

ELKではじめる お手軽Flowコレクター

ELK = Elasticsearch + Logstash + Kibana

2015/9/4 ENOG34

(株) 創風システム

外山 文規

ELKってなんぞや

▶ E = Elasticsearch

全文検索エンジン、json形式でデータを追加

▶ L = Logstash

ログを集めたりパースして、任意のDBやファイル等に出カ
fluentdのようなもの

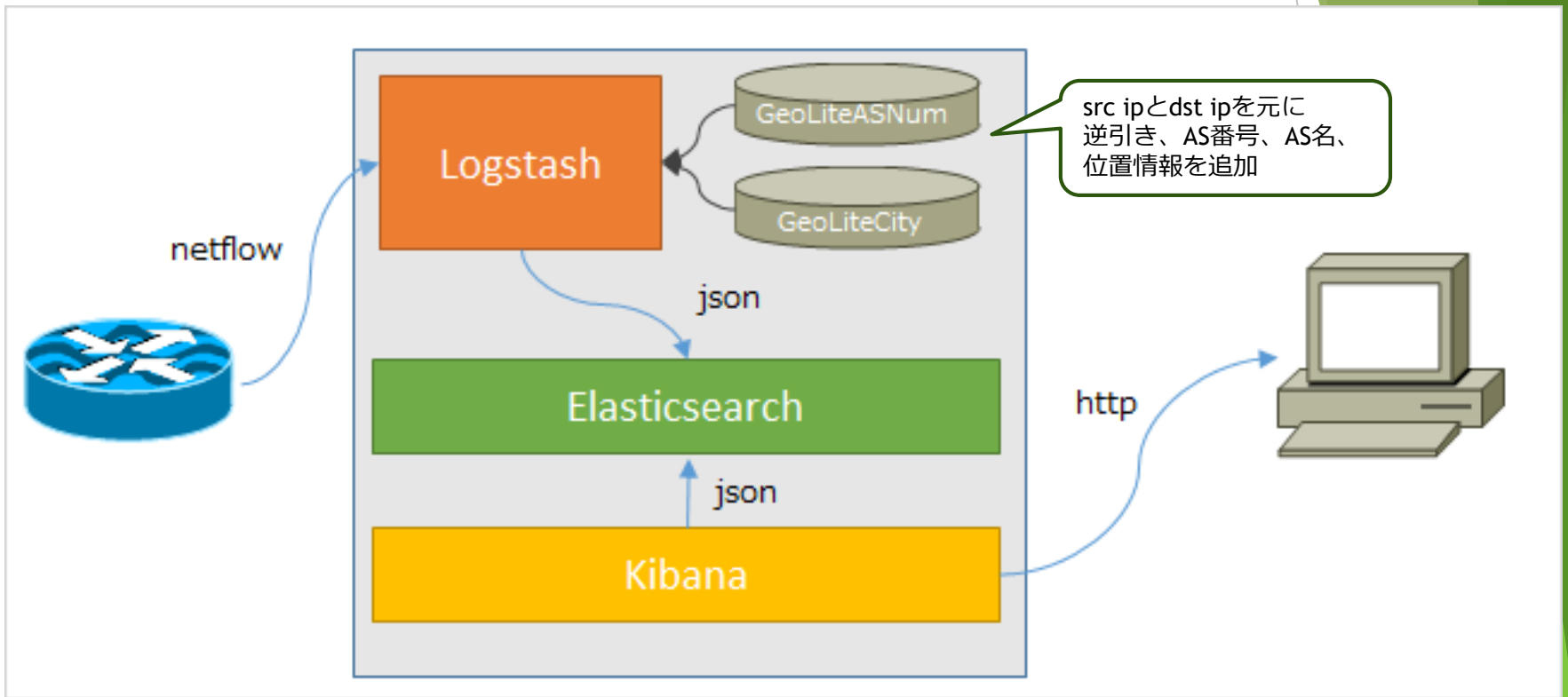
▶ K = Kibana

ログデータの可視化ツール、Elasticsearchのフロントエンド
検索、グラフ化できる

NetflowがKibanaで可視化できたら
カッコいいかも

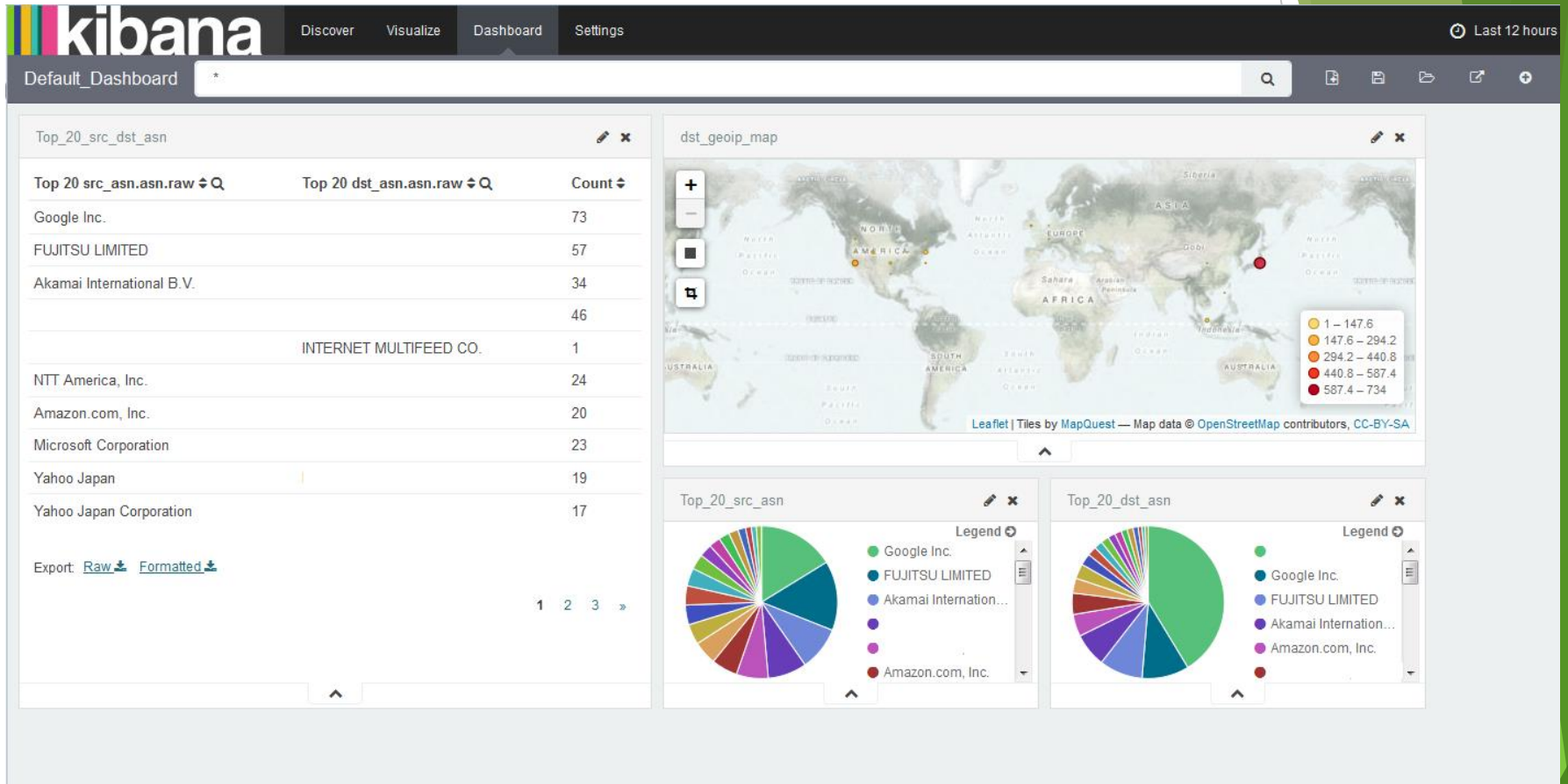
今回の環境

- ▶ CentOS 7
- ▶ Elasticsearch 1.6
- ▶ Logstash 1.5
- ▶ Kibana 4.1

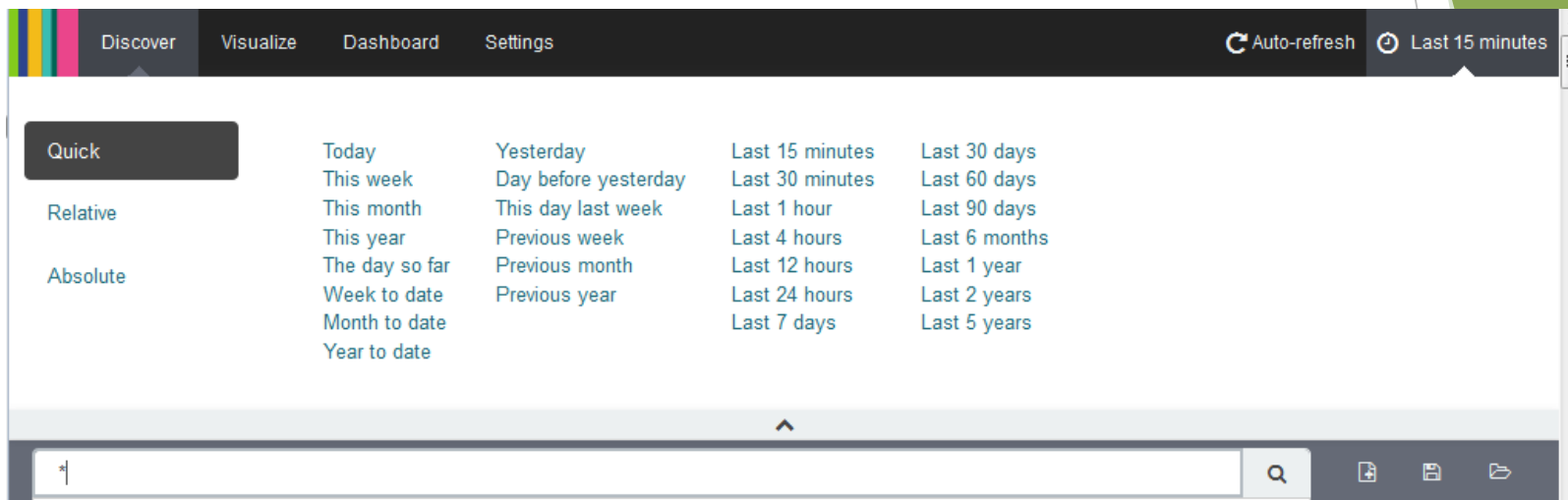


Netflowのデータにあるsrc_ipとdst_ipを元にmaxmindのGeoLiteASNum、GeoLiteCityを使って、AS情報と位置情報を付加しました。

ダッシュボード作成例



日時により指定できる フィルタ項目1



日時により指定できる フィルタ項目2

The screenshot displays a web application interface with a dark navigation bar at the top. The navigation bar contains the following elements from left to right: a multi-colored vertical bar, the text 'Discover', 'Visualize', 'Dashboard', and 'Settings', and two utility icons: 'Auto-refresh' and 'Last 15 minutes'. Below the navigation bar, the main content area is divided into sections. On the left, there is a 'Quick' section with two buttons: 'Relative' (which is highlighted in dark grey) and 'Absolute'. To the right of these buttons, the 'From' field is set to 'August 27th 2015, 14:20:53.435'. Below this, there is a numeric input field containing '15', a small square icon, and a dropdown menu currently showing 'Days ago'. A checkbox labeled 'round to the day' is positioned below the 'Days ago' dropdown. To the right of these fields, the 'To' field is set to 'Now', followed by a 'Go' button. At the bottom of the interface, there is a search bar containing an asterisk, a search icon, and three additional icons for document, folder, and share.

日時により指定できる フィルタ項目3

The screenshot shows a web application interface with a dark navigation bar at the top. The navigation bar contains the following elements from left to right: a colorful vertical bar, the text 'Discover', 'Visualize', 'Dashboard', and 'Settings', a refresh icon with the text 'Auto-refresh', and a clock icon with the text 'Last 15 minutes'.

Below the navigation bar, there is a main content area. On the left side of this area, there are three filter options: 'Quick', 'Relative', and 'Absolute'. The 'Absolute' option is currently selected and highlighted with a dark background.

In the center of the main content area, there are two date and time selection fields. The first field is labeled 'From:' and contains the text '2015-09-04 14:06:45.700'. Below this text is the format 'YYYY-MM-DD HH:mm:ss.SSS'. The second field is labeled 'To:' and contains the text '2015-09-04 18:21:45.700'. Below this text is the format 'YYYY-MM-DD HH:mm:ss.SSS'. To the right of these two fields is a dark button labeled 'Go'.

Below the 'From:' and 'To:' fields, there are two calendar views for the month of September 2015. Each calendar view shows the days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat) and the dates. The date '04' (September 4th) is highlighted in a dark blue box in both calendars.

At the bottom of the main content area, there is a search bar with a magnifying glass icon and a search button. To the right of the search bar are three icons: a plus sign, a document, and a share icon.

Elasticsearchのインストール

以下のURLを参考にして `yum install` で完了

https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-repositories.html#_yum

Elasticsearchの確認

```
# curl -X GET http://localhost:9200/
```

以下が返ってくる

```
{  
  "status" : 200,  
  "name" : "Magnus",  
  "cluster_name" : "elasticsearch",  
  "version" : {  
    "number" : "1.6.0",  
    "build_hash" : "cdd3ac4dde4f69524ec0a14de3828cb95bbb86d0",  
    "build_timestamp" : "2015-06-09T13:36:34Z",  
    "build_snapshot" : false,  
    "lucene_version" : "4.10.4"  
  },  
  "tagline" : "You Know, for Search"  
}
```

Logstashのインストール

以下のURLを参考にして yum
install で完了

https://www.elastic.co/guide/en/logstash/current/package-repositories.html#_yum

Logstashの設定 1 (netflowを受け取る)

※/etc/logstash/conf.d/ の下に ○○.conf で作成する
Netflowの packets 取得するための設定

```
input {  
  udp {  
    port => 2055  
    codec => netflow {  
      versions => [5]  
    }  
  }  
}
```

Logstashの設定 2 (逆引き情報追加の準備)

※/etc/logstash/conf.d/ の下に ○○.conf で作成する
Netflowのデータをもとに、geoip、ASN、逆引き情報を追加

```
filter {  
  mutate {  
    add_field => [ "[netflow][ipv4_dst_host]", "%{[netflow][ipv4_dst_addr]}" ]  
    add_field => [ "[netflow][ipv4_src_host]", "%{[netflow][ipv4_src_addr]}" ]  
  }  
}
```

※逆引き情報のために、IPアドレス情報をコピー

Logstashの設定 3 (src, dstのIPから逆引き情報追加)

```
dns {  
  action => 'replace'  
  reverse => "[netflow][ipv4_dst_host]"  
}  
dns {  
  action => 'replace'  
  reverse => "[netflow][ipv4_src_host]"  
}  
}
```

※先ほどコピーしたフィールドを逆引き情報に置換

Logstashの設定 4 (src,dstのIPから位置情報追加)

```
geoip {  
  database => "/usr/share/GeoIP/GeoLiteCity.dat"  
  source => "[netflow][ipv4_dst_addr]"  
  target => "dst_geoip"  
}  
  
geoip {  
  database => "/usr/share/GeoIP/GeoLiteCity.dat"  
  source => "[netflow][ipv4_src_addr]"  
  target => "src_geoip"  
}
```

※IPアドレスを元に位置情報を追加

Logstashの設定 5 (AS番号、AS名を追加)

```
geoip {  
  database => "/usr/share/GeoIP/GeoLiteASNum.dat"  
  source => "[netflow][ipv4_dst_addr]"  
  target => "dst_asn"  
}  
  
geoip {  
  database => "/usr/share/GeoIP/GeoLiteASNum.dat"  
  source => "[netflow][ipv4_src_addr]"  
  target => "src_asn"  
}
```

※IPアドレスをもとにASN情報を追加

Logstashの設定 6 (elasticsearchにデータ投げる)

加工した結果をelasticsearchに投げる

```
output {  
  elasticsearch {  
    index => "logstash-%{+YYYY.MM.dd}"  
    host => "localhost"  
  }  
}
```

位置情報はElasticsearchの
templateを修正しないと、正し
く位置情報として扱えません。

elasticsearchのtemplateの修正

※dst_geoipのテンプレートを設定

```
"dst_geoip" : {  
  "type" : "object",  
  "dynamic": true,  
  "properties" : {  
    "location": {  
      "geohash": true,  
      "geohash_precision": 10,  
      "geohash_prefix": true,  
      "lat_lon": true,  
      "type": "geo_point"  
    }  
  }  
},
```

elasticsearchのtemplateの修正

※src_geopipのテンプレートを設定

```
“src_geopip” : {  
  “type” : “object”,  
  “dynamic”: true,  
  “properties” : {  
    “location”: {  
      “geohash”: true,  
      “geohash_precision”: 10,  
      “geohash_prefix”: true,  
      “lat_lon”: true,  
      “type”: “geo_point”  
    }  
  }  
},
```

GeoIPのインストール設定、

```
# yum install GeoIP GeoIP-update -y
```

```
# vi /etc/GeoIP.conf
```

```
ProductIds 506 533
```

↓に変更

```
ProductIds GeoLite2-City GeoLite2-Country GeoLite-Legacy-IPv6-  
City GeoLite-Legacy-IPv6-Country 506 517 533
```

```
# geoipupdate
```

参考:

<http://dev.maxmind.com/geoip/geoipupdate/>

Logstashの確認

```
# curl -X GET http://localhost:9200/_cat/shards
```

```
logstash-2015.07.29 0 p STARTED 251554 127.3mb  
210.236.208.14 Karolina Dean
```


kibanaのインストール

```
# wget https://download.elastic.co/kibana/kibana/kibana-4.1.0-linux-x64.tar.gz
```

```
# tar -zxvf kibana-4.1.0-linux-x64.tar.gz
```

```
# mkdir -p /opt/kibana
```

```
# cp -vR kibana-4.1.0-linux-x64/* /opt/kibana/
```

kibanaのインストール

```
# vi /etc/systemd/system/kibana4.service
```

```
[Service]
```

```
ExecStart=/opt/kibana/bin/kibana
```

```
Restart=always
```

```
StandardOutput=syslog
```

```
StandardError=syslog
```

```
SyslogIdentifier=kibana4
```

```
User=root
```

```
Group=root
```

```
Environment=NODE_ENV=production
```

```
[Install]
```

```
WantedBy=multi-user.target
```

flow数が多かったり、貯める
データ数が多い場合は、シンプ
ルな構成では収まらないのでク
ラスタを組むなど対策が必要

参考情報

Blog:

Netflowコレクターを無償のFluend + ElasticSearch + Kibanaで構築する
<http://komeiy.hatenablog.com/entry/2014/09/26/212000>

Step-by-Step Setup of ELK for NetFlow Analytics

<http://blogs.cisco.com/security/step-by-step-setup-of-elk-for-netflow-analytics>

How To Install Elasticsearch, Logstash, and Kibana 4 on CentOS 7

<https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-4-on-centos-7>

書籍:

サーバ/インフラエンジニア養成読本 ログ収集~可視化編
(Software Design plus)