindexの名前が出てきます。コピー&ペーストで`Index pattern`にindex名を入れてしまいましょう。index名の指定をするときは、`*`（アスタリスク）を利用することができます。たとえば`logstash-*`と設定すれば`logstash-`で始まるindexを全て参照することができます。

デフォルトでは、Logstashからデータを Elasticsearchに連携するときに`logstash-`日付としてindexを作成します。なので、Logstash側でindexを指定していない場合、`logstash-*`をKibanaから参照するようにしておけば問題ありません。

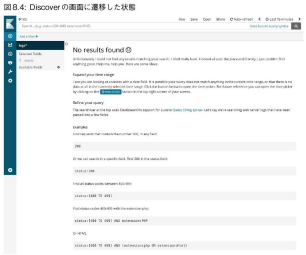
次に、どのfieldを時刻として参照するか設定します。

図8.3: どのfieldを時刻として参照するか設定する

`@timestamp`を選択すると、Logstashがデータを Elasticsearchに連携した時刻を基準としてデータを閲覧することになります。今回はいつGitにコミットが作成されたかを閲覧したいので、`author_date`を時刻として参照するようにします。

8.5　Discoverでgit logの様子を観察する

図8.4: Discoverの画面に遷移した状態



画面左端にあるコンパスのアイコンを押すと、`Discover`の画面に遷移します。`Discover`ではElasticsearchに保存されているデータを直接参照することが可能です。画面上部のグラフは、いつ・どのくらいのデータがElasticsearchに保存されたかを示しています。ここで先ほどindexの設定時に指定した時刻を利用します。

画面右上の時計マークでは、表示するデータの期間を指定しています。たとえば図8.4では、時刻が`Last 15 minutes`と設定されています。この場合、**今の時刻から**15分前までにコミットがあったデータ（＝`author_date`の時刻が現在から15分前のもの）を閲覧する状態となっています。

条件に当てはまるデータが存在しない場合、図8.4のようにデータが存在しないことを示す画面が表示されます。この場合、時計マークをクリックして時刻の範囲を変更しましょう。時刻を広めにとると何かしらのデータが表示されるはずです。それでもダメであれば、Elasticsearchにデータが保存されていない可能性があります。データの連係がきちんとできているかもう一度見直しましょう。

バージョン 6 で新しくなった Kibana の特徴と機能を解説

・Kubernetesのメトリクス
・MySQLのログ
・MySQLのメトリクス
・Netflow
・Nginxのログ
・Nginxのメトリクス
・Redisのログ
・Redisのメトリクス
・システムログ
・システムのメトリクス

Netflowは Cisco 社が開発したネットワークトラフィックの詳細情報を収集するための技術です。RedisはNoSQLデータベースの1種です。

Webサービスは性能が命ですから、性能やサービス監視の構築に手間をかけたくはありません。Modulesを利用すれば、監視環境の構築コストを下げることができます。

9.3 Visualizeの種類が増加

Visualizeを利用すると、自分でグラフを作成できるというのはこれまでの章で紹介したとおりです。このVisualizeがデフォルトで利用できるグラフが増えました。

Kibana5.4から増えたグラフは次のとおりです。

・Goal
・Coordinate Map
・Region Map
・Controls
・Vega

この中でも異彩を放つVegaについてここでは取り上げたいと思います。

9.3.1 Vega

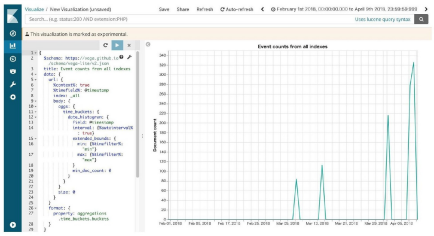
Vega（https://vega.github.io/vega/）は、The UW Interactive Data Lab（http://idl.cs.washington.edu/about）が作成・開発している、データをグラフに描画するためのツールです。

Kibanaと同じなのでは？と思う方もいるかもしれませんが、Vegaはデータ・グラフを描画するための設定をJSONで管理します。一方、Kibanaはグラフ描画に利用するデータはElasticsearchから取得しますし、グラフの描画はGUIを用いて行います。

また、Vegaで描画できるグラフの種類（https://vega.github.io/vega/examples/）はKibanaよりも多いです。特にデータ分析を行う場合に利用することが多い棒線グラフに標準偏差を記述することが可能です。

しかし、せっかくElasticsearchに投入されているデータが大量にあるのですから、それをより詳しく分析したいですよね。ということで、ベータ版ではありますがKibanaのGUIからVegaの機能を呼び出して利用できるようになりました。それがVisualize画面のVegaです。

図 9.1: Vega



このグラフはベータ版なので開発が中止される可能性があります。よって、本番環境でVegaを利用することは推奨できません。

9.4 何気に嬉しい便利機能

これから紹介する機能を知っていると、よりKibanaを便利に利用できるかもしれません。

9.4.1 Dev Toolsの入力補完

「Goではじめる Elasticsearch」の章ではコンソール上で直接ElasticsearchにQueryを発行していました。しかし、KibanaのGUIにはDev Toolsという画面があります。これがすばらしいのです。

＜＜目次＞＞

＜＜著者紹介＞＞

石井葵

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うインフラエンジニアだったが、最近配属が変わって新卒なエンジニアの教育を実施している。新卒エンジニアと一緒にプログラミングやアプリケーション開発手法を学ぶ日々を過ごしている。

前原応光
AWS/GCP などの大規模なクラウドの導入/プラットフォーム構築に従事。サービスのセキュリティ強化のコンサルを実施すると共に、Logstash/Elasticsearch/Kibana を用いての SIEM 導入/開発を行なっている。

須田桂伍
Hadoop/Spark/Kafka/Elasticsearch をはじめとするビッグデータを支える OSS プロダクトの案件導入/開発に従事。Elasticsearch を用いた記事検索システムや、Kafka によるデータ収集基盤の構築といったデータ分析基盤の導入/開発だけでなく、基幹領域での業務バッチ処理への Hadoop/Spark 導入など、ミッションクリティカルな領域でのプロダクト活用にも注力。

＜＜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】 https://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】 https://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。

【お問い合わせ先】
株式会社インプレス R&D NextPublishing センター
TEL 03-6837-4820
電子メール: np-info@impress.co.jp